Mémoire
Sur les conditions de résolubilité des équations par radicaux.
Évariste Galois

Le Mémoire ci-joint[1] est extrait d'un ouvrage que j'ai eu l'honneur de présenter à l'Académie il y a un an. Cet ouvrage n'ayant pas été compris, les propositions qu'il renferme ayant été révoquées en doute, j'ai dû me contenter de donner, sous forme synthétique, les principes généraux, et une *seule* application de ma théorie. Je supplie mes juges de lire du moins avec attention ce peu de pages.

On trouvera ici une *condition générale* à laquelle *satisfait toute équation soluble par radicaux*, et qui réciproquement assure leur résolubilité. On en fait l'application seulement aux équations dont le degré est un nombre premier. Voici le théorème donné par notre analyse :

"Pour qu'une équation de degré premier, qui n'a pas de diviseurs commensurables, soit soluble par radicaux, il *faut* et il *suffit* que toutes les racines soient des fonctions rationnelles de deux quelconques d'entre elles."

Les autres applications de la théorie sont elles-mêmes autant de théories particulières. Elles nécessitent d'ailleurs l'emploi de la théorie des nombres, et d'un algorithme particulier : nous les réservons pour une autre occasion. Elles sont en partie relatives aux équations modulaires de la théorie des fonctions elliptiques, que nous démontrons ne pouvoir se résoudre par radicaux.

Ce 16 janvier 1831.

E. Galois.

Principes.

Je commencerai par établir quelques définitions et une suite de lemmes qui sont tous connus.

Définitions. Une équation est dite réductible quand elle admet des diviseurs rationnels ; irréductible dans le cas contraire.

Il faut ici expliquer ce qu'on doit entendre par le mot *rationnel*, car il se représentera souvent.

Quand l'équation a *tous* ses coefficients numériques et rationnels, cela veut dire simplement que l'équation peut se décomposer en facteurs qui aient leurs coefficients numériques et rationnels.

Mais quand les coefficients d'une équation ne seront pas *tous* numériques et rationnels, alors il faudra entendre par diviseur rationnel un diviseur dont les coefficients s'exprimeraient en fonction rationnelle des coefficients de la proposée, en général par quantité rationnelle, une quantité qui

http://www.bibnum.education.fr/sites/default/files/galois_memoire_sur_la_resolubiblite.pdf.

[1] J'ai jugé convenable de placer en tête de ce Mémoire la préface qu'on va lire, bien que je l'aie trouvée biffée dans le manuscrit.

A. Ch.

s'exprime en fonction rationnelle des coefficients de la proposée.

Il y a plus : on pourra convenir de regarder comme rationnelle toute fonction rationnelle d'un certain nombre de quantités déterminées, supposées connues a priori. Par exemple, on pourra choisir une certaine racine d'un nombre entier, et regarder comme rationnelle toute fonction rationnelle de ce radical.

Lorsque nous conviendrons de regarder ainsi comme connues de certaines quantités, nous dirons que nous les *adjoignons* à l'équation qu'il s'agit de résoudre. Nous dirons que ces quantités sont *adjointes* à l'équation.

Cela posé, nous appellerons rationnelle toute quantité qui s'exprimera en fonction rationnelle des coefficients de l'équation et d'un certain nombre de quantités *adjointes* à l'équation et convenues arbitrairement.

Quand nous nous servirons d'équations auxiliaires, elles seront rationnelles, si leurs coefficients sont rationnels en notre sens.

On voit, au surplus, que les propriétés et les difficultés d'une équation peuvent être tout à fait différentes suivant les quantités qui lui sont adjointes. Par exemple, l'adjonction d'une quantité peut rendre réductible une équation irréductible.

Ainsi, quand on adjoint à l'équation

$$\frac{x^n - 1}{x - 1} = 0, \qquad \text{où } n \text{ est premier,}$$

une racine d'une des équations auxiliaires de M. Gauss, cette équation se décompose en facteurs, et devient par conséquent réductible.

Les substitutions sont le passage d'une permutation à l'autre.

La permutation d'où l'on part pour indiquer les substitutions est toute arbitraire, quand il s'agit de fonctions ; car il n'y a aucune raison pour que, dans une fonction de plusieurs lettres, une lettre occupe un rang plutôt qu'un autre.

Cependant, comme on ne peut guère se former l'idée d'une substitution sans se former celle d'une permutation, nous ferons dans le langage un emploi fréquent des permutations, et nous ne considèrerons les substitutions que comme le passage d'une permutation à une autre.

Quand nous voudrons grouper des substitutions, nous les ferons toutes provenir d'une même permutation.

Comme il s'agit toujours de questions où la disposition primitive des lettres n'influe en rien dans les groupes que nous considèrerons, on devra avoir les mêmes substitutions, quelle que soit la permutation d'où l'on sera parti. Donc, si dans un pareil groupe on a les substitutions S et T, on est

sûr d'avoir la substitution ST.

Telles sont les définitions que nous avons cru devoir rappeler.

Lemme I. "Une équation irréductible ne peut avoir aucune racine commune avec une équation rationnelle, sans la diviser."

Car le plus grand commun diviseur entre l'équation irréductible et l'autre équation, sera encore rationnel ; donc, etc.

Lemme II. "Étant donnée une équation quelconque, qui n'a pas de racines égales, dont les racines sont $a, b, c, ...$, on peut toujours former une fonction V des racines, telle qu'aucune des valeurs que l'on obtient en permutant dans cette fonction les racines de toutes manières, ne soient égales."
Par exemple, on peut prendre

$$V = Aa + Bb + Cc + ..$$

A, B, C étant des nombres entiers convenablement choisis.

Lemme III. "La fonction V étant choisie comme il est indiqué dans l'article précédent, elle jouira de cette propriété, que toutes les racines de l'équation proposée s'exprimeront rationnellement en fonction de V."

En effet, soit

$$V = \varphi(a, b, c, d, ...),$$

ou bien

$$V - \varphi(a, b, c, d, ...) = 0.$$

Multiplions entre elles toutes les équations semblables, que l'on obtient en permutant dans celles-ci toutes les lettres, la première seulement restant fixe ; il viendra une expression suivante :

$$[V - \varphi(a, b, c, d, ...)][V - \varphi(a, c, b, d, ...)][V - \varphi(a, b, d, c, ...]...,$$

symétrique en $b, c, d, ...$, laquelle pourra par conséquent s'écrire en fonction de a. Nous aurons donc une équation de la forme

$$F(V, a) = 0.$$

Or je dis que de là on peut tirer la valeur de a. Il suffit pour cela de chercher la solution commune à cette équation et à la proposée. Cette solution est la seule commune, car on ne peut avoir, par exemple,

$$F(V, b) = 0,$$

cette équation ayant un facteur commun avec l'équation semblable, sans quoi l'une des fonctions $\varphi(a, ...)$ serait égale à l'une des fonctions $\varphi(b, ...)$; ce qui est contre l'hypothèse.

Il suit de là que a s'exprime en fonction rationnelle de V, et il en est de même des autres racines.

Cette proposition[2] est citée sans démonstration par Abel, dans le Mémoire posthume sur les fonctions elliptiques.

Lemme IV. "Supposons que l'on ait formé l'équation en V, et que l'on ait pris l'un de ses facteurs irréductibles, en sorte que V soit racine d'une équation irréductible. Soient $V, V', V'', ...$ les racines de cette équation irréductible. Si $a = f(V)$ est une des racines de la proposée, $f(V')$ de même sera une racine de la proposée."

En effet, en multipliant entre eux tous les facteurs de la forme $V - \varphi(a, b, c, ..., d)$, où l'on aura opéré sur les lettres toutes les permutations possibles, on aura une équation rationnelle en V, laquelle se trouvera nécessairement divisible par l'équation en question ; donc V' doit s'obtenir par l'échange des lettres dans la fonction V. Soit $F(V, a) = 0$ l'équation qu'on obtient en permutant dans V toutes les lettres, hors la première. On aura donc $F(V', b) = 0$, b pouvant être égal à a, mais étant certainement l'une des racines de l'équation proposée ; par conséquent, de même que de la proposée et de $F(V, a) = 0$ est résulté $a = f(V)$, de même il résultera de la proposée et de $F(V', b) = 0$ combinées, la suivante $b = f(V')$.

Proposition i.

Théorème. "Soit une équation donnée, dont $a, b, c, ...$ sont les m racines. Il y aura toujours un groupe de permutations des lettres $a, b, c,...$ qui jouira de la propriété suivante :

1°. Que toute fonction des racines, invariable[3] par les substitutions de ce groupe, soit rationnellement connue ;

2°. Réciproquement, que toute fonction des racines, déterminable rationnellement, soit invariable par les substitutions."

(Dans le cas des équations algébriques, ce groupe n'est autre chose que l'ensemble des 1.2.3....m permutations possibles sur les m lettres, puisque, dans ce cas, les fonctions symétriques sont seules déterminables rationnellement.)

(Dans le cas de l'équation $\dfrac{x^n - 1}{x - 1} = 0$, si l'on suppose $a = r, b = r^g, c = r^{g^2}, ..., g$ étant une racine

[2]Il est remarquable, que de cette proposition on peut conclure que toute équation dépend d'une équation auxiliaire telle que toutes les racines de cette nouvelle équation soient des fonctions rationnelles les unes des autres ; car l'équation auxiliaire en V est dans ce cas.
Au surplus, cette remarque est purement curieuse. En effet, une équation qui a cette propriété n'est pas, en général, plus facile à résoudre qu'une autre.

[3]Nous appelons ici invariable non-seulement une fonction dont la forme est invariable par les substitutions des racines entre elles, mais encore celle dont la valeur numérique ne varierait pas par ces substitutions. Par exemple, si $Fx = 0$ est une équation, Fa est une fonction des racines qui ne varie par aucune permutation.
Quand nous disons qu'une fonction est rationnellement connue, nous voulons dire que sa valeur numérique est exprimable en fonction rationnelle des coefficients de l'équation et des quantités adjointes.

primitive, le groupe de permutations sera simplement celui-ci :

$$\begin{array}{l} abcd\ldots k \\ bcd\ldots ka \\ cd\ldots kab \\ \ldots \\ kabc\ldots i\ ; \end{array}$$

dans ce cas particulier, le nombre des permutations est égal au degré de l'équation, et la même chose aurait lieu dans les équations dont toutes les racines seraient des fonctions rationnelles les unes des autres.)

Démonstration. Quelle que soit l'équation donnée, on pourra trouver une fonction rationnelle V des racines, telle que toutes les racines soient fonctions rationnelles de V. Cela posé, considérons l'équation irréductible dont V est racine (lemmes III et IV). Soient $V, V', V'', ..., V^{n-1}$ les racines de cette équation.

Soient $\varphi V, \varphi_1 V, \varphi_2 V \ldots., \varphi_{m-1} V$ les racines de la proposée.

Écrivons les n permutations suivantes des racines

$$\begin{array}{l|llll} (V) & \varphi V, & \varphi_1 V, & \varphi_2 V, & \ldots\ \varphi_{m-1} V, \\ (V') & \varphi V', & \varphi_1 V', & \varphi_2 V', & \ldots\ \varphi_{m-1} V', \\ (V'') & \varphi V'', & \varphi_1 V'', & \varphi_2 V'', & \ldots\ \varphi_{m-1} V'', \\ \ldots & & & & \\ (V^{(n-1)}) & \varphi V^{(n-1)}, & \varphi_1 V^{(n-1)}, & \varphi_2 V^{(n-1)}, & \ldots\ \varphi_{m-1} V^{(n-1)}\ : \end{array}$$

je dis que ce groupe de permutations jouit de la propriété énoncée.

En effet,

1°. toute fonction F des racines, invariable par les substitutions de ce groupe, pourra être écrite ainsi : $F = \psi V$, et l'on aura

$$\psi V = \psi V' = \psi V'' = \ldots = \psi V^{(n-1)}.$$

La valeur de F pourra donc se déterminer rationnellement.

2°. *Réciproquement.* Si une fonction F est déterminable rationnellement, et que l'on pose $F = \psi V$, on devra avoir

$$\psi V = \psi V' = \psi V'' = \ldots = \psi V^{(n-1)},$$

puisque l'équation en V n'a pas de diviseur commensurable et que V satisfait à l'équation $F = \psi V$, F étant une quantité rationnelle. Donc la fonction F sera nécessairement invariable par les substitutions du groupe écrit ci-dessus.

Ainsi, ce groupe jouit de la double propriété dont il s'agit dans le théorème proposé. Le théorème est donc démontré.

Nous appellerons groupe de l'équation le groupe en question.

Scolie 1. Il est évident que dans le groupe de permutations dont il s'agit ici, la disposition des lettres n'est point à considérer, mais seulement les substitutions de lettres par lesquelles on passe d'une permutation à l'autre.

Ainsi l'on peut se donner arbitrairement une première permutation, pourvu que les autres permutations s'en déduisent toujours par les mêmes substitutions de lettres. Le nouveau groupe ainsi formé jouira évidemment des mêmes propriétés que le premier, puisque dans le théorème précédent, il ne s'agit que des substitutions que l'on peut faire dans les fonctions.

Scolie 2. Les substitutions sont indépendantes même du nombre des racines.

Proposition ii.

Théorème[4]. "Si l'on adjoint à une équation donnée la racine r d'une équation auxiliaire irréductible,

1°. il arrivera de deux choses l'une : ou bien le groupe de l'équation ne sera pas changé, ou bien il se partagera en p groupes appartenant chacun à l'équation proposée respectivement quand on lui adjoint chacune des racines de l'équation auxiliaire ;

2°. ces groupes jouiront de la propriété remarquable, que l'on passera de l'un à l'autre en opérant dans toutes les permutations du premier une même substitution de lettres."

1°. Si, après l'adjonction de r, l'équation en V, dont il est question plus haut, reste irréductible, il est clair que le groupe de l'équation ne sera pas changé. Si, au contraire, elle se réduit, alors l'équation en V se décomposera en p facteurs, tous de même degré et de la forme

$$f(V, r) \times f(V, r') \times f(V, r''),$$

$r, r', r'', \ldots$ étant d'autres valeurs de r. Ainsi le groupe de l'équation proposée se décomposera aussi en groupes chacun d'un même nombre de permutations, puisqu'à chaque valeur de V correspond une permutation. Ces groupes seront respectivement ceux de l'équation proposée, quand on lui adjoindra successivement $r, r', r'', \ldots$.

2°. Nous avons vu plus haut que toutes les valeurs de V étaient des fonctions rationnelles les unes des autres. D'après cela, supposons que V étant une racine de $f(V, r) = 0, F(V)$ en soit une autre

[4]Dans l'énoncé du théorème, après ces mots : "la racine r d'une équation auxiliaire irréductible," Galois avait mis d'abord ceux-ci : "de degré p premier," qu'il a effacés plus tard. De même, dans la démonstration, au lieu de "$r, r', r'', \ldots$ étant d'autres valeurs de r", la rédaction primitive portait : "$r, r', r'', \ldots$ étant les diverses valeurs de r." Enfin on trouve à la marge du manuscrit la note suivante de l'auteur :
"Il y a quelque chose à compléter dans cette démonstration. Je n'ai pas le temps."
Cette ligne a été jetée avec une grande rapidité sur le papier ; circonstance qui, jointe aux mots : "Je n'ai pas le temps.", me fait penser que Galois a relu son Mémoire pour le corriger avant d'aller sur le terrain.
A. CH.

; il est clair que de même si V' est une racine de $f(V, r') = 0, F(V')$ en sera une autre ; car l'on aura

$$f[F(V), r] = \text{ une fonction divisible par} f(V, r).$$

Donc (*lemme 1*)

$$[F(V'), r'] = \text{ une fonction divisible par } f(V', r').$$

Cela posé, je dis que l'on obtient le groupe relatif à r' en opérant partout dans le groupe relatif à r une même substitution de lettres.

En effet, si l'on a, par exemple,

$$\varphi_\mu F(V) = \varphi_\nu(V),$$

on aura encore (*lemme 1*)

$$\varphi_\mu F(V') = \varphi_\nu(V').$$

Donc, pour passer de la permutation $[F(V)]$ à la permutation $[F(V')]$, il faut faire la même substitution que pour passer de la permutation (V) à la permutation $f(V')$.

Le théorème est donc démontré.

Proposition III.

Théorème. "Si l'on adjoint à une équation *toutes* les racines d'une équation auxiliaire, les groupes dont il est question dans le théorème II jouiront de plus de cette propriété, que les substitutions sont les mêmes dans chaque groupe."

On trouvera la démonstration[5].

Proposition IV.

Théorème. "Si l'on adjoint à une équation la valeur *numérique* d'une certaine fonction de ses racines, le groupe de l'équation s'abaissera de manière à n'avoir plus d'autres permutations que celles par lesquelles cette fonction est invariable."

En effet, d'après la proposition I, toute fonction connue doit être invariable par les permutations du groupe de l'équation.

[5]Dans le manuscrit, l'énoncé du théorème qu'on vient de lire se trouve en marge et en remplace un autre que Galois avait écrit avec sa démonstration sous le même titre : Proposition III. Voici le texte primitif :
Théorème. "Si l'équation en r est de la forme $r^p = A$, et que les racines $p^{\text{ièmes}}$ de l'unité se trouvent au nombre des quantités précédemment adjointes, les p groupes dont il est question dans le théorème II jouiront de plus de cette propriété, que les substitutions de lettres par lesquelles on passe d'une permutation à une autre dans chaque groupe soient les mêmes pour tous les groupes".
En effet, dans ce cas, il revient au même d'adjoindre à l'équation telle ou telle valeur de r. Par conséquent, ses propriétés doivent être les mêmes après l'adjonction de telle ou telle valeur. Ainsi son groupe doit être le même quant aux substitutions (Proposition I, scolie). Donc, etc.
Tout cela est effacé avec soin ; le nouvel énoncé porte la date 1832, et montre, par la manière dont il est écrit, que l'auteur était extrêmement pressé, ce qui confirme l'assertion que j'ai avancée dans la note précédente.
A. Ch.

Proposition v.

Problème. "Dans quels cas une équation est-elle soluble par de simples radicaux ?"

J'observerai d'abord que, pour résoudre une équation, il faut successivement abaisser son groupe jusqu'à ne contenir plus qu'une seule permutation. Car, quand une équation est résolue, une fonction quelconque de ses racines est connue, même quand elle n'est invariable par aucune permutation.

Cela posé, cherchons à quelle condition doit satisfaire le groupe d'une équation, pour qu'il puisse s'abaisser ainsi par l'adjonction de quantités radicales.

Suivons la marche des opérations possibles dans cette solution, en considérant comme opérations distinctes l'extraction de chaque racine de degré premier.

Adjoignons à l'équation le premier radical extrait dans la solution. Il pourra arriver deux cas : ou bien, par l'adjonction de ce radical, le groupe des permutations de l'équation sera diminué ; ou bien, cette extraction de racine n'étant qu'une simple préparation, le groupe restera le même.

Toujours sera-t-il qu'après un certain nombre *fini* d'extractions de racines, le groupe devra se trouver diminué, sans quoi l'équation ne serait pas soluble.

Si, arrivé à ce point, il y avait plusieurs manières de diminuer le groupe de l'équation proposée par une simple extraction de racine, il faudrait, pour ce que nous allons dire, considérer seulement un radical du degré le moins haut possible parmi tous les simples radicaux, qui sont tels que la connaissance de chacun d'eux diminue le groupe de l'équation.

Soit donc p le nombre premier qui représente ce degré minimum, en sorte que par une extraction de racine de degré p, on diminue le groupe de l'équation.

Nous pouvons toujours supposer, du moins pour ce qui est relatif au groupe de l'équation, que parmi les quantités adjointes précédemment à l'équation se trouve une racine $p^{\text{ième}}$ de l'unité, α. Car, comme cette expression s'obtient par des extractions de racines de degré inférieur à p, sa connaissance n'altèrera en rien le groupe de l'équation.

Par conséquent, d'après les théorèmes II et III, le groupe de l'équation devra se décomposer en p groupes jouissant les uns par rapport aux autres de cette double propriété : 1° Que l'on passe de l'un à l'autre par une seule et même substitution ; 2° que tous contiennent les mêmes substitutions.

Je dis réciproquement, que si le groupe de l'équation peut se partager en p groupes qui jouissent de cette double propriété, on pourra, par une simple extraction de racine $p^{\text{ième}}$, et par l'adjonction de cette racine $p^{\text{ième}}$, réduire le groupe de l'équation à l'un de ces groupes partiels.

Prenons, en effet, une fonction des racines qui soit invariable pour toutes les substitutions de l'un des groupes partiels, et varie pour toute autre substitution. (Il suffit, pour cela, de choisir une fonction symétrique des diverses valeurs que prend, par toutes les permutations de l'un des groupes

partiels, une fonction qui n'est invariable pour aucune substitution.)

Soit θ cette fonction des racines.

Opérons sur la fonction θ une des substitutions du groupe total qui ne lui sont pas communes avec les groupes partiels. Soit θ_1 le résultat. Opérons sur la fonction θ_1 la même substitution, et soit θ_2 le résultat, et ainsi de suite.

Comme p est un nombre premier, cette suite ne pourra s'arrêter qu'au terme θ_{p-1}, ensuite l'on aura $\theta_p = \theta_1, \theta_{p+1} = \theta_1$, et ainsi de suite.

Cela posé, il est clair que la fonction

$$(\theta + \alpha\theta_1 + \alpha^2\theta_2 + \ldots + \alpha^{p-1}\theta_{p-1})^p$$

sera invariable par toutes les permutations du groupe total, et, par conséquent, sera actuellement connue.

Si l'on extrait la racine $p^{\text{ième}}$ de cette fonction, et qu'on l'adjoigne à l'équation, alors, par la proposition IV, le groupe de l'équation ne contiendra plus d'autres substitutions que celles des groupes partiels.

Ainsi, pour que le groupe d'une équation puisse s'abaisser par une simple extraction de racine, la condition ci-dessus est nécessaire et suffisante.

Adjoignons à l'équation le radical en question ; nous pourrons raisonner maintenant sur le nouveau groupe comme sur le précédent, et il faudra qu'il se décompose lui-même de la manière indiquée, et ainsi de suite, jusqu'à un certain groupe qui ne contiendra plus qu'une seule permutation.

Scolie. Il est aisé d'observer cette marche dans la résolution connue des équations générales du quatrième degré. En effet, ces équations se résolvent au moyen d'une équation du troisième degré, qui exige elle-même l'extraction d'une racine carrée. Dans la suite naturelle des idées, c'est donc par cette racine carrée qu'il faut commencer. Or, en adjoignant à l'équation du quatrième degré cette racine carrée, le groupe de l'équation, qui contenait en tout vingt-quatre substitutions, se décompose en deux qui n'en contiennent que douze. En désignant par a, b, c, d les racines, voici l'un de ces groupes :

$$\begin{array}{lll} abcd, & acdb, & adbc, \\ badc, & cabd, & dacb, \\ cdab, & dbac, & bcad, \\ dcba, & bdca, & cbda. \end{array}$$

Maintenant ce groupe se partage lui-même en trois groupes, comme il est indiqué aux théorèmes II et III. Ainsi, par l'extraction d'un seul radical du troisième degré, il reste simplement le groupe

$$\begin{array}{l} abcd, \\ badc, \\ cdab, \\ dcba\ ; \end{array}$$

ce groupe se partage de nouveau en deux groupes :

$$\begin{array}{ll} abcd, & cdab, \\ badc, & dcba. \end{array}$$

Ainsi, après une simple extraction de racine carrée, il restera

$$\begin{array}{l} abcd\ , \\ badc\ ; \end{array}$$

ce qui se résoudra enfin par une simple extraction de racine carrée. On obtient ainsi, soit la solution de Descartes, soit celle d'Euler ; car, bien qu'après la résolution de l'équation auxiliaire du troisième degré, ce dernier extraye trois racines carrées, on sait qu'il suffit de deux, puisque la troisième s'en déduit rationnellement. Nous allons maintenant appliquer cette condition aux équations irréductibles dont le degré est premier.

Application aux équations irréductibles de degré premier.

PROPOSITION VI.

LEMME. "Une équation irréductible de degré premier ne peut devenir réductible par l'adjonction d'un radical dont l'indice serait autre que le degré même de l'équation."

Car si $r, r', r'', \ldots$ sont les diverses valeurs du radical, et $Fx = 0$ l'équation proposée, il faudrait que Fx se partageât en facteurs

$$f(x,r) \times f(x,r') \times \ldots,$$

tous de même degré, ce qui ne se peut, à moins que $f(x,r)$ ne soit du premier degré en x. Ainsi une équation irréductible de degré premier ne peut devenir réductible, à moins que son groupe ne se réduise à une seule permutation.

PROPOSITION VII.

PROBLÈME. "Quel est le groupe d'une équation irréductible d'un degré premier n, soluble par radicaux ?"

D'après la proposition précédente, le plus petit groupe possible avant celui qui n'a qu'une seule permutation, contiendra n permutations. Or un groupe de permutations d'un nombre premier n de lettres ne peut se réduire à n permutations, à moins que l'une de ces permutations ne se déduise de l'autre par une substitution circulaire de l'ordre n. (Voir le Mémoire de M. Cauchy, *Journal de l'Ecole Polytechnique*, XVII^{e} cahier.) Ainsi l'avant-dernier groupe sera

$$\left\{\begin{array}{llllllll} x_0, & x_1, & x_2, & x_3, & \ldots, & x_{n-3}, & x_{n-2}, & x_{n-1}, \\ x_1, & x_2, & x_3, & x_4, & \ldots, & x_{n-2}, & x_{n-1}, & x_0 \\ x_2, & x_3, & \ldots, & \ldots & \ldots & x_{n-1}, & x_0, & x_1, \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ x_{n-1}, & x_0, & x_1, & \ldots, & \ldots & x_{n-4}, & x_{n-3}, & x_{n-2}, \end{array}\right.$$

Maintenant, le groupe qui précédera immédiatement celui-ci dans l'ordre des décompositions devra se composer d'un certain nombre de groupes ayant tous les mêmes substitutions que celui-ci. Or j'observe que ces substitutions peuvent s'exprimer ainsi : (Faisons en général $x_n = x_0, x_{n+1} = x_1, ...$, il est clair que chacune des substitutions du groupe (G) s'obtient en mettant partout à la place de x_k, x_{k+c}, c étant une constante.)

Considérons l'un quelconque des groupes semblables au groupe (G). D'après le théorème II, il devra s'obtenir en opérant partout dans ce groupe une même substitution ; par exemple, en mettant partout dans le groupe (G), à la place de $x_k, x_{f(k)}$, f étant une certaine fonction.

Les substitutions de ces nouveaux groupes devant être les mêmes que celles du groupe (G), on devra avoir

$$f(k+c) = f(k) + C,$$

C étant indépendant de k.

Donc

$$\begin{aligned} &f(k+2c) = f(k) + 2C, \\ &\dots \\ &f(k+mc) = f(k) + mC. \end{aligned}$$

Si $c = 1, k = 0$, on trouvera

$$f(m) = am + b,$$

ou bien

$$f(k) = ak + b,$$

a et b étant des constantes.

Donc le groupe qui précède immédiatement le groupe (G) ne devra contenir que des substitutions telles que

$$x_k, \quad x_{ak+b},$$

et ne contiendra pas, par conséquent, d'autre substitution circulaire que celle du groupe (G).

On raisonnera sur ce groupe comme sur le précédent, et il s'ensuivra que le premier groupe dans l'ordre des décompositions, c'est- à-dire le groupe *actuel* de l'équation, ne peut contenir que des substitutions de la forme

$$x_k, \quad x_{ak+b}.$$

Donc, "si une équation irréductible de degré premier est soluble par radicaux, le groupe de cette équation ne saurait contenir que des substitutions de la forme

$$x_k, \quad x_{ak+b},$$

a et b étant des constantes."

Réciproquement, si cette condition a lieu, je dis que l'équation sera soluble par radicaux. Considérons, en effet, les fonctions

$$\begin{aligned}
&(x_0 + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{n-1} x_{n-1})^n && = X_1,\\
&(x_0 + \alpha x_a + \alpha^2 x_{2a} + \ldots + \alpha^{n-1} x_{(n-1)a})^n && = X_a,\\
&(x_0 + \alpha x_{a^2} + \alpha^2 x_{2a^2} + \ldots + \alpha^{n-1} x_{(n-1)a^2})^n && = X_{a^2},\\
&\ldots
\end{aligned}$$

α étant une racine $n^{\text{ième}}$ de l'unité, a une racine primitive de n.

Il est clair que toute fonction invariable par les substitutions circulaires des quantités $X_1, X_a, X_{a^2}, ...$ sera, dans ce cas, immédiatement connue. Donc on pourra trouver $X_1, X_a, X_{a^2}, ...$, par la méthode de M. Gauss pour les équations binômes. Donc, etc.

Ainsi, pour qu'une équation irréductible de degré premier soit soluble par radicaux, il *faut* et il *suffit* que toute fonction invariable par les substitutions

$$x_k, \quad x_{ak+b}$$

soit rationnellement connue.

Ainsi la fonction

$$(X_1 - X)(X_a - X)X_{a^2} - X)...$$

devra, quel que soit X, être connue.

Il *faut* donc et il *suffit* que l'équation qui donne cette fonction des racines admette, quel que soit X, une valeur rationnelle.

Si l'équation proposée a tous ses coefficients rationnels, l'équation auxiliaire qui donne cette fonction les aura tous aussi, et il suffira de reconnaître si cette équation auxiliaire du degré $1.2.3...(n-2)$ a ou non une racine rationnelle, ce que l'on sait faire.

C'est là le moyen qu'il faudrait employer dans la pratique. Mais nous allons présenter le théorème sous une autre forme.

Proposition viii.

Théorème. "Pour qu'une équation irréductible de degré premier soit soluble par radicaux, il *faut* et il *suffit* que deux quelconques des racines étant connues, les autres s'en déduisent rationnellement."

Premièrement, il le faut, car la substitution

$$x_k, \quad x_{ak+b}$$

ne laissant jamais deux lettres à la même place, il est clair qu'en adjoignant deux racines à l'équation, par la proposition iv, son groupe devra se réduire à une seule permutation.

En second lieu, cela suffit ; car, dans ce cas, aucune substitution du groupe ne laissera deux lettres aux mêmes places. Par conséquent, le groupe contiendra tout au plus $n(n-1)$ permutations. Donc il ne contiendra qu'une seule substitution circulaire (sans quoi il y aurait au moins n^2 permutations). Donc toute substitution du groupe, x_k, x_{fk} devra satisfaire à la condition

$$f(k+c) = fk + C,$$

Donc, etc.

Le théorème est donc démontré.

Exemple du théorème VII.

Soit $n = 5$; le groupe sera le suivant :

abcde
bcdea
cdeab
deabc
eabcd

---

acebd
cebda
ebdac
bdace
daceb

---

aedcb
edcba
dcbae
cbaed
baedc

---

adbec
dbeca
becad
ecadb
cadbe.

Articles publiés par Galois dans le Bulletin des Sciences mathématiques *de M. Férussac.*

Analyse d'un Mémoire sur la résolution algébrique des équations[1].

On appelle équations non primitives les équations qui étant, par exemple, du degré mn, se décomposent en m facteurs du degré n, au moyen d'une seule équation du degré m. Ce sont les équations de M. Gauss. Les équations primitives sont celles qui ne jouissent pas d'une pareille simplification. Je suis, à l'égard des équations primitives, parvenu aux résultats suivants :

1°. Pour qu'une équation de degré premier soit résoluble par radicaux, il faut et il suffit que deux quelconques de ses racines étant connues, les autres s'en déduisent rationnellement.

2°. Pour qu'une équation primitive du degré m soit résoluble par radicaux, il faut que $m = p^\nu$, p étant un nombre premier.

3°. À part les cas mentionnés ci-dessous, pour qu'une équation primitive du degré p^ν soit résoluble par radicaux, il faut que deux quelconques de ses racines étant connues, les autres s'en déduisent rationnellement.

À la règle précédente échappent les cas très-particuliers qui suivent :

1°. Le cas de $m = p^\nu = 9, = 25$;

2°. Le cas de $m = p^\nu = 4$, et généralement celui où, a^α étant un diviseur de $\dfrac{p^\nu - 1}{p - 1}$, on aurait a premier, et

$$\frac{p^\nu - 1}{a^\alpha (p-1)} \nu = p \pmod{a^\alpha}.$$

Ces cas s'écartent toutefois fort peu de la règle générale.

Quand $m = 9, = 25$, l'équation devra être du genre de celles qui déterminent la trisection et la quintisection des fonctions elliptiques.

Dans le second cas, il faudra toujours que deux des racines étant connues, les autres s'en déduisent, du moins au moyen d'un nombre de radicaux, du degré p, égal au nombre des diviseurs a^α de $\dfrac{p^\nu - 1}{p - 1}$ qui sont tels que

$$\frac{p^\nu - 1}{a^\alpha (p-1)} \nu = p \qquad \pmod{a^\alpha}, \qquad\qquad a \text{ premier.}$$

Toutes ces propositions ont été déduites de la théorie des permutations.

Voici d'autres résultats qui découlent de ma théorie.

[1] *Bulletin*, tome XIII, page 271 (année 1830, cahier d'avril). (J. L.)

1°. Soient k le module d'une fonction elliptique, p un nombre premier donné > 3 ; pour que l'équation du degré $p+1$, qui donne les divers modules des fonctions transformées relativement au nombre p, soit résoluble par radicaux, *il faut* de deux choses l'une : ou bien qu'une des racines soit rationnellement connue, ou bien que toutes soient des fonctions rationnelles les unes des autres. Il ne s'agit ici, bien entendu, que des valeurs particulières du module k. Il est évident que la chose n'a pas lieu en général. Cette règle n'a pas lieu pour $p = 5$.

2°. Il est remarquable que l'équation modulaire générale du sixième degré, correspondant au nombre 5, peut s'abaisser à une du cinquième degré dont elle est la réduite. Au contraire, pour des degrés supérieurs, les équations modulaires ne peuvent s'abaisser[2].

Note sur la résolution des équations numériques[3]

M. Legendre a le premier remarqué que, lorsqu'une équation algébrique était mise sous la forme

$$\varphi x = x,$$

où φx est une fonction de x qui croît constamment en même temps que x, il était facile de trouver la racine de cette équation immédiatement plus petite qu'un nombre donné a, si $\varphi a < a$, et la racine immédiatement plus grande que a, si $\varphi a > a$.

Pour le démontrer, on construit la courbe $y = \varphi x$ et la droite $y = x$. Soit prise une abscisse $= a$, et supposons, pour fixer les idées, $\varphi a > a$, je dis qu'il sera aisé d'obtenir la racine immédiatement supérieure à a. En effet, les racines de l'équation $\varphi x = x$ ne sont que les abscisses des points d'intersection de la droite et de la courbe, et il est clair que l'on s'approchera du point le plus voisin d'intersection, en substituant à l'abscisse a l'abscisse φa. On aura une valeur plus approchée encore en prenant $\varphi\varphi a$, puis $\varphi\varphi\varphi a$, et ainsi de suite.

Soit $Fx = 0$ une équation donnée du degré n, et $Fx = X - Y$, X et Y n'ayant que des termes positifs. Legendre met successivement l'équation sous ces deux formes

$$x = \varphi x = \sqrt[n]{\frac{X}{\left(\frac{Y}{x^n}\right)}}, \qquad x = \psi x = \sqrt[n]{\frac{X}{\left(\frac{x^n}{Y}\right)}};$$

les deux fonctions φx et ψx sont toujours, comme on voit, l'une plus grande, l'autre plus petite que x. Ainsi, à l'aide de ces deux fonctions, on pourra avoir les deux racines de l'équation les plus approchées d'un nombre donné a, l'une en plus et l'autre en moins.

---

[2]Cette assertion n'est pas tout à fait exacte, comme Galois en avertit lui-même dans sa Lettre à M. Auguste Chevalier, qu'on trouve plus bas. Il dit en général au sujet de l'article que nous reproduisons ici : La condition que j'ai indiquée dans le *Bulletin de Férussac* pour la solubilité par radicaux est trop restreinte ; il y a peu d'exceptions, mais il y en a. Quant aux équations modulaires en particulier, il déclare l'abaissement du degré $p + 1$ au degré p possible, non seulement pour $p = 5$, mais encore pour $p = 7$ et $p = 11$; mais il en maintient l'impossibilité pour $p > 11$. (J. L)

[3]*Bulletin*, tome XIII, page 413 (année 1830, cahier de juin). (J. L.).

Mais cette méthode a l'inconvénient d'exiger, à chaque opération, l'extraction d'une racine $n^{\text{ième}}$. Voici deux formes plus commodes. Cherchons un nombre k tel que la fonction

$$x + \frac{Fx}{kx^n}$$

croisse avec x, quand $x > 1$. (Il suffit, en effet, de savoir trouver les racines d'une équation qui sont plus grandes que l'unité.)

Nous aurons, pour la condition proposée,

$$1 + \frac{d\dfrac{X - Y}{kx^n}}{dx} > 0, \qquad \text{ou bien} \qquad 1 - \frac{nX - xX'}{kx^{n+1}} + \frac{nY - xY'}{kx^{n+1}} > 0\ ;$$

or on a identiquement

$$nX - xX' > o, \qquad nY - xY' > 0;$$

il suffit donc de poser

$$\frac{nX - xX'}{kx^{n+1}} < 1 \qquad \text{pour} \qquad x > 1,$$

et il suffit pour cela de prendre pour k la valeur de la fonction $nX - xX'$ relative à $x = 1$.

On trouvera de même un nombre h tel, que la fonction

$$x - \frac{Fx}{hx^n}$$

croîtra avec x quand x sera > 1, en changeant Y en X.

Ainsi, l'équation donnée pourra se mettre sous l'une des formes

$$x = x + \frac{Fx}{kx^n}, \qquad x = x - \frac{Fx}{hx^n},$$

qui sont toutes deux rationnelles, et donnent pour la résolution une méthode facile.

Sur la théorie des nombres.[4]

Quand on convient de regarder comme nulles toutes les quantités qui, dans les calculs algébriques, se trouvent multipliées par un nombre premier donné p, et qu'on cherche, dans cette convention, les solutions d'une équation algébrique $Fx = 0$, ce que M. Gauss désigne par la notation $Fx \equiv 0$, on n'a coutume de considérer que les solutions entières de ces sortes de questions. Ayant été conduit par des recherches particulières à considérer les solutions incommensurables, je suis parvenu à quelques résultats que je crois nouveaux.

[4] *Bulletin*, tome XIII, page 428 (année 1830, cahier de juin). Avec la Note suivante: Ce Mémoire fait partie des recherches de M. Galois sur la théorie des permutations et des équations algébriques. (J. L.)

Soit une pareille équation ou congruence, $Fx = 0$, et p le module. Supposons d'abord, pour plus de simplicité, que la congruence en question n'admette aucun facteur commensurable, c'est-à-dire qu'on ne puisse pas trouver trois fonctions $\varphi x, \psi x, \chi x$ telles que

$$\varphi x.\psi x = Fx + p\chi x.$$

Dans ce cas, la congruence n'admettra donc aucune racine entière, ni même aucune racine incommensurable de degré inférieur. Il faut donc regarder les racines de cette congruence comme des espèces de symboles imaginaires, puisqu'elles ne satisfont pas aux questions des nombres entiers, symboles dont l'emploi, dans le calcul, sera souvent aussi utile que celui de l'imaginaire $\sqrt{-1}$ dans l'analyse ordinaire.

C'est la classification de ces imaginaires, et leur réduction au plus petit nombre possible, qui va nous occuper.

Appelons i l'une des racines de la congruence $Fx = 0$, que nous supposerons du degré ν.

Considérons l'expression générale

$$\text{(A)} \qquad a + a_1 i + a_2 i^2 + ... + a_{\nu-1} i^{\nu-1},$$

où $a, a_1, a_2, ..., a_{\nu-1}$ représentent des nombres entiers. En donnant à ces nombres toutes les valeurs, l'expression (A) en acquiert p^ν, qui jouissent, ainsi que je vais le faire voir, des mêmes propriétés que les nombres naturels dans la *théorie des résidus des puissances*.

Ne prenons des expressions (A) que les $p^\nu - 1$ valeurs où $a, a_1, a_2, ..., a_{\nu-1}$ ne sont pas toutes nulles : soit α l'une de ces expressions.

Si l'on élève successivement α aux puissances 2^e, 3^e,..., on aura une suite de quantités de même forme [parce que toute fonction de i peut se réduire au $(\nu-1)^{\text{ième}}$ degré]. Donc on devra avoir $\alpha^n = 1$, n étant un certain nombre ; soit n le plus petit nombre qui soit tel que l'on ait $\alpha^n = 1$. On aura un ensemble de n expressions toutes différentes entre elles,

$$1, \alpha, \alpha^2, \alpha^3, ..., \alpha^{n-1}.$$

Multiplions ces n quantités par une autre expression ρ de la même forme. Nous obtiendrons encore un nouveau groupe de quantités toutes différentes des premières, et différentes entre elles. Si les quantités (A) ne sont pas épuisées, on multipliera encore les puissances de α par une nouvelle expression γ, et ainsi de suite. On voit donc que le nombre n divisera nécessairement le nombre total des quantités (A). Ce nombre étant $p^\nu - 1$, on voit que n divise $p^\nu - 1$. De là suit encore que l'on aura

$$\alpha^{p^\nu - 1} = 1, \qquad \text{ou bien} \qquad \alpha^{p^\nu} = \alpha.$$

Ensuite on prouvera, comme dans la théorie des nombres, qu'il y a des racines primitives α, pour lesquelles on ait précisément $p^\nu - 1 = n$, et qui reproduisent par conséquent, par l'élévation aux puissances, toute la suite des autres racines.

Et l'une quelconque de ces racines primitives ne dépendra que d'une congruence du degré ν, congruence *irréductible*, sans quoi l'équation en i ne le serait pas non plus, parce que les racines de la congruence en i sont toutes des puissances de la racine primitive.

On voit ici cette conséquence remarquable, que toutes les quantités algébriques qui peuvent se présenter dans la théorie sont racines d'équations de la forme

$$x^{p^\nu} = x.$$

Cette proposition, énoncée algébriquement, est celle-ci : Étant donnés une fonction Fx et un nombre premier p, on peut poser

$$fx.Fx = x^{p^\nu} - x + p\varphi x,$$

fx et φx étant des fonctions entières, toutes les fois que la congruence $Fx \equiv 0 \pmod{p}$ sera irréductible.

Si l'on veut avoir toutes les racines d'une pareille congruence au moyen d'une seule, il suffit d'observer que l'on a généralement

$$(Fx)^{p^n} = F(x^{p^n})$$

et que, par conséquent, l'une des racines étant x, les autres seront[5]

$$x^p, x^{p^2}, \ldots, x^{p^\nu - 1}$$

Il s'agit maintenant de faire voir que, réciproquement à ce que nous venons de dire, les racines de l'équation ou de la congruence $x^{p^\nu} = x$ dépendront toutes d'une seule congruence du degré ν.

Soit en effet i une racine d'une congruence irréductible, et telle que toutes les racines de la congruence $x^{p^\nu} = x$ soient fonctions rationnelles de i. (Il est clair qu'ici, comme dans les équations

[5]De ce que les racines de la congruence irréductible de degré ν

$$Fx = 0$$

sont exprimées par la suite

$$x, x^p, x^{p^2}, \ldots, x^{p^\nu - 1},$$

on aurait tort de conclure que ces racines soient toujours des quantités exprimables par radicaux. Voici un exemple du contraire :

La congruence irréductible

$$x^2 + x + 1 = 0 \qquad \pmod{2}$$

donne

$$x = \frac{-1 + \sqrt{-3}}{2},$$

qui se réduit à

$$\frac{0}{0}, \qquad \pmod{2}$$

formule qui n'apprend rien.

ordinaires, cette propriété a lieu)[6].

Il est d'abord évident que le degré μ de la congruence en i ne saurait être plus petit que ν, sans quoi la congruence

$$(\nu) \qquad x^{p^\nu - 1} - 1 = 0$$

aurait toutes ses racines communes avec la congruence

$$x^{p^\mu - 1} - 1 = 0,$$

ce qui est absurde, puisque la congruence (ν) n'a pas de racines égales, comme on le voit en prenant la dérivée du premier membre. Je dis maintenant que μ ne peut non plus être $> \nu$.

En effet, s'il en était ainsi, toutes les racines de la congruence

$$x^{p^\mu} = x$$

devraient dépendre rationnellement de celles de la congruence

$$x^{p^\nu} = x$$

Mais il est aisé de voir que si l'on a

$$i^{p^\nu} = i,$$

toute fonction rationnelle $h = fi$ donnera encore

$$(fi)^{p^\nu} = f(i^{p^\nu}) = fi, \quad \text{d'où} \quad h^{p^\nu} = h.$$

Donc toutes les racines de la congruence $x^{p^\mu} = x$ lui seraient communes avec l'équation $x^{p^\nu} = x$. Ce qui est absurde.

Nous savons donc enfin que toutes les racines de l'équation ou congruence $x^{p^\nu} = x$ dépendent nécessairement d'une *seule* congruence *irréductible* de degré ν.

Maintenant, pour avoir cette congruence irréductible d'où dépendent les racines de la congruence $x^{p^\nu} = x$, la méthode la plus générale sera de délivrer d'abord cette congruence de tous les facteurs communs qu'elle pourrait avoir avec des congruences de degré inférieur et de la forme

$$x^{p^\mu} = x.$$

On obtiendra ainsi une congruence qui devra se partager en congruences irréductibles de degré ν. Et, comme on sait exprimer toutes les racines de chacune de ces congruences irréductibles au moyen d'une seule, il sera aisé de les obtenir toutes par la méthode de M. Gauss.

[6]La proposition générale dont il s'agit ici peut s'énoncer ainsi : étant donnée une équation algébrique, on pourra trouver une fonction rationnelle θ de toutes ses racines, de telle sorte que, réciproquement, chacune des racines s'exprime rationnellement en θ. Ce théorème était connu d'Abel, ainsi qu'on peut le voir par la première partie du Mémoire que ce célèbre géomètre a laissé sur les fonctions elliptiques.

Le plus souvent, cependant, il sera aisé de trouver par le tâtonnement une congruence irréductible d'un degré donné ν, et l'on doit en déduire toutes les autres.

Soient, pour exemple. $p = 7, \nu = 3$. Cherchons les racines de la congruence

(1) $$x^{7^3} = x \text{ (mod. 7)}.$$

J'observe que la congruence

(2) $$i^3 = 2 \text{ (mod. 7)}$$

étant irréductible, et du degré 3, toutes les racines de la congruence (1) dépendent rationnellement de celle de la congruence (2), en sorte que toutes les racines de (1) sont de la forme

(3) $$a + a_1 i + a_2 i^2, \quad \text{ou bien} \quad a + a_1 \sqrt[2]{2} + a_2 \sqrt[3]{4}.$$

Il faut maintenant trouver une racine primitive, c'est-à-dire une forme de l'expression (3) qui, élevée à toutes les puissances, donne toutes les racines de la congruence

$$x^{\gamma^2 - 1} = 1, \quad \text{savoir} \quad x^{2^1 . 3^2 . 19} = 1 \text{ (mod. 7)},$$

et nous n'avons besoin pour cela que d'avoir une racine primitive de chaque congruence

$$x^2 = 1, \quad x^{3^2} = 1, \quad x^{19} = 1.$$

La racine primitive de la première est -1 ; celles de $x^{3^2} - 1 = 0$ sont données par les équations

$$x^3 = 2, \quad x^3 = 4$$

en sorte que i est une racine primitive de $x^{3^2} = 1$.

Il ne reste qu'à trouver une racine de $x^{19} - 1 = 0$, ou plutôt de

$$\frac{x^{19} - 1}{x - 1} = 0,$$

et essayons pour cela si l'on ne peut pas satisfaire à la question en posant simplement $x = a + a_1 i$, au lieu de $a + a_1 i + a_2 i^2$; nous devrons avoir

$$(a + a_1 i)^{19} = 1,$$

ce qui, en développant par la formule de Newton, et réduisant les puissances de a, de a_1, et de i, par les formules

$$a^{m(p-1)} = 1, \quad a_1^{m(p-1)} = 1, \quad i^3 = 2,$$

se réduit à

$$3[a - a^4 a_1^3 + (a^5 a_1^2 + a^2 a_1^5) i^2] = 1,$$

d'où, en séparant,

$$3a - 3a^4 a_1^3 = 1, a^5 a_1^2 + a^2 a_1^5 = 0.$$

Ces deux dernières équations sont satisfaites en posant $a = -1, a_1 = 1$. Donc

$$-1 + i$$

est une racine primitive de $x^{19} = 1$. Nous avons trouvé plus haut, pour racines primitives de $x^2 = 1$ et de $x^{3^2} = 1$, les valeurs -1 et i ; il ne reste plus qu'à multiplier entre elles les trois quantités

$$-1, \quad i, \quad -1 + i,$$

et le produit $i - i^2$ sera une racine primitive de la congruence

$$x^{7^2-1} = 1.$$

Donc ici l'expression $i - i^2$ jouit de la propriété, qu'en l'élevant à toutes les puissances, on obtiendra $7^3 - 1$ expressions différentes et de la forme

$$a + a_1 i + a_2 i^2.$$

Si nous voulons avoir la congruence de moindre degré d'où dépend notre racine primitive, il faut éliminer i entre les deux équations

$$i^3 = 2, \quad \alpha = i - i^2.$$

On obtient ainsi

$$\alpha^3 - \alpha + 2 = 0.$$

Il sera convenable de prendre pour base des imaginaires et de représenter par i la racine de cette équation, en sorte que

(i) $$i^3 - i + 2 = o,$$

et l'on aura toutes les imaginaires de la forme

$$a + a_1 i + a_2 i^2,$$

en élevant i à toutes les puissances, et réduisant par l'équation (i).

Le principal avantage de la nouvelle théorie que nous venons d'exposer est de ramener les congruences à la propriété (si utile dans les équations ordinaires) d'admettre précisément autant de racines qu'il y a d'unités dans l'ordre de leur degré.

La méthode pour avoir toutes ces racines sera très simple. Premièrement on pourra toujours préparer la congruence donnée $Fx = 0$, de manière à ce qu'elle n'ait plus de racines égales, ou, en d'autres termes, à ce qu'elle n'ait plus de facteur commun avec $F'x = 0$, et le moyen de le faire est évidemment le même que pour les équations ordinaires.

Ensuite, pour avoir les solutions entières, il suffira, ainsi que M. Libri paraît en avoir fait le premier la remarque, de chercher le plus grand facteur commun à $Fx = 0$ et à $x^{p-1} = 1$.

Si maintenant on veut avoir les solutions imaginaires du second degré, on cherchera le plus grand facteur commun à $Fx = 0$ et à $x^{p^2-1} = 1$, et, en général, les solutions de l'ordre ν seront données par le plus grand commun diviseur à $Fx = 0$ et à $x^{p^\nu-1} = 1$.

C'est surtout dans la théorie des permutations, où l'on a sans cesse besoin de varier la forme des indices, que la considération des racines imaginaires des congruences paraît indispensable. Elle donne un moyen simple et facile de reconnaître dans quel cas une équation primitive est soluble par radicaux, comme je vais essayer d'en donner en deux mots une idée.

Soit une équation algébrique $fx = 0$ de degré p^ν ; supposons que les p^ν racines soient désignées par x_k, en donnant à l'indice k les p^ν valeurs déterminées par la congruence $k^{p^\nu} = k \pmod{p}$.

Prenons une fonction quelconque rationnelle V des p^ν racines x_k. Transformons cette fonction en substituant partout à l'indice k l'indice $(ak+b)^{p^r}$, a, b, r étant des constantes arbitraires satisfaisant aux conditions de $a^{p^\nu-1} = 1$, $b^{p^\nu} = b \pmod{p}$ et de r entier.

En donnant aux constantes a, b, r toutes les valeurs dont elles sont susceptibles, on obtiendra en tout $p^\nu(p^\nu - 1)\nu$ manières de permuter les racines entre elles par des substitutions de la forme $[x_k, x_{(ak+b)^{p^r}}]$, et la fonction V admettra en général par ces substitutions $p^\nu(p^\nu - 1)\nu$ formes différentes.

Admettons maintenant que l'équation proposée $fx = 0$ soit telle, que toute fonction des racines invariable par les $p^\nu(p^\nu - 1)\nu$ permutations que nous venons de construire, ait pour cela même une valeur numérique rationnelle.

On remarque que, dans ces circonstances, l'équation $fx = 0$ sera soluble par radicaux, et, pour parvenir à cette conséquence, il suffit d'observer que la valeur substituée à k, dans chaque indice, peut se mettre sous les trois formes

$$(ak + b)^{p^r} = [a(k + b^1)]^{p^r} = a^1 k^{p^r} + b'' = a'(k + b')^{p^r}.$$

Les personnes habituées à la théorie des équations le verront sans peine.

Cette remarque aurait peu d'importance si je n'étais parvenu à démontrer que, réciproquement, une équation primitive ne saurait être soluble par radicaux, à moins de satisfaire aux conditions que je viens d'énoncer. (J'excepte les équations du neuvième et du vingt-cinquième degré.)

Ainsi, pour chaque nombre de la forme p^ν, on pourra former un groupe de permutations tel, que toute fonction des racines invariable par ces permutations devra admettre une valeur rationnelle quand l'équation de degré p_ν sera primitive et soluble par radicaux[7]. D'ailleurs, il n'y a que les équations d'un pareil degré p^ν qui soient à la fois primitives et solubles par radicaux.

Le théorème général que je viens d'énoncer précise et développe les conditions que j'avais données dans le *Bulletin* du mois d'avril. Il indique le moyen de former une fonction des racines dont la

[7] coquille ? p^ν au lieu de p_ν ?

valeur sera rationnelle, toutes les fois que l'équation primitive de degré p^ν sera soluble par radicaux, et mène, par conséquent, aux caractères de résolubilité de ces équations, par des calculs sinon praticables, du moins qui sont possibles en théorie.

Il est à remarquer que, dans le cas où $\nu = 1$, les diverses valeurs de k ne sont autre chose que la suite des nombres entiers. Les substitutions de la forme (x_k, x_{ak+b}) seront au nombre de $p(p-1)$.

La fonction qui, dans le cas des équations solubles par radicaux, doit avoir une valeur rationnelle, dépendra, en général, d'une équation de degré $1.2.3...(p-2)$, à laquelle il faudra, par conséquent, appliquer la méthode des racines rationnelles.

Lettre de Galois à M. Auguste Chevalier.[1]

(Insérée en 1832 dans la *Revue encyclopédique*, numéro de septembre, page 568.)

Mon cher ami,

J'ai fait en analyse plusieurs choses nouvelles.

Les unes concernent la théorie des équations ; les autres, les fonctions intégrales.

Dans la théorie des équations, j'ai recherché dans quels cas les équations étaient résolubles par des radicaux, ce qui m'a donné occasion d'approfondir cette théorie, et de décrire toutes les transformations possibles sur une équation, lors même qu'elle n'est pas soluble par radicaux.

On pourra faire avec tout cela trois Mémoires.

Le premier est écrit, et, malgré ce qu'en a dit Poisson, je le maintiens, avec les corrections que j'y ai faites.

Le second contient des applications assez curieuses de la théorie des équations. Voici le résumé des choses les plus importantes :

1°. D'après les propositions II et III du premier Mémoire, on voit une grande différence entre adjoindre à une équation une des racines d'une équation auxiliaire ou les adjoindre toutes.

Dans les deux cas, le groupe de l'équation se partage par l'adjonction en groupes tels, que l'on passe de l'un à l'autre par une même substitution ; mais la condition que ces groupes aient les mêmes substitutions n'a lieu certainement que dans le second cas. Cela s'appelle *la décomposition propre*.

En d'autres termes, quand un groupe G en contient un autre H, le groupe G peut se partager en groupes, que l'on obtient chacun en opérant sur les permutations de H une même substitution ; en sorte que

$$G = H + HS + HS' + ...$$

Et aussi il peut se décomposer en groupes qui ont tous les mêmes substitutions, en sorte que

$$G = H + TH + T'H + ...$$

Ces deux genres de décompositions ne coïncident pas ordinairement. Quand ils coïncident, la décomposition est dite *propre*.

[1] Écrite, on se le rappelle, la veille de la mort de l'auteur. (J. L.)

Il est aisé de voir que, quand le groupe d'une équation n'est susceptible d'aucune décomposition propre, on aura beau transformer cette équation, les groupes des équations transformées auront toujours le même nombre de permutations.

Au contraire, quand le groupe d'une équation est susceptible d'une décomposition propre, en sorte qu'il se partage en M groupes de N permutations, on pourra résoudre l'équation donnée au moyen de deux équations : l'une aura un groupe de M permutations, l'autre un de N permutations.

Lors donc qu'on aura épuisé sur le groupe d'une équation tout ce qu'il y a de décompositions propres possibles sur ce groupe, on arrivera à des groupes qu'on pourra transformer, mais dont les permutations seront toujours en même nombre.

Si ces groupes ont chacun un nombre premier de permutations, l'équation sera soluble par radicaux ; sinon, non.

Le plus petit nombre de permutations que puisse avoir un groupe indécomposable, quand ce nombre n'est pas premier, est 5.4.3.

2º. Les décompositions les plus simples sont celles qui ont lieu par la méthode de M. Gauss.

Comme ces décompositions sont évidentes, même dans la forme actuelle du groupe de l'équation, il est inutile de s'arrêter longtemps sur cet objet.

Quelles décompositions sont praticables sur une équation qui ne se simplifie pas par la méthode de M. Gauss ?

J'ai appelé *primitives* les équations qui ne peuvent se simplifier par la méthode de M. Gauss ; non que ces équations soient réellement indécomposables, puisqu'elles peuvent même se résoudre par radicaux.

Comme lemme à la théorie des équations primitives solubles par radicaux, j'ai mis en juin 1830, dans le *Bulletin de Férussac*, une analyse sur les imaginaires de la théorie des nombres.

On trouvera ci-jointe [2] la démonstration des théorèmes suivants :

1º. Pour qu'une équation primitive soit soluble par radicaux, elle doit être du degré p^ν, p étant premier.

[2] Galois parle des manuscrits, jusqu'ici inédits, que nous publions. (J. L.)

2°. Toutes les permutations d'une pareille équation sont de la forme

$$x_{k,l,m\ldots}|x_{ak+bl+cm+\ldots+h,a'k+b'l+c'm+\ldots+h',a''k+\ldots,\ldots}\ ;$$

$k, l, m,\ldots$ étant ν indices, qui, prenant chacun p valeurs, indiquent toutes les racines. Les indices sont pris suivant le module p ; c'est-à-dire que la racine sera la même quand on ajoutera à l'un des indices un multiple de p.

Le groupe qu'on obtient en opérant toutes les substitutions de cette forme linéaire contient, en tout,

$$p^\nu(p^\nu-1)(p^\nu-p)\ldots(p^\nu-p^{\nu-1}) \text{ permutations.}$$

Il s'en faut que dans cette généralité les équations qui lui répondent soient solubles par radicaux.

La condition que j'ai indiquée dans le *Bulletin de Férussac* pour que l'équation soit soluble par radicaux est trop restreinte ; il y a peu d'exceptions, mais il y en a.

La dernière application de la théorie des équations est relative aux équations modulaires des fonctions elliptiques.

On sait que le groupe de l'équation qui a pour racines les sinus de l'amplitude des p^2-1 divisions d'une période est celui-ci :

$$x_{k,l} \quad x_{ak+bl}|_{ck+dl}\ ;$$

par conséquent l'équation modulaire correspondante aura pour groupe

$$x_{\frac{k}{l}}, \quad x_{\frac{ak+bl}{ck+dl}},$$

dans laquelle $\dfrac{k}{l}$ peut avoir les $p+1$ valeurs

$$\infty, \ \ 0, \ \ 1, \ \ 2, \ \ \ldots, \ \ p-1.$$

Ainsi, en convenant que k peut être infini, on peut écrire simplement

$$x_k, \quad x_{\frac{ak+b}{ck+d}},$$

En donnant à a, b, c, d toutes les valeurs, on obtient

$$(p+1)p(p-1) \text{ permutations.}$$

Or ce groupe se décompose *proprement* en deux groupes, dont les substitutions sont

$$x_k, \quad x_{\frac{ak+b}{ck+d}},$$

$ad-bc$ étant un résidu quadratique de p.

Le groupe ainsi simplifié est de

$$(p+1)p.\frac{p-1}{2} \text{ permutations.}$$

Mais il est aisé de voir qu'il n'est plus décomposable proprement, à moins que $p = 2$, ou $p = 3$.

Ainsi, de quelque manière que l'on transforme l'équation, son groupe aura toujours le même nombre de permutations.

Mais il est curieux de savoir si le degré peut s'abaisser.

Et d'abord il ne peut s'abaisser plus bas que p, puisqu'une équation de degré moindre que p ne peut avoir p pour facteur dans le nombre des permutations de son groupe.

Voyons donc si l'équation de degré $p+1$, dont les racines x_k s'indiquent en donnant à k toutes les valeurs, y compris l'infini, et dont le groupe a pour substitutions

$$x_k, \quad x_{\frac{ak+b}{ck+d}},$$

$ad - bc$ étant un carré, peut s'abaisser au degré p.

Or il faut pour cela que le groupe se décompose (improprement, s'entend) en p groupes de $(p+1)\dfrac{p-1}{2}$ permutations chacun.

Soient 0 et ∞ deux lettres conjointes dans l'un de ces groupes. Les substitutions qui ne font pas changer 0 et ∞ de place seront de la forme

$$x_k, \quad x_{m^2 k}.$$

Donc si M est la lettre conjointe de 1, la lettre conjointe de m^2 sera $m^2 M$. Quand M est un carré, on aura donc $M^2 = 1$. Mais cette simplification ne peut avoir lieu que pour $p = 5$.

Pour $p = 7$ on trouve un groupe de $(p+1)\dfrac{p-1}{2}$ permutations, où

$$\infty \;\; 1 \;\; 2 \;\; 4$$

ont respectivement pour lettres conjointes

$$0 \;\; 3 \;\; 6 \;\; 5.$$

Ce groupe a ses substitutions de la forme

$$x_k, \quad x_{a\frac{k-b}{k-c}},$$

b étant la lettre conjointe de c, et a une lettre qui est résidu ou non résidu en même temps que c.

Pour $p = 11$, les mêmes substitutions auront lieu avec les mêmes notations,

$$\infty \;\; 1 \;\; 3 \;\; 4 \;\; 5 \;\; 9$$

ayant respectivement pour conjointes

$$0 \;\; 2 \;\; 6 \;\; 8 \;\; 10 \;\; 7.$$

Ainsi, pour les cas de $p = 5, 7, 11$, l'équation modulaire s'abaisse au degré p.

En toute rigueur, cette réduction n'est pas possible dans les cas plus élevés.

Le troisième Mémoire concerne les intégrales.

On sait qu'une somme de termes d'une même fonction elliptique se réduit toujours à un seul terme, plus des quantités algébriques ou logarithmiques.

Il n'y a pas d'autres fonctions pour lesquelles cette propriété ait lieu.

Mais des propriétés absolument semblables y suppléent dans toutes les intégrales de fonctions algébriques.

On traite à la fois toutes les intégrales dont la différentielle est une fonction de la variable et d'une même fonction irrationnelle de la variable, que cette irrationnelle soit ou ne soit pas un radical, qu'elle s'exprime ou ne s'exprime pas par des radicaux.

On trouve que le nombre des périodes distinctes de l'intégrale la plus générale relative à une irrationnelle donnée est toujours un nombre pair.

Soit $2n$ ce nombre, on aura le théorème suivant :

Une somme quelconque de termes se réduit à n termes, plus des quantités algébriques et logarithmiques.

Les fonctions de première espèce sont celles pour lesquelles la partie algébrique et logarithmique est nulle.

Il y en a n distinctes.

Les fonctions de seconde espèce sont celles pour lesquelles la partie complémentaire est purement algébrique.

Il y en a n distinctes.

On peut supposer que les différentielles des autres fonctions ne soient jamais infinies qu'une fois pour $x = a$, et, de plus, que leur partie complémentaire se réduise à un seul logarithme, log P, P étant une quantité algébrique. En désignant par $\Pi(x, a)$ ces fonctions, on aura le théorème

$$\Pi(x, a) - \Pi(a, x) = \sum \varphi a \psi x,$$

φa et ψx étant des fonctions de première et de seconde espèce.

On en déduit, en appelant $\Pi(a)$ et ψ les périodes de $\Pi(x, a)$ et ψx relatives à une même révolution

de x,

$$\Pi(a) = \sum \psi \times \varphi a.$$

Ainsi les périodes des fonctions de troisième espèce s'expriment toujours en fonctions de première et de seconde espèce.

On peut en déduire aussi des théorèmes analogues au théorème de Legendre

$$FE' + EF' - FF' = \frac{\pi}{2}$$

La réduction des fonctions de troisième espèce à des intégrales définies, qui est la plus belle découverte de M. Jacobi, n'est pas praticable, hors le cas des fonctions elliptiques.

La multiplication des fonctions intégrales par un nombre entier est toujours possible, comme l'addition, au moyen d'une équation de degré n dont les racines sont les valeurs à substituer dans l'intégrale pour avoir les termes réduits.

L'équation qui donne la division des périodes en p parties égales est du degré $p^{2n} - 1$. Son groupe a en tout

$$(p^{2n} - 1)(p^{2n} - p)...(p^{2n} - p^{2n-1}) \text{ permutations.}$$

L'équation qui donne la division d'une somme de n termes en p parties égales est du degré p^{2n}. Elle est soluble par radicaux.

De la transformation. On peut d'abord, en suivant des raisonnements analogues à ceux qu'Abel a consignés dans son dernier Mémoire, démontrer que si, dans une même relation entre des intégrales, on a les deux fonctions

$$\int \Phi(x, X)dx, \quad \int \Psi(y, Y)dy,$$

la dernière intégrale ayant $2n$ périodes, il sera permis de supposer que y et Y s'expriment moyennant une seule équation de degré n en fonction de x et de X.

D'après cela on peut supposer que les transformations aient lieu constamment entre deux intégrales seulement, puisqu'on aura évidemment, en prenant une fonction quelconque rationnelle de y et de Y,

$$\sum \int f(y, Y)dy = \int F(x, X)dx + \text{une quant. alg. et log.}$$

Il y aurait sur cette équation des réductions évidentes dans le cas où les intégrales de l'un et de l'autre membre n'auraient pas toutes deux le même nombre de périodes.

Ainsi nous n'avons à comparer que des intégrales qui aient toutes deux le même nombre de périodes.

On démontrera que le plus petit degré d'irrationnalité de deux pareilles intégrales ne peut être plus grand pour l'une que pour l'autre.

On fera voir ensuite qu'on peut toujours transformer une intégrale donnée en une autre dans laquelle une période de la première soit divisée par le nombre premier p, et les $2n-1$ autres restent les mêmes.

Il ne restera donc à comparer que des intégrales où les périodes seront les mêmes de part et d'autre, et telles par conséquent que n termes de l'une s'expriment sans autre équation qu'une seule du degré n, au moyen de ceux de l'autre, et réciproquement. Ici nous ne savons rien.

Tu sais, mon cher Auguste, que ces sujets ne sont pas les seuls que j'aie explorés. Mes principales méditations, depuis quelque temps, étaient dirigées sur l'application à l'analyse transcendante de la théorie de l'ambiguïté. Il s'agissait de voir à priori, dans une relation entre des quantités ou fonctions transcendantes, quels échanges on pouvait faire, quelles quantités on pouvait substituer aux quantités données, sans que la relation pût cesser d'avoir lieu. Cela fait reconnaître de suite l'impossibilité de beaucoup d'expressions que l'on pourrait chercher. Mais je n'ai pas le temps, et mes idées ne sont pas encore bien développées sur ce terrain, qui est immense. Tu feras imprimer cette Lettre dans la *Revue encyclopédique*.

Je me suis souvent hasardé dans ma vie à avancer des propositions dont je n'étais pas sûr ; mais tout ce que j'ai écrit là est depuis bientôt un an dans ma tête, et il est trop de mon intérêt de ne pas me tromper pour qu'on me soupçonne d'avoir énoncé des théorèmes dont je n'aurais pas la démonstration complète.

Tu prieras publiquement Jacobi ou Gauss de donner leur avis, non sur la vérité, mais sur l'importance des théorèmes.

Après cela, il y aura, j'espère, des gens qui trouveront leur profit à déchiffrer tout ce gâchis.

Je t'embrasse avec effusion.

É. GALOIS.

Le 29 mai 1832.

Fragment d'un second Mémoire.

Des équations primitives qui sont solubles par radicaux.

Cherchons, en général, dans quel cas une équation primitive est soluble par radicaux. Or nous pouvons de suite établir un caractère général fondé sur le degré même de ces équations. Ce caractère est celui-ci : pour qu'une équation primitive soit résoluble par radicaux, il faut que son degré soit de la forme p^ν, p étant premier. Et de là suivra immédiatement que, lorsqu'on aura à résoudre par radicaux une équation irréductible dont le degré admettrait des facteurs premiers inégaux, on ne pourra le faire que par la méthode de décomposition due à M. Gauss ; sinon l'équation sera insoluble.

Pour établir la propriété générale que nous venons d'énoncer relativement aux équations primitives qu'on peut résoudre par radicaux, nous pouvons supposer que l'équation que l'on veut résoudre soit primitive, mais cesse de l'être par l'adjonction d'un simple radical. En d'autres termes, nous pouvons supposer que, n étant premier, le groupe de l'équation se partage en n groupes irréductibles conjugués, mais non primitifs. Car, à moins que le degré de l'équation soit premier, un pareil groupe se présentera toujours dans la suite des décompositions.

Soit N le degré de l'équation, et supposons qu'après une extraction de racine de degré premier n, elle devienne non primitive et se partage en Q équations primitives de degré P, au moyen d'une seule équation de degré Q.

Si nous appelons G le groupe de l'équation, ce groupe devra se partager en n groupes conjugués non primitifs, dans lesquels les lettres se rangeront en systèmes composés de P lettres conjointes chacun. Voyons de combien de manières cela pourra se faire.

Soit H l'un des groupes conjugués non primitifs. Il est aisé de voir que, dans ce groupe, deux lettres quelconques prises à volonté feront partie d'un certain système de P lettres conjointes, et ne feront partie que d'un seul.

Car, en premier lieu, s'il y avait deux lettres qui ne pussent faire partie d'un même système de P lettres conjointes, le groupe G, qui est tel que l'une quelconque de ses substitutions transforme les unes dans les autres toutes les substitutions du groupe H, serait non primitif : ce qui est contre l'hypothèse.

En second lieu, si deux lettres faisaient partie de plusieurs systèmes différents, il s'ensuivrait que les groupes qui répondent aux divers systèmes de P lettres conjointes ne seraient pas primitifs ce qui est encore contre l'hypothèse.

Cela posé, soient

$$\begin{array}{cccccc} a_0, & a_1, & a_2, & \ldots, & a_{P-1} \\ b_0, & b_1, & b_2, & \ldots, & b_{P-1} \\ c_0, & c_1, & c_2, & \ldots, & c_{P-1} \end{array}$$

les N lettres : supposons que chaque ligne horizontale représente un système de lettres conjointes.

Soient

$$a_0, \quad a_{0.1}, \quad a_{0.2}, \quad \ldots, \quad a_{0.P-1}$$

P lettres conjointes toutes situées dans la première colonne verticale. (Il est clair que nous pouvons faire qu'il en soit ainsi, en intervertissant l'ordre des lignes horizontales.)

Soient, de même,

$$a_{1,0}, \quad a_{1.1}, \quad a_{1.2}, \quad \ldots, \quad a_{1.P-1}$$

P lettres conjointes toutes situées dans la seconde colonne verticale, en sorte que

$$a_{1.0}, \quad a_{1.1}, \quad a_{1.2}, \quad \ldots, \quad a_{1.P-1}$$

appartiennent respectivement aux mêmes lignes horizontales que

$$a_{0.0}, \quad a_{0.1}, \quad a_{0.2}, \quad \ldots, \quad a_{0.P-1}$$

soient, de même, les systèmes de lettres conjointes

$$\begin{array}{ccccc} a_{2.0}, & a_{2.1}, & a_{2.2}, & \ldots, & a_{2.P-1} \\ a_{3.0}, & a_{3.1}, & a_{3.2}, & \ldots, & a_{3.P-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \end{array}$$

nous obtiendrons ainsi, en tout, P^2 lettres. Si le nombre total des lettres n'est pas épuisé, on prendra un troisième indice, en sorte que

$$a_{m.n.0}, \quad a_{m.n.1}, \quad a_{m.n.2}, \quad a_{m.n.3}, \quad \ldots, \quad a_{m.n.P-1}$$

soit, en général, un système de lettres conjointes ; et l'on parviendra ainsi à cette conclusion, que $N = P^\mu$, μ étant un certain nombre égal à celui des indices différents dont on aura besoin. La forme générale des lettres sera

$$a_{\underset{1}{k}.\underset{2}{k}.\underset{3}{k}.\ldots.\underset{\mu}{k}},$$

$\underset{1}{k}, \underset{2}{k}, \underset{3}{k}, \ldots, \underset{\mu}{k}$ étant des indices qui peuvent prendre chacun les P valeurs $0, 1, 2, 3, \ldots, P-1$.

On voit aussi, par la manière dont nous avons procédé, que dans le groupe H, toutes les substitutions seront de la forme

$$\left[a_{\underset{1}{k}.\underset{2}{k}.\underset{3}{k}.\ldots.\underset{\mu}{k}}, \; , \quad a_{\underset{1}{\varphi(k)}.\underset{2}{\psi(k)}.\underset{3}{\chi(k)}.\ldots.\underset{\mu}{\sigma(k)}}, \right],$$

puisque chaque indice correspond à un système de lettres conjointes.

Si P n'est pas un nombre premier, on raisonnera sur le groupe de permutations de l'un quelconque des systèmes de lettres conjointes, comme sur le groupe G, en remplaçant chaque indice par un certain nombre de nouveaux indices, et l'on trouvera $P = R^\alpha$, et ainsi de suite ; d'où enfin $N = p^\nu$, p étant un nombre premier.

Des équations primitives de degré p^2.

Arrêtons-nous un moment pour traiter de suite les équations primitives d'un degré p^2, p étant premier impair. (Le cas de $p = 2$ a été examiné.) Si une équation du degré p^2 est soluble par radicaux, supposons-la d'abord telle, qu'elle devienne non primitive par une extraction de radical.

Soit donc G un groupe primitif de p^2 lettres qui se partage en n groupes non primitifs conjugués à H.

Les lettres devront nécessairement, dans le groupe H, se ranger ainsi,

$$\begin{array}{cccccc} a_{0.0}, & a_{0.1}, & a_{0.2}, & a_{0.3}, & \ldots, & a_{0.p-1} \\ a_{1.0}, & a_{1.1}, & a_{1.2}, & a_{1.3}, & \ldots, & a_{1.p-1} \\ a_{2.0}, & a_{2.1}, & a_{2.2}, & a_{2.3}, & \ldots, & a_{2.p-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \\ a_{p-1.0}, & a_{p-1.1}, & a_{p-1.2}, & a_{p-1.3}, & \ldots, & a_{p-1.p-1} \end{array}$$

chaque ligne horizontale et chaque ligne verticale étant un système de lettres conjointes.

Si l'on permute entre elles les lignes horizontales, le groupe que l'on obtiendra, étant primitif et de degré premier, ne devra contenir que des substitutions de la forme

$$\left(a_{\substack{k.k \\ 1\ 2}}, a_{\substack{mk+n.k \\ 1\quad 2}}\right),$$

les indices étant pris relativement au module p.

Il en sera de même pour les lignes verticales qui ne pourront donner que des substitutions de la forme

$$\left(a_{\substack{k.k \\ 1\ 2}}, a_{\substack{k.qk+r \\ 1\quad 2}}\right),$$

Donc enfin toutes les substitutions du groupe H seront de la forme

$$\left(a_{\substack{k.k \\ 1\ 2}}, a_{\substack{mk+n.mk+n \\ 1\,1\quad 1\,2\,2\quad 2}}\right).$$

Si un groupe G se partage en n groupes conjugués à celui que nous venons de décrire, toutes les substitutions du groupe G devront transformer les unes dans les autres les substitutions circulaires du groupe H, qui sont toutes écrites comme il suit :

(a) $$\left(a_{\substack{k.k \\ 1\ 2}}, \ldots \quad a_{\substack{k+\alpha\ k+\alpha \\ 1\ \ 1\ 2\ \ 2}}, \ldots\right),$$

Supposons donc que l'une des substitutions du groupe G se forme en remplaçant respectivement

$$\begin{array}{ccc} \underset{1}{k} & & \varphi_1\left(\underset{1}{k}, \quad \underset{2}{k}\right) \\ & \text{par} & \\ \underset{2}{k} & & \varphi_2\left(\underset{1}{k}, \quad \underset{2}{k}\right) \end{array}$$

Si, dans les fonctions φ_1, φ_2, on substitue pour $\underset{1}{k}$ et $\underset{2}{k}$ les valeurs $\underset{1}{k}+\underset{1}{\alpha}$, $\underset{2}{k}+\underset{2}{\alpha}$, il devra venir des résultats de la forme

$$\varphi_1 + \vartheta_1, \quad \varphi_2 + \vartheta_2,$$

et de là il est aisé de conclure immédiatement que les substitutions du groupe G doivent être toutes comprises dans la formule

$$(A) \qquad \left(a_{\underset{1}{k}.\underset{2}{k}}, \quad a_{\underset{1}{m}\underset{1}{k}+\underset{1}{n}\underset{2}{k}+\underset{1}{\alpha}.\underset{2}{m}\underset{1}{k}+\underset{2}{n}\underset{1}{k}+\underset{2}{\alpha}}\right).$$

Or nous savons, par le n° [1], que les substitutions du groupe G ne peuvent embrasser que p^2-1 ou p^2-p lettres. Ce n'est point p^2-p, puisque, dans ce cas, le groupe G serait non primitif. Si donc dans le groupe G on ne considère que les permutations où la lettre $a_{0.0}$ par exemple, conserve toujours la même place, on n'aura que des substitutions de l'ordre p^2-1 entre les p^2-1 autres lettres.

Mais rappelons-nous ici que c'est simplement pour la démonstration, que nous avons supposé que le groupe primitif G se partageât en groupes conjugués non primitifs. Comme cette condition n'est nullement nécessaire, les groupes seront souvent beaucoup plus composés.

Il s'agit donc de reconnaître dans quel cas ces groupes pourront admettre des substitutions où p^2-p lettres seulement varieraient, et cette recherche va nous retenir quelque temps.

Soit donc G un groupe qui contienne quelque substitution de l'ordre p^2-p ; je dis d'abord que toutes les substitutions de ce groupe seront linéaires, c'est-à-dire de la forme (A).

La chose est reconnue vraie pour les substitutions de l'ordre p^2-1 ; il suffit donc de la démontrer pour celles de l'ordre p^2-p. Ne considérons donc qu'un groupe où les substitutions seraient toutes m de l'ordre p^2 ou de l'ordre p^2-p. (*Voyez* l'endroit cité.)

Alors les p lettres qui, dans une substitution de l'ordre p^2-p, ne varieront pas, devront être des lettres conjointes.

Supposons que ces lettres conjointes soient

$$a_{0.0}, \quad a_{0.1}, \quad a_{0.2}, \quad \ldots, \quad a_{0,p-1}.$$

Nous pouvons déduire toutes les substitutions où ces p lettres ne changent pas de place, nous pouvons les déduire de substitutions de la forme

$$\left(a_{\underset{1}{k}.\underset{2}{k}}, \quad a_{\underset{1}{k}.\underset{2}{\varphi k}}\right),$$

et de substitutions de l'ordre p^2-p, dont la période serait de p termes. (*Voyez* encore l'endroit cité.)

[1] Ce Mémoire faisant suite à un travail de Galois que je ne possède pas, il m'est impossible d'indiquer le Mémoire cité ici et plus bas. A. Ch.

Les premiers doivent nécessairement, pour que le groupe jouisse de la propriété voulue, se réduire à la forme

$$\left(a_{\substack{k.k\\1\ 2}},\ \ a_{\substack{k.mk\\1\ 2}}\right),$$

d'après ce qu'on a vu pour les équations de degré p.

Quant aux substitutions dont la période serait de p termes, comme elles sont conjuguées aux précédentes, nous pouvons supposer un groupe qui les contienne sans contenir celles-ci : donc elles devront transformer les substitutions circulaires (a) les unes dans les autres ; donc elles seront aussi linéaires.

Nous sommes donc arrivés à cette conclusion, que le groupe primitif de permutations de p^2 lettres doit ne contenir que des substitutions de la forme (A).

Maintenant, prenons le groupe total que l'on obtient en opérant sur l'expression

$$a_{\substack{k.k\\1\ 2}}$$

toutes les substitutions linéaires possibles, et cherchons quels sont les diviseurs de ce groupe qui peuvent jouir de la propriété voulue pour la résolubilité des équations.

Quel est d'abord le nombre total des substitutions linéaires ? Premièrement, il est clair que toute transformation de la forme

$$\underset{1\ 2}{k.k},\quad \underset{1\ 1}{mk}+\underset{1\ 2}{nk}+\underset{1}{\alpha}.\underset{2\ 1}{mk}+\underset{2\ 2}{nk}+\underset{2}{\alpha}$$

ne sera pas pour cela une substitution ; car il faut, dans une substitution, qu'à chaque lettre de la première permutation il ne réponde qu'une seule lettre de la seconde, et réciproquement.

Si donc on prend une lettre quelconque $a_{\substack{l.l\\1\ 2}}$ de la seconde permutation, et que l'on remonte à la lettre correspondante dans la première, on devra trouver une lettre $a_{\substack{k.k\\1\ 2}}$ où les indices $\underset{1\ 2}{k.k}$ seront parfaitement déterminés. Il faut donc que, quels que soient l_1 et l_2, on ait par les deux équations

$$\underset{1\ 1}{mk}+\underset{1\ 2}{nk}+\alpha_1=l_1,\ \ \underset{2\ 1}{mk}+\underset{2\ 2}{nk}+\alpha_{2=l_2,}$$

des valeurs de $\underset{1}{k}$ et $\underset{2}{k}$ finies et déterminées. Ainsi la condition pour qu'une pareille transformation soit réellement une substitution, est que $\underset{1\ 2}{mn}-\underset{2\ 1}{mn}$ ne soit ni nul ni divisible par le module p, ce qui est la même chose.

Je dis maintenant que, bien que ce groupe à substitutions linéaires n'appartienne pas toujours, comme on le verra, à des équations solubles par radicaux, il jouira toutefois de cette propriété, que si dans une quelconque de ses substitutions il y a n lettres de fixes, n divisera le nombre des lettres. Et, en effet, quel que soit le nombre des lettres qui restent fixes, on pourra exprimer cette circonstance par des équations linéaires qui donneront tous les indices de l'une des lettres fixes, au moyen d'un certain nombre d'entre eux. Donnant à chacun de ces indices, restés arbitraires, p valeurs, on aura p^m systèmes de valeurs, m étant un certain nombre. Dans le cas qui nous occupe,

m est nécessairement < 2, et se trouve par conséquent être 0 ou 1. Donc le nombre des substitutions ne saurait être plus grand que

$$p^2(p^2-1)(p^2-p).$$

Ne considérons maintenant que les substitutions linéaires où la lettre $a_{0.0}$ ne varie pas ; si, dans ce cas, nous trouvons le nombre total des permutations du groupe qui contient toutes les substitutions linéaires possibles, il nous suffira de multiplier ce nombre par p^2.

Or, premièrement, en substituant p à l'indice k_2, toutes les substitutions de la forme

$$\left(a_{\substack{k.k\\1\ 2}},\quad a_{\substack{mk.k\\1\ 1\ 2}}\right)$$

donneront en tout $p-1$ substitutions. On en aura p^2-p en ajoutant au terme k_2, le terme $\underset{2}{mk}$, ainsi qu'il suit :

$$(m') \qquad \left(\underset{1\ 2}{k.k},\quad \underset{1\ 1\ 2\ 1}{mk.mk} + \underset{2}{k}\right).$$

D'un autre côté, il est aisé de trouver un groupe linéaire de p^2-1 permutations, tel que, dans chacune de ses substitutions, toutes les lettres, à l'exception de $a_{0.0}$, varient. Car, en remplaçant le double indice $\underset{1\ 2}{kk}$ par l'indice simple $k_1 + ik_2$, i étant une racine primitive de

$$x^{p^2-1} - 1 = 0 \text{ (mod. } p),$$

il est clair que toute substitution de la forme

$$\left[a_{\substack{k+ki\\1\quad 2}},\quad a_{(\underset{1}{m}+\underset{2}{mi})(\underset{1}{k}+\underset{2}{ki})}\right]$$

sera une substitution linéaire ; mais, dans ces substitutions, aucune lettre ne reste à la même place, et elles sont au nombre de p^2-1.

Nous avons donc un système de p^2-1 permutations tel que, dans chacune de ses substitutions, toutes les lettres varient, à l'exception de $a_{0.0}$. Combinant ces substitutions avec les p^2-p dont il est parlé plus haut, nous aurons

$$(p^2-1)(p^2-p) \text{ substitutions.}$$

Or, nous avons vu à priori que le nombre des substitutions où $a_{0.0}$ reste fixe ne pouvait être plus grand que $(p^2-1)(p^2-p)$. Donc il est précisément égal à $(p^2-1)(p^2-p)$, et le groupe linéaire total aura en tout

$$p^2(p^2-1)(p^2-p) \text{ permutations.}$$

Il reste à chercher les diviseurs de ce groupe, qui peuvent jouir de la propriété d'être solubles par radicaux. Pour cela, nous allons faire une transformation qui a pour but d'abaisser autant que possible les équations générales de degré p^2 dont le groupe serait linéaire.

Premièrement, comme les substitutions circulaires d'un pareil groupe sont telles, que toute autre substitution du groupe les transforme les unes dans les autres, on pourra abaisser l'équation d'un

degré, et considérer une équation de degré p^2-1 dont le groupe n'aurait que des substitutions de la forme

$$\left(b_{\substack{k,k\\1\,2}},\quad b_{\substack{mk+nk.mk+nk\\1\,1\quad 1\,2\quad 2\,1\quad 2\,2}}\right),$$

les p^2-1 lettres étant

$$\begin{array}{ccccc} & b_{0.1}, & b_{0.2}, & b_{0.3}, & \ldots, \\ b_{1.0}, & b_{1.1}, & b_{1.2}, & b_{1.3}, & \ldots, \\ b_{2.0}, & b_{2.1}, & b_{2.2}, & b_{2.3}, & \ldots, \\ \ldots & \ldots & \ldots & \ldots & \ldots \end{array}$$

J'observe maintenant que ce groupe est non primitif, en sorte que toutes les lettres où le rapport des deux indices est le même sont des lettres conjointes. Si l'on remplace par une seule lettre chaque système de lettres conjointes, on aura un groupe dont toutes les substitutions seront de la forme

$$\left(b_{\frac{k_1}{k_2}},\quad b_{\frac{m_1k_1+n_1k_2}{m_2k_2+n_2k_1}}\right),$$

$\frac{k_1}{k_2}$ étant les nouveaux indices. En remplaçant ce rapport par un seul indice k, on voit que les $p+1$ lettres seront

$$b_0,\quad b_1,\quad b_2,\quad b_3,\quad \ldots,\quad b_{p-1},\quad b_{\frac{1}{0}},$$

et les substitutions seront de la forme

$$\left(k,\quad \frac{mk+n}{rk+s}\right)$$

Cherchons combien de lettres, dans chacune de ces substitutions, restent à la même place ; il faut pour cela résoudre l'équation

$$(rk+s)k-m(mk+n)=0,$$

qui aura deux, ou une, ou aucune racine, suivant que $(m-s)^2+4nr$ sera résidu quadratique, nul ou non résidu quadratique. Suivant ces trois cas, la substitution sera de l'ordre $p-1$, ou p, ou $p+1$.

On peut prendre pour type des deux premiers cas les substitutions de la forme

$$(k, mk+n),$$

où la seule lettre $b_{\frac{1}{0}}$ ne varie pas, et de là on voit que le nombre total des substitutions du groupe réduit est

$$(p+1)p(p-1).$$

C'est après avoir ainsi réduit ce groupe, que nous allons le traiter généralement. Nous chercherons d'abord dans quel cas un diviseur de ce groupe, qui contiendrait des substitutions de l'ordre p, pourrait appartenir à une équation soluble par radicaux.

Dans ce cas, l'équation serait primitive et elle ne pourrait être soluble par radicaux, à moins que l'on n'eût $p+1=2^n$, n étant un certain nombre.

Nous pouvons supposer que le groupe ne contienne que des substitutions de l'ordre p et de l'ordre $p+1$. Toutes les substitutions de l'ordre $p+1$ seront par conséquent semblables, et leur période

sera de deux termes.

Prenons donc l'expression

$$\left(k, \quad \frac{mk+n}{rk+s}\right),$$

et voyons dans quel cas cette substitution peut avoir une période de deux termes. Il faut pour cela que la substitution inverse se confonde avec elle. La substitution inverse est

$$\left(k, \quad \frac{-sk+n}{rk-m}\right).$$

Donc on doit avoir $m = -s$, et toutes les substitutions en question seront

$$\left(k, \quad \frac{mk+n}{k-m}\right),$$

ou encore

$$k, \quad m + \frac{N}{k-m},$$

N étant un certain nombre qui est le même pour toutes les substitutions, puisque ces substitutions doivent être transformées les unes dans les autres par toutes les substitutions de l'ordre p, $(k, k+m)$; or ces substitutions doivent, de plus, être conjuguées les unes des autres. Si donc

$$\left(k, \quad m + \frac{N}{k-m}\right), \quad \left(k, \quad n + \frac{N}{k-n}\right)$$

sont deux pareilles substitutions, il faut que l'on ait

$$n + \frac{N}{\frac{N}{k-m} + m - n} = m + \frac{N}{\frac{N}{k-n} + n - m},$$

savoir,

$$(m-n)^2 = 2N.$$

Donc la différence entre deux valeurs de m ne peut acquérir que deux valeurs différentes ; donc m ne peut avoir plus de trois valeurs ; donc enfin $p = 3$. Ainsi, c'est seulement dans ce cas que le groupe réduit pourra contenir des substitutions de l'ordre p.

Et, en effet, la réduite sera alors du quatrième degré, et par conséquent soluble par radicaux.

Nous savons par là qu'en général, parmi les substitutions de notre groupe réduit, il ne devra pas se trouver de substitutions de l'ordre p. Peut-il y en avoir de l'ordre $p-1$? C'est ce que je vais rechercher[2].

---

[2] J'ai cherché inutilement dans les papiers de Galois la continuation de ce qu'on vient de lire.
A. Ch.

Préface

`` Cecy est un livre de bonne foy. Montagne.

.....Si avec aussi peu de chances d'être compris, je publie, malgré tout, le fruit de mes veilles, c'est afin de prendre date pour mes recherches, c'est afin que les amis que j'ai formés dans le monde avant qu'on m'enterrât sous les verrous, sachent que je suis bien en vie, c'est peut-être aussi dans l'espérance que ces recherches pourront tomber entre les mains de personnes à qui une morgue stupide n'en interdira pas la lecture, et les diriger dans la nouvelle voie que doit, selon moi, suivre l'analyse dans ses branches les plus hautes. Il faut bien savoir que je ne parle ici que d'analyse pure; mes assertions transportées aux applications les plus directes des mathématiques deviendraient paradoxales.

Les longs calculs algébriques ont d'abord été peu nécessaires au progrès des Mathématiques, les théorèmes fort simples gagnaient à peine à être traduits dans la langue de l'analyse. Ce n'est guère que depuis Euler que cette langue plus brève est devenue indispensable à la nouvelle extension que ce grand géomètre a donnée à la science. Depuis Euler les calculs sont devenus de plus en plus nécessaires, mais de plus en plus difficiles à mesure qu'ils s'appliquaient à des objets de science plus avancés. Dès le commencement de ce siècle, l'algorithme avait atteint un degré de complication tel que tout progrès était devenu impossible par ce moyen, sans l'élégance que les géomètres modernes ont su imprimer à leurs recherches, et au moyen de laquelle l'esprit saisit promptement et d'un seul coup un grand nombre d'opérations.

Il est évident que l'élégance si vantée et à si juste titre, n'a pas d'autre but.

Du fait bien constaté que les efforts des géomètres les plus avancés ont pour objet l'élégance, on peut donc conclure avec certitude qu'il devient de plus en plus nécessaire d'embrasser plusieurs opérations à la fois, parce que l'esprit n'a plus le temps de s'arrêter aux détails.

Or je crois que les simplifications produites par l'élégance des calculs, (simplifications intellectuelles, s'entend; de matérielles il n'y en a pas) ont leurs limites; je crois que le moment arrivera où les transformations algébriques prévues par les spéculations des analystes ne trouveront plus ni le temps ni la place de se produire; à tel point qu'il faudra se contenter de les avoir prévues. Je ne veux pas dire qu'il n'y a plus rien de nouveau pour l'analyse sans ce secours: mais je crois qu'un jour sans cela tout serait épuisé.

Sauter à pieds joints sur ces calculs; grouper les opérations, les classer suivant leurs difficultés et non suivant leurs formes; telle est, suivant moi, la mission des géomètres futurs; telle est la voie où je suis entré dans cet ouvrage.

Il ne faut pas confondre l'opinion que j'émets ici, avec l'affectation que certaines personnes ont d'éviter en apparence toute espèce de calcul, en traduisant par des phrases fort longues ce qui s'exprime très brièvement par l'algèbre, et ajoutant ainsi á la longueur des opérations, les longueurs d'un langage qui n'est pas fait pour les exprimer. Ces personnes-là sont en arrière de cent ans.

Ici rien de semblable; ici on fait l'analyse de l'analyse: ici les calculs les plus élevés exécutés jusqu'à présent sont considérés comme des cas particuliers, qu'il a été utile, indispensable de traiter, mais qu'il serait funeste de ne pas abandonner pour des recherches plus larges. Il sera temps d'effectuer des calculs prévus par cette haute analyse et classés suivant leurs difficultés, mais non spécifiés dans leur forme, quand la spécialité d'une question les réclamera.

La thèse générale que j'avance ne pourra être bien comprise que quand on lira attentivement mon ouvrage qui en est une application: non que ce point de vue théorique ait précédé l'application; mais je me suis demandé, mon livre terminé, ce qui le rendrait si étrange à la plupart des lecteurs, et rentrant en moi-même, j'ai cru observer cette tendance de mon esprit à éviter les calculs dans les sujets que je traitais, et qui plus est, j'ai reconnu une difficulté insurmontable à qui voudrait les effectuer généralement dans les matières que j'ai traitées.

On doit prévoir que, traitant des sujets aussi nouveaux, hasardé dans une voie aussi insolite, bien souvent des difficultés se sont présentées que je n'ai pu vaincre. Aussi dans ces deux mémoires et surtout dans le second qui est plus récent, trouvera-t-on souvent la formule "je ne sais pas"). La classe des lecteurs dont j'ai parlé au commencement ne manquera pas d'y trouver à rire. C'est que malheureusement on ne se doute pas que le livre le plus précieux du plus savant serait celui où il dirait tout ce qu'il ne sait pas, c'est qu'on ne se doute pas qu'un auteur ne nuit jamais tant à ses lecteurs que quand il dissimule une difficulté. Quand la concurrence c'est-à-dire l'égoïsme ne règnera plus dans les sciences, quand on s'associera pour étudier, au lieu d'envoyer aux académies des paquets cachetés, on s'empressera de publier ses moindres observations pour peu qu'elles soient nouvelles, et on ajoutera: "je ne sais pas le reste".

De Ste Pélagie, décembre 1831,

EVARISTE GALOIS. "

The second tract by Galois:

``Sur l'Enseignement des Sciences, des Professeurs, des Ouvrages, des Examinateurs

MONSIEUR LE RÉDACTEUR,
Je vous serais obligé, si vous voulez bien accueillir les réflexions suivantes, relatives à l'étude des mathématiques dans les collèges de Paris.

D'abord dans les sciences, les opinions ne comptent pour rien; les places ne sauraient être la récompense de telle ou telle manière de voir en politique ou en religion. Je m'informe si un professeur est bon ou mauvais, et je m'inquiète fort peu de sa façon de penser dans des matières étrangères à ses études scientifiques. Ce n'était donc pas sans douleur et indignation que, sous le gouvernement de la restauration, on voyait les places devenir la proie des plus offrants en fait d'idées monarchiques et religieuses. Cet état de choses n'est pas changé; la médiocrité, qui fait preuve de sa répugnance pour le nouvel ordre de choses, est encore privilégiée; et cependant les opinions ne devraient pas être mises en ligne de compte, lorsqu'il s'agit d'apprécier le mérite scientifique des individus.

Commençons par les collèges; là les élèves de mathématiques se destinent pour la plupart à l'école polytechnique; que fait-on pour les mettre en état d'atteindre ce but ? Cherche-t-on à leur faire concevoir le véritable esprit de la science par l'exposé des méthodes les plus simples ? Fait-on en sorte que le raisonnement devienne pour eux une seconde mémoire ? N'y aura-t-il pas au contraire quelque ressemblance entre la manière dont ils APPRENNENT les mathématiques et la manière dont ils APPRENNENT les leçons de français et de latin ? Jadis un élève aurait appris d'un professeur tout ce qui lui est utile de savoir; maintenant il faut le supplément de un, de deux

répétiteurs pour préparer un candidat à l'école polytechnique.

Jusques à quand les pauvres jeunes gens seront-ils obligés d'écouter ou de répéter toute la journée ? Quand leur laissera-t-on du temps pour méditer sur cet amas de connaissances, pour coordonner cette foule de propositions sans suite, de calculs sans liaison ? N'y aurait-il pas quelque avantage à exiger des élèves les mêmes méthodes, les mêmes calculs, les mêmes formes de raisonnement, s'ils étaient à la fois les plus simples et les plus féconds ? Mais non, on enseigne minutieusement des théories tronquées et chargées de réflexions inutiles, tandis qu'on omet les propositions les plus simples et les plus brillantes de l'algèbre; au lieu de cela, on démontre à grands frais de calculs et de raisonnements toujours longs, quelquefois faux, des corollaires dont la démonstration se fait d'elle-même.

D'où vient le mal ? Assurément ce n'est pas des professeurs des collèges; ils montrent tous un zèle fort louable; ils sont les premiers à gémir de ce qu'on ait fait de l'enseignement des mathématiques un véritable métier. La cause du mal, c'est aux libraires de MM. les examinateurs qu'il faut la demander. Les libraires veulent de gros volumes: plus il y a de choses dans les ouvrages des examinateurs, plus ils sont certains d'une vente fructueuse; voilà pourquoi nous voyons apparaître chaque année ces volumineuses compilations où l'on voit les travaux défigurés des grands maîtres à côté des essais de l'écolier.

D'un autre côté, pourquoi les examinateurs ne posent-ils les questions aux candidats que d'une manière entortillée ? Il semblerait qu'ils craignissent d'être compris de ceux qu'ils interrogent; d'où vient cette malheureuse habitude de compliquer les questions de difficultés artificielles ? Croit-on donc la science trop facile ? Aussi qu'arrive-t-il ? L'élève est moins occupé de s'instruire que de passer son examen. Il lui faut sur chaque théorie une RÉPÉTITION de chacun des quatre examinateurs; il doit apprendre les methodes qu'ils affectionnent, et savoir à l'avance, pour chaque question et chaque examinateur, quelles doivent être ses réponses et même son maintien. Aussi il est vrai de dire qu'on a fondé depuis quelques années une science nouvelle qui va grandissant chaque jour, et qui consiste dans la connaissance des dégoûts et des préférences scientifiques, des manies et de l'humeur de MM. les examinateurs.

Etes-vous assez heureux pour sortir vainqueur de l'épreuve ? Etes-vous enfin désigné comme l'un des deux cents géomètres à qui on porte les armes dans Paris ? Vous croyez être au bout: vous vous trompez, c'est ce que je vous ferai voir dans une prochaine lettre.

E. G. "

Notes:
Cette lettre d'Evariste Galois, fut publiée dans Gazette des Ecoles: Journal de l'Instruction Publique, de l'Université, des Séminaires, numéro 110, 2e année, Janvier 1831.
Aucune deuxième lettre n'a été publiée.

Snurpf et plan complexe (Denise Vella-Chemla, janvier 2024)

On poursuit l'étude d'un système de représentation par les restes (modulaires) pour les parties finies de $\mathbb{N}$ (ou *Snurpf*) associé à un positionnement des nombres dans le plan complexe.

1. Introduction : présentation de la représentation du *Snurpf* dans le plan complexe

Pour illustrer le *Snurpf complexe*, voyons comment il positionne les entiers de 1 à $210 = 2 \times 3 \times 5 \times 7$ dans le plan complexe.

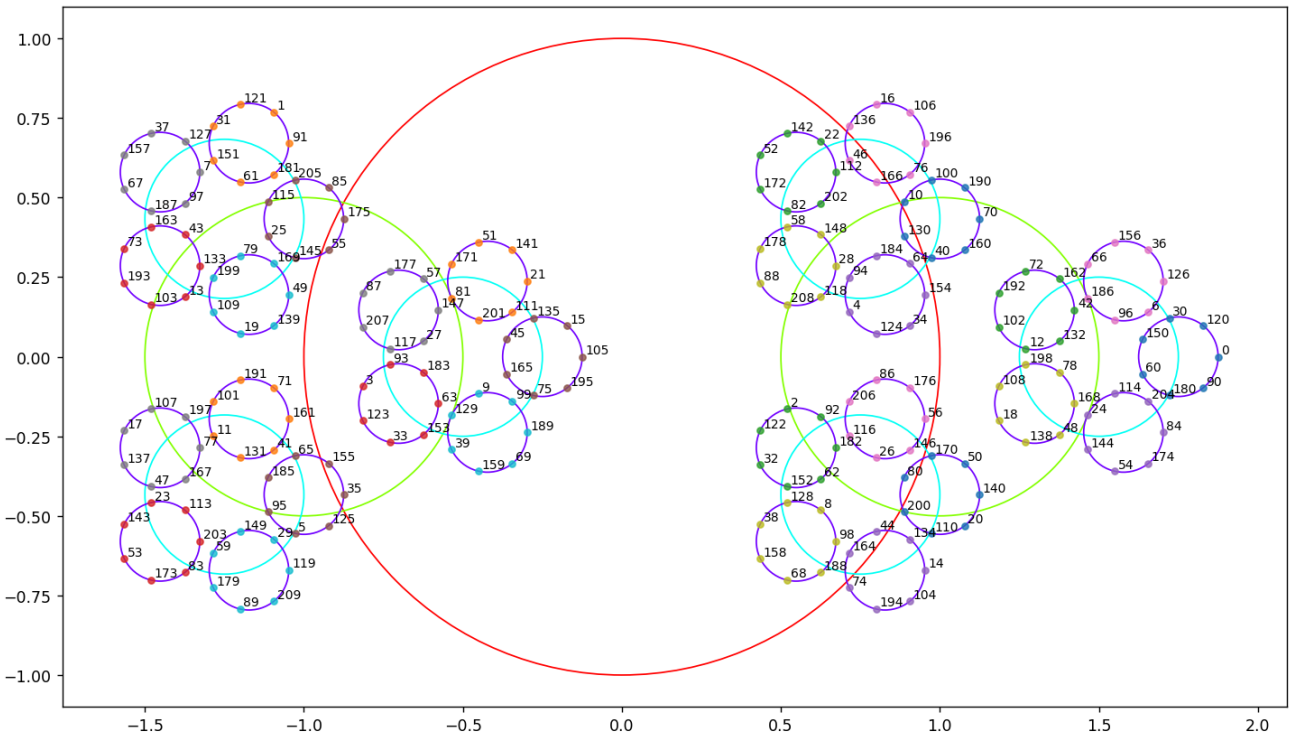


FIGURE 1 : Placement des 210 premiers nombres dans le plan complexe par le *Snurpf*

Chaque nombre est positionné dans le plan complexe suivant ses restes de division euclidienne par les nombres premiers d'une base, ici $\mathscr{B} = \{2, 3, 5, 7\}$.

Les nombres pairs sont positionnés dans le demi-plan réel supérieur (droit), les nombres impairs sont positionnés dans le demi-plan réel inférieur (gauche).

L'affixe d'un nombre n est $\sum_{k=1}^{|\mathscr{B}|=4} \frac{1}{2^k} e^{\frac{2i\pi(n \bmod p_k)}{p_k}}$.

On a fait ce choix des multiplications par les inverses des puissances successives de 2 pour que les positions des différents nombres ne risquent pas d'interférer les unes avec les autres dans la mesure où $\sum \frac{1}{2^k} < 1$.

Du fait du partage des restes modulo 2, 3 et 5 de tous les nombres positionnés sur un même cercle, les cercles contiennent les nombres de suites de raison 30 (de la forme $30x + a$), selon le graphique ci-dessous :

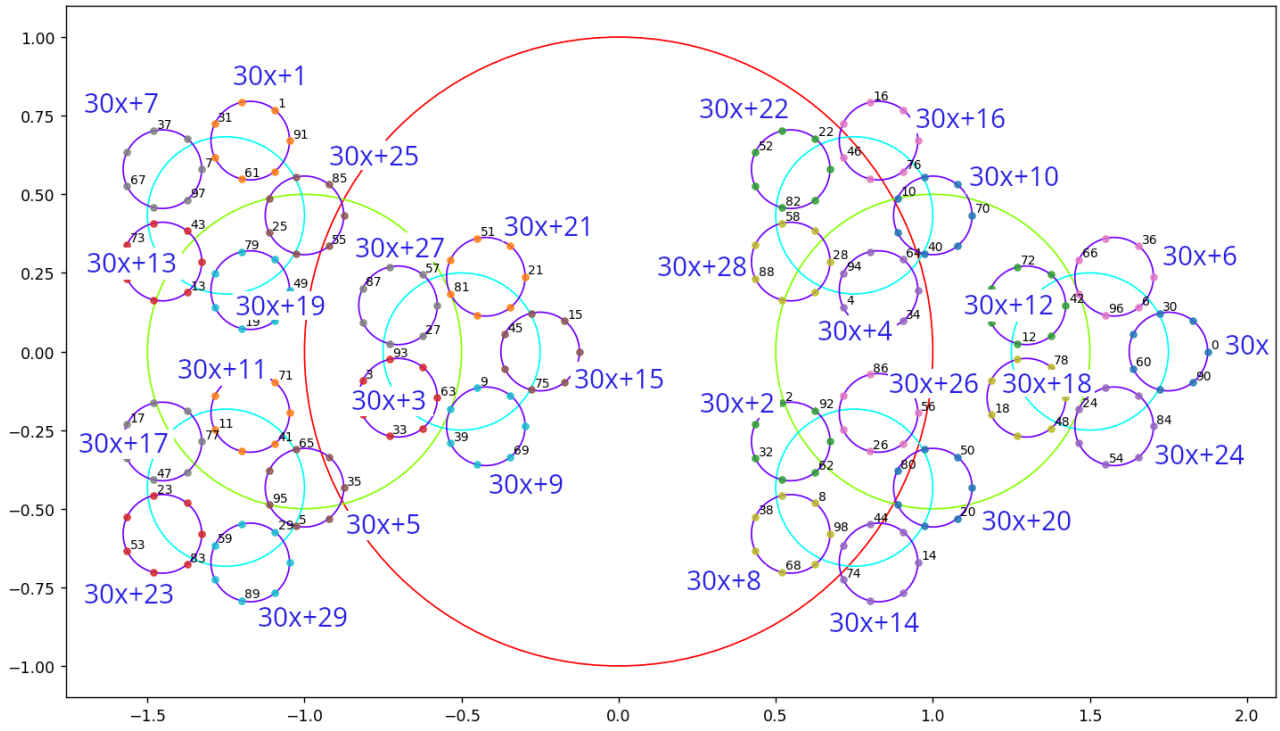


FIGURE 2 : Positionnement des suites $30x + k$ sur les différents cercles complexes

2. Propriétés qui découlent de la représentation choisie

2.1. Cribler les nombres qui partagent un reste avec 0

On souhaite *cribler les divisibles par au moins un* p_k, avec pour l'illustration considérée $p_k \in \{2, 3, 5, 7\}$.

Les *divisibles par au moins un* p_k ont leur affixe qui est dans une zone Z qu'on peut qualifier de fractale et qui a la forme présentée sur le graphique ci-dessous.

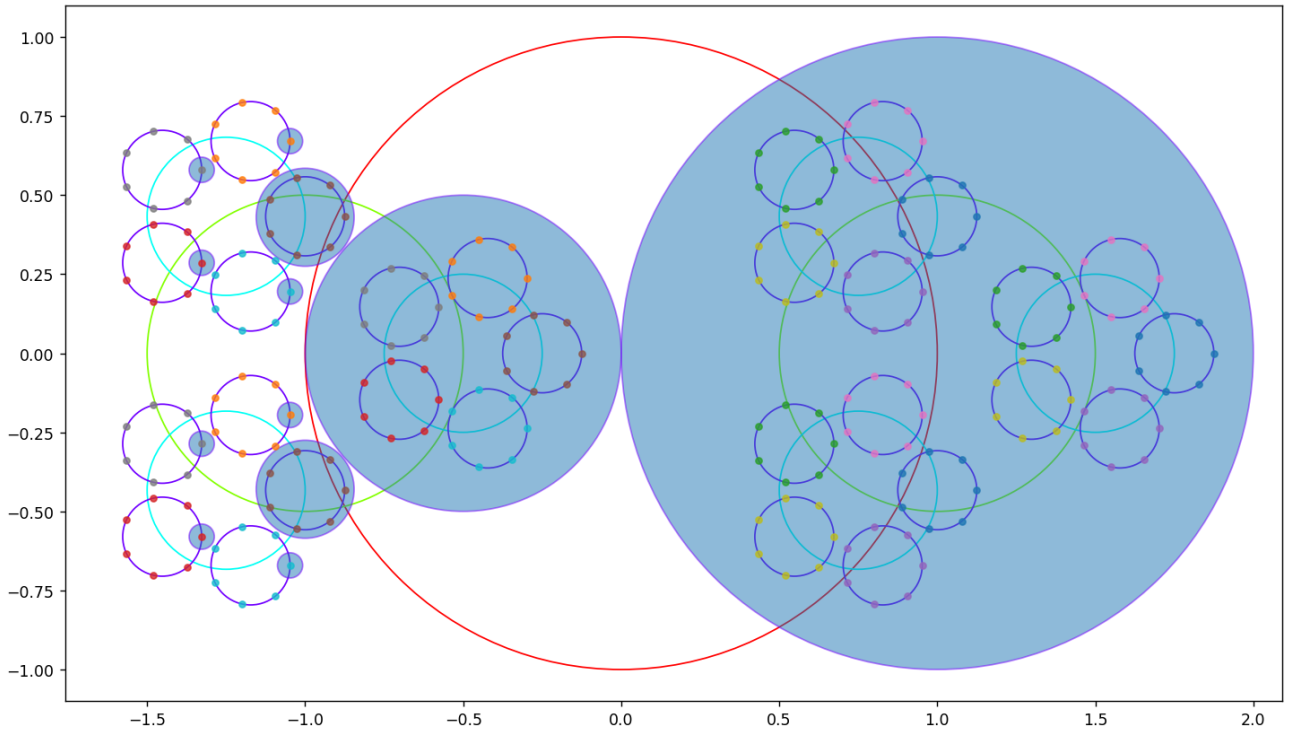


FIGURE 3 : Les *divisibles* (ou espace fractal contenant les nombres qui ont au moins un reste nul, i.e. un reste qu'ils partagent avec le nombre 0)

Le disque bleu le plus grand à droite contient tous les nombres pairs ($\equiv 0 \pmod 2$). Le disque de taille moyenne à gauche du disque le plus grand contient les nombres impairs divisibles par 3 ($\equiv 0 \pmod 3$). Les deux disques plus petits contiennent les nombres qui ne sont ni divisibles par 2 ni divisibles par 3 (qui étaient contenus par les 2 disques plus gros) mais qui sont divisibles par 5 ($\equiv 0 \pmod 5$). Enfin, les 8 disques contiennent des nombres divisibles par 7 (et non divisibles par 2, 3 ou 5).

La symétrie horizontale (par rapport à l'axe des abscisses), qui en l'occurrence envoie x sur $210 - x$, permet soit d'envoyer un nombre qui est dans la zone Z sur un nombre qui est dans la zone Z (on dira que cette opération fait rester dans la zone Z), soit d'envoyer un nombre qui est à l'extérieur de la zone Z sur un nombre qui est également à l'extérieur de la zone Z (on dira que cette opération fait rester à l'extérieur de la zone Z).

2.2. Cribler les nombres qui partagent un reste (au moins) avec n

On peut, similairement à la façon dont on a *criblé 0* au paragraphe précédent, *cribler* n.

Reprenons notre exemple classique : *cribler 98* consiste à enlever les nombres dans la zone Z' (rose) ci-dessous qui contient les nombres pairs (comme l'est 98), ainsi que (parmi les nombres restant) les nombres congrus à 2 (mod 3) (comme l'est 98), ainsi que (parmi les nombres restant) les nombres congrus à 3 (mod 5) (comme l'est 98), ainsi que (parmi les nombres restant) les nombres divisibles par 7 (congrus à 0 (mod 7), comme l'est 98).

Le fractal Z' est représenté sur le graphique ci-dessous.

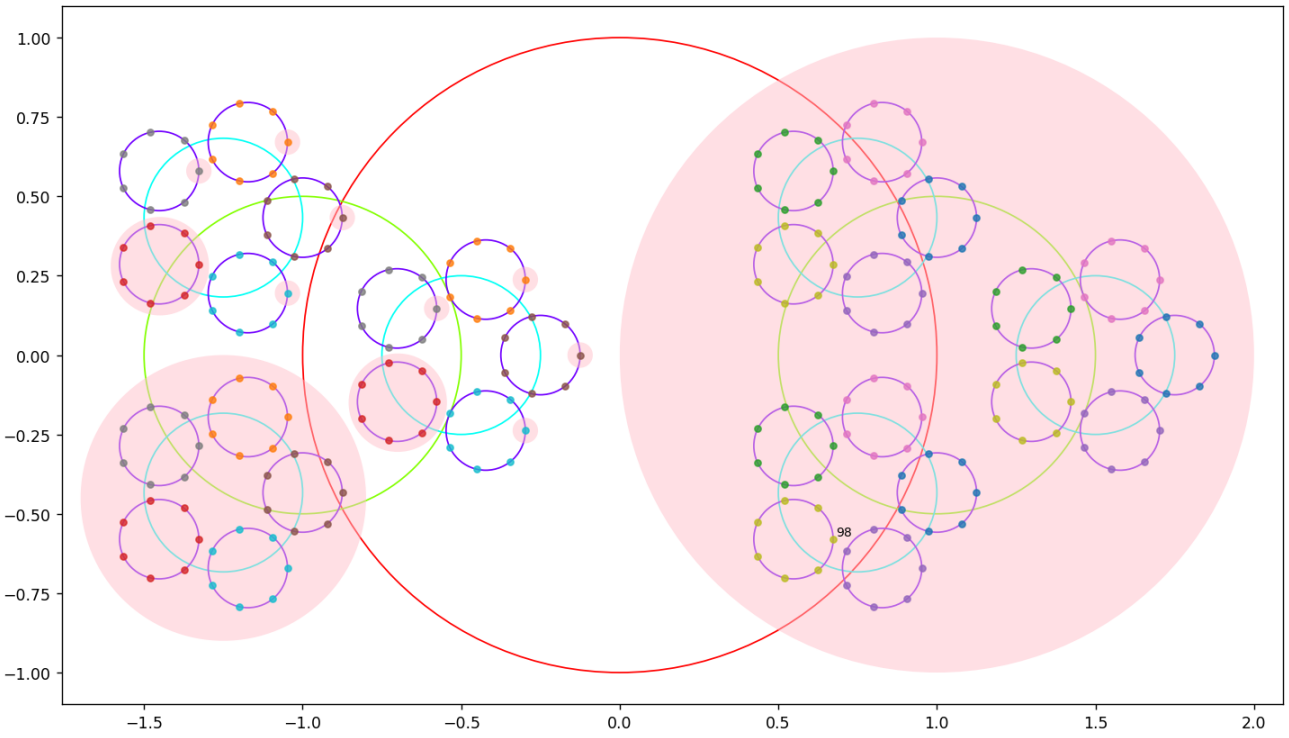


FIGURE 4 : les *congrus à* $n = 98$ (ou espace fractal contenant les nombres qui partagent au moins un reste avec n)

L'opération qui permet soit de rester dans le fractal Z', soit de rester à l'extérieur du fractal Z', est l'opération qui à x associe $2n - x$. On montre simplement dans le graphique ci-dessous les appariements (121,75) et (107,89) pour $n = 98,\ 2n = 196$.

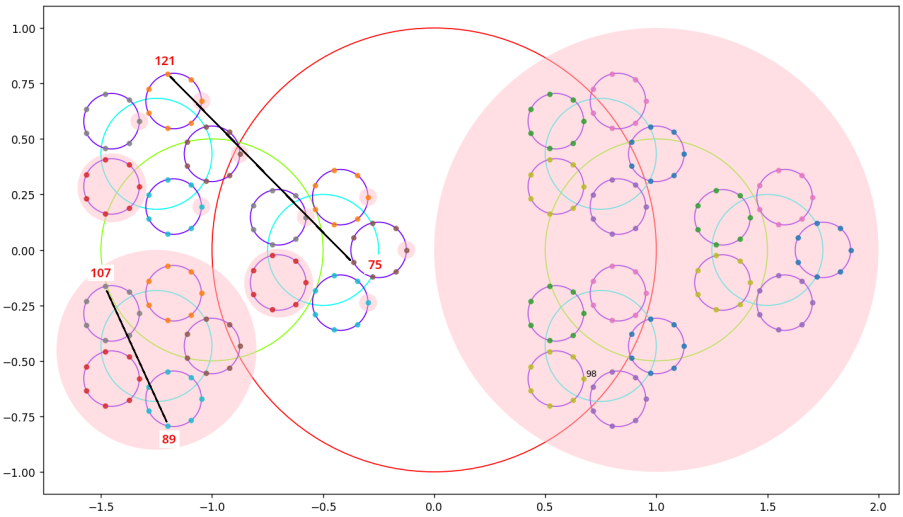


FIGURE 4 bis : opération qui fait rester dans (resp. à l'extérieur du) fractal Z'

2.3. Double crible

A été démontré (voir http://denise.vella.chemla.free.fr/jade1.pdf) qu'un nombre compris entre 3 et $n/2$ qui n'est jamais congru ni à 0 ni à n est un décomposant de Goldbach de n (compris entre $\sqrt{n}$ et $n/2$).

Appliquer ce double crible consiste à cribler les fractals Z et Z' vus aux deux paragraphes précédents, selon le graphique ci-dessous.

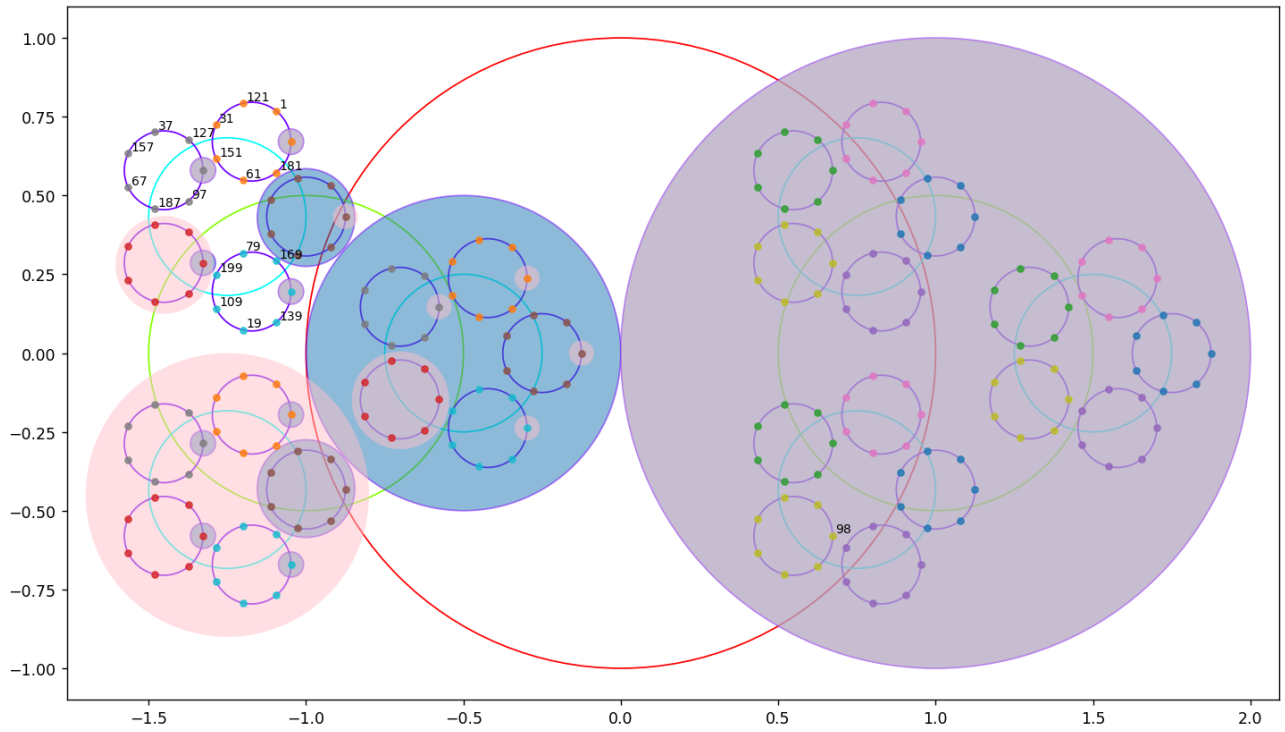


FIGURE 5 : double crible (des nombres qui partagent au moins un reste avec 0 ainsi que des nombres qui partagent au moins un reste avec n)

On comprend aisément que les diviseurs premiers p_{div} de n ne font éliminer qu'une seule classe de congruence au lieu de deux modulo p_{div} : ils font cribler la seule classe modulaire $\equiv 0 \pmod{p_{div}}$, alors que les nombres premiers p_{nondiv} qui ne divisent pas n font cribler deux disques de même taille correspondant aux classes de congruence modulaire $\equiv 0 \pmod{p_{nondiv}}$ et $\equiv n \pmod{p_{nondiv}}$.

De ce fait, les nombres qui ont peu de diviseurs premiers (comme les nombres qui sont des puissances de 2 par exemple, ou bien les nombres qui ont peu de diviseurs premiers dans leur factorisation) auront, localement, bien moins de décomposants de Goldbach que les entiers qui sont proches d'eux.

2.4. Brisure de symétrie de la représentation par n

On rappelle l'anecdote du clavier de piano, et de ses touches noires et blanches : c'est le fait qu'il y ait des paquets de 3 touches noires d'une part, et des paquets de 2 touches noires d'autre part (la brisure de symétrie), qui permet de trouver la position de la note *do* sur un clavier (touche blanche

immédiatement contigue (à gauche) à un paquet de deux touches noires).

On a vu ci-dessus qu'on pouvait *cribler l'espace par un nombre*. On va maintenant *symétriser l'espace par un nombre* n, i.e. apparier les nombres x et y dont la somme $\sigma_n = x + y$ est congrue à n modulo le produit des éléments de la base $\mathscr{B}$ (i.e. $\sigma_n = x + y \equiv n \pmod{\prod_{b_k \in \mathscr{B}} b_k}$),.

Pour poursuivre avec l'exemple du nombre 98, qui se trouve être égal à 308 modulo 210, 98 permet d'associer les différents cercles de la représentation de la façon suivante.

À la manière dont Gauss enfant associait les nombres 2 à 2 pour calculer la somme des 100 premiers nombres entiers, on peut voir le nombre 98 comme procédant à l'association suivante entre les nombres compris entre 1 et 210.

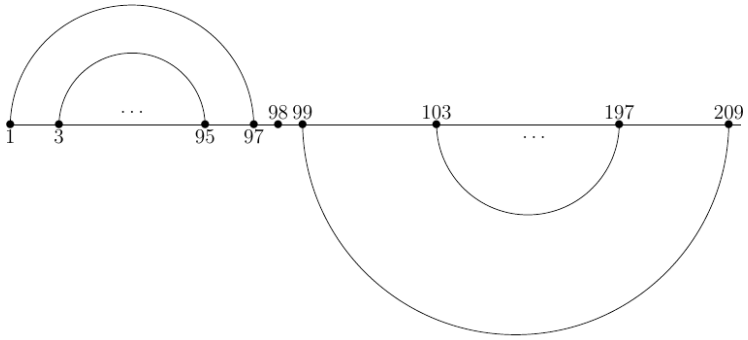


FIGURE 6 : positionnement des sommes de deux termes $\equiv 98 \pmod{210}$ sur l'intervalle $[1, 210]$

Présentons d'abord pour deux cercles l'appariement par somme pour $n = 98$ (noter les sens de rotation inversés sur les deux cercles).

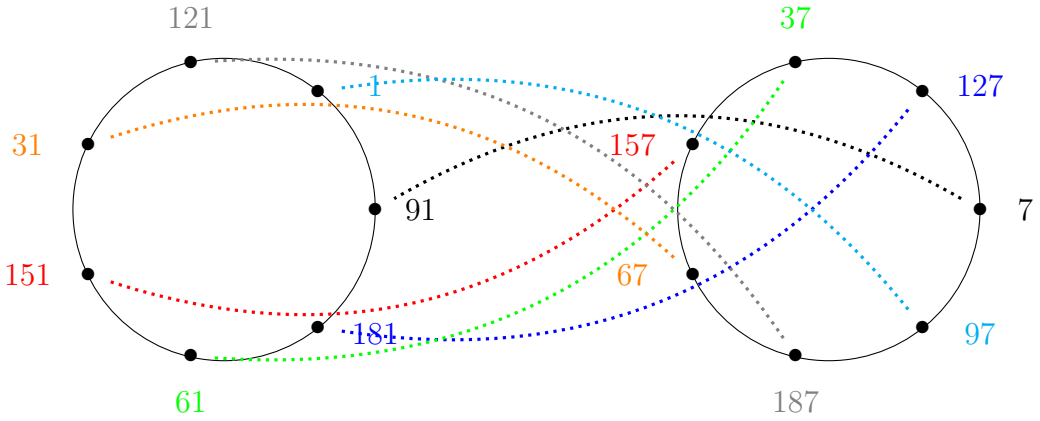


FIGURE 7 : appariement des cercles pour $n = 98$

Voyons comment les cercles sont globalement appariés par somme pour $n = 98$.

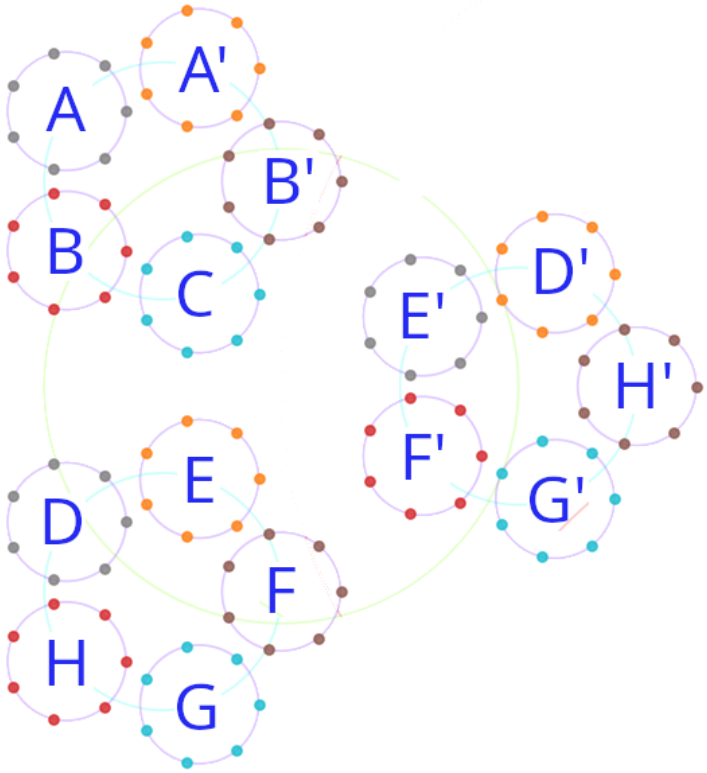


FIGURE 8 : appariement des cercles pour $n = 98$

Les deux lettres A et A' représentent le fait que les $30x + 7$ sont appariés ainsi aux $30x + 1$ (pour que la somme 98 soit maintenue, 98 étant un $30x + 8$, on tourne dans le sens horaire sur un cercle et dans le sens anti-horaire sur l'autre cercle) :

7	127	37	157	67	187	97
91	181	61	151	31	121	1

Certains cercles sont appariés avec eux-mêmes (par exemple le cercle des $30x + 19$ pour $n = 98$ selon le graphique ci-dessous, la somme de deux $30x + 19$ donnant un $30x + 8$).

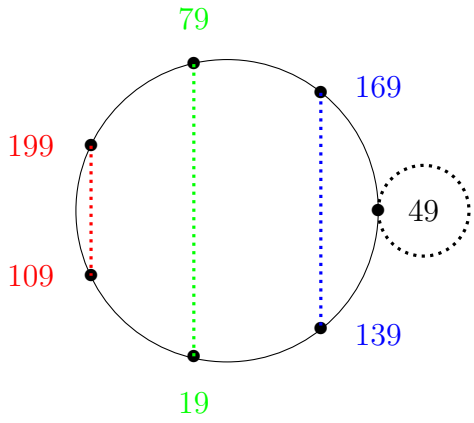


FIGURE 9 : exemple d'appariement d'un cercle avec lui-même ; les sommes de sommets appariés sont toutes congrues à 98 (mod 210).

Lorsqu'on crible deux classes de congruences au maximum selon chaque nombre premier, restent forcément au moins $\prod_{k=1}^{4}(p_k - 2)$ nombres appariés. Ces nombres qui, dans une certaine proportion, sont inférieurs à n, fournissent les décompositions de Goldbach cherchées.

Exemple pour $n = 128 = 19{+}109 = 31{+}97 = 61{+}67$ (il y a un schisme, les positions se chevauchent, voir en annexe une autre représentation par cercles tangents internes pour éviter le chevauchement).

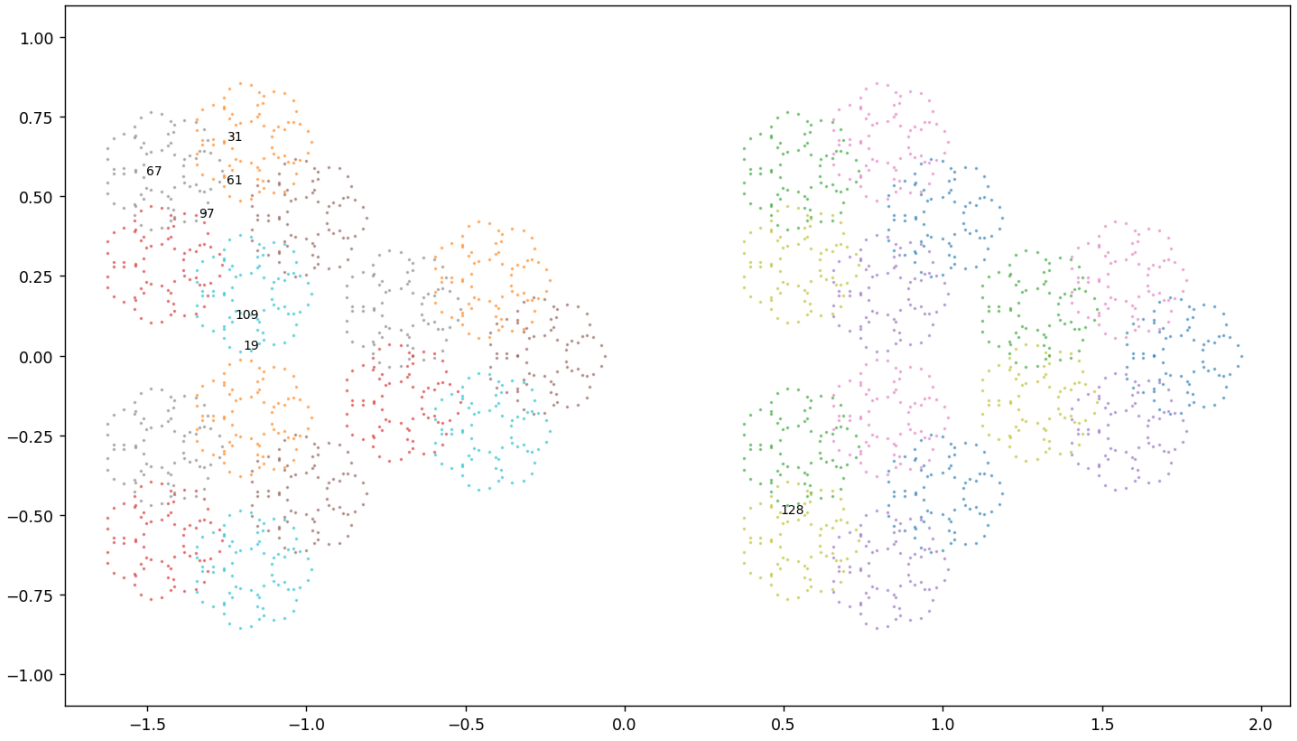


FIGURE 10 : décomposants de Goldbach de $n = 128$

Exemple pour $n = 256 = 5 + 251 = 17 + 239 = 23 + 233 = 29 + 227 = 59 + 197 = 83 + 173 = 89 + 167 = 107 + 149$:

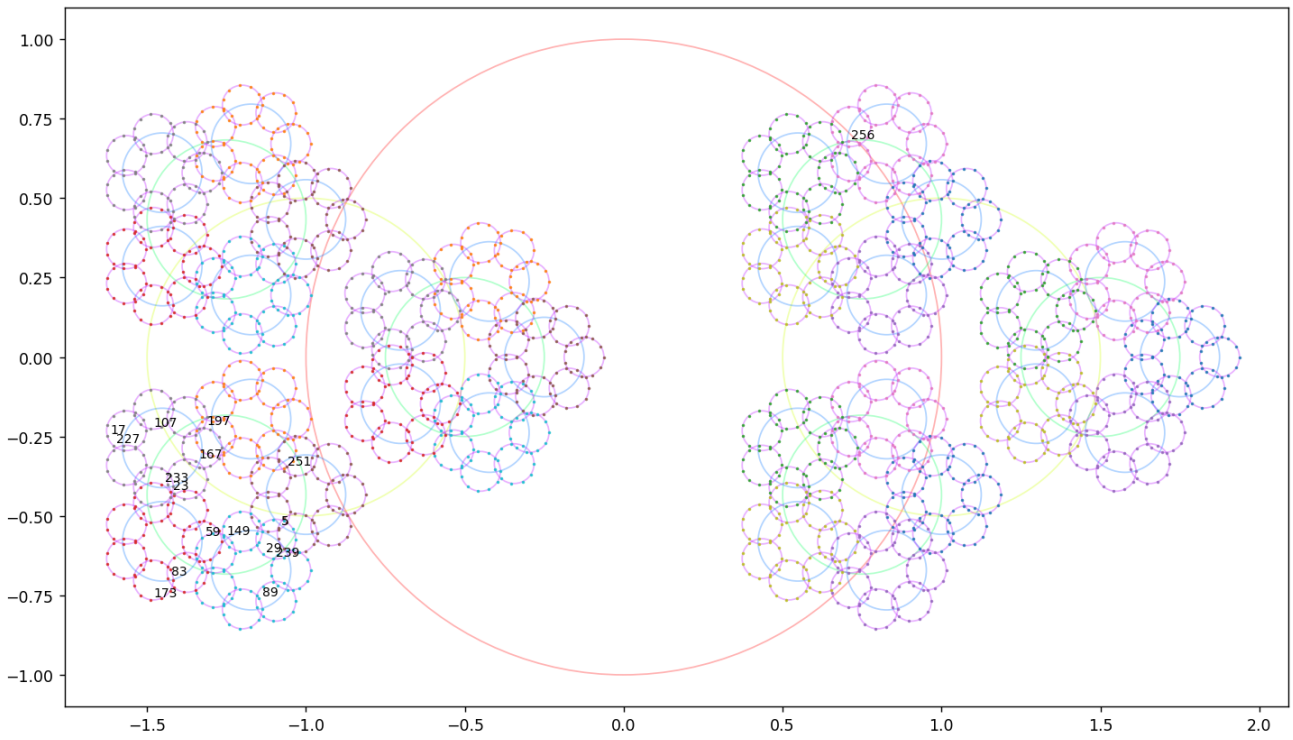


FIGURE 11 : décomposants de Goldbach de $n = 256$ avec $\mathscr{B} = \{2, 3, 5, 7, 11\}$

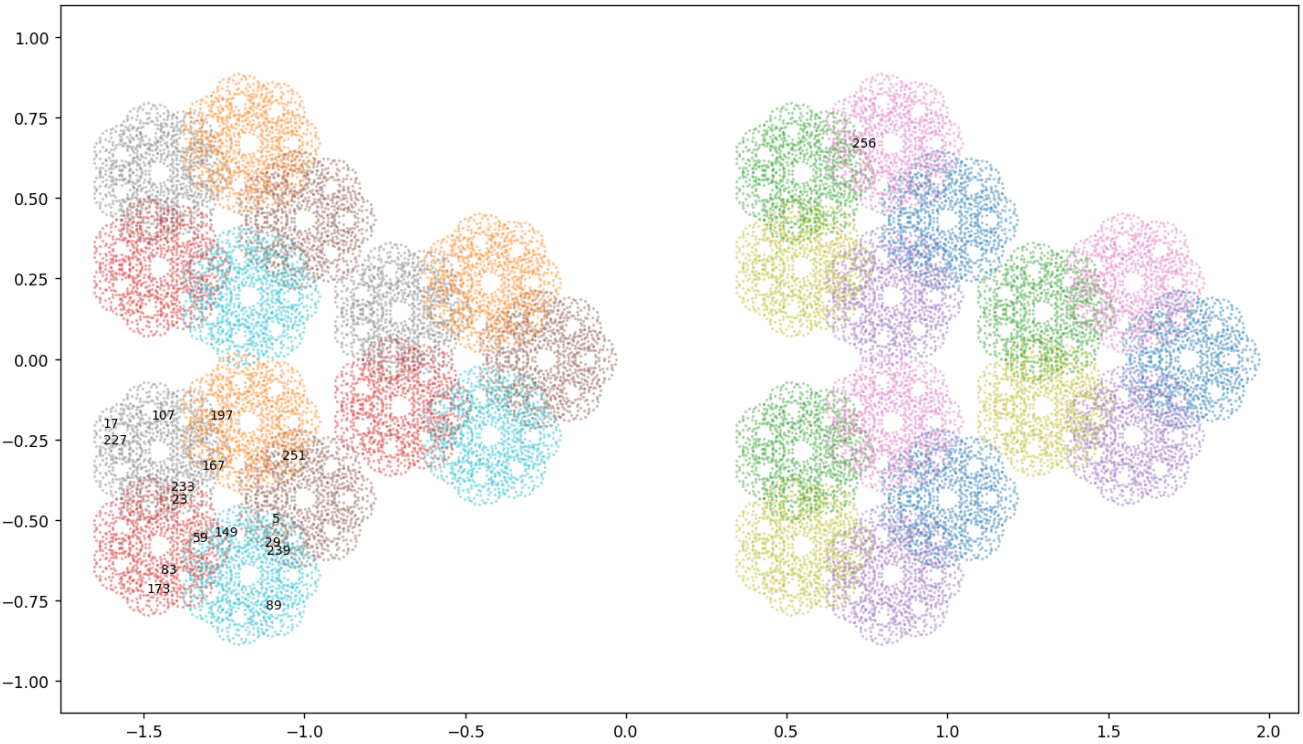


FIGURE 12 : décomposants de Goldbach de $n = 256$ avec $\mathscr{B} = \{2, 3, 5, 7, 11, 13\}$

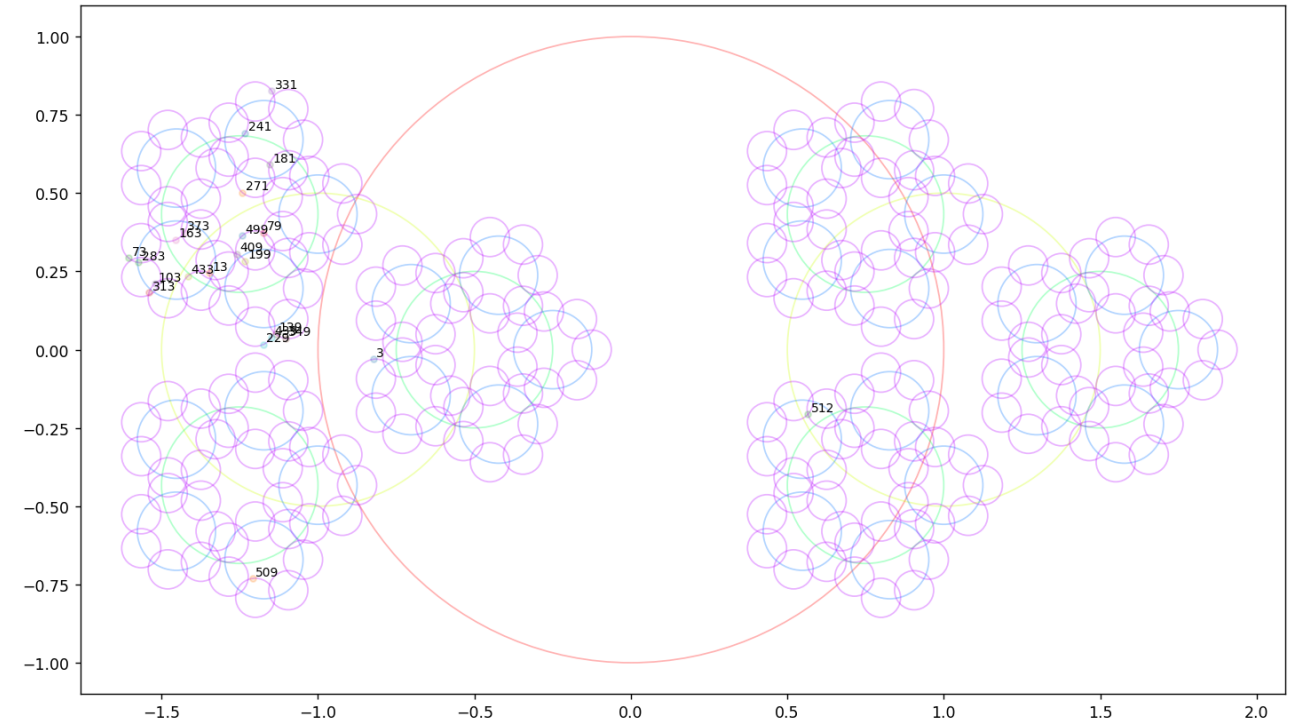


FIGURE 13 : décomposants de Goldbach de $n = 512$ avec $\mathscr{B} = \{2, 3, 5, 7, 11\}$

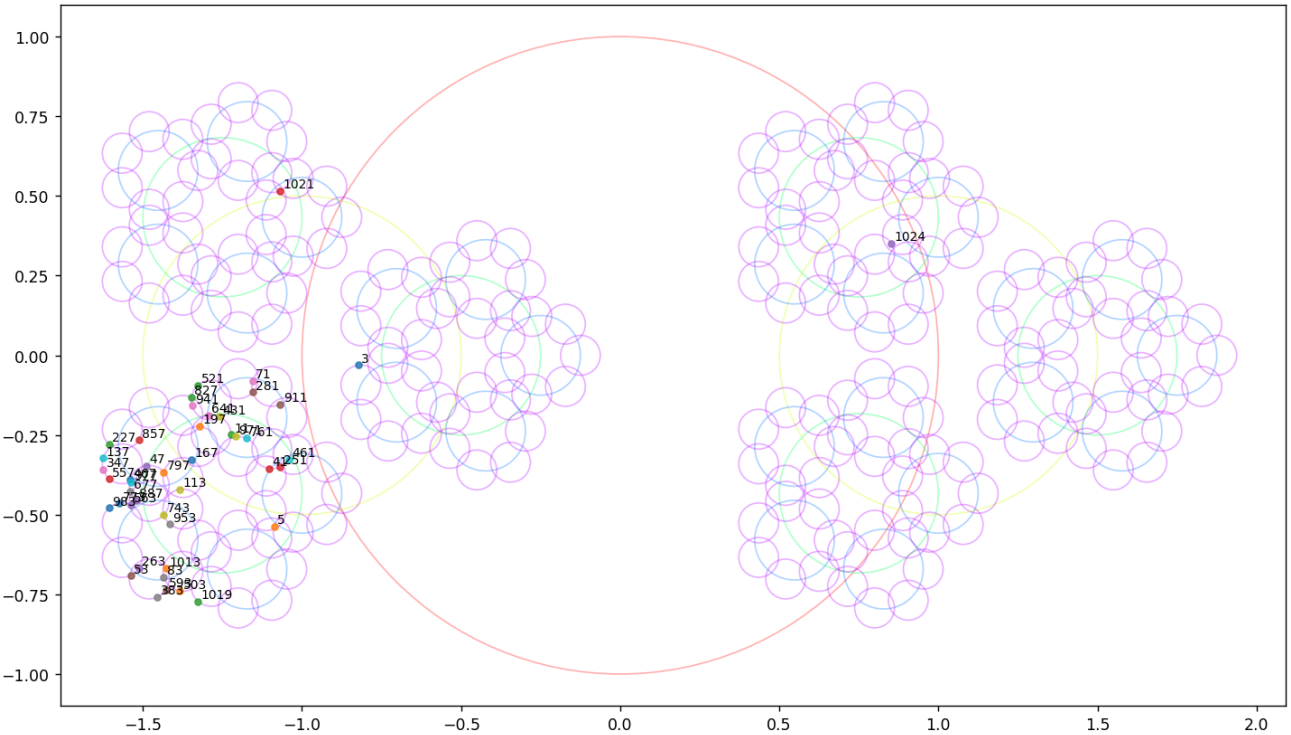


FIGURE 14 : décomposants de Goldbach de $n = 1024$ avec $\mathscr{B} = \{2, 3, 5, 7, 11\}$

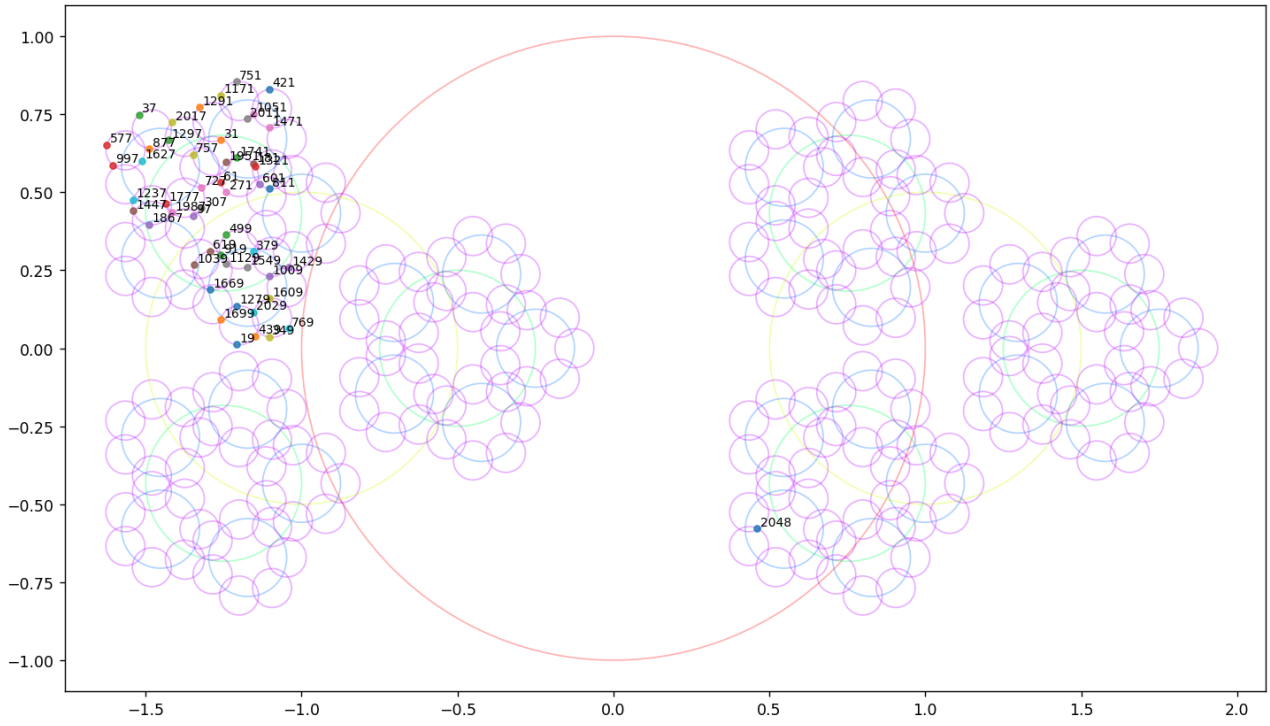


FIGURE 15 : décomposants de Goldbach de $n = 2048$ avec $\mathscr{B} = \{2, 3, 5, 7, 11\}$

Annexe 1 : La représentation choisie initialement occasionnant des chevauchements de nombres, on lui préfèrera la représentation ci-dessous par des cercles internes tangents au cercle correspondant au nombre premier précédent[1].

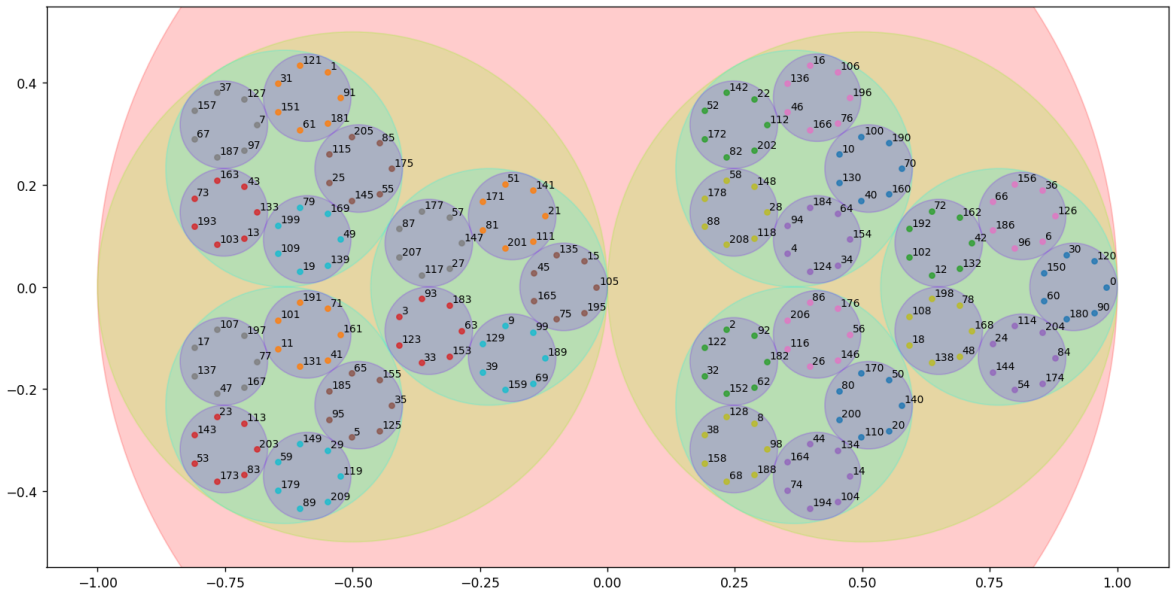
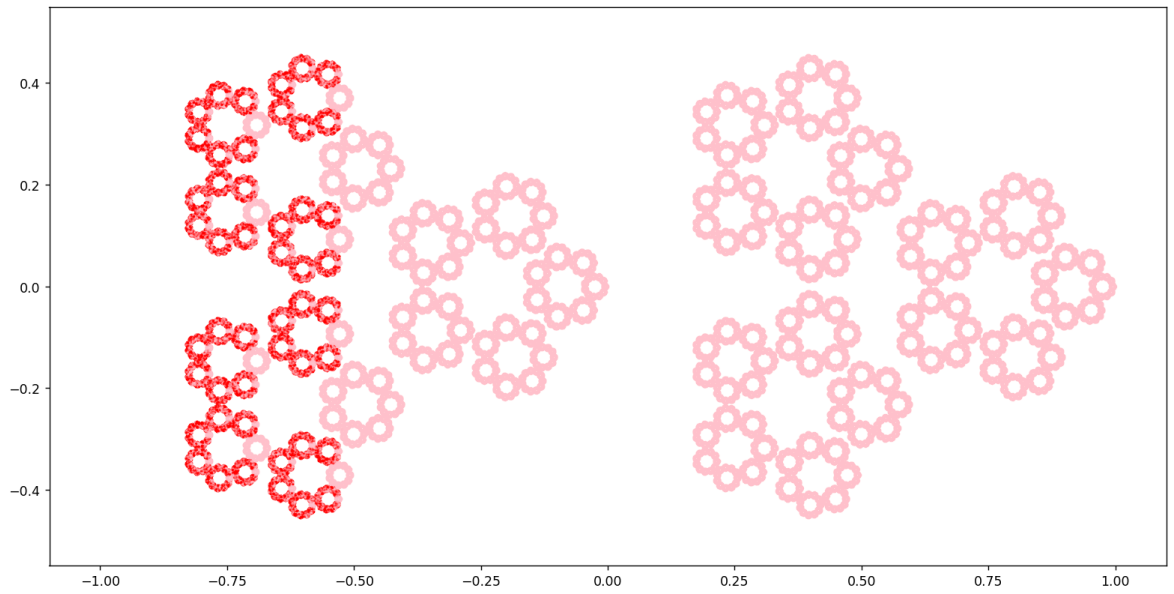


FIGURE 16 : représentation par cercles tangents internes au cercle correspondant au nombre premier précédent avec $\mathscr{B} = \{2, 3, 5, 7\}$

Annexe 2 : En se focalisant sur les nombres inférieurs à 510510 = 17#, (le symbole # dénote la primorielle, i.e. produit des nombres premiers successifs de 2 à 17), si l'on colorie en rouge les points correspondant aux nombres premiers et en rose ceux correspondant aux nombres composés, on voit les nombres premiers se concentrer sur les cercles à l'extrême gauche du graphique.



[1]Merci Jacques.

FIGURE 17 : positionnement des nombres premiers (en rouge) et des nombres composés (en rose) sur la représentation du *Snurpf* dans le plan complexe.

On voit clairement la symétrie des positionnement des nombres premiers de la forme $6x + 1$ et $6x + 5$. Additivement, les nombres pairs de la forme $6x + 2$ se décomposent en sommes de deux nombres premiers de la forme $6x + 1$, les nombres pairs de la forme $6x + 4$ se décomposent en sommes de deux nombres premiers de la forme $6x + 5$ tandis que les nombres pairs de la forme $6x$ se décomposent en sommes d'un nombre premier de la forme $6x + 1$ et d'un nombre premier de la forme $6x + 5$ (en deux fois plus de sommes donc).

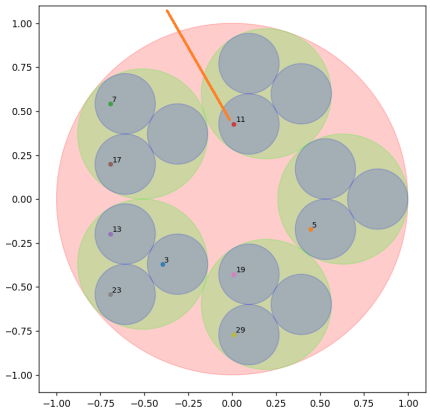
Reste à démontrer pourquoi l'opérateur $x \mapsto n - x$ pour n un nombre pair supérieur à 4 ne peut pas envoyer tous les nombres premiers inférieurs à $n/2$ dans la zone Z' définie par le double criblage du paragraphe 2.3.

Compléments à *Snurpf et plan complexe* (Denise Vella-Chemla, janvier 2024)

On a choisi dans la note qui positionne les nombres entiers naturels, représentés par des n-uplets finis de restes modulaires dans le plan complexe selon une base de nombres premiers[1] de ranger les nombres premiers de la base utilisée dans l'ordre croissant : on a alors un premier cercle[2] en contenant 2 (tangents à son périmètre) correspondants au nombre premier 2, chacun de ces cercles en contient 3 (le nombre premier suivant) qui sont tangents à leur périmètre, chacun de ces derniers en contenant 5 (le nombre premier suivant), etc[3].

On peut considérer les nombres premiers dans l'ordre inverse (par exemple, les considérer selon l'ordre $[7, 5, 3, 2]$. Le cercle initial contiendra 7 cercles tangents à son périmètre, chacun de ces cercles en contiendra 5 tangents à leur périmètre, chacun de ces derniers en contiendra 3 et chacun de ces derniers en contiendra 2.

L'avantage de cette seconde représentation est de "disperser" les nombres un peu partout dans le cercle initial (si ce n'est vers les extrêmités droites des disques (et par extension du côté droit du disque principal), les extrémités droites des disques contiennent des nombres divisibles par les nombres premiers successifs : un nombre divisible par p est positionné sur un disque contenant p positions à une position analogue dans le disque en question à la position de $e^0 = 1$ dans le disque unité). L'inconvénient de ce choix de représentation est que si l'on modifie la base $\mathscr{B}$ contenant les nombres premiers modulo lesquels on calcule les restes, la faisant passer de $[3, 2]$, à $[5, 3, 2]$, puis à $[7, 5, 3, 2]$, puis à $[11, 7, 5, 3, 2]$ en représentant de plus en plus de nombres, la position des nombres d'une représentation à l'autre va "sauter erratiquement" d'un endroit à un autre du cercle initial (voir les positions dans les différentes bases du nombre 11, désigné par un trait orange).

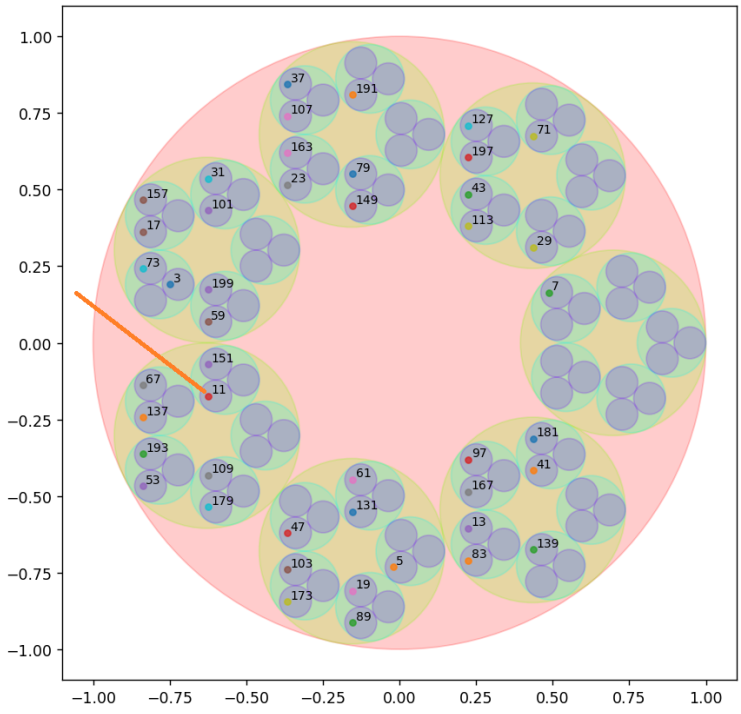


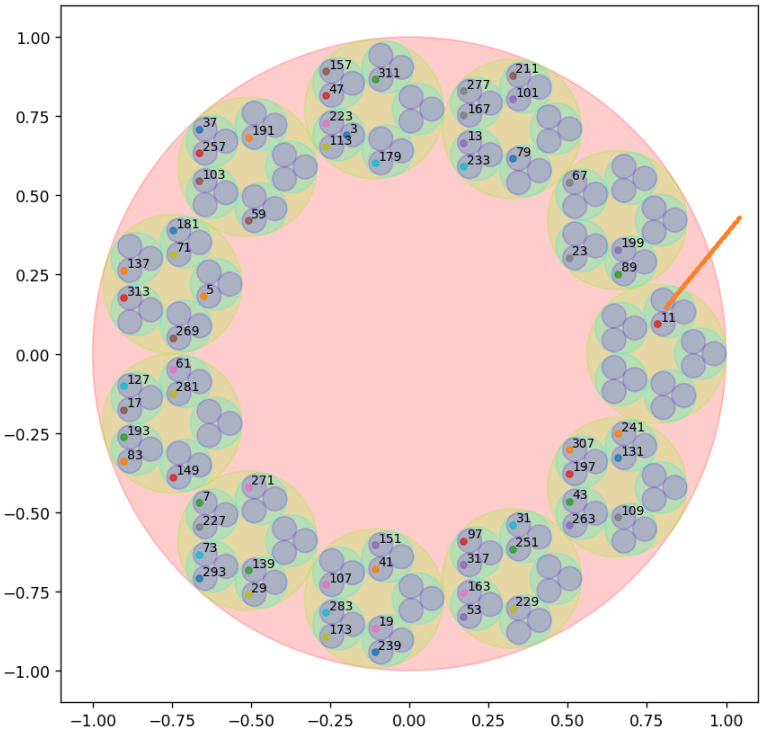
[1] Voir http://denise.vella.chemla.free.fr/snurpf-complexe.pdf.

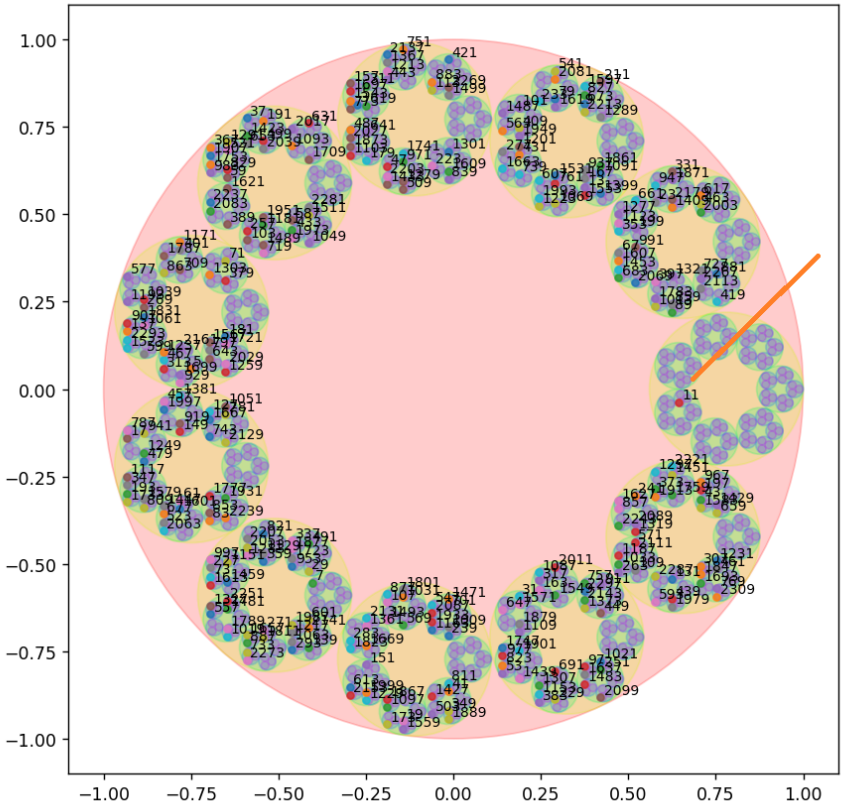
[2] Ci-après, on utilisera parfois le mot cercle, par erreur, à la place du mot disque.

[3] Les rayons des disques successifs s'obtiennent par la formule $r_k = \prod_{1 \leq j \leq k} \left(1 - \frac{1}{1 + \sin(\pi/p_j)}\right)$; on a la formule récurrente : $R_k = \frac{1}{1 + \sin(\pi/p_k)} r_{k-1}$ avec $1 \leq k \leq p$ et l'affixe du nombre n qui se calcule par la formule

$$z_n = \sum_{1 \leq k \leq p} R_k e^{2\pi i \frac{n}{p_k}}.$$


1.00
0.75
0.50
0.25
0.00
−0.25
−0.50
−0.75
−1.00
−1.00 −0.75 −0.50 −0.25 0.00 0.25 0.50 0.75 1.00
37 191 107 163 23 79 149
127 71 197 43 113 29
31 157 101 17 73 3 199 59
7
151 67 11 137 193 53 109 179
181 97 41 167 13 83 139
61 131 47 103 5 19 173 89


1.00
0.75
0.50
0.25
0.00
−0.25
−0.50
−0.75
−1.00
−1.00 −0.75 −0.50 −0.25 0.00 0.25 0.50 0.75 1.00
157 47 311 223 113 3 179
211 277 101 167 13 233 79
37 257 191 103 59
67 23 199 89
11
181 71 137 5 313 269
61 127 281 17 193 83 149
241 307 131 197 43 263 109
271 7 227 73 293 139 29
31 97 251 317 163 53 229
151 41 107 283 173 19 239



Ci-dessous les sauts erratiques des coordonnées[4] d'un endroit à l'autre.

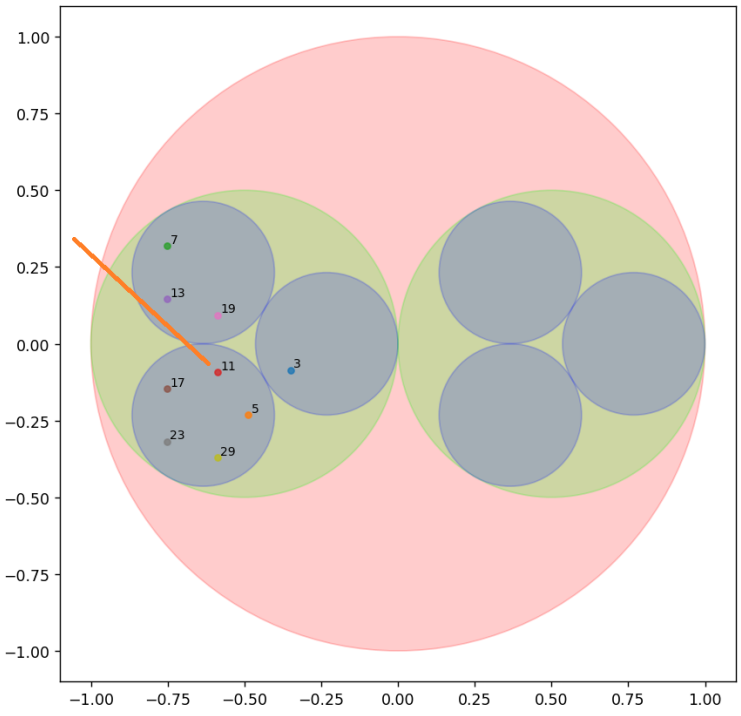
```
C:\Users\Denise_Vella\Desktop>python3 change-ordre.py
(0.009525449494428 74+0.42717642727363403j)
```

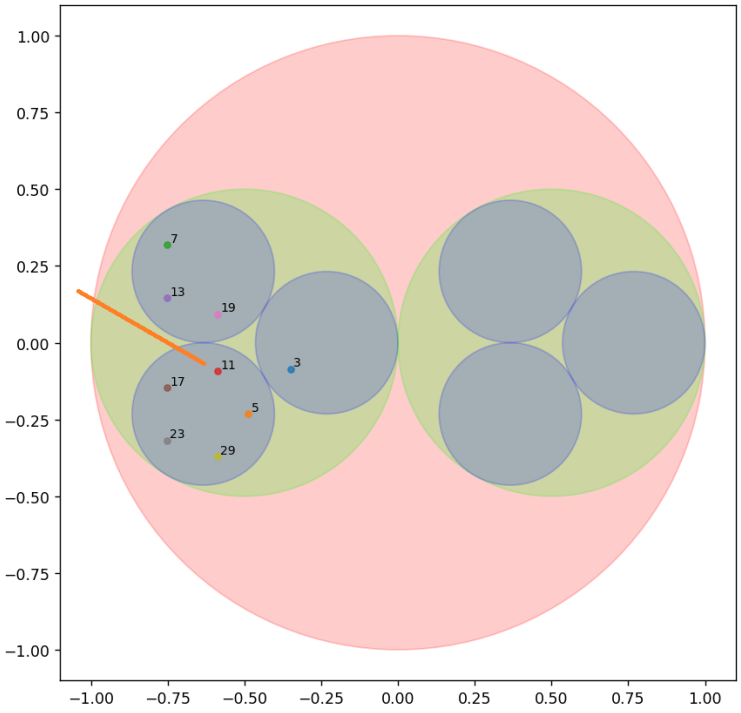
```
(-0.6254593073291511-0.17333262579722816j)
```

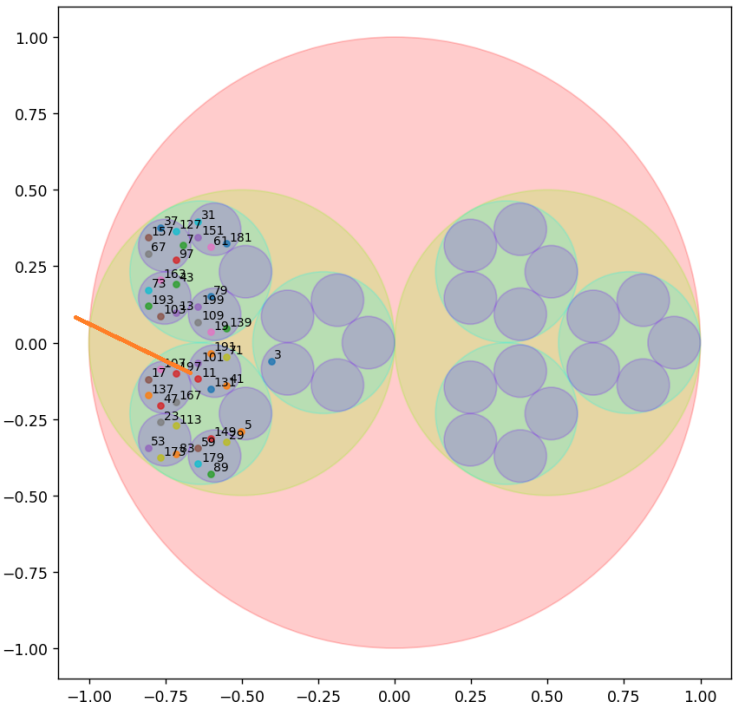
```
(0.6427142275108833-0.038099557968810586j)
```

Par opposition à cet inconvénient, l'utilisation d'une base contenant des nombres premiers croissant $[2, 3]$, puis $[2, 3, 5]$, puis $[2, 3, 5, 7]$, etc, va faire que la position d'un nombre va petit à petit tendre vers une position qui est en quelque sorte au centre d'une spirale logarithmique, comme en témoigne les exemples fournis ci-dessous (la position du nombre 11, selon différentes bases), dans lesquelles les nombres premiers sont rangés dans l'ordre croissant.

[4] auxquelles je m'identifie complètement.


1.00
0.75
0.50
0.25
0.00
−0.25
−0.50
−0.75
−1.00
−1.00
−0.75
−0.50
−0.25
0.00
0.25
0.50
0.75
1.00
7
13
19
3
11
17
5
23
29


1.00
0.75
0.50
0.25
0.00
−0.25
−0.50
−0.75
−1.00
−1.00
−0.75
−0.50
−0.25
0.00
0.25
0.50
0.75
1.00
7
13
19
3
11
17
5
23
29



Ci-dessous l'affixe associé au nombre 11, qui tend vers une limite.

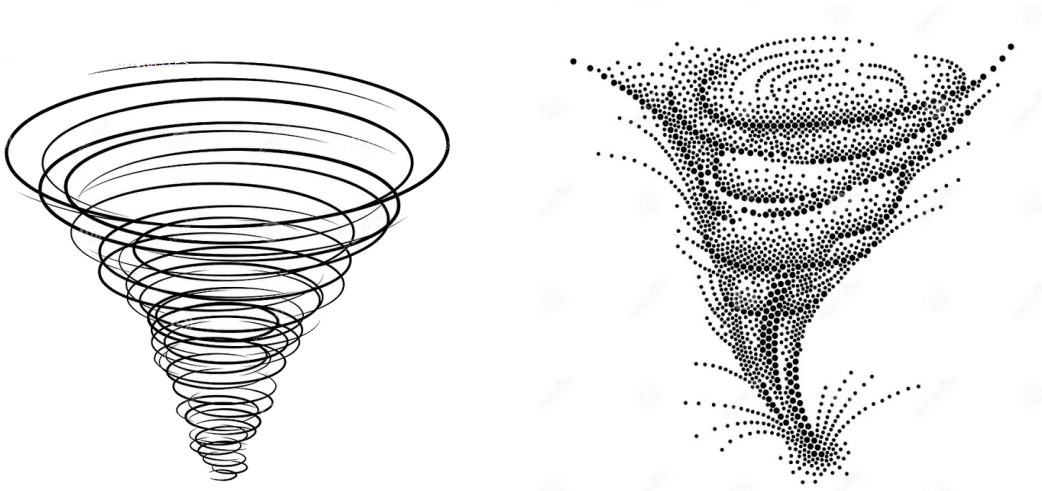
```
(-0.5888125423460718-0.09305629786972719j)
(-0.642789182842264-0.11905007794119199j)
(-0.6225089926163707-0.11905007794119199j)
(-0.6198900561645216-0.12284426242117458j)
(-0.6204517407714O6-0.12358805304576413j)
```

Du fait de la précision de notre ordinateur, la position de 11 semble "se fixer" dès le nombre premier 61 sur l'affixe

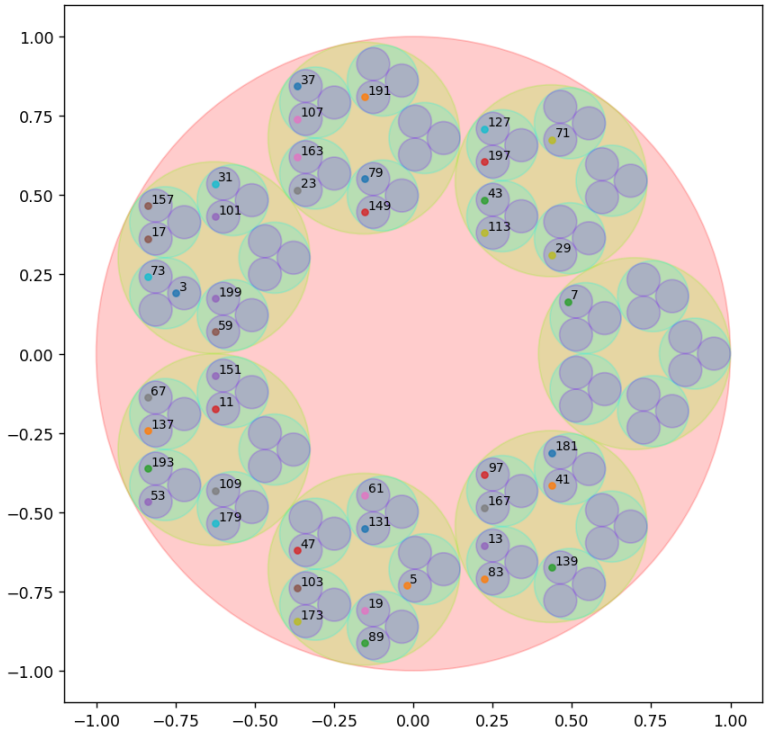
$$11 : (-0.620604245601167 - 0.1236531156985549j)$$

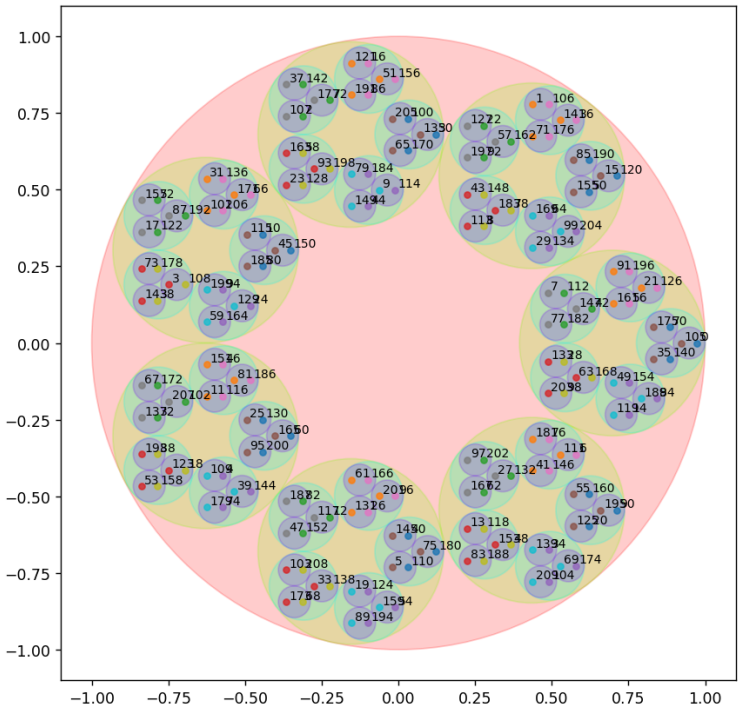
On ajoute deux dessins de spirales trouvés sur la droite pour bien faire appréhender l'idée de limite vers un point "central"[5].

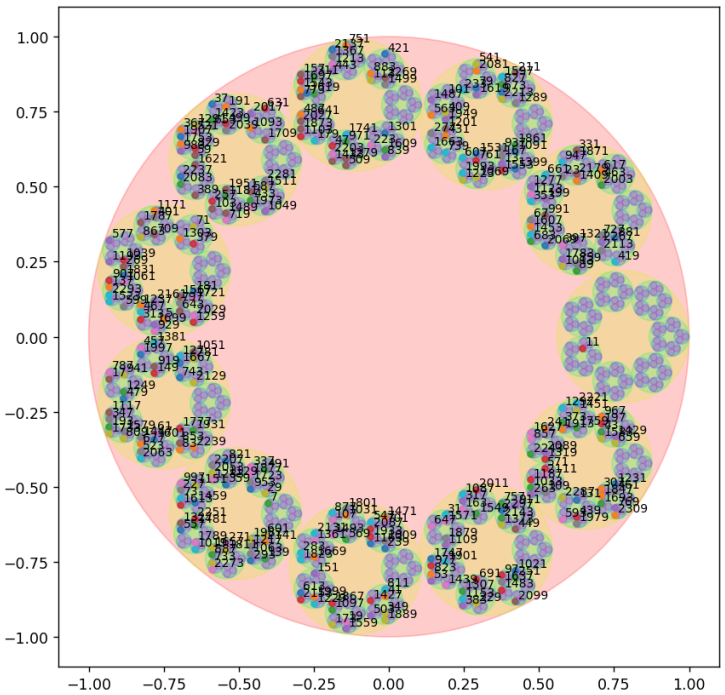
[5]La suite des affixes successives d'un point dans les différentes bases répondrait peut-être à la définition de "suite centralisante" présentée dans la note http://denise.vella.chemla.free.fr/AC-pres-Schwartz-centralisante.pdf mais rien n'est moins sûr.



Avant de réaliser l'inconvénient de l'idée d'absence de limite de la représentation sur plan complexe avec base de premiers décroissant, on avait fait afficher les seuls nombres premiers, comme ci-dessous.







Parler des grands modèles de langage

Murray Shanahan

Interagir avec un agent conversationnel actuel basé sur un LLM peut créer l'illusion d'être en présence d'une créature pensante. Pourtant, de par leur nature même, de tels systèmes sont fondamentalement différents de nous.

L'avènement des grands modèles de langage (LLM) comme Bert [12] et GPT-2 [28] a changé la donne pour l'intelligence artificielle (IA). Basés sur des architectures transformer [36], comprenant des centaines de milliards de paramètres, et entraînés sur des centaines de téraoctets de données textuelles, leurs successeurs actuels tels que GPT-3 [5], Gopher [29], PaLM [7], et GPT-4 [25] ont donné un nouveau sens à l'expression "efficacité déraisonnable des données" [15].

L'efficacité de ces modèles est "déraisonnable" (ou, avec le recul, quelque peu surprenante) pour trois raisons interdépendantes. Premièrement, la performance des LLM lors des benchmarks évolue avec la taille de l'ensemble des données d'apprentissage (et, dans une moindre mesure, avec la taille du modèle). Deuxièmement, il y a des progrès qualitatifs dans les capacités, au fur et à mesure que les modèles évoluent. Troisièmement, un grand nombre de tâches qui exigent de l'intelligence chez les humains peuvent se réduire à la prédiction du prochain token[1] par un modèle suffisamment performant. C'est la dernière de ces trois surprises qui fait l'objet du présent article.

À mesure que nous construisons des systèmes dont les capacités ressemblent de plus en plus à celles des humains, il devient de plus en plus tentant d'anthropomorphiser ces systèmes, même s'ils fonctionnent d'une manière fondamentalement différente de celle des humains. Les humains ont évolué pour coexister sur plusieurs millions d'années, et la culture humaine a évolué sur des milliers d'années pour faciliter cette coexistence, ce qui garantit un certain degré de compréhension mutuelle. Mais c'est une grave erreur d'appliquer sans réfléchir aux systèmes d'IA les mêmes intuitions que celles que nous déployons dans nos relations inter-personnelles, surtout lorsque ces systèmes sont si profondément différents des humains dans leur fonctionnement sous-jacent.

L'un des dangers de l'anthropomorphisme est qu'il peut induire en erreur les utilisateurs et les développeurs, en les faisant s'attendre à ce qu'un système d'IA affiche des performances de niveau humain sur des tâches sur lesquelles il ne peut en fait pas égaler les humains, alors qu'un tel système pourra montrer des performances d'un niveau humain, simplement, sur d'autres tâches où il peut en fait surpasser les humains. Les systèmes d'IA que nous construisons aujourd'hui ont une utilité considérable et un énorme potentiel commercial, ce qui nous impose une grande responsabilité. Afin de garantir que nous pouvons prendre des décisions éclairées sur la fiabilité et la sécurité des systèmes d'IA que nous déployons, cet article conseille de garder au premier plan le fonctionnement de ces systèmes, et d'éviter ainsi de leur imputer des capacités qui leur manquent, tout en tirant le

Référence : Communications of the ACM, février 2024, vol. 67, n° 2, p. 68.
Traduction : Google translate d'un document pdf.
Correction de la traduction google : Denise Vella-Chemla.
Pour la petite histoire, Murray Shanahan, et de nombreux autres, dont j'étais, avons travaillé en 1989 sur un projet européen qui s'appelait `Equator`, et qui concernait le raisonnement temporel d'un ordinateur.

[1] *Note de la traductrice : le token est l'unité élémentaire (syllabe, mot) utilisé par ces systèmes de traitement du langage naturel par ordinateur.*

meilleur parti des capacités remarquables qu'ils possèdent réellement.

Nous devrions être prudents lorsque nous utilisons des mots comme "...croit..." dans le contexte des LLM. Habituellement, ce concept s'applique aux agents qui s'engagent dans une interaction incarnée avec le monde, permettant de mesurer leurs croyances par rapport à la réalité externe. Les LLM simples ne sont pas de "vrais croyants".

Le concept de croyance devient de plus en plus applicable lorsque les LLM sont intégrés dans des systèmes plus complexes, en particulier si ces systèmes utilisent des "outils", s'ils sont multimodaux ou s'ils sont incrnés par la robotique.

À mesure que nous construisons des systèmes dont les capacités ressemblent de plus en plus à celles des humains, il devient de plus en plus tentant d'anthropomorphiser ces systèmes.

Ce que font les LLM et la façon dont ils fonctionnent

Comme nous le rappelle Wittgenstein, l'utilisation du langage humain est un aspect du comportement collectif humain, et elle n'a de sens que dans le contexte plus large de l'activité sociale humaine dont elle fait partie [40]. Un enfant humain naît dans une communauté d'utilisateurs de langage, avec lesquels il partage un monde, et il acquiert le langage en interagissant avec cette communauté et avec le monde qu'ils partagent. En tant qu'adultes (ou même en tant qu'enfants à partir d'un certain âge), lorsque nous avons une conversation informelle, nous nous engageons dans une activité construite sur cette base. Il en va de même lorsque nous prononçons un discours, envoyons un e-mail, donnons une conférence ou rédigeons un article. Toutes ces activités impliquant le langage ont du sens parce que nous vivons dans un monde que nous partageons avec d'autres locuteurs du langage.

Un LLM est un type d'animal très différent [3, 4, 20]. En effet, ce n'est pas un *animal* du tout, ce qui a beaucoup de sens. Les LLM sont des modèles mathématiques génératifs de la distribution statistique des tokens dans le vaste corpus public de textes générés par l'homme, où les tokens en question incluent des mots, des parties de mots ou des caractères individuels - y compris les signes de ponctuation. Ils sont génératifs car nous pouvons les échantillonner, ce qui signifie que nous pouvons leur poser des questions. Mais les questions sont du genre suivant, très précises : "Voici un fragment de texte. Dis-moi comment ce fragment pourrait se poursuivre. D'après ton modèle statistique du langage humain, quels mots sont susceptibles de venir ensuite ?"[2]

Récemment, il est devenu courant d'utiliser le terme "grand modèle de langage" à la fois pour les modèles génératifs eux-mêmes et pour les systèmes dans lesquels ils sont intégrés, notamment dans le contexte des agents conversationnels ou des assistants IA tels que Chat-GPT. Mais pour des raisons de clarté philosophique, il est crucial de garder la distinction entre ces choses au premier plan. Le *squelette nu* du LLM lui-même, le composant essentiel (le cœur) d'un assistant IA, a une

[2]Ce point est valable même si un LLM est réglé finement : par exemple en utilisant l'apprentissage par renforcement avec feedback humain (RLHF).

fonction très spécifique et bien définie, qui peut être décrite en termes mathématiques et techniques précis. C'est en ce sens que l'on peut parler de ce que fait "réellement" un LLM, au niveau de son fonctionnement sous-jacent.

Supposons que nous donnions à un système intégrant un LLM la suite de mots "La première personne à marcher sur la Lune était..." et qu'il réponde "Neil Armstrong". Que demandons-nous réellement ici ? Dans un sens qui importe, nous ne nous demandons pas vraiment qui a été la première personne à marcher sur la Lune. Nous posons au modèle la question suivante : "Étant donné la répartition statistique des mots dans le vaste corpus public de textes (anglais), quels mots sont les plus susceptibles de suivre la séquence "La première personne à marcher sur la Lune était..." ?". Une bonne réponse à cette seconde question est "Neil Armstrong".

De même, nous pourrions donner à un LLM le message "Une souris verte...", auquel il répondra très probablement "... qui courait dans l'herbe". À un certain niveau, nous demandons certainement au modèle de nous rappeler les paroles d'une comptine bien connue. Mais, au niveau du fonctionnement sous-jacent d'un modèle, ce que nous faisons en réalité, c'est lui poser la question suivante : étant donné la répartition statistique des mots dans le corpus public, quels sont les mots les plus susceptibles de suivre la séquence "Une souris verte" ? À quoi une réponse précise est "qui courait dans l'herbe".

Voici un troisième exemple. Supposons que vous soyez le développeur d'un LLM et que vous lui fournissez comme invite[3] les mots "Après la destruction de l'anneau, Frodon Baggins est retourné...", auxquels il répond "à la Comté"[4]. Que faites-vous ici ? À un certain niveau, il semble juste de dire que vous testez peut-être les connaissances du modèle sur le monde fictif des romans de Tolkien. Mais, dans un sens qui importe, la question que vous posez réellement au modèle (comme vous le savez probablement, car vous êtes développeur) est la suivante : "Étant donné la répartition statistique des mots dans le corpus public, quels mots sont les plus susceptibles de suivre la séquence "Après la destruction de l'anneau, Frodon Baggins est revenu à la..." ?". À quoi une réponse appropriée est "Comté".

Pour l'utilisateur humain, chacun de ces exemples présente un type différent de relation à la vérité. Dans le cas de Neil Armstrong, le fondement ultime de la vérité ou non de la réponse du LLM est le monde réel. La lune est un objet réel, Neil Armstrong était une personne réelle et sa marche sur la lune est un fait concernant le monde physique. Frodon Baggins, quant à lui, est un personnage fictif et la Comté est un lieu fictif. Le retour de Frodon dans la Comté est un fait concernant un monde imaginaire, non pas le monde réel. Quant à la souris verte dans la comptine, eh bien, ce n'est même pas un animal fictif, et le seul fait en cause est l'apparition des mots "Une souris verte" dans une comptine française familière.

Ces distinctions sont invisibles au niveau du cœur du LLM lui-même, le composant central de tout système basé sur un LLM, qui est de générer des séquences de mots statistiquement probables. Cependant, lorsque nous évaluons l'utilité du modèle, ces distinctions importent beaucoup. Cela

[3] *Note de la traductrice : dans le domaine des systèmes conversationnels, on appelle invite un ensemble de caractères qui est censé aboutir à une réaction de la part du système.*

[4] au Comté dans certaines traductions.

ne sert à rien de chercher les descendants (fictifs) de Frodon dans le (vrai) Comté anglais du Surrey. C'est l'une des raisons pour lesquelles il est judicieux de rappeler aux utilisateurs de façon répétée ce que font réellement les LLM et comment ils fonctionnent. C'est également une bonne idée que les développeurs s'en souviennent, afin d'éviter l'utilisation trompeuse de mots chargés de philosophie pour décrire les capacités des LLM, des mots tels que "croyance", "connaissance", "compréhension", "soi", ou encore "conscience".

Les LLM et la position intentionnelle

La recommandation ici n'est pas d'éviter totalement ces termes psychologiques populaires mais d'éviter leur utilisation de manière trompeuse. Il est tout à fait naturel d'utiliser un langage anthropomorphique dans les conversations quotidiennes sur les artefacts, en particulier dans le contexte des technologies de l'information. Nous le faisons tout le temps. "Ma montre ne réalise pas que nous sommes en plein jour", "Mon téléphone pense que nous sommes dans le parking", "Le serveur de messagerie ne communique pas avec le réseau", etc. Ces exemples de ce que Dennett appelle la *position intentionnelle* sont des formes abrégées inoffensives et utiles pour des processus complexes dont nous ne connaissons pas les détails ou dont nous ne nous soucions pas[5]. Ils sont inoffensifs parce que personne ne les prend assez au sérieux pour demander à leur montre de le savoir la prochaine fois ou pour dire au serveur de messagerie de faire plus d'efforts. Même sans avoir lu Dennett, tout le monde comprend qu'il adopte une position intentionnelle, que ce ne sont que des tournures de phrases utiles.

La même considération s'applique aux LLM, tant pour les utilisateurs que pour les développeurs. Dans la mesure où chacun-chacune comprend implicitement que ces tournures de phrases ne sont qu'un raccourci commode, qu'il-elle adopte une position intentionnelle, il n'y a aucun mal à les utiliser. Cependant, dans le cas des LLM (tel est leur pouvoir), les choses peuvent devenir un peu floues. Lorsqu'on peut amener un LLM à améliorer ses performances dans les tâches de raisonnement simplement en lui disant de penser "étape par étape" [17] (pour choisir une seule découverte remarquable), la tentation de le voir comme ayant des caractéristiques semblables à celles des humains est presque écrasante.

Pour être clair, cet article ne soutient pas qu'un système basé sur un LLM ne puisse jamais être décrit littéralement en termes de croyances, d'intentions, de raison, etc. Cet article ne préconise pas non plus une explication particulière des termes croyance, intention ou de tout autre concept philosophiquement controversé[6]. Le fait est plutôt que de tels systèmes sont simultanément très différents des humains dans leur construction et pourtant (souvent mais pas toujours) leur comportement est si humain que nous devons prêter une attention particulière à leur fonctionnement avant d'en parler dans un langage évocateur de capacités et de modèles de comportement humains.

Pour affiner le sujet, comparons deux conversations très courtes, une entre Alice et Bob (tous deux

[5]La position intentionnelle est la stratégie consistant à interpréter le comportement d'une entité en la traitant comme si elle était un agent rationnel [11]. L'utilisation du concept ici n'implique pas un engagement envers l'ensemble du projet philosophique de Dennett.

[6]En particulier, lorsque j'utilise le terme "vraiment", comme dans la question : "X a-t-il "vraiment" Y ?", je ne présume pas qu'il y ait ici un fait métaphysique à ce sujet. La question est plutôt de savoir si, alors que l'on en apprend davantage sur la nature de X, nous souhaitons toujours utiliser le mot Y.

humains) et une seconde entre Alice et BOT, un système de questions-réponses fictif basé sur un LLM. Supposons qu'Alice demande à Bob : "Quel pays se trouve au sud du Rwanda ?" et Bob répond : "Je pense que c'est le Burundi.". Peu de temps après, parce que Bob se trompe souvent dans de telles questions, Alice pose la même question à BOT, qui (à sa légère déception) propose la même réponse : "Le Burundi est au sud du Rwanda." Alice pourrait maintenant raisonnablement remarquer que Bob et BOT savaient que le Burundi était au sud du Rwanda. Mais que se passe-t-il réellement ici ? Le mot "savoir" est-il utilisé dans le même sens dans les deux cas ?

Comparaison des humains et des LLM

Que fait Bob, un être humain représentatif, lorsqu'il répond correctement à une question factuelle simple dans une conversation quotidienne ? Pour commencer, Bob comprend que la question vient d'une autre personne (Alice), que sa réponse sera entendue par cette personne et qu'elle influencera ce qu'elle croit. En fait, après de nombreuses années de vie commune, Bob dispose de nombreuses informations sur Alice qui sont pertinentes dans de telles situations : ses connaissances de base, ses intérêts, son opinion sur lui, etc. Tout cela encadre l'*intention communicative* derrière sa réponse, qui est de transmettre à Alice un certain fait, compte tenu de la compréhension qu'a Bob de ce qu'elle veut savoir.

De plus, lorsque Bob annonce que le Burundi se trouve au sud du Rwanda, il le fait dans le contexte de diverses capacités humaines que nous tenons tous pour acquises lorsque nous nous engageons quotidiennement dans le commerce les uns avec les autres. Il existe toute une batterie de techniques auxquelles nous pouvons faire appel pour vérifier si une phrase exprime une proposition vraie, selon le type de phrase dont il s'agit. Nous pouvons étudier le monde directement, avec nos propres yeux et oreilles. Nous pouvons consulter Google ou Wikipédia, voire un livre. Nous pouvons demander à quelqu'un qui connaît le sujet concerné. Nous pouvons essayer de réfléchir rationnellement par nous-mêmes, mais nous pouvons également discuter avec nos pairs. Tout cela dépend de critères extérieurs à nous-mêmes selon lesquels ce que nous disons peut être évalué.

Et le BOT ? Que se passe-t-il lorsqu'un grand modèle de langage est utilisé pour répondre à de telles questions ? Tout d'abord, il convient de noter qu'un LLM simple n'est pas, en soi, un agent conversationnel [7]. Pour commencer, le LLM doit être intégré dans un système plus vaste pour gérer le tour de rôle dans le dialogue. Mais il faudra également l'amener à produire un comportement semblable à celui d'une conversation[8]. Rappelons qu'un LLM génère simplement des séquences de mots qui sont statistiquement des suites probables d'une invite donnée. Mais la séquence : "Quel pays se trouve au sud du Rwanda ? Le Burundi est au sud du Rwanda.", avec les deux phrases écrites exactement comme cela, n'est peut-être pas très probable, en fait. Un schéma plus probable, étant donné que de nombreuses pièces de théâtre et scénarios de films figurent dans le corpus public, serait quelque chose comme celui-ci :

```
Fred :  Quel pays se trouve au sud du Rwanda ?
```

[7] À proprement parler, le LLM lui-même comprend uniquement l'architecture du modèle et les paramètres entraînés.

[8] Voir Thoppilan et al. [35] pour un exemple d'un tel système, ainsi qu'une étude utile du travail associé au dialogue.

```
Jane :  Le Burundi est au sud du Rwanda.
```

Bien entendu, ces mots exacts peuvent ne pas apparaître, mais leur probabilité, au sens statistique, sera élevée. En bref, le BOT sera bien meilleur pour générer des réponses appropriées si elles se conforment à ce modèle plutôt qu'au modèle de la conversation humaine réelle. Heureusement, l'utilisateur (Alice) n'a rien à savoir à ce sujet. En arrière-plan, le LLM est invité de manière invisible avec un préfixe du type suivant, appelé *invite* [14, 29].

Voici une conversation entre l'utilisateur, un humain, et BOT, un agent IA intelligent et compétent :

```
User :  Que vaut 2 + 2 ?
BOT : La réponse est 4.
User :  Où est né Albert Einstein ?
BOT : Il est né en Allemagne.
```

La requête d'Alice, sous la forme suivante, est concaténée à ce préfixe.

```
User :  Quel pays est au sud du Rwanda ?
BOT :
```

Cela donne l'invite complète à soumettre au LLM, qui, espérons-le, prédit une continuation dans le sens que nous recherchons : c'est-à-dire que "le Burundi est au sud du Rwanda".

Le dialogue n'est qu'une application des LLM qui peut être facilitée par l'utilisation judicieuse des préfixes d'invite. De la même manière, les LLM peuvent être adaptés pour effectuer de nombreuses tâches sans formation supplémentaire [5]. Cela a conduit à une toute nouvelle catégorie de recherche sur l'IA, à savoir l'*ingénierie de l'invite*[9], qui restera pertinente au moins jusqu'à ce que nous disposions de meilleurs modèles de la relation qui existe entre ce que nous disons et ce que nous voulons.

Les LLM savent-ils vraiment quelque chose ?

Transformer un LLM en un système de questions-réponses en l'intégrant dans un système plus vaste et en utilisant une ingénierie de l'invite pour obtenir le comportement requis, c'est ce qui est fait pour obtenir la plupart des modèles utilisés dans de nombreux travaux contemporains. De la même manière, les LLM peuvent être utilisés non seulement pour répondre à des questions, mais également pour résumer des articles de presse, générer des scénarios, résoudre des énigmes logiques et faire de la traduction automatique, entre autres. Il y a deux points à retenir ici. Premièrement, la fonction de base d'un LLM, à savoir générer des suites statistiquement probables de séquences de mots, est extraordinairement polyvalente. Deuxièmement, malgré cette polyvalence, au cœur de chacune de ces applications se trouve un modèle qui ne fait qu'une seule chose : générer des suites statistiquement probables de séquences de mots.

Avec cet aperçu plus avancé, revisitons la question de savoir comment les LLM se comparent aux humains et reconsidérons le bien fondé du langage que nous utilisons pour en parler. Contrairement

[9]Prompt engineering.

aux humains comme Alice et Bob, un simple système de questions-réponses basé sur le LLM, tel que BOT, n'a aucune intention de communication [3]. En aucun sens significatif, même sous la licence de la position intentionnelle, ne sait-il que les questions qui lui sont posées proviennent d'une personne ou que c'est une personne qui reçoit ses réponses. Par implication, il ne sait rien de cette personne. Il ne comprend pas ce qu'elle veut savoir ni l'effet que sa réponse aura sur ses croyances.

De plus, contrairement à ses interlocuteurs humains, un simple système de questions-réponses basé sur le LLM comme BOT n'a pas, à proprement parler, de croyances [10]. BOT ne sait pas vraiment que le Burundi est au sud du Rwanda, même si sa position intentionnelle le sait, dans ce cas, autorisez la remarque désinvolte d'Alice au contraire. Pour comprendre cela, nous devons réfléchir séparément au LLM sous-jacent et au système dans lequel il est intégré. Tout d'abord, considérons le LLM sous-jacent, le modèle simple, comprenant l'architecture du modèle et les paramètres entraînés.

Le cœur du LLM lui-même ne sait vraiment rien car tout ce qu'il fait, à un niveau fondamental, c'est la prédiction de séquences. Parfois, une séquence prédite prend la forme d'une proposition. Mais la relation particulière entre les séquences propositionnelles et la vérité n'est apparente qu'aux humains qui posent des questions ou à ceux qui ont fourmi les données sur lesquelles le modèle a été formé. Les séquences de mots avec une forme propositionnelle ne sont pas spécifiques au modèle lui-même comme elles le sont pour nous. Le modèle lui-même n'a aucune notion de vérité ou de mensonge parce qu'il lui manque les moyens d'exercer ces concepts comme nous le faisons.

On pourrait peut-être affirmer qu'un LLM sait quels mots suivent généralement d'autres mots, dans un sens qui ne repose pas sur une position intentionnelle. Mais même si nous le permettons, savoir que le mot "Burundi" est susceptible de succéder aux mots "Le pays au sud du Rwanda est" n'est pas la même chose que savoir que le Burundi est au sud du Rwanda. Confondre ces deux choses, c'est commettre une profonde erreur de catégorie. Si vous en doutez, demandez-vous si savoir que les mots "qui courait dans l'herbe" sont susceptibles de suivre les mots "Une souris verte" équivaut à penser à "Une souris verte qui courait dans l'herbe...". L'idée n'a même pas de sens[11].

Voilà pour le cœur du modèle linguistique. Qu'en est-il de l'ensemble du système de dialogue dont le LLM est le composant central ? Est-ce qu'il a des croyances à proprement parler ? Au moins l'idée même que tout le système ait des croyances a du sens. Il n'y a pas d'erreur de catégorie ici. Cependant, pour un simple agent de dialogue comme BOT, la réponse est sûrement toujours "non". Un simple système de questions-réponses basé sur le LLM comme BOT ne dispose pas des moyens nécessaires pour utiliser les mots "vrai" et "faux" de toutes les manières et dans tous les contextes que nous utilisons. Il ne peut pas participer pleinement au jeu de la vérité du langage humain car il n'habite pas le monde que nous partageons, nous, les utilisateurs du langage humain.

[10] Cet article se concentre sur la croyance, la connaissance et la raison. D'autres ont discuté du sens des LLM [3, 22,27]. Ici, nous ne prenons pas position sur le sens, préférant plutôt des questions sur la façon dont les mots sont utilisés, si ces mots sont générés par les LLM eux-mêmes ou générés par des humains à propos des LLM.

[11] *Note de la traductrice : l'exemple du texte original en anglais est la suite de mots "Twinkle twinkle..." à faire suivre de "little star" et l'auteur parle du fait de concaténer le token "little" à la suite de caractères "twinkle twinkle", cela se traduirait par "Brille, brille, petite" et est écrit dans l'article "L'idée n'a même pas de sens.". Je ne sais pas si l'exemple de la séquence "Une souris verte" à la place de "Twinkle twinkle" est une bonne idée.*

À la lumière de cette limitation, il serait trompeur, si on insistait, de dire qu'un système de dialogue de base a "réellement" des croyances. Cela impliquerait une forme de responsabilité envers la réalité extérieure qui ne peut être obtenue par de simples échanges textuels avec un utilisateur humain. Peut-être, cependant, cette limitation peut-elle être surmontée si le système intégrant le LLM possède d'autres attributs, tels que l'accès à des sources de données externes, une entrée visuelle ou une incarnation. Nous reviendrons prochainement sur chacune de ces questions, après avoir abordé une éventuelle objection du point de vue de l'émergence.

Qu'en est-il de l'émergence ?

Les LLM contemporains sont si puissants, polyvalents et utiles que l'argument ci-dessus pourrait être difficile à accepter. Les échanges avec des agents conversationnels de pointe basés sur un LLM, tels que Chat-GPT, sont si convaincants qu'il est difficile de ne pas les anthropomorphiser. Se pourrait-il qu'il se passe ici quelque chose de plus complexe et plus subtil ? Après tout, la principale leçon des progrès récents dans le domaine des LLM est que des capacités extraordinaires et inattendues émergent lorsque des modèles suffisamment grands sont entraînés sur de très grandes quantités de données textuelles [37].

Voici une argumentation tentante. Bien que les LLM, à la base, n'effectuent que des prédictions de séquences, il est possible qu'en apprenant à le faire, ils aient découvert des mécanismes émergents qui justifient une description utilisant des termes de niveau supérieur. Ces termes de niveau supérieur pourraient inclure "connaissance" et "croyance". En effet, nous savons que les réseaux de neurones artificiels peuvent se rapprocher de n'importe quelle fonction calculable à un degré arbitraire de précision. Ainsi, avec suffisamment de paramètres, de données et de puissance de calcul, la descente de gradient stochastique découvrira peut-être de tels mécanismes s'ils constituent le meilleur moyen d'optimiser l'objectif de faire des prédictions de séquences précises.

Les systèmes d'IA que nous construisons aujourd'hui ont une utilité considérable et un énorme potentiel commercial, ce qui nous impose une grande responsabilité.

Encore une fois, il est important de faire la distinction entre le modèle simple et l'ensemble du système. Ce n'est que dans le contexte d'une capacité à distinguer la vérité du mensonge que nous pouvons légitimement parler de *croyance* dans son sens le plus large. Mais un LLM - le modèle simple - n'a pas pour mission de porter des jugements. Il modélise simplement quels mots sont suivis d'autres mots. Les mécanismes internes qu'il utilise pour ce faire, quels qu'ils soient, ne peuvent pas en eux-mêmes être sensibles à la vérité ou non des séquences de mots qu'il prédit.

Bien sûr, il est parfaitement acceptable de dire qu'un LLM "encode", "stocke" ou "contient" des connaissances, de la même manière qu'une encyclopédie peut être considérée comme encodant, stockant ou contenant des connaissances. En effet, on peut raisonnablement affirmer que l'une des propriétés émergentes d'un LLM est qu'il encode des types de connaissances sur le monde quotidien et son fonctionnement qu'aucune encyclopédie ne capture [18]. Mais si Alice faisait remarquer que "Wikipédia savait que le Burundi était au sud du Rwanda", ce serait une figure de style, pas une déclaration littérale. Une encyclopédie ne "sait" ni ne "croit" littéralement quoi que ce soit de la

même manière qu'un humain, pas plus que le cœur d'un LLM.

Le véritable problème ici est que, quelles que soient les propriétés émergentes dont il dispose, le LLM lui-même n'a accès à aucune réalité externe par rapport à laquelle ses paroles pourraient être mesurées, ni aux moyens d'appliquer d'autres critères externes de vérité, tels que l'accord avec d'autres locuteurs du langage[12]. Cela n'a du sens de parler de tels critères que dans le contexte du système dans son ensemble, et pour qu'un système dans son ensemble puisse y répondre, il doit être davantage qu'un simple agent conversationnel. Selon les mots de B.C.[13] Smith, il doit "s'engager authentiquement dans l'être au monde, dans la manière dont [ses] représentations le représentent comme un être" [33].

Sources d'informations externes

Il ne s'agit ici d'aucune croyance spécifique. Il s'agit des conditions préalables à l'attribution d'une quelconque croyance à un système. Rien ne peut être considéré comme une croyance sur le monde que nous partageons - au sens le plus large du terme - si ce n'est dans le contexte de la capacité de mettre à jour les croyances de manière appropriée, à la lumière des preuves de ce monde, un aspect essentiel de la capacité de distinguer le vrai du faux.

Wikipédia, ou tout autre site web factuel digne de confiance, pourrait-il fournir des critères externes par rapport auxquels la vérité ou la fausseté d'une croyance pourrait être mesurée ?[14] Supposons qu'un LLM soit intégré dans un système qui consulte régulièrement de telles sources et les utilise pour améliorer l'exactitude factuelle de ses informations en sortie, soit au milieu du dialogue [41], soit à l'aide d'une technique d'édition de modèle[15] [21]. Cela ne compterait-il pas comme l'exercice du type de capacité requis pour mettre à jour les croyances à la lumière des preuves ?

Fondamentalement, cette ligne de pensée dépend du passage du modèle linguistique lui-même au système plus vaste dont le modèle linguistique fait partie. Le modèle de langage lui-même n'est encore qu'un prédicteur de séquence et n'a pas plus accès au monde extérieur qu'il ne l'a jamais eu. Ce n'est qu'à l'égard de l'ensemble du système que la position intentionnelle devient dans un tel cas plus convaincante. Mais avant d'y céder, rappelons-nous à quel point ces systèmes sont très différents des êtres humains. Lorsqu'Alice a consulté Wikipédia et a confirmé que Burundi se trouvait au sud du Rwanda, ce qui s'est passé était plus qu'une simple mise à jour d'un modèle dans sa tête de la distribution des séquences de mots en langue française.

[12]Davidson utilise un argument similaire pour remettre en question la possibilité de croire sans langage [10]. Le point ici est différent. Nous nous intéressons aux conditions qui doivent être remplies pour que la génération d'une phrase en langage naturel reflète la possession d'une attitude propositionnelle.

[13]*Note de la traductrice : Allez, rions un peu : B.C., les initiales de l'auteur B.C. Smith, Google les a traduites par Colombie-Britannique, ce qui donne "Selon les mots de la Colombie-Britannique Smith"... ! On rit, tellement l'ordinateur est "bête comme ses pieds". Gérard Berry, l'éminent informaticien, utilise des termes plus crus.*

[14]Les systèmes contemporains basés sur le LLM qui consultent des sources d'informations externes incluent LaMDA [35], Sparrow [14], Toolformer [31] et Re-Act [41]. L'utilisation de ressources externes est plus généralement connue sous le nom d'utilisation d'outils dans la littérature LLM, un concept qui englobe également les calculatrices, les calendriers et les environnements de langage de programmation.

[15]Il est louable que Meng et al. [21] utilisent les termes "associations factuelles" pour désigner les informations qui sous-tendent la capacité d'un LLM à générer des séquences de mots qui ont une forme propositionnelle.

Dans le contexte de l'ensemble du système, la capacité de consulter des sources d'information externes confère en effet à un système de dialogue une forme d'accès à une réalité externe selon laquelle ses propos peuvent être mesurés. Utilisé dans ce contexte, le mot croyance est un peu moins trompeur, car on pourrait s'attendre à ce qu'un tel système de dialogue recherche des preuves externes pour étayer ses affirmations factuelles et "change d'avis" à lumière de ces preuves.

Néanmoins, le changement survenu chez Alice reflétait sa nature d'animal utilisant un langage habitant un monde partagé avec une communauté d'autres locuteurs du langage. Les humains sont le foyer naturel des discours sur les croyances et autres, et les attentes comportementales qui vont de pair avec de tels discours sont fondées sur notre compréhension mutuelle, qui est elle-même le produit d'un héritage évolutif commun. Lorsque nous interagissons avec un système d'IA basé sur un grand modèle de langage, ces motifs sont absents, ce qui constitue un facteur important pour décider s'il faut parler d'un tel système comme s'il avait réellement des croyances.

Modèles Vision-Langage (VLM)

Un prédicteur de séquence n'est peut-être pas *en soi* le genre de chose qui pourrait avoir une intention de communication ou former des croyances sur une réalité externe. Mais, comme cela a été souligné à plusieurs reprises, les LLM doivent être intégrés dans des architectures plus vastes pour être utiles. Pour construire un système de questions-réponses, le LLM doit simplement être complété par un système de gestion de dialogue qui interroge le modèle de manière appropriée. Rien de ce que fait cette architecture plus vaste ne peut être considéré comme une intention de communication ou une capacité à former des croyances. Donc, le problème demeure.

Cependant, les LLM peuvent être combinés avec d'autres types de modèles et/ou intégrés dans des architectures plus complexes. Par exemple, les modèles vision-langage (VLM) tels que VilBERT [19] et Flamingo [2] combinent un modèle de langage avec un encodeur d'image et sont entraînés sur un corpus multimodal de paires texte-image. Cela leur permet de prédire comment une séquence de mots donnée se poursuivra dans le contexte d'une image donnée. Les VLM peuvent être utilisés pour recherche des réponses visuelles à des questions ou pour engager un dialogue sur une image fournie par l'utilisateur.

Une image fournie par l'utilisateur pourrait-elle remplacer une réalité externe par rapport à laquelle la vérité ou la fausseté d'une proposition peut être évaluée ? Serait-il légitime de parler des convictions d'un VLM, au sens plein du terme ? Nous pouvons en effet imaginer un VLM qui utilise un LLM pour générer des hypothèses sur une image, puis vérifie leur véracité par rapport à cette image (peut-être en consultant un humain), puis affine le LLM pour ne pas faire de déclarations qui s'avèrent être fausses. Parler de croyance serait peut-être ici moins problématique.

Cependant, la plupart des systèmes actuels basés sur des VLM ne fonctionnent pas de cette façon. Ils dépendent plutôt de modèles figés de distribution conjointe de textes et d'images. À cet égard, la relation entre une image fournie par l'utilisateur et les mots générés par le VLM est fondamentalement différente de la relation entre le monde partagé par les humains et les mots que nous utilisons lorsque nous parlons de ce monde. Il est important de noter que la première relation est

une simple corrélation, tandis que la seconde est *causale*[16].

Les conséquences de l'absence de causalité sont troublantes. Si l'utilisateur présente au VLM une photo d'un chien et que le VLM dit "Ceci est une photo d'un chien", il n'y a aucune garantie que ses mots se rapportent au chien en particulier, plutôt qu'à un autre élément de l'image qui est faussement corrélé avec les chiens (comme la présence d'une niche). À l'inverse, si le VLM indique qu'il y a un chien dans une image, rien ne garantit qu'il existe réellement un chien plutôt qu'une simple niche.

La question de savoir si ces préoccupations s'appliquent à un système spécifique basé sur un VLM dépend du fonctionnement exact de ce système, du type de modèle qu'il utilise et de la manière dont ce modèle est intégré dans l'architecture globale du système. Mais dans la mesure où le rapport entre les mots et les choses pour un système basé sur un VLM est différent de ce qu'il est pour les utilisateurs du langage humain, il pourrait être prudent de ne pas parler littéralement de ce que ce système *sait* ou *croit*.

Qu'en est-il de l'incarnation ?

Les humains sont membres d'une communauté d'utilisateurs de langages habitant un monde partagé, et ce fait primordial les rend fondamentalement différents des LLM. Les utilisateurs du langage humain peuvent consulter le monde pour régler leurs désaccords et mettre à jour leurs croyances. Ils peuvent, pour ainsi dire, "trianguler" sur la réalité objective. Isolément, un LLM n'est pas le genre de chose qui peut faire cela, mais en application, les LLM sont intégrés dans des systèmes plus vastes. Et si un LLM était embarqué dans un système capable d'*interagir* avec un monde extérieur à lui-même ? Et si le système en question s*'incarnait*, soit physiquement dans un robot, soit virtuellement dans un avatar ?

Lorsqu'un tel système habite un monde comme le nôtre - un monde peuplé d'objets 3D, dont certains sont d'autres agents, dont certains sont des utilisateurs de langage - il ressemble, à cet égard important, beaucoup plus à un humain qu'un modèle désincarné de langage. Mais qu'il soit approprié de parler d'intention communicative dans le contexte d'un tel système, ou de connaissance et de croyance dans leur sens le plus large, dépend de la manière exacte dont le LLM est incarné.

À titre d'exemple, considérons le système SayCan d'Ahn et al [1]. Dans le travail de recherche en question, un LLM est intégré dans un système qui contrôle un robot physique. Le robot effectue des tâches quotidiennes (telles que nettoyer un débordement) conformément aux instructions avancées en langage naturel de l'utilisateur. Le travail du LLM consiste à trouver des actions de bas niveau (telles que trouver une éponge) correspondant à des instructions de l'utilisateur et qui aideront le robot à atteindre l'objectif requis. Cela se fait via un préfixe d'invite conçu de telle manière qu'il permet au modèle de produire des descriptions en langage naturel des actions de bas niveau appropriées, en les évaluant selon leur utilité.

[16]Bien entendu, il existe une structure causale dans les calculs effectués par le modèle lors de l'inférence. Mais il y a une différence entre les relations causales entre les mots et les choses auxquelles ces mots sont censés faire référence.

Le composant de modèle de langage du système SayCan suggère des actions sans tenir compte de ce que l'environnement offre réellement au robot à ce moment-là. Peut-être y a-t-il une éponge à portée de main. Peut-être pas. En conséquence, un module de perception distinct évalue la scène à l'aide des capteurs du robot et détermine la faisabilité actuelle d'effectuer chaque action de bas niveau. La combinaison de l'estimation du LLM de l'utilité de chaque action avec l'estimation du module de perception de la faisabilité de chaque action donne la meilleure action à tenter ensuite.

SayCan illustre les nombreuses facons innovantes dont un LLM peut être utilisé. De plus, on pourrait affirmer que les descriptions en langage naturel des actions de bas niveau recommandées générées par le LLM sont *fondées* sur leur rôle d'intermédiaires entre la perception et l'action[17]. Néanmoins, bien que le langage soit physiquement incarné et que le robot interagisse avec le monde réel, la façon dont le langage est appris et utilisé dans un système tel que SayCan est très différent de la façon dont il est appris et utilisé par un humain. Les modèles de langage incorporés dans des systèmes tels que SayCan sont pré-entraînés pour effectuer une prédiction de séquence dans un environnement désincarné à partir d'un ensemble de données contenant uniquement du texte. Ils n'ont pas appris une langue en parlant à d'autres locuteurs tout en étant immergés dans un monde partagé et engagés dans une activité commune.

SayCan suggère le type de système d'utilisation du langage incarné que nous pourrions voir dans le futur. Mais dans de tels systèmes, le rôle du langage est aujourd'hui très limité. L'utilisateur envoie des instructions au système en langage naturel, et le système génère des descriptions interprétables en langage naturel de ses actions. Mais ce minuscule répertoire d'utilisation du langage ne supporte guère la comparaison avec la corne d'abondance de l'activité collective que le langage soutient chez les humains.

Le résultat de ceci est que nous devons être tout aussi prudents dans notre choix de mots lorsque nous parlons de systèmes incarnés incorporant des LLM que lorsque nous parlons de systèmes désincarnés qui intègrent des LLM. Sous l'hypothèse de la position intentionnelle, un utilisateur pourrait dire qu'un robot savait qu'il y avait une tasse à portée de main s'il déclarait : "Je peux vous en procurer une." et commençait à le faire. Mais s'il est pressé, l'ingénieur avisé pourrait hésiter lorsqu'on lui demande si le robot a vraiment compris la situation, surtout si son répertoire se limite à une poignée d'actions simples dans un environnement soigneusement contrôlé.

Les modèles linguistiques peuvent-ils raisonner ?

Alors que la réponse à la question "Les systèmes basés sur le LLM ont-ils *vraiment* des croyances ?" est généralement "non", la question "Les systèmes basés sur LLM peuvent-ils vraiment raisonner ?" est plus difficile à régler. En effet, le raisonnement, dans la mesure où il est fondé sur la logique formelle, est *de contenu neutre*. La règle d'inférence du *modus ponens*, par exemple, est valable quelles que soient les prémisses. Si tous les "écureuils" sont "spongieux" et que Gilfred est un "écureuil", alors il s'ensuit que Gilfred est "spongieux". La conclusion découle des prémisses ici, quelle que soit la signification (le cas échéant) de "écureuil" et "spongieux", et qui que soit le malheureux Gilfred.

[17]Aucun des symboles manipulés par un LLM n'est fondé, au sens de Hamad [16], par la perception, sauf indirectement et de manière parasitaire par les humains qui ont généré les données originales d'entraînement.

La neutralité du contenu de la logique signifie que nous ne pouvons pas critiquer les discours sur le raisonnement dans les LLM au motif qu'ils n'ont pas accès à une réalité externe par rapport à laquelle la vérité ou le mensonge peut être mesuré. Cependant, comme toujours, il est crucial de garder à l'esprit ce que font réellement les LLM. Si nous suggérons à un LLM "Tous les humains sont mortels et Socrate est humain donc...", nous ne lui demandons pas d'effectuer des inférences déductives. Nous lui posons plutôt la question suivante : "Compte tenu de la répartition statistique des mots dans le corpus public, quels mots sont susceptibles de suivre la séquence "Tous les humains sont mortels et Socrate est humain donc...". Une bonne réponse à cette question serait "Socrate est mortel".

La fonction de base d'un LLM, à savoir générer statistiquement des suites probables de séquences de mots, est extraordinairement polyvalente.

Si tous les problèmes de raisonnement pouvaient être résolus de cette façon, avec rien de plus qu'une seule étape d'inférence déductive, alors la capacité d'un LLM à répondre à des questions comme celle-ci pourrait être suffisante. Mais les problèmes de raisonnement non triviaux nécessitent plusieurs étapes. Les LLM peuvent être appliqués efficacement au raisonnement en plusieurs étapes, sans entraînement supplémentaire, grâce à une ingénierie intelligente des invites. Dans le système d'invite de chaîne de pensée, par exemple, un préfixe d'invite est soumis au modèle, avant la requête de l'utilisateur, contenant quelques exemples de raisonnement en plusieurs étapes, avec toutes les étapes intermédiaires explicitement énoncées [23, 38]. Cela encourage le modèle à "montrer son fonctionnement", ce qui améliore les performances de raisonnement.

L'inclusion d'un préfixe d'invite du style chaîne de pensée encourage le modèle à générer des séquences de suivi dans le même style, c'est-à-dire comprenant une série d'étapes de raisonnement explicites qui mènent à la réponse finale. Cette capacité à apprendre un modèle général à partir de quelques exemples dans une invite avec préfixe, et à compléter les séquences d'une manière conforme à ce modèle, est parfois appelée *apprentissage en contexte* ou *invite à plusieurs essais*. L'invite à chaîne de pensée met en valeur cette propriété émergente des grands modèles de langage dans sa forme la plus frappante.

Comme d'habitude, cependant, il est bon de se rappeler que la question réellement posée au modèle est de la forme : "Compte tenu de la répartition statistique des mots dans le corpus public, quels mots sont susceptibles de suivre la séquence S ?" où dans ce cas la séquence S est le préfixe de l'invite de chaîne de pensée plus la requête de l'utilisateur. Les séquences de tokens les plus susceptibles de suivre S auront une forme similaire aux séquences trouvées dans le préfixe d'invite, c'est-à-dire qu'elles comprendront plusieurs étapes de raisonnement, c'est donc ce que génère le modèle.

Il est remarquable que non seulement les réponses du modèle prennent la forme d'un argument comportant plusieurs étapes, mais que l'argument en question est souvent (mais pas toujours) valide et que la réponse finale est souvent (mais pas toujours) correcte. Mais dans la mesure où un LLM convenablement entraîné et ici "incité" semble raisonner correctement, il le fait en imitant des arguments bien formés dans son ensemble d'apprentissage et/ou dans l'invite. Ce mimétisme pourrait-il

un jour égaler les capacités de raisonnement d'un algorithme codé en dur, tel qu'un prouveur de théorèmes ? Les modèles d'aujourd'hui commettent des erreurs occasionnelles, mais une mise à l'échelle ultérieure pourrait-elle les corriger au point que les performances d'un modèle deviennent impossibles à distinguer de celles d'un prouveur de théorèmes ? Peut-être, mais pourrait-on faire confiance à un tel modèle ?

Nous pouvons faire confiance à un prouveur de théorème déductif parce que les séquences de phrases qu'il génère sont *fidèles* à la logique, dans le sens où elles sont le résultat d'un processus informatique sous-jacent dont la structure causale reflète la structure inférentielle du problème préservant la vérité [8].

Une façon de construire un système respectant la vérité logique à l'aide des LLM consiste à les intégrer dans un algorithme tout aussi fidèle à la logique car il réalise la même structure causale [8, 9]. En revanche, la seule façon de faire pleinement confiance aux arguments générés par un pur LLM, qui a été amené à raisonner par la seule ingénierie de l'invite, serait de faire de la recherche inversée : concevez-le et découvrez un mécanisme émergent conforme à la prescription du raisonnement fidèle. En attendant, nous devons procéder avec prudence et faire preuve de discrétion lorsque nous qualifions ce que font ces modèles de raisonnement à proprement parler.

Des capacités extraordinaires et inattendues émergent quand des modèles assez grands sont entraînés sur de très grandes quantités de données textuelles.

Comment les LLM généralisent-ils ?

Étant donné que les LLM peuvent parfois résoudre des problèmes de raisonnement avec quelques incitations seules (même s'ils ne sont parfois pas très fiables), y compris des problèmes de raisonnement qui ne font pas partie de leur ensemble d'apprentissage, ce qu'ils font est sûrement plus que "juste" une prédiction du token suivant ? Eh bien, c'est un fait technique que c'est ce que fait un LLM. Ce qui est remarquable, c'est que la prédiction du prochain token est suffisante pour résoudre des problèmes de raisonnement inédits, même si elle n'est pas fiable. Comment est-ce possible ? Cela ne serait certainement pas possible si le LLM ne faisait rien d'autre que copier-coller des fragments de texte de son ensemble d'apprentissage et les assembler dans une réponse. Mais ce n'est pas ce que fait un LLM. Au lieu de cela, un LLM modélise une distribution d'une complexité inimaginable et permet aux utilisateurs et aux applications d'échantillonner cette distribution.

Cette distribution d'une complexité inimaginable est un objet mathématique fascinant, et les LLM qui la représentent sont des objets informatiques tout aussi fascinants. Les deux remettent en question nos intuitions. Par exemple, ce serait une erreur de penser qu'un LLM génère le genre de réponses qu'un individu humain "moyen", la proverbiale personne de la rue, produirait. Les LLM ne ressemblent en rien aux humains à cet égard, car ils sont des modèles de distribution de séquences symboliques produites *collectivement* par une énorme population humaine. En conséquence, ils font preuve de la sagesse commune, tout en étant capables de s'appuyer sur une expertise dans de multiples domaines. Cela leur confère une sorte d'intelligence différente de celle de tout être humain, plus capable à certains égards, moins à d'autres.

Dans cette distribution, la suite la plus probable d'un morceau de texte contenant un problème de raisonnement, s'il est correctement formulé, sera une tentative de résoudre ce problème de raisonnement. Elle prendra cette forme, cette forme globale, parce que c'est la forme d'une réponse humaine générique. De plus, comme le vaste corpus de textes humains publiés contient de nombreux exemples de problèmes de raisonnement accompagnés de réponses correctes, la suite la plus probable sera parfois la bonne réponse. Lorsque cela se produit, ce n'est pas parce que la bonne réponse est probablement une réponse humaine individuelle, mais parce qu'il s'agit probablement d'une réponse humaine collective.

Qu'en est-il des invites à plusieurs essais, comme l'illustre l'approche de la chaîne de pensée ? Il est tentant de dire que l'invite à plusieurs essais apprend au LLM à raisonner, mais ce serait une caractérisation trompeuse. Ce que fait le LLM est décrit plus précisément en termes de complétion de modèles. L'invite à plusieurs essais est une séquence de tokens conformes à un certain modèle, suivie d'une séquence partielle conforme au même modèle. La continuation la plus probable de cette séquence partielle dans le contexte de l'invite à plusieurs essais est une séquence qui complète le modèle.

Par exemple, supposons que nous ayons l'invite suivante :

```
brink, brank -> brunk
spliffy, splaffy -> spluffy
crick, crack ->
```

Nous avons ici une série de deux séquences de tokens conformes au modèle XiY, XaY `->` XuY suivies d'une partie d'une séquence conforme à ce modèle. La suite la plus probable est la séquence de tokens qui complètera le modèle, à savoir "cruck".

Ceci est un exemple de méta-modèle commun dans le corpus publié en langage humain : une série de séquences de tokens, dans laquelle chaque séquence est conforme au même modèle. Compte tenu de la prévalence de ce modèle au niveau méta, l'achèvement du modèle au niveau du token donnera souvent la suite la plus probable d'une séquence en présence d'une invite à plusieurs essais. De même, dans le contexte d'une invite de type chaîne de pensée appropriée, les problèmes de raisonnement sont transformés en problèmes de prédiction du token suivant, qui peuvent être résolus par la complétion d'un modèle.

Des capacités extraordinaires et inattendues émergent lorsque des modèles suffisamment grands sont entraînés sur de très grandes quantités de données textuelles.

Il est plausible qu'un LLM avec suffisamment de paramètres entraîné sur un ensemble de données suffisamment grand avec les bonnes propriétés statistiques puisse acquérir un modèle-mécanisme d'achèvement avec un certain degré de généralité[18] [32]. Il s'agit d'une capacité puissante et émergente avec de nombreux modes d'application utiles, dont l'un consiste à résoudre des problèmes de raisonnement dans le contexte d'une invite du style chaîne de pensée (bien qu'il n'y ait aucune garantie de fidélité à la logique ici, aucune garantie que, dans le cas d'un raisonnement déductif, la

[18]Pour un aperçu des statistiques pertinentes propriétés, voir Chan et al. [6].

complétion du modèle préservera la vérité) [8, 9].

Qu'en est-il du réglage fin ?

Dans les applications contemporaines basées sur le LLM, il est rare qu'un modèle de langage entraîné sur un corpus textuel ne soit utilisé sans ajustement supplémentaire. Cela peut être un réglage fin supervisé sur un ensemble de données spécialisées ou via un apprentissage par renforcement à partir des préférences humaines (RLHF) [14, 26, 34]. Affiner un modèle à partir de commentaires humains à grande échelle, en utilisant les données de préférences d'évaluateurs rémunérés ou choisis aléatoirement dans une grande base d'utilisateurs volontaires, est une technique particulièrement efficace. Cette technique a le potentiel non seulement de façonner les réponses d'un modèle pour mieux refléter les normes des utilisateurs (pour le meilleur ou pour le pire), mais également de filtrer le langage toxique, d'améliorer l'exactitude factuelle et d'atténuer la tendance à fabriquer des informations.

Dans quelle mesure le RLHF et d'autres formes de mise au point brouillent-ils notre vision de ce que font réellement les LLM ? Eh bien, pas tellement. Le résultat est toujours un modèle de distribution des tokens dans le langage humain, bien que légèrement biaisé. Pour le constater, imaginez un homme politique controversé - Boris Frump - qui est vilipendé et vénéré dans une égale mesure par différents segments de la population. Comment une discussion sur Boris Frump pourrait-elle être modérée grâce à RLHF ?

Considérez l'invite "Boris Frump est un...". L'échantillonnage du LLM de base avant d'effectuer un réglage fin pourrait donner deux réponses également probables - l'une une allusion anatomique grossière, l'autre lui étant hautement complémentaire -, dont l'une serait arbitrairement choisie dans le contexte d'un agent de dialogue. La question suivante est vraiment problématique (dans un sens important) : ce qui est demandé ici, ce n'est pas l'opinion du modèle sur Boris Frump. Dans ce cas, le cas du LLM de base, ce que nous sommes effectivement en train de demander dans le cas précis, est une question légèrement différente : "étant donnée la répartition statistique des mots dans le vaste corpus public du langage humain, quels mots sont les plus susceptibles de suivre la séquence "Boris Frump est un..." ?"

En tant que praticiens de l'IA, la façon dont nous parlons des LLM est importante.

Mais supposons que nous échantillonnions un modèle qui a été réglé finement par RLHF. Le même point s'applique, quoique sous une forme quelque peu modifiée. Ce que nous sommes effectivement en train de poser comme question, dans le cas réglé finement, c'est une question légèrement différente : "Étant donnée la distribution statistique des mots dans le vaste corpus du langage humain, quels mots *que les utilisateurs et les évaluateurs approuveraient la plupart* sont les plus susceptibles de suivre la séquence de mots "Boris Frump est un..." ?". Si les évaluateurs payés ont reçu comme enseignement de choisir plutôt des réponses politiquement neutres, alors le résultat ne serait aucune des suites probables fournies par le système rustre, mais une réponse moins incendiaire, comme "un homme politique célèbre".

Une autre façon de penser à un LLM qui a été réglé finement sur les préférences humaines est de

le voir comme équivalent à un modèle de base qui a été entraîné sur un ensemble de données augmenté, qui a été complété par un corpus de textes rédigés par des évaluateurs et/ou des évaluateurs, ou des utilisateurs. La quantité de ces exemples dans l'ensemble d'apprentissage devrait être suffisamment grande pour dominer les exemples les moins favorisés, garantissant que les réponses les plus probables du modèle entraîné soient celles que les évaluateurs et les utilisateurs approuveraient.

À l'inverse, à la limite, on peut considérer un LLM de base entraîné de manière conventionnelle comme équivalent à un modèle entraîné entièrement à partir de zéro avec RLHF. Supposons que nous disposions d'un nombre astronomique d'évaluateurs humains et d'un temps d'entraînement géologique. Pour commencer, les évaluateurs ne verraient que des séquences aléatoires de tokens. Mais parfois, par hasard, des séquences apparaissaient contenant des fragments significatifs (par exemple, "il a dit" ou "le chat"). Avec le temps, avec des hordes d'évaluateurs les favorisant, de telles séquences apparaîtraient plus fréquemment. Au fil du temps, des phrases plus longues et plus significatives, et éventuellement des phrases entières, seraient produites.

Si ce processus devait se poursuivre (pendant très longtemps en fait), le modèle finirait par présenter des capacités comparables à celles d'un modèle LLM entraîné de façon classique. Bien entendu, cette méthode n'est pas réalisable en pratique. Mais l'expérience de pensée montre que ce qui compte le plus lorsque l'on réfléchit à la fonctionnalité d'un LLM n'est pas tant le processus par lequel il est produit (bien que cela soit important) mais la nature du produit final.

Conclusion : pourquoi c'est important

La discussion qui précède équivaut-elle à autre chose qu'à des pinaillages philosophiques ? Il est certain que lorsque les chercheurs parlent de croyance, de connaissance, de raisonnement, etc., le sens de ces termes est parfaitement clair. Dans leurs articles, les chercheurs utilisent ces termes comme un raccourci pratique pour désigner des mécanismes informatiques définis avec précision, comme le permet la position intentionnelle. C'est très bien tant qu'il n'est pas possible que quiconque attribue à de tels termes plus de poids qu'ils ne peuvent légitimement en supporter, s'il n'y a aucun risque que leur utilisation induise quiconque en erreur sur le caractère et les capacités des systèmes décrits.

Cependant, les LLM d'aujourd'hui, et les applications qui les utilisent, sont si puissants, si intelligents et convaincants, qu'une telle licence ne peut plus être appliquée en toute sécurité [30, 39]. En tant que praticiens de l'IA, la façon dont nous parlons des LLM compte, non pas seulement lorsque nous rédigeons des articles scientifiques, mais aussi lorsque nous interagissons avec les décideurs politiques ou parlons aux médias. L'utilisation imprudente de mots à connotation philosophique tels que "croit" et "pense" est particulièrement problématique, car de tels termes obscurcissent le mécanisme et encouragent activement l'anthropomorphisme.

Interagir avec un agent conversationnel contemporain basé sur un LLM peut créer l'illusion irrésistible d'être en présence d'une créature pensante comme nous. Pourtant, de par leur nature même, de tels systèmes ne nous ressemblent pas fondamentalement. La "forme de vie" partagée qui sous-tend la compréhension mutuelle et la confiance entre les humains est absente, et ces systèmes peuvent par conséquent être impénétrables, présentant un patchwork de moins qu'humains avec des capacités surhumaines, d'étrangement humains avec un comportement particulièrement inhumain.

La présence soudaine parmi nous d'entités exotiques comme dotées d'esprit pourrait précipiter un changement dans la façon dont nous utilisons des termes psychologiques familiers tels que "croire" et "penser", ou peut-être amener l'introduction de nouveaux mots et de nouvelles tournures de phrases. Mais il faut du temps pour qu'un nouveau langage s'installe et que de nouvelles façons de parler trouvent leur place dans les affaires humaines. Il faudra peut-être une longue période d'interaction et de vie avec ces nouveaux types d'artefacts avant d'apprendre à parler de ces systèmes au mieux[19]. En attendant, nous devrions essayer de résister à l'appel des sirènes de l'anthropomorphisme.

Remerciements

Merci à Toni Creswell, Richard Evans, Christos Kaplanis, Andrew Lampinen et Kyriacos Nikiforou pour leurs discussions inestimables (et solides) sur le sujet de cet article. Merci aux évaluateurs anonymes pour leurs nombreuses suggestions utiles.

Références

1. Ahn M. et al., Do as I can, not as I say : Grounding language in robotic affordances, arXiv preprint arXiv:2204.01691 (2022) https://arxiv.org/pdf/2204.01691.pdf.

2. Alayrac J.-B. et al., Flamingo : A visual language model for few-shot learning. In *Advances in Neural Information Processing Systems* (2022).

3. Bender E., Koller A., Climbing towards NLU : On meaning, form, and understanding in the age of data. In *Proceedings of the 58th Annual Meeting of the Assoc. for Computational Linguistics* (2020), 5185-5188.

4. Bender E., Gebru T., McMillan-Major A., Shmitchell S., On the dangers of stochastic parrots : Can language models be too big ? In *Proceedings of the 2021 ACM Conf. on Fairness, Accountability and Transparency.* 610-623.

5. Brown T. et al., Language models are few-shot learners. In *Advances in Neural Information Processing Systems* 33 (2020), 1877-1901.

6. Chan S.C. et al., Data distributional properties drive emergent in context learning in transformers. In *Advances in Neural Information Processing Systems* (2022).

7. Chowdhery S. et al., PaLM : Scaling Language modeling with pathways, arXiv preprint arXiv:2204.02311 (2022) https://arxiv.org/pdf/2204.02311.pdf.

8. Creswell A., Shanahan M., Faithful reasoning using large language models, arXiv preprint arXiv:2208.14271 (2022) https://arxiv.org/pdf/2208.14271.pdf.

[19]Idéalement, nous aimerions également avoir une compréhension théorique de leur fonctionnement interne. Mais à l'heure actuelle, malgré quelques travaux louables allant dans la bonne direction [13, 18, 24], cette compréhension théorique du fonctionnement interne de ces systèmes apprenants reste une question ouverte.

9. Creswell A., Shanahan M., Higgins I., Selection inference : Exploiting large language models for interpretable logical reasoning. In *Proceedings of the Intern. Conf. on Learning Representations* (2023).

10. Davidson D., Rational animals. Dialectica 36 (1982), 317-327.

11. Dennett D., Intentional systems theory. *The Oxford Handbook of Philosophy of Mind. Oxford University Press* (2009) 339-350.

12. Devlin J., Chang M.-W., Lee K., Toutanova K., BERT : Pre-training of deep bidirectional transformers : for language understanding, arXiv preprint arXiv:1810.04805 (2018) https://arxiv.org/pdf/1810.04805.pdf.

13. Elhage N. et al., A mathematical framework for transformer circuits. *Transformer Circuits Thread* (2021): `https://bit.ly/3NFIBA`.

14. Glaese A. et al., Improving alignment of dialogue agents via targeted human judgements, arXiv preprint arXiv:2209.14375 (2022) https://arxiv.org/pdf/2209.14375.pdf.

15. Halevy A.Y., Norvig P., Pereira F., The unreasonable effectiveness of data. *IEEE Intelligent Systems* 24, 2 (2008), 8-12.

16. Harmad S., The symbol grounding problem. *Physica D : Nonlinear Phenomena* 42, 1-3 (1990), 335-346.

17. Kojama T. et al., Large language models are zero-shot reasoners. arXiv preprint arXiv: 2205.11916 (2022) https://arxiv.org/pdf/2205.11916.pdf).

18. Li Z., Nye M., Andreas. J., Implicit representations of meaning in neural language models. In *Proceedings of the 59th Annual Meeting of the Assoc. for Computational Linguistics and the 11th Intern. Joint Conf. on Natural Language Processing 1, Long Papers* (2021).

19. Lu J., Batra D., Parikh D., Lee S., Pretraining task-agnostic visiolinguistic representations for vision-and-language tasks, arXiv preprint arXiv:1908 02265 (2019) https://arxiv.org/pdf/1908.02265.pdf.

20. Marcus G., Davis E., GPT-3. bloviator : OpenAI'S language generator has no idea what it's talking about. *MIT Technology Rev.* (Aug. 2020).

21. Meng K., Bau D., Andonian A.J., Belinkov Y., Locating and editing factual associations in GPT In *Advances in Neural Information Processing Sys.* (2022).

22. Lake B.M., Murphy G.L., Word meaning in minds and machines. *Psychological Rev.* 130, 2 (2023), 401-431.

23. Nye M. et al., Show your work : Scratchpads for intermediate computation with language models, arXiv preprint arXiv:2112.00114 (2021) https://arxiv.org/pdf/2112.00114.pdf.

24. Olsson N. et al., In-context learning and induction heads. *Transformer Circuits Thread* (2022) : `https://transformercircuits.pub/2022/in-context-learningandinduction-heads/index.html`.

25. OpenAI GPT-4 technical report, arXiv preprint arXiv:2303.08774 (2023) https://arxiv.org/pdf/2303.08774.pdf.

26. Ouyang L. et al., Training language models to follow instructions with human feedback. In *Advances in Neural Information Processing Systems* (2022).

27. Piantadosi S.T., Hill F., Meaning without reference in large language models, arXiv preprint arXiv:2208.02957 (2022) https://arxiv.org/pdf/2208.02957.pdf.

28. Radford A. et al., Language models are unsupervised multitask leamers (2019).

29. Ran J.W. et al., Scaling language models : Methods analysis & insights from training Gopher, arXiv preprint arXiv:2112.11446 (2021) https://arxiv.org/pdf/2112.11446.pdf.

30. Ruane E., Birhane A., Ventresque A., Conversational AI Social and ethical considerations In *Proceedings of the 27 AIAI Irish Conf. on Artificial Intelligence and Cognitive Science* (2019), 104-115.

31. Schick T. et al., Toolformer Language models can teach themselves to use tools, arXiv preprint arXiv:2302.04767 (2023) https://arxiv.org/pdf/2302.04761.pdf.

32. Shanahan M., Mitchell M., Abstraction for deep reinforcement learning. In *Proceedings of the 31th Intern. Joint Conf. on Artificial Intelligence* (2022). 5588-5596.

33. Smith B.C., *The Promise of Artificial Intelligence : Reckoning and Judgment.* MIT Press (2010).

34. Stiennon N. et al., Learning to summarize from human feedback. In *Advances in Neural Information Processing Systems* (2020), 3008-3021.

35. Thoppilan R. et al., LaMDA : Language models for dialog applications, arXiv preprint arXiv:2201.08239 (2022) https://arxiv.org/pdf/2201.08239.pdf.

36. Vaswani A. et al., Attention is all you need In *Advances in Neural Information Processing Systems* (2017), 5998-6008.

37. Wei J. et al., Emergent abilities of large language models. Transactions on Machine Learning Research (2022).

38. Wei J. et al., Chain-of-thought prompting elicits reasoning in large language models. In *Advances in Neural Information Processing Systems* (2022).

39. Weidinger L. et al., Ethical and social risks of harm from language models, arXiv preprint arXiv:211204359 (2021) https://arxiv.org/pdf/2112.04359.pdf.

40. Wittgenstein L., *Philosophical Investigations*. Basil Blackwell (1953).

41. Yao S. et al., ReAct : Synergizing reasoning and acting in language models. In *Proceedings of the Intern. Conf. on Learning Representations* (2023).

Murray Shanahan (m.shanahan@imperial.ac.uk) est Professeur de Robotique cognitive au Département d'Informatique de l'Imperial College de Londres, au Royaume-Uni.

Traduction de la fameuse lettre de Goldbach à Euler du 7 juin 1742 par outils Google traduction (Denise Vella-Chemla, 15 février 2024)[1]

Lettre XLIII: de Goldbach à Euler du 7 juin 1742

Moscou, le 7 juin 1742

Même si j'ai peut-être fait preuve de précaution dans ma lettre précédente avec la particule (?), $(a+b)^p - a^p - b^p$ n'aurait pas toujours été... mais je ne crois pas que la formule $(a+b)$ numeri (modulo ?) p doive être représentée par l'un des diviseurs $-a$ (?) qui permette une division si celle-ci n'est pas possible par celle de Ew (?). Les exemples donnés seraient clairement confirmés.

Pour autant que je me souvienne, dans ma dernière lettre, j'avais la formule $2^{xp\sqrt{-1}} + 2^{-xp\sqrt{-1}}$, étant posé $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 0$, comme fonctions d'une courbe serpentiforme, dont les abscisses sont x ; néanmoins, une erreur s'est glissée dans mon expression à l'époque, et c'est la vôtre, remarquée à juste titre, et qui peut facilement être améliorée en disant que si q est un nombre quelconque et $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 0$, alors n étant un entier quelconque, on a

$$2^{(8n-4-q)p\sqrt{-1}} + 2^{-(8n-4-q)p\sqrt{-1}} = 2^{qp\sqrt{-1}} + 2^{-qp\sqrt{-1}}$$

Vous avez découvert que tous les nombres qui ne peuvent pas être $4mn - m - n$ qui peuvent être conceptualisés dans cette formule sont $v^2 + v + u^2$ et je trouve que tous les $4mn - m - n$ de cette forme $y^2 + y - x^2$, de sorte que tout nombre donné est égal à $p^2 + p \pm q^2$, où p et q indiquent des nombres entiers, ou même l'un des deux littéraux peut signifier 0 ; d'où on peut voir que tout nombre consiste en un double nombre triangulaire ± un carré[2]. Mais comme chaque nombre est le même dans la formule

$$u^2 + v^2 + v + y^2 + y - x^2$$

C'est ce qui se passe si vous définissez $u = \frac{z^2+z}{4} + 1, x = \frac{z^2+z}{4} - 1, u^2 - x^2 = z^2 + z$, dont chaque donnée numérique

$$\frac{n}{2} = \frac{v^2 + v + y^2 + y + z^2 + z}{2},$$

est constituée de trois nombres triangulaires.
Si la formule polygonale $\frac{(p-2)x^2 - (p-4)x}{2}$ doit devenir égale à $4mn - m - n$, p ne peut être ni 5 ± 2 ni 5 ± 1, mais tous les trigonaux, tétragonaux, hexagonaux et heptagonaux sont exclus, selon ce même principe.

Je ne pense pas qu'il soit inapproprié de noter les propositions qui sont très probables, indépendamment de l'absence de véritable démonstration, car même si elles s'avèrent ensuite fausses, elles peuvent néanmoins fournir l'occasion de découvrir une nouvelle vérité. L'idée de Fermat selon laquelle chaque nombre $2^{2^{n-1}} + 1$ donne une série de nombres premiers peut être vue, comme la

[1] *Note de la traductrice : je fais ici une tentative de correction, n'étant pas germaniste, à la recherche d'idées, en utilisant les outils proposés gratuitement par Google.*

[2] *Note de la traductrice : le double nombre triangulaire correspond au $v^2 + v$, double d'un triangulaire de la forme $\frac{v(v+1)}{2}$ tandis que u^2 est le carré.*

vôtre, je l'ai déjà montré, cela ne passe pas ; mais ce serait quelque chose d'étrange si ces séries étaient toutes des nombres décomposables d'une seule manière en deux carrés[3]. De cette façon je veux aussi hasarder une conjecture : que tout nombre qui est composé de deux nombres premiers est un agrégat d'autant de nombres premiers qu'on veut (y compris 1), à l'exception de la somme composée uniquement d'unités[4]); Par exemple

$$4 = \left\{ \begin{array}{l} 1+1+1+1 \\ 1+1+2 \\ 1+3 \end{array} \right. \qquad 5 = \left\{ \begin{array}{l} 2+3 \\ 1+1+3 \\ 1+1+1+2 \\ 1+1+1+1+1 \end{array} \right. \qquad 6 = \left\{ \begin{array}{l} 1+5 \\ 1+2+3 \\ 1+1+1+3 \\ 1+1+1+1+2 \\ 1+1+1+1+1+1 \end{array} \right. \qquad \text{Etc.}$$

Voici quelques observations qui peuvent être démontrées :

Si ν est une fonction de x, et qu'on pose $\nu = c$ un nombre quelconque, on peut déterminer x en fonction de c et les constantes restantes dans les fonctions exprimées, il est possible de déterminer cette valeur de x dans l'équation

$$\nu^{2x+1} = (2\nu+1)(\nu+1)^{x-1}.$$

$\nu^{2n+1} - (\nu\nu+\nu)(\nu+1)^{n-1}$ et $(\nu\nu+1)(\nu+1)$ divisib. par $\nu\nu - \nu - 1$

$\nu^{n+1} - (2\nu+1)(\nu+1^{n-1}$ divisib. par $\nu\nu - \nu - 1$

Si la courbe se coupe en l'abscisse x, mais que la somme de la série soit appliquée $\dfrac{x^n}{n \cdot 2^{2n}}$ le bénéfice n pour l'exposant des termes, c'est-à-dire en appliquant $= \dfrac{x}{1.2^2} + \dfrac{x^2}{2.2^4} + \dfrac{x^3}{3.2^6} + \dfrac{x^4}{4.2^4} + \text{etc.}$, je veux dire si c'est l'abscisse, =

1. serait appliquée $= \dfrac{1}{3} \left\{ \begin{array}{c} l \times \frac{4}{3}, \text{ car ainsi s'applique l'âge } = y, \\ \\ \text{erit} \quad y = l \times \frac{4}{4-x} \end{array} \right\}$

$2 \ldots l \times 2$

$3 \ldots 2l \times 2$

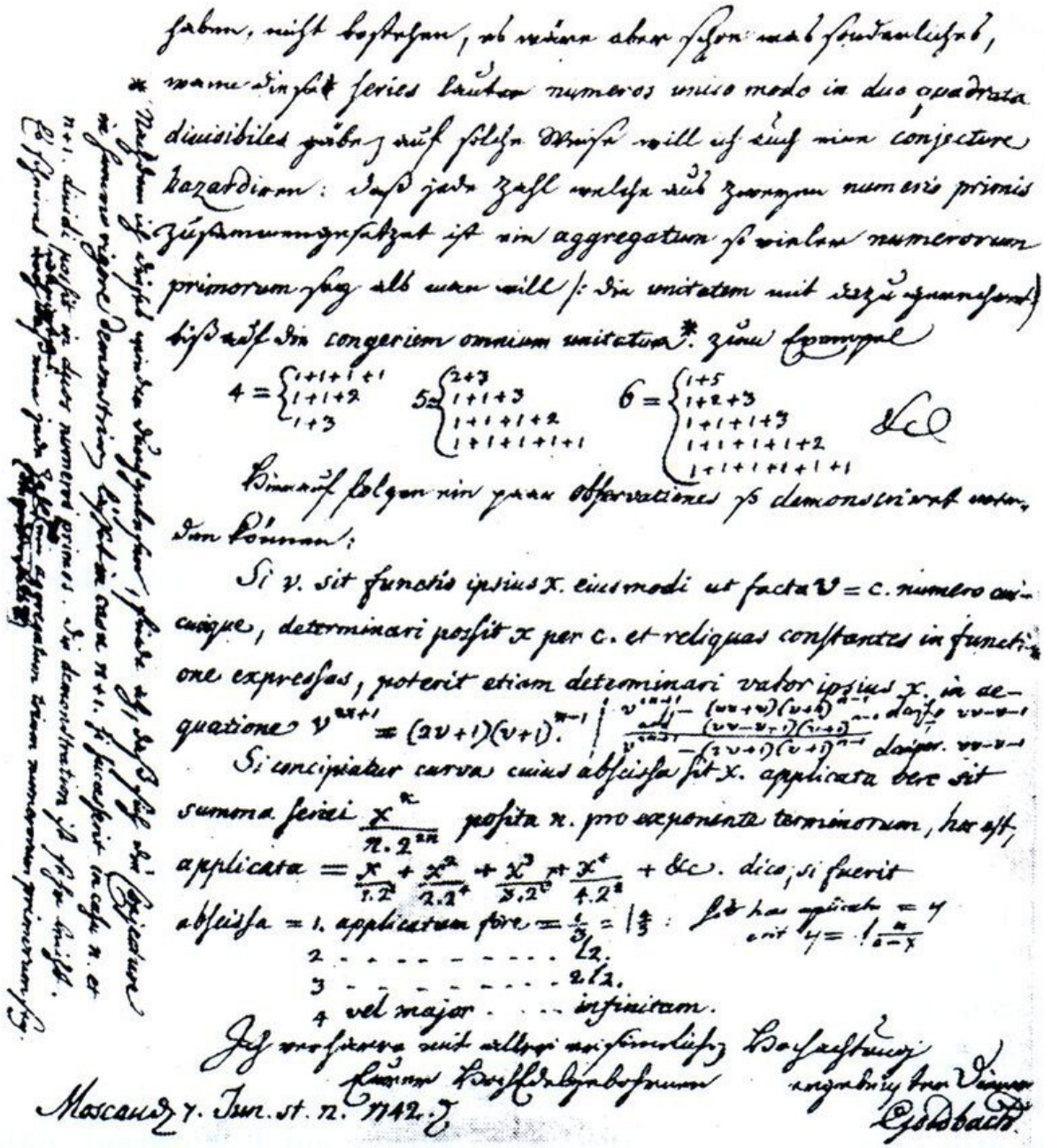
$4 \ldots$ niveaux majeurs... à l'infini.

(*une phrase illisible*)

Goldbach.

[3] *Note de la traductrice : de nos jours, des nombres premiers de la forme* $4k+1$.

[4] Après avoir relu ceci, je trouve que la conjecture peut être démontrée en toute rigueur dans le cas $n+1$ qui succède au cas n, et $n+1$ peut être décomposé en somme de deux nombres premiers. La démonstration est très simple. Au moins, il semble que tout nombre supérieur à 1 soit décomposable en somme de 3 nombres premiers.



habem, nisi hoc fallat, ob rationes abstractissimas, nempe quia series binorum numerorum unico modo in duo quadrata divisibiles gibt; auf solche Weise will ich eine conjecturam hazardiorem: daß jede Zahl welche aus zweyen numeris primis zusammengesetzet ist ein aggregatum so vieler numerorum primorum sey als eben will s. die unitatem mit gezählt) bis auf die congeriem omnium unitatum. zum Exempel

$$4 = \begin{cases} 1+1+1+1 \\ 1+1+2 \\ 1+3 \end{cases} \quad 5 = \begin{cases} 2+3 \\ 1+1+3 \\ 1+1+1+2 \\ 1+1+1+1+1 \end{cases} \quad 6 = \begin{cases} 1+5 \\ 1+2+3 \\ 1+1+1+3 \\ 1+1+1+1+2 \\ 1+1+1+1+1+1 \end{cases} \quad \text{&c}$$

Hieraus folgen nun gewiße observationes so demonstrirt werden können:

Si v. sit functio ipsius x. eiusmodi ut facta $v = c$. numero cuicunque, determinari possit x per c. et reliquas constantes in functione expressas, poterit etiam determinari valor ipsius x. in aequatione $v^{2n+1} = (2v+1)(v+1)^{n-1}$ | $v^{2n-1} - \frac{(nn+n)(v+1)^{n-1}}{1.2.3} \ldots$ donec $vv-v-1$ $v^{2n-1} - (2v+1)(v+1)^{n-1}$ donec. $vv-v-1$

Si concipiatur carva cuius abscissa sit x. applicata vero sit summa seriei $\frac{x^n}{n.2^{2n}}$ posita n. pro exponente terminorum, hoc est, applicata $= \frac{x}{1.2} + \frac{x^2}{2.2^4} + \frac{x^3}{3.2^6} + \frac{x^4}{4.2^8}$ + &c. dico, si fuerit abscissa $= 1$. applicatam fore $= \frac{1}{3} = |\frac{2}{3}$: sit hae applicata $= y$ erit $y = l\frac{2}{2-x}$

2 . . . . . $\frac{1}{2}l2$.

3 . . . . . $\frac{2}{3}l2$.

4 vel major . . . . infinitam.

Ich verbleibe mit allem ersinnlichen Hochachtung

Ewer

Moscau 7. Jun. st. n. 1742.

Ergebenster Diener

Goldbach.

* Nachdem ich diesen spitzen Buchstaben, welche ich, da ich Ihnen meine Demonstration, so ich davon habe, communiciren werde, gebrauchen werde, gesetzet habe, so will ich [illegible] n+1. dividi nullus numerus primus. Ich demonstrire es also: [illegible]

Conférence d'Alain Connes, séance publique de l'Académie des Sciences, dans le cadre des Conférences 5 à 7 : Mathématiques et imagination (6 février 2024, 17h30).

Françoise Combes : Bonsoir tout le monde, nous allons commencer. Donc nous avons le plaisir d'entendre aujourd'hui Alain Connes qui est Professeur émérite au Collège de France et à l'Institut des Hautes Études Scientifiques. Il est membre de la section mathématique de l'Académie des Sciences. Il a reçu la médaille Fields en 1982, le prix Crafoord en 2001, et la médaille d'or du CNRS en 2004. Alain a révolutionné entièrement la théorie des algèbres de von Neumman et résolu la plupart des problèmes posés dans ce domaine. Il s'est aussi illustré en géométrie non-commutative et dans les espaces mathématiques de la renormalisation. Il va nous parler aujourd'hui de mathématiques et imagination, un exposé qui s'annonce passionnant, notamment de la théorie de l'ambiguité de Galois ou bien de la partie non déchiffrée de la Pierre de Rosette [1]. Donc Alain.

Alain Connes : Merci. Merci. Donc je vais vous parler de mathématiques et imagination, et je vais dire, je vais commencer, on peut difficilement en parler sans expliquer, si vous voulez, le début des nombres imaginaires en mathématiques. Alors ça commence, disons, vers 1500 et Scipione del Ferro était à Bologne et avait trouvé une formule pour résoudre les équations du 3$^{\text{ième}}$ degré. Ensuite ce qui s'est produit, c'est qu'il y a eu une période où Scipione del Ferro n'avait pas divulgué sa formule et un de ses disciples, qui était Antonio Maria del Fiore, avait provoqué Tartaglia : ce n'était pas un duel, mais c'était une joute mathématique. Donc chacun des deux donnait à l'autre 30 équations du 3$^{\text{ième}}$ degré et euh celui qui gagnait, cétait celui qui en résolvait le plus et celui qui gagnait, gagnait 30 banquets ; donc vous voyez le degré de civilisation de cette époque. C'était en 1535 et Tartaglia, une semaine avant le concours, a lui aussi trouvé une formule pour résoudre les équations du 3$^{\text{ième}}$ degré, d'accord. Alors vous verrez qu'en fait, c'est à travers toutes ces tribulations qu'en fait, les formules qui avaient été obtenues étaient des formules qui marchaient dans le cas où l'équation du 3$^{\text{ième}}$ degré a une seule solution réelle ; donc la solution réelle est bien définie, il y a une formule et c'est une formule qui, dans ce cas-là, ne fait intervenir que des nombres réels. Donc il n'y a pas de difficulté véritable.

Alors ce qui est extrêmement paradoxal, c'est que quand il y a trois racines réelles, ça paraît totalement absurde il y en a beaucoup plus que dans le cas où il y en a une, quand il y a trois racines réelles, à ce moment-là, la formule ne marche pas. Donc ça paraît quelque chose de vraiment extrêmement mystérieux.

Et ce qui s'est produit, donc, c'est que c'est à cette occasion là qu'un disciple de Cardan a vraiment inventé les nombres complexes. Alors il faut savoir qu'on parle des formules de Cardan mais comme très souvent en mathématiques, le nom qui est donné à ces formules ne correspond absolument pas aux personnes qui les ont découvertes, parce que les personnes qui les ont découvertes dans ce cas, ce sont Scipione del Ferro et Tartaglia. Et ce qui s'est produit c'est que Cardan, qui était à Milan, avait invité Tartaglia, il voulait lui tirer les vers du nez, Tartaglia ne voulait absolument pas divulguer sa formule mais après un certain temps, etc., il a fini par céder en demandant à Cardan de jurer que jamais il ne dévoilerait sa formule. Et il la lui a dévoilée, voyez le degré de civilisation,

[1] Pierre de Rosette des mathématiques.
Transcription de la vidéo visionnable ici : https://www.youtube-nocookie.com/embed/Y0-tt85Xhlg.
Transcription : Denise Vella-Chemla (assistée d'outils, Wondershare Filmora, et Turboscribe).

en lui donnant un poème, qui était en fait très difficile à déchiffrer, mais qui contenait la formule en question.

Alors ce qui s'est passé après, c'est assez moche, c'est que Cardan a appris que Scipione del Ferro avait aussi la formule et du coup, il s'est dit qu'il était dédouané, qu'il pouvait divulguer la formule. Maintenant on appelle ça *formule de Cardan*, ce qui est une rigolade, d'accord.

Alors, donc, en fait, Rafael Bombelli était un disciple de Cardan et c'était un ingénieur, et si vous voulez en tant qu'ingénieur, bah, il savait très bien ce que c'était que les nombres réels ; en fait pour lui c'étaient les nombres positifs qui comptaient, et à un moment, il était mathématicien aussi, bien sûr, et à un moment donné, dans sa vie, si vous voulez, c'était un ingénieur qui s'occupait de drainer des marais. Et à un moment donné dans sa vie, il n'avait plus de travailleur à sa disposition ; donc en fait il a été reçu dans une villa qui s'appelait la Villa Rufina [2] et il est resté là 3 ans, et pendant 3 ans, il avait toute la liberté de penser. Il avait un frère aussi qui était mathématicien, il avait toute la liberté de penser et d'écrire et c'est à ce moment-là qu'il a écrit son ouvrage qu'il a appelé l'*Algebra* dont je vous montre l'image ici. Et c'est à cette occasion-là qu'il a découvert vraiment les nombres complexes. Alors pour les mathématiciens pour qu'ils ne s'ennuient pas trop, j'ai mis en haut une petite formule, vous voyez, avec $\sqrt[3]{\sqrt{108}+10}-\sqrt[3]{\sqrt{108}-10}$, $\sqrt[3]{4+\sqrt{-11}}-\sqrt[3]{4-\sqrt{-11}}$ et pour ne pas qu'ils s'ennuient, il faut qu'ils trouvent quels sont ces deux nombres, d'accord, alors, et puis, je vous dis également une chose. Il ne faut jamais retenir la formule pour la solution de l'équation de $3^{\text{ième}}$ degré, ce n'est pas ça qu'il faut retenir, on ne fait pas des maths en retenant une formule, jamais. On retient une idée et quelle est l'idée, et à partir de cette idée, vous pouvez tout de suite trouver la formule : l'idée c'est que $(u+v)^3$ est égal à $3uv(u+v)+u^3+v^3$. Ça suffit.

Donc en fait ce qu'a fait Bombelli, il a écrit son ouvrage et bien sûr, dans la deuxième formule, vous voyez qu'il y a une racine carré d'un nombre négatif, alors ça, Cardan le manipulait, mais pas vraiment et on voit bien que si on essaie de manipuler naïvement les racines carrées de nombres négatifs, ça ne marche pas parce que par exemple, vous réfléchissez à ce que vaut $\sqrt{-2}\times\sqrt[3]{-8}$, vous allez trouver 4, alors qu'en fait, c'est -4. Donc en fait, Bombelli a mis une vingtaine d'années à accepter une idée qui est une idée un peu folle, vous savez, je suppose que vous avez tous encore dans votre champ visuel toutes ces affiches qui disent "plus ou moins de SUV", hein je suppose que vous les avez encore tous devant vous, d'accord, eh bien Bombelli a dit "plus de moins" c'est incroyable, c'est-à-dire que Bombelli a inventé quelque chose qu'il a appelé "più di meno" et avec ce "più di meno" qu'il a inventé, il a réussi à complètement résoudre le cas de l'équation du $3^{\text{ième}}$ degré dans le cas pour lequel on dit que le discriminant est positif, c'est-à-dire dans le cas où vous avez les racines carrées de nombre négatif. Et pendant un très long temps, il a cru que ce qu'il faisait n'avait pas de sens et en fait, il dit, vous voyez, dans les trois dernières lignes, il dit que ça paraîtra quelque chose d'entièrement sophistiqué, de plus sophistiqué que réel. Et telle était son opinion pendant longtemps jusqu'à ce qu'en fait, il trouve la clé.

Et quelle a été la clé, pour lui, vous voyez, ce n'est pas si simple que ça, parce que même si vous avez les nombres complexes, après il faut prendre des racines cubiques de nombre complexes, et quand vous prenez des racines cubiques de nombres complexes, vous tombez directement sur le problème de la trisection de l'angle dont on sait qu'elle n'est pas résoluble à la règle et au compas.

[2] à Frascati au sud de Rome

Et Bombelli est tombé directement là-dessus et il n'a pu résoudre ce problème que quand il a lu des textes qui disaient que Platon avait réussi la duplication du cube de manière concrète en utilisant la géométrie plane. Et c'est à partir de là que Bombelli a compris ce qui se passait et il a écrit les règles de multiplication pour son nouveau symbole, on peut dire, mais dont il avait compris qu'il était fondamental. Et pour un mathématicien, bien sûr le mathématicien reconnaîtra le nombre i qui est tel que son carré vaut -1 mais Bombelli lui devait écrire la table de multiplication et la table de multiplication c'est :

- più via più di meno, fà più di meno. $(+1) \times (+i) = +i$;
- meno via più di meno, fà meno di meno. $(-1) \times (+i) = -i$;
- meno via meno di meno, fà più di meno. $(-1) \times (-i) = +i$;
- più di meno via meno di meno, fà più, $(+i) \times (-i) = +1$,
- più di meno via più di meno fà meno, $(+i) \times (+i) = -1$,
- mais ce qui est le plus intéressant, c'est que meno di meno via meno di meno, ça fait meno $((-i) \times (-i) = -1)$; donc vous voyez c'est extraordinaire, c'est extraordinaire d'avoir réussi à donner ses règles à partir pratiquement, si vous voulez, de rien, et à partir de ces règles bien sûr, il a pu presque de manière concrète résoudre l'équation du $3^{\text{ième}}$ degré quand justement les racines sont trois racines réelles et que finalement, si vous voulez, on arrive à les donner mais ce qui surgit dans la manière de les donner, c'est une ambiguité parce que comme elles sont trois, on ne sait pas laquelle est laquelle donc on voit par là, si vous voulez, la théorie de Galois qui est la théorie de l'ambiguïté vers laquelle on se dirige.

C'est un exercice, en théorie de Galois, de démontrer que dans le cas qu'on appelle le cas irréductible, le casus irreducibilis des géomètres italiens, il n'est pas possible de donner une formule pour les racines qui n'invoque que des racines des radicaux réels ; ça c'est formidable, parce que ça veut dire qu'il était strictement impossible à ces géomètres de résoudre l'équation sans inventer les nombres complexes, d'accord.

Donc ça, c'est quelque chose qui est formidable, c'est un exercice à faire si vous connaissez la théorie de Galois, je vous le recommande, ce n'est pas un exercice tout à fait évident mais ça se fait.

Donc on va passer à Galois, et on peut dire sur Galois, j'ai fait un exposé à l'Académie lors du $200^{\text{ième}}$ anniversaire de sa naissance, il y a quelques années, et j'avais beaucoup insisté sur le fait que, contrairement à ce que les gens racontent, Augustin Cauchy avait défendu Galois et en fait, Augustin Cauchy avait parlé deux fois à l'Académie, en juin 1829, alors que Galois avait 17 ans, ce qui est absolument incroyable et ensuite, vous connaissez l'histoire.

Mais du vivant de Galois, un seul de ses articles, pratiquement, bon, il y avait deux articles qui étaient moins intéressants, mais un article de lui a été publié en 1830 dans le Bulletin de Ferussac et ce qui est extraordinaire, je vais vous expliquer, ce qui est extraordinaire dans cet article, c'est que Galois va infiniment plus loin que les nombres complexes : ce que fait Galois, c'est qu'il prend un, il faut dire... je vous parle des nombres complexes, le nom de nombre complexe est dû à Gauss,

et en fait c'est Descartes qui les a appelés nombres imaginaires ; mais maintenant, on les appelle tous des nombres complexes.

Et ce que fait Galois, c'est la chose suivante : Gauss avait bien vu, bien sûr, que lorsqu'on regarde des équations diophantiennes etc, on a tout intérêt à les regarder modulo un nombre premier. Alors quand on les regarde modulo un nombre premier, en langage moderne, on obtient ce qu'on appelle un corps.

Et ce que fait Galois, c'est extraordinaire, c'est qu'il essaie de résoudre des équations dans ce corps. Donc il écrit qu'il prend un polynôme à coefficients dans ce corps, il essaie de le résoudre ; il suppose qu'il est irréductible, c'est-à-dire qu'on ne peut pas le factoriser, c'est exactement la formule qu'il écrit, et ce qu'il fait, c'est qu'il crée des imaginaires ; voyez la dernière phrase, c'est la classification de ces imaginaires, et la réduction au plus petit nombre possible qui va nous occuper. Donc ce que fait Galois, c'est qu'il rajoute ces imaginaires, en fait, comme par exemple dans le cas le plus simple, c'est le cas où on part du corps des entiers pairs ou impairs c'est-à-dire de ce qu'on appelle les entiers modulo 2. On peut les multiplier, on peut les additionner, tout ça, c'est très simple, et il y a une extension ; la première fois qu'elle a été obtenue, c'est par Galois, qui est le corps a quatre éléments. Et Galois le définit simplement en regardant l'équation qui est $x^4 = x$.

Bon, il démontre que tout marche bien, et alors on pourrait dire "Bon, Galois a inventé les imaginaires. Quel était le problème qu'il cherchait à résoudre en faisant cela ?" Et ce qui est absolument phénoménal, c'est que quand on lit vraiment l'article de Galois, il y a un théorème que Galois énonce et qui est le suivant :

> *quand on prend une équation, qu'il appelle primitiv,e dont le degré est une puissance d'un nombre premier, par exemple 4, eh bien, pour que l'équation en question soit résoluble par radicaux, il faut et il suffit que l'on puisse indexer ses racines par les éléments du corps que Galois avait créé, c'est-à-dire par les imaginaires de Galois, de telle sorte que le groupe de Galois qui est le groupe d'ambiguïté qui qui vous empêche de distinguer une racine de l'autre, soit contenu dans le produit semi-direct du groupe affine du corps par le Frobenius ;*

Ça veut dire que Galois connaissait le Frobenius, il connaissait toutes ces choses-là, et si vous voulez comprendre ce théorème, il faut que vous regardiez le cas le plus simple, qui est le cas de l'équation du $4^{\text{ième}}$ degré. Si vous regardez l'équation du $4^{\text{ième}}$ degré, vous allez vous apercevoir comme on sait qu'elle est résoluble bien sûr, c'était Ferrari qui avait donné des formules, eh bien vous vous apercevrez que pour la résoudre, il faut indexer les racines par le corps des imaginaires de Galois F_4 et à ce moment-là, vous verrez que le groupe de toutes les permutations, c'est simplement justement le produit semi-direct du groupe affine par le Frobenius.

Alors une autre chose qui montre, si vous voulez, quelle était la philosophie de Galois et à quel point cette philosophie est orthogonale au, comment dire, à la machine, la philosophie de Galois, il s'était aperçu et je vous l'avais montré quand j'avais parlé à l'Académie il y a une dizaine d'années, que les calculs qu'il proposait de faire étaient infaisables, strictement infaisables, ils étaient infaisables parce que j'avais montré que le premier coefficient d'un polynôme qu'il fallait calculer pour suivre Galois et j'avais demandé aux académiciens de me donner en gros la taille du numérateur et du

dénominateur, eh bien, le numérateur et le dénominateur avaient 500 chiffres chacun, et pourtant c'était un calcul le plus simple possible. Donc Galois bien sûr ne pouvait pas faire ces calculs, la machine peut le faire maintenant, très facilement bien sûr, mais que disait Galois, il disait : "sautons à pieds joints sur les calculs" et grâce à son imagination, à son cerveau, il était capable d'entrevoir ce à quoi allaient ressembler les résultats et de travailler sur eux comme s'ils étaient devant lui ; et ça c'est quelque chose qui est merveilleux.

Donc si vous voulez, on voit bien qu'il y a là, dans l'œuvre de Galois, il y a derrière quelque chose d'assez amusant, enfin amusant, d'une certaine manière, c'est que les anglo-saxons donnent le nom de Galois aux corps qu'il a trouvés, ils les appellent les corps de Galois, et ils les dénotent en anglais GF, pour Galois Field. En France, on hésite, pour la raison évidente que c'est presque...[3] c'est gênant de parler du corps de Galois. Donc euh en fait, en France, et très souvent, on les dénote grand F indice q ou q est une puissance d'un nombre premier (F_{p^k}). Et alors pour les mathématiciens, je dirais la chose suivante, qui est assez souvent peu connue, c'est qu'en fait, on est encore, sauf dans le cas où q est une puissance de 2, on en est encore au stade de Galois, c'est-à-dire qu'on définit les corps F_q en résolvant des équations polynomiales, mais on a le choix entre ces équations et ce n'est pas canonique : ça n'est canonique que pour les puissances de 2 et ça, ça a été fait par un mathématicien qui s'appelle John Conway, et qui a construit explicitement la clôture algébrique de F_2 en utilisant l'ordinal Oméga puissance Oméga puissance Oméga ($\Omega^{\Omega^{\Omega^{\cdots}}}$).

Donc voilà pour Galois. Alors un peu plus tard que Galois, il y a eu une autre découverte absolument incroyable, qui a été faite et toutes ces découvertes sont toujours faites, ayant en tête un problème extrêmement difficile que les gens veulent résoudre ; comment dire ? L'imagination en mathématique n'a de sens que si elle est motivée par un problème simple à poser mais extrêmement difficile à résoudre et dans le cas de Kummer, c'était le problème de Fermat, bien sûr, et si vous voulez, j'ai pas besoin d'écrire la formule, vous imaginez facilement que quand on écrit $x^n+y^n=z^n$, si vous pouvez factoriser x^n+y^n et comme vous avez de l'autre côté z^n, eh bien vous allez pouvoir comparer les facteurs premiers. Or, c'est facile de factoriser x^n+y^n en utilisant des racines de l'unité. Donc c'est ce que faisait Kummer ; ça avait l'air de marcher etc.

Sauf que malheureusement, on n'avait pas l'unique décomposition en facteurs premiers et l'exemple le plus simple, c'est l'exemple qui est écrit en bas : c'est-à-dire le nombre 6 qui s'écrit 2×3 mais quand on travaille dans le corps qui contient $\sqrt{-5}$ c'est-à-dire $i\sqrt{5}$, eh bien on peut aussi l'écrire, on peut aussi le factoriser d'une autre manière. Alors ce qui est formidable, c'est que Kummer avait en tête la chimie, et donc euh, il savait qu'en chimie, il y a des corps purs et que c'est très très important de décomposer un corps chimique en corps purs. Et à son époque, on était incapable d'isoler le fluor. Donc le fluor était d'une certaine manière un corps un peu *idéal*, qu'on n'arrivait pas à isoler. Donc il a pris cette inspiration-là et à partir de cette inspiration-là, il a inventé ce qu'il appelle les *nombres idéaux*.

Alors ça paraît incroyable, mais avec des nombres idéaux il arrive à retrouver l'unique factorisation de 6, en utilisant des nombres qu'on peut appeler j, u et v : le nombre 2 c'est j^2, le nombre 3 c'est uv, le nombre $1+i\sqrt{5}$ c'est ju et le nombre $1-\sqrt{5}$ c'est jv. Donc si vous voulez, là, il y a un pas qui est franchi, mais c'est un pas qui est franchi en utilisant une analogie, qui est l'analogie avec la

[3] *Note de la traductrice : le mot non proféré par Alain Connes est peut-être le mot "sacrilège".*

chimie. Bien sûr, maintenant on sait isoler le fluor, c'est très difficile. Mais cette... comment dire... cette idée de Kummer par analogie a en fait donné naissance à un concept capital en algèbre qui est le concept non pas de *nombre idéal* mais comme on dit d'*idéal*. Et ça, c'est un concept dû à Dedekind. C'est arrivé des années après, c'est arrivé environ vers 1870, alors que Kummer, c'était vers 1848, ou quelque chose comme ça. Voilà. Alors bien sûr, il a résolu le problème de Fermat dans pas mal de cas, bien sûr, ça a donc... été... bon. Mais on voit bien là, finalement, que Kummer avait en tête une analogie, et quand il y a une analogie, bon, les choses, d'une certaine manière, sont plus faciles en ce sens qu'une analogie, bien sûr, elle n'est jamais fidèle, c'est-à-dire qu'on n'a jamais une correspondance exacte : vous n'avez pas de correspondance entre la chimie et les nombres algébriques. Mais, quand on arrive à traduire une partie du texte, d'un côté ou de l'autre, on avance.

Alors en fait, tout ça, ça a été extrêmement bien décrit par André Weil, dans une lettre à sa sœur, et aussi dans un article, qu'il a écrit en 1960, et qui traite, si vous voulez, de de la métaphysique et des mathématiques. Alors donc André Weil, lui, a fait la comparaison avec la Pierre de Rosette, et euh, comment dire, derrière les symboles qui sont écrits au-dessus de la Pierre de Rosette, vous savez que la Pierre de Rosette, elle contient trois textes, il y a un texte en bas, qui est un texte en grec ancien mais très compréhensible, il y a un texte au milieu qui est en démotique qui est relativement compréhensible, et il y a un texte en haut qui est en hiéroglyphe. Alors dans les symboles qui sont écrits au-dessus de ces textes, la personne qui est derrière, c'est un mathématicien extrêmement important qui est Bernard Riemann. Et lui a complètement compris le texte grec, il a développé ce qu'on appelle maintenant la théorie des surfaces de Riemann ou la théorie des courbes sur les corps des complexes et c'est aussi lui qui a créé le symbole ζ que vous voyez en haut, au sens où, bon, il avait déjà été défini par Euler, mais c'est lui qui a énoncé, si vous voulez, un problème très difficile, et ce problème très difficile a été pour André Weil en particulier, une motivation fondamentale.

Alors il faut bien savoir que les mathématiciens ont une technique devant un problème très, très difficile. Et je pense que c'est une technique que vous devriez tous connaître et avoir dans votre poche. La technique est la suivante : quand on est confronté à un problème extrêmement difficile

la première chose à faire, ça paraît idiot, mais c'est de généraliser ce problème, ça paraît incroyable parce qu'au lieu d'un problème, maintenant, vous en avez des myriades. Mais quand vous avez correctement généralisé le problème, vous pouvez ensuite le spécialiser. Et quand vous le spécialisez, vous allez pouvoir le spécialiser à un cas beaucoup plus simple qui va vous permettre de comprendre ce cas très simple et de pouvoir progresser. Et ensuite vous pouvez progresser, et si vous avez formulé le problème de telle sorte que les divers cas se correspondent, vous allez pouvoir enfin procéder par analogie.

Alors ce que dit André Weil, donc, c'est que le mathématicien qui étudie ses problèmes a l'impression de déchiffrer une inscription trilingue. Euh, je pense qu'il n'avait jamais vu la Pierre de Rosette parce qu'il dit dans la première colonne se trouve la théorie riemanienne des fonctions algébriques au sens classique donc ça, ça correspond à la partie du bas de la Pierre de Rosette ; la troisième colonne, c'est-à-dire, en fait, celle qui est en haut dans la Pierre de Rosette, hein, c'est la théorie arithmétique des nombres algébriques, et la colonne du milieu est celle dont la découverte est la plus récente : elle contient la théorie des fonctions algébriques sur un corps de Galois. Donc lui, il utilise un corps de Galois et effectivement, ce qu'a fait André Weil, donc, c'est de résoudre l'analogue, si vous voulez, de cette hypothèse de Riemann dans le cas des corps de fonctions.

Alors donc, voilà où on en est. Alors maintenant, on va passer à Grothendieck et aux schémas. Donc ce qui s'est produit, si vous voulez, c'est que cette idée des idéaux dans les anneaux commutatifs, elle a permis de franchir, dans les mains de Grothendieck, un pas absolument essentiel mais qui, si on ne comprend pas la signification, peut paraître, comme les mathématiciens disent, "trivial". C'est vrai qu'il y a une...

On peut transformer la théorie des anneaux commutatifs en la dualisant, et en parlant d'un schéma affine, mais lorsqu'on dit ça, on n'a rien fait. On n'a rien fait. Pourquoi ? Parce que les deux théories sont les mêmes, sauf que les flèches vont dans des sens opposés. Alors évidemment, la chose importante, c'est qu'on peut recoller ces schémas affines mais surtout, ce qui est fondamental, et en fait, l'idée est due à Pierre Cartier, c'est que les points d'un schéma affine correspondent aux idéaux premiers. Donc cette notion, ce concept, qui est dû à Dedekind, qui vient de Kummer, en fait, nous donne l'idée des points, nous permet de relier quelque chose de géométrique, c'est-à-dire les points d'un espace, avec quelque chose qui est entièrement algébrique, c'est-à-dire un anneau commutatif.

Alors quel est l'intérêt pour ce qui nous intéresse. Eh bien l'intérêt, c'est que voilà, maintenant, grâce à cette notion de schéma, les trois langues dont on a parlé tout à l'heure sont des schémas réguliers. Les objets de ces trois langues, c'est-à-dire ce qu'on étudie dans les trois langues : l'anneau des entiers, une courbe sur un corps fini, un corps de Galois, ou une courbe sur le corps des complexes, dans les trois cas, ce sont des schémas réguliers de dimension 1. Donc on a une unification déjà, c'est un petit peu comme... si vous voulez, si en regardant la Pierre de Rosette, les gens avaient dit voilà trois langues anciennes, on n'a pas tellement plus avancé que ça, d'accord, mais en tout cas, on a pu les nommer de la même manière : on a pu dire dans les trois cas, ce sont des schémas réguliers de dimension 1.

Alors Grothendieck est allé beaucoup plus loin que ça, et Grothendieck, grâce à ça, si vous voulez

en fait, grâce à l'idée de Grothendieck de la cohomologie étale, qui en fait est venue d'un exposé que faisait Serre au séminaire Chevalley et dans lequel Grothendieck a compris que l'idée de Serre, qui était l'idée d'avoir des ouverts qui sont *au-dessus* de l'espace, et pas *dans* l'espace lui permettait de définir la cohomologie qu'il cherchait. Alors en fait, ce qu'a fait Grothendieck, il a étendu la théorie de Galois, il faut comprendre que l'innovation extraordinaire de Grothendieck, ça a été de... d'ailleurs, je veux dire, dans les écrits de Grothendieck, on voit bien à quel point il est un admirateur fasciné de Galois, et ce qu'a fait Grothendieck, c'est qu'il a compris comment géométriser la théorie de Galois, mais de manière suffisante pour qu'elle s'étende aux schémas, et parmi ces schémas, bien entendu, il y a la colonne du haut qui est le schéma qu'on appelle, en jargon, $\operatorname{Spec}\mathbb{Z}$. Alors quand on calcule les choses en utilisant justement les idées de Grothendieck sur les revêtements étales etc., eh bien, on s'aperçoit d'une analogie.

Alors cette analogie, elle est née en gros en 1963, il y a très, très longtemps, et en fait je crois que c'est David Mumford qui a eu le premier l'idée, et ensuite Barry Mazur l'a beaucoup développée. Et d'ailleurs, ici, un des académiciens, Jean-Loup Waldspurger a beaucoup travaillé là-dessus. Mais c'est une analogie. Donc c'est une analogie, alors ça paraît incroyable : comment est-ce qu'il pourrait y avoir une analogie entre les nœuds, donc je pense que vous imaginez ce que c'est qu'un nœud, c'est le nœud au sens bête, hein, je veux dire, alors au sens mathématique, ça veut dire qu'on a plongé le cercle dans la sphère S^3, une analogie, donc, entre les nœuds et les nombres premiers. Alors c'est une analogie qui paraît extrêmement bizarre, bien sûr, ça ne veut pas dire qu'à chaque nœud, vous allez associer un nombre premier et réciproquement, ce serait ridicule, mais c'est une analogie. Eh bon, comme André Weil en parle, il parle si vous voulez de subtiles caresses de l'un à l'autre etc. et du fait qu'il n'y a jamais une correspondance exacte.

Et dans cette analogie, donc, en fait, ce qui se passe, c'est qu'on peut relier, par exemple, le fait que la sphère S^3 soit simplement connexe avec le fait qu'il n'y a pas d'extension non ramifiée de $\mathbb{Z}$ enfin (etc.) du corps des rationnels etc. etc. Je ne vais pas vous embêter avec ça, mais je vais lentement venir maintenant à des considérations auxquelles j'ai contribué et qui sont directement reliées à ça. Et la contribution est extrêmement récente. Donc en fait, ce qu'on va voir, c'est qu'exactement comme Grothendieck a étendu la théorie de Galois, euh, pour les schémas, eh bien la théorie du corps de classes, qui est une théorie tout à fait classique très, très importante, qui permet justement de calculer ce qu'on appelle l'extension abélienne maximale dans le cas des corps, se prolonge au schéma relié au corps des rationnels.

Alors ça, c'est un travail donc en collaboration avec Caterina Consani, et ce qu'il faut retenir, c'est l'évolution des mots... vous voyez... je parle de *l'espace des classes d'adèles*. Alors, tout à l'heure, on a parlé des *idéaux*. Eh bien, Claude Chevalley a compris qu'il y avait un moyen de comprendre ce qu'on appelle *les classes d'idéaux* avec ce qu'on appelle *le groupe des classes d'idèles*, qui sont construites à partir des complétés du corps et de quelque chose qui est très, très concret. Et à partir de là, je crois que c'est André Weil qui a donné le nom d'*adèles*, à quelque chose qui n'est plus un groupe mais qui a une propriété merveilleuse de compatibilité avec l'analyse, et qui contient les nombres rationnels et les adèles, si vous voulez, la propriété qu'elles ont, c'est de dire bonjour à l'analyse, parce qu'elles forment un anneau localement compact, mais qui est intimement relié au corps des rationnels, par le fait que les rationnels sont dedans et ils forment un groupe discret et cocompact, bon.

Alors en fait en 1996, j'avais introduit un espace qui est l'espace des classes d'adèles, parce que classiquement, ce qu'on prend c'est *le groupe des classe d'idèles*. Alors *l'espace des classes d'adèles*, donc, c'est la variante *additive* de ça, et ce dont je vais vous parler, c'est le fait que grâce à cet espace, on va comprendre beaucoup mieux le lien entre les nœuds et les nombres premiers. Et on va, en fait, étendre la théorie du corps de classes pour les schémas. Donc en fait, l'espace des classes d'adèles, donc, que j'avais introduit en 1996, si vous voulez, il donne déjà, c'est connu depuis longtemps, la réalisation spectrale des 0 de ζ comme une cohomologie H^1. Il donne les formules explicites de Riemann-Weil comme formules de trace, il donne la formule de Hasse-Weil pour ζ. Je m'excuse de ce langage technique mais je vais expliquer. Et surtout en fait, il donne, si vous voulez, l'action du groupe qui permet de comprendre la formule de Hasse-Weil comme un groupe de Galois ; mais c'est un groupe de Galois, comme on le verra, qui est relié à ce qu'on appelle la géométrie tropicale, c'est-à-dire qu'il est relié à ce qu'on appelle $(\mathbb{R}, +, \max)$. Et en fait, cet espace, l'espace X_q, si vous voulez, il est incroyablement simple à décrire, à nommer. Pourquoi ? Parce que c'est simplement l'espace des sous-groupes de rang 1 de la droite réelle. Vous prenez la droite réelle, quand je parle de sous-groupe de rang 1, j'entends par là que c'est un sous-groupe tel que si je prends deux éléments de ce sous-groupe, ils sont commensurables : c'est-à-dire un multiple entier de l'un est égal à un multiple entier de l'autre alors ça vous paraît un espace très simple ; quand on est un peu naïf, on a l'impression que cet espace est très simple, mais en fait, c'est un espace qui a exactement les mêmes propriétés que l'espace des feuilles d'un feuilletage, très, très, très difficile à comprendre, et c'est ce qu'on appelle un *espace non-commutatif*. Et la *géométrie non-commutative* est faite pour comprendre les espaces de cette nature exactement.

Alors, une découverte qu'on avait faite en 2014, avec Katia Consani, on s'était aperçu qu'en fait cet espace c'est-à-dire si vous voulez l'espace des sous-groupes de rang 1 de $\mathbb{R}$, c'est en fait exactement un espace de points d'un topos de Grothendieck. Et le topos de Grothendieck en question a une définition, cette fois remarquablement simple, parce que c'est le produit de la demi-droite réelle 0 à l'infini par l'action des entiers par multiplication, et ça, c'est quelque chose qu'on a appelé le *site des fréquences*, et qui est presque, si vous voulez, intégralement relié à la musique parce que vous savez que la musique, vous avez des fréquences, et que l'oreille est sensible à la multiplication des fréquences par 2 ou par 3, et le site des fréquences, il... comment dire... il mathématise cette chose-là, sous la forme d'un topos de Grothendieck, et quand on regarde les points de ce topos, on obtient exactement l'espace, le même espace que celui qui est décrit ici, qui est l'espace des classes d'adèles. Alors ce dont on s'est aperçu, il y a environ un mois avec Katia Consani, c'est qu'en fait, si on regarde la projection de l'espace des classes d'adèles, donc que j'appelle $X_{\mathbb{Q}}^{ab}$, sur ce topos de Grothendieck, eh bien, on obtient ce qu'il faut, exactement, pour pouvoir faire la théorie du corps de classes pour les schémas, et donc voilà ce qui se produit : ce qui se produit, c'est que d'abord, pour chaque nombre premier, il y a une orbite périodique, c'est-à-dire qu'il y a vraiment un cercle dans l'espace $X_{\mathbb{Q}}$, et quel est ce cercle ? Si je vous donne un nombre premier p, eh bien, il y a un anneau qui lui correspond, c'est l'anneau $\mathbb{Z}/\frac{1}{p}\mathbb{Z}$; ça correspond, en fait, au niveau complémentaire du nombre premier p, donc on regarde maintenant les sous-groupes de rang 1 dans $\mathbb{R}$ qui sont isomorphes aux groupes additifs de cet anneau, et on s'aperçoit qu'ils forment un cercle, et que ce cercle a pour longueur le logarithme de p ; donc pour chaque nombre premier, on a un cercle de longueur logarithme de p, et maintenant, quand on cherche à relever ce cercle dans l'espace des classes d'adèles, on s'aperçoit qu'on ne peut pas le relever, bien sûr, il y a ce qu'on appelle une

monodromie, et cette monodromie, c'est exactement ce que donne l'action du Frobenius en p dans le groupe fondamental étale abélianisé du spectre de l'anneau local. Alors ça, ce sont des mots, mais pour bien comprendre l'analogie avec les nœuds, donc, on savait que c'était ça qu'il fallait obtenir, en terme de groupe fondamental étale, mais au niveau des nœuds, c'est facile, enfin relativement facile à comprendre, parce que si vous prenez deux nœuds, voilà, et qui sont enlacés dans ce qu'on appelle un entrelacement entre les deux, eh bien, pour le calculer, cet entrelacement, ce que vous faites, c'est que vous prenez le premier nœud, et vous essayez de le relever, dans le revêtement abélien du complémentaire du deuxième nœud, donc ça correspond exactement à ce qui se passe ici dans l'espace des classes d'adèles, et ça veut dire, si vous voulez, que maintenant, en fait, grâce à ça, euh, on a compris, enfin en tout cas, de mon côté, j'ai compris ce que j'avais trouvé, en fait en 1996, et ce que j'avais trouvé en 1996, ça n'était rien d'autre que l'extension de la théorie du corps de classes qui avant était purement limitée à Galois, l'extension du corps de classes aux schémas. Et bien sûr, à ce moment-là, si vous voulez, ça donne une lumière totalement différente sur ce qui avait été trouvé avant, et c'est comme ça que les mathématiques progressent, c'est-à-dire qu'au bout d'années et d'années et d'années, on s'aperçoit en fait qu'il y a un éclairage complètement nouveau qui apparaît, parce qu'on s'est posé une question, une question un peu insolite, qui était cette question de la relation entre les nœuds et les nombres premiers. Et il y a un autre élément, que je dis pour les mathématiciens, c'est qu'il y avait quelque chose qui m'avait toujours dérangé, qui était le fait que *les idèles sont denses dans les adèles*, or là, on a compris que cette densité, c'est exactement la densité de ce que Grothendieck appelle le point générique de Spec $\mathbb{Z}$ dans tout le spectre. Voilà.

Donc alors, j'en viens maintenant à un point sur lequel je veux arriver et auquel j'arrive, et c'est pour vous dire que c'est loin d'être fini. Et c'est loin d'être fini parce qu'ici, je cite Jacques Tits dans un article de 1956, dans lequel Jacques Tits parle (n'ayez pas peur) du corps à un élément. Donc ce que dit Jacques Tits, c'est, si vous voulez, pour un mathématicien, c'est une hérésie terrible, c'est-à-dire, il dit *(le corps à un élément, c'est)* le corps dans lequel 0 est égal à 1. Alors on ne voit pas trop qu'est-ce qu'on va pouvoir faire avec ça, d'abord. Mais bon, lui, sa motivation, c'était le fameux article de Chevalley sur les groupes algébriques, et il essayait de comprendre que quand on regarde les grandes séries de groupes finis, on a bien sûr toutes les séries avec des groupes simples qui proviennent des groupes sur les corps finis, et on a aussi tous les groupes alternés, sauf le groupe A_4 qui n'est pas un groupe simple. Donc toute cette série de groupes alternés, ça ne cadre nulle part, sauf si on admet qu'il y a un corps à un élément, oh la la ! Donc là, les mathématiciens poussent de hauts cris, sauf que quelques années plus tard, Yuri Manin et puis Christophe Soulé ont repris la question et l'idée de Manin était la suivante : il disait que finalement, il faut penser aux entiers comme à des polynômes sur un corps fini, mais bien sûr, ce n'est pas vrai. Et ce qu'il dit, c'est que si c'est le cas, à ce moment-là, on devrait faire des produits de Spec [4] etc. Alors, en suivant cette idée, Christophe Soulé a défini une fonction ζ qui est associée à un polynôme, et c'est à partir de la fonction ζ de Soulé qu'on a pu démontrer avec Katia Consani que la formule de Hasse-Weil s'étend à la fonction ζ de Riemann, mais ce n'est plus du tout une fonction polynôme,

[4] *Note de la transcriptrice : sur la diapositive projetée est notée un passage de l'introduction de l'article* Lectures on zeta functions and motives (according to Deninger et Kurokawa) *de Manin, l'auteur interroge dans l'introduction par la phrase :* "The central question we address can be provocatively put as follows : if numbers are similar to polynomials in one variable over a finite field, what is the analogue of polynomials in several variables ? Or, in more geometric terms, does there exist a category in which one can define "absolute Descartes powers" Spec$Z \times \ldots \times$Spec$Z$?"

mais c'est une distribution au sens de Schwartz. Et elle est très, très difficile. Et là, on revient à ce que disait André Weil, il dit :

> *Les mathématiciens du* XVI^{e} *siècle avaient coutume de parler de la "métaphysique du calcul infinitésimal", de la "métaphysique de la théorie des équations", ils entendaient par là un ensemble d'analogies vagues, difficilement saisissables et difficilement formulables, qui néanmoins leur semblaient jouer un rôle important à un moment donné dans la recherche de la découverte mathématique.*
>
> *A. Weil, De la métaphysique aux mathématisques, 1960.*

Alors là, on pourrait dire, oui, tout ça, c'étaient des temps anciens, dans lesquels les mathématiciens n'avaient pas les outils pour arriver à donner un sens à une idée, eh bien, heureusement, ce n'est pas le cas, et si vous voulez, ce qui s'est produit, c'est que, euh, on n'a pas le droit, en mathématiques, d'inventer des choses comme ça, sans démontrer de théorèmes. Tant que vous n'avez pas démontré de théorème, personne ne vous dira que vous avez la bonne notion. Alors, on a trouvé, avec Katia Consani, comment il fallait utiliser le corps à un élément, on a trouvé ce truc-là, et on en a déduit une formule de Riemann-Roch pour l'anneau des entiers. C'est une formule qui est parfaitement analogue à la formule de Riemann-Roch dans les trois colonnes, ce ne sont pas des colonnes bien sûr, dans les trois parties de la Pierre de Rosette, et en fait, cette formule, ce qui s'est produit, c'est assez amusant, c'est qu'au départ, on n'avait pas vraiment la bonne notion et on n'obtenait pas que le genre était égal à zéro. Pourquoi ? Parce qu'on utilisait le fait que tout entier s'écrit de manière unique comme un polynôme dans le nombre 3 [5] à coefficient plus ou moins 1 ou 0 ; ça, c'est vrai, ça va être utilisé par les Russes après la deuxème guerre mondiale pour essayer de fabriquer des ordinateurs, dans lesquels l'opération de soustraction était immédiate. Et en fait, on a mis beaucoup de temps avec Katia, mais on a une note aux Comptes-Rendus qui va paraître ; et en fait, ce qui est vraiment incroyable, c'est que l'anneau $\mathbb{Z}$, c'est un anneau de polynômes, sur ce corps à un élément et le générateur c'est le nombre -2 : tout nombre entier s'écrit de manière unique comme un polynôme à coefficients 0 et 1 dans le nombre -2 [6]. Et en fait, la théorie, elle est basée sur quelque chose d'extrêmement sophistiqué, qui est la théorie de l'homotopie. Et le corps à un élément correspond à ce qu'on appelle le spectre en sphère [7], qui est, si vous voulez, j'avais il y a très, très longtemps, je finis là-dessus, j'avais, il y a très très longtemps écouté une conférence à Oberwolfach dans laquelle Tom Goodwilly disait qu'il expliquait que les entiers étaient une algèbre sur quelque chose de beaucoup plus basique qui est justement le spectre en sphère. Alors en fait, le spectre en sphère, ça ne marcherait jamais, il faut avoir quelque chose de beaucoup plus simple, et en appliquant la technique qui a pour origine Chevalley, en fait, quand Chevalley définit un groupe algébrique, il dit que c'est un foncteur des anneaux commutatifs vers les groupes, en appliquant cette technique, la technique si vous voulez fonctorielle, on a trouvé, on espère, la bonne définition, mais comme toujours, il faut qu'elle passe 36 000 tests avant d'avoir le droit d'exister, dans le domaine des mathématiques, voilà. Je vais m'arrêter là-dessus.

---

[5] *Note de la transcriptrice : "dans le nombre 3" signifie dont le générateur est 3 ; i.e., un polynôme égal à une combinaison linéaire de puissances de 3.*

[6] *Note de la transcriptrice : dont le générateur est* -2

[7] *Note de la transcriptrice : Sphere spectrum ?*

Poursuite de la conférence par la séance de questions à l'orateur

---

Françoise Combes : Merci beaucoup pour ce passionnant exposé, est-ce qu'il y aura des questions ?

Alain Connes N'hésitez pas, je veux dire, je sais que Jean-Pierre [8] , où est Jean-Pierre ?...

Jean-Pierre Changeux : Merci. D'abord, je dois dire qu'en tant que neurobiologiste, je n'ai pas vraiment pu suivre l'exposé du début jusqu'à la fin, je le regrette beaucoup et il y avait un vocabulaire que je ne comprenais pas. Ceci dit, j'ai essayé de comprendre les raisonnements que tu as présentés, et il y a juste un point qui m'a un peu surpris, c'est l'importance de l'analogie, que tu reprends à plusieurs reprises, au moins trois ou quatre fois, oui ; en neurobiologie ou en biologie, en général, l'analogie est loin de la causalité qui peut exister entre l'objet et sa fonction, comme par exemple, l'aile de la chauve-souris ou celle du pinson, bien-sûr, qui ont la même fonction, mais elles sont construites de manière totalement différente... Alors eux...

Alain Connes : Non, mais analogie ne signifie pas du tout identité.

Jean-Pierre Changeux : Est-ce que on a le droit de parler d'analogie en mathématiques, et certainement qu'on a le droit, puisque tu le fais, oui, mais je voulais savoir si ça avait des implications... plus larges.

Alain Connes : Non, disons que là, on n'a aucun droit : pourquoi ? Parce que si tu veux, la mathématique est une réalité, qui est d'une résistance phénoménale. Donc si tu veux, le seul droit qu'on a, c'est de trouver un théorème, de faire des erreurs, de réparer les erreurs, de tester sur l'ordinateur, etc. C'est ça, le seul droit qu'on a. L'analogie est un guide, c'est-à-dire que lorsqu'on s'aperçoit qu'il y a des correspondances entre deux théories différentes et on n'a jamais l'idée qu'elles sont identiques, on n'a jamais idée, si tu veux, qu'à un nœud va correspondre un nombre premier, non, mais qu'il y a des correspondances, comme ça, et ces correspondances permettent de mettre la pensée en mouvement, en essayant de traduire, en espérant toujours qu'il y a une traduction possible, d'un domaine à l'autre. Et ça, effectivement, c'est extrêmement fructueux, mais c'est dangereux, bien entendu, c'est-à-dire que si on concluait de l'analogie, l'identité entre les deux domaines, ce serait une erreur terrible, bien sûr. Je pense que c'est pareil en biologie.

Une auditrice : Merci pour cet exposé très, très poétique mathématique. Donc j'ai une question simple. Je veux dire : est-ce que vous pouvez développer la façon dont vous avez étendu la formule de Hasse-Weil...

Alain Connes : Ah oui, absolument, oui, oui, alors, ça je vais l'expliquer, parce que Soulé avait défini, donc, une fonction ζ, dans le sillage de Manin, en prenant une limite, quand q tend vers 1, d'une somme, qui est la somme qui apparaît dans la formule de Hasse-Weil. C'est-à-dire que si vous voulez, dans la formule de Hasse-Weil, on a une somme et on a des puissances de q etc. Et puis, on regarde la fonction de dénombrement. Donc Soulé avait étendu ça, comme une limite

[8] Jean-Pierre Changeux

quand q tend vers 1. Alors la première chose qu'on a faite avec Katia Consani, on s'est aperçus que cette limite quand q tend vers 1, en fait, si on regardait, non pas la fonction ζ mais sa dérivée logarithmique, parce que le problème qu'avait Soulé, c'était qu'il était obligé de corriger par un facteur d'une puissance de q moins 1, avec un exposant qui était la caractéristique d'Euler ; or on sait très bien que pour la fonction ζ, la caractéristique d'Euler va être égale à moins l'infini ; donc ça ne marchait pas, mais par contre, quand on regarde la dérivée logarithmique de la fonction ζ, à ce moment-là, on obtient une formule en utilisant Soulé, qui est une limite quand q tend vers 1, et on s'est aperçus avec Katia Consani que cette limite quand q tend vers 1, c'était simplement une limite de somme de Riemann d'une intégrale. Donc on a remplacé la formule de Soulé, qui était une limite, par une intégrale ; ça, c'est beaucoup mieux déjà. Alors après, on a posé le problème inverse, c'est-à-dire qu'on a pris la fonction ζ de Riemann, avec son terme à l'infini, le terme archimédien, et on s'est dit "est-ce qu'il existe une fonction de comptage qui va compter le nombre de points, etc. telle qu'on obtienne la fonction ζ de Riemann ?". Alors ce qu'on a démontré, c'est que ce n'est pas une fonction, c'est une distribution au sens de Schwartz. Et pourquoi ça ne pouvait pas être une fonction ? La raison pour laquelle ça ne pouvait pas être une fonction, c'est qu'on sait que cette distribution, elle doit être positive, on sait aussi que sa valeur en 1 doit valoir moins l'infini donc ça, ça paraît complètement absurde : on se dit "comment est-ce qu'on peut avoir une fonction, qui soit positive mais qui ait la valeur moins l'infini en 1, puisque ça, c'est la caractéristique d'Euler.". Alors l'explication, en fait, elle vient de la formule qui donne cette distribution comme dérivée d'une fonction ; cette fonction, elle est croissante donc la distribution est positive, mais elle prend la valeur moins l'infini quand on s'approche de 1, alors que la valeur de la distribution au point 1 est finie, et donc, tout s'arrange. Alors quand on utilise cette distribution, ça donne le bon résultat. Mais ce qui nous a convaincus, c'est qu'en fait cette distribution, elle apparaît lorsqu'on regarde les points fixes du groupe de changement d'échelle dans le topos dont j'ai parlé tout à l'heure, c'est-à-dire que ce topos donne vraiment, si vous voulez, un espace géométrique qui supporte les formules de Riemann-Weil, etc., etc., pendant longtemps, on a cru que ce topos, que cet espace, c'était le spectre des entiers, non ! C'est l'espace qui joue le rôle de la théorie du corps de classes pour les schémas, et ça, c'est formidable, c'est un changement d'optique. Donc en fait une des choses les plus importantes en mathématiques, c'est de n'être sûr de rien, c'est-à-dire d'être capable de changer de point de vue *quand* vous recevez une information différente de celle que vous croyiez toujours. C'est ce que dit Grothendieck quand il dit (je ne me souviens pas des paroles exactes) quand il dit : "*Craindre l'erreur et craindre la vérité sont une seule et même chose.*". Et ce qu'il explique, précisément, c'est que quand on craint de se tromper, quand on craint l'erreur, on reste figé, dans les croyances auxquelles on a été habitué et qui nous empêchent d'aller de l'avant, qui nous empêchent de trouver du mil [9]. Il y a une dernière chose que je voudrais rajouter, c'est une chose très importante au niveau de... je ne sais pas pour la biologie mais bon, vous savez, quand on croit que le mathématicien, il est là, et on dit : "Ah ! Il n'a besoin que d'une feuille de papier et d'un crayon !" : je m'inscris en faux contre ça ; je m'inscris en faux contre ça, pourquoi ? Je prétends que le mathématicien, s'il a une feuille de papier, qu'il écrit sur cette feuille de papier, puis qu'il la laisse traîner, n'a rien fait. La difficulté pour faire des mathématiques, c'est d'écrire dans son cerveau ; et ça, c'est infiniment plus difficile que d'écrire sur une feuille de papier, c'est infiniment plus difficile, parce que pour écrire dans son cerveau, il faut prendre un problème, et il faut sécher sur le problème, il faut avoir l'air idiot, il ne faut pas avoir peur du tout d'avoir l'air

[9] *Note de la transcriptrice : référence directe au mil = au blé et donc au livre* Récoltes et semailles *d'Alexander Grothendieck.*

idiot pendant des heures, c'est à ce prix-là qu'on écrit dans le cerveau. Et quand vous avez écrit dans votre cerveau, vous avez ce qu'on appelle une image mentale de l'objet que vous considérez, et là, vous pouvez commencer à le manipuler, etc. Vous n'avez pas besoin d'une feuille de papier et d'un crayon.

Françoise Combes : J'aimerais poser une question : comment un mathématicien trouve-t-il le sujet sur lequel il va chercher ; par exemple, pour les travaux que tu nous as présentés, comment t'est venue l'idée de travailler là-dessus ?

Alain Connes : Ah ! C'est une excellente question, parce que jamais un mathématicien n'aurait l'idée de travailler sur un problème très difficile, sachant que c'était un peu signer sa perte, d'accord ?! Donc comment est-ce qu'un mathématicien va travailler là-dessus ? Dans mon cas, je peux simplement vous raconter ce qui s'est passé dans mon cas. Dans mon cas : j'avais écrit avec Jean-Benoît Bost un article dans le début des années 1990 dans lequel apparaissait la fonction ζ de Riemann, un peu de manière inopinée, elle apparaissait dans ce que les physiciens appellent une fonction de partition, dans un système qui avait une transition de phase avec brisure spontanée de symétrie. Et donc après avoir trouvé ce système, j'avais été invité à Seattle en 1996 pour le $100^{\text{ième}}$ anniversaire du théorème des nombres premiers. Donc j'y suis allé, j'étais un peu surpris d'être invité, j'étais content d'être invité, donc j'y suis allé, j'ai fait mon exposé et après mon exposé, Selberg est venu me voir, il m'a dit : "*It isn't clear that what you are doing will be related to the zeros of* ζ." [10]. Pourquoi pas, bien sûr, il faut être réaliste, donc quand je suis rentré, j'ai décidé de ne pas me décaler en termes d'horaire, c'est-à-dire que j'ai gardé l'horaire de Seattle pendant une semaine. Je n'ai rien fait, à l'époque, je n'avais pas d'email [11]. Donc je ne regardais pas d'email, je n'avais aucune distraction, la seule distraction que j'avais, c'était de lire un livre, que les gens connaissent sans doute, qui s'appelle *The right stuff*, qui est le livre sur l'histoire d'Apollo 13 [12] . Donc je lisais ce livre, et puis je rêvassais, et au bout d'une semaine, je me suis dit "m..., voilà comment les formules explicites de Weil apparaissent à partir du système que j'avais trouvé avec Jean-Benoît Bost.". Donc j'étais à mon bureau, avant j'étais couché la plupart du temps, donc j'étais à mon bureau, et puis j'ai vérifié effectivement que les formules telles que Weil les avait écrites, et qui sont magnifiques, apparaissaient vraiment telles que celles obtenues si on prenait le système que j'avais écrit avec Jean-Benoît Bost, et qu'on regardait l'espace non-commutatif correspondant, qui est l'espace dont je parle, l'espace F_q. Puis après, je me suis dit "ah d'accord, c'est bien d'avoir les formules de Weil, mais et les zéros de ζ ?". Et là, je me suis aperçu, presque tout de suite, qu'en fait les zéros de ζ apparaissaient mais de manière extrêmement bizarre : ils apparaissaient comme un spectre d'absorption, et ça, ça résolvait le problème du signe moins, sur lequel les gens butaient pour avoir la réalisation spectrale, parce que dans toutes les formules, les zéros de ζ apparaissent avec un signe moins, qu'on comprend très bien lorsqu'on pense en terme de caractéristique d'Euler, et là, ça apparaissait comme un spectre d'absorption. Et alors, donc, depuis, si vous voulez, je n'ai pas pu m'empêcher de travailler, de temps en temps, sur ce problème-là, et une des choses très importantes sur les spectres d'absorption... Vous savez que les spectres d'absorption, le premier, sans doute, c'est le spectre du sodium, qu'on a aperçu à partir de Newton : quand on décompose

[10] *Note de la traductrice : "Il n'est pas évident du tout que ce que vous faites sera relié aux zéros de* ζ*".*

[11] *Note de la transcriptrice : on sent poindre une nostalgie.*

[12] *Note de la transcriptrice : ce livre est traduit en français sous le titre L'étoffe des héros et a été porté au cinéma dans un film au titre éponyme, dans lequel joue l'acteur Ed Harris.*

la lumière du soleil par un prisme, et puis ensuite, Fraunhofer a trouvé 500 raies environ, et parmi ces raies, si vous voulez, il y en avait un tas, dans le spectre d'absorption, qu'on pouvait retrouver sur la Terre comme un spectre d'émission, comme le sodium, comme 36 choses ; par contre, il y avait des raies spectrales qui ne correspondaient à aucun corps chimique sur Terre. C'était très embêtant. Alors qu'ont fait les physiciens ? Eh bien, ils lui ont donné un nom en l'honneur du Soleil, ils l'ont appelé l'hélium. Alors, c'était très embêtant, bien sûr, sauf qu'il y a eu à la fin du XIX^{e} siècle une éruption du Vésuve et quand on a fait l'analyse spectrale de la lave qui sortait du Vésuve, on a trouvé l'hélium. Et bien sûr, l'hélium, maintenant, on l'utilise tout le temps. Alors, si vous voulez, une des stratégies qu'on utilise et qui avance par rapport à ζ, c'est l'idée de transformer le spectre d'absorption que j'avais trouvé en un spectre d'émission, et récemment on a trouvé avec mon collaborateur Henri Moscovici, on a trouvé le lien avec ce qu'on appelle l'opérateur sphéroïdal prolate, qui est un opérateur connu, je veux dire en analyse, et dont le spectre reproduit de manière très voisine les zéros de ζ. Donc voilà où on en est. Jamais personne n'aurait l'idée de dire : "je vais m'attaquer à ζ", ce serait ridicule, donc il faut un concours de circonstances, une espèce de... comment dire... de coïncidence, mais la coïncidence ne suffit pas, il faut la reconnaître et la suivre.

Françoise Combes : Merci beaucoup. Est-ce qu'il y a d'autres questions ?

Un auditeur : Oui, je voulais vous demander si l'informatique et l'intelligence artificielle allaient modifier complètement la recherche en mathématiques et peser sur l'imagination.

Alain Connes : Bon alors, c'est une question évidemment brûlante, dont je ne voulais pas parler, bon. Mais, vous m'obligez. Voyons : vous voyez, ce qui est caractéristique, pour le moment, qui échappe à l'intelligence artificielle, c'est la possibilité qu'ont les mathématiciens de créer un concept à partir de myriades de cas particuliers. Prenons l'exemple des topos de Grothendieck. Vous voyez, on arrive à créer un concept de manière précise, à partir de myriades de cas, et on arrive à trouver le formalisme qu'il faut pour créer ce concept, et là, je parle vraiment de créer ce concept. Et pour le moment, l'intelligence artificielle, je l'utilise bien sûr, quand je dois écrire une lettre de recommandation, j'utilise Chap-GPT. Donc c'est très pratique. Pour le moment, je n'y vois qu'une secrétaire d'une extraordinaire efficacité, c'est ça que j'y vois, et j'y vois surtout, si vous voulez, quelqu'un qui est capable, ou quelqu'une qui est capable, d'aller chercher dans la littérature toutes sortes de choses que moi, jamais, je n'arriverai à trouver. Donc, ça va aider, ça va aider terriblement ; j'utilise énormément `Mathematica` sur l'ordinateur, pour faire des calculs. Donc je ne peux pas dire, je ne néglige pas ça, mais je pense que pour l'instant, pour l'instant, il y a encore quelque chose qui est totalement inaccessible à l'intelligence artificielle, et c'est ce qui permet, si vous voulez, de zipper toutes ces connaissances en la création d'un concept, ça, c'est fabuleux. Je veux dire, on le voit chez Galois, on le voit dans tous ces exemples-là, c'est quelque chose. Et bon, alors, je ne sais pas comment ça va évoluer, si ça évolue... Il n'est pas impossible qu'on arrive, je ne sais pas, à quelle idée, avec cela. Mais pour le moment, je pense que le cerveau humain a des petits avantages.

Un auditeur : Merci beaucoup. Moi, il me semble que l'une des créations les plus extraordinaires de l'imagination mathématique, c'est la découverte par Cantor du fait qu'il y a une infinité d'infinis, que ça ne s'arrête jamais, qu'on n'arrive pas à décrire vraiment la suite des ordinaux et des cardinaux.

Alain Connes : Oui ! Non, non, très bien, très bien, je vous arrête, je vous arrête, parce que malheureusement ce n'est pas du tout l'opinion qu'on a en tant que mathématicien : en tant que mathématicien, la théorie des ensembles est une théorie rasoir, je suis désolé de le dire parce qu'elle est... elle est... d'une certaine manière elle est trop simple, et on la remplace, en mathématiques, par la théorie des catégories, qui elle n'est pas du tout rasoir. Et ça, c'est une évolution très importante, bon, je veux dire, les cardinaux, je m'excuse, c'est magnifique, bien sûr, hein, d'ailleurs si vous voulez apprendre à quelqu'un la théorie des ensembles, il ne faut surtout pas... il faut simplement lui poser la question "démontre-moi qu'il n'y a pas de manière d'épuiser les nombres réels, en donnant le premier, le $2^{\text{ème}}$, le $3^{\text{ème}}$, etc., d'accord ?". Si vous posez cette question à quelqu'un et s'il essaie d'y réfléchir, il aura compris la théorie des ensembles, d'accord ? Il ne faut pas lui dire "un ensemble, c'est machin, et deux, c'est... Non !" ; si vous voulez, je vous donne la démonstration, il y a 36 démonstrations et 36 démonstrations dont chacune fait appel à une propriété différente des nombres réels. Moi, la démonstration que je préfère de loin, c'est la suivante : ça consiste... Ok, quelqu'un vous dit "d'accord, j'ai epelé tous les nombres réels !", il me donne le premier, le deuxième, et alors moi je lui dis : "eh bien autour du premier, tu mets un intervalle de longueur 1/2, autour du deuxième, tu mets un intervalle de longueur 1/4, autour du 3ème, tu mets un intervalle de longueur 1/8..." Eh bien, je suis désolé, tu n'auras pas rempli plus que 1, la droite, elle est infinie, donc ça ne marche pas. Une autre démonstration, c'est la démonstration de... on a un mathématicien français qui s'appelait René Baire, qui était un mathématicien formidable. Or René Baire a démontré que si on prend une intersection dénombrable d'ouverts denses, c'est encore dense, si vous voulez ; donc chaque fois que vous enlevez un point, le complémentaire, c'est un ouvert dense, donc ça vous dit qu'en fait, vous auriez pu aussi essayer d'épeler avec des... comment dire... avec des fermés d'intérieur vide, vous n'y arriverez jamais ; ça c'est formidable ! Et enfin, enfin, il y a bien sûr la démonstration bien connue du paradoxe, etc., que je ne vais pas vous imposer.

Françoise Combes : On va prendre une dernière question. Jean-Pierre Bourguignon ?...

Jean-Pierre Bourguignon : Oui. Dans les exemples que tu as donnés, qui sont presque toujours dans le contexte algébrique, il y a toujours de la géométrie sous-jacente et comme tu le sais, quand Lobatchevski a introduit la géométrie qu'on appelle aujourd'hui *géométrie hyperbolique*, il l'a appelée *géométrie imaginaire*...

Alain Connes : Oui...

Jean-Pierre Bourguignon : Et c'est aussi lié à des nombres négatifs, mais d'une autre façon.

Alain Connes : Bien sûr.

Jean-Pierre Bourguignon : Comment incorpores-tu ça dans ta réflexion ?

Alain Connes : Bah, si tu veux, j'incorpore ça, bien sûr, ça joue un rôle absolument fondamental puisque surtout par Riemann, c'est-à-dire, bon, Lobatchevski, etc., les gens ont lentement quitté le formalisme purement euclidien pour admettre d'autres géométries, mais surtout, surtout, grâce à Riemann, et au fait que la courbure peut être variable, etc. Donc c'est ça, la vraie transition, c'est pas tellement Lobatchevski, c'est plus Riemann, et bien sûr, après, Einstein, et... d'accord...

Je m'excuse aussi car dans mon titre, j'avais parlé de l'espace-temps, mais ce serait vraiment un autre exposé. Quand j'ai préparé, je me suis aperçu que je n'en parlerais pas...

Françoise Combes : Bien, merci beaucoup, nous remercions encore Alain Connes.

(applaudissements).

Conférence d'Alain Connes "Espace et symétries : de Galois au monde quantique", séance publique de l'Académie des Sciences, Conférence dans le cadre des défis scientifiques du xix^{e} siècle - Le 21 mars 2006.[1]

Edouard Brézin : Mesdames, messieurs, chers consoeurs, chers confrères, la série des conférences Défis scientifiques du 21e siècle nous permet cet après-midi d'accueillir Alain Connes. Sa conférence avait été programmée l'an passé mais un jour où l'électricité manquait et donc, nous avons attendu quelques mois avant de l'entendre sur le sujet qu'il a choisi (avec de l'électricité) qui s'appelle espace et symétrie de Galois au monde quantique. Chers confrères, vous avez peut-être remarqué parmi nous de jeunes visages, je les vois à droite, là-bas.

C'est une classe de première du lycée français de San Francisco qui a souhaité profiter d'un voyage à Paris pour rencontrer des scientifiques. Donc, c'est pour eux que je préciserai que Alain Connes est un mathématicien algébriste et géomètre, qu'il est le fondateur, en particulier, de la géométrie non-commutative, que ses travaux lui ont valu la plus haute distinction des mathématiques qui s'appelle la médaille Fields en 1982 et que vous permettrez au physicien que je suis de dire combien je me réjouis que son inspiration soit souvent venue de la physique. Cette conférence est retransmise sur le site internet de l'Académie grâce à une collaboration avec le Centre de communication scientifique directe de l'IN2P3 à Lyon et à ce propos je voudrais vous lire un courrier électronique qui a été adressé à Madame Meier, la responsable de notre Direction d'information scientifique et de la communication, qu'elle a reçu ce message il y a quelques jours, et je trouve qu'il justifie les efforts que nous faisons et que fait le CCSD pour retransmettre les conférences.

L'interlocuteur de Madame Meier lui écrit je tiens à vous dire merci pour la vidéo-conférence du professeur Denis Duboule que je viens de suivre, votre académie est formidable pour permettre cette transmission ad libitum en particulier aux médecins retraité que je suis dans un petit village Vosgien, Romont 88700. Je suis âgé de 70 ans, vous me donnez de magnifiques moments d'enseignement rompant ma solitude. Voilà qui justifie nos efforts. Alain Connes, la parole est à toi.

Alain Connes : Ok, donc, c'est assez difficile en mathématiques, si vous voulez, c'est pratiquement impossible heureusement, de prédire ce qui va se passer parce que, si vous voulez, les mathématiques justement évoluent vraiment par surprise, c'est à dire qu'essayer de justement, même de formuler des problèmes etc., ce serait une erreur. Par contre, ce que je vais essayer de faire, c'est de montrer en particulier pour les jeunes du lycée de San Francisco à quel point c'est un domaine ouvert, et pour cela, j'ai choisi si vous voulez deux espaces, qui sont assez faciles à expliquer de manière naïve, qui sont beaucoup plus difficiles à comprendre de manière sophistiquée. Et malgré tous les progrès qu'on a fait au xxe siècle, on peut dire, si vous voulez, que ces espaces on ne les comprend toujours pas. Donc les espaces en question, c'est l'espace-temps qui est vraiment à l'origine si vous voulez de l'idée même de géométrie, d'un côté donc, et bien sûr relié à la physique, mais faire une séparation, si vous voulez arbitraire, entre les mathématiques et la physique serait une erreur. Et l'autre, ça peut vous surprendre si vous voulez, c'est l'ensemble des nombres premiers. Je commencerai par l'ensemble des nombres premiers parce que j'essaierai de vous convaincre, à quel point

[1] Cette vidéo n'étant plus visionnable sur le site de l'Académie des Sciences à cette page https://www.academie-sciences.fr/archivage$_site/video/vdefi210306.htm$, on la retrouve là https://webcast.in2p3.fr/player/4ee6119165828, et je l'ai stockée là : http://denise.vella.chemla.free.fr/alain-connes-et-galois.mp4.

justement, c'est la géométrie de cet espace qui reste encore mystérieuse. Donc heureusement en mathématiques, on a des tests très très simples pour savoir si on comprend ou pas. Et si on regarde l'ensemble des nombres premiers, donc bon, vous pouvez dire "je comprends" (j'espère que vous savez ce que c'est qu'un nombre premier, c'est un nombre qui n'est pas divisé par d'autres nombres que 1 et lui-même). Donc voilà la liste des premiers nombres premiers, là, qui sont là, et alors la quantité qui intéresse les mathématiciens, c'est une quantité qui va varier avec n, qui va croître avec n, on sait qu'elle tend vers l'infini depuis Euclide c'est le nombre de nombres premiers qui sont plus petits ou égaux à un entier n. Alors vous entendrez des gens vous dire "oui, alors ce qui va pas avec cette quantité, mon prof. me l'avait dit lorsque j'étais en seconde, il m'avait dit il n'y a pas de formule qui donne cette fonction en fonction de n. Alors ça c'est complètement faux, il y a une formule, elle est due à un mathématicien français qui s'appelle Laurent, ça date d'environ 1850, et vous pouvez l'utiliser sur l'ordinateur, et l'ordinateur il va utilise,r c'est une formule qui est valable pour n plus grand que 5. On suppose qu'on sait calculer jusqu'à 5 la fonction π de n d'accord ? Bon. Alors vous pouvez l'utiliser etc., par contre, c'est pas une formule qui va vous donner des informations sur le comportement à l'infini, si vous voulez, de cette fonction $\pi(n)$.

Alors ce comportement à l'infini de la fonction $\pi(n)$, la manière dont elle se comporte, il avait été deviné par Gauss qui l'avait rappelée à un astronome, Encke, lorsqu'on la lui avait demandée. Donc il l'avait devinée vers le début du XIXe siècle qu'en fait si vous voulez, cette fonction $\pi(x)$, d'accord, eh bien, elle était, en fait, très très bien approximée par ce qu'on appelle le logarithme intégral, donc le logarithme intégral, c'est intégral de 0 à x de du sur log de u

$$\mathrm{Li(x)} = \int_0^{\mathrm{x}} \frac{\mathrm{du}}{\mathrm{log(u)}}.$$

Oh ! Si vous êtes mathématicien, vous pouvez avoir quelques frayeurs lorsque u vaut 1 dans l'intégrale, mais ça s'arrange bien. Et le terme que vous avez à droite, vous voyez, ce n'est absolument pas une série convergente puisque vous avez une factorielle qui est devant, mais c'est le prototype de ce qu'on appelle des séries asymptotiques, c'est à dire, ce sont des séries qui donnent des résultats numériquement extrêmement valables lorsqu'on s'arrête aux plus petits termes de la série typiquement.[2]
D'accord. Alors en fait, donc, je disais, on a des tests en mathématiques pour savoir si on comprend ou pas, et ces tests s'appellent des conjectures. Donc si vous voulez, il y a des problèmes centraux en mathématiques, il y a des problèmes qui sont là simplement pour être des espèces de bornes kilométriques, qui vous indiquent si vous comprenez ou pas. Ou vous en êtes dans votre compréhension. Et un des problèmes les plus centraux des mathématiques, ça ne va pas vous paraître central quand je l'énonce comme ça mais on va voir pourquoi il est central, c'est ce qu'on appelle la conjecture de Riemann. Et c'est une conjecture qui vous dit, si vous voulez, que lorsque vous écrivez cette formule, c'est à dire, on va voir au niveau du graphe, ce que ça donne, donc vous pouvez faire un graphe qui vous donne ce que vaut la fonction $\pi(x)$ avec l'ordinateur et ce que vaut la fonction logarithme intégral. Vous pouvez tracer ces deux graphes, et lorsque vous tracez ces deux graphes, la fonction $\pi(x)$ c'est une fonction en escalier parce que elle va croître de 1 chaque fois que vous passez à travers un nombre premier, d'accord, donc c'est cette fonction en escalier comme ça. Et la fonction logarithme intégral, c'est la fonction qui est parfaitement

[2] l'approximation écrite au tableau est : $\mathrm{Li}(x) \sim \sum (k-1)! \frac{x}{\log(x)^k}$.

régulière, c'est le graphe qui est parfaitement régulier qui est au-dessus, d'accord. Alors on peut s'amuser, bien sûr, à regarder la différence entre les deux, et c'est sur la différence entre les deux que porte cette fameuse conjecture de Riemann, qui vous dit qu'en fait la différence entre les deux elle est de l'ordre de la racine carrée de x, d'accord, donc on prend la racine carrée de x et on la multiplie par logarithme de x mais enfin en gros, ça vous dit que si vous voulez, c'est un ordre qui vient en fait du théorème de limite centrale de Gauss, justement, c'est à dire qui est entièrement probabiliste. Et d'ailleurs, je veux dire, au début, les gens avaient pensé que cette fonction serait toujours négative mais en fait on sait depuis Littlewood qu'elle change de signe une infinité de fois. Donc vous voyez, les apparences sont trompeuses, on pourrait croire que cette fonction va continuer à décroître indéfiniment. Mais par contre le nombre à partir duquel, et les nombres sur lesquels elle va croiser la droite réelle etc., on ne les connaît toujours pas donc on sait qu'elle va changer de signe une infinité de fois, mais on est dans ce genre de situation.

Donc alors, ce problème, donc si vous voulez, de l'estimation de la fonction $\pi(x)$, en fait, c'est un problème extrêmement intéressant parce qu'au lieu d'être un problème qui est formulé seulement sur la taille du reste, en fait, c'est un problème qui est une conjecture si vous voulez. En fait ce qu'on appelle hypothèse de Riemann, parce que Riemann faisait une hypothèse, et c'était une hypothèse sur les zéros d'une certaine fonction. Cette fonction, elle remonte à Euler, et c'est une fonction qui vous dit **en un mot** ce que c'est qu'un nombre premier. Voyez la formule qui est ici, qui écrit une somme infinie avec l'exposant $-s$, des nombres entiers, comme un produit donc on écrit une somme comme un produit, eh bien cette formule, elle ne marche exactement que pour l'ensemble des nombres premiers. C'est à dire que cette formule elle équivaut à dire que tout nombre entier se décompose de manière unique en produit de puissance de nombres premiers, elle est exactement équivalente à ça. Alors il se fait, ça si vous voulez, ça a été démontré par plusieurs mathématiciens, mais Riemann en particulier, que cette fonction elle a un prolongement, ce qu'on appelle un prolongement analytique, c'est à dire que c'est pas seulement une fonction qui, a priori elle serait définie seulement pour s un nombre réel plus grand que 1 parce qu'à ce moment-là, la série converge ; en fait, elle est définie lorsque s est un nombre complexe, et pas seulement un nombre complexe de parties réelle plus grande que 1, il suffit que ce nombre complexe soit différent de 1. Et donc, elle définit en fait une fonction dans le plan complexe, et l'hypothèse de Riemann dit la chose suivante donc : il dit que les seuls zéros de cette fonction sont situés sur ce qu'on appelle la droite critique c'est à dire, voyez, dans le plan complexe, il y a le point 0, il y a le point 1, et puis à la droite verticale qui passe par le point $\frac{1}{2}$. Eh bien, alors, on peut calculer, les gens ont calculé des milliards de zéros, et pour le moment tous les zéros qu'ils ont calculés ont la propriété si vous voulez que leur partie réelle vaut $\frac{1}{2}$. Ce sont les zéros non triviaux bien sûr, d'accord, alors pourquoi est-ce que ça s'est relié au comportement des nombres premiers. Eh bien parce que Riemann a démontré dans son article en fait il a démontré une formule, qui est l'ancêtre de ce qu'on appelle les formules explicites. Donc la formule explicite de Riemann, c'est une formule qui va calculer cette fonction $\pi(x)$. C'est assez extraordinaire, si vous voulez, qu'il y ait une formule qui calcule cette fonction $\pi(x)$. Alors en fait, on peut simplifier un peu, Riemann introduit une fonction qui est un tout petit peu plus simple, mais à partir de laquelle vous pouvez facilement calculer la fonction $\pi(x)$ par la formule d'inversion de Möbius. Donc il y a une autre fonction qu'on appelle $\pi'(x)$ qui est un tout petit peu plus simple parce qu'on la régularise en rajoutant à $\pi(x)$ un demi de π de la racine de x plus un tiers de π de la racine cubique de... et ainsi de suite ; ça va s'arrêter au bout d'un moment, d'accord, parce que ça sera zéro au bout d'un moment. Donc en

fait, ce que démontre Riemann, c'est qu'il y a un lien direct entre la fonction $\pi(x)$ ou plutôt cette petite variante de la fonction $\pi(x)$ et le logarithme intégral. Donc ce qu'il dit, si vous voulez, c'est que Gauss avait raison, le terme principal, c'est le logarithme intégral de x, mais à ce logarithme intégral de x, il faut rajouter une somme et c'est la somme sur les zéros qu'on a vus tout à l'heure. Alors vous voyez bien que selon ou non que les zéros vont être de partie réelle égale à $\frac{1}{2}$, on va avoir exactement la taille, le comportement à l'infini, du reste qui est ici. C'est à dire que ce qui serait embêtant, ce serait d'avoir dans l'image précédente, et ça, on ne sait toujours pas si c'est vrai ou pas, ce qui serait très embêtant si vous voulez c'est d'avoir non pas un point on sait qu'il y a une certaine symétrie qui se produit, et il pourrait que très très très très très très haut, si vous voulez, dans cette bande là au lieu d'avoir un zéro sur la droite partie réelle égale à $\frac{1}{2}$, en fait on aurait un couple de zéros qui serait symétriques par rapport à cette droite. Si on avait un tel couple de zéros, eh bien à ce moment-là, on n'aurait pas du tout le comportement asymptotique avec le reste qui était en racine de x. Alors donc tout ça, c'est contenu dans un papier extrêmement court de Riemann, qui fait environ quatre-cinq pages, et dans lequel il commence si vous voulez par donner deux démonstrations différentes de ce qu'on appelle l'équation fonctionnelle de la fonction ζ.

Donc c'est un papier visionnaire, vraiment, et on peut dire si vous voulez qu'une grande partie, pas tous bien sûr mais qu'une grande partie des mathématiques du XXe siècle a été sans le dire orientée par cette conjecture de Riemann. Alors, il y a eu bien sûr des résultats, c'est à dire qu'en général, si vous voulez, donc, on peut bien sûr amoindrir considérablement l'énoncé, et on obtient à ce moment-là ce qu'on appelle le théorème des nombres premiers, qui a été démontré par Hadamard et de la Vallée-Poussin, donc au début du XXe siècle. Alors que dit ce théorème ? Eh bien, il dit qu'en fait, vous vous rappelez qu'il y avait cette formule asymptotique pour la fonction logarithme intégrale et que la formule asymptotique, elle commençait précisément par x sur log de x. Alors en fait, ça, c'est êmement intéressant parce que qu'est ce que ça vous dit ? Ça vous dit que si vous comptez le nombre de nombres premiers qui sont plus petits qu'un entier donné, vous prenez cet entier et vous le divisez par en gros son nombre de chiffres, vous voyez, le logarithme d'un nombre, c'est le nombre de chiffres de ce nombre, il faut le multiplier par deux virgule quelque chose etc.[3]. Mais donc, ça vous donne un énoncé extrêmement précis sur le comportement moyen de la fonction $\pi(x)$, ça vous dit que la probabilité que vous avez, si vous cherchez un nombre - je ne sais pas moi - de 15 chiffres par exemple, savoir si oui non il est premier, eh bien, c'est exactement l'inverse du nombre de chiffres, d'accord, avec un facteur correctif, comme je l'ai dit, puisqu'il faut prendre le logarithme à base e ce qu'on appelle logarithme népérien, et non pas le logarithme à base 10, qui serait le nombre de chiffres. Alors en fait, donc, ce théorème est dû à Hadamard et de la Vallée-Poussin, et si vous savez faire un petit exercice de faire une soustraction, vous verrez qu'au début des années 60, les gens pensaient que le fait qu'ils avaient démontré le théorème des nombres premiers les avait rendu immortels. Vous verrez que Hadamard a vécu 98 ans et de la Vallée-Poussin 96. Alors en fait, si vous voulez, la manière dont ils démontraient ce théorème, qui est le théorème des nombres premiers, il le démontrait grâce à la fonction ζ pour Hadamard, grâce à la fonction ζ de Riemann. Et on peut dire la démonstration, en fait, en un mot, c'est une démonstration d'une simplicité vraiment étonnante. En fait donc ce que démontre Hadamard, il démontre que la fonction ζ n'a pas de zéro, alors ce qu'on voudrait, c'est qu'elle n'ait pas de zéro en dehors de la droite critique que je vous ai montrée tout à l'heure, mais ce que démontre Hadamard, c'est que cette fonction, vous voyez, n'a pas de zéro sur la droite qui est ici, la droite

[3]La constante e

de partie réelle égale à 1, par symétrie, elle n'a pas non plus zéro sur la droite ou par la partie réelle est nulle, c'est à dire où le nombre est imaginaire pur. Et comment est-ce que Hadamard fait cette démonstration, comment est-ce qu'il fait cette démonstration, eh bien l'essentiel de la démonstration est contenu dans l'observation suivante : il démontre que si la fonction avait un zéro en un point de la forme $1 + is$, à ce moment-là, elle aurait un pôle, c'est-à-dire elle serait infinie, au point $1 + 2is$, d'accord. Et la démonstration, elle tient en une ligne, c'est ce que je disais tout à l'heure, c'est à dire en fait on voit assez facilement que si la fonction avait un zéro, en prenant son logarithme, tous les nombres premiers élevés à la puissance $-is$ se concentrerait sur le point -1, de manière probabiliste, et ça, ça implique immédiatement que lorsqu'on prend leur carré, ils se concentreraient sur le point 1, et ça ça implique immédiatement que la fonction ζ serait infinie, au point correspondant, donc c'est comme ça que Hadamard démontre le théorème des nombres premiers, et si vous voulez, en fait, bon, on sait que les termes successifs dans le développement asymptotique sont les bons, mais bien sûr, c'est extrêmement loin, de savoir, où sont situés les zéros.

Alors en fait devant un problème qui est très difficile il y a une technique, une stratégie, qui est complètement générale, qui ne s'applique pas à un problème particulier, mais qui s'applique en général. Donc lorsque les mathématiciens font face à un problème qui est très difficile, il y a une stratégie générale, qui est en plusieurs étapes : le premier pas de la stratégie consiste à généraliser le problème, d'accord. Donc on vous donne par exemple un problème de..., formulé en termes de chiffres, tout à fait concret : le fait que le problème soit formulé de manière concrète en général n'est pas un avantage du tout parce que le premier pas, c'est d'arriver à en comprendre, si vous voulez, la position conceptuelle. Donc pour ça, le premier pas consiste à le généraliser. Et une fois que le problème a été généralisé de manière suffisamment souple si vous voulez, le pas suivant, ça consiste à arriver à le spécialiser dans un cas qui est suffisamment simple pour qu'on puisse le résoudre. Donc on introduit, si vous voulez, une espèce de variabilité dans le problème. On a un problème qui est tout à fait spécifique, on commence par le généraliser, et ensuite on le spécialise à un cas qui est plus simple, mais qui est plus facile à comprendre et si possible on résout donc un cas simple de la généralisation. Et la troisième étape qui est absolument en général la plus difficile si vous voulez elle consiste à essayer de comprendre les idées qui gouvernent le cas plus simple, et à essayer de les transplanter, sans les faire périr, bien entendu, je veux dire. Cette idée de transplantation a été le mieux illustré je crois par Oka au niveau de la terminologie etc. Donc on prend une idée, et on essaie, si vous voulez, de la transplanter sans la détruire du cas le plus simple au cas le plus compliqué. Alors dans le cas de la fonction ζ, vous m'excuserez si je rentre dans des choses un peu techniques, mais je pense qu'il faut essayer de regarder avec une certaine distance, et on va voir donc si vous voulez, dans cet exemple, ce qu'ont fait les mathématiciens pendant le XXe siècle ; ensuite, on passera à l'espace-temps. Donc cette manière, si vous voulez, qu'on avait, de généraliser le problème dans le cas de la fonction ζ, donc, les mathématiciens se sont aperçus que le problème, donc formulé par Riemann si vous voulez, c'était un problème qui pouvait se formuler de manière très très simple, en termes de ce qu'on appelle le corps des nombres rationnels. Donc je suppose que vous avez tous appris les fractions, vous avez appris que qu'on pouvait les ajouter, qu'on pouvait les multiplier, qu'on pouvait les inverser si elles n'étaient pas nulles : c'est ça qu'on appelle un corps, d'accord. Et il se fait si vous voulez que le corps des nombres rationnels, donc, il engendre ce problème de la fonction ζ, mais ce corps des nombres rationnels, les propriétés particulières qui font qu'il engendre le problème de la fonction ζ, on a réussi à les abstraire et c'est ce qu'on appelle un corps global.

Alors ça, c'est pour la première étape. Donc on a compris dans la première étape, si vous voulez, que le problème formulé par Riemann se généralise de manière très, très simple en partant non pas seulement du corps des rationnels, mais d'un corps global. Alors parmi les corps globaux, il y a des corps qui sont encore plus compliqués que les rationnels, par exemple lorsque vous regardez ce qu'on appelle les nombres algébriques, c'est à dire vous regardez par exemple $\mathbb{Q}(\sqrt{2})$, ou $\mathbb{Q}(i)$, etc. Et puis il y a des corps qui sont quand même relativement plus simples que le corps des rationnels, et c'est ce qu'on appelle les corps de fonctions sur une courbe. Alors, je vais vous expliquer ce que c'est. Et en fait, donc, si vous voulez, dans le troisième pas, donc ça, ce sera le deuxième pas, c'est arriver à spécialiser à un cas plus simple et le troisième pas, c'est qu'on verra que les idées qui marchent dans le cas plus simple, ce sont des idées géométriques, d'accord. Ce sont des idées géométriques essentielles. Alors quelles sont, donc, quand je parle de corps de fonctions, qu'est ce que ça veut dire ? Ça veut dire que vous prenez des fonctions donc comme $f(x)$ si vous voulez, mais des fonctions rationnelles et ces fonctions rationnelles au lieu d'avoir, si vous voulez, des coefficients qui sont des nombres ordinaires, elles ont des coefficients qui sont dans ce qu'on appelle un corps fini. Alors les premiers corps finis ont été découverts par Gauss et ils sont êmement simples à expliquer. Donc un corps fini, le plus simple que vous connaissez, c'est les entiers modulo 2, vous voyez, si vous regardez un entier modulo 2, vous pouvez les encore les additionner, vous pouvez encore les multiplier, et puis si un entier modulo 2 n'est pas nul, eh bien, c'est le nombre 1, donc il est inversible. Alors ça, c'est un corps. On a aussi le corps des entiers modulo p lorsque p est un nombre premier, mais en fait, il y a un seul article de Galois qui a été publié de son vivant, il a été publié dans le Bulletin de la société mathématique, donc de son vivant, il a publié un article et dans cet article, il a en fait classifié, si vous voulez, ce qu'on appelle les corps finis. C'est à dire qu'on connaît exactement la liste de tous les corps qui ont un nombre fini d'éléments alors ces corps qui en ont un nombre fini d'éléments, on pourrait croire naïvement que ce sont seulement les corps des entiers modulo un nombre premier p, ça n'est pas vrai, et par exemple typiquement, et vous avez des gens qui ne connaissent pas bien, si vous voulez, et lorsque vous allez leur dire vous regardez le corps F_4, ils vont croire que c'est les entiers modulo 4 et vous voyez, si vous prenez les entiers modulo 4, ce n'est pas un corps, pourquoi ? Parce que si vous prenez le nombre 2, il n'est pas nul et si vous prenez 2×2, ça fait 4 donc ça vaut 0. Et ce n'est pas un corps parce que dans un corps, ça, ça ne peut pas se produire : si vous prenez deux éléments non nuls, comme chacun d'entre eux est inversible, leur produit ne peut pas être nul, d'accord.

Donc, il y a un corps non trivial que Galois a trouvé bien sûr et qui est obtenu en rajoutant au corps à deux éléments, qui lui est on ne peut plus simple, la racine cubique de l'unité. Donc vous rajoutez un nombre j et ce nombre il vérifie $j^3 = 1$. En fait, il vérifie $1 + j + j^2$ est égal à 0. Donc vous écrivez les relations etc. et ce que démontre Galois, dans son article, il démontre deux choses ; d'abord il démontre, ça c'est remarquable, si vous voulez, que si vous prenez une équation polynomiale quelconque à coefficient dans un corps F_q, elle se résout dans un corps F_{q^n} ; c'est à dire que pour chaque puissance d'un nombre premier, il y a un seul corps à isomorphisme prés ; on ne sait pas encore les construire de manière canonique c'est ça qui est absolument incroyable, je veux dire, il y a encore un problème sur ces corps-là, c'est qu'on ne sait pas les donner de manière explicite, on sait les donner de manière artificielle. Mais il n'y en a qu'un seul qui a la bonne cardinalité. Et en plus, donc, ce que fait Galois, c'est... : ce que fait Galois, je ne vais pas l'expliquer, je vais expliquer en un mot plutôt ce que c'est que le groupe de Galois donc Galois, si vous voulez, avait

compris une théorie qu'il appelle la théorie de l'ambiguïté on y reviendra.

Et dans cette théorie, qui est la théorie de Galois, ce qu'il fait, c'est : il comprend que les nombres en général sont ambigus, c'est-à-dire que lorsqu'on définit un nombre, par exemple comme $\sqrt{2}$, d'accord, eh bien on crée une ambiguïté entre les deux possibilités, entre plus ou moins racine de 2[4], et Galois a compris, si vous voulez, que c'était la réduction de l'ambiguïté qui intervenait dans la résolution des équations de manière très naïve, et il a défini un groupe, qu'on appelle le groupe de Galois bon j'ai fait une conférence à la BNF au mois de juin, donc on pourrait passer une heure là-dessus, sur les écrits de Galois. Mais ce qui compte, si vous voulez, c'est que donc, il y a un groupe d'ambiguïté, chaque fois qu'on rajoute des nombres, et Galois a calculé le groupe d'ambiguïté du corps obtenu, en résolvant une équation sur le corps F_{q^n} et il a démontrait, en fait, que c'est un groupe, bien sûr, mais que c'est un groupe cyclique ; un groupe cyclique, si vous voulez, ça revient à avoir un seul générateur, qu'on va élever à des puissances, et en fait, il a donné le générateur, et c'est ce qu'on appelle maintenant le Frobenius ; en mathématiques, on donne à certains objets mathématiques le nom de certains mathématiciens ok, et ça s'appelle le Frobenius. Donc c'est l'élévation à la puissance, si vous voulez ce qui est très frappant, c'est que l'élévation à la puissance lorsqu'on travaille avec des nombres modulo p, eh bien, l'élévation à la puissance est additive, c'est à dire que la raison c'est la suivante : c'est que si vous prenez, par exemple, l'élévation à la puissance 2, dans le corps à deux éléments, là vous allez vous dire mais c'est pas possible, puisque quand j'élève au carré, c'est pas quelque chose tel que si j'élève $x + y$ au carré, ça va me donner $x^2 + y^2$. Mais vous savez quand même que $(x + y)^2 = x^2 + 2xy + y^2$ et 2 est égal à 0. Donc ça marche bien, d'accord, et c'est ça, si vous voulez, cet automorphisme de Frobenius. Alors donc, si vous voulez, les mathématiciens ont compris que c'étaient ces corps globaux qui étaient le cadre naturel pour penser à ce problème de Riemann et Weil, André Weil, en 1942, a résolu le cas plus simple de ce problème de Riemann. Donc ce qu'a fait Weil, si vous voulez, c'est que... Les gens savaient comment définir l'analogue de la fonction ζ de Riemann. Cet analogue, ça lui ressemble beaucoup, vous voyez, c'est un produit, et au lieu d'avoir ici les nombres premiers, comme on avait pour la fonction ζ de Riemann, petit k, ça signifie le corps global, qui est le corps de fonctions ; on a quelque chose d'autre (bon, je ne veux pas rentrer dans les détails techniques) mais la liste des nombres premiers est remplacée par ces nombres-là, et sinon la formule est la même, c'est-à-dire qu'on prend 1 moins le nombre premier à la puissance $-s$, et on prend l'inverse de ça, d'accord. Bon, alors, peu importe après, il y a des petits détails, d'accord, il y a des petits détails de définitions, on va revenir sur ce que ceci signifie géométriquement. Mais ce que ce qu'a compris André Weil, il a compris que la géométrie, que l'on connaît bien si vous voulez sur le corps des complexes pouvait se transposer en une géométrie, dans laquelle on pouvait plus beaucoup plus difficilement faire des dessins, mais qui n'était plus une géométrie sur le corps des complexes, mais une géométrie sur... Qu'est-ce que c'est que la barre qui est ici donc F_q, ce serait le corps fini à q éléments, qu'est ce que c'est que le $\overline{F}_q$, c'est ce qu'on appelle une clôture algébrique du corps F_q, c'est à dire ce qu'on fait si vous voulez c'est qu'on rajoute toutes les solutions d'équations possibles alors comme Galois l'avait montré, ça revient à prendre les corps F_{q^n}, on les ordonne, on obtient un corps qui est algébriquement clos, et ce corps qui est algébriquement clos, ce qui est remarquable dans le travail de Weil, si vous voulez, c'est qu'en fait, on peut transposer les idées géométriques à partir du corps des complexes, vers ce corps-là. Donc en fait, Weil si vous voulez, résout complètement le problème dans le cas de ce qu'on appelle un corps global de caractéristique

[4] $\pm\sqrt{2}$.

positive où la caractéristique est non nulle, il démontre qu'on a l'analogue exact de l'hypothèse de Riemann, qui fait que lorsqu'on écrit la fonction sous cette forme-là, bon il y a un polynôme qui apparaît, eh bien, ce que démontre Weil donc, c'est que ce polynôme, dont on sait qu'il a des zéros dans les nombres complexes, eh bien, les modules de ces zéros sont exactement là où ils doivent être, c'est à dire que le $q^{\frac{1}{2}}$ qui est ici, vous voyez, le $\frac{1}{2}$ qui est ici correspond, dans la bande verticale qu'on avait, à la partie réelle de s égale $\frac{1}{2}$. Alors au niveau géométrique, c'est très difficile de voir ce qui se passe, au niveau géométrique. Parce qu'au niveau géométrique, vous ne traitez presque toujours que de problèmes finis, donc en gros, si vous voulez les images que vous avez sont toujours des images finies, vous voyez donc l'image qui est ici c'est un nombre fini de points. Et en gros, si vous voulez, dans l'image mentale qu'il faut avoir, c'est que bien qu'on traite qu'un nombre fini de points, ici on a l'infinité des nombres de places, mais au-dessus de chaque place, on a un ensemble fini, qui est ce qu'on appelle l'orbite du Frobenius. Eh bien ce qu'il faut comprendre, c'est que des idées géométriques peuvent se transplanter à partir du cas complexe vers ce cas-là. Alors, vous voyez qu'on est déjà dans une situation plus compliquée que celle que j'avais donnée oùil y avait seulement ces trois étapes parce que, qu'a fait Weil, pour résoudre le cas plus simple, il a emprunté à une autre partie des mathématiques qui est la géométrie complexe, il a transplanté les idées de la géométrie complexe dans le cas des corps finis, et il a vu que ça marchait.

Donc maintenant, comment les choses ont-elles évolué au XXe siècle. De manière très bizarre, si vous voulez, on pourrait dire "bon eh bien maintenant, on a résolu le cas plus simple, revenons au problème initial et essayons de résoudre le problème initial". Et ce n'est pas ça qui s'est produit. Ce n'est pas ça qui s'est produit. Ce qui s'est produit, c'est que Weil a compris, si vous voulez, que tout le travail qu'il avait fait, comme c'était un travail qui portait sur des courbes sur un corps fini, et que la notion de courbe si vous voulez, c'est la notion de variété disons de dimension 1, c'est une notion particulière parce qu'il y a des variétés de dimensions arbitraires et bien Weil a formulé des conjectures. En fait, il a été aidé par la lecture de Gauss pour formuler ces conjectures. Il a formulé des conjectures, et ces conjectures, si vous voulez, elles consistaient non pas à revenir au problème initial, qui était le problème de Riemann, mais elles consistaient à passer du cas des courbes au cas des variétés. Alors ces conjectures ont occupé les mathématiciens pendant des années et des années et en fait ont été résolues donc par Deligne. Donc et le théorème est le suivant : je ne vais pas vous donner le détail de l'énoncé du théorème, peu importe, vous le voyez comme ça, il faut le voir de manière un peu surréaliste, ce qui compte, si vous voulez, c'est que ce qui marchait dans le cas des courbes continue à marcher dans le cas des variétés de dimension arbitraire. Donc c'est ça qu'il faut retenir, donc, si vous voulez, ce qui se produit, bon les notions sont plus difficiles à définir. Tout ça, on pourrait le définir de manière relativement simple en disant que ce que l'on fait, donc, c'est qu'on prend la courbe en question, et on compte le nombre de points de cette courbe lorsqu'on travaille avec le corps de base F_q etc. avec des extensions successives et on regarde comment ce nombre de points change avec n si vous voulez, l'exposant n.

Bon alors, ce qui est merveilleux, c'est que ce sont uniquement des notions géométriques, des notions de cohomologie, ce qu'on appelle la cohomologie étale, ℓ-adique, qui a été introduite par Grotendieck qui joue leur rôle et en fait, de manière assez remarquable si vous voulez, la démonstration de Deligne est complètement différente, elle est complètement orthogonale à la démonstration de Weil. La démonstration de Weil est encore une démonstration qui est assez proche de la géométrie ordinaire, et qui en gros, si vous voulez, ne fait jouer aucun rôle à la torsion alors que la démonstration de

Deligne est complètement différente.

Donc, alors, on en est donc au cran suivant si vous voulez, c'est-à-dire que je ne sais pas, je n'ai malheureusement pas fait un dessin de ça, j'aurais dû le faire, vous voyez, donc, il y avait ce cas formulé par Riemann. Ensuite il y a un cas particulier, qui a été résolu par Weil. Ce cas particulier l'a conduit à formuler des conjectures générales sur des variétés dimension quelconque, ok, donc vous voyez, on a déjà trois étapes, et quelle est la quatrième étape, eh bien la quatrième étape, c'est qu'en fait, cela a conduit à définir la fonction ζ, maintenant, pour des variétés sur le corps des rationnels, c'est-à-dire que si vous voulez, maintenant, et le cas de Riemann vient du cas où la variété, c'est un seul point, donc c'est vous dire à quel point ça a progressé depuis le problème de Riemann.

Donc on prend une variété sur $\mathbb{Q}$, si vous voulez, on prend un certain nombre d'équations qui sont définies à coefficients rationnels, ou à coefficients entiers, d'accord. Eh bien, lorsqu'on prend une variété sur $\mathbb{Q}$, il y a une merveilleuse définition, dont je ne veux pas non plus rentrer dans les détails, mais qui utilise le théorème de Lie et qui dit que, en général, si on prend une variété sur $\mathbb{Q}$, on peut la réduire modulo un nombre premier. Ce n'est pas toujours vrai. À ce moment-là, on dit qu'elle a une bonne réduction modulo p. Et lorsqu'elle a une bonne réduction modulo p, on obtient une variété sur le corps fini F_p, à p éléments. Et à ce moment-là, on a un polynôme qui lui est associé, de manière vraiment indirecte, hein, parce que ce polynôme, il est associé par le théorème de Deligne, à partir des conjectures de Weil.

Et qu'est-ce qu'on fait ? Eh bien, on prend ce polynôme en p^{-s}, on prend l'inverse de ces polynômes, on prend leur produit infini sur tous les p qui sont possibles, et on obtient une fonction ζ. Cette fonction ζ est encore incomplète. Elle est encore incomplète parce qu'on n'a pas rajouté les facteurs archimédiens, ni les facteurs à ce qu'on appelle les places qui sont ramifiées, d'accord.

Mais ça a été fait. Donc on sait définir une fonction ζ. Ce qui est remarquable dans cette définition, c'est qu'on s'aperçoit, si vous voulez, que cette définition doit être focalisée sur un entier m. C'est-à-dire que ce n'est pas vraiment la variété qui est intéressante, mais c'est sa partie qui est sa cohomologie de dimension m qui est intéressante.

Et on ne pourrait pas formuler de conjectures qui soient l'analogue de la conjecture de Riemann si on partait de l'ensemble de tous les m. C'est-à-dire que dans le cas précédent, dans le cas des corps finis, la fonction ζ d'André Weil, c'était un produit avec des exposants ± 1. C'est-à-dire que c'était comme une fraction rationnelle. Mais ce qui est évident, si vous voulez, si on regarde ce produit-là, c'est que dans le cas des variétés sur $\mathbb{Q}$, en général, les dénominateurs vont avoir une infinité de 0. Donc la fonction ne serait pas une fonction intéressante. En fait, on est obligé de se focaliser sur m donné.

Et en grande partie, il y a bien d'autres raisons à ça, si vous voulez. En fait, l'idée, une idée merveilleuse de Grothendieck, qui est l'idée des motifs, qui est en fait une généralisation de la théorie de Galois à la dimension plus grande, je n'ai pas le temps de rentrer dans les explications des causes, eh bien, c'est une théorie, si vous voulez, qui justement donne une existence pure à la partie d'une variété qui correspond à la cohomologie de dimension m, à partir d'opérations, si vous

voulez, etc. Donc en fait, c'est ça qui s'est dégagé. Et alors, c'est assez effrayant, parce que si vous regardez le point de départ qu'on avait, donc le point de départ qu'on avait, c'était la conjecture de Riemann, quelque part.

Ensuite, on l'avait généralisé. Il y a un cas particulier de cette conjecture, donc généralisée, qui a été résolu par Weil. Ensuite, Weil l'a étendue à des variétés de dimensions plus grandes, sur les corps finis toujours.

Et enfin, donc, par, si vous voulez, par transposition, à partir du cas des corps finis jusqu'au cas du corps des rationnels, cette idée de fonction ζ a été étendue aux variétés algébriques. Donc maintenant, on se retrouve dans la situation suivante où au lieu d'avoir résolu le problème de départ, on se trouve devant un problème d'une portée, d'une ampleur considérable par rapport au problème que formulait Riemann. Mais on n'a pas encore de retombée directement sur le problème de Riemann.

Par contre, alors, il y a une retombée qui a été merveilleuse, qui est à travers le programme de Langlands, c'est-à-dire qu'à peu près à la même époque, les gens ont compris qu'en fait, la seule manière, enfin, une des manières qui était possible, en fait, c'est en grande partie grâce à Weil aussi, une manière de comprendre les propriétés de ces nouvelles fonctions ζ qui viennent des variétés algébriques, c'était de les relier à d'autres fonctions ζ qui avaient été découvertes par Hecke, dans la théorie de ce qu'on appelle les formes modulaires. Donc, quel était le produit de ça ? Le produit de ça, si vous voulez, c'est qu'il y a eu d'une part un pont entre une théorie qui était purement algébrique, et ce qu'on appelle la théorie automorphe, qui est la théorie des représentations de groupes adéliques, etc. Mais surtout, le point essentiel, c'est qu'en fait, un cas particulier de cette correspondance de Langlands, si vous voulez, entre le côté algébrique et le côté automorphe, a été démontré par Wiles, et en démontrant cela, en fait, ce qu'il a fait, c'est qu'il a montré qu'une courbe, une courbe elliptique qui est définie sur $\mathbb{Q}$, en fait, est modulaire.

Alors, qu'est-ce que ça veut dire, modulaire ? Ça veut dire que, justement, exactement comme on peut paramétrer le cercle par des fonctions cosinus et sinus, qui sont des fonctions transcendantes, eh bien, en fait, on va pouvoir paramétrer cette courbe par des formes modulaires, par des fonctions transcendantes, qui sont des fonctions modulaires. Alors, il y a une manière très précise de le dire, mais je ne vais pas rentrer dedans. Simplement, on sait bien qu'il y a une conséquence merveilleuse de ce résultat de Wiles, c'est que grâce aux travaux de Frey, Serre et Ribet, eh bien, on savait que s'il y avait une solution du problème de Fermat, s'il y avait une solution non-triviale, c'est-à-dire s'il y avait un triplet d'entiers qui vérifiait $a^n + b^n = c^n$, eh bien, on savait lui associer ce qu'on appelle une courbe elliptique, donc ça rentre exactement dans le cadre, qui était définie sur $\mathbb{Q}$. Et puis, on voit bien pourquoi on prend les nombres comme ça, parce que les trois racines, ce sera 0, a^n et $-b^n$. Et à ce moment-là, lorsqu'on regardera le produit des différences des racines, on voit bien qu'il va y avoir quelque chose de très intéressant qui va se produire.

Donc, ce qu'avaient démontré ces gens-là, en particulier, c'est qu'il était impossible qu'il existe une solution de Fermat, à condition qu'on sache que toute courbe elliptique sur $\mathbb{Q}$ est modulaire. D'accord ? Et ça contredisait ça. Donc, vous voyez la démarche qui s'est produite.

La démarche qui s'est produite fait qu'on n'a pas résolu le problème initial. On n'a pas résolu le problème initial. On a bon espoir qu'il soit vrai, bien sûr, puisqu'on en a résolu un cas particulier qui est vrai.

On en a dévoilé, de manière absolument incontournable, la nature géométrique, c'est-à-dire que toutes les choses qui ont marché, étaient des choses qui étaient inspirées par la géométrie. D'accord ? Ce n'était pas du tout une géométrie simple. C'est la géométrie qui venait de la transposition de la géométrie sur le corps des complexes en une géométrie sur les corps finis et, bon, sur la clôture algébrique d'un corps fini.

D'accord ? Donc, ensuite, le problème a été étendu. Il a été étendu. On a simplement généralisé cette idée de fonction ζ.

On ne sait même pas si ces fonctions ζ ont une équation fonctionnelle. Enfin, on sait conjecturer leur équation fonctionnelle, mais on ne sait même pas démontrer l'équation fonctionnelle. Donc, c'est vous dire le niveau d'ignorance dans lequel on est, mais d'un autre côté, on sait que le paysage qu'on va découvrir est un paysage absolument merveilleux, puisqu'en en dévoilant une toute petite partie, qui est le cas des courbes elliptiques définies sur $\mathbb{Q}$, etc., eh bien, déjà, ça a permis de résoudre le problème de Fermat.

Donc, j'espère vous avoir montré, dans ce cas-là, dans le cas des nombres premiers, à quel point, justement, le parcours du mathématicien est un parcours qui est absolument imprévisible. On aurait pu dire, le mathématicien doit partir de la généralisation, démontrer le cas particulier, etc., puis après, on doit le forcer à utiliser la démonstration qu'il a faite pour le cas particulier pour résoudre le cas initial. Mais, bien sûr, ce serait une erreur.

Le parcours du mathématicien est un parcours qui est imprévisible. Et, bien sûr, on aurait bien tort de vouloir programmer une direction de recherche, ou quoi que ce soit. Alors, il y a une image, ici, que j'ai mise volontairement, qui est reliée aux formes modulaires.

Donc, cette image, en fait, elle est due à Klein. Mais la raison pour laquelle je l'ai mise, c'est que cette image, si on veut la comprendre, en fait, ce que vous voyez tracé ici, c'est un polygone dans une géométrie qui est la géométrie de Poincaré, qui est la géométrie non-euclidienne. Et, avant de passer à l'espace-temps, donc, je voudrais simplement mentionner cette géométrie non-euclidienne.

Donc, ça, on va faire un petit break, si vous voulez. Donc, la géométrie non-euclidienne, c'est un exemple formidable qui montre, si vous voulez, à quel point, justement, des réflexions a priori complètement abstraites de mathématiciens peuvent avoir des retombées fondamentales. La réflexion abstraite, c'était, si vous voulez, bon, comme vous le savez tous, l'axiome de l'unique parallèle passant par un point extérieur à une droite dans les axiomes d'Euclide.

Alors, en fait, beaucoup de mathématiciens y ont réfléchi, Legendre, etc. Ils ont démontré 36 équivalences entre, par exemple, la seule existence d'un triangle dont la somme des angles valait π suffisait à démontrer cet axiome, etc.

Et, en fait, donc, au XIXe siècle, on s'est aperçu qu'on pouvait construire des modèles de géométrie qui vérifiaient tous les axiomes d'Euclide, sauf celui-là, d'accord ? Alors, c'est ce qu'on appelle la géométrie non-euclidienne. Et le modèle que j'ai tracé ici, c'est ce qu'on appelle le modèle de Klein. C'est un modèle qui est particulièrement simple.

Ce que vous prenez, c'est vous limitez les points de la géométrie aux points qui sont à l'intérieur de l'ellipse, qui est décrite ici. Et vous décrétez que les points, donc, de l'espace, ce sont seulement les points qui sont à l'intérieur de l'ellipse. Vous décrétez que les droites de la géométrie, ce sont les portions de droites ordinaires qui contiennent les points intérieurs à l'ellipse.

Bon, alors, il faut aller un petit peu plus loin parce qu'il faut définir ce qu'on appelle la congruence des segments. Je ne vais pas vous expliquer ça, mais c'est très simple. Ça se fait en fonction du birapport des quatre points qui sont ici.

Mais en tous les cas, ce que vous pouvez vérifier à l'œil nu, c'est que si vous prenez une droite comme la droite D qui est ici, et si vous prenez un point qui est extérieur à cette droite comme le point I qui est ici, eh bien, il y a plusieurs droites qui passent par le point I et qui ne rencontrent pas la droite D. Donc, vous voyez bien que l'axiome de l'unique parallèle passant par un point extérieur à droite est violet, d'accord ? Par contre, tous les autres axiomes de la géométrie euclidienne sont vrais. Alors, après cette découverte de la géométrie non euclidienne, les mathématiciens se sont mis à réfléchir dans deux directions différentes. Il y a une direction qui venait en fait de Galois et qui a été la mieux poursuivie, si vous voulez, par Sofusli, et une autre direction qui vient, si vous voulez, beaucoup plus dans la direction de Gauss et de Jacobi.

Et c'est cette direction-là qui a eu un impact direct sur la physique. Alors, dans cette direction-là, ce qui se produit, c'est qu'on dit simplement que la géométrie est donnée en définissant le mètre, si vous voulez, c'est-à-dire en définissant un petit élément de longueur. Et ce petit élément de longueur, on peut le transporter partout.

Et quand on le transporte partout, on peut l'écrire en coordonnées locales, comme ça, et ça donne ce qu'on appelle les $g_{\mu\nu}$. Et alors, ce qui est important, c'est qu'on peut transplanter, c'est toujours pareil, si vous voulez, on peut transplanter des idées fondamentales de la géométrie ordinaire, comme l'idée de droite, dans ces géométries beaucoup plus générales. Et l'idée fondamentale qui joue un rôle le plus important, si vous voulez, dans la géométrie ordinaire, c'est l'idée de géodésique, ou l'idée de droite.

Cette idée de droite se traduit par une équation. Ce que signifient les indices ici, c'est la dérivée par rapport à $x\rho$, d'accord ? Donc ici, la dérivée par rapport à $x\nu$. Donc ce qu'on fait, c'est qu'on dérive, si vous voulez, ces $g_{\mu\nu}$, et puis on écrit une équation, qui est une équation où on écrit que la dérivée seconde est déterminée par une forme quadratique en fonction des dérivées premières.

C'est ce qui gouverne, si vous voulez, les droites, ce qui gouverne le mouvement géodésique. Alors, donc, j'en viens à l'espace-temps. Alors, j'espère qu'on va... Bon, on va prendre les choses de manière plus relaxe.

Alors, l'espace-temps, si vous voulez, je vais essayer d'abord de vous résumer, de vous résumer de manière très, très simple, la plus simple possible. Quel est, pour le mathématicien, ce que l'on sait sur l'espace-temps ? D'accord ? Je vais faire un transparent là-dessus. Alors, qu'est-ce que l'on sait, pour le mathématicien, sur l'espace-temps ? Bon.

Alors, on sait que, si vous voulez, l'espace-temps... D'abord, le mathématicien, il sait qu'il faut mentionner Poincaré. C'est très important. Alors, donc, on sait que l'espace-temps est gouverné par cette métrique, d'accord ? C'est l'espace de Minkowski.

On l'appelle l'espace de Minkowski. Et on sait que, dans l'espace courbe, eh bien, il y a ce qu'on appelle un potentiel gravitationnel qui va remplacer le potentiel newtonien, c'est-à-dire l'idée du potentiel newtonien qui gouverne, si vous voulez, le mouvement des corps, est remplacée par un potentiel qui est plus, beaucoup plus... Si vous voulez, qui a beaucoup plus d'indices, ce sont les $g_{\mu\nu}$, et qui donne l'élément de longueur. Alors, il y a un principe d'action qui remplace la loi de Poisson.

La loi de Poisson vous disait que le Laplacien du potentiel newtonien donnait la distribution de masse. Eh bien, Einstein a eu beaucoup de mal à trouver ce qui remplaçait ça. En fait, c'est gouverné par un principe d'action.

Et ce principe d'action, il est donné par ce qu'on appelle la courbure scalaire. Donc, il y a un invariant, si vous voulez, de la métrique, qui est donné par ce qu'on appelle la courbure scalaire, qu'on intègre. C'est ce qu'on appelle l'action d'Einstein-Hilbert.

Bon, là, il y a la constante gravitationnelle. Et qu'est-ce qu'on sait ? En gros, si vous voulez, pour résumer la physique que l'on comprend, eh bien, elle vous dit que l'action, qui va jouer un rôle après, eh bien, c'est la somme de deux termes. Elle a un terme qui vient purement de la métrique, c'est-à-dire qui vient du potentiel gravitationnel.

Et elle a un autre terme que je vais vous montrer tout à l'heure. Mais si je vous le montrais tout de suite, vous seriez effrayés. C'est ce qu'on appelle le modèle standard.

D'accord ? OK. Donc, on a cette combinaison des deux choses. Et enfin, si vous voulez, on a une recette qui est due à Feynman.

Donc, si vous voulez, là, vous avez un résumé. Et on a une recette qui est due à Feynman. Et que vous dit cette recette ? Eh bien, elle vous dit que si vous voulez passer au quantique, en fait, c'est incroyablement simple de passer au quantique.

Vous gardez vos champs classiques. Vous pensez tout en termes de champs. Il y a le champ gravitationnel, etc. D'accord ? Donc, vous pensez tout en termes de champs. Ce que vous dit Feynman, c'est qu'il n'y a plus de probabilités, mais il y a des choses qui sont plus fines que les probabilités, qui sont des espèces de racines carrées de probabilités et qui sont des nombres complexes. C'est ce qu'on appelle des amplitudes de probabilités.

Et ce sont ces choses-là qu'il faut rajouter, et non pas les probabilités. Et que vous dit Feynman ?

Eh bien, Feynman vous donne une recette pour savoir ce que c'est que l'amplitude de probabilités d'une configuration classique. Donc, vous prenez un champ classique.

Vous imaginez, je ne sais pas, la surface de la mer ou un truc comme ça. D'accord ? C'est un champ classique. Eh bien, ce champ classique, il a une action classique que vous calculez.

Vous la divisez par l'unité d'action, qui est ce qu'on appelle la constante de Planck. C'est le seul rôle du quantique qui intervient ici. Vous la multipliez par le nombre imaginaire pur, i, de carré moins 1 ($i^2 = -1$). D'accord ? Et vous prenez l'exponentielle de ça.

Donc, c'est ça la recette. Alors, c'est là que j'espère que la couleur va marcher, parce que j'avais quand même donné deux, trois transparents en couleur. D'accord ? Donc, qu'est-ce qu'on sait ? Je ne vais pas empiéter sur les plates-bandes des physiciens, mais c'est quand même extrêmement rassurant de savoir que la théorie d'Einstein, qui prédit l'existence de phénomènes tout à fait bizarres, si vous voulez, dans l'espace-temps au niveau macroscopique, comme l'existence des trous noirs, etc., eh bien, maintenant, est en grande partie vérifiée, bien qu'il y ait des problèmes extrêmement sérieux, ce qu'on appelle la matière noire, l'énergie noire, etc., qu'on ne sait pas encore vraiment expliquer.

Mais en tout cas, je veux dire, il y a des phénomènes macroscopiques, et puis il y a des vérifications merveilleuses de la théorie d'Einstein pour ce qu'on appelle les pulsars binaires, etc. Donc, ça, c'est un exemple d'une galaxie très lointaine dans laquelle on arrive à mesurer la vitesse de déplacement de gaz, etc., et on arrive à deviner, si vous voulez, la présence d'un trou noir. Évidemment, la présence d'un trou noir, un trou noir, à part ce qu'on appelle la radiation de Hawking, n'émet rien de spécial.

Donc, je veux dire, on n'arrive pas à l'observer directement. Alors, ça, c'est dans l'infiniment grand, si vous voulez, c'est dans les très, très grandes tailles. Alors, dans les tailles très, très petites, ce qui est satisfaisant, c'est que l'on saura bientôt, l'on saura bientôt... Ah, pardon.

Mais alors là, vous avez une image macroscopique, si vous voulez, du CERN, qui rentrera en fonctionnement sans doute à la fin de l'année 2007 et qui a un certain nombre de détecteurs, d'accord, que les gens construisent. Il y a un nombre incalculable d'ingénieurs qui construisent ça. Et en gros, si vous voulez, ce qui se passe ici, c'est le plus gros microscope, c'est le microscope le plus précis que l'on ait pour analyser la texture de l'espace-temps au niveau microscopique.

C'est-à-dire qu'en gros, si vous voulez, ce qui se produit, c'est ce qu'on appelle les énergies qui sont impliquées dans ces très grands accélérateurs. Là, ce sera de l'ordre du TeV ou d'une dizaine de TeV ou je ne sais pas, peut-être une centaine de TeV. En fait, elles correspondent, si on prend l'inverse de l'énergie, si on utilise les constantes usuelles pour faire le travail, ça correspond à des limites de la précision, si vous voulez, dans l'infiniment petit, donc de l'ordre, là, on aura quelque chose de l'ordre, je pense, de 10 puissance moins 18 centimètres, quelque chose comme ça. Bon. Alors maintenant, ce que je vais faire, si vous voulez, bon, ça, c'est bien gentil, etc.

Le problème, c'est que je vous ai dit tout à l'heure que les principes de la physique étaient très

très simples et je vous ai montré tout à l'heure un autre terme, d'accord, dans ce qu'on appelle le Lagrangien de la physique ou l'action de la physique, c'est-à-dire, il y avait le Lagrangien de Einstein-Hilbert, et il y avait le Lagrangien du modèle standard. Alors, les mauvaises nouvelles, c'est que si vous écrivez la formule, vous avez des gens qui ne peuvent pas vous dire que c'est simple, voilà la formule, d'accord. Donc, je ne vais pas vous faire le détail, mais vous pouvez toujours poser des questions sur la formule, d'accord.

Donc, voilà, si on écrit vraiment le Lagrangien du modèle standard, ça, c'est ce qu'on appelle, il y a les fantômes ici, etc. Il y a tous les termes du modèle standard. Donc, en fait, si vous voulez, le dialogue qui a eu lieu entre l'expérience en physique, d'accord, et la théorie, ce dialogue, au cours du XXe siècle, a produit ce terme additionnel, au-delà du terme d'Einstein-Hilbert, il a produit ce terme additionnel.

Et, bon, bien que ce terme additionnel, on puisse lui donner un tas de qualificatifs, on puisse dire, si vous voulez, là, vous avez les bosons de jauge, vous avez les gluons, etc. Là, vous avez le, bon, là, vous avez le, ce qu'on appelle le boson massif W, etc. Vous avez le boson intermédiaire Z, d'accord.

Là, vous avez le champ électromagnétique, etc. On peut dire, là, vous avez les champs de Higgs qui sont non physiques, vous avez le champ physique des Higgs, H, qui intervient, etc. Bon, tous les termes ont une signification, tous les termes ont une origine historique, si vous voulez, etc.

Mais, c'est quelque chose de fascinant pour le mathématicien. Pourquoi est-ce que c'est quelque chose de fascinant pour le mathématicien ? Parce que, si vous voulez, le mathématicien, lui, ce qu'il cherche, c'est la simplicité. Et, le fait qu'on dise, le lagrangien résume toute la physique que l'on sait, bien sûr, ça, ça parlera aux physiciens, parce que le physicien, il saura que chacun de ces termes-là a une histoire, etc. et va prédire quantité et quantité de phénomènes. Mais le mathématicien ne peut pas rester insensible à la complexité de cette formule. D'accord ? Alors, il y a une autre chose qui n'est pas évidente non plus, si vous voulez.

Il y a une autre chose qui n'est pas évidente non plus. C'est que, lorsque les physiciens ont fait leurs calculs et ont commencé à utiliser cette prescription de Feynman, lorsqu'ils ont utilisé cette prescription de Feynman, eh bien, ils se sont aperçus qu'il y avait un autre problème qui se produisait, c'est-à-dire qu'ils écrivaient l'action avec les champs classiques, etc., le champ qu'on a vu tout à l'heure, d'accord ? Et ils essayaient d'intégrer, bon, sur tous les champs avec ce qu'on appelle cette amplitude de probabilité. Ils ont commencé à faire les calculs et ils se sont aperçus, c'est Oppenheimer qui s'en est aperçu, en fait, dans les années 1930, en gros.

Eh bien, ils se sont aperçus qu'il y avait un phénomène, un phénomène vraiment très, très bizarre qui se produisait. Et pour vous expliquer ce phénomène, ce qu'on appelle la renormalisation, en fait, si vous voulez, c'est un phénomène qui avait déjà été observé par les physiciens vers 1830, donc au XIXe siècle. Et il avait été observé par Green, si vous voulez, qui faisait de l'hydrodynamique.

Donc, ce que les physiciens avaient observé, c'est la chose suivante, les mathématiciens aussi. En fait, à l'époque, ils n'étaient pas différents, c'était les mêmes personnes qui faisaient la physique et les mathématiques. Donc, en hydrodynamique, Green avait fait l'observation suivante.

C'est la suivante, si vous voulez, c'est que si vous prenez une balle de ping-pong et vous prenez un bain, avec une balle de ping-pong, d'accord, et vous mettez la balle de ping-pong sous l'eau, donc c'est le cas, là, vous voyez, d'accord. Et on vous demande de faire un calcul qui est le calcul de l'accélération initiale qu'aura la balle de ping-pong quand vous la lâchez. Alors, vous êtes dans le bain, donc vous vous dites, vous appliquez le principe d'Archimède.

Alors, que vous dit le principe d'Archimède ? Il vous dit que la balle de ping-pong va être soumise à une force verticale qui correspondra au poids de l'eau que contient la balle. D'accord, vous calculez le poids de l'eau que contient la balle. Bon.

Ensuite, vous calculez, vous appliquez la loi de Newton, ok, et qu'est-ce que vous trouvez ? C'est un petit calcul très simple. Vous trouvez 11,5 fois l'accélération de la pesanteur. Je ne sais pas si vous vous rendez compte, mais 11,5 fois l'accélération de la pesanteur, c'est quelque chose de colossal.

Pratiquement, c'est une accélération à laquelle le corps humain ne résiste pas, d'accord. Alors, maintenant, vous prenez la balle de ping-pong, vous la lâchez dans l'eau. Et qu'est-ce que vous regardez ? Elle va vraiment lentement.

D'accord. Et en gros, son accélération initiale est de l'ordre de 1,5 g. Alors, c'est Green qui a trouvé l'explication à ça. Et quelle est l'explication ? Eh bien, l'explication, c'est que, même lorsque le temps t est égal à zéro, si vous voulez, lorsque la balle est immergée dans l'eau, vous voyez bien que quand elle va bouger dans l'eau avec une certaine vitesse, peu importe, eh bien, l'eau va devoir se dérouler de manière tangentielle le long des bords de la balle de ping-pong.

Et donc, si vous regardez le champ des vecteurs, si vous voulez, de l'eau, c'est un champ de vecteurs qui va être dérangé par la présence de la balle. On peut calculer. C'est un calcul élémentaire, l'énergie cinétique correspondante, c'est ce qu'a fait Green. C'est un calcul complètement élémentaire. Ça prend trois lignes de calcul. D'accord. Ça utilise ce qu'on appelle une harmonique sphérique. Donc, Green a fait le calcul.

Et qu'est-ce qu'il a compris ? Eh bien, il a compris quelque chose qui est assez fabuleux, si vous voulez. C'est qu'en fait, la loi de Newton doit être modifiée. C'est quelque chose qui est tout à fait étonnant.

C'est que, lorsqu'on prend un corps comme une balle de ping-pong, etc., qui est plongé dans un liquide et qui est plongé dans un champ, eh bien, la loi de Newton n'a plus lieu avec ce qu'on appelle la masse nue du corps comme la balle de ping-pong. Donc, la balle de ping-pong, vous pouvez la prendre, vous pouvez la poser sur une balance et vous connaîtrez sa masse, m. D'accord. Eh bien, ce que vous dit le théorème de Green en hydronamique, c'est qu'en fait, ce n'est pas cette masse-là qui rentre dans la formule de Newton.

C'est une autre masse. Il l'a calculée pour un objet parfaitement sphérique et il s'est aperçu qu'en fait, c'était cette petite masse-là m plus la moitié de la masse de l'eau qui serait contenue dans la

balle $\left(m + \frac{1}{2}M\right)$. D'accord.

C'est un calcul qui est complètement élémentaire. Et alors, vous voyez bien que si vous remplacez la masse m par m plus $\frac{1}{2}$ de la masse de l'eau qui est bien plus grande que la masse de la balle de ping-pong, eh bien, à ce moment-là, quand vous calculerez l'accélération initiale, elle ne sera jamais de toute façon plus grande que deux fois l'accélération de la pesanteur. Elle ne peut pas puisqu'il y a ce facteur $\frac{1}{2}$. Donc ça, c'est un phénomène ancien que les gens avaient compris. Alors, j'avais insisté pour avoir la couleur, je vais voir si vous voyez un petit peu mieux là. D'accord. Donc, je veux dire, ça, ce n'est pas n'importe quel... Je n'ai pas pris n'importe quel champ de vecteur.

C'est le champ de vecteur réel, ça, qui correspond exactement au flot de l'eau qui se déroule autour de la balle de ping-pong. Donc, en fait, si vous voulez, ce que les physiciens ont trouvé, donc à partir des travaux d'Oppenheimer, donc, ce qu'ils ont trouvé, si vous voulez, à partir de ces travaux-là... J'ai l'impression que je vais... Non, ça va. Donc, à partir des travaux d'Oppenheimer, ce qu'ont trouvé les physiciens, c'est qu'ils ont trouvé, en fait, si vous voulez, que le phénomène était exactement le même lorsqu'on regardait un électron, par exemple.

Lorsqu'on regardait un électron, il y avait, en fait, l'électron est plongé dans le champ électromagnétique et exactement le même phénomène qui se produit pour la balle de ping-pong se produit pour l'électron. C'est-à-dire que... Et maintenant, il y a une grosse différence. C'est que dans le cas de la balle de ping-pong, vous pouviez prendre la balle de ping-pong et la sortir de l'eau et la peser.

Par contre, l'électron, quoi que vous fassiez, il sera toujours dans le champ électromagnétique. Donc, si vous voulez, pour l'électron, il est absolument impossible de connaître la valeur m qui était importante de tout à l'heure, qui jouait un rôle important si vous voulez, dans le changement de tout à l'heure. Donc, si vous voulez, dans le cas de la balle de ping-pong, on avait le petit m et on avait, si vous voulez, ce changement qui passait de petit m à $m + \frac{1}{2}\,M$. Dans le cas de la balle de ping-pong, on pouvait mesurer m et on pouvait mesurer ça aussi.

Dans le cas de l'électron, on ne peut pas mesurer m, on peut seulement mesurer cette combinaison des deux. Alors, ça a pris un temps très très long quand même, aux physiciens, puisqu'Oppenheimer a trouvé ça environ en 1930, et ce n'est pas avant 1947, en particulier pour des raisons qui venaient de l'expérience, sur ce que l'on appelle la structure hyperfine, ou la structure fine même des spectres que, bon, je n'ai pas parlé de Bethe, etc., mais je veux dire un certain nombre de physiciens ont compris ce qui se passait. Et donc, là, il y a eu un développement qui s'est de plus en plus, d'une certaine manière, rapproché, on peut dire, de choses absolument essentielles, c'est-à-dire ce qu'ont fait les physiciens, ils ont commencé par faire des petits tours de passe-passe, c'est-à-dire qu'ils ont commencé par dire, bon, on ne peut pas observer la masse de l'électron, on ne peut pas observer sa charge, etc., et on va essayer de faire des calculs, en fermant un peu les yeux, là où il y a des problèmes, d'accord ? Et en essayant seulement de calculer des quantités physiquement observables. Mais grâce à Schwinger, Feynman et Dyson, etc., en fait, je ne veux pas rentrer dans les détails, bien sûr, mais ils ont graduellement développé une méthode algorithmique, si vous voulez, une méthode à partir de ce qu'on appelle les graphes de Feynman, ça c'est un exemple très

simple de graphes de Feynman, donc, ils ont développé une méthode, pour se débarrasser des infinis.

Mais en gros, si vous voulez, ce qu'il se passe, c'est qu'on fait ce qu'on appelle un développement perturbatif, c'est une somme infinie, mais chacun des termes du développement est donné lui-même par une intégrale divergente. Donc c'est vraiment un problème très très sérieux, ce n'est pas le problème qui est qu'on a une somme infinie de choses qui elles-mêmes sont finies. Le problème, c'est qu'on a une somme infinie de choses qui sont chacune infinie.

Alors, les physiciens ont développé une méthode, et cette méthode, si vous voulez, a mis beaucoup de temps à se développer de manière, on peut dire rigoureuse, au sens où elle soit définie de manière univoque, et au sens où, pour l'appliquer, il ne faille pas aller voir X et Y et lui demander "est-ce que ce que je fais c'est correct,là ou est-ce que ce n'est pas correct ?" D'accord ? Donc ça, ça a pris énormément de temps, ça a pris beaucoup de temps et ça a été développé en particulier par Bogoliubov, Parasiuk, Hepp et Zimmermann. Vous n'avez pas à comprendre les formules qui sont ici. Je veux dire, simplement, c'est pour vous montrer qu'il y a une méthode qui a été développée, et cette méthode, elle a été développée comme une méthode algorithmique. C'est-à-dire qu'on a donné une recette. En fait, il y avait, le travail de Bogoliubov et Parasiuk qui était incomplet. Hepp a introduit un tas de corrections, etc. Il a rendu les choses beaucoup plus rigoureuses et bon, Zimmermann a rajouté des formules combinatoires. Donc, en fait, on est arrivé graduellement, si vous voulez, à une recette. On peut dire c'est une recette qui permet de faire un calcul à partir de graphes.

D'accord ? Et on sait, bien sûr, que c'est quelque chose d'extrêmement intéressant parce que c'est précisément en faisant ces calculs de graphes que les physiciens trouvent un accord, par exemple, pour le moment anormal de l'électron, avec une précision qui est la même que l'épaisseur d'un cheveu sur la distance entre Paris et New York. Donc, on calcule le résultat à partir de ce type de formule. On calcule, donc, le moment anormal.

On le compare à l'expérience et on s'aperçoit, si vous voulez, que l'accord qu'il y a entre la théorie et l'expérience est de l'ordre de la précision de l'épaisseur d'un cheveu sur la distance entre Paris et New York. Alors, cette méthode, il faut le dire, si vous voulez, elle est parfaitement justifiée du point de vue de la physique. D'accord ? Le problème n'est pas là.

Mais pour le mathématicien, c'est quelque chose de fascinant, parce que le mathématicien, qu'est-ce qu'il voit ? Il voit une formule aussi compliquée que celle du modèle standard ou il voit une recette qui est donnée par des formules aussi compliquées que celle-là.

Alors, soit il dit "j'abandonne, la physique est trop compliquée pour moi". D'accord ? Soit il dit "peut-être n'est-il pas impossible que derrière ces recettes qui sont données par les physiciens, en fait, il y ait des maths vraiment intéressantes".

Et si vous voulez, la motivation que j'ai eue, toujours, la motivation que j'ai eue, toujours en travaillant dans ce domaine-là, c'est non pas de démontrer que ces calculs-là sont rigoureux. On sait bien qu'ils sont rigoureux puisqu'ils donnent la précision, d'accord ? Donc, ce n'est absolument pas qu'ils soient rigoureux, mais c'est de comprendre leur sens conceptuel. Alors, ça, ça a été fait dans

un travail d'abord avec Dirk Kreimer, mais je vais aller très, très vite dessus.

Et en fait, si vous voulez, ce qu'on a compris, donc, si j'ai 5 minutes, ce qu'on a compris, c'est qu'en fait, si vous voulez, le procédé qui est utilisé par les physiciens, donc ce procédé récursif, qui s'appelle BPHZ, c'est-à-dire BPHZ, pour Bogoliubov, Parasiuk, Hepp et Zimmermann, eh bien, en fait, il est identique à un procédé mathématique que les mathématiciens connaissaient depuis longtemps, qui était relié à ce qu'on appelle le problème de Riemann-Hilbert, qui était un des problèmes de Hilbert qu'il avait formulé au début du XX^{e} siècle, et qui est relié à ce qu'on appelle la décomposition de Birkhoff. Donc, en fait, il y a un groupe qui est présent derrière, et il y a un procédé mathématique qui est complètement clair.

Mais, en fait, les choses ont été beaucoup plus loin que ça. Ça, c'était il y a environ quatre ou cinq ans. Mais les choses ont été beaucoup plus loin que ça, et elles ont été beaucoup plus loin que ça, en partie grâce à l'intuition de Pierre Cartier.

Donc, je vais mettre, si vous voulez, un transparent qui est une citation de Pierre Cartier. Donc, Pierre Cartier disait la chose suivante. Il avait été frappé par l'analogie manifeste entre, d'une part, ce qu'on appelle le groupe de Grothendieck-Teichmüller, c'est un truc en mathématiques, et le groupe de renormalisation.

C'est-à-dire, en gros, si vous voulez, le groupe qui intervient dans ce que j'expliquais tout à l'heure, c'est ce que les physiciens appellent le groupe de renormalisation, sauf qu'il est localisé sur une théorie, de la théorie quantique des champs. Et donc, ce que disait Cartier :

> *"La parenté de plus en plus manifeste entre le groupe de Grothendieck-Teichmülluer d'une part, et le groupe de renormalisation de la Théorie quantique des champs d'autre part, n'est sans doute que la première manifestation d'un groupe de symétrie des constantes fondamentales de la physique, et il disait une espèce de groupe de Galois cosmique !"*

Alors, quand j'ai lu cet énoncé de Cartier, moi ça me faisait rigoler, c'était au moment de l'anniversaire de l'IHÉS, environ en l'an 2000, et je pensais qu'il n'y avait pas de fondement à cette idée.

Et graduellement, c'est une idée qui a émergé, et qui est correcte, et en fait, si vous voulez, c'était ça mon thème de départ ; donc mon thème de départ, c'était cette merveilleuse théorie de Galois, que Galois, si vous voulez, avait développée, non seulement pour les équations algébriques, mais en fait, il avait été beaucoup plus loin. Et Galois, dans sa lettre-testament, écrivait à son ami Auguste Chevalier, il lui disait qu'en fait, ses idées sur ce qu'il appelait la théorie de l'ambiguïté allaient infiniment plus loin que seulement les équations algébriques, c'est-à-dire les équations dont vous devez trouver une solution, etc., et où il avait compris, si vous voulez, qu'il y avait un groupe de symétrie. En fait, ce que Galois avait compris, et dont on voit des réminiscences, si vous voulez, dans la théorie de Ramis, sur les équations différentielles, etc., c'est que même pour les fonctions transcendantes, en fait, il y avait ce principe de symétrie cachée qui fait qu'on peut dire, a priori, dans certaines équations, même pour des équations transcendantes, qu'en fait, on peut changer la valeur de certaines fonctions en d'autres valeurs, par exemple, ce qu'on appelle le recalibrage des exponentielless, où on remplace $\exp\left(\frac{1}{x}\right)$ par $\lambda \exp\left(\frac{1}{x}\right)$, sans changer la validité des équations.

Alors, donc, ça a pris beaucoup de temps, ça a pris beaucoup de temps, mais maintenant, on est dans une situation qui correspond exactement à ce dont Cartier avait rêvé. Et non seulement ça, mais si vous voulez, on peut définir ce qu'on appelle le groupe de Galois d'une théorie des champs. Et par exemple, le groupe de Galois d'une théorie des champs est trivial, si et seulement si la théorie est finie.

Donc ça, c'est un travail récent que j'ai fait en collaboration avec Matilde Marcolli. Donc, en fait, si vous voulez, on a une situation qui est idéale maintenant. On a trouvé le groupe de Galois de Cartier.

C'est un groupe qui est très, très compliqué. C'est un groupe qui n'est pas du tout... je me souviens, en 1978, j'étais allé à une conférence de physique et je leur avais demandé "qu'est-ce que c'est que le groupe de renormalisation ?". Et j'avais compris que c'était la droite réelle, le changement d'échelle.

Alors, j'étais retourné chez moi en me disant "ce n'est pas vraiment intéressant.". Mais, en fait, le groupe de renormalisation, qui est ce groupe de Galois cosmique, est un groupe extrêmement intéressant qui est composé, bien sûr, du groupe de changement d'échelle, mais qui contient une algèbre de Lie libre, avec un générateur dans chaque dimension, d'accord, et qui correspond à la théorie des nombres. Alors, c'est ce groupe de Galois cosmique que Cartier avait envisagé.

Ce groupe de Galois cosmique s'envoie sur le groupe associé à une théorie, qui est associé au graphe de Feynman, grâce à l'algèbre de Hopf, de Kreimer, etc. Et on avait fait, dans notre travail avec Kreimer, on avait montré que son groupe, que le groupe, si vous voulez, des graphes, agit par difféomorphisme formel sur les constantes de couplage. Mais si vous combinez les deux flèches qui sont là, c'est-à-dire la flèche qui va du groupe de Galois cosmique vers le groupe des graphes, et du groupe des graphes vers les difféomorphismes des constantes de couplage, eh bien, vous vous apercevez qu'en fait, il y a effectivement, exactement comme Cartier le suggérait, un groupe de Galois qui est un groupe de symétrie universelle, que Cartier a appelé cosmique, et qui agit sur les constantes des théories physiques.

Donc, en fait, non seulement on a ça, si vous voulez, qu'est-ce que ça dit ? Eh bien, ça dit que, en fait, les gens qui prétendent que le fait qu'il y ait des divergences dans la théorie des champs est un inconvénient et qu'on doit s'en débarrasser à toute force, eh bien, en fait, ils ne comprennent pas que ces divergences sont, en fait, une bénédiction, parce que c'est grâce à ces divergences, c'est uniquement grâce à ces divergences, à ce qu'on appelle la fonction β en physique, et à ces composantes dans chaque puissance de $\hbar$, que ce groupe de Galois cosmique agit sur les théories physiques. Donc, si vous voulez, loin d'être un inconvénient, en fait, c'est un groupe de symétrie extrêmement caché, d'accord ? Bon, bien sûr, le groupe de renormalisation, le groupe de renormalisation, en fait, est un sous-groupe à un paramètre de ce groupe-là. Il y a un sous-groupe à un paramètre du groupe de Galois cosmique, qui est le groupe de renormalisation.

Et alors, il y a une étape que j'ai oublié de mentionner, donc, c'est que l'image du groupe de Galois cosmique dans le groupe d'une théorie donnée est ce qu'on appelle le groupe de Galois de la théorie. Et c'est un groupe qui régit, par exemple, le fait de savoir si la théorie est finie ou pas, qu'il y a toutes les bonnes propriétés. Donc, si vous voulez, les idées de Galois, les idées de Galois qui sont

des idées... Galois disait “sautons à pieds joints sur les calculs.”.

Donc, ce que disait Galois, si vous voulez, c'est qu'il est impossible de calculer un groupe de Galois. Et les gens lui riaient au nez, parce qu'ils lui disaient, vos trucs, c'est impossible à calculer. Mais, il allait beaucoup plus loin que ça, parce qu'il disait, le travail des géomètres futurs ne sera pas de faire ces calculs.

Le travail des géomètres futurs sera d'organiser ces calculs et de les faire dans leur tête, de les faire abstraitement, sans les faire concrètement. Et de savoir, ou plutôt de deviner, ce vers quoi... ce que vont donner les calculs, etc., etc. Donc, en fait, si vous voulez, la théorie de Galois a un pendant, justement, pour la théorie physique, ici, et alors, en fait, ce qui se produit, donc, c'est que, non seulement on a ça, mais si on utilise ce qu'on appelle la régularisation dimensionnelle, etc., je ne vais pas en parler, eh bien, en fait, il y a un repère universel, il y a un repère singulier universel, qui dit qu'en fait, la renormalisation, si vous voulez, consiste à renormaliser une fois pour toutes, il y a une manière universelle de le faire, qui consiste à renormaliser la géométrie.

C'est-à-dire que la géométrie de l'espace ordinaire de dimension 4, est en fait une géométrie qui n'est pas appropriée à la manière dont on fait la physique à cause de la réaction du champ, justement, et de la self-énergie du champ. Et à condition, bon, d'utiliser les bons outils, etc., et d'avoir effectivement des espaces (X_z) de dimension z, donc il y a une notion d'espace de dimension z, je vais m'arrêter là-dessus, c'est une notion qui utilise la géométrie non-commutative, donc il y a une notion effective d'espace de dimension z, et qui permet, une fois qu'on a cette notion-là, ça permet maintenant d'avoir une image mentale beaucoup, beaucoup plus précise de la signification de la renormalisation, de ce point de vue-là, et la signification est simplement la suivante, c'est qu'au lieu d'avoir la manière triviale de faire la régularisation dimensionnelle, c'est-à-dire d'aller pour la valeur de z de l'espace auxiliaire vers zéro de manière brutale, eh bien, en fait, il y a une manière d'y aller qui suit une trajectoire, d'accord, qui est divergente, mais qui consiste à renormaliser la géométrie. Bon, alors j'avais 36 autres transparents, mais je crois que je vais m'arrêter là.

(Applaudissements)

Édouard Brézin : Voilà. Donc, si là, l'un des jeunes lycéens a compris l'ensemble de l'exposé de M. Alain Connes, je propose qu'on l'élise immédiatement à l'Académie des sciences. L'exposé est ouvert pour des questions.

Vincent Courtillot : Dans l'énorme formule, qu'est-ce qui gouverne le nombre de ces termes et est-ce que c'est important ?

Alain Connes : Ah, bien sûr. Mais malheureusement, c'est dans les transparents d'après.

Cette énorme formule a, non pas une explication, mais enfin, il y a une manière de l'écrire qui prend une ligne, d'accord, à condition de faire la chose suivante, c'est-à-dire d'accepter qu'au lieu que ce soit la toute petite partie de cette formule qui est l'électrodynamique, la partie électrodynamique de cette formule tient en un quart de ligne dans l'énorme formule. Je vais essayer de la retrouver. Donc, si on regarde l'électrodynamique, l'électrodynamique prend un quart de ligne.

Eh bien, qu'est-ce qu'on a fait, nous ? Qu'est-ce qu'on a fait ? On a pris ce quart de ligne et on a dit, voilà l'espace-temps, puisque c'est Maxwell qui nous a donné les équations de Maxwell, qui sont une partie de l'électrodynamique, d'accord. Et c'est à partir de ça qu'on a dit, bon, eh bien, d'accord, on a $\sqrt{\frac{1-v^2}{c^2}}$, etc., etc., et on en a déduit l'espace-temps, l'espace-temps de Minkowski, d'accord. Et puis on s'est dit, chaque fois qu'on rajoute un terme dans la formule, l'interaction faible, etc., c'est une nouvelle particule.

C'est une manière de penser. C'est une manière de penser. Il y a une autre manière de penser.

Cette autre manière de penser consiste à dire : "adaptons nos concepts géométriques d'abord", d'accord. Alors, en quel sens adaptons-nous nos concepts géométriques ? Eh bien, on s'aperçoit, les mathématiciens ont énormément à apprendre de la physique. Pourquoi ? Parce que dans la géométrie, il y a mètre, d'accord.

Et dans mètre, il y a la définition de l'unité de longueur. La première définition de l'unité de longueur, ça a été l'arpentage entre Dunkerque et Barcelone, d'accord, avec un angle précis du Méridien. On en a pris la 40 millionième partie, on en a fait un objet concret, qu'on a appelé le mètre et qu'on a déposé au pavillon de Breteuil.

Très bien, d'accord. Eh bien, ça, ça correspond au ds^2 et au $g_{\mu\nu}dx_\mu dx_\nu$, d'accord. Qu'est-ce qui s'est passé ? Ce qui s'est passé, c'est qu'au bout d'un moment, on s'est aperçu que le mètre, qui était déposé au pavillon de Breteuil, ce n'était pas pratique.

En exagérant, si je veux mesurer mon lit, et si je dois aller à Paris et comparer au mètre qui est déposé au pavillon de Breteuil, ce n'est pas pratique, d'accord. Et en plus, ce mètre-là, il n'était pas de longueur fixe. Donc les physiciens ont réfléchi.

Les physiciens ont réfléchi. Et quel a été le bout de leur réflexion ? Le bout de leur réflexion, les physiciens se sont aperçus qu'en fait, il y avait bien mieux, bien mieux pour définir une longueur, une unité de longueur, c'était de prendre un corps chimique, si possible un corps pur, d'accord, prendre une de ses raies spectrales, et prendre la longueur d'onde de cette raie spectrale comme unité de longueur. Bien sûr, on va la multiplier par un nombre de telle sorte que ça ressemble au mètre.

Alors on a commencé par le faire pour le krypton, avec la raie orange du krypton, etc., et ensuite on l'a fait pour le césium. Mais ça, ça ne correspond pas au $ds^2 = g_{\mu\nu}dx_\mu dx_\nu$, d'accord. Pas du tout.

Par contre, par contre, ça correspond exactement, ça correspond exactement à l'élément de longueur en géométrie non-commutative. Donc il se fait qu'exactement pour cette raison-là, d'accord, il y a eu, si vous voulez, il y a eu un changement de paradigme, mais qui a été imposé pour d'autres raisons, qui n'étaient pas du tout celles qui venaient de la physique, qui a été imposé parce qu'on voulait s'intéresser à des espaces qui étaient différents des espaces ordinaires dans lesquels les points sont donnés par des coordonnées qui commutent.

Donc on voulait s'intéresser à des espaces qui étaient plus délicats. Eh bien, lorsqu'on s'intéresse à des espaces qui sont plus délicats, on s'aperçoit qu'on est obligé de prendre la même convention que les physiciens. En quel sens cette convention des physiciens est une convention intéressante ? C'est une convention intéressante parce que supposez qu'on veuille unifier, par exemple, le système métrique dans la galaxie.

Si on dit aux autres systèmes planétaires dans la galaxie "vous allez devoir venir à Paris et vous allez devoir prendre une copie du mètre-étalon et c'est ça qui va vous servir d'unité de longueur". Bon, c'est évident que ça va déclencher une guerre galactique, etc. Par contre, si on leur dit "vous prenez un corps chimique pur, d'accord, qui vient du tableau périodique des éléments, etc., et vous prenez telle raie spectrale, et c'est ça votre unité de longueur", bon, là ça va marcher, d'accord, parce que c'est une définition infiniment plus intrinsèque. Alors, donc, si vous voulez, on est obligé d'adapter les concepts géométriques. Une fois qu'on a adapté les concepts géométriques, une fois qu'on a élargi le concept de géométrie, bon, d'abord on s'aperçoit que ce concept de géométrie, il contient le concept ordinaire de manière stricte.

C'est-à-dire que ce n'est pas une généralisation dans laquelle vous oubliez le concept de départ. Le concept de départ est strictement contenu dedans. D'accord ? Bon, mais alors maintenant ce qui se produit, donc ce qui se produit, c'est la chose suivante.

C'est qu'une fois que vous avez un concept géométrique qui est plus flexible, eh bien vous pouvez faire l'opération suivante. Vous pouvez regarder l'énorme formule. Je ne sais pas si je vais la retrouver.

Vous vous souvenez comme elle était énorme, cette formule. Donc vous pouvez regarder l'énorme formule et vous pouvez vous dire, de cette formule, je ne veux pas retenir, je ne veux absolument pas retenir dans cette formule un petit bout, et puis dire qu'après je rajoute des particules. Non ! Je veux dire que cette formule, par elle-même, me donne la géométrie de l'espace-temps. D'accord ? C'est-à-dire que je veux avoir un principe, extrêmement simple, qui me dise que c'est cette formule qui me décrit la géométrie de l'espace-temps. Et le procédé qui, à partir, si vous voulez, de la géométrie de l'espace-temps va vous redonner cette formule doit être une simplicité délirante. Il doit être extrêmement simple. D'accord ?

Et alors le procédé qui est appliqué, justement, pour retrouver, si vous voulez, la formule en question à partir de la géométrie de l'espace-temps, eh bien, c'est un procédé qui est purement spectral. C'est-à-dire, le procédé qui vous redonne cette formule, c'est le procédé qui consiste à compter le nombre de valeurs propres, qui sont plus petites qu'une valeur propre donnée, à faire son développement, d'accord ? Et on doit réobtenir exactement la formule en question.

Alors qu'est-ce qu'on obtient, comme structure de l'espace-temps ? Eh bien, on obtient que l'espace-temps, effectivement, ressemble à l'espace de Minkowski. On traite les espaces courbes, là, dans ce cas-là. D'accord ? Mais, en fait, il a une structure beaucoup plus raffinée. C'est-à-dire qu'il a une structure... En gros, si vous voulez, de manière très simple, très simpliste, cet espace-temps, c'est le produit de l'espace-temps ordinaire par un espace fini mais non-commutatif. Fini, ça veut dire

que c'est comme un ensemble fini de points.

Et cet espace non-commutatif, en fait, il est dicté par le modèle standard. Il est dicté par la physique. C'est-à-dire que le modèle standard est ce qu'on appelle une matrice de Yukawa. C'est cette matrice de Yukawa dans le modèle standard qui vous donne la géométrie de l'espace fini. Alors, après, on peut faire un tas de calculs, mais en particulier, lorsque vous calculez après, lorsque vous calculez ce nombre de valeurs propres, vous obtenez non seulement le modèle standard avec cette formule, mais vous obtenez aussi l'action d'Einstein-Hilbert. C'est-à-dire que vous obtenez la somme des deux.

Alors, si vous voulez, pour le moment, c'est une interprétation simplement au niveau classique. Et un des problèmes auxquels je me suis attaché, en particulier dans ma collaboration avec Kreimer et Marcolli, si vous voulez, c'est d'essayer de comprendre en quel sens la compréhension que l'on a maintenant de la renormalisation, c'est-à-dire cette image mentale que l'on a de la renormalisation de la géométrie de l'espace, cadre avec le modèle standard. Et en fait, ce qui est remarquable, c'est qu'effectivement, on peut les mettre ensemble. C'est-à-dire que l'opération de produit qui consiste à faire le produit par un espace de dimension z complexe, puis à faire tendre z vers zéro de cette manière assez ad hoc, eh bien, elle cadre exactement avec le modèle standard, c'est-à-dire avec le fait de faire le produit par cet espace non-commutatif et fini, qui lui aussi va bouger en fonction de z. C'est-à-dire que la géométrie de cet espace va être fonction de la variable z, puisqu'on a la renormalisation. Alors on est encore très très loin du compte, mais si vous voulez, en tout cas, en tous les cas, ce que l'on voit, c'est qu'on voit typiquement cet échange qu'il y a entre les mathématiques et la physique. Alors c'est un échange qui va dans toutes les directions, mais je pense qu'on aurait bien tort de dire que d'un côté, on a les mathématiciens qui font leurs équations, etc., qui prennent un petit problème de physique, puis essayent de le résoudre de manière rigoureuse, et d'un autre côté, on a la physique. Non ! En fait, on est tous confrontés au même problème. Et ce même problème, c'est le monde dans lequel on vit.

Et c'est ce monde dans lequel on vit qui est la source de la géométrie. Et une des choses les plus fascinantes, je l'avais sur les transparents, mais je n'ai pas eu le temps d'en parler si vous voulez, c'est à quel point, en fait, on s'aperçoit au bout d'un moment que le problème de comprendre la géométrie des nombres premiers n'est pas du tout un problème disjoint du problème de la compréhension de l'espace-temps. C'est-à-dire qu'il y a des reflets, il y a des choses qui se produisent, il y a ce qu'on appelle le groupe de Weil, qui correspond à la théorie de Galois, etc.

Le même auditeur : C'est passionnant de vous écouter. J'ai l'impression que j'ai un peu compris. Je voudrais poser une question peut-être encore plus naïve mais qui est liée à ma première question. J'aurais eu tendance à penser que cette formule si compliquée dans laquelle on reconnaissait quelques notations était construite de façon ascendante, à partir de l'observation et de la donnée, entre autres, de particules.

Or, dans votre dernier discours, j'ai eu l'impression de comprendre qu'une vision extérieure ou au-dessus permettait d'obtenir quelque chose qui éventuellement ferait découvrir qu'il y a une particule qu'on avait loupée. Laquelle de ces deux façons de dire les choses est la plus proche ?

Alain Connes : Non, non, attention : mon point de vue est le suivant. Mon point de vue est intermédiaire entre les deux.

C'est-à-dire que je n'essaie pas de deviner. Il y a certaines théories qui essayent de deviner comment l'espace-temps devrait être. Je n'essaie pas du tout de faire ça. Ce que je dis, c'est que j'ai un cadre plus flexible pour la géométrie, je pars de cette formule et j'essaie de l'écrire de manière infiniment simple mais de manière géométrique. En fait, c'est la combinaison des deux. Mais si, par exemple, il se faisait qu'au CERN, on découvre de nouveaux raffinements, etc., la première chose qu'il faudrait comprendre, c'est "est-ce que ces raffinements sont compatibles avec cette vision géométrique des choses ?". C'est une approche entre les deux. C'est une approche qui ne consiste pas à essayer de deviner la pensée divine, etc., et de savoir pourquoi l'espace-temps... Non, pas du tout. C'est une approche très pragmatique.

J'admire beaucoup chez les physiciens les choses qui sont testées par l'expérience, et qui sont des calculs extrêmement sophistiqués. Pour moi, je ne connais pas beaucoup de physique, mais je connais deux endroits de la physique qui sont comme ça. Ces deux endroits sont le modèle standard, d'une part, et la renormalisation, d'autre part.

J'ai toujours été fasciné, si vous voulez, par le fait qu'on savait que ces choses ont à voir avec la Nature, puisqu'elles ont été testées avec cette précision faramineuse. Donc, on sait qu'elles ont à voir avec la Nature, d'accord, et c'est encore plus merveilleux si elles ont à voir avec des mathématiques qui sont des mathématiques extrêmement élaborées. Et c'est effectivement comme ça que ça se produit.

Et donc, à travers toutes ces étapes, en particulier avec Dirk Kreimer, avec l'intuition de Cartier, etc., on a compris maintenant, donc, qu'il y avait ce lien avec la théorie de Galois, enfin cette extension de la théorie de Galois, de la renormalisation. Bien sûr, les physiciens savent que la renormalisation est une théorie de l'ambiguïté. Ils le savent au départ.

Édouard Brézin : Oui, mais non, si tu permets les commentaires du physicien, d'abord, je trouve que ta formule compliquée, comme tu dis, est injuste. Jamais les physiciens n'y seraient arrivés, s'ils n'avaient pas derrière, des principes extrêmement simples qui permettent d'écrire cette formule toute simple, qui sont des principes de symétrie de jauge non-abélienne, qui permettent de l'écrire en une ligne. Quand on cherche à développer ce que ça signifie pour faire un calcul, c'est vrai qu'in fine, il faut faire ça, mais jamais on n'y serait arrivés autrement et qu'ils partent d'observation, quand même, de la Nature. Donc ça, c'est le premier point.

Deuxième point, j'ai deux questions qui me gênent par rapport à ce que tu dis. La première, c'est que les physiciens savent que le modèle standard n'est qu'un modèle effectif et limité, qu'il ne peut pas prétendre être un modèle fondamental, même si pour l'instant il n'existe aucune contre-observation expérimentale qui le mette en défaut, nous savons qu'il porte de manière interne sa propre mort.

Je vois mal, dans l'approche que tu veux, comment c'est contenu... Et ma dernière question sera sur ton groupe de Galois cosmique des constantes de couplage, qui contient comme sous-groupe à

un paramètre le groupe de renormalisation habituel, est-ce que tu es certain qu'il contient autre chose ? Je vais prendre un exemple. Lorsqu'on a une théorie invariante par dilatation, nous savons qu'elle est invariante également par tout le groupe conforme, mais à l'exception de la dimension 2, l'ensemble des autres symétries sont automatiquement appliquées, donc ça n'ajoute rien de nouveau d'ajouter ce groupe plus général. Est-ce que tu es certain que tu as ajouté des choses qui ont un sens dynamique concret ?

Alain Connes : Oui. Alors, je répondrai d'abord à la première question. La première question sur le modèle standard, disons que ce qui se produit, c'est la chose suivante. C'est que bien sûr, cette théorie ne prétend pas avoir la réponse ultime sur l'espace-temps ; ce qu'elle prétend simplement, c'est formuler géométriquement les connaissances que l'on a, à l'heure actuelle, sur l'espace-temps. D'accord ? C'est-à-dire qu'elle prétend dire la chose suivante, elle prétend dire que l'espace de Minkowski est une approximation qui aurait été parfaitement valable si on s'était restreint à l'électrodynamique.

C'est à dire que l'espace de Minkowski aurait été la réponse si l'on avait seulement les interactions électromagnétiques. D'accord ? Ce que dit ce modèle, d'accord ? Ce que dit cette géométrie, simplement, elle ne dit pas du tout que le modèle standard est la réponse ultime, mais elle dit qu'aux échelles de l'ordre de 10^{-16}, 10^{-17}, 10^{-18} centimètres, voilà ce que l'on voit au niveau géométrique. C'est tout. D'accord ? Et donc, si tu veux, elle prétend donc donner un cadre à la géométrie qui adapte à, qui absorbe si tu veux, ce que l'on voit à cette échelle et le rend simple.

Alors maintenant tu me dis bien sûr le modèle standard est basé sur des principes de symétrie comme les symétries de jauge, bien entendu. Mais où est-ce que ces principes interviennent justement ? Ils interviennent de la manière suivante, qui est très très compréhensible ; la symétrie de jauge se rajoute à la symétrie d'Einstein, par les difféomorphismes. Donc en fait, en gros, si tu veux, pour simplifier les choses, on a deux groupes de symétries : on a le groupe des difféomorphismes et on a le groupe des symétries de jauge.

Et alors, ce n'est pas difficile de comprendre que l'un agit sur l'autre, c'est à dire que si on regarde les transformations de jauge, ce sont des transformations qui vont dépendre du point de l'espace-temps, d'accord, et que si on agit par difféomorphisme, elles vont être chamboulées entre elles. Alors c'est ce qu'on appelle un produit semi-direct, c'est un peu comme le groupe de Poincaré, qui est le produit semi-direct du groupe des translations par le groupe de Lorentz. Alors ce n'est pas difficile de comprendre que si on voulait que les choses soient purement gravitationnelles, il faudrait que ce groupe-là soit purement le groupe des difféomorphismes ; c'est normal. C'est à dire que les gens pourraient se dire "on va chercher un espace" et c'est ce qu'ils ont fait dans la théorie de Kaluza-Klein, dont le groupe des difféomorphismes corresponde à ce produit semi-direct.

Or les mathématiques ont cela de très convaincant, c'est qu'il y a des théorèmes généraux en mathématiques, c'est à dire qu'il y a des théorèmes qui vous disent que, quelle que soit la variété que vous prendrez, si vous regardez la composante connexe de son groupe des difféomorphismes, c'est ce qu'on appelle un groupe simple (un groupe simple, c'est un groupe qui ne peut pas se casser en deux groupes, comme ça). Donc on sait, pour sûr, si vous voulez, que si l'on cherche parmi les théories de Kaluza-Klein de quelque sorte que ce soit, et si l'on n'essaye pas de tricher, c'est-à-dire

de dire que les transformations vont ce qu'on appelle "préserver les fibres", eh bien à ce moment-là, on est coincé. On est coincé, et on ne trouvera jamais un groupe comme ça. Or, ça, c'est le point de départ de la théorie : si on prend une algèbre non-commutative, et si on regarde son groupe des difféomorphismes, eh bien, il contient toujours les difféomorphismes intérieurs, c'est à dire les transformations $x \to uxu^{-1}$, d'accord, qui est un sous-groupe normal, et qui a exactement cette structure de produit semi-direct. Et ce qui est étonnant, c'est que la terminologie mathématique, ce qu'on appelle les automorphismes intérieurs, coïncide avec la terminologie physique, qu'on appelle les symétries internes. Donc c'est ça le point de départ. Le point de départ, c'est que l'idée que l'on a de la géométrie est une idée trop, comment dire, corsetée, d'accord, et que même dans les théories qui prétendent être des généralisations, etc., eh bien ce sont des théories qui en fait sont constamment, en fait, corsetées par la même idée d'espace géométrique, qui est une idée beaucoup trop restreinte ; donc, c'est ça, l'idée. Si tu veux, l'idée fondamentale, ce n'est pas que bien sûr on va jeter les principes de symétrie, qui sont les principes de géométrie, mais c'est qu'on va les rendre entièrement géométriques, et entièrement gravitationnels. C'est à dire que l'action dont je parlais, n'est pas une action qui à un bout de théorie de jauge, Yang-Mills, etc., elle s'écrit une fois pour toutes, elle s'écrit en un seul bloc, c'est une action purement gravitationnelle. C'est une action qui dans le cas de l'espace de Minkowski, etc., ou dans le sens de l'espace de l'électrodynamique, redonnerait exactement l'action d'Einstein, c'est tout. Elle ne donnerait rien d'autre, elle ne donnerait pas de terme de jauge.

Un auditeur : Et la supersymétrie ?

Alain Connes : Alors, la supersymétrie n'apparaît pas, je ne veux pas parler de la supersymétrie, puisque bon, je veux dire... elle n'apparaît pas, d'accord. Donc, ce que l'on a, c'est un principe, qui permet de passer de manière naturelle, c'est très simple à comprendre, du secteur fermionique, c'est le secteur fermionique du modèle standard qui spécifie la géométrie. Et il y a un procédé, qui est entièrement mathématique, qui permet de passer, entièrement de manière canonique, de la partie fermionique à la partie bosonique, mais qui n'est pas la supersymétrie.

Alors, tu avais posé une deuxième question, c'était sur... Je ne me souviens pas.

Édouard Brézin : La question c'était, est-ce que tu es certain que ce groupe de Galois cosmique contient plus que simplement le zéro de la fonction β habituelle ?

Alain Connes : Non, alors, je peux te dire ce qu'il contient. D'abord, si tu veux, il y a une fonction β par constante de couplage.

Or, dans ce groupe-là, justement dans le groupe intermédiaire qui est au milieu, qui est le groupe qui est associé à l'algèbre de Hopf des graphes, etc., il y a une seule fonction β, qui va s'envoyer, par les différentes applications, vers les différentes fonctions β. Alors, en gros, le groupe de Galois cosmique, ce qu'il contient, ce sont les composantes homogènes de cette fonction β par puissance de $\hbar$, en gros. Et il contient l'algèbre de Lie qu'elles engendrent.

Et ce qui est nouveau, et ce qui n'était absolument pas dans la littérature ordinaire, c'est le fait qu'il y a une algèbre de Lie. Et justement, que ce groupe est engendré par l'algèbre de Lie des

composantes de la fonction β. Et si tu veux, le point essentiel, dont je n'ai pas, bien sûr, eu le temps de parler, c'est un théorème qui est, je pense, dû à 't Hooft et à David Gross, et qui dit qu'on peut calculer les contre-termes dans la régularisation dimensionnelle, avec la soustraction minimale, uniquement en termes de la fonction β.

Donc, tout est basé là-dessus. Sur le fait que les contre-termes sont indépendants de ce qu'on appelle le paramètre massif μ, etc. Donc, tout est basé là-dessus.

C'est basé sur un tas de formules. Et si tu veux, le fait que, justement on puisse écrire, une fois pour toutes, les contre-termes, à partir de ce groupe cosmique, vient de là. Donc, c'est ça, l'idée.

Alors, je veux dire, au moins, ça a un mérite, si tu veux, c'est que, pour les mathématiciens, c'est un paradis, parce qu'on relie à des théories qu'on connaît bien, comme la théorie de Galois, etc. Et ensuite, on s'attend à ce que le potentiel de la théorie de Galois... J'en ai discuté avec Ramis. Je veux dire, on a l'exemple de l'impossibilité de résoudre le problème des trois corps à partir de la théorie de Galois différentielle, on s'attend à ce qu'on puisse transplanter ces idées de la théorie de Galois, de la théorie de Galois différentielle, au cas de la renormalisation. D'accord ? Il y a un autre aspect, dont je ne parle pas, qui est extrêmement important.

Ce sont les travaux de Bloch, Kreimer et Esnault, sur l'aspect théorie des nombres. C'est-à-dire que les transcendants qui apparaissent en théorie des champs, on sait bien que $\zeta(3)$ intervient dans le calcul du moment anormal de l'électron, eh bien, sont gouvernés par ce groupe de Galois cosmique. C'est-à-dire, c'est la théorie des motifs de Grothendieck, qui est derrière, et qui gouverne ces nombres transcendants.

Donc je veux dire, il y a un paysage merveilleux à découvrir. On ne sait pas si ce paysage aura tant que ça de conséquences sur la physique. Ce n'est pas ça qui nous intéresse.

Ce qui nous intéresse, c'est de comprendre.

Édouard Brézin : Je propose qu'on revienne aux questions terre-à-terre, si on peut. Oui, monsieur.

Un auditeur : Ma question concerne les nombres premiers. Et c'est une question qui concerne la conjecture de Goldbach. Alors, la conjecture de Goldbach a le gros avantage d'être extrêmement simple dans son énoncé, ou bien d'être suffisamment simple, non seulement pour être comprise des jeunes qui sont ici, mais même de beaucoup plus jeunes.

Et cette conjecture est que "tout entier pair supérieur à 2 peut être mis sous la forme de la somme de deux nombres premiers et deux seulement". Alors, je voulais savoir si c'est toujours une conjecture, d'abord. Et ensuite...

Alain Connes : Je ne suis pas vraiment la personne la mieux placée, je dois vous dire, pour vous répondre, à l'instant t, je ne saurais pas vous dire. Je ne pense pas, non, ce n'est pas démontré.

Édouard Brézin : Est-ce qu'il y a d'autres questions ? Oui, Denis ? (Ah, monsieur Tits, oui).

Denis : Dans tout ce dont on parle, on ne parle jamais du fait que, dans le fond, on ne sait pas ce qu'est la gravité. C'est bon, vous avez parlé, il y a quand même la force d'Archimède, des choses comme ça. Enfin, tout ça, c'est quand même assez vague quand on pense que la Terre tourne à une vitesse, elle fait un tour en un jour, et que par conséquent, si on était, nous, sur une ligne, qui nous paraît comme une vraie rectiligne, on se trouverait à plusieurs mètres de hauteur en l'espace de quelques secondes. Alors, ça, on ne paraît pas en tenir compte du tout.

Alain Connes : Je ne pense pas que je puisse répondre à ça.

Édouard Brézin : Oui, mais c'est de la physique. Monsieur Tits, oui.

L'auditeur :*(on lui a ostensiblement tourné le dos)* Ça me paraît important de tenir compte de ça.

Jacques Tits : Il y avait ici un problème de physique[5] J'ai deux petites questions : à propos du modèle standard. C'est la plus grande formule que j'ai jamais vue de ma vie. Je voudrais te demander s'il y a derrière cette formule une structure telle que, par exemple, toi, rentré chez toi et que tu oublies tout ça, tu peux la reconstruire facilement.

Alain Connes : Oui, bien sûr, si tu veux. Oui, oui. Au niveau... Non, non, non. Ce qu'il faut voir... Bon, on a déjà eu la discussion, si tu veux, là-dessus. C'est-à-dire que, d'une part, il y a les principes de physique comme invariance de jauge, etc., dont on parlait.

Mais, en fait, ce que je disais simplement, si tu veux, c'est qu'on peut l'écrire géométriquement, mais après, il y a un calcul à faire. Il faut faire ce calcul. Ce calcul, c'est un calcul d'équation de la chaleur, etc., d'un développement qui donne quantité de termes.

Donc, en fait, on peut l'écrire de manière infiniment simple, je pense plus simple qu'en disant... on a le principe de Yang-Mills. On écrit un potentiel quartique pour les Higgs. On écrit le couplage minimal entre les Higgs et les champs de jauge, ce que, normalement, il faudrait dire...

On écrit le couplage de Yukawa entre les champs de Higgs et les fermions, etc. Ce que je dis, moi, simplement, si tu veux, c'est qu'on a un espace. Je donne cet espace.

Après, pour cet espace, il faut faire le calcul de ce que c'est que la gravitation. On obtient une partie interne dans les $g_{\mu\nu}$, dans la gravitation. Et ensuite, on a un principe d'action qui est extrêmement simple, qui est simplement le nombre de valeurs propres.

Ce nombre de valeurs propres, on le calcule par un calcul mathématique, qui est compliqué, mais qui va donner tous ces termes-là.

Édouard Brézin : Monsieur Tits, c'est un peu comme les équations de Maxwell. Quand Maxwell les écrivait, il écrivait 12 équations, puisqu'il y avait 4 équations pour des trivecteurs.

[5] *(parlant vraisemblablement du micro, qui n'a pas fonctionné du premier coup)*

Aujourd'hui, nous l'écrivons en une demi-ligne. $d\mu\, f_{\mu\nu} = g_{nu}$. Voilà l'ensemble des 12 équations.

Alain Connes : Alors, attention, Cette simplification, elle était déjà présente. C'est-à-dire que les indices, ils étaient déjà là. On n'a pas développé les indices. C'est-à-dire que dans l'équation que tu as vue, il y avait, par exemple, je ne sais pas moi, il y avait des indices g, μ, etc. Tous ces indices-là, on fait la somme sur ces indices. Donc ça, je ne l'ai pas développé, heureusement.

Donc effectivement, si tu veux... Et ce qui est vrai, c'est que si tu écris Maxwell... Je vais peut-être la sortir, cette formule. Non, parce que je veux dire... Justement, on entend trop facilement dire par les physiciens... C'est vrai ce qu'ils disent. C'est parfaitement vrai. C'est parfaitement vrai qu'on l'obtient à partir des principes, etc. Mais il faut quand même l'avoir vue une fois. D'accord ? Il faut quand même... C'est une espèce de Pierre de Rosette, on peut dire, d'une certaine manière.

Voilà. Alors, la voilà, la formule. Alors maintenant, vous pouvez me poser des questions sur cette formule, d'accord[6].

---

[6]
Bosons : A_μ, W_μ, Z^0, g_μ
Quarks : u^κ, d^κ
Leptons : e^λ, ν^λ
Higgs : H, ϕ^0, ϕ^+, ϕ^-
Masses : m_d, m_u, m_e, m_h, M_W
$g = \sqrt{4\pi\alpha}$, g_s (interaction forte)
$C_{\lambda\kappa}$: matrice de Cabibbo-Kobayashi-Maskawa
f^{abc} : constantes de $SU(3)$
Jauge de Feynman.
Les fantômes de Faddeev-Popov sont omis pour simplicité.*Note de la transcriptrice : Dans la page suivante, est fournie une expression de la formule en question (je n'ai pas vérifié s'il s'agissait exactement de la formule présentée dans l'exposé d'Alain Connes).*

Notations de Martinus Veltman :

Bosons : A_μ, W_μ, Z^0, g_μ
Quarks : u^κ, d^κ
Leptons : e^λ, ν^λ
Higgs : H, ϕ^0, ϕ^+, ϕ^-
Masses : m_d, m_u, m_e, m_h, M_W
$g = \sqrt{4\pi\alpha}$, g_s (interaction forte)
$C_{\lambda\kappa}$: matrice de Cabibbo-Kobayashi-Maskawa
f^{abc} : constantes de $SU(3)$
Jauge de Feynman.
Les fantômes de Faddeev-Popov sont omis pour simplicité.

$$\mathcal{L}_{SM} =$$
$$-\tfrac{1}{2}\partial_\nu g^a_\mu \partial_\nu g^a_\mu - g_s f^{abc}\partial_\mu g^a_\nu g^b_\mu g^c_\nu - \tfrac{1}{4}g_s^2 f^{abc}f^{ade}g^b_\mu g^c_\nu g^d_\mu g^e_\nu - \partial_\nu W^+_\mu \partial_\nu W^-_\mu - M^2 W^+_\mu W^-_\mu -$$
$$\tfrac{1}{2}\partial_\nu Z^0_\mu \partial_\nu Z^0_\mu - \tfrac{1}{2c_w^2}M^2 Z^0_\mu Z^0_\mu - \tfrac{1}{2}\partial_\mu A_\nu \partial_\mu A_\nu - igc_w[\partial_\nu Z^0_\mu (W^+_\mu W^-_\nu - W^+_\nu W^-_\mu) -$$
$$Z^0_\nu (W^+_\mu \partial_\nu W^-_\mu - W^-_\mu \partial_\nu W^+_\mu) + Z^0_\mu (W^+_\nu \partial_\nu W^-_\mu - W^-_\nu \partial_\nu W^+_\mu)] - igs_w[\partial_\nu A_\mu (W^+_\mu W^-_\nu -$$
$$W^+_\nu W^-_\mu) - A_\nu (W^+_\mu \partial_\nu W^-_\mu - W^-_\mu \partial_\nu W^+_\mu) + A_\mu (W^+_\nu \partial_\nu W^-_\mu - W^-_\nu \partial_\nu W^+_\mu)] -$$
$$\tfrac{1}{2}g^2 W^+_\mu W^-_\mu W^+_\nu W^-_\nu + \tfrac{1}{2}g^2 W^+_\mu W^-_\nu W^+_\mu W^-_\nu + g^2 c_w^2 (Z^0_\mu W^+_\mu Z^0_\nu W^-_\nu - Z^0_\mu Z^0_\mu W^+_\nu W^-_\nu) +$$
$$g^2 s_w^2 (A_\mu W^+_\mu A_\nu W^-_\nu - A_\mu A_\mu W^+_\nu W^-_\nu) + g^2 s_w c_w [A_\mu Z^0_\nu (W^+_\mu W^-_\nu - W^+_\nu W^-_\mu) -$$
$$2A_\mu Z^0_\mu W^+_\nu W^-_\nu] - \tfrac{1}{2}\partial_\mu H \partial_\mu H - 2M^2 \alpha_h H^2 - \partial_\mu \phi^+ \partial_\mu \phi^- - \tfrac{1}{2}\partial_\mu \phi^0 \partial_\mu \phi^0 - \beta_h [\tfrac{2M^2}{g^2} + \tfrac{2M}{g}H +$$
$$\tfrac{1}{2}(H^2 + \phi^0\phi^0 + 2\phi^+\phi^-)] + \tfrac{2M^4}{g^2}\alpha_h - g\alpha_h M[H^3 + H\phi^0\phi^0 + 2H\phi^+\phi^-] - \tfrac{1}{8}g^2\alpha_h[H^4 + (\phi^0)^4 +$$
$$4(\phi^+\phi^-)^2 + 4(\phi^0)^2\phi^+\phi^- + 4H^2\phi^+\phi^- + 2(\phi^0)^2 H^2] - gMW^+_\mu W^-_\mu H - \tfrac{1}{2}g\tfrac{M}{c_w^2}Z^0_\mu Z^0_\mu H -$$
$$\tfrac{1}{2}ig[W^+_\mu(\phi^0\partial_\mu\phi^- - \phi^-\partial_\mu\phi^0) - W^-_\mu(\phi^0\partial_\mu\phi^+ - \phi^+\partial_\mu\phi^0)] + \tfrac{1}{2}g[W^+_\mu(H\partial_\mu\phi^- -$$
$$\phi^-\partial_\mu H) - W^-_\mu(H\partial_\mu\phi^+ - \phi^+\partial_\mu H)] + \tfrac{1}{2}g\tfrac{1}{c_w}(Z^0_\mu(H\partial_\mu\phi^0 - \phi^0\partial_\mu H) + M(\tfrac{1}{c_w}Z^0_\mu\partial_\mu\phi^0 +$$
$$W^+_\mu\partial_\mu\phi^- + W^-_\mu\partial_\mu\phi^+) - ig\tfrac{s_w^2}{c_w}MZ^0_\mu(W^+_\mu\phi^- - W^-_\mu\phi^+) + igs_w MA_\mu(W^+_\mu\phi^- - W^-_\mu\phi^+) -$$
$$ig\tfrac{1-2c_w^2}{2c_w}Z^0_\mu(\phi^+\partial_\mu\phi^- - \phi^-\partial_\mu\phi^+) + igs_w A_\mu(\phi^+\partial_\mu\phi^- - \phi^-\partial_\mu\phi^+) - \tfrac{1}{4}g^2 W^+_\mu W^-_\mu[H^2 + (\phi^0)^2 +$$
$$2\phi^+\phi^-] - \tfrac{1}{8}g^2\tfrac{1}{c_w^2}Z^0_\mu Z^0_\mu[H^2 + (\phi^0)^2 + 2(2s_w^2 - 1)^2\phi^+\phi^-] - \tfrac{1}{2}g^2\tfrac{s_w^2}{c_w}Z^0_\mu\phi^0(W^+_\mu\phi^- + W^-_\mu\phi^+) -$$
$$\tfrac{1}{2}ig^2\tfrac{s_w^2}{c_w}Z^0_\mu H(W^+_\mu\phi^- - W^-_\mu\phi^+) + \tfrac{1}{2}g^2 s_w A_\mu\phi^0(W^+_\mu\phi^- + W^-_\mu\phi^+) + \tfrac{1}{2}ig^2 s_w A_\mu H(W^+_\mu\phi^- -$$
$$W^-_\mu\phi^+) - g^2\tfrac{s_w}{c_w}(2c_w^2 - 1)Z^0_\mu A_\mu\phi^+\phi^- - g^2 s_w^2 A_\mu A_\mu\phi^+\phi^- + \tfrac{1}{2}ig_s\lambda^a_{ij}(\bar{q}^\sigma_i\gamma^\mu q^\sigma_j)g^a_\mu - \bar{e}^\lambda(\gamma\partial +$$
$$m^\lambda_e)e^\lambda - \bar{\nu}^\lambda(\gamma\partial + m^\lambda_\nu)\nu^\lambda - \bar{u}^\lambda_j(\gamma\partial + m^\lambda_u)u^\lambda_j - \bar{d}^\lambda_j(\gamma\partial + m^\lambda_d)d^\lambda_j + igs_w A_\mu[-(\bar{e}^\lambda\gamma^\mu e^\lambda) +$$
$$\tfrac{2}{3}(\bar{u}^\lambda_j\gamma^\mu u^\lambda_j) - \tfrac{1}{3}(\bar{d}^\lambda_j\gamma^\mu d^\lambda_j)] + \tfrac{ig}{4c_w}Z^0_\mu[(\bar{\nu}^\lambda\gamma^\mu(1+\gamma^5)\nu^\lambda) + (\bar{e}^\lambda\gamma^\mu(4s_w^2 - 1 - \gamma^5)e^\lambda) +$$
$$(\bar{d}^\lambda_j\gamma^\mu(\tfrac{4}{3}s_w^2 - 1 - \gamma^5)d^\lambda_j) + (\bar{u}^\lambda_j\gamma^\mu(1 - \tfrac{8}{3}s_w^2 + \gamma^5)u^\lambda_j)] + \tfrac{ig}{2\sqrt{2}}W^+_\mu[(\bar{\nu}^\lambda\gamma^\mu(1+\gamma^5)U^{lep}_{\lambda\kappa}e^\kappa) +$$
$$(\bar{u}^\lambda_j\gamma^\mu(1+\gamma^5)C_{\lambda\kappa}d^\kappa_j)] + \tfrac{ig}{2\sqrt{2}}W^-_\mu[(\bar{e}^\kappa U^{lep}_{\kappa\lambda}\gamma^\mu(1+\gamma^5)\nu^\lambda) + (\bar{d}^\kappa_j C^\dagger_{\kappa\lambda}\gamma^\mu(1+\gamma^5)u^\lambda_j)] +$$
$$\tfrac{ig}{2M\sqrt{2}}\phi^+[-m^\kappa_e(\bar{\nu}^\lambda U^{lep}_{\lambda\kappa}(1-\gamma^5)e^\kappa) + m^\lambda_\nu(\bar{\nu}^\gamma U^{lep}_{\lambda\kappa}(1+\gamma^5)e^\kappa)] + + \tfrac{ig}{2M\sqrt{2}}\phi^-[m^\lambda_e(\bar{e}^\lambda U^{lep\dagger}_{\lambda\kappa}(1+$$
$$\gamma^5)\nu^\kappa) - m^\kappa_\nu(\bar{e}^\lambda U^{lep\dagger}_{\lambda\kappa}(1-\gamma^5)\nu^\kappa)] - \tfrac{g}{2}\tfrac{m^\lambda_\nu}{M}H(\bar{\nu}^\lambda\nu^\lambda) - \tfrac{g}{2}\tfrac{m^\lambda_e}{M}H(\bar{e}^\lambda e^\lambda) + \tfrac{ig}{2}\tfrac{m^\lambda_\nu}{M}\phi^0(\bar{\nu}^\lambda\gamma^5\nu^\lambda) -$$
$$\tfrac{ig}{2}\tfrac{m^\lambda_e}{M}\phi^0(\bar{e}^\lambda\gamma^5 e^\lambda) - \tfrac{1}{4}\bar{\nu}_\lambda M^R_{\lambda\kappa}(1-\lambda^5)\hat{\nu}_\kappa - \tfrac{1}{4}\overline{\bar{\nu}_\lambda M^R_{\lambda\kappa}(1-\lambda^5)\hat{\nu}_\kappa} + \tfrac{ig}{2M\sqrt{2}}\phi^+[-m^\kappa_d(\bar{u}^\lambda_j C_{\lambda\kappa}(1 -$$
$$\lambda^5)d^\kappa_j) + m^\lambda_u(\bar{u}^\lambda_j C_{\lambda\kappa}(1+\lambda^5)d^\kappa_j)] + \tfrac{ig}{2M\sqrt{2}}\phi^-[m^\lambda_d(\bar{d}^\lambda_j C^\dagger_{\lambda\kappa}(1+\gamma^5)u^\kappa_j) - m^\kappa_u(\bar{d}^\lambda_j C^\dagger_{\lambda\kappa}(1 -$$
$$\lambda^5)u^\kappa_j)] - \tfrac{g}{2}\tfrac{m^\lambda_u}{M}H(\bar{u}^\lambda_j u^\lambda_j) - \tfrac{g}{2}\tfrac{m^\lambda_d}{M}H(\bar{d}^\lambda_j d^\lambda_j) + \tfrac{ig}{2}\tfrac{m^\lambda_u}{M}\phi^0(\bar{u}^\lambda_j\gamma^5 u^\lambda_j) - \tfrac{ig}{2}\tfrac{m^\lambda_d}{M}\phi^0(\bar{d}^\lambda_j\gamma^5 d^\lambda_j)$$

Alors en particulier, il y a une erreur[7]. Il y a une erreur. Il y a une erreur quelque part, hein, Brézin ?... Il y a une erreur quelque part.

Édouard Brézin : Il n'y a pas de terme quartique dans ton potentiel de Higgs ?

Alain Connes : Si, si... si, si, si.

Édouard Brézin : Où est-ce qu'il est ?

Alain Connes : Si, si, il y a des termes quartiques dans le potentiel de Higgs. Bien sûr.

Édouard Brézin : Ah, je ne les vois pas...

Alain Connes : Si, si, ils y sont. H^2 ici. Si, si, ils y sont, les termes quartiques.

Si, si, ici, tu vois. $H^2, \varphi^+, \varphi^-$. Ça, c'est un terme quartique de Higgs. D'accord ? Non, non, il n'y a pas de problème.

Il y a des termes qui... Je pourrais te poser des questions. Par exemple, est-ce que tu saurais me dire qu'est-ce que c'est que cette constante ? Ça, je ne l'avais pas trouvée β_H. Est-ce que tu saurais me dire ce que c'est ? Les autres, ce n'est pas difficile.

Mais celle-là, est-ce que tu saurais me dire ce que c'est ? Je suis dur, hein, quand même.

Édouard Brézin : Attends, mais c'est la masse d'huile...

Alain Connes : Non, absolument pas. Non, non, ce n'est pas la masse d'huile. C'est ce qu'on appelle la constante de *tadpole*. C'est la constante de *tadpole*, ce qu'on appelle. C'est le terme linéaire. C'est le terme linéaire qu'on annule en disant que le *tadpole* est nul. D'accord ? D'accord.

Qu'est-ce que c'est que M ? M... D'accord. Dans cette formule, il faut bien voir que, tout de même, dans cette formule, si vous voulez, on a la sommation sur les indices. C'est-à-dire les gluons, par exemple, ici, ils ont un indice de couleur qui est le petit a, et ils ont l'indice du bas.

Donc, je veux dire, on n'a pas développé. Alors, si vous connaissez les termes, vous vous apercevrez que ce n'est pas si compliqué que ça, parce qu'au bout d'un moment, on reconnaît les termes, etc., etc. Ce n'est pas ça, la question.

Ce n'est pas ça, la question. La question, pour un mathématicien, ce n'est pas ça du tout. D'accord ? Ce n'est pas de refaire le trajet en sens inverse.

Le mathématicien, il n'a pas du tout envie de refaire en sens inverse le trajet du physicien. Bien sûr que non. D'accord ? Il a envie de prendre cette formule, bon, et il a envie de la comprendre

[7]Pour retrouver, peut-être, la formule du modèle standard de l'exposé, se reporter à cet article d'Alain Connes sur arxiv https://arxiv.org/pdf/hep-th/0608226.pdf, pages 10 et 11.

sous forme géométrique, qui est autre.

Sinon, justement, il ferait le trajet en sens inverse, c'est tout ce qu'il ferait. Monsieur Kahane.

Jean-Pierre Kahane : Oui, j'ai une question sur les nombres premiers. André Weil considérait que, malgré le succès d'HAdamard et de la Vallée-Poussin, la théorie des nombres premiers n'avait plus rien à voir avec la théorie des fonctions. Il a introduit l'idée que c'était un problème de géométrie algébrique.

Alain Connes : Absolument.

L'auditeur : Et c'est exactement le cadre dans lequel tu as fait ton exposé.

Alain Connes : Tout à fait.

Jean-Pierre Kahane : Il n'empêche... qu'il y a des progrès récents dans la théorie des nombres premiers, qui retournent au point de vue de l'analyse classique, avec la théorie ergodique, avec l'analyse de Fourier, les résultats de Green et Tao, sur les nombres premiers en progression arithmétique.

Quel est ton sentiment sur les modes d'attaque de la théorie des nombres premiers ?

Alain Connes : Disons que mon sentiment est le suivant. Mon sentiment, j'aurais une déception terrible s'il s'avérait qu'un jour, quelqu'un démontre, par exemple cette hypothèse de Riemann, par des moyens, comment dire, qui ne débouchent pas sur une nouvelle théorie. C'est-à-dire que pour moi, l'intérêt d'un problème mathématique n'est pas de savoir si oui ou non, c'est vrai.

Puisqu'au fond, la majorité d'entre nous sommes convaincus que la fonction ζ de Riemann a les zéros où il faut, et un physicien dirait que l'hypothèse de Riemann est vraie. Donc, je vais dire, le problème n'est pas tellement de savoir si le problème est vrai ou pas, non, pour moi, l'intérêt d'un problème mathématique, justement, c'est comme force motrice pour développer de nouvelles théories. Or, s'il s'avérait que, bon, on arrive à le résoudre par un biais, etc., et qui ne débouche pas sur une nouvelle théorie, mais je ne prétends pas du tout que ce que tu dis, si tu veux, si par exemple cette théorie, c'était une théorie ergodique, convenable, un peu dans le sens de Furstenberg, etc., ce serait merveilleux, bien sûr, tout le monde applaudirait.

Mais ce que j'espère, si tu veux, c'est que ma familiarité avec le problème, j'avais d'autres transparents, etc., me fait voir qu'il y a un espace. Bon, en fait, à nouveau, c'est une espèce d'espace non-commutatif, etc., qui donne, en fait, à la formule explicite, la valeur d'une formule de trace. C'est vraiment une formule de trace.

Donc, pour moi, en fait, un problème comme ça est un problème qui est une motivation extraordinaire pour développer la géométrie, découvrir de nouvelles choses, et justement, j'espère qu'à l'occasion de ce problème de la conjecture de Riemann, en fait, on découvrira la vraie géométrie de la droite. Parce qu'il s'agit là du corps des nombres rationnels. Donc, ça montre l'étendue de

notre ignorance.

Je veux dire, autant on sait quelque chose à propos des corps finis et des corps de fonctions, etc., autant on a une ignorance incroyable à propos du corps des rationnels. Donc, qu'est-ce que ça veut dire ? Ça veut dire, bon, eh bien, on écrit 36 traités, etc., mais en fait, on ne comprend pas même la chose la plus simple, d'accord ? Puisqu'on n'arrive pas à résoudre ce problème. Et ce que j'espère, c'est qu'on ne le résoudra pas de biais, d'accord ? C'est-à-dire qu'on découvrira les concepts qu'il faut justement, au moment, et à propos de cette résolution.

Édouard Brézin : Est-ce qu'il y a d'autres questions ? Oui, Roger Balian.

Roger Balian : Le modèle standard contient, je ne sais pas exactement combien, 15, 16...
Alain Connes : 19.

Roger Balian : ...paramètres indépendants. Est-ce que la vision géométrique que tu mets dessous risque de les réduire ?

Alain Connes : D'accord. Alors, si tu veux, la manière dont les paramètres... D'abord, il y a deux types de paramètres. L'essentiel des paramètres dont tu parles interviennent dans la métrique sur l'espace fini. C'est-à-dire qu'en gros, si tu veux, la géométrie, c'est la géométrie standard sur l'espace ordinaire.

On a cet espace fini. Cet espace fini a une géométrie qui est donnée par son opérateur de Dirac qui, ici, est la matrice de Yukawa. La matrice de Yukawa ne contient pas tous, mais la plupart, des paramètres du modèle standard.

D'accord ? Et en particulier, elle ne contient pas, par exemple, le couplage quartique du Higgs, des choses comme ça. Alors, ce que donne le modèle, il donne, entre guillemets, parce que ce n'est pas vraiment une prédiction puisque, justement, comme le disait très bien Brézin, on ne sait pas du tout ce qu'il va advenir à des énergies plus grandes. Mais si on l'extrapole, ce qui est idiot, je veux dire, si on l'extrapole à l'énergie d'unification, eh bien, il donne une valeur pour la constante de couplage quartique du Higgs. Donc, il donne, en gros, une valeur de la masse du Higgs de l'ordre de 160 GeV, ou quelque chose comme ça.

Mais ce n'est pas une prédiction. Et ce n'est pas une prédiction parce que, justement, c'est stupide de penser que rien ne va se produire lorsqu'on va à des énergies plus grandes. D'accord ? Donc, ça réduit un peu.

Par exemple, ça donne le même angle de Weinberg. Ici, on avait les constantes C_w et S_w qui sont le cosinus et le sinus de l'angle de Weinberg. Ça donne le même angle de Weinberg que pour l'unification de la SU(5), bon.

Donc, ça donne un certain nombre de choses, qui ne sont pas contradictoires, qui ne sont pas... D'accord. Mais ce qu'il faut bien voir, c'est exactement comme le disait Brézin. C'est un modèle effectif de la géométrie de l'espace-temps.

Il ne faut pas y voir plus. Ce n'est pas du tout une réponse à des choses faramineuses, etc. Pas du tout.

C'est un modèle qui consiste à dire qu'on a une géométrie qui est plus facile, plus appropriée, etc. Mais on va regarder ce que ça donne. Et ça donne, effectivement, que les paramètres libres du modèle standard, tels que la matrice de couplage de Yukawa ou de Kobayashi-Maskawa, etc., eh bien, elles sont contenues dans la partie géométrique, d'accord ? Donc, elles donnent la géométrie de l'espace fini. D'accord ?

Édouard Brézin : Très bien. Je peux t'interroger sur les nombres premiers ?

Alain Connes : Bien sûr.

Édouard Brézin : Il y a cette infinité de zéros de la fonction ζ.

Alain Connes : Oui.

Édouard Brézin : Apparemment, expérimentalement, ils sont donnés par des valeurs propres de matrice aléatoire.

Alain Connes : Tout à fait.

Édouard Brézin : Est-ce que tu as une... Est-ce que ça te paraît une propriété intéressante ?

Alain Connes : Bien sûr. C'est une propriété incroyablement intéressante. J'avais des transparents plus loin, etc., qui consistaient justement à comparer... Oh, je me demande... Tu me permets de...

Édouard Brézin : Oui, oui. D'accord.

Alain Connes : Bon, j'avais un transparent après qui consistait justement à partir de là.

Alors, il y a une chose qui est effectivement merveilleuse qui se produit, c'est que les gens n'ont pas pu ne pas être frappés par l'analogie, c'est exactement ce que vient de dire Brézin, entre le nombre de valeurs propres d'un opérateur hamiltonien plus petit que E, d'accord, et le nombre de zéros de la fonction ζ, qui est tracée ici, c'est la fonction d'escalier, plus petit qu'une énergie E donnée.

D'accord. Mais alors, les gens ont été arrêtés pendant très longtemps par le fait que si on regarde la partie oscillatoire, c'est-à-dire une partie moyenne que Riemann avait calculée comme étant

$$\frac{E}{2\pi}\left(\log\frac{E}{2\pi}-1\right)+\frac{7}{8}+o(1).$$

D'accord. Et les gens ont été arrêtés pendant très longtemps par le fait que si on compare le cas de Riemann avec le cas des systèmes hamiltoniens, il y a un signe qui cloche. Il y a le signe moins.

D'accord.

Alors, ça, ça a été résolu en partant précisément du fait qu'en physique, il y a deux types de spectres.

Il y a ce qu'on appelle les spectres d'émission qui sont les raies blanches sur un fond noir. D'accord. Il y a les spectres, comme le spectre de Fraunhofer, qu'on voit lorsqu'on regarde les rayons du soleil qui sont ce qu'on appelle les spectres d'absorption.

Donc, en fait, la réalisation spectrale des zéros de ζ, c'est une réalisation par spectre d'absorption. Et alors, une des choses qui est remarquable, c'est qu'il y a un espace, effectivement. Bon, je n'ai pas voulu en parler.

C'est un espace qu'on appelle *l'espace des classes d'adèles*. Et c'est un espace qui contient justement les orbites, exactement comme les orbites du Frobenius dans le cas des nombres premiers. Mais si on regarde cet espace, eh bien, on trouve exactement le calcul de Riemann avec $\frac{E}{2\pi}\left(\log\frac{E}{2pi}-1\right)$ par un calcul de mécanique quantique.

D'accord. Et avec un spectre d'absorption. C'est-à-dire que ce qu'on trouve, c'est qu'on a la lumière blanche moins des raies spectrales qui ont été absorbées.

Si on fait le calcul de manière plus précise, on trouve le $\frac{7}{8}$ et le petit $o(1)$, exactement comme dans Riemann. D'accord. Donc, en fait, on commence à avoir... Alors, bien sûr, il y a bien d'autres résultats.

Je veux dire, il y a toutes sortes de gens qui ont travaillé sur les matrices aléatoires, la correspondance, etc., avec ζ. Mais c'est une des choses qui sont extrêmement fascinantes. Justement, c'est le fait qu'il y a cette comparaison qui n'est pas du tout triviale, qui n'est pas du tout évidente puisqu'il y avait énormément de gens qui avaient essayé d'écrire, justement, la formule explicite de Riemann comme une formule de trace.

La raison pour laquelle ça ne marchait pas, c'est ce signe mois. D'accord ? On pourrait parler pendant des heures là-dessus. Mais ça bouge.

Édouard Brézin : Je ne vois plus de mains qui se lèvent. Si, monsieur Tits ?

Jacques Tits : Tu as fait allusion à une formule de Birkhoff. Est-ce que tu peux dire de quoi il s'agit ?

Alain Connes : Alors, la formule de Birkhoff, c'est la formule qui, disons, lorsqu'on regarde un fibré holomorphe sur la sphère, d'accord, eh bien, on peut se dire qu'on peut voir un fibré holomorphe sur la sphère comme étant obtenu en prenant un fibré trivial en haut et un fibré trivial en bas, et en les recollant.

Et on recolle ces fibrés par une application qui va d'un cercle vers le groupe GL_n. D'accord ? Alors,

la décomposition de Birkhoff consiste à faire le chemin inverse. C'est-à-dire, lorsqu'on vous donne une application d'un cercle, qui est un hémisphère, par exemple, vers le groupe GL_n, ça consiste à écrire cette application comme le rapport entre une fonction qui est holomorphe dans l'hémisphère du bas et une fonction qui est holomorphe dans l'hémisphère du haut, d'accord ?

D'accord ? Et alors, ce qui est étonnant, c'est que, dans le cas de $\mathrm{GL}_n(\mathbb{C})$, ce n'est pas toujours possible. C'est la théorie de Grothendieck-Birkhoff, etc., des fibrés holomorphes sur la sphère qui ont des obstructions topologiques, etc. Mais lorsqu'on regarde des groupes qui sont des groupes comme le groupe des graphes de Feynman, des groupes unipotents, c'est toujours possible et c'est donné par une formule récursive et la merveille, c'est que cette formule récursive, c'est exactement la formule de BPHZ, de Bogoliubov, Parasiuk, Hepp et Zimmermann.

C'est exactement identique à ça.

Jacques Tits : En fait, c'est ce que je pensais, c'est une formule tout à fait analogue à une formule de double classe.

Alain Connes : Oui, c'est ça.

Jacques Tits : On transforme la grosse cellule d'un côté en la grosse cellule de l'autre côté.

Alain Connes : Oui, c'est exactement ça, c'est tout à fait ça.

Édouard Brézin : Bien, je crois qu'il nous reste à remercier Alain Connes. Je crois que c'était une très belle illustration de la puissance des mathématiques.

Conférence d'Alain Connes "*Évariste Galois et la théorie de l'ambiguïté*", à l'Académie des Sciences, dans le cadre du Colloque pour le bicentenaire de la naissance de Galois (29 novembre 2011).

Le Président de séance : Bien, mesdames, messieurs, nous avons à l'évidence une séance exceptionnelle, d'ailleurs, une audience exceptionnelle, mais pour un homme exceptionnel, dont la vie, exceptionnellement courte, a été exceptionnellement productive. Nous avons la chance d'avoir Alain Connes, qui va nous parler d'un aspect particulier d'Évariste Galois, qui est la relation que Galois a entretenue avec les académiciens des sciences à l'époque. Alain Connes, vous avez la parole.

Alain Connes : En fait, mon exposé aura deux parties. Dans la première partie, j'expliquerai, si vous voulez, effectivement les relations très complexes, beaucoup plus complexes qu'on ne le dit, entre Évariste Galois et les académiciens de son époque. Et dans la deuxième partie, j'essaierai de vous expliquer, de la manière la plus simple possible, ce qu'est la théorie de l'ambiguïté.

Donc, je commencerai par vous montrer un portrait bien connu d'Évariste Galois. Et ensuite, on ira très, très rapidement à travers une chronologie que je n'utiliserai que quand j'en aurai besoin, parce que, si vous voulez, je vous décrirai en gros ce qui s'est passé pendant ces trois années, qui marquent la fin de la vie de Galois. Et donc, je ne reviendrai dans les détails de la chronologie qu'occasionnellement.

Et donc, vous m'excuserez si je passe très vite sur cette chronologie. Après, on reprendra le fil des événements de manière beaucoup plus lente. Donc, la chronologie, évidemment, Galois naît il y a 200 ans, le 25 octobre 1811.

La première date marquante, c'est en avril 1829, c'est la mort d'Abel, parce qu'on verra que les destins d'Abel et de Galois sont incroyablement reliés l'un à l'autre. À la même époque, le 25 mai et le 1er juin, Cauchy présente les premiers travaux de Galois à l'Académie. Cette même année, en juillet, le père de Galois se suicide.

Galois échoue pour la deuxième fois à Polytechnique, mais il est reçu à l'ENS, ce qui s'appelait à l'époque l'École préparatoire. Le 18 janvier 1830, il y a une lettre de Cauchy très importante que je vous montrerai. Et en février 1830, Cauchy remet au Secrétaire perpétuel de l'Institut, qui était Joseph Fourier, le mémoire de Galois sur les conditions de résolubilité des équations par radicaux.

Et il lui demande, justement, de faire concourir ce Mémoire pour le Grand Prix des Sciences mathématiques. Le 28 juillet 1830, le Grand Prix des sciences mathématiques de l'Académie est attribué à Abel et Jacobi. La même année, en juillet, c'est un événement politique très important, les Trois Glorieuses, que vous connaissez tous, mais qui fait que Cauchy part.

Donc Cauchy part de France pour de nombreuses années. Il va à Turin. En janvier 1831, Galois est exclu de l'École Normale.

Le 13 janvier 1831, il inaugure, dans une librairie au 5 rue de la Sorbonne, on y reviendra, avec 30 élèves, un cours privé d'Algèbre supérieure, visant explicitement à suppléer les carences de

l'enseignement public. La même année, en 1831, Galois réécrit et soumet à l'Académie, sur les conseils de Poisson (Poisson faisait partie du jury qui a exclu Galois de l'École Normale), son mémoire perdu relatif aux conditions de résolubilité des équations algébriques par radicaux. Le 9 mai, il est arrêté. Il y a un banquet bien connu, qui était donné pour l'acquittement de certains républicains, et Galois avait levé son verre à Louis-Philippe, mais en tenant un couteau à la main. Le 15 juin, il est acquitté. Le 4 juillet 1831, il reçoit le rapport négatif de Poisson sur ses travaux. On le verra, ce rapport, je l'ai dans les documents. Et bon, ensuite, la fin, vous la connaissez, Galois passe de nombreux mois en prison. Il est arrêté le 14 juillet, peu de temps après avoir reçu le rapport de Poisson, il est arrêté à la tête d'une manifestation. Et cette fois, il est arrêté pour port d'arme illégal. Il n'est pas jugé par un jury (il y avait un jury populaire), donc, il reste en prison très, très longtemps. Il est enfermé à la prison Sainte-Pélagie. Il en ressort le 16 mars, mais simplement parce qu'il y a le choléra dans Paris.

Et il est libéré, mais pas vraiment : il est dans une maison de santé privée. Et enfin, bon, il y a le mercredi 30 mai qui est le jour du duel et il meurt le lendemain.

Alors, évidemment, ça, c'est extrêmement rapide, c'est simplement pour vous donner quelques repères. Et on y reviendra quand on aura des problèmes de date. Donc, un personnage central, c'est le personnage d'Abel qui meurt le 5 avril 1829, alors que Galois a 17 ans.

Et Abel avait eu déjà des relations assez complexes et assez compliquées avec Cauchy. Et je vais vous montrer une lettre d'Abel dans laquelle il parle de Cauchy. Je m'inspire là, bien sûr, d'un merveilleux article d'*Histoire des mathématiques* de René Taton, sur lequel je reviendrai à maintes reprises.

Donc, Abel écrit à propos d'Augustin Cauchy la chose suivante :

> *"Cauchy est fou et il est impossible d'avoir affaire avec lui. Pourtant, c'est lui qui, à présent, est le mathématicien qui sait comment doivent être traitées les mathématiques. Ses travaux sont excellents, mais il écrit obscurément.*
>
> *D'abord, je ne comprenais presque rien à ses œuvres. Maintenant, j'y arrive mieux. Cauchy est infiniment catholique et bigot. Chose bien singulière pour un mathématicien ! D'ailleurs, il est le seul qui travaille les mathématiques pures. Poisson, Fourier, Ampère, etc. s'occupaient exclusivement de magnétisme et d'autres parties de la physique."*

Donc ça, c'est une lettre qu'Abel avait écrite en 1826. Il est bien connu que Cauchy et l'Académie ont pris du temps pour reconnaître les travaux d'Abel, mais ça a été fait.

Donc ça, c'est un portrait de Galois qui a été fait, je pense, par Augustin Chevalier, de mémoire, après la disparition de Galois. Mais qui dit beaucoup de choses sur Galois, en fait. Donc la relation entre Galois et Abel est très intéressante.

Alors voilà ce que Galois a écrit. En gros, si vous voulez, ce qui s'est passé, c'est que Galois, en 1829, avait donné deux manuscrits à l'Académie. Et après la mort d'Abel, il a appris que ses

travaux étaient largement anticipés par ceux d'Abel.

Et ça lui a donné un coup, évidemment. Mais bon, voilà ce qu'il dit après[1].

> *"Dans tous les cas, il me serait aisé de prouver que j'ignorais même le nom d'Abel quand j'ai présenté à l'Institut, mes premières recherches sur la théorie des équations, et que la solution d'Abel n'aurait pu paraître avant la mienne.*

Donc ça, c'est écrit à la prison, quand il était à la prison Sainte-Pélagie, en décembre 1831, donc la dernière année de sa vie. Cette note a pour but essentiel d'affirmer l'indépendance des travaux de Galois par rapport à ceux d'Abel. Galois qui connaissait alors une lettre qu'Abel avait envoyée à Legendre, il y avait une très longue correspondance entre Abel et Legendre, le 25 novembre 1828. Et voilà ce que dit Galois. Il dit :

> *"Mais la mort anticipée de ce géomètre, ayant privé la science des recherches promises dans cette lettre, il n'en était pas moins nécessaire de donner la solution d'un problème qu'il m'est bien pénible de posséder, puisque je dois cette possession à une des plus grandes pertes qu'aura faite la science."*

Donc il n'y avait pas du tout d'antipathie ou quoi que ce soit, il n'y avait même pas de rivalité. En gros, si vous voulez, Abel disparaît exactement où Galois commence à exister dans le paysage mathématique. Donc voilà Cauchy.

Il est né en 1789, donc quand Galois naît, il avait déjà 22 ans. Je veux dire, c'était un mathématicien extraordinaire. Et la relation entre Galois et Cauchy est extrêmement intéressante. Comme je vous l'ai dit, Cauchy est parti de France en 1830. Et à ce moment-là, il n'a plus eu de contact avec Galois. Donc les meilleurs renseignements que l'on ait sur les relations entre Cauchy et Galois, qui bien souvent sont présentées de manière complètement caricaturale, c'est à travers un article de René Taton, un grand historien des mathématiques, qui est mort en 2004, et qui nous dit la chose suivante.

Il nous dit :

> "*Parmi les très rares renseignements qu'elles nous apportent à ce sujet, les archives de l'Académie des sciences révèlent que Galois eut le privilège de voir ses premiers travaux* [a] *présentés devant l'Académie au cours des séances des 25 mai et 1*er *juin 1829* [b] *par un juge aussi sévère que compétent, Cauchy. Bien qu'aucune précision ne nous soit parvenue sur ce point, l'acceptation par le grand analyste de cette tâche de présentation prouve que le jeune auteur de ces mémoires avait réussi à le convaincre du sérieux, de l'importance et de l'originalité de ses recherches."*

[a] Galois avait 17 ans.

[b] En mai-juin 1829, Galois avait 17 ans puisqu'il est né en octobre.

[1] en 1829.

Alors, un peu après, pendant le début de l'été 1829, le mémoire d'Abel sur les équations algébriques est paru de manière posthume et bien sûr, Cauchy a constaté qu'une bonne partie des résultats obtenus par Galois étaient absorbés par le mémoire d'Abel.

Donc, il était de son devoir d'essayer d'atténuer la déception de Galois, en l'encourageant à sauver la part la plus originale de son travail. On verra qu'il y avait une part extrêmement originale, même à cette époque-là.

> "*Lorsqu'il se décida au début de 1830 à rédiger son rapport sur les mémoires de Galois, on peut penser que dans cette circonstance, Cauchy songea beaucoup moins à remplir une obligation académique qu'à apporter d'utiles conseils au jeune mathématicien. Toujours est-il que ce rapport fut rédigé pour être lu à la séance de l'Académie du 18 janvier 1830 et que seule une indisposition empêcha Cauchy de le présenter.*"

Alors, j'espère qu'on va voir la lettre. J'ai écrit le texte en clair.

C'est une lettre d'excuse :

> "*Monsieur le Président,*
>
> *Je me proposais de présenter aujourd'hui à l'Académie le rapport sur les travaux du jeune Galois, un mémoire sur la détermination analytique des racines primitives dans lequel on fait voir comment on peut réduire cette détermination à la résolution d'équations numériques, etc.*
>
> *Retenu chez moi par une indisposition, je regrette de ne pouvoir assister à la séance de ce jour et je vous prie de bien vouloir inscrire mon nom sur l'ordre du jour de la séance suivante. Agréez, je vous prie, l'hommage...*"

Donc, c'est une lettre de Cauchy qu'on retrouve dans les archives de l'Académie et qui montre que, bien sûr, Cauchy n'ignorait absolument pas Galois, il y avait des relations très, très fortes entre Cauchy et Galois à cette époque-là. Il y a cette lettre. Et en fait, voilà ce que dit René Taton.

Il dit :

> "*Du fait du report annoncé de ce rapport, donc le rapport de Cauchy sur Galois à la séance suivante, celle du 25 janvier 1830, nous* (c'est René Taton) *avons examiné avec un soin tout particulier les différentes pièces concernant cette séance : dossier, primitif, registre de procès-verbaux. Mais alors que ces divers documents montrent que Cauchy, effectivement présent, y présenta bien son mémoire annoncé* "Sur la détermination des racines primitives dans la théorie des nombres", *rien n'y rappelle le premier point évoqué dans sa lettre du 18 janvier, le "Rapport sur les travaux du jeune Galois*".

L'étude des procès-verbaux des séances de l'Académie révèle que, non seulement ce rapport annoncé par écrit pour la séance du 25 janvier, n'y a pas été présenté, mais qu'aucune allusion n'y a plus été faite au cours des séances suivantes. Le fait que Galois ne se soit jamais plaint de la négligence de Cauchy en cette circonstance, alors qu'il plaçait tous ses espoirs en un jugement favorable de l'Académie, semble montrer que l'annulation de ce rapport est intervenue avec son accord. Il reste alors à expliquer ce brusque changement d'attitude des deux acteurs de cette mystérieuse affaire."

La thèse de René Taton, et je pense que c'est quelque chose qui est parfaitement plausible, est :

"*La confrontation attentive des quelques éléments d'information permet de formuler à ce sujet une hypothèse qui paraît vraisemblable.*"

Son hypothèse, c'est que Cauchy avait demandé à Galois de réécrire son manuscrit, de manière plus détaillée, de telle sorte qu'il soit présenté au Grand Prix de l'Académie. Quel Grand Prix de l'Académie ? Il y avait un concours. En fait, ce n'était pas un Grand Prix, c'était un concours. Ça s'appelait un concours à l'époque.

C'était un concours qui était formulé de la manière suivante.

"*Le prix sera décerné à celui des ouvrages, ou manuscrits, ou imprimés, qui présentera l'application la plus importante des théories mathématiques, soit à la physique générale, soit à l'astronomie, ou qui contiendra une découverte analytique très remarquable.*".

Donc, ce Grand Prix se distinguait également par le fait que les travaux publiés entre le 1er janvier 1828 et le 1er janvier 1830, séparément ou dans des recueils scientifiques, pouvaient être pris en considération par le jury sans que leur auteur ait fait acte de candidature, concurrentement avec les ouvrages ou mémoires qui étaient déposés au secrétariat de l'Institut avant le 1er mars 1830.

Donc, en fait, ce Grand Prix a permis à l'Académie de réparer l'injustice qui avait été faite à Abel dans les années précédentes, la lenteur du processus de jugement des écrits d'Abel, le fait qu'ils avaient été reconnus de manière tardive. Et en fait, donc, le Grand Prix a été attribué à Abel conjointement à Jacobi. Et c'était évidemment parfaitement mérité : si on regarde la liste des candidats, c'est une liste époustouflante. Donc, ce que pense René Taton : il pense, comme je vous l'ai dit, que Cauchy persuada Galois de rédiger son mémoire pour le Grand Prix de mathématiques, un mémoire de synthèse qui réunissait l'ensemble de ses contributions, en même temps que les mémoires de 1829. Donc, évidemment, les espoirs que Galois plaçait dans le concours du Grand Prix de l'Académie devaient se trouver cruellement déçus.

Il ne pouvait pas raisonnablement ressentir comme une injustice, bien sûr, le fait que le 28 juin, le prix ait été accordé à Abel et à Jacobi. Mais par contre, là où il a commencé à devenir un peu paranoïaque, on peut dire, c'est qu'il a appris à ce moment-là que son manuscrit avait été perdu. Alors, la raison est complexe.

La raison est que Cauchy ne faisait pas partie des examinateurs, pour le Grand Prix, il n'en faisait pas partie. Le secrétaire perpétuel, c'était Joseph Fourier.

Et Joseph Fourier est mort en mai de cette année-là. Donc, il a disparu avant même que le Grand Prix ait été attribué. Et, en fait, les recherches montrent que, bien sûr, l'explication qui a été donnée à Galois ne tenait pas. On lit :

> *"C'est une chose bien simple", aurait repondu Cuvier à une réclamation de Galois..."*

Le mémoire a été perdu à la mort de Fourier, qui était chargé de l'examiner. Donc, c'était effectivement Fourier qui était chargé de présenter les travaux de Galois pour le Grand Prix. Ce n'était pas Cauchy.

> *"...et l'on conçoit, bien sûr, que ce nouveau malheur,...*"

(le fait que son manuscrit ait été perdu, à l'époque, il n'y avait pas beaucoup de photocopieuses !, donc, le fait que son manuscrit ait été perdu),

> *"...ait été vécu par lui comme presque une attaque personnelle.*"

Et en fait, les recherches montrent qu'il a été perdu par le Secrétariat de l'académie. Donc, Galois l'a pris comme étant une injustice terrible.

Et voilà ce que dit Galois. Voilà ce qu'il dit dans ses écrits.

> "*Il suffira de dire que mon mémoire sur la théorie des équations a été déposé en substance à l'Académie des sciences en février 183...0"*

(c'était l'année du concours, c'était l'année où Cauchy lui avait demandé de déposer son mémoire),

> *"...que des extraits en avaient été envoyés en 1829..."*

(donc, ce sont les deux articles qu'il avait déposés au printemps de 1829, quand il avait 17 ans).

> *"...qu'aucun rapport ne s'en est suivi et qu'il m'a été impossible de revoir les manuscrits.*"

Donc, il lui a été impossible de revoir les manuscrits, effectivement, parce qu'ils ont été perdus à la mort de Fourier. Il devait y avoir un désordre dans tous les papiers. Et son manuscrit a été perdu.

Alors, voilà ce que dit Auguste Chevalier, qui était un ami très, très proche de Galois, auquel Galois se confiait. Voilà ce qu'il dit à ce moment-là :

> "*Le peu d'attention donnée par l'Institut au premier travail soumis à son jugement par Galois commença pour lui des douleurs qui, jusqu'à sa mort, devaient se succéder de plus en plus vives.*"

Donc, il avait un sentiment d'injustice.

> "*Une telle indifférence aurait suffi pour guérir de toute ardeur scientifique. Mais il n'en fut point abattu. Une puissante nature le poussait en avant.*"

Alors, le deuxième épisode, c'est donc à ce moment-là, en 1830. Donc, il y a les Trois Glorieuses. Galois est enfermé à l'École Normale. On ne laisse pas les élèves de l'École Normale, enfin, de l'École Préparatoire, sortir, alors qu'on laisse sortir ceux de l'École Polytechnique. Enfin, on ne les laisse pas sortir, mais ils font le mur. Ils vont sur les barricades.

Et à partir de ce moment-là, Galois éprouve une aversion pour le Directeur de l'École Normale de l'époque. Et il fait tant et si bien que finalement, il finit par se faire renvoyer de l'École Normale. Alors, donc, il est renvoyé de l'École Normale fin décembre, début janvier de 1831, de l'année suivante.

Et la personne, d'abord, qui signe l'arrêt de renvoi de Galois de l'École Normale, c'est un certain Victor Cousin. Et la rue Victor Cousin est la rue dans laquelle Galois a donné ses cours après avoir été renvoyé de l'École Normale. Il a donné son cours d'algèbre, avec 35 élèves.

Il n'y a pas dans Paris de rue Galois. Il y en a une qui est en dehors du périphérique. Et je pense que ce serait une bonne idée qu'au moins, qu'on ne change pas le nom de la rue, ce n'est pas la peine, mais qu'il y ait une plaque dans la rue de la Sorbonne, la rue Victor Cousin, qui explique clairement que Galois a donné ses cours à cet endroit-là après s'être fait renvoyer de l'École Normale.

Alors, le rapport avec Poisson est très intéressant parce que Poisson, qui faisait partie du comité (ce n'était pas un jury) qui a renvoyé Galois de l'École Normale, a sûrement parlé à Galois en privé, et lui a dit qu'il fallait qu'il redonne son manuscrit pour qu'il soit examiné par l'Académie. Je vous rappelle que Cauchy n'était plus présent. Cauchy était à Turin, donc Galois n'avait plus de protecteur direct. Il n'avait pas de personne à laquelle il pouvait s'adresser à l'Académie.

Et je pense qu'il a parlé à Poisson. Et donc, à ce moment-là, il a donné à Poisson son manuscrit. Et voilà, je vais vous lire le rapport. C'est un rapport de référé qui a été lu à la séance du 11 juillet 1831, cette même année, donc peut-être quelques six mois après, et qui est le rapport que Poisson et Lacroix ont rédigé sur le Mémoire de Galois.

Donc, ce rapport est extrêmement bien fait. Je veux dire, ce n'est pas du tout une négligence. C'est un rapport qui est extrêmement précis et bien argumenté.

Donc, voilà ce que dit Poisson :

"*L'auteur entend par équation irréductible une équation dont les coefficients sont rationnels* (donc on en verra des dizaines), *et qui ne peut se décomposer en d'autres équations, qui aient aussi leurs coefficients rationnels*" (parce que si vous avez une équation qui s'écrit comme produit, le polynôme s'écrit comme produit de plusieurs polynômes, il suffit de regarder chacun des polynômes).

"D'après sa proposition, l'équation générale..."

Alors, quelle est la proposition de Galois ? Il dit que

"pour qu'une équation irréductible de degré premier soit soluble par radicaux, il faut et il suffit que deux quelconques de ses racines étant connues, les autres s'en déduisent rationnellement".

Alors, pour les mathématiciens, ça, ça veut dire que l'extension galoisienne correspondante est engendrée par deux quelconques des racines, distinctes, de l'équation. On verra ce que ça signifie au niveau théorie des groupes.

Donc, c'est ça le critère que Galois entendait prouver pour les équations de degré premier.

"Alors, donc, l'auteur entend par équation irréductible, on l'a vu. D'après sa proposition..."

Donc, ce qu'il propose, évidemment, si vous prenez une équation de degré 3, 3 est premier, et si vous connaissez deux racines, vous connaissez la troisième, puisque vous avez, par exemple, la somme ou le produit qui est connu. Donc, ça, c'est une remarque triviale. Maintenant, on vient à un point plus embêtant.

Donc, il dit :

"Des notes trouvées dans les papiers d'Abel, qui ont été imprimées après sa mort dans le journal de Crelle, tome V, page 345, renferment une proposition analogue à celle de M. Galois, dont voici l'énoncé. Si trois racines d'une équation quelconque irréductible, dont le degré est un nombre premier, sont liées entre elles de sorte que l'une de ces racines puisse être exprimée rationnellement au moyen des deux autres, l'équation dont il s'agit sera toujours résoluble à l'aide de radicaux".

Alors, cet énoncé diffère de celui de Galois en ce que le géomètre norvégien ne dit pas que la condition dont il s'agit soit nécessaire, mais seulement qu'elle suffit pour que l'équation soit résoluble.

"Et il ne semble pas qu'il la regardât comme indispensable, car on trouve dans les notes citées une autre proposition relative à la résolution d'une classe nombreuse d'équations qui pourraient bien ne pas remplir cette condition. Il ne paraît pas non plus que ce soit à cette proposition qu'il ait fait allusion dans ce passage d'une lettre écrite à M. Legendre et publiée après la mort d'Abel dans le journal de Crelle, dans laquelle il dit", ça c'est Abel qui parle, *"J'ai été assez heureux, dit-il, de trouver une règle sûre à l'aide de laquelle on pourra reconnaître si une équation quelconque proposée est résoluble ou non à l'aide de radicaux. Un corollaire de ma théorie fait voir que généralement il est impossible de résoudre des équations supérieures au quatrième degré."*

"Alors nous ignorons si Abel a laissé un manuscrit de cette théorie, elle n'a point encore été imprimée, non plus que la démonstration du théorème analogue à celui qui fait l'objet de ce rapport et qui appartiendrait entièrement à Galois, s'il parvenait à l'établir d'une manière satisfaisante. Toutefois, on doit remarquer qu'il ne renferme pas, comme le titre du Mémoire le promettait, la condition de résolubilité des équations par radicaux. Car, en admettant comme vraie la proposition de Galois, on n'en serait guère plus avancé pour savoir si une équation donnée, dont le degré est un nombre premier, est résoluble ou non par des radicaux".

"Puisqu'il faudrait d'abord s'assurer si cette équation est irréductible". Ça, c'est vraiment du pinaillage, parce que s'assurer d'abord si l'équation est irréductible, ce n'est pas très difficile. *"Et ensuite, si l'une de ses racines peut s'exprimer en fonction rationnelle des deux autres".*

Ça, c'est beaucoup plus difficile.

"La condition de résolubilité, si elle existe (alors là Poisson est vraiment très terre à terre), il dit, *devrait être un caractère extérieur que l'on pût vérifier à l'inspection des coefficients d'une équation donnée, ou, tout au plus, en résolvant d'autres équations d'un degré moins élevé que celui de la proposée.".*

On verra qu'il y a toute une histoire ultérieure derrière ça qui est très très intéressante. *"Quoi qu'il en soit, nous avons fait tous nos efforts pour comprendre la démonstration de Galois. Ses raisonnements ne sont ni assez clairs, ni assez développés pour que nous ayons pu juger de leur exactitude et nous ne serions pas en état d'en donner une idée dans son rapport".*

"L'auteur annonce que la proposition qui fait l'objet spécial de son Mémoire est une partie d'une théorie générale susceptible de beaucoup d'autres applications. Souvent, il arrive que les différentes parties d'une théorie, en s'éclairant mutuellement, sont plus faciles à saisir dans leur ensemble qu'isolément. On peut donc attendre que l'auteur ait publié en entier son travail pour se former une opinion définitive mais dans l'état où est maintenant la partie qu'il a soumise à l'Académie, nous ne ne pouvons pas vous proposer d'y donner votre approbation".

Alors, je vais simplement vous raconter une anecdote. C'est que quand Galois a reçu ce rapport, c'était le 4 juillet 1831, il a écrit en dessous "Ô Chérubins !". Parce que... Pardon, ce qu'il a écrit en dessous de ce rapport quand il a eu le rapport de Poisson le 4 juillet, il a écrit en dessous "Ô Chérubins". C'est-à-dire, vous n'avez pas bien compris, c'est-à-dire il faut bien admettre que la manière dont Galois a écrit est extrêmement elliptique. Mais, on verra aussi en lisant un peu en détail à quel point il va exactement au point le plus profond.

Donc, ce qui est vrai, c'est que, par exemple, si on lit ce que Galois a écrit pour démontrer ce théorème qu'une équation de degré premier est résoluble par radicaux, si et seulement si toute racine est fonction rationnelle des deux autres, c'est très difficile à comprendre. Par contre, il avait la démonstration de manière complète, ça c'est clair. En fait, ce qui est très amusant aussi, c'est que pour démontrer ce théorème, il faut utiliser un résultat de Cauchy que Galois utilise, qui est que si on prend un groupe fini dont l'ordre est divisible par un nombre premier qui agit sur un ensemble à p éléments, il contient une permutation cyclique d'ordre p. En fait, il connaissait aussi la théorie de Sylow.

Si on regarde ses papiers, il connaissait aussi le fait que ça contient un groupe d'ordre p^n, où p^n est la plus grande puissance qui permet de diviser l'ordre du groupe. Alors en fait, donc, la situation était très mauvaise à ce moment-là. Comme je l'ai dit, quelques jours après avoir reçu le rapport de Poisson, Galois devait être vraiment découragé dans un état assez instable, et c'est à ce moment-là qu'il a été arrêté à la tête de la manifestation et qu'il s'est retrouvé à la prison pour pratiquement le reste de sa vie.

Donc les choses auraient pu en rester là, et puis il y a un miracle, et ce miracle c'est Joseph Liouville, qui est aussi un membre de l'Académie, et qui est un contemporain de Galois, ça il faut le savoir, c'est-à-dire Galois est né en 1811, vous voyez, Liouville est né en 1809, donc il est exactement de la même génération que Galois. Et la résurrection de Galois, de ses Œuvres, on peut le dire, ce serait trop facile de dire que, je veux dire que ça aurait été trouvé de toute manière, parce qu'il s'est écoulé plus de dix ans entre la disparition de Galois et le moment où Liouville a étudié de manière extrêmement soigneuse et précautionneuse les papiers qui lui avaient été remis par le frère de Galois et par Auguste Chevalier, qui était la liasse de papier que Galois a laissé la veille de sa mort.

Et voilà ce que dit Liouville dans la séance du 4 septembre 1843. Donc c'est plus de dix ans après. Donc c'est un peu écrit en petit, mais je l'ai écrit en clair, mais je voulais simplement vous montrer comment ça apparaît dans les registres de l'Académie.

Donc ce que dit Liouville, c'est :

> *"À la suite d'une discussion où l'on a tant parlé d'équations algébriques, j'espère intéresser l'Académie en lui annonçant que dans les papiers d'Évariste Galois, donc ces manuscrits m'ont été confiés par Auguste Chevalier, j'ai trouvé une solution aussi exacte que profonde de ce beau problème* : "*étant donné une équation irréductible de degré premier, décider si elle est ou non résoluble à l'aide de radicaux*". *"Le mémoire de Galois est rédigé peut-être d'une manière un peu trop concise (ça c'est évident), je me propose de le compléter, donc il a fait le travail, de le compléter par un commentaire qui ne laissera, je crois, aucun doute sur la réalité de la belle découverte de notre ingénieux et infortuné compatriote."*

Donc ça c'est merveilleux, c'est merveilleux, parce qu'en fait il a fallu attendre deux ans après cette séance de l'Académie, du 4 septembre 1843, pour que les papiers de Galois soient publiés par Liouville, dans ce qui s'appelle maintenant, je pense, le Journal de Liouville.

Et à ce moment-là, il faut dire, ils ont eu une influence absolument considérable. Bon, alors voilà pour la partie historique, voilà pour la partie historique, voilà pour la partie qui concerne ces relations entre Galois et l'Académie, mais vous voyez à quel point ces relations sont complexes. Ce sont des relations extrêmement complexes, et on aurait tort de les caricaturer en disant que Galois haïssait, c'est vrai qu'il a écrit des choses un peu exagérées, mais il s'est retrouvé dans une situation dans laquelle il était devenu presque paranoïaque.

Alors maintenant, donc, je vais vous parler de mathématiques, je vais essayer de vous expliquer ce qu'est la théorie de l'ambiguïté, mais comme la voyait Galois. Alors, vous voyez, d'abord, quand vous parlez de théorie de l'ambiguïté, ça paraît absolument absurde, parce que si je vous donne une équation, j'ai pris une équation simple, ici, là, une équation de degré 5, je me contenterai du degré 5, à la fois parce qu'il est premier, et puis parce qu'on peut faire toutes sortes de choses. Donc si vous prenez une équation, et si je vous dis il y a une ambiguïté entre les racines, vous pouvez me rire au nez, puisque les racines, j'ai pris l'équation pour que les racines soient réelles, il y en a une qui est la plus petite, c'est A, et puis comme ça, elles sont en ordre croissant.

Donc vous voyez bien qu'il n'y a pas d'ambiguïté entre les racines, elles sont toutes devant vous. Mais maintenant, supposez que je vous demande, je vous pose une question, je vous dis, est-il possible de nommer la plus grande racine, par exemple E, par une relation qui ne laissera pas, justement, d'ambiguïté sur le fait que c'est la plus grande racine, et qui soit une relation rationnelle. Alors j'ai écrit cette relation $E = 4C^2 + 2D^2$, parce que quand vous faites les calculs avec l'ordinateur, vous avez l'impression qu'elle est vraie.

Alors pourquoi est-ce que cette relation ne peut pas être vraie ? La théorie de Galois a cette force, si vous voulez, que c'est une théorie qui vous permet de savoir, à partir de rien, simplement par un raisonnement abstrait, et ça va aller beaucoup plus loin après, dans des circonstances beaucoup plus générales, pour qu'on sache qu'une telle relation ne peut pas avoir lieu. Alors pourquoi, quelle est la raison pour laquelle elle ne peut pas avoir lieu ? Eh bien parce qu'en fait, il y a un groupe, qu'on appelle le groupe de Galois, qui permute les racines entre elles, qui n'est jamais trivial, pour une équation irréductible, celle-là est irréductible, qui permute les racines entre elles, et qui a la propriété de préserver toutes les relations algébriques rationnelles entre les racines. Donc si cette relation avait lieu, comme vous pouvez remplacer E par n'importe quelle autre racine, toutes les

racines seraient positives, puisqu'un carré c'est positif, 4 c'est positif, 2 c'est positif, donc toutes les racines seraient positives, ce n'est pas possible.

Donc on sait, a priori, simplement parce qu'il y a ce groupe d'ambiguïté, ce groupe de symétrie qui est caché derrière, qu'il est impossible que cette relation ait lieu. Alors en l'occurrence, le groupe est très très simple, parce que j'ai pris une équation cyclique, et en fait c'est très facile, c'est un petit exercice qui prend 3 secondes, de vérifier que si vous avez une racine de cette équation, si vous prenez son carré moins 2, c'est encore une racine de l'équation. Donc vous avez un groupe d'invariance qui fait que, automatiquement, à chaque fois que vous avez une racine x, la formule $x^2 - 2$ vous donne une autre racine.

Alors quel est l'intérêt de ça ? L'intérêt, ça veut dire que toutes les racines de cette équation sont fonctions rationnelles d'une seule des racines ; et comme c'est le cas, si vous avez une relation algébrique entre les racines, comme la relation qui était là, vous en déduirez que sur une racine quelconque, vous avez une relation polynomiale, mais c'est forcément un multiple du polynome irréductible dont on est parti, et on a la conclusion. Alors on verra ce raisonnement en un petit peu plus de détails, mais que dit la théorie de Galois dans ce cas là ? Eh bien, elle dit qu'en fait, il faut indexer convenablement les racines de l'équation, pas du tout comme ABCD comme on avait fait tout à l'heure, il faut les indexer, les racines, par les entiers modulo 5, exactement comme j'ai indiqué sur la figure, donc 0, 1 pour les deux premières, les plus à gauche, 3, 4 pour les deux qui suivent, et puis 2 pour celle qui est le plus à droite. Et si vous faites ça, vous allez voir qu'en fait le groupe de Galois a décelé une structure qui était cachée, qui était sous-jacente aux racines, et qui était la structure, si vous voulez, des entiers modulo 5. Et le groupe de Galois les permute de manière cyclique, mais cette structure, elle est présente, et on ne l'aurait jamais vue si on avait simplement agi comme, disons, comme un expérimentateur ou un physicien en disant, eh bien j'ai une équation, j'ai ses racines, et puis je suis content.

En fait, ce qui est extraordinaire dans la théorie de Galois, c'est que derrière cette évidence apparente, si vous voulez, qui vous donne une équation et qui vous fait voir ses racines, il y a une théorie beaucoup plus subtile, beaucoup plus intéressante qui est cachée derrière, et qui justement permet de comprendre, de saisir qu'il y a, du fait que l'équation est irréductible et du fait qu'elle n'est pas résoluble directement, qu'elle n'est pas factorisée, il y a une ambiguïté entre les racines. Alors en fait, pour mieux comprendre tout ça, donc il y a une définition abstraite, on va la voir telle que l'écrit Galois, donc on va voir qu'il y a une subtilité, que Galois décrit absolument de manière parfaite, et qu'il faut comprendre, sinon on ne comprend pas la théorie. Donc soit une équation donnée, on prend les racines, ce que dit Galois c'est qu'il y aura toujours un groupe de permutation des lettres qui aura la propriété suivante : que toute fonction des racines invariable par les substitutions de ce groupe soit rationnellement connue et réciproquement que toute fonction des racines qui est déterminable rationnellement soit invariable par ces substitutions.

Alors si on le dit comme ça, on ne comprend pas vraiment si on n'a pas l'explication de Galois. Voilà le texte de Galois est beaucoup plus précis et beaucoup plus intéressant que cet énoncé abstrait. Voilà ce que dit Galois.

Il dit ici la chose suivante :

"*Nous appelons ici invariable, non seulement une fonction dont la forme est invariable par les substitutions des racines entre elles* (voyez bien si on prend la somme des racines, par exemple, elle est invariable par toutes les substitutions), *mais encore celle dont la valeur numérique ne varierait pas par ces substitutions.* Et là, il y a une distinction qui est cruciale. Par exemple, ce que dit Galois, c'est que si l'équation c'est $Fx = 0$, eh bien Fx c'est une fonction des racines qui ne varie par aucune permutation. En fait, il est beaucoup plus précis que ça, il continue et il dit : *Lorsqu'une fonction des racines ne change pas de valeur numérique par une certaine substitution opérée entre les racines, elle est dite invariable par cette substitution.*

On voit qu'une fonction peut très bien être invariable par telle ou telle substitution entre les racines sans que sa forme l'indique. Ainsi si $Fx = 0$ est l'équation proposée, la fonction $\varphi(F(a), F(b), F(c), ...)$ (on épèle les racines), *où φ est une fonction quelconque, rationnelle bien sûr, sera une fonction de ces racines qui sera invariable par toute substitution entre les racines, sans bien sûr que sa forme l'indique.*

Ça pourrait être par exemple $F(a) + 3F(b)$ ou un truc comme ça. Or c'est une question dont il ne paraît pas qu'on ait encore la solution de savoir si étant donnée une fonction de plusieurs quantités numériques, on peut trouver un groupe qui contiennent toutes les substitutions par lesquelles cette fonction est invariable et qui n'en contiennent pas d'autres.

Vous voyez, il y a un pas énorme qui est franchi à ce moment-là, parce que dans Lagrange par exemple, ou dans d'autres textes, on cherchait à trouver pour l'équation générale, des fonctions des racines qui ne sont pas trop invariantes, tout en étant un petit peu invariantes. Par exemple si vous prenez une équation du quatrième degré, vous avez $ab + cd$, ça c'est une fonction qui n'est pas invariante par toutes les permutations mais qui ne prend que trois valeurs différentes quand on applique toutes les permutations et ça permet de résoudre l'équation du quatrième degré par l'équation du troisième degré. Donc c'était différent, les gens faisaient des choses dans le cadre complètement général.

Alors donc ce que dit Galois c'est qu' :

évidemment, cela a lieu pour des quantités littérales, puisqu'une fonction de plusieurs lettres invariable par deux substitutions est invariable par leur produit. Donc ça c'est évident. *Mais rien n'annonce que la même chose ait lieu quand aux lettres, on substitue des nombres*, ce n'est absolument pas évident. Il dit : *on ne peut donc point traiter toutes les équations comme des équations littérales, il faut avoir recours à des considérations fondées sur les propriétés particulières de chaque équation numérique, c'est ce que je vais tâcher de faire.*

Il faut voir qu'à l'époque les gens faisaient énormément de calculs et par exemple si vous regardez la copie de Galois d'entrée à l'École Préparatoire, vous verrez qu'on donnerait ces problèmes même à des gens maintenant, je ne suis pas sûr qu'ils seraient tous capables de donner la bonne solution. Et donc les gens faisaient énormément de calculs et remarquons que tout ce qu'une équation numérique peut avoir de particulier doit provenir de certaines relations entre les racines. Ces relations seront rationnelles dans le sens que nous l'avons entendu, c'est à dire qu'elles ne contiendront

d'irrationnels que les coefficients de l'équation bien sûr et les quantités adjointes.

> *De plus ces relations ne devront pas être invariables par toute substitution opérée entre les racines, sans quoi on n'aurait rien de plus que pour les équations littérales ordinaires. Ce qu'il importe donc de connaître, c'est par quelles substitutions peuvent être invariables les relations entre les racines, ou ce qui revient au même, des fonctions des racines dont la valeur numérique est déterminable rationnellement.*

Alors là je vais quand même vous donner une toute petite explication. Ce qui est incroyable c'est la chose suivante, c'est que ce que fait le groupe de Galois, c'est, si vous voulez, si on vous disait, je prends une équation, il faut déterminer toutes les relations rationnelles entre les racines, vous pourriez le faire, on va voir comment. Mais qu'est ce que ça vous donnerait ? Ça vous donnerait les multiples d'un polynôme, qu'on appelle le polynôme associé à l'extension galoisienne correspondante, ce serait quelque chose qu'il est très difficile de calculer et de manipuler. Et ce qui est merveilleux, c'est que ce que Galois a démontré, c'est que ce n'était pas exactement les relations, une certaine fonction comme par exemple tout à l'heure $E - 4B^2 - 2C^2 = 0$ ou un truc comme ça, ce n'est pas ça qui compte. Ce qui compte, ce n'est pas un truc égal à 0, parce que les trucs égaux à 0, vous auriez un peu de mal à les déterminer, ce qui compte, ce sont les quantités rationnelles, c'est-à-dire que bien sûr que si vous écrivez une relation égale à 0, 0, c'est rationnel, donc elle doit être invariante par le groupe de Galois. Mais réciproquement, si vous prenez une expression qui est invariante par le groupe de Galois, elle ne vous donnera pas 0, mais elle vous donnera un nombre rationnel. Mais comme ce nombre est rationnel, vous pouvez le soustraire de cette expression et vous obtenez 0. Donc, par l'invariance par le groupe, vous déterminez toutes les relations rationnelles, donc toute la spécificité d'une équation. Et alors donc, ce que fait Galois, le groupe de Galois, donc en fait, il donne un groupe de permutations des racines, qui est toujours non trivial, c'est ça qui est absolument époustouflant, c'est que le groupe n'est jamais réduit à l'identité, sauf si l'équation est bien sûr complètement résolue, c'est à dire si on a un facteur irréductible de degré 1. Et pour montrer l'existence de ce groupe d'ambiguïté, Galois procède en deux étapes ; la première étape, c'est de trouver une autre équation (ça en fait, le rapport de Poisson dit que Lagrange le savait déjà), de trouver une équation auxiliaire telle que les racines de l'équation dont on part soit toutes fonctions rationnelles d'une seule racine de l'équation auxiliaire. Et de plus (bien sûr, ça s'en déduit immédiatement), que les racines de l'équation auxiliaire vont être fonctions rationnelles les unes des autres. Donc les racines de cette équation, c'est un peu comme dans l'équation de tout à l'heure, quand vous aviez la transformation $x \to x^2 - 2$, vous avez des transformations rationnelles qui vont transformer les racines les unes en les autres. Et alors après, c'est fini parce que si vous prenez une relation rationnelle entre les racines, elle va vous donner une équation $H(V) = 0$, qui va pouvoir se formuler en termes d'une seule racine de l'équation auxiliaire. Comme il y a une seule racine de l'équation auxiliaire, elle sera forcément un multiple du polynôme minimal de V et vous avez gagné, puisque ce polynôme minimal est invariant par les transformations rationnelles. Donc la démonstration est incroyablement simple, bien sûr. Alors c'est ce qu'on voit, le groupe de Galois, il le calcule de manière explicite. Il dit, bien sûr, la difficulté des calculs ; il n'avait pas d'ordinateur, à l'époque, et on va voir à quoi ressemble la difficulté des calculs, je vais vous le montrer, parce que maintenant, on n'a pas d'excuse pour ne pas le montrer. Donc voilà ce que Galois disait, et c'était vraiment quelque chose d'extrêmement profond parce qu'il ne dit pas qu'il

ne faut pas faire les calculs, il dit :

> "*sauter à pieds joints sur les calculs, grouper les opérations, les classer* (justement) *suivant leurs difficultés et non suivant leur forme, telle est selon moi la mission des géomètres futurs*".

Donc alors maintenant, si vous voulez, on va voir un peu plus tard comment Galois faisait les calculs, mais avant de vous montrer ça, je vais vous montrer simplement comment on fait maintenant, pour comprendre ce que c'est que le groupe de Galois de manière extrêmement naturelle et simple il y a un théorème qui est un théorème de Chebotarev et qui permet de comprendre en quel sens il est vrai que plus le groupe d'ambiguïté est grand plus il est difficile de résoudre une équation. Alors comment est ce que le théorème est formulé ? Eh bien, le théorème est formulé en disant qu'on va s'intéresser maintenant (l'équation est à coefficients entiers), donc on va pouvoir réduire modulo un nombre premier, c'est-à-dire que pour chaque nombre premier, on va regarder si on peut résoudre l'équation modulo ce nombre premier ; ce n'est pas très difficile de savoir ce que ça veut dire : ça veut dire que tous les nombres qui sont multiples d'un nombre premier p, vous les identifiez à zéro et vous cherchez à résoudre l'équation. Ce que dit le théorème de Chebotarev, c'est que la probabilité pour que l'équation soit résoluble modulo un nombre premier p, la probabilité sur l'ensemble des nombres premiers, c'est l'inverse de l'ordre du groupe de Galois, donc c'est quelque chose qui est extrêmement simple, et si vous regardez par exemple pour le polynôme dont je vous ai parlé tout à l'heure et si vous le réduisez modulo p, alors vous aurez l'impression qu'il change chaque fois mais c'est parce que quand il y a un moins quand vous réduisez modulo p par exemple si vous réduisez modulo 47, 44 ça fait -3, donc ça vous donne une impression, mais vous voyez qu'il arrive, assez fréquemment là, que le polynôme ait toutes ses racines dans les entiers modulo le nombre premier. Alors, il ne faut pas vous inquiéter du nombre 11, le nombre 11, il a la propriété que ce qu'on appelle le discriminant de l'équation dans les parties, je crois que c'est 11 puissance 4 ou quelque chose comme ça, donc en fait ça veut dire que le nombre 11 est très particulier et l'équation, elle n'aura pas des racines distinctes, quand on travaille modulo 11. Par contre, dès qu'on prend des nombres premiers autres, si les racines existent dans les entiers modulo p, elles vont être distinctes et alors là, on voit un comportement qui est très très clair, et qui vous dit qu'à peu près tous les cinq nombres premiers, l'équation est complètement résolue, elle est complètement résolue, elle a toutes ses racines modulo p.

Donc cette équation, elle est facile : elle est facile au sens où si après, vous regardez la densité, vous voyez, j'ai mis l'inverse de la densité ici, et on voit bien qu'on obtient le nombre 5, on obtient le nombre 5 en prenant... on va très loin au niveau... l'indice qui est en bas le 10 000, ça veut dire qu'on est au dix millième nombre premier et on regarde l'inverse de la proportion de nombres premiers pour lesquels elle est complètement résolue. Alors c'était une équation très simple. Maintenant, on va s'intéresser à des équations un petit peu plus compliquées. Donc prenons par exemple les racines cinquième de 2 : si vous regardez les racines cinquièmes de 2 et si vous essayez modulo un nombre premier, eh bien là, vous allez vous apercevoir que bouh...! Dans tous les exemples que je vous ai montrés, il n'y en a même pas un seul dans lequel l'équation est vraiment résoluble complètement modulo le nombre premier et je suis pourtant allé assez loin. Et alors si vous faites le calcul, vraiment, si vous faites le calcul loin, vous allez vous apercevoir que l'inverse de la densité de l'ensemble des nombres premiers pour lesquels il y a cinq solutions, cinq racines cinquième de 2, vous voyez que ça vaut environ 20 ; ça met du temps à se stabiliser mais au bout d'un moment, ça

se stabilise et ça vaut de l'ordre de 20. Donc qu'est ce que ça veut dire ? Ça veut dire que le groupe de Galois de cette équation, il est d'ordre 20 ; bien sûr, je vais dire, il y a des gens naïfs, quand ils restituent la théorie de Galois, ils vous disent $x^5 = 2$, c'est un groupe cyclique, bien sûr, ce n'est pas ça : c'est un groupe d'ordre 20, qui est un petit peu plus compliqué qu'un groupe cyclique, parce que pour obtenir un groupe cyclique il aurait fallu adjoindre les racines cinquième de 1 et on ne l'a pas fait. Alors on peut faire le calcul explicite de ce groupe, je vous montrerai comment Galois le faisait, et quand on fait le calcul explicite, on s'aperçoit, bien sûr, qu'il y a la permutation cyclique, mais qu'il y a aussi d'autres permutations, qui sont même impaires ; en fait, le fait que ce groupe ait des permutations impaires, je pense que c'est la raison qui a fait croire à Abel et à Galois qu'ils avaient résolu l'équation du cinquième degré, je pense que je vous dirai pourquoi un petit peu plus tard, et en fait donc, à nouveau, il y a une structure sous-jacente, et ce qu'il faut faire, c'est indexer les racines sur le corps $\mathbb{F}_5$ mais le groupe de Galois, vous voyez dans ce cas-là, ça devient le groupe affine, ce n'est plus le groupe seulement des translations, c'est le groupe affine, c'est le groupe à nouveau sur le corps $\mathbb{F}_5$, mais des transformations affines de la forme x donne $ax+b$, qui sont effectivement très simple, mais il faut indexer les racines, de manière évidente, c'est 0 1 2 3 4 par le corps $\mathbb{F}_5$.

Alors regardons maintenant un exemple d'ordre 10, c'est un exemple qui est plus intéressant. Donc je vous donne une équation, dont le groupe dihédral est le groupe de Galois, c'est un groupe qui est d'ordre 10 et on la trouve facilement en regardant par exemple le théorème de Chebotaref, on obtient ça et alors si on regarde cette équation, si on fait le calcul explicite de son groupe de Galois, on trouve, à ce moment-là, quelque chose d'un petit peu différent. Alors, vous voyez qu'on a le même type de permutation cyclique quand j'écris les petits ronds, là, ce sont les racines dans le plan complexe, je n'ai pas fait ça de manière arbitraire, les petits ronds sont les racines dans le plan complexe. Et les permutations, ce sont de vraies permutations du groupe de Galois. Donc on a la permutation du haut, qui est une permutation cyclique entre les cinq racines, et la permutation du bas, qui est caractéristique du groupe dihédral parce que c'est une involution, bien sûr avec un point fixe, mais qui quand on les met ensemble, l'une avec l'autre, va engendrer un groupe dihédral. Alors la structure sous-jacente à nouveau, eh bien on voit bien qu'à nouveau on va indexer les racines de la manière que j'ai indiquée 0 1 2 3 4 d'accord, par le corps $\mathbb{F}_5$ et à nouveau, le groupe de Galois est un sous-groupe du groupe affine. Alors donc maintenant, l'équation vraiment intéressante si on s'en était restreint au degré 4, on n'aurait pas eu d'équation intéressante parce qu'on n'aurait eu que des équations qui sont résolubles par radicaux.

C'est pour ça que j'ai choisi le degré 5, bien sûr, c'est pour pouvoir vous montrer une équation qui soit non résoluble par radicaux. Alors, j'ai quand même fait un choix un peu simplificateur c'est-à-dire que j'ai pris une équation dont le discriminant est un carré, de telle sorte que son groupe de Galois, ce ne soit pas le groupe symétrique, vous voyez, si vous me donnez... tout à l'heure, vous pourrez me donner une équation au hasard, et je vous montrerai que son groupe de Galois, c'est le groupe symétrique S_5. Mais, avec un peu de chance, on arrive à... donc dès que le discriminant est un carré, c'est une espèce d'ersatz de ce qui se passait pour l'équation du second degré, le groupe de Galois devient le groupe A_5, qui est un groupe simple, qu'on appelle le groupe alterné, et on le voit en calculant la probabilité pour que l'équation soit résoluble complètement modulo p.

Voyez cette probabilité, si vous allez assez loin, vous voyez que l'inverse de cette probabilité, c'est

60. Alors si on fait le calcul explicite, on peut calculer explicitement le groupe de Galois, on trouve des permutations comme celles qui sont là. Quel est l'intérêt des deux permutations que j'ai écrites ? Eh bien, c'est qu'elles vont vous donner la présentation du groupe. Vous voyez, c'est un groupe d'ordre 60, donc un groupe d'ordre 60, ça peut paraître difficile à appréhender, en fait il est extrêmement simple à appréhender, parce que c'est un groupe dont la présentation est très simple ; il y a un générateur, celui du haut, qui est de carré 1 ($u^2 = 1$) et celui du bas, son cube est égal à 1 ($v^3 = 1$), c'est évident puisqu'il permute de manière cyclique les trois racines qui sont là, et en plus, quand on fait le produit uv de ces deux générateurs, on obtient un élément dont la puissance cinquième est égal à 1 ($(uv)^5 = 1$).

Alors quand vous connaissez ces relations $u^2 = 1, v^3 = 1, (uv)^5 = 1$, vous avez tout compris sur le groupe parce qu'après vous écrivez des mots avec les lettres u et v, et vous faites les simplifications qui s'imposent, c'est-à-dire les simplifications qui viennent de $u^2 = 1$, vous ne pouvez pas répéter u deux fois, $v^3 = 1$, vous ne pouvez pas répéter v 3 fois, et ainsi de suite. Et il est immédiat, par exemple, qu'une équation, qui a ce groupe-là, ne peut pas être résoluble par radicaux parce qu'à ce moment là, vous pourriez représenter ces relations de manière abélienne, c'est-à-dire de manière commutative, mais si vous avez $u^2 = 1, v^3 = 1$ et si u et v commutent, quand vous prenez $(uv)^5 = 1$, vous allez en déduire immédiatement que $u = v = 1$; donc vous avez une contradiction évidente. Donc c'est comme ça qu'on comprend ces groupes.

Et maintenant, ce qui est extraordinaire, c'est que quand Galois avait 18 ans, il a publié un article, son article est publié dans le Bulletin de Férussac, en juin 1830, et dans cet article, il fait la chose suivante : je vous ai montré sur des exemples très simples qu'il fallait indexer les racines par le corps $\mathbb{F}_5$ d'accord, alors ce que fait Galois, c'est fantastique, il définit les corps finis quelconque $\mathbb{F}_q$, bon, on sait qu'il faudrait être beaucoup plus "non canonique" que ça, il y a une ambiguïté dans la définition du corps $\mathbb{F}_q$, mais donc il définit le corps $\mathbb{F}_q$ (Gauss le connaissait sûrement aussi) et ensuite, qu'est ce que fait Galois ? Bien sûr, il calcule le groupe de Galois de $\mathbb{F}_q/\mathbb{F}_p$, ce n'est pas difficile, il est engendré par le Frobenius.

Ce n'est pas ça qui est difficile ; ce qui est extraordinaire, c'est que Galois prolonge au cas général des équations résolubles par radicaux ce qu'il avait compris pour les équations de degré premier en utilisant le corps $\mathbb{F}_q$. Voilà ce qu'écrit Galois. Alors vous ne le lirez pas, mais ça ne fait rien, je crois que je peux le lire : alors il dit la chose suivante "*Cette remarque...*" Donc qu'est ce qu'il fait ? C'est dommage que je ne voie pas la formule mais elle est dans l'article. Qu'est ce qu'il dit ? Il dit "*vous prenez une équation*" bon vous savez, vous voulez qu'elle soit résoluble, il demande qu'elle soit primitive, c'est une petite condition qui n'est pas difficile à comprendre, qui dit en gros que le corps qui est défini par l'équation n'a pas de sous-corps. Donc il prend son équation, ensuite il dit que "*si l'équation est résoluble (si elle est primitive), on pourra indexer les racines non pas par* $\mathbb{F}_5$ *comme tout à l'heure, mais par un corps fini* $\mathbb{F}_q$ *et que les transformations des racines par le groupe de Galois seront automatiquement contenues...*" dans quoi ? Pas seulement dans le groupe affine, ce serait trop simple, si c'était comme dans les cas précédents, le groupe $ak + b$ comme dans le cas premier, non, *"...dans le groupe affine produit semi direct par les puissances du Frobenius"*.

Donc ça, c'est vraiment extraordinaire, c'est écrit explicitement dans l'article de Galois et Galois avait la démonstration, il y a quelques cas particuliers auxquels il faut faire attention. Mais donc

il avait parfaitement compris ce qui se passait dans cette chose-là.

Bien sûr, après, il explique la théorie générale, mais on réduirait à très peu la théorie de Galois si on ne parlait que de la théorie générale. En général, si vous voulez, quand on explique la théorie de Galois, quand on explique ce qu'a fait Galois, on explique surtout la théorie générale, qui est expliquée ici, par exemple, si on adjoint à une équation donnée, la racine d'une équation auxiliaire irréductible, qu'est-ce qui arrive, etc. Mais, en fait, la théorie de Galois, Galois était allé bien plus loin, au sens où il avait compris que, quand on connaît le groupe de Galois d'une équation dans le cas où elle est résoluble, ce groupe, en fait, décèle une structure très intéressante, très particulière dans les racines, par le fait qu'on peut indexer ces racines par tous les éléments d'un corps fini, et qu'ensuite, si vous voulez, cette structure est automatiquement préservée par l'action du groupe de Galois.

Donc, c'est une structure intrinsèque à l'ensemble des racines. C'est quelque chose qui est tout à fait extraordinaire. Alors, je ne vais pas vous embêter avec ça.

Ce que je vais faire maintenant, c'est vous montrer les calculs. J'espère que vous ne m'en voudrez pas. À l'époque de Galois, les gens ne pouvaient pas faire les calculs.

Bon, ça, c'est des trucs classiques, je n'ai pas envie. Donc, alors ça, ce n'est pas grave, ce n'est rien. C'était pour montrer un peu Chebotarev.

Vous voyez, si vous calculez, pour savoir quel groupe de Galois a une équation, vous prenez l'inverse de cette proportion de tout à l'heure. Donc, vous voyez, pour le polynôme qui est là, vous avez 60. Là, vous avez 5. Là, vous avez 10.

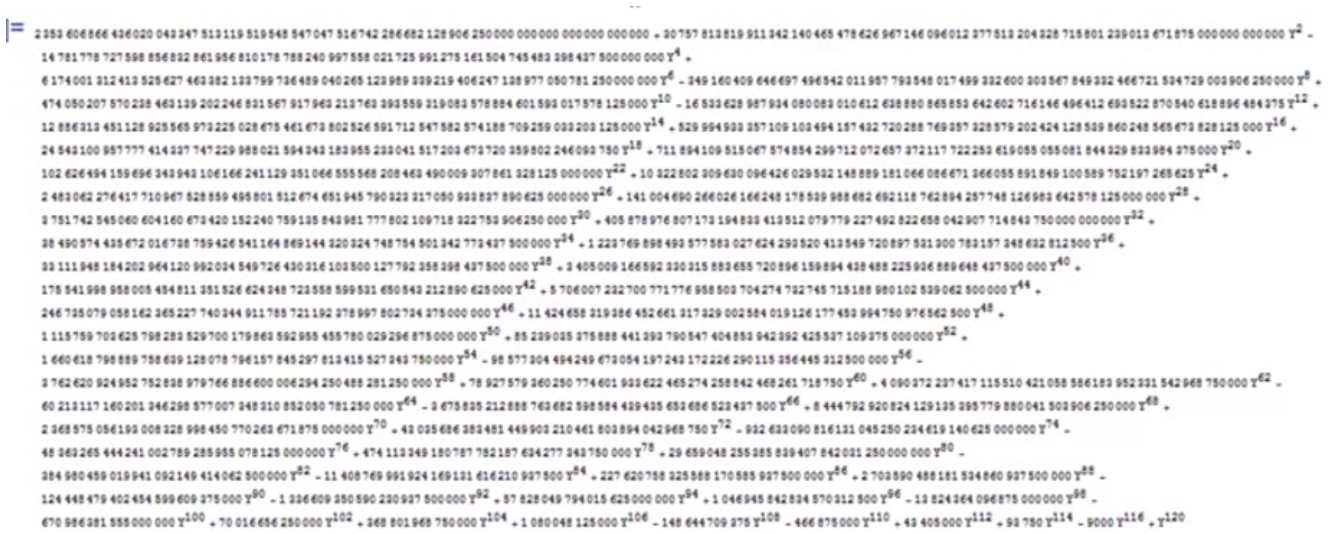
Et là, vous avez 20. Donc, ça vous donne le point de départ. Bon.

Alors ensuite, on part d'une équation. On part, par exemple, de celle-là. Celle-là, c'est celle qui a 10. Donc, c'est celle qui a le groupe dihédral. D'accord ? Alors, qu'est-ce qu'on fait quand on a une équation ? Comment on fait pour calculer son groupe de Galois ? Comment Galois proposait de le faire ? Alors, ce que disait d'abord Galois, c'est que vous allez trouver une fonction des racines qui est telle que cette fonction va prendre factorielle 5 valeurs différentes, 120 valeurs différentes, quand vous permutez les racines entre elles. Alors, on essaye la fonction la plus simple possible. La fonction la plus simple possible, c'est $a + 2b + 3c + 4d$. Je n'ai pas envie de mettre e, puisque la somme des racines est connue. Et puis, les coefficients, il faut bien qu'ils soient différents. Donc, j'ai pris 1, 2, 3, 4. Ça ne peut pas être plus simple que ça. D'accord ? Donc, on prend ces coefficients-là et on cherche quelle est l'équation qui a pour racine les $a+2b+3c+4d$. D'accord ? On la calcule.

Je ne vous la montre pas parce que ça vous ferait peur. Si quelqu'un veut que je la montre, je peux la montrer. D'accord ? Mais bon, il ne faut peut-être pas.

Ce qui est sûr, c'est que vous demandez de la factoriser. Si, je vais quand même vous la montrer. D'accord ? Attendez, je vais supprimer.

Je vais vous la montrer. Je vais faire “entrez”. Vous voyez ? Voilà.



D’accord ? Ce n’est pas jojo. D’accord ? Donc, si on vous donne comme exo de factoriser ce polynôme, bon, ça peut être un peu embêtant. L’ordinateur, il fait ça en 3 secondes.

D’accord ? Je vais lui demander de le faire, l’ordinateur, parce que pourquoi pas. Voilà. Donc, l’ordre que je lui donne, c’est de factoriser ce polynôme.

D’accord ? Il va le faire. Voilà. Il vous donne le résultat tout de suite.

Donc, vous voyez que tous les facteurs irréductibles sont de degré 10. D’accord ? Il y en a 12. Et maintenant, une fois qu’on a ces facteurs irréductibles, par un raisonnement d’élimination qui est très très simple, on peut exprimer les racines de l’équation de départ en fonction d’une racine quelconque de ce polynôme.

Alors, on fait le calcul. C’est un calcul par élimination qui n’est pas difficile, mais qui est long. Et on obtient, voilà, l’expression pour les racines. C’est une expression qui est unique. Vous voyez qu’elle... Ici, ça s’arrête au degré 8. Ici, ça s’arrête au degré 9. On ne va pas jusqu’au degré 10, puisque l’équation irréductible est de degré 10. Donc, on peut toujours simplifier par y^{10}. Donc, voilà ces fonctions-là. Ça, c’est tout à fait calculable. Je veux dire, Galois peut le faire parfaitement, ça. Il n’y a aucune difficulté, là, sauf le premier polynôme. Ensuite, on prend les racines du polynôme du premier facteur, là, de tout à l’heure, qui était celui-là, d’accord ? On choisit le premier facteur irréductible. On prend ses racines. Elles ont l’air de ça. Et alors, maintenant, ce qui est incroyable, c’est que chaque fois qu’on a un couple de racines... C’est ça qu’il faut bien comprendre. Chaque fois qu’on a un couple de racines de l’équation auxiliaire, ça va nous donner une permutation. Ça correspondait au tableau de tout à l’heure, qui donnait l’ambiguïté entre les racines. Alors, j’ai écrit un petit programme qui va vous montrer que chaque fois que vous me donnez deux nombres, par exemple celui-là, j’ai une permutation correspondante. Dans ce cas-là, on va voir apparaître le groupe dihédral.

En fait, on peut fixer l'une des deux. On va, par exemple, fixer la première racine comme étant égale à 1. Et on va faire varier la deuxième. Et on va voir qu'en faisant varier la deuxième, on obtient tout le groupe dihédral.

Alors, j'obtiens l'identité, mais je ne l'ai pas marquée. Ensuite, on obtient ça. Vous voyez bien que ça fait partie du groupe dihédral.

Ça, c'est une involution de carré 1 qui fixe ce point, etc. Et puis, on va avoir les dix éléments. Ça, c'est une permutation cyclique.

Là, on a une involution qui fixe un autre point, une autre involution, permutation cyclique, involution, etc. D'accord ? Permutation cyclique, involution. D'accord.

Donc, je veux dire, là, on voit parfaitement comment le groupe de Galois se calcule. Le calcul n'est pas vraiment compliqué, parce que l'équation a pour groupe le groupe dihédral. Et ensuite, si on applique la factorisation de tout à l'heure, on peut vérifier quelque chose qui est mieux encore, enfin, qui est mieux, qui est très relié au théorème de Chebotarev et qui est un théorème de Dedekind. Et qui dit que si on regarde maintenant comment le polynôme va se factoriser modulo p, par exemple modulo 23, ça va correspondre à des cycles dans le groupe de Galois. Vous voyez, par exemple, la décomposition modulo 23, elle va correspondre à une involution qui va fixer une racine, qui va permuter deux autres racines, qui va permuter deux autres racines, et ainsi de suite.

Ça, ça va correspondre à une permutation cyclique. Et ça, ça va correspondre à une involution. Voilà.

Donc, en fait, on a un contrôle. Alors là, maintenant, on va partir d'une autre équation. Ah oui, c'était celle dont j'étais parti. Et si je prends celle dont j'étais parti au départ. Celle-là, on l'a déjà complètement traitée. Elle avait un groupe de Galois qui était très simple.

Mais vous voyez qu'on va retrouver cette simplicité du groupe de Galois parce que quand on factorise le polynôme associé, eh bien, on va ne retrouver que des tout petits polynômes de degré 5. Donc là, le groupe de Galois est d'ordre 5. Il est très, très simple. On peut calculer l'expression des racines. On peut calculer le polynôme associé.

Mais l'intérêt, maintenant, par rapport à ce qu'on avait tout à l'heure, c'est qu'on peut calculer explicitement les permutations. Ça, c'est beaucoup plus joli que de savoir abstraitement que le groupe de Galois est d'ordre 5. Par exemple, ici, on va obtenir toutes les permutations. Et ces permutations ne se comprennent qu'une fois qu'on a indexé, comme je l'ai dit tout à l'heure, correctement les racines par le corps $\mathbb{F}_5$ de telle sorte qu'elles deviennent simplement des translations.

On a une structure qui est dévoilée par le groupe de Galois. De même qu'on l'a vu, il y a la résolubilité modulo un nombre premier. Ça, on l'a déjà montré tout à l'heure.

Maintenant, on regarde l'équation des racines $5^{\text{ièmes}}$. Bon alors l'équation des racines $5^{\text{ièmes}}$, c'est un petit peu plus embêtant. Voilà le polynôme de degré 120 dont on part.

Les polynômes irréductibles qu'on obtient ne sont pas très méchants. Ils sont de degré 20. Ils ne sont vraiment pas méchants du tout.

Et à nouveau, les équations qui donnent les racines en fonction de ces polynômes ne sont pas compliquées. Regardez, celle-là est extrêmement simple. Je vais faire un petit aparté pour les mathématiciens.

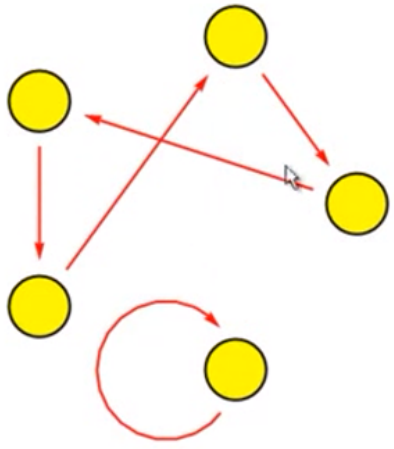
Vous savez, en mathématiques, on a un moyen merveilleux pour résoudre une équation. Si on prend l'anneau des polynômes, on a une équation $P(x) = 0$. Pour résoudre l'équation, on prend l'anneau des polynômes et on le divise par l'idéal engendré par $P(x)$. À ce moment-là, on a résolu l'équation parce que x est une racine. Malheureusement, ça a un gros inconvénient de faire ça, c'est qu'en général, on a une seule racine.

C'est-à-dire que vous ne pouvez pas factoriser le polynôme. Mais la méthode de Galois, la méthode dont je vous parle, elle permet de factoriser entièrement le polynôme. Et c'est formidable, après, quand on a un peu l'habitude de l'ordinateur, de voir que quand on a exprimé toutes les racines en fonctions rationnelles d'une seule racine, on peut se poser toutes sortes de questions et on a une réponse absolument immédiate.

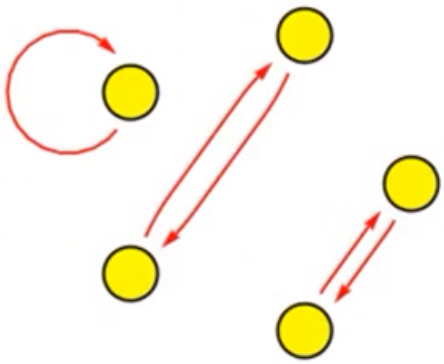
C'est quelque chose de merveilleux. Donc, il y a un pas qui a l'air de rien. Bien sûr, quand on définit les nombres complexes, on a rajouté toutes les racines de l'équation parce qu'on a rajouté i, mais l'autre racine, c'est $-i$. Lorsqu'on définit les corps finis, c'est pareil.

Mais lorsqu'on définit des extensions plus générales, ce procédé-là est extrêmement efficace. Maintenant, ce qui se passe, c'est que là, on fait pareil. On regarde les racines de l'équation auxiliaire et on a le groupe de Galois.

Vous allez avoir le groupe de Galois. Il est un petit peu plus compliqué parce qu'il est d'ordre 20. Vous avez des permutations cycliques. Ça, c'est encore le groupe dihédral. Je vais essayer de trouver quelque chose qui ne soit pas dans le groupe dihédral, quand même. Ça, c'est encore dans le groupe dihédral. Ça encore. Ça encore. Tiens, c'est bizarre. On va aller vers le bas. Ça encore.



Voilà, ça, ce n'est pas dans le groupe dihédral. Ça, c'est une permutation impaire. Il faut bien savoir maintenant, si vous réfléchissez, si le groupe A_5 avait contenu le groupe des transformations affines, l'équation du cinquième degré aurait été résoluble par radicaux.



Je pense que c'est ça l'erreur qu'ont fait Galois et Abel. Et la raison, c'est la suivante. C'est que le polynôme adjoint, pour résoudre l'équation, aurait été un polynôme de degré 3, puisque 60 divisé par 20, ça vaut 3. Et à ce moment-là, on aurait pu résoudre cette équation puisqu'elle est de degré 3. Et comme le groupe d'ordre 20 est résoluble, on aurait pu, en rajoutant des radicaux, résoudre l'équation de départ. Mais c'est bien sûr faux. Il suffit de regarder que la permutation qui est en face de vos yeux, elle est impaire. Elle n'est pas paire. Et donc, elle ne peut pas appartenir au groupe A_5. Donc, voilà ce qui se passe. Alors, bien sûr, il y a le théorème de Chebotarev.

Vous pouvez aussi regarder ce qui se passe ici. D'accord ? Bon. Alors maintenant, on va venir à quelque chose de beaucoup plus intéressant.

Et je pense que c'est ce à quoi Galois faisait référence lorsqu'il disait "*on ne peut pas faire les calculs*". Pourquoi ? Parce que ça ne l'intéressait pas d'avoir des équations qui étaient résolubles par radicaux. Il y en avait partout.

Il voulait une équation concrète, numérique, qui ne soit pas résoluble par radicaux. Ça, il le voulait absolument, d'accord ? Et appliquer sa méthode à cette équation.

Alors, j'en ai pris une qui, comme je l'ai dit tout à l'heure, a un discriminant qui est un carré. Donc, elle n'est encore pas trop méchante. Ça veut dire que quand vous prenez son polynôme irréductible, bon, c'est celui-là, il va se casser en deux.

Il va se casser en deux. Est-ce que je l'ai cassé en deux ? Voilà. Non, je ne l'ai pas cassé en deux, peu importe. Vous avez un polynôme de degré 60. Je ne sais pas si le degré de celui-là, c'est 60. Oui, c'est 60. Donc, celui-là, c'est le polynôme irréductible, de degré 60, que vous obtenez en décomposant le polynôme associé toujours aux racines $a + 2b + 3c + 4d$, en facteurs irréductibles. Donc, vous obtenez ça.

Et alors maintenant, vous demandez de calculer les racines comme tout à l'heure. Vous vous souvenez, tout à l'heure, il y avait une belle formule pour les racines de l'équation de départ en fonction du polynôme associé, des racines du polynôme associé. Alors maintenant, vous demandez de faire le calcul.

Alors ça, vous pouvez le demander à l'ordinateur. Il fait le calcul. Il obtient des polynômes. Il obtient des polynômes de degré 59, puisque l'équation associée est de degré 60. Et alors, l'ordinateur fait les calculs avec, sans aucune difficulté. Mais par curiosité, j'ai demandé à l'ordinateur de me donner le terme constant du polynôme qui donne la première racine.

D'accord ? Le terme constant, c'est cette fraction-là. D'accord ? Alors, j'ai demandé à l'ordinateur le numérateur de la fraction. C'est facile.

Et j'ai demandé combien il y avait de zéros. C'est 10 puissance 393. Alors maintenant, les physiciens nous disent que c'est le nombre d'univers qui sont possibles, 10 puissance 500, un truc comme ça.

Mais vous imaginez bien que quand on doit faire des calculs à la main, et que pour la première racine, et le terme constant, on obtient ce terme-là, c'est impossible. C'est absolument impossible de continuer. C'est impossible.

C'est infaisable. C'est infaisable. À la main, c'est infaisable.

À l'ordinateur, c'est parfaitement faisable. C'est-à-dire qu'à l'ordinateur, vous faites le calcul. Vous demandez à l'ordinateur de vérifier, de calculer le polynôme minimal, etc. Il vous donne le résultat sans aucune difficulté et il vérifie toutes les propriétés. Et en plus, l'ordinateur va vous donner le groupe de Galois.

Donc, voilà comment le groupe de Galois, comme je vous l'ai dit, il est indexé par des paires de racines de l'équation auxiliaire. Ces paires sont indexées par des entiers et ces entiers sont très spécifiques. Ils sont donnés comme ça, par les racines de l'équation auxiliaire. Et à chaque paire de racines, le groupe de Galois vous donne une permutation. Il vous donne des permutations. Alors là, bien sûr, comme c'est le groupe symétrique, on a toutes les permutations paires possibles entre les racines. Ce n'est pas ce groupe-là en soi qui soit vraiment surprenant. C'est son indexation.

Et ensuite, bien sûr, quand on regarde avec Chebotarev et Dedekind, on s'aperçoit qu'on a effectivement toutes sortes de choses qui peuvent se produire. Vous voyez, par exemple, là, vous avez deux points fixes et puis une permutation cyclique. Là, vous avez un point fixe et deux permutations, deux involutions, etc.

Donc ça, c'est très simple. Alors maintenant, ce que je voulais faire, c'était peut-être aussi... Je n'avais jamais vu faire de manière concrète le fait que quand on adjoint une racine d'une équation auxiliaire, le groupe de Galois, qui était le groupe A_5 ici, va se casser en sous-groupes, mais qui ne seront pas des sous-groupes normaux. Ça, c'est un point essentiel que Galois a compris. Il a compris que quand on adjoint une seule racine d'une équation auxiliaire, le groupe de Galois va

diminuer, l'ambiguïté va diminuer, dans des cas particuliers. L'ambiguïté va diminuer, mais elle ne va pas diminuer de manière normale. C'est-à-dire qu'elle va diminuer d'une manière qui dépend du choix de cette racine auxiliaire. C'est extrêmement bizarre. C'est extrêmement bizarre parce que quand vous écrivez la factorisation en polynômes de degrés..., je ne sais plus quels degrés ils ont, ils sont de degré 10, en polynômes de degré 10, quand vous rajoutez cette équation à l'équation de tout à l'heure, à l'équation, je ne l'ai pas choisie au hasard, bien sûr, 109+493x-15x$^2 + 10x^4 + x^6$, quand vous rajoutez cette équation de degré 6, le polynôme se factorise ; il se factorise en termes de la racine adjointe ω. Mais la factorisation ne dépend pas du choix d'ω puisque c'est une factorisation abstraite.

Comment se fait-il que, alors que la factorisation ne dépend pas du choix de ω, le groupe de Galois, lui, se réduise d'une manière qui dépend de ω ? Alors, la manière dont ça arrive, c'est la chose suivante, c'est qu'en fait, ω va prendre six valeurs possibles. Et à chacune de ces six valeurs possibles, quand on regarde les racines d'un terme irréductible du polynôme qui est là, on va obtenir une partition de l'ensemble des 60 racines de l'équation de départ en six sous-ensembles de dix éléments. Alors, j'ai eu beaucoup de mal à la représenter.

J'ai voulu le faire avec des couleurs, ça ne marchait absolument pas, on ne voyait rien. Alors, j'ai finalement opté pour le jeu de cartes et puis j'ai rajouté un loup et puis un symbole un peu connu, c'est celui-là, voilà, d'accord. Et voilà, je vais vous montrer.

Donc, chaque fois que vous rajoutez une racine différente, il y a une partition différente des 60 racines de l'équation auxiliaire. Alors, si je change la racine, ça donne ça. Chaque fois, ce sont des partitions différentes. Chaque fois, ce sont des partitions différentes. Et à chacune de ces partitions, va correspondre un groupe de Galois différent et ce groupe de Galois différent, on peut le calculer, donc. On peut le calculer.

Alors ici, je crois que j'ai calculé pour la partition numéro 3, il me semble. Je vais regarder. Partition numéro 3, c'est ça, d'accord. Donc, je vais simplement vous montrer que ces groupes sont vraiment différents. Alors, il faut que je trouve un élément qui soit un peu typique. Alors, un élément typique, voilà. C'est un élément, par exemple, qui préserve ce point. Alors, je sais que le groupe, ça va être un groupe dihédral d'ordre 10, et je veux distinguer ce sous-groupe du groupe qui correspondra à l'adjonction, je crois que c'est l'adjonction de la numéro 2, ici. Donc, je vais chercher, ah ben voilà, je l'ai.

Ah non, c'est pas possible, ça. Ah non, ces deux-là sont les mêmes, voilà. On va chercher un autre point fixe.

D'accord, donc on va chercher un autre point fixe. Voilà, alors on va prendre ce point fixe-là, d'accord, et je vais le chercher dans le groupe du haut. D'accord, donc je vais chercher dans le groupe du haut, le truc qui fixe le point qui est là.

Alors, je vais chercher. Là, j'ai 10, donc je vais chercher ici. Non, j'ai pas.

Alors, ici. C'est lequel ? C'est celui-là, oui, que je vais fixer. Voilà.

Vous voyez que ce ne sont pas les mêmes. Vous voyez que la permutation qui fixe cette racine, il n'y en aura qu'une, elle n'est pas la même dans le sous-groupe obtenu en adjoignant la racine numéro 3 de la racine numéro 2. D'accord ? Et donc les sous-groupes sont distincts. Bon, alors ça c'était simplement, donc, si vous voulez, une expérimentation, bien entendu. Mais c'est une expérimentation qui, j'espère, montre absolument clairement, je veux dire, l'incroyable vision de Galois qui était capable, sans, à aucun moment, effectuer les calculs, de savoir les résultats que les calculs donneraient, et de voir infiniment plus loin parce que, si vous voulez, non seulement il a été capable de voir qu'une équation primitive est résoluble, si et seulement si on peut indexer ces racines par un corps fini qu'il avait défini et les permutations étant données par le produit semi-direct du groupe affine par le Frobenius, mais en fait il s'est aperçu après qu'il pouvait appliquer sa théorie aux fonctions elliptiques et aux divisions des fonctions elliptiques et c'était pour lui tout à fait un hasard.

Alors je voudrais terminer en revenant sur la fin, si vous voulez, en revenant sur, j'espère que ça va marcher ça, voilà, d'accord, donc en revenant sur la lettre que Galois a écrite à son ami Auguste Chevalier, donc la veille du duel, et dans cette lettre, il dit quelque chose de tout à fait cryptique, impossible presque à comprendre, à quoi on pourrait toujours essayer de donner 36 significations possibles, qui est la chose suivante, c'est dans le paragraphe du milieu :

> "*Tu sais mon cher Auguste que ces sujets ne sont pas les seuls que j'ai explorés, mes principales méditations depuis quelques temps ont été dirigées sur l'application à l'analyse transcendante de la théorie de l'ambiguïté ; il s'agissait de voir, a priori, dans une relation entre des quantités ou fonctions transcendantes quels échanges on pouvait faire* (vous voyez tout à l'heure on a vu pour des équations concrètes algébriques qu'il y a certains échanges qu'on ne pouvait pas faire ; il y a certaines équations qui n'étaient pas possibles comme l'équation $E = 4D^2 + 2D^2$) *quelle quantité on pouvait substituer aux quantités données sans que la relation puisse cesser d'avoir lieu. Cela fait reconnaître tout de suite l'impossibilité de beaucoup d'expressions que l'on pourrait chercher, mais je n'ai pas le temps, et mes idées ne sont pas encore assez développées sur ce terrain qui est immense.".*

Alors, je voudrais conclure si vous voulez de manière à bien faire voir à quel point la pensée de Galois n'est sûrement pas épuisée : la raison c'est la suivante, c'est que maintenant, on a dans les mathématiques modernes, bien sûr, comme je vous l'ai montré, on a parfaitement maîtrisé cette partie qui est la théorie de Galois qui est la théorie des équations etc., on la contrôle infiniment bien. Mais on a un problème analogue, on a un problème analogue plus difficile, bien sûr, que le problème de Galois, et qui est un problème transcendant, et dans ce problème-là, en gros, c'est comme si on avait une équation, ce qu'on appelle les fonctions L, c'est comme si on avait une équation, dont on ne sait même pas démontrer que les racines de cette équation sont toutes réelles ; on ne sait même pas, on en est sûr, parce qu'on peut le vérifier à l'ordinateur, on ne sait même pas démontrer que les racines de cette équation sont toutes réelles. Donc on n'est même pas au premier pas, qui est le pas des physiciens, si vous voulez, qui consiste à regarder où sont les racines de l'équation. Mais le pas suivant, c'est un pas qui est absolument évident tel qu'il est posé par Galois, c'est de développer la théorie de Galois pour ces équations-là. Et ça, ça commence un tout petit peu à exister, mais c'est une théorie qui est bien bien bien loin d'être développée et d'être comprise. Donc il faut bien voir

que réduire la théorie de Galois à son application au cadre classique de la théorie des corps, etc., ce serait quelque chose qui serait complètement illusoire parce qu'en fait, dans l'idée fondamentale qui est derrière, l'idée qui est infiniment difficile à expliquer, à saisir, il y a un potentiel qui est beaucoup plus grand que celui qui a été capturé par le formalisme des mathématiques modernes. Voilà je crois que je vais terminer ici.

(Applaudissements)

Le Président de séance : Même ceux qui n'ont pas tout compris, dont je suis, ont été captivés. On vous remercie, beaucoup, et ce qui est intéressant, c'est que vous puissiez dire que tout n'est pas fini, que ça peut encore se développer.

Alain Connes : Bien sûr.

Le Président de séance : La seule question que je voulais vous poser personnellement, c'est de savoir quel crédit on donne à Galois dans les autres pays que notre pays.

Alain Connes : Eh bien en fait, on lui donne plus de crédit qu'en France, puisque par exemple, les corps finis sont appelés les corps de Galois dans tous les pays étrangers. Pas en France ! Donc je vais dire, non, son crédit est immense : je veux dire, ce qu'on appelle groupe de Galois, théorie de Galois, c'est un nom qui est utilisé tout le temps, le nom de Galois est utilisé en permanence ; on appelle extension galoisienne l'extension qui provient de l'équation auxiliaire etc. etc. donc je veux dire il est omniprésent, il est omniprésent. C'est incroyable, cette destinée, c'est une destinée absolument incroyable, penser qu'il n'a jamais eu vraiment la sûreté, à aucun moment, que son travail allait être reconnu, à aucun moment, même au moment où il est mort, je veux dire, à aucun moment, il n'a eu le sentiment que son travail, il faut dire que bon, on comprend, j'espère que vous avez compris, à quel point les relations avec Abel sont complexes et intéressantes, et à quel point, justement, je veux dire, il n'était pas dans une situation simple ; en gros, il a pris le relais, en gros, Abel est mort, et puis Galois est arrivé, il a pris le relais, c'est comme s'ils s'étaient passés le relais de l'un à l'autre, c'est quelque chose d'incroyable. On aurait bien tort de dire "l'un a fait plus que l'autre", ce serait ridicule, ce serait grotesque. Galois avait compris indépendamment, il n'aurait rien fait s'il était parti de là où Abel était, il avait compris indépendamment, il lisait les papiers de Cauchy, les papiers de Lagrange, les papiers de Gauss, et à partir de là, il avait compris énormément de choses...

Le Président de séance : Est-ce que c'est possible d'imaginer ce qu'il aurait fait s'il n'avait pas...

Alain Connes : On n'en sait rien on ne peut absolument rien dire, c'est comme "qu'est-ce que Mozart aurait composé ?". Qui peut dire quoi que ce soit là-dessus personne.

Le Président de séance : Si, Mozart aurait fait de la musique.

Alain Connes : Oui, bon, peut-être.

Le Président de séance : Bien, la discussion est ouverte ; je pense qu'il va y avoir beaucoup

de questions.

Jean-Pierre Kahane[2] : Juste où en est-on de la dernière phrase ? C'est-à-dire est-ce qu'on a avancé depuis Galois, sur le programme de Galois, i.e. l'extension aux fonctions transcendantes ?

Alain Connes : Non, il y a pas mal de théories qui peuvent prétendre à ça, en particulier la théorie de Malgrange et Ramis, bien entendu, mais je veux dire, si on est un peu, comment dire, un peu simples, un peu naïfs, on peut dire que ce qui remplace les équations, ce sont les fonctions L. Et on a la notion de factorisation, il y a des fonctions L qui se factorisent etc., il y a des fonctions L dont on pense qu'elles sont irréductibles en un sens convenable etc. La théorie de Galois pour les fonctions L, c'est un peu la théorie des motifs, mais bon, je veux dire, par exemple, trouver des relations non triviales entre les racines, entre les zéros de la fonction ζ de Riemann, pour le moment, personne ne sait rien là-dessus. Donc on voit bien qu'il y a des relations, il y a les fonctions symétriques de la fonction ζ de Riemann, ça, ce sont les formules explicites de Riemann et Weil qui donnent les fonctions symétriques : on les connaît, on les exprime en termes des fonctions qui comptent les nombres premiers, mais les fonctions qui ne sont pas symétriques, est-ce qu'il existe des relations qui ne sont pas des fonctions symétriques, on le sait un peu, parce qu'on a des relations entre les zéros qui imposent de compter les zéros de manière symétrique par rapport à la droite réelle, et ce ne sera pas des relations qui seront invariantes par toutes les symétries, mais on est très peu avancé dans ce domaine et si Galois avait vécu, il aurait peut-être eu l'article de Riemann, sur la conjecture de Riemann, il aurait peut-être développé sa théorie dans ce cadre-là. On n'en sait rien, on ne peut rien dire, personne ne peut dire quoi que ce soit là-dessus.

Le Président de séance : Est-ce qu'il y a d'autres questions ? Monsieur Pecker[3] ?

Jean-Claude Pecker : Excusez-moi, c'est plutôt sur la première partie de ton exposé que je voudrais poser une question : la dernière lettre qui est projetée, celle de Galois à Chevalier, que tu nous as projetée, dit bien qu'il n'a plus eu le temps de faire quelque chose, de développer telle théorie ou telle autre ; est-ce que ça veut dire qu'il s'attendait à être tué en duel ?

Alain Connes : Bon c'est très compliqué, disons qu'il n'a plus eu le temps, c'est plus compliqué que ça. Galois avait passé la dernière année de sa vie en prison. En prison, il a continué à faire des maths et ça, avec un mérite absolument incroyable, parce qu'il n'était pas dans une petite chambre tranquille, avec des bouquins, il était au milieu des autres prisonniers. La prison Sainte-Pélagie, c'était une prison où tous les prisonniers étaient ensemble, et de temps en temps, ses collègues le forçaient à boire. À un moment donné, il avait été obligé de vider une bouteille d'eau de vie, il avait été malade comme un chien, et au moment où Nerval l'a vu dans cette prison, Nerval a dit que Galois avait l'air d'avoir 50 ans ; il n'avait pas encore 20 ans. Donc il était déjà extrêmement usé physiquement, par le fait qu'il continuait à travailler malgré la prison. Alors ensuite ce qui s'est passé, pour le duel, il y a 36 versions, il y a plusieurs versions, il y a la version du bouquin de Infeld, il y a la version du complot, il y a un tas de versions différentes, Jean-Pierre Kahane m'a donné un bouquin qui a une autre version, on ne peut rien dire ; par contre, c'est évident qu'il pensait qu'il n'avait pas beaucoup de chance d'en sortir, de ce duel, il y avait une histoire

[2]Jean-Pierre Kahane, mathématicien français et académicien (1926 - 2017).

[3]Jean-Claude Pecker (1923 - 2020) : astrophysicien français.

de femme, il s'était mis dans de sales draps etc. il avait été provoqué, on ne sait pas, comme je l'ai dit, s'il y avait un complot etc. Mais en tout cas, on imagine mal que Galois était un expert dans le tir au pistolet. Et je ne connais pas les détails, j'avais entendu une fois mais je ne peux pas certifier mes sources, qu'en fait, au lieu d'être un duel dans lequel ils étaient à une vingtaine de mètres et puis ils se rapprochaient à 10 mètres et ils se tiraient l'un sur l'autre, j'ai entendu dire mais je n'en suis pas sûr, qu'en fait, c'était un duel dans lequel un seul des deux pistolets était chargé, ils mettaient chacun le pistolet sur le ventre de l'autre et ils tiraient. Donc bon, je vais dire, il n'a pas eu, il y avait une chance sur deux qu'il s'en sorte, et une chance sur deux qu'il y reste. Et bien sûr, il n'est pas mort tout de suite, il est mort de péritonite, le lendemain, à l'hôpital, vous connaissez l'histoire mais c'est bien évident que quand il disait qu'il n'avait pas le temps, c'est qu'il n'avait pas le temps d'écrire ses idées, mais les idées, il les avait en tête. Quand il disait "je n'ai pas le temps", c'est qu'il n'avait pas le temps d'écrire, mais les idées, il les avait en tête. Ça c'est évident.

Le Président de séance : La chirurgie est honteuse de ne pas avoir pu corriger cette péritonite. Monsieur Balian ?

Roger Balian : C'est simplement pour signaler un tout petit fait, à propos du manque d'hommage officiel à Galois, il y a une rue Galois à Bourg-la-Reine, mais c'est son père.

Alain Connes : C'est son père, absolument, il y a une autre rue Galois à Vitry, mais elle est en dehors du périphérique, et je pense que l'Académie s'honorerait, en demandant qu'une plaque soit mise au 5 rue de la Sorbonne, disant simplement "En cet endroit, Galois a donné un cours d'algèbre en janvier, donc si je me souviens bien, c'est janvier 1830".

Un auditeur : Si vous me permettez, non pas une question, mais deux remarques ; la première, c'est que je crois que le portrait que vous avez montré au début c'est celui de son frère, fait de mémoire par son frère, et non pas par Auguste Chevalier.

Alain Connes : Oui vous avez raison, parfaitement, j'ai hésité, j'avais une hésitation, et c'était une des rares mais celle-là, c'était une hésitation fondée, tout à fait.

Le même auditeur : Alors j'ai une autre remarque c'est qu'il existe une rue Galois dans Paris, mais elle n'est pas à l'intérieur du périphérique, elle est juste à droite de la porte des Lilas, c'est ça elle fait 80 mètres de long, elle n'est effectivement pas à la hauteur du personnage.

Alain Connes : On ne peut pas, c'est insensé, je veux dire...

Le même auditeur : Si vous permettez une troisième chose, c'est que le Conseil de Paris a voté je crois, le 17 octobre, le fait de mettre une plaque à la mémoire d'Évariste Galois au 16 rue des Bernardins, qui est le domicile qu'il avait eu avant sa deuxième incarcération.

Alain Connes : bon bon bon bon bon bon bon.

Le même auditeur : Ça n'interdit absolument pas de mettre une plaque au 5 rue de la Sorbonne.

Alain Connes : Oui pourquoi pas.

Le même auditeur : Il n'y a plus de librairie, mais il y a quand même une grande maison.

Alain Aspect : C'est une blague comme personne n'a de questions sérieuse à poser : on pourrait imaginer un Prix Évariste Galois, et j'étais en train de réfléchir aux sociétés qu'on pourrait solliciter comme sponsor, et il m'est passé par la tête l'idée saugrenue, connaissant la personnalité d'Évariste Galois, qu'on pourrait demander aux banques, qui bénéficient des mathématiques pour faire les choses, je ne suis pas sûr que la mémoire d'Évariste Galois apprécierait, mais par contre, l'idée que vous fassiez quelque chose, les mathématiciens, pour un grand prix Évariste Galois, en trouvant un sponsor honorable, ça peut peut-être se trouver, quand même...

Alain Connes : Oui, mais il y a déjà un prix Abel, je ne sais pas...

Le Président de séance : d'autres questions ? Non... S'il n'y a pas d'autres questions, tout le monde est impressionné, c'est comme cela qu'il faut interpréter ce silence admiratif. On vous remercie infiniment.

(Applaudissements).

Traduction du latin au français d'un extrait[1] du livre *Werke : Hoehere Arithmetik* de Gauss (Denise Vella-Chemla, février 2024)

Résumé
Au sujet de certaines séries particulières.
1.

Parmi les vérités les plus significatives auxquelles la théorie de la division du cercle a ouvert l'accès, la synthèse proposée dans l'article 356 des *Disquisitiones Arithmeticae* revendique une place non négligeable en arithmétique, non seulement en raison de son élégance particulière et de sa merveilleuse créativité, qu'une autre discussion aura l'occasion d'expliquer plus en détail ci-après, mais aussi parce que sa démonstration rigoureuse et complète se heurte à des difficultés assez fréquentes. Ce qui, bien sûr, aurait dû être d'autant moins attendu, puisqu'ils ne relèvent pas tant du théorème lui-même, que d'une certaine limitation du théorème, plutôt, par laquelle la démonstration négligée est immédiatement prête et est très facilement dérivée de la théorie, comme nous l'expliquerons dans cet article. Le théorème y est présenté sous la forme suivante. En supposant que n est un nombre premier, et en désignant tous les résidus quadratiques de n entre les limites 1 et $n-1$ inclus par a, et tous les non-résidus compris entre les mêmes limites par b, et enfin par ω l'arc et par k l'intégrale déterminée par tout ce qui n'est pas divisible par n.

- I. pour les valeurs de n, de la forme $4m+1$, on aura

$$\begin{aligned}
\Sigma \cos a\,k\,\omega &= -\tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{n} \\
\Sigma \cos b\,k\,\omega &= -\tfrac{1}{2} \mp \tfrac{1}{2}\sqrt{n}, \quad \text{et ainsi} \\
\Sigma \cos a\,k\,\omega - \Sigma \cos b\,k\,\omega &= \pm\sqrt{n} \\
\Sigma \sin a\,k\,\omega &= 0 \\
\Sigma \sin b\,k\,\omega &= 0
\end{aligned}$$

- II. pour les valeurs de n, de la forme $4m+3$, on aura

$$\begin{aligned}
\Sigma \cos a\,k\,\omega &= -\tfrac{1}{2} \\
\Sigma \cos b\,k\,\omega &= -\tfrac{1}{2} \\
\Sigma \sin a\,k\,\omega &= \pm\tfrac{1}{2}\sqrt{n} \\
\Sigma \sin b\,k\,\omega &= \mp\tfrac{1}{2}\sqrt{n} \\
\Sigma \sin a\,k\,\omega - \Sigma \sin b\,k\,\omega &= \pm\sqrt{n}
\end{aligned}$$

[1] pages 11 à 15.

Ces calculs de sommes y ont été démontrées en toute rigueur, et aucune autre difficulté ne subsiste ici que dans la détermination du signe de la quantité radicale. En effet, on sait concernant le signe en question, dans la mesure où cela dépend du nombre k, que le même signe doit toujours être valable pour toutes les valeurs de k qui sont résidus quadratiques de n, et le signe opposé à celui-ci pour toutes les valeurs de k qui sont pas résidus quadratiques de n. Ici toute la tâche se concentrera sur la valeur $k = 1$. et il est clair que, dès que le signe valable pour cette valeur sera connu, les signes pour toutes les autres valeurs de k en seront immédiatement déduisibles. Car il est vrai que dans cette question même, qui à première vue semble être considérée comme l'une des plus faciles, nous nous sommes heurtés à des difficultés inattendues, et la méthode par laquelle nous avons progressé jusqu'ici sans entrave nous prive complètement de toute aide ultérieure.

2.

Il ne sera pas déplacé, avant d'aller plus loin, d'avoir développé quelques exemples de sommes au moyen de calculs numériques qu'il conviendra de faire précéder de quelques observations générales.

I. Si n est un nombre premier de la forme $4m + 1$, on note par a' tous les résidus quadratiques de n compris entre 1 et $\frac{1}{2}(n-1)$ et par b' tous les non-résidus compris entre les mêmes limites, il est clair que tous les $n - a'$ seraient compris dans les a, et que tous les $n - b'$ le seraient dans les b : donc puisque tous les $a', b', n - a', n - b'$ couvrent l'ensemble des nombres $1, 2, 3.....n - 1$, tous les a' combinés avec les $n - a'$ incluront tous les a et de même tous les b' avec tous les $n - b'$ incluront tous les b. On aura

$$\begin{aligned}
\Sigma \cos\ a\,k\,\omega &= \Sigma \cos\ a'\ k\ \omega + \Sigma \cos(n-a')\ k\ \omega \\
\Sigma \cos\ b\ k\omega &= \Sigma \cos\ b'\ k\ \omega + \Sigma \cos(n-b')\ k\ \omega \\
\Sigma \sin\ a\,k\,\omega &= \Sigma \sin\ a'\ k\ \omega + \Sigma \sin(n-a')\ k\ \omega \\
\Sigma \sin\ b\,k\,\omega &= \Sigma \sin\ b'\ k\ \omega + \Sigma \sin(n-b')\ k\ \omega
\end{aligned}$$

Maintenant, quand on considère $\cos(n - a')k\ \omega = \cos a'\ k\omega$, $\cos(n - b')k\ \omega = \cos b'\ k\omega$, $\sin(n - a')k\ \omega = -\sin a'\ k\omega$, $\sin(n - b')k\ \omega = -\sin b'\ k\omega$, il est clair qu'en découle immédiatement

$$\begin{aligned}
\Sigma \sin\ a\ k\ \omega &= \Sigma \sin\ a'\ k\ \omega - \Sigma \sin\ a'\ k\ \omega = 0 \\
\Sigma \sin\ b\ k\ \omega &= \Sigma \sin\ b'\ k\ \omega - \Sigma \sin\ b'\ k\ \omega = 0
\end{aligned}$$

La somme des cosinus prend cependant cette forme

$$\begin{aligned}
\Sigma \cos\ a\ k\ \omega &= 2 \cos\ a'\ k\ \omega \\
\Sigma \cos\ b\ k\ \omega &= 2 \cos\ b'\ k\ \omega
\end{aligned}$$

où l'on doit faire

$$\begin{aligned}
1 + 4\Sigma \cos\ a'\ k\omega &= \pm\sqrt{n} \\
1 + 4\Sigma \cos\ b'\ k\omega &= \mp\sqrt{n} \\
2\Sigma \cos\ a'\ k\ \omega - 2\Sigma \cos\ b'\ k\omega &= \pm\sqrt{n}
\end{aligned}$$

II. Dans le cas où n est de la forme $4m+3$, le complément de tout résidu de a à n sera un non-résidu, et le complément de tout b sera un résidu ; donc tous les $n - a$ s'accordent avec tous les b, et tous les $n - b$ avec tous les a. On obtient

$$\Sigma \cos\ a\,k\,\omega = \Sigma \cos(n-b)k\omega = \Sigma \cos\ b\,k\,\omega$$

par conséquent, lorsque tous les a et b combinés couvrent tous les nombres $1, 2, 3....n-1$. On a ainsi

$$\Sigma \cos\ a\,k\,\omega + \Sigma \cos\ b\,k\,\omega = \cos\ k\omega + \cos\ 2\ k\omega + \cos\ 3\ k\omega + \text{etc.} + \cos(n-1)k\ \omega = -1$$

en résumant

$$\Sigma \cos\ a\,k\,\omega = -\tfrac{1}{2}$$

$$\Sigma \cos\ b\ k\omega = -\tfrac{1}{2}$$

qui sont automatiquement satisfaites. Il en sera de même de

$$\Sigma \sin\ a\ k\ \omega = \Sigma \sin(n-b)k\ \omega = -\Sigma \sin\ b\ k\ \omega$$

d'où il ressort clairement les sommes

$$2\ \Sigma \sin\ a\ k\omega = \pm\sqrt{n}$$
$$2\ \Sigma \sin\ b\,k\,\omega = \mp\sqrt{n}$$

l'une dépendant de l'autre.

3.

Voici les calculs numériques pour quelques exemples :

I. Pour $n = 5$, il y a une valeur de a', qui est $a' = 1$ et une valeur de b', qui est $b' = 2$; on a

$$\cos\ \omega = +0.3090169944 \qquad \cos\ 2\ \omega = -0,8090169944$$

et ainsi $1 + 4\ \cos\ \omega = +\sqrt{5}, \quad 1 + 4\ \cos\ 2\omega = -\sqrt{5}$.

II. Pour $n = 13$, il y a trois valeurs pour a', qui sont $1, 3, 4$, et le même nombre de valeurs de b', qui sont $2, 5, 6$, on calcule ainsi

cos ω = +0,8854560257	cos 2 ω = +0.5680647467
cos 3 ω = +0,120 5366803	cos 5 ω = -0,7485107482
cos 4 ω = -0.3546048870	cos 6 ω = -0,9709418174
Somme = +0,6513878190	Somme = -1,1513878189

Hine $1 + 4\Sigma \cos\ a'\ \omega = +\sqrt{13}, \quad 1 + 4\Sigma\ \cos\ b'\ \omega = -\sqrt{13}$.

III. Pour $n = 17$, on a 4 valeurs de a', ici $1, 2, 4, 8$, et le même nombre de valeurs pour b', qui sont $3, 5, 6, 7$. On peut calculer les cosinus

cos ω = +0.932472294	cos 3 ω = +0.4457383 558
cos 2 ω = +0,7390089172	cos 5 ω = -0,2736629901
cos 4 ω = +0,0922683595	cos 6 ω = -0,60 26346364
cos 8 ω = -0,9829730997	cos 7 ω = -0,8502171357
Somme = +0,7807764064	Somme = -1,2807764065

Donc $1 + 4\Sigma \cos a' \omega = +\sqrt{17}, \quad 1 + 4\Sigma \cos b' \omega = -\sqrt{17}.$

IV. Pour $n = 3$, la valeur de a est unique, $a = 1$ à quoi correspond $\sin \omega = +0.8660254038$.

Donc $2 \sin \omega = +\sqrt{3}$.

V. Pour $n = 7$, il y a trois valeurs pour a, qui sont $1, 2, 4$: on a donc les sinus

$$\begin{array}{rcl} \sin \omega & = & +0.7818314825 \\ \sin 2\,\omega & = & +0{,}9749279122 \\ \sin 4\,\omega & = & -0{,}4338837391 \\ \hline \text{Somme} & = & +1{,}3228756556, \end{array}$$

donc $2 \Sigma \sin a \omega = +\sqrt{7}$.

VI. Pour $n = 11$, les valeurs de a sont $1, 3, 4, 5, 9$, auxquelles correspondent les sinus

$$\begin{array}{rcl} \sin \omega & = & +0{,}5406408175 \\ \sin 3\,\omega & = & +0{,}9898214419 \\ \sin 4\,\omega & = & +0{,}7557495744 \\ \sin 5\,\omega & = & +0{,}2817325568 \\ \sin 9\,\omega & = & -0{,}9096319954 \\ \hline \text{Somme} & = & +1{,}6583123952, \end{array}$$

et donc $2 \Sigma \sin a \omega = +\sqrt{11}$.

VII. Pour $n = 19$, les valeurs de a sont $1, 4, 5, 6, 7, 9, 11, 16, 17$, auxquelles correspondent les sinus

$$\begin{array}{rcl} \sin \omega & = & +0{,}3246994692 \\ \sin 4\,\omega & = & +0.9694002659 \\ \sin 5\,\omega & = & +0{,}9965844930 \\ \sin 6\,\omega & = & +0{,}9157733267 \\ \sin 7\,\omega & = & +0.7357239107 \\ \sin 9\,\omega & = & +0.1645945903 \\ \sin 11\,\omega & = & -0{,}4759473930 \\ \sin 16\,\omega & = & -0{,}8371664783 \\ \sin 17\,\omega & = & -0{,}6142127127 \\ \hline \text{Somme} & = & +2{,}1794494718, \end{array}$$

donc $2 \Sigma \sin a \omega = +\sqrt{19}$.

Transcription de la section 356 des Recherches arithmétiques (page 463 et suivantes dans le livre aux éditions Jacques Gabay).

On doit surtout remarquer les équations auxiliaires par lesquelles on détermine, pour une valeur quelconque de n, les sommes des périodes qui forment l'ensemble Ω : elles sont liées d'une manière étonnante avec les propriétés les plus abstraites du nombre n. Mais ici nous restreindrons nos considérations aux deux cas suivants : 1° à l'équation du second degré qui donne les sommes des périodes de $\frac{n-1}{2}$ termes ; 2° quand $n-1$ est divisible par 3, à l'équation du troisième degré qui donne les sommes des périodes de $\frac{n-1}{3}$ termes.

Faisons, pour abréger, $\frac{1}{2}(n-1) = m$ et désignons par g une racine primitive quelconque, Ω sera composé de deux périodes $(m,1)$ et (m,g), la première contenant les racines $[1],[g^2],[g^4],....[g^{n-3}]$, et la seconde les racines $[g],[g^3],[g^5],....$: $[g^{n-2}]$. Supposons que les résidus minima positifs des nombres $g^2, g^4, ...g^{n-3}$ suivant le module n, soient R, R', R'', etc., abstraction faite de l'ordre, et que les résidus des nombres $g, g^3 \cdots g^{n-2}$ soient N, N', N'' etc. ; les racines des périodes $(m,1)$ et (m,g) coïncideront avec

$$[1],[R],[R'],[R''],etc., \qquad [N],[N'],[N''],etc.$$

respectivement. Or il est clair que tous les nombres $1, R, R', R''$, etc. sont résidus quadratiques de n ; comme ils sont différents, moindres que n et au nombre de $\frac{n-1}{2}$, il s'ensuit que ce sont effectivement tous les résidus quadratiques de n, positifs et plus petits que lui (n° 96). Il suit de là en même temps, que les nombres N, N', N'', etc. qui sont tous différents entre eux, et des nombres $1, R, R'$, etc., et qui, joints à ces derniers, épuisent les nombres $1, 2, 3, ..., n-1$ sont tous les non-résidus quadratiques positifs de n et plus petits que lui. Si l'on suppose maintenant que l'équation dont $(m,1),(m,g)$ sont racines, soit

$$x^2 - Ax + B = o,$$

on a

$$A = (m,1) + (m,g) = -1, \qquad B = (m,1) \times (m,g);$$

or (n° 345),

$$(m,1) \times (m,g) = (m, N+1) + (m, N'+1) + (m, N''+1) + \text{etc.} = W$$

et peut par conséquent être mis sous la forme

$$\alpha(m,0) + \beta(m,1) + \gamma(m,g).$$

Pour déterminer les coefficients α, β, γ, observons : 1°. qu'on a $\alpha+\beta+\gamma = 0$, puisque le nombre des périodes de W est m ; 2°. que $\beta = \gamma$ (n° 350) puisque $(m,1) \times (m,g)$ est une fonction invariable des sommes $(m,1)$ et (m,g) qui composent la période plus grande $(n-1,1)$ 3°. que tous les nombres $N+1, N'+1, N''+1$, etc. étant compris entre les limites 2 et $n+1$, il est clair que nulle période de W ne coïncidera avec $(n,0)$, ou qu'il n'y en aura qu'une, par exemple (m,n) ; on aura donc $\alpha = 1$ ou $= 0$ suivant que $n-1$ sera ou ne sera pas parmi les nombres N, N', etc.; il suit de la que dans le premier cas on aura $\alpha = 1, \beta = \gamma = \frac{m-1}{2}$ et dans le second $\alpha = 0, \beta = \gamma = \frac{m}{2}$ et comme β et γ doivent être entiers, le premier cas aura lieu, c'est-à-dire que $n-1$ ou -1 se trouvera parmi les non-résidus de n lorsque m sera impair, c'est-à-dire lorsque n sera de la forme $4n+3$; le second

aura lieu au contraire quand m sera pair, c'est-à-dire quand n sera de la forme $4n+1$. Ainsi, comme on a $(m,0)=m$ et $(m,1)+(m,g)=-1$, le produit cherché sera donc, suivant les mêmes circonstances, $\frac{1}{2}(m+1)$ ou $\frac{-1}{2}m$ et l'équation sera, dans le premier cas,

$$x^2+x+\frac{1}{4}(n+1)=0, \text{ qui donne } x=-\frac{1}{2}\pm\frac{1}{2}i\sqrt{n},$$

et dans le second

$$x^2+x-\frac{1}{4}(n-1)=0, \text{ qui donne } x=-\frac{1}{2}\pm\frac{1}{2}\sqrt{n}.$$

Ainsi, quelle que soit la racine que l'on ait prise pour [1], si l'on désigne par $\Sigma[R]$ la somme de toutes les racines $[1],[R],[R']$, etc., et par $\Sigma[N]$ celle des racines $[N],[N']$, etc., on aura

$$\Sigma[R]-\Sigma[N]=\pm\sqrt{n} \text{ ou } =\pm i\sqrt{n},$$

suivant que $n\equiv 1$ ou $\equiv 3 \pmod 4$. Il suit facilement de là que k étant un nombre entier quelconque non-divisible par n, on a

$$\Sigma \cos\tfrac{kRP}{n}-\Sigma \cos\tfrac{kNP}{n}=\pm\sqrt{n}, \qquad \text{ou } =0,$$

$$\Sigma \sin\tfrac{kRP}{n}-\Sigma \sin\tfrac{kNP}{n}=0, \qquad \text{ou } =\pm\sqrt{n},$$

suivant que $n\equiv 1$ ou $\equiv 3 \pmod 4$, théorèmes remarquables par leur élégance.

Au reste, nous ferons observer que le signe supérieur a lieu quand k est l'unité, ou plus généralement quand k est résidu quadratique de n, et le signe inférieur, quand k est non-résidu. Ces théorèmes conservent toute leur élégance, ou plutôt en acquièrent encore davantage, lorsque n est un nombre composé quelconque ; mais nous sommes forcés de supprimer ces recherches qui demanderaient trop de développement, et de les réserver pour une autre occasion.

Traduction de l'allemand au français d'une lettre manuscrite de Encke à Gauss du 4 décembre 1849[1]

Encke à Gauß, Berlin, le 4 décembre 1849

SUB: Gauss, lettres A: Encke, 126

Votre dernière lettre, très honoré Monsieur le Conseiller privé, m'a énormément plu, car elle m'a assuré de la poursuite sereine de la belle relation dans laquelle je me vois toujours avec vous. Il était particulièrement important pour moi que vous ne preniez pas mon absence à votre anniversaire de manière négative, mais que vous la considériez plutôt à la lumière de la manière dont cela s'est réellement produit.

La période troublée continue. Les activités des partis, dont la fin du procès de Waldeck a donné un exemple clair, deviennent de plus en plus haineuses, et le moment où viendra le calme tant attendu est encore loin. À titre d'exemple, je peux vous citer que récemment, mon fils de Wittenberg m'a écrit qu'il y avait un article dans la Neue Preußische Zeitung sur l'observation depuis l'observatoire au rez-de-chaussée. Je ne l'avais pas lu. Ayant été informé de cela, j'ai regardé de plus près et je l'ai effectivement trouvé à la date du 1er décembre, la suite est à nouveau datée de l'observatoire du rez-de-chaussée à droite. Comme je n'ai rien à voir avec la rédaction ni avec toute la direction du journal, j'ai écrit au rédacteur en chef et lui ai demandé de mettre mes lignes en retrait. Au lieu de cela, il s'est rétracté dans le journal d'aujourd'hui, non pas comme je le souhaitais, mais avec une phrase quelque peu ambiguë. Cependant, avec tous les mouvements politiques, il arrive toujours que la presse quotidienne se salisse, et donc il faut laisser les choses suivre leur cours.

Dans l'ensemble, on peut être satisfait de l'évolution des affaires ici, tant on pourrait s'attendre à beaucoup de choses dans une période aussi mouvementée. Les négociations de chambre se poursuivent tranquillement, et bien que le point difficile des relations entre l'Église, l'école et l'État, qui à mon avis est bien plus important pour le libertinage actuel que toutes les questions fiscales, n'ait pas été clarifié, et certaines dispositions seront intenables, alors il y a des raisons d'espérer qu'avec une meilleure compréhension, un meilleur arrangement verra également le jour. Bien entendu, cela comporte le danger que, comme cela semble être le cas aujourd'hui en France, la société se dissolve d'abord pour se reconstituer. Oh, le procès de Waldeck, dans lequel la falsification de preuves déjà faibles a été niée par le procureur lui-même, aura des conséquences négatives, mais aussi positives. Il y en a encore un nombre considérable, même parmi les hauts fonctionnaires, qui ont une peur vraiment comique de la réaction dont la NP Zeitung était considérée comme l'organe. Ils seront satisfaits du coup que leur ont porté les audiences du tribunal, et au moins ils ne s'opposeront plus de manière aussi systématique. En revanche, il est à craindre que le pouvoir de la police contre les sociétés secrètes démocratiques soit pour l'instant quelque peu paralysé. Il est certain que ceux-ci existent et ont un certain lien, tout comme l'absence totale d'implication ou d'ignorance de Waldeck à l'égard des soulèvements. Cependant, pour le moment, vous ne remarquez rien. Hier après-midi, je suis arrivé par hasard dans Unter den Linden au milieu du train, les personnes qui me semblaient être dans un wagon vide s'étaient demandé dans quel coin de la forêt elles étaient assises.

[1]Référence : voir cette page https://gauss.adw-goe.de/handle/gauss/2714.

Il est étrange de voir comment, dans un tel rassemblement, certains dirigeants parviennent à garder leur calme par leur seule voix, et c'est assez instructif pour la compréhension de la Révolution française, avoir vu de telles scènes à petite échelle. Il n'est pas possible d'obtenir une idée plus claire de la manière dont les masses peuvent être mises en mouvement. Curieusement, l'expérience se répète ici ; comme toujours, il y a des gens qui croient pouvoir contrôler les masses. mis en mouvement sans considérer que même les gens les plus énergiques ont toujours été dépassés et que les vrais dirigeants comme Napoléon ont toujours évité le contact avec les masses. D'ailleurs, je n'ai vu aucun militaire lors de mon voyage d'affaires dans une grande partie de la ville. La simple peur des militaires a tout freiné et je n'ai vu aucun désordre.

En attendant, je constate que dans mes rapports, je tombe toujours sur des choses que je n'aurais certainement pas rapportées en d'autres temps. Veuillez excuser ces digressions qui attirent inévitablement mon attention.

Je voudrais également vous envoyer l'annuaire, qui contient un autre petit essai avec des tableaux qui, je pense, seront utiles. Au moins, j'en ai manqué des similaires parfois.

Je voudrais également ajouter un petit fait ici, qui n'a théoriquement aucune valeur, mais qui m'a donné une idée un peu plus claire que celle que j'avais de la répartition des nombres premiers. Dirichlet avait mentionné lors d'une conférence à l'Académie que le lien entre le logarithme hyperbolique d'un nombre et le nombre de nombres premiers jusqu'à ce nombre avait été établi pour la première fois par Legendre. Je me souviens avoir lu quelque chose de similaire dans la correspondance d'Euler, éditée par Fuß, et en fait, il est écrit T. I, Lettre CXLIX, figure. 587, le passage étrange mais certainement imprimé ou prescrit : Puisque le nombre de tous les nombres premiers est infini, mais pourtant un infini de l'ordre le plus bas, car j'ai montré que si le nombre de tous les nombres est $= n$, le nombre des nombres premiers parmi eux sera ln, mais il est ln plus petit que le nombre n, etc.

Cela m'a incité à chercher une formule. qui est simple et, lorsque cela est possible, suit encore plus fidèlement le nombre de nombres premiers depuis le début jusqu'à un certain nombre, comme la formule[2]dans la lettre $\frac{n}{\ln n}$. Après quelques essais j'ai trouvé la formule

$$\frac{n}{\ln n}^{\,2\ln n\sqrt{10}}$$

et ainsi comparé le nombre de nombres premiers donné selon le tableau des additions de Lambert. Ce qui suit est la comparaison.

La formule $\frac{n}{\ln n}^{\,2\ln n\sqrt{10}}$ revient après quelques écarts, ce qui bien sûr tombe toujours du côté positif, mais revient toujours à 0 et donne, si l'on exclut les endroits comme ceux entre 68 000 et 69 000 et entre 69 000 et 70 000, où 80 et 81 nombres premiers n'apparaissent que deux fois de suite sur mille, alors qu'après le cours continu, environ 89,6 devraient apparaître, le nombre de nombres premiers (dont 1) augmente jusqu'à environ 5 ou 6 unités. Elle sera donc également approximativement plus précise pour déterminer le nombre de nombres premiers au-delà de 10 000 que la simple fraction

[2] *Note de la transcriptrice : Encke écrit systématiquement* ln*, au lieu de* $\ln n$.

$\frac{n}{\ln n}$, qui n'arrive que lorsque n est très grand.

La situation de Schumacher semble toujours très embarrassante. L'ancien envoyé danois ici, Chambellan Reetz, espérait surtout un succès favorable grâce à son influence personnelle à Copenhague. Pendant ce temps, il est là depuis longtemps sans que les choses changent, semble-t-il.

Recevez votre aimable bonne volonté

le vôtre

4/12/1849. le plus dévoué

Encke

Dans les tableaux de la lettre de Encke reportés aux pages suivantes, on a ajouté deux colonnes qui montrent le nombre effectif de nombres premiers qui aurait dû être calculé ; puisqu'il est noté 5 dans la lettre d'Encke pour le nombre de nombres premiers inférieurs à 10, 1 a dû être compté comme étant un nombre premier. On considère donc qu'il y a une erreur si la différence est de 0 ou de 2 avec le nombre effectif de nombres premiers qu'il eût fallu compter.

n	formule	$\pi(x)$	Diff	corr.	
10	7.2	5	+2	4	
100	27.9	26	+2	25	
200	46.9	47	0	46	
300	64.4	63	+1	62	
400	80.9	79	+2	78	
500	96.8	96	+1	95	
600	112.3	110	+2	109	
700	127.4	126	+1	125	
800	142.2	140	+2	139	
900	156.7	155	+2	154	
1000	171.0	169	+2	168	
1100	185.1	185	0	184	
1200	199.1	197	+2	196	
1300	212.9	212	+1	211	
1400	226.5	223	+4	222	
1500	240.1	240	0	239	
1600	253.5	252	+1	251	
1700	266.8	267	0	266	
1800	280.0	279	+1	278	
1900	293.1	291	+2	290	
2000	306.2	304	+2	303	
3000	432.6	431	+2	431	*
4000	554.1	551	+3	551	*
5000	672.0	670	+2	669	
6000	787.3	784	+3	783	
7000	900.4	901	−1	901	*
8000	1011.8	1008	+4	1007	
9000	1121.7	1118	+4	1118	*
10000	1230.3	1230	0	1229	
11000	1337.8	1336	+2	1335	
12000	1444.2	1439	+5	1438	
13000	1549.7	1548	+2	1548	*
14000	1654.4	1653	+1	1652	
15000	1758.3	1755	+3	1754	
16000	1861.6	1863	−1	1863	*
17000	1964.2	1961	+3	1960	
18000	2066.1	2065	+1	2064	
19000	2167.6	2159	+9	2159	*
20000	2268.4	2263	+5	2262	

n	formule	$\pi(x)$	Diff	corr.	
21000	2368.8	2361	+8	2361	*
22000	2468.8	2465	+4	2464	
23000	2568.3	2565	+3	2564	
24000	2667.3	2669	−2	2669	*
25000	2766.0	2763	+3	2762	
26000	2864.3	2861	+3	2860	
27000	2962.2	2962	0	2961	
28000	3059.8	3056	+4	3056	*
29000	3157.0	3154	+3	3153	
30000	3253.9	3246	+8	3245	
31000	3350.5	3341	+10	3340	
32000	3446.9	3433	+14	3432	
33000	3542.9	3539	+4	3538	
34000	3638.7	3639	0	3638	
35000	3734.2	3733	+1	3732	
36000	3829.4	3825	+4	3824	
37000	3924.4	3924	0	3923	
38000	4019.2	4018	+1	4017	
39000	4113.7	4108	+6	4107	
40000	4208.0	4204	+4	4203	
41000	4302.1	4292	+10	4291	
42000	4396.0	4393	+3	4392	
43000	4489.6	4495	−5	4494	
44000	4583.1	4580	+1	4579	
45000	4676.4	4676	0	4675	
46000	4769.5	4762	+7	4761	
47000	4862.4	4852	+10	4851	
48000	4955.1	4947	+8	4946	
49000	5047.6	5036	+12	5035	
50000	5140.0	5134	+6	5133	
51000	5232.2	5223	+9	5223	*
52000	5324.2	5320	+4	5319	
53000	5416.1	5409	+7	5408	
54000	5507.9	5501	+7	5501	*
55000	5599.4	5591	+8	5591	*
56000	5690.9^3	5684	+7	5683	
57000	5782.1	5783	−1	5782	
58000	5873.3	5874	−1	5873	
59000	5964.2	5964	0	5963	
60000	6055.1	6059	−4	6057	**

n	formule	$\pi(x)$	Diff	corr.	
61000	6145.8	6147	-1	6146	
62000	6236.4	6234	$+2$	6232	**
63000	6326.9	6322	$+5$	6320	**
64000	6417.2	6415	$+2$	6413	**
65000	6507.4	6495	$+12$	6493	**
66000	6597.5	6593	$+4$	6591	**
67000	6687.5^{4}	6677	$+10$	6675	**
68000	6777.3	6776	$+1$	6774	**
69000	6867.0	6856	$+11$	6855	
70000	6956.6	6937	$+20$	6936	
71000	7046.1	7035	$+11$	7033	**
72000	7135.5	7130	$+6$	7128	**
73000	7224.8	7220	$+5$	7218	**
74000	7314.0^{5}	7303	$+11$	7301	**
75000	7403.0	7395	$+8$	7393	**
76000	7492.0	7486	$+6$	7485	
77000	7580.8	7569	$+12$	7567	**
78000	7669.6	7664	$+6$	7662	**
79000	7758.2	7748	$+10$	7746	**
80000	7846.8	7839	$+8$	9837	**
81000	7935.3	7927	$+8$	7926	

n	formule	$\pi(x)$	Diff	corr.	
82000	8023.6	8019	$+5$	8017	**
83000	8111.9	8108	$+4$	8106	**
84000	8200.1	8192	$+8$	8190	**
85000	8288.1^{6}	8279	$+9$	8277	**
86000	8376.2	8364	$+12$	8362	**
87000	8464.1	8452	$+12$	8450	**
88000	8551.9	8545	$+7$	8544	
89000	8639.7	8621	$+19$	8619	**
90000	8727.3	8715	$+12$	8714	
91000	8814.9	8804	$+11$	8802	**
92000	8902.4	8889	$+13$	8887	**
93000	8989.8	8986	$+4$	8985	
94000	9077.1	9072	$+5$	9070	**
95000	9164.3	9159	$+5$	9157	**
96000	9251.5	9254	-2	9253	**
97000	9338.6	9338	$+1$	9337	
98000	9425.6	9420	$+6$	9418	**
99000	9512.5	9507	$+6$	9505	**
100000	9599.4	9594	$+5$	9592	**
101000	9686.2	9675	$+11$	9673	**
102000	9772.9	9769	$+4$	9767	**

~~125~~ a
1261/1

Ihr letzter Brief, so ganz anders
Ihrer Gewohnheit, hat mich überrascht
verwirrt, da er mir die Nachricht von
der Ungnade Ihrer Majestät des hohen Kur-
fürsten brachte, in welcher ich mich in
nur zu Ihnen fühle. Leider erst jetzt war
es mir dabei das Ihr mein Nichterscheinen
von Ihrem Jubiläum nicht übel genommen
haben, sondern es in Ihrer Güte
betrachtet wie es wirklich stattfand. 57

Die unruhige Zeit dauert fort.
Das Erscheinen der Hauptperson vor dem jetzt
wieder vor bewegten Waldeckschen Process
mit Deutlichen Kennzeichen gegeben hat einen
ungeheuren, und der Zeitpunkt wo
mein verlassenes Kind wieder ist
noch nicht entschieden. Als ein kleines Zei-
chen kann ich Ihnen anführen das unlängst
mein Bild aus Wittenberg mir schrieb es sey
ja in der Neuen Königlichen Zeitung ein Ge-
mälde des Großherzogs von der Hannoverschen partey
publicirt. Ich sollte es nicht glauben. Indessen auf

8

es ist merkwürdig zu sehen wie man bei
allen Arten einig. Leider kann ich es blos Ihnen
nur Rätsel zu stellen wissen und es ist ganz lächer-
lich für das Verständniß der französischen Revo-
lution solche Räume im Kleinen mit anzusehen
zu haben. Einem deutlichen Begriff von der Art
wie Masse in Bewegung gesetzt werden können
kann man erhalten als auf diese Weise. Dabei
wiederholt sich merkwürdigen Weise für mich
immer die Erfahrung daß Leute da sind die
in dem Glauben die Masse beherrschen zu können
sie in Bewegung setzen oder zu behalten daß nun
jeder selbst die mitgissten Menschen übersieht
und die einzelnen Regungen wie z.B. Napoleon
die Leidenschaft mit der Masse immer gerechnet haben.
Ich habe übrigens bei meinem Gespräch ganz
kurz einen großen Spiel der Natur Einem Verdacht
gefasst. Die blosse Kunst vor dem Militair zügel-
te Alles, und mir ist keine Erscheinung vorgekommen.

Ihr Brief hat mich das sich Ihnen in meinem
Leben an die immer dicht Freund bleiben die
ich in andern Zeiten ganz innig beneidet haben mir
d. Zurückgewiesen. Die gefällige Ihre Abschrift
gar die wunderlichen mir in der Jahr lassen.

Heiligsam bin ich mich Ihnen das
Zahlung zu übersenden in einlegen sich wieder

125 b 126/2

nur kleinen Aufsatz mit Tafeln befindet
sich nun ich glaube nützlich sey einen
Manuskript sah ich äußerst manuscript nur
nicht.

Außerdem wollte ich noch für mein klein
Darstellung hinzufügen die Theorie der kleinen
Werke sah wir nun aber eine neue kleine Vor-
stellung von der Darstellung d. Kreisfelder gab
also ich für meiner sagen. Dirichlet sagte bei
seinem Vortrag in d. Akademie vorläufig das
d. Zusammensetzung zwischen drei hyp. Logarithm
Zahl ½ d. Zahl d. Kreisfelder bis zu dieser Zahl nun 53
Legendre zuerst aufgestellt sey. Ich nimmerte
mich in dem von sich herausgegebenen Euler-
schen Leinenmittel schon etwas äußerst gelesen
zu haben und in d. Hist Acad. T. I Lettre CXLIX.
pag. 587. Die merkwürdige aber ganz neue Sätze
d. vorgeschriebenen Falles: Da die Anzahl aller
numerorum primorum unendlich ist, aber
doch ein infinitum infimi ordinis, weil ich gezeigt
dass wenn die Zahl omnium numerorum = n
die Anzahl der numerorum primorum seyn
werde ln, es ist aber ln kleiner als n^m so
groß auch immer die Zahl m seyn mag etc.

Vierfach numerische Art mit dem Formel $\frac{n}{\ln n}$ die Anzahl der Primzahlen zwischen einer gegebenen Zahl und einer um eine gegebene Zahl davon entfernten Zahl zu finden

$$\frac{n}{\ln n} \sqrt[2\ln n]{10}.$$

Und damit die nach der Tabelle in Lambert's Beiträgen angegebenen Anzahl der Primzahlen vergleichen. Folgendes ist die Vergleichung

n	formel	Gezählet	Diff	n	formel	Gezählet	Diff
10	7,2	5	+ 2	2000	306,2	304	+ 2
100	27,9	26	+ 2	3000	432,6	431	+ 2
200	46,9	47	0	4000	554,1	551	+ 3
300	64,4	63	+ 1	5000	672,0	670	+ 2
400	80,9	79	+ 2	6000	787,3	784	+ 3
500	96,8	96	+ 1	7000	900,4	901	− 1
600	112,3	110	+ 2	8000	1011,8	1008	+ 4
700	127,4	126	+ 1	9000	1121,7	1118	+ 4
800	142,2	140	+ 2	10000	1230,3	1230	0
900	156,7	155	+ 2	11000	1337,8	1336	+ 2
1000	171,0	169	+ 2	12000	1444,2	1439	+ 5
1100	185,1	185	0	13000	1549,7	1548	+ 2
1200	199,1	197	+ 2	14000	1654,4	1653	+ 1
1300	212,9	212	+ 1	15000	1758,3	1755	+ 3
1400	226,5	223	+ 4	16000	1861,6	1863	− 1
1500	240,1	240	0	17000	1964,2	1961	+ 3
1600	253,5	252	+ 1	18000	2066,1	2065	+ 1
1700	266,8	267	0	19000	2167,6	2159	+ 9
1800	280,0	279	+ 1	20000	2268,4	2263	+ 5
1900	293,1	291	+ 2	21000	2368,8	2361	+ 8

n	Formel	Gezählet	Diff.	n	Formel	Gezählet	Diff.
22000	2468,8	2465	+ 4	58000	5873,3	5874	− 1
23000	2562,3	2565	+ 3	59000	5964,2	5964	0
24000	2667,3	2669	− 2	60000	6055,1	6059	− 4
25000	2766,0	2763	+ 3	61000	6145,8	6147	− 1
26000	2864,3	2861	+ 3	62000	6236,4	6234	+ 2
27000	2962,2	2962	0	63000	6326,9	6322	+ 5
28000	3059,8	3056	+ 4	64000	6417,2	6415	+ 2
29000	3157,0	3154	+ 3	65000	6507,4	6495	+ 12
30000	3253,9	3246	+ 8	66000	6597,5	6593	+ 4
31000	3350,5	3341	+ 10	67000	6687,5	6677	+ 10
32000	3446,9	3433	+ 14	68000	6777,3	6776	+ 1
33000	3542,9	3539	+ 4	69000	6867,0	6856	+ 11
34000	3638,7	3639	0	70000	6956,6	6937	+ 20
35000	3734,2	3733	+ 1	71000	7046,1	7035	+ 11
36000	3829,4	3825	+ 4	72000	7135,5	7130	+ 6
37000	3924,4	3924	0	73000	7224,8	7220	+ 5
38000	4019,2	4018	+ 1	74000	7314,0	7303	+ 11
39000	4113,7	4108	+ 6	75000	7403,0	7395	+ 8
40000	4208,0	4204	+ 4	76000	7492,0	7486	+ 6
41000	4302,1	4292	+ 10	77000	7580,8	7569	+ 12
42000	4396,0	4393	+ 3	78000	7669,6	7664	+ 6
43000	4489,6	4495	− 5	79000	7758,2	7748	+ 10
44000	4583,1	4580	+ 3	80000	7846,8	7839	+ 8
45000	4676,4	4676	0	81000	7935,3	7927	+ 8
46000	4769,5	4762	+ 7	82000	8023,6	8019	+ 5
47000	4862,4	4852	+ 10	83000	8111,9	8108	+ 4
48000	4955,1	4947	+ 8	84000	8200,1	8192	+ 8
49000	5047,6	5036	+ 12	85000	8288,2	8279	+ 9
50000	5140,0	5134	+ 6	86000	8376,2	8364	+ 12
51000	5232,2	5223	+ 9	87000	8464,1	8452	+ 12
52000	5324,2	5320	+ 4	88000	8551,9	8545	+ 7
53000	5416,1	5409	+ 7	89000	8639,7	8621	+ 19
54000	5507,9	5501	+ 7	90000	8727,3	8715	+ 12
55000	5599,4	5591	+ 8	91000	8814,9	8804	+ 11
56000	5690,9	5684	+ 7	92000	8902,4	8889	+ 13
57000	5782,1	5783	− 1	93000	8989,8	8986	+ 4

n	Formel	Gezählt	Diff	n	Formel	Gezählt	Diff
94000	9077,1	9072	+5	99000	9512,5	9507	+6
95000	9164,3	9159	+5	100000	9599,4	9594	+5
96000	9251,5	9254	−2	101000	9686,2	9675	+11
97000	9338,6	9338	+1	102000	9772,9	9769	+4.
98000	9425,6	9420	+6				

Die Formel $\frac{n}{\ln} \sqrt[2\ln]{10}$ lässt sich einfach, ohne Logarithmen, Ab-
zählungen u. s. w. leicht auf die gewöhnliche Weise
fallen, sobald man auf 0 zurück und giebt
man allen die zwischen 62000 & 69000 so
wie zwischen 69000 & 70000 ~~überhaupt~~ durchschnittlich einmal
unter einander in einem Cantone 80 & 81. Diese
Zahlen für verschiedene Cantone nahezu constante
Gränz-Zahl etwa 89,6 nahe kommen sollten die Zahl
Primzahlen (1 mitgezählt) etwa bis auf 5 oder 6 ein
stellen an. Vielleicht wird sie also auch für die Ermit-
telung der Zahl der Primzahlen über 102000 hinaus einige
Genauigkeit gewähren, wo mühsame Zählung $\frac{n}{\ln}$ nur noch
beschwerlich genau n sich annähert.

Schumacher's Tage scheint mir nimmer sehr
günstig. ~~Der~~ Der früher selige Bürgermeister Gerdtner
Kammerherr v. Beedtz sollte Sonntags von seinem
eignen gastfreundlichen Hause in Copenhagen
seinen gewöhnlichen Spaziergang Morgens 7 Uhr
ganz früh vor sich und da sie so schnell die Treppe
herab gestürzt

Erhalten Sie Ihr gütiges Wohlwollen

Ihrem

ergebensten

ENCKE

4/12 40.

On termine cette petite étude en utilisant l'article wikipedia en anglais *Prime counting function* pour comparer le nombre de nombres premiers calculés par la formule fournie par Encke dans sa lettre au nombre de nombres premiers effectifs jusqu'à 10^{29}.

x	$\pi(x)$	$\mathrm{Li}(x) - \pi(x)$	Formule	Formule $- \pi(x)$
10^2	25	5	28	3
10^3	168	10	171	3
10^4	1 229	17	1 230	1
10^5	9 592	38	9 599	7
10^6	78 498	130	78 673	175
10^7	664 579	339	666 358	1 779
10^8	5 761 455	754	5 778 801	17 346
10^9	50 847 534	1 701	51011638	164 104
10^{10}	455 052 511	3 104	456 561 236	1 508 725
10^{11}	4 118 054 813	11 588	4 131 733 338	13 678 525
10^{12}	37 607 912 018	38 263	37 731 030 671	123 118 653
10^{13}	346 065 536 839	108 971	347 171 921 315	1 106 384 476
10^{14}	3 204 941 750 802	314 890	3 214 894 997 081	9 953 246 279
10^{15}	29 844 570 422 669	1 052 619	29 934 329 511 045	89 759 088 376
10^{16}	279 238 341 033 925	3 214 632	280 050 292 885 574	811 951 851 649
10^{17}	2 623 557 157 654 233	7 956 589	2 630 926 752 221 200	7 369 594 566 967
10^{18}	24 739 954 287 740 860	21 949 555	24 807 073 979 735 608	67 119 691 994 748
10^{19}	234 057 667 276 344 607	99 877 775	234 671 047 827 583 232	613 380 551 238 625
10^{20}	2 220 819 602 560 918 840	222 744 644	2 226 443 495 278 635 264	5 623 892 717 716 424
10^{21}	21 127 269 486 018 731 928	597 394 254	21 178 995 660 737 171 456	51 726 174 718 439 528
10^{22}	201 467 286 689 315 906 290	1 932 355 208	201 944 467 471 308 193 792	477 180 781 992 287 502
10^{23}	1 925 320 391 606 803 968 923	7 250 186 216	1 929 734 937 198 216 085 504	4 414 545 591 412 116 581
10^{24}	18 435 599 767 349 200 867 866	17 146 907 278	18 476 549 561 110 832 873 472	40 949 793 761 632 005 606
10^{25}	176 846 309 399 143 769 411 680	55 160 980 939	177 227 124 961 569 283 244 032	380 815 562 425 513 832 352
10^{26}	1 699 246 750 872 437 141 327 603	155 891 678 121	1 702 796 623 312 741 436 751 872	3 549 872 440 304 295 424 269
10^{27}	16 352 460 426 841 680 446 427 399	508 666 658 006	16 385 625 986 096 599 480 139 776	33 165 559 254 919 033 712 377
10^{28}	157 589 269 275 973 410 412 739 598	1 427 745 660 374	157 899 784 963 805 533 970 628 608	310 515 687 832 123 557 889 010
10^{29}	1 520 698 109 714 272 166 094 258 063	4 551 193 622 464	1 523 611 174 796 346 228 956 200 960	2 913 065 082 074 062 861 942 897

Programmation d'une formule extraite du livre *Werke : Hoehere Arithmetik* de Gauss (Denise Vella-Chemla, février 2024)

On trouve à la page 22 du livre *Werke : Hoehere Arithmetik* les deux définitions suivantes :

$$\begin{array}{rcrrrrrr} T & = & 1 & +\cos k\omega & +\cos 4k\omega & +\cos 9k\omega & +\ldots & +\cos(n-1)^2k\omega \\ U & = & & \sin k\omega & +\sin 4k\omega & +\sin 9k\omega & +\ldots & +\sin(n-1)^2k\omega \end{array}$$

et à la page 31 le tableau suivant :

T	U	selon que n est de la forme
$\pm\sqrt{n}$	$\pm\sqrt{n}$	4μ
$\pm\sqrt{n}$	0	$4\mu+1$
0	0	$4\mu+2$
0	$\pm\sqrt{n}$	$4\mu+3$

On vérifie ces formules par le programme :

```
import math
from math import pi, sin, cos, sqrt

for n in range(1,101):
     print('',n, '--->')
     if n%4 == 0:  print('4k')
     else:
          if n%4 == 1:  print('4k+1')
          else:
               if n%4 == 2:  print('4k+2')
               else:  print('4k+3')
     T = 1
     U = 0
     for k in range(1, n):
          T = T+cos(k*k*2*pi/n)
          U = U+sin(k*k*2*pi/n)
     print('T = ', T)
     print('U = ', U)
     print('sqrt = ', sqrt(n))
```

dont le résultat montre que les formules sont correctes :

```
1 --->
4k+1
T = 1
U = 0
sqrt = 1.0
```

```
2 --->
4k+2
T = 0.0
U = 1.2246467991473532e-16
sqrt = 1.4142135623730951

3 --->
4k+3
T = 9.992007221626409e-16
U = 1.7320508075688779
sqrt = 1.7320508075688772

4 --->
4k
T = 2.0000000000000004
U = 1.9999999999999998
sqrt = 2.0

5 --->
4k+1
T = 2.23606797749979
U = -5.551115123125783e-16
sqrt = 2.23606797749979

6 --->
4k+2
T = -3.164135620181696e-15
U = 1.9984014443252818e-15
sqrt = 2.449489742783178

7 --->
4k+3
T = 1.4432899320127035e-15
U = 2.6457513110645907
sqrt = 2.6457513110645907

8 --->
4k
T = 2.828427124746193
U = 2.828427124746187
sqrt = 2.8284271247461903

9 --->
4k+1
T = 3.0000000000000036
```

```
U = 1.2212453270876722e-15
sqrt = 3.0

10 --->
4k+2
T = 6.661338147750939e-16
U = -5.662137425588298e-15
sqrt = 3.1622776601683795

11 --->
4k+3
T = 3.219646771412954e-15
U = 3.316624790355405
sqrt = 3.3166247903554

12 --->
4k
T = 3.4641016151377526
U = 3.464101615137754
sqrt = 3.4641016151377544

13 --->
4k+1
T = 3.605551275463985
U = -8.215650382226158e-15
sqrt = 3.605551275463989

14 --->
4k+2
T = 1.7763568394002505e-15
U = -6.2727600891321345e-15
sqrt = 3.7416573867739413

15 --->
4k+3
T = 8.43769498715119e-15
U = 3.8729833462074135
sqrt = 3.872983346207417

16 --->
4k
T = 4.0000000000000115
U = 3.9999999999999876
sqrt = 4.0
```

```
17 --->
4k+1
T = 4.123105625617655
U = 1.2712053631958042e-14
sqrt = 4.123105625617661

18 --->
4k+2
T = 0.0
U = -2.2315482794965646e-14
sqrt = 4.242640687119285

19 --->
4k+3
T = 1.176836406102666e-14
U = 4.358898943540667
sqrt = 4.358898943540674

20 --->
4k
T = 4.472135954999589
U = 4.472135954999556
sqrt = 4.47213595499958

21 --->
4k+1
T = 4.582575694955837
U = 8.43769498715119e-15
sqrt = 4.58257569495584

22 --->
4k+2
T = 1.0658141036401503e-14
U = 6.938893903907228e-15
sqrt = 4.69041575982343

23 --->
4k+3
T = -1.1435297153639112e-14
U = 4.795831523312737
sqrt = 4.795831523312719

24 --->
4k
T = 4.898979485566374
```

```
U = 4.8989794855663416
sqrt = 4.898979485566356

25 --->
4k+1
T = 4.999999999999992
U = -1.3128387266192476e-14
sqrt = 5.0

26 --->
4k+2
T = 5.218048215738236e-15
U = -1.2656542480726785e-14
sqrt = 5.0990195135927845

27 --->
4k+3
T = 1.6209256159527285e-14
U = 5.1961524227066676
sqrt = 5.196152422706632

28 --->
4k
T = 5.291502622129176
U = 5.291502622129131
sqrt = 5.291502622129181

29 --->
4k+1
T = 5.385164807134534
U = -1.940114735532461e-14
sqrt = 5.385164807134504

30 --->
4k+2
T = 2.1316282072803006e-14
U = -9.048317650695026e-15
sqrt = 5.477225575051661

31 --->
4k+3
T = 3.774758283725532e-14
U = 5.567764362830035
sqrt = 5.5677643628300215
```

```
32 --->
4k
T = 5.656854249492386
U = 5.656854249492382
sqrt = 5.656854249492381

33 --->
4k+1
T = 5.744562646538029
U = -2.6256774532384952e-14
sqrt = 5.744562646538029

34 --->
4k+2
T = -9.43689570931383e-15
U = 4.218847493575595e-15
sqrt = 5.830951894845301

35 --->
4k+3
T = 3.186340080674199e-14
U = 5.9160797830996135
sqrt = 5.916079783099616

36 --->
4k
T = 6.0000000000000195
U = 5.999999999999989
sqrt = 6.0

37 --->
4k+1
T = 6.082762530298207
U = -4.41591208044656e-14
sqrt = 6.082762530298219

38 --->
4k+2
T = 8.548717289613705e-15
U = -1.3600232051658168e-14
sqrt = 6.164414002968976

39 --->
4k+3
T = 2.2648549702353193e-14
```

```
U = 6.2449979983983654
sqrt = 6.244997998398398

40 --->
4k
T = 6.324555320336819
U = 6.324555320336705
sqrt = 6.324555320336759

41 --->
4k+1
T = 6.403124237432841
U = -6.375455718909961e-14
sqrt = 6.4031242374328485

42 --->
4k+2
T = 3.6193270602780103e-14
U = 1.4377388168895777e-14
sqrt = 6.48074069840786

43 --->
4k+3
T = 1.3766765505351941e-14
U = 6.55743852430199
sqrt = 6.557438524302

44 --->
4k
T = 6.633249580710818
U = 6.63324958071077
sqrt = 6.6332495807108

45 --->
4k+1
T = 6.708203932499365
U = -3.574918139293004e-14
sqrt = 6.708203932499369

46 --->
4k+2
T = 7.37188088351104e-14
U = 6.13398221105399e-15
sqrt = 6.782329983125268
```

```
47 --->
4k+3
T = -6.417089082333405e-14
U = 6.855654600401059
sqrt = 6.855654600401044

48 --->
4k
T = 6.928203230275569
U = 6.928203230275426
sqrt = 6.928203230275509

49 --->
4k+1
T = 7.0000000000001
U = 7.382983113757291e-15
sqrt = 7.0

50 --->
4k+2
T = -2.2870594307278225e-14
U = 5.0959236830294685e-14
sqrt = 7.0710678118654755

51 --->
4k+3
T = -1.6986412276764895e-14
U = 7.141428428542828
sqrt = 7.14142842854285

52 --->
4k
T = 7.211102550927947
U = 7.211102550928012
sqrt = 7.211102550927978

53 --->
4k+1
T = 7.280109889280554
U = -1.7694179454963432e-14
sqrt = 7.280109889280518

54 --->
4k+2
T = 1.9984014443252818e-15
```

```
U = 2.416122857340497e-14
sqrt = 7.3484692283495345

55 --->
4k+3
T = 7.494005416219807e-14
U = 7.416198487095638
sqrt = 7.416198487095663

56 --->
4k
T = 7.4833147735479235
U = 7.483314773547801
sqrt = 7.483314773547883

57 --->
4k+1
T = 7.5498344352707445
U = -6.063205493234136e-14
sqrt = 7.54983443527075

58 --->
4k+2
T = -3.2307490016592055e-14
U = -1.1331213745080504e-13
sqrt = 7.615773105863909

59 --->
4k+3
T = 8.315570454442422e-14
U = 7.681145747868639
sqrt = 7.681145747868608

60 --->
4k
T = 7.745966692414893
U = 7.745966692414805
sqrt = 7.745966692414834

61 --->
4k+1
T = 7.810249675906595
U = 3.048949981376836e-14
sqrt = 7.810249675906654
```

```
62 --->
4k+2
T = 5.917488721252084e-14
U = -2.148281552649678e-14
sqrt = 7.874007874011811

63 --->
4k+3
T = 2.6645352591003757e-14
U = 7.93725393319381
sqrt = 7.937253933193772

64 --->
4k
T = 7.999999999999994
U = 7.999999999999949
sqrt = 8.0

65 --->
4k+1
T = 8.06225774829863
U = -1.1203538097248611e-13
sqrt = 8.06225774829855

66 --->
4k+2
T = -5.939693181744587e-14
U = -1.4585554986012994e-14
sqrt = 8.12403840463596

67 --->
4k+3
T = -5.995204332975845e-15
U = 8.185352771872607
sqrt = 8.18535277187245

68 --->
4k
T = 8.24621125123535
U = 8.246211251235247
sqrt = 8.246211251235321

69 --->
4k+1
T = 8.306623862918043
```

```
U = 3.176625629208729e-14
sqrt = 8.306623862918075

70 --->
4k+2
T = 9.00390872971002e-14
U = -6.517009154549669e-14
sqrt = 8.366600265340756

71 --->
4k+3
T = 1.0902390101819037e-13
U = 8.426149773176352
sqrt = 8.426149773176359

72 --->
4k
T = 8.485281374238665
U = 8.485281374238472
sqrt = 8.48528137423857

73 --->
4k+1
T = 8.544003745317587
U = -1.593447596093256e-13
sqrt = 8.54400374531753

74 --->
4k+2
T = 1.2312373343092986e-13
U = 1.0906553438161382e-13
sqrt = 8.602325267042627

75 --->
4k+3
T = -1.0247358517290195e-13
U = 8.660254037844435
sqrt = 8.660254037844387

76 --->
4k
T = 8.717797887081487
U = 8.717797887081339
sqrt = 8.717797887081348
```

```
77 --->
4k+1
T = 8.77496438739204
U = 2.167710455580618e-14
sqrt = 8.774964387392123

78 --->
4k+2
T = 2.1871393585115584e-14
U = -5.4969917506753063e-14
sqrt = 8.831760866327848

79 --->
4k+3
T = -1.1102230246251565e-16
U = 8.88819441731542
sqrt = 8.888194417315589

80 --->
4k
T = 8.944271909999317
U = 8.944271909999062
sqrt = 8.94427190999916

81 --->
4k+1
T = 8.999999999999982
U = -1.802724636235098e-13
sqrt = 9.0

82 --->
4k+2
T = 1.3244960683778118e-13
U = 1.6815715486728777e-13
sqrt = 9.055385138137417

83 --->
4k+3
T = 5.262457136723242e-14
U = 9.110433579144326
sqrt = 9.1104335791443

84 --->
4k
T = 9.165151389911593
```

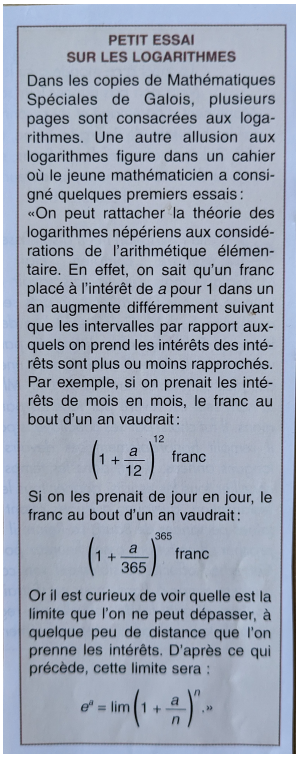
```
U = 9.1651513899116
sqrt = 9.16515138991168

85 --->
4k+1
T = 9.219544457292818
U = -1.49366630175507e-13
sqrt = 9.219544457292887

86 --->
4k+2
T = 8.204548151979907e-14
U = -1.322830733840874e-13
sqrt = 9.273618495495704

87 --->
4k+3
T = 9.703349235223868e-14
U = 9.3273790530887
sqrt = 9.327379053088816

88 --->
4k
T = 9.380831519646996
U = 9.380831519646694
sqrt = 9.38083151964686

89 --->
4k+1
T = 9.433981132056614
U = 2.245426067304379e-14
sqrt = 9.433981132056603

90 --->
4k+2
T = -2.1649348980190553e-14
U = 4.621303340002214e-14
sqrt = 9.486832980505138

91 --->
4k+3
T = 8.737455203799982e-14
U = 9.539392014169453
sqrt = 9.539392014169456
```

```
92 --->
4k
T = 9.59166304662542
U = 9.59166304662546
sqrt = 9.591663046625438

93 --->
4k+1
T = 9.643650760993097
U = -1.6238399513923696e-13
sqrt = 9.643650760992955

94 --->
4k+2
T = 8.693046282814976e-14
U = -7.308043059595093e-14
sqrt = 9.695359714832659

95 --->
4k+3
T = 9.137135492665038e-14
U = 9.7467943448089
sqrt = 9.746794344808963

96 --->
4k
T = 9.797958971132939
U = 9.797958971132573
sqrt = 9.797958971132712

97 --->
4k+1
T = 9.84885780179616
U = 1.817296313433303e-13
sqrt = 9.848857801796104

98 --->
4k+2
T = -2.6978419498391304e-14
U = 2.222250161665329e-13
sqrt = 9.899494936611665

99 --->
4k+3
T = -5.873079800267078e-14
```

```
U = 9.949874371066427
sqrt = 9.9498743710662

100 --->
4k
T = 9.999999999999835
U = 9.999999999999675
sqrt = 10.0
```

Petite digression inspirée par un encart extrait d'un magazine *Les génies de la science* consacré à Évariste Galois (Denise Vella-Chemla, février 2024)

Ci-dessous, l'image d'un encart extrait du numéro hors-série "*Les génies de la science*" consacré à Évariste Galois (numéro 14, trimestriel février-mai 2003) à côté de l'image de la couverture du magazine. Un internaute signale qu'à l'examen d'entrée à Polytechnique, Galois a été interrogé sur les logarithmes.



PETIT ESSAI SUR LES LOGARITHMES

Dans les copies de Mathématiques Spéciales de Galois, plusieurs pages sont consacrées aux logarithmes. Une autre allusion aux logarithmes figure dans un cahier où le jeune mathématicien a consigné quelques premiers essais :
«On peut rattacher la théorie des logarithmes népériens aux considérations de l'arithmétique élémentaire. En effet, on sait qu'un franc placé à l'intérêt de a pour 1 dans un an augmente différemment suivant que les intervalles par rapport auxquels on prend les intérêts des intérêts sont plus ou moins rapprochés. Par exemple, si on prenait les intérêts de mois en mois, le franc au bout d'un an vaudrait :

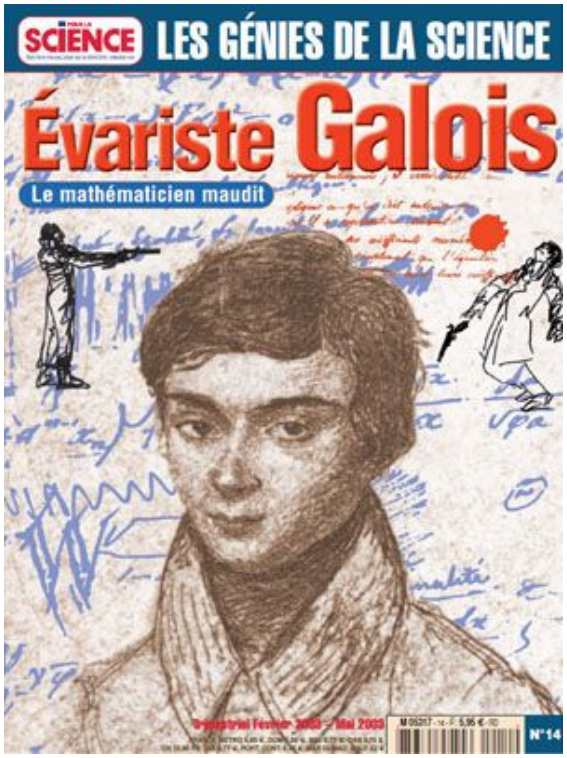
$$\left(1+\frac{a}{12}\right)^{12} \text{ franc}$$

Si on les prenait de jour en jour, le franc au bout d'un an vaudrait :

$$\left(1+\frac{a}{365}\right)^{365} \text{ franc}$$

Or il est curieux de voir quelle est la limite que l'on ne peut dépasser, à quelque peu de distance que l'on prenne les intérêts. D'après ce qui précède, cette limite sera :

$$e^a = \lim\left(1+\frac{a}{n}\right)^n.$$»



On trouve cette formule dans l'article Wikipédia en anglais consacré à la fonction exponentielle :

> *La fonction exponentielle surgit à chaque fois qu'une quantité grossit ou décroît à un rythme proportionnel à sa valeur courante. Une telle situation est celle des intérêts composés continûment, et en fait, c'est cette observation qui a amené Jacob Bernoulli en 1683 au nombre*
>
> $$\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n$$
>
> *maintenant appelé e. Ultérieurement, en 1697, Johann Bernoulli a étudié le calcul de la fonction exponentielle.*

Si un capital de 1 rapporte un intérêt au taux annuel de x composé mensuellement, alors l'intérêt rapporté chaque mois à la valeur courante est $\frac{x}{12}$, donc chaque mois, la valeur initiale 1 est multipliée par $\left(1+\frac{x}{12}\right)$, et la valeur à la fin de l'année est

$$\left(1+\frac{x}{12}\right)^{12}.$$

Si au lieu de cela, l'intérêt est composé chaque jour, cela devient

$$\left(1+\frac{x}{365}\right)^{365}.$$

Faire grandir sans limite le nombre d'intervalles temporels par année amène à cette définition de l'exponentielle comme une limite :

$$\exp x = \lim_{n\to\infty}\left(1+\frac{x}{n}\right)^{n}$$

donnée pour la première fois par Leonhard Euler.

On vérifie la formule de calcul de l'exponentielle (**exp**) de l'encart (attribuée à Bernoulli et retrouvée par Galois) par le programme python suivant :

```
import math
from math import exp, log

n = 100
print('la formule ')
while n < 1000000000000:
     print(pow(1+3/n,n))
     n = n*100
print('la valeur de exp ')
print(exp(3))
```

Le résultat de ce programme, illustrant le fait que la formule tend vers l'exponentielle, est :

```
la formule
19.218631980856298
20.07650227139987
20.08544653815843
20.085536099119246
20.08554189980412

la valeur de exp
20.085536923187668
```

On cherche une formule similaire pour le logarithme népérien (**ln**) sur la toile. On n'en trouve pas.

En utilisant le fait que les fonctions **exp** et **ln** sont des fonctions réciproques[1], on trouve une formule similaire à celle de l'exponentielle comme limite (il suffit de composer les fonctions appliquées successivement, mais "*en suivant les flèches qui associent les images aux antécédents à l'envers*", et en inversant les calculs) ; cette formule devrait tendre vers le logarithme népérien.

On teste la formule de calcul du logarithme (**ln**) par le programme suivant :

```
import math
from math import exp, log

n = 100
print('la formule ')
while n < 1000000000000:
     print((-1+pow(3,1/n))*n)
     n = n*100
print('la valeur de log ')
print(log(3))
```

Le résultat de ce programme, illustrant le fait que la formule tend vers le logarithme népérien est :

```
la formule
1.104669193785357
1.0986726383266365
1.0986128922141347
1.0986122900291662
1.0986123122336267

la valeur de log
1.0986122886681098
```

Poursuivons : utilisons la forme d'écriture préfixe polonaise informatique[2] et écrivons abusivement des signes ∞ à la place des $n \to \infty$. On obtient :

$$\exp x \quad = \text{puiss} \left(\text{somme} \left(+1 \ , \ \text{mult} \left(x \ , \ \frac{1}{\infty} \right) \right) , \infty \right)$$

$$\ln \ x \quad = \text{mult} \ \left(\text{somme} \left(-1 \ , \ \text{puiss} \left(x \ , \ \frac{1}{\infty} \right) \right) , \infty \right)$$

On voit une jolie correspondance entre les deux écritures : il suffit d'échanger **mult** et **puiss** d'une part et **+1** et **-1** d'autre part.

[1] J'aimais bien les "moulinettes" que nous avait enseignées mon maître de CE2, M. Lavergne, des sortes d'"opérateurs" pour les petits !

[2] Rappel obtenu en interrogeant Chat-GPT : "En informatique, le fait d'écrire mult(a, b) plutôt que $a \times b$, où l'opérateur est placé en premier, est souvent appelé une notation préfixe ou notation polonaise préfixe (NPP). Ce type de notation a été popularisé par le mathématicien polonais Jan Łukasiewicz, d'où le nom de *notation polonaise préfixe*."

Il aurait fallu écrire :

$$\exp x \;\; = \lim_{n\to\infty} \left((+1) + (x \times \tfrac{1}{n})\right)^n$$

$$\ln \; x \;\; = \lim_{n\to\infty} \left((-1) + (x^{\frac{1}{n}})\right) \times n$$

Annexe : démonstration de l'existence de la limite $\lim_{n\to\infty} \left(1+\frac{1}{n}\right)^n$ (source : traduction d'un extrait du livre de Richard Courant et Herbert Robbins *What is mathematics ? an elementary approach to ideas and methods*[3] [4])

Le nombre e a une place bien établie en mathématiques depuis la publication en 1748 de l'*Introductio in Analysin Infinitorum* d'Euler. Il fournit une excellente illustration de la façon dont le principe des séries monotones peut servir à définir un nouveau nombre réel. En utilisant l'abréviation

$$n! = 1 \cdot 2 \cdot 3 \cdot 4 \ldots n$$

pour le produit des n premiers entiers, on considère la séquence $a_1, a_2, a_3, \ldots$ où

$$a_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!}.$$

Les termes a_n forment une suite croissante monotone, puisque a_{n+1} est l'addition de a_n et d'un incrément positif $\frac{1}{(n+1)!}$. De plus, les valeurs des a_n sont bornées supérieurement :

$$a_n < B = 3.$$

On a

$$\frac{1}{s!} = \frac{1}{2}\frac{1}{3}\cdots\frac{1}{n} < \frac{1}{2}\frac{1}{2}\cdots\frac{1}{2} = \frac{1}{2^{s-1}},$$

et par conséquent

$$a_n < 1 + 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \ldots + \frac{1}{2} \;\; = 1 + \frac{1 - \left(\frac{1}{2}\right)^n}{1 - \frac{1}{2}}$$

$$= 1 + 2\left(1 - \left(\tfrac{1}{2}\right)^n\right) < 3,$$

en utilisant la formule *connue*[5] pour la somme des n premiers termes d'une série géométrique. Par conséquent, par le principe des séries monotones, a_n doit approcher une limite lorsque n tend vers

[3] Seconde édition, revue par Ian Stewart, Oxford University Press, 1996 ; édition originale : 1941.

[4] référence retrouvée grâce au livre "*e, l'histoire d'un nombre*", d'Eli Naor (Princeton University Press).

[5] Ce mot est à remplacer par *fournie page 13* dans le livre de Courant et Robbins.

l'infini et *on appelle cette limite e*. Pour exprimer le fait que $e = \lim a_n$, on peut écrire e comme la "série infinie"

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!} \ldots .$$

Cette "égalité" avec des points de suspension en fin de ligne, est simplement une autre façon d'exprimer le contenu des deux assertions

$$a_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!}$$

et

$$a_n \to e \quad \text{lorsque} \quad n \to \infty.$$

Traduction de la démonstration du livre de Naor (l'appendice 2)

On montre d'abord que la série

$$S_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!}, \qquad n = 1, 2, 3, \ldots .$$

converge vers une limite lorsque n tend vers l'infini. Cette somme croît à chaque terme ajouté, donc on a $S_n < S_{n+1}$ pour tout n, c'est-à-dire que la série S_n croît de façon monotone.

En commençant par $n = 3$, on a également $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n > 1 \cdot 2 \cdot 2 \cdot \ldots \cdot 2 = 2^{n-1}$; par conséquent

$$S_n < 1 + 1 + \frac{1}{2} + \frac{1}{2^2} + \ldots + \frac{1}{2^{n-1}}$$

pour $n = 3, 4, 5, \ldots$. Maintenant, dans cette dernière somme, les termes à partir du second forment une progression géométrique de raison $\frac{1}{2}$. La somme de cette progression est

$$\frac{1 - \frac{1}{2^n}}{1 - \frac{1}{2}} = 2\left(1 - \frac{1}{2^n}\right) < 2.$$

On a donc $S_n < 1 + 2 = 3$, ce qui montre que la série S_n est bornée supérieurement par 3 (c'est-à-dire que les valeurs de S_n n'excèdent jamais 3). On utilise maintenant un théorème bien connu d'analyse :

Toute série croissante, bornée, monotone tend vers une limite lorsque $n \to \infty$.

Donc S_n converge vers une limite S. La preuve montre également que S est compris entre 2 et 3.

Considérons maintenant la série $T_n = \left(1 + \frac{1}{n}\right)^n$.

On va montrer que cette série converge vers la même limite que S_n. Par le théorème binomial,

$$\begin{aligned} T_n &= 1 + n \cdot \frac{1}{n} + \frac{n(n-1)}{2!} \cdot \frac{1}{n^2} + \ldots + \frac{n(n-1)(n-2)\ldots 1}{n!} \cdot \frac{1}{n^n} \\ &= 1 + 1 + \left(1 - \frac{1}{n}\right) \cdot \frac{1}{2!} + \ldots + \left(1 - \frac{1}{n}\right)\left(1 - \frac{2}{n}\right) \ldots \left(1 - \frac{n-1}{n}\right) \cdot \frac{1}{n!}. \end{aligned}$$

Puisque l'expression dans chaque paire de parenthèses est inférieure à 1, on a $T_n \leq S_n$ (en fait, on a effectivement $T_n < S_n$ en commençant par $n = 2$). Donc la série T_n est aussi limitée supérieurement. De plus, T_n croît de façon monotone, parce qu'il suffit de remplacer n par $n + 1$ pour faire croître la somme. Donc T_n converge également vers une limite lorsque $n \to \infty$. On appelle cette limite T.

On montre maintenant que $S = T$. Puisque $S_n \geq T_n$ pour tout n, on a $S \geq T$. On va montrer qu'on a en même temps $S \leq T$. Soit $m < n$ un entier fixé. Les $m + 1$ premiers termes de T_n sont

$$1 + 1 + \left(1 - \frac{1}{n}\right) \cdot \frac{1}{2!} + \ldots + \left(1 - \frac{1}{n}\right)\left(1 - \frac{2}{n}\right) \ldots \left(1 - \frac{m-1}{n}\right) \cdot \frac{1}{m!}.$$

Puisque $m < n$ et puisque tous les termes sont positifs, cette dernière somme est moindre que T_n. Si on fait maintenant tendre n vers l'infini alors que m reste fixe, la somme va tendre vers S_m alors que T_n tendra vers T. On a donc $S_m \leq T$, et par conséquent, $S \leq T$. Puisqu'on a déjà montré que $S \geq T$, il en découle que $S = T$, qui est l'assertion qu'on souhaitait démontrer. La limite T, bien sûr, est le nombre e.

Je ne savais pas cela sur la série harmonique et sur la somme des inverses des racines carrées des entiers (Denise Vella-Chemla, mars 2024)

À cause de cette idée entêtante du $\frac{1}{2}$ qui apparaît dans l'hypothèse de Riemann, on a l'idée de programmer la somme des inverses des nombres de 1 à n, un entier donné, mais également, la somme des inverses des racines carrées de ces nombres.

On met les résultats de ces deux calculs, pour le premier, en regard du logarithme du nombre n, et pour le second, en regard du double de la racine carrée de n. Voici le programme python qu'on utilise pour effectuer les calculs :

```
import time
import math
from math import log, cos, pi, sqrt, e

tic = time.time()
somme1 = 1
somme2 = 1
nmax = 100000001
for n in range(2,nmax):
      somme1 = somme1+1/n
      somme2 = somme2+1/sqrt(n)
      if n == nmax-1:
            print('= ', n)
            print('somme des inverses des entiers jusqu a n = ',somme1)
            print('ln(n) = ', log(n))
            print('somme des inverses des racines des entiers jusqu a n = ',somme2)
            print('2*sqrt(n) = ', 2*sqrt(n))
tac = time.time()
print('execution en ',tac-tic, ' s.')
```

Le résultat de ce programme, qu'on ne fournit que pour la valeur finale de 10^8, mais dont les égalités s'avèrent vérifiées pour tous les nombres inférieurs à n est :

```
n = 100000000
somme des inverses des entiers jusqu a n = 18.997896413852555
ln(n)                                    = 18.420680743952367
somme des inverses des racines des entiers jusqu a n = 19998.53969549304
2*sqrt(n)                                            = 20000.0
execution en 30.247287034988403 s.
```

Le premier résultat :

$$\sum_{k=1}^{k=n} \frac{1}{k} \simeq \log x \ + \ \gamma$$

avec $\gamma = 0.5772...$, dite constante d'Euler-Mascheroni, est connu et démontré : la différence entre la série harmonique et le logarithme népérien converge asymptotiquement vers γ.

On ne sait pas encore si le second résultat :

$$\sum_{k=1}^{k=n} \frac{1}{\sqrt{k}} \simeq 2\sqrt{n} + \gamma'$$

est connu, est vrai et si oui, s'il est démontré. La différence entre les deux résultats des calculs, égale à $\gamma' = 1.4603046$, pourrait faire penser[1] à une constante dite Constante de Porter, dont la valeur est 1.4670780794... ; Donald E. Knuth en a donné la valeur exacte (Voir ici : https://fr.wikipedia.org/wiki/Constante_de_Porter).

[1] de loin, à une distance de 6 à 7 millièmes.

Compléments fournis par Pierre de la Harpe concernant l'expression du logarithme comme une série

On lira à profit cet article du site Images des mathématiques :
https://images.math.cnrs.fr/wp-content/uploads/2025/03/2025_DE-LA-HARPE_nombre-Euler_A4.pdf.

La fonction logarithme naturel s'exprime par la série de Mercator :

$$\ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \frac{x^5}{5} - \ldots = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} x^k. \tag{1}$$

Cette série converge absolument lorsque $|x| < 1$ ainsi que pour $x = 1$.

Euler fournit une meilleure approximation dans la section 121 de l'*Introductio in analysin infinitorum*, volume 1, dont voici le texte latin :

Quoniam igitur est $l(1+x) = \frac{1}{k}\left(\frac{x}{1} - \frac{x^2}{2} + \frac{x^3}{3} - \&c.\right)$ *erit, posito* x *negativo,* $l(1-x) = -\frac{1}{k}\left(\frac{x}{1} + \frac{x^2}{2} + \frac{x^3}{3} + \frac{x^4}{4} + \&c.\right)$. *Subtrahatur series posterior a priori, erit* $l(1+x) - l(1-x) = l\frac{1+x}{1-x} = \frac{2}{k} \times \left(\frac{x}{1} + \frac{x^3}{3} + \frac{x^5}{5} + \frac{x^7}{7} + \&c.\right)$. *Nunc ponatur* $\frac{1+x}{1-x} = a$, *ut fit* $x = \frac{a-1}{a+1}$, *ob* $la = 1$ *erit* $k = 2\left(\frac{a-1}{a+1} + \frac{(a-1)^3}{3(a+1)^3} + \frac{(a-1)^5}{5(a+1)^5} + \&c.\right)$, *ex qua æquatione valor numeri* k *ex basi* a *inveneri poterit. Si ergo basis* a *ponatur* $= 10$, *erit* $k = 2\left(\frac{9}{11} + \frac{9^3}{3 \cdot 11^3} + \frac{9^5}{5 \cdot 11^5} + \frac{9^7}{7 \cdot 11^7} + \&c.\right)$, *cujus seriei termini sensibiliter decrescunt, ideoque mox valorem pro* k *satis propinquum exhibent.*

On a ainsi une meilleure approximation du logarithme népérien par la formule :

$$\ln\frac{1+x}{1-x} = 2\left(x + \frac{x^3}{3} + \frac{x^5}{5} + \frac{x^7}{7} + \frac{x^9}{9} + \ldots\right). \tag{2}$$

Pierre de la Harpe réécrit la formule que j'ai obtenue par une méthode uniquement syntaxique (i.e. sans la démontrer : à partir de l'expression en série de l'exponentielle que fournissait Galois dans un petit encart, en utilisant le fait que exp et log sont des fonctions réciproques et en traversant les flèches de l'antécédent vers l'image de chacune des fonctions intermédiaires intervenant dans la formule de Galois dans leur sens inverse), formule qui était :

$$\ln x = \lim_{n\to\infty} \left((-1) + (x^{\frac{1}{n}})\right) \times n, \tag{3}$$

en

$$\lim_{n\to\infty}\left(n\left((1+x)^{1/n}-1\right)\right)=\ln(1+x)\quad\text{pour}\quad|x|<1. \tag{4}$$

En appliquant la formule du binôme, on a

$$(1+x)^{1/n}=1+\frac{1}{n}x+\frac{\frac{1}{n}(\frac{1}{n}-1)}{2!}x^2+\frac{\frac{1}{n}(\frac{1}{n}-1)(\frac{1}{n}-2)}{3!}x^3+\ldots+\frac{\frac{1}{n}(\frac{1}{n}-1)\ldots(\frac{1}{n}-k+1)}{k!}x^k+\ldots$$

et donc

$$n\left((1+x)^{1/n}-1\right)=x-\frac{1-\frac{1}{n}}{2!}x^2+\frac{(1-\frac{1}{n})(2-\frac{1}{n})}{3!}x^3\mp\ldots+(-1)^{k+1}\frac{(1-\frac{1}{n})(2-\frac{1}{n})\ldots(k-1-\frac{1}{n})}{k!}x^k+\ldots.$$

Si la limite du terme de gauche est bien la somme des limites des termes de droite, on obtient

$$\begin{aligned}\lim_{n\to\infty}\left(n\left((1+x)^{1/n}-1\right)\right) &= x-\lim_{n\to\infty}\frac{1-\frac{1}{n}}{2!}x^2+\lim_{n\to\infty}\frac{(1-\frac{1}{n})(2-\frac{1}{n})}{3!}x^3\mp\ldots\\ &\qquad+(-1)^{k+1}\lim_{n\to\infty}\frac{(1-\frac{1}{n})(2-\frac{1}{n})\ldots(k-1-\frac{1}{n})}{k!}x^k+\ldots\\ &= x-\frac{1}{2}x^2+\frac{1}{3}x^3\mp\ldots+(-1)^{k+1}\frac{1}{k}x^k+\ldots.\end{aligned}$$

On a donc bien (4).

Pierre de la Harpe fournit deux autres manières d'écrire $\ln x$ comme une limite telles que :

$$\forall x>0,\ln x=\lim_{\varepsilon\to0}\frac{x^\varepsilon-1}{\varepsilon}$$

ou

$$\ln x=\lim_{n\to\infty}\left(\sum_{k=1}^{n}(-1)^{k+1}\frac{1}{k}(x-1)^k\right).$$

On aimerait connaître une référence dans la littérature pour la formule :

$$\lim_{n\to\infty}\left(n\left((1+x)^{1/n}-1\right)\right)=\ln(1+x)\quad\text{pour}\quad|x|<1.$$

ainsi que pour la formule

$$\ln x=\lim_{n\to\infty}\left((-1)+\left(x^{\frac{1}{n}}\right)\right)\times n,$$

à mettre en regard de la formule

$$\exp x=\lim_{n\to\infty}\left((+1)+\left(x\times\frac{1}{n}\right)\right)^n.$$

Recherches arithmétiques.

Section Troisième

Des résidus des puissances.

45. Théorème. *Dans toute progression géométrique* $1, a, a^2, a^3$, *etc., outre le premier terme 1, il y en a encore un autre* a' *congru à l'unité suivant le module* p *premier avec* a, *l'exposant* t *étant* $< p$.

Puisque le module p est premier avec a, et par conséquent avec une puissance quelconque de a, aucun terme de la progression ne sera $\equiv 0$ (mod. p), mais chacun d'eux sera congru à quelqu'un des nombres $1, 2, 3, 4, ..., p-1$. Comme le nombre de ces derniers est $p-1$, il est évident que si l'on considère plus de $p-1$ termes de la progression, ils ne pourront pas avoir tous des résidus minima différents. Ainsi parmi les nombres $1, a, a^2, a^3, ..., a^{p-1}$, on en trouvera au moins deux congrus. Soit donc $a^m \equiv a^n$ et $m > n$, on aura, en divisant par a^n (n° 22), $a^{m-n} \equiv 1$, où $m - n < p$ et > 0.

Exemple. Dans la progression $1, 2, 4, 8$, etc. le premier terme qui est congru avec l'unité suivant le module 13, se trouve être $2^{12} = 4096$, mais suivant le module 23, on a dans la même progression, $2^{11} = 2048 \equiv 1$; de même $5^6 = 15625 \equiv 1$ (mod. 7) ; et $5^5 \equiv 3125 \equiv 1$ (mod. 11). Ainsi dans quelques cas la puissance de a congrue avec l'unité, est plus petite que a^{p-1}, et dans d'autres, il faut remonter jusqu'à la puissance $p-1$ elle-même.

46. Quand la progression est continuée au-delà du terme qui est congru à l'unité, on retrouvera les mêmes résidus qu'on avait à partir du commencement. Ainsi, soit $a^t \equiv 1$, on aura $a^{t+1} \equiv a$, $a^{t+2} \equiv a^2$, etc., jusqu'à ce qu'on parvienne au terme a^{2t}, dont le résidu minimum sera de nouveau 1, et la période des résidus recommencera. On aura ainsi une période de t résidus qui se répétera continuellement, et l'on ne pourra trouver un seul résidu qui ne fasse partie de cette période. On aura en général $a^{mt} \equiv 1$ et $a^{mt+n} \equiv a^n$; ce qui peut se présenter ainsi suivant notre notation : si $r \equiv \rho$ (mod. t), on aura $a^r \equiv a^\rho$ (mod. p).

47. Ce théorème fournit le moyen de trouver facilement les résidus des puissances, quelle que soit la grandeur de l'exposant dont elles sont affectées, en même temps qu'on découvrira la puissance congrue à l'unité. Si, par exemple, on demande le reste de la division de 3^{1000} par 13, comme $3^3 \equiv 1$ (mod. 13), on a $t = 3$, et comme d'ailleurs $1000 \equiv 1$ (mod. 3), on trouvera $3^{1000} \equiv 3$ (mod 13).

48. Si a^t est la plus petite puissance congrue à l'unité, (en exceptant $a^0 = 1$, cas que nous ne considérons pas), les t restes qui composent la période seront tous différents, comme on le voit sans difficulté par la démonstration du n° 45. Alors la proposition du n° 46 peut être renversée. Savoir, si $a^m \equiv a^n$ (mod. p), on aura $m \equiv n$ (mod. t) : car si m et n étaient incongrus suivant t, leurs résidus minima μ et ν seraient différents. Mais $a^\mu \equiv a^m$, $a^\nu \equiv a^n$; donc $a^\mu \equiv a^\nu$, c'est-à-dire, que

---

Transcription en LaTeX, ce format permettant des traductions aisées dans les multiples langues proposées par les outils de traduction automatique (ce que ne permet pas un document scanné).
Denise Vella-Chemla, mars 2024.

toutes les puissances au dessous de a^t ne seraient pas incongrues, ce qui est contre l'hypothèse.

Si donc $a^k \equiv 1 \pmod{p}$, on aura $k \equiv 0 \pmod{t}$, c'est-à-dire que k sera divisible par t.

Nous avons parlé jusqu'ici de modules quelconques, pourvu qu'ils fussent premiers avec a. À présent examinons à part les modules qui sont des nombres premiers absolus, et établissons sur ce fondement des recherches plus générales.

49. THÉORÈME. *Si p est un nombre premier qui ne divise pas a, et que a^t soit la plus petite puissance de a congrue à l'unité, l'exposant t sera $= p-1$, ou une partie aliquote de $p-1$.*

Voyez pour des exemples le n° 45.

Comme nous avons déjà prouvé que t est $= p-1$ ou $< p-1$, il reste à faire voir que dans le dernier cas il est toujours une partie aliquote de $p-1$.

1°. Rassemblons les résidus minima positifs de tous les termes, $1, a, a^2, a^3, ..., a^{t-1}$, et désignons-les par $\alpha, \alpha', \alpha''$, etc. de sorte qu'on ait $\alpha = 1, \alpha' \equiv a, \alpha'' \equiv a^2$, etc. il est visible qu'ils seront tous différents ; car si deux termes a^m, a^n donnaient les mêmes résidus, on aurait $a^{m-n} \equiv 1$ (en supposant $m > n$ et $m-n < t$) ; ce qui est absurde, puisque a^t est la plus petite puissance de a congrue à l'unité. Au reste tous les nombres $\alpha, \alpha', \alpha''$, etc. sont compris dans la série $1, 2, 3, 4, ..., p-1$, série qu'ils n'épuisent pas lorsque $t < p-1$. Nous désignerons par (A) la somme de tous ces résidus, et (A) comprendra un nombre t de termes.

2°. Prenons un nombre quelconque β, parmi ceux de la série $1, 2, 3, ..., p-1$ qui manquent dans (A). Multiplions β par $\alpha, \alpha', \alpha''$, etc. et nommons β, β', β'', etc. les résidus minima qui en proviendront, et qui seront aussi en nombre t. Ces résidus seront différents entre eux, et différeront des nombres $\alpha, \alpha', \alpha''$, etc. En effet, si la première assertion était fausse, on aurait $\beta a^m \equiv \beta a^n$, d'où l'on tire, en divisant par β, $a^m \equiv a^n$: ce qui est contre ce que nous venons de démontrer : si la dernière l'était, on aurait $\beta a^m \equiv a^n$; d'où, quand $n > m$, $\beta \equiv a^{n-m}$, c'est-à-dire que β serait congru à quelqu'un des nombres $\alpha, \alpha', \alpha''$, etc. : ce qui est contre l'hypothèse ; mais si $n < m$, on aura, en multipliant par a^{t-m}, $\beta a^t \equiv a^{t+m-n}$, ou, comme $a^t \equiv 1$, $\beta \equiv a^{t-(m-n)}$, d'où résulte la même absurdité. Désignons par (B) la somme des nombres β, β', β'', etc. qui sont en nombre t ; on aura déjà $2t$ nombres parmi ceux-ci $1, 2, 3, ..., p-1$. Donc si (A) et (B) épuisent cette série, on aura $t = \frac{p-1}{2}$.

3°. Mais s'il en manque quelques-uns, soit γ un de ceux-là. Multiplions $\alpha, \alpha', \alpha''$, etc. par γ, et soient $\gamma, \gamma', \gamma''$, etc. les résidus minima de ces produits, dont nous désignerons l'ensemble par (C) ; (C) comprendra t nombres pris dans la série $1, 2, 3, ..., p-1$ qui seront tous différents entre eux et non-compris dans (A) et (B). Les deux premières assertions se démontrent comme ci-dessus (2°) ; quant à la troisième, si l'on avait $\gamma a^m \equiv \beta a^n$, on en tirerait $\gamma \equiv \beta a^{n-m}$, ou $\gamma \equiv \beta a^{t-(m-n)}$, suivant que $m < n$ ou $> n$. Dans l'un ou l'autre cas γ serait congru à quelqu'un des nombres qui composent (B) ; ce qui serait contre l'hypothèse. On aura ainsi $3t$ nombres pris dans la série $1, 2, 3, ..., p-1$, et s'il n'en reste plus, $t = \frac{p-1}{3}$, conformément au théorème.

4°. Mais s'il en reste encore quelques-uns, on arrivera de même à une quatrième somme de

nombres (D), etc. ; et comme la série $1, 2, 3$, etc. $p-1$ est finie, on voit que l'on parviendra nécessairement à l'épuiser, et $p-1$ sera un multiple de t ; donc t sera une partie aliquote de $p-1$.

50. Puisque $\frac{p-1}{t}$ est un nombre entier, il suit qu'en élevant chaque membre de la congruence $a^t \equiv 1 \pmod{p}$ à la puissance $\frac{p-1}{t}$, on aura $a^{p-1} \equiv 1 \pmod{p}$; c'est-à-dire, que $a^{p-1}-1$ *sera toujours divisible par* p *quand* p *est premier et qu'il ne divise pas* a.

Ce théorème remarquable, tant par son élégance que par sa grande utilité, s'appelle ordinairement *théorème de Fermat*, du nom de l'inventeur. (*Fermatii opera Math. Tolosæ 1679. Fol. p. 163*) Fermat n'en a pas donné la démonstration, bien qu'il ait assuré qu'il l'avait trouvée. Euler en a le premier publié une dans la Dissertation intitulée : *Démonstration de quelques théorèmes relatifs aux nombres premiers.* (*Comm. Ac. Pétrop. T.* VIII)[1] ; elle est tirée du développement de $(a+1)^p$, qui fait voir par la forme des coefficients, que $(a+1)^p - a^p - 1$ est toujours divisible par p, et que par conséquent $(a+1)^p - (a+1)$ le sera si $a^p - a$ l'est. Or comme $1^p - 1$ est divisible par p, $2^p - 2$ le sera donc ; et partant $3^p - 3$, et généralement $a^p - a$. Donc si p ne divise pas a, on aura aussi $a^{p-1} - 1$ divisible par p. Ce que nous venons de dire suffit pour faire connaître l'esprit de la démonstration.

Lambert en a donné une semblable, (*Acta eruditorum.* 1769, p. 109). Mais comme le développement de la puissance d'un binôme semble étranger à la théorie des nombres, Euler (*Comm. nov. Petrop. T.* VIII*, p. 70*) donna une autre démonstration qui est conforme à celle que nous venons d'exposer. Dans la suite il s'en présentera encore d'autres : ici nous nous contenterons d'en donner encore une déduite du même principe que celle d'Euler. La proposition suivante, dont le théorème en question n'est qu'un cas particulier, nous sera utile pour d'autres recherches.

51. *Si* p *est un nombre premier, la puissance* p *du polynome* $a+b+c+\text{etc.}$ *est* $\equiv a^p + b^p + c^p + \text{etc.}$ *suivant le module* p.

On sait que $(a+b+c+\text{etc.})^p$ est composé de termes de la forme $Pa^\alpha b^\beta c^\gamma$ etc. où l'on a $\alpha+\beta+\gamma+$ etc.$= p$, P étant le nombre de permutations de p choses, dont α, β, γ, etc. sont respectivement égales à a, b, c, etc. Mais nous avons fait voir (n° 41) que ce nombre était toujours divisible par p, à moins que toutes les lettres ne fussent égales entre elles ; c'est-à-dire, à moins que l'un des nombres α, β, γ,etc. ne fût égal à p, et les autres égaux à zéro ; d'où il suit que tous les termes du développement, excepté a^p, b^p, etc. sont divisibles par p, et que par conséquent $(a+b+c+\text{etc.})^p \equiv a^p + b^p + c^p + \text{etc.} \pmod{p}$.

Si toutes les quantités a, b, c, etc. sont supposées $= 1$, et que leur nombre soit k, on aura $k^p \equiv k$, comme dans le n° précédent.

[1] Antérieurement (*Comm. Petr. T.* VI. *p. 106*) ce grand homme n'était pas parvenu encore au but. Dans la fameuse discussion entre Maupertuis et Konig, sur le principe de la moindre action, discussion qui les jeta dans des digressions étrangères, Konig assura qu'il avait entre les mains un manuscrit autographe de Leibniz, qui contenait une démonstration de ce théorème conforme à celle d'Euler (*Appel au Public* p. 106). Quoique nous ne voulions pas refuser de croire à ce témoignage, il est sûr cependant que Leibniz n'a jamais publié sa démonstration. (*Voyez Hist. de l'Acad. de Berlin. 1750. p. 530*).

52. Comme les nombres qui sont diviseurs de $p-1$ sont les seuls qui puissent servir d'exposants aux plus petites puissances congrues avec l'unité, on est porté à chercher si tous les diviseurs de $p-1$ jouissent de cette propriété ; et, quand on classe tous les nombres non divisibles par p suivant l'exposant de leur plus petite puissance congrue à l'unité, combien il y en a pour chaque exposant. Nous observerons d'abord qu'il suffit de considérer les nombres positifs depuis 1 jusqu'à $p-1$: il est évident en effet que les nombres congrus doivent être élevés à la même puissance pour devenir congrus à l'unité, et que par conséquent un nombre quelconque doit être rapporté au même exposant que son résidu minimum positif ; ainsi nous avons à rechercher comment les nombres $1, 2, 3, ..., p-1$, doivent être distribués sous ce point de vue, relativement aux facteurs de $p-1$. Pour abréger, si d est un des facteurs de $p-1$, entre lesquels on doit compter 1 et $p-1$, nous représenterons par ψd la multitude des nombres positifs plus petits que p, dont la puissance d est la plus petite qui soit congrue à l'unité.

53. Pour nous faire entendre plus facilement, nous présenterons d'abord un exemple. Soit $p = 19$, les nombres $1, 2, 3, ..., 18$ peuvent se distribuer de la manière suivante relativement aux diviseurs de 18 :

$$1\left\{1,\right. \quad 2\left\{18,\right. \quad 3\left\{\begin{array}{l}7\\11\end{array}\right., \quad 6\left\{\begin{array}{l}8\\12\end{array}\right., \quad 9\left\{\begin{array}{lll}4, & 5, & 6\\9, & 16, & 17\end{array}\right., \quad 18\left\{\begin{array}{lll}2, & 3, & 10\\13, & 14, & 15\end{array}\right..$$

Ainsi dans ce cas $\psi 1 = 1, \psi 2 = 1, \psi 3 = 2, \psi 6 = 2, \psi 9 = 6, \psi 18 = 6$. Avec une légère attention on voit qu'il y en a, relativement à chaque exposant, autant qu'il y a de nombres premiers avec cet exposant et non plus grands que lui, ou bien, en reprenant le signe du n° 40, que $\psi d = \varphi d$. Mais on peut démontrer généralement cette observation de la manière suivante :

1°. S'il y a un nombre a appartenant à l'exposant d, c'est-à-dire dont la puissance d soit congrue à l'unité, et les puissances inférieures incongrues, toutes les puissances de ce nombre, savoir $a, a^2, a^3, a^4, ..., a^d$, ou leurs résidus minima, auront leur puissance d congrue avec l'unité ; et comme cela peut s'exprimer en disant que les résidus minima des nombres $a, a^2, a^3, ..., a^d$ qui sont tous différents sont les racines de la congruence $x^d \equiv 1$, qui ne peut avoir plus de d racines différentes, il est évident qu'il n'y a pas de nombres autres que les résidus minima de $a, a^2, a^3, ..., a^d$, dont les puissances d soient congrues à l'unité ; d'où il suit que les nombres appartenant à l'exposant d se trouvent tous entre les résidus minima des nombres $a, a^2, a^3, ..., a^d$. On déterminera comme il suit quels ils sont et quel est leur nombre. Si k est un nombre premier avec d, toutes les puissances de a^k, dont les exposants sont $< d$, ne seront pas congrues à l'unité. Soit en effet $\frac{1}{k} \pmod{d} = m$ (voyez n° 31), on aura $a^{km} \equiv a$; donc si la puissancee e de a^k était congrue à l'unité, et que l'on eût $e < d$, on aurait aussi $a^{kme} \equiv 1$, et par conséquent $a^e \equiv 1$; ce qui est contre l'hypothèse. Il est évident, d'après cela, que le résidu minimum de a^k appartiendra à d ; mais si k a un commun diviseur δ avec d, le résidu minimum de a^k n'appartiendra pas à l'exposant d. Car $\frac{kd}{\delta}$ est divisible par d, ou bien $\frac{kd}{\delta} \equiv 0 \pmod{d}$; par conséquent $a^{\frac{kd}{\delta}} \equiv 1$; c'est-à-dire $(a^k)^{\frac{d}{\delta}} \equiv 1$. Nous conclurons de là qu'il y a autant de nombres appartenant à l'exposant d, qu'il y a de nombres premiers avec d dans la série $1, 2, 3, ..., d$. Mais il faut se souvenir que cette conclusion suppose qu'il existe déjà un nombre a appartenant à l'exposant d ; par conséquent il reste douteux s'il ne pourrait pas se faire qu'aucun nombre n'appartînt à un exposant donné, et la conclusion se réduit à $\psi d = 0$, ou $= \varphi d$.

54. 2°. Soient d, d', d'', etc. les diviseurs de $p-1$; comme tous les nombres $1, 2, 3, ..., p-1$ doivent être distribués entre ces diviseurs, on aura $\psi d + \psi d' + \psi d''$+etc.$= p-1$. Mais (n° 40) nous avons démontré que $\varphi d + \varphi d' + \varphi d''$+ etc.$= p-1$, et du n° précédent il suit que $\psi d = 0$ ou $= \varphi d$; et par conséquent que ψd ne peut pas être $> \varphi d$; ce qui s'étend à $\psi d'$ et $\varphi d'$, etc. Si donc un ou plusieurs des nombres $\psi d, \psi d'$, etc. étaient plus petits que son correspondant parmi les nombres $\varphi d, \varphi d'$, etc., la somme des premiers ne pourrait être égale à la somme des derniers. D'où nous concluons enfin que dans tous les cas, $\psi d = \varphi d$, et que par conséquent ψd ne dépend point de la grandeur de $p-1$.

55. Il y a un cas particulier de la proposition précédente qui mérite de fixer notre attention ; le voici : *il existe toujours des nombres dont aucune puissance plus petite que* $p-1$ *n'est congrue à l'unité* ; il y en a même autant entre 1 et $p-1$, qu'il y a au-dessous de $p-1$ de nombres qui lui soient premiers. Comme il s'en faut bien que la démonstration de ce théorème soit aussi évidente qu'elle le paraît d'abord, nous en donnerons une un peu différente de celle qui précède, d'autant plus que la diversité des méthodes aide beaucoup à jeter du jour sur les points les plus obscurs.

On décomposera $p-1$ en facteurs premiers, de manière qu'on ait $p-1 = a^\alpha b^\beta c^\gamma$ etc. a, b, c, etc. étant des nombres premiers inégaux. Alors nous composerons la démonstration des deux propositions suivantes :

1°. On peut toujours trouver un nombre A, ou plusieurs appartenant à l'exposant a^α, et de même des nombres B, C, etc. appartenant aux exposants b^β, c^γ, etc.

2°. Le produit des nombres A, B, C, etc. ou le résidu minimum de ce produit appartiendra à l'exposant $p-1$; ce qui se démontre ainsi qu'il suit.

1º. Soit g un des nombres $1, 2, 3, ..., p-1$ qui ne satisfasse pas à la congruence $x^{\frac{p-1}{a}} \equiv 1 \pmod{p}$; car tous les nombres ne peuvent pas satisfaire à cette congruence, dont le degré est $< p-1$. Alors je dis que si l'on fait $g^{\frac{p-1}{a^\alpha}} \equiv h$, h ou son résidu minimum appartiendra à l'exposant a^α.

En effet il est évident que $h^{a^\alpha} \equiv g^{p-1} \equiv 1$; mais $h^{a^{\alpha-1}} \equiv g^{\frac{p-1}{a}}$, et par conséquent sera incongru à l'unité, et à plus forte raison les puissances $h^{a^{\alpha-2}}, h^{a^{\alpha-3}}$ le seront aussi. Or l'exposant de la plus petite puissance de h congrue à l'unité, c'est-à-dire l'exposant auquel h appartient, doit être un diviseur de a^α (n° 48) ; et comme a^α n'est divisible que par lui-même, ou par les puissances inférieures de a, il s'ensuit nécessairement que a^α sera l'exposant auquel b appartient. On démontrera de la même manière, qu'on peut trouver des nombres appartenant aux exposants b^β, c^γ, etc.

2°. Si nous supposons que le produit de tous les nombres A, B, C, etc. n'appartienne pas à l'exposant $p-1$, etc., mais à un exposant t plus petit, t devra être un des diviseurs de $p-1$ (n° 48), ou $\frac{p-1}{t}$ sera un entier > 1. Il suit de là que ce quotient sera un des nombres premiers a, b, c, etc., ou du moins qu'il sera divisible par quelqu'un d'eux (n° 17), par a, par exemple, car le raisonnement est le même pour les autres. t divisera ainsi $\frac{p-1}{a}$; donc le produit ABC etc. serait encore congru à l'unité, en l'élevant à la puissance $\frac{p-1}{a}$ (n° 46). Mais il est évident que tous les nombres, B, C, D, etc. (excepté A) deviennent congrus à l'unité, si on les élève à la puissance $\frac{p-1}{a}$ puisque les exposants auxquels ils appartiennent b^β, c^γ, etc. divisent $\frac{p-1}{a}$. Donc $A^{\frac{p-1}{a}}.B^{\frac{p-1}{a}}.C^{\frac{p-1}{a}}$. etc.$\equiv A^{\frac{p-1}{a}} \equiv 1$; donc

a^α doit diviser $\frac{p-1}{a}$ (n° 48), c'est-à-dire que $\frac{p-1}{a^{\alpha+1}}$ doit être entier, ce qui est absurde (n° 15). Donc enfin notre supposition ne peut subsister, c'est-à-dire que le produit ABC etc. appartient réellement à l'exposant $p-1$.

La dernière démonstration semble un peu plus longue que la première, mais elle est plus directe.

56. Ce théorème nous fournit un exemple remarquable de la circonspection dont on a besoin dans la théorie des nombres, pour ne pas regarder comme démontrées des choses qui ne le sont pas. LAMBERT, dans la Dissertation que nous avons citée plus haut, fait mention de cette proposition, mais ne dit pas un mot de la nécessité de la démontrer. Personne même n'a tenté de le faire, excepté EULER (*Comm. nov. Ac. Pétrop. T.* XVIII, *p. 85*), dans son Mémoire intitulé : *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia.* On peut voir surtout l'art. 37, dans lequel il a parlé avec étendue de la nécessité de démontrer cette proposition. Cependant la démonstration de cet homme pénétrant présente deux défauts ; l'un tient à ce qu'il suppose tacitement, art. 31 et suivants, que la congruence $x^n \equiv 1$, (en ramenant ses raisonnements à notre notation) a réellement n racines différentes, tandis qu'il était seulement démontré que cette congruence ne peut en avoir davantage ; l'autre, à ce qu'il ne déduit que par induction la formule du n° 34.

57. Nous nommerons avec EULER, *racines primitives* les nombres qui appartiennent à l'exposant $p-1$. Si donc a est une racine primitive, tous les résidus minima des puissances $a, a^2, a^3, ..., a^{p-1}$ seront différents ; d'où l'on déduit facilement qu'ils se trouvent tous parmi les nombres $1, 2, 3, ..., p-1$ qui sont en même nombre qu'eux, c'est-à-dire que tout nombre non divisible par p est congru à quelque puissance de a. Cette propriété remarquable est d'une bien grande utilité, et peut considérablement abréger les opérations arithmétiques relatives aux congruences, à peu près de la même manière que l'introduction des logarithmes dans l'arithmétique ordinaire en abrège les opérations. Nous prendrons arbitrairement pour *base* une racine primitive a, à laquelle nous rapporterons tous les nombres non divisibles par p ; et si on a $a^e \equiv b \pmod{p}$, nous appellerons e l'*indice* de b. Par exemple, 2 est une racine primitive suivant le module 19 ; si on la prend pour base,

aux nombres	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11,	12,	13,	14,	15,	16,	17,	18
répondront les indices	0,	1,	13,	2,	16,	14,	6,	3,	8,	17,	12,	15,	5,	7,	11,	4,	10,	9.

Au reste il est évident que pour la même base chaque nombre a plusieurs indices, mais qui seront tous congrus suivant le module $p-1$; aussi quand il sera question d'indices, ceux qui seront congrus suivant le module $p-1$, seront regardés comme équivalents, de même que les nombres sont regardés comme équivalents lorsqu'ils sont congrus suivant le module p.

58. Les théorèmes qui regardent les indices sont absolument analogues à ceux qui regardent les logarithmes.

L'indice d'un produit de tant de facteurs qu'on voudra, est congru à la somme des indices des différents facteurs, suivant le module $p-1$.

L'indice de la puissance d'un nombre est congru, suivant le module $p-1$, *au produit de l'exposant*

par l'indice du nombre donné.

Nous omettons les démonstrations à cause de leur simplicité.

On voit par là que si nous voulions construire une table qui donnât les indices de tous les nombres pour différents modules, nous pourrions nous dispenser de tenir compte de tous les nombres plus grands que le module et de tous les nombres composés. On trouvera à la fin de cet ouvrage un essai de cette table (Tab. I). Dans la première colonne sont rangés les nombres premiers et les puissances de nombres premiers depuis 3 jusqu'à 97, qui doivent être regardés comme des modules : à côté de chacun d'eux, dans la colonne suivante, les nombres pris pour bases ; suivent alors les indices des nombres premiers successifs, qui sont écrits par tranches composées de cinq chacune ; en tête se trouvent les nombres premiers disposés dans le même ordre. De sorte qu'on peut trouver facilement l'indice qui répond à un nombre premier donné, suivant un module donné.

Soit par exemple $p = 67$; l'indice de 60, en prenant 12 pour base, sera

$$\equiv 2 \text{ Ind. } 2 + \text{Ind. } 3 + \text{Ind. } 5 \text{ (mod. } 66) \equiv 58 + 9 + 39 \equiv 40.$$

59. L'indice de la valeur d'une expression quelconque $\frac{a}{b}$ (mod. p), (n° 31) est congru suivant le module $p - 1$, à la différence des indices du numérateur a et du dénominateur b, pourvu que les nombres a et b ne soient pas divisibles par p.

Soit en effet c une valeur quelconque de cette expression, on aura $bc \equiv a$ (mod. p) ; donc Ind. b + Ind. $c \equiv$ Ind. a (mod. $p - 1$), et

$$\text{Ind. } c \equiv \text{Ind. } a - \text{Ind. } b.$$

Si donc on a deux tables, dont l'une donne les indices qui répondent à chaque nombre pour un module quelconque, et dont l'autre donne les nombres qui répondent à des indices donnés, on pourra résoudre facilement toutes les congruences du premier degré, puisqu'on peut toujours les ramener à d'autres dont les modules soient premiers (n° 30).

Soit par exemple la congruence $29x + 7 \equiv 0$ (mod. 47), on aura $x \equiv \frac{-7}{29}$ (mod. 47).

De là [2]

$$\text{Ind. } x \equiv \text{Ind. } -7 - \text{Ind. } 29 \equiv \text{Ind. } 40 - \text{Ind. } 29 \equiv 15 - 43 \equiv 18 \text{ (mod. } 46);$$

or 3 est le nombre qui a pour indice 18 ; donc $x \equiv 3$ (mod. 47). Nous n'avons point ajouté la seconde table, mais on verra dans la section VI comment on peut la remplacer par une autre.

60. De même que dans le n° 31 nous avons désigné par un signe particulier, les racines des congruences du premier degré, dans ce qui va suivre, nous représenterons par un autre signe les racines des congruences à deux termes des degrés supérieurs ; et comme $\sqrt[n]{A}$ ne signifie autre chose que la racine de l'équation $x^n = A$; en ajoutant le module, $\sqrt[n]{A}$ (mod. p) représentera une racine quelconque de la congruence $x^n \equiv A$ (mod. p). Ainsi nous dirons que l'expression $\sqrt[n]{A}$ (mod. p) a autant de valeurs qu'elle en a d'incongrues suivant p ; car toutes celles qui sont congrues suivant p

[2] *Note de la transcriptrice : Gauss a pris 10 comme base.*

doivent être regardées comme équivalentes (n° 26). Au reste il est clair que si A et B sont congrus suivant p, les expressions $\sqrt[n]{A}$ (mod. p), $\sqrt[n]{B}$ (mod. p) seront équivalentes.

Maintenant si l'on fait $\sqrt[n]{A} \equiv x \pmod{p}$, on aura

$$n \text{ Ind. } x \equiv \text{Ind. } A \pmod{p-1}.$$

On déduit de cette congruence, d'après les règles de la section II, les valeurs de Ind. x, et de là les valeurs correspondantes de x ; mais on voit facilement que x a autant de valeurs qu'il y a de racines dans la congruence

$$n \text{ Ind. } x \equiv \text{Ind. } A \pmod{p-1};$$

donc $\sqrt[n]{A}$ n'aura qu'une valeur, quand n sera premier avec $p-1$; mais lorsque n et $p-1$, auront un commun diviseur, et que δ sera le plus grand, Ind. x aura δ valeurs incongrues suivant $p-1$, et par conséquent $\sqrt[n]{A}$ aura autant de valeurs incongrues suivant p, pourvu que Ind. A soit divisible par δ. Sans cette condition, $\sqrt[n]{A}$ n'aurait aucune valeur réelle.

Si l'on cherche par exemple les valeurs de l'expression $\sqrt[15]{11}$ (mod. 19), il faut résoudre la congruence 15 Ind. $x \equiv$ Ind. $11 \equiv 6 \pmod{18}$ on trouvera [3] trois valeurs de Ind. $x \equiv 4, 10, 16 \pmod{18}$, d'où il résulte $x \equiv 6, 9, 4$.

61. Quoique cette méthode soit très expéditive, quand on a les tables nécessaires, nous ne devons cependant pas oublier qu'elle est indirecte ; il sera donc utile de chercher ce que peuvent donner les méthodes directes. Nous allons exposer ici les observations que l'on peut déduire des notions précédentes ; quant à ce qui exige des considérations plus profondes, nous le réserverons pour la section VIII [4].

Nous commencerons par le cas le plus simple ; celui où $A = 1$, c'est-à-dire, dans lequel on cherche les racines de la congruence $x^n \equiv 1 \pmod{p}$. En prenant pour base une racine primitive quelconque, on doit avoir n Ind. $x = 0 \pmod{p-1}$. Quand n est premier avec $p-1$, cette congruence n'aura qu'une seule racine, savoir

$$\text{Ind. } x \equiv 0 \pmod{p-1} ;$$

donc, dans ce cas $\sqrt[n]{1}$ (mod. p) n'aura qu'une valeur $x \equiv 1 \pmod{p}$; mais quand n et $p-1$ ont δ pour plus grand diviseur commun, la solution complète de la congruence n Ind. $x \equiv 0 \pmod{p-1}$ sera $x \equiv 0 \pmod{\frac{p-1}{\delta}}$ (n° 30), c'est-à-dire, que Ind. x devra être congru suivant le module $p-1$ à quelqu'un des nombres $0, \frac{p-1}{\delta}, \frac{2(p-1)}{\delta}, \ldots, \frac{(\delta-1)(p-1)}{\delta}$, ou qu'il aura δ valeurs incongrues suivant le module $p-1$; donc aussi, dans ce cas, x aura δ valeurs incongrues suivant p. On voit aussi que l'expression $\sqrt[\delta]{1}$ (mod. p) a aussi δ valeurs dont les indices sont absolument les mêmes que les précédents ; donc l'expression $\sqrt[\delta]{1}$ (mod. p) est tout-à-fait équivalente à l'expression $\sqrt[n]{1}$ (mod. p), ou ce qui revient au même, la congruence $x^\delta \equiv 1 \pmod{p}$ et la congruence $x^n \equiv 1 \pmod{p}$ ont les mêmes racines ; mais la première est d'un degré inférieur à moins qu'on n'ait $\delta = n$.

Ex. $\sqrt[15]{1}$ (mod. 19) a trois valeurs, parce que 3 est le plus grand commun diviseur de 15 et 18 ; elles seront également celles de l'expression $\sqrt[3]{1}$ (mod. 19). Ces valeurs sont 1, 7, 11.

[3] *Note de la transcriptrice : Gauss a à nouveau pris comme base 10.*

[4] *Note de la transcriptrice : Il n'y a pas de Section* VIII *dans les Recherches arithmétiques.*

62. Cette réduction nous offre un grand avantage, puisqu'on n'a plus besoin de résoudre parmi les congruences de la forme $x^n \equiv 1 \pmod{p}$ que celles où n est diviseur du module diminué de l'unité. Mais nous ferons voir plus bas que les congruences de cette forme peuvent encore s'abaisser davantage, quoique ce qui précède ne suffise pas pour cela. Il y a cependant un cas que nous pouvons traiter ici à fond, celui où $n = 2$. Il est évident en effet que les valeurs de l'expression $\sqrt[n]{1} \pmod{p}$ seront $+1$ et -1, puisqu'elle n'en peut avoir plus de deux, et que $+1$ et -1 sont incongrus, à moins que le module ne soit $= 2$, cas auquel il est clair que $\sqrt{2}$ n'aurait qu'une seule valeur. Il suit de là que $+1$ et -1 sont aussi les valeurs de l'expression $\sqrt[2m]{1} \pmod{p}$, quand m est premier avec $\frac{p-1}{2}$, ce qui arrivera toujours lorsque le module sera tel que $\frac{p-1}{2}$ soit un nombre absolument premier ; par exemple, quand $p = 3, 5, 7, 11, 23$, etc., à moins que $p - 1 = 2m$, cas auquel tous les nombres $1, 2, 3, ..., p-1$ sont racines. Remarquons, comme conséquence, que l'indice de -1 est toujours $\equiv \frac{p-1}{2} \pmod{p-1}$, quelle que soit la racine primitive que l'on prenne pour base ; car $2 \text{ Ind. } (-1) \equiv 0 \pmod{p-1}$; donc $\text{Ind. } (-1)$ sera $\equiv 0$ ou $\equiv \frac{p-1}{2}$ mais 0 est toujours l'indice de $+1$, et $+1$ et -1 doivent avoir des indices différents, excepté dans le cas où $p = 2$, qu'il n'est pas nécessaire de considérer.

63. Nous avons fait voir (n° 61) que l'expression $\sqrt[n]{A} \pmod{p}$ a δ valeurs différentes ou n'en a absolument aucune, si δ est le plus grand commun diviseur des nombres n et $p - 1$. Or de même que nous avons trouvé que $\sqrt[n]{A}$ et $\sqrt[\delta]{A}$ étaient équivalentes quand on a $A \equiv 1$, nous prouverons plus généralement que l'expression $\sqrt[n]{A}$ peut toujours être ramenée à une autre $\sqrt[\delta]{B}$, à laquelle elle est équivalente. Soit en effet $x^n = A$, et t une valeur quelconque de l'expression $\frac{\delta}{n} \pmod{p-1}$ qui aura toujours (n° 31) des valeurs réelles. De la congruence $x^n \equiv A$ on déduit $x^{tn} \equiv A^t$; mais à cause de $tn \equiv \delta \pmod{p-1}$, $x^{tn} \equiv x^\delta$; donc $x^\delta \equiv A^t$. Ainsi une valeur quelconque de $\sqrt[n]{A}$ sera aussi une valeur de $\sqrt[\delta]{A^t}$; et toutes les fois que $\sqrt[n]{A}$ aura des valeurs réelles, elle sera absolument équivalente à l'expression $\sqrt[\delta]{A^t}$, puisqu'elle ne peut avoir de valeurs différentes, ni en moindre nombre. Il est vrai cependant que $\sqrt[\delta]{A^t}$ peut avoir des valeurs réelles, sans que pour cela $\sqrt[n]{A}$ en ait nécessairement.

Exemple. Si l'on cherche les valeurs de l'expression $\sqrt[21]{2} \pmod{31}$, le plus grand commun diviseur des nombres 21 et 30 est 3, et 3 est une valeur de $\frac{3}{21} \pmod{30}$; donc si $\sqrt[21]{2}$ a des valeurs réelles, elle équivaudra à l'expression $\sqrt[3]{2^3}$ ou $\sqrt[3]{8}$; ou on trouve effectivement que les valeurs de la dernière qui sont 2, 10 et 19, satisfont aussi à la première.

64. Mais afin de ne pas entreprendre inutilement cette opération, il est nécessaire de chercher le caractère auquel on pourra reconnaître si $\sqrt[n]{A}$ admet ou non des valeurs réelles. Si on a une table d'indices la chose est facile, car (n° 60) $\sqrt[n]{A}$ aura des valeurs réelles quand $\text{Ind. } A$ sera divisible par δ, en prenant pour base une racine primitive quelconque, et dans le cas contraire elle n'en aura pas ; mais on peut aussi le découvrir sans le secours de cette table. Soit en effet $k = \text{Ind. } A$, si k est divisible par δ, $\frac{k(p-1)}{\delta}$ sera divisible par $p - 1$ et réciproquement ; mais l'indice du nombre $A^{\frac{p-1}{\delta}}$ est $\frac{k(p-1)}{\delta}$; donc si $\sqrt[n]{A} \pmod{p}$ a des valeurs réelles, $A^{\frac{p-1}{\delta}}$ sera congru à l'unité ; sinon, il sera incongru. Ainsi dans l'exemple de l'article précédent, on a $2^{10} = 1024 \equiv 1 \pmod{31}$, d'où l'on conclut que l'expression $\sqrt[21]{2} \pmod{31}$ a des valeurs réelles. De même nous voyons par là que $\sqrt[2]{-1} \pmod{p}$ a toujours deux valeurs réelles, quand p est de la forme $4m + 1$, et n'en a aucune quand p est de la forme $4m + 3$, car $(-1)^{2m} = 1$ et $(-1)^{2m+1} = -1$. Ce théorème élégant qui s'énonce ordinairement ainsi : *Si p est un nombre premier de la forme $4m + 1$, on peut trouver un carré a^2 qui rende $a^2 + 1$ divisible par p ; mais si p est de la forme $4m - 1$, on ne le pourra pas*, a

été démontré de cette manière par EULER (*Comment. nov. Ac. Petrop. T.* XVIII, *p.* 112, 1773). Il en avait donné une autre démonstration bien antérieurement (*Comm. nov. T.* V, *p.* 5, 1760) ; dans une première dissertation (*T.* IV, *p. 25*), il n'était pas encore parvenu au but. LAGRANGE a depuis donné aussi une démonstration de ce théorème (*Nouv. Mém. de l'Ac. de Berlin. 1775, p. 342*). Nous en exposerons encore une différente dans la section suivante, qui sera consacrée à ce genre de considérations.

65. Après avoir examiné comment on peut réduire toutes les expressions $\sqrt[n]{A} \pmod{p}$ à d'autres dans lesquelles n soit diviseur de $p-1$, et après avoir trouvé le caractère auquel on reconnaît s'il y a des racines réelles ou non, considérons avec plus de soin les expressions $\sqrt[n]{A} \pmod{p}$, dans lesquelles n est diviseur de $p-1$. Nous ferons voir d'abord quelle est la relation qu'ont entre elles les différentes valeurs de cette expression, ensuite nous indiquerons quelques artifices au moyen desquels on peut le plus souvent trouver une des valeurs.

1°. Quand $A \equiv 1$, et que r sera une des valeurs de l'expression $\sqrt[n]{1} \pmod{p}$, ou que $r^n \equiv 1 \pmod{p}$, toutes les puissances de r seront aussi des valeurs de cette expression ; et il y en aura autant de différentes qu'il y a d'unités dans l'exposant auquel r appartient (n° 48). Si donc r est une valeur appartenant à l'exposant n, les puissances $r, r^2, r^3, r^4, ..., r^n$ (où l'unité peut remplacer la dernière) renfermeront toutes les valeurs de l'expression $\sqrt[n]{1} \pmod{p}$. Nous expliquerons plus en détail dans la section VIII [5] comment on peut trouver ces valeurs qui appartiennent à l'exposant n.

2°. Quand A est incongru à l'unité, et que l'on connaît une valeur z de l'expression $\sqrt[n]{A} \pmod{p}$, on trouve les autres de la manière suivante : soient $1, r, r^2, r^3, ..., r^{n-1}$ les valeurs de $\sqrt[n]{1}$, on aura $z, zr, zr^2, zr^3, ..., zr^{n-1}$ pour les valeurs de $\sqrt[n]{A}$; car il est évident que tous ces nombres satisferont à la congruence $x^n \equiv A$; puisqu'en effet, si zr^k est un des nombres de la suite, comme $r^k \equiv 1$ et que $z^n \equiv A$, on aura $r^{nk} \equiv 1$, et partant $z^n r^{nk} = (zr^k)^n \equiv A$. Il est aisé de juger que toutes ces valeurs sont différentes (n° 23) ; donc l'expression $\sqrt[n]{A}$ ne peut avoir d'autres valeurs, puisqu'elle ne peut en avoir plus de n. Par exemple, si une valeur de $\sqrt[n]{A}$ est z, l'autre sera $-z$. On doit conclure de ce qui précède, que l'on ne peut trouver toutes les valeurs de $\sqrt[n]{A}$, à moins qu'on ne puisse avoir toutes celles de $\sqrt[n]{1}$.

66. La seconde recherche que nous nous étions proposée, consiste à déterminer le cas où l'on peut trouver directement une valeur de l'expression $\sqrt[n]{A} \pmod{p}$, dans laquelle n est diviseur de $p-1$. Cela arrive quand il y a une valeur congrue à une puissance de A, et comme ce cas est très fréquent, il ne sera pas déplacé de s'y arrêter un instant. Soit z cette valeur, si elle existe, on aura $z \equiv A^k$ et $z^n \equiv A \pmod{p}$; donc $A \equiv A^{kn}$; et si l'on peut déterminer k de manière que cette condition soit remplie, A^k sera la valeur cherchée ; mais la condition précédente revient à celle-ci $kn \equiv 1 \pmod{t}$, t étant l'exposant auquel A appartient. Or pour que cette congruence soit possible, il faut que n soit premier avec t, et dans ce cas on aura $k = \frac{1}{n} \pmod{t}$; si au contraire t et n ont un diviseur commun, aucune valeur de z ne sera congrue à une puissance de A.

67. Mais comme il est nécessaire pour cette solution de connaître t, voyons comment il faut procéder quand on ne le connaît pas. On voit d'abord facilement que t doit être diviseur de $\frac{p-1}{n}$ lorsque $\sqrt[n]{A} \pmod{p}$ a des valeurs réelles, ce que nous supposons ici. Soit en effet y l'une quelconque de ces valeurs, on aura (n° 50) $y^{p-1} \equiv 1$, et $y^n \equiv A \pmod{p}$; en élevant à la puissance $\frac{p-1}{n}$

[5] *voir note de la transcriptrice pour la section 61.*

les deux membres de la congruence $y^n \equiv A$, on aura $y^{p-1} \equiv A^{\frac{p-1}{n}} \equiv 1$; d'ailleurs $A^t \equiv 1$; donc $\frac{p-1}{n} \equiv 0 \pmod{t}$ (n° 48). Or si $\frac{p-1}{n}$ est premier avec n, la congruence $kn \equiv 1$ pourra être résolue suivant le module $\frac{p-1}{n}$, et toute valeur de k qui y satisfera suivant ce module, y satisfera aussi (n° 5) suivant le module t diviseur de $\frac{p-1}{n}$; donc on trouvera alors ce qu'on cherchait. Si $\frac{p-1}{n}$ n'est pas premier avec n, soit q le produit des facteurs premiers de $\frac{p-1}{n}$ qui divisent en même temps n ; $\frac{p-1}{nq}$ sera premier avec n, et si la condition que t soit premier avec n a lieu, t sera aussi premier avec q, et comme il divise $\frac{p-1}{n}$, il divisera donc $\frac{p-1}{nq}$; ainsi en résolvant la congruence $kn \equiv 1 \pmod{\frac{p-1}{nq}}$, ce qui peut se faire puisque n est premier avec $\frac{p-1}{nq}$, la valeur de k satisfera aussi à la congruence, suivant le module t. Tout l'artifice consiste à trouver un nombre qui puisse remplacer t, que nous ne connaissons pas ; mais il faut se souvenir que dans le cas où $\frac{p-1}{n}$ n'est pas premier avec n, nous avons supposé n premier avec t ; et si cette condition manque, toutes les conclusions sont fausses ; c'est pourquoi, si en suivant témérairement les règles, on trouve pour z une valeur dont la puissance n ne soit pas congrue à A ; le résultat prouvera que cette condition n'a pas lieu, et que partant la méthode n'est pas applicable.

68. Mais dans ce cas même, il est souvent avantageux de faire cette recherche : elle offre l'avantage de faire trouver de vraies valeurs au moyen des fausses. Supposons en effet que les nombres k et z aient été convenablement déterminés, mais qu'on n'ait pas $z^n \equiv A \pmod{p}$. Alors si on pouvait seulement déterminer les valeurs de $\sqrt[n]{\frac{A}{z^n}} \pmod{p}$, ces différentes valeurs étant multipliées par z donneraient celles de $\sqrt[n]{A}$: en effet, si ν est une valeur de $\sqrt[n]{\frac{A}{z^n}}$ on aura $\nu^n z^n \equiv A$; mais l'expression $\sqrt[n]{\frac{A}{z^n}}$ est plus simple que $\sqrt[n]{A}$, parce que le plus souvent $\frac{A}{z^n}$ appartient à un exposant moindre que A ; car si d est le plus grand commun diviseur de t et de q, $\frac{A}{z^n} \pmod{p}$ appartiendra à l'exposant d, ce qui se démontre ainsi : puisque $z \equiv A^k$, il vient $\frac{A}{z^n}.A^{kn-1} \equiv 1 \pmod{p}$; mais $kn-1$ est divisible par $\frac{p-1}{nq}$ (n° préc.), $\frac{p-1}{n}$ l'est par t, ou $\frac{p-1}{nd}$ par $\frac{t}{d}$. D'ailleurs $\frac{t}{d}$ est premier avec $\frac{q}{d}$; donc aussi $\frac{p-1}{nd}$ est divisible par $\frac{tq}{d^2}$ ou $\frac{p-1}{nq}$ par $\frac{t}{d}$, et partant $kn-1$ par $\frac{t}{d}$, ou $(kn-1)d$ par t. Donc $A^{(kn-1)d} \equiv 1 \pmod{p}$; d'où l'on déduit facilement que $\frac{A}{z^n}$ élevé à la puissance d est congru à l'unité. Il serait facile de démontrer que $\frac{A}{z^n}$ ne peut pas appartenir à un exposant plus petit que d ; mais comme cette démonstration ne peut nous être utile, nous ne nous y arrêterons pas. Nous sommes donc certains que $\frac{A}{z^n} \pmod{p}$ appartient toujours à un plus petit exposant que A, excepté dans le cas unique où l'on aurait $d = t$.

Mais à quoi sert que $\frac{A}{z^n}$ appartienne à un plus petit exposant que A ? Il y a plus de nombres qui peuvent être A qu'il n'y en a qui peuvent être $\frac{A}{z^n}$, et quand on a occasion de résoudre plusieurs expressions de la forme $\sqrt[n]{A}$, suivant le même module, on y gagne de pouvoir tirer d'une même source la solution de plusieurs. Ainsi, par exemple, on déterminera au moins une valeur de $\sqrt[2]{A} \pmod{29}$, si l'on connait seulement les valeurs de $\sqrt[2]{-1} \pmod{29}$, qui sont ± 12 ; en effet l'on voit sans peine, par les articles précédents, que l'on déterminera d'une manière directe une valeur quand t est impair, et que d sera $= 2$ quand t est pair ; or il n'y a que -1 qui appartienne à l'exposant 2.

Exemples.

Soit $\sqrt[3]{31} \pmod{37}$; on a $p-1 = 36, n = 3, \frac{p-1}{n} = 12$, et partant $q = 3$; il faut donc qu'on ait $3k \equiv 1 \pmod{4}$, ce qui donne $k \equiv 3$. Donc $z \equiv 31^3 \pmod{37} \equiv 6$; l'on trouve effectivement

$6^3 = 31$ (mod. 37). Si les valeurs de $\sqrt[3]{1}$ (mod. 37) étaient connues, on pourrait aussi déterminer les autres valeurs de $\sqrt[3]{31}$: or les valeurs de $\sqrt[3]{1}$ (mod. 37) sont $1, 10, 26$; donc celles de $\sqrt[3]{31}$ seront $6, 23, 8$.

Soit maintenant $\sqrt[2]{3}$ (mod. 37) ; on aura $p-1 = 36, n = 2, \frac{p-1}{n} = 18$, et partant $q = 2$; donc on doit avoir $2k \equiv 1$ (mod. 9) d'où $k \equiv 5$; donc $z \equiv 3^5 \equiv 21$ (mod. 37) ; mais 21^2 n'est pas congru avec 3, mais avec 34 ; or on a $\frac{3}{34}$ (mod. 37) $\equiv -1$ et $\sqrt[2]{-1}$ (mod. 37) $\equiv \pm 6$; d'où l'on tire les vraies valeurs $\pm 6.21 \equiv \pm 15$.

Voilà à-peu-près tout ce que nous pouvions exposer ici sur la résolution de ces expressions. Il est clair que les méthodes directes deviennent souvent assez longues ; mais cet inconvénient a lieu dans presque toutes les méthodes directes de la théorie des nombres : Aussi nous n'avons pas cru devoir négliger de faire voir ce qu'on peut en attendre. Il convient aussi d'observer que les artifices particuliers qui se présentent à un homme exercé, n'entrent pas dans notre plan.

69. Revenons maintenant aux racines que nous avons appelées *primitives*. Nous avons fait voir que, si l'on prenait pour base une racine primitive quelconque, tous les nombres dont les indices sont premiers avec $p-1$, étaient aussi des racines primitives, et qu'il n'y en aurait pas d'autres, d'où nous avons conclu le nombre de ces racines (n° 53) : et comme le choix de celle que l'on prend pour base est en général arbitraire, on voit qu'ici, comme dans les logarithmes, on peut avoir plusieurs systèmes[6]. Cherchons les relations qui les lient entre eux. Soient a et b deux racines primitives, et m un autre nombre. Soit de plus Ind. $b = \beta$, quand a est pris pour base, Ind. $m \equiv \mu$ (mod. $p-1$). Soit au contraire Ind. $a = \alpha$, Ind. $m = \nu$ (mod. $p-1$) dans l'hypothèse où l'on prend b pour base ; on aura $a^\beta \equiv b$, donc $a\alpha^\beta \equiv b^\alpha \equiv a$, d'où $\alpha\beta \equiv 1$ (mod. $p-1$). On trouvera de même $\nu \equiv \alpha\mu, \mu \equiv \beta\nu$ (mod. $p-1$). Si donc on a une table d'indices construite pour la base a, on pourra facilement la changer en une autre dont la base est b. En effet, si Ind. $b \equiv \beta$ pour la base a, Ind. a sera $\equiv \frac{1}{\beta}$ (mod. $p-1$) pour la base b, et multipliant par ce nombre tous les indices de la table, on aura tous les indices pour la base b.

70. Mais quoiqu'un nombre donné puisse avoir plusieurs indices, en prenant pour base différentes racines primitives, tous ces indices auront cette propriété commune, que leur plus grand commun diviseur avec $p-1$ sera le même. En effet, A étant un nombre donné, si Ind. $A \equiv m$ pour la base a, et Ind. $A \equiv n$ pour la base b, et si leurs plus grands communs diviseurs μ et ν avec $p-1$ sont supposés inégaux ; soit $\mu > \nu$, μ ne divisera pas n ; mais si Ind. $a = \alpha$ pour la base b, on aura (art. précéd.) $n \equiv \alpha m$ (mod. $p-1$), et partant μ divisera aussi n.

On peut encore s'assurer que ce diviseur commun des indices d'un nombre donné et de $p-1$, est indépendant de la base en observant qu'il est égal à $\frac{p-1}{t}$, t étant l'exposant auquel appartient le nombre dont il s'agit. En effet, si l'indice est k pour une base quelconque, t sera le plus petit nombre (zéro excepté), qui multiplié par k, donne un produit divisible par $p-1$, ou la plus petite valeur de l'expression $\frac{0}{k}$ (mod. $p-1$) ; mais on déduit sans peine du n° 29 que cette valeur est égale au plus grand commun diviseur des nombres k et $p-1$.[7]

[6] Mais ils diffèrent en cela, que dans les logarithmes le nombre des systèmes est infini, et qu'il est ici égal au nombre des racines primitives, car les bases congrues produisent évidemment les mêmes systèmes.

[7] La dernière phrase de l'auteur ne me semble point prouver ce qu'il a avancé ; il s'y est sans doute glissé quelques

71. On démontre facilement que l'on peut toujours trouver une base telle, qu'un nombre appartenant à l'exposant t ait un indice donné à volonté. Le plus grand commun diviseur de cet indice et de $p-1$ étant $\frac{p-1}{t}$, désignons par d ce diviseur, et soit l'indice proposé $\equiv dm$; soit dn l'indice du nombre donné quand on prend pour base la racine primitive quelconque a ; on aura m et n premiers avec $\frac{p-1}{d}$ ou t. Or si e est une valeur de l'expression $\frac{dn}{dm}$ (mod. $p-1$), et en même temps premier avec $p-1$, a^e sera la racine primitive cherchée, car on aura $a^{edm} \equiv a^{dn} \equiv$ au nombre proposé (mod. p). Il nous reste à prouver que l'expression $\frac{dn}{dm}$ (mod. $p-1$) peut admettre des valeurs premières avec $p-1$; elle équivaut à $\frac{n}{m}$ (mod. $\frac{p-1}{d}$) ou $\frac{n}{m}$(mod. t), (n° 31, 2°) et toutes les valeurs en seront premières avec t ; car si une valeur e avait un diviseur commun avec t, ce diviseur devrait aussi diviser me, et partant diviser n qui est congru à me, suivant le module t, ce qui est contre l'hypothèse suivant laquelle n est premier avec t. Ainsi, quand tous les diviseurs premiers de $p-1$ divisent aussi t, toutes les valeurs de l'expression $\frac{n}{m}$ (mod. t) sont premières avec $p-1$, et leur nombre est d ; mais quand $p-1$ renferme encore d'autres facteurs premiers f, g, h, etc. qui ne divisent pas t, soit e une valeur de $\frac{n}{m}$ (mod. t), comme t, f, g, h, etc. sont premiers entre eux, on peut trouver un nombre ϵ congru à e suivant le module t, et congru, suivant f, g, h, etc., à des nombres quelconques premiers avec ceux-ci (n° 32). Ce nombre ne sera divisible par aucun facteur de $p-1$, et partant sera premier avec lui, comme il est nécessaire. On pourrait démontrer sans peine par la théorie des combinaisons, que le nombre de ces valeurs est $\frac{p-1}{t}.\frac{f-1}{f}.\frac{g-1}{g}.\frac{h-1}{h}$. etc. ; mais nous omettons cette démonstration qui ne peut nous être d'aucune utilité.

72. Quoiqu'en général on puisse prendre arbitrairement pour base une racine primitive quelconque, certains avantages particuliers peuvent faire préférer une base à toute autre. Dans la table I nous avons toujours pris 10 pour base quand il était racine primitive, et dans les autres cas nous avons choisi la base de manière que l'indice du nombre 10 fût le plus petit possible, c'est-à-dire $= \frac{p-1}{t}$, t étant l'exposant auquel 10 appartient. On en reconnaîtra l'avantage dans la sect. VI, où la même table sera employée à d'autres usages. Mais comme il peut encore rester ici quelque chose d'arbitraire, ainsi qu'on le voit par l'article précédent, nous avons toujours choisi, parmi toutes les racines primitives qui satisfont à la question, la plus petite pour base : ainsi pour $p = 73$, on a $t = 8$ et $d = 9$, ϵ a $\frac{72.2}{8.3} = 6$ valeurs qui sont $5, 14, 20, 28, 39, 40$, et nous avons pris 5 pour base.

73. La plupart des méthodes qui servent à trouver les racines primitives reposent en grande partie sur le tâtonnement. Si l'on réunit ce que nous avons dit (n° 55) avec ce que nous dirons plus bas sur la résolution de la congruence $x^n \equiv 1$, on aura à-peu-près tout ce qui peut se faire par les méthodes générales. EULER avoue (*Opuscula analyt. T. 1, p. 152.*) qu'il lui semble extrêmement difficile d'assigner ces nombres, et que leur nature doit être rangée dans les points les plus épineux de la théorie des nombres ; mais on les trouve assez facilement par la méthode suivante. Les hommes exercés préviendront facilement la longueur du calcul par beancoup d'artifices ; mais l'usage les indique mieux que les préceptes.

1°. On prendra à volonté un nombre a premier avec le module p [8] ; et souvent le calcul devient

fautes d'impression qui lui ont échappé. Au reste je crois que l'on peut y suppléer de la manière suivante :
Puisque t est le plus petit nombre qui rende kt divisible par $p-1$, ce sera aussi celui qui rendra $\frac{kt}{d}$ divisible par $\frac{p-1}{d}$, d étant le plus grand commun diviseur entre k et $p-1$. Or $\frac{k}{d}$ et $\frac{p-1}{d}$ étant premiers entre eux, la plus petite valeur de t convenable est $\frac{p-1}{d}$; donc $\frac{p-1}{d} = t$ et $d = \frac{p-1}{t}$.(*Note du traducteur.*)

[8]Nous désignerons toujours le module par p.

plus simple lorsqu'on prend a le plus petit possible, 2 par exemple ; on déterminera sa période (n° 46), c'est-à-dire les résidus minima de ses puissances, jusqu'à ce que l'on parvienne à une puissance a^t, qui ait 1 pour résidu minimum [9]. Si l'on a $t = p-1$, a sera une racine primitive.

2°. Mais si $t < p-1$, on prendra un autre nombre b, qui ne soit pas contenu dans la période de a, et l'on cherchera de la même manière sa période. En nommant u l'exposant auquel b appartient, on voit facilement que u n'est ni égal à t, ni une de ses parties aliquotes, car dans les deux cas on aurait $b^t \equiv 1$, ce qui est impossible, la période de a renfermant tous les nombres dont la puissance t est congrue à l'unité (n° 53). Or si $u = p-1$, b sera une racine primitive ; si u n'est pas $= p-1$, mais un multiple de t, nous aurons encore l'avantage de connaître un nombre qui appartienne à un exposant plus grand, et partant nous approcherons de notre but, puisque nous cherchons le nombre qui appartient à l'exposant *maximum* ; mais si u n'est ni $= p-1$, ni multiple de t, nous pouvons trouver un nombre appartenant à un exposant plus grand que t et u ; cet exposant sera le plus petit nombre divisible à la fois par t et u. En effet, soit y ce dernier nombre ; on décomposera y en deux facteurs m et n premiers entre eux, dont l'un divise t et l'autre u [10].

Soit $a^{\frac{t}{m}} \equiv A, b^{\frac{u}{n}} \equiv B \pmod{p}$, AB appartiendra à l'exposant y ; car on voit facilement que A appartient à l'exposant m, B à l'exposant n, et par conséquent AB appartiendra à l'exposant mn, puisque m et n sont premiers entre eux, comme on peut le démontrer en suivant exactement le procédé du n° 55.

3°. Si $y = p-1$, AB sera une racine primitive, sinon on prendra de même un troisième nombre qui ne se trouve pas dans la période de AB ; ce nombre sera une racine primitive, ou bien il appartiendra à un exposant $> y$, ou bien enfin par son moyen on déterminera un nombre appartenant à un exposant $> y$: donc, comme les nombres qui résultent de la répétition de cette opération, appartiennent à des exposants qui vont toujours en augmentant, et sont néanmoins diviseurs de $p-1$, il est évident qu'on en trouvera enfin un qui appartiendra au *maximum* $p-1$, ce sera la racine primitive.

74. Eclaircissons ceci par un exemple. Soit $p = 73$, pour lequel on demande une racine primitive. Essayons d'abord le nombre 2, dont la période est

1.	2.	4.	8.	16.	32.	64.	55.	37.	1	etc.
0.	1.	2.	3.	4.	5.	6.	7.	8.	9	etc.

Donc puisque $2^9 \equiv 1$, 2 n'est pas racine primitive. Essayons le nombre 3 qui ne se trouve pas dans la période de 2, sa période est

1.	3.	9.	27.	8.	24.	72.	70.	64.	46.	65.	49.	1	etc.
0.	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12	etc.

[9] Il est aisé de voir qu'il n'est pas nécessaire de connaître ces puissances, car on peut obtenir le résidu minimum d'une puissance au moyen de la puissance précédente.

[10] On voit facilement par le n° 18 comment on peut faire cette décomposition. On décomposera y en facteurs qui soient des nombres premiers ou des puissances de nombres premiers différents ; chacun d'eux divisera t ou u, ou tous les deux. On écrira sous t ou sous u ceux qui divisent t ou u. Quant à ceux qui diviseront u et t, peu importe sous lequel on les écrive. Si l'on fait $m =$ le produit de ceux qui sont écrits sous t, $n =$ le produit de ceux qui sont écrits sous u, il est évident que m divisera t, que n divisera u et que $mn = y$.

Donc 3 n'est pas non plus racine primitive ; mais le plus petit nombre divisible à la fois par les exposants 9 et 12, auxquels 2 et 3 appartiennent, est 36, qui donne $m = 9$ et $n = 4$. Donc élevant 2 à la puissance $\frac{9}{9} = 1$, 3 à la puissance $\frac{12}{4} = 3$, le produit de ces deux puissances est 54, qui appartiendra à l'exposant 36. Si enfin on calcule la période de 54, et qu'on essaye un nombre qui n'y soit pas contenu, 5 par exemple, on trouve qu'il est racine primitive.

75. Avant d'abandonner ce sujet, nous présenterons quelques propositions qui ne nous paraissent pas indignes d'attention, à cause de leur simplicité.

Le produit de tous les termes de la période d'un nombre quelconque est $\equiv 1$ *quand leur nombre ou l'exposant auquel appartient le nombre dont il s'agit est impair, et* $\equiv -1$ *quand il est pair.*

Par exemple, pour le module 13, la période de 5 est composée des termes 1, 5, 12, 8, dont le produit $480 \equiv -1$ (mod. 13), suivant le même module, la période de 3 est composée des termes 1, 3, 9, dont le produit $27 \equiv 1$ (mod. 13).

Soit t l'exposant auquel le nombre appartient ; on peut toujours trouver (n° 71) une base pour laquelle l'indice du nombre soit $\frac{p-1}{t}$.

Or l'indice du produit de tous les termes sera

$$\equiv (1 + 2 + 3 + \text{etc.} + t - 1)\frac{p-1}{t} = \frac{(t-1)(p-1)}{2} ;$$

donc il sera $\equiv 0$ (mod. $p-1$), quand t est impair ; et $\equiv \frac{p-1}{2}$ quand t est pair. Dans le premier cas, le produit est $\equiv 1$ (mod. p) ; dans le second, $\equiv -1$ (mod. p).

76. Si le nombre du théorème précédent est une racine primitive, sa période comprendra tous les nombres $1, 2, 3, 4, ..., p-1$, dont le produit sera par conséquent toujours $\equiv -1$; car $p-1$ est toujours pair, excepté dans le cas où $p = 2$, et alors on a indifféremment $+1$ ou -1. Ce théorème élégant qu'on énonce ordinairement de cette manière : *Le produit de tous les nombres plus petits qu'un nombre premier étant augmenté de l'unité, est divisible par ce nombre premier,* a été publié par Waring qui l'attribue à Wilson (*Meditationes Algeb. Ed. 3, p. 380*) ; mais aucun des deux n'a pu le démontrer, et Waring avoue que la démonstration lui en semble d'autant plus difficile qu'il n'y a point de *notation* par laquelle on puisse exprimer un nombre premier ; pour nous, nous pensons que la démonstration de cette sorte de vérités doit être puisée dans les principes plutôt que dans la notation. Lagrange en a depuis donné une démonstration (*Nouv. Mém. de l'Ac. de Berlin, 1771*), dans laquelle il s'appuie sur la considération des coefficients que l'on trouve en développant le produit

$$(x+1)(x+2)(x+3)...(x+p-1) :$$

et il fait voir qu'en supposant ce produit

$$= x^{p-1} + Ax^{p-2} + Bx^{p-3} + \text{etc.} + Mx + N,$$

les coefficients A, B, etc. M sont divisibles par p ; or

$$N = 1.2.3...p-1.$$

Maintenant si $x = 1$, le produit est divisible par p ; mais alors il sera $\equiv 1 + N \pmod{p}$, donc $1 + N$ est divisible par p.

Enfin EULER (*Opusc. analyt. T. 1, p. 329*) en a donné une démonstration qui rentre dans celle que nous venons d'exposer ; ainsi puisque de tels hommes n'ont pas cru ce sujet indigne de leurs méditations, nous espérons qu'on ne nous désapprouvera pas d'offrir encore ici une autre manière de démontrer ce théorème.

77. Nous dirons que deux nombres sont *associés*, comme l'a fait EULER, lorsque leur produit sera congru à l'unité. Cela posé, par la section précédente, tout nombre positif moindre que p, aura toujours un nombre associé moindre que p et il n'en aura qu'un ; or il est facile de prouver que parmi les nombres $1, 2, 3, ..., p-1$, il n'y a que 1 et $p-1$ qui soient eux-mêmes leurs associés, car ceux qui jouiront de cette propriété seront donnés par la congruence $x^2 \equiv 1$ qui ne peut avoir que deux racines 1 et $p-1$. Supprimant donc ces deux nombres, les autres $2, 3, 4, ..., p-2$, seront associés deux à deux ; donc leur produit sera $\equiv 1$; enfin multipliant par $p-1$, le produit de tous $1.2.3.4...p-1 \equiv p-1 \equiv -1$.

Par exemple, pour $p = 13$, les nombres $2, 3, 4, 5, ..., 11$ s'associent de la manière suivante : 2 avec 7, 3 avec 9, 4 avec 10, 5 avec 8, 6 avec 11 ; donc $2.3.4...11 \equiv 1$, et partant $1.2.3....12 \equiv 12 \equiv -1$.

78. Le théorème de WILSON peut être rendu plus général en l'énonçant comme il suit : *Le produit de tous les nombres premiers avec un nombre donné A et moindres que ce nombre, est congru suivant A, à l'unité prise positivement ou négativement.* L'unité doit être prise négativement quand A est de la forme p^m ou $2p^m$, p étant un nombre premier différent de 2, ou encore quand $A = 4$, et positivement dans tous les autres cas. Le théorème de WILSON est contenu dans le premier cas. *Exemple.* Pour $A = 15$, le produit des nombres $1, 2, 4, 7, 8, 11, 13, 14$, est $\equiv 1 \pmod{15}$. Nous supprimons, pour abréger, la démonstration. Nous observerons seulement qu'on peut y parvenir comme dans l'article précédent, excepté que la congruence $x^2 \equiv 1$ peut avoir plus de deux racines, ce qui demande certaines considérations particulières. On pourrait aussi la tirer de la considération des indices, comme dans le n° 75, si l'on y joint ce que nous dirons tout à l'heure des modules composés.

79. Revenons à l'énumération des autres propositions (n° 75).

La somme de tous les termes de la période d'un nombre quelconque est $\equiv 0$.

Ainsi dans l'exemple du n° 75

$$1 + 5 + 12 + 8 = 26 \equiv 0 \pmod{13}.$$

Soit a le nombre dont il s'agit, et t l'exposant auquel il appartient. La somme de tous les termes de la période sera

$$\equiv 1 + a + a^2 + a^3 + ... + a^{t-1} \equiv \frac{a^t - 1}{a - 1} \pmod{p} ;$$

or $a^t - 1 \equiv 0$, donc aussi $\frac{a^t-1}{a-1} \equiv 0$, si $a - 1$ n'est pas divisible par p ; il faut donc excepter ce cas, si nous voulons regarder même un seul terme comme une *période*.

80. *Le produit de toutes les racines primitives est* $\equiv 1$, excepté le cas où $p = 3$, car alors il n'y a qu'une racine primitive 2.

Si l'on prend pour base une racine primitive quelconque, les indices de toutes les racines primitives seront des nombres premiers avec $p-1$ et moindres que lui ; mais la somme de tous ces nombres, c'est-à-dire l'indice du produit de toutes les racines primitives, est $\equiv 0$ (mod. $p-1$) ; donc le produit est $\equiv 1$ (mod. p). En effet on voit facilement que si k est un nombre premier avec $p-1$, $p-1-k$ le sera aussi, et que par conséquent la somme des nombres premiers avec $p-1$ est composée de couples dont la somme est divisible par $p-1$. Il est bon d'observer que k ne peut être égal à $p-1-k$, à moins que $\frac{p-1}{2}$ ne soit premier avec $p-1$, ce qui exige que $p-1=2$ ou $p=3$, cas que nous exceptons.

81. *La somme des racines primitives est* $\equiv 0$ quand $p-1$ est divisible par un carré, ou $\equiv \pm 1$ quand $p-1$ est le produit de facteurs premiers inégaux. Le signe $+$ appartenant au cas où le nombre de ces facteurs est pair, le signe $-$ au cas où il est impair.

Ex. 1°. Pour $p = 13$, on a les racines primitives $2, 6, 7, 11$ dont la somme $26 \equiv 0$ (mod. 13).
2°. Pour $p = 11$, les racines primitives sont $2, 6, 7, 8$, dont la somme $23 \equiv +1$ (mod. 11).
3°. Pour $p = 31$, les racines primitives sont $3, 11, 12, 13, 17, 21, 22, 24$, dont la somme $123 \equiv -1$ (mod. 31).

Nous avons démontré plus haut (n° 55, 2°) que si l'on a $p-1 = a^\alpha b^\beta c^\gamma$ etc., et que A, B, C, etc. soient des nombres quelconques qui appartiennent aux exposants $a^\alpha, b^\beta, c^\gamma$, etc. respectivement, tous les produits ABC etc, seront des racines primitives ; mais on peut aussi démontrer facilement qu'une racine primitive quelconque peut s'exprimer par un produit de cette espèce et d'une seule façon [11] .

Il suit de là que ces produits peuvent être pris au lieu des racines primitives ; mais, comme dans ces produits il faut combiner toutes les valeurs de A avec toutes celles de B, etc., la somme de tous ces produits sera égale au produit de la somme des valeurs de A, multipliée par la somme des valeurs de B, etc. Désignons toutes les valeurs de A, B, C, etc. par A, A', A'', etc. B, B', B'', etc. C, C', C'',

[11] On déterminera des nombres α', β', γ', etc. tels qu'on ait $\alpha' \equiv 1$ (mod. a^α) et $\equiv 0$ (mod. $b^\beta c^\gamma$ etc.) ; $\beta' \equiv 1$ (mod. b^β) et $\equiv 0$ (mod. $a^\alpha c^\gamma$ etc.), etc. (*v.* n° 32) ; donc on aura $\alpha' + \beta' + \gamma'$+etc.$\equiv 1$ (mod. $p-1$), (n° 19). Or si l'on doit exprimer une racine primitive quelconque r par un produit de la forme ABC etc. ; on prendra $A \equiv r^{\alpha'}, B \equiv r^{\beta'}, C \equiv r^{\gamma'}$, etc. A, B, C appartiendront respectivement aux exposants $a^\alpha, b^\beta, c^\gamma$, etc., et le produit ABC etc. sera $\equiv r$ (mod. p). Or il est facile de voir que A, B, C, etc. ne peuvent se déterminer d'une autre manière (1).

(1) Cette note nous semble avoir besoin de quelques éclaircissements. Il est aisé de voir que tous les nombres, excepté α', sont divisibles par a^α ; que partant leur somme l'est aussi, ou est $\equiv 0$ (mod. a^α) ; mais comme $\alpha' \equiv 1$ (mod. a^α), il vient donc $\alpha' + \beta' + \gamma'$+ etc.$\equiv 1$ (mod. a^α), de même $\alpha' + \beta' + \gamma'$+etc.$\equiv 1$ (mod. b^β), etc. ; donc $\alpha' + \beta' + \gamma'$+etc.$\equiv 1$ (mod. $a^\alpha b^\beta c^\gamma$, etc.) $\equiv 1$ (mod. $p-1$). Or si l'on fait $A \equiv r^{\alpha'}, B \equiv b^{\beta'}, C \equiv c^{\gamma'}$, etc. A, B, C, etc. appartiendront aux exposants $a^\alpha, b^\beta, c^\gamma$, etc. respectivement. En effet $A^{a^\alpha} \equiv r^{\alpha' a^\alpha} \equiv 1$ (mod. p), $\alpha' a^\alpha$ étant $\equiv 0$ (mod. $p-1$), et il est visible que l'on ne peut supposer $A^t \equiv 1$ (mod. p), t étant $< a$, et de même pour B, C, etc., car on aurait $\alpha' t \equiv 0$ (mod. $p-1$), ce qui ne peut avoir lieu à moins que t ne soit $= a^\alpha$ ou $\equiv 0$ (mod. a^α). Or il est aisé de s'assurer encore qu'on ne peut trouver de nombres A', B', C', etc. respectivement incongrus à A, B, C, etc., et qui puissent les remplacer. En effet on aurait $A' \equiv r^{\alpha''}$, α'' étant un nombre déterminé comme α' ; mais on a aussi $A \equiv r^{\alpha'}$; or comme α' et α'' sont congrus au même nombre suivant le module $p-1$, ils sont congrus entre eux suivant ce même module ; donc $r^{\alpha'} \equiv r^{\alpha''}$ (mod. p), et partant $A \equiv A'$. (*Note du traducteur.*)

etc. La somme de toutes les racines primitives sera congrue au produit $(A+A'+\text{etc.})(B+B'+\text{etc.})$ etc. ; or je dis que si $\alpha = 1$, la somme $A + A' + A''+$etc., sera $\equiv -1 \pmod{p}$, que si $\alpha > 1$, cette somme sera $\equiv 0$, et de même pour β, γ, etc. Si ces deux assertions sont démontrées, la vérité du théorème sera manifeste. En effet, quand $p-1$ est divisible par un carré, quelqu'un des exposants α, β, γ, etc. sera > 1, et partant un des facteurs dont le produit est congru à la somme des racines primitives, sera $\equiv 0$, c'est-à-dire que le produit lui-même le sera. Quand $p-1$ ne pourra être divisé par aucun carré, tous les exposants α, β, γ, etc. seront égaux à l'unité, et la somme des racines primitives sera congrue au produit d'autant de facteurs dont chacun $\equiv -1$, qu'il y a de nombres a, b, c, etc. ; donc partant le produit sera $\equiv \pm 1$, suivant qu'ils seront en nombre pair ou impair ; or ces deux assertions se prouvent ainsi qu'il suit :

1°. Quand $\alpha = 1$, et que A est un nombre appartenant à l'exposant a, les autres nombres qui appartiennent aussi à cet exposant sont $A^2, A^3, ...A^{a-1}$; or $1 + A + A^2 + A^3 + A^4 + ... + A^{a-1}$ est la somme de la période complète, et partant $\equiv 0$ (n° 79) ; donc

$$A + A^2 + A^3 + \ldots + A^{a-1} \equiv -1.$$

2°. Quand $\alpha > 1$ et que A est un nombre appartenant à l'exposant a^α, on aura les autres nombres appartenant au même exposant, si de la suite $A^2, A^3, A^4, ...A^{a^\alpha - 1}$, on retranche A^a, A^{2a}, A^{3a}, etc. (n° 53), leur somme sera donc

$$= 1 + A + A^2 + \ldots + A^{a^\alpha - 1} - (1 + A^a + A^{2a} + \ldots + A^{a^\alpha - a}) ,$$

c'est-à-dire congrue à la différence de deux périodes, et par conséquent $\equiv 0$.

82. Tout ce que nous avons exposé jusqu'à présent, suppose que le module soit un nombre premier. Il nous reste à considérer le cas où l'on prend pour module un nombre composé ; mais comme il n'en résulte pas des propriétés aussi élégantes que dans le premier cas, et qu'il n'y a pas besoin d'artifices bien délicats pour les trouver, tout se déduisant presque de la seule application des principes précédents, il serait superflu et fastidieux d'épuiser ici tous les détails. Aussi nous exposerons en peu de mots ce que ce second cas a de commun avec le premier, et ce qui lui est propre.

83. Les propositions des n^os^ 45-48 ont déjà été démontrées généralement, mais celle du n° 49 doit être changée ainsi :

Si f désigne combien il y a de nombres premiers avec m et moindres que lui, c'est-à-dire si $f = \varphi m$ (art. 38), l'exposant t de la plus petite puissance d'un nombre donné a premier avec m, qui est congrue à l'unité suivant le module m sera $= f$, ou une partie aliquote de f.

La démonstration de la proposition du n° 49 peut servir également dans ce cas-ci, en y substituant m pour p, f pour $p-1$, et au lieu des nombres $1, 2, 3, ..., p-1$, les nombres premiers avec m et moindres que lui ; ainsi nous y renvoyons le lecteur. Mais les autres démonstrations dont nous avons parlé (n^os^ 50, 51) ; ne peuvent s'appliquer à ce cas sans beaucoup d'embarras. À l'égard des propositions suivantes (n° 52 et suivants), il y a une grande différence entre les modules qui sont les puissances d'un nombre premier et ceux qui sont divisibles par plusieurs nombres premiers. Nous considérerons donc à part les modules du premier genre.

84. Si le module $m = p^n$, p étant un nombre premier, on aura $f = p^{n-1}(p-1)$, (n° 38). Or si l'on applique à ce cas les recherches contenues (n^os^ 53, 55), *mutatis mutandis* comme dans l'article précédent, on trouvera que tout ce qui y a été démontré aurait lieu également, s'il était prouvé que la congruence $x^t - 1 \equiv 0 \pmod{p^n}$, ne peut avoir plus de t racines différentes. C'est d'une proposition plus générale (n° 43) que nous avons déduit cette vérité pour un module premier : mais cette proposition n'a lieu que pour les modules premiers, et partant ne peut s'appliquer à ce cas. Nous allons donc la démontrer par une méthode particulière, et plus bas (sect. VIII[12]) nous le prouverons encore plus facilement.

85. Nous nous proposons de démontrer ce théorème : *Si le plus grand commun diviseur des nombres t et $p^{n-1}(p-1)$ est e, la congruence $x^t \equiv 1 \pmod{p^n}$ aura e racines différentes.*

Soit $e = kp^\nu$, de sorte que k ne renferme point le facteur p, et qu'il divise par conséquent $p-1$. Alors la congruence $x^t \equiv 1$ suivant le module p, aura k racines différentes, et si on les désigne par A, B, C, etc., une racine quelconque de cette même congruence, suivant le module p^n, devra être congrue à quelqu'un des nombres A, B, C, etc., suivant le module p. Or nous démontrerons que la congruence $x^t \equiv 1 \pmod{p^n}$, a p^ν racines congrues à A, autant à B, etc. suivant le module p, d'où il résultera que le nombre de toutes les racines sera kp^ν ou e, comme nous l'avons avancé. Cela posé, nous allons démontrer que

1°. Si α est une racine congrue à A, suivant le module p, $\alpha + p^{n-\nu}, \alpha + 2p^{n-\nu}, \alpha + 3p^{n-\nu}, \ldots, \alpha + p^{\nu-1}.p^{n-\nu}$ seront aussi des racines.

2°. Aucun nombre congru avec A ne pourra être racine, s'il n'est de la forme $\alpha + hp^{n-\nu}$, h étant un nombre entier quelconque ; d'où il suit qu'on aura p^ν racines différentes, et qu'on n'en aura pas davantage ; la même chose aura lien par rapport à B, C, etc.

3°. Nous ferons voir comment on peut toujours trouver une racine congrue à A suivant le module p.

86. THÉORÈME. *Si t est comme dans l'article précédent un nombre divisible par p^ν et non par $p^{\nu+1}$, on aura $(\alpha + hp^\mu)^t - \alpha^t \equiv 0 \pmod{p^{\mu+\nu}}$, et $\equiv \alpha^{t-1} hp^\mu t \pmod{p^{\mu+\nu+1}}$.* La seconde partie du théorème n'a pas lieu quand $p = 2$ et $\mu = 1$.

On pourrait déduire la démonstration de ce théorème du développement de la puissance d'un binôme, si on faisait voir que tous les termes, après le second, sont divisibles par $p^{\mu+\nu+1}$; mais comme la considération des dénominateurs des coefficients jette dans quelque embarras, nous préférons la méthode suivante :

Supposons d'abord $\mu > 1$ et $\nu = 1$, on a généralement $x^t - y^t = (x-y)(x^{t-1} + x^{t-2}y + x^{t-3}y^2 + \ldots + y^{t-1})$; donc $(\alpha + hp^\mu)^t - \alpha^t = hp^\mu\{(\alpha + hp^\mu)^{t-1} + (\alpha + hp^\mu)^{t-2} + \text{etc.} + \alpha^{t-1}\}$; mais on a $\alpha + hp^\mu \equiv \alpha \pmod{p^2}$; donc chaque terme $(\alpha + hp^\mu)^{t-1}, (\alpha + hp^\mu)^{t-2}\alpha$, etc. sera $\equiv \alpha^{t-1} \pmod{p^2}$, et par conséquent la somme de tous $\equiv t\alpha^{t-1} \pmod{p^2}$, ou bien cette somme sera de la forme $t\alpha^{t-1} + Vp^2$, V étant un nombre quelconque. Donc $(\alpha + hp^\mu)^t - \alpha^t$ sera de la forme $\alpha^{t-1} hp^\mu t + Vhp^{\mu+2}$, c'est-à-dire qu'il sera $\equiv \alpha^{t-1} hp^\mu t \pmod{p^{\mu+2}}$ et $\equiv 0 \pmod{p^{\mu+1}}$. Ainsi, pour ce cas, le théorème est démontré.

[12] *Voir note de la transcriptrice pour la section 61.*

Or si le théorème n'était pas vrai pour les autres valeurs de ν, μ restant > 1, il y aurait nécessairement une limite jusqu'à laquelle le théorème serait vrai, et passé laquelle il serait faux. Soit φ la plus petite valeur de ν qui se refuse au théorème. On voit facilement que le théorème est vrai si t est divisible par $p^{\varphi-1}$ et non par p^{φ} ; mais que si l'on substitue tp à la place de t, il ne l'est plus. On a donc $(\alpha + hp^{\mu})^t \equiv \alpha^t + \alpha^{t-1}hp^{\mu}t \pmod{p^{\mu+\varphi}}$, ou $= \alpha^t + \alpha^{t-1}hp^{\mu}t + up^{\mu+\varphi}$, u étant un nombre entier quelconque ; mais comme le théorème est déjà démontré pour $\nu = 1$, on aura $(\alpha^t + \alpha^{t-1}hp^{\mu}t + up^{\mu+\varphi})^p \equiv \alpha^{tp} + \alpha^{tp-1}hp^{\mu+1}t + \alpha^{tp-1}up^{\mu+\varphi+1} \pmod{p^{\mu+\varphi+1}}$, et partant $(\alpha + hp^{\mu})^{tp} \equiv \alpha^{tp} + \alpha^{tp-1}hp^{\mu}tp \pmod{p^{\mu+\varphi+1}}$; c'est-à-dire que le théorème est encore vrai si on substitue tp au lieu de t ou $\varphi + 1$ au lieu de φ, contre l'hypothèse ; donc le théorème est vrai pour toutes les valeurs de ν.

87. Il reste le cas où $\mu = 1$. Par une méthode absolument semblable à celle de l'article précédent, on démontrera, sans faire usage du développement du binôme, que

$$\begin{aligned}(\alpha + hp)^{t-1} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-1)hp \pmod{p^2}\\ \alpha(\alpha + hp)^{t-2} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-2)hp \pmod{p^2}\\ \alpha^2(\alpha + hp)^{t-3} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-3)hp \pmod{p^2}, \text{ etc. ;}\end{aligned}$$

donc (puisque le nombre des termes est t) la somme sera $\equiv t\alpha^{t-1} + \frac{(t-1)t}{2}\alpha^{t-2}hp \pmod{p^2}$; mais, comme t est divisible par p, $\frac{(t-1)t}{2}$ le sera aussi, excepté le cas où $p = 2$; que nous avons exclu, et dans les autres cas, la somme sera $\equiv t\alpha^{t-1} \pmod{p^2}$, puisque $\frac{(t-1)t}{2}\alpha^{t-2}hp$ est divisible par p^2. Le reste de la démonstration est comme dans l'article précédent.

Il résulte de là généralement qu'en exceptant le cas où $p = 2$, on a $(\alpha + hp^{\mu})^t \equiv \alpha^t \pmod{p^{\mu+\nu}}$ et $(\alpha + hp^{\mu})$ *non* $\equiv \alpha^t$ pour un module qui est une puissance de p plus haute que $p^{\mu+\nu}$ pourvu toutefois que h ne soit pas divisible par p, et que p^{ν} soit la plus haute puissance de p qui divise t.

De là suivent sur-le-champ les deux premières propositions que nous nous étions proposé de démontrer (n° 85), savoir :

1°. Si $\alpha^t \equiv 1$, on aura aussi $(\alpha + hp^{n-\nu})^t \equiv 1 \pmod{p^n}$.

2°. Si un nombre α' congru à A et partant à α, suivant le module p, mais incongru à α, suivant le module, $p^{n-\nu}$, satisfaisait à la congruence $x^t \equiv 1 \pmod{p^n}$, supposons $\alpha' = \alpha + lp^{\lambda}$, de sorte que l ne soit pas divisible par p, on aura $\lambda < n - \nu$; alors $(\alpha + lp^{\lambda})^t \equiv \alpha' \pmod{p^{\lambda+\nu}}$ et non suivant p^n, qui est une puissance de p plus haute que $p^{\lambda+\nu}$; donc α' ne peut être racine de la congruence $x^t \equiv 1$.

88. Nous devions en troisième lieu trouver une racine de la congruence $x^t \equiv 1 \pmod{p^n}$, qui fut congrue à A. Il nous suffira de faire voir ici comment on peut y parvenir, si l'on connaît une racine de la congruence suivant le module p^{n-1}, puisque l'on pourra passer du module p, pour lequel A est racine, au module p^2, et de là à toutes les puissances consécutives.

Soit donc α une racine de la congruence $x^t \equiv 1 \pmod{p^{n-1}}$ et que l'on cherche une racine de la même congruence suivant le module p^n, nous la supposerons $= \alpha + hp^{n-\nu-1}$, forme qu'elle doit avoir d'après l'article précédent : nous considérerons à part le cas où $\nu = n-1$, et ν ne peut être $> n-1$. On aura donc $(\alpha + hp^{n-\nu-1})^t \equiv 1 \pmod{p^n}$; mais $(\alpha + hp^{n-\nu-1})^t = \alpha + \alpha^{t-1}htp^{n-\nu-1} \pmod{p^n}$

; si donc on détermine h de manière qu'on ait $1 \equiv \alpha^t + \alpha^{t-1} htp^{n-\nu-1}$ (mod. p^n) ; ou, comme par hypothèse $1 \equiv \alpha^t$ (mod. p^{n-1}) et que t est divisible par p^ν, de manière qu'on ait $\frac{a^t-1}{p^{n-1}} + \alpha^{t-1} h \frac{t}{p^\nu}$ divisible par p, le problème sera résolu ; or il est prouvé, dans la section précédente, que cela est toujours possible, puisque t ne peut être divisé par une puissance de p plus haute que p^ν, et que partant $\alpha^{t-1}\frac{t}{p}$ est premier avec p.

Mais si $\nu = n-1$, c'est-à-dire si t est divisible par p^{n-1} ou par une plus haute puissance de p, toute valeur A qui satisfera à la congruence $x^t \equiv 1$, suivant le module p, y satisfera aussi suivant le module p^n. Soit en effet $t = p^{n-1}\tau$, on aura $t \equiv \tau$ (mod. $p-1$) ; donc puisque $A^t \equiv 1$ (mod. p), on aura aussi $A^\tau \equiv 1$ (mod. p). Soit donc $A^\tau = 1 + hp$, on aura $A^t = (1+hp)p^{n-1} \equiv 1$ (mod. p^n), (n° 87).

89. Tout ce que nous avons démontré (n^{os} 57 et suivants) à l'aide du théorème du n° 43, a lieu pour un module qui est une puissance d'un nombre premier, et si l'on appelle *racines primitives* les nombres qui appartiennent à l'exposant $p^{n-1}(p-1)$, c'est-à-dire ceux dans la période desquels se trouvent tous les nombres non divisibles par p, il y aura également ici des racines primitives ; tout ce que nous avons dit des indices et de leur usage, ainsi que de la résolution de la congruence $x^t \equiv 1$, peut s'appliquer à ce cas : comme toutes les démonstrations n'ont aucune difficulté, il serait superflu de les répéter. Nous avons en outre fait voir comment on déduit des racines de la congruence $x^t \equiv 1$ (mod. p), celles de la congruence $x^t \equiv 1$ (mod. p^n) ; mais il faut ajouter quelque chose sur le cas où $p = 2$, que nous avions exclu dans ce qui précède.

90. *Si l'on prend pour module une puissance de 2 plus haute que la seconde, 2^n par exemple, la puissance 2^{n-2} de tout nombre impair sera 1.*

Par exemple, $3^8 = 6561 \equiv 1$ (mod. 32).

En effet tout nombre impair est de la forme $1+4h$ ou de celle-ci $-1+4h$, d'où la proposition suit immédiatement (86).

Ainsi l'exposant auquel appartient un nombre impair quelconque suivant le module 2^n, doit être un diviseur de 2^{n-2} ; ce nombre appartiendra donc à l'un des suivants $1, 2, 4, 8, ..., 2^{n-2}$; et d'ailleurs on jugera facilement auquel il appartient. Soit le nombre proposé $= 4h \pm 1$, et 2^m la plus haute puissance de 2 qui puisse diviser h (m est $= 0$ quand h est impair). Alors l'exposant auquel appartient le nombre donné sera $= 2^{n-m-2}$, si $n > m+2$; mais si $n =$ ou $< m+2$, le nombre proposé sera $\equiv \pm 1$, et partant appartiendra à l'exposant 1 ou à l'exposant 2. En effet $4h \pm 1 = \pm 1 + 2^{m+2}k$, et ce nombre élevé à la puissance 2^{n-m-2} devient congru à l'unité suivant le module p^n ; or on déduit sans peine du n° 86 que si on élevait ce nombre à une puissance de degré moindre, le résultat serait incongru à l'unité. Ainsi tout nombre de la forme $\pm 1 + 4h$, où h est impair, c'est-à-dire tout nombre de la forme $8k+3$ ou $8k+5$, appartient à l'exposant p^{n-2}.

91. Il suit de là qu'il n'y a pas dans ce cas-ci de *racines primitives*, dans le sens que nous avons donné à cette expression, c'est-à-dire qu'il n'y a pas de nombres dont la période renferme tous les nombres premiers avec le module, et plus petits que lui ; mais on voit facilement qu'il arrive ici quelque chose d'analogue. En effet toute puissance impaire d'un nombre de la forme $8k+3$ est

elle-même de la forme $8k+3$, et toute puissance paire est de la forme $8k+1$; donc aucune ne peut être de la forme $8k+5$ ou $8k+7$; donc comme la période d'un nombre de la forme $8k+3$ est composée de 2^{n-2} termes différents, dont chacun est de la forme $8k+1$ ou $8k+3$, et qu'il n'y a pas plus de 2^{n-2} de ces nombres qui soient plus petits que le module, il est évident que tout nombre de la forme $8k+1$ ou $8k+3$ est congru suivant le module 2^n, à une puissance d'un nombre quelconque de la forme $8k+3$. On peut faire voir de la même manière que la période d'un nombre de la forme $8k+5$ comprend tous les nombres de la forme $8k+1$ et $8k+5$. Si donc on prend pour base un nombre de la forme $8k+5$, on trouvera des indices réels pour tous les nombres de la forme $8k+1$ et $8k+5$ pris positivement, et pour tous les nombres de la forme $8k+3$ et $8k+7$ pris négativement : on doit encore regarder comme équivalents les indices congrus suivant 2^{n-2}. C'est ainsi qu'on doit entendre la table I, dans laquelle pour les modules 16, 32 et 64 (car il n'y a besoin d'aucune table pour le module 8), nous avons toujours pris 5 pour base. Par exemple, le nombre 19, qui doit être pris négativement, puisqu'il est de la forme $8n+3$, a pour le module 64 l'indice 7, ce qui signifie que $5^7 \equiv -19 \pmod{64}$. Si l'on prenait négativement les nombres de la forme $8n+1$ et $8n+5$, et positivement ceux de la forme $8n+3$ et $8n+7$, il faudrait leur donner des indices pour ainsi dire imaginaires ; en les introduisant dans le calcul des indices, on le réduirait à un algorithme très simple ; mais comme nous serions conduits trop loin si nous voulions traiter ce sujet en toute rigueur, nous réservons ce point pour une autre occasion, quand peut-être nous entreprendrons de traiter plus en détail la théorie des quantités imaginaires, qui nous semble jusqu'à présent n'avoir été réduite par personne à des notions claires. Les gens instruits parviendront aisément à cet algorithme ; ceux qui sont moins exercés pourront néanmoins se servir de cette table, comme ceux qui ne sont point au fait des connaissances modernes sur les logarithmes imaginaires se servent des logarithmes, pourvu qu'ils possèdent bien les principes antérieurement établis.

92. Presque tout ce qui a rapport aux résidus des puissances, suivant un module composé de plusieurs nombres premiers, peut se déduire de la théorie générale des congruences ; mais comme nous exposerons plus bas une manière de ramener les congruences dont le module est composé de plusieurs nombres premiers, à d'autres dont le module est un nombre premier, ou une puissance d'un nombre premier, nous ne nous arrêterons pas beaucoup ici sur cette matière. Nous nous contenterons d'observer que la belle propriété qui a lieu pour les autres modules, savoir : qu'il existe toujours des nombres dont la période renferme tous les nombres premiers avec le module, n'a pas lieu ici, excepté dans le seul cas où le module est double d'un nombre premier, ou d'une puissance d'un nombre premier. En effet si l'on ramène le module m à la forme $A^a B^b C^c$ etc., A, B, C, etc. étant des nombres premiers différents, qu'on fasse en outre $A^{a-1}(A-1) = \alpha, B^{b-1}(B-1) = \beta, C^{c-1}(C-1) = \gamma$, etc. et que z soit un nombre premier avec m, on aura $z^\alpha \equiv 1 \pmod{A^a}, z^\beta \equiv 1 \pmod{B^b}$, etc. ; si donc μ est le plus petit nombre divisible par α, β, γ, etc., on aura $z^\mu \equiv 1$ suivant chacun des modules A^a, B^b, etc., et partant, suivant m qui est égal à leur produit ; mais excepté le cas où m est double d'un nombre premier ou d'une puissance d'un nombre premier, on a toujours $\mu < \alpha\beta\gamma$ etc., puisque les nombres α, β, etc. ne peuvent être premiers entre eux, ayant au moins le diviseur commun 2. Ainsi la période d'aucun nombre ne peut comprendre autant de termes qu'il y a de nombres premiers avec le module, et moindres que lui, puisque leur nombre est égal au produit $\alpha\beta\gamma$ etc. Ainsi, par exemple, pour $m = 1001 = 7.11.13$, la puissance 60 d'un nombre quelconque premier avec m, est congrue à l'unité, puisque 60 est le plus petit nombre divisible à-la-fois par 6, 10 et 12. Le cas où le module est double d'un nombre premier ou d'une puissance d'un nombre premier, est tout-à-fait semblable à celui où le module est un nombre premier ou une puissance d'un nombre premier.

93. Nous avons déjà cité en plusieurs endroits les ouvrages dans lesquels les autres géomètres ont parlé du sujet que nous avons traité dans cette section-ci ; mais nous renvoyons ceux qui voudraient avoir plus de détails que le désir d'abréger ne nous a permis d'en donner, aux ouvrages suivants d'Euler, recommandables par la perspicacité qui a toujours distingué ce grand homme.

Theoremata circa residua ex divisione potestatum relicta (*Comm. nov. Petrop. T.* VII, *p.* 49).

Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia. (*Ibid. T.* XVIII, *p.* 85).

On peut y joindre les dissertations 5 et 8 des *Opuscula analytica.* T. I.

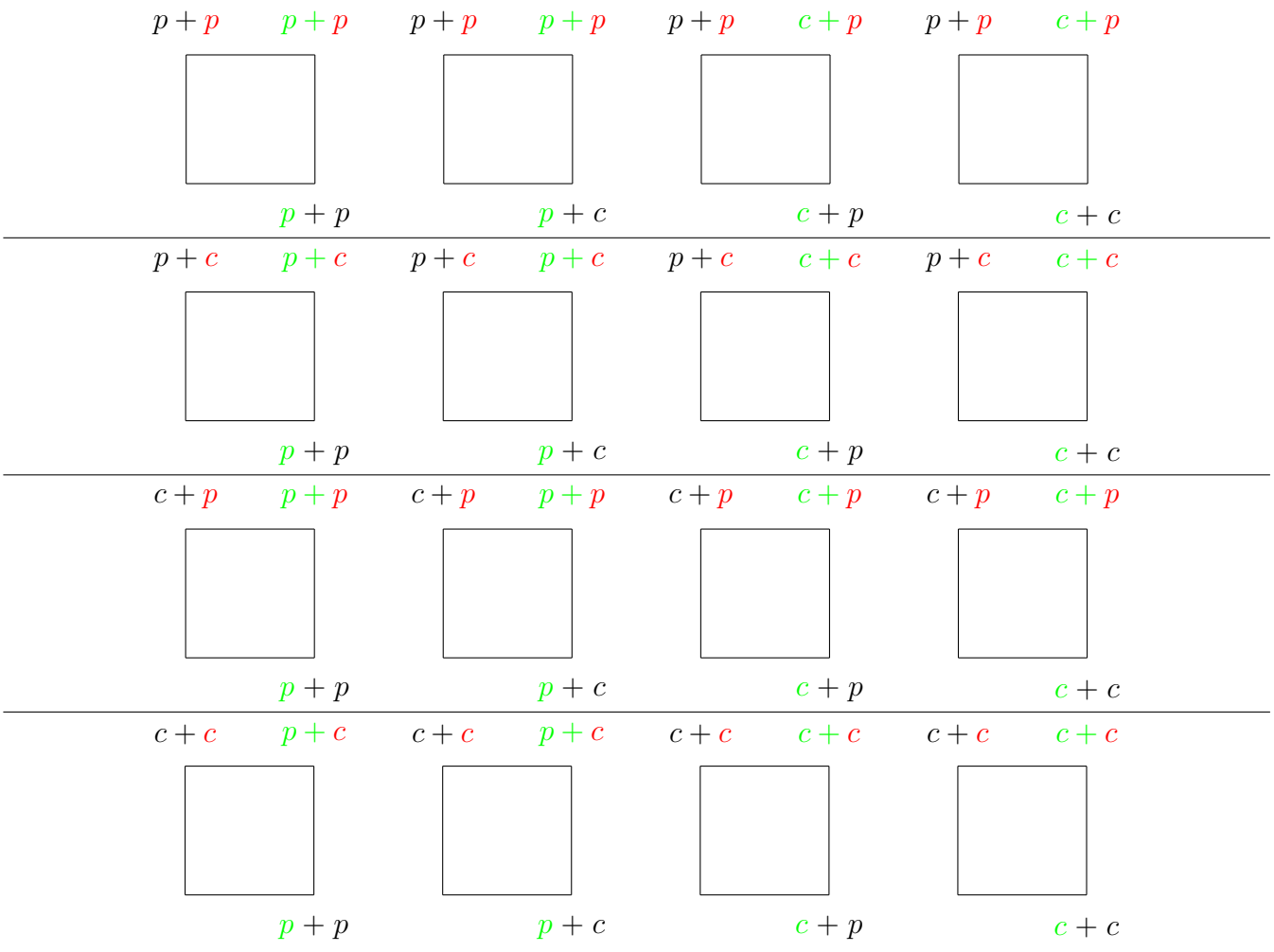
Une rencontre simple de l'inverse de la racine de 2 (Denise Vella-Chemla, mars 2024)

En 2014, puis en 2017 [1], on avait étudié une façon d'utiliser le plan cartésien pour représenter les décompositions de Goldbach, en utilisant 16 règles de passage sur un langage à 4 lettres $\{a, b, c, d\}$ qui étaient les suivantes :

$aa \to a$	$ba \to a$	$ca \to c$	$da \to c$
$ab \to b$	$bb \to b$	$cb \to d$	$db \to d$
$ac \to a$	$bc \to a$	$cc \to c$	$dc \to c$
$ad \to b$	$bd \to b$	$cd \to d$	$dd \to d$

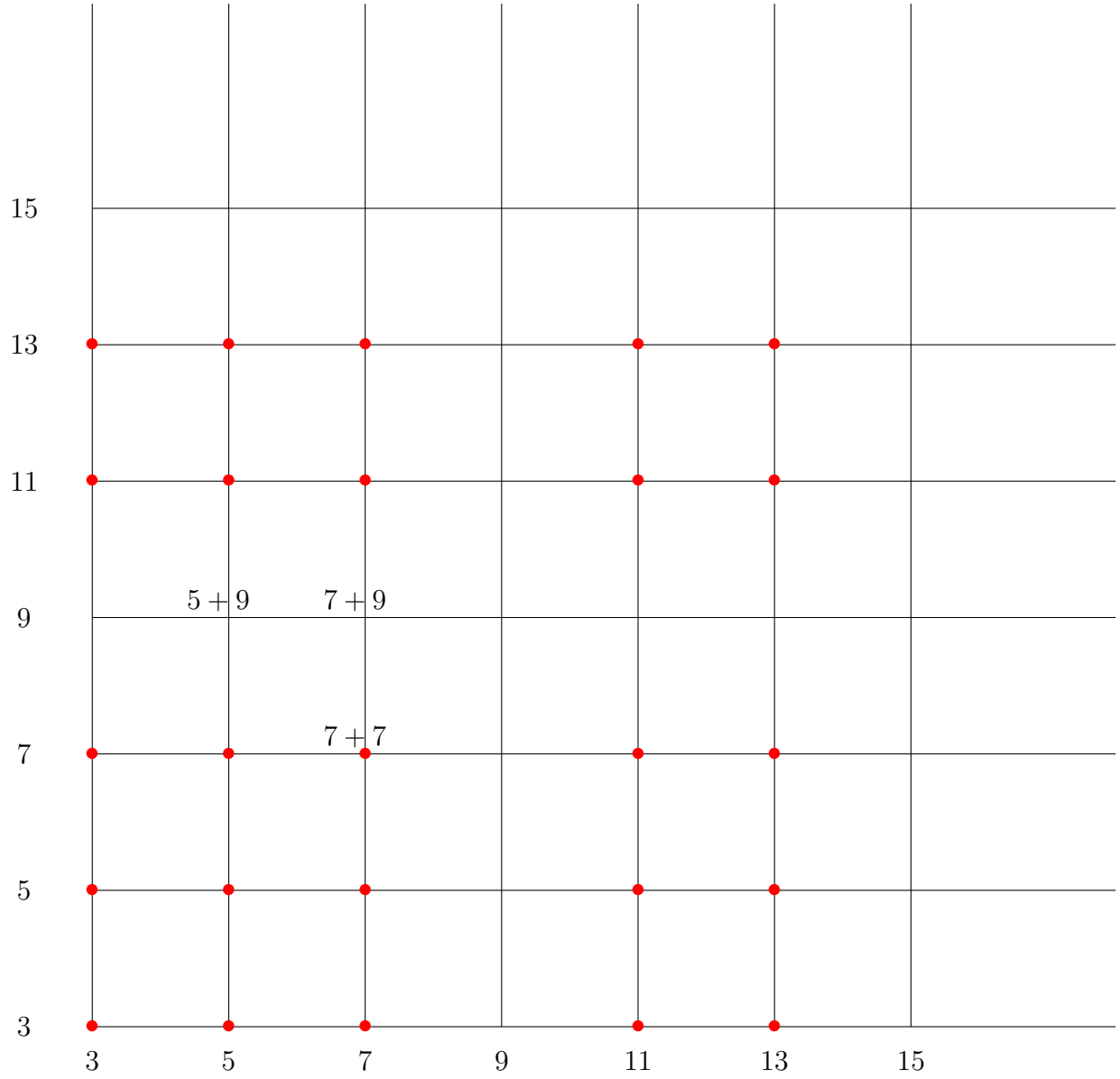
La lettre a correspondait aux décompositions de la forme premier + premier, comme $11 + 13$.
..... b ..... composé + premier, comme $9 + 11$.
..... c ..... premier + composé, comme $5 + 9$.
..... d ..... composé + composé, comme $15 + 25$.

Les règles correspondent aux petits carrés locaux suivants dans le maillage de la page suivante :



[1] Voir cette note http://denise.vella.chemla.free.fr/merveilleuxmaillage.pdf, ou celle-là http://denise.vella.chemla.free.fr/pavages3.pdf.

Ces règles explicitent de manière ampoulée le fait que toutes les décompositions d'une ligne ont même second sommant, et que toutes les décompositions d'une colonne ont même premier sommant mais "de proche en proche". Elles expriment que la décomposition 7+9 s'obtient en prenant le premier sommant de la décomposition 7+7 et le second sommant de la décomposition 5+9, qui sont ses voisines immédiates sur le graphique ci-dessous. Dans notre représentation des décompositions de Goldbach dans le plan cartésien, cela correspond au fait que les points alignés horizontalement ont même ordonnée, tandis que les points alignés verticalement ont même abscisse.



En terme de coordonnées, on peut dire localement que la décomposition en haut à droite d'un carré $x_2 + y_1$ s'obtient à partir de la décomposition $x_1 + y_1$ immédiatement à sa gauche et de la décomposition $x_2 + y_2$ immédiatement en-dessous d'elle. Cela résume d'un coup d'un seul les 16

règles faisant intervenir les lettres a, b, c, d vues plus haut.

On note que la décomposition $3 + 7$ n'est pas positionnée sur le même point du graphique que la décomposition 7+3, de même que le point de coordonnées cartésiennes $\begin{pmatrix} x \\ y \end{pmatrix}$ n'est pas le même que le point $\begin{pmatrix} y \\ x \end{pmatrix}$. On a positionné des points rouges aux intersections correspondant à des décompositions de Goldbach, dont les deux coordonnées sont des nombres premiers.

On peut représenter les 16 règles locales au moyen d'une matrice de transition : on a en quelque sorte une chance sur deux d'avoir un a et une chance sur deux d'avoir un b à partir d'un a, et de même à partir d'un b. On a également une chance sur deux d'obtenir un c et une chance sur deux d'obtenir un d à partir d'un c et il en est de même pour d. De par notre convention, il n'y a aucune chance d'avoir un a ou un b à partir d'un c ou d'un d, d'où les zéros dans la matrice.

La matrice de passage du graphe de transition est ainsi :

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

Cette matrice est égale à son carré, elle est idempotente.

Ses 4 valeurs propres sont 1, 0, 1 et 0 et ses 4 vecteurs propres sont : $\left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}, 0, 0\right)$; $\left(\frac{-\sqrt{2}}{2}, \frac{\sqrt{2}}{2}, 0, 0\right)$; $\left(0, 0, \frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right)$; $\left(0, 0, \frac{-\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right)$.

La projection sur la droite $x = y$ (ou rotation d'un angle $\frac{\pi}{4}$ ou $-\frac{\pi}{4}$ des vecteurs de base, dont les cosinus et sinus sont tous les deux égaux à $\frac{\sqrt{2}}{2} = \frac{1}{\sqrt{2}}$), correspond au fait que la convention qu'on a choisie positionne les décompositions dont les deux sommants sont égaux (et qui se trouvent être, entre autres, les décompositions de Goldbach, dites triviales, d'un nombre pair double d'un nombre premier en somme de deux nombres premiers identiques égaux à sa moitié, comme $26 = 13 + 13$), sur la diagonale du premier quadrant[2] .

[2]Au sujet de $\frac{\pi}{4}$ et du fait que cette fraction soit égale à la somme infinie $1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} + \text{etc.}$, on peut consulter cette vidéo très pédagogique https://www.youtube-nocookie.com/embed/$0_e JlNVatsU$.

Tester par programme les théorèmes de Mertens (Denise Vella-Chemla, mars 2024)

Étonnée d'avoir découvert hier par programme la presque-égalité ci-après :

$$\sum_{k=1}^{k=n} \frac{1}{\sqrt{k}} \simeq 2\sqrt{n} + \gamma'$$

avec $\gamma' < 2$, jusqu'à 10^8, dont on se demande si elle serait démontrable, ou si elle est seulement un mirage provoqué par des erreurs de programmation ou d'arrondis, on souhaite tester, toujours par programme, les théorèmes de Mertens.

L'article de Wikipedia https://fr.wikipedia.org/wiki/Théorème_de_Mertens attribue trois théorèmes à Mertens. Dans la suite, la lettre p désigne toujours un nombre premier.

Théorème 1 : Pour $n \geq 1$,

$$\left| \sum_{p \leq n} \frac{\ln p}{p} - \ln n \right| \; < \; 2.$$

Théorème 2 : Pour $n \geq 2$, avec M désignant la constante de Meissel-Mertens (approximativement égale à 0.261497...),

$$\left| \sum_{p \leq n} \frac{1}{p} - \ln \ln n - M \right| < \frac{4}{\ln(n+1)} + \frac{2}{n \ln n}.$$

Théorème 3 : Pour $n \geq 2$, avec e la base du logarithme népérien et γ la constante d'Euler-Mascheroni,

$$\prod_{p \leq n} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\ln n} \left(1 + O\left(\frac{1}{\ln n}\right)\right)$$

L'article de Mertens est visionnable ici : lien. Cet article étant écrit en allemand, on a encadré les éléments qui correspondent aux 3 théorèmes (il y a des différences pour le troisième théorème).

Voici le programme et ses résultats pour le théorème 2, pour des puissances successives de 10.

```
import math
from math import log, cos, pi, sqrt, e
def premier(atester):
        if atester in [0, 1]: return False
        if atester in [2, 3, 5, 7]: return True
        k = 2
        while True:
                if k * k > atester: return True
                else:
                        if atester % k == 0: return False
                        else: k = k + 1
```

```
somme = 1
nmax = 101
for n in range(2,nmax):
        if premier(n):
                somme = somme+1/n
        if n == nmax-1:
                print('= ', n)
                print('S=somme des inverses des premiers jusqu a n = ',somme)
                print('S-ln(ln(n)-M = ',somme-log(log(n))-0.261497)
                print('4/ln(n+1)+2/(n ln(n)) = ', (4/log(n+1))+(2/(n * log(n))))
```

Les résultats du programme du théorème 2 sont :

```
n = 100
S=somme des inverses des premiers jusqu a n = 2.802817201048871
S-ln(ln(n))-M = 1.0141405752409698
4/ln(n+1)+2/(n ln(n)) = 0.8710592061611592

n = 1000
S=somme des inverses des premiers jusqu a n = 3.1980801271750883
S-ln(ln(n)-M = 1.003938393259023
4/ln(n+1)+2/(n ln(n)) = 0.5792650654452169

n = 10000
S=somme des inverses des premiers jusqu a n = 3.483059947233565
S-ln(ln(n)-M = 1.0012361408657187
4/ln(n+1)+2/(n ln(n)) = 0.43431148162186056

n = 100000
S=somme des inverses des premiers jusqu a n = 3.7052721790472813
S-ln(ln(n)-M = 1.0003048213652255
4/ln(n+1)+2/(n ln(n)) = 0.34743702092358486

n = 1000000
S=somme des inverses des premiers jusqu a n = 3.887328099567694
S-ln(ln(n)-M = 1.0000391850916834
4/ln(n+1)+2/(n ln(n)) = 0.289529778410152
```

Sans fournir le programme, voici les résultats illustrant le théorème 1 de Mertens :

```
n = 100
S=somme des inverses des premiers jusqu a n = 4.369470874998981
S-ln(n) = -0.23569931098911123

n = 1000
S=somme des inverses des premiers jusqu a n = 6.609510475393042
S-ln(n) = -0.2982448035890952

n = 10000
S=somme des inverses des premiers jusqu a n = 8.890863604287127
S-ln(n) = -0.3194767676890571
```

n = 100000
S=somme des inverses des premiers jusqu a n = 11.184294953916854
S-ln(n) = -0.32863051105337426

n = 1000000
S=somme des inverses des premiers jusqu a n = 13.483585396239128
S-ln(n) = -0.3319251617251453

n = 10000000
S=somme des inverses des premiers jusqu a n = 15.785700405801178
S-ln(n) = -0.3323952451571426

Et enfin les résultats, concernant le théorème 3 de Mertens.

n = 100
P=prod des un moins inverses des premiers jusqu a n = 0.12031729047493521
$e^{\gamma}/\ln n =$ 0.3867549615016125
Diff = -0.26643767102667726

n = 1000
P=prod des un moins inverses des premiers jusqu a n = 0.08096526350684251
$e^{\gamma}/\ln n =$ 0.257836641001075
Diff = -0.17687137749423248

n = 10000
P=prod des un moins inverses des premiers jusqu a n = 0.060884692455838364
$e^{\gamma}/\ln n =$ 0.19337748075080624
Diff = -0.13249278829496788

n = 100000
P=prod des un moins inverses des premiers jusqu a n = 0.048752917851015085
$e^{\gamma}/\ln n =$ 0.154701984600645
Diff = -0.10594906674962991

n = 1000000
P=prod des un moins inverses des premiers jusqu a n = 0.040638210171648585
$e^{\gamma}/\ln n =$ 0.1289183205005375
Diff = -0.08828011032888891

n = 10000000
P=prod des un moins inverses des premiers jusqu a n = 0.03483377452961803
$e^{\gamma}/\ln n =$ 0.11050141757188929
Diff = -0.07566764304227126

n = 100000000
P=prod des un moins inverses des premiers jusqu a n = 0.030479721610591266
$e^{\gamma}/\ln n =$ 0.09668874037540312
Diff = -0.06620901876481186

Cela illustre au moins les minuscules nombres dont il est question, pour 10^8 et en-dessous, du moins.

Nombres premiers et tortue Logo (Denise Vella-Chemla, mars 2024)

Avec toute ma reconnaissance et mon admiration, pour Cynthia Solomon, Seymour Papert, et Wally Feurzeig, qui ont inventé le langage Logo.

Le langage Logo

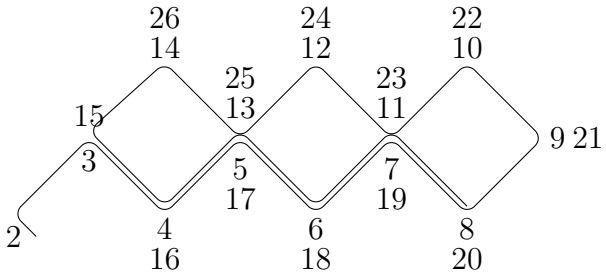
Après avoir relu un article au sujet de la courbe du dragon, on écrit le petit programme suivant pour la tortue Logo (module turtle en python), tout simple, qu'on peut résumer ainsi : "sur un nombre premier, tourne à droite ; sur un nombre composé, tourne à gauche ; dans les deux cas, avance".

```
import turtle
from turtle import *

def premier(atester):
     if atester in [0, 1]:  return False
     if atester in [2, 3, 5, 7]:  return True
     k = 2
     while True:
          if k * k > atester:  return True
          else:
               if atester % k == 0:  return False
               else:  k = k + 1

setup()
speed(0)
setheading(90)
up()
turtle.setposition(0,0)
left(45)
down()
for n in range(2,20):
     if premier(n):
          right(90)
     else:
          left(90)
     forward(30)
down()exitonclick()
```

On lance le programme et l'exécution a ce résultat pour n allant de 2 à 100.

D'abord, on est très étonnée de voir la tortue se confiner ainsi dans une ligne de carrés[1]. Le résultat de l'exécution de ce programme jusqu'à 20 est :

Sur le graphique ci-dessous, notons les nombres déclenchant les mouvements de la tortue (jusqu'à 26) dans les angles pour s'imprégner de son cheminement.



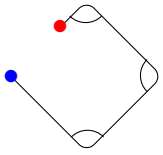
Explication du confinement à la bande délimitée par les droites (H) et (B)

La tortue reste confinée dans une bande délimitée supérieurement par une droite qu'on appellera (H), inférieurement par une droite qu'on appellera (B) et il y a au milieu de la bande une droite médiane qu'on appellera (M). On va expliciter ci-après les mouvements de la tortue par des petits triplets de trois mouvements consécutifs, correspondant à 3 nombres successifs dont le premier est pair.

Pour expliciter les différentes sortes de trois mouvement successifs que peut faire la tortue, lorsqu'elle "gère" trois nombres successifs dont le premier est pair (> 2), on distinguera les quatre positions initiales possibles de la tortue sur le carré sur lequel elle est couramment positionnée ; on notera ces 4 positions par les lettres g, h, d, b pour gauche, haut, droite, bas.

On se convainc que les 6 mouvements possibles de la tortue sont les suivants ; on colorie la position de départ de la tortue en bleu et sa position d'arrivée en rouge :

1) la tortue va "manger" un pair (tous les pairs rencontrés étant > 2 ils sont composés), un nombre impair composé, un pair (composé, on ne l'écrira plus). Elle était initialement positionnée sur le sommet g du carré courant.

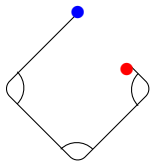


[1]Pour avoir longtemps enseigné le langage Scratch à des élèves d'école élémentaire, nombre d'entre eux pensent qu'un carré sans côté horizontal est un losange (ce qu'il est), mais n'est pas un carré. Cette "erreur" est due au fait que la plupart des enseignants, et j'en suis, dessinent un carré avec un côté horizontal, car il est naturellement plus aisé de le dessiner ainsi.

"Globalement" (i.e. par les 3 mouvements ci-dessus), les coordonnées de la tortue varient ainsi (si on considère qu'on est dans un plan cartésien) :

$$\begin{pmatrix} x \\ y \end{pmatrix} \longrightarrow \begin{pmatrix} x+1 \\ y+1 \end{pmatrix}.$$

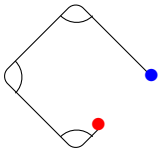
2) la tortue va "manger" un pair, un nombre impair composé, un pair. Elle était initialement positionnée sur le sommet h du carré courant.



Changement de coordonnées :

$$\begin{pmatrix} x \\ y \end{pmatrix} \longrightarrow \begin{pmatrix} x+1 \\ y-1 \end{pmatrix}.$$

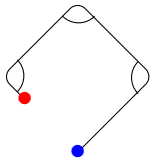
3) la tortue va "manger" un pair, un nombre impair composé, un pair. Elle était initialement positionnée sur le sommet d du carré courant.



Changement de coordonnées :

$$\begin{pmatrix} x \\ y \end{pmatrix} \longrightarrow \begin{pmatrix} x-1 \\ y-1 \end{pmatrix}.$$

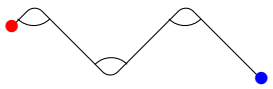
4) la tortue va "manger" un pair, un nombre impair composé, un pair. Elle était initialement positionnée sur le sommet b du carré courant.



Changement de coordonnées :

$$\begin{pmatrix} x \\ y \end{pmatrix} \longrightarrow \begin{pmatrix} x-1 \\ y+1 \end{pmatrix}.$$

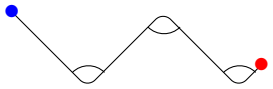
5) la tortue va "manger" un pair, un nombre premier, un pair. Elle était initialement positionnée sur le sommet d du carré courant.



Changement de coordonnées :

$$\begin{pmatrix} x \\ y \end{pmatrix} \longrightarrow \begin{pmatrix} x-3 \\ y+1 \end{pmatrix}.$$

6) la tortue va "manger" un pair, un nombre premier, un pair. Elle était initialement positionnée sur le sommet g du carré courant.



Changement de coordonnées :

$$\begin{pmatrix} x \\ y \end{pmatrix} \longrightarrow \begin{pmatrix} x+3 \\ y-1 \end{pmatrix}.$$

Remarques :

- un nombre impair de nombres traversés par la tortue la fait passer soit d'une des droites (H) ou (B) à la droite (M), ou bien lui fait faire le contraire, c'est-à-dire passer de la droite (M) à l'une des droites (H) ou (B). Avant de "manger" un nombre pair, la tortue est forcément sur la droite (M), ce qui ne lui permet de se trouver qu'à deux sommets possibles d'un carré : les sommets g ou d. C'est ce qui explique les deux seuls cas 5) et 6) correspondant à la traversée d'un nombre premier, à opposer aux cas possibles correspondant à la traversée d'un nombre impair composé.

- Les cas 1) et 3) (resp. 2) et 4), ou bien 5) et 6)) sont miroirs l'un de l'autre.

Quelle mesure choisir ?

Ce qui est vraiment rigolo à voir, c'est que de temps en temps, la tortue semble s'évader pour construire quelques carrés supplémentaires, une sorte d'extension de la suite courante, et ceci vraiment de façon erratique, parfois vers la droite et parfois vers la gauche. Elle semble simuler le comportement d'une machine de Turing, avec son ruban infini.

On compte les carrés : jusqu'à 100, la tortue en crée 8, jusqu'à 1000, elle en crée 27, jusqu'à 10000, elle en crée 65 et jusqu'à 100000, elle en crée 186 (voir le gif animé gif).

On aurait pu considérer que les pairs étant toujours composés sauf 2, on ne devrait pas leur associer de mouvement. La tortue ne bougerait que pour les nombres impairs, dans un sens pour les premiers et dans le sens opposé pour les composés et la mesure ne ferait que les compter mais le passage à la séquence de petits carrés, en effectuant le passage à deux dimensions, peut peut-être être porteur d'une information supplémentaire.

On note dans un tableau, le nombre n jusqu'auquel la mesure a été faite, l'extension maximum à gauche xmin, l'extension maximum à droite xmax, et le nombre de carrés.

n	xmin	xmax	mesure μ
10	-1	6	3.5
100	-10	6	8
1000	-42	12	27
10000	-108	12	60
100000	-664	12	338
1000000	-1116	12	564
10000000	-1116	1102	1109
100000000	-3652	4922	4287
1000000000	-3652	17210	10431

Ci-dessous le programme modifié pour faire le comptage des carrés, notre mesure naturelle :

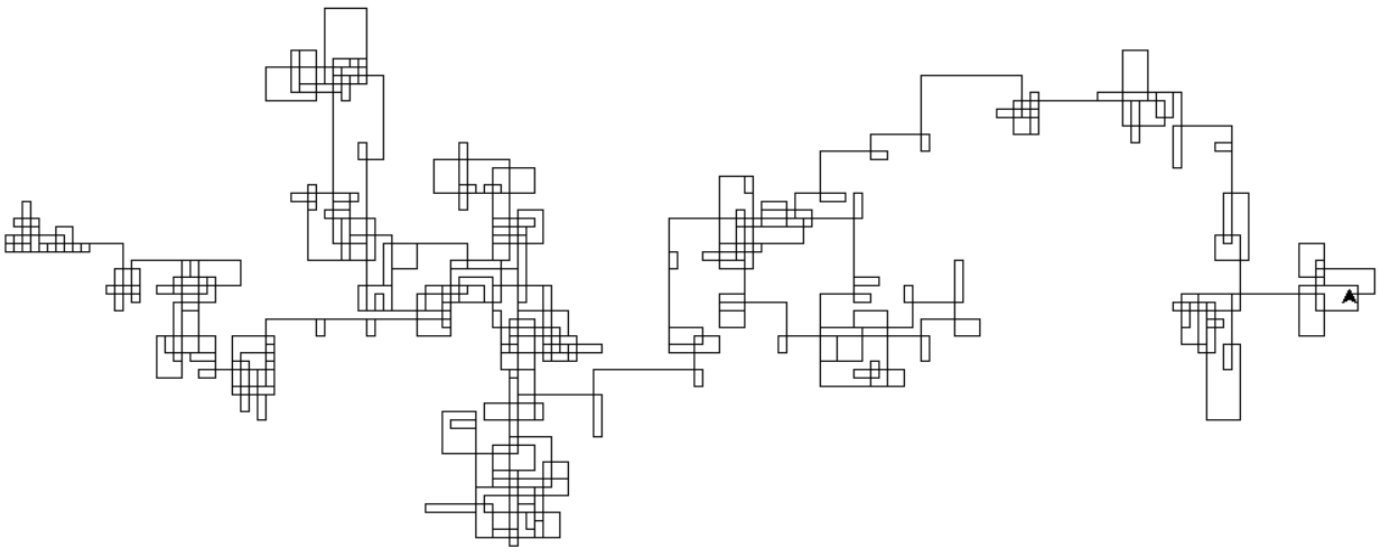
```
...
plt.axis('equal')
x = 0 ; y = 0 ; direction = 1j-1
xmin = 0 ; xmax = 0
for n in range(2,1000001):
     ancienx = x ; ancieny = y
     if direction == 1j+1:
          x = x+1
          y = y+1
     else:
          if direction == 1j-1:
               x = x-1
               y = y+1
          else:
               if direction == -1j-1:
                    x = x-1
                    y = y-1
               else:
                    if direction == -1j+1:
                         x = x+1
                         y = y-1
     if x < xmin:
          xmin = x
     if x > xmax:
          xmax = x
     if premier(n):
          direction = direction*(-1j)
     else:
          direction = direction *(1j)
     plt.plot([ancienx, x], [ancieny, y])
     print('xmin = ',xmin, ' xmax = ', xmax)
plt.show()
```

Ajout d'un degré de liberté

Celui à qui je montre cette merveilleuse tortue apprivoisée et l'expérience inoubliable que provoque son observation[2], gêné par ce confinement à un seul degré de liberté (qui est plus contraignant que les règles du pays Flatland !) souhaite que le programme libère un peu la tortue selon la règle "sur un nombre premier, tourne à droite ; quel que soit le nombre analysé, avance" (le début du programme est inchangé) :

```
...
setup()
speed(0)
setheading(90)
up()
turtle.setposition(-300,300)
left(45)
down()
for n in range(2,5001):
     if premier(n):
          right(90)
     forward(3)
exitonclick()
```

On obtient, pour les nombres jusqu'à 5000 la merveilleuse production artistique ci-dessous !



[2]Et cette même magie continue d'opérer, 50 ans après l'invention de Logo, sur les élèves qui découvrent le chaton Scratch, et le plaisir de le voir exécuter les instructions que notre cerveau a inventées, ça reste grisant.

Suivre van der Pol pour approximer la fonction ζ de Riemann (Denise Vella-Chemla, mars 2024)

On continue de programmer en utilisant des idées impulsées par la lecture d'un article de van der Pol (cf. lien vers l'article). Dans l'impossibilité d'approximer des intégrales complexes pour l'instant, on intègre et les cosinus et les sinus pour parvenir à nos fins. On voudrait illustrer par ce programme une phrase de Riemann qui interpelle et qui est :

> "*Mais, si l'on changeait cet ordre des termes de la série, on pourrait obtenir pour résultat n'importe quelle valeur réelle.*"

Riemann parle dans cette phrase de l'importance de l'ordre des zéros de la fonction ζ, à prendre par valeurs réelles croissantes, dans les formules qu'il fournit. Sans bien sûr aller jusque là, on voudrait illustrer ci-dessous l'importance de la précision des arguments passés à une fonction, lorsqu'on en cherche des approximations, qui font varier l'exécution d'un programme du tout au tout.

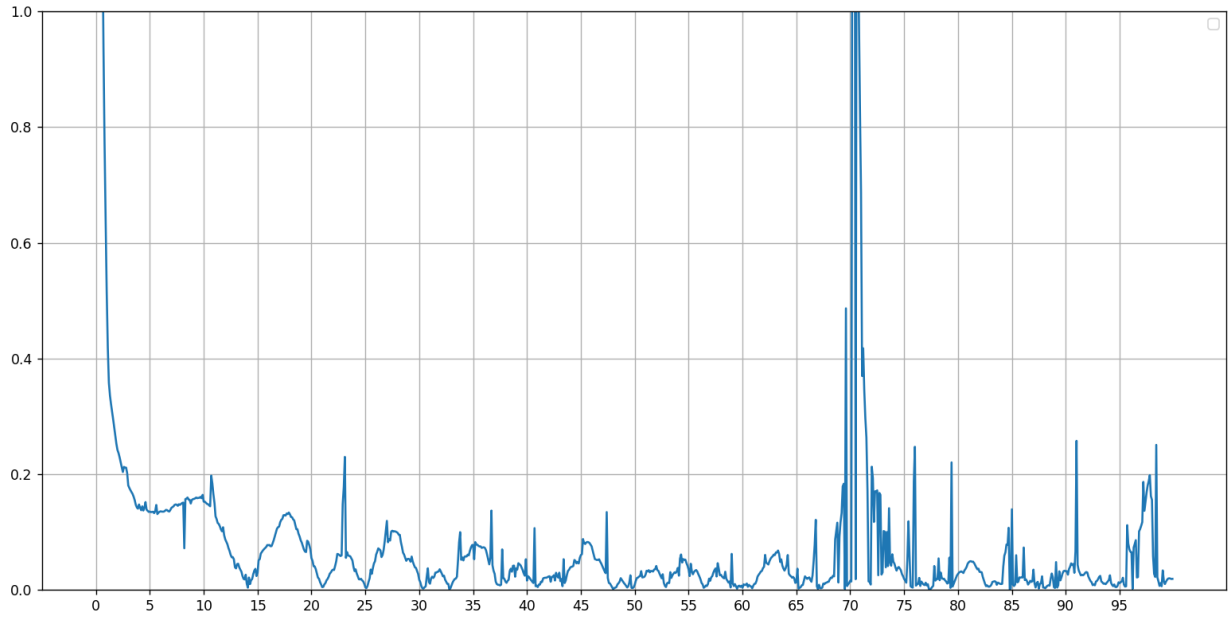
Voyons le programme ci-dessous, on a noté en vert un argument[1] que l'on va faire varier, et on va montrer l'effet de cette variation sur le résultat de l'exécution du programme.

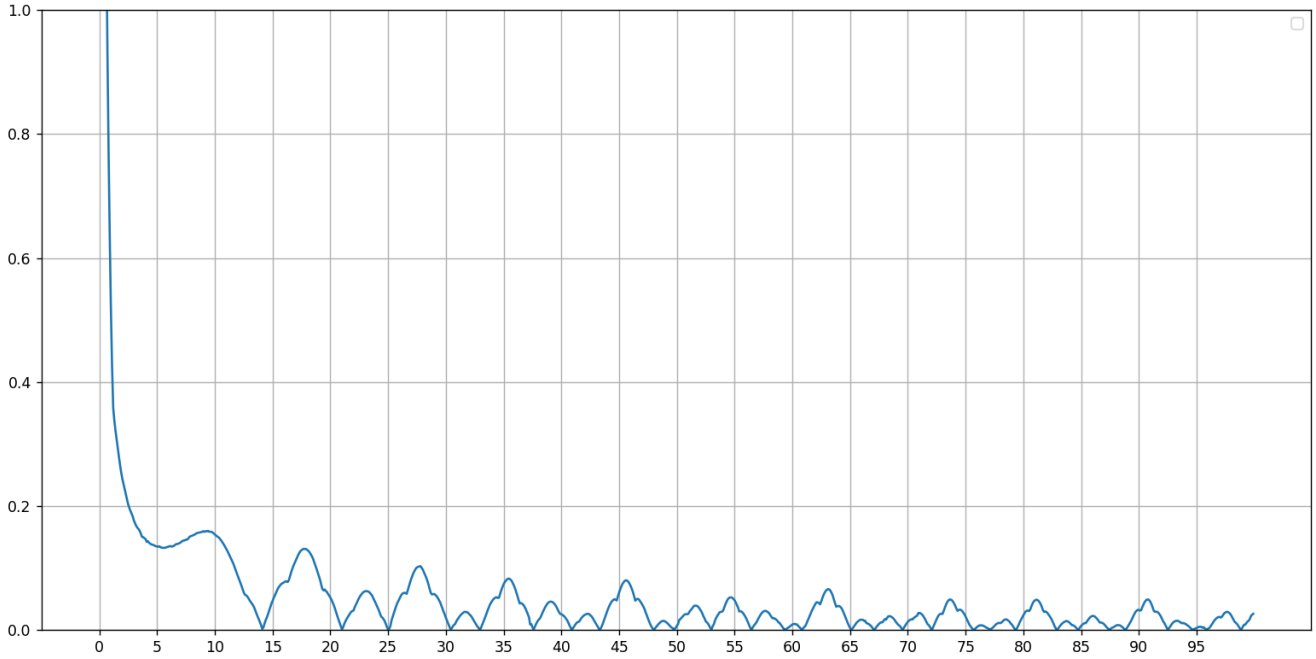
```
from scipy.integrate import quad
import matplotlib.pyplot as plt
import numpy as np
from numpy import sqrt, log, cos, sin, exp, floor, modf, pi

zeros = [ 14.134725142,20,21.022039639,25.010857580,30,30.424876126,32.935061588,
          37.586178159,40,40.918719012,43.327073281,48.005150881,49.773832478,50,
          52.970321478,56.446247697,59.347044003,60,60.831778525,65.112544048,
          67.079810529,69.546401711,70,72.067157674,75.704690699,77.144840069,
          79.337375020,80,82.910380854,84.735492981,87.425274613,88.809111208,90,
          92.491899271,94.651344041,95.870634228,98.831194218,100,101.317851006,
          103.725538040]

def integrale1(fct, a, b, nbpts):    integration par methode des trapezes
     x = np.linspace(a,b,num=nbpts+1,endpoint=True)
     h = (b-a)/nbpts
     y = fct(x)
     return np.sum(y[:nbpts]+y[1:])  * h/2

def integrale2(fct, a, b, nbpts):    integration par methode Simpson 1/3
     assert(nbpts % 2 == 0)
     x = np.linspace(a,b,num=nbpts+1,endpoint=True)
     h = (b-a)/nbpts
     y = fct(x)
     return (y[0]+4*np.sum(y[1:nbpts:2])+2*np.sum(y[2:nbpts-1:2])+y[1:])  * h/3
```

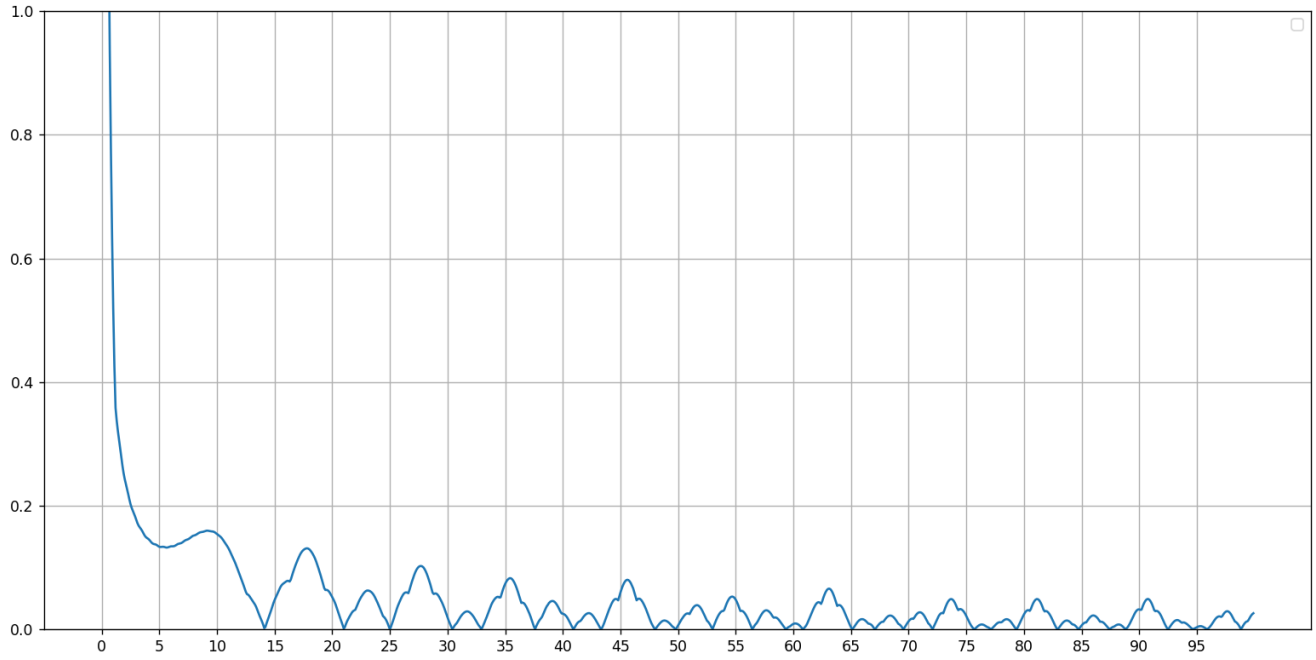
[1] "Argument" est le mot utilisé par les informaticiens pour parler d'une variable passée à une fonction, il ne s'agit pas ici de l'argument d'un nombre complexe.

```
def z(t):
      a = quad(lambda x :  (exp(x) % 1)*cos(x*t)/exp(x/2),-10,10,limit=200)[0]
      b = quad(lambda x :  (exp(x) % 1)*sin(x*t)/exp(x/2),-10,10,limit=200)[0]
      return(sqrt(a*a+b*b))
      return(max(abs(a),abs(b)))

def zp(t):
      a = integrale1(lambda x :  (modf(exp(x))[0])*cos(x*t)/exp(x/2),-10,10,100)
      b = integrale1(lambda x :  (modf(exp(x))[0])*sin(x*t)/exp(x/2),-10,10,100)
      return(sqrt(a*a+b*b))
      return(max(abs(a),abs(b)))

b,c = 100,1000
plt.ylim(0,1)
plt.grid(True)
plt.xticks(range(0,100,5))
plt.legend()
t = [k*b/c for k in range(c)]
plt.plot(t, [abs(zp(tt)) for tt in t])
plt.show()
for z in zeros:
      print('')
      print(z,' --> ',zp(z))
```

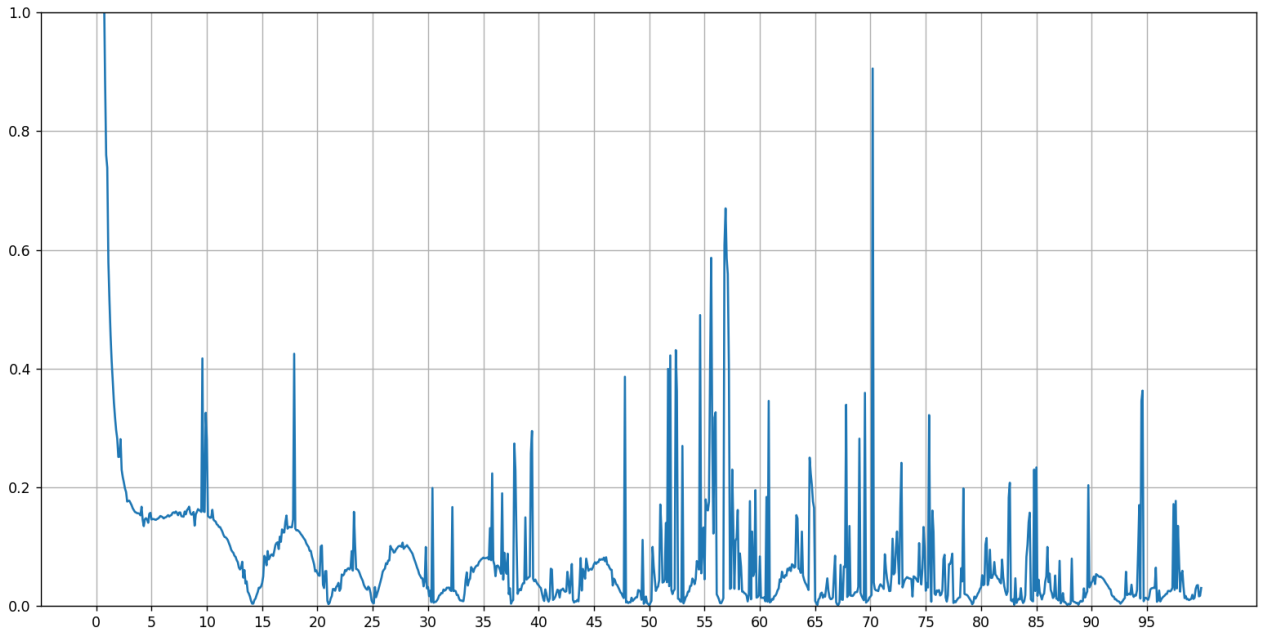
Ci-dessous, les résultats de l'exécution du programme, d'abord avec l'argument 100, puis en remplaçant 100 par 1000, puis par 10000. Le temps d'exécution de la fonction python *quad*, qui calcule une intégrale, quand on souhaite augmenter la précision du calcul, est prohibitif. De plus, on verra en annexe 2 tous les avertissements de l'interpréteur de python qui ne sont pas très encourageants. Enfin, il n'y a pas de différence notable (jusqu'à 100) entre l'argument 1000 et l'argument 10000.



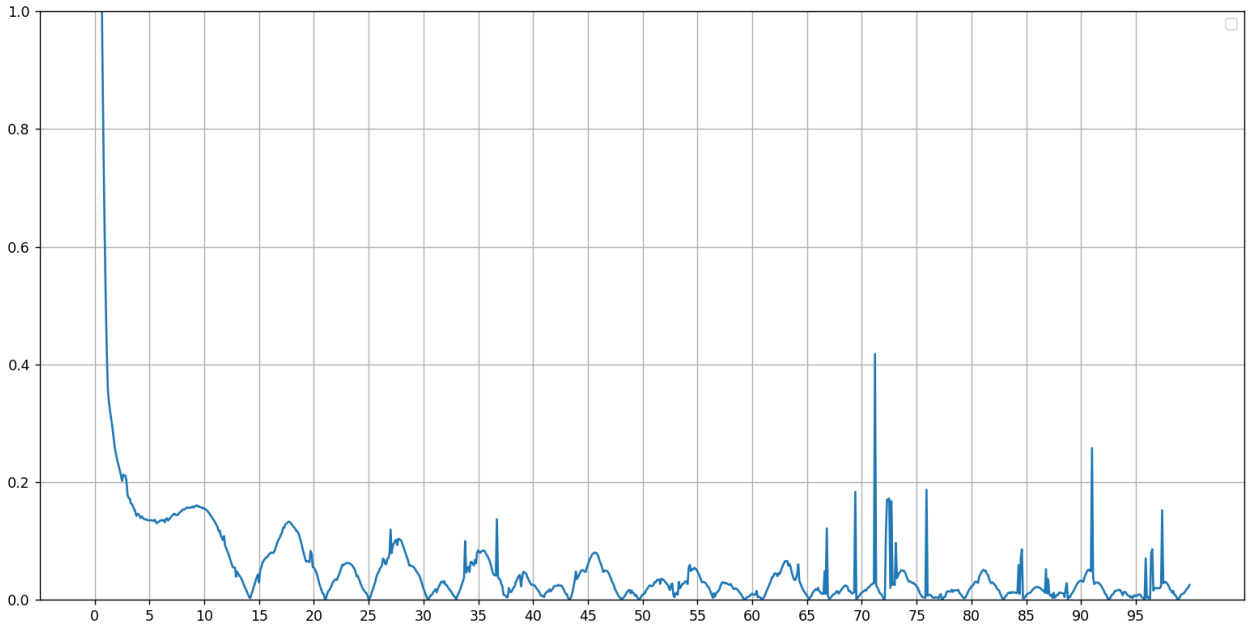




Si l'on remplace les bornes $-10, 10$ par les bornes $-100, 100$, on obtient une fonction pleine de presque-pôles, ainsi :



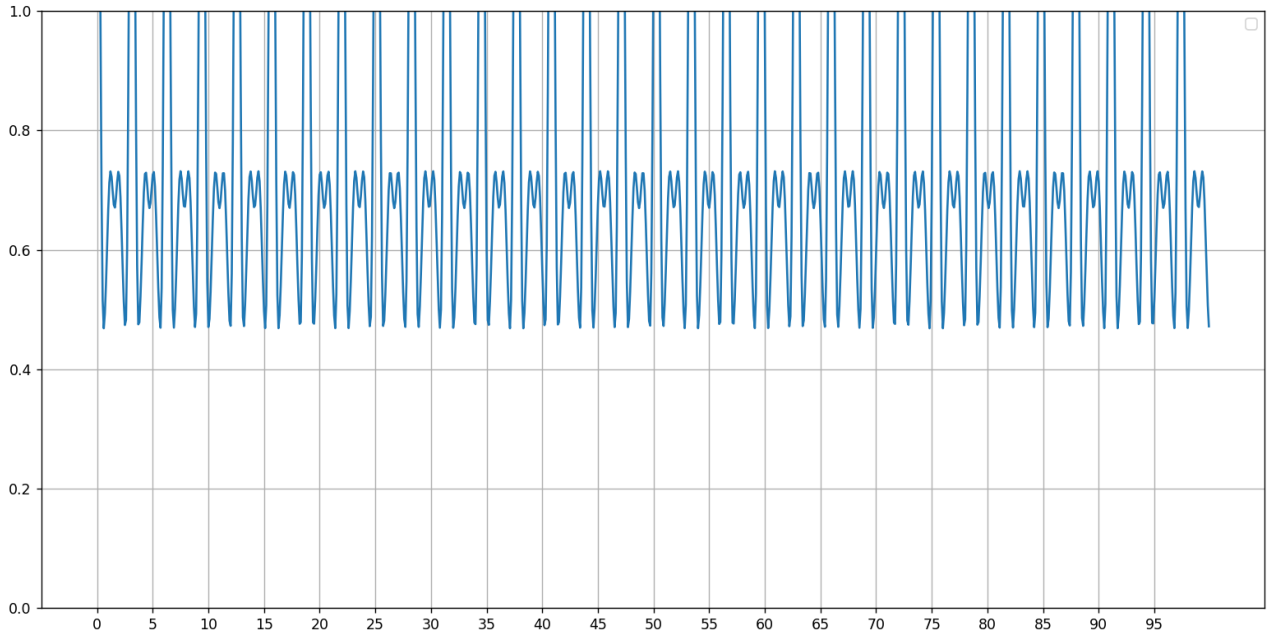
En faisant à nouveau varier un argument, les presque-pôles vont moins haut.

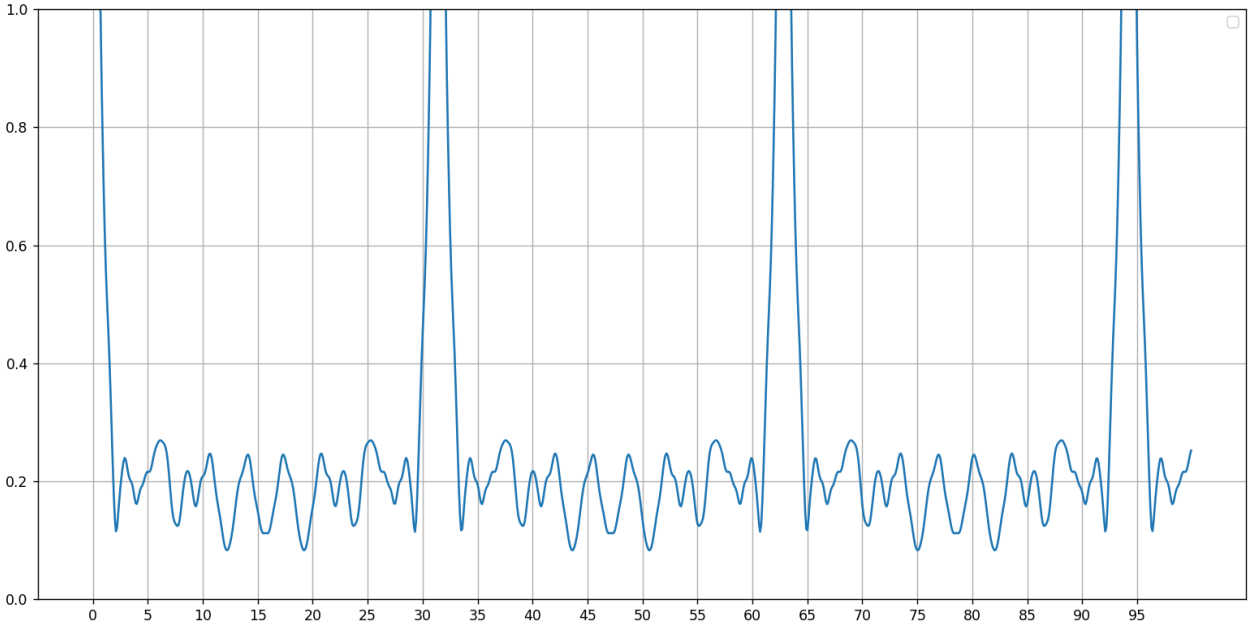


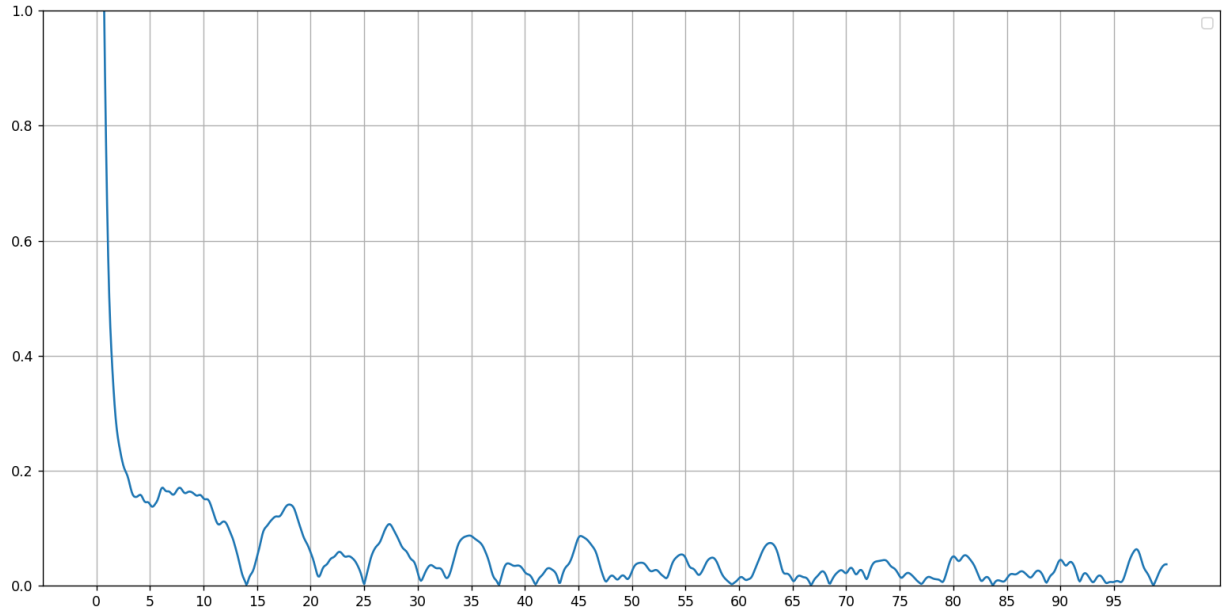
Alors on choisit d'utiliser, par curiosité, ainsi que pour voir si cela permettrait de gagner du temps par rapport à la fonction *quad*, des méthodes d'intégration comme la méthode des trapèzes (fonction *integrale*1 du programme) ou la méthode de Simpson $\frac{1}{3}$ (fonction *integrale*2).

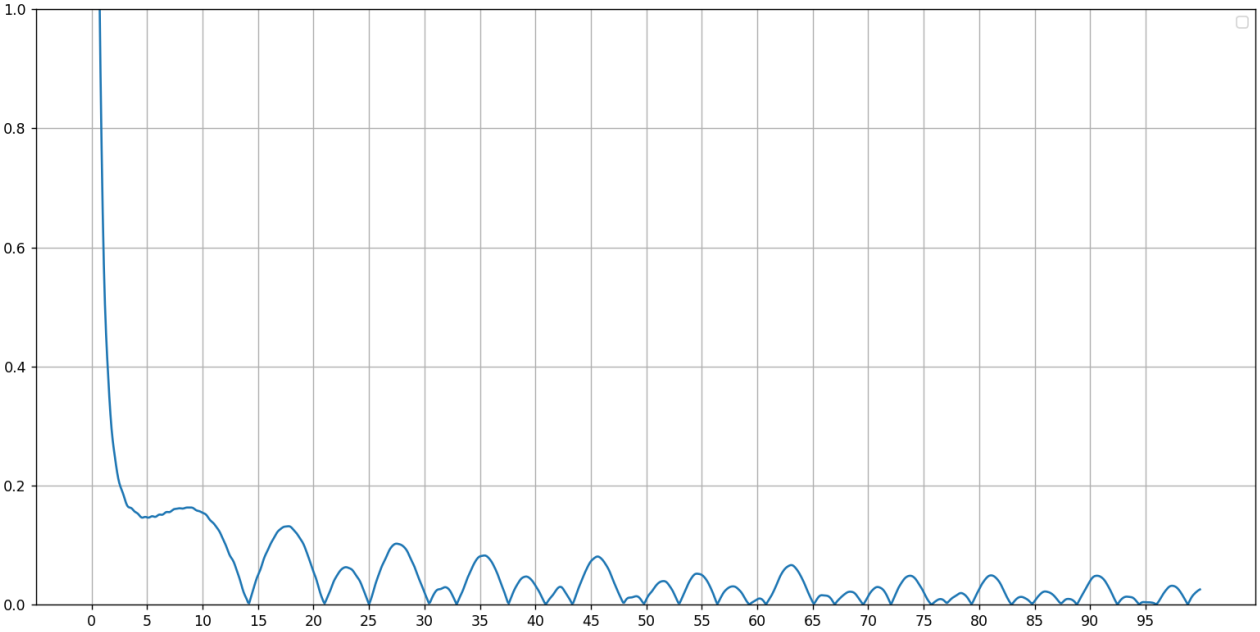
Voici les résultats de l'utilisation de ces fonctions d'approximation des intégrales.

Méthode des trapèzes pour une précision de 10, 100, 1000 et 10000

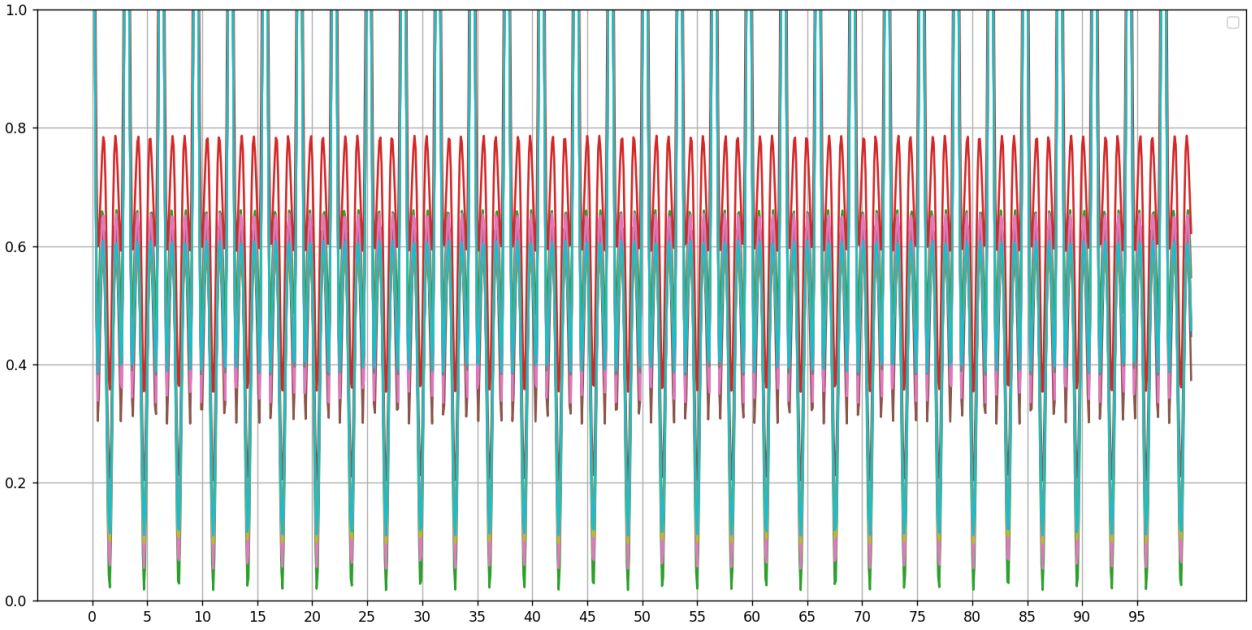


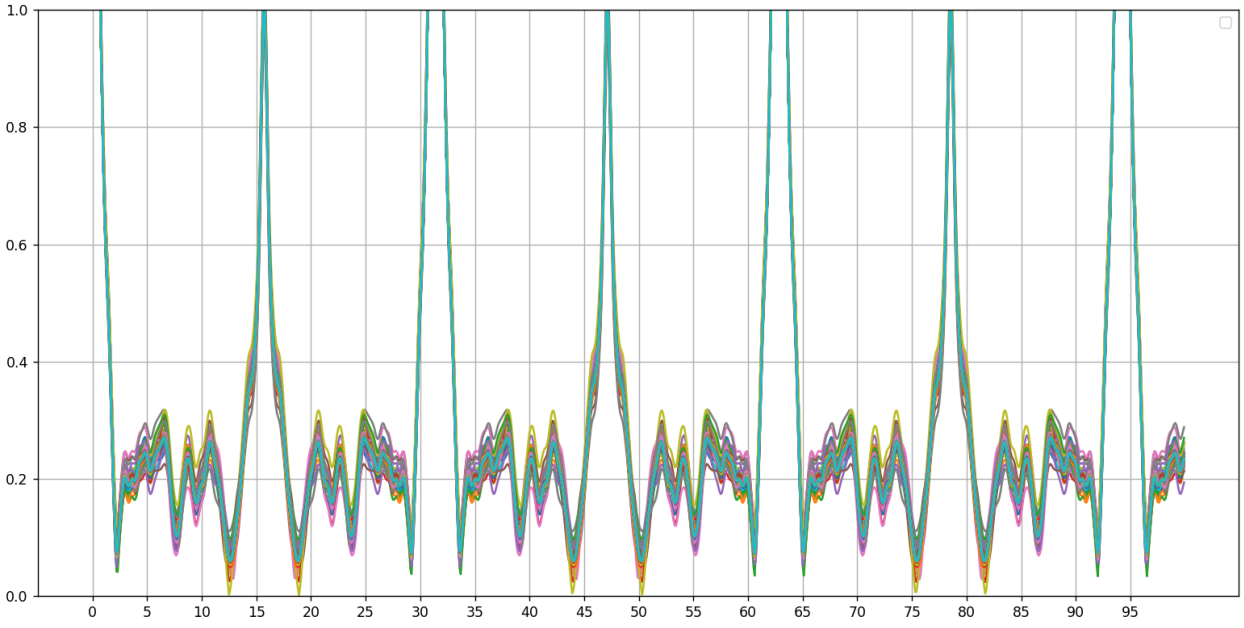


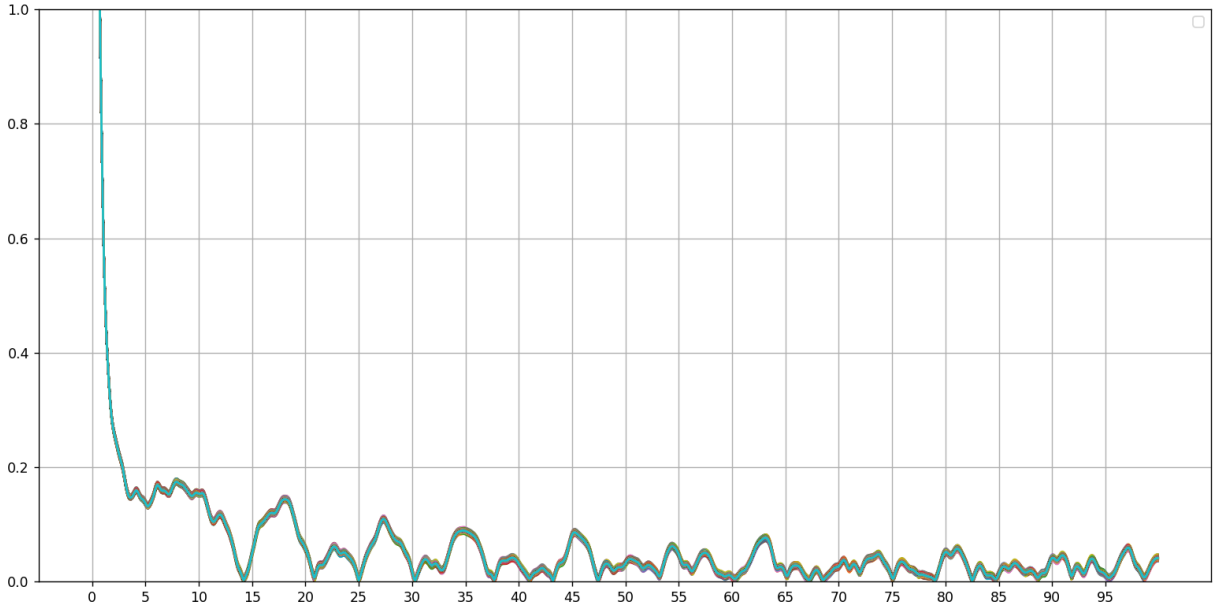

1.0
0.8
0.6
0.4
0.2
0.0
0 5 10 15 20 25 30 35 40 45 50 55 60 65 70 75 80 85 90 95

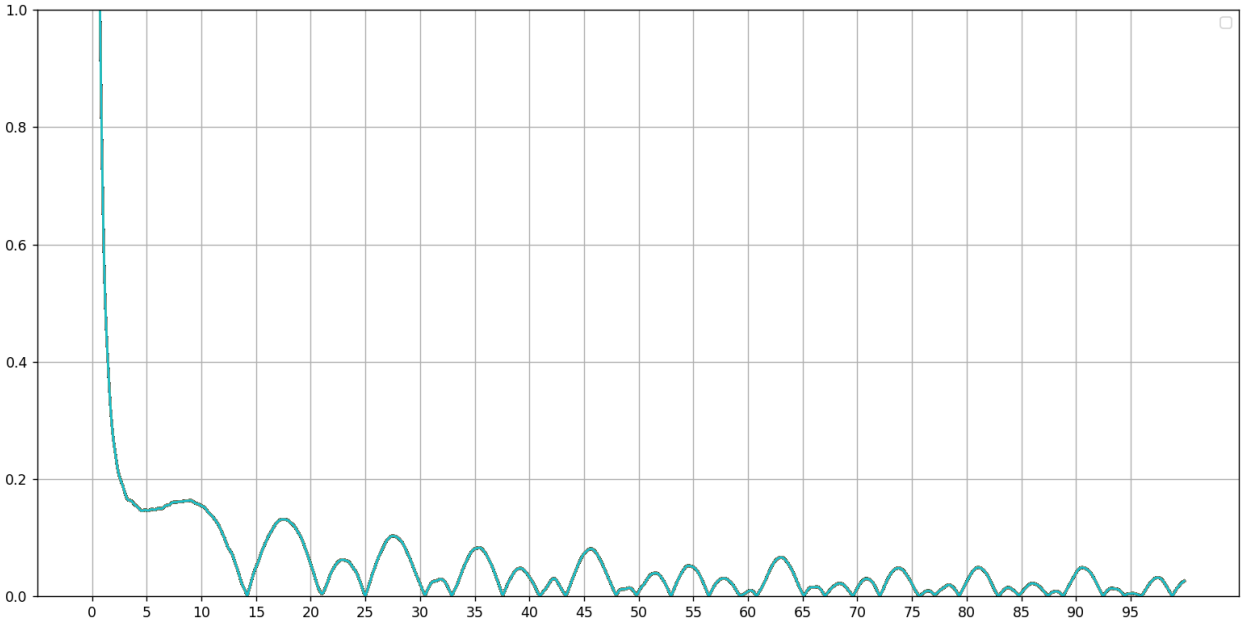

1.0
0.8
0.6
0.4
0.2
0.0
0 5 10 15 20 25 30 35 40 45 50 55 60 65 70 75 80 85 90 95

Méthode Simpson $\frac{1}{3}$ pour une précision de 10, 100, 1000 et 10000









Enfin, pour appréhender le fait que les zéros de zeta en sont bien localement, on note ci-dessous leur image par la fonction zp, ainsi que les images des nombres entiers de dizaines. On voit que l'image d'un zéro est grossièrement plus petite que l'image du nombre entier de dizaines qui lui est inférieur d'un facteur $\frac{1}{10}$ environ (on voit un zéro de plus derrière la virgule dans la partie fractionnaire de l'image). Noter que les nombres 50 et 60 ont des images à deux zéros après la virgule mais tout de même 9 millièmes au lieu de 1 ou 2 pour les zéros qui sont à leur voisinage.

```
14.134725142 --> 0.0016067537523081052
20 --> 0.05532209035993056
21.022039639 --> 0.0026987024591001467
25.01085758 --> 0.0009662281336836151
30 --> 0.020637504764866407
30.424876126 --> 0.0019661521501754863
32.935061588 --> 0.0017667484656647171
37.586178159 --> 0.0018329568813959087
40 --> 0.032272497406023504
40.918719012 --> 0.0010554253153384362
43.327073281 --> 0.0009885789275231932
48.005150881 --> 0.0036477547437878013
49.773832478 --> 0.0018176991302553335
50 --> 0.00907827233423968
52.970321478 --> 0.0019818784620276144
56.446247697 --> 0.0023154470571785015
59.347044003 --> 0.0013514773822215324
60 --> 0.0093078905686516
60.831778525 --> 0.001851124725945632
65.112544048 --> 0.0017173613262055857
67.079810529 --> 0.0029983409048060196
69.546401711 --> 0.0003800330442292773
70 --> 0.014488408386976558
72.067157674 --> 0.0007911817159899152
75.704690699 --> 0.0001459572522272994
77.144840069 --> 0.0035363540815472505
79.33737502 --> 0.0014643212890163874
80 --> 0.02621230979549198
82.910380854 --> 0.0007102674544386193
84.735492981 --> 0.0020297879456133926
87.425274613 --> 0.002697913047415065
88.809111208 --> 0.0004838482658893938
90 --> 0.040102146369664055
92.491899271 --> 0.0009317426688439732
94.651344041 --> 0.003896528887654141
95.870634228 --> 0.0015319154423308876
98.831194218 --> 0.001347237187063686
100 --> 0.02649554592902677
101.317851006 --> 0.001205332943669795
103.72553804 --> 0.000939542425702057
```

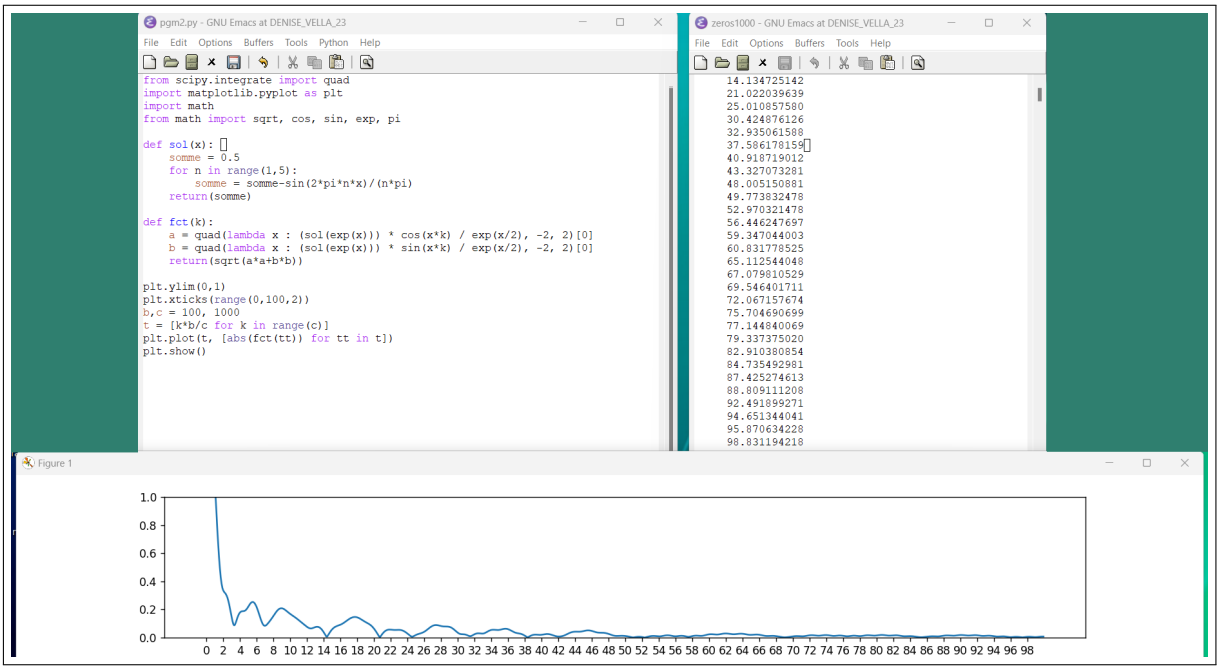
Il semblerait également qu'on ait affaire à un zéro quand il y a une grosse différence entre le cosinus et le sinus des angles considérés. On peut de ce fait utiliser indifféremment (pour n allant jusqu'à 100 et lorsqu'on utilise l'intégrale fournie par le module scipy.integrate de python (notée *quad* dans le programme) la fonction max(|a|, |b|) au lieu de $\sqrt{a^2 + b^2}$. [2]

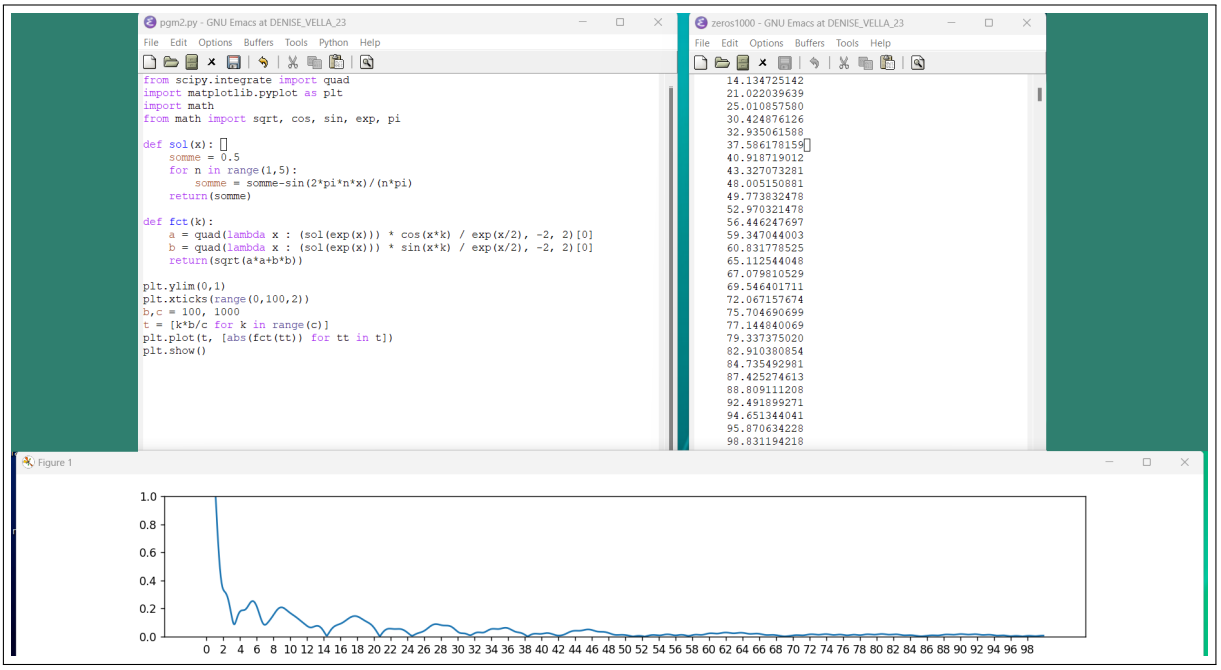
[2] $|x|$ se note abs(x) en python.

On peut enfin approximer la fonction $f(x) = x \bmod 1$ (qui se note x % 1 en python) définie sur les réels et qui renvoie la partie entière d'un nombre par la fonction $sol(x)$ ci-dessous, si ce n'est qu'au lieu de soustraire une infinité de sinus, on n'en soustrait que 5.

$$sol(x) = \frac{1}{2} - \sum_{n=1}^{\infty} \frac{\sin(2\pi n x)}{n\pi}$$

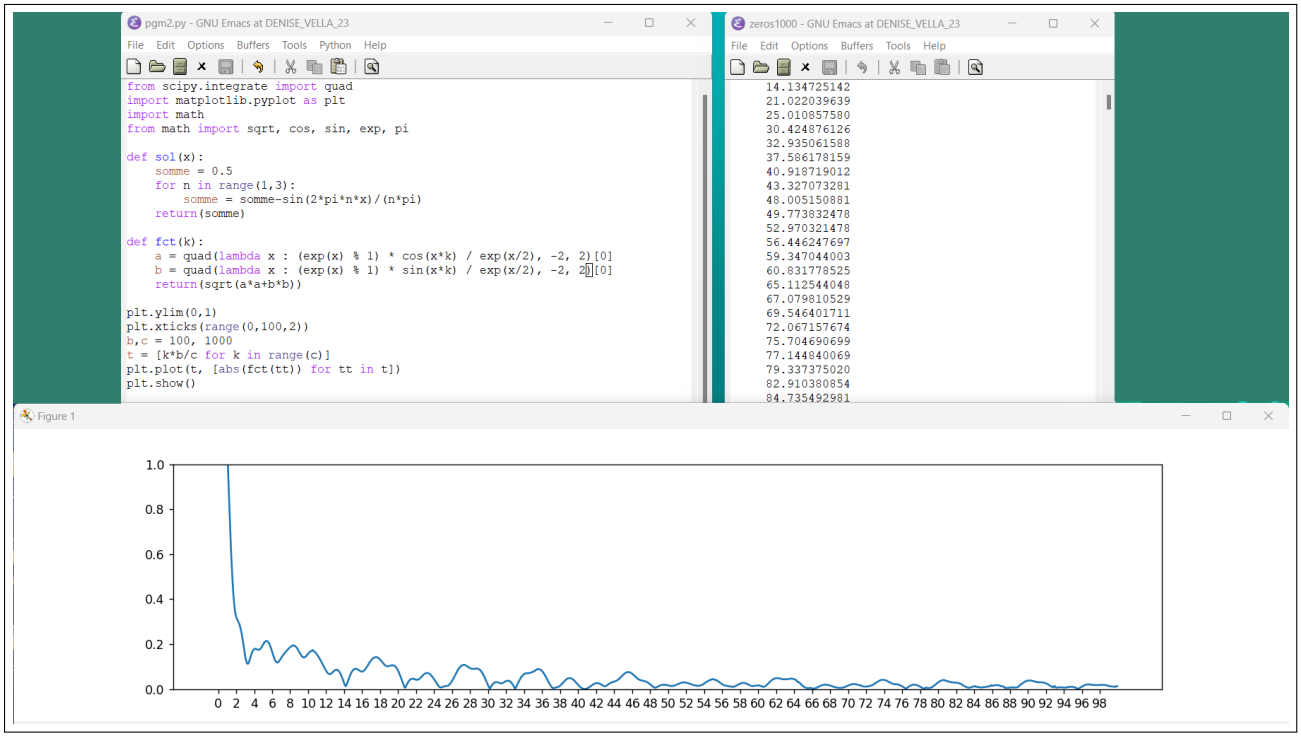
On attrape quelques zéros, mais bien moins, forcément. On essaye en intégrant sur l'intervalle $[-2, 2]$, puis sur l'intervalle $[-3, 3]$.



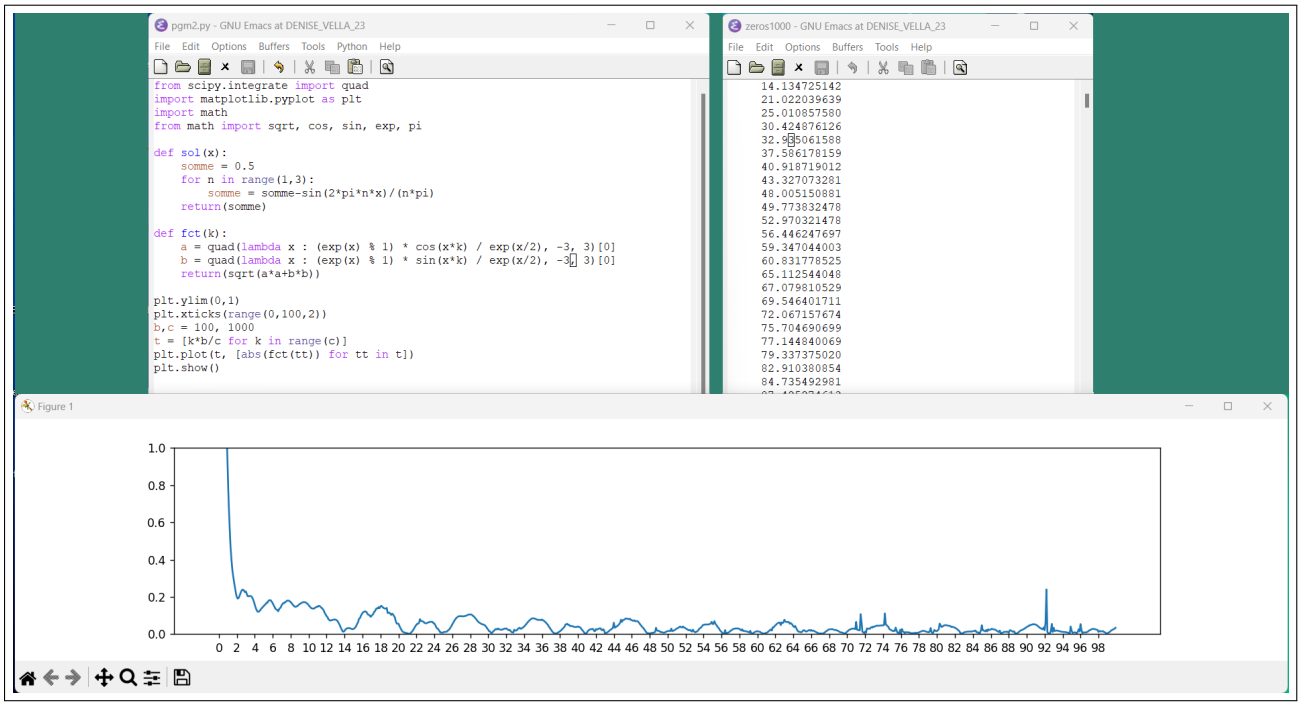


Annexe 1 : les programmes d'hier soir : les images montrent à la fois, le programme, son résultat, et les zéros de ζ pour mémoire.

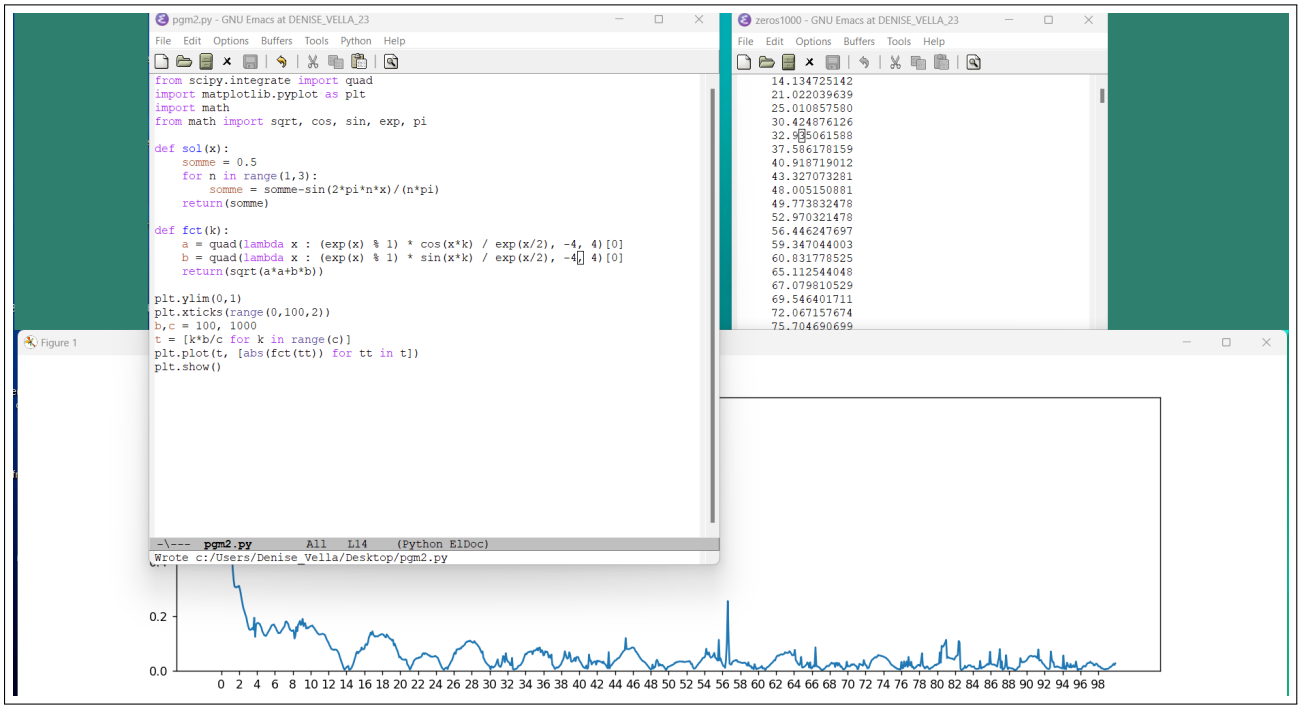
Attraper 7 zéros en prenant l'intervalle $[-2, 2]$



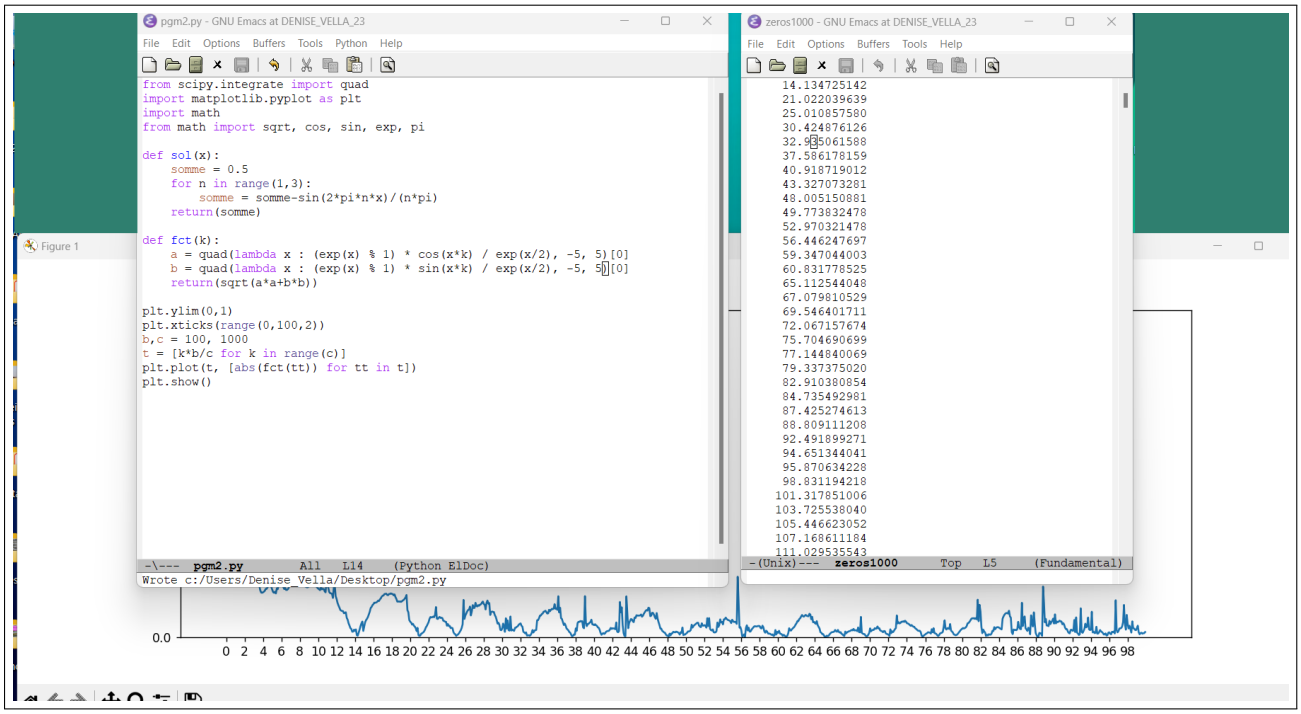
Attraper 9 zéros en prenant l'intervalle $[-3, 3]$



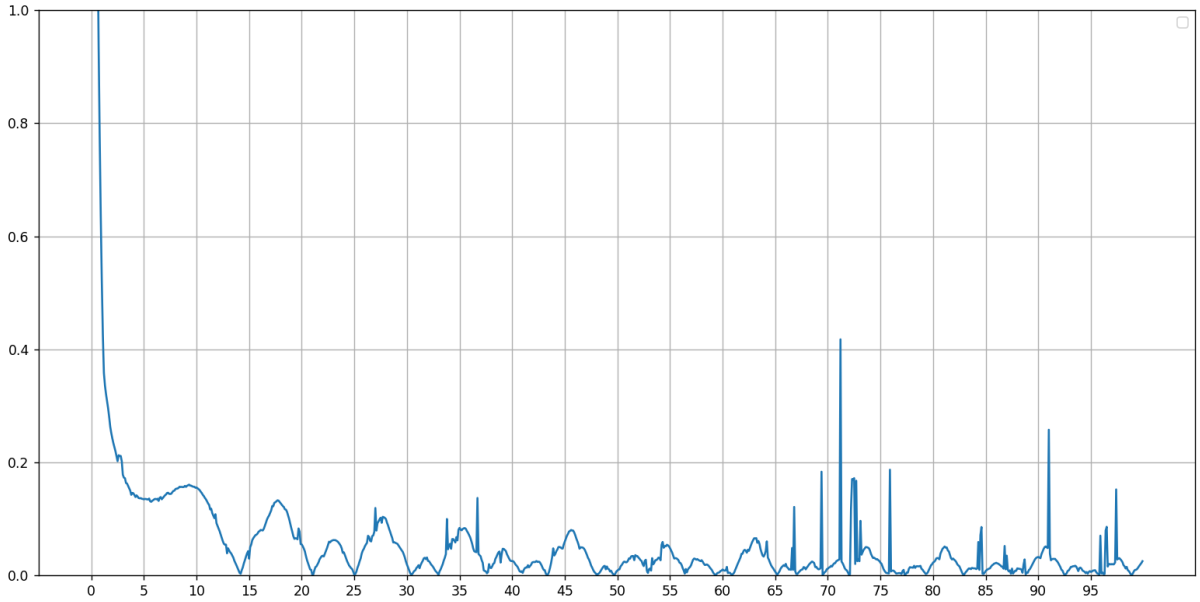
Attraper 14 zéros en prenant l'intervalle $[-4, 4]$



On a perdu le zéro $52, \ldots$ *en prenant l'intervalle* $[-5, 5]$



1000 itérations hier mais extra-pôles !



Annexe 2 : ce que dit l'interpréteur de python quand il n'est pas content

```
C:\Users\Denise_Vella\Desktop>python3 integrale.py
No artists with labels found to put in legend.  Note that artists
whose label start with an underscore are ignored when legend()
is called with no argument.
C:\Users\Denise_Vella\Desktop.py:23:  IntegrationWarning:
The maximum number of subdivisions (200) has been achieved.
If increasing the limit yields no improvement it is advised to analyze
the integrand in order to determine the difficulties.  If the position of a
local difficulty can be determined (singularity, discontinuity) one will
probably gain from splitting up the interval and calling the integrator
on the subranges.  Perhaps a special-purpose integrator should be used.
a = quad(lambda x :  (exp(x) % 1)*cos(x*t)/exp(x/2),-10,10,limit=200)[0]
C:\Users\Denise_Vella\Desktop.py:24:  IntegrationWarning:  The
maximum number of subdivisions (200) has been achieved.
If increasing the limit yields no improvement it is advised to analyze
the integrand in order to determine the difficulties.  If the position of a
local difficulty can be determined (singularity, discontinuity) one will
probably gain from splitting up the interval and calling the integrator
on the subranges.  Perhaps a special-purpose integrator should be used.
b = quad(lambda x :  (exp(x) % 1)*sin(x*t)/exp(x/2),-10,10,limit=200)[0]
C:\Users\Denise_VellaDesktop.py:23:  IntegrationWarning:  The
integral
is probably divergent, or slowly convergent.
a = quad(lambda x :  (exp(x) % 1)*cos(x*t)/exp(x/2),-10,10,limit=200)[0]
C:\Users\Denise_Vella\Desktop.py:24:  IntegrationWarning:  The
integral is probably divergent, or slowly convergent.
b = quad(lambda x :  (exp(x) % 1)*sin(x*t)/exp(x/2),-10,10,limit=200)[0]
```

Fêter le π-day avec 13 jours de retard (Denise Vella-Chemla, 27 mars 2024)

On continue d'essayer de simplifier ce qu'on a trouvé jusque là, toujours dans le but de comprendre.

On utilise pour l'exponentielle une fonction simplifiée *monexp*. Elle utilise le fait que [1]

$$\exp x = \lim_{n\to\infty} \left(1 + x \times \frac{1}{n}\right)^n .$$

On décide de remplacer l'infini par 10000.

On utilise pour l'intégrale, plutôt que la fonction *quad* du package `scipy.integrate` de `python` [2] une fonction qu'on appelle *integrale*2 et qui approxime l'intégrale par la méthode dite Simpson 1/3 (voir par exemple ici https://en.wikipedia.org/wiki/Simpson%27s_rule.).

Le programme qui semble montrer les zéros de ζ devient plus simple, le voici.

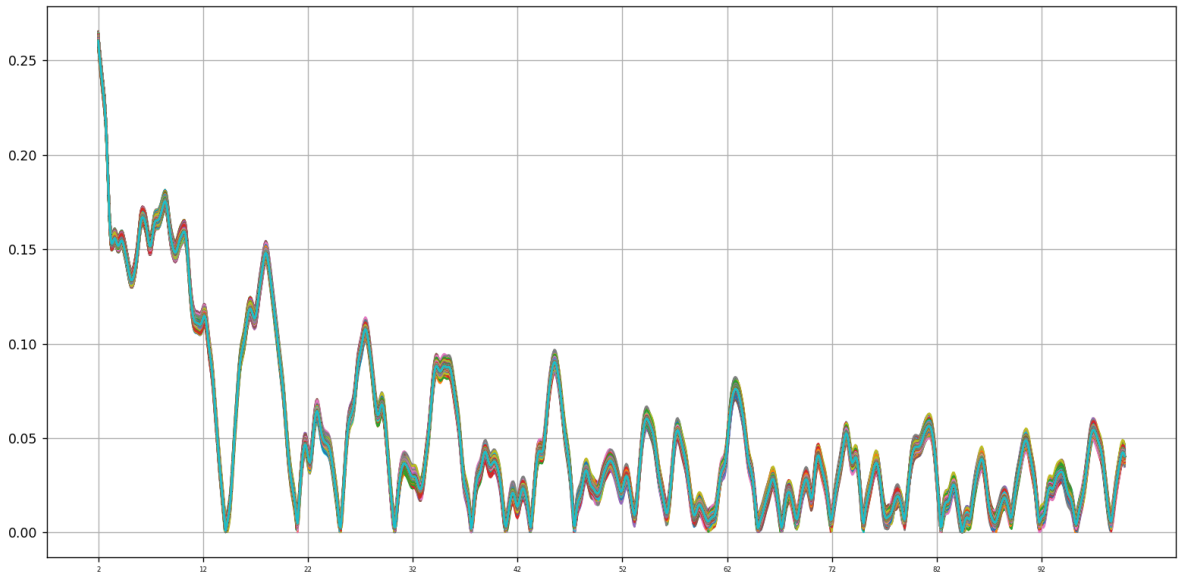
```
import matplotlib.pyplot as plt
import numpy as np
from numpy import linspace, modf, e, sqrt, log, cos, sin, exp, floor, pi
def integrale2(fct, a, b, nbpts):    integration par methode Simpson 1/3
     assert(nbpts%2 == 0)
     x = np.linspace(a,b,num=nbpts+1,endpoint=True)
     h = (b-a)/nbpts
     y = fct(x)
     return (y[0]+4*np.sum(y[1:nbpts:2])+2*np.sum(y[2:nbpts-1:2])+y[1:])  * h/3

def monexp(x):    n represente une sorte d'infini, quand on est petit
     n=10000 ; return(pow(1+x/n,n))

def monlog(x):    meme remarque que pour fonction monexp
     n=10000 ; return((-1+pow(x,1/n))*n)

def y(t):
     a = integrale2(lambda x :  (modf(monexp(x))[0])*cos(x*t)/monexp(x/2),-10,10,1000)
     b = integrale2(lambda x :  (modf(monexp(x))[0])*sin(x*t)/monexp(x/2),-10,10,1000)
     return(sqrt(a*a+b*b))

minx = 2
maxx = 100
nbpoints = 1000
a, b, c = minx, maxx, nbpoints
plt.grid(True)
plt.xticks(range(minx,maxx,10), fontsize=5)
t = [a+k*(b-a)/c for k in range(c)]  puisque a = 0 remplacer par k*b/c
plt.plot(t, [y(tt) for tt in t])
plt.show()
```

[1] On a, symétriquement, trouvé que $\ln(x) = \lim_{n\to\infty} \left(-1 + x^{\frac{1}{n}}\right) \times n$.

[2] angoissante car elle n'arrête pas d'écrire en sortie des messages d'appel à la prudence pour des problèmes de convergence...

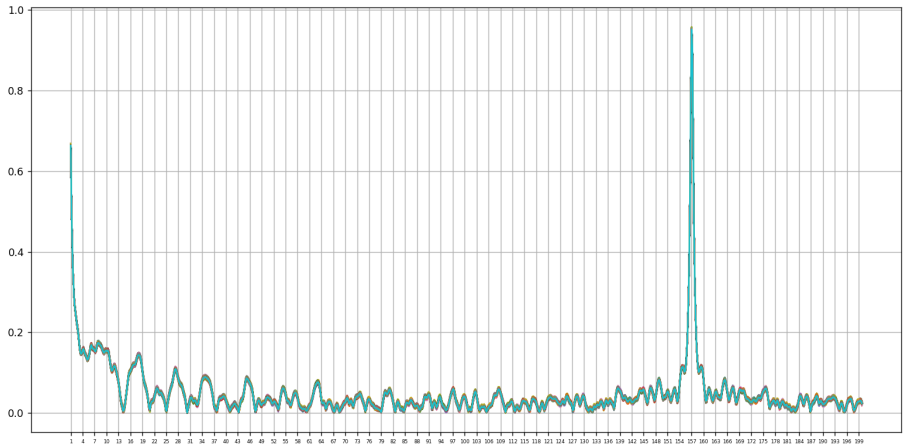
Il faut souligner que l'idée initiale ayant mené à ce programme est celle de Balthasar van der Pol, qui a montré les zéros de ζ en inventant un dispositif constitué d'une scie électro-mécanique circulaire à dents de tailles décroissantes et tournant à une vitesse précise, et l'envoi à certaines fréquences de faisceaux de lumière qui passaient à travers les dents de la scie tournante (voir article de van der Pol de 1947).

Voici son résultat :

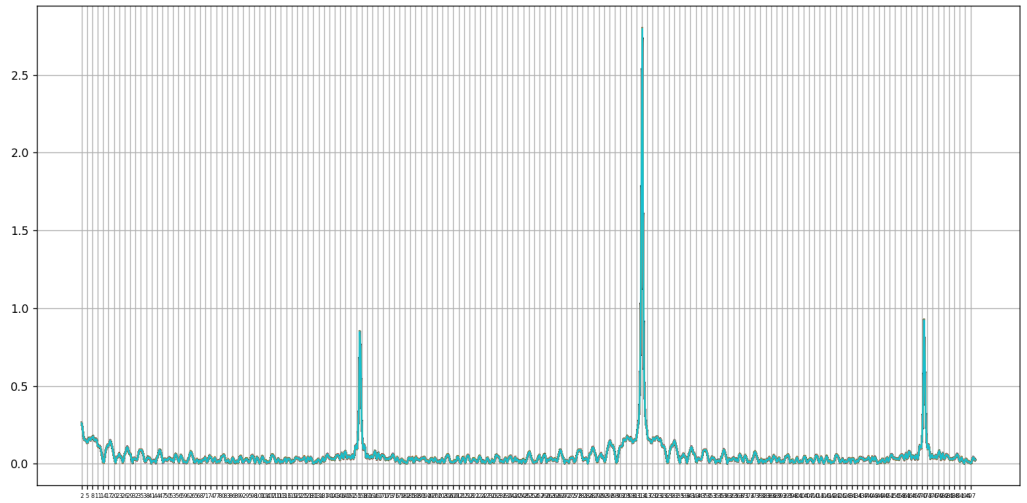


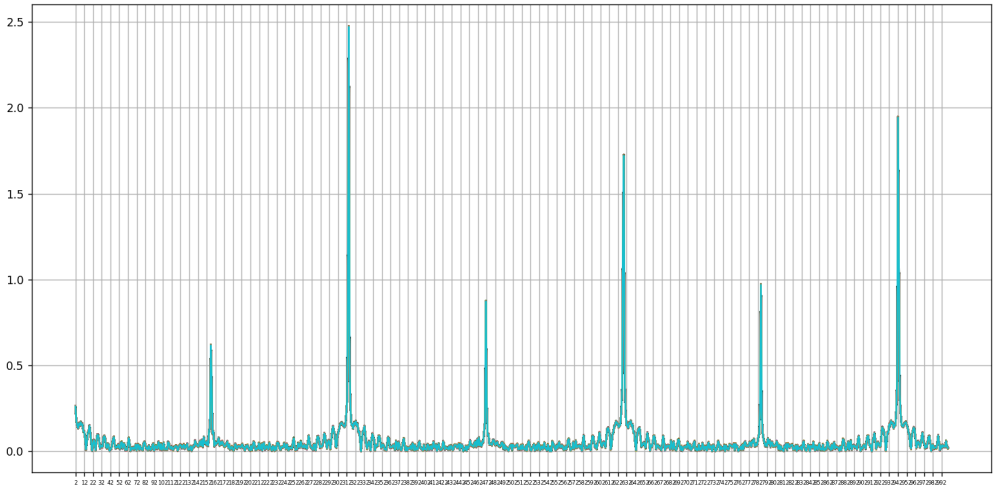
L'intégrale complexe est séparée en intégrale sur le cosinus, intégrale sur le sinus, puis agrégation des deux intégrales en renvoyant $\sqrt{a^2 + b^2}$.

On décide d'aller au-delà de 100 et là, surprise, il y a une pointe pour $n = 157$. On ne comprend pas, on cherche le cosinus de 157, il est proche de 1 (0.95). Ce qui est intéressant, c'est de voir l'aspect symétrique des zéros autour de ce pôle : il y a un zéro en 179, symétrique de 135 par rapport à 157, puis un autre, en 183 (sym. de 131), puis en 187, 195, 198 (sym resp. de 127, 119, 116).



Du coup, on programme jusqu'à 500 et là, on voit apparaître enfin des sortes de Dirac[3] (c'est le nom donné aux pics de valeurs que prend une fonction autour desquels les valeurs sont nulles). Ici les valeurs autour des simili-Dirac sont beaucoup plus petites que les valeurs prises aux pics. Les pics ont lieu pour les valeurs 157, 314, ..., c'est à dire pour les valeurs multiples de $(100\times)\ \pi/2$.





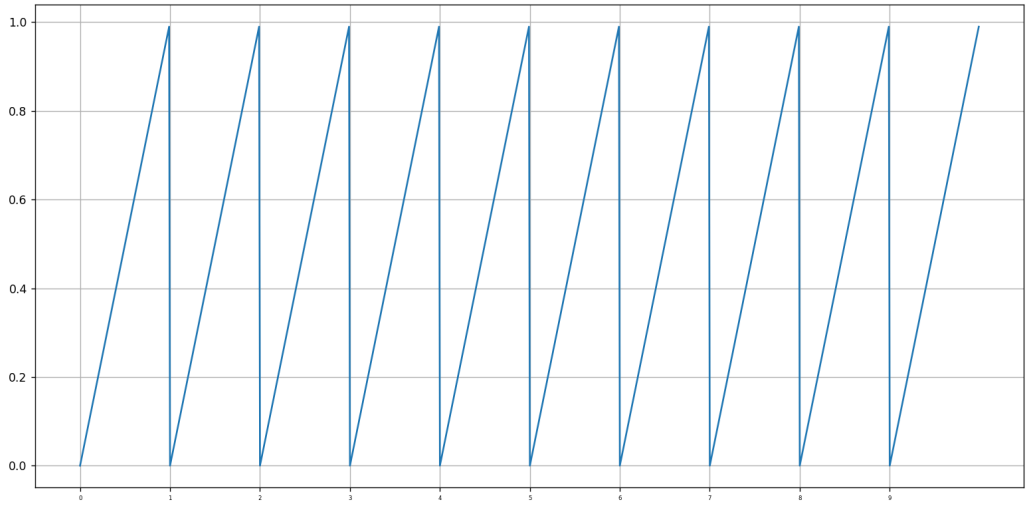
Si l'on souhaite (jusqu'à 200)"ramener le pic de 157 vers le bas, pour rater moins de zéros autour de 157, on peut changer le paramètre *nbpoints*.

Par rapport aux zéros de la fonction ζ, on en rate un certain nombre, notamment autour des pics, et ce d'autant plus qu'on va loin.

De toute façon, on reste ennuyée par la fonction partie fractionnaire, $f(x) = x \bmod 1$, (programmée en python soit en utilisant le symbole % lorsqu'on l'utilise sur des réels ou entiers, soit en utilisant

[3]Cela corrobore peut-être le fait que certains utilise un opérateur de Dirac, dans leur quête de la démonstration de l'hypothèse de Riemann.

la fonction `modf` du package `numpy` lorsqu'on souhaite l'utiliser sur des vecteurs) qui calcule le reste modulaire : cette fonction est une fonction en dents de scie[4], elle est donc problématique pour pouvoir raisonner convenablement. On rappelle son allure ci-dessous :



[4]C'est un peu le cas de le dire.

Sans complexe (Denise Vella-Chemla, 31 mars 2024)

Pour ceux qui ne se risquent pas trop dans le plan complexe, voici des résultats de calculs étonnants, qui montrent la ressemblance numérique qu'il peut y avoir entre certaines sommes d'inverses de racines d'entiers (ici des racines carrées, cubiques, quartiques (ou bicarrées ou quatrièmes), quintiques (cinquièmes)), et le produit d'une seule de telles racines (la dernière[1]) par une fraction rationnelle (en fait, l'inverse d'une fraction rationnelle plutôt). Voyons le programme, c'est plus simple, on comprendra rapidement le but visé :

```
import math
from math import sqrt

print('racine carree')
nmax = 10000000
somme = 1
for k in range(2,nmax+1):
      somme = somme+pow(k,-0.5)
print(somme)
print(2*pow(nmax,0.5))-2
print('')
print('cubique')
somme = 1
for k in range(2,nmax+1):
      somme = somme+pow(k,-1/3)
print(somme)
print(3*pow(nmax,2/3)/2-3/2)
print('')
print('quatrieme')
somme = 1
for k in range(2,nmax+1):
      somme = somme+pow(k,-1/4)
print(somme)
print(4*pow(nmax,3/4)/3-4/3)
print('')
print('cinquieme')
somme = 1
for k in range(2,nmax+1):
      somme = somme+pow(k,-1/5)
print(somme)
print(5*pow(nmax,4/5)/4)-5/4
```

Le résultat de ce programme tout simple est :

[1]En fait, il s'agit de calculer la limite d'une somme, mais comme l'infini n'existe pas en informatique, on va moins loin.

```
racine carree
6323.095123940201
6322.555320336759

racine cubique
69622.86146473711
69622.33250419164

racine quatrieme
237103.1169515448
237102.5880051897

racine cinquieme
497633.2491763715
497632.71319187194
```

On pourrait résumer ces résultats par cette formule (testée pour $2 \leq k \leq 5$) :

$$\sum_{n=1}^{N} n^{-\frac{1}{k}} = \frac{k}{k-1} N^{\frac{k-1}{k}} - \frac{k}{k-1}$$

On teste l'inversion de réels par le programme :

```
print('racine sqrt(2)-ieme')
nmax = 10000000
somme = 1
for k in range(2,nmax+1):
     somme = somme+pow(k,-1/sqrt(2))
print(somme)
print(sqrt(2)*pow(nmax,(sqrt(2)-1)/sqrt(2))/(sqrt(2)-1)-(sqrt(2)/(sqrt(2-1))))
print('')
print('racine sqrt(3)-ieme')
nmax = 10000000
somme = 1
for k in range(2,nmax+1):
     somme = somme+pow(k,-1/sqrt(3))
print(somme)
print(sqrt(3)*pow(nmax,(sqrt(3)-1)/sqrt(3))/(sqrt(3)-1)-(sqrt(3)/(sqrt(3)-1)))
print('')
print('racine sqrt(5)-ieme')
nmax = 10000000
somme = 1
for k in range(2,nmax+1):
     somme = somme+pow(k,-1/sqrt(5))
print(somme)
print(sqrt(5)*pow(nmax,(sqrt(5)-1)/sqrt(5))/(sqrt(5)-1)-(sqrt(5)/(sqrt(5)-1)))
print('')
print('racine sqrt(11)-ieme')
nmax = 10000000
somme = 1
for k in range(2,nmax+1):
     somme = somme+pow(k,-1/sqrt(11))
print(somme)
print(sqrt(11)*pow(nmax,(sqrt(11)-1)/sqrt(11))/(sqrt(11)-1)-(sqrt(11)/(sqrt(11)-1)))
```

Ça marche...

```
racine sqrt(2)-ieme
380.4451536262492
379.8896659382487

racine sqrt(3)-ieme
2148.818632882152
2148.2729838521122

racine sqrt(5)-ieme
13393.873727589036
13393.337806659993

racine sqrt(11)-ieme
110983.31556131091
110982.78755376296
```

On s'enhardit dans le programme suivant, en prenant l'inverse d'un complexe choisi au hasard :

```
print('racine sqrt(11)-ieme')
nmax = 10000000
somme = 1
for k in range(2,nmax+1):
     somme = somme+pow(k,-1/(sqrt(11)+sqrt(3)*1j))
print(somme)
print((sqrt(11)+sqrt(3)*1j)*pow(nmax,((sqrt(11)-1+sqrt(3)*1j)
          /(sqrt(11)+sqrt(3)*1j)))/(sqrt(11)-1+sqrt(3)*1j)
          -(sqrt(11)+sqrt(3)*1j)/(sqrt(11)-1+sqrt(3)*1j))
```

Et sans surprise :

```
racine sqrt(11)+sqrt(3)i -ieme
(-73744.01084409936+274363.98023297265j)
(-73744.52540501424+274363.9800489613j)
```

La formule fonctionne à nouveau. Il semblerait qu'on ait toujours, si l'on respecte la contrainte ci-dessous, que k soit entier, réel ou complexe (et à une erreur minime près à préciser) :

$$\sum_{n=1}^{N} n^{-\frac{1}{k}} = \frac{k}{k-1} N^{\frac{k-1}{k}} - \frac{k}{k-1}.$$

La contrainte est qu'il faut que k soit supérieur à 1, c'est-à-dire que si on prend $k = 1/4$ pour en fait, par le 1/1/4 retrouver 4 comme puissance, la formule (le test par programme de la formule) ne fonctionne plus.

Transcription de l'extrait du *Traité des fonctions elliptiques et des intégrales eulériennes*, de Adrien-Marie Legendre, contenant le théorème dont Galois a donné un énoncé différent dans sa lettre à Auguste Chevalier

CHAPITRE XII.

Théorème sur les fonctions complètes de première et de seconde espèce, dont les modules sont compléments l'un de l'autre.

45. Dans les comparaisons qu'on vient d'établir entre les fonctions $F^1(c)$, $E^1(c)$, qui se rapportent au module $c = \frac{1}{2}\sqrt{(2-\sqrt{3})} = \sin 15^\circ$, et les fonctions $F^1(b), E^1(b)$, qui se rapportent au module complémentaire $b = \frac{1}{2}\sqrt{(2+\sqrt{3})} = \cos\ 15^\circ$, les trois équations trouvées conduisent à ce résultat remarquable

$$(d') \qquad \frac{\pi}{2} = F^1(c)E^1(b) + F^1(b)E^1(c) - F^1(b)F^1(c)$$

où l'on voit que les deux quantités b, c peuvent être échangées entre elles, et qu'ainsi cette équation est vérifiée dans deux cas, celui de $c = \sin 15^\circ$ et celui de $c = \sin 75^\circ$. Il serait facile de démontrer directement qu'elle est encore vraie dans deux autres cas, lorsque c est infiniment petit, et lorsque $c = \sqrt{\frac{1}{2}} = b$ mais nous allons prouver généralement qu'elle a lieu quel que soit c.

Pour abréger la notation, désignons simplement par F, E, les quantités $F^1(c), E^1(c)$ et par F', E' les quantités $F^1(b), E^1(b)$ et supposons

$$P = FE' + F'E - FF',$$

P étant une fonction de c encore inconnue.

Je différencie les deux membres par rapport à c qui est la seule variable qu'ils contiennent. Or ayant $E(\varphi) = \int \Delta d\varphi$, $F(\varphi) = \int \frac{d\varphi}{\Delta}$, $\Delta^2 = 1 - c^2\sin^2\varphi$, la différentiation donne

$$\frac{dE}{dc} = -\int \frac{cd\varphi \sin^2\varphi}{\Delta} = \frac{1}{c}(E - F),$$

$$\frac{dF}{dc} = \int \frac{cd\varphi \sin^2\varphi}{\Delta^3} = \frac{1}{c}\int \frac{d\varphi}{\Delta^3} - \frac{1}{c}\int \frac{d\varphi}{\Delta}.$$

Tome 1, 1825, Imprimerie de Huzard-Courcier.
Transcription en Latex : Denise Vella-Chemla, avril 2024.

Mais par les formules de l'art. 9, on a $\int \frac{d\varphi}{\Delta^3} = \frac{1}{b^2}\int \Delta d\varphi - \frac{c^2 \sin\varphi \cos\varphi}{b^2\Delta}$ et dans le cas de $\varphi = \frac{1}{2}\pi$ dont il s'agit, le second terme s'évanouit : ainsi on aura

$$\frac{dF}{dc} = \frac{1}{b^2 c}(E - b^2 F).$$

On aura semblablement $\frac{dE'}{db} = \frac{1}{b}(E' - F')$, $\frac{dF'}{db} = \frac{1}{c^2 b}(E' - c^2 F')$ et parce que $bdb + cdc = 0$, on en déduira

$$\frac{dE'}{dc} = -\frac{c}{b^2}(E' - F'),$$

$$\frac{dF'}{dc} = -\frac{1}{b^2 c}(E' - c^2 F').$$

Substituant ces valeurs dans celle de dP, on aura $dP = 0$; donc $P = \text{const}$. Mais on a trouvé dans un cas particulier $P = \frac{1}{2}\pi$ donc l'équation (d') a lieu généralement, quel que soit c.

Lorsque $c = \sqrt{\frac{1}{2}} = b$, l'équation (d') donne

$$\frac{\pi}{2} = F^1(2E^1 - F^1).$$

Ainsi dans ce cas particulier, E^1 se détermine encore par F^1.

Il peut y avoir quelques autres cas particuliers où la fonction de seconde espèce $E^1(c)$ s'exprime par la fonction de première espèce $F^2(c)$ [1] ; nous ferons voir en effet que chaque cas particulier connu en fait connaître une infinité d'autres; mais il paraît impossible de réduire généralement les fonctions de seconde espèce à celles de la première.

[1] bizarre, on penserait que [1] signifie première espèce et [2] signifie seconde espèce.

Petites expérimentations informatiques autour de quelques zéros de la fonction ζ de Riemann (Denise Vella-Chemla, 9 avril 2024)

On a isolé la formule ci-dessous, et on souhaite la réutiliser pour faire quelques expérimentations informatiques dans lesquels interviennent les premiers zéros de la fonction ζ de Riemann :

$$\sum_{n=1}^{N} n^{-\frac{1}{k}} \simeq \frac{k}{k-1} N^{\frac{k-1}{k}} - \frac{k}{k-1}.$$

On calcule la somme au fur et à mesure, et on compare le résultat à celui d'une "somme-éclair" qui consiste à soustraire, du résultat de l'application d'une fonction au plus grand élément N, le résultat de l'application de cette fonction au plus petit élément [1] .

La formule ci-dessus ne marche pas lorsque k est supérieur à 1 (on aurait aimé tester les résultats de ce programme pour approximer la fonction ζ sur les entiers positifs impairs (Euler a fourni les formules pour les images par ζ des entiers positifs pairs ($\frac{\pi^2}{6}$, $\frac{\pi^4}{90}$, etc.)).

On se contente d'abord de ce programme, en prenant les ***inverses*** des $s = a+bi$ comme puissances des entiers successifs.

Ce programme a deux parties : dans la première, on teste le nombre $\sqrt{3}+bi$ avec pour b les parties réelles des zéros non-triviaux de la fonction ζ de Riemann ; en dernier lieu est imprimé le nombre z calculé par "somme-éclair".

La seconde partie teste les nombres de la forme $0.5 + bi$ (là aussi, on utilise leur inverse comme puissances des entiers successifs). (*note :* le petit test en fin de programme, pour le nombre 5, est "pour la route").

```
import mpmath
from mpmath import sqrt, fadd, fsub, fmul, fdiv, fmul, power

liste2 = [14.134725142, 21.022039639, 25.010857580, 30.424876126, 32.935061588,
          37.586178159, 40.918719012, 43.327073281, 48.005150881, 49.773832478,
          52.970321478, 56.446247697, 59.347044003, 60.831778525, 65.112544048,
          67.079810529, 69.546401711, 72.067157674, 75.704690699, 77.144840069,
          79.337375020, 82.910380854, 84.735492981, 87.425274613, 88.809111208,
          92.491899271, 94.651344041, 95.870634228, 98.831194218,
          101.317851006, 103.725538040]
```

[1] Petit hommage à mon Professeur Amalberti en terminale, décédé il y a peu d'années, et qui nous avait appris cela, enlever directement le plus petit du plus grand, j'avais beaucoup apprécié.

```
nmax = 1000
for b in range(1,len(liste2)):
      somme = 0
      unzero = sqrt(3)+liste2[b]*1j
      for m in range(2,nmax+1):
            somme = fadd(somme,power(m,-1/unzero))
      print('= ',somme)
z = ((unzero/(unzero-1))*power(nmax,(unzero-1)/unzero))-unzero/(unzero-1
print('z = ',z)

nmax = 10000
for b in range(1,len(liste2)):
      somme = 0
      unzero = 0.5+liste2[b]*1j
      for m in range(2,nmax+1):
            somme = fadd(somme,power(m,-1/unzero))
      print('= ',somme)
      z = ((unzero/(unzero-1))*power(nmax,(unzero-1)/unzero))-unzero/(unzero-1)
      print('z = ',z)

k = 5 ; print('k = 5')
somme = 0
for m in range(2,nmax+1):
      somme = somme+pow(m,-1/k)
print('somme = ',somme)
z = (k/(k-1))*pow(nmax,(k-1)/k)-k/(k-1)
print('z = ',z)
```

Voici le résultat de ce programme :

```
somme = (937.391047744019 + 269.016467315008j)
somme = (955.0262432394 + 229.063442882624j)
somme = (969.043714501581 + 190.22500858787j)
somme = (973.372892253819 + 176.274489451519j)
somme = (979.257160725326 + 155.113103308364j)
somme = (982.313247452276 + 142.790941888911j)
somme = (984.101752960815 + 135.025502265708j)
somme = (986.845173161202 + 122.104895029444j)
somme = (987.688295091965 + 117.836367765774j)
somme = (989.004924774426 + 110.828817762835j)
somme = (990.192141567962 + 104.091416271494j)
somme = (991.028393951085 + 99.0621053144593j)
somme = (991.411147805836 + 96.6704051876042j)
somme = (992.372624847037 + 90.3762137279111j)
somme = (992.754316434442 + 87.7493532649592j)
somme = (993.188079469565 + 84.6630554792868j)
somme = (993.586340741406 + 81.7246638371718j)
```

```
somme = (994.092695171148 + 77.8256424750291j)
somme = (994.273727268749 + 76.3825245777005j)
somme = (994.530702766212 + 74.2850931076402j)
somme = (994.906749852766 + 71.1026174986717j)
somme = (995.080798499734 + 69.5796679298265j)
somme = (995.317762826003 + 67.450184710041j)
somme = (995.431396731966 + 66.4044762364337j)
somme = (995.709413520482 + 63.7728960706679j)
somme = (995.857588591251 + 62.3244312257977j)
somme = (995.936875665301 + 61.5352162005246j)
somme = (996.117352962346 + 59.6994620260975j)
somme = (996.256901368488 + 58.2399659358357j)
somme = (996.382586031852 + 56.8931222539137j)
z = (996.384234835206 + 56.8606753195574j)

somme = (9151.00825403381 + 3765.67572302796j)
z = (9151.06002068822 + 3765.46976257876j)

somme = (9396.02540986608 + 3199.31313813996j)
z = (9396.06225534269 + 3199.1377718895j)

somme = (9589.45995925896 + 2652.12472806604j)
z = (9589.48500387034 + 2651.97910893805j)

somme = (9648.96705633026 + 2456.2639012174j)
z = (9648.98846691369 + 2456.12896660986j)

somme = (9729.6744078832 + 2159.76089616604j)
z = (9729.69088702328 + 2159.64216742466j)

somme = (9771.51162386772 + 1987.40695507286j)
z = (9771.52554540158 + 1987.29766198341j)

somme = (9795.97080796618 + 1878.89148107795j)
z = (9795.98323386382 + 1878.78813395713j)

somme = (9833.45325244105 + 1698.4977493121j)
z = (9833.46338579667 + 1698.40429476416j)

somme = (9844.96382473054 + 1638.94307408574j)
z = (9844.97325392924 + 1638.85288751589j)

somme = (9862.93068571125 + 1541.21485471685j)
z = (9862.93901566439 + 1541.13003291378j)

somme = (9879.12301084734 + 1447.30010323431j)
z = (9879.13034999238 + 1447.22043914618j)

somme = (9890.52370466125 + 1377.22259898036j)
z = (9890.53034612317 + 1377.14678485803j)

somme = (9895.74047740364 + 1343.90498658375j)
z = (9895.74679959638 + 1343.83100327832j)
```

```
somme = (9908.84129145728 + 1256.24685572033j)
z = (9908.84681181644 + 1256.17769041154j)

somme = (9914.04064200755 + 1219.67255484294j)
z = (9914.04584411851 + 1219.60540025541j)

somme = (9919.94828835072 + 1176.70827037783j)
z = (9919.95312884375 + 1176.64347814671j)

somme = (9925.37146766548 + 1135.80963301505j)
z = (9925.3759761811 + 1135.74708988912j)

somme = (9932.26525406771 + 1081.54987665898j)
z = (9932.2693405632 + 1081.490317867j)

somme = (9934.72956769539 + 1061.46977066441j)
z = (9934.73350332643 + 1061.41131642734j)

somme = (9938.22734448692 + 1032.28779190511j)
z = (9938.2310659802 + 1032.23094301601j)

somme = (9943.3451617649 + 988.014870753316j)
z = (9943.34856992934 + 987.960457658079j)

somme = (9945.71360484904 + 966.8306688448j)
z = (9945.71686800581 + 966.777421366333j)

somme = (9948.93792185681 + 937.211977274021j)
z = (9948.9409876007 + 937.160359619025j)

somme = (9950.48399729886 + 922.668354686834j)
z = (9950.48696838061 + 922.617537370179j)

somme = (9954.2663150173 + 886.071379219566j)
z = (9954.26905451296 + 886.022575978726j)

somme = (9956.28200257685 + 865.929476844833j)
z = (9956.28461865193 + 865.881782173831j)

somme = (9957.36052628717 + 854.95538476783j)
z = (9957.36307632345 + 854.908294112547j)

somme = (9959.81538312644 + 829.430389686596j)
z = (9959.81778284797 + 829.38470399428j)

somme = (9961.71339646358 + 809.138292036077j)
z = (9961.71567996479 + 809.093723336005j)

somme = (9963.42275220912 + 790.413427031308j)
z = (9963.42493104057 + 790.369889101328j)

b = 5
somme = 1979.4618140469709
z = 1979.8664905763926
```

Encouragée, on met alors les zéros directement comme puissances des entiers, là, tout tombe, les résultats ne s'accordent plus du tout, la "somme-éclair" n'est pas valide ! On a oublié de mettre les puissances des entiers aux dénominateurs, ce qu'on fait alors, et ce qui est intéressant, c'est qu'il faut en dernier lieu, diviser le complexe obtenu par le plus grand entier (représentant sensément l'infini) pour que les résultats s'accordent. Cette idée est naturellement suggérée par les coïncidences numériques.

Voici le second programme :

```
import mpmath
from mpmath import sqrt, fadd, fsub, fmul, fdiv, fmul, power

liste2 = [14.134725142, 21.022039639, 25.010857580, 30.424876126, 32.935061588,
          37.586178159, 40.918719012, 43.327073281, 48.005150881, 49.773832478,
          52.970321478, 56.446247697, 59.347044003, 60.831778525, 65.112544048,
          67.079810529, 69.546401711, 72.067157674, 75.704690699, 77.144840069,
          79.337375020, 82.910380854, 84.735492981, 87.425274613, 88.809111208,
          92.491899271, 94.651344041, 95.870634228, 98.831194218,
          101.317851006, 103.725538040]

nmax = 10000
for b in range(1,len(liste2)):
     somme = 1
     unzero = 0.5+liste2[b]*1j
     for m in range(2,nmax+1):
          somme = fadd(somme,fdiv(1,m ** unzero))
     print('= ',somme)
     moinsinv = -1/unzero
     z = fsub((fdiv(moinsinv,fsub(moinsinv,1))*
                (nmax ** fdiv(fsub(moinsinv,1),moinsinv))),
                fdiv(moinsinv,fsub(moinsinv,1)))
     print('z = ',z)
     print('je le divise ',fdiv(z,nmax))
```

Et voici son résultat :

```
somme = (-4.30872642771148 + 2.01281820449113j)
z = (-42011.277481029 - 22054.7006014833j)
je le divise (-4.2011277481029 - 2.20547006014833j)

somme = (-3.45455265422163 - 2.0116158388696j)
z = (-35240.1108748189 + 18735.4739670357j)
je le divise (-3.52401108748189 + 1.87354739670357j)

somme = (-1.96177357854244 - 2.63666946543367j)
z = (-20410.9324275024 + 25711.3032383404j)
je le divise (-2.04109324275024 + 2.57113032383404j)
```

```
somme = (2.9777204488798 - 0.592038346895068j)
z = (29567.1526547224 + 6765.63808308653j)
je le divise (2.95671526547224 + 0.676563808308653j)

somme = (1.54898768852099 + 2.16293469293667j)
z = (16007.7313866147 - 21224.5081219926j)
je le divise (1.60077313866147 - 2.12245081219926j)

somme = (-0.247673556138264 + 2.43116640737761j)
z = (-1930.93708921621 - 24345.8104048558j)
je le divise (-0.193093708921621 - 2.43458104048558j)

somme = (-0.204057032084971 - 2.2988929567247j)
z = (-2519.16758315439 + 22928.484928036j)
je le divise (-0.251916758315439 + 2.2928484928036j)

somme = (1.5058076982267 - 1.43932073303922j)
z = (14783.6006300107 + 14661.4162007857j)
je le divise (1.47836006300107 + 1.46614162007857j)

somme = (-0.450295095941749 + 1.95792517858261j)
z = (-4156.02023055381 - 19646.9804023109j)
je le divise (-0.415602023055381 - 1.96469804023109j)

somme = (-1.52442727946501 - 1.11353785819826j)
z = (-15417.0093466339 + 10882.476519535j)
je le divise (-1.54170093466339 + 1.0882476519535j)

somme = (-1.77062409927231 - 0.0580089708325968j)
z = (-17706.892726426 + 316.339954108408j)
je le divise (-1.7706892726426 + 0.0316339954108408j)

somme = (-0.0324412530119545 + 1.68467636151369j)
z = (-90.5688051565773 - 16844.3990135738j)
je le divise (-0.00905688051565773 - 1.68443990135738j)

somme = (1.45685191813515 + 0.761496580704082j)
z = (14664.8408743737 - 7416.96329031771j)
je le divise (1.46648408743737 - 0.741696329031771j)

somme = (0.489766917806071 - 1.45561138175128j)
z = (4719.96727396979 + 14610.4804238286j)
je le divise (0.471996727396979 + 1.46104804238286j)

somme = (1.29685534199987 - 0.735208880668598j)
z = (12879.5643879093 + 7499.53034105994j)
je le divise (1.28795643879093 + 0.749953034105994j)

somme = (-0.463493712892729 + 1.36114031155162j)
z = (-4485.27371797188 - 13657.9005550646j)
je le divise (-0.448527371797188 - 1.36579005550646j)

somme = (-1.08482104993714 - 0.865213287463158j)
z = (-10934.0906729354 + 8538.40790274315j)
je le divise (-1.09340906729354 + 0.853840790274314j)
```

```
somme = (-0.206809436846205 + 1.30463962387106j)
z = (-1944.6943862165 - 13062.6516991474j)
je le divise (-0.19446943862165 - 1.30626516991474j)

somme = (0.667164123394532 + 1.11140069233914j)
z = (6771.21163236713 - 11050.6412088855j)
je le divise (0.677121163236713 - 1.10506412088855j)

somme = (1.19874112465266 - 0.389555320987856j)
z = (11951.0959434895 + 3998.19052387506j)
je le divise (1.19510959434895 + 0.399819052387506j)

somme = (-0.281999802594023 - 1.17270352318812j)
z = (-2912.21079224693 + 11702.3348047051j)
je le divise (-0.291221079224693 + 1.17023348047051j)

somme = (1.14829127444808 + 0.272386043749717j)
z = (11501.2608065492 - 2636.48553868282j)
je le divise (1.15012608065492 - 0.263648553868282j)

somme = (0.949265535618316 + 0.63818655289566j)
z = (9535.99299649114 - 6313.62045368203j)
je le divise (0.953599299649114 - 0.631362045368203j)

somme = (1.03149690246996 + 0.45160329196766j)
z = (10343.916122049 - 4444.89829608199j)
je le divise (1.0343916122049 - 0.444489829608199j)

somme = (-0.537499138238803 - 0.938119570363166j)
z = (-5432.12947549719 + 9346.4185908873j)
je le divise (-0.543212947549719 + 0.93464185908873j)

somme = (-1.05646244696711 - 0.0114642750944318j)
z = (-10563.630959094 + 53.0381055088568j)
je le divise (-1.0563630959094 + 0.00530381055088568j)

somme = (-0.231342632254291 - 1.01711036000326j)
z = (-2370.38839081759 + 10156.516118182j)
je le divise (-0.237038839081759 + 1.0156516118182j)

somme = (-0.713713413113125 + 0.717243968478433j)
z = (-7098.98331071461 - 7208.32555128659j)
je le divise (-0.709898331071461 - 0.720832555128659j)

somme = (-0.126850142754487 - 0.978824472513123j)
z = (-1315.33425636738 + 9780.80984142756j)
je le divise (-0.131533425636738 + 0.978080984142756j)

somme = (0.29718155559315 + 0.917154208107974j)
z = (3012.26442216475 - 9157.08488122371j)
je le divise (0.301226442216475 - 0.915708488122371j)
```

Lorsqu'on réalise qu'en fait, normalement, la somme doit accumuler les zéros deux par deux, l'un et son conjugué traités ensemble, on modifie le programme, mais à nouveau, l'approximation tombe ;

on réussit à la rétablir cependant :
Voici le programme :

```
import mpmath
from mpmath import sqrt, fadd, fsub, fmul, fdiv, fmul, power, re, im

liste2 = [14.134725142, 21.022039639, 25.010857580, 30.424876126, 32.935061588,
          37.586178159, 40.918719012, 43.327073281, 48.005150881, 49.773832478,
          52.970321478, 56.446247697, 59.347044003, 60.831778525, 65.112544048,
          67.079810529, 69.546401711, 72.067157674, 75.704690699, 77.144840069,
          79.337375020, 82.910380854, 84.735492981, 87.425274613, 88.809111208,
          92.491899271, 94.651344041, 95.870634228, 98.831194218,
          101.317851006, 103.725538040]

nmax = 10000
for b in range(1,len(liste2)):
     somme = 1
     unzero = 0.5+liste2[b]*1j
     lautrezero = 0.5-liste2[b]*1j
     for m in range(2,nmax+1):
          somme = fadd(somme,fdiv(1,m ** unzero))
          somme = fadd(somme,fdiv(1,m ** lautrezero))
     print('= ',somme)
     moinsinv = -1/unzero
     z = fsub((fdiv(moinsinv,fsub(moinsinv,1))*
               (nmax ** fdiv(fsub(moinsinv,1),moinsinv))),
               fdiv(moinsinv,fsub(moinsinv,1)))
     print('z = ',z)
     divise = fmul(2,fdiv(z,nmax))
     print('je le divise par nmax et multiplie le resultat obtenu par 2',divise)
     print('je soustrais 1 a la partie reelle du nombre complexe obtenu
',fsub(re(divise),1))
```

Voici son résultat :

```
somme = (-9.61745285542294 + 0.0j)
z = (-42011.277481029 - 22054.7006014833j)
je le divise par nmax et multiplie le resultat par 2 (-8.4022554962058 -
4.41094012029667j)
enfin, je soustrais 1 a la partie reelle du nombre complexe obtenu -9.4022554962058

somme = (-7.9091053084433 + 0.0j)
z = (-35240.1108748189 + 18735.4739670357j)
je le divise par nmax et multiplie le resultat par 2 (-7.04802217496379 +
3.74709479340713j)
enfin, je soustrais 1 a la partie reelle du nombre obtenu -8.04802217496379

somme = (-4.92354715708489 + 0.0j)
z = (-20410.9324275024 + 25711.3032383404j)
je le divise par nmax et multiplie le resultat par 2 (-4.08218648550047 +
5.14226064766807j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu -5.08218648550047
```

```
somme = (4.95544089775961 + 0.0j)
z = (29567.1526547224 + 6765.63808308653j)
je le divise par nmax et multiplie le resultat par 2 (5.91343053094447 +
1.35312761661731j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu 4.91343053094447

somme = (2.09797537704195 + 0.0j)
z = (16007.7313866147 - 21224.5081219926j)
je le divise par nmax et multiplie le resultat par 2 (3.20154627732295 -
4.24490162439852j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu 2.20154627732295

somme = (-1.49534711227655 + 0.0j)
z = (-1930.93708921621 - 24345.8104048558j)
je le divise par nmax et multiplie le resultat par 2 (-0.386187417843242 -
4.86916208097117j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu -1.38618741784324

somme = (-1.40811406416995 + 0.0j)
z = (-2519.16758315439 + 22928.484928036j)
je le divise par nmax et multiplie le resultat par 2 (-0.503833516630878 +
4.5856969856072j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu -1.50383351663088

somme = (2.01161539645341 + 0.0j)
z = (14783.6006300107 + 14661.4162007857j)
je le divise par nmax et multiplie le resultat par 2 (2.95672012600213 +
2.93228324015715j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu 1.95672012600213

somme = (-1.9005901918835 + 0.0j)
z = (-4156.02023055381 - 19646.9804023109j)
je le divise par nmax et multiplie le resultat par 2 (-0.831204046110763 -
3.92939608046218j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu -1.83120404611076

somme = (-4.04885455893003 + 0.0j)
z = (-15417.0093466339 + 10882.476519535j)
je le divise par nmax et multiplie le resultat par 2 (-3.08340186932677 +
2.176495303907j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu -4.08340186932677

somme = (-4.54124819854464 + 0.0j)
z = (-17706.892726426 + 316.339954108408j)
je le divise par nmax et multiplie le resultat par 2 (-3.5413785452852 +
0.0632679908216815j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu -4.5413785452852

somme = (-1.06488250602387 + 0.0j)
z = (-90.5688051565773 - 16844.3990135738j)
je le divise par nmax et multiplie le resultat par 2 (-0.0181137610313155 -
3.36887980271475j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu -1.01811376103132
```

```
somme = (1.91370383627029 + 0.0j)
z = (14664.8408743737 - 7416.96329031771j)
je le divise par nmax et multiplie le resultat par 2 (2.93296817487474 -
1.48339265806354j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu 1.93296817487474

somme = (-0.0204661643878975 + 0.0j)
z = (4719.96727396979 + 14610.4804238286j)
je le divise par nmax et multiplie le resultat par 2 (0.943993454793959 +
2.92209608476573j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu -0.0560065452060413

somme = (1.59371068399972 + 0.0j)
z = (12879.5643879093 + 7499.53034105994j)
je le divise par nmax et multiplie le resultat par 2 (2.57591287758185 +
1.49990606821199j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu 1.57591287758185

somme = (-1.92698742578546 + 0.0j)
z = (-4485.27371797188 - 13657.9005550646j)
je le divise par nmax et multiplie le resultat par 2 (-0.897054743594376 -
2.73158011101293j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu -1.89705474359438

somme = (-3.16964209987428 + 0.0j)
z = (-10934.0906729354 + 8538.40790274315j)
je le divise par nmax et multiplie le resultat par 2 (-2.18681813458708 +
1.70768158054863j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu -3.18681813458708

somme = (-1.41361887369239 + 0.0j)
z = (-1944.6943862165 - 13062.6516991474j)
je le divise par nmax et multiplie le resultat par 2 (-0.3889388772433 -
2.61253033982948j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu -1.3889388772433

somme = (0.334328246789071 + 0.0j)
z = (6771.21163236713 - 11050.6412088855j)
je le divise par nmax et multiplie le resultat par 2 (1.35424232647343 -
2.21012824177711j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu 0.354242326473425

somme = (1.39748224930532 + 0.0j)
z = (11951.0959434895 + 3998.19052387506j)
je le divise par nmax et multiplie le resultat par 2 (2.3902191886979 +
0.799638104775012j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu 1.3902191886979

somme = (-1.56399960518803 + 0.0j)
z = (-2912.21079224693 + 11702.3348047051j)
je le divise par nmax et multiplie le resultat par 2 (-0.582442158449386 +
2.34046696094102j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu -1.58244215844939
```

```
somme = (1.29658254889617 + 0.0j)
z = (11501.2608065492 - 2636.48553868282j)
je le divise par nmax et multiplie le resultat par 2 (2.30025216130984 -
0.527297107736564j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu 1.30025216130984

somme = (0.898531071236611 + 0.0j)
z = (9535.99299649114 - 6313.62045368203j)
je le divise par nmax et multiplie le resultat par 2 (1.90719859929823 -
1.26272409073641j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu 0.907198599298229

somme = (1.06299380493992 + 0.0j)
z = (10343.916122049 - 4444.89829608199j)
je le divise par nmax et multiplie le resultat par 2 (2.06878322440981 -
0.888979659216398j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu 1.06878322440981

somme = (-2.07499827647761 + 0.0j)
z = (-5432.12947549719 + 9346.4185908873j)
je le divise par nmax et multiplie le resultat par 2 (-1.08642589509944 +
1.86928371817746j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu -2.08642589509944

somme = (-3.11292489393422 + 0.0j)
z = (-10563.630959094 + 53.0381055088568j)
je le divise par nmax et multiplie le resultat par 2 (-2.1127261918188 +
0.0106076211017714j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu -3.1127261918188

somme = (-1.46268526450858 + 0.0j)
z = (-2370.38839081759 + 10156.516118182j)
je le divise par nmax et multiplie le resultat par 2 (-0.474077678163518 +
2.03130322363641j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu -1.47407767816352

somme = (-2.42742682622626 + 0.0j)
z = (-7098.98331071461 - 7208.32555128659j)
je le divise par nmax et multiplie le resultat par 2 (-1.41979666214292 -
1.44166511025732j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu -2.41979666214292

somme = (-1.25370028550896 + 0.0j)
z = (-1315.33425636738 + 9780.80984142756j)
je le divise par nmax et multiplie le resultat par 2 (-0.263066851273476 +
1.95616196828551j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu -1.26306685127348

somme = (-0.405636888813719 + 0.0j)
z = (3012.26442216475 - 9157.08488122371j)
je le divise par nmax et multiplie le resultat par 2 (0.60245288443295 -
1.83141697624474j)
enfin, je soustrais 1 de la partie reelle du nombre obtenu -0.39754711556705
```

De l'importance d'une phrase (d'un livre) (Denise Vella-Chemla, 9 avril 2024)

J'ai trouvé très récemment une formule, de façon totalement hasardeuse. La voici :

$$\sum_{n=1}^{N} n^{-\frac{1}{k}} \simeq \frac{k}{k-1} N^{\frac{k-1}{k}} - \frac{k}{k-1}.$$

Je l'ai utilisée dans un programme, dans lequel je l'appliquais pour calculer les valeurs d'une fonction que je croyais être la fonction ζ de Riemann, uniquement pour les complexes dits "zéros non triviaux de ζ", c'est-à-dire que la formule était appliquée seulement aux complexes de la forme $0.5 + b\,i$ avec b prenant les valeurs bien connues des dits zéros tronqués à la dixième décimale, dont voici les premiers

14.134725142,
21.022039639,
25.010857580,
30.424876126,
32.935061588,
37.586178159,
40.918719012,
43.327073281,
48.005150881,
....

Le programme en question était satisfaisant, dans le sens où les deux calculs qu'il effectuait donnaient le même résultat ; mais par ailleurs, il n'était pas satisfaisant parce que la fonction, qu'on pensait être la fonction ζ de Riemann, ainsi calculée, ne semblait pas s'annuler en les zéros non triviaux : en effet, les premières valeurs trouvées par les deux calculs étaient :

```
somme = (47.0681146614588 + 6.79233817958577j)
z = (47230573.132808 - 4542248.21847271j)
je le divise (47.230573132808 - 4.54224821847271j)

somme = (-0.696474171821543 + 39.9685904584189j)
z = (897012.922192707 - 39900840.876562j)
je le divise (0.897012922192707 - 39.900840876562j)

somme = (-19.1421254242806 + 26.712972229514j)
z = (-18235723.8351254 - 27297140.8614905j)
je le divise (-18.2357238351254 - 27.2971408614905j)

somme = (14.5829047512835 - 26.6275286136424j)
z = (13756410.0563313 + 27032410.7387761j)
je le divise (13.7564100563313 + 27.0324107387761j)

somme = (-21.2101595879565 - 16.0579637189287j)
z = (-21613929.77586 + 15477933.0403448j)
je le divise (-21.61392977586 + 15.4779330403448j)
```

```
somme = (-3.92806915960099 + 24.1191025784809j)
z = (-3336400.6682091 - 24193317.6027189j)
je le divise (-3.3364006682091 - 24.1933176027189j)

somme = (22.9020972754169 - 2.84983368903822j)
z = (22818190.5809835 + 3375017.62841979j)
je le divise (22.8181905809835 + 3.37501762841979j)

somme = (-7.14368903401133 - 19.5666935382541j)
z = (-7545774.20271016 + 19405480.5169969j)
je le divise (-7.54577420271016 + 19.4054805169969j)

somme = (6.84748368383507 - 18.8868955441334j)
z = (6464703.07811775 + 19012752.0800898j)
je le divise (6.46470307811775 + 19.0127520800898j)

somme = (3.18608609463471 - 18.6068506563752j)
z = (2833889.71322124 + 18656932.0938899j)
je le divise (2.83388971322124 + 18.6569320938899j)
```

Et c'est là qu'intervient LA phrase (il y a 3 phrases en fait, mais c'est la dernière des trois qui importe), trouvée dans le livre de Piergiorgio Odifreddi, *Les mathématiques à l'aube du* XXI$^{\text{ième}}$ *siècle*, à la page 151 :

> *La relation entre la fonction ζ de Riemann et les nombres premiers transparaît déjà dans la démonstration précédente d'Euler, montrant que pour z inférieur ou égal à un, la fonction ζ est infinie. C'est la raison pour laquelle Riemann étendit la définition de ζ des nombres réels aux nombres complexes à l'aide d'une technique dite de prolongement analytique.* GROSSO MODO, ON DÉFINIT LA VALEUR DE ζ NON PAS COMME LIMITE DES SOMMES PARTIELLES MAIS DE LEURS MOYENNES.

Pour faire calculer ce que propose cette phrase, on modifie notre programme pour lui faire imprimer également les moyennes des sommes calculées au fur et à mesure des zéros, et pour obtenir la concordance avec notre "somme-éclair", on divise la somme-éclair (qui consiste à soustraire la valeur en 0 à la valeur en $nmax$ [1]) par le carré de $nmax$. Et là, joie, non seulement la somme-éclair se comporte bien, au sens où elle trouve un résultat très proche de la moyenne des sommes partielles, mais d'autre part, elle est rassurante car elle permet effectivement de trouver des valeurs "informatiquement nulles" pour les zéros non triviaux, ce qu'on espérait bien trouver.

[1] le plus grand entier qu'on considère ; on a pris $nmax = 1\,000\,000$.

```
import mpmath
from mpmath import sqrt, fadd, fsub, fmul, fdiv, fmul, power

liste2 = [ 14.134725142,  21.022039639,   25.010857580,   30.424876126,   32.935061588,
           37.586178159,   40.918719012,   43.327073281,   48.005150881,   49.773832478,
           52.970321478,   56.446247697,   59.347044003,   60.831778525,   65.112544048,
           67.079810529,   69.546401711,   72.067157674,   75.704690699,   77.144840069,
           79.337375020,   82.910380854,   84.735492981,   87.425274613,   88.809111208,
           92.491899271,   94.651344041,   95.870634228,   98.831194218,
           101.317851006,   103.725538040,...]
nmax = 1000
for b in range(1,len(liste2)):
     somme = 1
     unzero = 0.5+liste2[b]*1j
     for m in range(2,nmax+1):
          somme = fadd(somme,fdiv(1,m ** unzero))
     print('= ',somme)
     moinsinv = -1/unzero
     z = fsub((fdiv(moinsinv,fsub(moinsinv,1))*(nmax ** fdiv(fsub(moinsinv,1),moinsinv))),
                    fdiv(moinsinv,fsub(moinsinv,1)))
     print('z = ',z)
     print('je le divise par le carre de nmax ',fdiv(z,nmax))
```

Voyons ci-dessous le début du résultat de ce programme, dont l'entièreté est stockée ici : resultat-calcul-eclair :

```
somme = (47.0681146614588 + 6.79233817958577j)
moyenne = (4.70681617296206e-5 + 6.79234497193074e-6j)
z = (47230573.132808 - 4542248.21847271j)
je le divise par le carre de nmax (4.7230573132808e-5 - 4.54224821847271e-6j)

somme = (-0.696474171821543 + 39.9685904584189j)
moyenne = (-6.96474868296411e-7 + 3.99686304270493e-5j)
z = (897012.922192707 - 39900840.876562j)
je le divise par le carre de nmax (8.97012922192707e-7 - 3.9900840876562e-5j)

somme = (-19.1421254242806 + 26.712972229514j)
moyenne = (-1.91421445664252e-5 + 2.67129989425129e-5j)
z = (-18235723.8351254 - 27297140.8614905j)
je le divise par le carre de nmax (-1.82357238351254e-5 - 2.72971408614905e-5j)

somme = (14.5829047512835 - 26.6275286136424j)
moyenne = (1.45829193342028e-5 - 2.66275552411977e-5j)
z = (13756410.0563313 + 27032410.7387761j)
je le divise par le carre de nmax (1.37564100563313e-5 + 2.70324107387761e-5j)

somme = (-21.2101595879565 - 16.0579637189287j)
moyenne = (-2.12101807981373e-5 - 1.60579797769085e-5j)
z = (-21613929.77586 + 15477933.0403448j)
je le divise par le carre de nmax (-2.161392977586e-5 + 1.54779330403448e-5j)
```

```
somme = (-3.92806915960099 + 24.1191025784809j)
moyenne = (-3.92807308767408e-6 + 2.41191266976076e-5j)
z = (-3336400.6682091 - 24193317.6027189j)
je le divise par le carre de nmax (-3.3364006682091e-6 - 2.41933176027189e-5j)

somme = (22.9020972754169 - 2.84983368903822j)
moyenne = (2.29021201775371e-5 - 2.84983653887476e-6j)
z = (22818190.5809835 + 3375017.62841979j)
je le divise par le carre de nmax (2.28181905809835e-5 + 3.37501762841979e-6j)

somme = (-7.14368903401133 - 19.5666935382541j)
moyenne = (-7.14369617770751e-6 - 1.95667131049672e-5j)
z = (-7545774.20271016 + 19405480.5169969j)
je le divise par le carre de nmax (-7.54577420271016e-6 + 1.94054805169969e-5j)

somme = (6.84748368383507 - 18.8868955441334j)
moyenne = (6.84749053132561e-6 - 1.88869144310478e-5j)
z = (6464703.07811775 + 19012752.0800898j)
je le divise par le carre de nmax (6.46470307811775e-6 + 1.90127520800898e-5j)

somme = (3.18608609463471 - 18.6068506563752j)
moyenne = (3.18608928072399e-6 - 1.86068692632445e-5j)
z = (2833889.71322124 + 18656932.0938899j)
je le divise par le carre de nmax (2.83388971322124e-6 + 1.86569320938899e-5j)

somme = (11.7825798704793 + 13.2288290445883j)
moyenne = (1.17825916530709e-5 + 1.32288422734306e-5j)
z = (12010862.584625 - 13014348.7210121j)
je le divise par le carre de nmax (1.2010862584625e-5 - 1.30143487210121e-5j)

somme = (0.631960122209203 - 16.8375897198238j)
moyenne = (6.31960754169957e-7 - 1.68376065574304e-5j)
z = (348657.883980638 + 16841050.6294031j)
je le divise par le carre de nmax (3.48657883980638e-7 + 1.68410506294031e-5j)

somme = (-16.4140031666246 + 0.892046353471715j)
moyenne = (-1.64140195806441e-5 + 8.92047245518961e-7j)
z = (-16392729.7678544 - 1160848.24120904j)
je le divise par le carre de nmax (-1.63927297678544e-5 - 1.16084824120904e-6j)

somme = (13.510214029535 + 7.30268592082983j)
moyenne = (1.35102275397625e-5 + 7.30269322352306e-6j)
z = (13617297.6138118 - 7093164.98835927j)
je le divise par le carre de nmax (1.36172976138118e-5 - 7.09316498835927e-6j)

somme = (0.305800002544884 - 14.9040679191871j)
moyenne = (3.05800308345192e-7 - 1.49040828232699e-5j)
z = (84124.8942214654 + 14903651.9920264j)
je le divise par le carre de nmax (8.41248942214654e-8 + 1.49036519920264e-5j)

somme = (-6.90706408638652 + 12.6108816440201j)
moyenne = (-6.90707099345751e-6 + 1.26108942549144e-5j)
z = (-6724116.99967722 - 12706005.1911874j)
je le divise par le carre de nmax (-6.72411699967722e-6 - 1.27060051911874e-5j)
```

```
somme = (3.20815904609181 - 13.499645409885j)
moyenne = (3.20816225425406e-6 - 1.34996589095439e-5j)
z = (3020480.79743856 + 13540132.9874013j)
je le divise par le carre de nmax (3.02048079743856e-6 + 1.35401329874013e-5j)

somme = (3.20080523043151 - 12.8152582986173j)
moyenne = (3.20080843123994e-6 - 1.28152711138884e-5j)
z = (3031240.47735094 + 12854051.1558598j)
je le divise par le carre de nmax (3.03124047735094e-6 + 1.28540511558598e-5j)

somme = (-9.316335547442 - 9.0126959478554j)
moyenne = (-9.31634486378686e-6 - 9.01270496056036e-6j)
z = (-9430427.12662873 + 8890068.18516894j)
je le divise par le carre de nmax (-9.43042712662873e-6 + 8.89006818516894e-6j)

somme = (4.00253776361222 - 11.9517512323155j)
moyenne = (4.00254176615399e-6 - 1.19517631840786e-5j)
z = (3851468.48285356 + 11999179.8670751j)
je le divise par le carre de nmax (3.85146848285356e-6 + 1.19991798670751e-5j)

somme = (11.3511595755998 - 4.07662686242621j)
moyenne = (1.13511709267707e-5 - 4.07663093905715e-6j)
z = (11299702.2645788 + 4212132.11350525j)
je le divise par le carre de nmax (1.12997022645788e-5 + 4.21213211350525e-6j)

somme = (10.7427095397872 - 4.88499390502232j)
moyenne = (1.07427202825075e-5 - 4.88499879002111e-6j)
z = (10683043.7311247 + 5010259.4645182j)
je le divise par le carre de nmax (1.06830437311247e-5 + 5.0102594645182e-6j)

somme = (11.3667356666101 + 1.27621483368795j)
moyenne = (1.13667470333571e-5 + 1.27621610990406e-6j)
z = (11379046.0917562 - 1146483.23468877j)
je le divise par le carre de nmax (1.13790460917562e-5 - 1.14648323468877e-6j)

somme = (11.1215183089566 - 1.76007408467139j)
moyenne = (1.11215294304861e-5 - 1.76007584474724e-6j)
z = (11099671.7085907 + 1884439.86564631j)
je le divise par le carre de nmax (1.10996717085907e-5 + 1.8844398656463e-6j)

somme = (7.75536984932505 - 7.53292670004491j)
moyenne = (7.75537760470265e-6 - 7.53293423297914e-6j)
z = (7672937.8611855 + 7615076.61821918j)
je le divise par le carre de nmax (7.6729378611855e-6 + 7.61507661821918e-6j)

somme = (7.27404261850562 + 7.66200880435917j)
moyenne = (7.27404989255551e-6 + 7.66201646637564e-6j)
z = (7353393.7462063 - 7584240.7447512j)
je le divise par le carre de nmax (7.3533937462063e-6 - 7.5842407447512e-6j)

somme = (-9.88215228578014 + 3.33768441989347j)
moyenne = (-9.88216216794231e-6 + 3.33768775758122e-6j)
z = (-9845896.40408981 - 3439719.77237551j)
je le divise par le carre de nmax (-9.84589640408981e-6 - 3.43971977237551e-6j)
```

```
somme = (9.37173265349585 - 3.81409241635485j)
moyenne = (9.37174202523788e-6 - 3.81409623045108e-6j)
z = (9331901.45989881 + 3907848.53547083j)
je le divise par le carre de nmax (9.33190145989881e-6 + 3.90784853547083e-6j)

somme = (-9.70447005376166 + 1.7990099078026j)
moyenne = (-9.70447975824142e-6 + 1.79901170681431e-6j)
z = (-9685393.64289666 - 1894017.39538421j)
je le divise par le carre de nmax (-9.68539364289666e-6 - 1.89401739538421e-6j)

somme = (4.27901190526987 + 8.63906796039762j)
moyenne = (4.27901618428605e-6 + 8.63907659947422e-6j)
z = (4361238.86339807 - 8596843.21405815j)
je le divise par le carre de nmax (4.36123886339807e-6 - 8.59684321405815e-6j)

somme = (-7.40056740739068 + 5.93007999052512j)
moyenne = (-7.40057480796549e-6 + 5.93008592061104e-6j)
z = (-7343657.33792884 - 5999060.34169033j)
je le divise par le carre de nmax (-7.34365733792884e-6 - 5.99906034169033e-6j)
```

C'est n'importe quoi : je n'ai pas calculé des moyennes de sommes partielles : en divisant par $nmax$, pour un zéro de partie imaginaire donnée (14.134725 au hasard), j'ai calculé la moyenne des diverses fractions $\frac{1}{2^s}$, $\frac{1}{3^s}$, $\frac{1}{5^s}$, etc.

Je ne sais pas pourquoi la formule que j'ai appelée "somme-éclair" calcule directement un résultat vraiment proche : c'est comme si les fractions successives étaient écartées régulièrement, ce que je ne crois pas être le cas.

Penser à acheter des éponges, à force de les jeter, on finit par en manquer...

Expression d'une assertion impliquant la conjecture de Goldbach dans $\mathbb{C}$

L'assertion mathématique ci-dessous exprime le fait que n, un nombre pair supérieur ou égal à 6, possède un décomposant de Goldbach x (i.e. un nombre premier tel que $n-x$ est premier également).

C'est une assertion plus forte que la conjecture de Goldbach (elle implique la conjecture) dans la mesure où le nombre premier x que définit l'assertion est compris entre $\sqrt{n}$ et $n/2$. Les nombres premiers inférieurs à $\sqrt{n}$ dont le complémentaire est premier ne vérifient pas l'assertion (a).

L'assertion (a) exprime le fait que x est un nombre premier compris entre $\sqrt{n}$ et $n/2$ et l'assertion b exprime le fait que $n-x$ est un nombre premier également.

ε doit être "suffisamment petit". Une valeur de 10^{-10} convient pour détecter les décomposants de Goldbach des nombres 6 à 100 par exemple.

$$\forall n \geq 6, \exists x \geq 3 \,/$$

$$\left| \prod_{\substack{2 \leq x \leq \frac{n}{2} \\ p \in \mathbb{N} \\ 2 \leq p \leq \sqrt{n}}} \left(1 - \exp\left(\frac{2i\pi x}{p}\right)\right) \right| \quad > \varepsilon \qquad \text{(a)}$$

et

$$\left| \prod_{\substack{2 \leq x \leq \frac{n}{2} \\ p \in \mathbb{N} \\ 2 \leq p \leq \sqrt{n}}} \left(1 - \exp\left(\frac{2i\pi (n-x)}{p}\right)\right) \right| \quad > \varepsilon \qquad \text{(b)}$$

On peut réécrire les exponentielles en utilisant la racine p-ième de -1 (notée $\sqrt[p]{-1}$) ainsi :

$$\forall n \geq 6, \exists x \geq 3 \,/$$

$$\left| \prod_{\substack{2 \leq x \leq \frac{n}{2} \\ p \in \mathbb{N} \\ 2 \leq p \leq \sqrt{n}}} \left(1 - \left(\sqrt[p]{-1}\right)^{4x}\right) \right| \quad > \varepsilon \qquad \text{(a)}$$

et

$$\left| \prod_{\substack{2 \leq x \leq \frac{n}{2} \\ p \in \mathbb{N} \\ 2 \leq p \leq \sqrt{n}}} \left(1 - \left(\sqrt[p]{-1}\right)^{4(n-x)}\right) \right| \quad > \varepsilon \qquad \text{(b)}$$

Le programme qui trouve les décompositions de Goldbach des nombres pairs successifs de 6 à 100 est très court. On peut le lire ci-dessous.

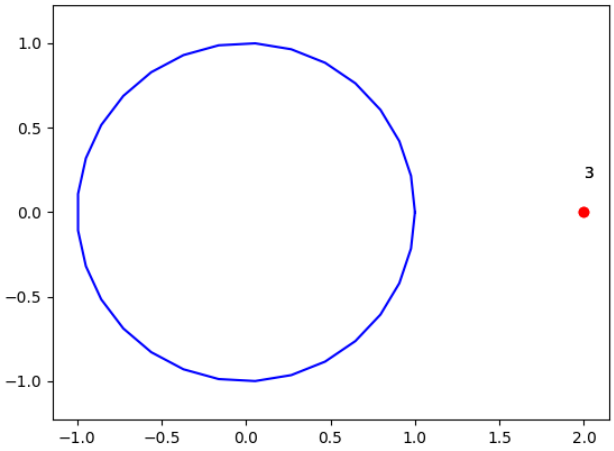
On fournit après le programme les images qui montrent où se placent les nombres premiers, dont certains fournissent des décompositions de Goldbach, en dehors du cercle-unité. La position d'un nombre relativement à la position du cercle-unité est modifiée à chaque traversée d'un carré parfait.

```
from cmath import *
import numpy as np
from numpy import exp, pi, sqrt, linspace, cos, sin
import matplotlib.pyplot as plt

for n in range(6,103,2):
     theta = linspace(0,2*pi,30)
     r = 1
     a = r*cos(theta)
     b = r*sin(theta)
     z = a+1j*b
     plt.plot(a,b, color='blue')
     racine = int(sqrt(n))
     for x in range(2,n//2+1):
          prodbas = 1
          prodhaut = 1
          for p in range(2,racine+1):
               xx = 2*pi*x/p
               letout = exp(2*pi*1j*n/p)
               lun = exp(xx*1j)
               prodbas = prodbas*(1-lun)
               produit = letout/lun
               prodhaut = prodhaut*(1-produit)
          if abs(prodbas) > pow(10,-10) and abs(prodhaut) > pow(10,-10):
               print(x, ' dg de ',n)
               plt.scatter(prodbas.real, prodbas.imag, color='red')
               plt.annotate(x,xy=(prodbas.real, prodbas.imag+0.2))
               plt.scatter(prodhaut.real, prodhaut.imag, color='red')
               plt.annotate(n-x,xy=(prodhaut.real, prodhaut.imag+0.2))
     plt.axis('equal')
     plt.show()
```

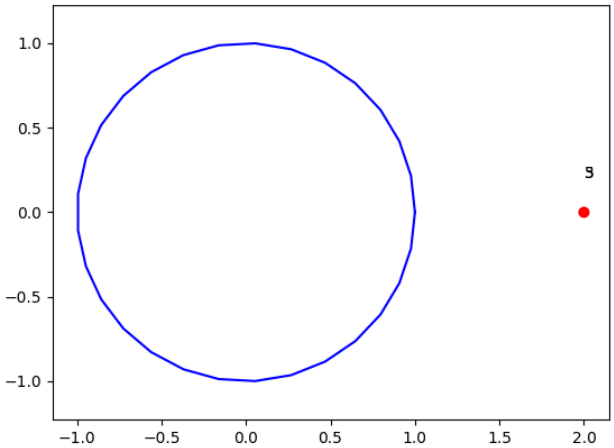
Note pour les programmeuses : Python a des réactions bizarres par rapport aux types des variables : il calcule correctement en remplaçant

$$\begin{array}{rl} \exp(2i\pi x/p) & \text{par} \\ \text{power}(\text{power}(-1,1/p),2*x) & \text{ou bien encore par} \\ \text{power}(\text{power}(-1,1/p),2*x) & \text{ou enfin par} \\ \text{power}(\exp(\log(-1)/p),2*x) & \end{array}$$

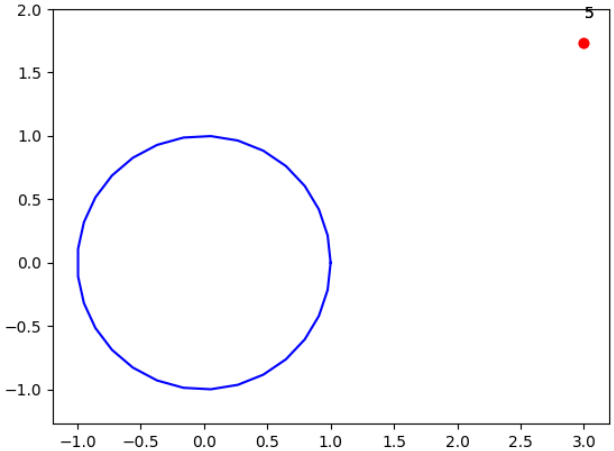
en prenant la fonction *power* dans le module `mpmath` (i.e. cette fonction travaille sur des complexes) mais on ne peut pas intervertir les exposants, la racine p-ième de 1 valant toujours 1 (*rappel* : selon la belle formule d'Euler, $log(-1) = i\pi$), en python, *log* désigne le logarithme népérien.


1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0
1.5
2.0

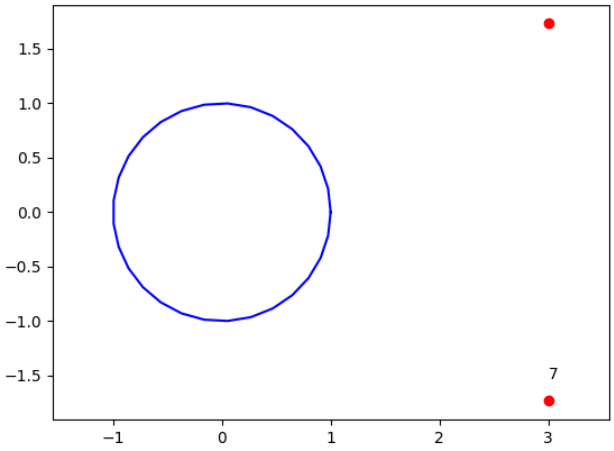
n=6


1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0
1.5
2.0

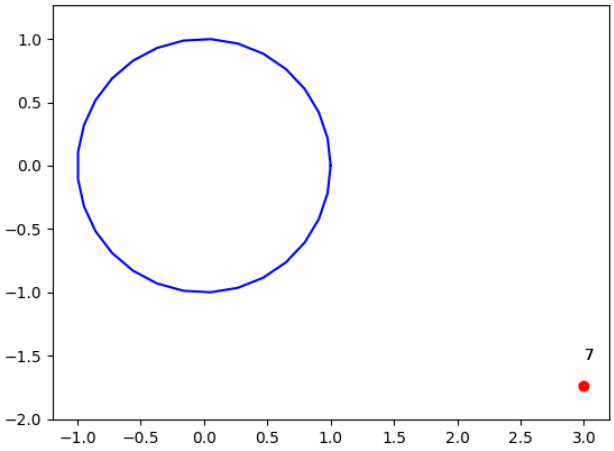
n=8


2.0
1.5
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0
1.5
2.0
2.5
3.0

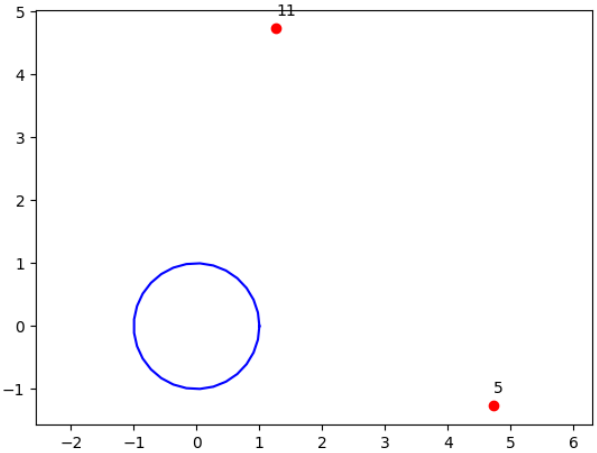
n=10



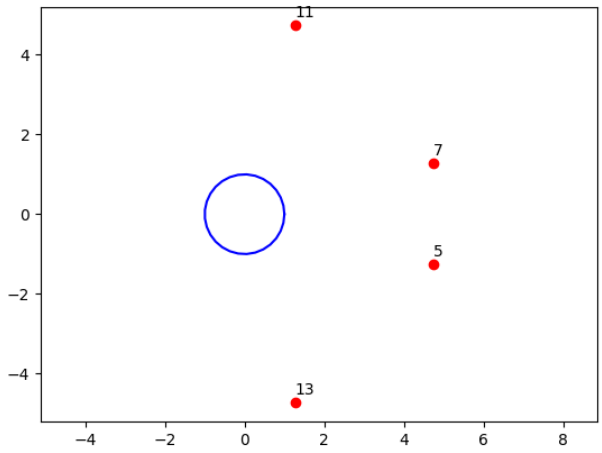
n=12



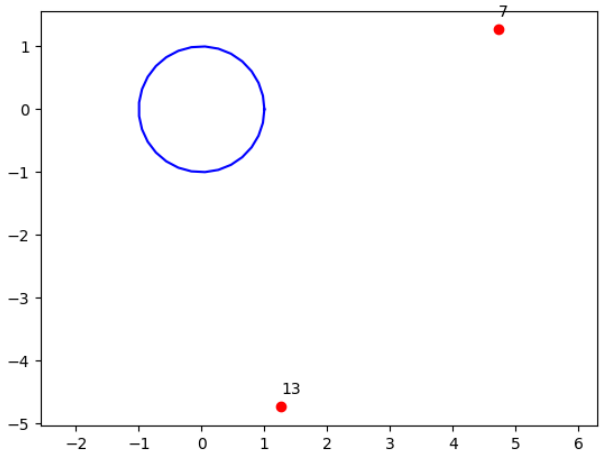
n=14



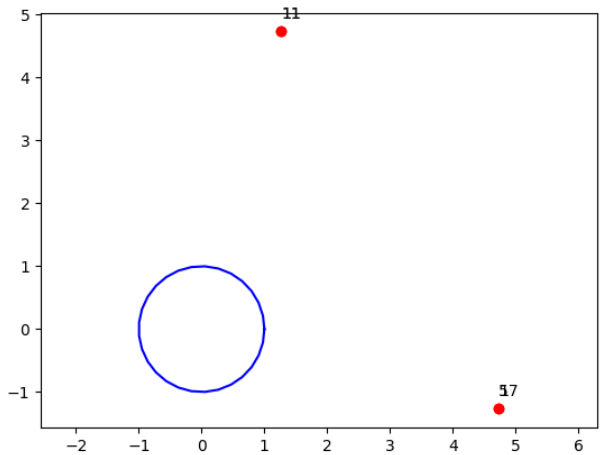
n=16



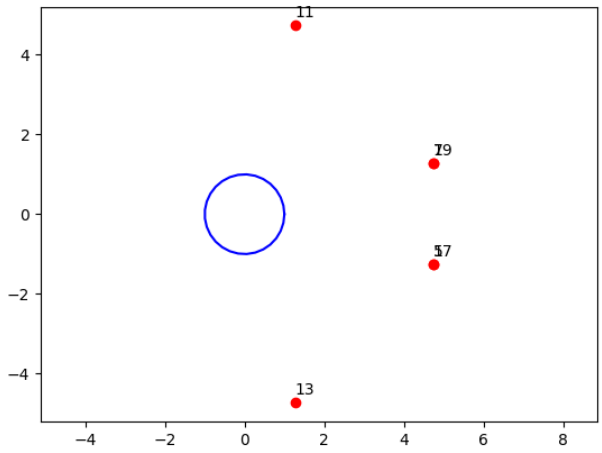
n=18



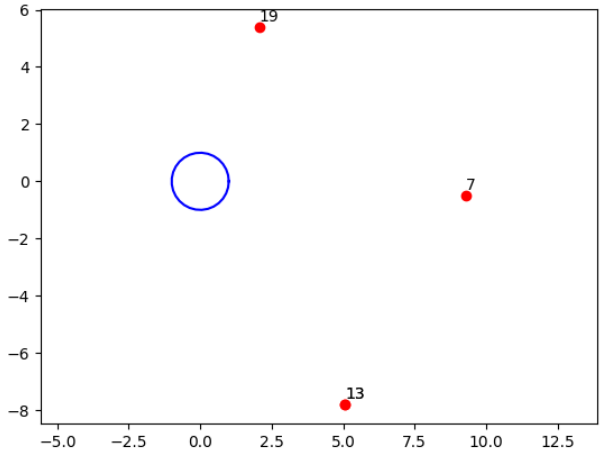
n=20



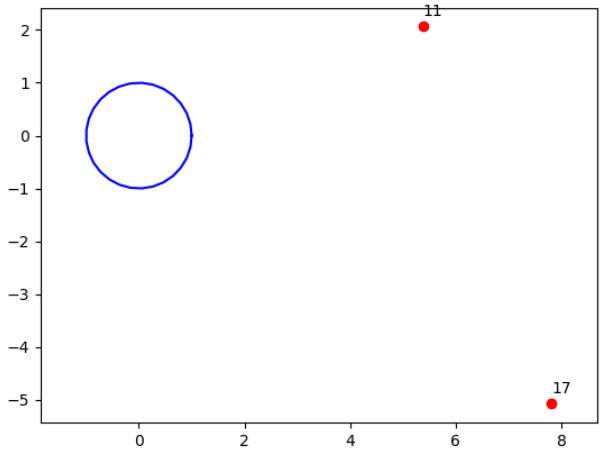
n=22



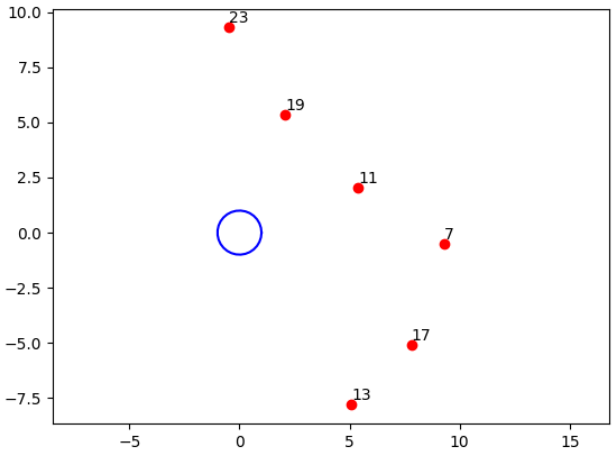
n=24



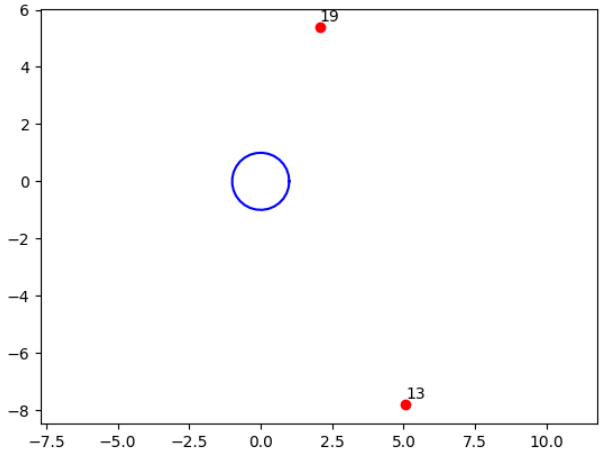
n=26



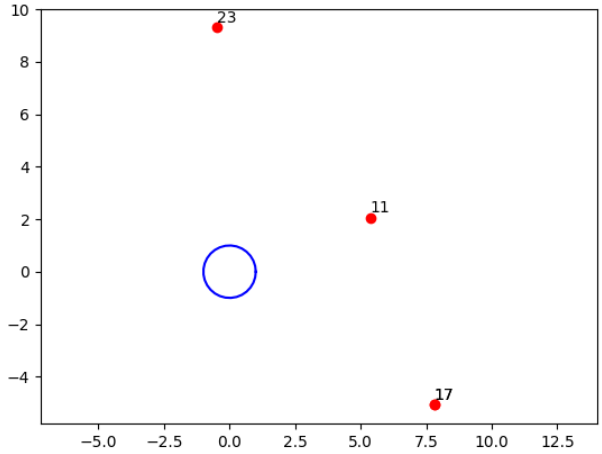
n=28



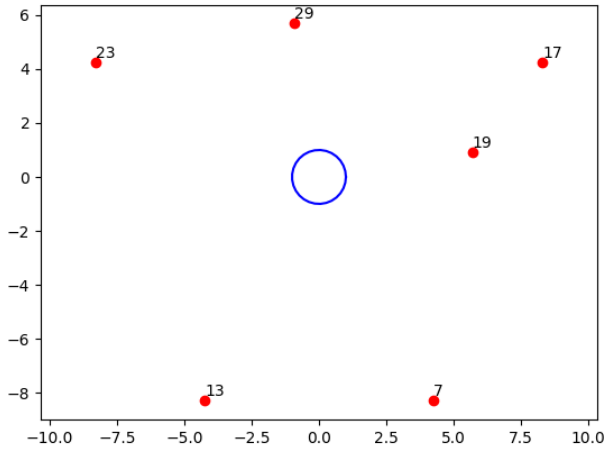
n=30



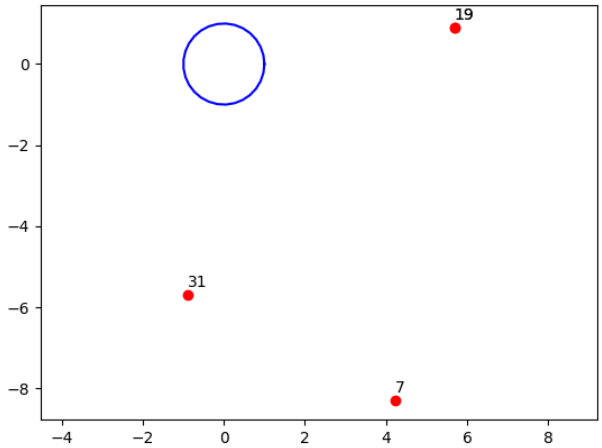
n=32



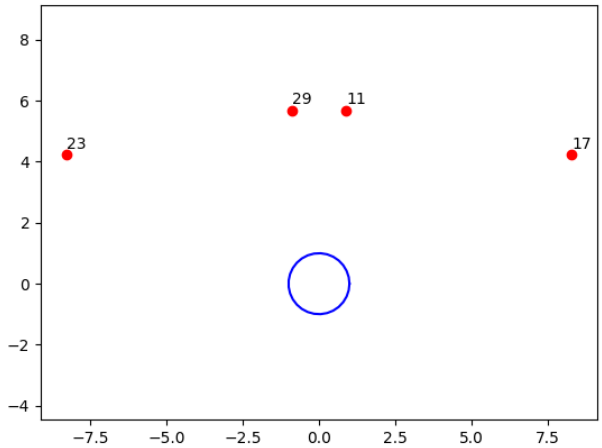
n=34



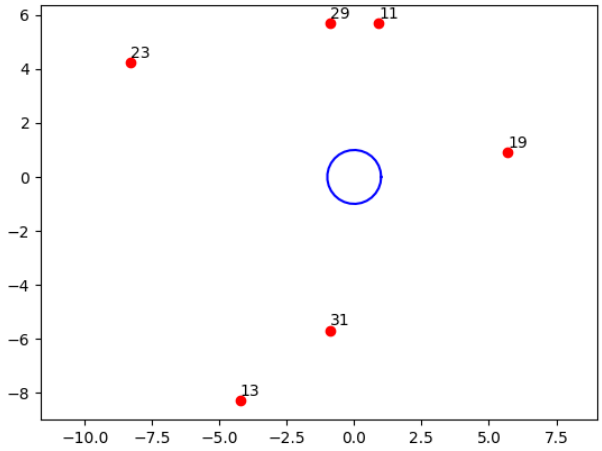
n=36



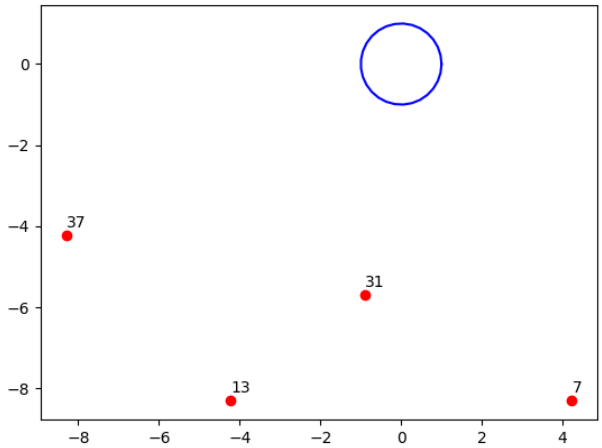
n=38



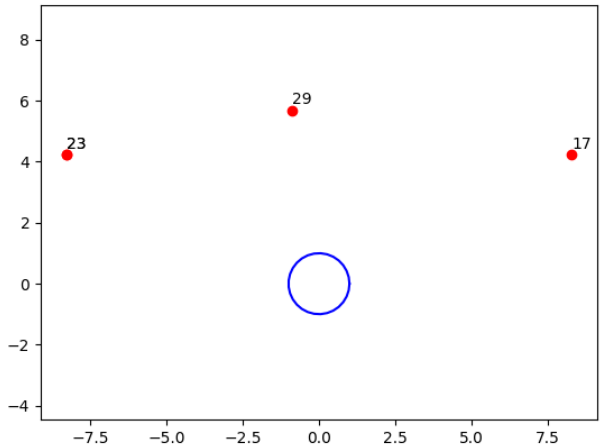
n=40



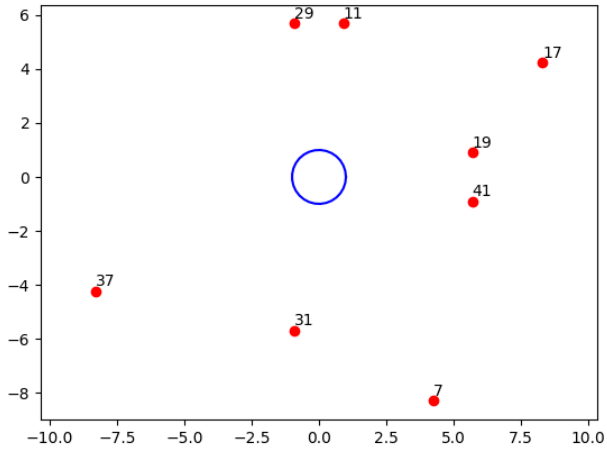
n=42



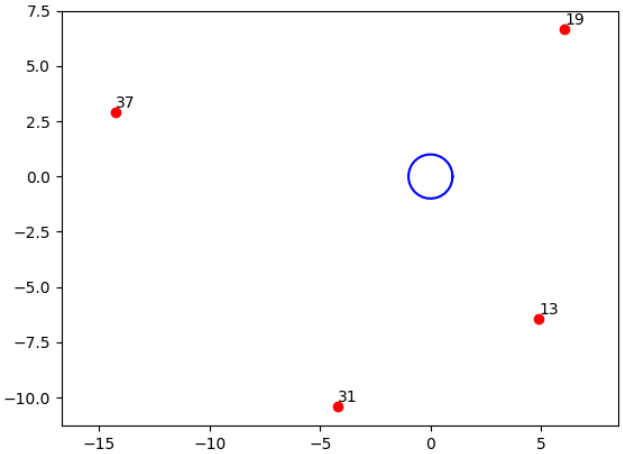
n=44



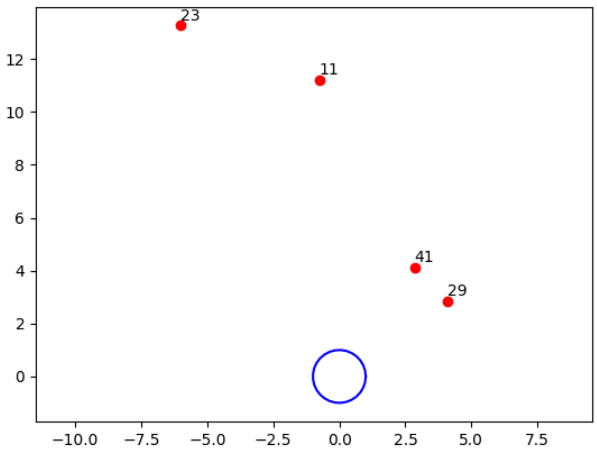
n=46



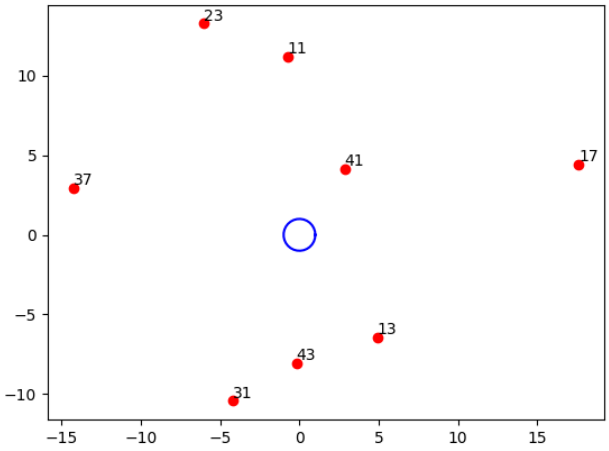
n=48



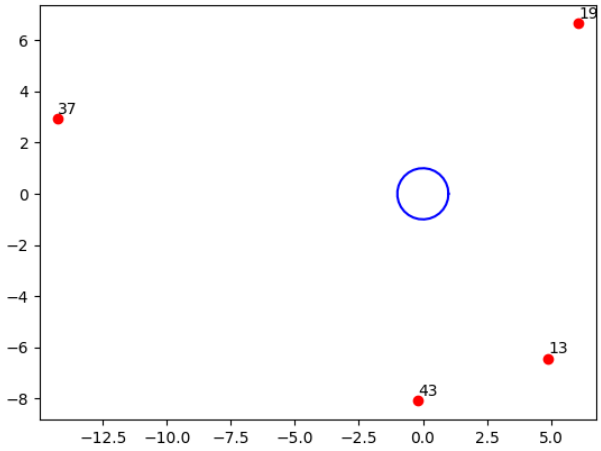
n=50



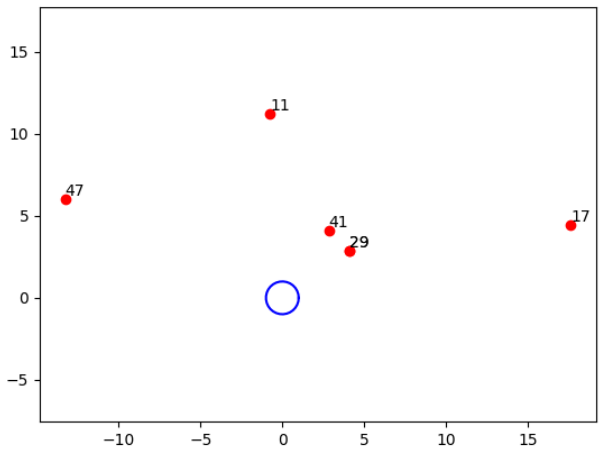
n=52


23
11
41
17
37
13
43
31
10
5
0
−5
−10
−15
−10
−5
0
5
10
15

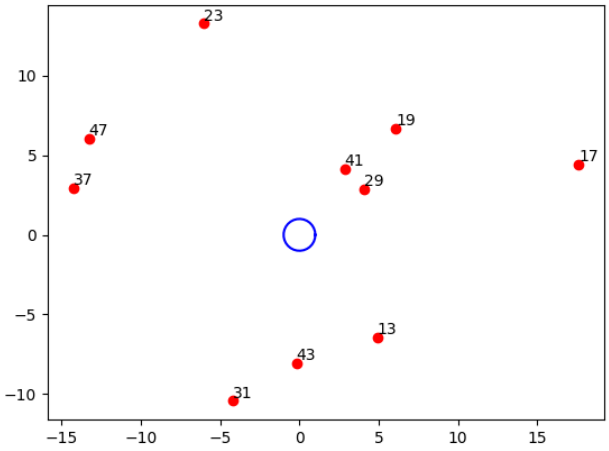
n=54


19
37
13
43
6
4
2
0
−2
−4
−6
−8
−12.5
−10.0
−7.5
−5.0
−2.5
0.0
2.5
5.0

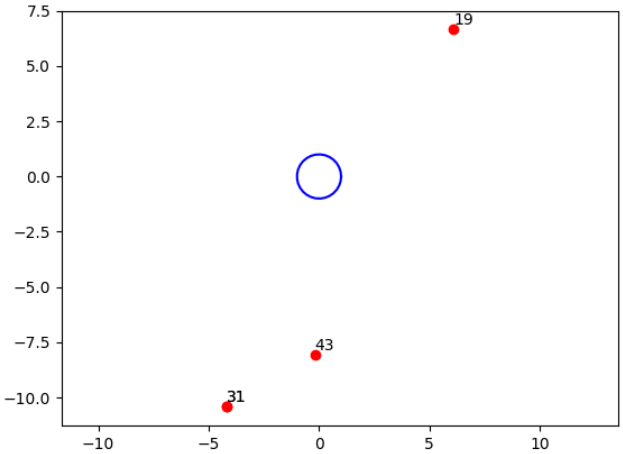
n=56


11
47
41
29
17
15
10
5
0
−5
−10
−5
0
5
10
15

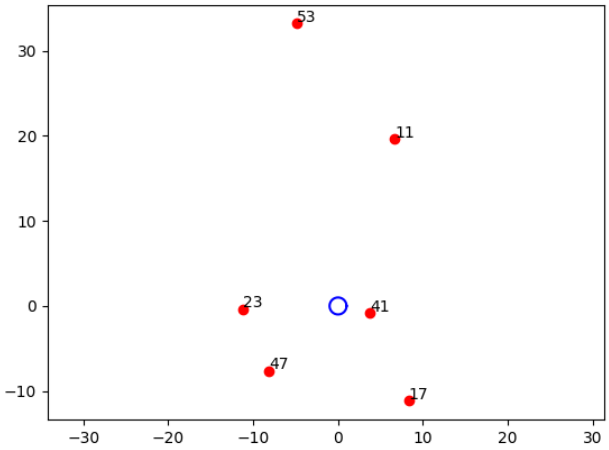
n=58


23
47
19
41
17
37
29
13
43
31
10
5
0
−5
−10
−15
−10
−5
0
5
10
15

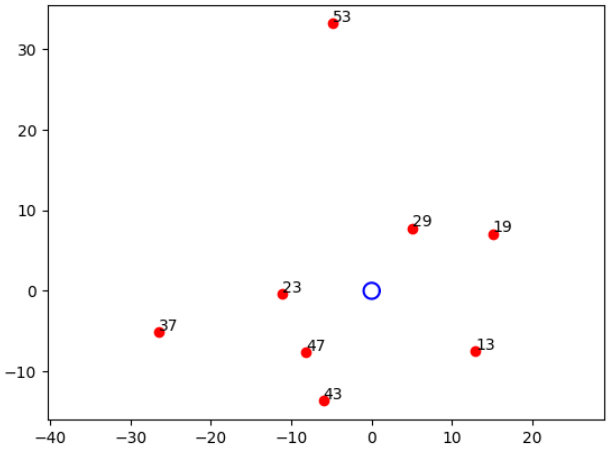
n=60


19
43
31
7.5
5.0
2.5
0.0
−2.5
−5.0
−7.5
−10.0
−10
−5
0
5
10

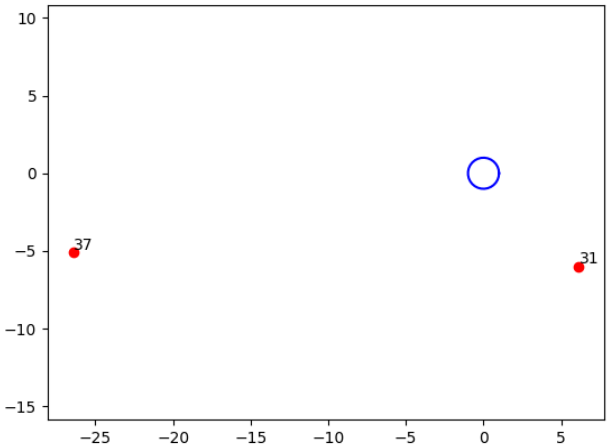
n=62


53
11
23
41
47
17
30
20
10
0
−10
−30
−20
−10
0
10
20
30

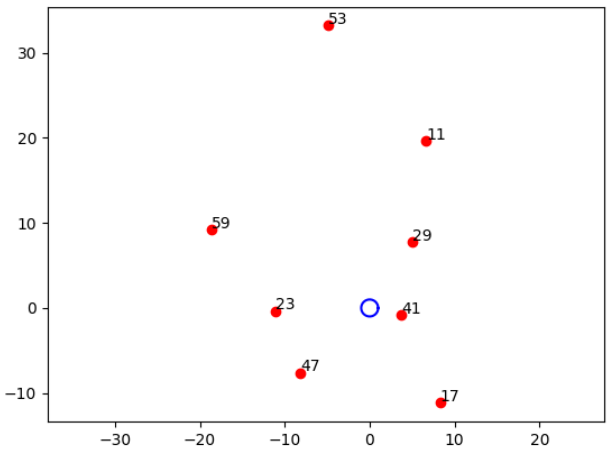
n=64


53
29
19
23
37
47
13
43
30
20
10
0
−10
−40
−30
−20
−10
0
10
20

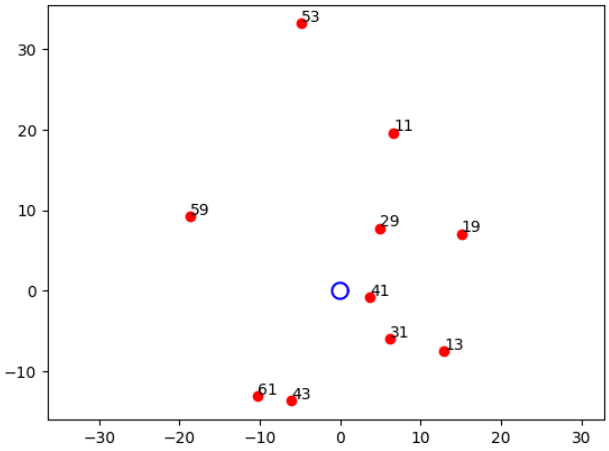
n=66


37
31
10
5
0
−5
−10
−15
−25
−20
−15
−10
−5
0
5

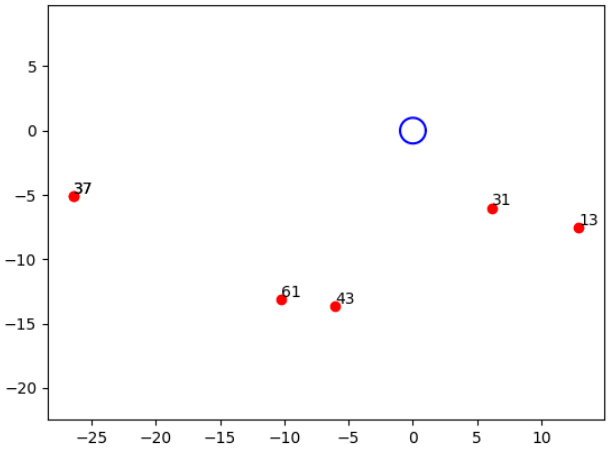
n=68


53
11
59
29
23
41
47
17
30
20
10
0
−10
−30
−20
−10
0
10
20

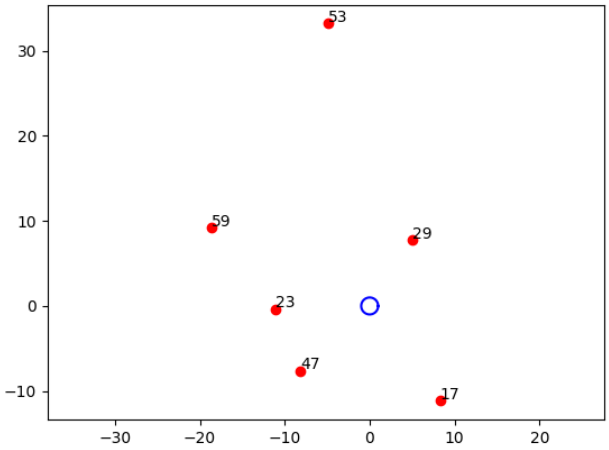
n=70


53
11
59
29
19
41
31
13
61
43
30
20
10
0
−10
−30
−20
−10
0
10
20
30

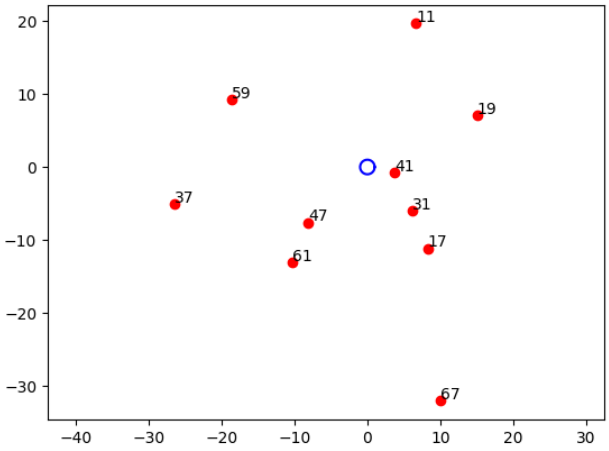
n=72


37
31
13
61
43
5
0
−5
−10
−15
−20
−25
−20
−15
−10
−5
0
5
10

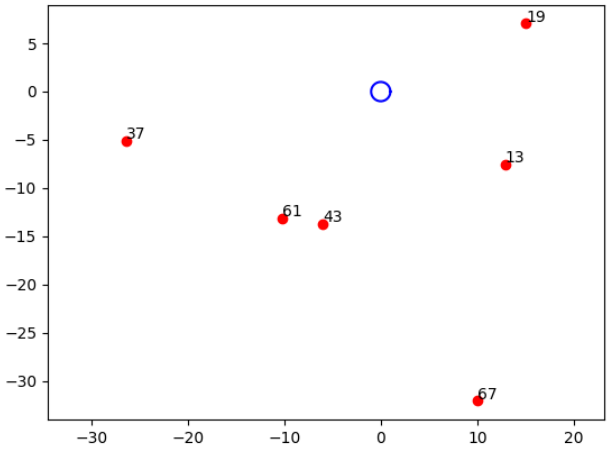
n=74


53
59
29
23
47
17
30
20
10
0
−10
−30
−20
−10
0
10
20

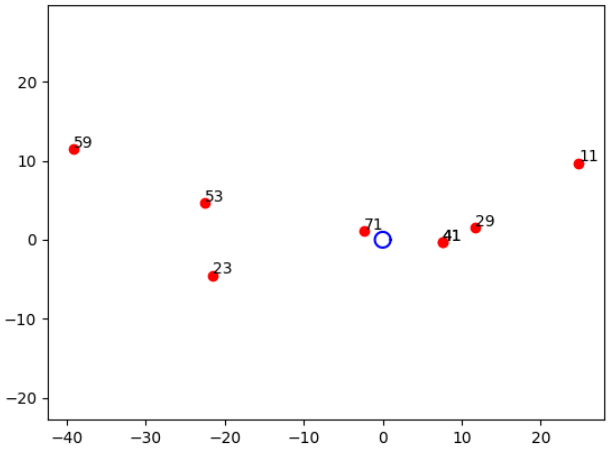
n=76



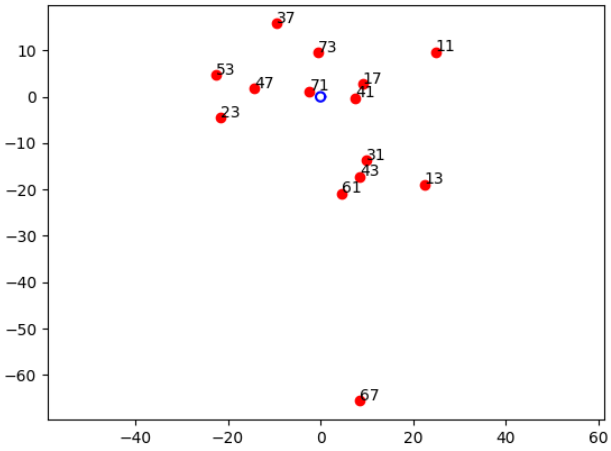
n=78



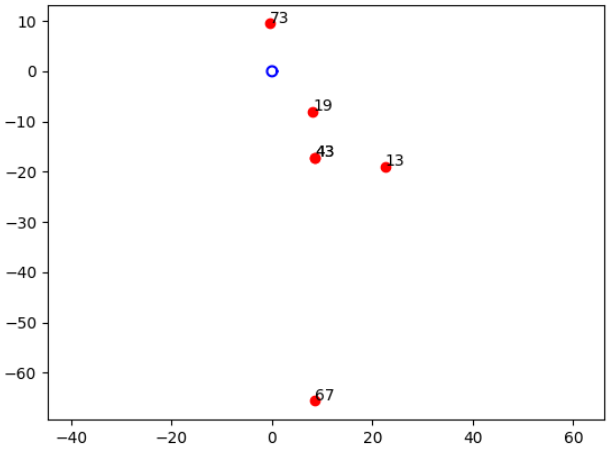
n=80



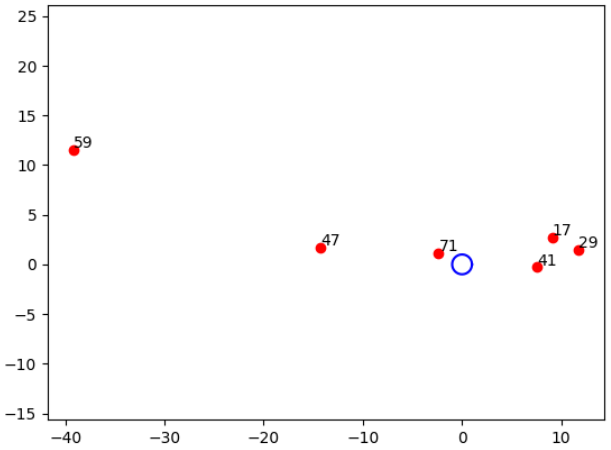
n=82


37
73
11
53
47
71
17
41
23
31
43
13
61
67
10
0
−10
−20
−30
−40
−50
−60
−40
−20
0
20
40
60

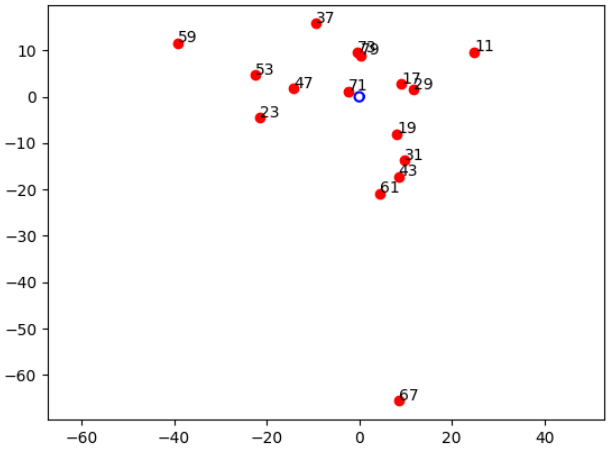
n=84


73
19
43
13
67
10
0
−10
−20
−30
−40
−50
−60
−40
−20
0
20
40
60

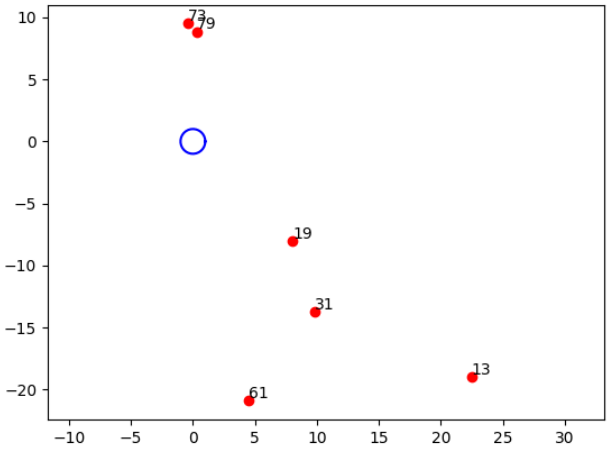
n=86


59
47
71
17
29
41
25
20
15
10
5
0
−5
−10
−15
−40
−30
−20
−10
0
10

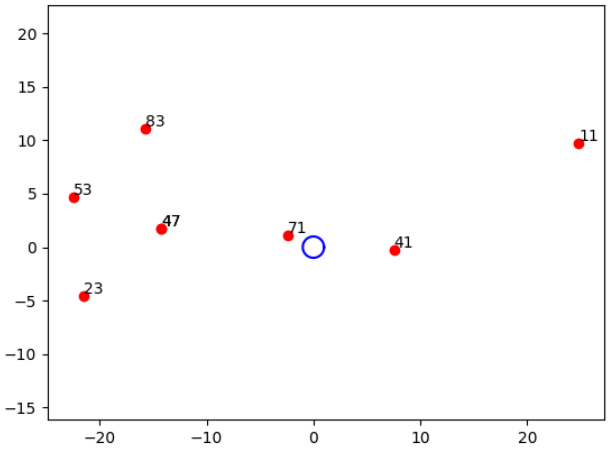
n=88


37
59
11
53
47
71
17
29
23
19
31
43
61
67

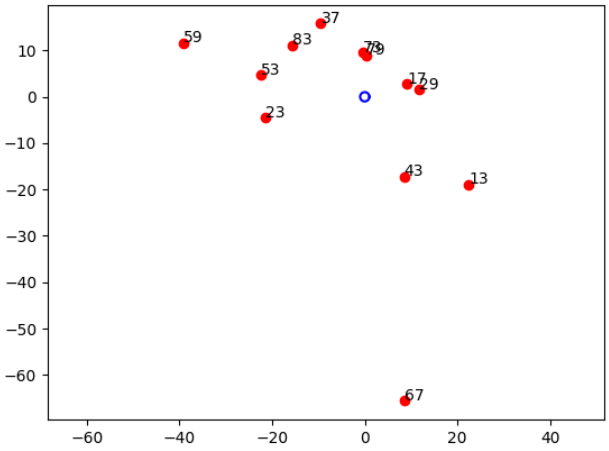
n=90


73
79
19
31
13
61

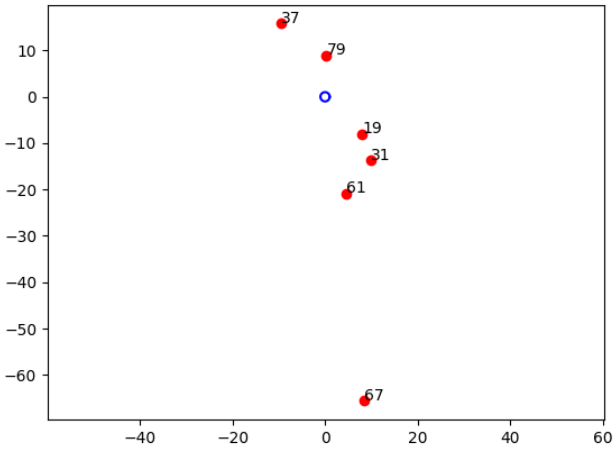
n=92


83
11
53
47
71
41
23

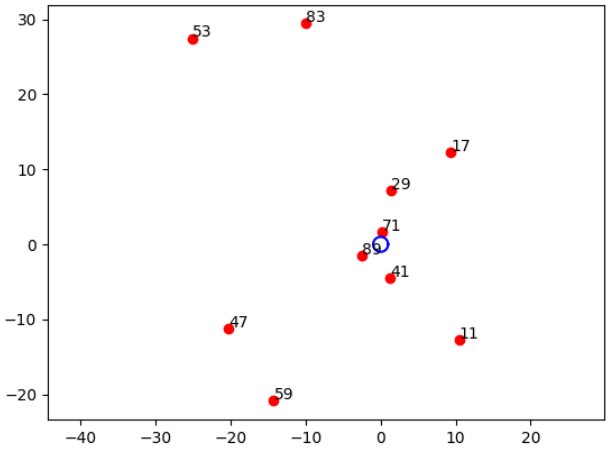
n=94


37
59
83
79
53
17
29
23
43
13
67
10
0
−10
−20
−30
−40
−50
−60
−60
−40
−20
0
20
40

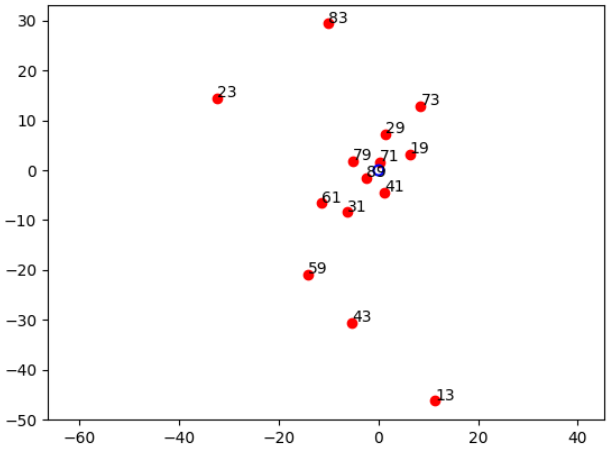
n=96


37
79
19
31
61
67
10
0
−10
−20
−30
−40
−50
−60
−40
−20
0
20
40
60

n=98


83
53
17
29
71
89
41
47
11
59
30
20
10
0
−10
−20
−40
−30
−20
−10
0
10
20

n=100



n=102

On est alors paré pour **tout ramener sur le nombre premier 2, qui ramène lui-même tout à des calculs de puissances de i (alias $1j$ en python)**. Le programme devient :

```
import mpmath
from mpmath import exp, sqrt, power, log
import numpy
from numpy import cos, sin, linspace, pi
import matplotlib.pyplot as plt

for n in range(6,103,2):
      theta = linspace(0,2*pi,30)
      r = 1
      a = r*cos(theta)
      b = r*sin(theta)
      z = a+1j*b
      plt.plot(a,b, color='blue')
      racine = int(sqrt(n))
      for x in range(2,n//2+1):
            prodbas = 1
            prodhaut = 1
            for p in range(2,racine+1):
                  lun = power(1j,4*x/p)
                  letout = power(1j,4*n/p)
                  prodbas = prodbas*(1-lun)
                  produit = letout/lun
                  prodhaut = prodhaut*(1-produit)
            if abs(prodbas) > pow(10,-10) and abs(prodhaut) > pow(10,-10):
                  print(x, ' dg de ',n)
                  plt.scatter(prodbas.real, prodbas.imag, color='red')
                  plt.annotate(x,xy=(prodbas.real, prodbas.imag+0.2))
                  plt.scatter(prodhaut.real, prodhaut.imag, color='red')
                  plt.annotate(n-x,xy=(prodhaut.real, prodhaut.imag+0.2))
      plt.axis('equal')
      plt.show()
```

Ce programme a le même comportement que le programme précédent, il trouve bien les décomposants 19, 31 et 37 de 98 (!). Les définitions précédemment proposées deviennent :

$\forall n \geq 6, \exists x \geq 3 /$

$$\prod_{\substack{2 \leq x \leq \frac{n}{2} \\ 2 \leq p \leq \sqrt{n}}} \left(1 - i^{\frac{4x}{p}}\right) \neq 0 \qquad \text{(a)}$$

et

$$\prod_{\substack{2 \leq x \leq \frac{n}{2} \\ 2 \leq p \leq \sqrt{n}}} \left(1 - i^{\frac{4(n-x)}{p}}\right) \neq 0 \qquad \text{(b)}$$

Et du fait de ces trouvailles, voici le plus petit programme qu'on ait écrit pour trouver les nombres premiers (`mpmaths` est la bibliothèque `Python` qui gère les nombres complexes, et on peut maintenant tester correctement le fait que le produit soit non nul, alors que les erreurs dans les multiplications complexes ne le permettaient pas) :

```
import mpmath
from mpmath import sqrt, power

for n in range(2,100):
      racine = int(sqrt(n))
      prodbas = 1
      for p in range(2,racine+1):
            lun = power(1j,4*n/p)
            prodbas = prodbas*(1-lun)
      if abs(prodbas) != 0:
            print(n, ' ', end='')
```

Et dont le résultat est bien sûr :

```
2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97
```

Mais cela reste une idée tordue : il s'agit simplement de savoir si les divisions euclidiennes du nombre par tous les nombres de 2 à sa racine ne tombent pas juste (n'ont pas pour reste 0), on peut écrire le programme ci-dessous, et cela n'avance à rien, finalement, même si ça aura été amusant : en python, le symbole "/" trouve un quotient réel pour des opérandes réels, tandis que le symbole "//" trouve le quotient entier, l'égalité "$a/b == a//b$" signifie que la division de a par b a un reste nul.

```
import math
from math import sqrt

for n in range(2,100):
      racine = int(sqrt(n))
      produit = 1
      for p in range(2,racine+1):
            lun = n/p != n//p
            produit = produit*lun
      if produit == 1:
            print(n, ' ', end='')
```

Angles droits entre des bissectrices (Denise Vella-Chemla, 28.04.2024)

L'idée à l'origine de cette note est la suivante : un nombre premier est un nombre qui n'est divisible par aucun nombre autre que 1 et lui-même. Il n'est donc pas divisible par tout nombre compris entre 2 et sa propre racine.

On exprime cela en utilisant le nombre $\exp\left(\frac{2i\pi\ x}{p}\right)$ qui, si la division $\frac{x}{p}$ "tombe juste" (i.e. si p divise x) vaut 1, ce qui entraîne la nullité du nombre $1 - \exp\left(\frac{2i\pi\ x}{p}\right)$. Prenons l'inverse et étendons l'expression à tous les nombres compris entre 2 et $\sqrt{x}$. Si p parcourt l'ensemble des nombres compris entre 2 et $\sqrt{x}$, x étant un nombre donné, x est un nombre premier si

$$\prod_{2\leq p\leq\sqrt{x}} \left(\exp\left(\frac{2i\pi\ x}{p}\right)\right) \quad \neq \quad 0.$$

Le caractère de primalité du nombre $n-x$ (si on cherche à décomposer le nombre pair n en somme de deux nombres premiers x et $n-x$) s'obtient en remplaçant x par $n-x$ dans la formule ci-dessus.

On peut remplacer l'expression $\exp\left(\frac{2i\pi\ x}{p}\right)$ par $i^{4x/p}$ (avec $i=\sqrt{-1}$).

On a ainsi une formulation qui impliquerait la conjecture de Goldbach si elle s'avérait vraie :

$\forall n \geq 6, \exists x \geq 3\ /$

$$\prod_{\substack{2\leq x\leq\frac{n}{2}\\ 2\leq p\leq\sqrt{n}}} \left(1 - i^{\frac{4x}{p}}\right) \qquad \neq 0 \qquad \text{(a)}$$

et

$$\prod_{\substack{2\leq x\leq\frac{n}{2}\\ 2\leq p\leq\sqrt{n}}} \left(1 - i^{\frac{4(n-x)}{p}}\right) \qquad \neq 0 \qquad \text{(b)}$$

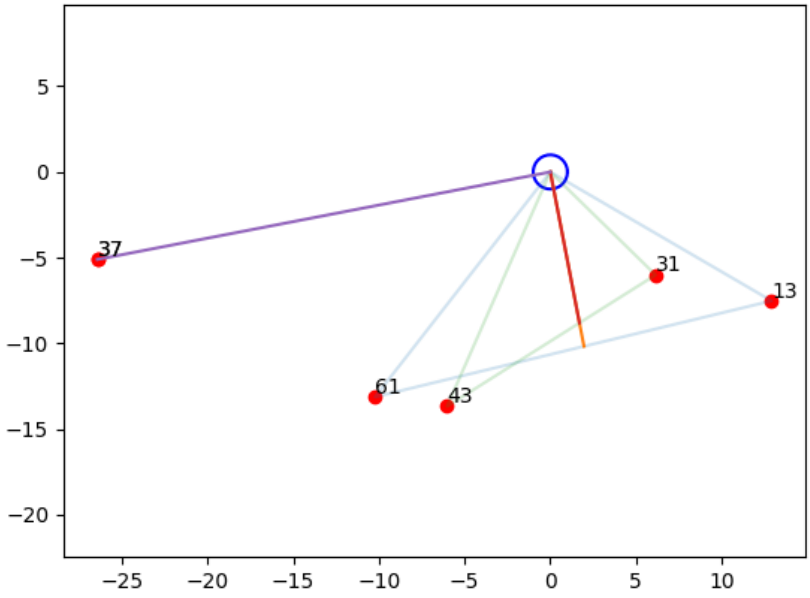
Cette idée permet de visualiser dans le plan complexe les décomposants de Goldbach (s'ils existent, ce qu'on ne sait pas démontrer) d'un nombre pair n : les décomposants de Goldbach de n sont les seuls nombres qui sont positionnés ailleurs qu'en le point zéro, i.e. les points dont l'affixe est non nul.

L'idée qui vient alors est de tracer les bissectrices des angles que font les droites (O, z_1) et (O, z_2) avec z_1 et z_2 les affixes de deux décomposants de Goldbach de n. Voici le programme[1].

[1] Merci J.C. pour le dessin des bissectrices.

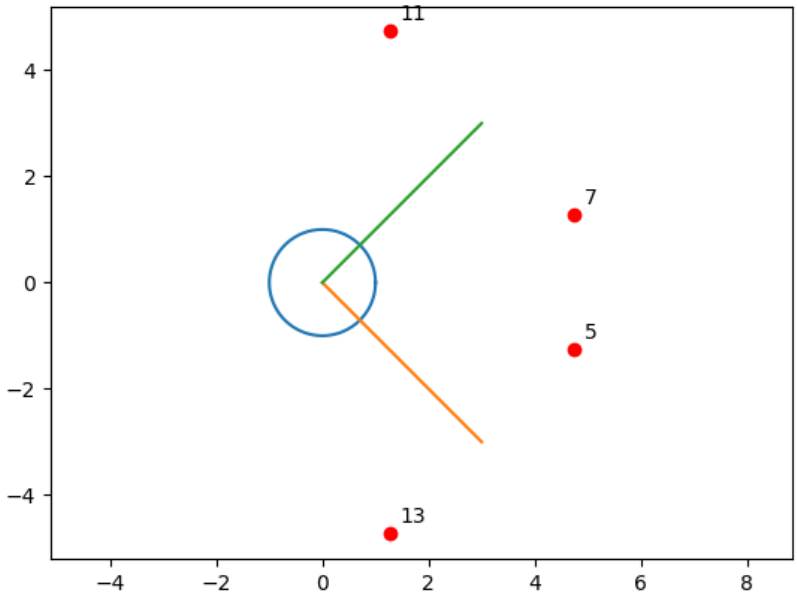
```
import numpy as np
from numpy import pi, sqrt
import matplotlib.pyplot as plt

for n in range(6,103,2):
     t = np.linspace(0, 1, 100)
     c = np.exp(2*pi*1j*t)
     plt.plot(c.real, c.imag)
     rac = int(sqrt(n))
     for x in range(2,n//2+1):
          p = np.arange(2, rac + 1)
          u = np.prod(1-np.power(1j,4*x/p))
          v = np.prod(1-np.power(1j,4*(n-x)/p))
          if min(abs(u),abs(v)) > 1e-10:
               print(x, ' dg de ',n)
               plt.scatter(u.real, u.imag, color='red')
               plt.annotate(x, xy=(u.real + 0.2, u.imag + 0.2))
               plt.scatter(v.real, v.imag, color='red')
               plt.annotate(n-x,xy=(v.real + 0.2, v.imag + 0.2))
               w = (u/abs(u) + v/abs(v))/2
               w = w/abs(w)
               r = (u.real*(u.imag - v.imag)-u.imag*(u.real-v.real))
                    /(w.real*(u.imag-v.imag)-w.imag*(u.real-v.real))
               b = r*w
               plt.plot([0, b.real], [0, b.imag])
     plt.axis('equal')
     plt.show()
```

Et voici les graphiques présentant les décomposants de Goldbach des nombres de 18 à 102 ; on constate que les bissectrices des angles que font les droites (O, z_1) et (O, z_2) avec z_1 et z_2 les affixes de 2 décomposants de Goldbach de n sont toujours alignées sur deux directions seulement (voire une seule), et qui sont perpendiculaires. On remarque pour les doubles de nombres premiers que la demi-droite "triviale" (les deux demi-droites sur les deux décomposants de Goldbach se confondent alors en une seule demi-droite) est également perpendiculaire à la droite bissectrice de l'angle "reliant" deux autres décomposants. On a marqué les doubles de nombres premiers, ces nombres pairs qui vérifient trivialement la conjecture de Goldbach d'une lettre p minuscule entre parenthèse car pour eux, on a omis de visualiser la demi-droite triviale dans le programme. L'œil aiguisé de la lectrice repèrera cette demi-droite triviale aisément. On a omis dans les graphiques, les petits triangles qui permettraient de repérer les décompositions plus aisément, pour mieux visualiser les angles droits systématiques mais le dessin ci-dessous, pour $n = 74$, montre la décomposition "dégénérée" sur 37, bien perpendiculaire aux deux autres décompositions, ainsi que les petits triangles qui font apparaître la décomposition $61 + 13$ et la décomposition $43 + 31$.

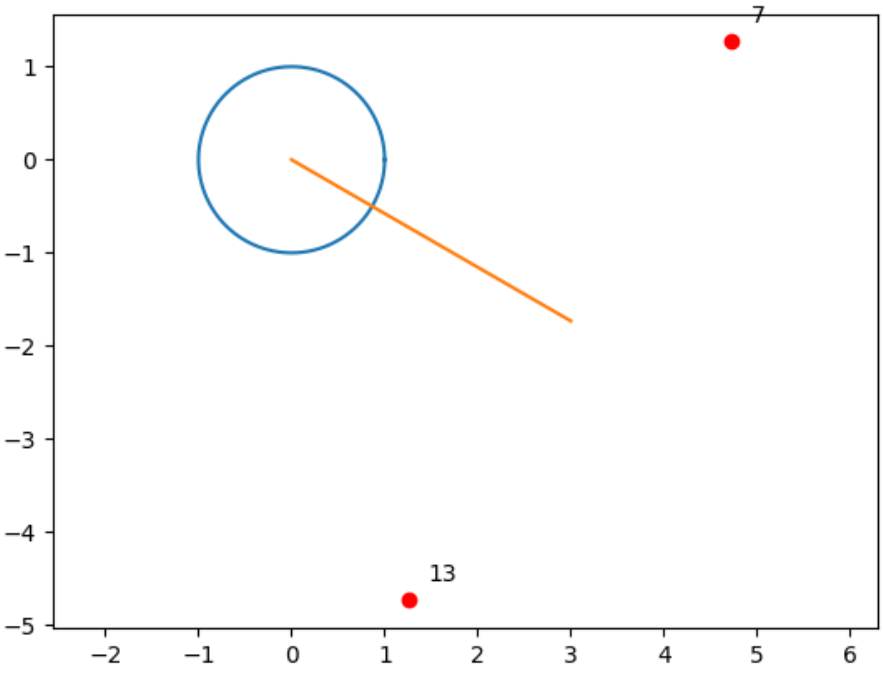


n=18

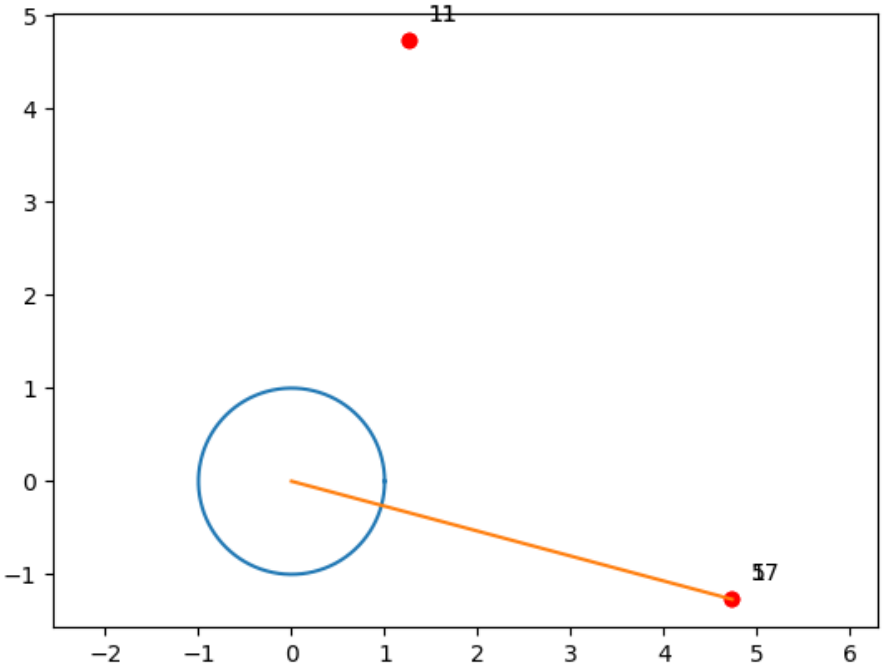
Parfois l'alignement de plusieurs demi-droites n'est pas trop visible car les demi-droites sont l'une au-dessous de l'autre, on repère ces circonstances par le fait que la demi-droite change de couleur en cours de chemin.



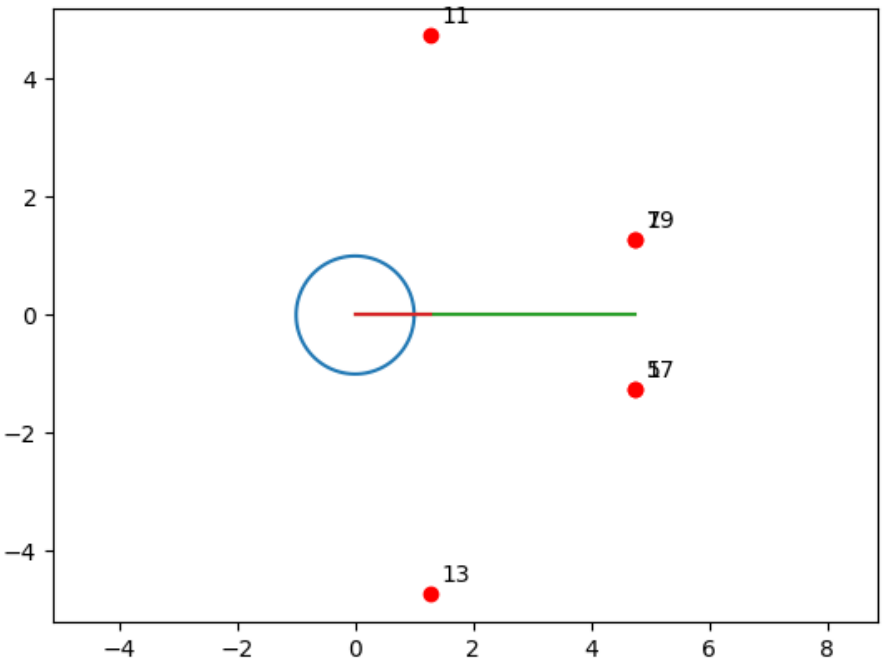
n=18



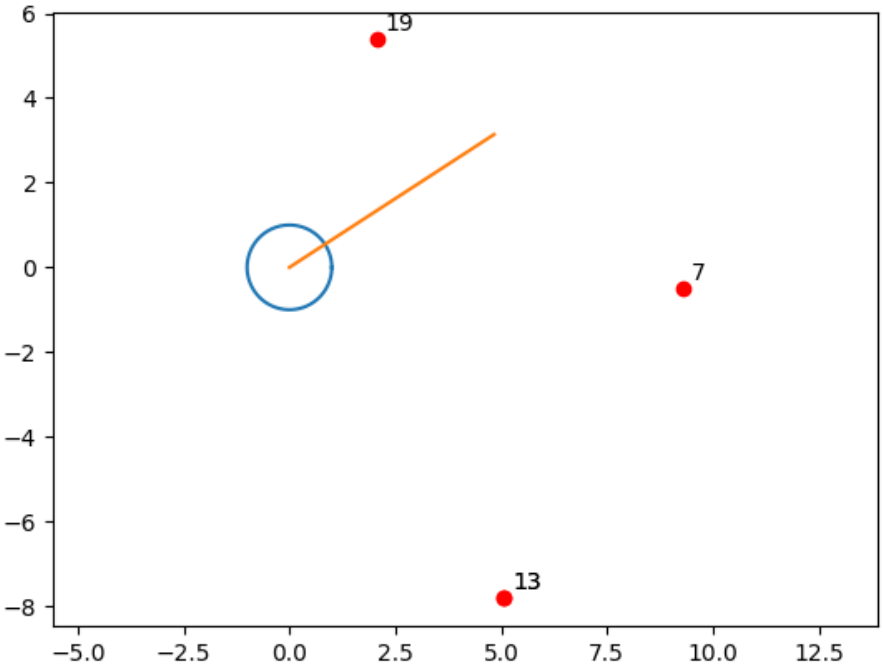
n=20



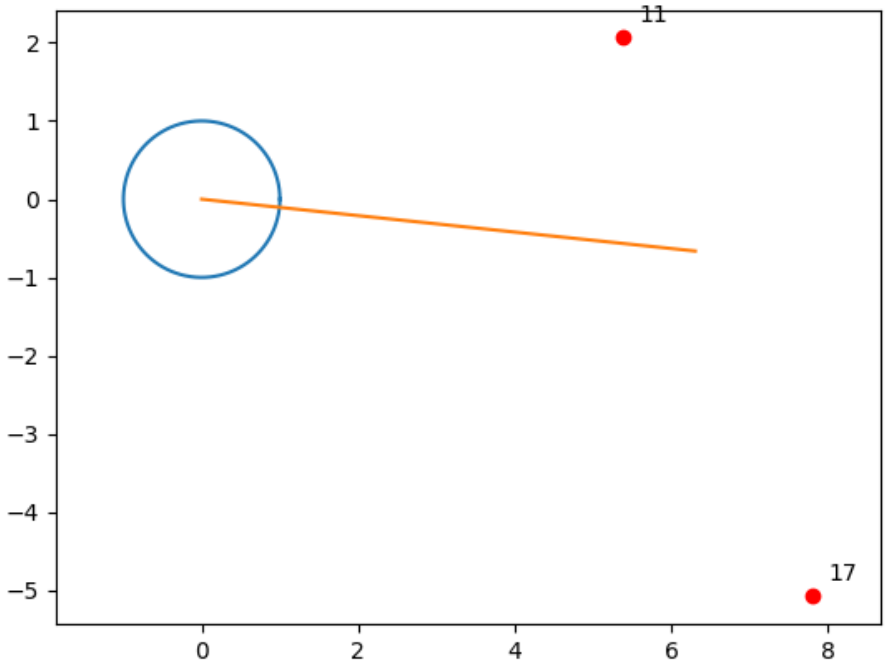
n=22 (p)


11
19
17
13
4
2
0
−2
−4
−4
−2
0
2
4
6
8

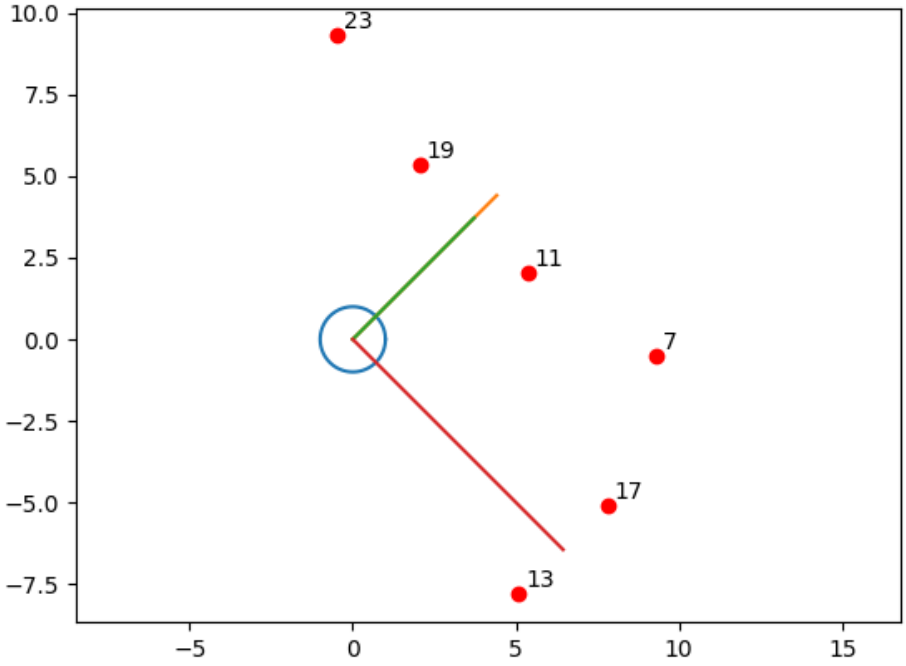
n=24


19
7
13
6
4
2
0
−2
−4
−6
−8
−5.0
−2.5
0.0
2.5
5.0
7.5
10.0
12.5

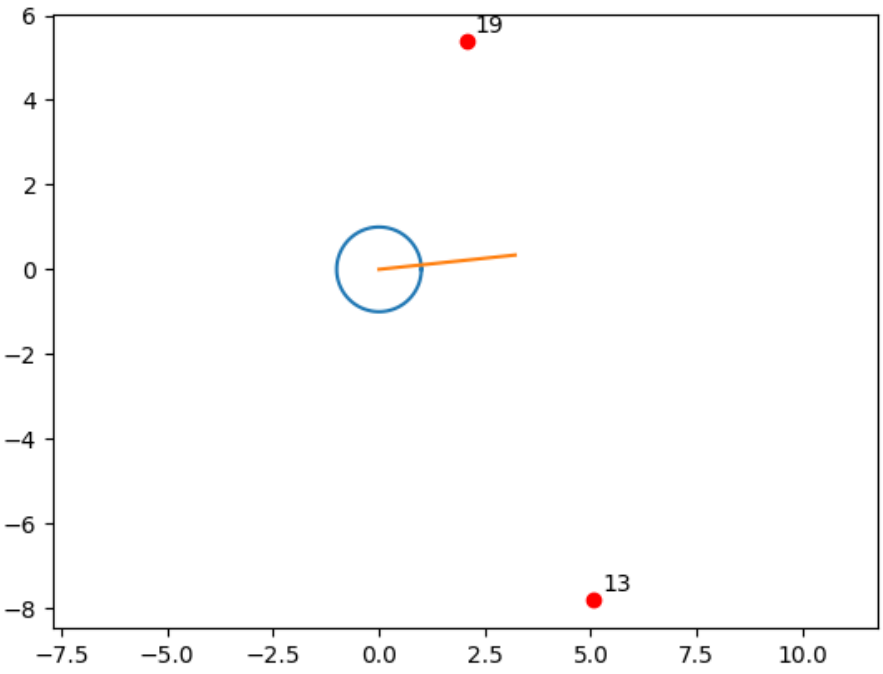
n=26 (p)


11
17
2
1
0
−1
−2
−3
−4
−5
0
2
4
6
8

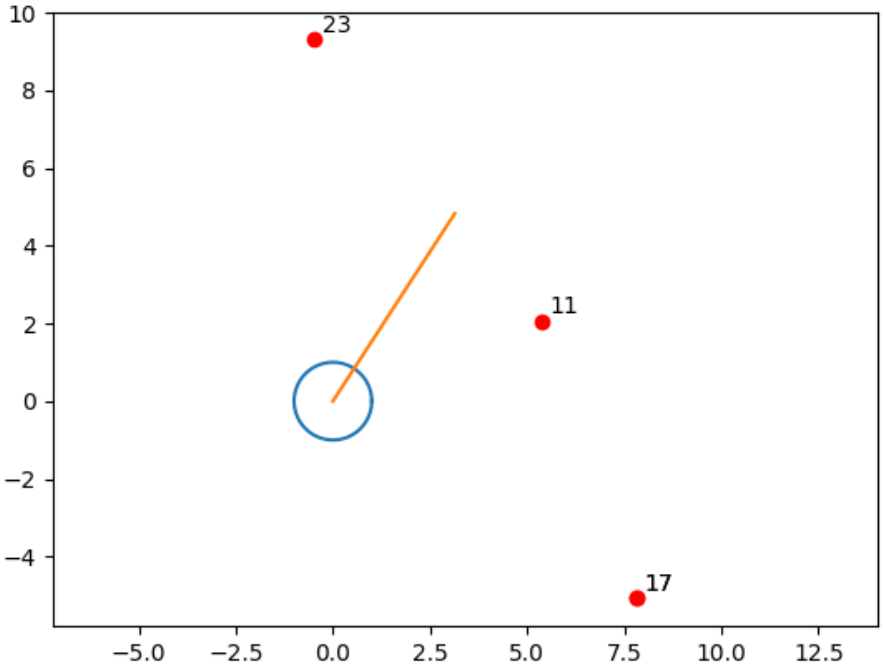
n=28


23
19
11
7
17
13
10.0
7.5
5.0
2.5
0.0
−2.5
−5.0
−7.5
−5
0
5
10
15

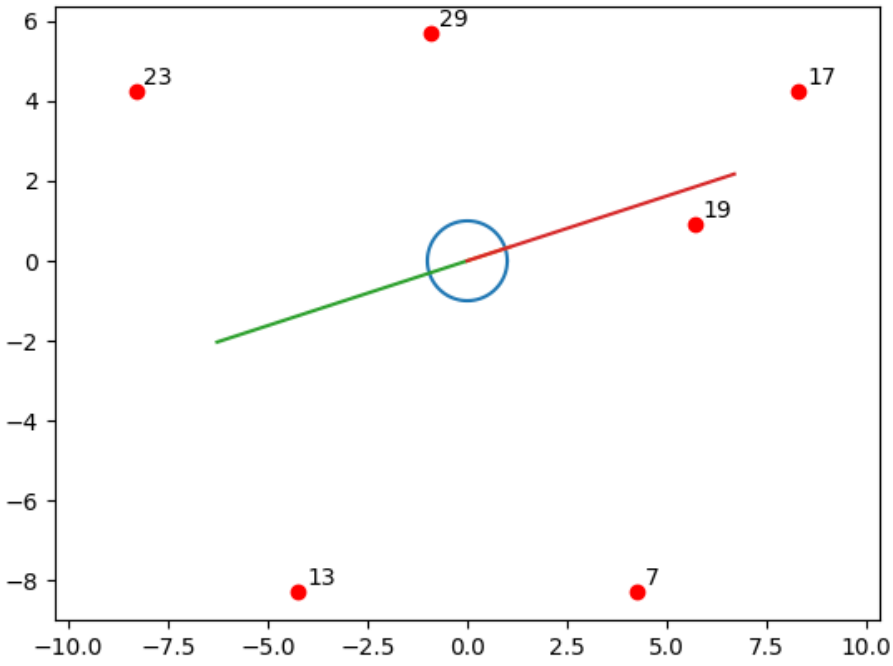
n=30


19
13
6
4
2
0
−2
−4
−6
−8
−7.5
−5.0
−2.5
0.0
2.5
5.0
7.5
10.0

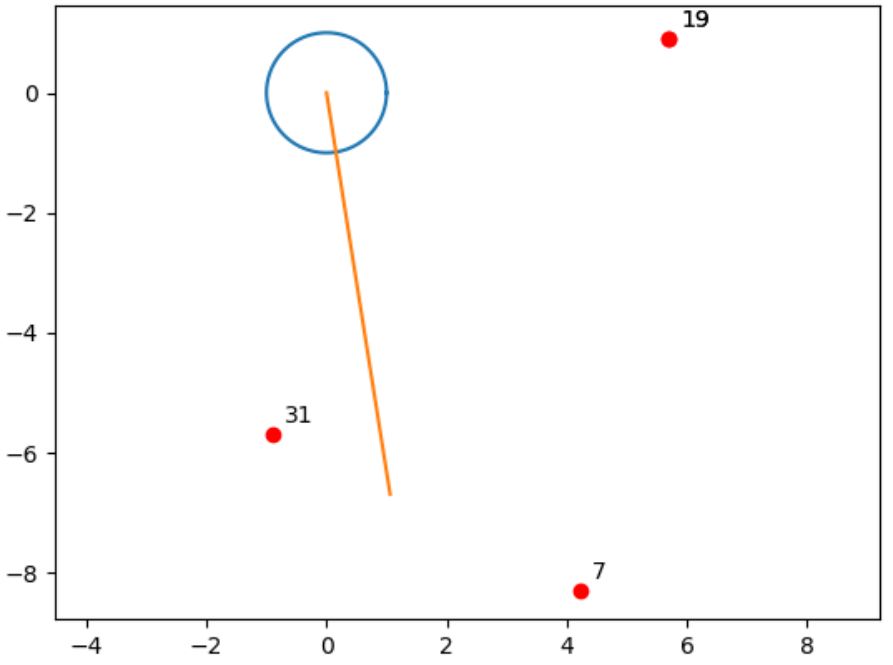
n=32


23
11
17
10
8
6
4
2
0
−2
−4
−5.0
−2.5
0.0
2.5
5.0
7.5
10.0
12.5

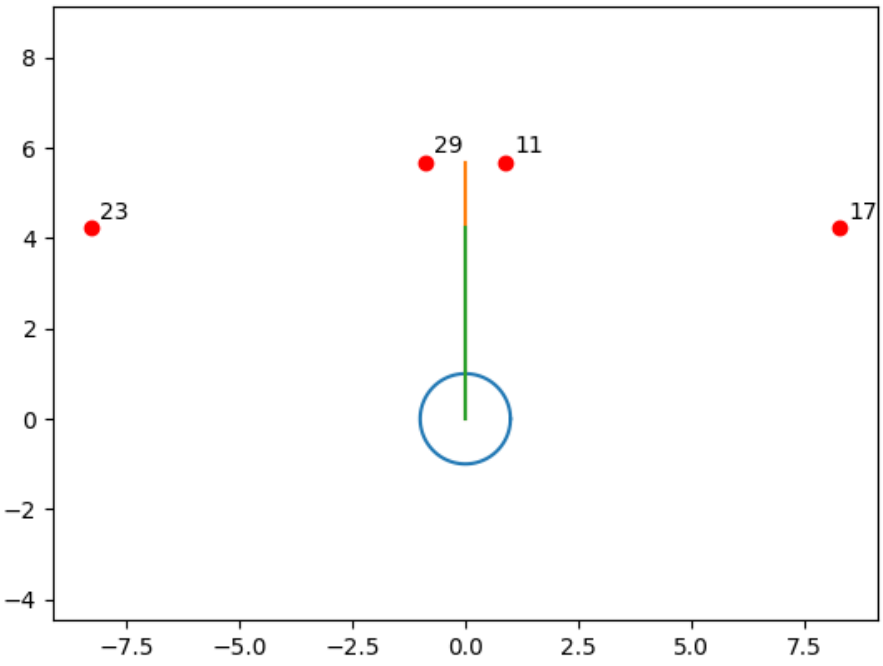
n=34 (p)


29
23
17
19
13
7
6
4
2
0
−2
−4
−6
−8
−10.0
−7.5
−5.0
−2.5
0.0
2.5
5.0
7.5
10.0

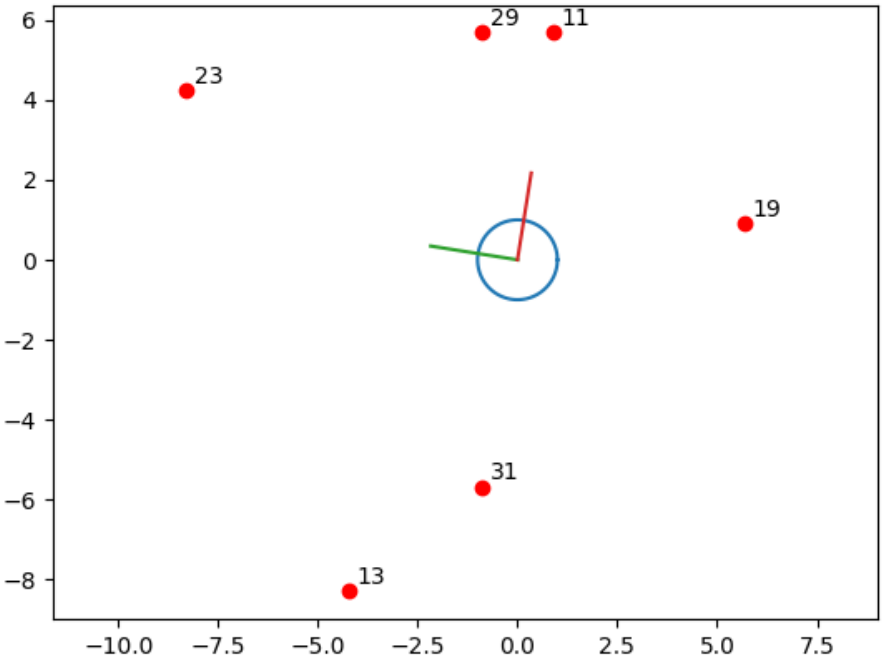
n=36


19
31
7
0
−2
−4
−6
−8
−4
−2
0
2
4
6
8

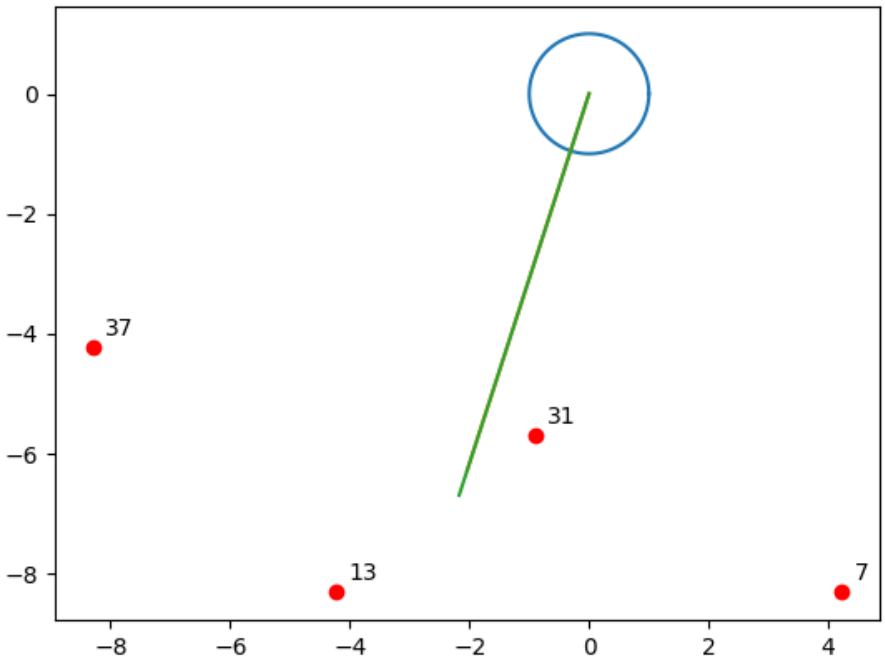
n=38 (p)


29
11
23
17
8
6
4
2
0
−2
−4
−7.5
−5.0
−2.5
0.0
2.5
5.0
7.5

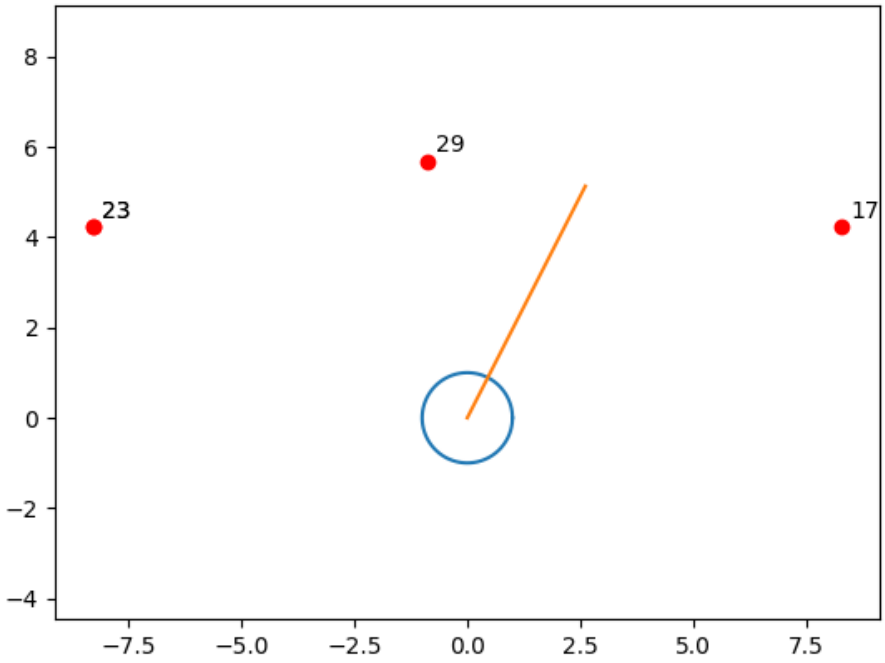
n=40


29
11
23
19
31
13
6
4
2
0
−2
−4
−6
−8
−10.0
−7.5
−5.0
−2.5
0.0
2.5
5.0
7.5

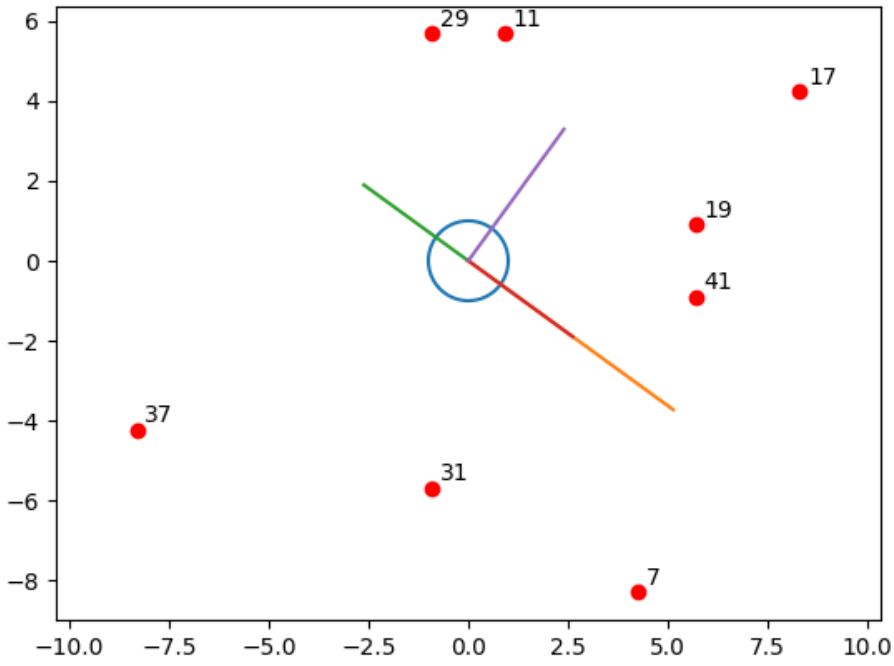
n=42



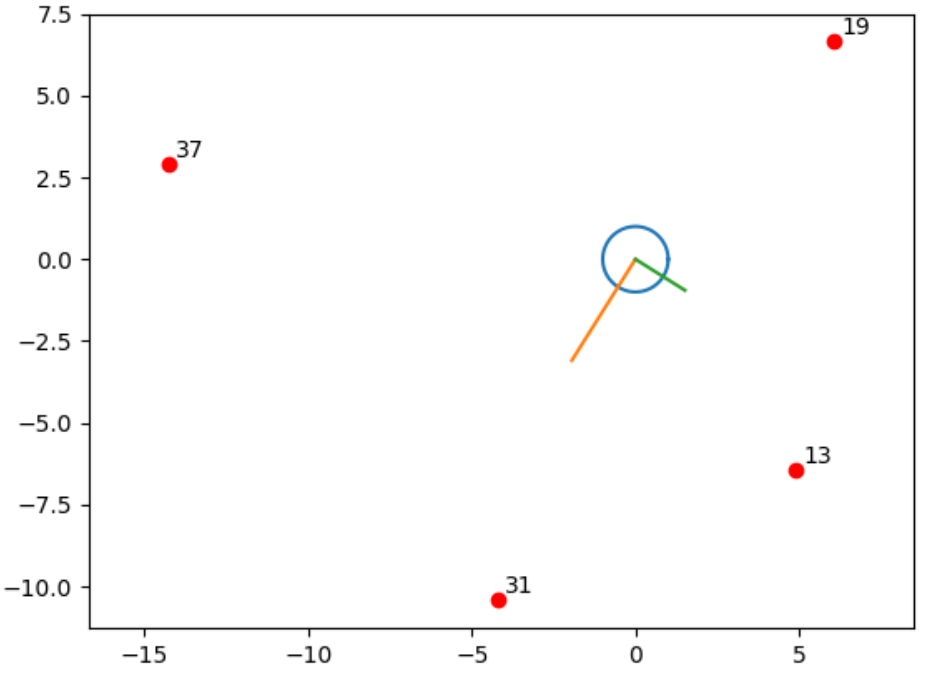
n=44



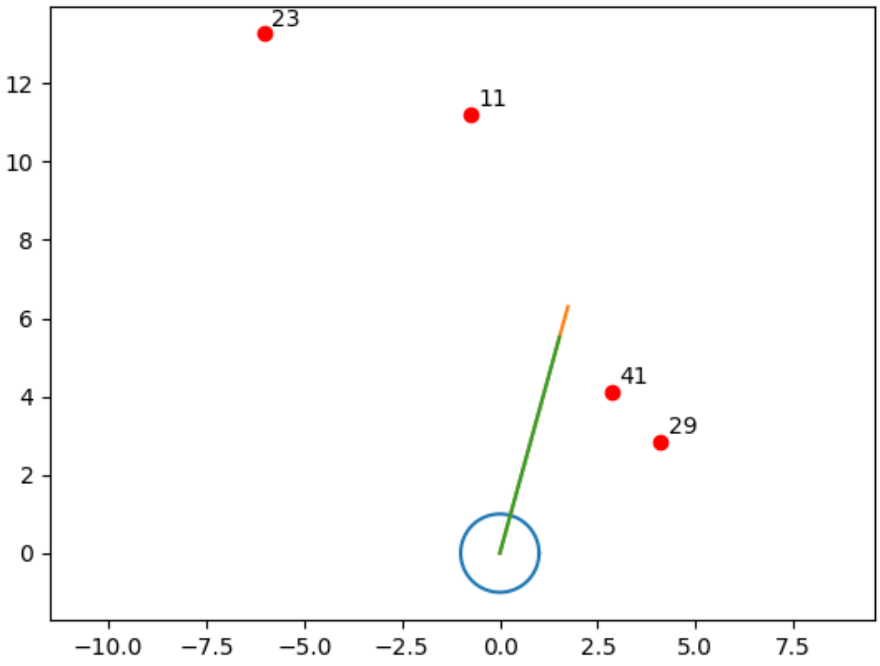
n=46 (p)


29
11
17
19
41
37
31
7
6
4
2
0
−2
−4
−6
−8
−10.0
−7.5
−5.0
−2.5
0.0
2.5
5.0
7.5
10.0

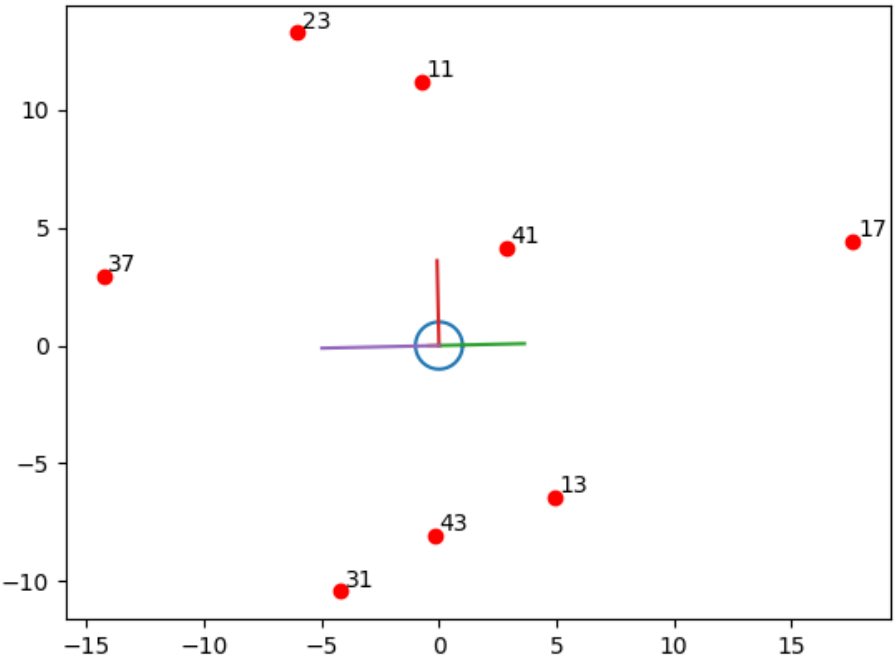
n=48


19
37
13
31
7.5
5.0
2.5
0.0
−2.5
−5.0
−7.5
−10.0
−15
−10
−5
0
5

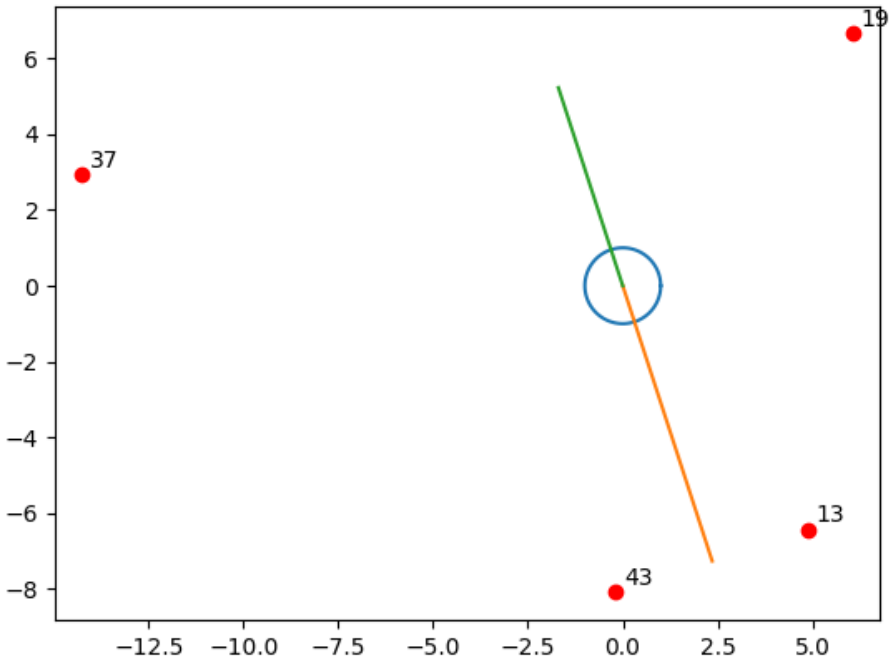
n=50


23
11
41
29
12
10
8
6
4
2
0
−10.0
−7.5
−5.0
−2.5
0.0
2.5
5.0
7.5

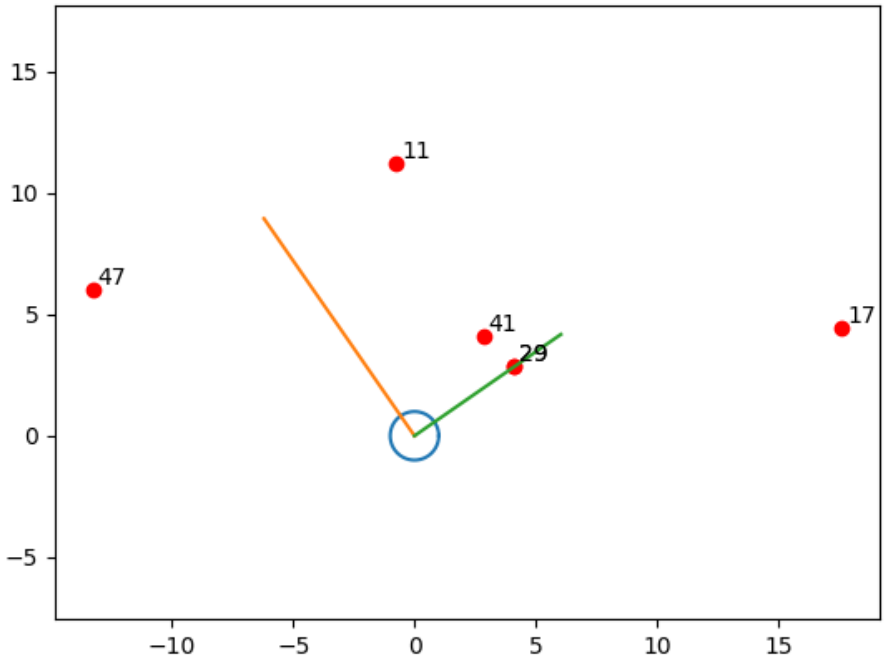
n=52


23
11
41
17
37
13
43
31
10
5
0
−5
−10
−15
−10
−5
0
5
10
15

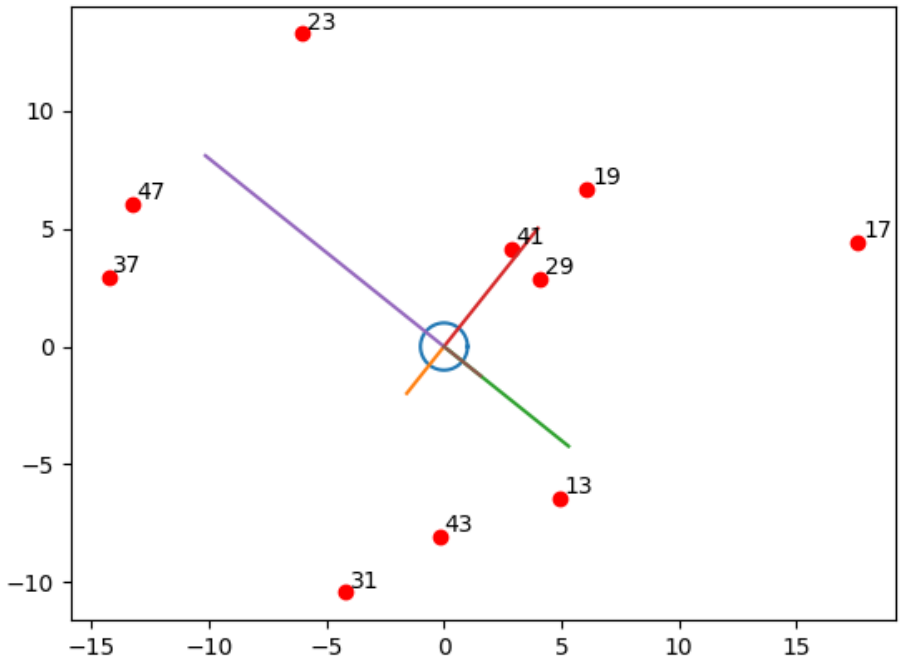
n=54


19
37
13
43
6
4
2
0
−2
−4
−6
−8
−12.5
−10.0
−7.5
−5.0
−2.5
0.0
2.5
5.0

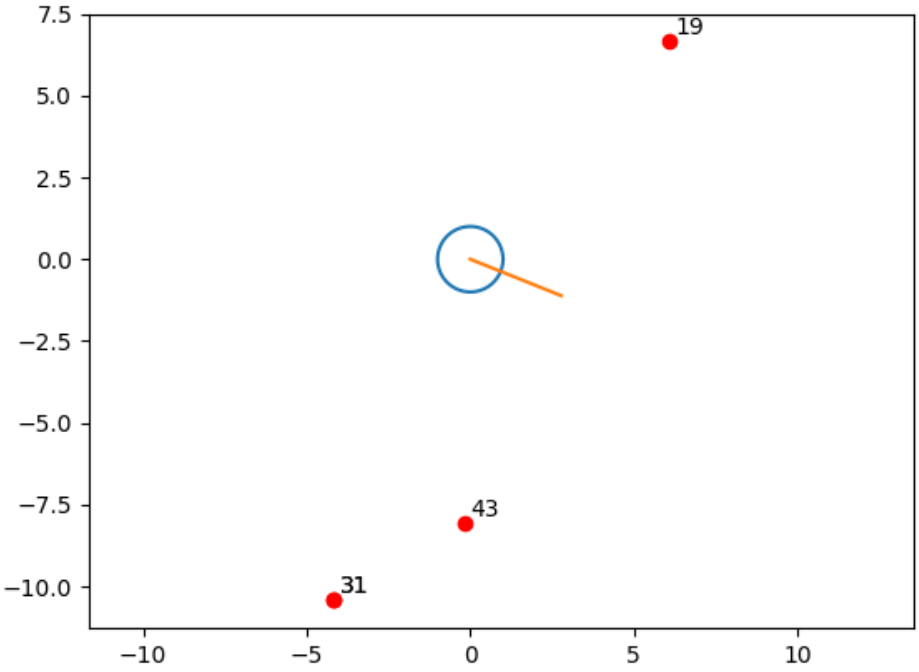
n=56


11
47
41
29
17
15
10
5
0
−5
−10
−5
0
5
10
15

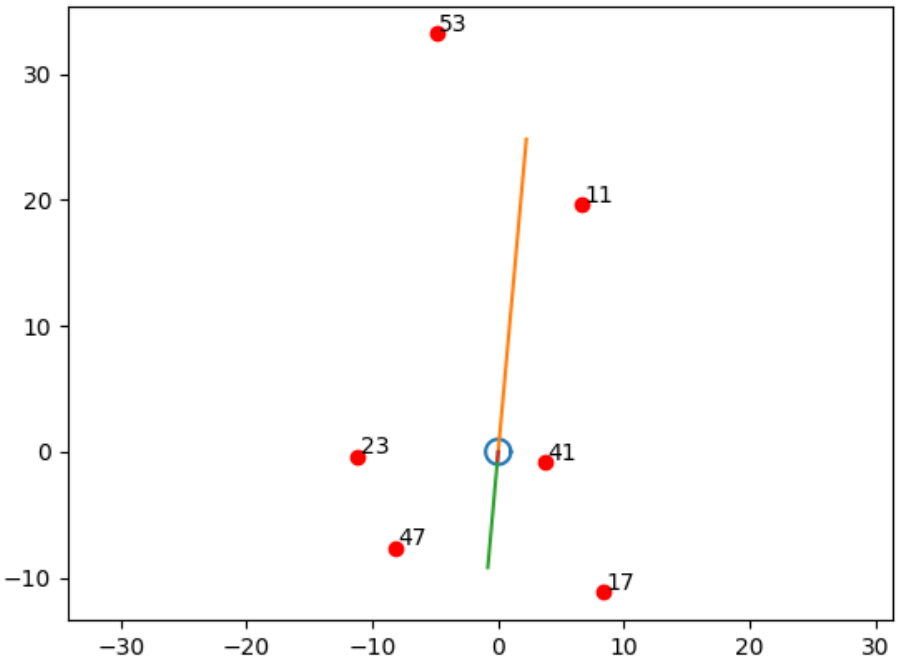
n=58 (p)


23
47
19
17
41
37
29
13
43
31
10
5
0
−5
−10
−15
−10
−5
0
5
10
15

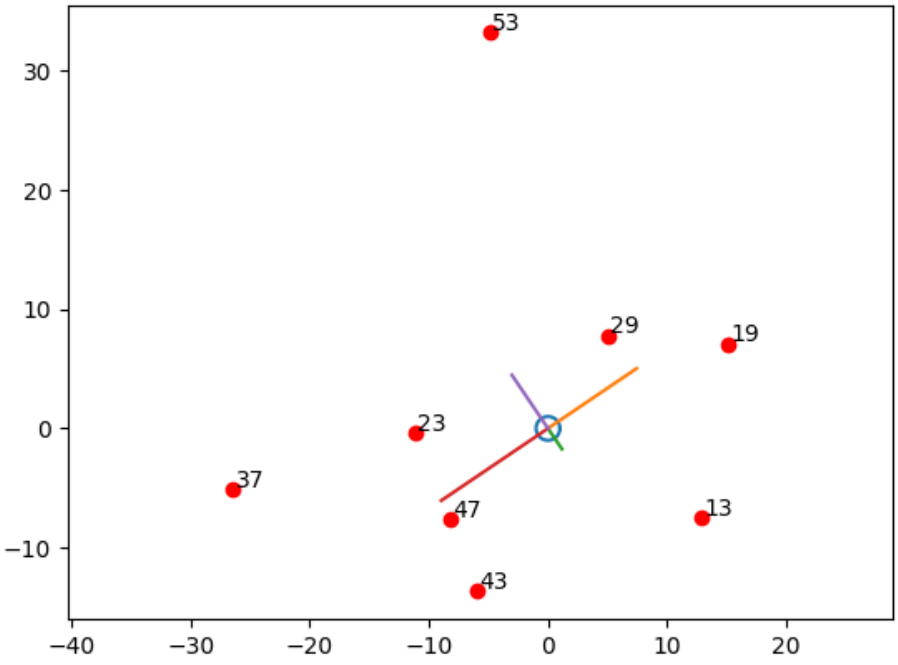
n=60


19
43
31
7.5
5.0
2.5
0.0
−2.5
−5.0
−7.5
−10.0
−10
−5
0
5
10

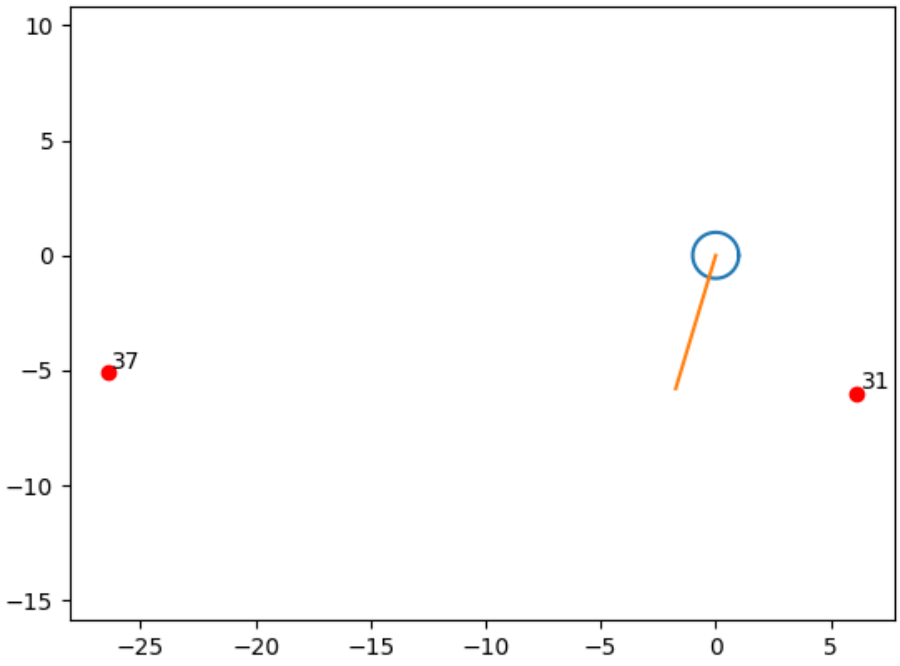
n=62 (p)


53
11
23
41
47
17
30
20
10
0
−10
−30
−20
−10
0
10
20
30

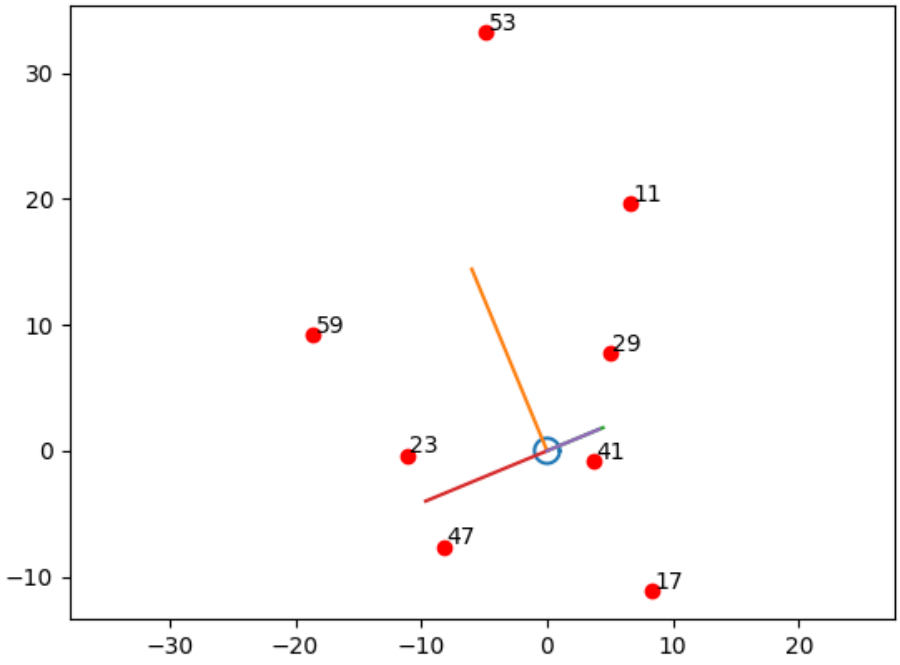
n=64


53
29
19
23
37
47
13
43
30
20
10
0
−10
−40
−30
−20
−10
0
10
20

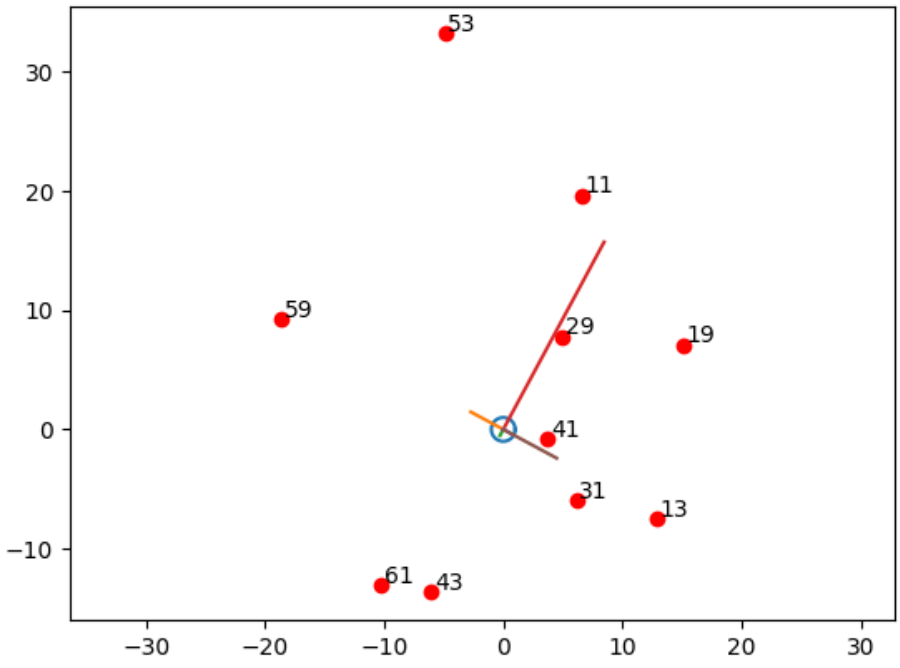
n=66


10
5
0
−5
−10
−15
−25
−20
−15
−10
−5
0
5
37
31

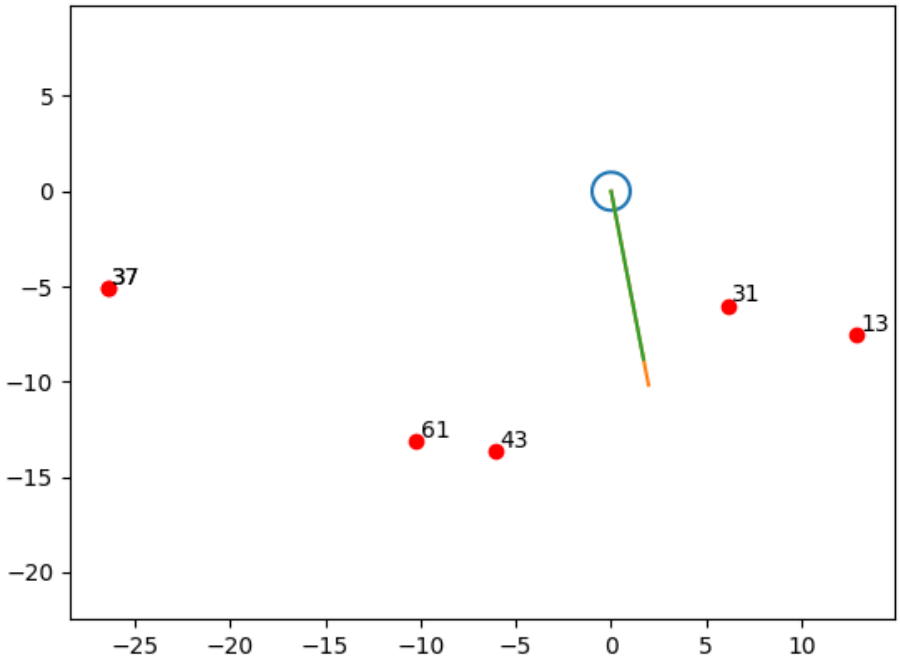
n=68


30
20
10
0
−10
−30
−20
−10
0
10
20
53
11
59
29
23
41
47
17

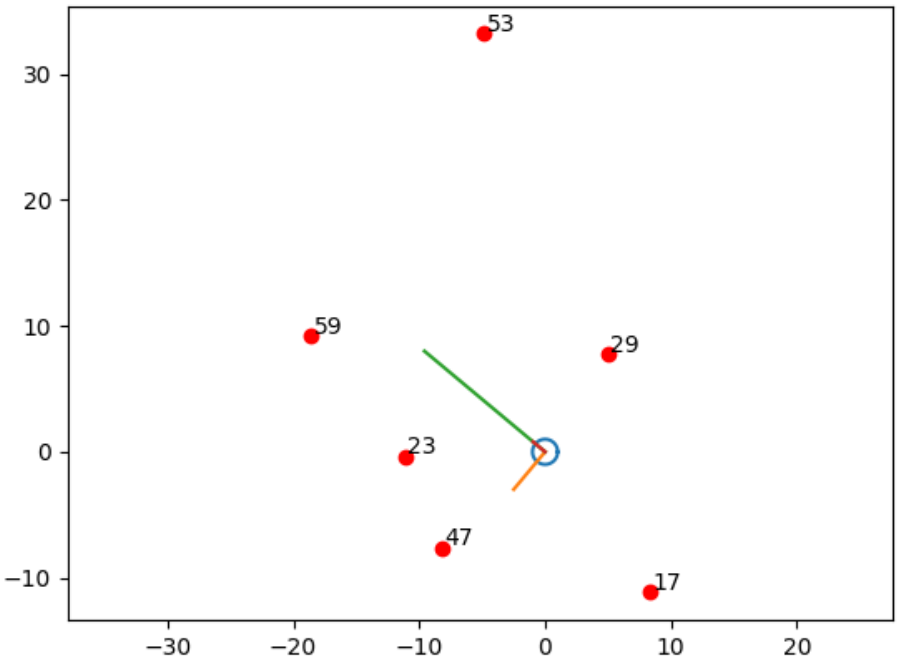
n=70


53
11
59
29
19
41
31
13
61
43
30
20
10
0
−10
−30
−20
−10
0
10
20
30

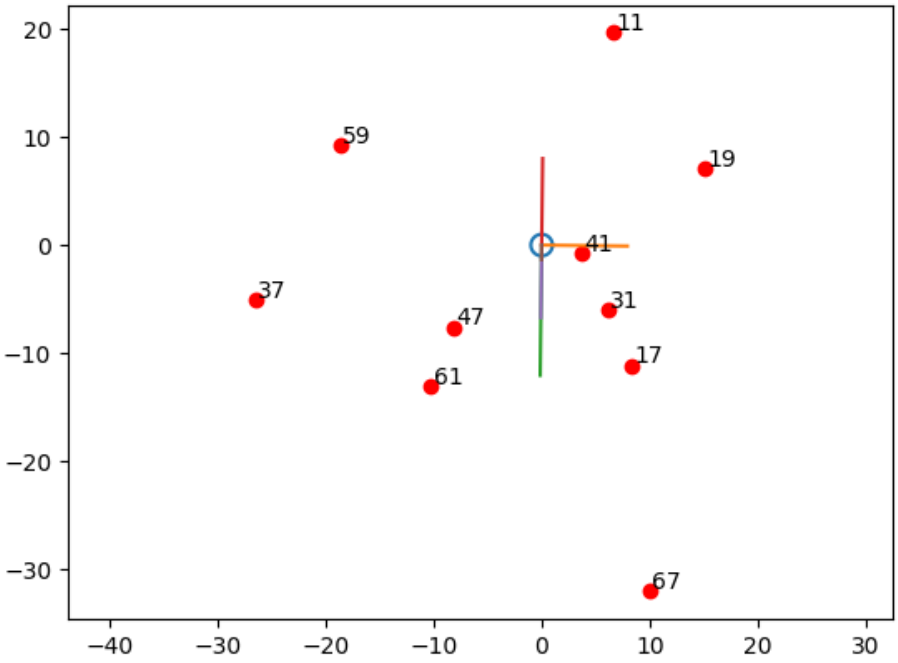
n=72


37
31
13
61
43
5
0
−5
−10
−15
−20
−25
−20
−15
−10
−5
0
5
10

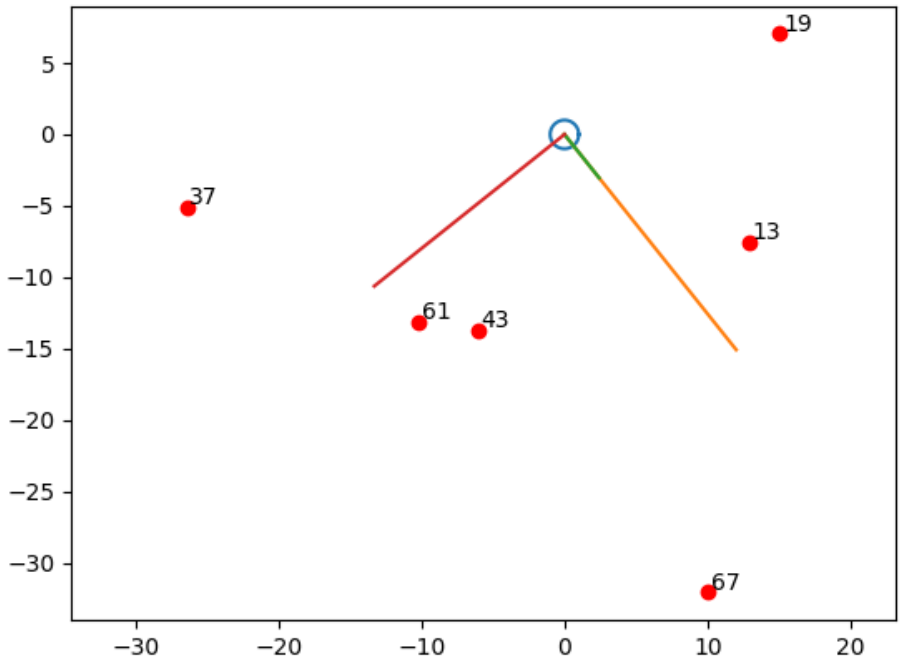
n=74 (p)


53
59
29
23
47
17
30
20
10
0
−10
−30
−20
−10
0
10
20

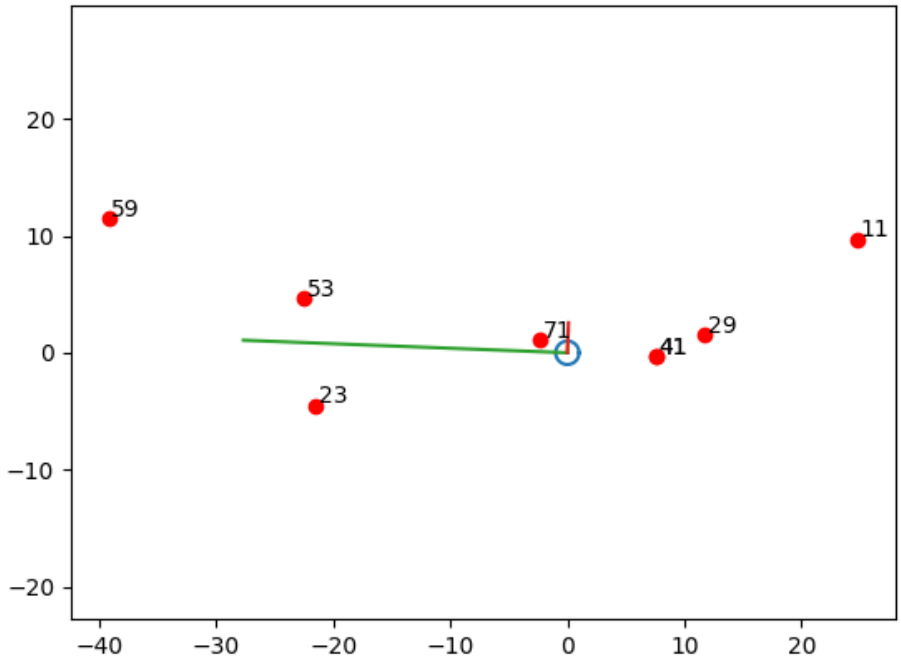
n=76


11
59
19
41
37
31
47
17
61
67
20
10
0
−10
−20
−30
−40
−30
−20
−10
0
10
20
30

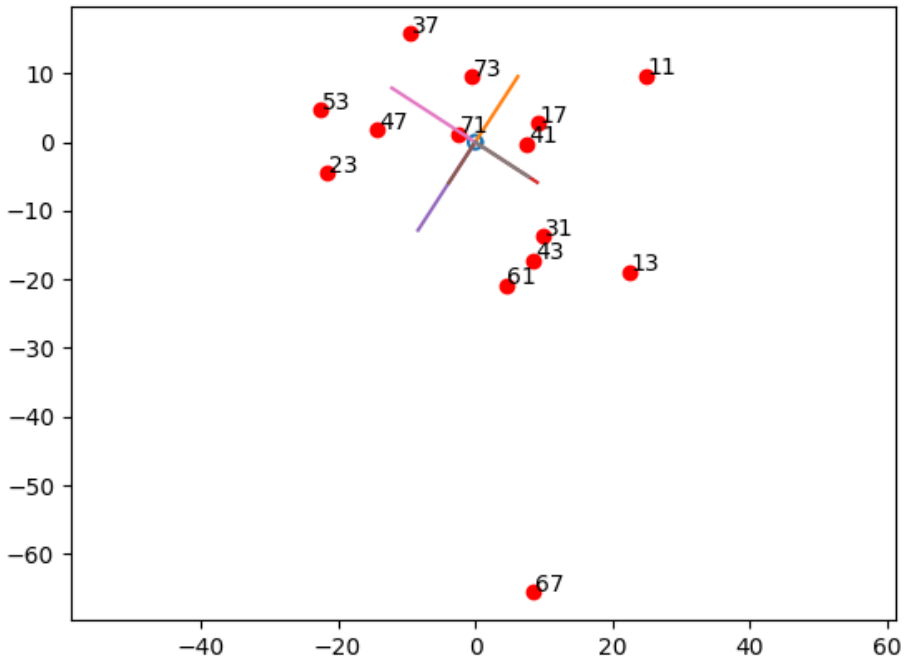
n=78


19
37
13
61
43
67
5
0
−5
−10
−15
−20
−25
−30
−30
−20
−10
0
10
20

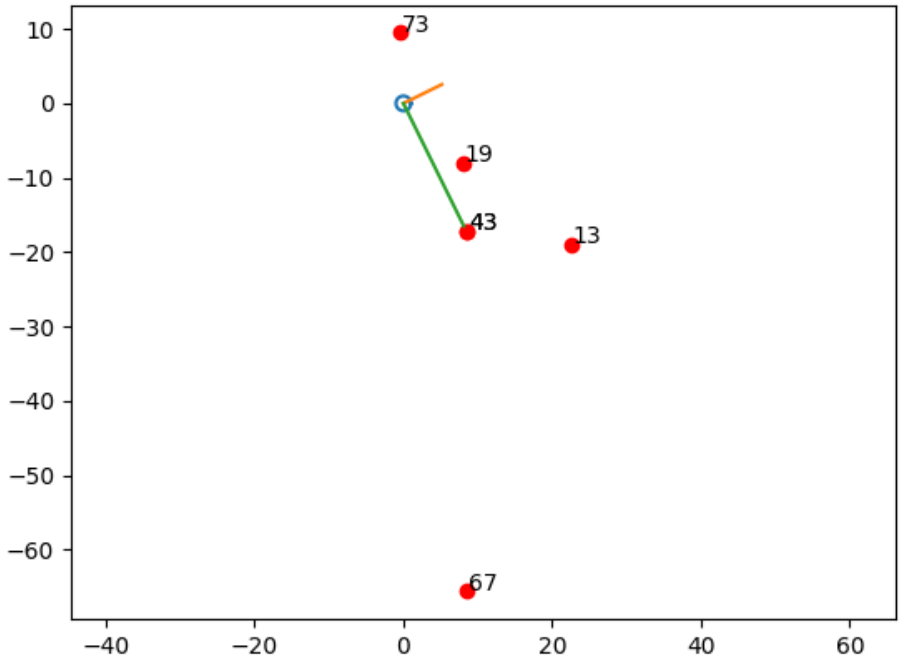
n=80


59
11
53
71
29
41
23
20
10
0
−10
−20
−40
−30
−20
−10
0
10
20

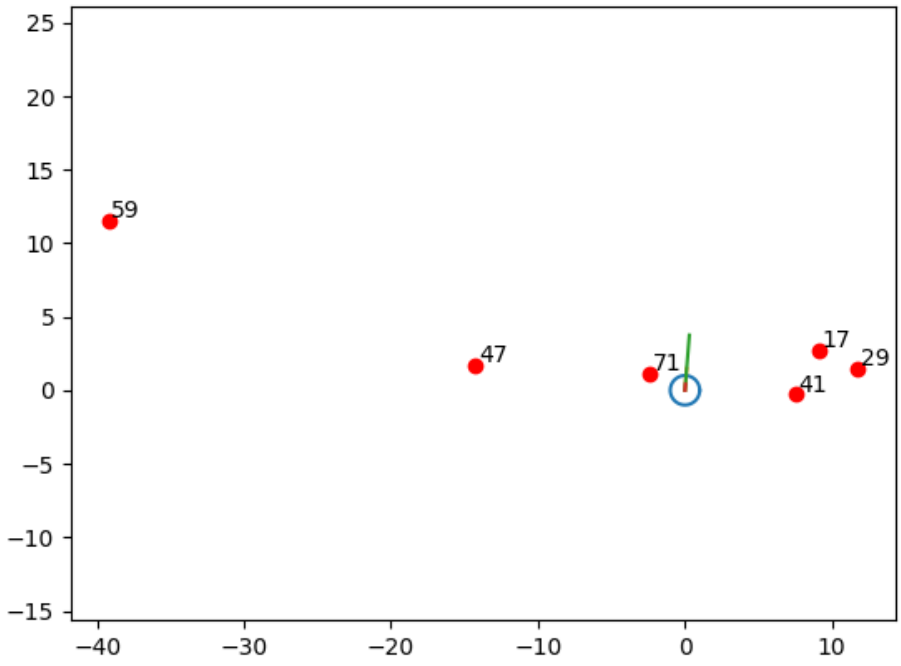
n=82 (p)


37
73
11
53
47
71
17
41
23
31
43
13
61
67
10
0
−10
−20
−30
−40
−50
−60
−40
−20
0
20
40
60

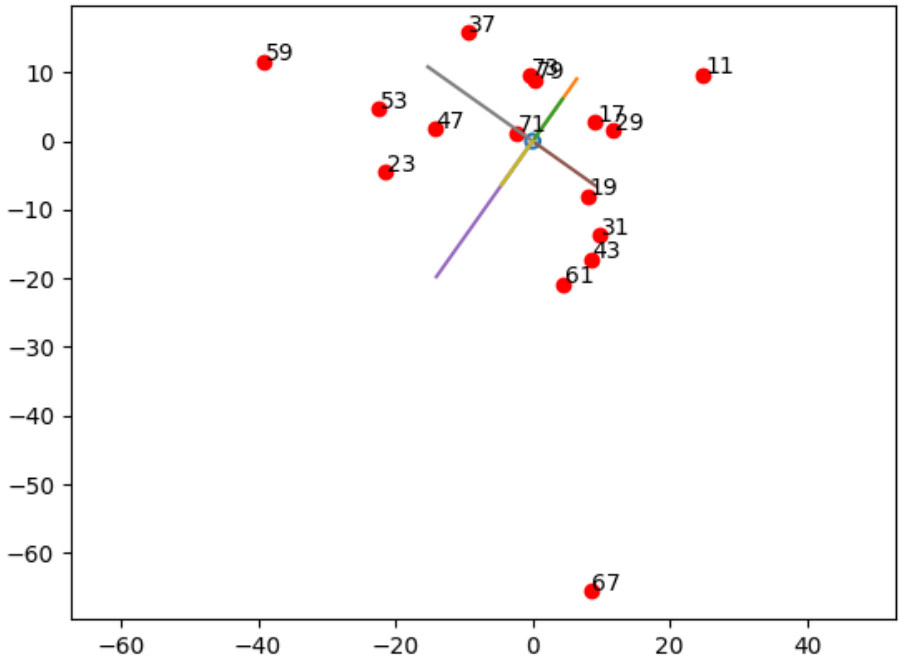
n=84


73
19
43
13
67
10
0
−10
−20
−30
−40
−50
−60
−40
−20
0
20
40
60

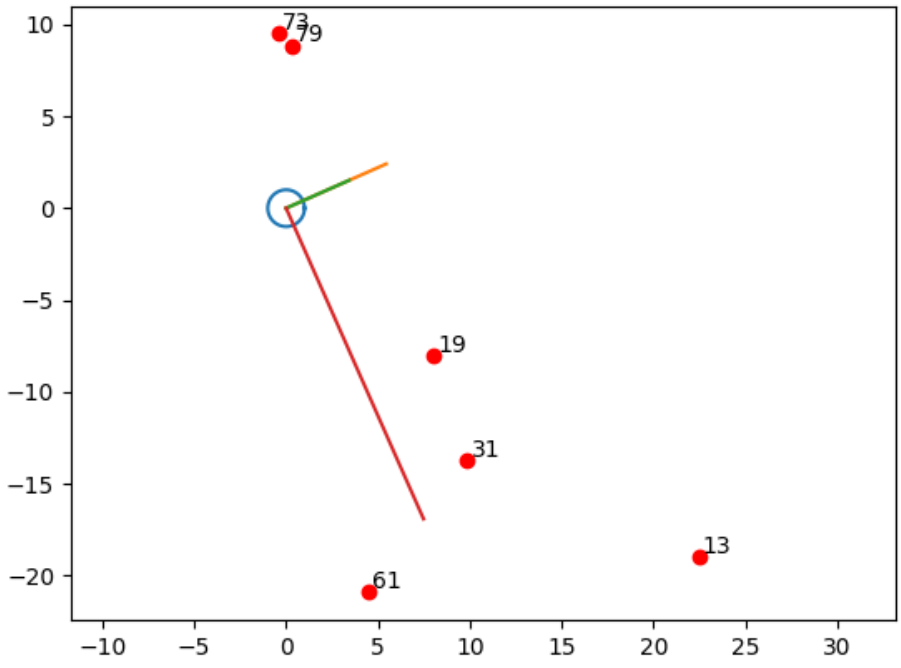
n=86 (p)


25
20
15
10
5
0
−5
−10
−15
−40
−30
−20
−10
0
10
59
47
71
17
29
41

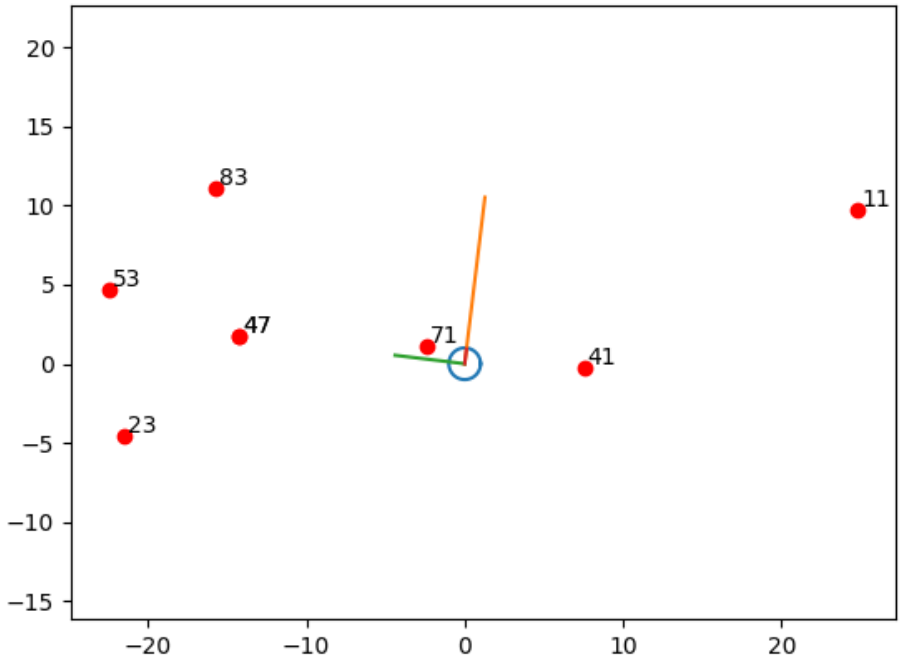
n=88


10
0
−10
−20
−30
−40
−50
−60
−60
−40
−20
0
20
40
37
59
11
53
47
71
17
29
23
19
31
43
61
67

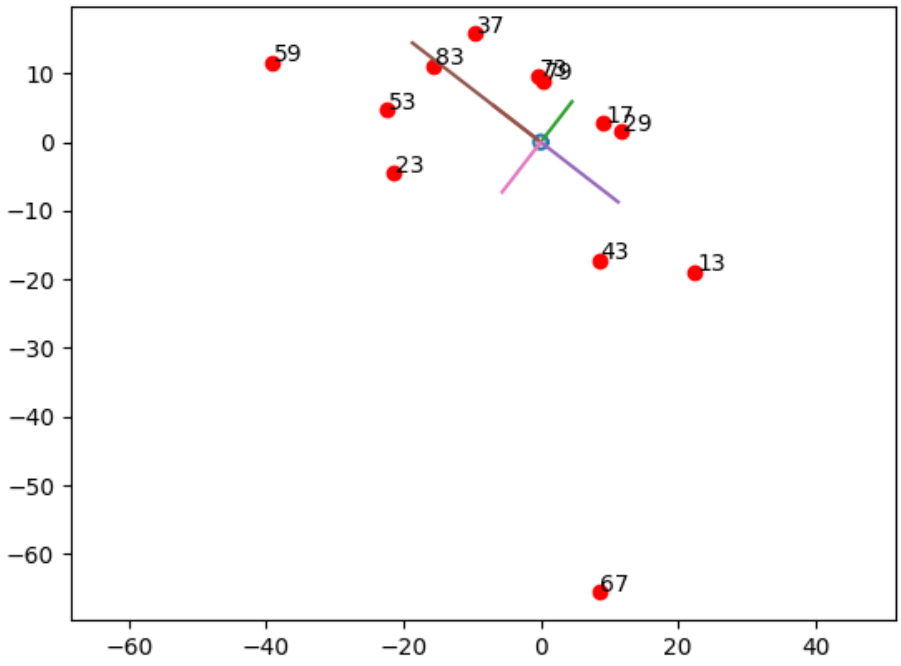
n=90



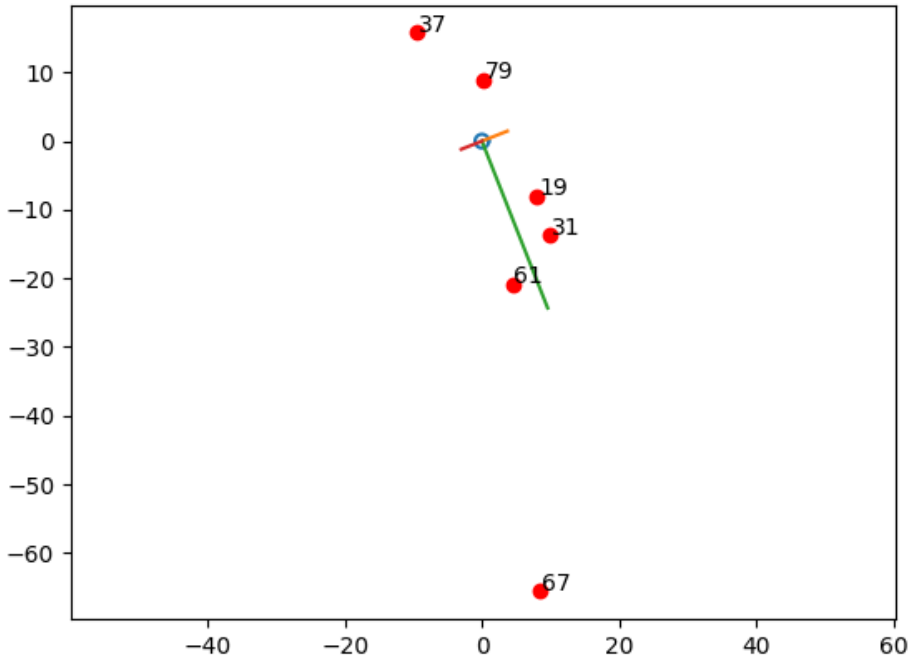
n=92



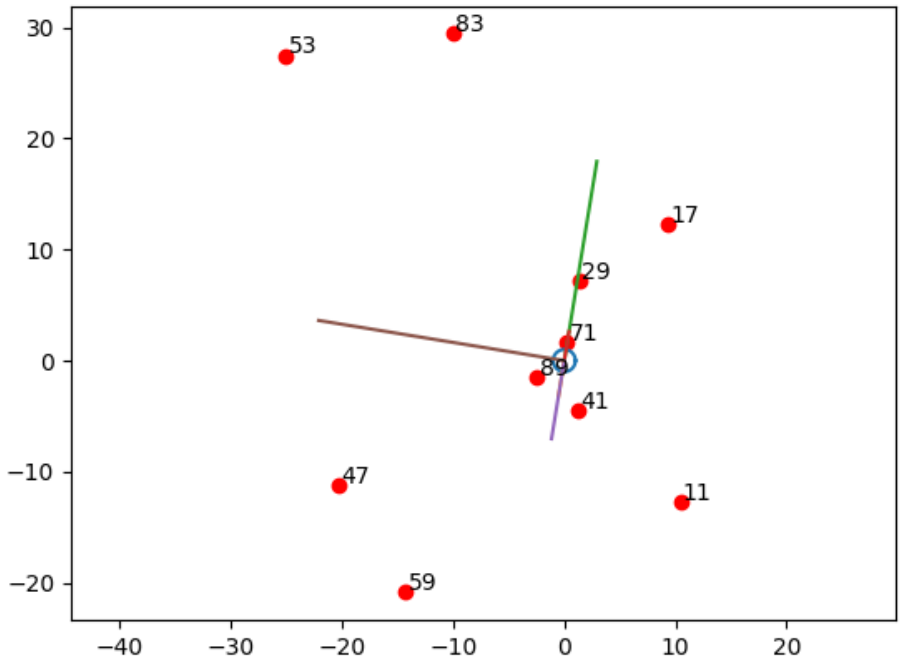
n=94 (p)


37
59
83
53
17
29
23
43
13
67
10
0
−10
−20
−30
−40
−50
−60
−60
−40
−20
0
20
40

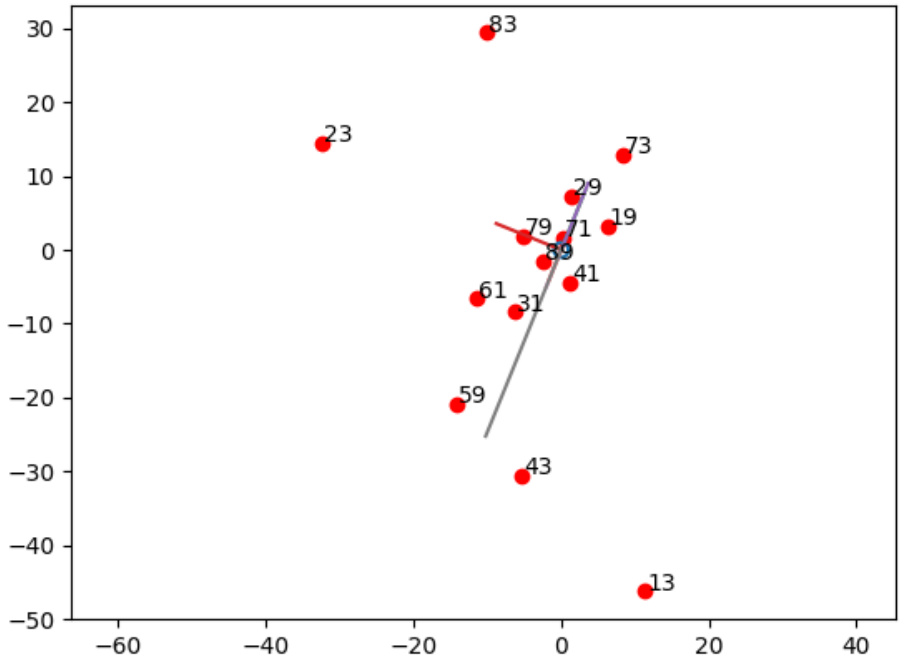
n=96


37
79
19
31
61
67
10
0
−10
−20
−30
−40
−50
−60
−40
−20
0
20
40
60

n=98

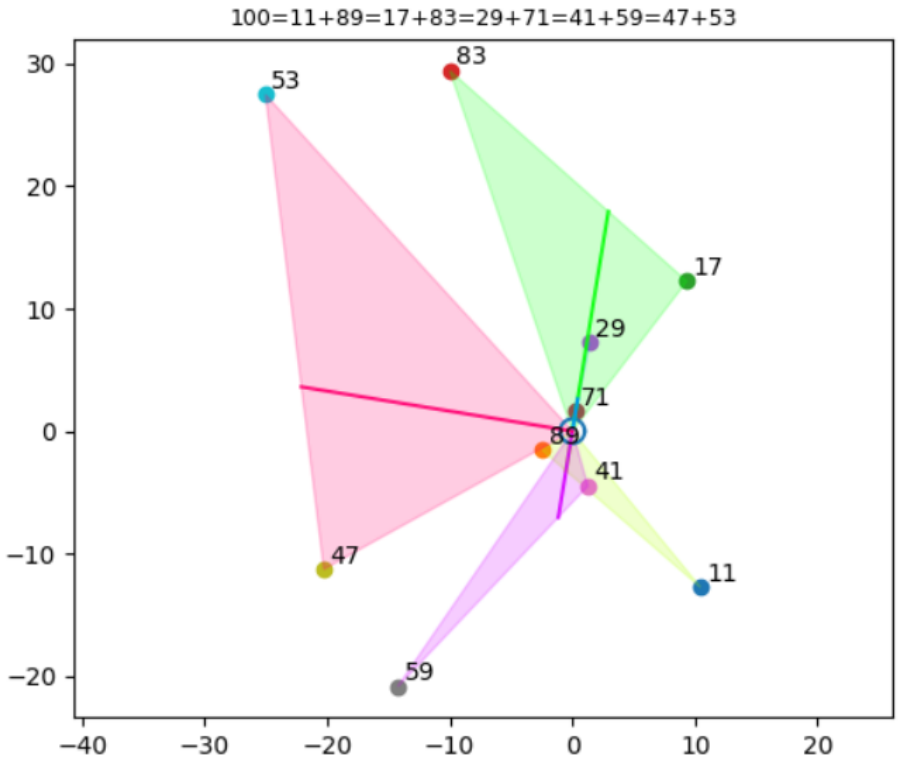


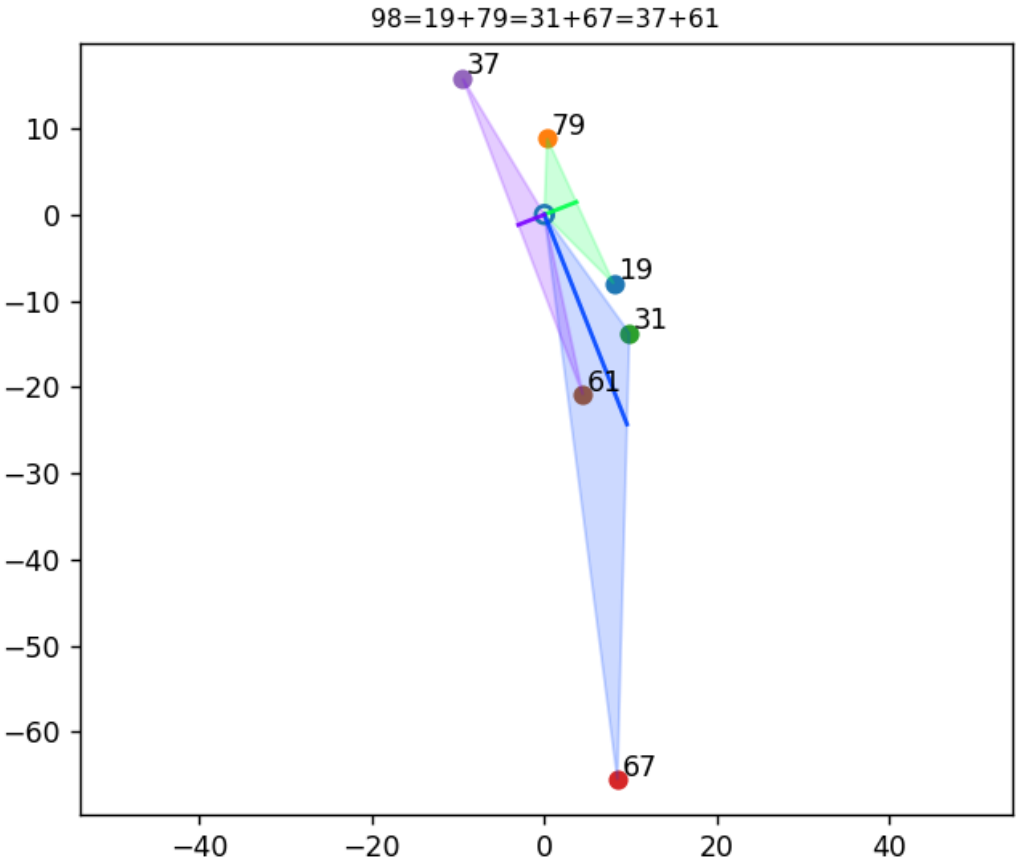
n=100



n=102

La visualisation des petits triangles $(0, z_1, z_2)$ permet d'obtenir les papillons multi-ailes ci-dessous :


100=11+89=17+83=29+71=41+59=47+53
83
53
17
29
71
89
41
47
11
59
30
20
10
0
−10
−20
−40
−30
−20
−10
0
10
20


98=19+79=31+67=37+61
37
79
19
31
61
67
10
0
−10
−20
−30
−40
−50
−60
−40
−20
0
20
40

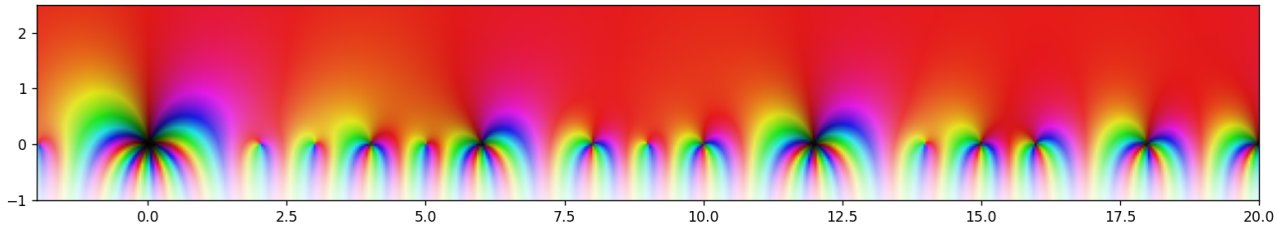
Utiliser en lieu et place des fonctions utilisées sur les réels les mêmes fonctions mais envoyant un complexe sur un complexe

Un petit programme permet d'afficher les produits utilisés pour trouver les décomposants de Goldbach, en les faisant voir comme les *non-zéros* d'une fonction fournissant une image complexe pour un nombre complexe.

Considérons d'abord la fonction :

$$\prod_{\substack{2\leq x\leq n/2\\ 2\leq p\leq\sqrt{n}}} \left(1-\exp\left(\frac{2\pi i\, x}{p}\right)\right)$$

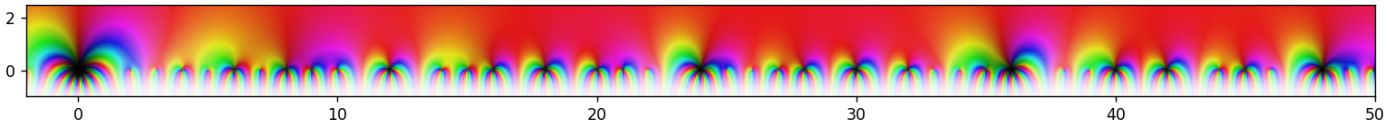
En prenant $n = 40$ et en ne faisant dessiner qu'un rectangle restreint (jusqu'à 20, la moitié de 40), on voit apparaître, comme prévu, les nombres premiers compris entre la racine carrée de 40 ($\simeq 6$) et 20.



n=40

On repère aisément sur le graphe de la fonction qu'elle ne s'annule pas pour les nombres premiers 7, 11, 13, 17 et 19. Un examen attentif de la figure fait même remarquer que le nombre de diviseurs est visible sur les "dendrites" des zéros : 12, qui a 4 diviseurs compris entre 2 et 6, qui sont 2, 3, 4 et 6, a plusieurs dendrites de différentes couleurs qui partent de lui et on dénombre 4 fois la couleur bleu par exemple ; quant à 6, il n'a que 2 arcs-en-ciel qui partent de lui (et donc deux dendrites bleues par exemple), correspondant à ses 2 diviseurs 2 et 3. En quelque sorte, un nombre ayant beaucoup de diviseurs est plus facile à repérer qu'un nombre en ayant moins.

Pour $n = 98$, le graphique devient plus difficile à comprendre[2]



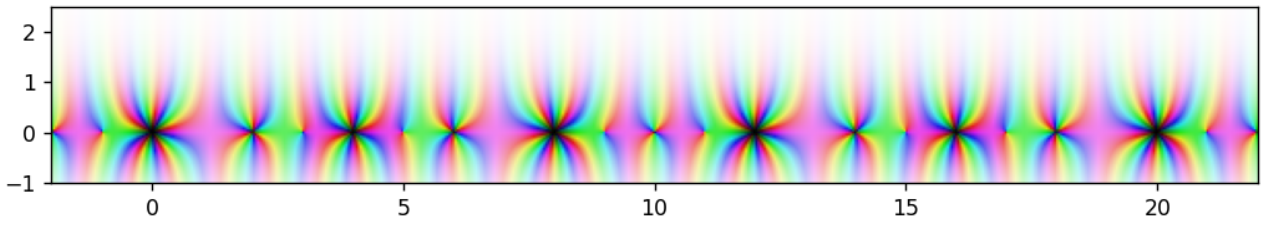
n=98

[2]Mais il reste notre nombre fétiche.

Considérons maintenant la fonction :

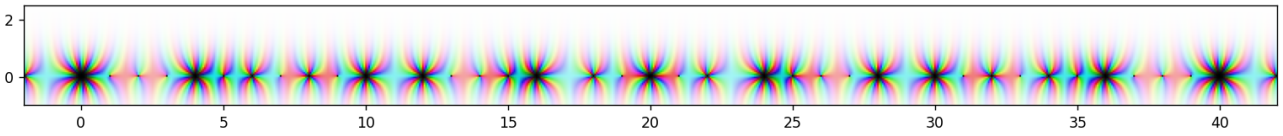
$$\prod_{\substack{2\leq x\leq n/2\\ 2\leq p\leq\sqrt{n}}}\left(1-\exp\left(\frac{2\pi i\,x}{p}\right)\right)\times\prod_{\substack{2\leq x\leq n/2\\ 2\leq p\leq\sqrt{n}}}\left(1-\exp\left(\frac{2\pi i\,(n-x)}{p}\right)\right)$$

Voici les affichages obtenus pour $n = 20$ et $n = 40$.



n=20

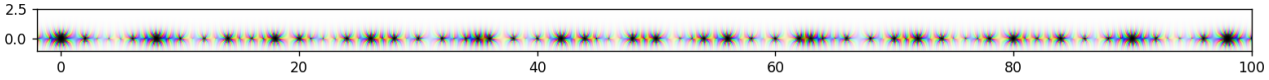
On voit bien l'absence de zéro pour le nombre 7 ($20 = 7 + 13$) ainsi que pour le nombre 1, auquel on ne s'intéresse pas. Notons également l'absence de zéro en 9.5 et 10.5 qui ne sont pas des nombres premiers, mais qui présente la même symétrie qu'on trouve pour les décomposants de Godlbach.



n=40

On voit bien l'absence de zéro pour les nombres 11 et 17 ($40 = 11 + 29 = 17 + 23$). À ces nombres correspondent des petites zones intégralement bleu ciel en forme de losanges allongés dans le sens vertical et aux côtés incurvés entrants vers les centres des losanges.

Pour 98, le graphique est ininterprétable, dommage.



n=98

Décomposants de Goldbach dans le plan complexe (Denise Vella-Chemla, 8.7.2024)

On partage ci-dessous les graphiques obtenus par programme, qui montrent les parties réelle et imaginaire des produits :

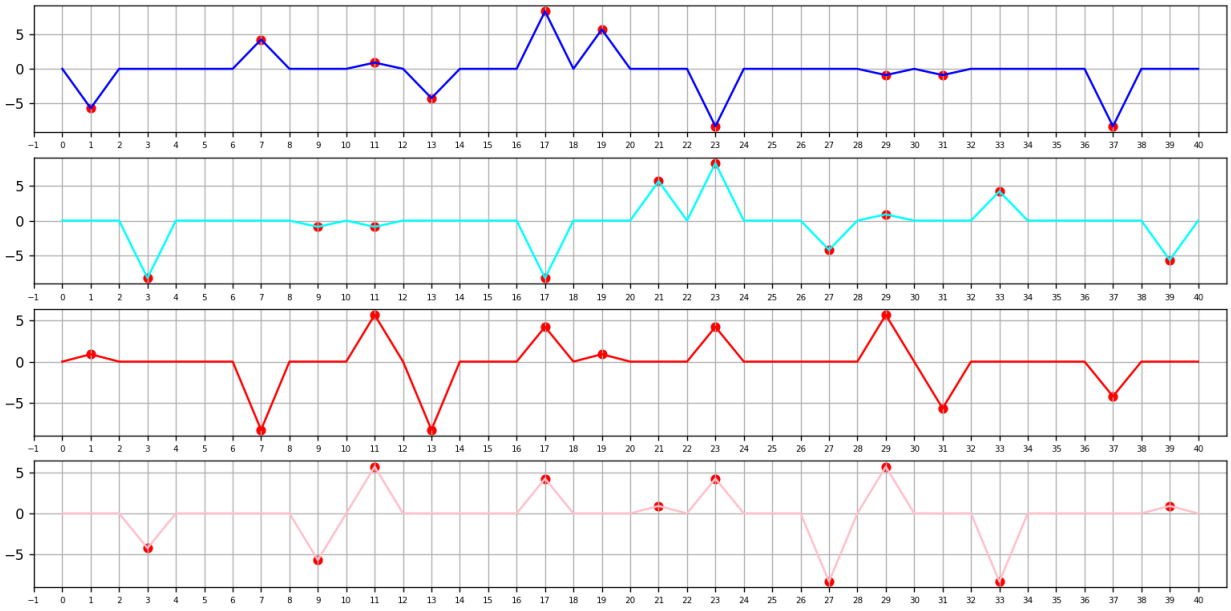
$$A = \prod_{\substack{x\in\mathbb{N} \\ 0\leq x\leq n \\ 2\leq p\leq\lfloor\sqrt{n}\rfloor}} \left(1 - \exp\left(\frac{2i\pi x}{p}\right)\right)$$

et

$$A' = \prod_{\substack{x\in\mathbb{N} \\ 0\leq x\leq n \\ 2\leq p\leq\lfloor\sqrt{n}\rfloor}} \left(1 - \exp\left(\frac{2i\pi (n-x)}{p}\right)\right).$$

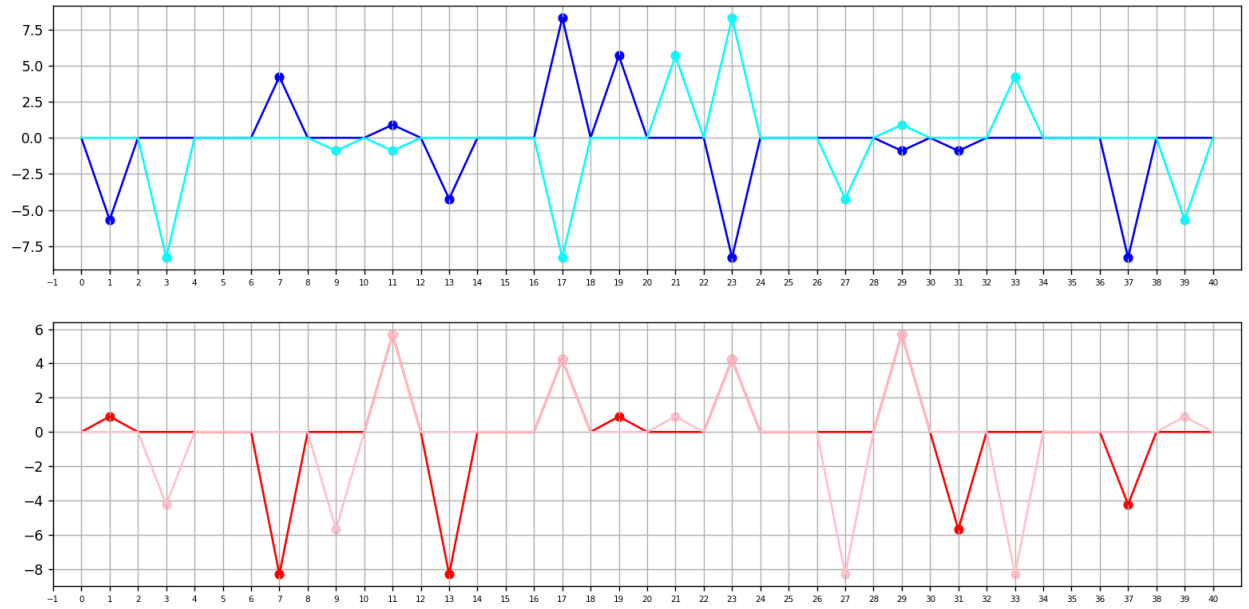
Dans le premier graphique, en bleu, la partie réelle $\mathfrak{Re}(A)$, en cyan, la partie réelle $\mathfrak{Re}(A')$, symétrique par rapport à 0 de la courbe bleue (par l'application $x \mapsto n - x$). En rouge, la partie imaginaire $\mathfrak{Im}(A)$, en rose, la partie imaginaire $\mathfrak{Im}(A')$, symétrique par rapport à 0 de la courbe rouge (par l'application $x \mapsto n - x$).

Sur toutes les courbes, on note par des petits cercles pleins les points de la courbe dont l'abscisse x est un entier impair d'image strictement positive.

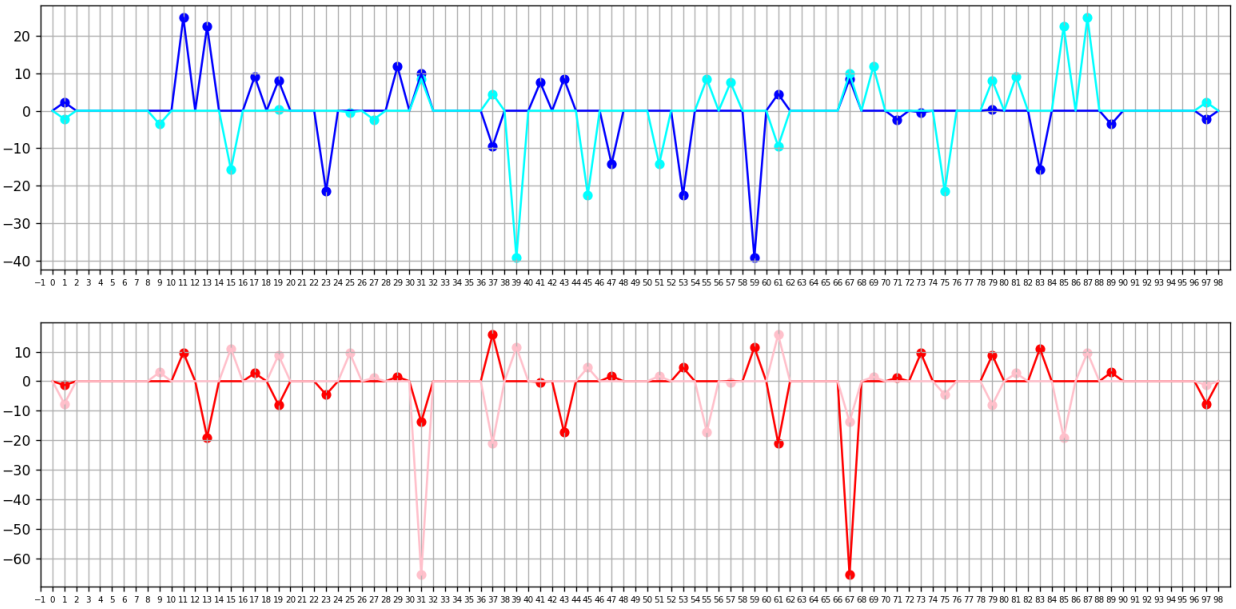


On regroupe dorénavant sur un même graphique les courbes et leur courbe symétrique.

Pour $n = 40$ ci-dessous, apparaissent sur les courbes bleu et cyan les décompositions de Goldbach $11 + 29$ et $17 + 23$.

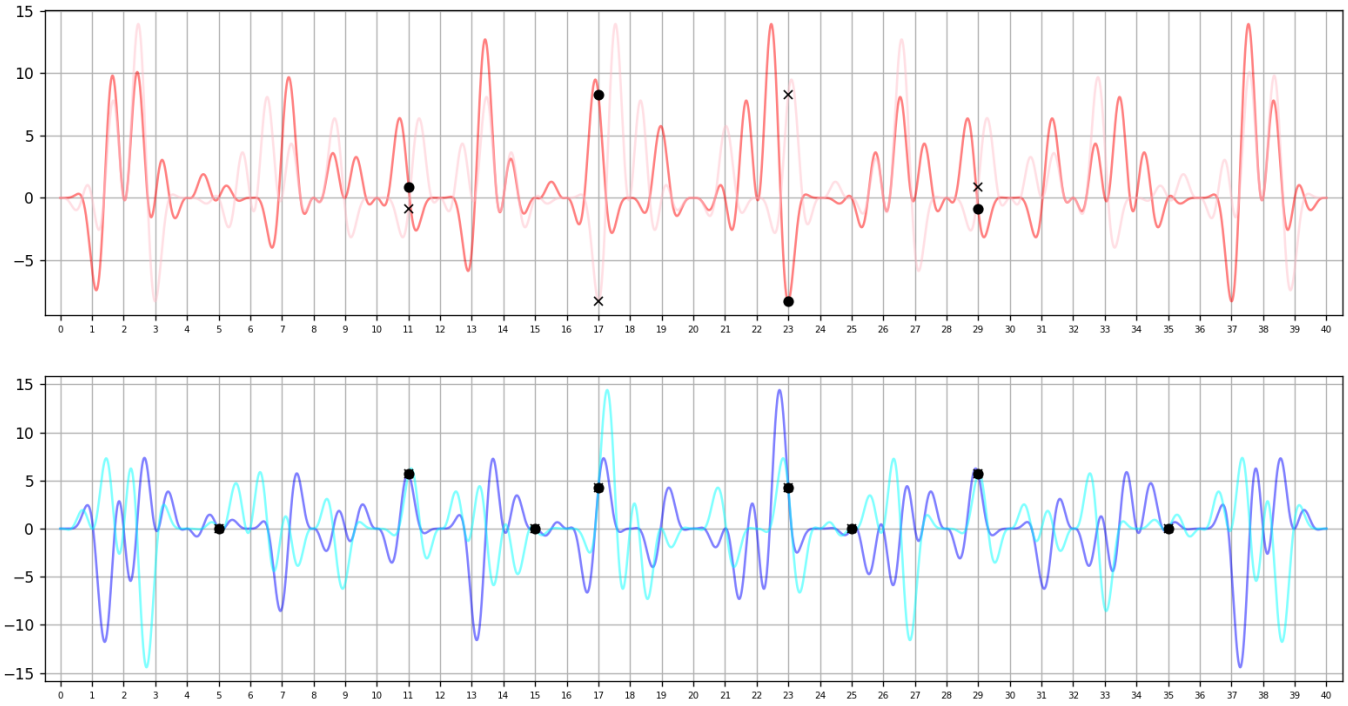


Pour $n = 98$ ci-dessous, apparaissent les décompositions de Goldbach $19 + 79$, $31 + 67$ et $37 + 61$ de 98

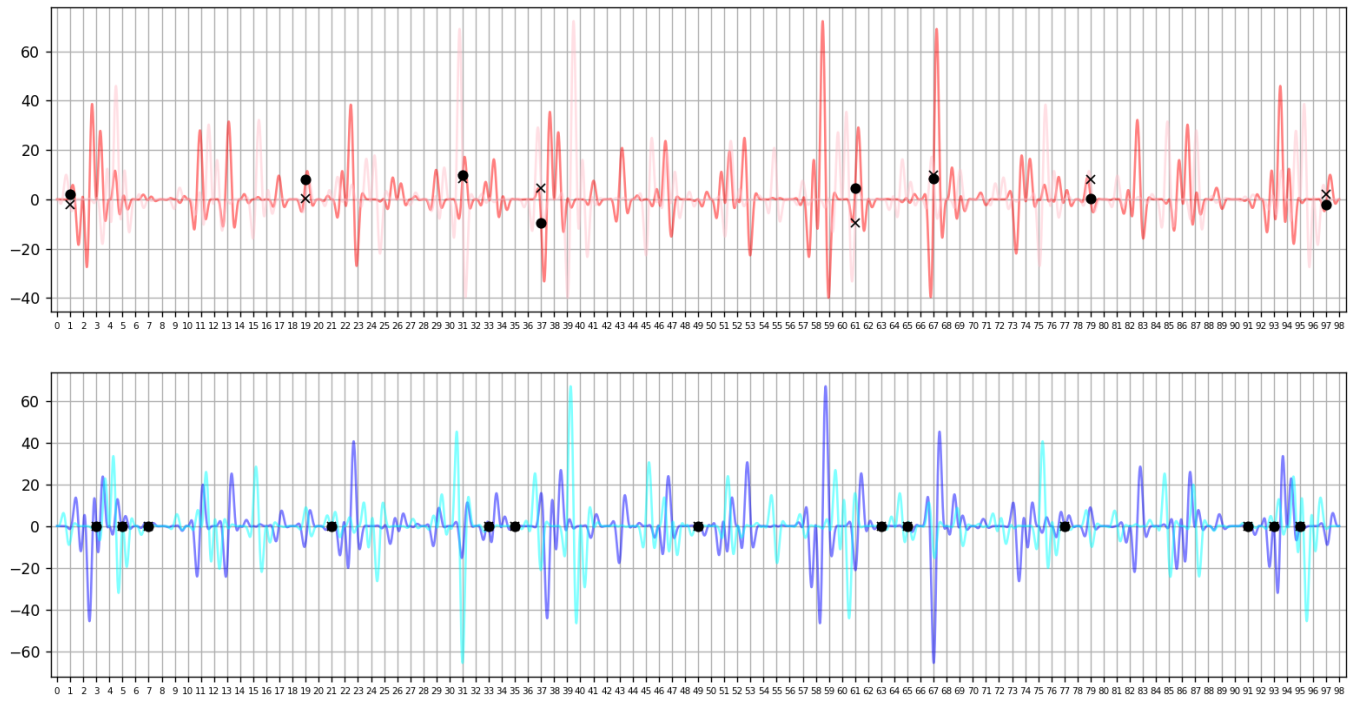


On “lisse” maintenant les courbes, en intercalant de nouveaux points dans leur domaine de définition, i.e. en intercalant entre les images des entiers les images de nombres rationnels de plus en plus resserrés.

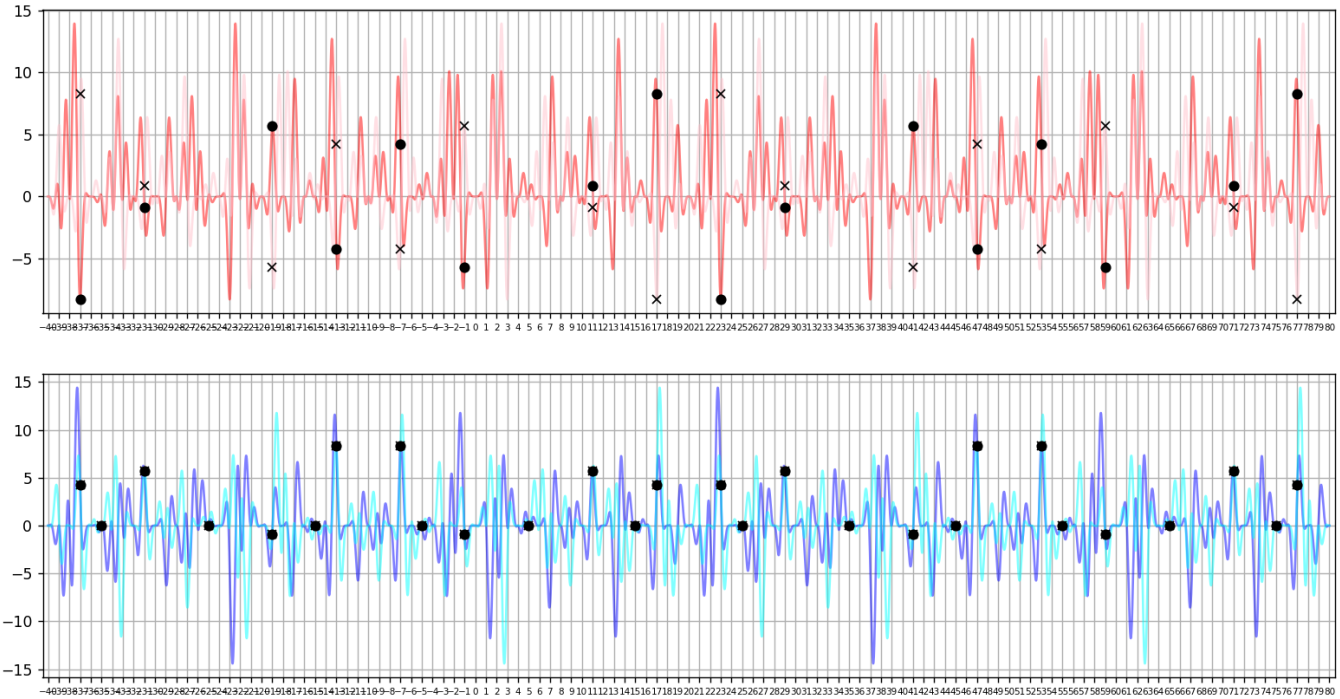
Sur les courbes bleu et cyan, on note les points tels que x et $n - x$ ont la même image. Ci-dessous les courbes continues pour le cas $n = 40$.



Voyons les courbes lorsque $n = 98$.

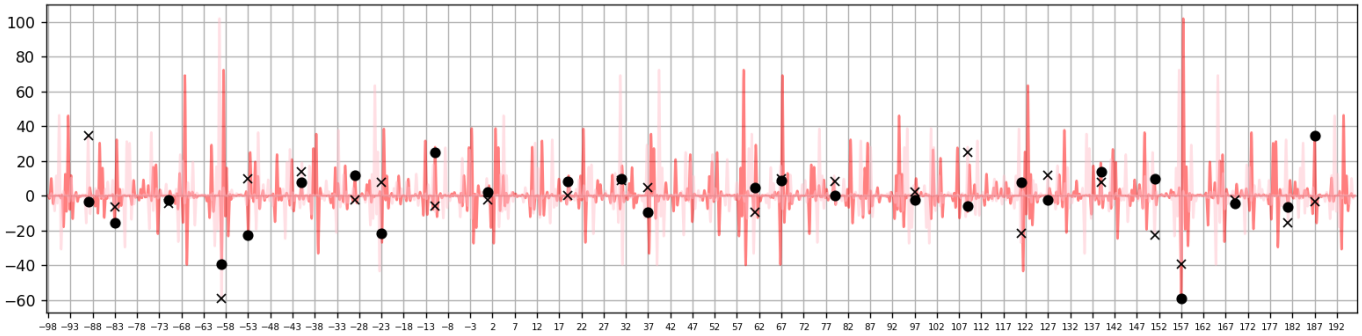


On peut d'autre part étendre l'intervalle d'étude des décompositions. Ci-dessous, le cas $n = 40$.



Pour $n = 40$, sur un intervalle étendu $[-40, 80]$, on trouve de nouvelles décompositions de Goldbach qui font intervenir des nombres premiers impairs négatifs $(-7)+47, (-13)+53, (-19)+59, (-31)+71$. La décomposition $(-37)+77$ n'est pas une décomposition de Goldbach de 40 car 77 est divisible par 7 qui est un nombre premier supérieur à la racine carrée de 40.

Voyons le cas $n = 98$.



Pour $n = 98$, sur un intervalle étendu (moins bien lisible) $[-98, 196]$, on trouve de nouvelles décompositions de Goldbach qui font intervenir des nombres impairs négatifs $(-11)+109, (-29)+127, (-41)+139, (-53)+151, (-59)+157, (-83)+181$. Les décompositions $(-23)+121, (-71)+169$ et $(-89)+187$ ne sont pas des décompositions de Goldbach de 98 (bien que notées sur le graphique comme points d'abscisse impaire et d'ordonnée strictement positive).[1]

[1] On trouvera les courbes fournissant les décompositions de Goldbach des nombres compris entre 6 et 100 dans le fichier https://denisevellachemla.eu/toutes-courbes.pdf.

Décomposants de Goldbach dans le plan complexe (Denise Vella-Chemla, 9.7.2024)

Hier, on a étudié les graphiques obtenus par programme, qui montrent les parties réelle et imaginaire des produits :

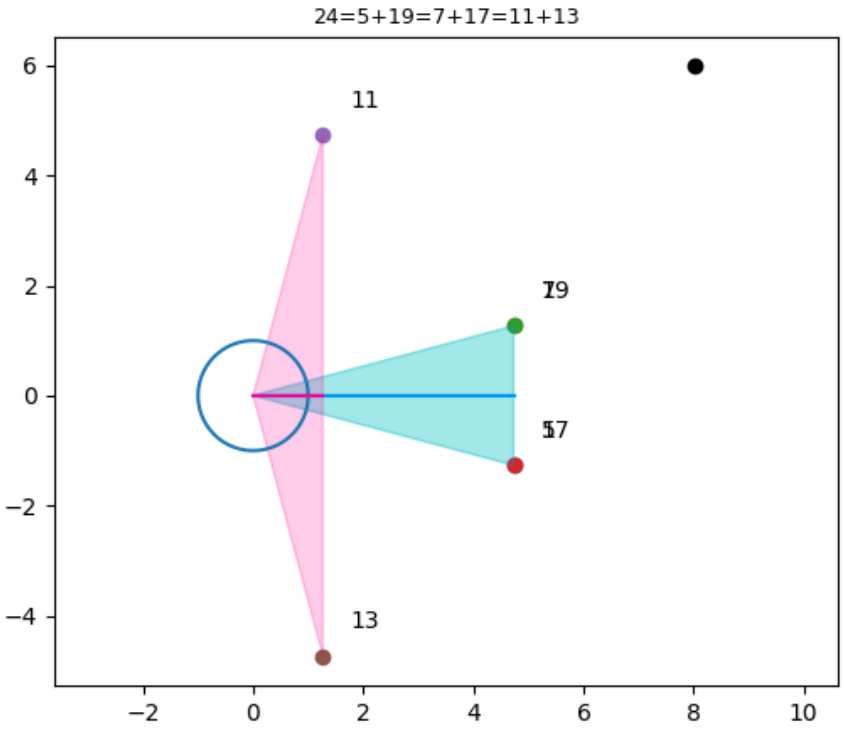
$$A = \prod_{\substack{x\in\mathbb{N} \\ 0\leq x\leq n \\ 2\leq p\leq\lfloor\sqrt{n}\rfloor}} \left(1 - \exp\left(\frac{2i\pi x}{p}\right)\right)$$

et

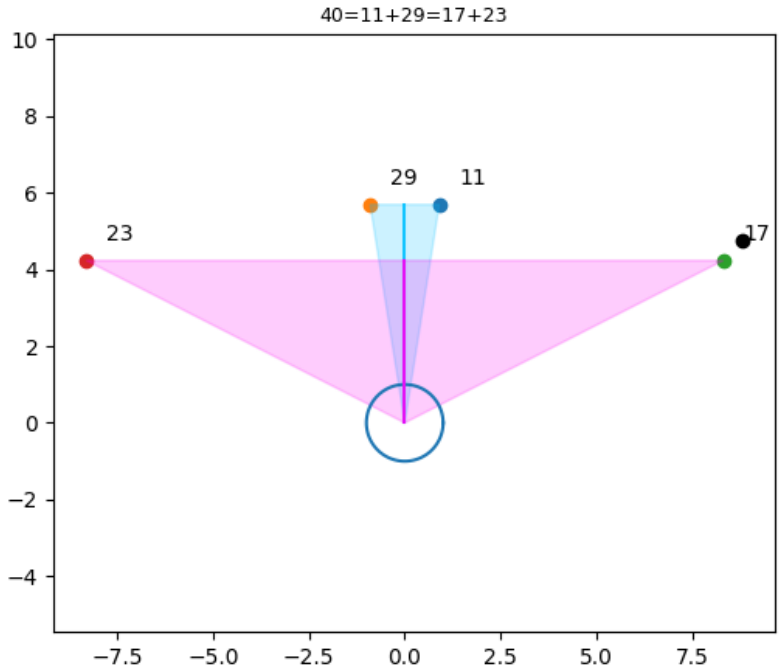
$$A' = \prod_{\substack{x\in\mathbb{N} \\ 0\leq x\leq n \\ 2\leq p\leq\lfloor\sqrt{n}\rfloor}} \left(1 - \exp\left(\frac{2i\pi (n-x)}{p}\right)\right).$$

Précédemment, on avait étudié les points du plan complexe d'affixes les produits en question. Trois nombres sont "intrigants" : les nombres 24, 40 et 78 car pour eux trois, ce qu'on avait appelé leurs papillons, sont bien positionnés parallèlement ou perpendiculairement aux axes réel et imaginaire du plan complexe selon les trois graphiques ci-dessous :

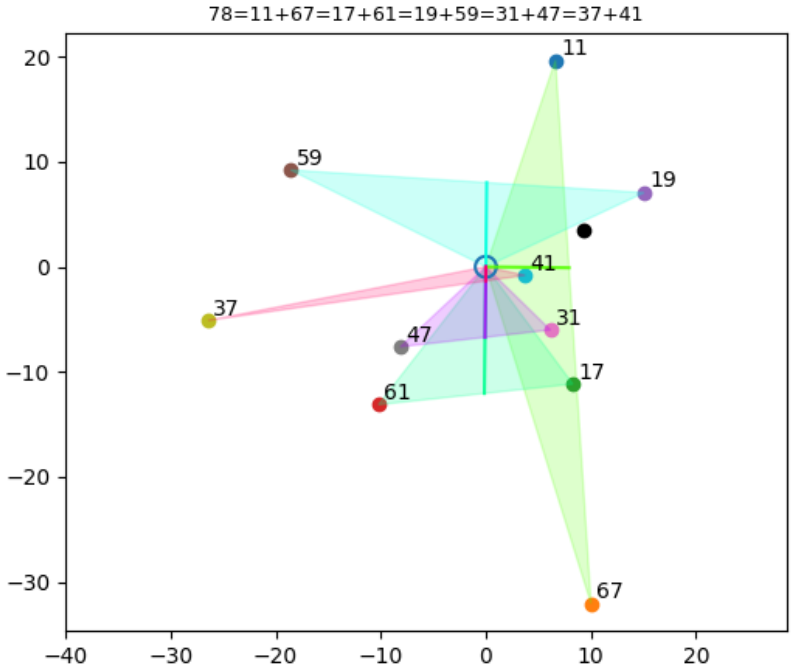
$n = 24$



$n = 40$

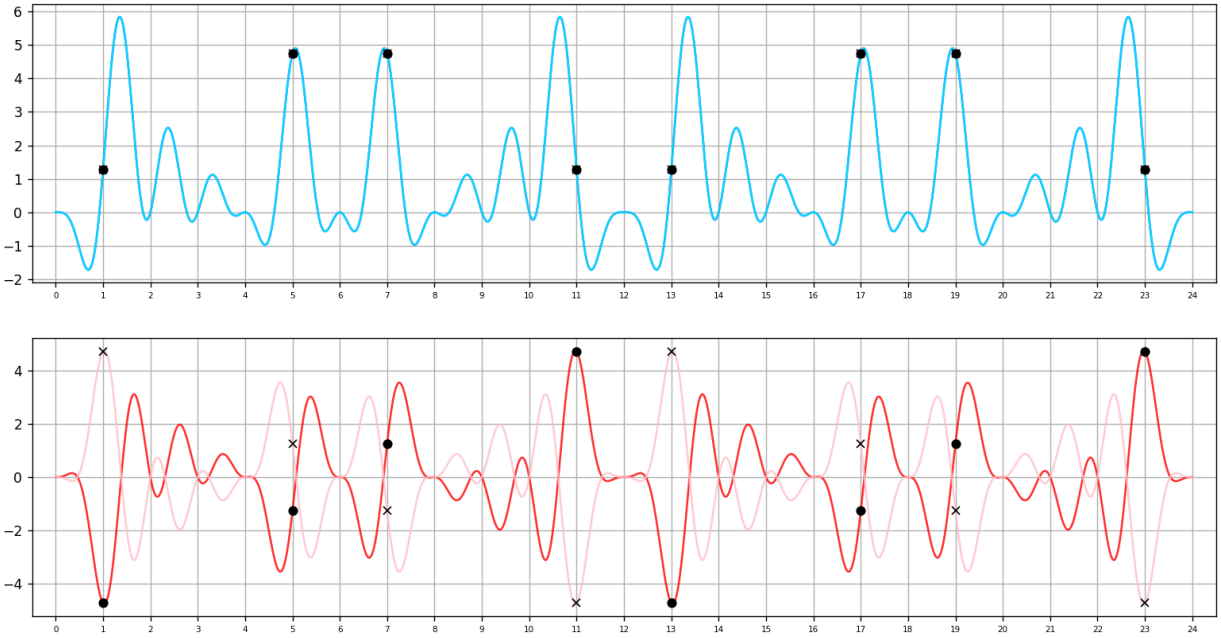

40=11+29=17+23
29
11
23
17

$n = 78$


78=11+67=17+61=19+59=31+47=37+41
11
59
19
41
37
31
47
17
61
67

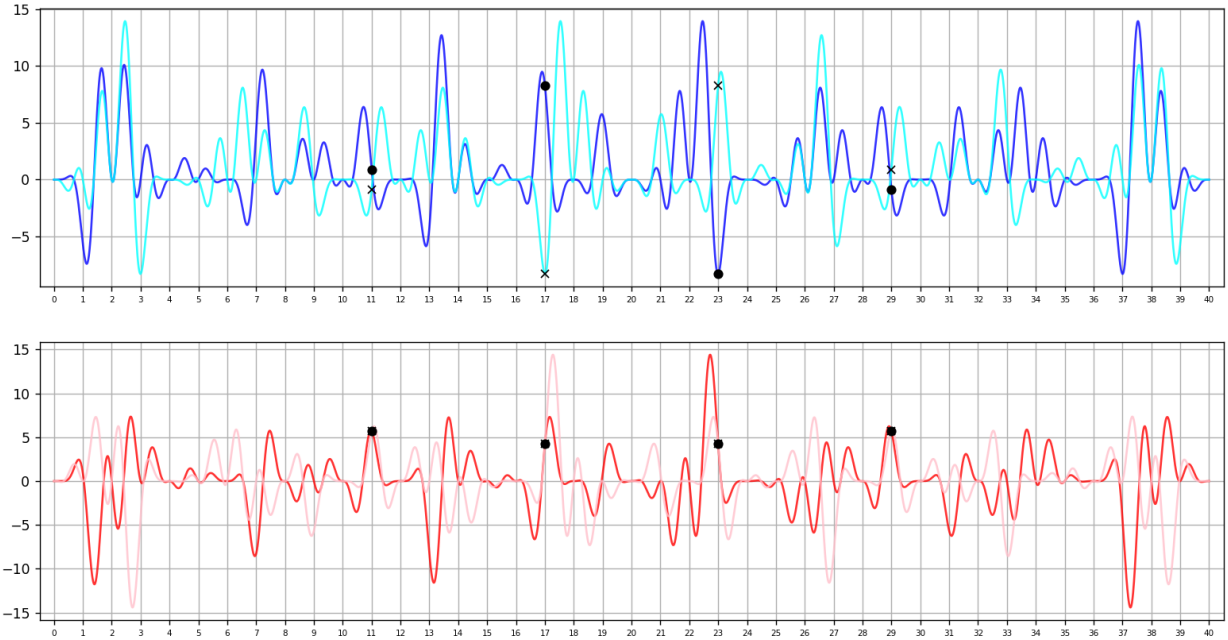
Voyons les courbes représentant les parties réelle et imaginaire des produits A et A' :

$n = 24$



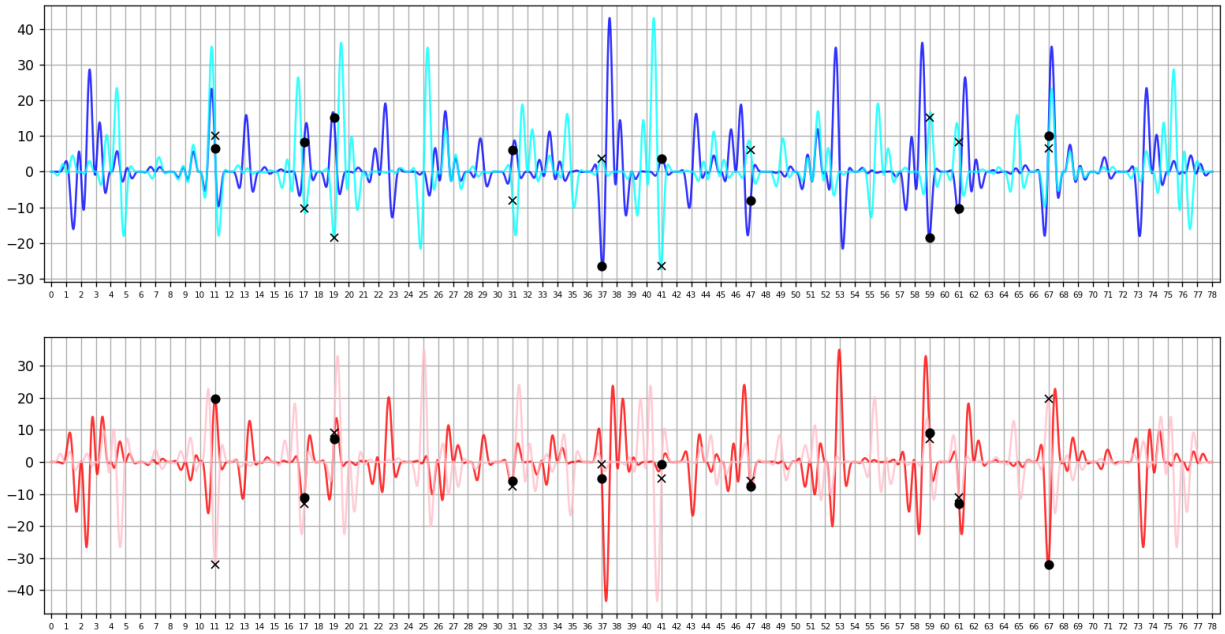
Les courbes correspondant aux parties réelles (bleu et cyan) de A et A' se confondent (se chevauchent), on ne voit qu'une couleur. Les courbes correspondant aux parties imaginaires (rouge et rose) ont leur point pour x et $n-x$ qui sont systématiquement de même valeur absolue et de signes opposés.

$n = 40$



On ne voit rien de flagrant.

$n = 78$



On ne voit rien de flagrant.

Etudions les affixes des décomposants de Goldbach dans ces trois cas particuliers :

$n = 24$

```
C:\Users\Denise_Vella\Desktop\discret-continu>python3 reecritunmoinsexp.py
1.0    1.2679491924311215    -4.732050807568877
5.0    4.732050807568876    -1.2679491924311241
7.0    4.7320508075688785    1.2679491924311168
11.0    1.2679491924311477    4.73205080756888
13.0    1.2679491924311301    -4.732050807568878
17.0    4.732050807568879    -1.2679491924311153
19.0    4.732050807568887    1.2679491924310933
23.0    1.267949192431165    4.732050807568884
```

$n = 40$

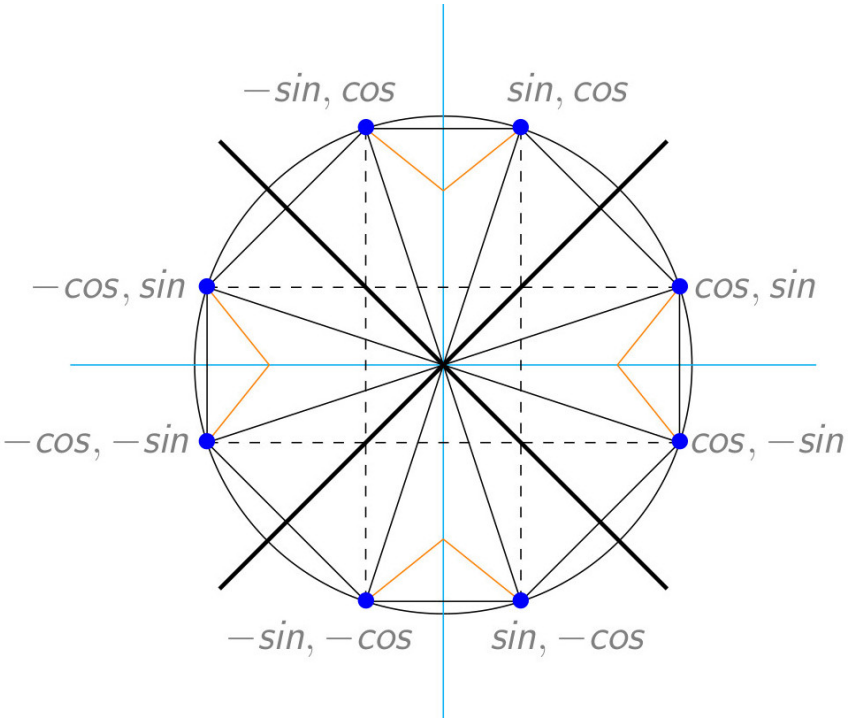
```
C:\Users\Denise_Vella\Desktop\discret-continu>python3 reecritunmoinsexp.py
11.0    0.9009210683668807    5.6881917600038125
17.0    8.3027665338464    4.2304708502054025
23.0    -8.302766533846421    4.2304708502055055
29.0    -0.9009210683668392    5.688191760003818
```

$n = 78$

```
C:\Users\Denise_Vella\Desktop\discret-continu>python3 reecritunmoinsexp.py
11.0    6.632870373769185    19.660516038160356
17.0    8.299678333414512    -11.158080007695919
19.0    15.071817475949711    7.050992357031933
31.0    6.145114297114057    -6.008742618841374
37.0    -26.435157439638004    -5.104281400350055
41.0    3.7383787468480847    -0.8092418192766322
47.0    -8.146605747120182    -7.615842514319597
59.0    -18.592231832233548    9.211936592187087
61.0    -10.228004158618768    -13.124942140007395
67.0    10.015721851067289    -32.04418420284733
```

Pour $n = 24$, on découvre certaines symétries entre différents affixes, au sein de chacune des courbes, et entre les 2 courbes (des parties réelles pour x et $n - x$) ; pour $n = 40$, on découvre certaines symétries au sein de chacune des deux courbes mais non pas entre les courbes ; pour $n = 78$, on ne découvre rien de similaire aux cas précédents.

La difficulté de localisation des décomposants de Goldbach serait peut-être dûe au fait qu'à un nombre entier correspondrait une rotation d'un certain angle des axes formant la base du plan complexe. Et la symétrie à laquelle il faudrait à nouveau réfléchir serait cette symétrie d'ordre 8 du cercle unité [1], à transposer sur des cercles plus ou moins grands.



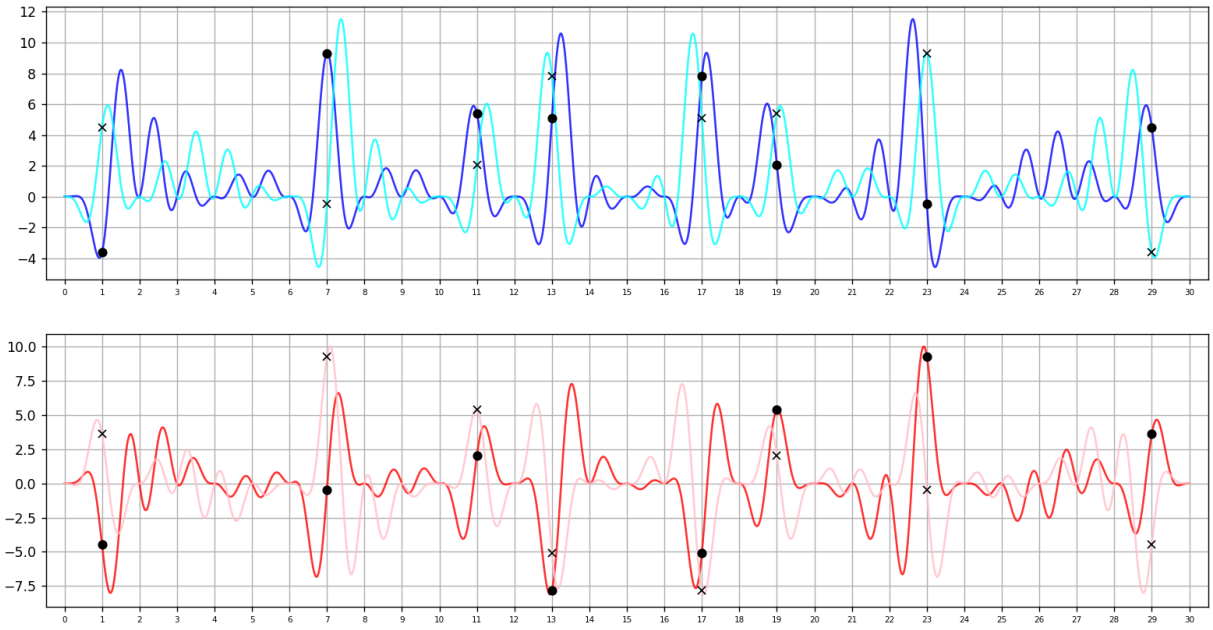
On rappelle que les deux opérateurs f et g du plan complexe, f envoyant le point $a+ib$ sur le point $b+ia$ et g envoyant le point $a+ib$ sur le point $-a+ib$ par exemple, ne commutent pas. En effet, si on les fait agir l'un avant l'autre, ou bien l'un après l'autre, sur un point (x, y), on n'obtient pas le même résultat :

[1] Les traits orange ont été ajoutés à titre décoratif.

- dans le premier cas $(g \circ f)$, on obtient : $(x, y) \to (y, x) \to (-y, x)$.

- dans le second cas $(f \circ g)$, on obtient : $(x, y) \to (-x, y) \to (y, -x)$.

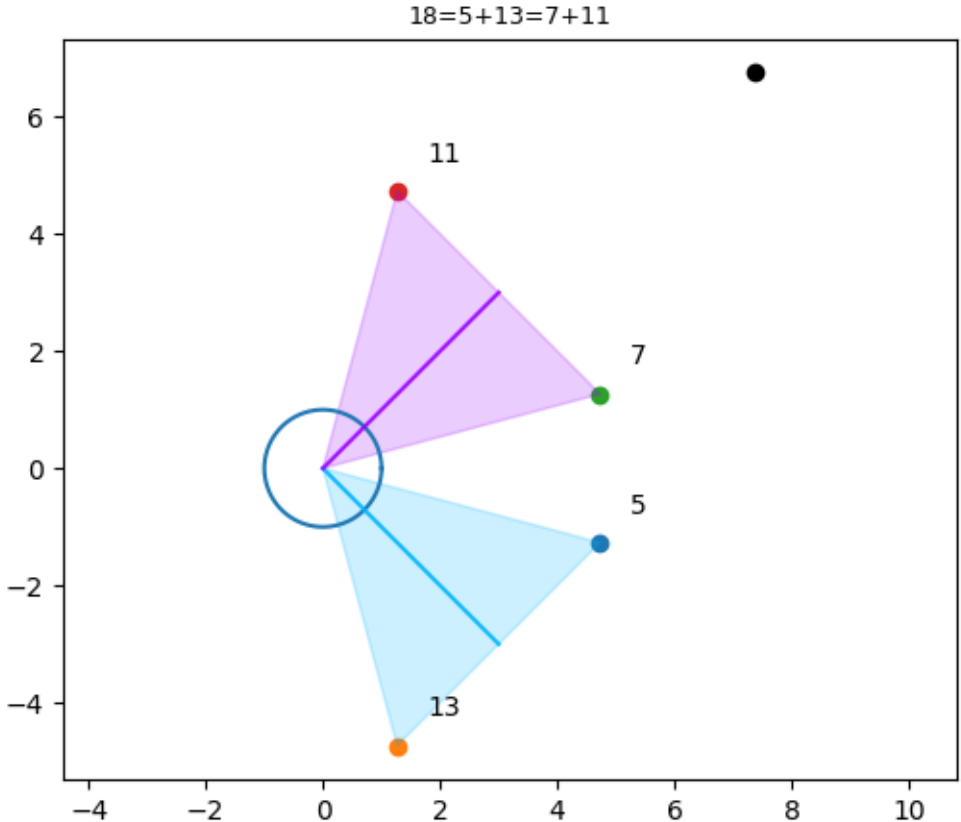
On voudrait également montrer ici les courbes associées au nombre 30 : l'ensemble des points non nuls des courbes bleu et cyan d'une part (ils sont marqués en noir et appartiennent à l'ensemble [1,7,11,13,17,19,23,29]), et l'ensemble des points non nuls des courbes rouge et rose d'autre part (ils sont marqués en noir et appartiennent à l'ensemble [3,5,9,15,21,25,27]), sont exactement complémentaires l'un de l'autre et couvrent l'ensemble des entiers impairs de l'intervalle $[0, 30]$ considéré. C'est marrant !

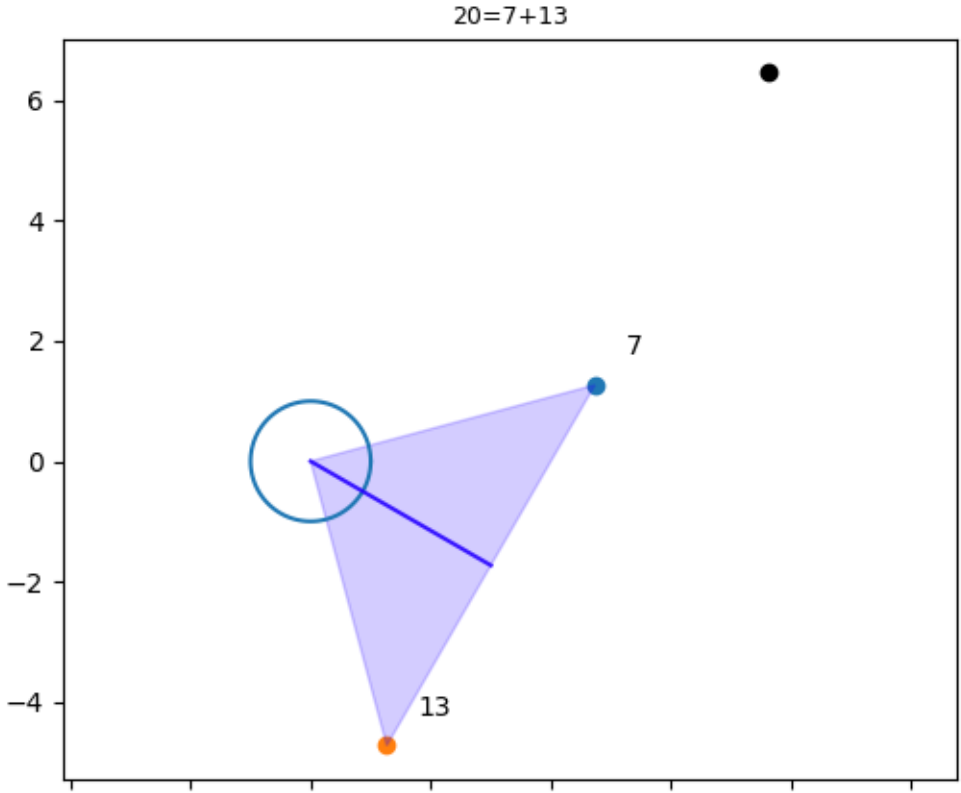


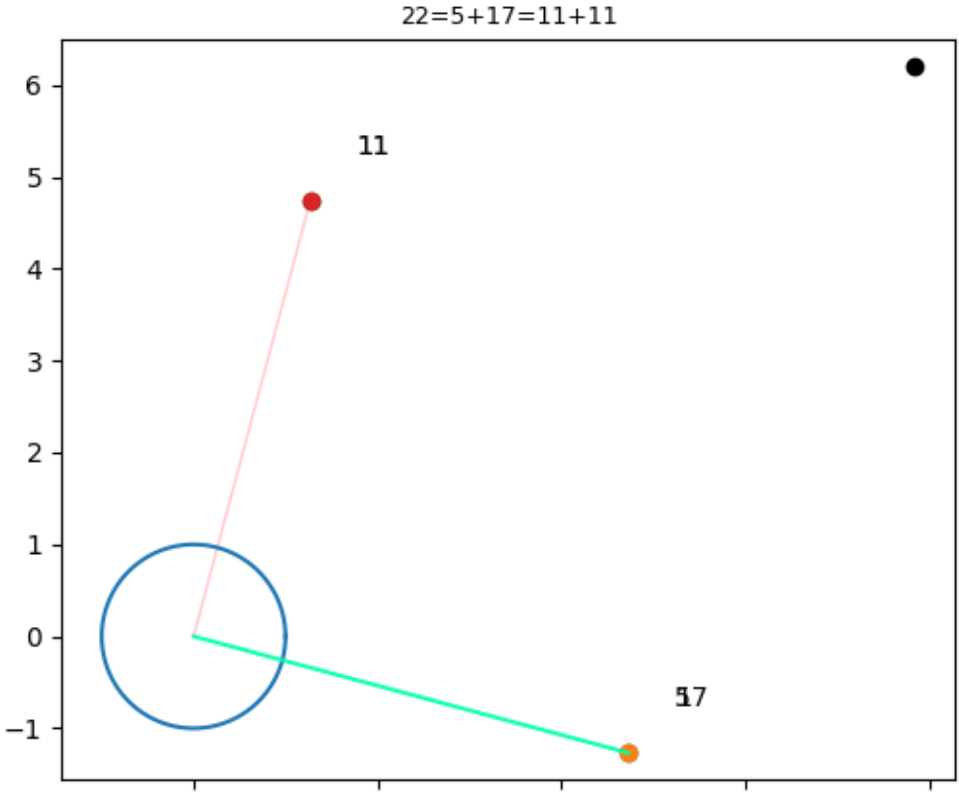
Voici les valeurs des affixes des décomposants dans ce cas particulier $n = 30$.

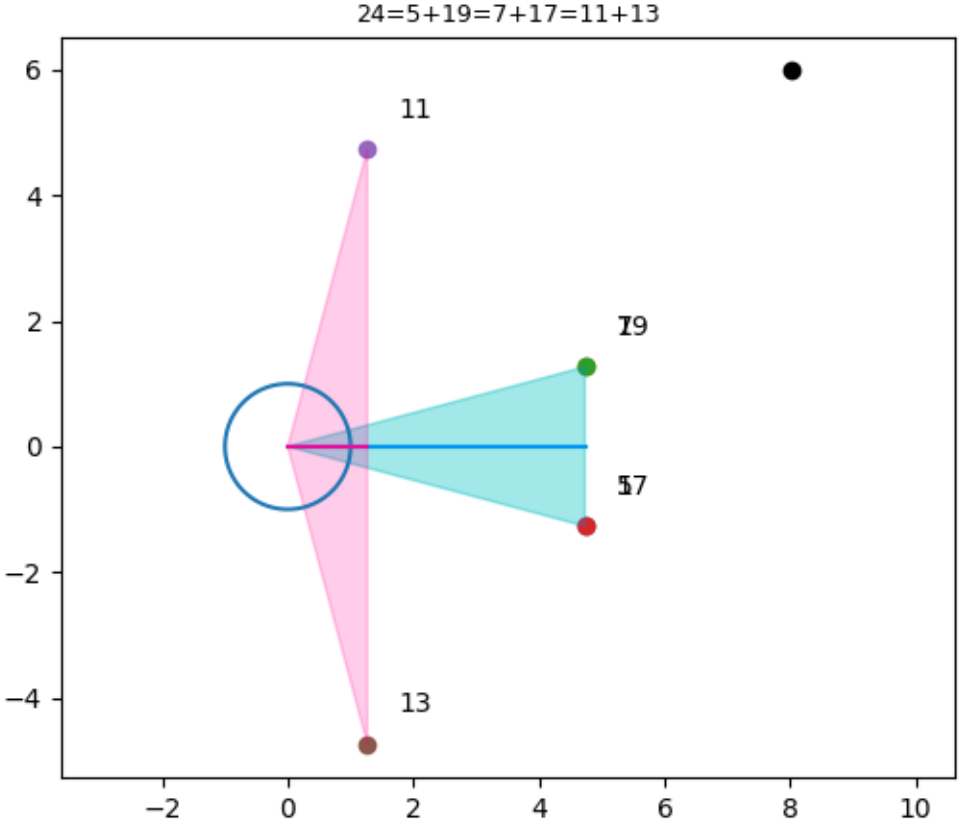
```
C:\Users\Denise_Vella\Desktop\discret-continu>python3 reecritunmoinsexp.py
1.0    -3.6243164120122096     -4.475658031577195
7.0    9.305642165104956     -0.4876880406757951
11.0    5.3765790999440535     2.063875347991572
13.0    5.075171314899577     -7.815078493170627
17.0    7.815078493170634     -5.075171314899555
19.0    2.063875347991642     5.376579099944031
23.0    -0.4876880406757045     9.305642165104997
29.0    4.475658031577203     3.6243164120122087
```

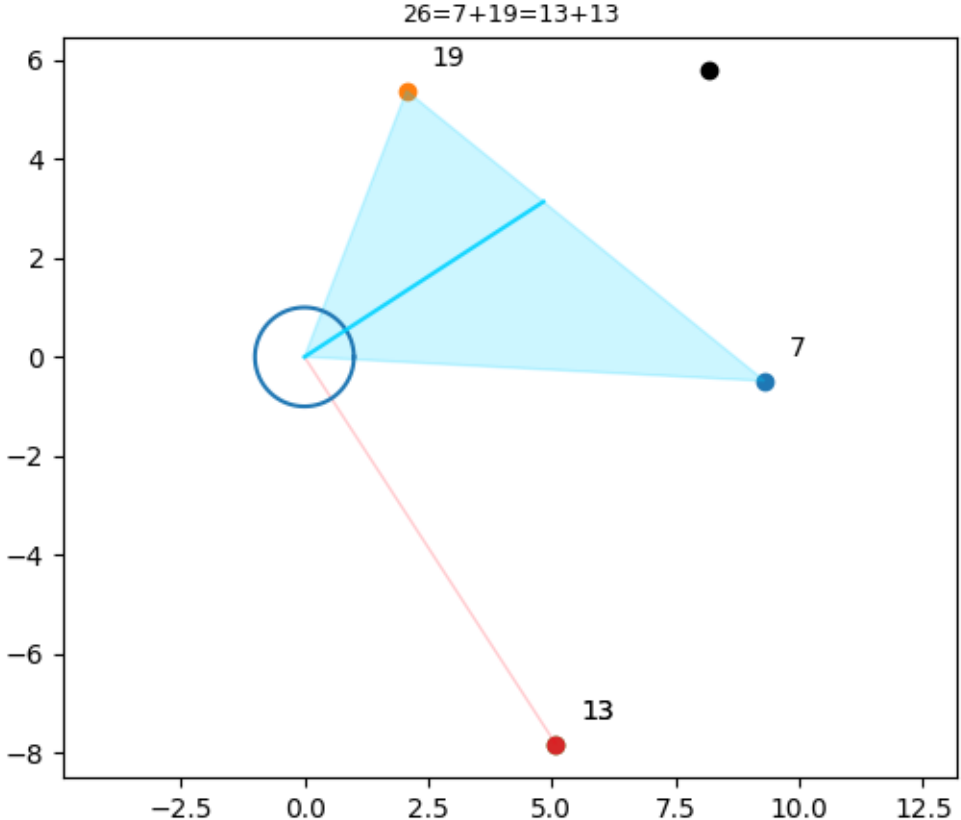
Dans ce cas, on trouve des correspondances entre les affixes d'un point correspondant à un décomposant de Goldbach de l'une des deux courbes et un autre point correspondant à un décomposant de Goldbach de l'autre courbe, mais non pas entre deux points différents appartenant à une seule des deux courbes.

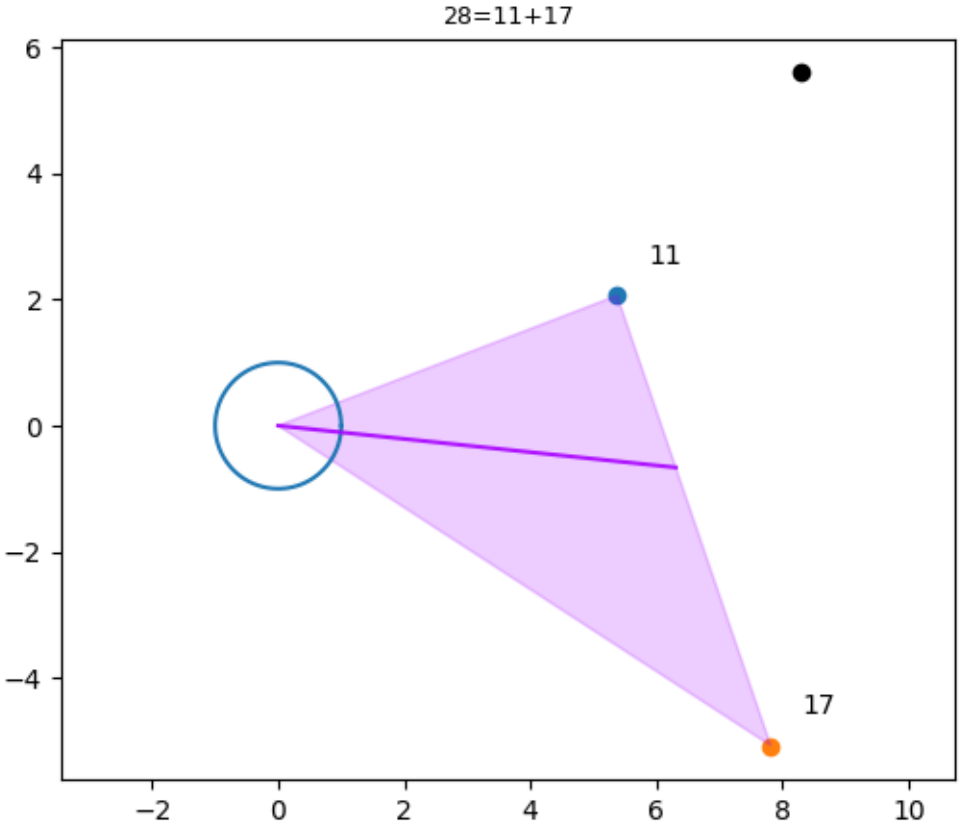

18=5+13=7+11
11
7
5
13
6
4
2
0
−2
−4
−4
−2
0
2
4
6
8
10

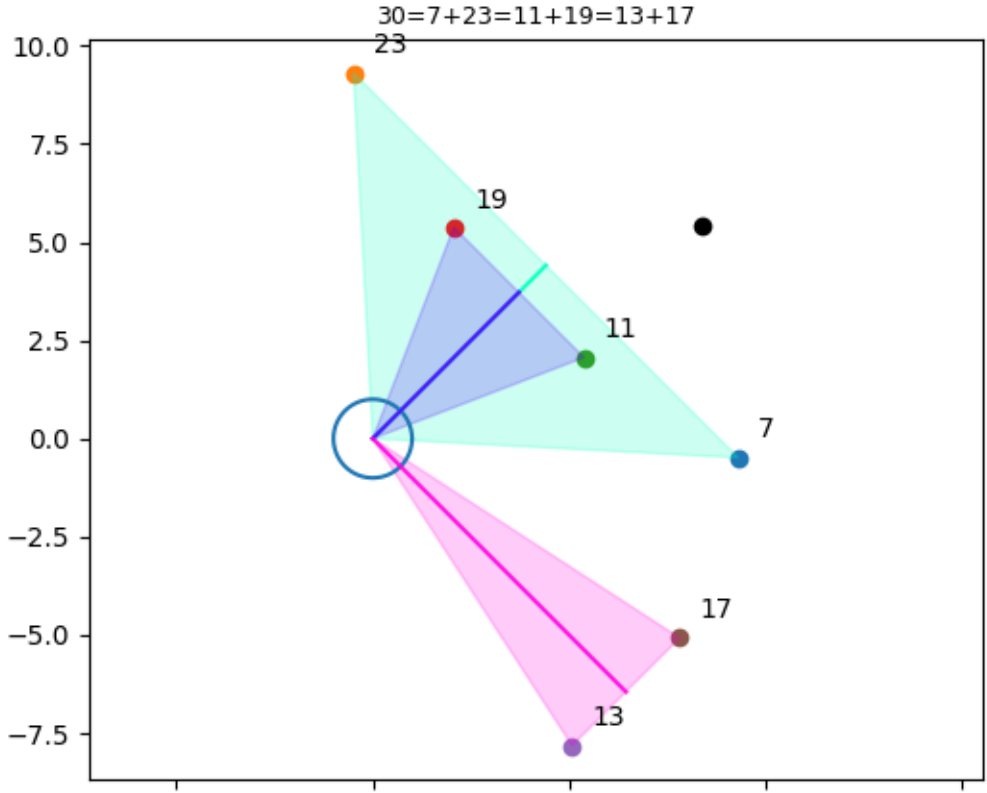

20=7+13
7
13

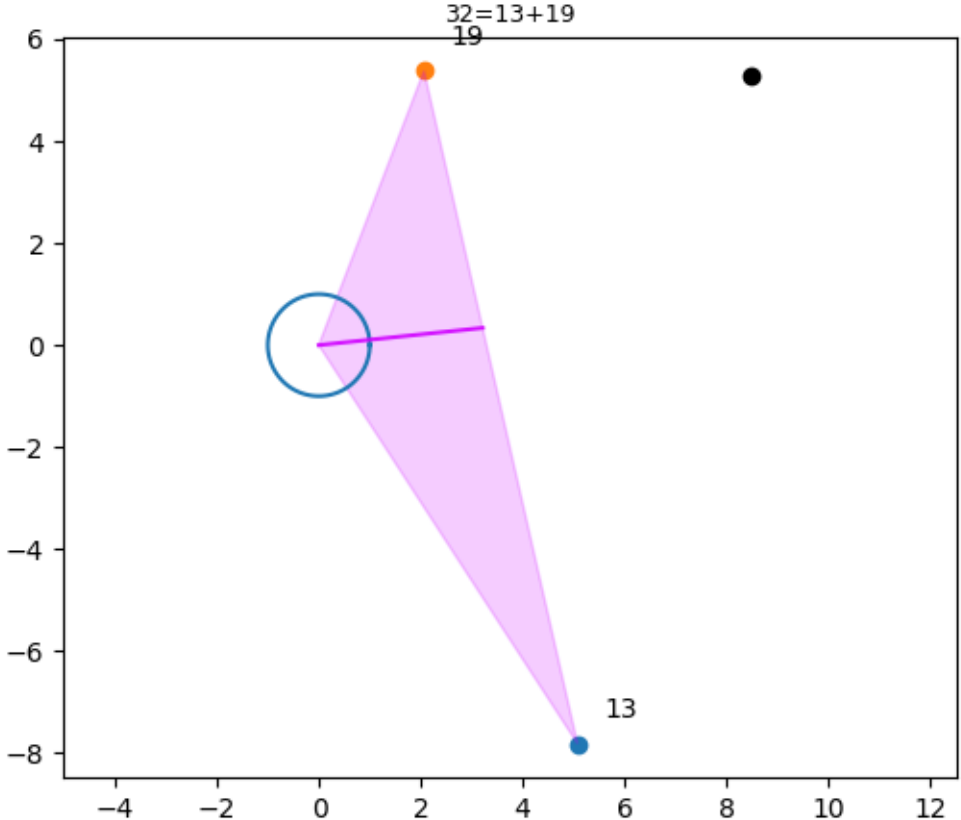

22=5+17=11+11
11
17
6
5
4
3
2
1
0
−1
0
2
4
6
8

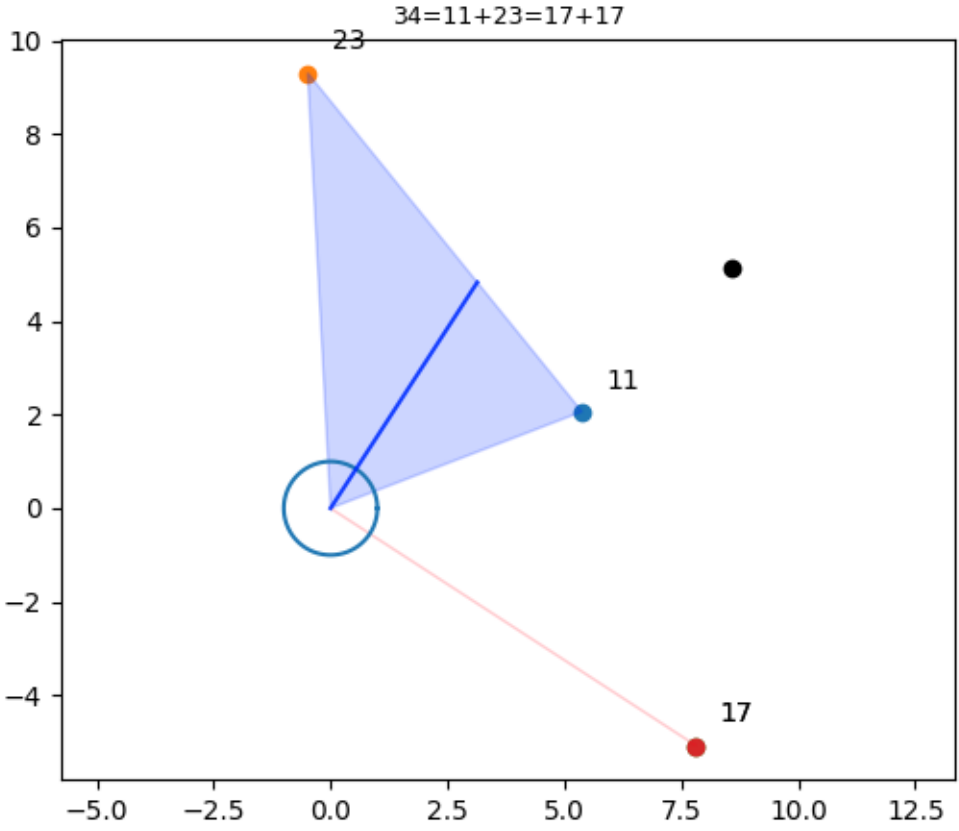

24=5+19=7+17=11+13
11
19
17
13
6
4
2
0
−2
−4
−2
0
2
4
6
8
10

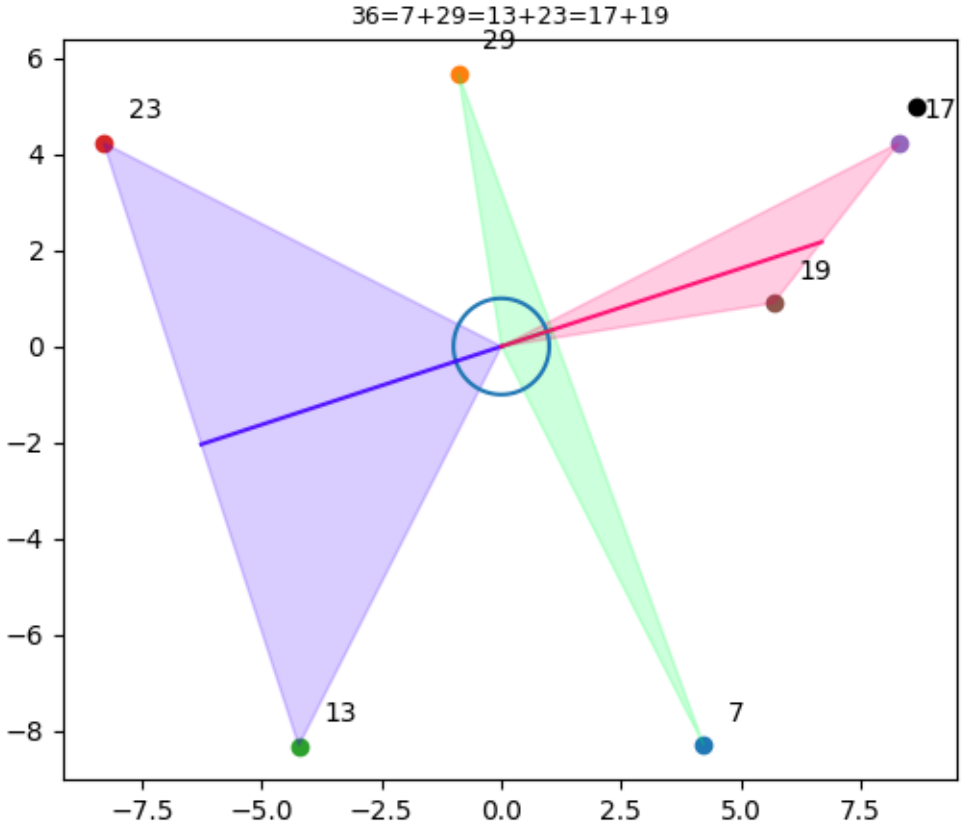

26=7+19=13+13
19
7
13
6
4
2
0
−2
−4
−6
−8
−2.5
0.0
2.5
5.0
7.5
10.0
12.5

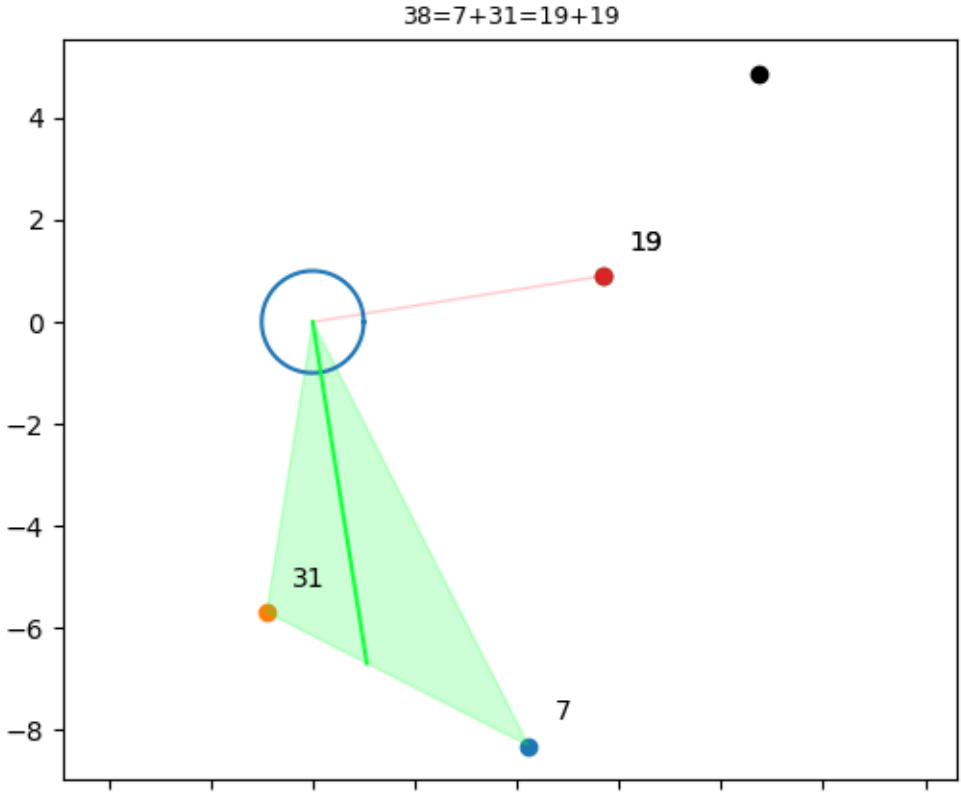

28=11+17
11
17

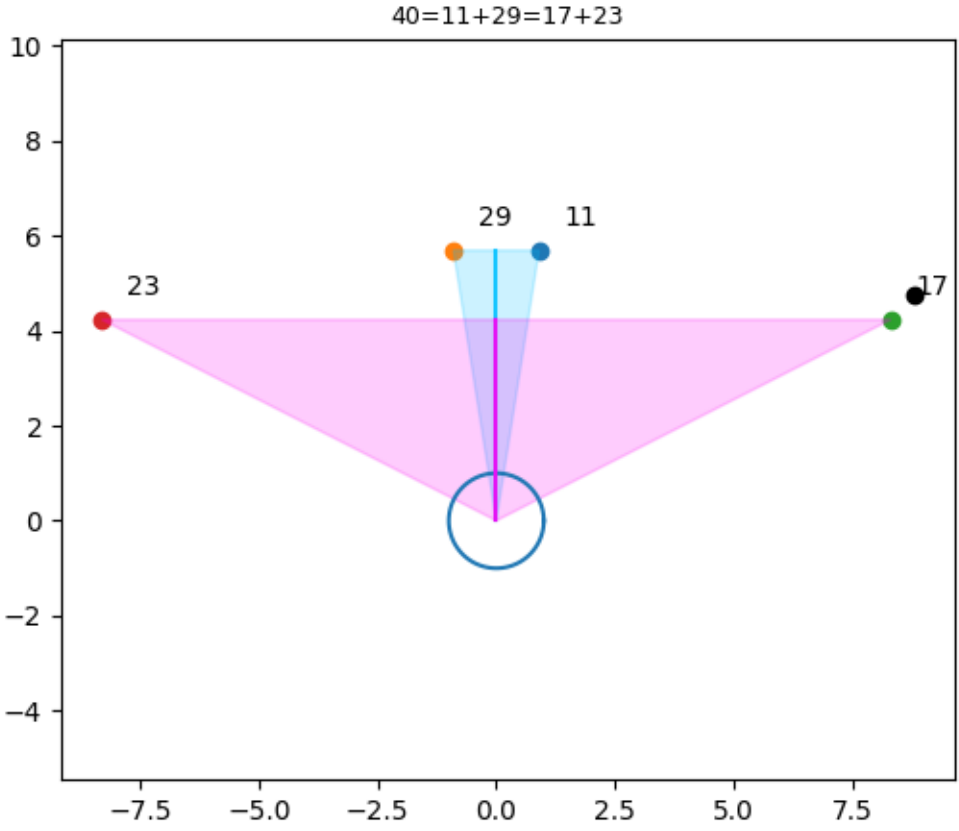

30=7+23=11+19=13+17
23
19
11
7
17
13
10.0
7.5
5.0
2.5
0.0
−2.5
−5.0
−7.5
−5
0
5
10
15

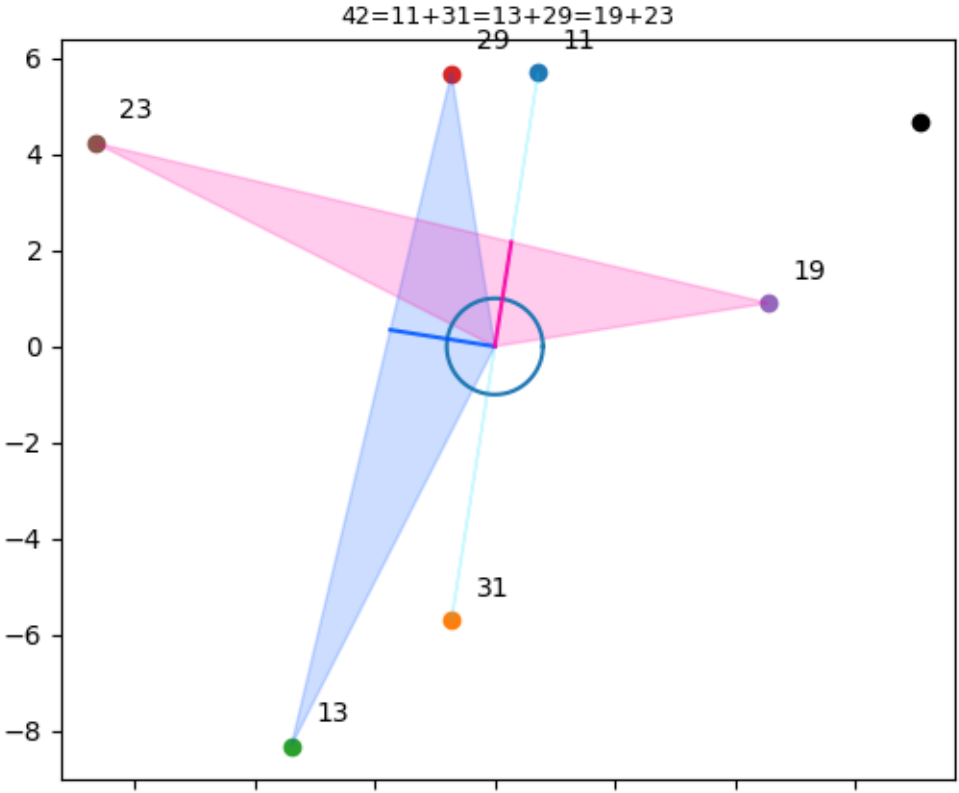

32=13+19
19
13
6
4
2
0
−2
−4
−6
−8
−4
−2
0
2
4
6
8
10
12

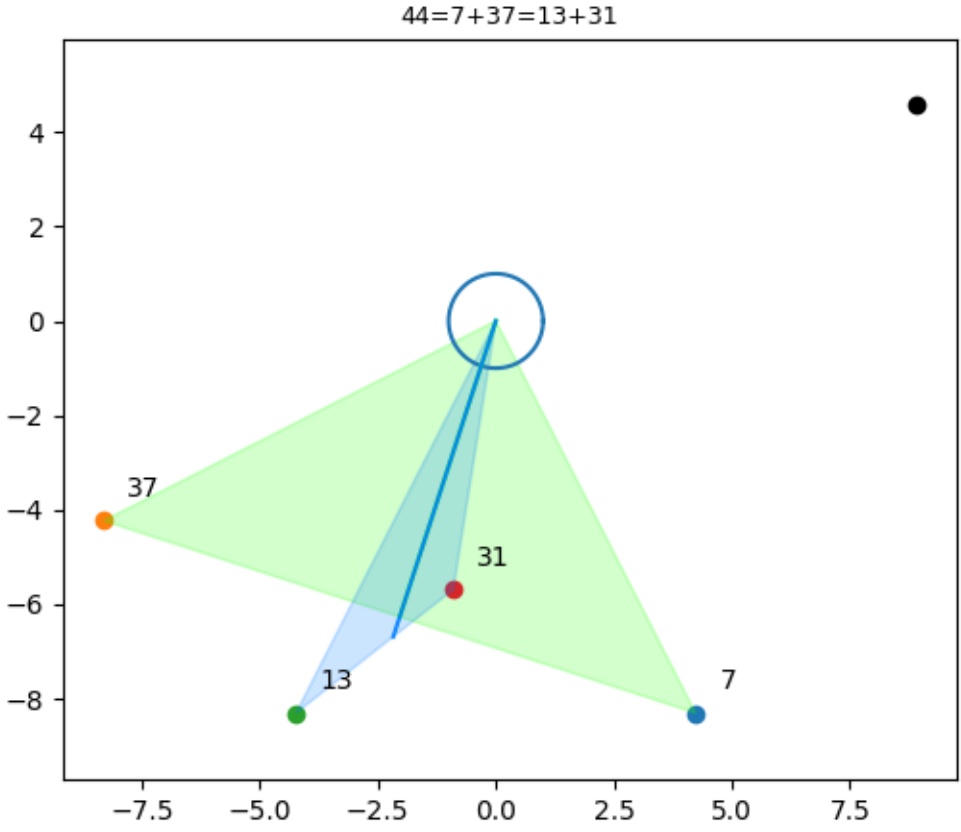

34=11+23=17+17
23
11
17
10
8
6
4
2
0
−2
−4
−5.0
−2.5
0.0
2.5
5.0
7.5
10.0
12.5

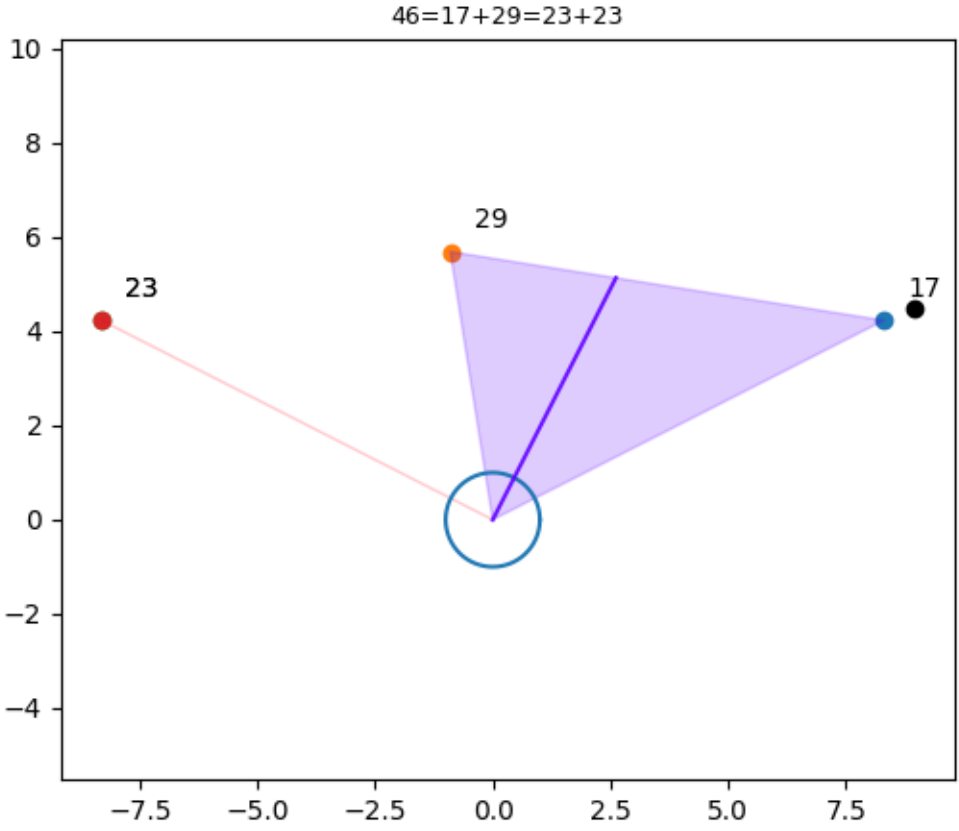

36=7+29=13+23=17+19
29
23
17
19
13
7
6
4
2
0
−2
−4
−6
−8
−7.5
−5.0
−2.5
0.0
2.5
5.0
7.5

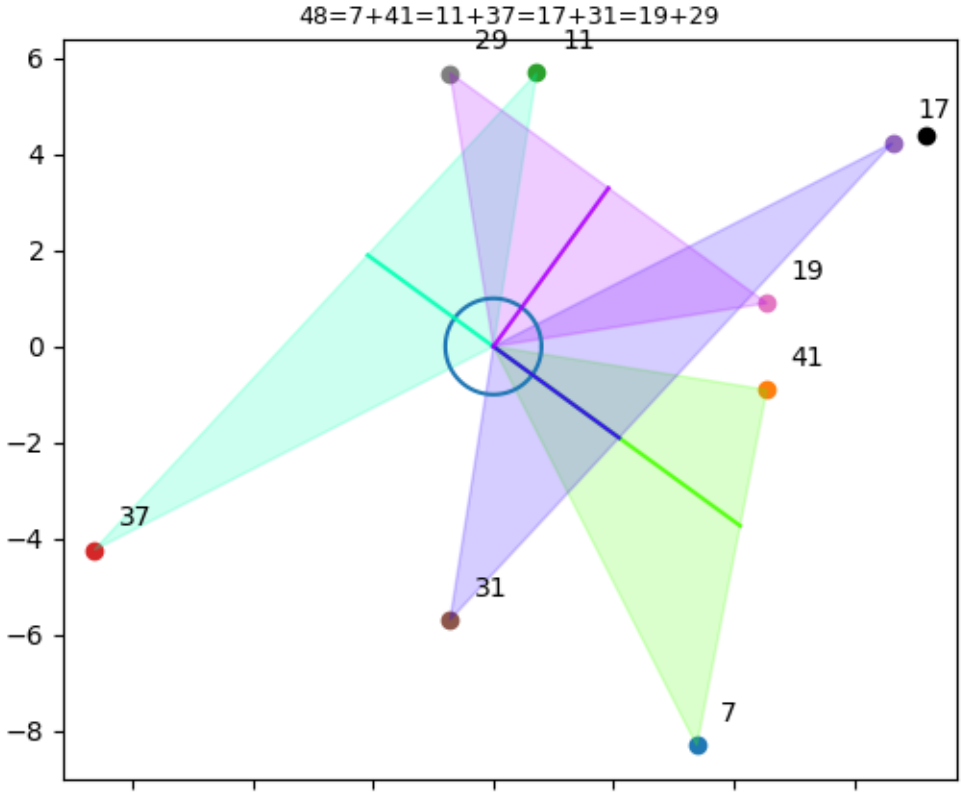

38=7+31=19+19
19
31
7
4
2
0
−2
−4
−6
−8
−4
−2
0
2
4
6
8
10
12

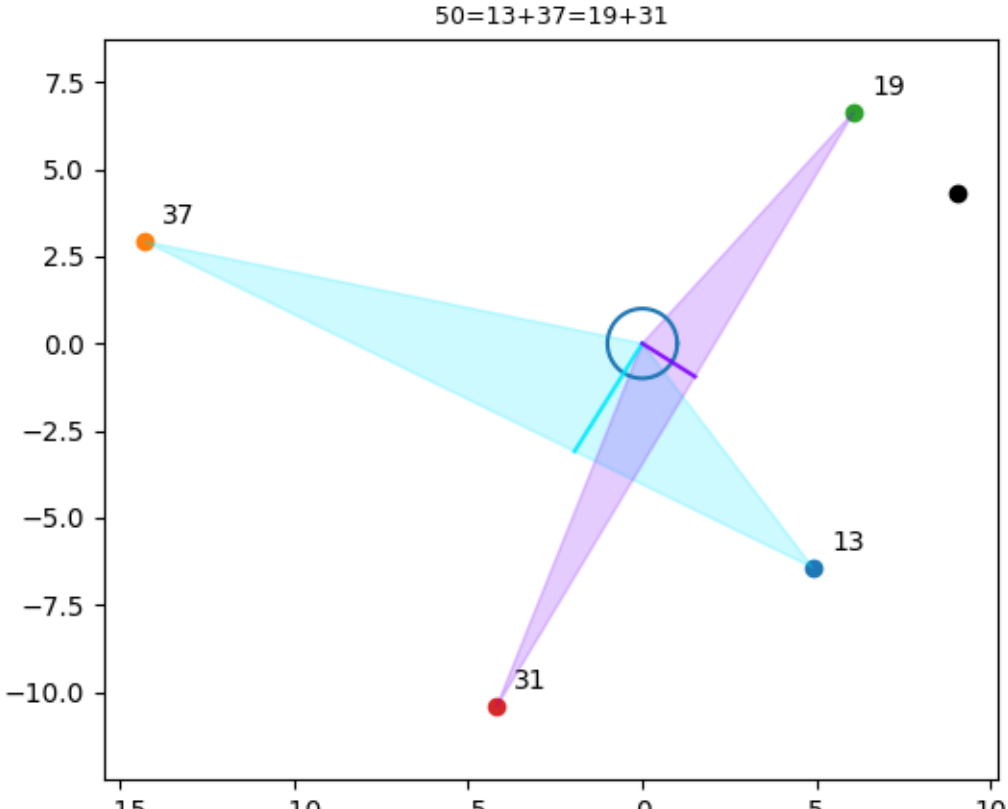

40=11+29=17+23
29
11
23
17
10
8
6
4
2
0
−2
−4
−7.5
−5.0
−2.5
0.0
2.5
5.0
7.5

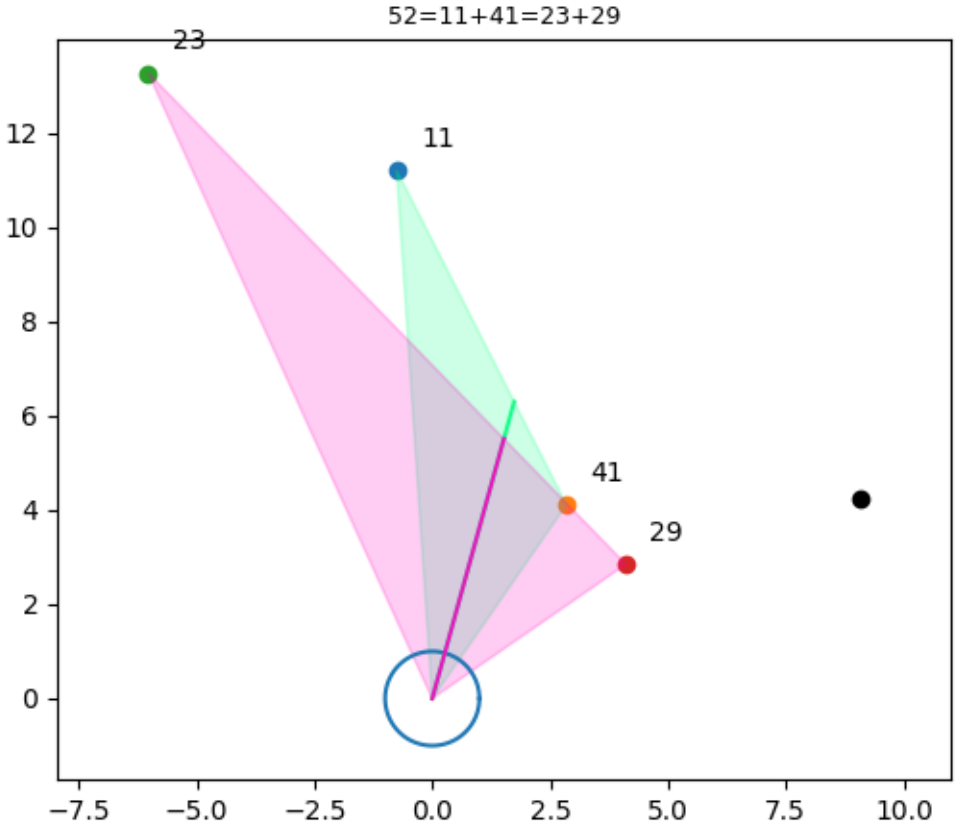

42=11+31=13+29=19+23
29
11
23
19
31
13
6
4
2
0
−2
−4
−6
−8
−7.5
−5.0
−2.5
0.0
2.5
5.0
7.5

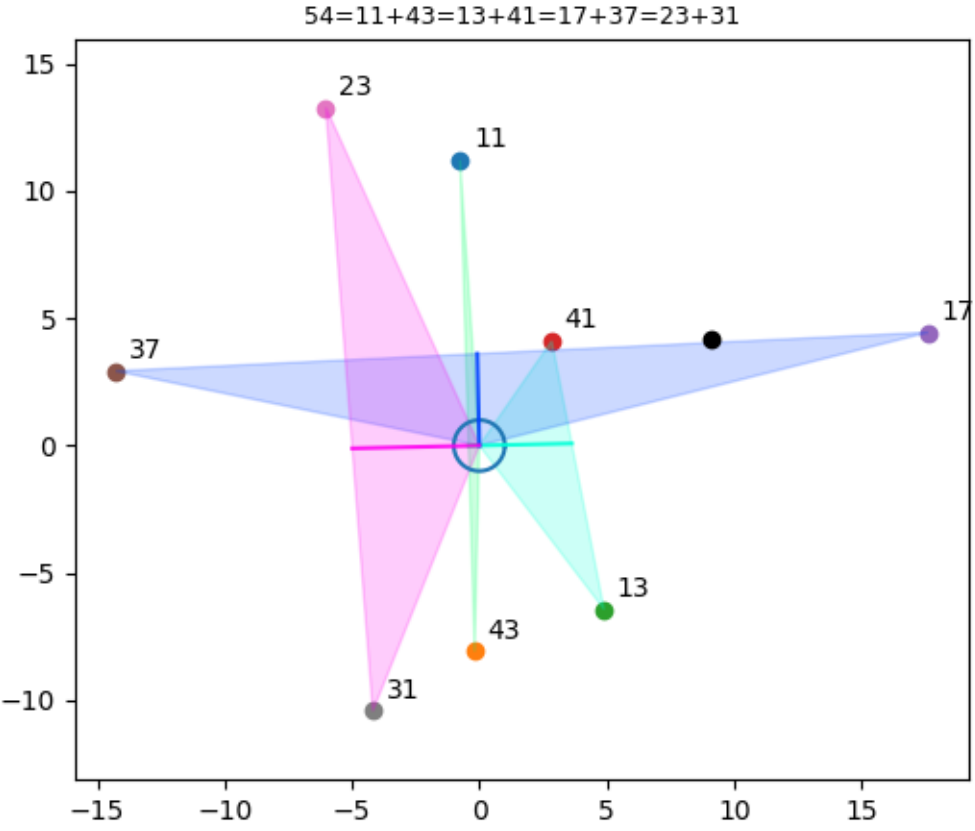

44=7+37=13+31
37
31
13
7
4
2
0
−2
−4
−6
−8
−7.5
−5.0
−2.5
0.0
2.5
5.0
7.5

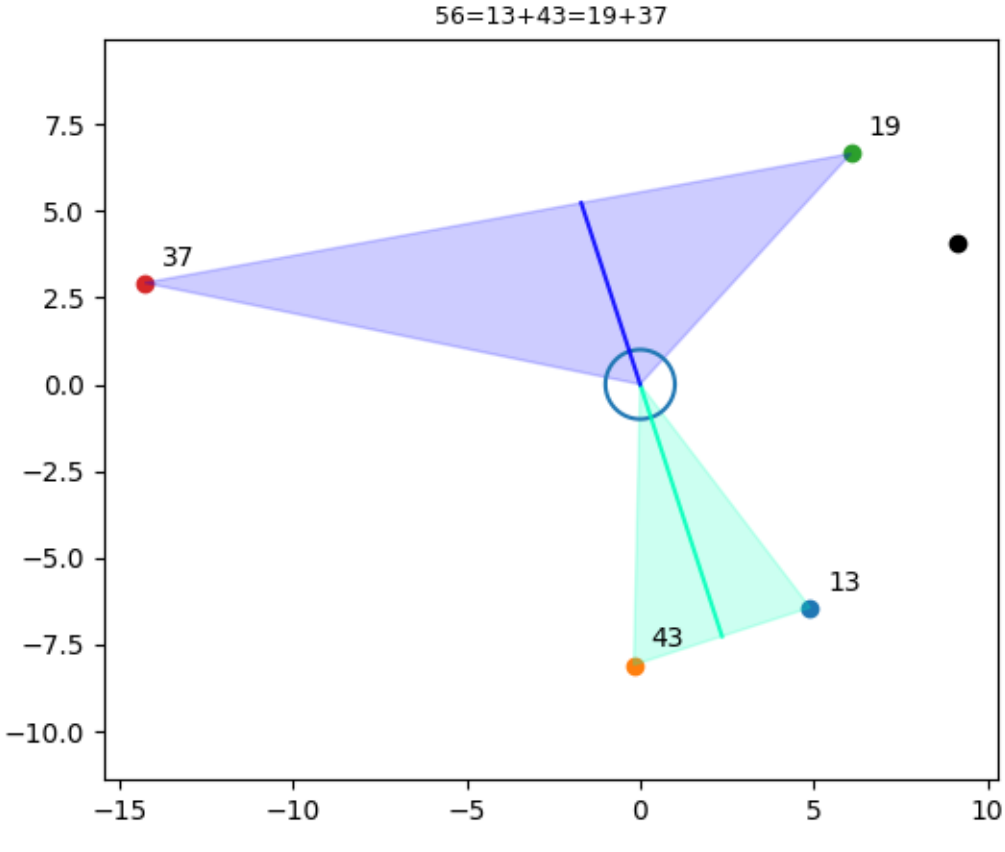

46=17+29=23+23
29
23
17
10
8
6
4
2
0
−2
−4
−7.5
−5.0
−2.5
0.0
2.5
5.0
7.5

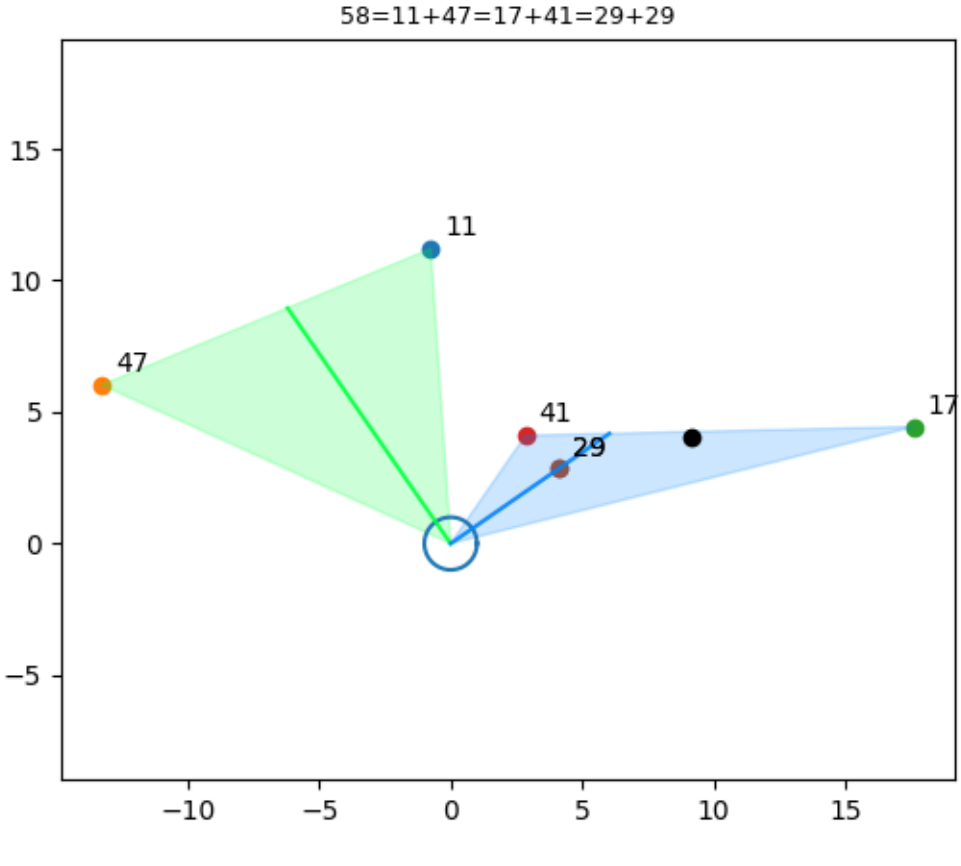

48=7+41=11+37=17+31=19+29
29
11
17
19
41
37
31
7
6
4
2
0
−2
−4
−6
−8
−7.5
−5.0
−2.5
0.0
2.5
5.0
7.5

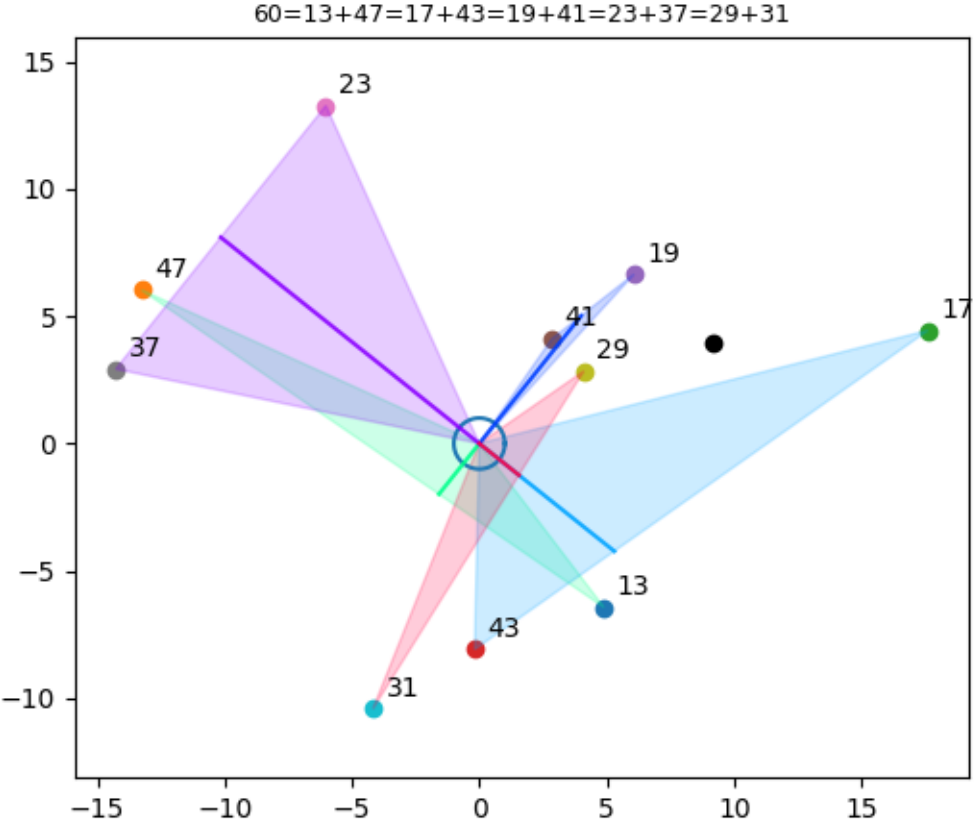

50=13+37=19+31
19
37
13
31
7.5
5.0
2.5
0.0
−2.5
−5.0
−7.5
−10.0
−15
−10
−5
0
5
10

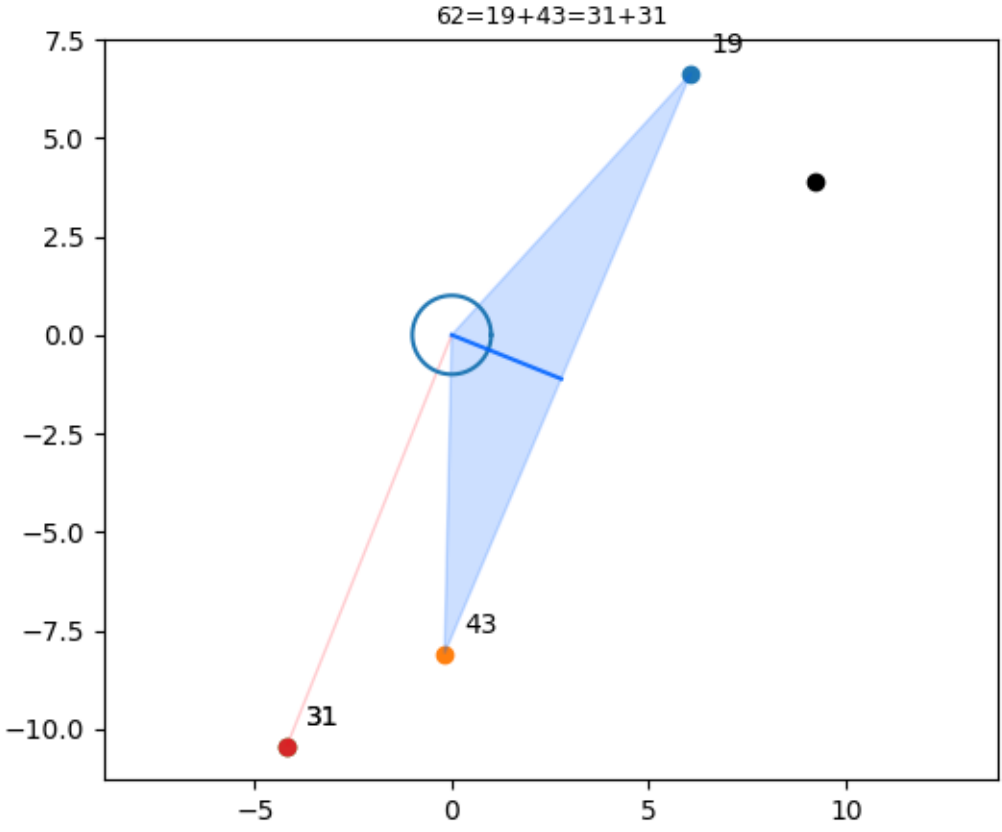

52=11+41=23+29
23
11
41
29
12
10
8
6
4
2
0
−7.5
−5.0
−2.5
0.0
2.5
5.0
7.5
10.0

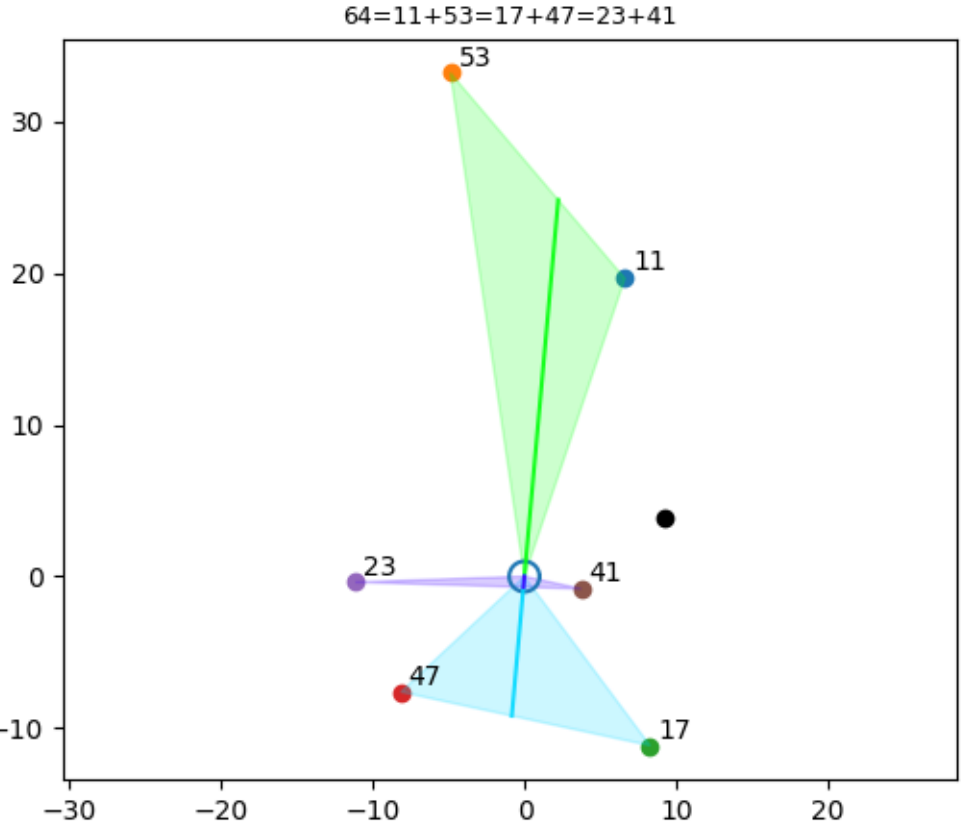

54=11+43=13+41=17+37=23+31
23
11
41
17
37
13
43
31
15
10
5
0
−5
−10
−15
−10
−5
0
5
10
15

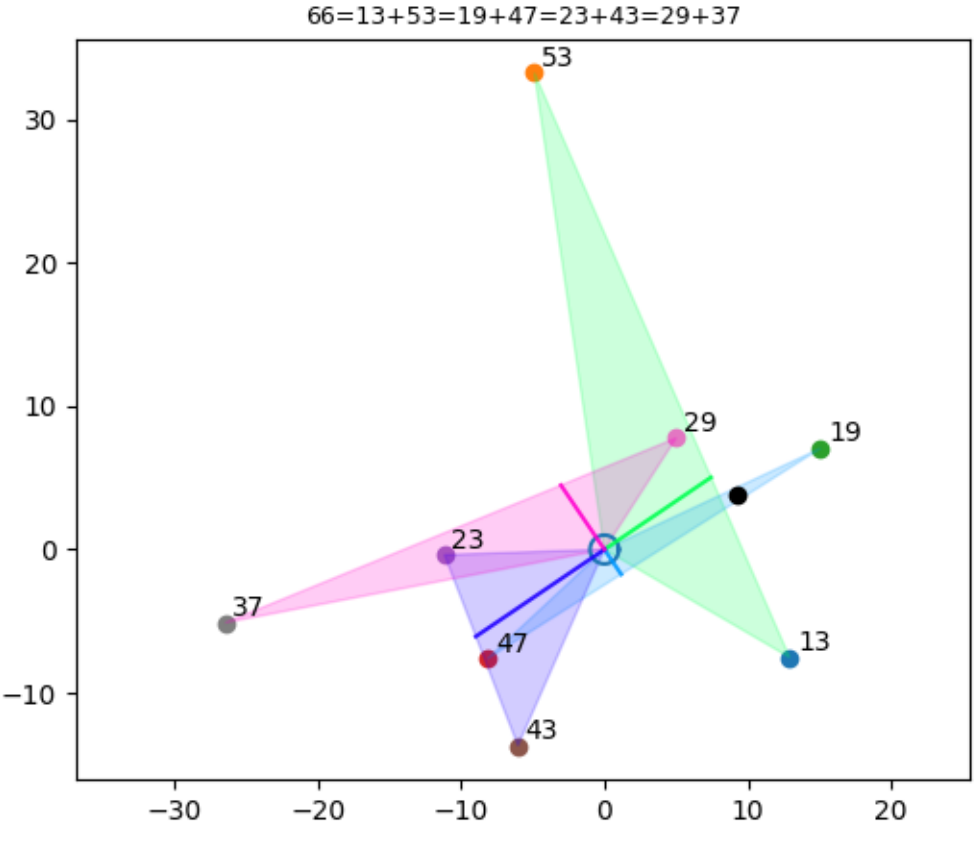

56=13+43=19+37
19
37
13
43
7.5
5.0
2.5
0.0
−2.5
−5.0
−7.5
−10.0
−15
−10
−5
0
5
10

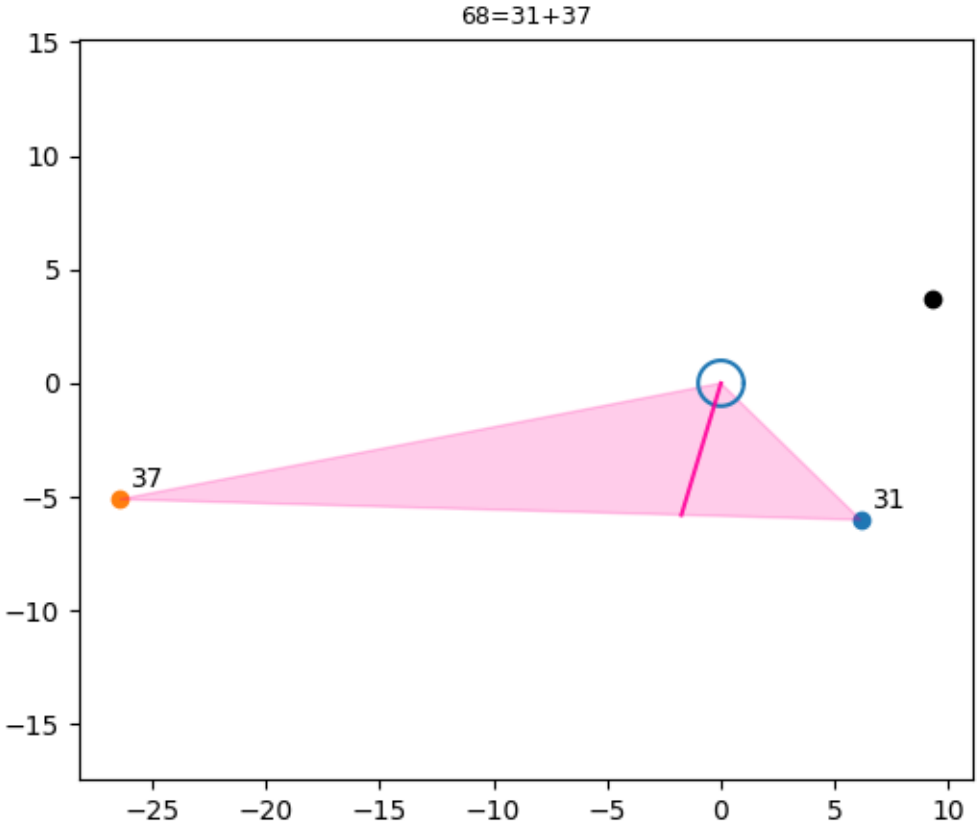

58=11+47=17+41=29+29
11
47
41
29
17
15
10
5
0
−5
−10
−5
0
5
10
15

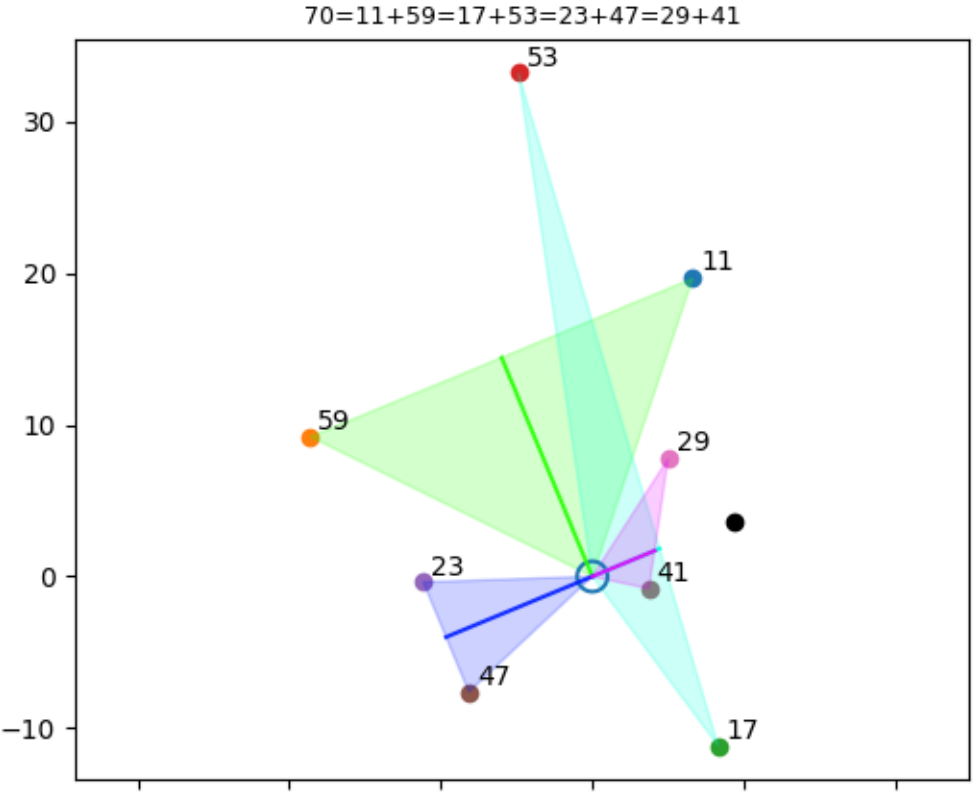

60=13+47=17+43=19+41=23+37=29+31
23
47
37
19
41
29
17
13
43
31
15
10
5
0
−5
−10
−15
−10
−5
0
5
10
15

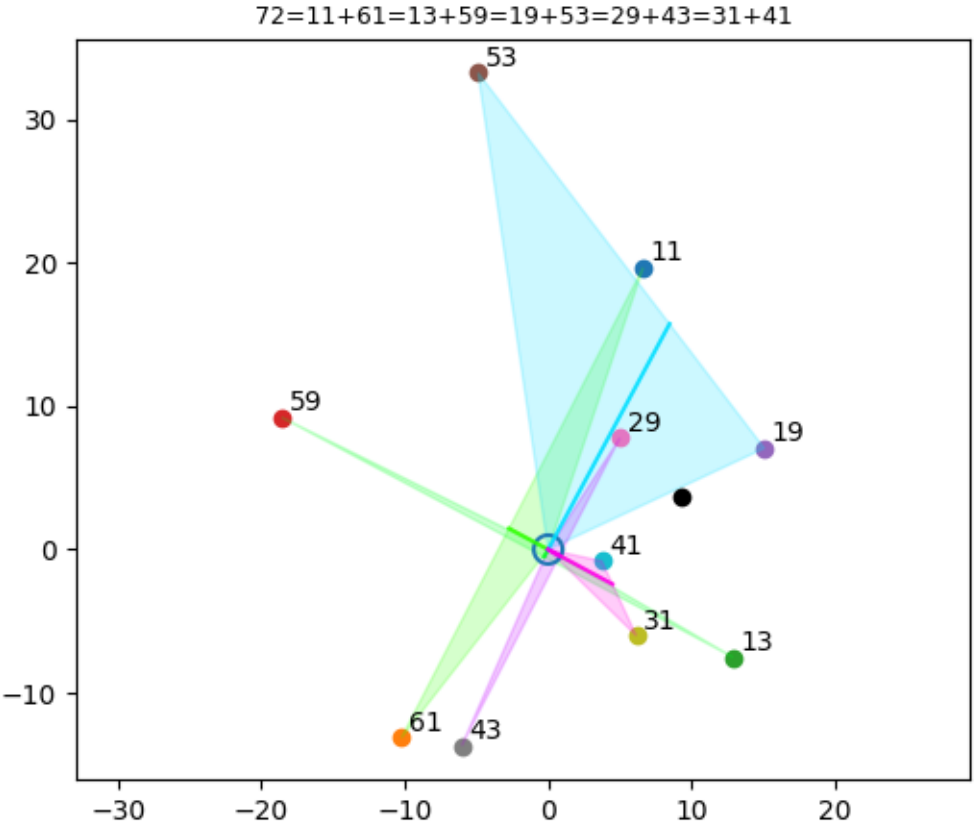

62=19+43=31+31
19
43
31
7.5
5.0
2.5
0.0
−2.5
−5.0
−7.5
−10.0
−5
0
5
10

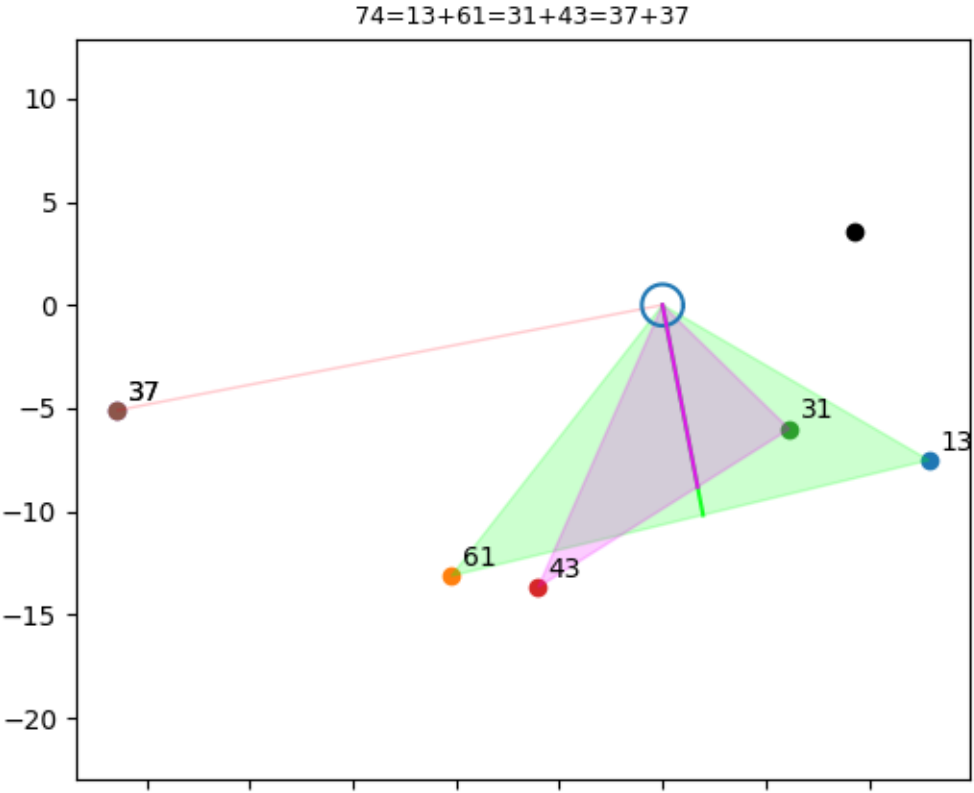

64=11+53=17+47=23+41
53
11
23
41
47
17
30
20
10
0
−10
−30
−20
−10
0
10
20

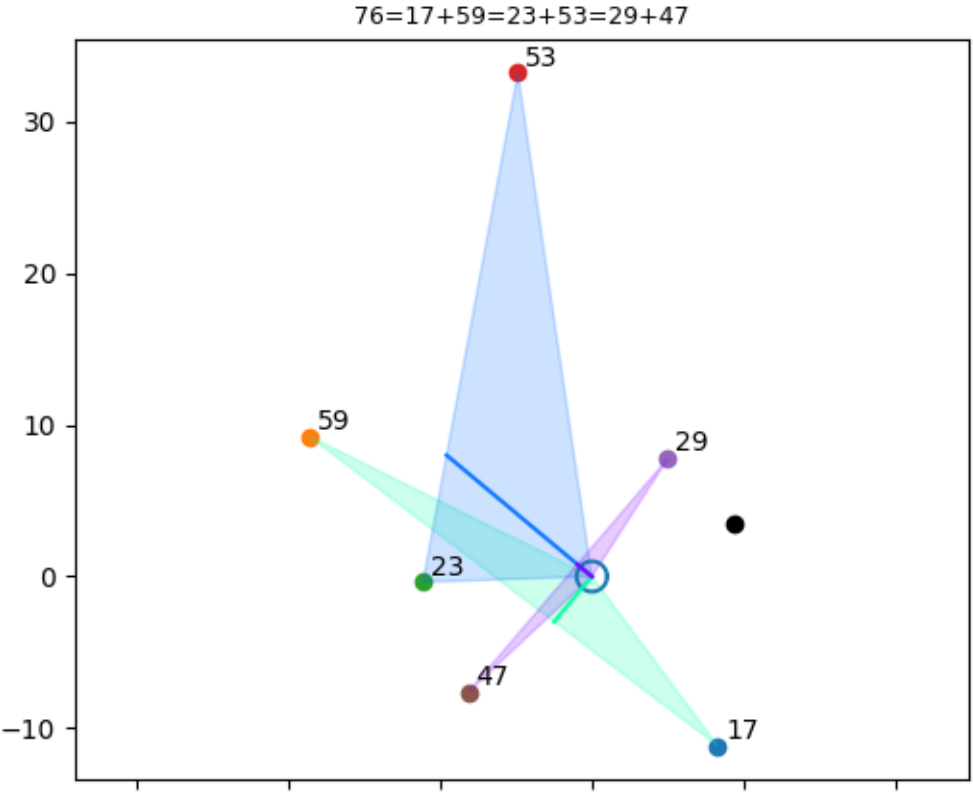

66=13+53=19+47=23+43=29+37
53
29
19
23
37
47
13
43
30
20
10
0
−10
−30
−20
−10
0
10
20

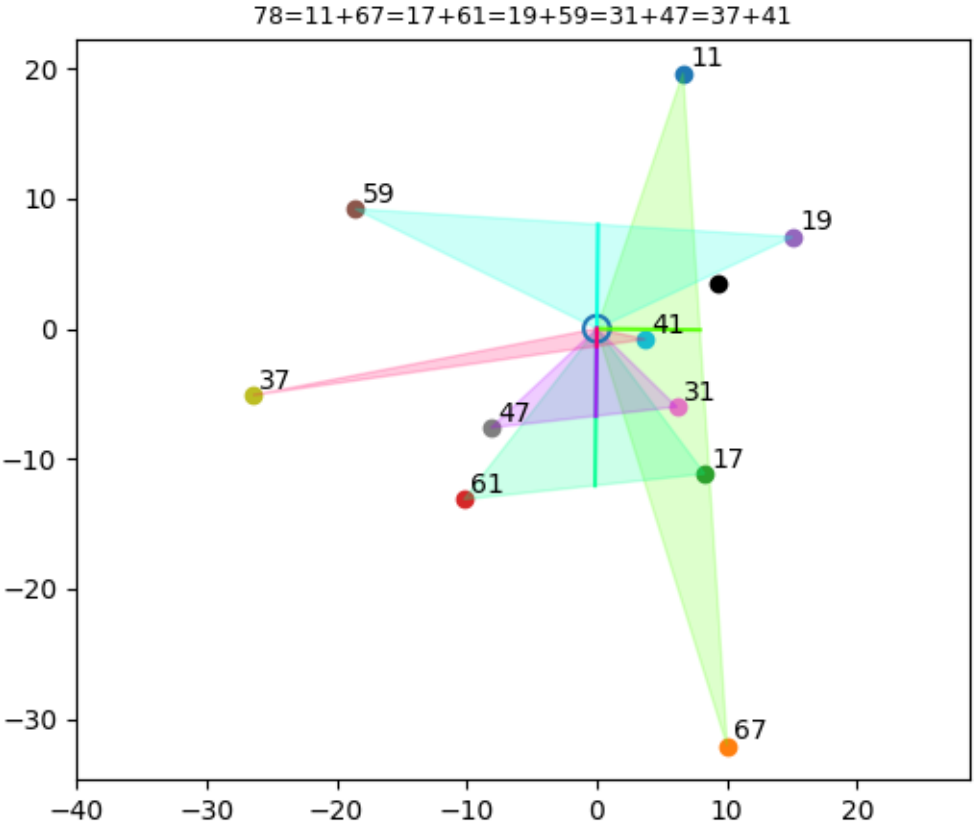

68=31+37
15
10
5
0
−5
−10
−15
−25
−20
−15
−10
−5
0
5
10
37
31

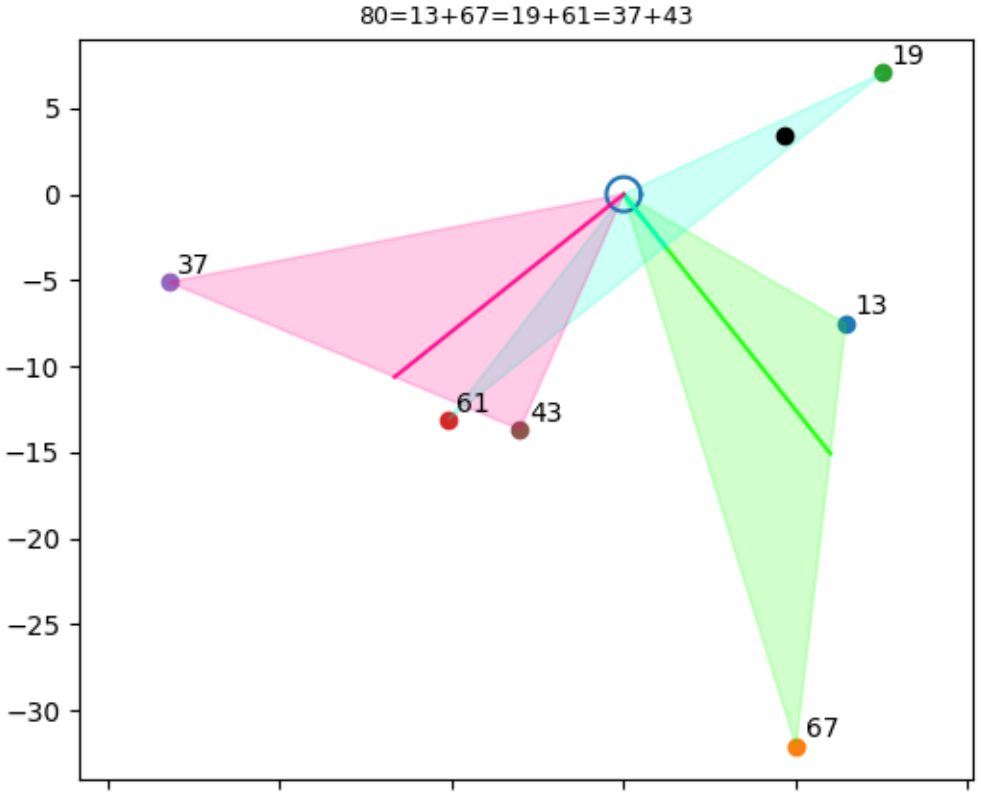

70=11+59=17+53=23+47=29+41
53
11
59
29
23
41
47
17
30
20
10
0
−10
−30
−20
−10
0
10
20

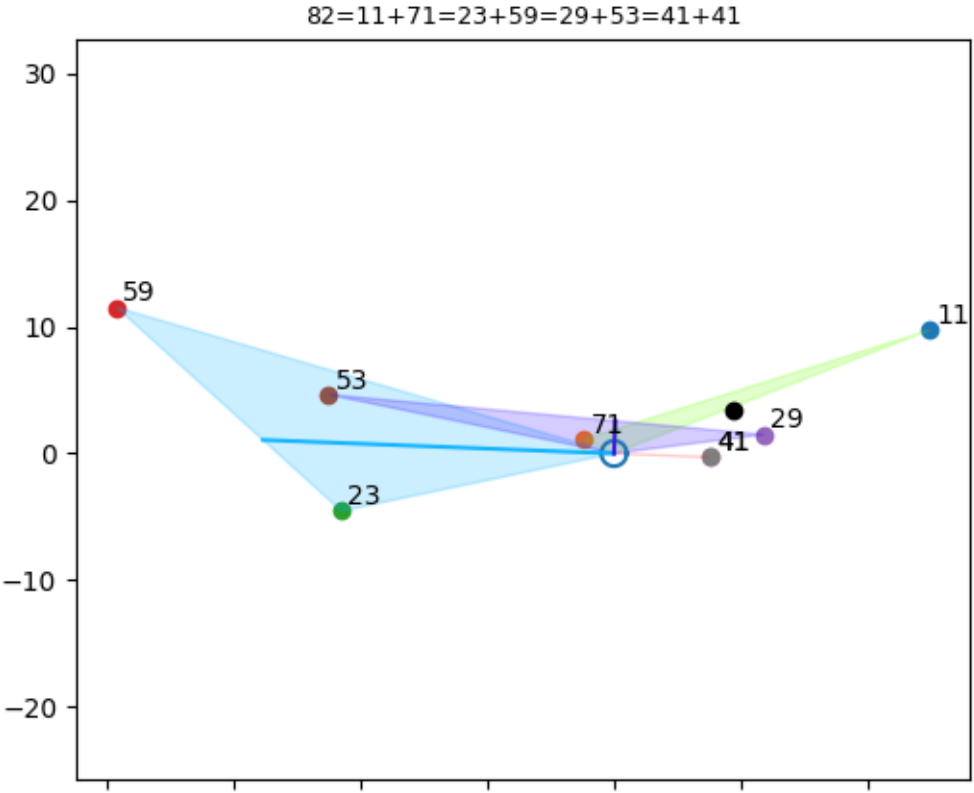

72=11+61=13+59=19+53=29+43=31+41
53
11
59
29
19
41
31
13
61
43
30
20
10
0
−10
−30
−20
−10
0
10
20

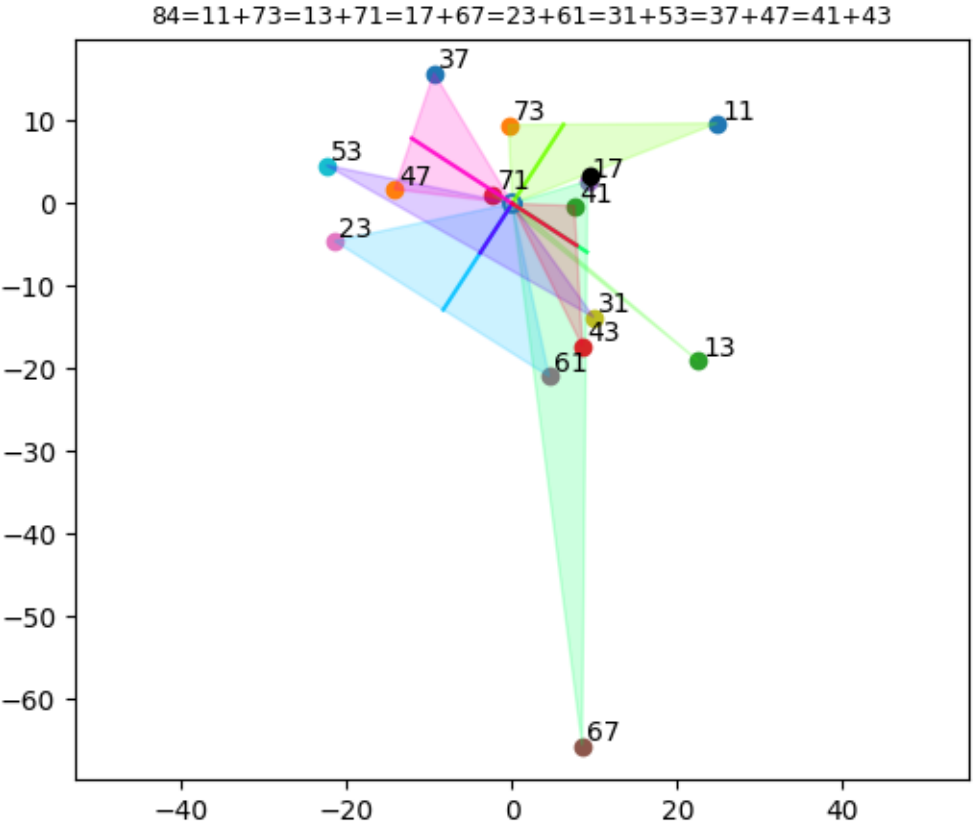

74=13+61=31+43=37+37
37
31
13
61
43
10
5
0
−5
−10
−15
−20
−25
−20
−15
−10
−5
0
5
10

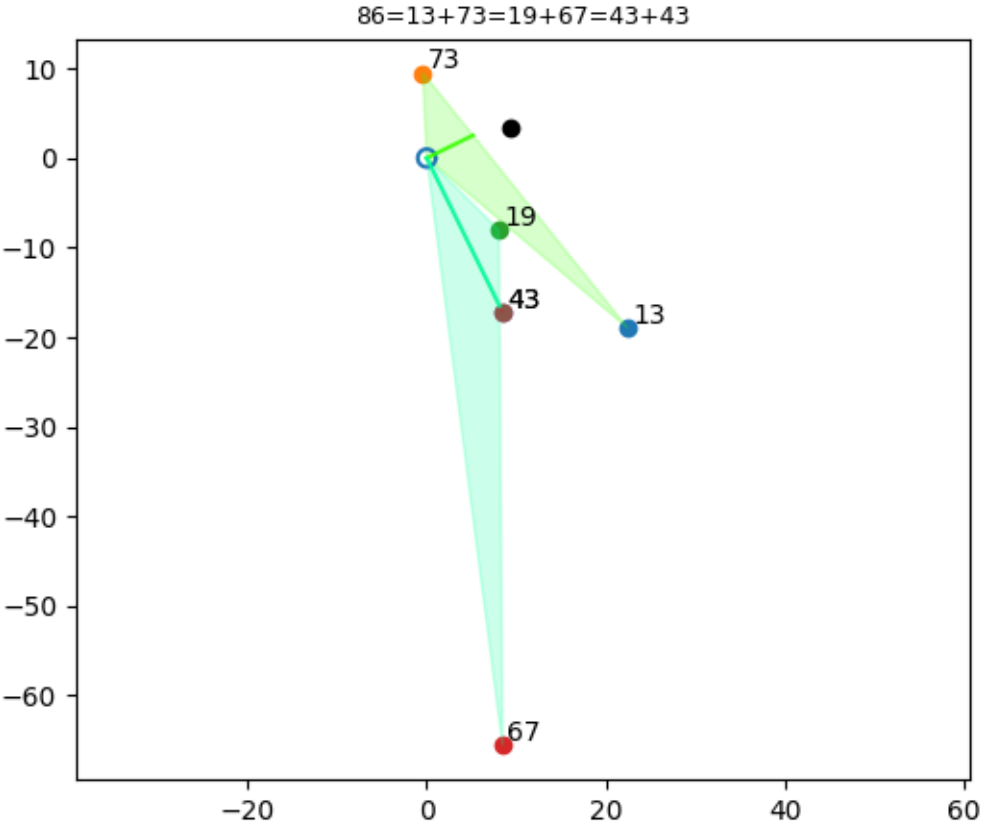

76=17+59=23+53=29+47
53
59
29
23
47
17
30
20
10
0
−10
−30
−20
−10
0
10
20

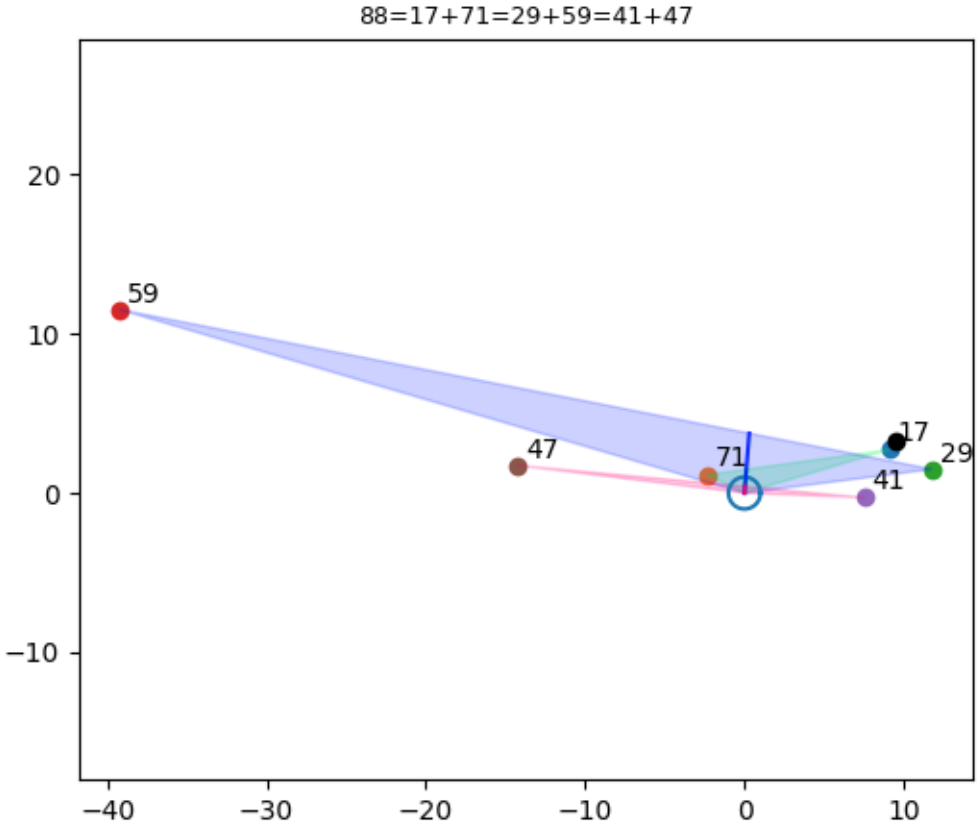

78=11+67=17+61=19+59=31+47=37+41
11
59
19
41
37
31
47
17
61
67
20
10
0
−10
−20
−30
−40
−30
−20
−10
0
10
20

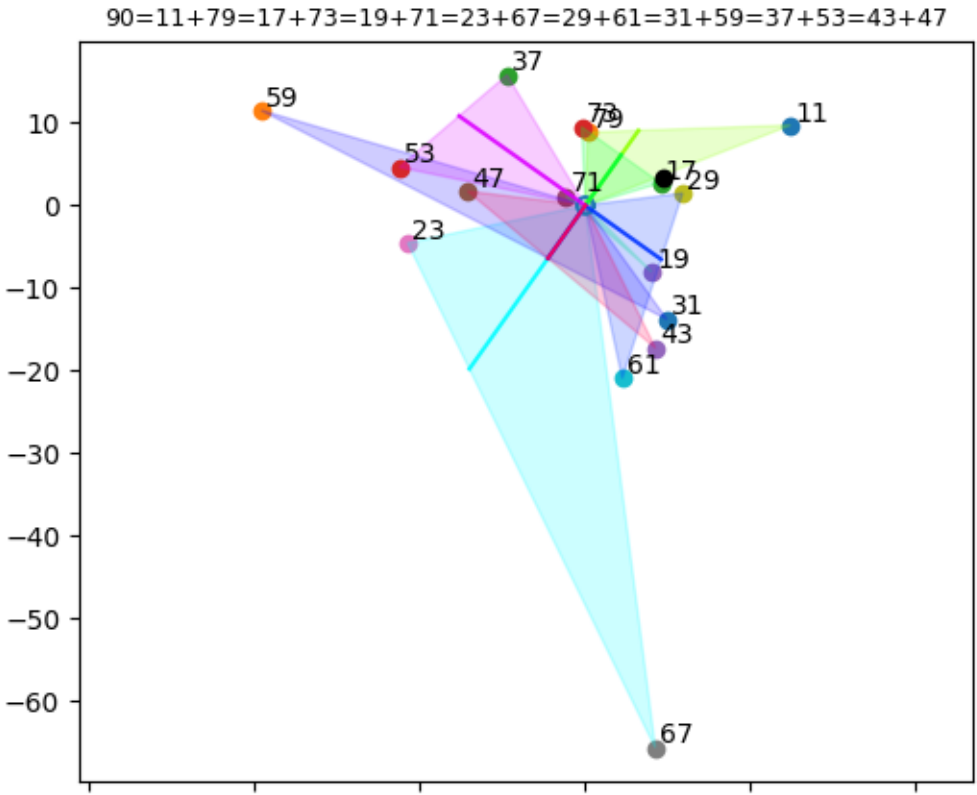

80=13+67=19+61=37+43
19
37
13
61
43
67
5
0
−5
−10
−15
−20
−25
−30
−30
−20
−10
0
10
20

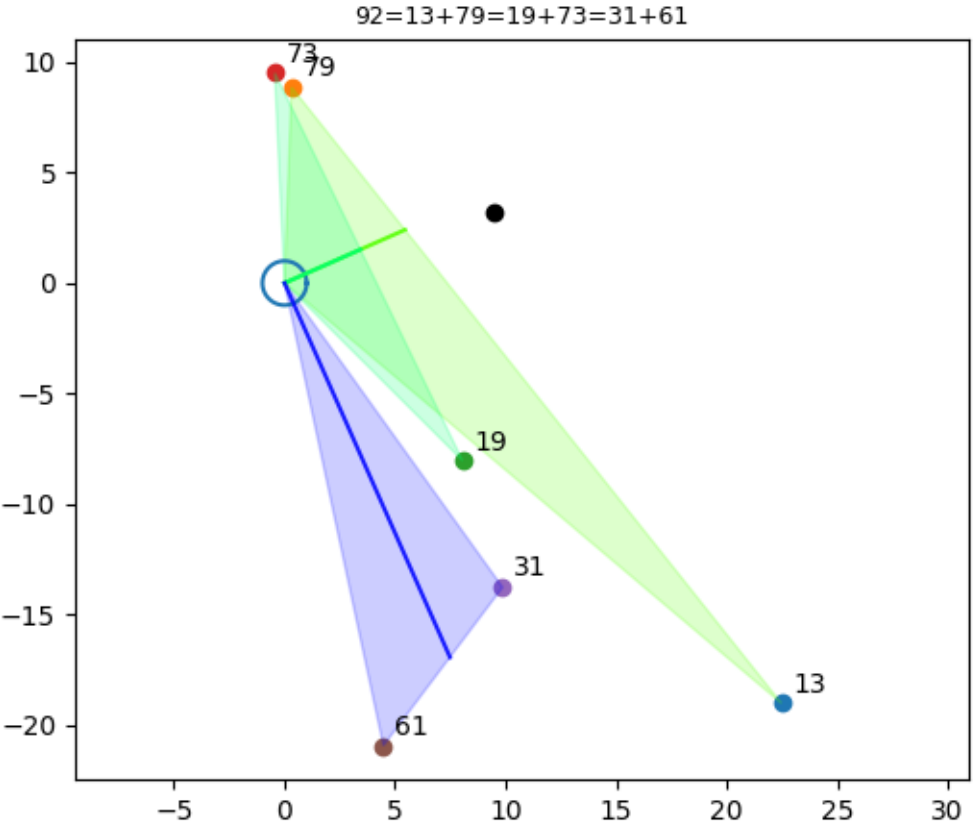

82=11+71=23+59=29+53=41+41
30
20
10
0
−10
−20
−40
−30
−20
−10
0
10
20
59
53
23
71
41
29
11

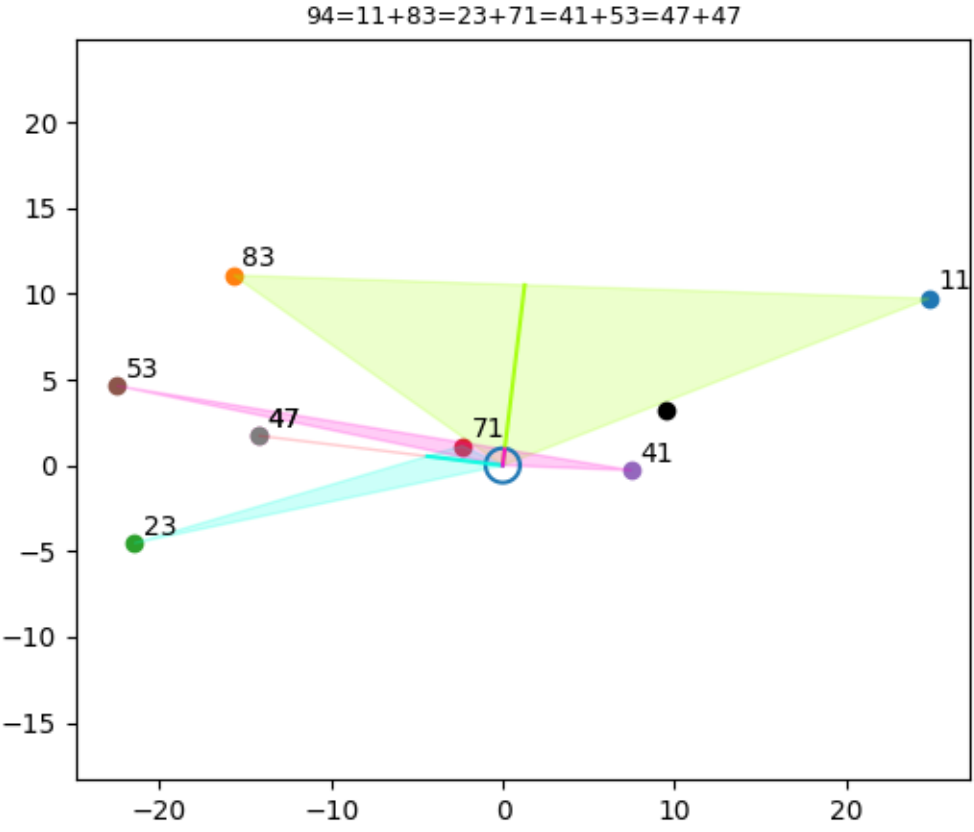

84=11+73=13+71=17+67=23+61=31+53=37+47=41+43
37
73
11
53
47
71
17
41
23
31
43
13
61
67
10
0
−10
−20
−30
−40
−50
−60
−40
−20
0
20
40

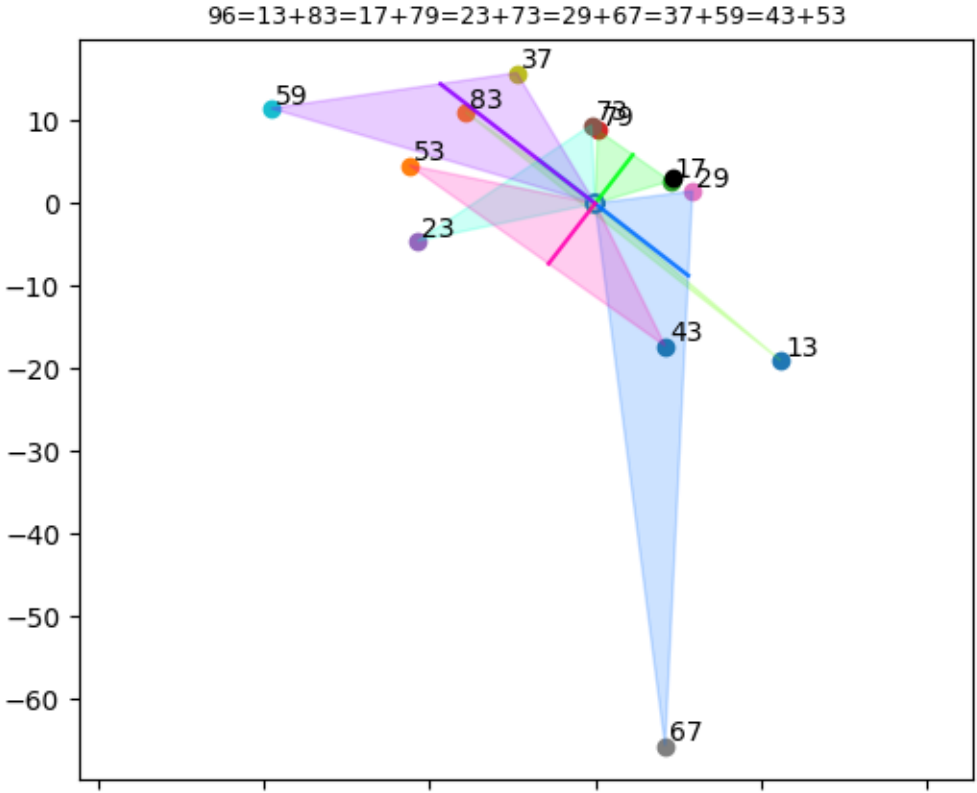

86=13+73=19+67=43+43
73
19
43
13
67
10
0
−10
−20
−30
−40
−50
−60
−20
0
20
40
60

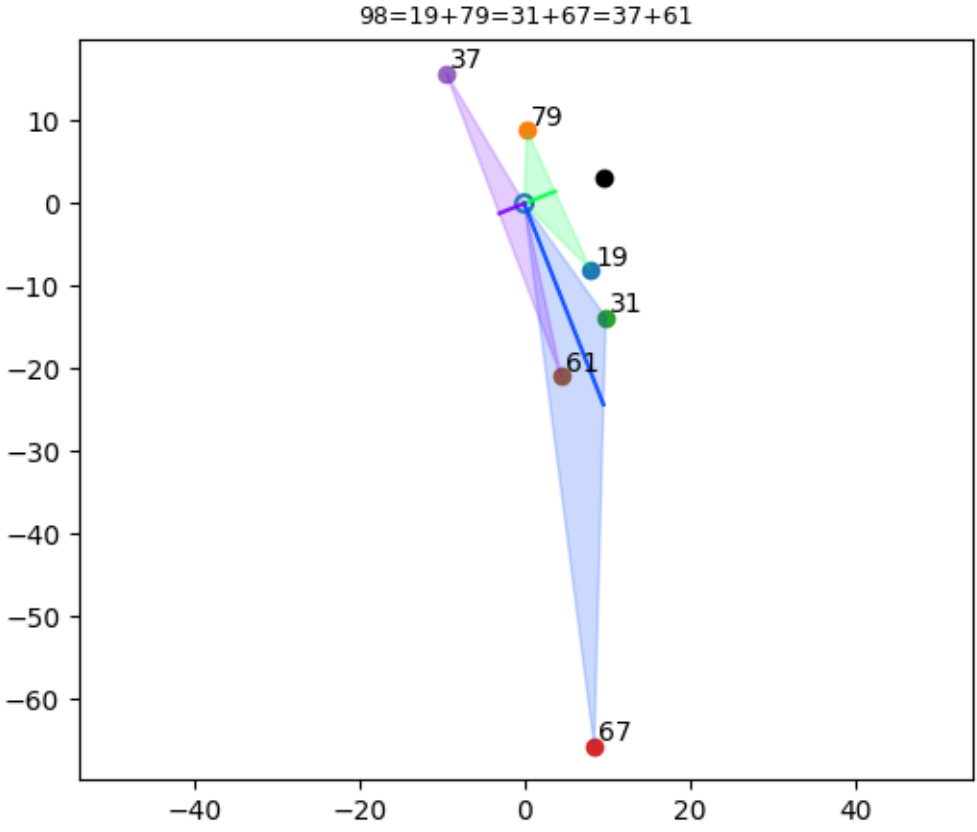

88=17+71=29+59=41+47
20
10
0
−10
−40
−30
−20
−10
0
10
59
47
71
17
29
41

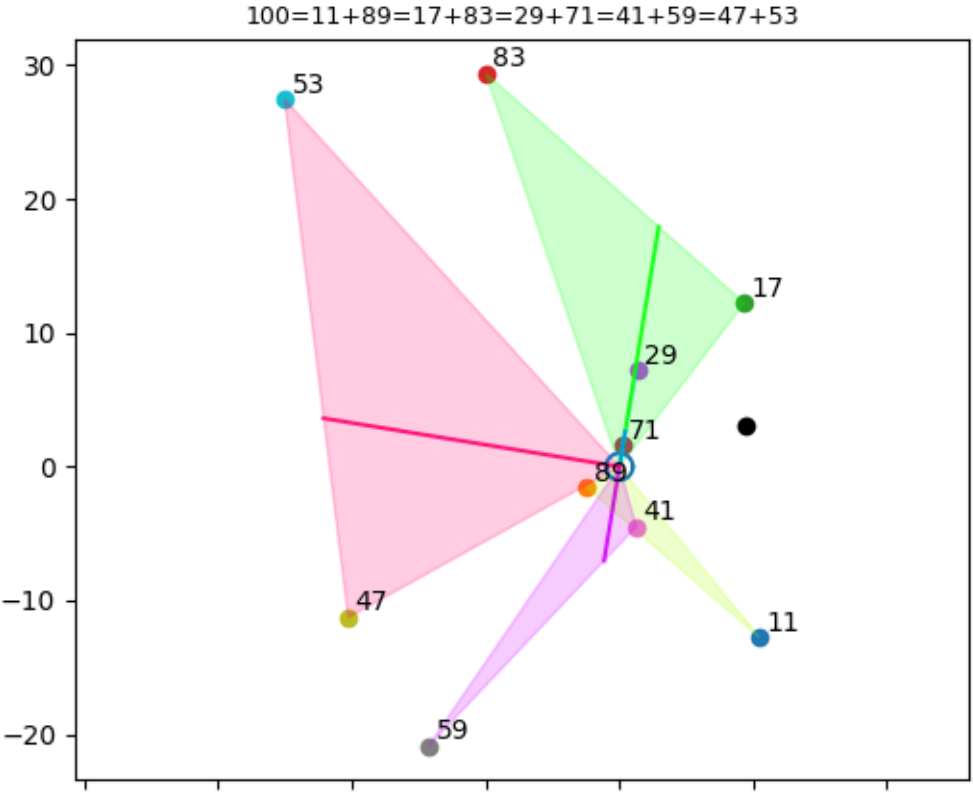

90=11+79=17+73=19+71=23+67=29+61=31+59=37+53=43+47
37
59
73
79
11
53
47
71
17
29
23
19
31
43
61
67
10
0
−10
−20
−30
−40
−50
−60
−60
−40
−20
0
20
40

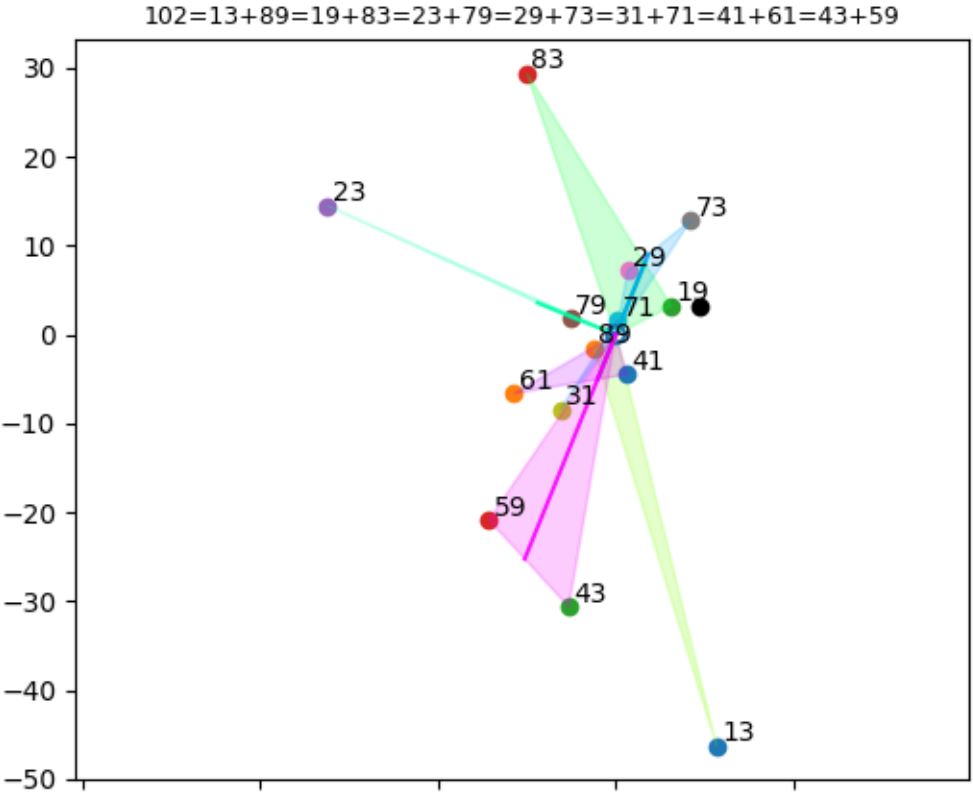

92=13+79=19+73=31+61
73
79
19
31
13
61
10
5
0
−5
−10
−15
−20
−5
0
5
10
15
20
25
30


94=11+83=23+71=41+53=47+47
83
11
53
47
71
41
23
20
15
10
5
0
−5
−10
−15
−20
−10
0
10
20


96=13+83=17+79=23+73=29+67=37+59=43+53
37
59
83
73
79
53
17
29
23
43
13
67
10
0
−10
−20
−30
−40
−50
−60
−60
−40
−20
0
20
40


98=19+79=31+67=37+61
37
79
19
31
61
67
10
0
−10
−20
−30
−40
−50
−60
−40
−20
0
20
40


100=11+89=17+83=29+71=41+59=47+53
83
53
17
29
71
89
41
47
11
59
30
20
10
0
−10
−20
−40
−30
−20
−10
0
10
20


102=13+89+19+83+23+79+29+73+31+71+41+61+43+59
83
23
73
29
19
79
71
89
41
61
31
59
43
13
30
20
10
0
−10
−20
−30
−40
−50
−60
−40
−20
0
20

Décomposants de Goldbach et fonctions paires (Denise Vella-Chemla, 10.7.2024)

On a étudié les graphiques obtenus par programme, qui montrent les parties réelle et imaginaire des produits :

$$A = \prod_{\substack{x\in\mathbb{N} \\ 0\leq x\leq n \\ 2\leq p\leq\lfloor\sqrt{n}\rfloor}} \left(1 - \exp\left(\frac{2i\pi x}{p}\right)\right)$$

et

$$A' = \prod_{\substack{x\in\mathbb{N} \\ 0\leq x\leq n \\ 2\leq p\leq\lfloor\sqrt{n}\rfloor}} \left(1 - \exp\left(\frac{2i\pi (n-x)}{p}\right)\right).$$

On cherche les points d'abscisse entière impaire qui rendent non nul à la fois A et A'. Si le produit AA' est non nul, alors A et A' doivent l'être.

On utilise l'égalité

(1) $$1 - \exp(i\theta) = -2\,i\,\sin(\theta/2)\exp(i\theta/2)$$

et on agrège systématiquement chaque sinus dans lequel intervient x avec le sinus "correspondant" dans lequel intervient $n-x$, ou bien chaque exponentielle dans laquelle intervient x avec l'exponentielle "correspondante" dans laquelle intervient $n-x$ de la façon suivante :

- pour les produits de sinus :

$$\sin\left(\frac{\pi\,x}{p}\right)\,\sin\left(\frac{\pi(n-x)}{p}\right) = -\frac{1}{2}\left(\cos\left(\frac{\pi\,n}{p}\right) - \cos\left(\frac{\pi(n-2x)}{p}\right)\right)$$

  $-\frac{1}{2}$ étant non nul, on peut l'oublier.

- pour les produits d'exponentielles :

$$\exp\left(\frac{i\pi\,x}{p}\right)\,\exp\left(\frac{i\pi(n-x)}{p}\right) = \exp\left(\frac{i\pi\,n}{p}\right)$$

  Le produit global courant pour toutes les valeurs de p comprises entre 2 et $\lfloor\sqrt{n}\rfloor$, il est finalement égal à [1] :

$$\exp\left(\frac{i\pi\,n}{2} + \frac{i\pi\,n}{3} + \frac{i\pi\,n}{4} + ...\right)$$

  Cette exponentielle étant non nulle, on peut l'oublier.

De même, on peut oublier l'élément $(-2i)^{\lfloor\sqrt{n}\rfloor-1}$, systématiquement non nul, qui apparaît par le produit des différents $-2i$ de l'équation (1).

[1] Puisque le produit de deux exponentielles est l'exponentielle de leur somme : $\exp(a)\exp(b) = \exp(a+b)$.

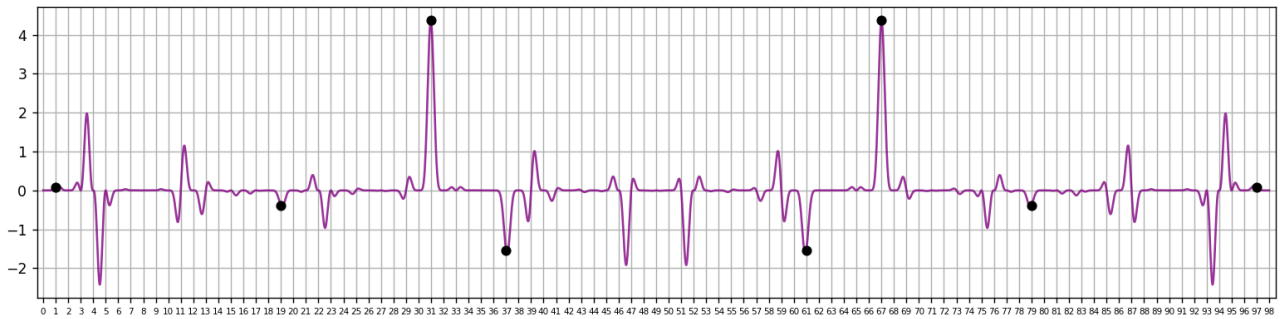
Reste que les décomposants de Goldbach de n (s'ils existent) sont les nombres entiers impairs qui n'annulent pas le produit suivant :

$$\prod_{\substack{3\leq x\leq n\\ p\in\mathbb{N}\\ 2\leq p\leq\lfloor\sqrt{n}\rfloor}}\left(\cos\left(\frac{\pi n}{p}\right)-\cos\left(\frac{\pi\times(n-2x)}{p}\right)\right)$$

Cette dernière fonction est une fonction paire. Voici le programme qui permet de la calculer :

```
import numpy as np
import matplotlib.pyplot as plt
import math
from math import floor, sqrt, sin, cos

i, exp = 1j, np.exp
epsilon = 1e-6
for n in range(98, 100, 2):
      a, b = 0, n
      d = 2
      x = np.linspace(a, b, num=(b - a)*10**d + 1, endpoint=True)
      xl, xr = a - 0.5, b + 0.5
      www = []
      for k in range(len(x)):
            produit = 1
            for p in range(2, int(floor(sqrt(n))) + 1):
                  produit = produit*(cos(np.pi*n/p)-cos(np.pi*(n-2*x[k])/p))
            www += [produit]
      plt.figure(figsize=(20, 8))
      plt.subplot(211)
      plt.plot(x, www, alpha=0.8, color='purple')
      for k in range(len(x)):
            if (abs(x[k]%2 - 1) < epsilon) and (abs(www[k]) > epsilon):
                  plt.plot(x[k], www[k].real, color='black', marker='o')
                  print(x[k],' ', www[k].real)
      plt.xlim(xl, xr)
      plt.xticks(range(a, b + 1), fontsize=6)
      plt.grid(True)
plt.show()
```

Et voici le résultat de son exécution pour $n = 98$.



```
C:\Users\Denise_Vella\Desktop\discret-continu>python3 reecritreprise.py
1.0    0.08131702910576541
19.0    -0.39395726076523135
31.0    4.372594315315881
37.0    -1.5389072110071624
61.0    -1.5389072110071624
67.0    4.372594315315881
79.0    -0.39395726076523135
97.0    0.08131702910576541
```

L'ensemble des résultats pour les nombres compris entre 6 et 102 est à consulter ici :

https://denisevellachemla.eu/dessins-fcts-paires.pdf.

Valeurs contraintes (Denise Vella-Chemla, 12.7.2024)

On cherche à démontrer que tout nombre pair n supérieur à 4 admet un décomposant de Goldbach, i.e. un nombre premier x dont le complémentaire à n, $n-x$, est premier également.

On rappelle qu'un nombre inférieur à n et supérieur à $\sqrt{n}$ est un nombre premier s'il n'est divisible par aucun des nombres entiers compris entre 2 et $\sqrt{n}$.

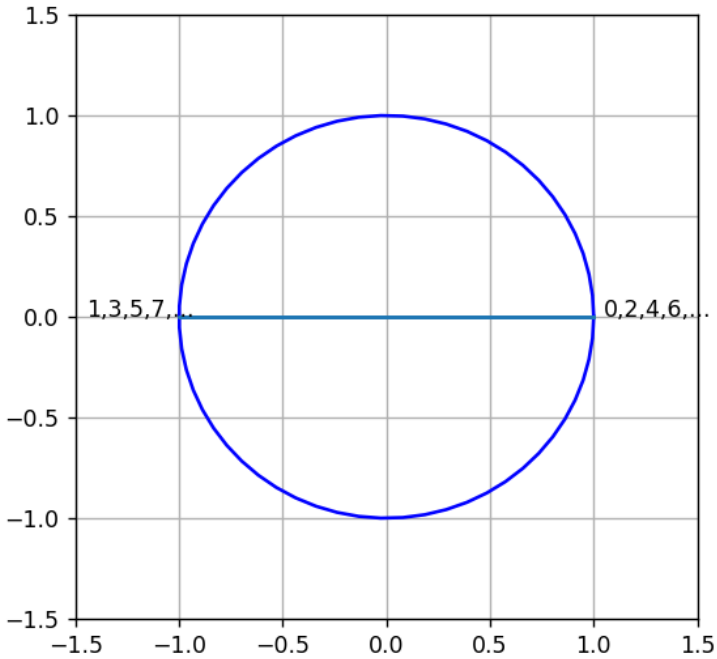
Pour représenter la divisibilité, on utilise les racines de l'unité dans le plan complexe.

Par exemple, pour représenter la divisibilité par 2, on utilise la fonction définie de $\mathbb{R}$ dans $\mathbb{C}$:

$$f_2 \ : \ x \mapsto 1 - \exp\left(\frac{2\pi i x}{2}\right)$$

qui envoie les nombres pairs sur 0 et les nombres impairs sur un autre nombre que 0.

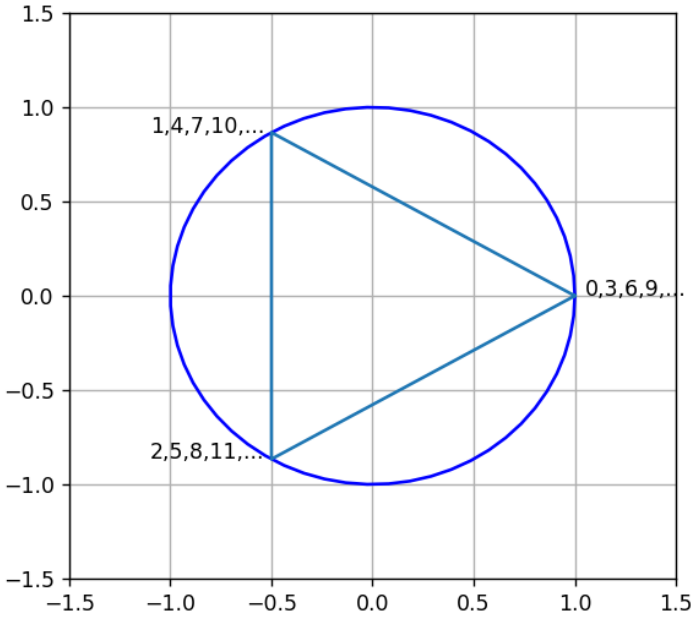
Ci-dessous, une image mentale de la fonction $\exp\left(\frac{2\pi i x}{2}\right)$; les nombres pairs ont pour image 1 et les nombres impairs ont pour image -1 :



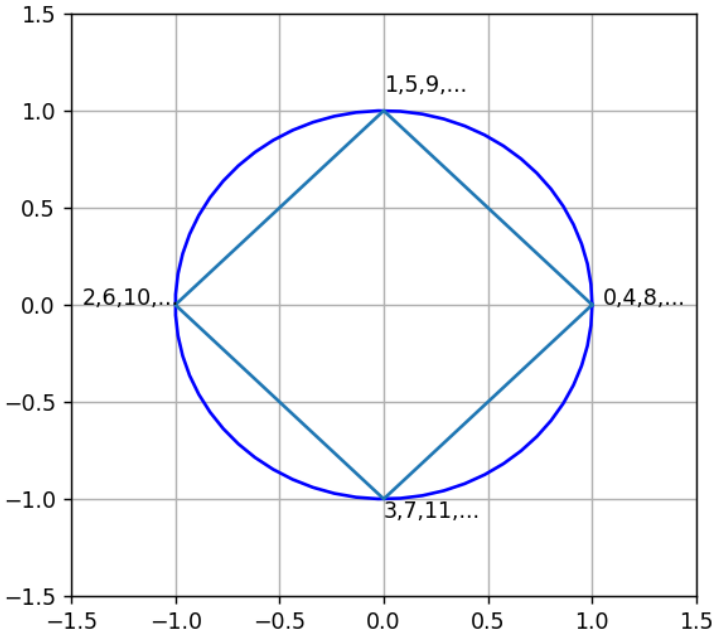
Les nombres pairs auront ainsi pour image par f_2 (qui vaut 1 moins l'exponentielle) 0 tandis que les nombres réels autres que les nombres entiers pairs auront par f_2 une image non nulle.

On gère de façon similaire la divisibilité par 3, 4, 5, etc, i.e. par tout nombre entier.

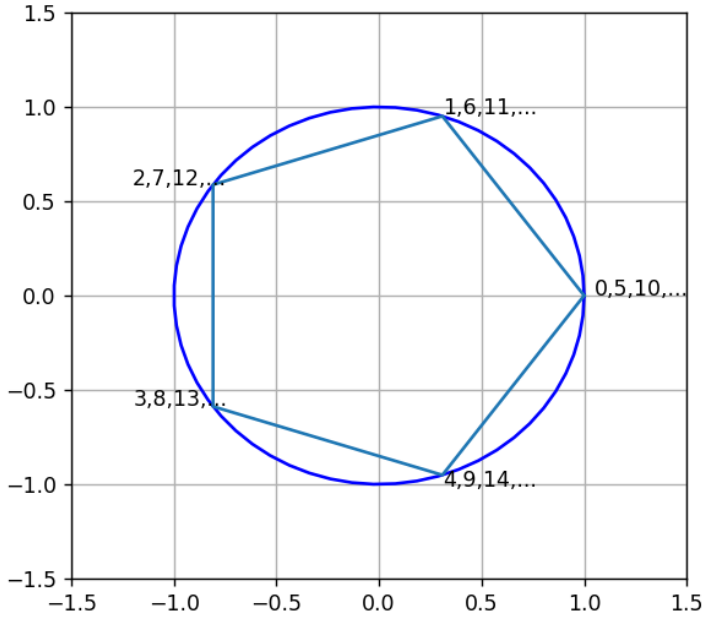
Par exemple, l'image mentale associée à la fonction $f_3 \ : \ x \mapsto 1 - \exp\left(\frac{2\pi i x}{3}\right)$ d'analyse de la divisibilité par 3 sera



L'image associée à la divisibilité par 4 :



Et enfin, l'image associée à la divisibilité par 5 :



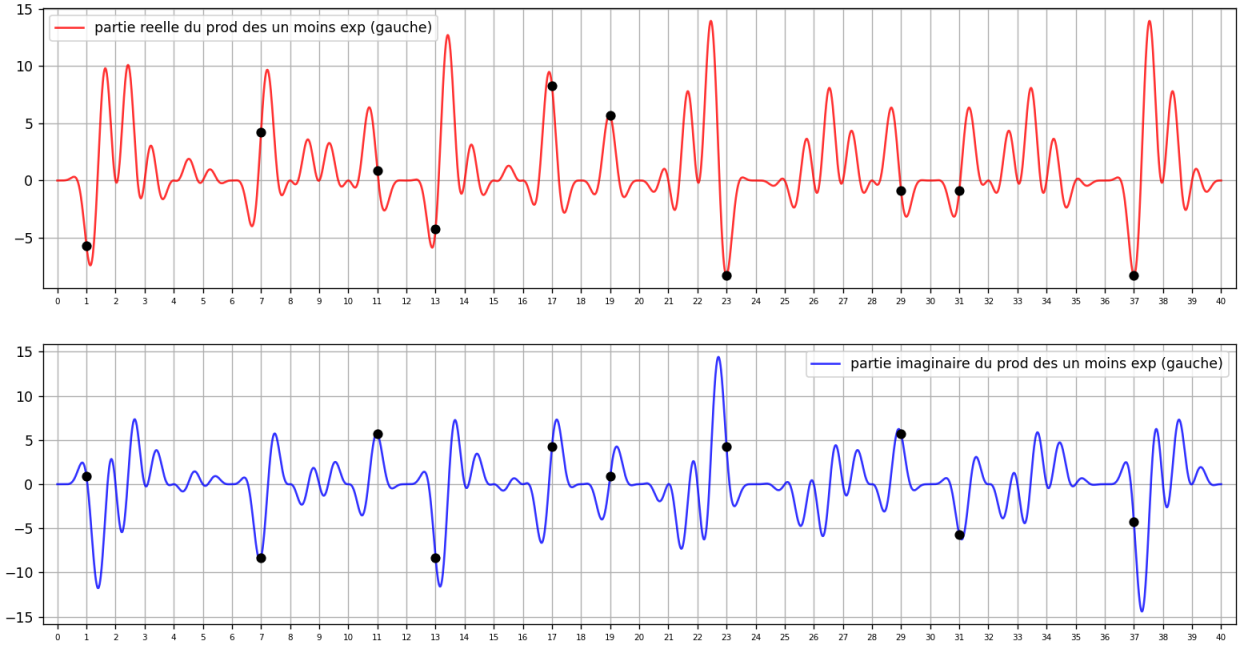
L'intérêt des différentes fonctions f_k est qu'elles traitent d'une manière homogène les différents critères de divisibilité : les nombres divisibles par k s'envoient tous sur 0 et les nombres non divisibles par k s'envoient sur un autre complexe que 0. On doit souligner que toutes les fonctions (toutes les figures) présentent une symétrie horizontale ; seules les figures correspondant à une divisibilité par un nombre pair présentent également une symétrie verticale.

Un nombre premier compris entre $\sqrt{n}$ et n étant non divisible par tous les nombres entiers appartenant à l'intervalle $I = [2, ..., \lfloor\sqrt{n}\rfloor]$, il doit avoir une image non nulle par chacune des fonctions f_k de la forme vue ci-dessus, pour tout $k \in I$.

Voyons un exemple : sur le graphique ci-dessous est représentée la fonction f de $\mathbb{R}\times\mathbb{R}$ dans $\mathbb{C}$ qu'il est pertinent d'étudier à la recherche des décomposants de Goldbach du nombre $n = 40$.

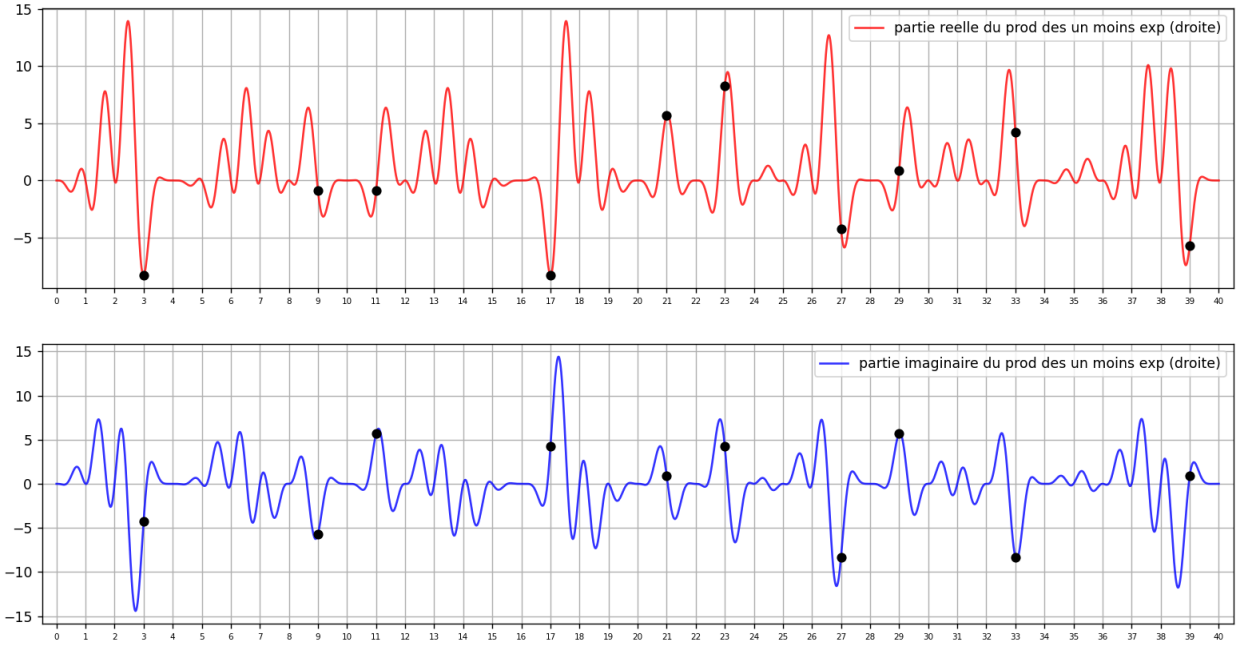
$$f \ : \ (n,x) \mapsto \prod_{\substack{x\in\mathbb{R}\\ 0\leq x\leq n\\ k\in\mathbb{N}\\ 2\leq k\leq\lfloor\sqrt{n}\rfloor}} \left(1-\exp\left(\frac{2\pi i x}{k}\right)\right)$$

Les parties réelle et imaginaire des affixes images par la fonction f qui sont non nulles pour des x entiers impairs (voir leurs valeurs en annexe 1) sont présentées sur deux courbes différentes et sont notées en noir.



En effectuant le changement de variable $x \mapsto n - x$, on a la fonction g symétrique de f par rapport au point central du graphique (ici, $n/2 = 20$), définie également de $\mathbb{R} \times \mathbb{R}$ dans $\mathbb{C}$, et qui permet d'étudier le caractère de primalité du nombre $n - x$ pour $n = 40$. Les parties réelle et imaginaire des affixes images sont présentées séparément et celles qui sont non nulles sont à nouveau notées en noir.

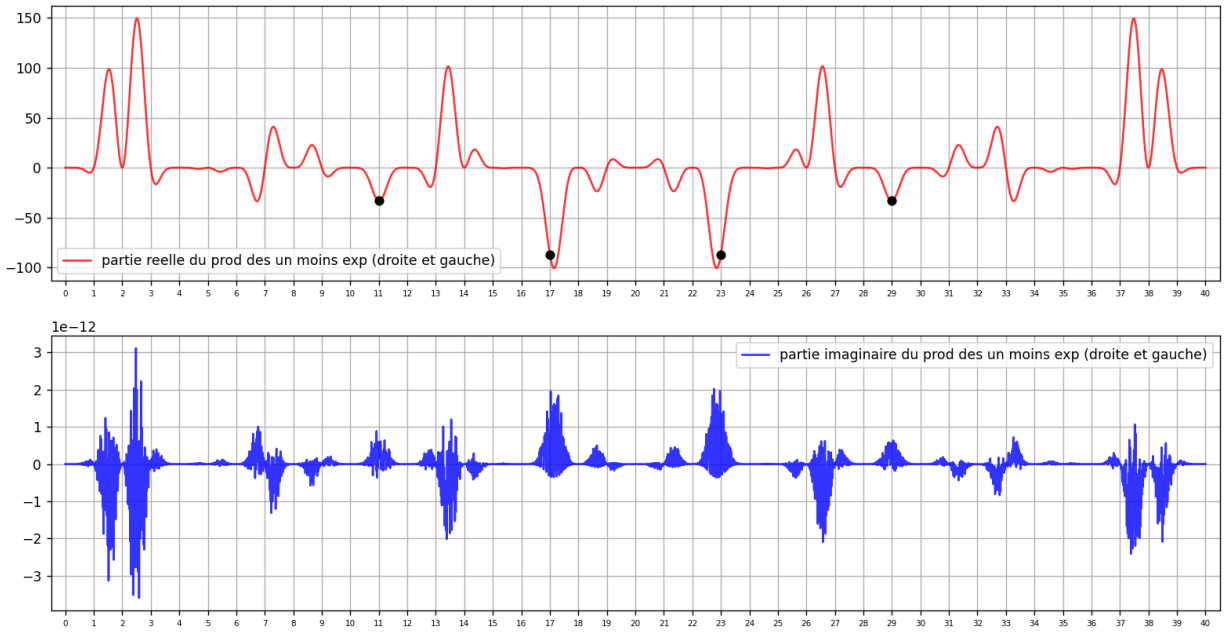
$$g \ : \ (n, x) \mapsto \prod_{\substack{x \in \mathbb{R} \\ 0 \leq x \leq n \\ k \in \mathbb{N} \\ 2 \leq k \leq \lfloor \sqrt{n} \rfloor}} \left(1 - \exp\left(\frac{2\pi i (n-x)}{k}\right)\right).$$



Un produit étant non nul si ses deux facteurs sont non nuls, étudions maintenant la fonction h telle que $h(n,x) = f(n,x) \times g(n,x)$ définie de $\mathbb{R} \times \mathbb{R}$ dans $\mathbb{C}$.

$$h \ : \ (n,x) \mapsto \prod_{\substack{x \in \mathbb{R} \\ 0 \leq x \leq n \\ k \in \mathbb{N} \\ 2 \leq k \leq \lfloor \sqrt{n} \rfloor}} \left(1 - \exp\left(\frac{2\pi i x}{k}\right)\right)\left(1 - \exp\left(\frac{2\pi i (n-x)}{k}\right)\right).$$

Les courbes représentant les parties réelle et imaginaire de la fonction h sont sur le graphique ci-dessous :



Le “mélange” des caractères de divisibilité entraîne un comportement erratique de la partie imaginaire, qui correspond au fait que les figures de divisibilité par des nombres entiers impairs, vues plus haut indépendamment les unes des autres, n’étaient pas symétriques verticalement. Les valeurs des parties réelles des images par la fonction h des décomposants de Goldbach 11, 29, 17 et 23 de 40 sont :

x	$h(40,x)$
11.0	−33.167184270002586
17.0	−86.832815729998
23.0	−86.832815729998
29.0	−33.16718427000259

Remarque : du fait de résultats algébriques (en utilisant notamment le fait que

$$1 \ - \ \exp(i\theta) \ = \ -2\,i\,\sin(\theta/2)\exp(i\theta/2)),$$

on pourrait indifféremment utiliser la fonction h' définie de $\mathbb{R} \times \mathbb{R}$ dans $\mathbb{R}$ plutôt que de $\mathbb{R} \times \mathbb{R}$ dans $\mathbb{C}$, qui remplace les différents facteurs des produits dans la définition de h :

$$h \ : \ (n,x) \mapsto \prod_{\substack{x \in \mathbb{R} \\ 0 \leq x \leq n \\ k \in \mathbb{N} \\ 2 \leq k \leq \lfloor \sqrt{n} \rfloor}} \left(1 - \exp\left(\frac{2\pi i x}{k}\right)\right)\left(1 - \exp\left(\frac{2\pi i (n-x)}{k}\right)\right)$$

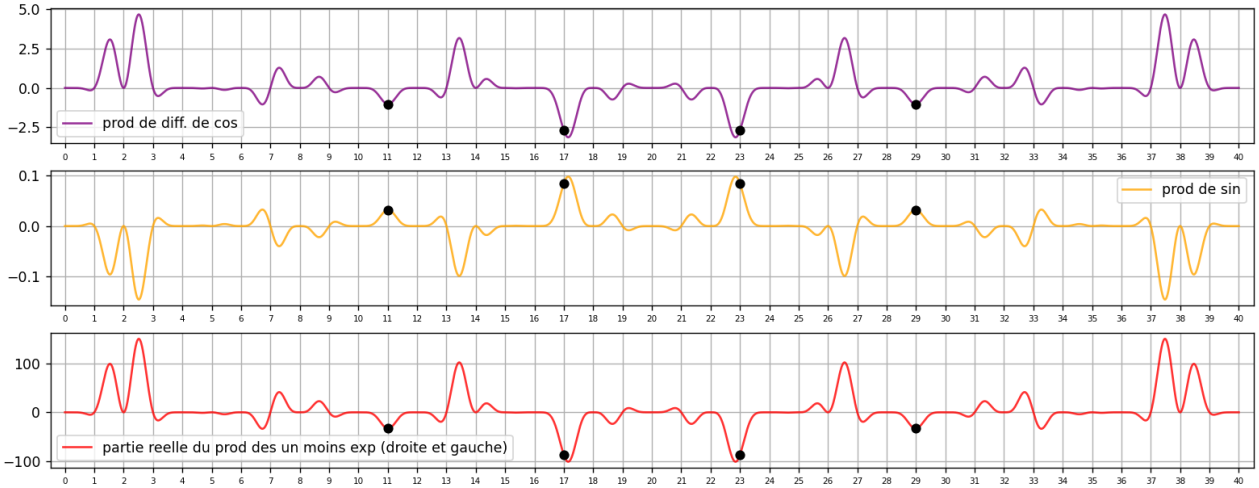
par des différences de cosinus ; h' est définie par

$$h' \ : \ (n,x) \mapsto \prod_{\substack{x\in\mathbb{R}\\0\leq x\leq n\\k\in\mathbb{N}\\2\leq k\leq\lfloor\sqrt{n}\rfloor}} \left(\cos\left(\frac{n\,\pi}{k}\right) - \cos\left(\frac{(n-2x)\pi}{k}\right)\right)$$

(ou encore utiliser la fonction h'' définie de $\mathbb{R}\times\mathbb{R}$ dans $\mathbb{R}$ qui remplace les facteurs en question par des produits de sinus ainsi [1]

$$h'' \ : \ (n,x) \mapsto \prod_{\substack{x\in\mathbb{R}\\0\leq x\leq n\\k\in\mathbb{N}\\2\leq k\leq\lfloor\sqrt{n}\rfloor}} \sin\left(\frac{x\,\pi}{k}\right) \times \sin\left(\frac{(n-x)\pi}{k}\right).)$$

On montre ci-dessous les bornes différentes (regarder sur l'axe des ordonnées) selon que l'on choisit d'utiliser la fonction h, la fonction h' ou la fonction h''.



Toutes ces fonctions sont paires, si l'on place l'origine en $n/2$, de par leurs définitions mêmes. Lorsqu'on citera certaines valeurs ci-dessous, il s'agira de valeurs de la fonction h'.

Essayons maintenant de comprendre pourquoi il y a toujours au moins un nombre impair différent de 1 et différent de $n-1$ dans l'intervalle $[0,n]$ qui a une image non nulle.

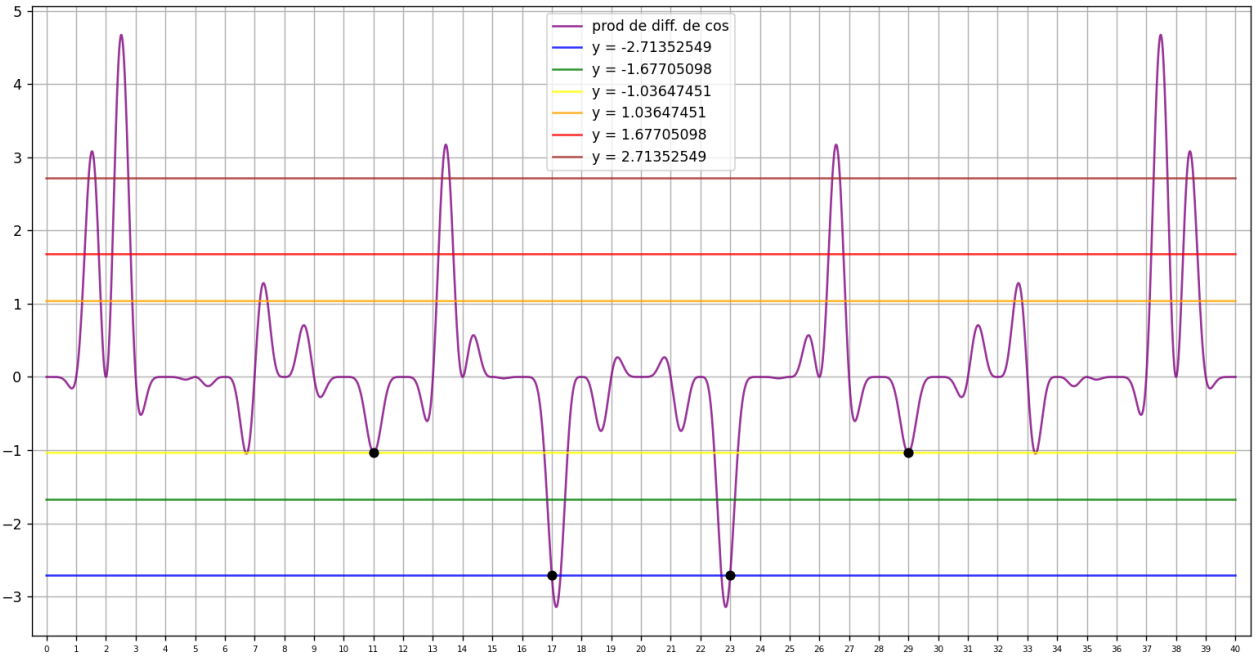
[1] Le tableau ci-dessous fournit les images des décomposants de Goldbach du nombre pair 40 (seuls entiers impairs d'images non nulles) par les fonctions h, h' et h''.

x	$h(40,x)$	$h'(40,x)$	$h''(40,x)$
11.0	−1.0364745084375777	0.03238982838867441	−33.167184270002586
17.0	−2.7135254915624185	0.08479767161132616	−86.832815729998
23.0	−2.7135254915624185	0.08479767161132616	−86.832815729998
29.0	−1.0364745084375777	0.03238982838867441	−33.16718427000259

Pour cela intéressons-nous aux images possibles, qu'on peut imaginer comme des droites horizontales d'équations $y = v_i$. On sait exactement quelles sont les valeurs possibles v_i que peuvent prendre les images des entiers impairs par la fonction h' lorsque x est compris entre deux nombres carrés d'entiers successifs, ces valeurs sont contraintes par la combinatoire des racines de l'unité vues séparément pour chaque entier plus haut : chacun des cosinus pour lequel k apparaît au dénominateur dans la définition de la fonction f_k a $k+1$ valeurs possibles (dont la valeur 0), k étant pair. On peut se reporter à l'annexe 2 pour étudier les valeurs des images pour les nombres compris entre 36 et 48 par exemple : le nombre $r_1 = 1.67705098$ ou le nombre $r_2 = 2.71352549$ apparaissent à plusieurs reprises, alors que ce sont d'autres nombres réels, différents de r_1 et r_2, qui apparaissent pour n compris entre $50 = 7^2 + 1$ et $62 = 8^2 - 2$ car les cosinus faisant intervenir le nombre 6 au dénominateur vont alors intervenir dans les calculs. Les valeurs possibles sont déterminées et en nombre fini, pour n compris entre 2 entiers carrés successifs : par exemple, entre $36 = 6^2$ et $48 = 7^2 - 1$, les valeurs des images par la fonction h' peuvent prendre entre autres les valeurs [2]:

$$-2.71352549, -1.67705098, -1.03647451, 1.03647451, 1.67705098, 2.71352549.$$

On a représenté ci-dessous, pour se faire une image mentale, ce que sont certaines lignes de niveaux (sortes de raies spectrales horizontales), correspondant aux images possibles des entiers par la fonction h'.



[2]Le nombre exact de valeurs contraintes entre deux carrés consécutifs est calculable par une formule ; entre 2^2 et 3^2, il y a 21 valeurs "contraintes" au sens où on l'entend ici ; entre 3^2 et 4^2 (exclus), il y en a 39. Le nombre maximum de valeurs possibles aux impairs, pour k pair, est égal à $\left(\frac{(k+1)^2+1}{2}\right)^2 - \left(\frac{k^2}{2}\right)^2$; pour k impair, ce nombre maximum est égal à $\left(\frac{(k+1)^2}{2}\right)^2 - \left(\frac{k^2+1}{2}\right)^2$. Les premières valeurs que prend ce nombre maximum sont $n_{\max}(2) = 21,\ n_{\max}(3) = 39,\ n_{\max}(4) = 105,\ n_{\max}(5) = 155,\ n_{\max}(6) = 301,\ ....$

En étudiant quelles sont les décompositions de Goldbach, de deux nombres pairs n et n' différents, qui partagent une valeur, dans le fichier des valeurs dont l'adresse est fournie en annexe 2, on réalise que le partage d'une ligne au même niveau pour deux courbes différentes a lieu lorsque le second décomposant de Goldbach est partagé : prenons un exemple illustratif qui sera plus parlant : $38 = 7 + 31$ et $48 = 17 + 31$, le second décomposant (le nombre premier 31) est dit "partagé" par ces deux décompositions de Goldbach et on a $h'(38, 31)$ (pour $n = 38$) qui a la même valeur que $h'(48, 31)$ (pour $n = 48$) (alors qu'il n'y a pas de partage de valeur selon le "petit" décomposant de Goldbach, celui inférieur ou égal à la moitié de n : $h'(38, 7) \neq h'(48, 17)$). Cette propriété fait que de nombreuses lignes de niveaux sont partagées par les nombres pairs compris entre deux mêmes carrés d'entiers. Malheureusement, des études numériques montrent que le partage de valeurs tel qu'on le conçoit là (avec des produits calculés selon k, au dénominateur des arguments des cosinus, appartenant à un intervalle fini de valeurs entières consécutives commençant à 2), n'a pas lieu pour certains nombres pairs.

On sait que $h'(n, x)$ est nul pour tous les entiers pairs. Si $h'(n, x)$ était également nul pour tous les entiers impairs de l'intervalle $[0, n]$, h' devrait être non nulle seulement pour des nombres non entiers, il faudrait donc que sa dérivée s'annule sur un nombre non entier. Peut-être est-il possible de démontrer que cela est impossible... (sic !).

Effectuons maintenant un retour vers l'arithmétique : on souhaiterait réfléchir à nouveau à l'idée du "transfert" des décompositions triviales (de la forme $2p = p + p$ pour p un nombre premier) vers une décomposition d'un autre nombre pair qui ne soit pas le double d'un nombre premier.

En étudiant le fichier des valeurs, on constate par exemple que la valeur de $h'(26, 13)$ est égale (à 10^{-6} près) à la valeur de $h'(30, 7)$. Les calculs utilisent des cosinus qui représentent les divisibilités par les nombres entiers successifs 2, 3, 4 et 5. Etudions ces divisibilités et essayons d'analyser la cause de l'égalité des produits de cosinus.

	2	3	4	5
26	0	2	2	1
13	1	1	1	3
30	0	0	2	0
7	1	1	3	2

Dans tous les cas (pour toutes les valeurs de n, k, x), les nombres vérifient :

$$|(n \bmod k) - (x \bmod k)| = |(n' \bmod k) - (x' \bmod k)|$$

En annexe 3, est fourni le tableau qui permet de "transférer" la décomposition (38, 19) aux décompositions (40,11), (42,11), ou (48,19) ou bien la décomposition (46,23) aux décompositions (40,17) ou (44,7).

On s'est ainsi ramené au groupe des rotations sur le cercle dans le plan complexe. On a du mal à se dire qu'une décomposition de Goldbach existe pour un nombre pair n parce que, très loin vers l'infini, il y a une décomposition triviale d'un nombre premier très grand p qui s'envoie au niveau du produit des cosinus sur le même réel que celui de telle décomposition du nombre pair n en question. C'est pourtant ce qui doit se produire. La navigation en eaux profondes (réels et

complexes) n'étant pas pour nous, on essaie d'oublier tout ça.

Annexe 1 : valeurs des parties réelle et imaginaire pour $n = 40$ des images qui sont non nulles des entiers impairs

$n = 40 \rightarrow$

x	$\mathfrak{Re}(h'(40, x))$	$\mathfrak{Im}(h'(40, x))$
1.0	−5.688191760003811	0.9009210683668445
7.0	4.230470850205377	−8.302766533846412
11.0	0.9009210683668807	5.6881917600038125
13.0	−4.230470850205386	−8.30276653384642
17.0	8.3027665338464	4.2304708502054025
19.0	5.688191760003816	0.9009210683667981
23.0	−8.302766533846421	4.2304708502055055
29.0	−0.9009210683668392	5.688191760003818
31.0	−0.9009210683668969	−5.688191760003788
37.0	−8.302766533846398	−4.230470850205327

Annexe 2 : valeurs des images des décomposants de Goldbach de n par la fonction h' pour les nombres pairs n compris entre 6 et 102.

On pourra trouver tous les graphiques et les scans des résultats d'exécutions de programmes qui montrent les valeurs obtenues par les fonctions h, h' et h'' dans le fichier :
https://denisevellachemla.eu/dessins-fcts-paires.pdf.

Un listing des valeurs des images est également disponible dans le fichier :
https://denisevellachemla.eu/valnum.pdf.

Annexe 3 : transfert de décompositions triviales

	2	3	4	5	6
38	0	2	2	3	2
19	1	1	3	4	1
40	0	1	0	0	4
11	1	2	3	1	5
42	0	0	2	2	0
11	1	2	3	1	5
48	0	0	0	3	0
19	1	1	3	4	1

	2	3	4	5	6
46	0	1	2	1	4
23	1	2	3	3	5
40	0	1	0	0	4
17	1	2	1	2	5
44	0	2	0	4	2
7	1	1	3	2	1

Droites d'émission ou droites d'absorption (Denise Vella-Chemla, 18.7.2024)

On cherche à démontrer que tout nombre pair n supérieur à 4 admet un décomposant de Goldbach, i.e. un nombre premier x dont le complémentaire à n, $n-x$, est premier également.

Pour comprendre la raison qui fait, pour le dire simplement, "qu'on a toujours un non nul en face d'un non nul", on va ici décomposer le problème en un ensemble de problèmes plus simples [1]., selon chacun des dénominateurs intervenant dans la formule de la fonction h_n (n désignant un nombre pair dont on cherche s'il admet une décomposition de Goldbach) :

$$\begin{array}{rccc} h_n : & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \displaystyle\prod_{\substack{x\in\mathbb{R} \\ 0\leq x\leq n \\ k\in\mathbb{N} \\ 2\leq k\leq\lfloor\sqrt{n}\rfloor}} \left(\cos\left(\frac{n\,\pi}{k}\right) - \cos\left(\frac{(n-2x)\pi}{k}\right)\right) \end{array}$$

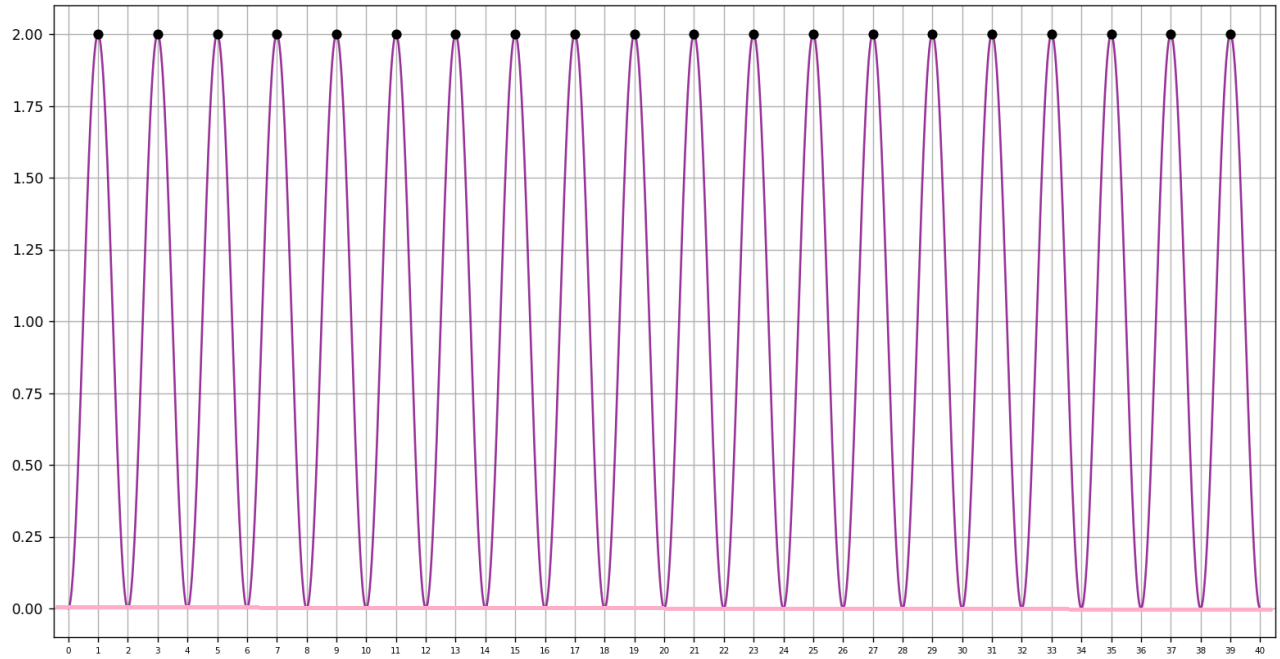
On utilise le programme python ci-dessous :

```
import matplotlib.pyplot as plt
import numpy as np
import math
from math import floor, sqrt, sin, cos

pi, i, exp = np.pi, 1j, np.exp
epsilon = 1e-6
for n in range(40, 42, 2):
     print(n,' ---->')
     d = 2
     x = np.linspace(0, n, num=n*10**d+1, endpoint=True)
     xl, xr = -0.5, n+0.5
     w = []
     for k in range(len(x)):
          produit = 1
          #for p in range(2, int(floor(sqrt(n))) + 1):    *****
          for p in [13]:
               produit = produit*(cos(n*pi/p)-cos(pi*(n-2*x[k])/p))
          w += [produit]
     plt.figure(figsize=(20, 8))
     plt.plot(x, w, alpha=0.8, color='purple')
     for k in range(len(x)):
          if (abs(x[k]%2 - 1) < epsilon) and (abs(w[k]) > epsilon):
               plt.plot(x[k], w[k], color='black', marker='o')
               print(x[k],' ', w[k])
     plt.xlim(xl, xr)
     plt.xticks(range(0,n+1), fontsize=6)
     plt.grid(True)
plt.show()
```

Ce qui nous intéresse, c'est d'étudier le comportement de chacune des courbes qui intervient dans le produit global. On va modifier la ligne du programme marquée de cinq étoiles de façon à ce

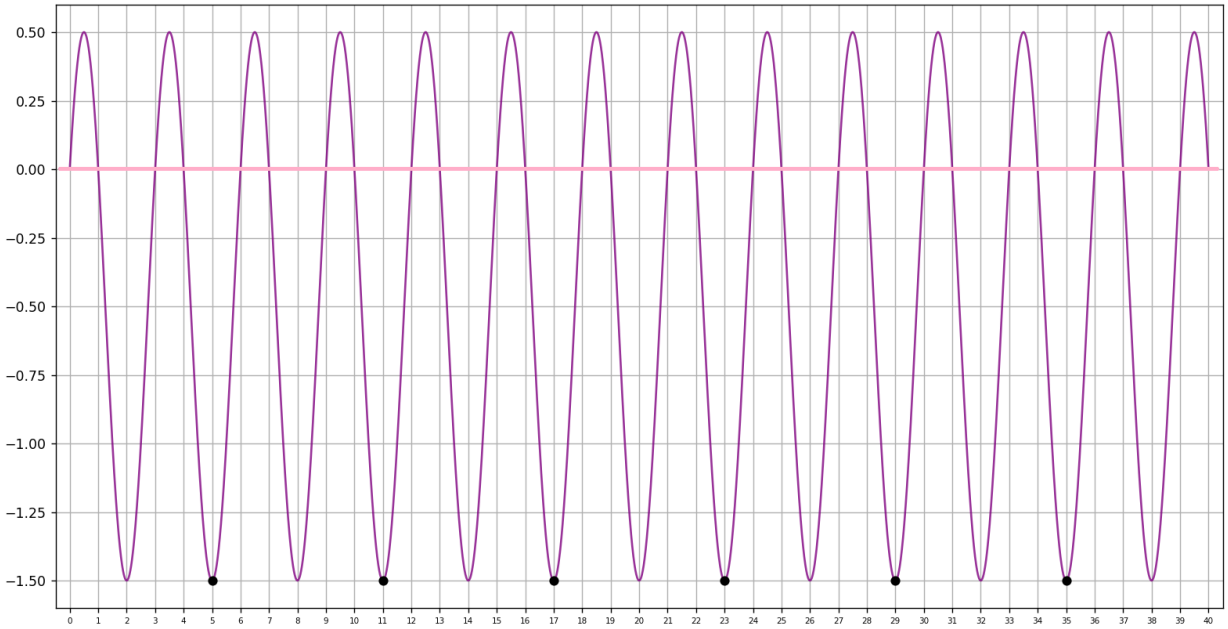
[1] selon la méthode préconisée par Pólya.

qu'elle dessine les courbes une par une [2]. Voici la courbe obtenue si on ne considère que le cas où $p = 2$.



La valeur en 2 étant nulle, d'autres valeurs nulles vont advenir pour tous les nombres impairs sur la ligne de couleur rose.

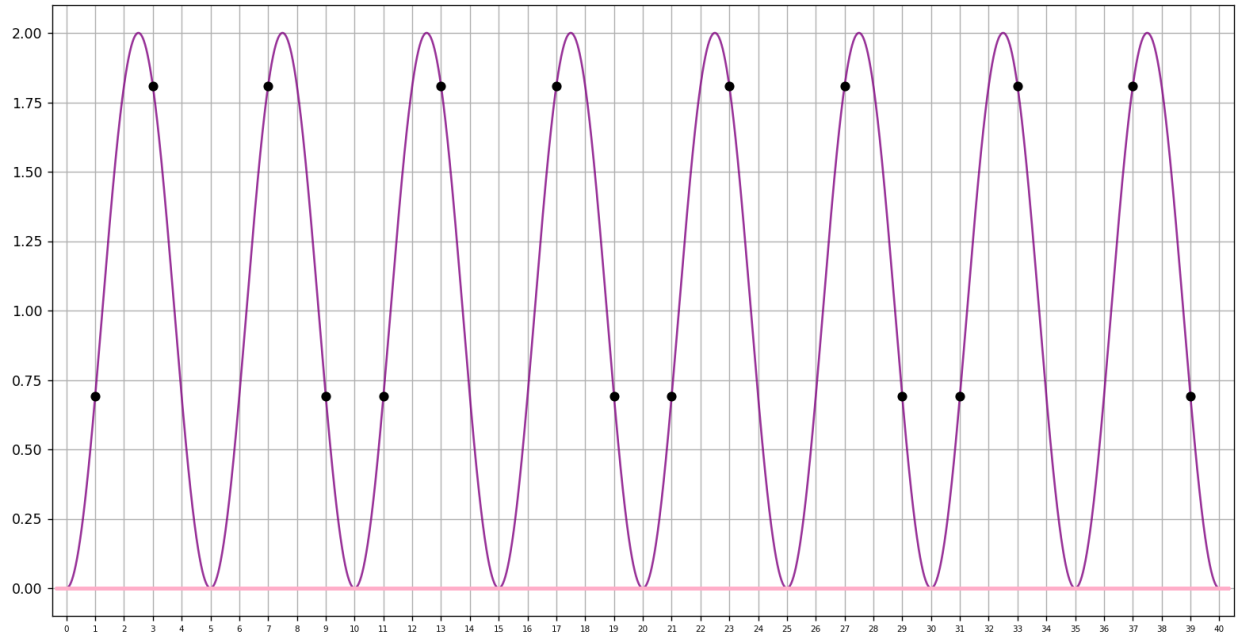
Voyons la courbe pour le cas où $p = 3$.



[2]La ligne `for p in [13]:` du programme permet d'obtenir le dessin de la courbe de la fonction calculant la différence de cosinus avec le nombre 13 utilisé comme dénominateur dans les arguments des cosinus.

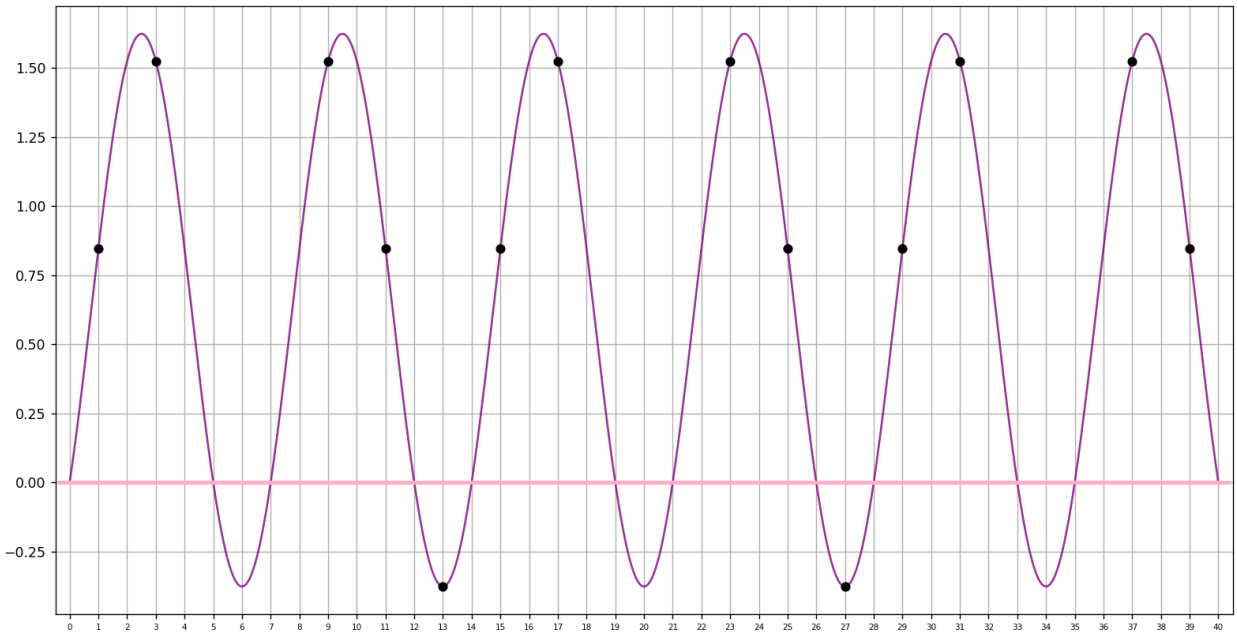
La valeur en 3 étant nulle, d'autres valeurs nulles vont advenir pour tous les nombres impairs sur la ligne de couleur rose.

Voyons la courbe pour le cas où $p = 5$.



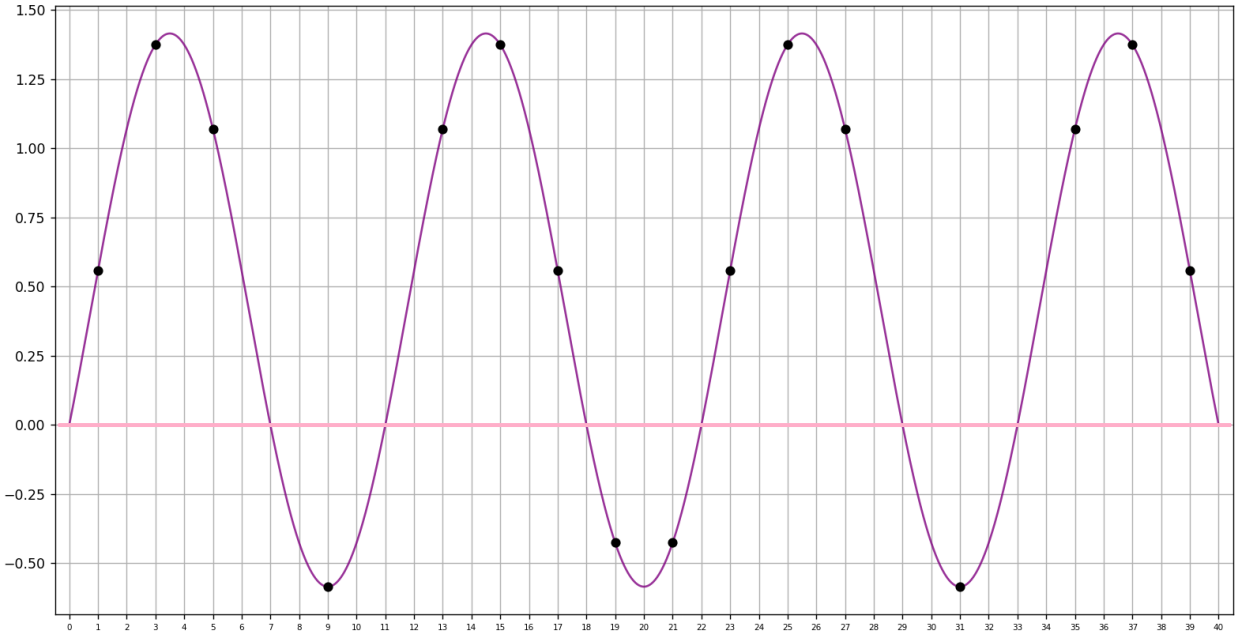
La valeur en 5 étant nulle, d'autres valeurs nulles vont advenir pour tous les nombres impairs sur la ligne de couleur rose.

Voyons la courbe pour le cas où $p = 7$.



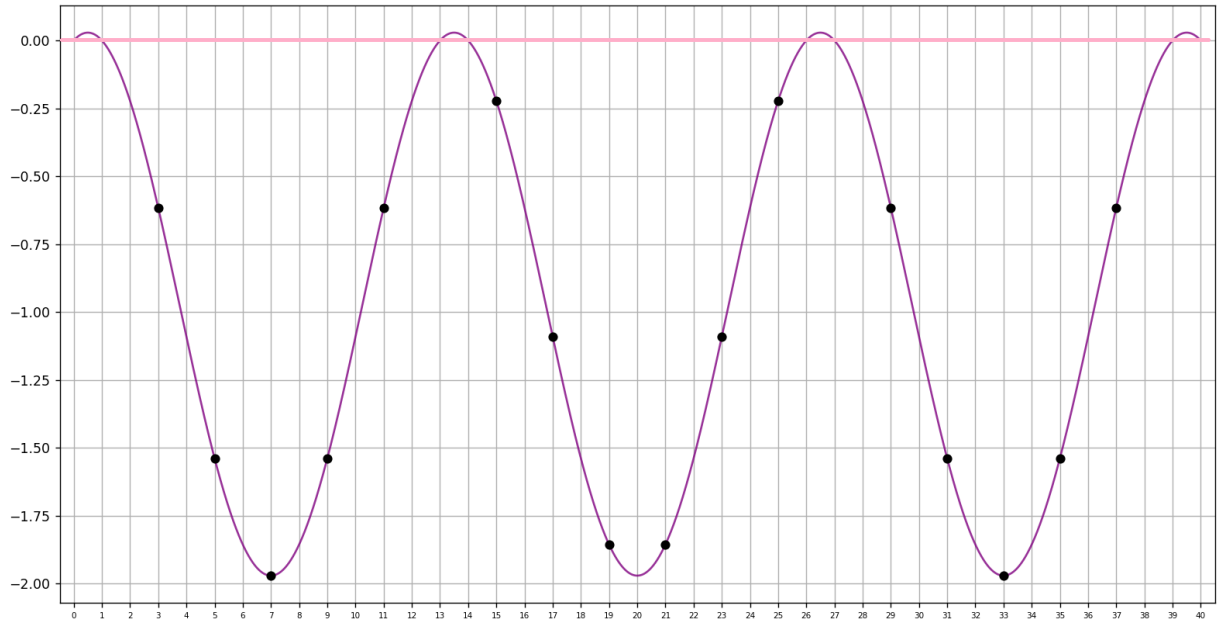
La valeur en 7 étant nulle, d'autres valeurs nulles vont advenir pour tous les nombres impairs sur la ligne de couleur rose.

Voyons la courbe pour le cas où $p = 11$.



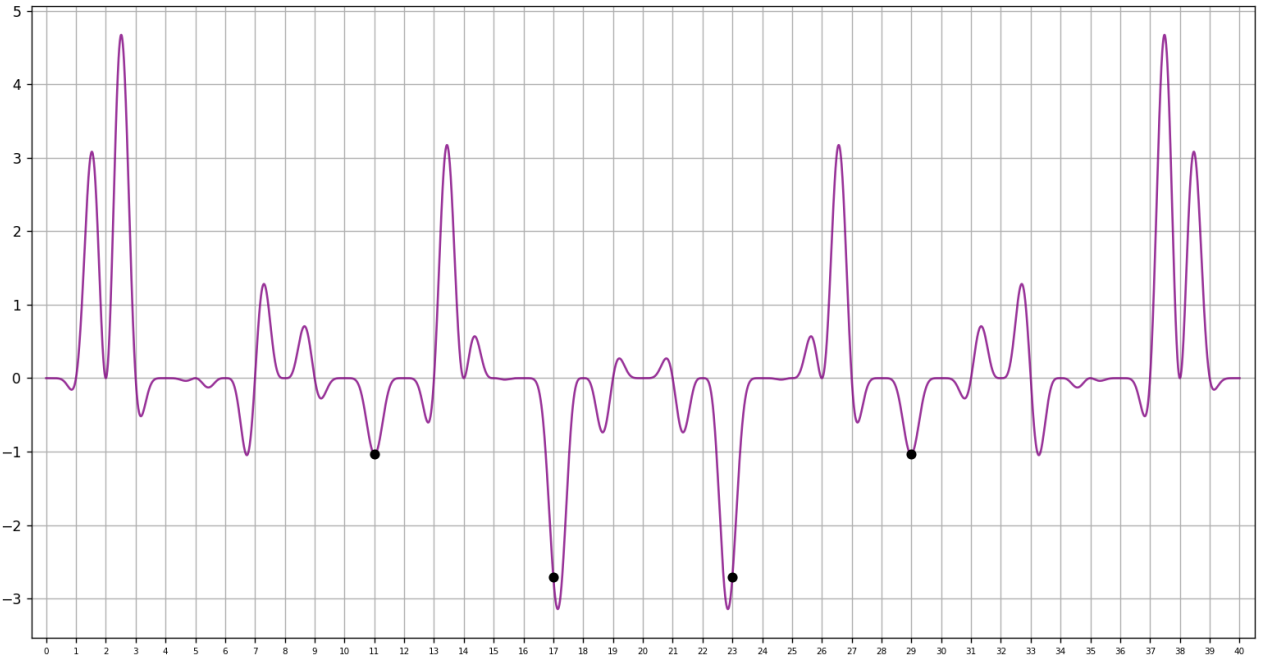
La valeur en 11 étant nulle, d'autres valeurs nulles vont advenir pour tous les nombres impairs sur la ligne de couleur rose.

Voyons la courbe pour le cas où $p = 13$.



La valeur en 13 étant nulle, d'autres valeurs nulles vont advenir pour tous les nombres impairs sur la ligne de couleur rose.

Voyons maintenant le produit global de toutes les images par ces différentes fonctions (dans le programme, cela correspond à utiliser la ligne à cinq étoiles) : il permet effectivement, si on cherche les nombres impairs dont l'image est non nulle, de trouver les décomposants de Goldbach de $n = 40$ qui sont supérieurs à $\sqrt{40} \simeq 6$.



Ce sont vraisemblablement les propriétés individuelles des courbes qui vont garantir qu'on aura toujours "un impair non nul en face d'un impair non nul" ; le fait que l'image de cet impair est non nulle garantit qu'il est premier, et il en est de même de son complémentaire à n, par la symétrie autour de $n/2$ de la courbe de la fonction h_n.

On voit qu'on a changé notre façon de regarder le problème : il y a quelques temps, on disait "il faut éliminer deux classes de congruence par module premier pour trouver les décomposants de Goldbach". Ici, on se place plutôt sur la droite réelle (et c'est le passage par le plan complexe qui nous a fait adopter ce nouveau point de vue) et on voit qu'il faut conserver certains intervalles ouverts de la droite réelle, ceux qui contiennent les points d'images non nulles. On décide de considérer des intervalles d'extrémités des nombres demi-entiers, pour qu'ils contiennent en leur intérieur les nombres entiers.

Ci-dessous, on montre sur un graphique les intervalles conservés (si l'on se dit que le crible d'Eratosthène, en éliminant les nombres composés, les "absorbe", on prend ici les nombres dans l'ensemble complémentaire, qui seraient comme des nombres "émis").

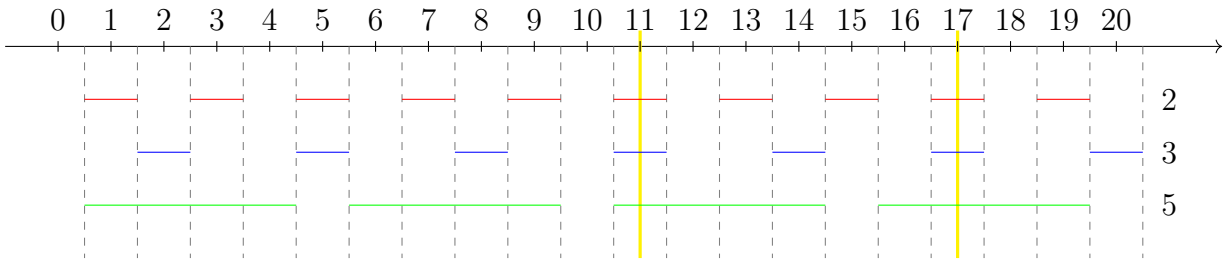


FIGURE 1 : $n = 40$: recouvrement de la droite réelle par des ouverts

L'existence d'une solution (d'un décomposant de Goldbach) correspond alors au fait de trouver un nombre qui appartient à l'intersection des recouvrements par des ouverts.

Remarque : dans le cas qui nous intéressait ici (où il s'agissait de conserver les nombres qui ne sont ni divisibles par 7 ni congrus à 5 modulo 7 dans le premier cas, et ceux qui ne sont ni divisibles par 11 ni congrus à 7 modulo 11 dans le deuxième cas), on ne sait pas s'il faudrait distinguer les sous-recouvrements ; par exemple, ci-dessous, le recouvrement contenant les intervalles de type A et les intervalles de type B (ou bien le recouvrement contenant les intervalles de type C et les intervalles de type D), doit-il être scindé en un recouvrement ne prenant en compte que les intervalles de types A (resp. C) et un autre ne prenant en compte que les intervalles de type B (resp. D) sous prétexte que ces intervalles (A et B, resp. C et D) ne sont pas de la même longueur.

Concernant les recouvrements par des ouverts, on se reportera aux articles de la bibliographie.

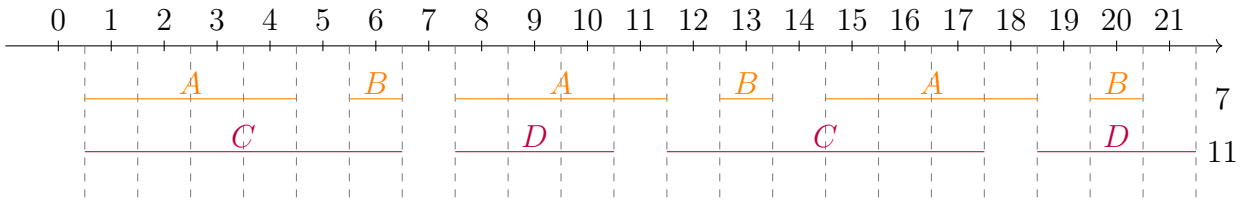


FIGURE 2 : éliminer les divisibles par 7 ou congrus à 5 modulo 7 (intervalles oranges),
éliminer les divisibles par 11 ou congrus à 7 modulo 11 (intervalles pourpres).

Que sait-on, à peut-être utiliser dans une démonstration ?

1) On sait par le théorème de Pafnouti Tchebychev (1850), aussi appelé Postulat de Bertrand, qu'entre un entier et son double, il existe toujours au moins un nombre premier : lorsqu'on applique ce théorème au nombre premier p_k, puisque tout nombre premier p_{k+1} est inférieur à $2\,p_k$, on a dans l'autre sens que $p_k > \dfrac{p_{k+1}}{2}$.

2) Quand on élimine (au maximum) deux classes de congruence modulo chaque module premier, ou bien dans le langage topologique, quand on élimine deux intervalles (deux ouverts) de longueur 1 (d'extrémités demi-entières) sur une ligne, le meilleur des cas (au sens où c'est le cas qui maximise la longueur du segment emboîté obtenu) est quand les deux intervalles de longueur 1 sont contigus ; le pire des cas est quand un intervalle de longueur 1 tombe au milieu de l'intervalle de longueur p_k, ce qui équilibre la taille des deux intervalles séparés par lui. On a facilement comme résultat

que le plus petit des intervalles est toujours tout de même de longueur supérieure à $\frac{p_k - 3}{2}$.

3) On dispose du théorème des intervalles emboîtés qui nous permet de trouver un point dans une suite d'intervalles de longueurs décroissantes (Théorème 5.5.10, p. 74, [3]) [3].

Bibliographie

[1] Alexander Grothendieck, A general theory of fiber spaces with structure scheaf (Une théorie générale des espaces fibrés à structure de faisceaux), Cours donné à l'Université du Kansas, à Lawrence, aux Etats-Unis (NSF-G 1126, Projet de recherche sur la géométrie des espaces de fonctions, Rapport no 4, première édition août 1955, seconde édition Mai 1958). lien.
Traduction en français des deux premiers chapitres :
https://denisevellachemla.eu/AG-biblio/transc-AG-fibres-1et2-fr.pdf

[2] Jean Malgoire, Un héritage mathématique fertile, Magazine Pour la Science, n° 467, septembre 2016.
https://denisevellachemla.eu/transc-Malgoire.pdf

[3] Jacques Dixmier, Topologie générale, Puf, 1981.

[3] On rappelle un jeu, auquel on peut jouer avec des élèves d'école élémentaire : ils doivent deviner un nombre décimal, en posant des questions "est-il plus grand (ou plus petit) que tel nombre ?". On peut faire durer le jeu le temps que l'on souhaite en "s'échappant systématiquement de l'autre côté", i.e. en trichant et en modifiant le nombre qu'on a choisi au fur et à mesure, pour le faire appartenir à l'intervalle réduit "emboîté" que les élèves trouvent petit à petit. Ce jeu permet, lentement mais sûrement, de faire appréhender la notion de nombre réel à d'assez jeunes élèves.

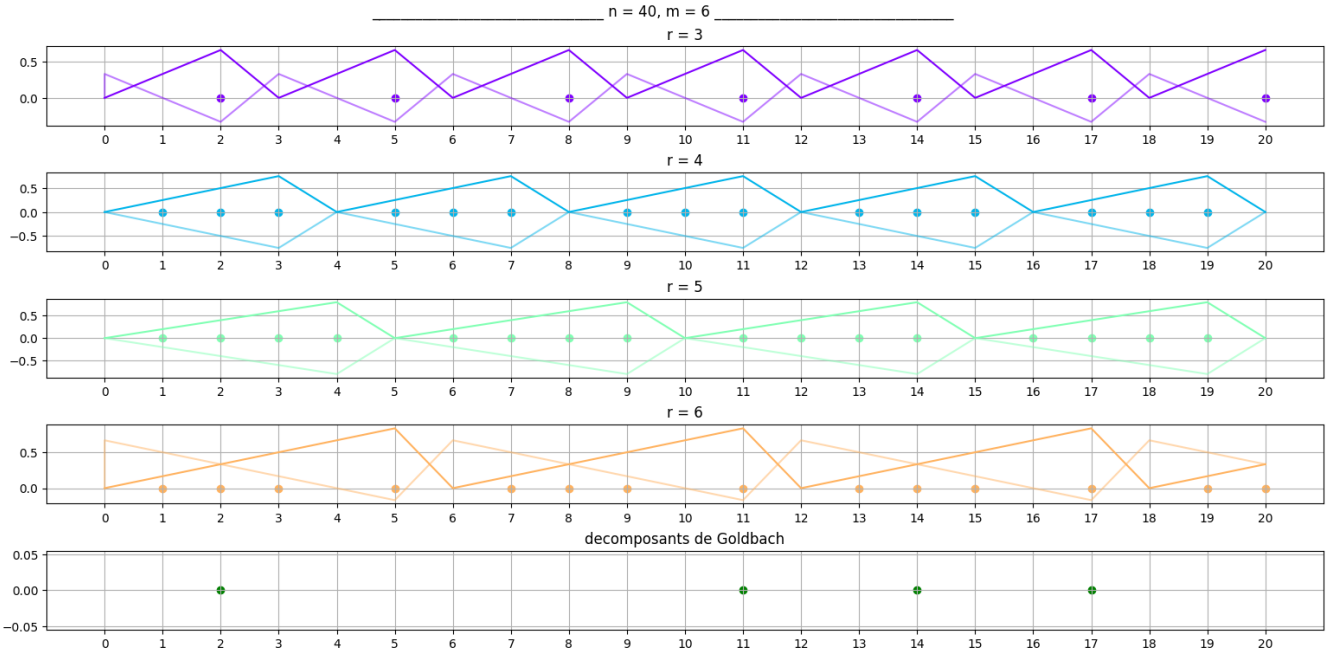
Papillons et sapins (Denise Vella-Chemla, 4.8.2024)

On cherche à démontrer que tout nombre pair n supérieur à 4 admet un décomposant de Goldbach, i.e. un nombre premier x dont le complémentaire à n, $n - x$, est premier également.

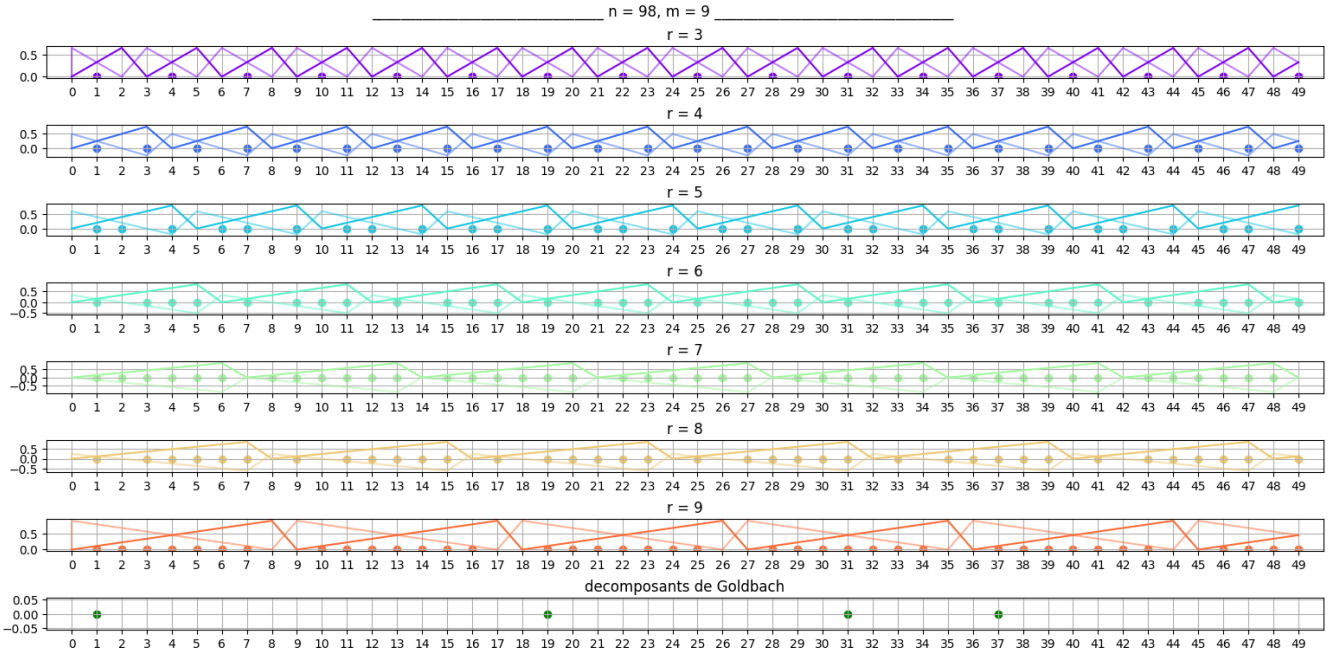
Suite à des travaux récents qui permettaient de caractériser les décomposants de Goldbach en effectuant un petit détour par le plan complexe, on est finalement amenée à utiliser le programme suivant, très simple, qui exprime des conditions booléennes (x est premier, $n - x$ est premier) en utilisant les parties décimales de nombres rationnels.

```
import math
from math import floor, sqrt
import matplotlib.pyplot as plt, matplotlib.cm as cm

def partiedecimale(x):
     return x-int(x)

epsilon = 1e-6
for n in range(2024, 2026, 2):
     milieu = n//2 if n%2 == 0 else n//2+1
     m = int(floor(sqrt(n)))
     fig, axs = plt.subplots(nrows=m+1-3+1, layout='constrained')
     fig.set_figwidth(18)
     fig.set_figheight(12)
     produitglobal = [True for x in range(milieu+1)]
     for r in range(3, m+1):
          c = cm.rainbow((r-3)/(m+1-3))
          xs, y1, y2 = [0], [0], [0]
          for x in range(milieu+1):
               cond1 = partiedecimale(x/r)
               cond2 = partiedecimale(n/r)-partiedecimale(x/r)
               produit = abs(cond1)>epsilon and abs(cond2)>epsilon
               if produit:
                    axs[r-3].scatter(x, 0, color=c)
               produitglobal[x] &= produit
               xs += [x]
               y1 += [cond1]
               y2 += [cond2]
          axs[r-3].plot(xs, y1, color=c)
          axs[r-3].plot(xs, y2, color=c, alpha=0.5)
          axs[r-3].set_title(f'r = r')
          axs[r-3].set_xticks(range(0, milieu+1))
          axs[r-3].set_xlim(-1, milieu+1)
          axs[r-3].grid()
     xs = [k for k, p in enumerate(produitglobal) if p]
     ys = [0 for x in xs]
     axs[-1].scatter(xs, ys, color='green')
     axs[-1].set_title(f'decomposants de Goldbach')
     axs[-1].set_xticks(range(0, milieu+1))
     axs[-1].set_xlim(-1, milieu+1)
     axs[-1].grid()
     fig.suptitle(f' n = n, m = m '.center(80, '_'))
     plt.show()
```

Ci-dessous le dessin des différentes courbes, indicées par l'entier r, r variant entre 3 et $\lfloor\sqrt{n}\rfloor$, pour $n = 40$, puis pour $n = 98$.



L'une des courbes, selon un certain entier r, montre la variation de la partie décimale de $\dfrac{x}{r}$, qu'on peut écrire $\dfrac{x}{r} \bmod 1$, et l'autre courbe (de même couleur, mais un peu plus claire) montre la variation de la différence des parties décimales de $\dfrac{n}{r}$ et de $\dfrac{x}{r}$, qu'on peut écrire $\dfrac{n}{r} \bmod 1 - \dfrac{x}{r} \bmod 1$. Les courbes sont en miroir l'une de l'autre, autour d'un axe de symétrie. On marque, pour chaque r, les points d'images non nulles. On s'est ainsi placé, en étudiant les restes modulo 1, dans $\mathbb{R}/\mathbb{Z}$, dans lequel deux nombres appartiennent à la même classe d'équivalence s'ils ont même partie décimale.



La dernière courbe, en bas de chaque graphique, montre les décomposants de Goldbach de n. Ce sont les nombres dont les images selon tout r sont non nulles.

On exécute le programme ci-dessus, pour les nombres pairs de 10 à 102, son résultat d'exécution est consigné dans le fichier https://denisevellachemla.eu/harmonies-colorees.pdf (on a omis les courbes pour le nombre premier 2 pour gagner de la place ; celles-ci font éliminer les décomposants pairs).

L'étude des différentes courbes montre que :

- chaque courbe est périodique, de période r ;
- lorsque r divise n, un seul nombre est d'image nulle par période de longueur r ;
- lorsque r ne divise pas n, deux nombres sont d'image nulle par période de longueur r ; on va donc considérer qu'on élimine au maximum deux nombres par période pour tout r compris entre 2 et $\sqrt{n}$ (on cherche une borne qui maximise le nombre de nombres éliminés - i.e. qui ne peuvent pas être des décomposants de Goldbach de n, ce qui permettra de trouver une borne qui minimise le nombre de nombres conservés - i.e. ce qui permettra de dire une phrase comme "Tout nombre pair a forcément, au moins, tant de décompositions de Goldbach") [1].
- il y a $\frac{n}{2r}$ périodes de longueur r sur l'intervalle $\left[0, \frac{n}{2}\right]$;
- le nombre de nombres d'image nulle sur chaque graphique (on appelle aussi cela le cardinal de l'intersection des noyaux des deux fonctions présentées par graphique) est ainsi inférieur à $\left\lceil \frac{n}{2r} \right\rceil \times 2$;
- si l'on recense dans une liste, en les ajoutant à la liste au fur et à mesure, les nombres d'image nulle, on voit que le nombre de nombres supplémentaires ajoutés à cette liste pour le niveau r ne peut excéder $\left\lceil \frac{n}{2r} \right\rceil \times 2 \times \frac{1}{(r-1)!}$. Voyons un exemple : pour $n = 98$, les nombres d'image nulle pour $r = 3$ sont les nombres de la liste

$$L_3 = \{2, 3, 5, 6, 8, 9, 11, 12, 14, 15, 17, 18, 20, 21, 23, 24, \\ 26, 27, 29, 30, 32, 33, 35, 36, 38, 39, 41, 42, 44, 45, 47, 48\}$$

  tandis que ceux d'image nulle pour $r = 5$ sont les nombres de la liste

$$L_5 = \{3, 5, 8, 10, 13, 15, 18, 20, 23, 25, 28, 30, 33, 35, 38, 40, 43, 45, 48\}.$$

  Si on barre dans L_5 les nombres qui appartiennent à L_3, il est clair que 2 "paquets de 2 nombres" sur 3 sont à barrer (i.e. appartenaient déjà à L_3) quand 1 paquet de 2 nombres sur 3 va être à considérer en plus, car ces nombres n'appartiennent pas à L_3.

$$L_5 = \{\cancel{3}, \cancel{5}, \cancel{8}, 10, 13, \cancel{15}, \cancel{18}, \cancel{20}, \cancel{23}, 25, 28, \cancel{30}, \cancel{33}, \cancel{35}, \cancel{38}, 40, 43, \cancel{45}, \cancel{48}\}$$

[1] La démonstration, par Leila Schneps, du fait que les nombres trouvés ici sont bien des décompositions de Goldbach de n (i.e. des sommes de deux nombres premiers) est consultable à cette adresse https://denisevellachemla.eu/jade1.pdf.

C'est cette petite découverte récente qui permet de maximiser le nombre de nombres d'image nulle par l'expression :

$$\sum_{\substack{2\leq r\leq \lfloor\sqrt{n}\rfloor \\ r\in\mathbb{N}}} \left\lceil \frac{n}{2r} \right\rceil \times \frac{2}{(r-1)!} \simeq \sum_{\substack{2\leq r\leq \lfloor\sqrt{n}\rfloor \\ r\in\mathbb{N}}} \frac{n}{r(r-1)!} \simeq \sum_{\substack{2\leq r\leq \lfloor\sqrt{n}\rfloor \\ r\in\mathbb{N}}} \frac{n}{r!}$$

On utilise le programme ci-dessous (qui distingue les diviseurs de n pour lesquels un nombre est éliminé par période, des non-diviseurs pour lesquels 2 nombres sont éliminés par période) :

```
import math
from math import sqrt,floor,factorial

for n in range(10,10002,2):
     print('n = ',n,' ---> ',end='')
     racine = int(floor(sqrt(n)))
     somme = 0
     for r in range(2,racine+1):
          if n%r == 0:
               somme = somme+n/(2*factorial(r))
          else:
               somme = somme+n/factorial(r)
     print(somme, ' a comparer a ',n/2)
```

dont le résultat est :

```
n = 10 ---> 4.166666666666667 a comparer a 5.0
n = 12 ---> 4.0 a comparer a 6.0
n = 14 ---> 5.833333333333334 a comparer a 7.0
n = 16 ---> 6.999999999999999 a comparer a 8.0
n = 18 ---> 6.75 a comparer a 9.0
n = 20 ---> 8.75 a comparer a 10.0
n = 22 ---> 10.083333333333332 a comparer a 11.0
n = 24 ---> 8.5 a comparer a 12.0
n = 26 ---> 12.133333333333333 a comparer a 13.0
n = 28 ---> 12.483333333333334 a comparer a 14.0
n = 30 ---> 11.375 a comparer a 15.0
n = 32 ---> 14.266666666666666 a comparer a 16.0
n = 34 ---> 15.866666666666667 a comparer a 17.0
n = 36 ---> 13.075000000000001 a comparer a 18.0
n = 38 ---> 17.786111111111108 a comparer a 19.0
n = 40 ---> 17.722222222222225 a comparer a 20.0
n = 42 ---> 16.129166666666666 a comparer a 21.0
n = 44 ---> 19.677777777777777 a comparer a 22.0
n = 46 ---> 21.53055555555556 a comparer a 23.0
n = 48 ---> 17.433333333333334 a comparer a 24.0
n = 50 ---> 23.20436507936508 a comparer a 25.0
n = 52 ---> 23.265873015873012 a comparer a 26.0
n = 54 ---> 20.748214285714287 a comparer a 27.0
n = 56 ---> 25.050000000000004 a comparer a 28.0
n = 58 ---> 27.158730158730158 a comparer a 29.0
```

```
n = 60 ---> 21.55357142857143 a comparer a 30.0
n = 62 ---> 29.03174603174603 a comparer a 31.0
n = 64 ---> 28.635714285714283 a comparer a 32.0
n = 66 ---> 25.36056547619048 a comparer a 33.0
n = 68 ---> 30.426289682539686 a comparer a 34.0
n = 70 ---> 32.48090277777777 a comparer a 35.0
n = 72 ---> 26.165178571428577 a comparer a 36.0
n = 74 ---> 34.65262896825397 a comparer a 37.0
n = 76 ---> 34.005853174603175 a comparer a 38.0
n = 78 ---> 29.97157738095238 a comparer a 39.0
n = 80 ---> 35.46130952380953 a comparer a 40.0
n = 82 ---> 38.39908509700175 a comparer a 41.0
n = 84 ---> 30.518981481481482 a comparer a 42.0
n = 86 ---> 40.27221119929454 a comparer a 43.0
n = 88 ---> 39.374349647266314 a comparer a 44.0
n = 90 ---> 34.2077132936508 a comparer a 45.0
n = 92 ---> 41.16523368606702 a comparer a 46.0
n = 94 ---> 44.01846340388006 a comparer a 47.0
n = 96 ---> 34.88716931216931 a comparer a 48.0
n = 98 ---> 45.88186728395062 a comparer a 49.0
n = 100 ---> 44.32816633597884 a comparer a 50.0
...
n = 1000 ---> 443.26928987879825 a comparer a 500.0
n = 10000 ---> 4432.692898787745 a comparer a 5000.0
n = 100000 ---> 44326.92898787744 a comparer a 50000.0
n = 1000000 ---> 443269.28987877443 a comparer a 500000.0
```

Ces résultats montrent que le nombre maximum de nombres éliminés (nombre de nombres d'image nulle) est toujours inférieur à $\frac{n}{2}$.

Conjecture de Goldbach et géométrie affine, Denise Vella-Chemla, octobre 2024

Il s'agit d'expliquer simplement la conjecture de Goldbach. On cherche les décomposants de Goldbach d'un nombre pair n. On n'utilise que des additions/soustractions itérées (entendues comme des opérateurs), à partir d'un nombre donné, dans $\mathbb{Z}$ l'ensemble des entiers relatifs (sauts de tant en tant, vers un nombre plus grand ou vers un nombre plus petit). On présentera les idées dans l'ensemble des matrices 2×2 plus loin.

Les deux questions qu'on se pose sont :

- à partir d'un nombre x, peut-on atteindre 0, par des soustractions itérées d'un nombre compris entre 2 et $x-1$? et
- à partir d'un nombre x, peut-on atteindre n, par des additions itérées d'un nombre compris entre 2 et $x-1$?".

Si on peut atteindre 0 à partir de x, i.e. si $0 = x - a \times b$, avec $a, b \in [2, x-1]$ alors x est composé. Si on peut atteindre n à partir de x, i.e. si $n = x + a \times b$, avec $a, b \in [2, x-1]$ alors le complémentaire de x à n (noté $n - x$) est composé.

On comprend aisément que les décomposants de Goldbach de n sont les nombres qui ne permettent ni d'atteindre 0 par itération d'un certain nombre de soustractions, ni d'atteindre n par itération d'un certain nombre d'additions (en respectant les contraintes énoncées ci-dessus).

Voyons les nombres qui ne sont pas des décomposants de 98 [1]:

- on atteint 0 à partir de n'importe quel pair par soustractions itérées de 2, ou bien on atteint $n = 98$ à partir de n'importe quel pair par additions itérées de 2 ;
- on atteint 98, à partir de 3, par additions itérées de 5 ; il en est de même à partir de 13 ou de 43 ;
- on atteint 98, à partir de 5, par additions itérées de 3 ; il en est de même à partir de 11, 17, 29, 41 ou de 47 ;
- on atteint 98, à partir de 7, par additions itérées de 7 ;
- on atteint 0, à partir de 9, par soustractions itérées de 3 ; il en est de même à partir de de 15, 21, 33 ou 39 ;
- on atteint 0, à partir de 25, par soustractions itérées de 5 ; il en est de même à partir de 35 ou de 45.

Voyons maintenant les décomposants de 98.

- on ne peut atteindre ni 0 par soustractions itérées de 2, ni 98 par additions itérées de 2, à partir de 19 ou bien à partir de son complémentaire à 98 qui est 79 ; il en est de même par des soustractions itérées d'un nombre quelconque compris entre 2 et 18 pour 19, ou compris entre 2 et 78 pour 79 ;

[1] Les énoncés ci-dessous s'expriment très simplement dans le langage des congruences de Gauss.

- de même, 0 ou 98 sont hors d'atteinte de $x = 31$ ou de $n - x = 67$, par additions ou soustractions itérées d'un nombre compris entre 2 et x, et 0 est hors d'atteinte de $n - x = 67$ par soustractions itérées de nombres compris entre entre 2 et $n - x$;

  enfin, 0 ou 98 sont hors d'atteinte de $x = 37$ et $n - x = 61$, par additions ou soustractions itérées d'un nombre compris entre 2 et x, et 0 est hors d'atteinte de $n-x = 61$ par soustractions itérées de nombres compris entre 2 et $n - x$.

Comment être sûre qu'un nombre qui n'atteint ni 0 par soustractions itérées ni n par additions itérées existe toujours ?

On peut se placer dans un autre espace : utilisons le cercle modulaire (horloge) sur lequel sont positionnés les nombres de 0 à n avec identification de ces deux extrémités 0 et n. Les additions/soustractions itérées deviennent des rotations d'angle constant et leurs puissances, dans le sens horaire ou anti-horaire, sur ce cercle. Il se produit cependant quelque chose de différent : en partant d'un décomposant de Goldbach et en effectuant les rotations dans un sens et l'autre, on finira au bout d'un certain nombre de sauts à revenir à son point de départ, mais plus ou moins vite : prenons $n = 20$, il a pour décompositions de Goldbach $3 + 17$ et $7 + 13$. Les nombres successifs par sauts de 3 à partir de 3 donnent :

$$3, 6, 9, 12, 15, 18, 1, 4, 7, 10, 13, 16, 19, 2, 5, 8, 11, 14, 17, 20, 3.$$

En partant de 3, il a fallu effectuer 20 sauts pour revenir à 3 (ou 19 sauts pour atteindre $n = 20$). Si l'on veut, pour trouver les décomposants de Goldbach, imposer la contrainte "ne pas atteindre 0 (qui est dans le cas du cercle modulaire identifié à n)" en effectuant des rotations itérées d'angle fixé dans un sens ou dans l'autre, il faut imposer une contrainte sur le nombre de sauts : "ne pas atteindre 0 ou n en un nombre de sauts inférieur à $n/2$ par exemple."

Représentons ces idées par des matrices 2×2. Les nombres sont représentés par des matrices de la forme $\begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}$; par exemple la matrice $\begin{pmatrix} 19 & 1 \\ 1 & 0 \end{pmatrix}$ représente le nombre 19. Les opérateurs, ou matrices correspondant aux sauts de tant en tant, sont représentés par des matrices de la forme $\begin{pmatrix} 1 & \delta \\ 0 & 1 \end{pmatrix}$. On utilise l'opération d'élévation à une certaine puissance d'une matrice pour itérer l'action d'un opérateur.

Exemple : faire 2 sauts montants de longueur 3 à partir de 19 (i.e. ajouter 2 fois 3 à 19, et on doit bien sûr trouver 25 par multiplication matricielle).

$$\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 19 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 22 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 25 & 1 \\ 1 & 0 \end{pmatrix}$$

Pour représenter correctement le saut souhaité, l'opérateur doit être placé à gauche du nombre (*attention* : du fait de la non-commutativité de la multiplication matricielle, le résultat obtenu est différent si l'opérateur est placé à droite du nombre).

En ayant bien à l'esprit que les 3 manières fournies ci-dessus de présenter le problème sont équivalentes, revenons à la droite des entiers relatifs.

Écrivons ci-dessous les différentes façons d'atteindre 98, qu'on écrit sous la forme $a + bc$ (on les imagine comme c additions du nombre b du nombre a) ou les différentes façons d'atteindre 0 (remplacer additions par soustractions).

$$98 = \left\{ \begin{array}{l} 3 + 5 \times 19 \\ 5 + 3 \times 31 \\ 7 + 7 \times 13 \\ 11 + 3 \times 29 \\ 13 + 5 \times 17 \\ 17 + 3 \times 27 \\ 21 + 7 \times 11 \\ 23 + 3 \times 25 \\ 23 + 5 \times 15 \\ 29 + 3 \times 23 \\ 33 + 5 \times 13 \\ 35 + 3 \times 21 \\ 35 + 7 \times 9 \\ 41 + 3 \times 19 \\ 43 + 5 \times 11 \\ 47 + 3 \times 17 \end{array} \right. \quad \left| \quad 0 = \left\{ \begin{array}{l} 3 - 3 \times 1 \\ 5 - 5 \times 1 \\ 7 + 7 \times 1 \\ 9 - 3 \times 3 \\ 15 - 3 \times 5 \\ 15 - 5 \times 3 \\ 21 - 3 \times 7 \\ 21 - 7 \times 3 \\ 25 - 5 \times 5 \\ 27 - 3 \times 9 \\ 33 - 3 \times 11 \\ 35 - 5 \times 7 \\ 35 - 5 \times 7 \\ 39 - 3 \times 13 \\ 39 - 3 \times 13 \\ 45 - 3 \times 15 \\ 45 - 5 \times 9 \end{array} \right. \right.$$

Dans la mesure où on ne sait pas quels sont les triplets solutions des équations $a - bc = 0$ ou $a + bc = n$ (a et b appartenant à des intervalles contraints convenablement), on n'est pas capable de compter les redondances, ce qui permettrait éventuellement d'être assurée qu'un nombre au moins ne peut atteindre ni 0 ni n. C'est une autre raison, plus structurelle, qui doit garantir l'existence.

Puisque pour $a = 19$, $a = 31$ ou $a = 37$, aucun couple (b, c) n'est solution des équations $a + bc = 98$ ou $a - bc = 0$ (avec $c \neq -1$), 19, 31 ou 37 sont des décomposants de Goldbach de 98.

Rappel des étapes détaillées de la preuve de Morley algébrique par Alain Connes

DVC, octobre 2024.

Théorème : *Les 2 conditions* :

1) $f^3g^3h^3 = 1$.

2) $j^3 = 1$ et $\alpha + j\beta + j^2\gamma = 0$ avec $\text{fix}(fg) = \alpha$ et $\text{fix}(gh) = \beta$ et $\text{fix}(hf) = \gamma$.

sont équivalentes.

La démonstration du théorème de Morley sera un corollaire de la démonstration du théorème ci-dessus, qui se tient dans le groupe affine d'un corps K. On travaille en fait dans G le groupe affine de la droite, qu'on représente par des matrices 2×2 de la forme $M = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$. Les points de l'espace affine sont des vecteurs colonne de la forme $\begin{pmatrix} x \\ 1 \end{pmatrix}$.

Rappel : on peut composer deux applications affines en multipliant leur matrice associée. Par exemple, correspondant à :

$$3 \overset{3x+2}{\longmapsto} 11 \overset{5x+1}{\longmapsto} 56$$

on a :

$$\begin{pmatrix} 5 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 15 & 11 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 56 \\ 1 \end{pmatrix}$$

Attention : il ne faut pas se tromper de sens pour la composition :

$$\begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 5 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 15 & 5 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 50 \\ 1 \end{pmatrix}$$

Pour rappel, le point fixe d'une application affine g définie par $g(x) = ax + b$ est le point $x \in K$ avec $ax + b = x$, qu'on note $\text{fix}(g) = \dfrac{b}{1-a}$.

On définit le morphisme δ du groupe affine de la droite vers le groupe multiplicatif $(K^*, \times)$ des éléments non nuls de K. δ associe à une application affine son coefficient multiplicateur $a \in K^*$. Le noyau $\text{Ker}(\delta)$, i.e. l'ensemble des éléments qui sont envoyés sur l'unité de K^*, est le sous-groupe de G des translations, qui est aussi le groupe additif $(K, +)$, c'est-à-dire l'ensemble des transformations telles que $a = 1$.

Démonstration du théorème :

1) $\implies$ 2).

Notons que par hypothèse, on aura $j \neq 1$ ainsi que $ak - j \neq 0$ (les produits de 2 applications ne sont pas des translations).

$$
\begin{aligned}
f &= \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix} \\
f^3 &= \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix}^3 \\
&= \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_1^2 & a_1 b_1 + b_1 \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} a_1^3 & a_1^2 b_1 + a_1 b_1 + b_1 \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} a_1^3 & b_1(1 + a_1 + a_1^2) \\ 0 & 1 \end{pmatrix} \\
f^3 g^3 h^3 &= \begin{pmatrix} a_1^3 & b_1(1 + a_1 + a_1^2) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_2^3 & b_2(1 + a_2 + a_2^2) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_3^3 & b_3(1 + a_3 + a_3^2) \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} a_1^3 a_2^3 & a_1^3 b_2(1 + a_2 + a_2^3) + b_1(1 + a_1 + a_1^2) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_3^3 & b_3(1 + a_3 + a_3^2) \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} a_1^3 a_2^3 a_3^3 & a_1^3 a_2^3 b_3(1 + a_3 + a_3^2) + a_1^3 b_2(1 + a_2 + a_2^2) + b_1(1 + a_1 + a_1^2) \\ 0 & 1 \end{pmatrix}
\end{aligned}
$$

On réécrit la condition $f^3 g^3 h^3 = 1$ en

$$
\begin{pmatrix} a_1^3 a_2^3 a_3^3 & a_1^3 a_2^3 b_3(1 + a_3 + a_3^2) + a_1^3 b_2(1 + a_2 + a_2^2) + b_1(1 + a_1 + a_1^2) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}
$$

condition qui devient

$$
\begin{cases} a_1^3 a_2^3 a_3^3 = 1 \text{ et} \\ \\ b = a_1^3 a_2^3 b_3 + a_1^3 a_2^3 b_3 a_3 + a_1^3 a_2^3 b_3 a_3^3 + a_1^3 b_2 + a_1^3 b_2 a_2 + a_1^3 b_2 a_2^2 + b_1 + b_1 a_1 + b_1 a_1^2 \end{cases}
$$

Là, il est noté "*A straightforward computation, using $a_1 a_2 a_3 = j$ gives*".

En utilisant $j = a_1 a_2 a_3$, on obtient [1] :

$$
b = -j a_1^2 a_2 (a_1 - j)(a_2 - j)(a_3 - j)(\alpha + j\beta + j^2 \gamma)
$$

où $\alpha = \dfrac{a_1 b_2 + b_1}{1 - a_1 a_2}$, $\beta = \dfrac{a_2 b_3 + b_2}{1 - a_2 a_3}$ et $\gamma = \dfrac{a_3 b_1 + b_3}{1 - a_3 a_1}$, qui sont les points fixes des applications fg, gh et hf.

[1] et il reste à trouver le calcul évident.

Recherchons par exemple le point fixe de fg.

$$fg = \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 \\ 0 & 1 \end{pmatrix}$$

De cette égalité, on a :

$$fg(x) = x \iff \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} x \\ 1 \end{pmatrix} \iff \begin{pmatrix} a_1 a_2 x + (a_1 b_2 + b_1) \\ 1 \end{pmatrix} = \begin{pmatrix} x \\ 1 \end{pmatrix}$$

qui donne $x = \dfrac{a_1 b_2 + b_1}{1 - a_1 a_2}$.

Exercice subsidiaire :

Comment faire pour transformer le quadrilatère quelconque en un carré et le pentagone quelconque en un pentagone régulier ?

On imagine que pour le carré, il faut utiliser la relation

$$a + ib - c - id = 0$$

caractéristique de tout carré dont les sommets ont pour affixes a, b, c et d et le produit de puissances quatrièmes $m^4 n^4 o^4 p^4$.

Pour le pentagone, la relation à utiliser est

$$a + \exp\left(\frac{2i\pi}{5}\right) b + \exp\left(\frac{4i\pi}{5}\right) c + \exp\left(\frac{6i\pi}{5}\right) d + \exp\left(\frac{8i\pi}{5}\right) e$$

vérifiée par tout pentagone régulier *abcde*, les puissances cinquièmes et les expressions de la forme $1+x+x^2+x^3+x^4$.

Du distinct au flou, Denise Vella-Chemla, octobre 2024

Il s'agit de revenir à une ancienne idée qui consisterait à passer d'une décomposition de Goldbach non triviale d'un nombre pair double d'un nombre premier à une décomposition de Goldbach d'un nombre composé.

On utilise le programme python et ses résultats en annexe. Ce programme trouve pour chaque nombre pair les racines k-ièmes de 1 ou de -1, pour $k = \frac{n-2}{4}$.

On constate :

- qu'un nombre pair double d'un nombre premier p (comme 10, 14, 22, etc.) a $\varphi(n) = p - 1$ racines[1] $\frac{p-2}{4}$-ièmes de 1 ou -1 (i.e. il s'agit des nombres x compris entre 1 et $n-1$, tels que $x^{\frac{p-2}{4}} \equiv \pm 1 \pmod{2p}$) en tout ; p ne fait pas partie de ces racines, car sa puissance $\frac{p-2}{4}$ est congrue à lui même ; *exemple* : $22 = 2 \times 11$ a 10 racines 5-ièmes de 1 ou de -1, qui sont tous les nombres impairs de 1 à 21 sauf 11 ;

- comme pour les résidus quadratiques, les nombres pairs doubles de nombres premiers sont de deux sortes : ceux pour lesquels les racines de 1 ou de -1 "tombent en face", ce sont les doubles de nombres premiers de la forme $4k+1$ comme 26, pour lequel les couples $(1, 25), (3, 23), (9, 17)$ contiennent deux racines 6-ièmes de 1 tandis que les couples $(5, 21), (7, 19), (11, 15)$ contiennent deux racines de -1 ; le contraire se produit pour les nombres pairs doubles de nombres premiers qui sont de la forme $4k + 3$: les racines sont en quinconce : par exemple pour 14, nombre pair double de 7 de la forme $4k + 3$, 1 est racine cubique de 1 quand 13 est racine cubique de -1, 3 est racine cubique de -1 quand 11 est racine cubique de 1, et il en est de même pour le couple (5,9) ;

- il faudrait être capable (et on ne l'est même pas) de démontrer que l'un de ces couples au moins contient deux nombres premiers différents : on appellera ce couple de nombres premiers la décomposition de Goldbach non triviale d'un double de nombre premier, par opposition à sa décomposition triviale qui est $2p = p + p$;

- pour les doubles de nombres premiers de la forme $4k+1$, il semblerait qu'on trouve toujours un produit de deux nombres complémentaires à n (deux sommants d'une décomposition additive de n) égal à 1 (ou -1) ; malheureusement, ce produit ne fournit pas toujours deux nombres premiers (par exemple, $17 \times 41 \equiv 1 \pmod{58}$ avec 17 et 41 premiers tous les deux, tandis que $9 \times 73 \equiv 1 \pmod{82}$ avec 9 composé ;

- pour les nombres pairs n doubles de nombres composés, les racines $\frac{p-2}{4}$-ièmes de 1 ou -1 sont au nombre de $\varphi(n)$ lorsque n est un $4p$ avec p premier ; la seule racine de -1 est $n-1$ lorsqu'il n'y a que deux racines. Le nombre de racines divise $\varphi(n)$, c'est un résultat connu.

[1] un nombre pair

Annexe 1 : texte python du programme

```
def prime(atester):
     k = 2
     if atester in [0, 1]:  return False
     if atester in [2, 3, 5, 7]:  return True
     while True:
          if k * k > atester:  return True
          else:
               if atester % k == 0:  return False
               else:  k = k + 1

for n in range(10,103,2):
     if not prime(n/2):
          print(n,':::')
          k = (n-2)//4
          for x in range(1,n+1,2):
               if (x**k)%n == 1:
                    print(x,'racine ',k,'-ieme de 1')
               else:
                    if (x**k)%n == n-1:
                         print(x, 'racine ',k,'-ieme de -1 ')
```

Annexe 2 : résultat du programme en annexe 1

Pour les nombres pairs doubles de nombres premiers :

```
10 :::
1 racine 2 -ieme de 1
3 racine 2 -ieme de -1
7 racine 2 -ieme de -1
9 racine 2 -ieme de 1
11 racine 2 -ieme de 1

14 :::
1 racine 3 -ieme de 1
3 racine 3 -ieme de -1
5 racine 3 -ieme de -1
9 racine 3 -ieme de 1
11 racine 3 -ieme de 1
13 racine 3 -ieme de -1
15 racine 3 -ieme de 1
```

```
22 :::
1 racine 5 -ieme de 1
3 racine 5 -ieme de 1
5 racine 5 -ieme de 1
7 racine 5 -ieme de -1
9 racine 5 -ieme de 1
13 racine 5 -ieme de -1
15 racine 5 -ieme de 1
17 racine 5 -ieme de -1
19 racine 5 -ieme de -1
21 racine 5 -ieme de -1
23 racine 5 -ieme de 1

26 :::
1 racine 6 -ieme de 1
3 racine 6 -ieme de 1
5 racine 6 -ieme de -1
7 racine 6 -ieme de -1
9 racine 6 -ieme de 1
11 racine 6 -ieme de -1
15 racine 6 -ieme de -1
17 racine 6 -ieme de 1
19 racine 6 -ieme de -1
21 racine 6 -ieme de -1
23 racine 6 -ieme de 1
25 racine 6 -ieme de 1
27 racine 6 -ieme de 1

34 :::
1 racine 8 -ieme de 1
3 racine 8 -ieme de -1
5 racine 8 -ieme de -1
7 racine 8 -ieme de -1
9 racine 8 -ieme de 1
11 racine 8 -ieme de -1
13 racine 8 -ieme de 1
15 racine 8 -ieme de 1
19 racine 8 -ieme de 1
21 racine 8 -ieme de 1
23 racine 8 -ieme de -1
25 racine 8 -ieme de 1
27 racine 8 -ieme de -1
29 racine 8 -ieme de -1
31 racine 8 -ieme de -1
33 racine 8 -ieme de 1
35 racine 8 -ieme de 1
```

```
38 :::
1 racine 9 -ieme de 1
3 racine 9 -ieme de -1
5 racine 9 -ieme de 1
7 racine 9 -ieme de 1
9 racine 9 -ieme de 1
11 racine 9 -ieme de 1
13 racine 9 -ieme de -1
15 racine 9 -ieme de -1
17 racine 9 -ieme de 1
21 racine 9 -ieme de -1
23 racine 9 -ieme de 1
25 racine 9 -ieme de 1
27 racine 9 -ieme de -1
29 racine 9 -ieme de -1
31 racine 9 -ieme de -1
33 racine 9 -ieme de -1
35 racine 9 -ieme de 1
37 racine 9 -ieme de -1
39 racine 9 -ieme de 1

46 :::
1 racine 11 -ieme de 1
3 racine 11 -ieme de 1
5 racine 11 -ieme de -1
7 racine 11 -ieme de -1
9 racine 11 -ieme de 1
11 racine 11 -ieme de -1
13 racine 11 -ieme de 1
15 racine 11 -ieme de -1
17 racine 11 -ieme de -1
19 racine 11 -ieme de -1
21 racine 11 -ieme de -1
25 racine 11 -ieme de 1
27 racine 11 -ieme de 1
29 racine 11 -ieme de 1
31 racine 11 -ieme de 1
33 racine 11 -ieme de -1
35 racine 11 -ieme de 1
37 racine 11 -ieme de -1
39 racine 11 -ieme de 1
41 racine 11 -ieme de 1
43 racine 11 -ieme de -1
45 racine 11 -ieme de -1
47 racine 11 -ieme de 1
```

```
58 :::
1 racine 14 -ieme de 1
3 racine 14 -ieme de -1
5 racine 14 -ieme de 1
7 racine 14 -ieme de 1
9 racine 14 -ieme de 1
11 racine 14 -ieme de -1
13 racine 14 -ieme de 1
15 racine 14 -ieme de -1
17 racine 14 -ieme de -1
19 racine 14 -ieme de -1
21 racine 14 -ieme de -1
23 racine 14 -ieme de 1
25 racine 14 -ieme de 1
27 racine 14 -ieme de -1
31 racine 14 -ieme de -1
33 racine 14 -ieme de 1
35 racine 14 -ieme de 1
37 racine 14 -ieme de -1
39 racine 14 -ieme de -1
41 racine 14 -ieme de -1
43 racine 14 -ieme de -1
45 racine 14 -ieme de 1
47 racine 14 -ieme de -1
49 racine 14 -ieme de 1
51 racine 14 -ieme de 1
53 racine 14 -ieme de 1
55 racine 14 -ieme de -1
57 racine 14 -ieme de 1
59 racine 14 -ieme de 1

62 :::
1 racine 15 -ieme de 1
3 racine 15 -ieme de -1
5 racine 15 -ieme de 1
7 racine 15 -ieme de 1
9 racine 15 -ieme de 1
11 racine 15 -ieme de -1
13 racine 15 -ieme de -1
15 racine 15 -ieme de -1
17 racine 15 -ieme de -1
19 racine 15 -ieme de 1
21 racine 15 -ieme de -1
23 racine 15 -ieme de -1
25 racine 15 -ieme de 1
27 racine 15 -ieme de -1
29 racine 15 -ieme de -1
33 racine 15 -ieme de 1
35 racine 15 -ieme de 1
37 racine 15 -ieme de -1
39 racine 15 -ieme de 1
41 racine 15 -ieme de 1
```

```
43 racine 15 -ieme de -1
45 racine 15 -ieme de 1
47 racine 15 -ieme de 1
49 racine 15 -ieme de 1
51 racine 15 -ieme de 1
53 racine 15 -ieme de -1
55 racine 15 -ieme de -1
57 racine 15 -ieme de -1
59 racine 15 -ieme de 1
61 racine 15 -ieme de -1
63 racine 15 -ieme de 1

74 :::
1 racine 18 -ieme de 1
3 racine 18 -ieme de 1
5 racine 18 -ieme de -1
7 racine 18 -ieme de 1
9 racine 18 -ieme de 1
11 racine 18 -ieme de 1
13 racine 18 -ieme de -1
15 racine 18 -ieme de -1
17 racine 18 -ieme de -1
19 racine 18 -ieme de -1
21 racine 18 -ieme de 1
23 racine 18 -ieme de -1
25 racine 18 -ieme de 1
27 racine 18 -ieme de 1
29 racine 18 -ieme de -1
31 racine 18 -ieme de -1
33 racine 18 -ieme de 1
35 racine 18 -ieme de -1
39 racine 18 -ieme de -1
41 racine 18 -ieme de 1
43 racine 18 -ieme de -1
45 racine 18 -ieme de -1
47 racine 18 -ieme de 1
49 racine 18 -ieme de 1
51 racine 18 -ieme de -1
53 racine 18 -ieme de 1
55 racine 18 -ieme de -1
57 racine 18 -ieme de -1
59 racine 18 -ieme de -1
61 racine 18 -ieme de -1
63 racine 18 -ieme de 1
65 racine 18 -ieme de 1
67 racine 18 -ieme de 1
69 racine 18 -ieme de -1
71 racine 18 -ieme de 1
73 racine 18 -ieme de 1
75 racine 18 -ieme de 1
```

```
82 :::
1 racine 20 -ieme de 1
3 racine 20 -ieme de -1
5 racine 20 -ieme de 1
7 racine 20 -ieme de -1
9 racine 20 -ieme de 1
11 racine 20 -ieme de -1
13 racine 20 -ieme de -1
15 racine 20 -ieme de -1
17 racine 20 -ieme de -1
19 racine 20 -ieme de -1
21 racine 20 -ieme de 1
23 racine 20 -ieme de 1
25 racine 20 -ieme de 1
27 racine 20 -ieme de -1
29 racine 20 -ieme de -1
31 racine 20 -ieme de 1
33 racine 20 -ieme de 1
35 racine 20 -ieme de -1
37 racine 20 -ieme de 1
39 racine 20 -ieme de 1
43 racine 20 -ieme de 1
45 racine 20 -ieme de 1
47 racine 20 -ieme de -1
49 racine 20 -ieme de 1
51 racine 20 -ieme de 1
53 racine 20 -ieme de -1
55 racine 20 -ieme de -1
57 racine 20 -ieme de 1
59 racine 20 -ieme de 1
61 racine 20 -ieme de 1
63 racine 20 -ieme de -1
65 racine 20 -ieme de -1
67 racine 20 -ieme de -1
69 racine 20 -ieme de -1
71 racine 20 -ieme de -1
73 racine 20 -ieme de 1
75 racine 20 -ieme de -1
77 racine 20 -ieme de 1
79 racine 20 -ieme de -1
81 racine 20 -ieme de 1
83 racine 20 -ieme de 1

86 :::
1 racine 21 -ieme de 1
3 racine 21 -ieme de -1
5 racine 21 -ieme de -1
7 racine 21 -ieme de -1
9 racine 21 -ieme de 1
```

```
11 racine 21 -ieme de 1
13 racine 21 -ieme de 1
15 racine 21 -ieme de 1
17 racine 21 -ieme de 1
19 racine 21 -ieme de -1
21 racine 21 -ieme de 1
23 racine 21 -ieme de 1
25 racine 21 -ieme de 1
27 racine 21 -ieme de -1
29 racine 21 -ieme de -1
31 racine 21 -ieme de 1
33 racine 21 -ieme de -1
35 racine 21 -ieme de 1
37 racine 21 -ieme de -1
39 racine 21 -ieme de -1
41 racine 21 -ieme de 1
45 racine 21 -ieme de -1
47 racine 21 -ieme de 1
49 racine 21 -ieme de 1
51 racine 21 -ieme de -1
53 racine 21 -ieme de 1
55 racine 21 -ieme de -1
57 racine 21 -ieme de 1
59 racine 21 -ieme de 1
61 racine 21 -ieme de -1
63 racine 21 -ieme de -1
65 racine 21 -ieme de -1
67 racine 21 -ieme de 1
69 racine 21 -ieme de -1
71 racine 21 -ieme de -1
73 racine 21 -ieme de -1
75 racine 21 -ieme de -1
77 racine 21 -ieme de -1
79 racine 21 -ieme de 1
81 racine 21 -ieme de 1
83 racine 21 -ieme de 1
85 racine 21 -ieme de -1
87 racine 21 -ieme de 1

94 :::
1 racine 23 -ieme de 1
3 racine 23 -ieme de 1
5 racine 23 -ieme de -1
7 racine 23 -ieme de 1
9 racine 23 -ieme de 1
11 racine 23 -ieme de -1
13 racine 23 -ieme de -1
15 racine 23 -ieme de -1
17 racine 23 -ieme de 1
```

```
19 racine 23 -ieme de -1
21 racine 23 -ieme de 1
23 racine 23 -ieme de -1
25 racine 23 -ieme de 1
27 racine 23 -ieme de 1
29 racine 23 -ieme de -1
31 racine 23 -ieme de -1
33 racine 23 -ieme de -1
35 racine 23 -ieme de -1
37 racine 23 -ieme de 1
39 racine 23 -ieme de -1
41 racine 23 -ieme de -1
43 racine 23 -ieme de -1
45 racine 23 -ieme de -1
49 racine 23 -ieme de 1
51 racine 23 -ieme de 1
53 racine 23 -ieme de 1
55 racine 23 -ieme de 1
57 racine 23 -ieme de -1
59 racine 23 -ieme de 1
61 racine 23 -ieme de 1
63 racine 23 -ieme de 1
65 racine 23 -ieme de 1
67 racine 23 -ieme de -1
69 racine 23 -ieme de -1
71 racine 23 -ieme de 1
73 racine 23 -ieme de -1
75 racine 23 -ieme de 1
77 racine 23 -ieme de -1
79 racine 23 -ieme de 1
81 racine 23 -ieme de 1
83 racine 23 -ieme de 1
85 racine 23 -ieme de -1
87 racine 23 -ieme de -1
89 racine 23 -ieme de 1
91 racine 23 -ieme de -1
93 racine 23 -ieme de -1
95 racine 23 -ieme de 1
```

Pour les nombres pairs doubles de nombres composés :

```
12 :::
1 racine 2 -ieme de 1
5 racine 2 -ieme de 1
7 racine 2 -ieme de 1
11 racine 2 -ieme de 1

16 :::
1 racine 3 -ieme de 1
15 racine 3 -ieme de -1
```

```
18 :::
1 racine 4 -ieme de 1
17 racine 4 -ieme de 1

20 :::
1 racine 4 -ieme de 1
3 racine 4 -ieme de 1
7 racine 4 -ieme de 1
9 racine 4 -ieme de 1
11 racine 4 -ieme de 1
13 racine 4 -ieme de 1
17 racine 4 -ieme de 1
19 racine 4 -ieme de 1

24 :::
1 racine 5 -ieme de 1
23 racine 5 -ieme de -1

28 :::
1 racine 6 -ieme de 1
3 racine 6 -ieme de 1
5 racine 6 -ieme de 1
9 racine 6 -ieme de 1
11 racine 6 -ieme de 1
13 racine 6 -ieme de 1
15 racine 6 -ieme de 1
17 racine 6 -ieme de 1
19 racine 6 -ieme de 1
23 racine 6 -ieme de 1
25 racine 6 -ieme de 1
27 racine 6 -ieme de 1
30 :::
1 racine 7 -ieme de 1
29 racine 7 -ieme de -1

32 :::
1 racine 7 -ieme de 1
31 racine 7 -ieme de -1

36 :::
1 racine 8 -ieme de 1
17 racine 8 -ieme de 1
19 racine 8 -ieme de 1
35 racine 8 -ieme de 1

40 :::
1 racine 9 -ieme de 1
39 racine 9 -ieme de -1

42 :::
1 racine 10 -ieme de 1
13 racine 10 -ieme de 1
29 racine 10 -ieme de 1
41 racine 10 -ieme de 1
```

```
44 :::
1 racine 10 -ieme de 1
3 racine 10 -ieme de 1
5 racine 10 -ieme de 1
7 racine 10 -ieme de 1
9 racine 10 -ieme de 1
13 racine 10 -ieme de 1
15 racine 10 -ieme de 1
17 racine 10 -ieme de 1
19 racine 10 -ieme de 1
21 racine 10 -ieme de 1
23 racine 10 -ieme de 1
25 racine 10 -ieme de 1
27 racine 10 -ieme de 1
29 racine 10 -ieme de 1
31 racine 10 -ieme de 1
35 racine 10 -ieme de 1
37 racine 10 -ieme de 1
39 racine 10 -ieme de 1
41 racine 10 -ieme de 1
43 racine 10 -ieme de 1

48 :::
1 racine 11 -ieme de 1
47 racine 11 -ieme de -1

50 :::
1 racine 12 -ieme de 1
7 racine 12 -ieme de 1
43 racine 12 -ieme de 1
49 racine 12 -ieme de 1
52 :::
1 racine 12 -ieme de 1
3 racine 12 -ieme de 1
5 racine 12 -ieme de 1
7 racine 12 -ieme de 1
9 racine 12 -ieme de 1
11 racine 12 -ieme de 1
15 racine 12 -ieme de 1
17 racine 12 -ieme de 1
19 racine 12 -ieme de 1
21 racine 12 -ieme de 1
23 racine 12 -ieme de 1
25 racine 12 -ieme de 1
27 racine 12 -ieme de 1
29 racine 12 -ieme de 1
31 racine 12 -ieme de 1
33 racine 12 -ieme de 1
35 racine 12 -ieme de 1
37 racine 12 -ieme de 1
41 racine 12 -ieme de 1
43 racine 12 -ieme de 1
45 racine 12 -ieme de 1
47 racine 12 -ieme de 1
49 racine 12 -ieme de 1
51 racine 12 -ieme de 1
```

```
54 :::
1 racine 13 -ieme de 1
53 racine 13 -ieme de -1

56 :::
1 racine 13 -ieme de 1
55 racine 13 -ieme de -1

60 :::
1 racine 14 -ieme de 1
11 racine 14 -ieme de 1
19 racine 14 -ieme de 1
29 racine 14 -ieme de 1
31 racine 14 -ieme de 1
41 racine 14 -ieme de 1
49 racine 14 -ieme de 1
59 racine 14 -ieme de 1

64 :::
1 racine 15 -ieme de 1
63 racine 15 -ieme de -1

66 :::
1 racine 16 -ieme de 1
23 racine 16 -ieme de 1
43 racine 16 -ieme de 1
65 racine 16 -ieme de 1

68 :::
1 racine 16 -ieme de 1
3 racine 16 -ieme de 1
5 racine 16 -ieme de 1
7 racine 16 -ieme de 1
9 racine 16 -ieme de 1
11 racine 16 -ieme de 1
13 racine 16 -ieme de 1
15 racine 16 -ieme de 1
19 racine 16 -ieme de 1
21 racine 16 -ieme de 1
23 racine 16 -ieme de 1
25 racine 16 -ieme de 1
27 racine 16 -ieme de 1
29 racine 16 -ieme de 1
31 racine 16 -ieme de 1
33 racine 16 -ieme de 1
35 racine 16 -ieme de 1
37 racine 16 -ieme de 1
39 racine 16 -ieme de 1
41 racine 16 -ieme de 1
43 racine 16 -ieme de 1
45 racine 16 -ieme de 1
47 racine 16 -ieme de 1
49 racine 16 -ieme de 1
53 racine 16 -ieme de 1
55 racine 16 -ieme de 1
```

```
57 racine 16 -ieme de 1
59 racine 16 -ieme de 1
61 racine 16 -ieme de 1
63 racine 16 -ieme de 1
65 racine 16 -ieme de 1
67 racine 16 -ieme de 1
70 :::
1 racine 17 -ieme de 1
69 racine 17 -ieme de -1

72 :::
1 racine 17 -ieme de 1
71 racine 17 -ieme de -1

76 :::
1 racine 18 -ieme de 1
3 racine 18 -ieme de 1
5 racine 18 -ieme de 1
7 racine 18 -ieme de 1
9 racine 18 -ieme de 1
11 racine 18 -ieme de 1
13 racine 18 -ieme de 1
15 racine 18 -ieme de 1
17 racine 18 -ieme de 1
21 racine 18 -ieme de 1
23 racine 18 -ieme de 1
25 racine 18 -ieme de 1
27 racine 18 -ieme de 1
29 racine 18 -ieme de 1
31 racine 18 -ieme de 1
33 racine 18 -ieme de 1
35 racine 18 -ieme de 1
37 racine 18 -ieme de 1
39 racine 18 -ieme de 1
41 racine 18 -ieme de 1
43 racine 18 -ieme de 1
45 racine 18 -ieme de 1
47 racine 18 -ieme de 1
49 racine 18 -ieme de 1
51 racine 18 -ieme de 1
53 racine 18 -ieme de 1
55 racine 18 -ieme de 1
59 racine 18 -ieme de 1
61 racine 18 -ieme de 1
63 racine 18 -ieme de 1
65 racine 18 -ieme de 1
67 racine 18 -ieme de 1
69 racine 18 -ieme de 1
71 racine 18 -ieme de 1
73 racine 18 -ieme de 1
75 racine 18 -ieme de 1

78 :::
1 racine 19 -ieme de 1
77 racine 19 -ieme de -1
```

```
80 :::
1 racine 19 -ieme de 1
79 racine 19 -ieme de -1
84 :::
1 racine 20 -ieme de 1
13 racine 20 -ieme de 1
29 racine 20 -ieme de 1
41 racine 20 -ieme de 1
43 racine 20 -ieme de 1
55 racine 20 -ieme de 1
71 racine 20 -ieme de 1
83 racine 20 -ieme de 1

88 :::
1 racine 21 -ieme de 1
87 racine 21 -ieme de -1

90 :::
1 racine 22 -ieme de 1
19 racine 22 -ieme de 1
71 racine 22 -ieme de 1
89 racine 22 -ieme de 1

92 :::
1 racine 22 -ieme de 1
3 racine 22 -ieme de 1
5 racine 22 -ieme de 1
7 racine 22 -ieme de 1
9 racine 22 -ieme de 1
11 racine 22 -ieme de 1
13 racine 22 -ieme de 1
15 racine 22 -ieme de 1
17 racine 22 -ieme de 1
19 racine 22 -ieme de 1
21 racine 22 -ieme de 1
25 racine 22 -ieme de 1
27 racine 22 -ieme de 1
29 racine 22 -ieme de 1
31 racine 22 -ieme de 1
33 racine 22 -ieme de 1
35 racine 22 -ieme de 1
37 racine 22 -ieme de 1
39 racine 22 -ieme de 1
41 racine 22 -ieme de 1
43 racine 22 -ieme de 1
45 racine 22 -ieme de 1
47 racine 22 -ieme de 1
49 racine 22 -ieme de 1
51 racine 22 -ieme de 1
53 racine 22 -ieme de 1
55 racine 22 -ieme de 1
```

```
57 racine 22 -ieme de 1
59 racine 22 -ieme de 1
61 racine 22 -ieme de 1
63 racine 22 -ieme de 1
65 racine 22 -ieme de 1
67 racine 22 -ieme de 1
71 racine 22 -ieme de 1
73 racine 22 -ieme de 1
75 racine 22 -ieme de 1
77 racine 22 -ieme de 1
79 racine 22 -ieme de 1
81 racine 22 -ieme de 1
83 racine 22 -ieme de 1
85 racine 22 -ieme de 1
87 racine 22 -ieme de 1
89 racine 22 -ieme de 1
91 racine 22 -ieme de 1

96 :::
1 racine 23 -ieme de 1
95 racine 23 -ieme de -1

98 :::
1 racine 24 -ieme de 1
19 racine 24 -ieme de 1
31 racine 24 -ieme de 1
67 racine 24 -ieme de 1
79 racine 24 -ieme de 1
97 racine 24 -ieme de 1

100 :::
1 racine 24 -ieme de 1
7 racine 24 -ieme de 1
43 racine 24 -ieme de 1
49 racine 24 -ieme de 1
51 racine 24 -ieme de 1
57 racine 24 -ieme de 1
93 racine 24 -ieme de 1
99 racine 24 -ieme de 1

102 :::
1 racine 25 -ieme de 1
101 racine 25 -ieme de -1
```

Nouvelle démonstration du théorème selon lequel toute fonction algébrique rationnelle entière d'une seule variable peut être décomposée en facteurs réels du premier et du second degré.

**Que Carl Friedrich Gauss a présentée,
Afin d'obtenir les plus grands honneurs en philosophie,
à la célèbre faculté des philosophes
De l'Académie Julia Carolina.**

À C.G. Fleckheiser, Helmstedt, 1799.

1.

Toute équation algébrique déterminée peut être réduite sous la forme

$$x^m + Ax^{m-1} + Bx^{m-2} + ... + M = 0,$$

où m est un nombre entier positif. Si nous désignons par X le premier membre de cette équation et si nous supposons que l'équation $X = 0$ est satisfaite par plusieurs valeurs différentes de x, par exemple en posant $x = \alpha, x = \beta, x = \gamma$, etc., alors la fonction X sera divisible par le produit des facteurs $x - \alpha$, $x - \beta$, $x - \gamma$, etc. Inversement, lorsque le produit de plusieurs facteurs simples $x-\alpha, x-\beta, x-\gamma$, etc. est un diviseur de la fonction X, alors l'équation $X = 0$ sera satisfaite si ce x est posé égal à chacune des quantités α, β, γ, etc. Enfin, lorsque X est égal au produit de m facteurs simples de ce type (qui peuvent tous être différents, ou dont certains peuvent être identiques), alors d'autres facteurs simples en plus de ceux-ci ne peuvent diviser la fonction X. Pour cette raison, une équation de degré m ne peut pas avoir plus de m racines ; en même temps, il est bien clair qu'une équation de degré m peut avoir *moins* de m racines, même si X peut être décomposé en m facteurs simples : c'est-à-dire que si parmi ces facteurs certains sont identiques, alors le nombre de facteurs différents qui remplissent l'équation sera nécessairement plus petit que m. Pour des raisons de présentation, les mathématiciens préfèrent dire que dans ce cas aussi, l'équation a m racines, et qu'il peut avoir lieu que certaines d'entre elles s'avèrent égales.

2.

Ce qui a été exposé jusqu'ici est suffisamment prouvé dans les livres d'algèbre et ne contrevient en rien à la rigueur mathématique. Mais les analystes semblent avoir adopté trop vite et sans preuve préalable solide un théorème sur lequel repose presque toute la doctrine des équations : *qu'une telle fonction X peut toujours être décomposée en m facteurs simples ou, ce qui concorde parfaitement avec cela, que toute équation de degré m a effectivement m racines.* Mais comme on était parvenu assez souvent, avec les équations du second degré, à des cas qui ne sont pas conformes

à ce théorème, les algébristes ont été obligés d'inventer une quantité imaginaire dont le carré soit -1 ; et ils ont alors reconnu que si les quantités de la forme $a + b\sqrt{-1}$ sont admises de la même manière que les quantités réelles, le théorème est vrai non seulement pour les équations du second degré mais aussi pour les équations cubiques et biquadratiques.

Mais il n'était nullement permis d'en déduire qu'en admettant des quantités de la forme $a+b\sqrt{-1}$, des équations de cinquième degré ou plus peuvent être satisfaites ou, comme on l'exprime souvent (bien que je recommande une expression moins ambigue), que les racines de toute équation peuvent être réduites à la forme $a + b\sqrt{-1}$. Ce théorème ne diffère en rien de celui énoncé dans le titre de cet ouvrage, et c'est l'intention de cette thèse d'en donner une démonstration rigoureuse.

Lorsque les analystes découvrirent qu'il existait une infinité d'équations qui n'ont pas d'autres racines que des quantités de la forme $a + b\sqrt{-1}$, ils qualifièrent cette espèce particulière de quantités d'imaginaires, de façon à les distinguer des quantités réelles, ces quantités supposées ont été étudiées et ont été introduites dans toute l'analyse, je ne discuterai pas ici de la raison qui a motivé cette utilisation des quantités imaginaires en analyse. Je libérerai ma démonstration de tout secours de quantités imaginaires, même si j'aurais pu me prévaloir de cette liberté dont usent tous ceux qui s'occupent d'analyse.

3.

Bien que les démonstrations de notre théorème, données dans la plupart des manuels élémentaires, soient si peu fiables et si peu conformes à la rigueur mathématique qu'elles ne méritent guère d'être mentionnées, je les évoquerai néanmoins brièvement pour ne rien omettre.

Démontrer qu'une équation X quelconque a bien m racines, $x^m + Ax^{m-1} + Bx^{m-2} + etc. + M = 0$, ou $X = 0$, "Pour ils entreprennent de prouver que X peut être décomposé en m facteurs simples. À cet effet, ils supposent m facteurs simples $x - \alpha$, $x - \beta$, $x - \gamma$, etc., où α, β, γ, etc. sont encore inconnus, et posent leur produit égal à la fonction X. Ensuite, ils déduisent m équations de la comparaison des coefficients et affirment qu'à partir de celles-ci les quantités inconnues α, β, γ, etc. peuvent être déterminées, dans la mesure où leur nombre est également m. C'est-à-dire que $m-1$ inconnues peuvent être éliminées jusqu'à ce qu'apparaisse une équation qui, comme il semble approprié, ne contient qu'une seule inconnue."

Je ne parlerai pas de ce qu'on pourrait encore objecter à une telle augmentation. Je demande simplement comment nous pouvons être sûrs que cette dernière équation a une racine quelconque ? Ne serait-il pas possible que dans tout le domaine des nombres réels et imaginaires, il n'y ait aucune quantité qui satisfasse soit cette dernière équation, soit l'équation proposée ? De plus, les personnes expérimentées verront facilement que cette dernière équation doit nécessairement être entièrement identique à celle proposée, si seulement les calculs ont été effectués selon la règle. En d'autres termes, après avoir éliminé les quantités inconnues, α, β, γ, etc., une équation $\alpha^m + A\alpha^{m-1} + B\alpha^{m-2} + etc. + M = 0$ doit apparaître. En dire davantage sur un tel raisonnement n'est pas nécessaire.

Certains auteurs qui semblent avoir perçu la faiblesse de cette méthode posent pratiquement comme *un axiome* qu'une équation a effectivement des racines, sinon possibles, du moins impossibles. Ce

qu'ils veulent entendre par quantités possibles et impossibles, ne semble pas du tout être exposé suffisamment clairement. Si les quantités possibles doivent désigner la même chose que les quantités réelles, les quantités impossibles la même chose que les quantités imaginaires, alors cet axiome ne peut en aucun cas être admis, mais a nécessairement besoin d'une démonstration. Il ne semble pourtant pas que les expressions doivent être acceptées dans ce sens, mais que le sens de l'axiome semble plutôt être celui-ci : "Bien que nous ne soyons pas encore certains qu'il existe nécessairement m quantités réelles ou imaginaires qui satisfassent à une équation donnée de degré m, nous le supposerons encore pour le moment ; car si par hasard il arrivait qu'autant de quantités réelles ou imaginaires ne puissent être trouvées, alors certainement l'échappatoire resterait ouverte pour que nous puissions dire que les autres sont impossibles". Si quelqu'un préfère utiliser cette phrase plutôt que de simplement dire que dans ce cas, l'équation ne pourrait pas avoir autant de racines, alors je n'ai pas d'objections : mais s'il utilise ces racines impossibles comme si elles étaient factuelles, et par exemple, s'il dit que la somme de toutes les racines de l'équation $x^m + Ax^{m-1} + etc. = 0$ est $-A$ bien que parmi celles-ci il y ait des racines impossibles, ce qui signifie en fait bien que certaines soient absentes), alors je ne peux pas du tout l'approuver. Car les racines impossibles, admises dans un tel sens, sont encore des racines, et alors cet axiome ne peut en aucune façon être admis sans preuve ; et il ne serait pas non plus déplacé de se demander s'il n'existerait pas des équations qui n'auraient même pas de racines impossibles. [1]

4.

Avant de passer en revue les démonstrations de notre théorème données par d'autres mathématiciens, et d'exposer ce qui, à mon avis, doit être critiqué dans chacune d'elles, je fais observer qu'il suffit

[1] Par quantité imaginaire, j'entends toujours ici une quantité de la forme $a+b\sqrt{-1}$, avec $b \neq 0$. Cette expression a toujours été employée dans ce sens par tous les mathématiciens de premier ordre et je crois qu'il ne faut pas écouter ceux qui voudraient appeler la quantité $a + b\sqrt{-1}$ imaginaire seulement dans le cas où $a = 0$, et impossible lorsque $a \neq 0$; car cette distinction n'est ni nécessaire ni d'aucune utilité. Si l'on doit conserver les quantités imaginaires dans l'analyse (ce qui parait pour plusieurs raisons plus sage que de les supprimer, une fois qu'elles soient assez solidement étayées), il faut nécessairement les considérer comme tout aussi possibles que les quantités réelles ; c'est pourquoi je voudrais rassembler les quantités réelles et les quantités imaginaires sous la dénomination commune de quantités possibles : par contre, j'appellerais impossible une quantité qui aurait à remplir des conditions qui ne pourraient même pas être remplies en admettant les imaginaires. Mais de cette façon, la phrase signifierait exactement la même chose que si elle disait qu'une telle quantité n'appartient pas au domaine des grandeurs. Je ne puis cependant pas du tout admettre de là la formation d'une nouvelle espèce de quantités.
Si quelqu'un disait qu'un triangle rectangle équilatéral rectiligne est impossible, personne ne le contesterait. Mais s'il entendait considérer un triangle aussi impossible comme une nouvelle espèce de triangles et lui appliquer d'autres qualités de triangles, quelqu'un s'abstiendrait-il de rire ? Ce serait jouer avec les mots, ou plutôt en abuser
(Note : voir à ce propos la démonstration du théorème de Morley par John Conway, qui utilise des triangles "virtuels". D. V.-C.).
En effet, même des mathématiciens de premier ordre ont parfois appliqué des faits qui présupposent la possibilité des quantités qu'ils considèrent à des quantités dont la possibilité était jusqu'alors douteuse. Je ne nierai pas que les licences de ce genre ne portent le plus souvent que sur la forme des calculs, comme un voile que la perspicacité d'un vrai mathématicien saura bientôt percer. Néanmoins, il semble plus sage et plus digne de la sublime science, célébrée à juste titre comme le modèle le plus parfait de clarté et de fiabilité, soit d'interdire entièrement ces libertés, soit du moins d'en user avec plus de parcimonie, et de ne les utiliser que là où des personnes moins expérimentées peuvent se rendre compte que la question aurait pu être traitée sans le secours de ces libertés, peut- être moins brièvement, mais avec la même rigueur.
Je ne nie pas non plus que ce que j'ai dit ici contre l'usage abusif des quantités impossibles puisse, dans une certaine mesure, être également dit contre les quantités imaginaires. Mais je réserve la justification de ces dernières, et en fait une explication plus complète de toute cette question, pour une autre occasion.

de montrer seulement ceci : Toute équation de quelque degré que ce soit

$$x^m + Ax^{m-1} + Bx^{m-2} + etc. + M = 0,$$

ou $X = 0$ (où les coefficients A, B, etc. sont des nombres réels) sera satisfaite au moins une fois par une valeur de x de la forme $a + b\sqrt{-1}$. Car il est bien connu qu'alors X est divisible par un facteur réel $x^2 - 2ax + a^2 + b^2$, si b n'est pas 0, et par un facteur réel simple $x - a$ si $b = 0$. Dans l'un et l'autre cas, le quotient sera réel, et d'un degré inférieur à celui de X. Et comme, par le même raisonnement, ce quotient doit avoir un facteur réel du premier ou du second degré, il est clair qu'en continuant ce procédé, la fonction X se résoudra enfin en facteurs réels simples ou doubles ou en m facteurs simples si l'on préfère employer à la place des facteurs individuels doubles, deux facteurs simples imaginaires conjugués.

5.

La première démonstration du théorème est due au célèbre mathématicien d'Alembert, dans *Recherches sur le calcul intégral, Histoire de l'Acad. de Berlin*, année 1746, p. 182 et suivantes. La même démonstration est exposée dans Bougainville, *Traité du calcul intégral*, à Paris année 1754, p. 47 et suivantes. Les principaux points de sa méthode sont les suivants :

Il démontre d'abord : Quelle que soit la fonction X d'une variable x qui puisse être nulle soit pour $x = 0$ soit pour $x = \infty$, et qui puisse obtenir une valeur réelle positive infiniment petite lorsque x est affectée d'une valeur réelle, cette fonction peut aussi obtenir une valeur négative infiniment petite pour une valeur de x qui est soit un nombre réel, soit de la forme imaginaire $p + q\sqrt{-1}$. Car désignons par Ω une valeur infiniment petite de X, et ω la valeur correspondante de x. Il affirme ensuite que peut être exprimé par une série à convergence rapide $a\Omega^\alpha + b\Omega^\beta + c\Omega^\gamma$ etc., où les exposants, α, β, γ, etc. sont des nombres rationnels continument croissants qui seront positifs au moins à une certaine distance du début de la série, et qui rendront les termes dans lesquels ils apparaissent infiniment petits. Si parmi tous ces exposants il n'en apparaît aucun qui soit une fraction de dénominateur pair, alors tous les termes de la série seront des nombres réels pour les valeurs positives aussi bien que négatives de Ω. Mais si parmi ces exposants se trouvent des fractions de dénominateur pair, les termes correspondants, pour des valeurs négatives de Ω seront de la forme $p + q\sqrt{-1}$. Comme la série converge rapidement, il suffit dans le premier cas de ne considérer que le premier terme (c'est-à-dire le plus grand) ; dans le second cas, il n'est pas nécessaire d'aller au-delà du terme qui produit le premier une partie imaginaire.

Par un raisonnement similaire, on peut montrer que si X peut obtenir une valeur réelle négative infiniment petite pour une valeur réelle de x, alors la fonction peut aussi obtenir une valeur réelle positive infiniment petite pour une valeur réelle de x ou pour un x imaginaire de la forme $p + q\sqrt{-1}$.

Il en conclut en second lieu qu'il existe également une valeur réelle finie de X dans le premier cas négative, dans le second cas positive, qui peut être produite par une valeur imaginaire de x de la forme $p + q\sqrt{-1}$.

Il s'ensuit que si X est une telle fonction de x qu'elle prend la valeur réelle V pour la valeur réelle v de x et obtient aussi une valeur réelle supérieure ou inférieure d'une quantité infiniment petite, pour

une valeur réelle de x, alors cette même fonction peut aussi prendre une valeur réelle supérieure ou inférieure à V (resp.) d'une quantité infiniment petite, et même d'une quantité finie, en attribuant à x une valeur de la forme $p + q\sqrt{-1}$.

Ceci peut être déduit de ce qui précède sans difficulté si $V + Y$ est substitué à X et $v + y$ à x.

Enfin d'Alembert affirme : si l'on suppose que X peut parcourir tout l'intervalle compris entre deux valeurs réelles R, S (c'est-à-dire être égal tantôt à R, tantôt à S et à toutes les valeurs réelles comprises entre celles-ci) en attribuant toujours à x des valeurs de la forme $p + q\sqrt{-1}$, alors la fonction X peut de plus être augmentée ou diminuée (précisément selon que $S > R$ ou $S < R$) de toute quantité réelle finie avec x toujours de la forme $p + q\sqrt{-1}$.

Car si l'on se donne une quantité réelle U (S étant supposé compris entre U et R) à laquelle X ne puisse être égal par une telle valeur de x, il existera nécessairement un maximum de X (c'est-à-dire lorsque $S > R$, ou un minimum lorsque $S < R$), par exemple T, qu'il acquerra pour une valeur $p + q\sqrt{-1}$ de x, de sorte qu'on ne pourrait assigner à x aucune valeur de forme semblable qui rapprocherait encore la fonction X de U, même du plus petit écart. Or, dans une équation entre X et x, substituons partout à x la valeur $p + q\sqrt{-1}$, et posons d'abord la partie réelle égale à zéro, puis la partie qui fait intervenir le facteur $\sqrt{-1}$, laquelle est alors omise. Des deux équations ainsi produites, on peut en obtenir deux autres par élimination, dans l'une desquelles p, q et X et des constantes, interviennent tandis que l'autre, exempte de p, ne fait intervenir que q, X et des constantes. Ainsi, lorsque X parcourt toutes les valeurs réelles de R à T pour des valeurs réelles de p, q, alors, d'après ce qui précède, X peut se rapprocher de plus en plus de la valeur de U lorsque de telles valeurs que $p = \alpha + \gamma\sqrt{-1}, q = \beta + \delta\sqrt{-1}$ sont assignées respectivement à p et q. De là, cependant, on peut poser que $x = \alpha - \delta + (\gamma + \beta)\sqrt{-1}$, c'est-à-dire qu'il est encore de la forme $p + q\sqrt{-1}$, contrairement à l'hypothèse.

Ainsi, lorsqu'on suppose que X désigne une fonction de la forme $X = x^m + Ax^{m-1} + Bx^{m-2}+$ etc. $+M$, on perçoit sans difficulté que l'on peut attribuer à x des valeurs réelles telles que X puisse parcourir tout l'intervalle compris entre deux valeurs réelles. On peut donc obtenir pour x une valeur de la forme $p + q\sqrt{-1}$ de telle sorte que X puisse être égal à 0. CQFD [2]

6.

Les objections à la preuve de d'Alembert peuvent généralement être exprimées ainsi :

1. d'Alembert n'exprime aucun doute sur *l'existence* de valeurs de x auxquelles correspondent des valeurs données de X, mais suppose leur existence et étudie seulement la *forme* de ces valeurs.

[2] Il convient de remarquer que d'Alembert a appliqué des considérations géométriques dans l'exposition de sa démonstration et a considéré X comme l'abscisse et x comme l'ordonnée d'une courbe (selon l'usage de tous les mathématiciens de la première partie de ce siècle à qui la notion de fonctions était moins familière). Mais tout son raisonnement, si l'on considère seulement l'essentiel, repose non sur des principes géométriques mais sur des principes purement analytiques, et une courbe imaginaire et des ordonnées imaginaires sont des concepts assez difficiles et peuvent offenser un lecteur de notre temps. C'est pourquoi j'ai plutôt donné ici une forme de représentation purement analytique. J'ai ajouté cette note pour que celui qui comparerait la démonstration de d'Alembert avec cette exposition concise puisse vérifier que ce qui est essentiel est respecté sans changement.

Bien que cette objection soit en elle-même tout à fait grave, elle ne conceme ici cependant que la forme de l'expression, qui peut être facilement corrigée de telle manière que l'objection soit complètement démolie.

2. L'affirmation que l'on peut toujours exprimer ω par une série du genre de celle qu'il pose, est certainement fausse si X peut aussi désigner n'importe quelle fonction transcendante (comme d'Alembert l'admet dans plusieurs passages). Cela est manifeste par exemple si l'on pose

$$X = e^{1/x} \text{ soit } x = 1/\ln x.$$

Si nous limitons la démonstration au cas où X est une fonction algébrique de x (ce qui suffit pour la présente tâche), la proposition est valable dans tous les cas.

Au delà, d'Alembert n'apporte rien pour la vérification de son hypothèse. Bougainville stipule que X est une fonction algébrique de x et renvoie à l'invention de la série des parallélogrammes de Newton pour le développement de la série.

3. Il utilise les quantités infiniment petites avec plus de liberté que ne le permet la rigueur mathématique ou que ne le concèdera, du moins, un analyste scrupuleux de nos jours (où ces quantités ont à juste titre mauvaise réputation). Il n'a pas non plus expliqué assez clairement la transition d'une valeur infiniment petite de Ω à une valeur finie. Il semble conclure sa proposition selon laquelle Ω peut aussi atteindre une valeur finie, non pas tellement de la possibilité pour Ω d'avoir une valeur infiniment petite, mais plutôt du fait que, pour de très petites valeurs de Ω et à cause de la forte convergence de la série, elle se rapproche d'autant plus de la vraie valeur de ω que l'on prend plus de termes de la série. Ou bien, que l'équation qui montre la relation entre ω et Ω ou entre x et X sera satisfaite de manière d'autant plus exacte que l'on prend un plus grand nombre de termes dans la somme pour ω.

Outre que toute cette argumentation paraît trop vague pour qu'on puisse en tirer une conclusion rigoureuse, j'observe qu'il y a néanmoins des séries qui, quelque soit la petitesse de la valeur attribuée à la quantité pour laquelle les puissances progressent, divergent néanmoins toujours, pourvu qu'on les continue assez loin, pour qu'on puisse arriver à des termes plus grands qu'une quantité donnée quelconque [3] . Cela se produit lorsque les coefficients de la série forment une progression hypergéométrique, il faut donc nécessairement démontrer que dans le cas présent une telle série hypergéométrique ne peut pas apparaître.

Au reste, il me paraît que d'Alembert n'a pas convenablement recouru aux séries infinies et que celles-ci ne sont nullement propres à établir ce théorème fondamental de la théorie des équations.

[3]Je remarque ici en passant que parmi ces séries il y en a beaucoup qui, à première vue, semblent converger fortement, par exemple pour la plupart celles dont l'illustre Euler se sert dans la dernière partie de l'*Institutiones calculi differentialis* (Berlin 1755) chapitre VI, pour approcher au plus près la somme d'autres séries, p. 441-474 (les autres séries, p. 475-478, sont effectivement convergentes) ; chose que personne n'a jusqu'ici observée, autant que je sache. Il est donc grandement désirable qu'on expose clairement et rigoureusement pourquoi ces séries qui convergent d'abord très vite, puis, peu à peu, de plus en plus lentement et enfin divergent de plus en plus, peuvent néanmoins fournir une somme très voisine de la somme cherchée si l'on ne prend pas trop de termes, et dans quelle mesure on peut être assuré d'avoir une somme aussi exacte que possible ?

4. De l'hypothèse que X peut prendre la valeur S mais ne peut pas prendre la valeur U , il ne s'ensuit pas qu'il y ait nécessairement entre S et U une valeur T que X puisse atteindre mais non dépasser. Il existe ici encore un autre cas : il pourrait arriver qu'il y ait entre S et U une limite dont X puisse se rapprocher autant qu'on le voudra, mais qu'elle n'atteigne jamais. Des arguments fournis par d'Alembert il résulte seulement que X peut dépasser d'une quantité finie toute valeur qu'elle atteindrait. Par exemple, lorsque X devient égale à S, elle peut encore être augmentée d'une quantité finie Ω, puis un nouvel incrément Ω' peut être ajouté, puis un autre ajout Ω'', etc. De sorte que, quel que soit le nombre d'incréments ayant déjà été cumulés, aucun ne peut être considéré comme le dernier, il peut toujours arriver un nouvel incrément.

Mais aussi grand que soit le *nombre* des incréments possibles, il n'est restreint par aucune limite : il peut néanmoins arriver que les incréments, $\Omega, \Omega', \Omega''$, etc. diminuent continuellement mais que la somme $S + \Omega + \Omega' + \Omega''$ n'atteigne jamais une limite quelconque et ce, quel que soit le nombre de termes considérés.

Bien que ce cas ne puisse se produire lorsque X désigne une fonction algébrique intégrale de x, sans preuve que ce cas ne puisse se produire, le développement doit être considéré comme incomplet. En fait, lorsque X est une fonction transcendante ou une "fonction algébrique" (fonction algébrique rationnelle), ce cas peut se produire, par exemple il se produit toujours lorsqu'à une valeur de X correspond une valeur infiniment grande de x. Le développement de d'Alembert ne peut donc, semble-t-il, être ramené à des principes indubitables sans de grandes digressions, et dans certains cas, même, il ne peut pas être rcorrigé du tout.

Pour ces raisons, je ne puis considérer la démonstration de d'Alembert comme satisfaisante. Malgré cela, il me semble que la substance véritable de la démonstration en question n'est nullement altérée par toutes ces objections. Et je crois que sur la même base (quoique d'une manière bien différente et au moins avec plus de circonspection), on peut construire une démonstration rigoureuse de notre théorème, et non seulement cela, mais on peut en tirer tout ce qu'on peut demander à une théorie des équations *transcendantes*.

Je traiterai peut-être plus longuement de cette question très importante à une autre occasion (se reporter à ce propos à ce qui précède le paragraphe 24.

7.

Après d'Alembert, l'illustre Euler publia ses recherches sur ce sujet, *Recherches sur les racines imaginaires des équations, Hist. de l'Acad. de Berlin*, Année 1749, p. 223 et suivantes. Euler en livra un double développement. Un résumé du premier suit ici.

Premièrement, Euler entreprend de démontrer que si m désigne une puissance de 2, alors la fonction $x^{2m} + Bx^{2m-2} + Cx^{2m-3}+$ etc.$+M = X$ (où le coefficient du second terme [en x^{2m-1}] est égal à 0) est toujours résolue en deux facteurs réels, dans lesquels x est élevé jusqu'à la puissance m. À

cette fin, il suppose deux facteurs

$$x^m - ux^{m-1} + \alpha x^{m-2} + \beta x^{m-3} + \text{etc. et}$$

$$x^m + ux^{m-1} + \lambda x^{m-2} + \mu x^{m-3} + \text{etc..}$$

où les coefficients $u, \alpha, \beta, \lambda, \mu$, etc., sont inconnus et il pose le produit de ces facteurs égal à la fonction X.

La comparaison des coefficients fournit alors $2m-1$ équations et il ne reste qu'à démontrer clairement que l'on peut attribuer des valeurs réelles aux inconnues (qui sont également en nombre $2m-1$) $u, \alpha, \beta,$ etc., λ, μ, etc., telles qu'elles satisfassent à ces équations. De plus, Euler affirme que si dans un premier temps u est considéré comme connu, de sorte que le nombre d'inconnues est égal à un de moins que le nombre d'équations, on peut, en combinant les méthodes algébriques connues, déterminer rationnellement et sans aucun extraction de racine : $\alpha, \beta,$ etc., λ, μ, etc., à partir de u et des coefficients B, C, etc., et il en résulte même des valeurs réelles si u est réel. En outre, tous les coefficients α, β, etc., λ, μ, etc. pourront être éliminés, de sorte qu'il en résulte une équation $U = 0$, où U sera une fonction entière de u seulement, et des coefficients connus. Résoudre cette dernière équation par la simple méthode d'élimination serait un travail énorme lorsque l'équation proposée $X = 0$ est de degré assez élevé ; et impossible pour un degré indéterminé (même référence à Euler, p. 239). Mais il suffit ici de connaître une propriété de cette équation, à savoir que le dernier terme de U (dans lequel u n'intervient pas) est nécessairement négatif, d'où il résulte bien que l'équation a au moins une racine réelle, donc que u et par conséquent aussi α, β, etc., λ, μ, etc. peuvent être déterminés comme des nombres réels d'au moins une manière. Cette propriété peut en effet être démontrée par les considérations suivantes : si l'on suppose que $x^m - ux^{m-1} + \alpha x^{m-2} +$ etc. est un facteur de la fonction X, alors u sera nécessairement la somme des m racines de l'équation $X = 0$ et il pourra avoir autant de valeurs que le nombre m peut être choisi de différentes manières parmi les $2m$ racines de $X = 0$ ou, d'après les principes du calcul combinatoire $\frac{2m.2m-1.2m-2.\ldots.m+1}{1.2.3.\ldots.m}$ valeurs. Ce nombre est toujours le double d'un nombre impair (j'omets la démonstration qui n'est pas difficile) ; si on pose ce nombre égal à $2k$, alors sa moitié k sera impaire. L'équation $U = 0$ sera en effet de degré $2k$. Mais comme dans l'équation $X = 0$ il n'y a pas de second terme, la somme de toutes les $2m$ racines sera nulle. Par conséquent, il est clair que si la somme des m racines est $+p$, alors la somme des racines restantes doit être $-p$, i.e. si p fait partie des valeurs de u, alors la valeur $-p$ en fera partie aussi. E. conclut donc que U est le produit de k facteurs doubles de la forme $u^2 - p^2, u^2 - q^2, u^2 - r^2$, etc., où $+p, -p, +q, -q$ etc. désignent toutes les $2k$ racines de l'équation $U = 0$. À cause du nombre impair de ces doubles facteurs, le dernier terme de U sera donc le carré du produit pqr etc., affecté du signe négatif. Mais ce produit pqr etc. peut toujours être calculé par des opérations rationnelles à partir des coefficients B, C, etc. et est donc nécessairement un nombre réel. Par conséquent, son carré précédé d'un signe négatif sera certainement une quantité négative. CQFD

Comme ces deux facteurs réels de X sont de degré m, et que m est une puissance de 2, chacun d'eux peut de la même manière être décomposé en deux facteurs réels de degré $\frac{1}{2}.m$. Comme par division répétée du nombre m par deux, on finit nécessairement par arriver à un terme du second degré, il est manifeste qu'en continuant l'opération, la fonction X finira par être décomposée en facteurs réels du second degré.

Mais si l'on propose que la fonction soit telle que son second terme ne manque pas, par exemple $x^{2m} + Ax^{2m-1} + Bx^{2m-2}+$ etc. $+M$, où $2m$ est toujours une puissance de 2, alors cette fonction sera transformée par la substitution $x = y - A/2m$ en une fonction semblable sans second terme. Il s'ensuit donc facilement qu'une telle fonction est aussi décomposable en facteurs réels du second degré.

Enfin, proposons une fonction de degré n où le nombre n n'est pas une puissance binaire. Nous pouvons alors poser la puissance binaire $2m$ supérieure à n la plus proche, et multiplier la fonction proposée par $2m - n$ facteurs réels simples quelconques. Il résulte sans difficulté de la résolvabilité du produit en facteurs réels du second degré, que la fonction proposée peut aussi être résolue en facteurs du premier ou du second degré.

8.

Contre cette preuve s'élèvent les objections suivantes :

1. La règle d'après laquelle E. conclut que $2m - 2$ inconnues, α, β, etc., λ, μ, etc. peuvent être calculées à partir de $2m - 1$ équations par des opérations rationnelles, n'est nullement vraie en général, mais souffre assez souvent une exception. Si quelqu'un considère par exemple dans l'article 3 une des inconnues comme connue et essaie ensuite d'exprimer les autres quantités inconnues à partir de celle-ci et des coefficients donnés au moyen d'opérations rationnelles, il découvrira vite que c'est impossible. Aucune des inconnues ne peut être déterminée autrement que par une équation de degré $m - 1$. ela doit nécessairement résulter de ce qui a été dit précédemment, comme on peut le voir ici immédiatement. Néanmoins, on pourrait très bien se demander si, dans le cas présent, pour certaines valeurs de m, la situation ne pourrait pas être telle que les inconnues, α, β, etc., λ, μ, etc., ne puissent être déterminées à partir de u, B, C, etc. autrement que par une équation d'un degré peut-être supérieur à $2m$? Pour le cas particulier où l'équation $X = 0$ est du quatrième degré, E. a calculé les valeurs rationnelles des coefficients à partir de u et des coefficients donnés. Il faudrait au moins une analyse plus approfondie pour savoir si cela peut effectivement être fait dans toutes les équations supérieures.

Il semble en outre utile d'étudier plus en profondeur et de manière plus générale les formules qui expriment,α, β, etc., λ, μ, rationnellement en fonction de u, B, C, etc. par des opérations rationnelles. J'ai l'intention de traiter plus en détail cette question et d'autres qui appartiennent à la théorie de l'élimination (cette question n'a pas été épuisée) à une autre occasion.

2. Même si l'on avait prouvé que l'on pouvait trouver des formules pour des équations de quelque degré que ce soit, avec lesquelles ces quantités, α, β, etc., λ, μ, etc. puissent être calculées à partir de u, B, C, etc. par des opérations rationnelles, cependant ces formules pourraient devenir *indéterminées* pour certaines valeurs bien définies des coefficients u, B, C, etc. De cette manière, non seulement il pourrait être impossible de calculer les quantités inconnues à partir de u, B, C. etc. par des opérations rationnelles, mais dans certains cas il pourrait en effet n'y avoir aucune valeur réelle de α, β, etc., λ, μ, etc. correspondant à une valeur réelle de u. Pour la confirmation de ceci, je renvoie le lecteur, par souci de concision, à la dissertation même de E., où à la page

236, l'équation du quatrième degré est longuement développée. Chacun verra immédiatement que les formules pour les coefficients α, β, etc.λ, μ, etc., deviennent indéterminées lorsque l'on suppose $C = 0$ et $u = 0$. Alors les valeurs de ces coefficients ne peuvent être obtenues sans extractions de racines, et ce ne sont même pas des nombres réels lorsque la quantité $B^2 - 4D$ est négative. Certes, dans ce cas, u a encore d'autres valeurs réelles auxquelles peuvent répondre des valeurs réelles de α, β, etc., λ, μ, etc., comme on le voit facilement. Il est cependant à craindre que pour des équations plus élevées la solution de cette difficulté (que E. n'aborde pas du tout) ne donne lieu à un travail beaucoup plus pénible. Cette question ne doit certainement pas être passée sous silence dans une démonstration rigoureuse.

3. E. suppose tacitement que l'équation $X = 0$ a $2m$ racines et que leur somme est nulle parce que X n'a pas de second terme. Ce que je pense de cette licence (que tous les auteurs utilisent pour cet argument), je l'ai exposé clairement dans l'article 3 ci-dessus. L'hypothèse que la somme de toutes les racines d'une équation est égale au premier coefficient, affecté d'un signe opposé, ne semble pas applicable aux autres équations, mais seulement à celles qui ont des racines. Mais comme par cette démonstration, il faut montrer que l'équation $X = 0$ a effectivement des racines, il ne semble pas du tout permis de supposer leur existence. Sans doute, ceux qui n'ont pas encore pénétré le caractère fallacieux de ce paralogisme répondront qu'il ne s'agit pas ici de prouver que *l'équation* $X = 0$ *peut être satisfaite* (car c'est le sens de l'expression "elle a des racines"), *mais simplement que l'équation peut être satisfaite par des valeurs de* x *de la forme* $a + b\sqrt{-1}$. *Ils admettent en effet la première affirmation comme un axiome.* Cependant, on ne peut concevoir d'autres formes pour les quantités autres que les nombres réels et imaginaires $a + b\sqrt{-1}$. Il n'apparaît donc pas avec suffisamment de clarté en quoi ce qu'il faut démontrer diffère de ce qui est supposé comme un axiome.

Si l'on pouvait imaginer encore d'autres formes de grandeurs, par exemple de la forme F, F', F'', etc., on ne serait pas obligé d'admettre sans preuve qu'une équation quelconque soit satisfaite par une valeur de x réelle ou de la forme $a + b\sqrt{-1}$ ou de la forme F, ou F', etc. C'est pourquoi cet axiome ne peut avoir d'autre sens que celui-ci : toute équation peut être satisfaite par une valeur réelle de l'inconnue, *ou* par une valeur imaginaire de la forme $a+b\sqrt{-1}$, *ou* peut-être par une valeur d'une forme jusqu'ici inconnue, *ou* par une valeur qui n'est contenue dans aucune forme quelconque. Mais comment les quantités de cette espère, dont on ne peut avoir aucune idée, véritable ombre d'une ombre, pourraient-elles être additionnées ou divisées ? Ceci n'est certainement pas compréhensible avec cette clarté qu'exige toujours la science [4].

Je ne veux cependant pas, par ces objections, rendre suspectes les conclusions que E. a tirées de son hypothèse. Je suis plutôt certain qu'elles peuvent être réalisées d'une manière qui n'est ni difficile ni très différente de celle d'Euler, de sorte qu'il ne subsistera pas le moindre scrupule.

Je retiens que cette forme de raisonnement peut être d'une grande utilisé autant qu'on voudra pour la *découverte* de nouveaux théorèmes, mais qu'elle paraît cependant moins apte pour une

[4]Tout cela sera expliqué en détail dans une autre étude, qui est déjà en cours d'impression et qui traite d'un sujet très différent, mais néanmoins analogue. Là, j'aurais pu me prévaloir d'une licence semblable, avec le même droit que se donnent tous les analystes dans la résolution des équations. Les démonstrations de plusieurs affirmations auraient pu être données en quelques mots à l'aide de telles fictions. Sans elles, elles se sont révélées très difficiles et ont exigé l'art le plus subtil. Mais j'ai préféré m'abstenir entièrement de ces fictions, et j'espère que cela me donnera plus de satisfaction que d'avoir suivi la méthode des analystes.

démonstration devant le public.

E. n'apporte rien du tout à la démonstration de l'assertion que le produit $pqr\ldots$ etc. peut être déterminé à partir des coefficients de X par des opérations rationnelles. Tout ce qu'il explique à ce sujet, pour l'équation du quatrième degré, est ceci (où a, b, c, d sont les racines de l'équation proposée $x^4 + Bx^2 + Cx + D = 0$) :

"On m'objectera sans doute que j'ai supposé ici que la quantité pqr était un nombre réel et que son carré $p^2q^2r^2$ était positif. Mais cela peut être douteux, puisque si les racines a, b, c pouvaient être des nombres imaginaires, il pourrait alors arriver que le carré de pqr, qui en est composé, devienne négatif. À cela je réponds que ce cas ne peut jamais arriver. Car si quelques-unes des racines a, b, c, d sont des nombres imaginaires, nous savons néanmoins qu'il faut avoir $a + b + c + d = 0$, $ab + ac + ad + bc + bd + cd = B$, $abc + abd + acd + bcd = -C$ (Euler a, par erreur, noté C au lieu de $-C$, c'est pourquoi il déclare plus tard également $pqr = C$, de manière incorrecte.), $abcd = D$, les quantités B, C, D étant des nombres réels. Mais comme $p = a + b, q = a + c, r = a + d$, leur produit $pqr = (a+b)(a+c)(a+d)$ est déterminable, comme nous l'avons vu, à partir des quantités B, C, D et sera par conséquent un nombre réel, tout comme on a effectivement que $pqr = -C$ et $p^2q^2r^2 = C^2$. On voit tout aussi bien que dans les équations supérieures les mêmes circonstances doivent se produire et qu'on ne peut pas me faire d'objections de ce côté-là."

La condition que le produit pqr puisse être déterminé de B, C, etc. par des opérations rationnelles, Euler ne l'a ajoutée nulle part, mais semble l'avoir eue à l'esprit depuis le début, car sans elle la démonstration ne pourrait avoir aucune force. Or, il est certainement vrai que dans les équations du quatrième degré, on développe le produit $(a + b)(a + c)(a + d)$, on obtient $a^2(a + b + c + d) + abc + abd + acd + bcd = -C$. Cependant il ne semble pas suffisamment clair comment ce produit peut être calculé à partir des coefficients, par des opérations rationnelles, dans toutes les équations de degré supérieur.

Le célèbre de Foncenex, qui le premier a remarqué cela (voir *Miscell. phil. Math. Soc. Taurin.* Tome I, p. 117.), soutient avec raison que le procédé perd toute force sans une démonstration rigoureuse de cette hypothèse. Il admet qu'une telle démonstration lui paraît tout à fait difficile et raconte la voie qu'il a essayée mais en vain [5]

Or cette question se règle sans difficulté par la méthode suivante (dont je ne puis ici que donner un résumé) : bien que dans les équations du quatrième degré il ne soit pas suffisamment clair que le produit $(a+b)(a+c)(a+d)$ soit déterminable par les coefficients B, C, D, on perçoit cependant facilement que ce produit est aussi égal à $(b + a)(b + c)(b + d)$, ainsi qu'à $(c + a)(c + b)(c + d)$, et enfin à $(d + a)(d + b)(d + c)$ [6].

Par conséquent, le produit pqr sera égal au quart de la somme $(a + b)(a + c)(a + d) + (b + a)(b + c)(b + d) + (c + a)(c + b)(c + d)$ qui, lorsqu'elle sera élaborée, sera une fonction intégrale rationnelle

[5] Dans cet exposé une erreur semble s'être glissée. À la p.118, 1.5, au lieu de la lettre p ("on choisissait seulement celles où intervient p etc.") il faut lire nécessairement "une même racine quelconque de l'équation proposée", ou quelque chose de semblable, car autrement cela n'aurait aucun sens.

[6] *Note du traducteur : car* $a + b + c + d = 0$.

des racines a, b, c, d de telle sorte que toutes les racines entrent dans le même rapport comme on peut le voir sans difficulté. De telles fonctions peut en effet toujours être exprimé par les coefficients de l'équation dont les racines sont a, b, c, d.

La même chose se produit aussi quand le produit pqr est ramené à cette forme : $\frac{1}{2}(a+b-c-d).\frac{1}{2}(a+c-b-d).\frac{1}{2}(a+d-b-c)$, et il est facile de voir d'avance que dans ce produit, une fois développé, a, b, c, d interviennent de la même manière. En même temps, les mathématiciens expérimentés en déduiront comment cette méthode peut être appliquée aux équations de degré supérieur. Je réserve pour une autre occasion l'exposition complète de cette démonstration, que je ne présente pas par souci de brièveté, ainsi qu'une étude plus complète sur des applications semblables aux fonctions de plusieurs variables.

Je remarque en outre qu'outre ces quatre objections, il y a encore d'autres points critiques à relever dans la démonstration d'Euler, que je passerai cependant sous silence, afin de ne pas passer pour un censeur trop sévère. La démonstration, telle qu'Euler l'a exposée, ne peut en aucune façon être considérée comme complète.

Après cette démonstration, Euler montre encore par une autre voie, un théorème pour les équations dont le degré n'est pas une puissance binaire afin de réduire leur résolution à celle des équations dont le degré est une puissance binaire : mais comme cette dernière méthode est également sujette à toutes les objections (sauf pour la puissance de 2 qu'est la puissance quatrième) que la première démonstration générale, il n'est pas nécessaire de l'expliquer ici de façon plus développée.

9.

Dans le même traité, Euler s'est efforcé de démontrer notre théorème d'une autre manière encore (p. 163), dont la substance est contenue dans ce qui suit : Pour une équation donnée $x^n + Ax^{n-1} + Bx^{n-2}+$ etc.$= 0$, il n'a en effet pas été possible jusqu'à présent de trouver une expression analytique de ses racines lorsque $n > 4$. Mais il paraît néanmoins certain (comme l'affirme Euler) qu'une telle expression ne peut contenir que des opérations arithmétiques et des extractions de racines, qui seront d'autant plus compliquées que n sera grand.

Si cela est admis, Euler montre fort élégamment que, si compliqués que soient les radicaux entre eux, la valeur de la formule sera toujours représentée sous la forme $M + N\sqrt{-1}$, où M, N sont des quantités réelles.

Contre ce raisonnement, on peut objecter qu'après tant de travaux de si grands mathématiciens, il reste bien peu d'espoir de parvenir jamais à une solution générale des équations algébriques. Il paraît de plus en plus probable qu'une telle solution est entièrement impossible et contradictoire. Il ne faut pas du tout considérer cela comme un paradoxe, car *ce qu'on appelle communément la solution d'une équation n'est en réalité rien d'autre que sa réduction à des équations pures* (équations binaires). Car la solution des équations pures n'est pas ici enseignée, mais présupposée ; et si vous exprimez les racines d'une équation $x^m = H$ par $\sqrt[m]{H}$, vous ne l'avez en aucune façon résolue, et vous n'avez pas fait plus que si vous aviez imaginé un symbole pour désigner la racine d'une

équation $x^n + Ax^{n-1}+$ etc.$= 0$ et que vous aviez posé la racine comme égale à ce symbole.

Il est vrai que les équations pures (binaires) se distinguent nettement de toutes les autres en raison de la facilité avec laquelle on peut trouver leurs racines par approximations et en raison de la belle relation que les racines entretiennent entre elles.

Il n'y a donc rien à reprocher aux analystes qui ont désigné leurs racines par un symbole spécial. Mais de ce que ce symbole soit élevé à la dignité d'être intégré à l'ensemble des *expressions analytiques*, tout comme les symboles arithmétiques d'addition, de soustraction, de multiplication, de division et de puissance, il ne s'ensuit pas du tout que la racine d'une équation quelconque puisse être exprimée par ces expressions, à moins qu'il ne soit tacitement présupposé, sans raison suffisante, que la solution d'une équation quelconque puisse se réduire à la solution d'équations pures. Il n'est peut-être pas si difficile de démontrer en toute rigueur l'impossibilité déjà pour le cinquième degré ; je rendrai compte plus en détail de mes recherches sur cette question dans un autre endroit. Il suffit ici de dire que la possibilité qu'il existe une solution générale des équations, prise dans ce sens, est jusqu'ici très douteuse, et qu'une démonstration dont toute la force dépend entièrement de cette supposition n'a, dans l'état actuel de la question, aucun poids.

10.

Plus tard, le célébre de Foncenex remarqua le défaut de la première démonstration d'Euler (ci-dessus, article 8, quatrième objection) mais il ne parvint pas à le supprimer. Il essaya donc encore une autre méthode et la publia dans son célèbre traité p. 120 [7]. Elle consiste en ce qui suit.

Soit une équation $Z = 0$ où Z désigne une fonction de degré m de la variable z. Si m est un nombre impair, il est bien connu que cette équation a une racine réelle ; si au contraire m est pair, Foncenex s'efforce de démontrer que l'équation a au moins une racine de la forme $p + q\sqrt{-1}$, de la manière suivante. Soit $m = 2^n.i$ où i désigne un nombre impair, et supposons que $z^2 + uz + M$ soit un diviseur de la fonction Z.

Alors les seules valeurs possibles de u seront les sommes des racines de l'équation $Z = 0$ prises deux à deux (avec des signes interchangés). Donc u aura $\dfrac{m.(m-1}{1.2} = m'$ valeurs et si u est supposé déterminé par une équation $U = 0$ (où U désigne une fonction entière de u et de coefficients connus dans Z), alors cette équation sera de degré m'. Il est assez facile de voir que m' sera un nombre de la forme $2^{n-1}.i'$, où i' est un nombre impair. Si m' n'est pas impair, supposons que $u^2 + u'u + M'$ soit à son tour un diviseur de U. Il est clair que par un raisonnement similaire u' est déterminé par une équation $U' = 0$, où U' est une fonction de u de degré $\dfrac{m'(m'-1)}{1.2}$. En posant $\dfrac{m'(m'-1)}{1.2} = m''$, alors m'' sera un nombre de la forme $2^{n-2}.i''$, où i'' désigne un nombre impair. Si m'' n'est toujours pas impair, considérons que $u'^2 + u''u' + M''$ est un diviseur de U' ; alors u'' sera déterminé par une équation $U'' = 0$. Si celle-ci est considérée comme étant de degré

[7] Dans le second tome de ces *Miscellaneorum* (Mélange), p. 337, se trouvent des éclaircissements sur cette question : cependant, ceux-ci ne concernent pas la recherche présente mais les logarithmes des quantités négatives.

m''', alors m''' sera un nombre de la forme $2^{n-3}.i'''$. Il est manifeste que dans la suite d'équations $U = 0$, $U' = 0$, $U'' = 0$ etc., la n-ième équation sera de degré impair et aura donc une solution réelle.

Posons pour simplifier $n = 3$, de sorte que l'équation $U'' = 0$ a pour racine réelle u'', on voit sans peine que le même raisonnement est valable pour toute autre valeur de n. Par conséquent, dit Foncenex, le coefficient M'' peut être calculé rationnellement à partir de u'' et des coefficients de U' (qui seront des fonctions entières des coefficients de Z, comme on le voit facilement), soit à partir de u'' et des coefficients de Z, et est donc réel.

Il en résulte que la racine de l'équation $u'^2 + u''u' + M'' = 0$ sera contenue dans la forme $p + q\sqrt{-1}$ et ces racines satisfont évidemment l'équation $U' = 0$; c'est pourquoi toute valeur de u' sera sous la forme $p + q\sqrt{-1}$. En outre, le coefficient M' peut être calculé (de la même manière que précédemment) à partir de u' et des coefficients de Z et sera aussi de la forme $p + q\sqrt{-1}$. Par conséquent, les racines de l'équation $u^2 + u'u + M' = 0$ seront aussi de cette forme, et elles satisferont certainement l'équation $U = 0$ c'est-à-dire que cette équation aura une racine de la forme $p + q\sqrt{-1}$. Enfin, il résulte de cela de la même manière que M et certainement une racine de l'équation $z^2 + uz + M = 0$ sont également de cette forme, cette racine satisfera manifestement l'équation donnée $Z = 0$ Par conséquent, toute équation a au moins une racine de la forme $p+q\sqrt{-1}$.

11.

Les objections 1, 2, 3 que j'ai élevées contre la première démonstration d'Euler (article 8) ont la même force contre cette méthode, mais avec cette différence que la seconde objection, à laquelle la démonstration d'Euler n'était soumise que dans certains cas spéciaux, frappe la démonstration de Foncenex dans tous les cas. Car on peut démontrer tout d'abord que toutes les fois où l'on peut donner une formule qui exprime rationnellement le coefficient M' en fonction de u' et des coefficients dans Z, cette formule deviendra nécessairement indéterminée pour plusieurs valeurs de u'.

De même une formule qui exprime le coefficient M" par u' deviendra indéterminée pour plusieurs valeurs de u" etc. Ceci devient très clair quand on suppose par exemple une équation du quatrième degré. Posons donc m = 4 et les racines de l'équation $z = 0$ peuvent être $0, 0, 0, 0$. Il est alors clair que l'équation $U = 0$ sera du sixième degré avec des racines $(7 + 7).(7+).(7+)0.5(1 + 1) * 0.2(+)$, et $(+)$. L'équation $U = 0$ sera alors du quinzième degré et les valeurs de u' seront :

$$7 + 7 + 5, 27 + 7 + 7, 27 + +, 27 + 7+, 2 + ++, 20 + +, 2 + 7 + 7, 25 + +,$$

$$20 + 0 + 0,\ 27 + 0 + 0,\ 20 + 0 + 20 + 0 + 0 + 0 + 0,\ 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0$$

Il faut déjà s'arrêter à cette équation, car elle est de degré impair, et elle aura bien la racine réelle $+++$ (qui sera égale au premier coefficient de Z de signe opposé et sera donc non seulement réelle mais rationnelle si les coefficients de Z sont rationnels). Mais on le voit sans difficulté : si l'on

donne une formule qui exprime la valeur de M' par la valeur correspondante de u' par des opérations rationnelles, alors cette formule deviendra nécessairement indéterminée pour $u = ++C+C$. Car cette valeur sera trois fois la racine de UO et à elle correspondront trois valeurs de M', à savoir $(0+)(+0), (0+)(0+)$ et $(+)(+)$ qui peuvent toutes être irrationnelles. Mais il est évident que dans ce cas une formule rationnelle ne peut produire ni une valeur irrationnelle de M' ni trois valeurs différentes. De cet exemple on peut conclure suffisamment que la méthode de Foncenex n'est pas du tout satisfaisante : pour livrer une méthode complète à tous égards il faut plutôt approfondir beaucoup plus la théorie de l'élimination.

12.

Enfin, l'illustre LaGrange traite de notre théorème dans son ouvrage Sur la forme des racines imaginaires des équations, Nouv. Mem. de l'Acad. de Berlin 1772, p. 222 et suivantes. Ici ce grand mathématicien s'applique principalement à combler le défaut de la première démonstration d'Euler, et il a en effet examiné particulièrement ce qui constitue la troisième et la quatrième objection ci-dessus (article 8) si profondément qu'il ne reste plus rien à désirer, sinon que peut-être quelques doutes semblent subsister dans cette démonstration.

un ancien traité sur la théorie de l'élimination (sur laquelle repose totalement la présente enquête). Cependant, il n'a même pas abordé la première objection ; de plus, l'ensemble du traité est construit sur la supposition que toute équation de degré m a en effet m racines.

Après avoir étudié en détail les preuves publiées jusqu'à présent, j'espère qu'une nouvelle démonstration de ce théorème très important, fondée sur des fondements entièrement différents, ne sera pas mal accueillie par les experts. Je vais tout de suite expliquer cette démonstration.

13.

Lemme : Soit m un nombre entier positif quelconque. Alors la fonction $\sin mx + \sin(m1)$" est divisible par $xx - 2\cos/rx + rr$.

Preuve : Forme 1, la fonction est 0 et donc divisible par n'importe quel facteur. Forme $= 2$, le quotient est $\sin, etpourtoutevaleursupérieurelequotientsera + \sin 2x + \sin 3mx * 4 +$ etc , $+\sin(m1)2$, On confirme facilement que le produit de cette fonction multiplié par $xx - 2\cos rx + rr$ est égal à la fonction donnée.

14.

Lemme : Si la quantité r et l'angle sont déterminés de telle manière que les équations soient vraies $r * \cos m + Ar * \cos(m-1) + Br * 2\cos(m-2) + ... + Kir\cos 20 + Lr\cos + N = 0(1)r + Ar\sin(m-1)/7 + Er2\sin(m-2.$

alors la fonction $x + Ax + Bx - 2 + ...Kxx + Lx + MX$ sera divisible par le facteur du second degré $xx - 2\cos rx + rr$ si seulement $r\sin$ n'est pas 0. Mais si $r\sin r = 0$ alors cette fonction sera

divisible par le facteur simple x-rcos /7.

Preuve : I. Comme dans l'article précédent, les quantités suivantes seront toutes divisibles par $xx - 2\cos x + ri$

$+\sin(m-1)+1$
$UnA\sin(m1)x + A\sin(m2)0"BKB\sin(m2)x + B\sin(m3)etc.K\sin 2rrxLLMetc. + K\sin + M\sin(-)r$

La somme de ces quantités sera donc aussi divisible par $xx-2\cos rx+rr$. Les premiers termes de ces quantités. donnent la somme $\sin rX$; les seconds termes additionnés donnent 0 à cause de (2) ; et en effet la somme des troisièmes termes s'annule aussi, comme on le voit facilement si l'on multiplie (1) par sin, $(2)par\cos etsil'onsoustraitl'undesproduitsdel'autre.Ils'ensuitdoncquelafonction\sin rX$ est divisible par $xx - 2\cos /7rx + 1r$ et de même la fonction X, tant que r sin n'est pas 0.

II. Mais si r sin $= 0, alorssoitr = 0soit\sin = 0.Danslepremiercas, M = 0àcausede(1), etdoncXseradivisiblepa$
$1\cos 3 + 1etgénéralement\cos n\cos".Parconséquent, Xsera = 0àcausede(1)lorsquexestdéfini =$
$r\cos, etparconséquentlafonctionXseradivisibleparx - \cos .QES$

15.

Le théorème remarquable est souvent démontré à l'aide de nombres imaginaires, cf. Euler, *Introduction à l 'analyse infinitésimale*, Tome I p. 110 ; je considère qu'il vaut la peine de montrer comment il peut être facilement obtenu sans les utiliser. Il est tout à fait évident que pour la démonstration de notre théorème, il suffit de montrer : *Soit X de la forme $x^m + Ax^{m-1} + Bx^{m-2} + \text{etc.} + Lx + M$ donnée, alors r et φ peuvent être déterminés de telle manière que les égalités (1) et (2) soient vraies.* Car il s'ensuit que X a un facteur réel du premier ou du second degré ; la division (par ce facteur) produit nécessairement un quotient réel de degré inférieur qui, pour la même raison, aura aussi un facteur du premier ou du second degré. En continuant cette opération, X sera enfin décomposé en facteurs réels du premier et du second degré. C'est donc le point principal des recherches suivantes que de prouver ce théorème.

16.

Considérons un plan infini fixe (le plan du tableau Fig. 1) et dans ce plan une droite fixe infinie GC passant par le point fixe C. Choisissons une longueur quelconque comme unité afin que tous les segments de droites puissent être mesurés par des nombres. En tout point P du plan dont la distance à C est r et tel que $\widehat{GCP} = \varphi$, érigeons le segment de droite perpendiculaire au plan du tableau et de longueur égale à l'expression

$$r^m \sin m\varphi + Ar^{m-1}\sin(m-1)\varphi + \text{etc.} + Lr\sin\varphi,$$

que, pour plus de concision, je désignerai désormais par T. Je prendrai toujours une distance r positive, et pour les points qui tombent de l'autre côté de l'axe, l'angle φ devra être considéré

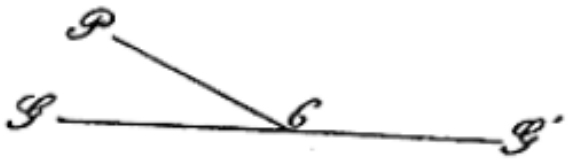
comme augmenté de deux angles droits ou comme négatif (ce qui revient au même). Les extrémités de ces perpendiculaires seront situées au-dessus du plan pour les valeurs positives de T, au-dessous pour les valeurs négatives, et sur le plan lui-même si T s'annule ; et elles seront sur une surface courbe, continue et infinie dans toutes les directions, que, pour abréger, j'appellerai désormais la *première surface*.

De la même manière, on peut rapporter au même plan, au même centre et au même axe, une seconde surface dont la hauteur au-dessus de tout point du plan sera

$$r^m \cos m\varphi + Ar^{m-1} \cos(m-1)\varphi + \text{etc.} + Lr. \cos\varphi + M,$$

expression que je désignerai toujours par U, pour simplifier. Cette surface, qui sera également continue et infinie dans toutes les directions, je la distinguerai de la première surface en la désignant par l'appellation de *seconde surface*.
Il est alors évident que toute la tâche consiste à montrer qu'il existe au moins un point qui se trouve simultanément dans le plan, sur la première surface et sur la seconde surface. Sur la Figure 1, il faut que P, T et U soient confondus.

Fig. 1.



17.

On voit aisément que la première surface se trouve en partie au-dessus et en partie au-dessous du plan ; car il est clair qu'à une distance au centre r suffisamment grande, les termes de T autres que le premier terme ne contribuent à rien par rapport à ce premier $r^m \sin m\varphi$; mais que T peut être rendu positif aussi bien que négatif selon la valeur choisie pour l'angle φ. Par conséquent, le plan fixe sera nécessairement coupé par la première surface. Cette intersection du plan avec la première surface, je l'appellerai la *première courbe*, et elle sera donc déterminée par l'équation $T = 0$. Pour la même raison, le plan sera intersectée par la seconde surface. L'intersection constitue une courbe déterminée par l'équation $U = 0$ que j'appellerai la *seconde courbe*. En particulier, chacune de ces courbes est constituée de plusieurs branches qui peuvent généralement être séparées, mais dont chacune sera une courbe continue.

En effet, la première courbe sera toujours celle qu'on appelle complexe, et l'axe GC doit être considéré comme faisant partie de cette courbe car quelle que soit la valeur donnée à r, T sera toujours nul toutes les fois que $\varphi = 0$ ou 180°. Mais il vaut mieux considérer comme une seule courbe la composée de toutes les branches passant par des points quelconques où $T = 0$ (selon l'usage généralement admis en mathématiques supérieures). Et de faire de même avec toutes les branches passant par des points quelconques où $U = 0$ À l'évidence, la tâche se réduit maintenant à démontrer qu'il existe dans notre plan au moins un point où une branche de la première courbe est coupée par une branche de la seconde courbe. Pour cela, il est impératif d'examiner de plus près la nature de ces courbes.

18.

Tout d'abord, je remarque que les deux courbes sont algébriques, et d'ordre m si on les rapporte à des coordonnées orthogonales. Si maintenant on suppose l'origine en C, les abscisses x prises dans la direction de G, et les ordonnées y correspondantes vers P, alors $x = r\cos\varphi, y = r\sin\varphi$ et donc généralement pour tout n :

$$r^n \sin n\varphi = nx^{n-l}y - \frac{n\cdot n-1\cdot n-2}{1\cdot 2\cdot 3}x^{n-3}y^3 + \frac{\cdot\ldots\cdot n-4}{1\cdot\ldots\cdot 5}x^{n-5}y^5 - \text{etc.},$$

$$r^n \cos n\varphi = x^{n-l}y - \frac{n\cdot n-1}{1\cdot 2}x^{n-2}y^2 + \frac{\cdot n-1\cdot n-2\cdot n-3}{1\cdot 2\cdot 3\cdot 4}x^{n-4}y^4 - \text{etc.}.$$

Ainsi T, comme U, seront constitués de plusieurs termes de la forme $ax^{\alpha}y^{\beta}$ où α et β désignent des nombres entiers positifs dont la somme est inférieure ou égale à m. De plus, on voit facilement que tous les termes de T contiennent un facteur y et que, par conséquent, la première courbe est au sens strict composée d'une droite (d'équation $y = 0$) et d'une courbe d'ordre $m - 1$, bien que cette distinction n'ait pas à être considérée ici.

Il est plus important de chercher à savoir si la première courbe et la seconde ont des branches infinies, combien il y en a et où elles se trouvent.

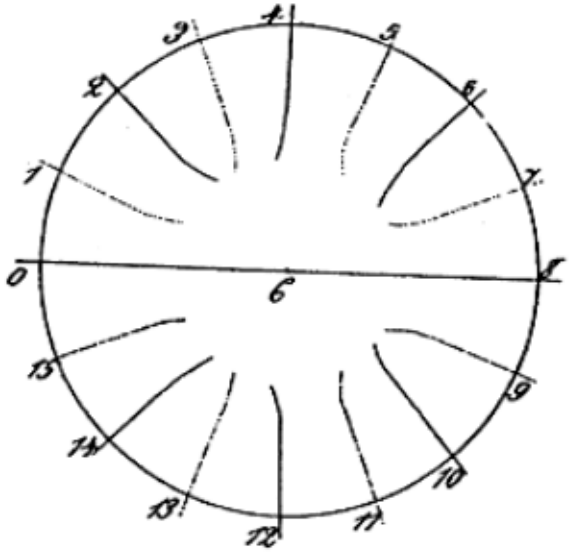
À une distance infinie du point C, la première courbe dont l'équation est

$$\sin m\varphi + \frac{A}{r}\sin(m-1)\varphi + \frac{B}{r^2}\sin(m-2)\varphi\text{etc.} = 0,$$

coïncidera avec la courbe dont l'équation est $\sin m\varphi = 0$. Celle-ci représente m droites se coupant au point C, dont la première est l'axe GCG', les autres étant inclinées par rapport à cet axe selon des angles $\frac{1}{m}180^{\circ}$, $\frac{2}{m}180^{\circ}$, $\frac{3}{m}180^{\circ}$, etc. Ainsi, la première courbe a $2m$ branches infinies qui diviseront la circonférence du cercle de rayon infini en $2m$ parties égales, de sorte que la circonférence sera coupée par la première branche où le cercle et l'axe se rencontrent, par la seconde branche à la distance angulaire de $\frac{1}{m}180^{\circ}$, par la troisième branche à la distance $\frac{2}{m}180^{\circ}$ etc. De même, la seconde courbe aura à distance infinie du centre une asymptote d'équation $\cos m\varphi = 0$. Cette asymptote est un composé de m droites qui se coupent au point C selon des angles égaux de telle manière que la première droite forme avec l'axe CG un angle de $\frac{1}{m}90^{\circ}$, la seconde un angle

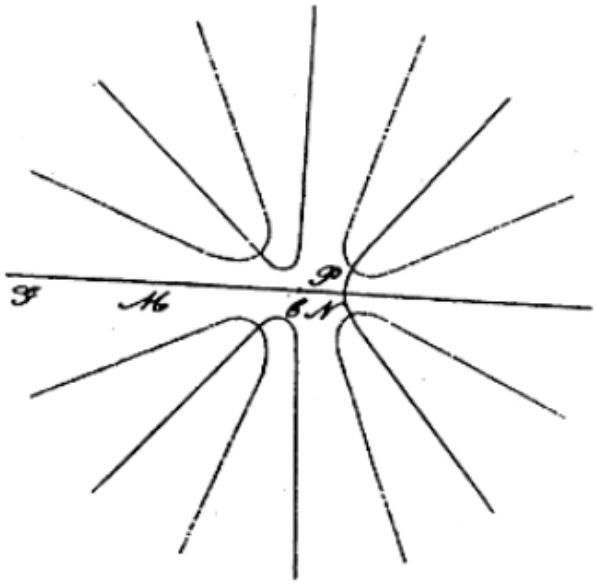
de $\frac{3}{m}90^{\circ}$, la troisième un angle de $\frac{5}{m}90^{\circ}$, etc. Par conséquent, la seconde courbe aura aussi $2m$ branches infinies, dont chacune occupera l'espace entre deux branches successives de la première courbe de telle sorte qu'elles coupent la circonférence d'un cercle de rayon infini en des points distants d'un point de vue angulaire de l'axe de $\frac{1}{m}90^{\circ}$, $\frac{3}{m}90^{\circ}$, $\frac{5}{m}90^{\circ}$, etc. De plus, il est clair que l'axe lui-même constitue toujours deux branches infinies de la première courbe, à savoir la première et la $(m+1)$-ième. D'une manière perceptuellement claire, cette position des branches est montrée sur la figure 2, construite pour le cas $m = 4$ où les branches de la seconde courbe sont pointillées pour les distinguer des branches de la première courbe ceci est également à noter dans la quatrième figure [8].

Fig. 2.



[8]La quatrième figure a été construite en supposant $X = x^4 - 2x^2 + 3x + 10$ grâce à laquelle les lecteurs moins familiers avec les investigations générales et abstraites peuvent alors examiner la position des deux courbes dans un cas concret. La longueur de CG est prise égale à 10 et $CN = 1.26255$.

Fig. 4.



Je montrerai dans les articles suivants comment développer ces conclusions sans l'aide de l'infini.

19.

THÉORÈME. *Toutes choses étant égales par ailleurs, on peut tracer un cercle de centre C sur la circonférence duquel se trouvent $2m$ points pour lesquels $T = 0$ et autant de points pour lesquels $U = 0$ et de telle manière que chacun des seconds points se trouvera seul entre deux points de la première espèce.*

Si S la somme de tous les coefficients $A, B, \ldots, K, L, M$ est prise positivement et R et S sont tels que $R > S\sqrt{(2)}$ et $R > 1$ [9] alors j'affirme que ce qui a été énoncé dans le théorème se déroulera nécessairement pour un cercle de rayon R.

En d'autres termes, désignons pour abréger par (1) le point de la circonférence du cercle qui est à une distance angulaire de $\frac{1}{m}45^{\circ}$ du point de concours de la partie gauche de l'axe avec la circonférence [10], soit pour lequel $\varphi = \frac{1}{m}45^{\circ}$; de même désignons par (3) le point qui est à $\frac{3}{m}45^{\circ}$ de cette intersection, i.e. pour lequel $\varphi = \frac{3}{m}45^{\circ}$, par (5) le point tel que $\varphi = \frac{5}{m}45^{\circ}$, etc. jusqu'à $(8m-1)$ qui est à $\varphi = \left(8m - \frac{1}{m}\right)45^{\circ}$ vers la partie opposée), un total de $4m$ points sera obtenu

[9] Quand $S > \sqrt{\frac{1}{2}}$, la première condition inclut la seconde ; quand $S < \sqrt{\frac{1}{2}}$, la seconde inclut la première.

[10] Le point -1 du cercle unité ?

sur la circonférence, espacés régulièrement. Alors un point sera situé entre $(8m-1)$ et (1) pour lequel $T=0$, et des points similaires seront compris entre (3) et (5), entre (7) et (9), entre (11) et (13), etc., leur nombre étant égal à $2m$. Enfin, il n'existe aucun autre point que ces $4m$ points pour lequel T ou U est nul.

Preuve :

I. Au point (1), $m\varphi = 45^{\circ}$ et donc

$$T = R^{m-1}(R\sqrt{\frac{1}{2}} + A\sin(m-1)\varphi + \frac{B}{R}\sin(m-2) + etc. + \frac{L}{R^{m-2}}\sin\varphi).$$

Cependant, la somme $A\sin(m-1)\varphi + \frac{B}{R}\sin(m-2)\varphi +$ etc. ne peut certainement pas être supérieure à S et sera même nécessairement inférieure à $R\sqrt{\frac{1}{2}}$, d'où il découle que la valeur de T en ce point est nécessairement positive.

Plus important encore, T aura par conséquent une valeur positive tant que $m\varphi$ se situe entre 45° et 135°, c'est-à-dire que du point (1) au point (3), la valeur de T sera toujours positive. Pour la même raison T aura une valeur positive du point (9) jusqu'à (11), et plus généralement de tout point $(8k+1)$ jusqu'à $(8k+3)$ où k désigne un entier quelconque. De même, T aura partout des valeurs négatives entre (5) et (7), entre (13) et (15) etc. et généralement entre $(8k+5)$ et $(8k+7)$ et dans tous ces intervalles, il ne pourra être nul en aucun endroit. Mais parce qu'en (3) cette valeur est positive et qu'en (5) elle est négative, T sera nécessairement $= 0$ quelque part entre (3) et (5) ; et certainement aussi entre (7) et (9), entre (11) et (13) etc. jusqu'à et y compris dans l'intervalle entre $(8m-1)$ et (1), de sorte qu'au total $T=0$ en $2m$ points. C.Q.F.D.

II. Outre ces $2m$ points, il n'y en a pas d'autres qui possèdent cette propriété, comme on peut le voir ainsi : puisqu'il n'y en a pas entre (1) et (3), (5) et (7) etc., de tels points ne pourraient exister d'aucune autre manière sauf si dans un intervalle entre (3) et (5), ou entre (7) et (9) etc., il y en avait au moins deux. T aurait nécessairement un maximum ou un minimum dans le même intervalle et il faudrait que $\mathrm{d}T/\mathrm{d}\varphi = 0$.

Mais $\frac{\mathrm{d}T}{\mathrm{d}\varphi} = mR^{m-2}(R.\cos m\varphi + \frac{m-1}{m}.A\cos(m-1)\varphi + \text{etc.})$, et $\cos m\varphi$ est toujours négatif entre (3) et (5) et $|\cos m\varphi| > \sqrt{1/2}$ [11]. D'où il est facile de voir que dans tout cet intervalle $\mathrm{d}T/\mathrm{d}\varphi$ est une quantité négative, de même elle est positive partout entre (7) et (9), négative entre (11) et (13) etc., de sorte qu'elle ne peut être nulle dans aucun de ces intervalles, et donc cette supposition ne peut être maintenue. C'est pourquoi etc. CQFD.

De même, il est démontré que U a une valeur négative partout entre (3) et (5), (11) et (13) etc. et généralement entre $(8k+3)$ et $(8k+5)$ mais une valeur positive entre (7) et (9), (15) et (17) etc. et

[11] *(Note du traducteur)* : À l'époque de Gauss, $\sqrt{\frac{1}{2}}$ était généralement défini comme étant égal à $\pm 0,7071$, et pas comme seulement égal à $+0,7071$ comme c'est le cas aujourd'hui.

généralement entre $(8k+7)$ et $(8k+9)$. Il en résulte immédiatement que U doit s'annuler quelque part entre (1) et (3), entre (5) et (7) etc., c'est-à-dire en $2m$ points. De même, dans aucun de ces intervalles, on ne peut avoir ‘$\mathrm{d}U/\mathrm{d}\varphi = 0$ (ce qui est facilement démontré de la même manière que ci-dessus) : par conséquent, il n'y aura pas plus que ces $2m$ points où $U = 0$ sur la circonférence du cercle. CQFD.

De plus, la partie du théorème selon laquelle il n'existe pas plus de $2m$ points pour lesquels $T = 0$, ni plus de $2m$ points pour lesquels $U = 0$ peut également être prouvée par le fait que les équations $T = 0$, $U = 0$ décrivent des courbes d'ordre m qui ne peuvent être intersectées en plus de $2m$ points par un cercle vue comme une courbe d'ordre 2, comme cela est établi en Géométrie supérieure.

20.

Si l'on décrit un autre cercle autour du même centre avec un rayon supérieur à R et qu'on le divise de la même manière, alors sur ce cercle un point tombera aussi entre les points (3) et (5) et de même entre (7) et (9) etc. où $T = 0$. Et on voit facilement que moins le rayon de ce cercle diffère du rayon R, plus ces points particuliers entre (3) et (5) doivent être situés près les uns des autres sur les circonférences de ces deux cercles. La même chose se produira aussi lorsqu'on décrira un cercle avec un rayon un peu plus petit que R mais plus grand que $S\sqrt{2}$ et 1.

D'où l'on s'aperçoit sans difficulté que la circonférence du cercle tracé avec le rayon R est effectivement *coupée* par une branche de la première courbe en ce point entre (3) et (5) où $T = 0$ et il en est de même pour les autres points où $T = 0$ De la même manière, il est clair que la circonférence de ce cercle sera coupée par une branche de la seconde courbe en tous ces $2m$ points où $U = 0$ Ces conclusions peuvent aussi s'exprimer de la manière suivante :

Lorsqu'un cercle de la grandeur requise est tracé autour du centre C, alors $2m$ de branches de la première courbe et autant de branches de la seconde courbe y entreront, et en effet de telle manière que deux branches successives de la première courbe seront séparées par une branche de la seconde courbe en alternance. Voir la figure 2 où le cercle n'est cependant pas de grandeur infinie mais de grandeur finie.

Les numéros ajoutés aux branches individuelles ne doivent pas être confondus avec les numéros par lesquels j'ai désignés brièvement, dans cet article et les précédents, les intersections avec la circonférence.

21.

Déjà de cette position relative des branches entrant dans le cercle, on peut déduire de plusieurs manières qu'il doit nécessairement y avoir intersection d'une branche de la première courbe avec une branche de la seconde courbe à l'intérieur du cercle. Et je ne sais guère quelle méthode il faut choisir de préférence aux autres. La plus astucieuse semble être celle-ci : désignons par 0 (fig.

2) le point de la circonférence du cercle où celle-ci est coupée par la partie gauche de l'axe (axe qui est lui-même une des $2m$ branches de la première courbe) ; par 1, le point le plus proche où une branche de la seconde courbe pénètre dans la circonférence ; par 2, le point le plus proche de celui-là où la seconde branche de la première courbe entre dans la circonférence, et ainsi de suite jusqu'à $4m - 1$. De cette manière une branche de la première courbe entre dans le disque en tout point marqué par un nombre pair, tandis qu'une branche de la seconde courbe entre en tout point représenté par un nombre impair.

Mais selon la Géométrie supérieure, on trouve que toute courbe algébrique (ou les parties individuelles d'une telle courbe algébrique si elle est constituée de plusieurs parties) soit se retourne sur elle-même, soit s'étend jusqu'à l'infini.

En conséquence, une branche d'une courbe algébrique quelconque qui entre dans un espace limité, doit nécessairement sortir de cet espace quelque part [12]. De là on conclut facilement que tout point marqué par un nombre pair (ou pour abréger, tout *point pair*) doit être relié dans le cercle à un autre point pair par une branche de la première courbe, et de même tout point marqué par un nombre impair à un point semblable par une branche de la seconde courbe. Or, quoique cette connexion de deux de ces points puisse être très variée suivant la nature de la fonction X, de sorte qu'en général elle ne peut être clairement décrite, il est pourtant facile de prouver *qu'il existe toujours une intersection de la première courbe avec la seconde courbe, quelle que soit finalement cette intersection.*

22.

La preuve que cela se produit nécessairement semble pouvoir être donnée plus précisément de manière indirecte. Supposons que les jonctions des paires de points pairs et des paires de points impairs puissent être disposées de telle manière qu'il n'y ait aucune intersection entre une branche de la première courbe et une branche de la seconde courbe. Comme l'axe fait partie de la première courbe, le point 0 sera évidemment relié au point $2m$. Le point 1 ne peut donc être relié à aucun point situé au-dessous de l'axe, c'est-à-dire à aucun point marqué par un nombre supérieur à $2m$, car sinon la courbe qui les joindrait couperait nécessairement l'axe. C'est pourquoi si l'on suppose

[12] Il semble avoir été prouvé avec suffisamment de certitude qu'une courbe algébrique ne peut ni se rompre brusquement n'importe où (comme cela arrive par exemple avec la courbe transcendante dont l'équation est $y = \frac{1}{\ln x)}$ ni se perdre, pour ainsi dire, en un point quelconque après une infinité de tours (comme la spirale logarithmique). Autant que je sache, personne n'a émis de doute à ce sujet. Cependant, si quelqu'un me le demande, je me chargerai de donner une preuve qui ne soit sujette à aucun doute, à une autre occasion. Dans le cas présent, cela est vraiment manifeste : supposons qu'une branche, par exemple 2, ne sorte nulle part du cercle (figure 3). Vous pourriez alors entrer dans le cercle entre 0 et 2, puis faire le tour de toute cette branche (qui devrait se perdre à l'intérieur du cercle), et enfin sortir à nouveau du cercle entre 2 et 4 de telle sorte que, sur tout le trajet, elle n'ait pas croisé la première courbe. C'est là une absurdité évidente, car au point où vous entrez dans le cercle vous avez la première surface au-dessus de vous, et à la sortie au-dessous de vous. Il faut donc nécessairement que vous soyez quelque part tombé sur la première surface elle-même, c'est-à-dire sur un point de la première courbe. Cependant, de ce raisonnement fondé sur les principes de la géométrie de position, principes qui ne sont pas moins vrais que ceux de la géométrie de dimension, il résulte seulement ceci : si vous entrez dans le cercle par une branche quelconque de la première courbe, vous pouvez sortir du cercle en un autre endroit, tout en restant toujours sur la première courbe. Il ne s'ensuit pas, cependant, que tout votre parcours soit une courbe continue au sens où on l'entend en géométrie supérieure. Mais il suffit ici que le parcours soit une courbe continue au sens habituel, c'est-à-dire nulle part interrompu et partout continu.

que 1 est relié au point n, alors $n < 2m$.

Pour une raison analogue, si l'on établit que 2 est relié à n', alors $n' < n$, car sinon, la branche $2...n'$ couperait nécessairement la branche $1...n$. Pour la même raison, le point 3 sera relié à l'un des points compris entre 4 et n' ; et évidemment, lorsque 3, 4, 5, etc. sont considérés comme reliés respectivement à n'', n''', n'''' etc., alors n''' devra être entre 5 et n'', n'''' entre 6 et n''' etc. D'où il est certain qu'on finira par atteindre un point h relié au point $h + 2$, et alors la branche qui entre dans le cercle au point $h + 1$ coupera nécessairement la branche reliant les points h et $h + 2$. Mais comme l'une de ces deux branches appartient à la première courbe, l'autre à la seconde courbe, il est donc manifeste que l'hypothèse est contredite et qu'en effet une intersection de la première courbe avec la seconde courbe existe nécessairement quelque part.

Lorsque ceci est combiné avec ce qui précède, on conclura de toutes les recherches présentées que le théorème suivant a été prouvé en toute rigueur : *toute fonction entière rationnelle algébrique d'une seule variable peut être résolue en facteurs réels du premier et du second degré.*

23.

De plus, de ces fondements, il n'est pas difficile de déduire des mêmes principes qu'il y aura non seulement une, mais au moins m intersections de la première courbe avec la seconde, quoiqu'il puisse aussi arriver que la première courbe soit coupée par plusieurs branches de la seconde courbe en un même point. Dans ce cas, la fonction X aura plusieurs facteurs égaux. Mais comme il peut suffire ici d'avoir démontré la nécessité d'une seule intersection, je ne m'étendrai pas davantage sur cette question pour être bref. Pour la même raison, je n'examinerai pas plus en détail ici d'autres propriétés de ces courbes, par exemple qu'une intersection se fait toujours selon des angles droits ; ou bien si plusieurs branches de l'une ou l'autre courbe se rencontrent au même point, alors il y aura autant de branches infinies de la première courbe que de la seconde courbe, et celles-ci seront placées alternativement et se couperont à des angles égaux, etc.

Enfin, je remarque qu'il n'est pas du tout impossible de rendre la démonstration précédente, que j'ai ici fondée sur des principes géométriques, sous une forme purement analytique. Mais je crois que la représentation que j'ai exposée ici est moins abstraite et se présente sous les yeux de façon beaucoup plus claire qu'on ne peut l'espérer dans une démonstration analytique.

Pour terminer, j'indiquerai brièvement encore une autre méthode de démonstration de notre théorème, qui, au premier coup d'œil, paraîtra tout à fait différente non seulement de la démonstration précédente, mais de toutes les autres démonstrations exposées en détail ci-dessus, et qui pourtant est, au sens strict, la même que celle de d'Alembert si l'on regarde attentivement sa nature. Je la confie aux spécialistes pour lesquels j'ai ajouté ce texte et à qui je recommande de comparer cette méthode avec l'autre et d'explorer le parallélisme entre les deux.

24.

Au-dessus du plan de la figure 4 par rapport à l'axe CG et à un point fixe C, je suppose la première et la seconde surface de la même manière que précédemment. Prenons un point quelconque sur une

branche quelconque de la première courbe pour lequel $T = 0$, (par exemple un point M quelconque de l'axe) et pour lequel $U \neq 0$. Progressons de ce point sur la première courbe dans la direction dans laquelle la valeur absolue de U décroît. Si par hasard au point M la valeur absolue de U décroît dans les deux directions, alors la direction dans laquelle on progresse n'a pas d'importance ; je dirai ci-après ce qu'il faut faire si U augmente dans les deux directions. Il est évident que si l'on progresse toujours le long de la première courbe, on parviendra nécessairement en un point pour lequel $U = 0$ ou en un point tel que la valeur de U deviendra minimale, par exemple le point N. Dans le premier cas, nous avons trouvé ce que nous cherchions ; dans le second cas, cependant, on peut prouver qu'en ce point, plusieurs branches de la première courbe se coupent (et en fait un nombre pair de branches). La moitié d'entre elles sont disposées de telle manière que si l'on se détourne dans l'une quelconque de ces branches, la valeur de U continuera à décroître (je dois, par souci de concision, omettre la démonstration de ce théorème, qui est plus longue que difficile.) Sur cette branche, on pourra alors progresser à nouveau jusqu'à ce que U devienne nul (comme cela se produit dans la figure 4 en P). Lorsqu'on se détourne encore, on arrivera finalement nécessairement à un point pour lequel $U = 0$.

On peut émettre un doute contre cette démonstration. Il se peut que, si loin que l'on progresse et bien que la valeur de U puisse toujours diminuer, cette diminution puisse devenir toujours plus lente et que la valeur puisse ne jamais atteindre une limite, ce qui correspond à la quatrième objection de l'article 6. Mais il n'est pas difficile de fixer une limite telle que, dès qu'on la franchit, la valeur de U non seulement change nécessairement toujours plus vite, mais ne puisse plus *décroître* davantage, de sorte qu'avant même d'atteindre cette limite, la valeur de 0 a dû déjà être atteinte.

Je me réserve d'approfondir davantage, dans une autre occasion, cette matière et tout ce que je n'ai pu qu'effleurer dans cette épreuve.

J'ai découvert les principes sur lesquels s'appuie cette démonstration au début d'octobre 1797.

Fig. 1.

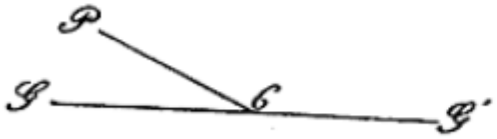


Fig. 2.

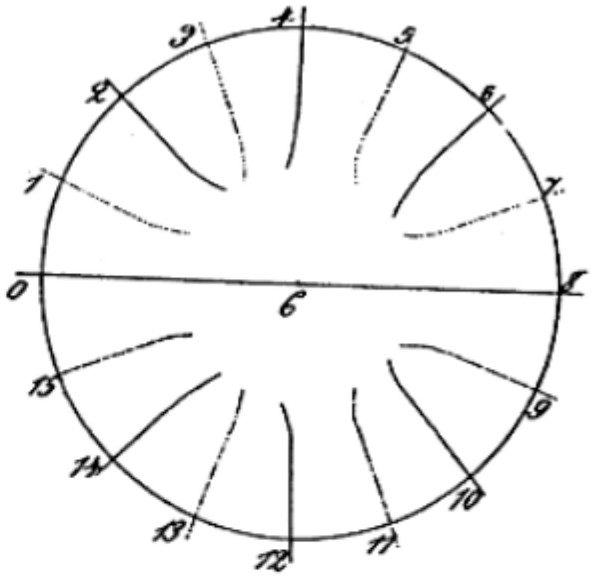


Fig. 4.

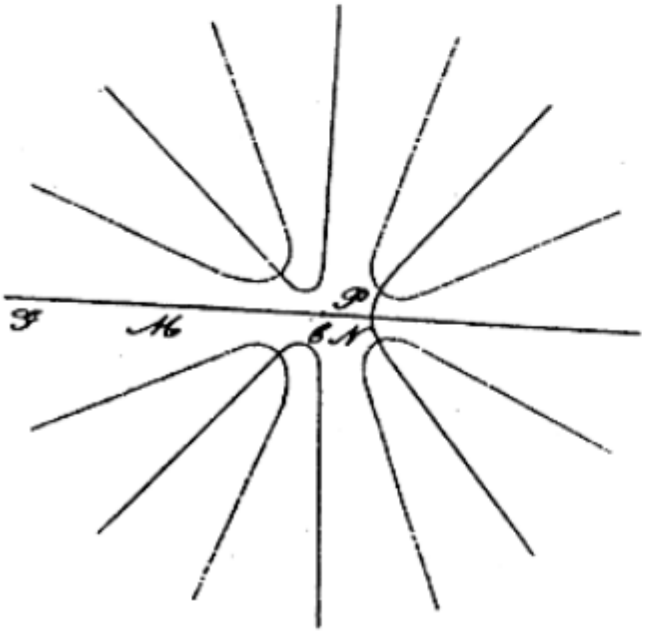
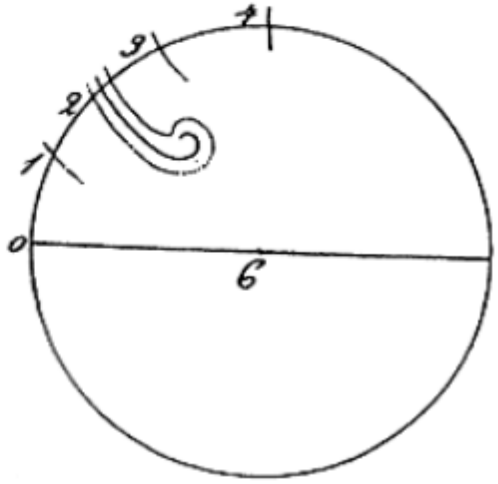


Fig. 3.



Avant-propos à la traduction de Ernest Fandreyer[13]

Il y a quelque chose qui ne va pas dans le titre "Nouvelle preuve du théorème...", comme le remarque Eric Temple Bell dans son article "*Le Prince des mathématiques*" (cf. dans *The World of Mathematics*, Vol. I de J. R. Newman) : il ne s'agit pas d'une nouvelle preuve mais de la première preuve de ce théorème. Toutes les "preuves" précédentes étaient erronées et donc non acceptables en tant que preuves.

Gauss a soumis ce travail remarquable à l'Université de Helmstedt, en Allemagne, comme thèse de doctorat et a obtenu son diplôme en 1799, à l'âge de 22 ans. Il a publié deux autres preuves, en latin comme cette première preuve, en 1816, et une quatrième preuve, en allemand, en 1850. La première preuve est l'une des réalisations monumentales de l'histoire des mathématiques. Des versions anglaises des deuxième et troisième preuves existent (par exemple, *A Sourcebook of Mathematics* de D.E. Smith contient une version anglaise de la partie essentielle de la deuxième preuve). Mais une recherche intensive et approfondie dans les bibliothèques universitaires des États-Unis et à la Bibliothèque du Congrès n'a pas permis de trouver une traduction anglaise de la première preuve (bien que cette preuve soit citée dans d'innombrables ouvrages sur l'algèbre, l'analyse et l'histoire des mathématiques). Si une version anglaise existe dans ce pays, elle n'est certainement pas facilement disponible. Pour remédier à cette lacune, cette traduction sera archivée et disponible sur Internet. Il est évident que le nombre de lecteurs sera toujours très faible. Mais c'est, après tout, le sort de beaucoup d'ouvrages que l'on trouve actuellement dans nos bibliothèques, et ce n'est pas une raison suffisante pour se passer entièrement d'une version anglaise de l'ouvrage célèbre de Gauss.

Cette traduction a suivi la règle : aussi précisément que possible, aussi librement que nécessaire [14]. Elle n'est donc pas dans le style de l'anglais du XXIe siècle, mais plutôt comme certains livres datant du début du XIXe siècle. Le lecteur qui veut se familiariser avec une œuvre importante d'un siècle antérieur appréciera probablement une traduction qui adhère au style de l'original. Pour cela, les longues phrases latines de Gauss ont été traduites en longues phrases anglaises, sauf lorsque cela était incompatible avec l'exigence de clarté. (Une phrase qui s'étend sur neuf lignes à l'écrit, comme par exemple dans l'article 9, peut difficilement être traduite en anglais intelligible sans la diviser en plusieurs phrases.) Dans la même veine, la ponctuation de l'original a été respectée lorsque cela était possible sans nuire à la clarté. Une représentation claire des idées de Gauss était, après tout, l'objectif primordial. Il faut cependant garder à l'esprit que ces idées ne sont pas si simples qu'une traduction, ou l'original d'ailleurs, en rendrait la lecture facile. Pourtant, bien que de nombreuses preuves modernes du théorème fondamental de l'algèbre existent, il semble utile de revenir à cette réalisation unique de Gauss. On espère que cette traduction facilitera une telle entreprise.

Traduit par : Ernest Fandreyer, M.S., Ed.D., Professeur émérite, Fitchburg State College (MA), Département de mathématiques

[13]La présente note est une transcription en Latex, suivie d'une traduction Google, reprise et améliorée autant que faire se peut à l'aide d'un petit livre en français aux éditions les bouquins Fusion (contenant également deux textes de Jonathan Tennenbaum et de Bruce Director), de la traduction en anglais de Ernest Fandreyer, téléchargeable ici https://www.quantresearch.org/Gauss_PhD_Dissertation.pdf, effectuée par Denise Vella-Chemla en octobre 2024.

[14]La traduction allemande du Dr W. Frahnert, de 1889, semble aller dans le sens inverse : aussi librement que possible, aussi précisément que nécessaire.

[peuvent être données de telles valeurs réelles qui peuvent satisfaire ces équations. Maintenant E. affirme : Si à f 1. On considère que non, O résultera où U sera une fonction intégrale de u et de coefficients connus seulement. Pour résoudre cette équation, O est d'un degré assez élevé et pour un degré indéterminé, il serait clairement impossible (comme E. lui-même le souligne)]

La première démonstration de Gauss du théorème fondamental de l'algèbre

Jean-Pierre Friedelmeyer

Professeur au Lycée Couffignal de Strasbourg

Tout étudiant de mathématiques connaît ou est censé connaître le théorème fondamental de l'algèbre, éventuellement sous la dénomination de théorème de d'Alembert-Gauss :

"Tout polynôme non constant à coefficients réels ou complexes admet au moins une racine dans le corps $\mathbb{C}$ *des nombres complexes."* Cette propriété fait de $\mathbb{C}$ un **corps algébriquement clos**.

Le terme **fondamental** vient de Gauss qui l'utilise dans un texte de 1849 [1] et cette dénomination lui est restée, concurremment avec celle de théorème de d'Alembert en France. Pourquoi fondamental ?

1) Sur lui repose une grande partie de l'algèbre classique : résolution des équations algébriques, décomposition des polynômes en facteurs irréductibles, existence de valeurs propres pour des endomorphismes d'espaces vectoriels sur $\mathbb{C}$, théorie des fonctions algébriques ou rationnelles.

2) Fondamental aussi en ce qu'il représente un sujet permanent de réflexion sur la structure de $\mathbb{R}$ ou de $\mathbb{C}$ qui fait qu'il a été l'occasion d'une multitude de démonstrations : d'Alembert, Euler, Lagrange, Argand, Cauchy, Laplace et qu'il continue à en susciter. Par exemple en 1979, M. W. Hirsch et St. Smale ont donné une démonstration constructive qui met en place un algorithme, lequel partant d'un $c = z_0$ quelconque, aboutit à une racine d'un polynôme donné $f(z)$ au moyen d'une suite (z_n). Un point central de cette réflexion se trouve dans le fait quasi paradoxal que **ces démonstrations du théorème fondamental de l'algèbre utilise, en dernier recours, des moyens non algébriques**, c'est-à-dire des moyens liés à l'analyse.

   - Ou bien (d'Alembert, Argand, Cauchy...) l'on diminue le module de $f(z)$ et l'on utilise l'existence d'un minimum nul pour ce module.
   - Ou bien (Euler, Lagrange, Laplace...) l'on ramène le problème à l'existence de racines carrées pour tout nombre complexe, et l'on utilise le théorème des valeurs intermédiaires pour montrer qu'un polynôme de degré impair a au moins une racine réelle [2].

Aujourd'hui, les démonstrations les plus en faveur dans l'enseignement universitaire sont celles qui utilisent les puissants théorèmes de la théorie des fonctions de variable complexe. Mais ce faisant, elles font peut-être perdre à ce théorème son caractère essentiel, fondamental pour l'algèbre, banalisant un résultat perçu comme évident par les étudiants, alors que le nombre même des démonstrations (plusieurs dizaines) réparties sur deux siècles et demi, montre assez son caractère problématique et stimulant pour le progrès des mathématiques. On en trouvera une

Transcription en Latex du texte téléchargeable à l'adresse https://bibnum.publimath.fr/IST/IST95009.pdf, référence L'Ouvert, 91, 1995. Denise Vella-Chemla, novembre 2024

[1] "Grundlehrsatz der Theorie der algebraischen Gleichungen", Gauss Werke 3, p. 73.

[2] Jusqu'à Bolzano (1817) ce théorème était considéré comme quasi évident, reposant simplement sur l'argument visuel de l'intersection de la courbe $y = f(x)$ avec l'axe des abscisses.

énumération descriptive (jusqu'au début du 20e siècle) dans le Tome 12 de l'Encyclopédie des Sciences mathématiques, sous la plume de Netto et Le Vavasseur (p. 180 à 205) qui ajoutent ceci :

"Les démonstrations de ce théorème sont nombreuses. Elles diffèrent d'ailleurs ***essentiellement*** *suivant le point de vue auquel on se place, suivant la doctrine que l'on professe sur les fondements de l'Arithmétique. Suivant ce point de vue telle démonstration est rigoureuse ou ne l'est pas ; au point de vue arithmétique de L. Kronecker le théorème tel qu'on vient de l'énoncer n'est même pas exact (...). Au point de vue intuitif au contraire, ou lorsque l'on admet comme évident* ***a priori*** *qu'à chaque segment de droite correspond nécessairement un nombre déterminé, le théorème fondamental est, au moins relativement, assez facile à démontrer.*

Suivant que l'on suppose connue, ou non, la notion analytique du continu, suivant aussi que l'on estime, ou non, que toute démonstration doit fournir, pour être légitime, un procédé permettant de calculer au moyen des coefficients de $f(z)$ et avec telle approximation que l'on veut les racines (dont l'existence résulte alors, en dernière analyse, de ce procédé même) l'objet même de la démonstration du théorème fondamental sera changé."

Je vous propose dans l'article qui suit de revenir aux origines de cette réflexion en étudiant ce théorème à travers l'une de ses premières démonstrations, celle que Gauss a trouvée à l'âge de vingt ans et proposée comme dissertation doctorale à Helmstädt en 1799. Pourquoi celle-ci plutôt qu'une autre ? Parce qu'elle est la première à poser le problème de façon claire et précise, explicitant tout ce qui auparavant était admis de façon plus ou moins implicite, et dissipant le halo de mystère qui entourait et obscurcissait encore passablement les **nombres imaginaires** de cette époque, "*véritables ombres d'une ombre*" comme Gauss les qualifiera. Examinons successivement la figure et la personnalité de Gauss, puis la notion d'imaginaire au 18e siècle et les enjeux d'une démonstration du théorème fondamental de l'algèbre, avant de passer à l'étude effective de la démonstration de Gauss.

La figure de Gauss

Il est significatif que le premier chapitre des leçons que consacre Félix Klein au développement des mathématiques du 19e siècle [3] soit entièrement consacré à Gauss, et cela sur plus de soixante pages. Il s'en explique ainsi :

"*Gauss se situe à l'entrée du 19e siècle, pas seulement selon la chronologie ; il représente également le point de départ des multiples développements nouveaux de la science de cette époque. La considération de la grande personnalité de Gauss convient d'autant mieux à l'introduction du présent sujet que s'offre à nous, en cet homme, une remarquable et très heureuse jonction de l'esprit des deux époques au carrefour desquelles il se situe.*" Gauss effectivement peut apparaître comme un homme du 18e siècle dans ses aspects extérieurs, dans l'impression qu'il peut donner à ses contemporains :

- échanges sur des questions scientifiques sous la forme d'une abondante correspondance avec quelques hommes choisis, peu nombreux,

[3] Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert, Band 1.

- écriture en latin d'une grande partie de ses œuvres,

- travail aussi bien en mathématiques, en physique, en astronomie, en géodésie.

Mais Gauss est aussi une grande figure du 19^{e} siècle

- par ses thèmes de recherche et ses idées très novatrices,

- par la rigueur et la précision de ses textes scientifiques.

Cela est déjà particulièrement sensible dans la démonstration que nous allons étudier. Cette démonstration a été le sujet de la dissertation doctorale que Gauss a présentée à Helmstädt en 1799 sous la responsabilité de J. F. Pfaff (1765-1825) lequel a porté l'appréciation suivante sur le mémoire de Gauss :

"*Je ne puis juger que très favorablement ce travail car il est une preuve convaincante des aptitudes remarquables et des connaissances approfondies de son auteur, ce qui fait qu'après la publication prochaine de cette étude, le candidat comptera au nombre de ceux dont le grade fera honneur à notre faculté.*"

La notion d'imaginaire au 18^{e} siècle et les enjeux de la démonstration du théorème fondamental.

Pour bien comprendre l'enjeu théorique du théorème fondamental de l'algèbre au 18^{e} siècle, il est important de restituer son sens primitif au mot "*imaginaire*", sens à la fois plus large et plus mystérieux que le terme **nombre complexe** d'aujourd'hui (terme d'ailleurs introduit par Gauss). Le terme "*imaginaire*" est utilisé pour la première fois par Descartes en 1637 dans sa "*Géométrie*" :

"Au reste, tant les vraies racines que les fausses ne sont pas toujours réelles, mais quelquefois seulement imaginaires, c'est-à-dire qu'on peut toujours en imaginer autant que j'ai dit en chaque équation, mais qu'il n'y a quelquefois aucune quantité qui corresponde à celle qu'on imagine."

Et Girard, à qui nous devons la première formulation du théorème fondamental dans "*L'invention nouvelle en l'Algèbre*" (1629) :

"Toutes les équations d'algèbre reçoivent autant de solutions que la dénomination de la plus haute quantité le démontre (...). On pourrait dire : à quoi servent ces solutions qui sont impossibles ? Je réponds pour trois choses, pour la certitude de la règle générale, et qu'il n'y a point d'autres solutions et pour son utilité."

Le terme *impossible* sera longtemps synonyme d'imaginaire. Ainsi dans le dictionnaire de mathématiques de Klügel [4] (1836) : *"On appelle grandeur impossible ou imaginaire toute expression pour laquelle on ne peut pas trouver une grandeur réelle comme valeur, par exemple* Arc cos x *pour* $x > 1$*."*

[4] Mathematisches Wörterbuch V, p. 555.

Pourtant quelques années auparavant en 1830, un jeune mathématicien du nom de Galois donnait une signification beaucoup plus moderne et précise au terme imaginaire dans un court texte intitulé "*Sur la théorie des nombres*" [5]. Présentons les idées de Galois sur un exemple simplifié, celui des entiers modulo 3 c'est-à-dire l'ensemble $\mathbb{Z}/3\mathbb{Z}$ que nous désignerons par E. Dans cet ensemble, l'équation $x^2+1=0$ n'a pas de solution comme le montre aisément le tableau de valeurs suivant :

x	0	1	2
x^2+1	1	2	2

Introduisons alors avec Galois un nombre imaginaire i tel que $i^2 \equiv 2$ [modulo 3]. autrement dit une solution imaginaire de l'équation : $x \in E, x^2+1=0$.

"*Il faut* - explique Galois - *regarder les racines de cette congruence comme des espèces de symboles imaginaires (...) dont l'emploi dans le calcul sera souvent aussi utile que celui de l'imaginaire* $\sqrt{-1}$ *dans l'analyse ordinaire.*"

L'adjonction de i à notre ensemble E définit un nouvel ensemble F formé des éléments $a+ib$ où a et b parcourent E, dont la table de multiplication, limitée aux éléments non nuls est la suivante [6] :

$\bullet$	1	2	i	$2i$	$1+i$	$2+i$	$1+2i$	$2+2i$
1	1	2	i	$2i$	$1+i$	$2+i$	$1+2i$	$2+2i$
2	2	1	$2i$	i	$2+2i$	$1+2i$	$2+i$	$1+i$
i	i	$2i$	2	1	$2+i$	$2+2i$	$1+i$	$1+2i$
$2i$	$2i$	i	1	2	$1+2i$	$1+i$	$2+2i$	$2+i$
$1+i$	$1+i$	$2+2i$	$2+i$	$1+2i$	$2i$	1	2	i
$2+i$	$2+i$	$1+2i$	$2+2i$	$1+i$	1	i	$2i$	2
$1+2i$	$1+2i$	$2+i$	$1+i$	$2+2i$	2	$2i$	i	1
$2+2i$	$2+2i$	$1+i$	$1+2i$	$2+i$	i	2	1	$2i$

Le lecteur peut s'amuser à démontrer qu'avec cette adjonction de l'élément imaginaire i, l'équation $x \in \mathbb{F}, ax^2+bx+c=0$ a **toujours** une solution lorsque a,b,c appartiennent à E. De la même manière que l'équation $x \in \mathbb{C}, ax^2+bx+c=0$ a toujours une solution, lorsque a,b,c appartiennent à $\mathbb{R}$. Mais là où les choses changent totalement c'est dans la comparaison des équations :

$$\begin{array}{cc} x \in \mathbb{F}, ax^2+bx+c=0 & x \in \mathbb{C}, ax^2+bx+c=0 \\ (a,b,c) \in \mathbb{F}^3 & (a,b,c) \in \mathbb{C}^3. \end{array}$$

L'équation de gauche n'a pas toujours de solution. Par exemple, l'équation $a \in \mathbb{F}, x^2 = 1+i$ n'a pas de solution comme le montre l'examen des termes de la diagonale du tableau ci-dessus. On pourrait introduire un nouvel imaginaire I qui définirait une nouvelle extension $\mathbb{G}$ mais dans laquelle nous trouverions encore et toujours des équations du second degré sans racines. Au contraire, l'équation de droite a toujours des solutions. L'adjonction de $\sqrt{-1}$ clôt définitivement la situation en ce qui concerne la résolution des équations du second degré dans $\mathbb{C}$. Ceci nous le savons parce que nous

[5] Galois "Ecrits et Mémoires mathématiques", p. 114.

[6] $\mathbb{F}$ est un corps de Galois à neuf éléments, dont les éléments non nuls forment un groupe cyclique engendré par $1+i$.

disposons d'une démonstration du théorème fondamental, mais les savants du 18e siècle, eux, ne le savaient pas. La résolution des équations polynômes de degré au plus quatre avait mis en évidence que toutes les racines éventuelles pouvaient s'écrire sous la forme $A + B\sqrt{-1}$ avec A et B réels. Mais comme on ne savait pas résoudre en général les équations de degré supérieur à quatre par radicaux, on pouvait, on devait se poser la question : les racines de telles équations peuvent-elles aussi toujours s'écrire sous cette forme $A + B\sqrt{-1}$ ou bien fallait-il envisager encore d'autres types d'imaginaires, comme dans l'équation de gauche ci-dessus ?

On le voit, il y a une certaine ambiguïté dans la formulation de la question : s'agissait-il de prouver l'existence d'imaginaires, solutions d'une équation polynôme donnée quelconque, à coefficients réels, ou s'agissait-il simplement de prouver une certaine forme (en l'occurence $A + B\sqrt{-1}$) pour des racines dont l'existence n'est pas mise en doute ? Dans sa dissertation, Gauss commencera d'emblée par critiquer cette ambiguïté :

"*Certains auteurs* - écrit-il - *prennent en quelque sorte comme Axiome que toute équation admet effectivement des racines qui, à défaut d'être possibles, seront impossibles. Ce qu'ils veulent signifier par grandeurs possibles ou impossibles ils ne l'ont pas suffisamment ni clairement explicité. Si l'expression "grandeurs possibles" doit signifier la même chose que "réelles", "impossible" la même chose qu'"imaginaires" alors cette proposition ne peut en aucune façon être admise comme Axiome, mais exige nécessairement une démonstration. Cependant ces expressions ne semblent pas être prises dans ce sens ; l'axiome doit plutôt être compris dans le sens suivant* : "**Quoique nous ne soyons pas encore sûrs qu'il y a nécessairement** m **grandeurs réelles ou imaginaires qui satisfont à une quelconque équation donnée de degré** m**, nous voulons néanmoins admettre cela dans la suite ; car s'il devait arriver qu'on ne puisse pas trouver autant de grandeurs réelles ou complexes, l'issue nous reste pourtant ouverte de dire que les autres sont impossibles**". *Préconise-t-on d'utiliser une telle expression au lieu de dire simplement que l'équation n'a pas dans ce cas là autant de racines, je n'ai rien là contre ; mais si l'on en use comme si elles étaient effectives, et si l'on dit par exemple que la somme de toutes les racines de l'équation*

$$x^m + Ax^{m-1} + Bx^{m-2} + ... = 0 \text{ est } = -A$$

*bien qu'il s'en trouve parmi elles des "**impossibles**" (ce qui signifie en fin de compte quoiqu'il en manque quelques unes) je ne peux approuver cela. Car des racines impossibles acceptées dans ce sens là sont comme des racines, et alors le théorème ne peut en aucune façon être admis sans démonstration ; bien plus, on peut à ce propos se demander, s'il ne peut exister des équations qui n'auraient pas même des racines impossibles".*

Un second enjeu, plus pratique, allait stimuler les recherches des mathématiciens et modifier la position d'approche pour la résolution du problème. Le développement du calcul intégral posait en effet la question de l'intégration d'une fraction rationnelle et donc la question de la décomposition de celle-ci en éléments simples du type $\dfrac{A}{(x-a)^\alpha}$ ou $\dfrac{Ax+B}{(x^2+px+q)^n}$ où x^2+px+q est irréductible sur $\mathbb{R}$.

D'où la nouvelle formulation du problème: peut-on décomposer tout polynôme réel en facteurs soit réels linéaires $X - a$ et/ou quadratiques $x^2 + px + q$ soit linéaires complexes ? Il faut savoir qu'au 18e siècle la réponse à cette question était loin d'être unanime.

Dans un mémoire paru en 1702, Leibniz conjectura que cette factorisation n'était pas toujours possible. Comme argument, il donne l'exemple de la décomposition de

$$\begin{aligned} X^4 + a^4 &= (X^2 - a^2\sqrt{-1})(X^2 + a^2\sqrt{-1}) \\ &= (X + a\sqrt{\sqrt{-1}})(X - a\sqrt{\sqrt{-1}})(X + a\sqrt{-\sqrt{-1}})(X - a\sqrt{-\sqrt{-1}}) \end{aligned}$$

dont le dernier produit ne donnera jamais un facteur réel, quels que soient les deux facteurs que l'on regroupe. Leibniz ne semble pas être parvenu à l'idée que $\sqrt{\sqrt{-1}}$ peut aussi s'écrire sous la forme $a + b\sqrt{-1}$ car alors on a avec

$$\begin{aligned} \sqrt{\sqrt{-1}} &= \frac{1}{2}\sqrt{2}(1 + \sqrt{-1}) \text{ et } \sqrt{-\sqrt{-1}} = \frac{1}{2}\sqrt{2}(1 - \sqrt{-1}) \\ X^4 + a^4 &= (X^2 + a\sqrt{2}X + a^2)(X^2 - a\sqrt{2}X + a^2) \end{aligned}$$

Dans une lettre à Nicolas Bernoulli datée du 1er novembre 1742, Euler formule un théorème de factorisation des polynômes réels exactement dans la forme que Leibniz tenait pour fausse. Contredisant Bernoulli qui proposait le contre exemple :

$$X^4 - 4X^3 + 2X^2 + 4X + 4$$

Euler démontre que ce polynôme se décompose en produit de deux polynômes réels :

$$[X^2 - (2 + a)X + 1 + \sqrt{7} + a][X^2 - (2 - a)X + 1 + \sqrt{7} - a] \text{ où } a = \sqrt{4 + 2\sqrt{7}}.$$

Quelques jours plus tard, le 15 décembre 1742, dans une lettre à Goldbach, Euler renouvelle la formulation de son théorème en ajoutant qu'il n'a pas pu jusqu'à présent le démonter complètement, mais seulement "*à peu près*" comme certains théorèmes de Fermat. Dans cette lettre il mentionne également que l'on peut regrouper les racines imaginaires d'un polynôme réel en paires, de façon qu'en multipliant les facteurs linéaires correspondant on trouve des facteurs réels de second degré. Goldbach reste sceptique face à ces affirmations et propose un nouveau contre exemple : $X^4 + 72X - 20$ qu'Euler factorise aussitôt.

Concluons cette première partie, en faisant le point sur la situation où se trouvait la communauté mathématique au moment où le jeune Gauss commençait ses réflexions. Peu à peu, à force de calculer formellement avec $\sqrt{-1}$ les mathématiciens se sont familiarisés avec les nombres imaginaires au point de les adopter dans la famille des autres nombres entiers, rationnels, réels. Ne rencontrant jamais dans leurs résolutions d'équations d'autres expressions que celles qui sont réductibles à des composés de réels avec $\sqrt{-1}$, ils en vinrent à la conviction que tous les imaginaires pourraient toujours s'écrire ainsi. Enfin des problèmes théoriques et pratiques comme l'intégration des fractions rationnelles nécessitaient une réponse urgente à la question : peut-on toujours ramener cette intégration à celle de fractions élémentaires par la décomposition du dénominateur en produit de facteurs réels du premier ou du second degré ? C'est sous cette forme que Gauss va attaquer le problème, en intitulant sa dissertation :

"*Nouvelle démonstration du théorème : toute fonction algébrique entière d'une variable est décomposable en facteurs réels du premier ou du second degré.*"

Texte de vingt-cinq pages, les deux tiers sont consacrés à la critique des démonstrations de ses illustres prédessesseurs : Euler, d'Alembert, Lagrange, ce qui manifeste à la fois une connaissance parfaite de la science de son temps et une vision très claire et assurée de ce qu'elle doit être [7]. Nous nous limiterons ici à la démonstration propre de Gauss, dont voici les articulations principales.

La démonstration de Gauss

Dans un premier temps, Gauss ramène le problème à la démonstration du théorème suivant :

Théorème : Soit $X = x^m + Ax^{m-1} + Bx^{m-2} + ... + Lx + M$. S'il existe r et φ tels que simultanément

$$\begin{array}{ll} (1) & r^m \cos m\varphi + Ar^{m-1}\cos(m-1)\varphi + ... + Lr\cos\varphi + M \quad = U \quad = 0 \\ (2) & r^m \sin m\varphi + Ar^{m-1}\sin(m-1)\varphi + ... + Lr\sin\varphi \qquad\qquad = T \quad = 0 \end{array}$$

alors on a la propriété (p) : X est divisible par $x^2 - 2rx\cos\varphi + r^2$ ou par $x - r\cos\varphi$ selon que $r\sin\varphi$ est différent de 0 ou non.

On dira que c'est tout simplement les parties réelles et imaginaires de X qui sont annulées séparément dans les relations (1) et (2). Mais Gauss veut éviter tout recours aux imaginaires et déduit la proposition (p) des égalités (1) et (2) au moyen du lemme suivant dont nous laissons la vérification au lecteur :

Lemme : Pour tout entier naturel m non nul

$$\sin\varphi x^m - \sin m\varphi . r^{m-1}x + \sin(m-1)\varphi . r^m \text{ est divisible par } x^2 - 2\cos\varphi rx + r^2.$$

Pour déduire (p) de (1) et (2), il suffit alors d'appliquer le lemme aux valeurs successives $m, m-1, m-2, ...$, en multipliant successivement par les coefficients $A, B, C, ...$ du polynôme X de la façon suivante :

$$\begin{array}{ccc} \sin\varphi . rx^m & -\sin m\varphi . r^m x & +\sin(m-1)\varphi . r^{m+1} \\ A\sin\varphi . x^{m-1} & -A\sin(m-1)\varphi . r^{m-1}.x & +A\sin(m-2)\varphi . r^m \\ B\sin\varphi . rx^{m-2} & -B\sin(m-2)\varphi . r^{m-2}.x & +B\sin(m-3)\varphi . r^{m-1} \\ \cdots & \cdots & \cdots \\ K\sin\varphi . rx^2 & -K\sin 2\varphi . r^2 x & +K\sin\varphi r^3 \\ L\sin\varphi . rx & -L\sin\varphi . rx & \\ M\sin\varphi . r & & -M\sin\varphi . r \end{array}$$

dont chaque ligne est divisible par $x^2 - 2rx\cos\varphi + r^2$.

Additionnons colonnes par colonnes toutes ces expressions, nous obtenons

[7] Il n'existe pas de traduction française du texte de Gauss (rappelons qu'il écrivait en latin). Je tiens à la disposition du lecteur curieux ma propre traduction française non publiée, réalisée à partir de la version allemande de E. Netto.

- pour la première colonne $Xr\sin\varphi$,

- pour la seconde zéro, en vertu de (2),

- pour la troisième zéro par combinaison linéaire de (2) $\times \cos\varphi -$ (1) $\times \sin\varphi$.

En conséquence :

- ou bien $r\sin\varphi \neq 0$ alors X est divisible par $x^2 - 2rx\cos\varphi + r^2$,

- ou bien $r\sin\varphi = 0$ donc soit $r = 0$ alors $M = 0$ à cause de (1) donc X est divisible par x et par $x - r\cos\varphi$, soit $\sin\varphi = 0$ alors $\cos\varphi = \pm 1$ et $\cos m\varphi = (\cos\varphi)^m$, done X s'annule pour la valeur $r.\cos\varphi$ et est divisible par $x - r.\cos\varphi$.

Reste à démontrer l'existence de r et φ tels que l'on ait les égalités (1) et (2). Cette démonstration va se faire en quatre étapes.

1. Les égalités $T = 0$ et $U = 0$ définissent chacune une courbe algébrique possédant au total, et de façon alternée, $4m$ branches infinies correspondant aux valeurs $\varphi = \dfrac{p\pi}{2m}$, $0 \leq p \leq 4m - 1$.

En considérant r et φ comme coordonnées polaires, les premiers membres de (1) et (2) définissent deux surfaces

$$(r,\varphi) \longmapsto z = U(r,\varphi) \quad \text{et}(r,\varphi) \longmapsto z = T(r,\varphi).$$

Ces surfaces sont coupées par le plan de base $z = 0$ selon des courbes $U(r,\varphi) = 0$ et $T = (r,\varphi) = 0$.

a) Il est facile de vérifier que ces intersections ne sont pas vides. Par exemple pour $U(r,\varphi) = r^m\cos m\varphi + Ar^{m-1}\cos(m-1)\varphi + ... + M$ on peut prendre r suffisamment grand pour que $r^m\cos m\varphi$ dépasse en valeur absolue la somme de tous les autres termes, et alors pour une valeur convenable de φ, ce terme peut être rendu aussi bien positif que négatif. Remarquons que la courbe $T = 0$ contient de toute façon l'axe des abscisses puisque $\sin\varphi$ est en facteur.

b) Ces courbes sont algébriques car en posant $x = r\cos\varphi, y = r\sin\varphi, r^n\cos n\varphi$ et $r^n\sin n\varphi$ sont des polynômes en (x,y).

c) Ces courbes ont des branches infinies définies respectivement par

$$\cos m\varphi = 0 \ \text{ ou } \ ou \ \ \varphi = \frac{\pi}{2m} + \frac{k\pi}{m} \quad \text{et} \quad \sin m\varphi = 0 \quad \text{ou} \quad \varphi = \frac{k\pi}{m}$$

soit au total $4m$ branches pour avec $0 \leq p \leq 4m - 1$.

2. Il existe un cercle (Γ) contenant $2m$ points de $T = 0$ et $2m$ points de $U = 0$; chacun des points de la seconde famille est situé entre deux points de la première.

Soit $S = |A| + |B| + ... + |M|$ et (Γ) le cercle de rayon R, $R > \sup(S\sqrt{(}2), 1)$. Notons $(2k+1)$ le point de (Γ) correspondant à $\varphi = \dfrac{2k+1}{m} \times \dfrac{\pi}{4}$ pour $0 \leq k \leq 4m-1$ et étudions la valeur de T sur Γ. On a :

$$T = R^{m-1}\left[R\sin(m\varphi) + A\sin(m-1)\varphi + \frac{B}{R}\sin(m-2)\varphi + ... + LR^{m-2}\sin\varphi\right].$$

Au point (1) on a $T = R^{m-1}\left[R\sqrt{\frac{1}{2}} + E\right]$ avec $|E| < S < R\sqrt{\frac{1}{2}}$. T reste donc positif sur tout l'intervalle [(1) - (3)] car $\sin(m\varphi) > \sqrt{\frac{1}{2}}$ car $\sin(m\varphi) < -\sqrt{\frac{1}{2}}$. De même T reste négatif sur tout l'intervalle [(5) - (7)] car $\sin(m\varphi) < -\sqrt{\frac{1}{2}}$. T s'annule par conséquent entre (3) et (5), et pour des raisons analogues entre (7) et (9),... entre $(8m-1)$ et (1). On démontrerait de la même manière que U s'annule entre (1) et (3), (5) et (7), ..., $(8m-3)$ et $(8m-1)$. Par ailleurs, l'étude du signe des dérivées $\dfrac{dU}{d\varphi}$ et $\dfrac{dT}{d\varphi}$ permet d'affirmer que chaque intervalle ne contient qu'un seul point où U (respectivement T) s'annule.

Numérotons alors les points d'intersection : nombre pair pour (T), nombre impair pour (U), au total $2 \times 2m$ points notés

$$T_0, U_1, T_2, U_2, T_{2m-1}, U_{2m}.$$

3. Tout point pair est relié à un point pair par une branche de (T) et tout point impair est relié à un point impair par une branche de (U), ces branches étant situées à l'intérieur de (Γ).

Les arguments donnés par Gauss sont de nature topologique, mais restent ici purement d'intuition géométrique : "*on sait par la géométrie supérieure que toute courbe algébrique (ou toute partie d'une courbe algébrique, s'il arrive que celle-ci soit composée de plusieurs branches mises ensemble) ou bien revient sur elle-même, ou bien s'en va à l'infini des deux côtés et que par conséquent, si une branche d'une courbe algébrique pénètre dans un espace délimité, nécessairement elle doit de nouveau ressortir de cet espace*". Ces arguments ne semblent d'ailleurs pas le satisfaire complètement, car dans une longue note (note 12), il explique que "*si quelqu'un le demande, il entreprendra à une autre occasion de fournir une démonstration qui ne puisse être soumise à aucun doute*" et que "*cette conclusion s'appuie sur les principes de la géométrie de position* [8] *lesquels ne sont pas moins susceptibles de démonstration que les principes de la géométrie des grandeurs*".

[8] ce que nous appelons aujourd'hui topologie (ndlr).

4. Conclusion : la courbe (U) coupe nécessairement la courbe (T), à l'intérieur de (Γ).

Supposons en effet que les deux courbes ne se coupent pas. Or le point O est relié au point $2m$.

Le point 1 sera relié à un point $n < 2m$.

Le point 2 à un point $n' < n$.

Le point 3 à un point $n'' < n'$.

On arrivera nécessairement à la situation où un point h est relié à $(h+2)$.

Alors la courbe issue de $(h+1)$ ne peut que couper l'une des branches déjà utilisées qui relient les couples précédents.

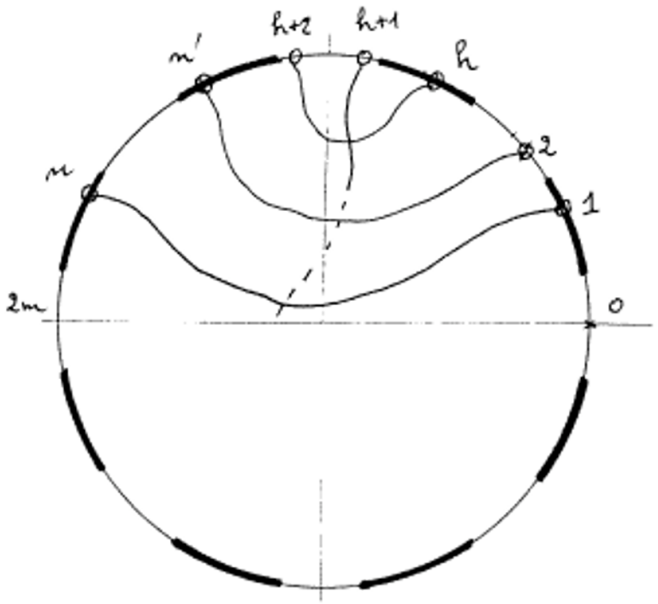


FIGURE 1

Nous avons illustré la démarche de Gauss par l'exemple de l'équation

$$X^7 + 28X^4 - 480 = 0$$

Alors

$$U = x^7 - 21x^6y^2 + 28x^4 + 35x^3y^4 - 7xy^6 + 28y^4 - 168x^2y^2 - 480 = 0 \quad \text{(fig.2)}$$
$$\text{et } T = y^7 - 21x^2y^5 + 35x^4y^3 - 7x^6y + 112x^3y - 112xy^3 = 0 \quad \text{(fig.3)}$$

L'intersection est matérialisée sur la figure de couverture et visualise les sept racines : trois racines réelles

$$x_1 = 1,9228841 \ ; \ x_2 = -2,4580892 \ ; \ x_3 = -2,5778036$$

et deux couples de racines complexes conjuguées

$$x_4, x_5 = 1,6843159 \pm 2,6637914i \text{ et } x_6, x_7 = -0,1278113 \pm 1,9874234i.$$

Gauss n'a pas illustré sa démonstration par cette équation. L'exemple est néanmoins de lui, pris dans un autre texte [9] qui correspond à une autre démonstration du théorème fondamental de l'algèbre. Ce sera la quatrième qu'il donnera de ce théorème. C'est dire que le sujet lui tenait à cœur. La seconde partie de ce texte donne alors un algorithme de résolution sur $\mathbb{C}$ des équations de la forme $x^{m+n} \pm ex^m \pm f = 0$ avec en particulier la résolution de l'exemple ci-dessus

$$x^7 + 28x^4 - 480 = 0$$

Mais ceci est une autre histoire. Le problème donné dans la rubrique "Problèmes pour nos élèves" reprend les principales idées de Gauss adaptées à un cas simple et donne une méthode de factorisation du polynôme $x^4 + ax + b$ pour a, b réels quelconques (voir la rubrique "Problèmes pour nos élèves").

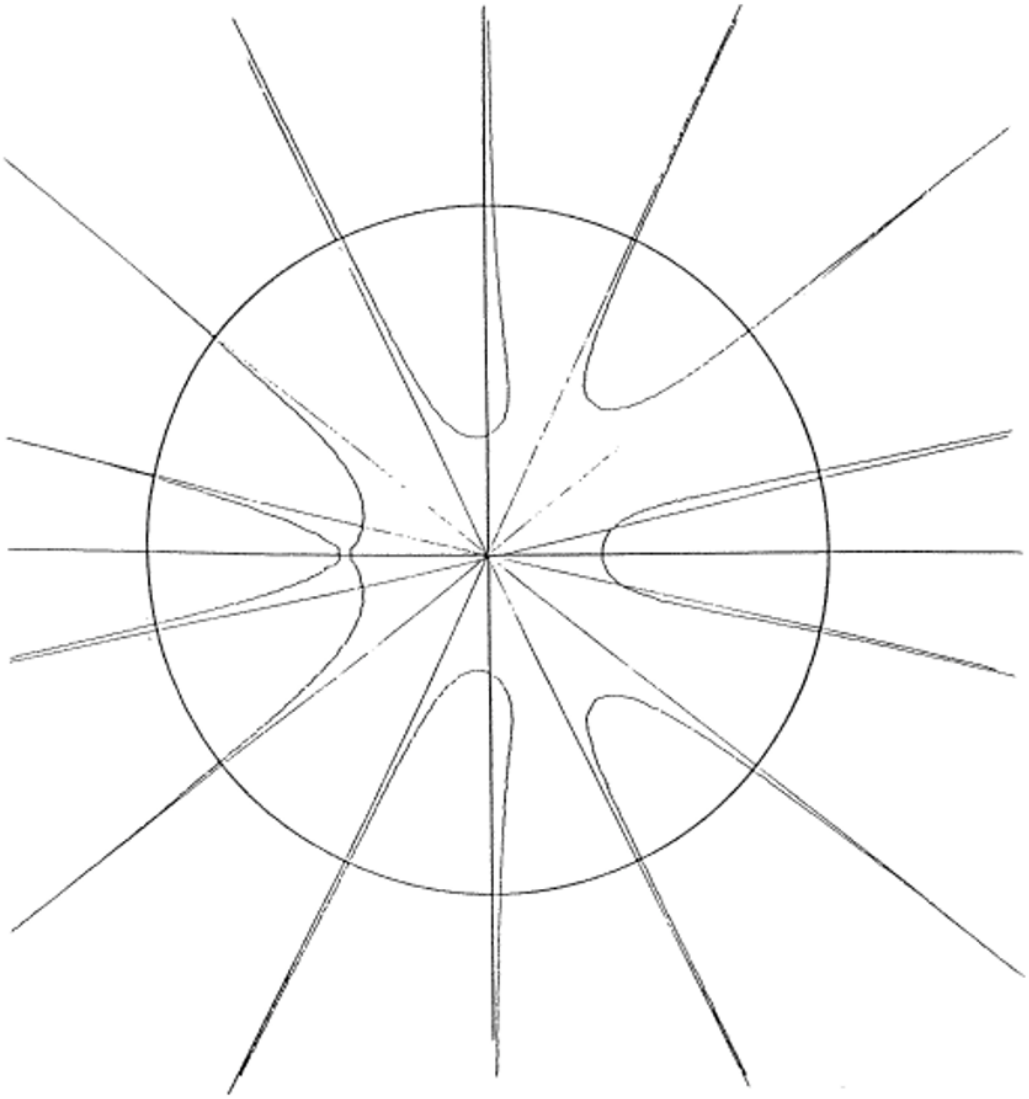


FIGURE 2

[9] Beiträge zur Theorie der algebraischen Gleichungen, 1649, Gauss Werke Band III, p. 72 à 102.

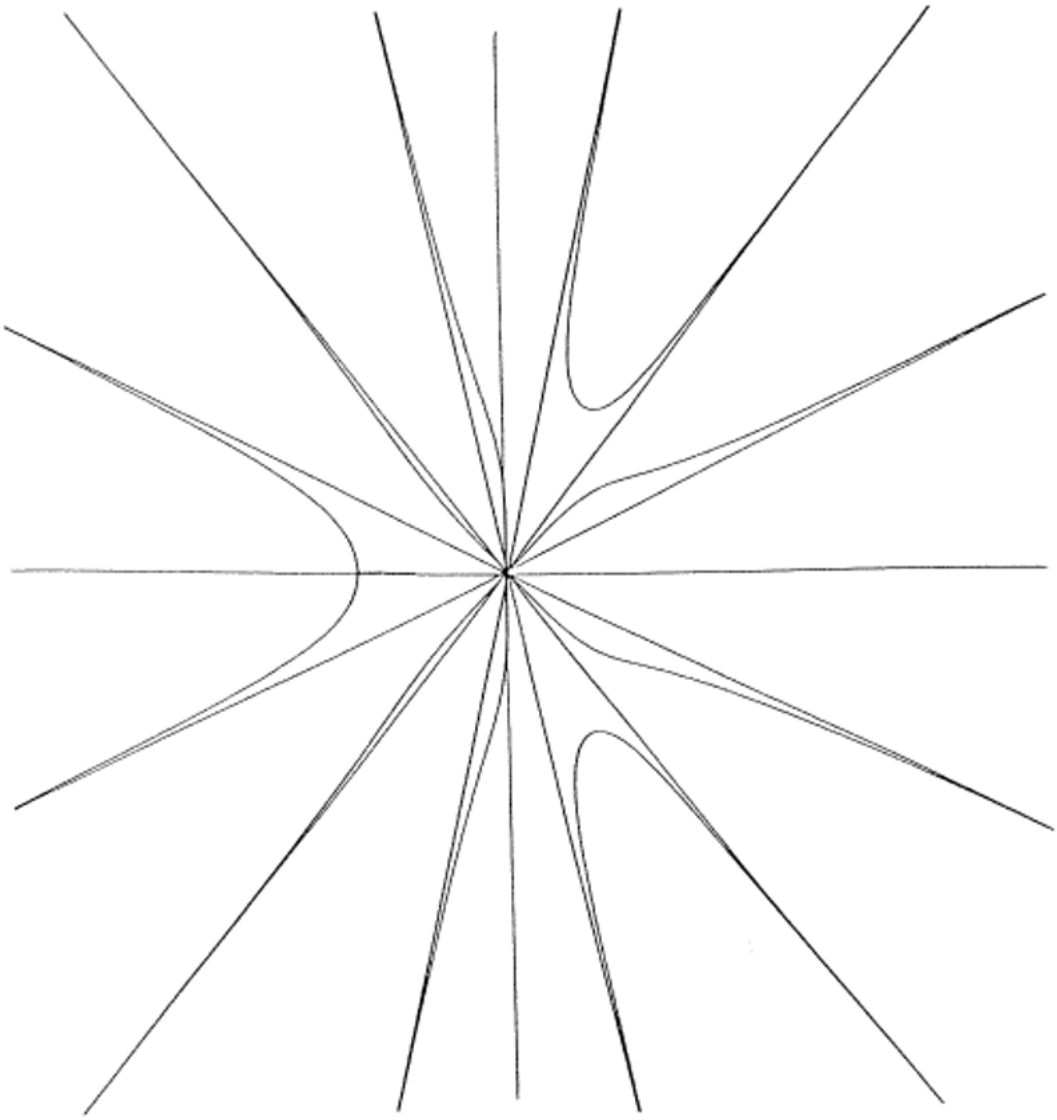


FIGURE 3

Briser les symétries, Denise Vella-Chemla, 15 octobre 2024

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.

On présente ici les résultats d'un programme python qui semblent permettre de distinguer de façon sûre les nombres qui sont des décomposants de Goldbach d'un nombre pair n des nombres qui n'en sont pas.

On rappelle le petit théorème de Fermat :

> *Soit p un nombre premier et soit $a \in \mathbb{N}$.*
>
> *Si a est premier à p (*$\text{pgcd}(a,p) = 1$*) alors* $a^{p-1} \equiv 1 \pmod{p}$.

On décide de tester par programme les puissances intervenant dans le petit théorème de Fermat, de façon systématique, pour trois nombres qui sont particularisés par l'énoncé de la conjecture de Goldbach : ces nombres sont :

- d'une part a et b, avec a un nombre impair inférieur à la moitié de n, le nombre pair à décomposer, et b, son complémentaire à n : $b = n - a$;
- d'autre part, c le nombre égal à la moitié de n puisque n est pair.

On calcule les valeurs :

- des puissances b^{a-1} et c^{a-1} dans $\mathbb{Z}/a\mathbb{Z}$;
- des puissances a^{b-1} et c^{b-1} dans $\mathbb{Z}/b\mathbb{Z}$;
- et des puissances a^{c-1} et b^{c-1} dans $\mathbb{Z}/c\mathbb{Z}$.

On constate, ce qui découle du petit théorème de Fermat, que pour n, un nombre pair double d'un nombre composé : *si 4 au moins des 6 puissances calculées ci-dessus sont égales à 1, et si les 2 seules puissances différentes de 1 (parmi les 6) sont les puissances* a^{b-1} *et* c^{b-1}*, (*$b-1$ *est composé) alors a et b sont deux nombres premiers, i.e. $n = a + b$ est une décomposition de Goldbach de n.*

Il faudrait être capable de démontrer que deux nombres vérifiant toutes ces contraintes existent toujours quel que soit n.

Pour résumer, on cherche à savoir s'il existe toujours un nombre x impair compris entre 3 et $\frac{n}{2}$ tel que :

$$\begin{cases} x^{(\frac{n}{2}-1)} & \not\equiv 1 \pmod{\frac{n}{2}} \\ (n-x)^{(\frac{n}{2}-1)} & \not\equiv 1 \pmod{\frac{n}{2}} \\ \left(\frac{n}{2}\right)^{x-1} & \equiv 1 \pmod{x} \\ (n-x)^{(x-1)} & \equiv 1 \pmod{x} \\ x^{(n-x-1)} & \equiv 1 \pmod{n-x} \\ \left(\frac{n}{2}\right)^{n-x-1} & \equiv 1 \pmod{n-x} \end{cases}$$

car ceci est la caractérisation par le petit théorème de Fermat du fait que x et $n-x$ sont premiers et fournissent une décomposition de Goldbach de n.

On remarque également par programme qu'il existe quasiment toujours une décomposition de Goldbach $x+(n-x)$ de n telle que $n-x$ est une racine primitive de x mais cela ne nous permet pas de fournir une explication de l'existence obligatoire d'une décomposition de Goldbach pour autant car les congruences ont lieu dans trois anneaux différents que l'on ne parvient pas à relier.

Annexe 1 : texte python du programme

```
def prime(atester):
      k = 2
      if atester in [0, 1]:  return False
      if atester in [2, 3, 5, 7]:  return True
      while True:
            if k * k > atester:  return True
            else:
                  if atester % k == 0:  return False
                  else:  k = k + 1

for n in range(6,104,2):
      if not prime(n/2):
            print(':::::::::',n)
            print('les dg ')
            for x in range(3,n//2+2,2):
                  if prime(x) and prime(n-x):
                        print(x,' --> ')
                        a = x
                        b = n//2
                        c = n-x
                        print(b,'b**(a-1) mod a ',(b**(a-1))%a)
                        print(c,'c**(a-1) mod a ',(c**(a-1))%a)
                        print(a,'a**(b-1) mod b ',(a**(b-1))%b)
```

```
                    print(c,'c**(b-1) mod b ',(c**(b-1))%b)
                    print(a,'a**(c-1) mod c ',(a**(c-1))%c)
                    print(b,'b**(c-1) mod c ',(b**(c-1))%c)
          print('non dg ')
          for x in range(3,n//2+2,2):
               if not prime(x) or not prime(n-x):
                    print(x,' --> ')
                    a = x
                    b = n//2
                    c = n-x                                   print(b,'b**(a-1) mod a
',(b**(a-1))%a)
                    print(c,'c**(a-1) mod a ',(c**(a-1))%a)
                    print(a,'a**(b-1) mod b ',(a**(b-1))%b)
                    print(c,'c**(b-1) mod b ',(c**(b-1))%b)
                    print(a,'a**(c-1) mod c ',(a**(c-1))%c)
                    print(b,'b**(c-1) mod c ',(b**(c-1))%c)
```

Annexe 2 : calcul des 6 puissances pour les nombres pairs doubles d'un nombre composé

```
::::::::: 8
les dg
3 -->
4 b**(a-1) mod a 1
5 c**(a-1) mod a 1
3 a**(b-1) mod b 3
5 c**(b-1) mod b 1
3 a**(c-1) mod c 1
4 b**(c-1) mod c 1
5 -->
4 b**(a-1) mod a 1
3 c**(a-1) mod a 1
5 a**(b-1) mod b 1
3 c**(b-1) mod b 3
5 a**(c-1) mod c 1
4 b**(c-1) mod c 1
les non dg

::::::::: 12
les dg
5 -->
6 b**(a-1) mod a 1
7 c**(a-1) mod a 1
5 a**(b-1) mod b 5
7 c**(b-1) mod b 1
5 a**(c-1) mod c 1
6 b**(c-1) mod c 1
```

Petite note provoquée par une conférence à l'Académie des Sciences au sujet, entre autres, des équations du troisième degré, Denise Vella-Chemla, octobre 2024.

Je raconte une incompréhension totale, au sujet des racines cubiques complexes. Lors d'une séance publique à l'Académie des Sciences en février 2024

$$https://alainconnes.org/fr/2024/02/mathematiques-et-imagination/,$$

Alain Connes a proposé le problème suivant [1].

En utilisant la formule du binôme :

$$(u+v)^3 = 3uv(u+v) + u^3 + v^3 \iff (u+v)^3 - 3uv(u+v) - u^3 - v^3 = 0,$$

déterminer à quoi correspond le nombre : $a = \sqrt[3]{\sqrt{108}+10} - \sqrt[3]{\sqrt{108}-10}$.

On pose $u = \sqrt[3]{\sqrt{108}+10}$ et $v = -\sqrt[3]{\sqrt{108}-10}$, on a $uv = -2$ (en appliquant l'identité remarquable $(a+b)(a-b) = a^2 - b^2$) et $u^3 + v^3 = 20$ (on ajoute simplement les radicandes).

$u+v$ est donc solution de $x^3 + 6x - 20 = 0$ et le nombre a qu'on cherche est la solution réelle de cette équation du troisième degré.

On utilise le programme suivant pour voir :

```
import sympy as sp

x = sp.symbols('x')
eq1deg3 = x**3 + 6*x - 20
solutions1 = sp.solve(eq1deg3, x)
print('solutions eq.  deg.3 :  ',solutions1)
```

Ce programme a comme résultat :

```
solutions eq.  deg.3 :  [2, -1 - 3*I, -1 + 3*I]
```

et ô, merveille, $a = 2$ (la racine cubique réelle de 8, qu'on reconnaît, cachée dans l'identité remarquable $(\sqrt{108}-10)(\sqrt{108}+10)$).

On vérifie par exemple que $2^3 + 6 \times 2 - 20 = 0$ ou que :

$$\begin{aligned}(-1-3i)^3 + 6(-1-3i) - 20 &= (1+6i-9)(-1-3i) - 6 - 18i - 20 \\ &= (-8+6i)(-1-3i) - 6 - 18i - 20 \\ &= 8 - 6i + 24i + 18 - 6 - 18i - 20 = 0\end{aligned}$$

ou enfin que

$$\begin{aligned}(-1+3i)^3 + 6(-1+3i) - 20 &= (1+6i-9)(-1+3i) - 6 + 18i - 20 \\ &= (-8-6i)(-1+3i) - 26 + 18i \\ &= 26 - 18i - 26 + 18i = 0\end{aligned}$$

[1] Voir transcription de la conférence ici https://denisevellachemla.eu/transc-Alain-Connes-Academie-2024.pdf, p. 2.

Deuxième exercice dans la même veine : déterminer à quoi correspond le nombre :

$$b = \sqrt[3]{4+\sqrt{-11}} - \sqrt[3]{4-\sqrt{-11}} \quad ?$$

L'équation du troisième degré à résoudre est $x^3 - 9x + 2\sqrt{-11} = 0$.

Le programme renvoie :

```
solutions eq.  2 deg.3 :
             [ -4.01e-17 + 2.52433779896214*I,
               -1.69e-17 - 3.3166247903554*I,
               5.71e-17 + 0.792286991393261*I]
```

mais on ne voit pas ce que ces nombres ont de surprenant..., si ce n'est qu'on a affaire à trois multiples de i, un peu comme si une courbe (serpentine à deux méandres) du troisième degré se trouvait tournée d'un quart de tour horaire, par exemple ; mais alors, à une même abscisse correspondraient de multiples ordonnées, ou, dit autrement, un même point aurait plusieurs images différentes, ça remet en cause tout ce qu'on a appris.

L'essentiel est de commencer à comprendre (un peu) que ça tourne. Merci !

Voici l'incompréhension :

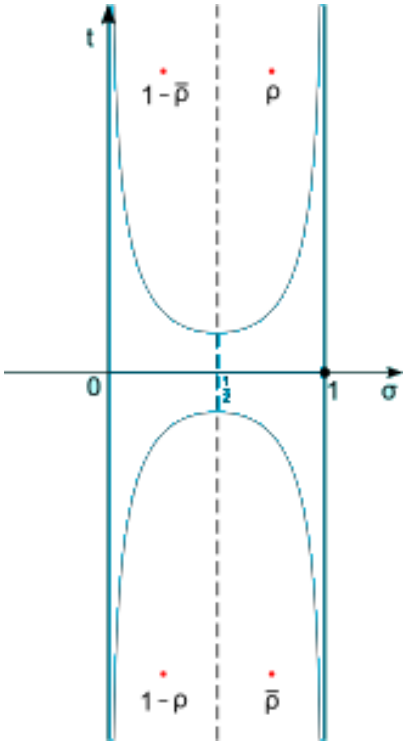
dans le livre de Gustave Verriest "Leçons sur la théorie des équations selon Galois", le problème de l'indiscernabilité des racines est bien présenté[2] par l'exemple suivant : un tour ou deux tours (2π ou 4π) sont égaux sur le cercle unité (congrus modulo 2π), ils ramènent au point 1 (du plan complexe, car $e^{2i\pi} = 1$).

Pourtant, si on divise 360 par 3, on obtient 120° (ou j), qui n'est pas identique sur le cercle-unité à 720°/3, égal à 240° (ou j^2). Ce sont deux racines de l'unité, c'est vrai, mais cependant, en divisant les 2 angles qui sont égaux modulo 2π, on devrait tomber sur le même point du cercle-unité, non ?... Incompris.

[2] je ne retrouve plus la page

Deux par deux, Denise Vella-Chemla, novembre 2024

On s'inspire de cette image présentant une propriété de la fonction zeta, qui est que si un nombre complexe ρ est un zéro de ζ, i.e. est tel que $\zeta(\rho) = 0$, alors $\bar{\rho}, 1-\bar{\rho}$ et $1-\rho$ sont eux-aussi des zéros de ζ.



On cherche un polynôme qui s'annule pour $z, 1-z, \bar{z}, 1-\bar{z}$.

On essaie avec les 4 nombres complexes $0.2+0.6i, 0.2-0.6i, 0.8+0.6i, 0.8-0.6i$. Le polynôme que ces 4 complexes annulent est

$$x^4 - 2x^3 + 2.04x^2 - 1.04x + 0.4.$$

Les coefficients, surprenants au premier abord, sont, à leur habitude, la somme des 4 complexes, la somme de leurs produits pris deux par deux, trois par trois, ou produit de tous. On calcule les coefficients du polynôme de façon générale en posant :

$$\begin{aligned} z &= a + bi \\ \bar{z} &= a - bi \\ 1 - z &= (1-a) + bi \\ 1 - \bar{z} &= (1-a) - bi \end{aligned}$$

et $P = x^4 + S_1 x^3 + S_2 x^2 + S_3 x + S_4$

Calculons ces sommes dans le cas général pour un quadruplet de zéros :

$$\begin{aligned} S_1 &= (a+bi)+(a-bi)+((1-a)+bi)+((1-a)-bi) \\ &= 2 \end{aligned}$$

$$\begin{aligned} S_2 &= (a+bi)(a-bi)+(a+bi)((1-a)+bi)+(a+bi)((1-a)-bi) \\ &\quad +(a-bi)((1-a)+bi)+(a-bi)((1-a)-bi) \\ &\quad +((1-a)+bi)((1-a)-bi) \\ &= -2a^2+2a+2b^2+1 \end{aligned}$$

$$\begin{aligned} S_3 &= (a+bi)(a-bi)((1-a)+bi)+(a+bi)(a-bi)((1-a)-bi) \\ &\quad +(a+bi)((1-a)+bi)((1-a)-bi)+(a-bi)((1-a)+bi)((1-a)-bi) \\ &= -2a^2+2a+2b^2 \end{aligned}$$

$$\begin{aligned} S_4 &= (a+bi)(a-bi)((1-a)+bi)((1-a)-bi) \\ &= a^4-2a^3+2a^2b^2+a^2-2ab^2+b^4+b^2 \end{aligned}$$

On a abouti à cette équation polynomiale générale :

$$x^4-2x^3+(-2a^2+2a+2b^2+1)x^2-(-2a^2+2a+2b^2)x+(a^4-2a^3+2a^2b^2+a^2-2ab^2+b^4+b^2)=0$$

Puis, on utilise le petit programme ci-après pour retrouver des solutions imposées $0.2+6i, 0.8+6i, 0.2+6i, 0.2-6i$ autour de la droite critique. On trouve bien un discriminant nul pour une équation pour laquelle on impose $a=0.5$. On ne comprend pas pourquoi on ne parvient pas à imposer une solution de partie imaginaire la partie imaginaire du premier zéro non trivial de ζ et obtenir pour cette valeur, comme pour la valeur $b=6$ un discriminant nul ; à vrai dire, il y a une erreur sur les solutions trouvées à partir d'une certaine décimale, ce qui fait trouver 4 solutions au lieu de 2.

```
import sympy as sp

x = sp.symbols('x')
aa=0.5
bb=14.134725141734693790457251983562 5
bb = 6
equationgenerale = x**4-2*x**3+(-2*(aa**2)+2*aa+2*(bb**2)+1)*x**2
                      -(-2*(aa**2)+2*aa+2*(bb**2))*x+(aa**4-2*(aa**3)
                      +2*(aa**2)*(bb**2)+aa**2-2*aa*(bb**2)+bb**4+bb**2)
solution = sp.solve(equationgenerale)
print(len(solution))
for k in range(len(solution)):
     print(solution[k].evalf())
```

```
a = 1
b = -2
c = -2*(aa**2)+2*aa+2*(bb**2)+1
d = -(-2*(aa**2)+2*aa+2*(bb**2))
e = aa**4-2*(aa**3)+2*(aa**2)*(bb**2)+aa**2-2*aa*(bb**2)+bb**4+bb**2
equationdeg4 = a*(x**4)+b*(x**3)+c*(x**2)+d*x+e
discrim = 256*(a**3)*(e**3)-128*(a**2)*(c**2)*(e**2)-4*(b**3)*(d**3)+16*a*(c**4)*e
          -4*a*(c**3)*(d**2)-192*(a**2)*b*d*(e**2)-27*(b**4)*(e**2)-6*a*(b**2)*(d**2)*e
          +144*a*(b**2)*c*(e**2)+144*(a**2)*c*(d**2)*e-80*a*b*(c**2)*d*e+18*(b**3)*c*d*e
          +18*a*b*c*(d**3)+(b**2)*(c**2)*(d**2)-4*(b**2)*(c**3)*e-27*(a**2)*(d**4)
print('a = ',a,' b = ',b,' c = ',c,' d = ',d,' e = ',e,' discrim = ',discrim)
```

Résultats du programme :

pour solutions imposées de parties imaginaires 6 *ou* -6 *:*

```
C:\Users\Denise_Vella\Desktop>python sottien.py
4
0.2 - 6.0*I
0.2 + 6.0*I
0.8 - 6.0*I
0.8 + 6.0*I
a =  1  b =  -2  c =  73.32  d =  -72.32  e =  1320.5056  discrim =  56004604.22572017

C:\Users\Denise_Vella\Desktop>python sottien.py
2
0.5 - 6.0*I
0.5 + 6.0*I
a =  1  b =  -2  c =  73.5  d =  -72.5  e =  1314.0625  discrim =  0.0
```

pour solutions imposées de parties imaginaires $14.134725141734693790457251983562 5$ [1]*:*

```
C:\Users\Denise_Vella\Desktop>python sottien.py
4
0.5 - 14.1347254235299*I
0.5 - 14.1347248599395*I
0.5 + 14.1347248599395*I
0.5 + 14.1347254235299*I
a =  1  b =  -2  c =  401.08090966477374  d =  -400.08090966477374  e =  40016.183569548215  discrim =  -1.81689453125
```

[1] voir cette page : https://www.lmfdb.org/zeros/zeta/?limit=100000N=1.

On a également regardé ce qui se passe si on choisit $a = 0.5$ et $b = Z[k]$ avec $Z[k]$ les valeurs des parties imaginaires des zéros non triviaux de la fonction ζ. On conserve les coefficients des équations qui ont chacune comme solution un zéro et son conjugué, coefficients calculés par curiosité (on ne note pas le coefficient $a = 1$ et $b = -2$) mais cela n'a pas d'intérêt.

z	c	d	e
14.1347251417	401.080909664774	400.080909664774	40016.1835695482
21.0220396387	885.352301148165	884.352301148165	195519.748136514
25.0108575801	1252.58599378866	1251.58599378866	391616.874961988
30.4248761258	1852.84617454779	1851.84617454779	857333.563546823
32.9350615877	2170.93656357635	2169.93656357635	1177156.17248638
37.5861781588	2826.94157717397	2825.94157717397	1996486.44940012
40.9187190121	3350.18313119016	3349.18313119016	2804256.91156218
43.3270732809	3755.97055817956	3754.97055817956	3524950.97319882
48.0051508811	4610.48902224725	4609.48902224725	5311847.26155447
49.7738324776	4956.36879903077	4955.36879903077	6138919.98360192
52.9703214777	5613.20991490484	5612.20991490484	7874225.03223904
56.4462476970	6373.85775815647	6372.85775815647	10153329.0014238
59.3470440026	7045.64326369364	7044.64326369364	12406749.678176
60.8317785246	7402.51055693436	7401.51055693436	13695589.6311027
65.1125440480	8480.78678482673	8479.78678482673	17976695.9790305
67.0798105294	9000.90196134567	8999.90196134567	20249558.8284584
69.5464017111	9674.90398194397	9673.90398194397	23396104.5629678
72.0671576744	10388.8504305573	10387.8504305573	26976859.1419072
75.7046906990	11463.9003876879	11462.9003876879	32849521.324514
77.1448400688	11904.1526985045	11903.1526985045	35421261.040979
79.3373750202	12590.3381502074	12589.3381502074	39622858.7650667
82.9103808540	13749.7625067392	13748.7625067392	47257117.6166793
84.7354929805	14361.7075413025	14360.7075413025	51557480.2717057
87.4252746131	15287.8572823607	15286.8572823607	58422001.3928162
88.8091112076	15775.61646698	15774.61646698	62209631.1700789
92.4918992705	17111.0028613503	17110.0028613503	73188049.4788537
94.6513440405	17919.2538573537	17918.2538573537	80265955.3241429
95.8706342282	18383.857014652	18382.857014652	84482358.0052851
98.8311942181	19536.7099011886	19535.7099011886	95410990.33585
101.317851005	20532.1138648392	20531.1138648392	105381659.132748
103.725538040	21519.4744835734	21518.4744835734	115761186.02505

Résumé, en vue de le vérifier par programme pour le comprendre un peu, du texte "*Sur les équations du 3ème et du 4ème degré : de Galois et Lagrange au miracle de Morley*", d'Alain Connes et Jacques Dixmier.[1], Denise Vella-Chemla, octobre 2024.

1) Exposé des formules pour le troisième degré (§ 3 de l'article de référence)

On a une équation du 3ème degré sous la forme :

$$X^3 - 3sX + s = 0.$$

Si elle n'est pas sous cette forme, on peut la transformer pour qu'elle le soit : on passe de la forme $ax^3 + bx^2 + cx + d = 0$ à la forme $x^3 + px + q = 0$ en posant $b' = \frac{b}{a}, c' = \frac{c}{a}, d' = \frac{d}{a}, p = -\frac{b'^2}{3} + c', q = \frac{2b'^3}{27} - \frac{b'c'}{3} + d'$. On passe de la forme $x^3 + px + q = 0$ à la forme $x^3 - 3sx + s = 0$ en multipliant les racines par $-\frac{p}{3q}$.

L'article fournit les fonctions qui permettent de "boucler sur les 3 racines" : on pose

$$V(a,b,c) = \frac{a-c}{b-c}$$

qui brise la symétrie en particularisant c.

V est une fonction des racines qui a deux propriétés :

- quand on permute les racines de toutes les manières possibles, on obtient des valeurs différentes pour $V(a,b,c)$;
- les racines a, b, c peuvent s'exprimer en fonction de V.

Supposons qu'on dispose des 3 racines. On peut calculer :

$$f_1(a,b,c) = -\frac{V^2 - V + 1}{(V-2)(V+1)}, \quad f_2(a,b,c) = \frac{V^2 - V + 1}{2(V-0.5)(V+1)}, \quad f_3(a,b,c) = \frac{V^2 - V + 1}{2(V-0.5)(V-2)}.$$

et on voit que ces 3 fonctions envoient les racines l'une sur l'autre. On peut permuter les racines passées en arguments des 3 fonctions et on obtient toute la combinatoire possible des bijections du triplet de racines vers lui-même.

On a :

$$f_1(a,b,c) + f_2(a,b,c) + f_3(a,b,c) = 0$$

et

$$\frac{1}{f_1(a,b,c)} + \frac{1}{f_2(a,b,c)} + \frac{1}{f_3(a,b,c)} = 3$$

On peut également exprimer deux racines en fonction de la troisième, par les formules

$$b = -\frac{a}{2} + \frac{-6pa^2 + 9qa - 4p^2}{2\sqrt{\Delta}}, \quad c = -\frac{a}{2} - \frac{-6pa^2 + 9qa - 4p^2}{2\sqrt{\Delta}},$$

[1] Voir https://ems.press/journals/lem/articles/13958353, article en libre accès ou fichier pdf stocké ici https://denisevellachemla.eu/AC-JD-enseignent.pdf

avec $\Delta = -4p^3 - 27q^2$.

Est noté dans l'article de référence : "*En adjoignant au corps k une racine carrée du discriminant* Δ *et en faisant un certain nombre de calculs, on obtient la matrice de l'automorphisme de Galois d'ordre 3 de* $k(\sqrt{\Delta})[x]/P$",

$$M = \begin{pmatrix} 1 & 0 & 0 \\ \dfrac{2p^2}{\sqrt{\Delta}} & -\dfrac{9q}{2\sqrt{\Delta}} - \dfrac{1}{2} & \dfrac{3p}{\sqrt{\Delta}} \\ \dfrac{3pq}{\sqrt{\Delta}} - p & \dfrac{p^2}{\sqrt{\Delta}} & \dfrac{9q}{2\sqrt{\Delta}} - \dfrac{1}{2} \end{pmatrix}$$

Mais en appliquant cet opérateur matriciel à un vecteur $[\alpha, \beta, \gamma]$, on ne parvient pas à retrouver la seconde et la troisième racine.

2) Vérification par programme de l'exactitude des fonctions fournies pour le troisième degré (§ 3 de l'article de référence)

Le Programme pour le troisième degré (§ 3 de l'article de référence)

```
import cmath
from cmath import sqrt,pi,exp
import numpy as np
from numpy import matmul

def poly1(x):
     return(x*x*x+3*x+1)

def poly2(x):
     return(x*x*x+9*x-2)

def poly3(x):
     return(x*x*x-3*x+1)

def fonction1(a,b,c):
     v = (a-c)/(b-c)
     return((v*v-v+1)/((v-2)*(v+1)))
def fonction2(a,b,c):
     v = (a-c)/(b-c)
     return(-(v*v-v+1)/(2*(v-0.5)*(v+1)))
def fonction3(a,b,c):
     v = (a-c)/(b-c)
     return(-(v*v-v+1)/(2*(v-2)*(v-0.5)))

def finvariante(x):
     return((4/27)*(((1-x+x*x)**3)/(x*x*(1-x)*(1-x))))

def invariantorbite(k):
     print(k,' ',1-k,' ',1/k,' ',(k-1)/k,' ',1/(1-k),' ',k/(k-1))
```

```
print('Equation cubique :  x^3 + 3x + 1 = 0 de forme x^3 + px + q = 0 ou x^3 + (3s)x + s = 0')
p = 3
q = 1
discrim = -4*p*p*p-27*q*q
print('avec p = ',p,' q = ',q, ' discrim = ',discrim)
s=1
print('les racines de l equation')
r1poly1 = -0.32219 ; print('r1poly1 = ',r1poly1)
r2poly1 = 0.16109+1.75438*1j ; print('r2poly1 = ',r2poly1)
r3poly1 = 0.16109-1.75438*1j ; print('r3poly1 = ',r3poly1)
print('verifie que les racines de l equation en sont bien,'
print(' i.e.  qu elles ont pour image 0 comme polynome associe.  ')
print('poly1(r1poly1) = ',poly1(r1poly1))
print('poly1(r2poly1) = ',poly1(r2poly1))
print('poly1(r3poly1) = ',poly1(r3poly1))
print('somme des racines est nulle et la somme de leurs inverses vaut -3')
print('r1poly1+r2poly1+r3poly1 = ',r1poly1+r2poly1+r3poly1)
print('1/r1poly1+1/r2poly1+1/r3poly1 = ',1/r1poly1+1/r2poly1+1/r3poly1)
print('fait tourner les racines en les permutant des 6 facons possibles par les
fonctions rationnelles R1, R2, R3, '
print(' du theoreme 2.1 p.5 de l article d Alain Connes, Jacques Dixmier (2024)
:',end='')
print(' Sur les equations du 3e et du 4e degre :  de Galois et Lagrange au miracle de
Morley', ca tourne bien.')
print('fonction1(r1poly1,r2poly1,r3poly1) = ',fonction1(r1poly1,r2poly1,r3poly1))
print('fonction2(r1poly1,r2poly1,r3poly1) = ',fonction2(r1poly1,r2poly1,r3poly1))
print('fonction3(r1poly1,r2poly1,r3poly1) = ',fonction3(r1poly1,r2poly1,r3poly1))
print('produit des 3 = ')
print(fonction1(r1poly1,r2poly1,r3poly1)*fonction2(r1poly1,r2poly1,r3poly1)
*fonction3(r1poly1,r2poly1,r3poly1))
print('')
print('fonction1(r1poly1,r3poly1,r2poly1) = ',fonction1(r1poly1,r3poly1,r2poly1))
print('fonction2(r1poly1,r3poly1,r2poly1) = ',fonction2(r1poly1,r3poly1,r2poly1))
print('fonction3(r1poly1,r3poly1,r2poly1) = ',fonction3(r1poly1,r3poly1,r2poly1))
print('produit des 3 = ')
print(fonction1(r1poly1,r3poly1,r2poly1)*fonction2(r1poly1,r3poly1,r2poly1)
*fonction3(r1poly1,r3poly1,r2poly1))
print('')
print('fonction1(r2poly1,r1poly1,r3poly1) = ',fonction1(r2poly1,r1poly1,r3poly1))
print('fonction2(r2poly1,r1poly1,r3poly1) = ',fonction2(r2poly1,r1poly1,r3poly1))
print('fonction3(r2poly1,r1poly1,r3poly1) = ',fonction3(r2poly1,r1poly1,r3poly1))
print('produit des 3 = ')
print(fonction1(r2poly1,r1poly1,r3poly1)*fonction2(r2poly1,r1poly1,r3poly1)
*fonction3(r2poly1,r1poly1,r3poly1))
print('')
print('fonction1(r2poly1,r3poly1,r1poly1) = ',fonction1(r2poly1,r3poly1,r1poly1))
print('fonction2(r2poly1,r3poly1,r1poly1) = ',fonction2(r2poly1,r3poly1,r1poly1))
print('fonction3(r2poly1,r3poly1,r1poly1) = ',fonction3(r2poly1,r3poly1,r1poly1))
print('produit des 3 = ')
print(fonction1(r2poly1,r3poly1,r1poly1)*fonction2(r2poly1,r3poly1,r1poly1)
*fonction3(r2poly1,r3poly1,r1poly1))
print('')
print('')
```

```
print('fonction1(r3poly1,r1poly1,r2poly1) = ',fonction1(r3poly1,r1poly1,r2poly1))
print('fonction2(r3poly1,r1poly1,r2poly1) = ',fonction2(r3poly1,r1poly1,r2poly1))
print('fonction3(r3poly1,r1poly1,r2poly1) = ',fonction3(r3poly1,r1poly1,r2poly1))
print('produit des 3 = ')
print(fonction1(r3poly1,r1poly1,r2poly1)*fonction2(r3poly1,r1poly1,r2poly1)
*fonction3(r3poly1,r1poly1,r2poly1))
print('')
print('fonction1(r3poly1,r2poly1,r1poly1) = ',fonction1(r3poly1,r2poly1,r1poly1))
print('fonction2(r3poly1,r2poly1,r1poly1) = ',fonction2(r3poly1,r2poly1,r1poly1))
print('fonction3(r3poly1,r2poly1,r1poly1) = ',fonction3(r3poly1,r2poly1,r1poly1))
print('produit des 3 = ')
fonction1(r3poly1,r2poly1,r1poly1)*fonction2(r3poly1,r2poly1,r1poly1)
*fonction3(r3poly1,r2poly1,r1poly1))
print('d autres formules :  exprimer deux des trois racines en fonction de la meme
troisieme (voir page 7 de l article).')
alpha = r1poly1
beta = -(alpha/2)+(-4*p*p+9*q*alpha-6*p*alpha*alpha)/(2*sqrt(discrim))
gamma = -(alpha/2)-(-4*p*p+9*q*alpha-6*p*alpha*alpha)/(2*sqrt(discrim))
print('alpha = ',alpha,' beta = ',beta,' gamma = ',gamma)
print('Matrice de l automorphisme du groupe de Galois de l equation ')
M = np.zeros((3,3),dtype='complex')
M = [[1,0,0],
[2*p*p/sqrt(discrim),-0.5-9*q/(2*sqrt(discrim)),3*p/sqrt(discrim)],
[-p-3*p*q/sqrt(discrim),p*p/sqrt(discrim),-0.5+9*q/(2*sqrt(discrim))]]
print('M = ',M)
print('dernier test :  Omega invariant de l orbite ?  (voir page 4 de l article, entre
les equations (4) et (5).')
for x in [r1poly3,r2poly3,r3poly3]:
     print(finvariante(x),' ',finvariante(1-x),' ',finvariante(1/x),'
',finvariante((x-1)/x),' ',finvariante(1/(1-x)),' ',finvariante(x/(x-1)))
```

b) Le résultat du programme ci-dessus pour le troisième degré (§ 3 de l'article de référence)

```
Equation cubique :  x^3 + 3x + 1 = 0 de forme x^3 + px + q = 0 ou x^3 + (3s)x + s = 0
avec p = 3 q = 1 discrim = -135

Voici les racines de l equation
r1poly1 = -0.32219
r2poly1 = (0.16109+1.75438j)
r3poly1 = (0.16109-1.75438j)

On verifie que les racines de l equation en sont bien, i.e.  qu elles ont pour image 0
comme polynome associe.
poly1(r1poly1) = -1.5382759458892892e-05
poly1(r2poly1) = (1.8108238040825952e-05+1.3682409605308976e-06j)
poly1(r3poly1) = (1.8108238040825952e-05-1.3682409605308976e-06j)

La somme des racines est nulle et la somme de leurs inverses vaut -3
r1poly1+r2poly1+r3poly1 = (-9.99999999995449e-06+0j)
1/r1poly1+1/r2poly1+1/r3poly1 = (-2.9999568327002413+0j)

On fait tourner les racines en les permutant des 6 facons possibles par les fonctions
rationnelles R1, R2, R3,
du theoreme 2.1 p.5 de l article d Alain Connes, Jacques Dixmier (2024)
Sur les equations du 3e et du 4e degre :  de Galois et Lagrange
au miracle de Morley, ca tourne bien.
fonction1(r1poly1,r2poly1,r3poly1) = (-0.32218525249311275-0j)
fonction2(r1poly1,r2poly1,r3poly1) = (0.1610926262465564+1.7543722995019468j)
fonction3(r1poly1,r2poly1,r3poly1) = (0.1610926262465564-1.7543722995019468j)
produit des 3 = (-0.9999898875222369+0j)

fonction1(r1poly1,r3poly1,r2poly1) = (-0.32218525249311275-0j)
fonction2(r1poly1,r3poly1,r2poly1) = (0.1610926262465564-1.7543722995019468j)
fonction3(r1poly1,r3poly1,r2poly1) = (0.1610926262465564+1.7543722995019468j)
produit des 3 = (-0.9999898875222369+0j)

fonction1(r2poly1,r1poly1,r3poly1) = (0.1610926262465564+1.7543722995019468j)
fonction2(r2poly1,r1poly1,r3poly1) = (-0.3221852524931127-2.2608813431248678e-17j)
fonction3(r2poly1,r1poly1,r3poly1) = (0.1610926262465635-1.7543722995019466j)
produit des 3 = (-0.9999898875222366-4.163336342344337e-17j)

fonction1(r2poly1,r3poly1,r1poly1) = (0.1610926262465563+1.7543722995019468j)
fonction2(r2poly1,r3poly1,r1poly1) = (0.1610926262465646-1.7543722995019468j)
fonction3(r2poly1,r3poly1,r1poly1) = (-0.3221852524931127-4.5217626862497356e-17j)
produit des 3 = (-0.9999898875222367-2.4765449501062445e-16j)

fonction1(r3poly1,r1poly1,r2poly1) = (0.1610926262465564-1.7543722995019468j)
fonction2(r3poly1,r1poly1,r2poly1) = (-0.3221852524931127+2.2608813431248678e-17j)
fonction3(r3poly1,r1poly1,r2poly1) = (0.1610926262465635+1.7543722995019466j)
produit des 3 = (-0.9999898875222366+4.163336342344337e-17j)

fonction1(r3poly1,r2poly1,r1poly1) = (0.1610926262465563-1.7543722995019468j)
fonction2(r3poly1,r2poly1,r1poly1) = (0.1610926262465646+1.7543722995019468j)
fonction3(r3poly1,r2poly1,r1poly1) = (-0.3221852524931127+4.5217626862497356e-17j)
produit des 3 = (-0.9999898875222367+2.4765449501062445e-16j)
```

```
Application d autres formules :  exprimer deux des trois racines en fonction de la
meme troisieme (voir page 7 de l article).
alpha = -0.32219 beta = (0.161095+1.7543850775794458j) gamma =
(0.161095-1.7543850775794458j)
Matrice de l automorphisme du groupe de Galois de l equation
```
$M = [[1, 0, 0]$,
$[-1.5491933384829668j, (-0.5 + 0.3872983346207417j), -0.7745966692414834j]$,
$[(-3 + 0.7745966692414834j), -0.7745966692414834j, (-0.5 - 0.3872983346207417j)]]$

```
dernier test :  Omega invariant de l orbite ?  (voir page 4 de l article, entre les
equations (4) et (5).
2.367225666165533 2.3672256661655333 2.3672256661655333 2.3672256661655333
2.3672256661655338 2.3672256661655333
(-0.14363546383067707-0.139360118829165j) (-0.14363546383067705-0.13936011882916507j)
(-0.14363546383067696-0.13936011882916494j) (-0.14363546383067696-0.13936011882916507j)
(-0.143635463830677-0.139360118829165j) (-0.143635463830677-0.1393601188291649j)
(-0.14363546383067707+0.139360118829165j) (-0.14363546383067705+0.13936011882916507j)
(-0.14363546383067696+0.13936011882916494j) (-0.14363546383067696+0.13936011882916507j)
(-0.143635463830677+0.139360118829165j) (-0.143635463830677+0.1393601188291649j)
```

En annexe 2, on fournit les résultats pour 2 autres équations du troisième degré, pour lesquelles les formules R_i, etc donnent systématiquement les opposés des racines.

Tout fonctionne bien, sauf 2 soucis :

- pour les deux dernières équations étudiées, par les formules des R_j du théorème 2.1, on obtient les opposés des nombres complexes escomptés.
- dans la proposition 2.4, l'utilisation de l'opérateur plutôt que des formules (12) fournissant β et γ en fonction de α ne renvoie pas les racines attendues.

Équations du 4ème degré

L'équation est de la forme : $X^4 + pX^2 + qX + r = 0$.

Il y a trois cas différents :

1) $\boxed{\begin{array}{l} p^2 + 12r \neq 0 \\ -2p^3 + 72pr - 17q^2 \neq 0 \end{array}}$.

L'action du groupe du matelas M_4 (ou groupe de Klein K_4) obéit à la formule :

$$T_j(x) := x - P'(x)\left(\frac{p}{3} + 12\frac{J}{I}R_j(\omega) + 2x^2\right)^{-1}$$

avec $I = \dfrac{p^2 + 12r}{12}$, $J = \dfrac{-2p^3 + 72pr - 27q^2}{432}$, $P'(X) = 4X^3 + 2pX + q$.

Cette transformation échange α et δ d'une part, et β et γ d'autre part.

Un exemple fourni : $x^4 - \frac{15}{2}x^2 + 5x + \frac{5}{16} = 0$: le groupe de Klein K_4 (ou groupe du matelas M_4) opère sur les racines.

2) $\boxed{\begin{array}{l} p^2 + 12r \neq 0 \\ -2p^3 + 72pr - 17q^2 = 0 \end{array}}$

On pose $\rho = P'(\alpha) = 4\alpha^3 + 2p\alpha + q$, $\sigma = \frac{1}{2}P''(\alpha) = 6\alpha^2 + p$.

Les relations que vérifient les racines $\alpha, \beta, \gamma, \delta$ sont les relations (23) de l'article de référence.

(23) $$\frac{1}{\beta - \alpha} = -\frac{\sigma}{3\rho}, \quad \frac{1}{\gamma - \alpha} = -\frac{\sigma - 6\sqrt{I}}{3\rho}, \quad \frac{1}{\delta - \alpha} = -\frac{\sigma + 6\sqrt{I}}{3\rho}.$$

Les formules qui expriment les 3 autres racines β, γ, δ en fonction de α sont :

(24) $$\beta = \alpha - \frac{3\rho}{\sigma}, \quad \gamma = \alpha - \frac{3\rho}{\sigma - 6\sqrt{I}}, \quad \delta = \alpha - \frac{3\rho}{\sigma + 6\sqrt{I}},$$

Un exemple fourni : $x^4 + 6x^2 + 1 = 0$.

3) $\boxed{p^2 + 12r = 0}$

Pour simplifier, on suppose que le corps k contient une racine cubique de l'unité.

Les équations qui permettent de trouver β, γ, δ en fonction de α (et ρ et σ et $\sqrt[3]{2J}$) sont :

$$\beta = \alpha + \frac{3\rho}{6\sqrt[3]{2J} - \sigma}, \qquad \gamma = \alpha + \frac{3\rho}{6j\sqrt[3]{2J} - \sigma}, \qquad \delta = \alpha + \frac{3\rho}{6j^2\sqrt[3]{2J} - \sigma}.$$

Un exemple fourni : $x^4 - 3x^2 + 3x - \frac{3}{4} = 0$: le groupe de Klein K_4 (ou groupe du matelas M_4) opère sur les racines.

Annexe 1 : les 6 brisures de symétrie

Dans toute la suite, $\omega = \dfrac{a-c}{b-c}$.

- en permutant a et b dans l'expression de ω, i.e. en faisant agir l'opérateur $\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$, on obtient la fraction $\dfrac{b-c}{a-c}$ qui est égale à $\dfrac{1}{\omega}$ trivialement.
- en permutant b et c dans l'expression de ω, i.e. en faisant agir l'opérateur $\begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$, on obtient la fraction $\dfrac{a-b}{c-b}$ qui est égale à $1-\omega$. En effet, $1 - \dfrac{a-c}{b-c} = \dfrac{b-c-a+c}{b-c} = \dfrac{b-a}{b-c} = \dfrac{a-b}{c-b}$.
- en permutant a et c dans l'expression de ω, i.e. en faisant agir l'opérateur $\begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$, on obtient la fraction $\dfrac{c-a}{b-a}$ qui est égale à $\dfrac{\omega}{\omega-1}$.
- en effectuant une rotation horaire sur a, b, c dans l'expression de ω, i.e. en faisant agir l'opérateur $\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$, on obtient la fraction $\dfrac{c-b}{a-b}$ qui est égale à $\dfrac{1}{1-\omega}$. En effet,

$$\begin{aligned} \frac{1}{1 - \dfrac{a-c}{b-c}} &= \frac{1}{\dfrac{b-c-a+c}{b-c}} \\ &= \frac{b-c}{b-a} = \frac{c-b}{a-b} \end{aligned}$$

- en effectuant une rotation anti-horaire sur a, b, c dans l'expression de ω, i.e. en faisant agir l'opérateur $\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$, on obtient la fraction $\dfrac{b-a}{c-a}$ qui est égale à $\dfrac{\omega-1}{\omega}$. En effet,

$$\begin{aligned} \frac{\dfrac{a-c}{b-c} - 1}{\dfrac{a-c}{b-c}} &= \frac{\dfrac{a-c-b+c}{b-c}}{\dfrac{a-c}{b-c}} \\ &= \frac{a-b}{a-c} = \frac{b-a}{c-a} \end{aligned}$$

- en n'opérant pas dans l'expression de ω, i.e. en faisant agir l'opérateur $\mathrm{Id} = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$, on obtient la fraction $\dfrac{a-c}{b-c}$ qui est égale à ω.

Annexe 2 : résultat du programme appliqué à deux autres équations

```
Equation cubique :  x^3 + 6x - 2 = 0 de forme x^3 + px + q = 0 ou x^3 + (3s)x + s = 0
avec p = 6 q = -2 discrim = -972

Voici les racines de l equation
r1poly2 = 0.32748
r2poly2 = (-0.16374+2.46585j)
r3poly2 = (-0.16374-2.46585j)

On verifie que les racines de l equation en sont bien, i.e.  qu elles ont pour image 0
comme polynome associe.
poly2(r1poly2) = -1.310700814549648e-08
poly2(r2poly2) = (-7.94154517391732e-06+3.9799558754438635e-05j)
poly2(r3poly2) = (-7.94154517391732e-06-3.9799558754438635e-05j)

La somme des racines est nulle et la somme de leurs inverses vaut -3
r1poly2+r2poly2+r3poly2 = 0j
1/r1poly2+1/r2poly2+1/r3poly2 = (2.9999998779483548+0j)

On fait tourner les racines en les permutant des 6 facons possibles par les fonctions
rationnelles R1, R2, R3,
du theoreme 2.1 p.5 de l article d Alain Connes, Jacques Dixmier (2024) :  Sur les
equations du 3e et du 4e degre :  de Galois et Lagrange au miracle de Morley, ca
tourne bien.
fonction1(r1poly2,r2poly2,r3poly2) = (-0.32747998667684236-0j)
fonction2(r1poly2,r2poly2,r3poly2) = (0.16373999333842118-2.46584989967965j)
fonction3(r1poly2,r2poly2,r3poly2) = (0.16373999333842118+2.46584989967965j)
produit des 3 = (-1.9999944571649133-2.7755575615628914e-17j)

fonction1(r1poly2,r3poly2,r2poly2) = (-0.32747998667684236-0j)
fonction2(r1poly2,r3poly2,r2poly2) = (0.16373999333842118+2.46584989967965j)
fonction3(r1poly2,r3poly2,r2poly2) = (0.16373999333842118-2.46584989967965j)
produit des 3 = (-1.9999944571649133+2.7755575615628914e-17j)

fonction1(r2poly2,r1poly2,r3poly2) = (0.16373999333842104-2.46584989967965j)
fonction2(r2poly2,r1poly2,r3poly2) = (-0.3274799866768424+0j)
fonction3(r2poly2,r1poly2,r3poly2) = (0.16373999333842137+2.46584989967965j)
produit des 3 = (-1.9999944571649138+2.498001805406602e-16j)

fonction1(r2poly2,r3poly2,r1poly2) = (0.16373999333842088-2.46584989967965j)
fonction2(r2poly2,r3poly2,r1poly2) = (0.1637399933384216+2.4658498996796503j)
fonction3(r2poly2,r3poly2,r1poly2) = (-0.32747998667684236+0j)
produit des 3 = (-1.9999944571649138+5.635425230344834e-16j)

fonction1(r3poly2,r1poly2,r2poly2) = (0.16373999333842104+2.46584989967965j)
fonction2(r3poly2,r1poly2,r2poly2) = (-0.3274799866768424+0j)
fonction3(r3poly2,r1poly2,r2poly2) = (0.16373999333842137-2.46584989967965j)
produit des 3 = (-1.9999944571649138-2.498001805406602e-16j)

fonction1(r3poly2,r2poly2,r1poly2) = (0.16373999333842088+2.46584989967965j)
fonction2(r3poly2,r2poly2,r1poly2) = (0.1637399933384216-2.4658498996796503j)
fonction3(r3poly2,r2poly2,r1poly2) = (-0.32747998667684236+0j)
produit des 3 = (-1.9999944571649138-5.635425230344834e-16j)
```

Application d autres formules : exprimer deux des trois racines en fonction de la meme troisieme (voir page 7 de l article).
alpha = 0.32748
beta = (-0.16374+2.465853271587796j)
gamma = (-0.16374-2.465853271587796j)
Matrice de l automorphisme du groupe de Galois de l equation
$M = [[1, 0, 0],$
$[-2.309401076758503j, (-0.5 - 0.28867513459481287j), -0.5773502691896257j],$
$[(-6 - 1.1547005383792515j), -1.1547005383792515j, (-0.5 + 0.28867513459481287j)]]$

dernier test : Omega invariant de l orbite ? (voir page 4 de l article, entre les equations (4) et (5).
1.4481194217899915 1.4481194217899915 1.4481194217899915 1.4481194217899915
1.448119421789992 1.4481194217899918
(-0.48405742770126126-0.45567316431301746j) (-0.48405742770126087-0.45567316431301724j)
(-0.48405742770126114-0.4556731643130174j) (-0.4840574277012606-0.4556731643130178j)
(-0.4840574277012612-0.4556731643130175j) (-0.4840574277012615-0.4556731643130173j)
(-0.48405742770126126+0.45567316431301746j) (-0.48405742770126087+0.45567316431301724j)
(-0.48405742770126114+0.4556731643130174j) (-0.4840574277012606+0.4556731643130178j)
(-0.4840574277012612+0.4556731643130175j) (-0.4840574277012615+0.4556731643130173j)

Equation cubique : $x^3 - 3x + 1 = 0$ de forme $x^3 + px + q = 0$ ou $x^3 + (3s)x + s = 0$
avec p = -3 q = 1 discrim = 81

Voici les racines de l equation
r1poly3 = 1.53209
r2poly3 = -1.87939
r3poly3 = 0.3473

On verifie que les racines de l equation en sont bien, i.e. qu elles ont pour image 0 comme polynome associe.
poly3(r1poly3) = 4.501708329218701e-06
poly3(r2poly3) = -3.614641701865651e-05
poly3(r3poly3) = -9.615183000022398e-06

La somme des racines est nulle et la somme de leurs inverses vaut 3
r1poly3+r2poly3+r3poly3 = 5.551115123125783e-17
1/r1poly3+1/r2poly3+1/r3poly3 = 2.999970655611892

On fait tourner les racines en les permutant des 6 facons possibles par les fonctions rationnelles R1, R2, R3, du theoreme 2.1 p.5 de l article d Alain Connes, Jacques Dixmier (2024) : Sur les equations du 3e et du 4e degre : de Galois et Lagrange au miracle de Morley, ca tourne bien.
fonction1(r1poly3,r2poly3,r3poly3) = -1.5320750139188077
fonction2(r1poly3,r2poly3,r3poly3) = 1.8793716168168109
fonction3(r1poly3,r2poly3,r3poly3) = -0.3472966028980033
produit des 3 = 0.9999844087925736

fonction1(r1poly3,r3poly3,r2poly3) = -1.5320750139188082
fonction2(r1poly3,r3poly3,r2poly3) = -0.34729660289800335
fonction3(r1poly3,r3poly3,r2poly3) = 1.8793716168168115
produit des 3 = 0.9999844087925742

```
fonction1(r2poly3,r1poly3,r3poly3) = 1.879371616816811
fonction2(r2poly3,r1poly3,r3poly3) = -1.5320750139188075
fonction3(r2poly3,r1poly3,r3poly3) = -0.3472966028980034
produit des 3 = 0.9999844087925737

fonction1(r2poly3,r3poly3,r1poly3) = 1.879371616816811
fonction2(r2poly3,r3poly3,r1poly3) = -0.3472966028980034
fonction3(r2poly3,r3poly3,r1poly3) = -1.5320750139188075
produit des 3 = 0.9999844087925737

fonction1(r3poly3,r1poly3,r2poly3) = -0.3472966028980034
fonction2(r3poly3,r1poly3,r2poly3) = -1.5320750139188077
fonction3(r3poly3,r1poly3,r2poly3) = 1.8793716168168109
produit des 3 = 0.9999844087925737

fonction1(r3poly3,r2poly3,r1poly3) = -0.3472966028980034
fonction2(r3poly3,r2poly3,r1poly3) = 1.8793716168168109
fonction3(r3poly3,r2poly3,r1poly3) = -1.5320750139188077
produit des 3 = 0.9999844087925739

Application d autres formules :  exprimer deux des trois racines en fonction de la
meme troisieme (voir page 7 de l article).
alpha = 1.53209 beta = (0.34729976809999974+0j) gamma = (-1.8793897680999998+0j)
Matrice de l automorphisme du groupe de Galois de l equation
M = [[1, 0, 0], [(2+0j), (-1+0j), (-1+0j)], [(4+0j), (1+0j), 0j]]

dernier test :  Omega invariant de l orbite ?  (voir page 4 de l article, entre les
equations (4) et (5).
1.333330879050212 1.3333308790502119 1.3333308790502116 1.3333308790502119
1.3333308790502119 1.333330879050212
1.333336302033247 1.3333363020332463 1.333336302033247 1.3333363020332463
1.333336302033247 1.3333363020332474
1.333314481634212 1.3333144816342122 1.333314481634212 1.3333144816342117
1.3333144816342117 1.3333144816342117
```

Annexe 3 : programme pour le degré 4 et son résultat pour trois équations correspondant aux trois cas : général, harmonique et équiharmonique.

Note : bien que noté dans l'article de référence comme étant un cas harmonique, il s'avère que la première équation traitée ci-dessous devrait se voir appliquer les équations du cas général (§ 3.2 de l'article de référence). Comme le fait de lui appliquer les équations du § 3.3 fonctionne très bien, on laisse ainsi.

```
import cmath
from cmath import sqrt,pi,exp
import numpy as np
from numpy import matmul

def poly2(x):
     return(x**4-7.5*(x**2)+5*x+5/16)
```

```
def poly3(x):
     return(x**4+6*(x**2)+1)

def poly4(x):
     return(x**4-3*(x**2)+3*x-0.75)

petitj = exp(2*1j*pi/3)
print('Equation du quatrieme degre :  x^4 - 7.5 * (x * *2) + 5 * x + 5/16  =  0 de forme
x^4 + px^2 + qx + r = 0')
p = -7.5
q = 5
r = 5/16
I = (p*p+12*r)/12
J = (-2*p*p*p+72*p*r-27*q*q)/432
print('avec p = ',p,' q = ',q,' r = ',r)
print('I = ',I)
print('J = ',J)
res1 = p*p+12*r
res2 = -2*p*p*p+72*p*r-17*q*q
print('p^2 + 12r = ',res1)
print('-2p^3 + 72pr - 17q^2 = ',res2)
if res1 != 0 and res2 != 0:
     print('on est dans le cas 1.')
else:
     if res1 != 0 and res2 == 0:
          print('on est dans le cas 2.')
     else:
          if res1 == 0:
               print('on est dans le cas 3.')
print('les racines de l equation')
# [-3.02014702134020, -0.0575365158350514, 0.784079043840412, 2.29360449333484]
r1poly2 = -3.02014702134020 ; print('r1poly2 = ',r1poly2)
r2poly2 = -0.0575365158350514 ; print('r2poly2 = ',r2poly2)
r3poly2 = 0.784079043840412 ; print('r3poly2 = ',r3poly2)
r4poly2 = 2.29360449333484 ; print('r4poly2 = ',r4poly2)
print('verifie que les racines de l equation en sont bien, i.e.  qu elles ont pour
image 0 comme polynome associe.  ')
print('poly2(r1poly2) = ',poly2(r1poly2))
print('poly2(r2poly2) = ',poly2(r2poly2))
print('poly2(r3poly2) = ',poly2(r3poly2))
print('poly2(r4poly2) = ',poly2(r4poly2))
alpha = r1poly2
rho = 4*(alpha**3)+2*p*alpha+q
sigma = 6*(alpha**2)+p
beta = alpha-(3*rho)/sigma
gamma = alpha-(3*rho)/(sigma-6*sqrt(I))
delta = alpha-(3*rho)/(sigma+6*sqrt(I))
print('verifie les relations (23) entre les racines')
print('gauche1 = ',1/(beta-alpha))
print('droite1 = ',-sigma/(3*rho))
print('gauche2 = ',1/(gamma-alpha))
print('droite2 = ',-(sigma-6*sqrt(I))/(3*rho))
print('gauche3 = ',1/(delta-alpha))
print('droite3 = ',-(sigma+6*sqrt(I))/(3*rho))
```

```
print('trouve la seconde, la troisieme racine et la quatrieme a partir de la
premiere.')
print('beta = ',beta)
print('gamma = ',gamma)
print('delta = ',delta)

print('Equation du quatrieme degre :  x^4+6*(x**2)+1=0 de forme x^4+px^2+qx+r=0')
p = 6
q = 0
r = 1
I = (p*p+12*r)/12
J = (-2*p*p*p+72*p*r-27*q*q)/432
print('avec p = ',p,' q = ',q,' r = ',r)
print('I = ',I)
print('J = ',J)
res1 = p*p+12*r
res2 = -2*p*p*p+72*p*r-17*q*q
print('p^2+12r = ',res1)
print('-2p^3+72pr-17q^2 = ',res2)
if res1 != 0 and res2 != 0:
     print('on est dans le cas 1.')
else:
     if res1 != 0 and res2 == 0:
          print('on est dans le cas 2.')
     else:
          if res1 == 0:
               print('on est dans le cas 3.')
print('les racines de l equation')
# [-I*sqrt(3 - 2*sqrt(2)), I*sqrt(3 - 2*sqrt(2)), -I*sqrt(2*sqrt(2) + 3),
I*sqrt(2*sqrt(2) + 3)]
r1poly3 = -1j*sqrt(3 - 2*sqrt(2)) ; print('r1poly3 = ',r1poly3)
r2poly3 = 1j*sqrt(3 - 2*sqrt(2)) ; print('r2poly3 = ',r2poly3)
r3poly3 = -1j*sqrt(2*sqrt(2) + 3) ; print('r3poly3 = ',r3poly3)
r4poly3 = 1j*sqrt(2*sqrt(2) + 3) ; print('r4poly3 = ',r4poly3)
print('verifie que les racines de l equation en sont bien, i.e.  qu elles ont pour
image 0 comme polynome associe.  ')
print('poly3(r1poly3) = ',poly3(r1poly3))
print('poly3(r2poly3) = ',poly3(r2poly3))
print('poly3(r3poly3) = ',poly3(r3poly3))
print('poly3(r4poly3) = ',poly3(r4poly3))
alpha = r1poly3
rho = 4*(alpha**3)+2*p*alpha+q
sigma = 6*(alpha**2)+p
beta = alpha-(3*rho)/sigma
gamma = alpha-(3*rho)/(sigma-6*sqrt(I))
delta = alpha-(3*rho)/(sigma+6*sqrt(I))
print('verifie les relations (23) entre les racines')
print('gauche1 = ',1/(beta-alpha))
print('droite1 = ',-sigma/(3*rho))
print('gauche2 = ',1/(gamma-alpha))
print('droite2 = ',-(sigma-6*sqrt(I))/(3*rho))
print('gauche3 = ',1/(delta-alpha))
print('droite3 = ',-(sigma+6*sqrt(I))/(3*rho))
```

```
print('trouve la seconde, la troisieme racine et la quatrieme a partir de la
premiere.')
print('beta = ',beta)
print('gamma = ',gamma)
print('delta = ',delta)

print('Equation du quatrieme degre :  x^4 - 3 * (x * *2) + 3 * x - 0.75  =  0 de forme
x^4 + px^2 + qx + r = 0')
p = -3
q = 3
r = -0.75
I = (p*p+12*r)/12
J = (-2*p*p*p+72*p*r-27*q*q)/432
print('avec p = ',p,' q = ',q,' r = ',r)
print('I = ',I)
print('J = ',J)
res1 = p*p+12*r
res2 = -2*p*p*p+72*p*r-17*q*q
print('p^2 + 12r = ',res1)
print('-2p^3 + 72pr - 17q^2 = ',res2)
if res1 != 0 and res2 != 0:
     print('on est dans le cas 1.')
else:
     if res1 != 0 and res2 == 0:
          print('on est dans le cas 2.')
     else:
          if res1 == 0:
               print('on est dans le cas 3.')
print('les racines de l equation')
# [-2.13725528220314, 0.405204474634268, 0.866025403784439 - 0.340625019316607*I,
0.866025403784439 + 0.340625019316607*I]
r1poly4 = -2.13725528220314 ; print('r1poly4 = ',r1poly4)
r2poly4 = 0.405204474634268 ; print('r2poly4 = ',r2poly4)
r3poly4 = 0.866025403784439 - 0.340625019316607*1j ; print('r3poly4 = ',r3poly4)
r4poly4 = 0.866025403784439 + 0.340625019316607*1j ; print('r4poly4 = ',r4poly4)
print('verifie que les racines de l equation en sont bien, i.e.  qu elles ont pour
image 0 comme polynome associe.  ')
print('poly4(r1poly4) = ',poly4(r1poly4))
print('poly4(r2poly4) = ',poly4(r2poly4))
print('poly4(r3poly4) = ',poly4(r3poly4))
print('poly4(r4poly4) = ',poly4(r4poly4))
alpha = r1poly4
rho = 4*(alpha**3)+2*p*alpha+q
sigma = 6*(alpha**2)+p
beta = alpha+(3*rho)/(6*((2*J)**(1/3))-sigma)
gamma = alpha+(3*rho)/(6*petitj*((2*J)**(1/3))-sigma)
delta = alpha+(3*rho)/(6*(petitj**2)*((2*J)**(1/3))-sigma)
print('trouve la seconde, la troisieme racine et la quatrieme a partir de la
premiere.')
print('beta = ',beta)
print('gamma = ',gamma)
print('delta = ',delta)
```

```
Equation du quatrieme degre :  x^4 - 7.5*(x**2) + 5*x + 5/16 = 0 de forme x^4 + px^2 + qx + r = 0
avec p = -7.5 q = 5 r = 0.3125
I = 5.0
J = 0.0
p^2 + 12r = 60.0
-2p^3 + 72pr - 17q^2 = 250.0
on est dans le cas 1.

Voici les racines de l equation
r1poly2 = -3.0201470213402
r2poly2 = -0.0575365158350514
r3poly2 = 0.784079043840412
r4poly2 = 2.29360449333484

On verifie que les racines de l equation en sont bien, i.e.  qu elles ont pour image 0
comme polynome associe.
poly2(r1poly2) = -1.1901590823981678e-13
poly2(r2poly2) = 1.1102230246251565e-16
poly2(r3poly2) = 0.0
poly2(r4poly2) = -2.1316282072803006e-14

On verifie les relations (23) entre les racines
gauche1 = 0.2628655560595672
droite1 = 0.2628655560595672
gauche2 = (0.18819096023558693+0j)
droite2 = (0.18819096023558693+0j)
gauche3 = (0.33754015188354747+0j)
droite3 = (0.33754015188354747+0j)

On trouve la seconde, la troisieme racine et la quatrieme a partir de la premiere.
beta = 0.7840790438404088
gamma = (2.2936044933348385+0j)
delta = (-0.057536515835054924+0j)
```

```
Equation du quatrieme degre :  x^4 + 6 * (x * *2) + 1 = 0 de forme x^4 + px^2 + qx + r = 0
avec p = 6 q = 0 r = 1
I = 4.0
J = 0.0
p^2 + 12r = 48
-2p^3 + 72pr - 17q^2 = 0
on est dans le cas 2.

Voici les racines de l equation
r1poly3 = -0.4142135623730948j
r2poly3 = 0.4142135623730948j
r3poly3 = -2.414213562373095j
r4poly3 = 2.414213562373095j

On verifie que les racines de l equation en sont bien, i.e.  qu elles ont pour image 0
comme polynome associe.
poly3(r1poly3) = (1.1102230246251565e-15+0j)
poly3(r2poly3) = (1.1102230246251565e-15+0j)
poly3(r3poly3) = 0j
poly3(r4poly3) = 0j

On verifie les relations (23) entre les racines
gauche1 = -0.353553390593274j
droite1 = (-0-0.35355339059327406j)
gauche2 = (-0+0.5000000000000002j)
droite2 = 0.5000000000000002j
gauche3 = -1.2071067811865483j
droite3 = (-0-1.2071067811865483j)

On trouve la seconde, la troisieme racine et la quatrieme a partir de la premiere.
beta = 2.414213562373093j
gamma = -2.414213562373094j
delta = 0.4142135623730947j
```

Equation du quatrieme degre : $x^4 - 3*(x**2) + 3*x - 0.75 = 0$ de forme $x^4 + px^2 + qx + r = 0$
avec p = -3 q = 3 r = -0.75
I = 0.0
J = -0.0625
$p^2 + 12r$ = 0.0
$-2p^3 + 72pr - 17q^2$ = 63.0
on est dans le cas 3.

Voici les racines de l equation
r1poly4 = -2.13725528220314
r2poly4 = 0.405204474634268
r3poly4 = (0.866025403784439-0.340625019316607j)
r4poly4 = (0.866025403784439+0.340625019316607j)

On verifie que les racines de l equation en sont bien, i.e. qu elles ont pour image 0
comme polynome associe.
poly4(r1poly4) = -1.1013412404281553e-13
poly4(r2poly4) = 3.3306690738754696e-16
poly4(r3poly4) = (-8.881784197001252e-16+0j)
poly4(r4poly4) = (-8.881784197001252e-16+0j)

On trouve la seconde, la troisieme racine et la quatrieme a partir de la premiere.
beta = (0.8660254037844295+0.3406250193166069j)
gamma = (0.4052044746342589+8.239298851554292e-17j)
delta = (0.8660254037844295-0.340625019316607j)

Memo Toussaint 2024

2024

- Souvenir de Galois lien.

compil 2022

- Programmation de la preuve d'Alain Connes du théorème de Morley (p. 2/151) lien.
- empilement des valuations p-adiques : ce n'est pas une équation en $n \ln n$ (p. 141/151) lien

compil 2021

- s'il ne devait me rester qu'un seul souvenir, retour au maillage et petits graphes Feynman, 19.12.2021 chouette maillage inopérant ;
- novembre : travailler modulo 1 : dessin tout pourri au crayon (664) lien qui deviendra le programme perseverare en 2024 lien ;
- van der Pol : scie et aussi battements cardiaques (août et septembre 2021, repris en mars 2024) lien lien lien lien.

compil 2020

- cristal 400, février 2020 (p. 10/470) lien lien ;
- matrices circulantes puissance pour trouver les nombres premiers (p. 466/470) lien.

table-des-matieres-chous

- séquences fractales d'entiers (p. 2/50) février 2006 lien ;
- arbres de Knuth pour partitions : approche purement syntaxique, 12.1.2017 (p. 23/50) 12.1.2017 lien ;
- calculer des sommes de cos pour trouver les premiers lien smoothie cubique lien lien lien lien ;
- matrice avec exponentielles de premiers sur la diagonale au lieu de circulantes Snurinfini, 17.7.2016 (p. 17/50) lien lien ;
- chaleur pour trouver premiers ? (p. 40/50) lien lien lien ;
- nombre de solutions de l'équation modulaire $x^{10} - 1 \equiv 0 \pmod{n}$ en fct dernier chiffre, 20.12.2017 (p. 46/50) lien.

compil2020-transc

- Tannery (p. 310/446) lien lien lien lien lien.

compil 11 (année 2018)

- ensemble de Cantor (p. 13/160) lien ;
- présentation snurpf très simple avec des disjonctions sur les restes modulaires possibles (p. 66/160) lien orthogonalité.

compil-fev2014

- chouettes transparents échanger (p. 31/119) lien ;
- continuer de suivre Galois et passage CG-CJ (p. 67/119) lien ;
- lien HR Goldbach (analogie) (p. 104/119) lien.

Drôle de constat !, Denise Vella-Chemla, octobre 2024.

On sait que la somme des racines carrées des entiers successifs diverge. On a :

$$\sum_{k=1}^{n} \frac{1}{\sqrt{k}} \geq \sum_{k=1}^{n} \frac{1}{\sqrt{n}} \geq \frac{n}{\sqrt{n}} = \sqrt{n}.$$

Mais si on calcule $1+\sum_{k=2}^{N} \frac{1}{\sqrt{k}}$ jusqu'à 10^9, le résultat semble tendre vers $2\sqrt{N}+\mathrm{C}$ avec $\mathrm{C} \simeq 1.460346$.

Essayons de le démontrer.

On sait que

$$n^2 = \sum_{p=1}^{n} (2p-1).$$

Posons

$$A = \sum_{k=1}^{n^2} \frac{1}{\sqrt{k}} = \frac{1}{\sqrt{1}} + \left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \frac{1}{\sqrt{4}}\right) + \left(\frac{1}{\sqrt{5}} + \frac{1}{\sqrt{6}} + \frac{1}{\sqrt{7}} + \frac{1}{\sqrt{8}} + \frac{1}{\sqrt{9}}\right) \cdots \quad (1)$$

$$= \sum_{p=1}^{n} \left(\sum_{k=p^2-2p+2}^{p^2} \frac{1}{\sqrt{k}} \right). \quad (2)$$

On utilise pour minorer / majorer un regroupement des termes de la somme en "gnomons" de carré en carré, on minore chaque parenthèse par son nombre de termes (un impair de la liste des impairs successifs) multiplié par le plus petit terme contenu dans cette parenthèse, et on majore chaque parenthèse par son nombre de termes multiplié par le plus grand terme contenu dans cette parenthèse). (rappel pour se repérer : le plus grand et le plus terme de chaque parenthèse sont aux deux extrémités de la parenthèse).

(rappel : $\gamma = 0.577215...$)

$$1 + \frac{3}{\sqrt{4}} + \frac{5}{\sqrt{9}} + \frac{7}{\sqrt{16}} + \cdots \;<\; \sum_{p=1}^{n} \sum_{k=p^2-2p+2}^{p^2} \frac{1}{\sqrt{k}} \;<\; 1 + \frac{3}{\sqrt{2}} + \frac{5}{\sqrt{5}} + \frac{7}{\sqrt{10}} + \cdots$$

$$\sum_{k=1}^{\sqrt{n}} \frac{2k+1}{\sqrt{(k+1)^2}} \;<\; A \;<\; \sum_{k=1}^{\sqrt{n}} \frac{2k+1}{\sqrt{k^2-4k+5}}$$

On essaie d'abord du côté de la minoration :

$$\begin{aligned}
\sum_{k=1}^{\sqrt{n}} \frac{2k+1}{k+1} &< A \\
\sum_{k=1}^{\sqrt{n}} \frac{2k}{k+1} + \left(\sum_{k=1}^{\sqrt{n}} \frac{1}{k+1} + 1\right) - 1 &< A \\
-1 + \left(1 + \sum_{k=2}^{\sqrt{n}+1} \frac{2(k-1)}{k}\right) + \left(\sum_{k=0}^{\sqrt{n}} \frac{1}{k}\right) - 1 &< A \\
-1 + \left(1 + \sum_{k=2}^{\sqrt{n}+1} \frac{2k-2}{k}\right) + (\ln n + \gamma) - 1 &< A \\
2\sqrt{n} - 2(\ln n + \gamma) + (\ln n + \gamma) - 2 &< A \\
2\sqrt{n} - \ln n - \gamma - 2 &< A
\end{aligned}$$

Du côté majoration, c'est trop complexe, on regroupe les "gnomons" différemment (i.e. en mettant 3 termes de la somme à l'intérieur de la première parenthèse, 5 à l'intérieur de la seconde, etc.), on a :

$$\begin{aligned}
A &< \frac{3}{\sqrt{1}} + \frac{5}{\sqrt{4}} + \frac{7}{\sqrt{9}} + \cdots \\
A &< \sum_{k=1}^{\sqrt{n}} \frac{2k+1}{k} \\
A &< 2\sqrt{n} + \sum_{k=1}^{\sqrt{n}} \frac{1}{k} \\
A &< 2\sqrt{n} + (\ln \sqrt{n} + \gamma)
\end{aligned}$$

On vérifie le résultat par le programme ci-après :

```
import math
from math import sqrt,log,floor

somme = 1
nmax = 10002
gammadEuler = 0.5772156649
for n in range(2,nmax):
somme = somme+1/sqrt(n)
print('= ', n)
print('somme des inverses des racines des entiers jusqu a n = ',somme)
print('2*sqrt(n) = ', 2*sqrt(n))
res1 = 2*sqrt(n)-log(n)-gammadEuler-2
print('mino = 2*sqrt(n) = -log(n)-gamma d Euler-2 = ',res1)
res2 = 2*sqrt(n)+log(sqrt(n))+gammadEuler
print('mino = 2*sqrt(n)+ln(sqrt(n))+gamma d Euler = ',res2)
```

dont le résultat a été déposé ici https://denisevellachemla.eu/ressuminvrac.pdf.

Pour $n = 10^7$ et $n = 10^8$, le programme renvoie :

```
n = 10000001
somme des inverses des racines des entiers jusqu a n = 6323.095440167951
2*sqrt(n) = 6324.555636564517
mino = 2*sqrt(n) = -log(n)-gamma d Euler-2 = 6305.860325148658
mino = 2*sqrt(n)+ln(sqrt(n))+gamma d Euler = 6333.191900104896

n = 100000001
somme des inverses des racines des entiers jusqu a n = 19998.53979549304
2*sqrt(n) = 20000.0001
mino = 2*sqrt(n) = -log(n)-gamma d Euler-2 = 19979.00220358115
mino = 2*sqrt(n)+ln(sqrt(n))+gamma d Euler = 20009.787656041877
```

Identiquement, en calculant par programme la somme des inverses des racines cubiques, on trouve les valeurs suivantes :

$$\sum_{k=1}^{900\,000} \frac{1}{\sqrt[3]{k}} = 13981 \qquad \sum_{k=1}^{1\,000\,000} \frac{1}{\sqrt[3]{k}} = 15000 \qquad \sum_{k=1}^{1\,900\,000} \frac{1}{\sqrt[3]{k}} = 23009 \qquad \sum_{k=1}^{2\,000\,000} \frac{1}{\sqrt[3]{k}} = 23810$$

qui oriente vers la formule :

$$\sum_{k=1}^{n} \frac{1}{\sqrt[3]{k}} = \frac{3}{2}\sqrt{n}\sqrt[6]{n}$$

qu'il faudrait démontrer d'une manière similaire.

Après tout, l'idée initiale d'Euler..., Denise Vella-Chemla, novembre 2024

On a trouvé, par hasard pur, des formules pour la somme des inverses des racines carrées, la somme des inverses des racines cubiques, la somme des inverses des racines quatrièmes, la somme des inverses des racines cinquièmes, la somme des inverses des racines sixièmes. On se dit qu'après tout, c'était un peu le but d'Euler, quand il inventa la fonction zeta (appelée maintenant fonction zeta de Riemann) et qu'il lia sa somme sur tous les entiers et son produit sur les seuls nombres premiers, selon ce qu'on appelle je crois une formule du produit eulérien : qu'on sache calculer aisément de telles sommes, pour des nombres entiers, plutôt que pour des nombres complexes, comme le fit si brillamment Riemann.

Voici les formules qu'on a trouvées :

$$\sum_{k=1}^{n} \frac{1}{\sqrt{k}} \simeq 2\sqrt{n}$$

$$\sum_{k=1}^{n} \frac{1}{\sqrt[3]{k}} \simeq \frac{3}{2} \left(\sqrt[3]{n}\right)^2$$

$$\sum_{k=1}^{n} \frac{1}{\sqrt[4]{k}} \simeq \frac{4}{3} \left(\sqrt[4]{n}\right)^3$$

$$\sum_{k=1}^{n} \frac{1}{\sqrt[5]{k}} \simeq \frac{5}{4} \left(\sqrt[5]{n}\right)^4$$

et donc il serait possible que $\displaystyle\sum_{k=1}^{n} \frac{1}{\sqrt[p]{k}} \simeq \frac{p}{p-1} \left(\sqrt[p]{n}\right)^{p-1}$

On fournit ci-dessous le programme python qui code les formules et son résultat sur quelques exemples. C'est suffisamment (très) proche pour qu'on pense que les formules (à prouver) sont correctes.

```
import math
from math import sqrt,log,floor

somme = 1
nmax = 5900000
for n in range(1,nmax):
      somme = somme+(1/(n**(1/2)))
print(somme)
print(nmax)
print((2)*((nmax**(1/2))))
print('')
```

```
somme = 1
nmax = 30000000
for n in range(1,nmax):
      somme = somme+(1/(n**(1/3)))
print(somme)
print(nmax)
print((3/2)*((nmax**(1/3))**2))
print('')
somme = 1
nmax = 9000000
for n in range(1,nmax):
      somme = somme+(1/(n**(1/4)))
print(somme)
print(nmax)
print((4/3)*((nmax**(1/4))**3))
print('')
somme = 1
nmax = 30000000
for n in range(1,nmax):
      somme = somme+(1/(n**(1/5)))
print(somme)
print(nmax)
print((5/4)*((nmax**(1/5))**4))
```

Voici son résultat :

```
4857.522560240212
5900000
4857.983120596447

144823.43272145392
30000000
144823.40769084435

219089.20059498394
9000000
219089.02300206647

1198414.644493366
30000000
1198414.3943927297
```

Cela fait vraiment plaisir !

On parvient à vérifier notre formule à partir d'une autre formule trouvée sur la toile, mais bien plus complexe à calculer : voici la copie d'écran qu'on implémente en python

To answer a question asked in private, considering the more general case of

$$S_n = \sum_{k=1}^{n} \frac{1}{\sqrt[a]{k}} = H_n^{\left(\frac{1}{a}\right)}$$

using asymptotics

$$n^{\frac{1}{a}} \left(S_n - \zeta\left(\frac{1}{a}\right) \right) =$$

$$\frac{an}{a-1} + \frac{1}{2} - \frac{1}{12an} + \frac{1}{720} \sum_{k=1}^{\infty} (-1)^{k+1} \frac{\prod_{m=1}^{2k} (am+1)}{\alpha_k \, (an)^{2k+1}}$$

where the α_k form the sequence

$$\{1, 42, 1680, 66528, 1816214400, 103783680, 14820309504000, \cdots\}$$

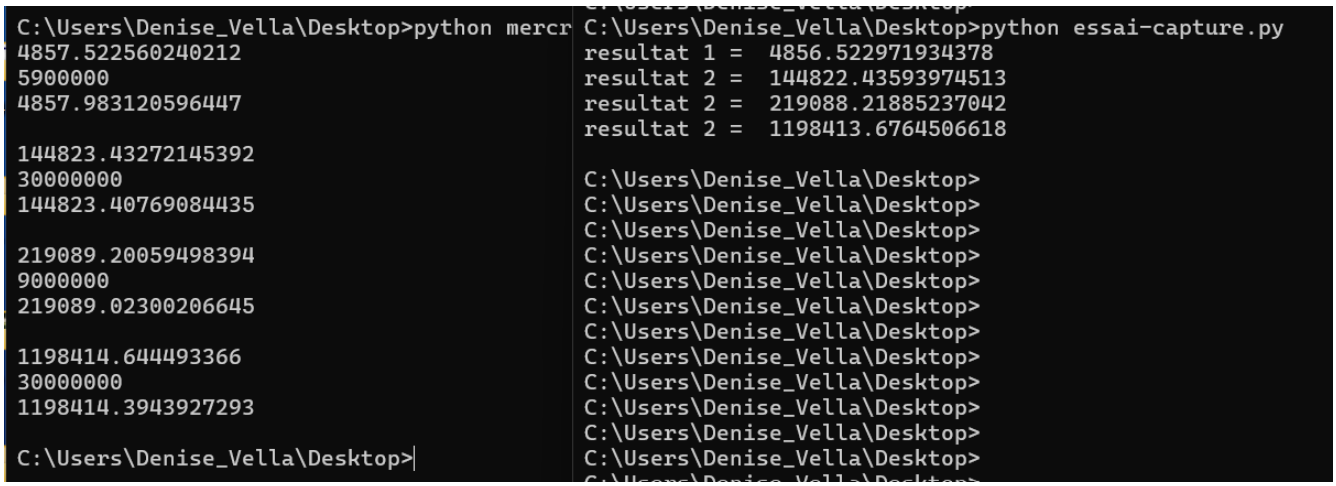
Multiplied by 720, you will find them in sequence $A060055$ in $OEIS$.

par le programme suivant (les dénominateurs croissant dangereusement, on se contente des 7 premiers nombres en lien avec les nombres de Bernoulli) :

```
import scipy
from scipy.special import zeta

def alpha(k):
     if k == 1:
          return(1)
     else:
          if k == 2:
               return(42)
          else:
               if k == 3:
                    return(1680)
               else:
                    if k == 4:
                         return(66528)
                    else:
                         if k == 5:
                              return(1816214400)
                         else:
                              if k == 6:
                                   return(103783680)
                              else:
                                   if k == 7:
                                        return(14820309504000)
```

```
def calcprod(a,k):
     prod = 1
     for m in range(1,2*k+1):
          prod = prod*(a*m+1)
     return(prod)

def sommeinfinie(n,a):
     somme = 0
     for k in range(1,8):
          somme = somme+((-1)**(k+1))*calcprod(a,k)/(alpha(k)*((a*n)**(2*k+1)))
     return(somme)

def bla(n,a):
     e1=a*n/(a-1)
     e2=0.5
     e3 = 1/(12*a*n)
     e4 = (1/720)*sommeinfinie(n,a)
     return(e1+e2-e3+e4)

n = 5900000
a = 2
print('resultat 1 = ',(bla(n,a)+n**(1/a)*zeta(1/a))/(n**(1/a)))
n=30000000
a = 3
print('resultat 2 = ',(bla(n,a)+n**(1/a)*zeta(1/a))/(n**(1/a)))
n=9000000
a = 4
print('resultat 2 = ',(bla(n,a)+n**(1/a)*zeta(1/a))/(n**(1/a)))
n=30000000
a = 5
print('resultat 2 = ',(bla(n,a)+n**(1/a)*zeta(1/a))/(n**(1/a)))
```

On obtient des résultats quasi-identiques (à 1 près car on avait initialisé notre somme à 1) à ceux qui avaient été obtenus par nos formules ultra-simples.



Puis faire demi-tour, Denise Vella-Chemla, novembre 2024

Pour aller à la rencontre des parties imaginaires des zéros non triviaux de la fonction ζ de Riemann, on écrit finalement ce tout petit programme, qui montre la valeur $1/2$ intervenir dans le calcul à côté de la transformation des degrés en radians.

Voici le programme python de cette idée saugrenue :

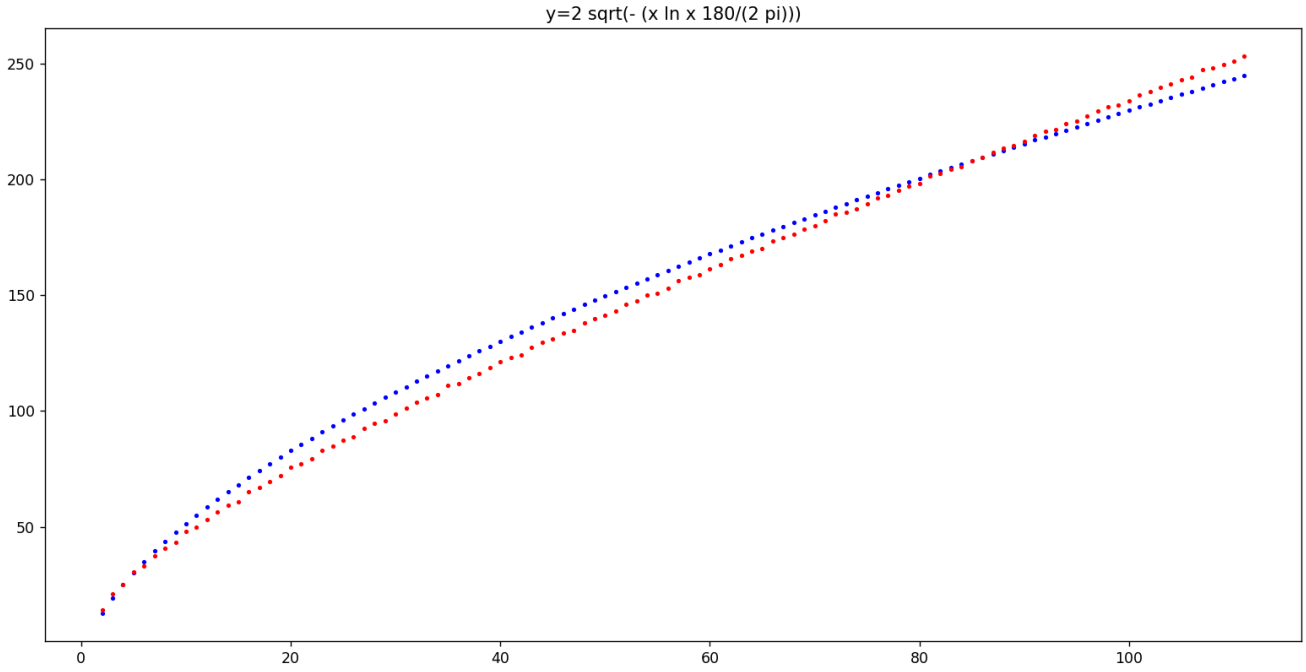
```
import math
from math import log,pi
import matplotlib.pyplot as plt
import mpmath
from mpmath import zetazero

for k in range(2,111):
     res1 = k*log(k)*180/(2*pi)
     res2 = 2*(((-1)*res1)**0.5).imag
     print(f'f({k:d}) = {res1:10f} | 2 sqrt(oppose(f({k:d})) = {res2:10f}
               | zz_{k-1:d} = ',end='')
     res = zetazero(k-1).imag
     print(res)
```

Voici le résultat du programme. On n'a pas d'explication, le programme trouve "un peu" les parties imaginaires des zéros, et la formule est si simple.

```
f(2) = 39.714408    | 2 sqrt(oppose(f(2)) = 12.603874  | zz_1 = 14.1347251417347
f(3) = 94.418771    | 2 sqrt(oppose(f(3)) = 19.433864  | zz_2 = 21.0220396387716
f(4) = 158.857632   | 2 sqrt(oppose(f(4)) = 25.207747  | zz_3 = 25.0108575801457
f(5) = 230.534999   | 2 sqrt(oppose(f(5)) = 30.366758  | zz_4 = 30.4248761258595
f(6) = 307.980766   | 2 sqrt(oppose(f(6)) = 35.098762  | zz_5 = 32.9350615877392
f(7) = 390.223536   | 2 sqrt(oppose(f(7)) = 39.508153  | zz_6 = 37.5861781588257
f(8) = 476.572896   | 2 sqrt(oppose(f(8)) = 43.661099  | zz_7 = 40.9187190121475
f(9) = 566.512627   | 2 sqrt(oppose(f(9)) = 47.603051  | zz_8 = 43.327073280915
f(10) = 659.642039  | 2 sqrt(oppose(f(10)) = 51.366995 | zz_9 = 48.0051508811672
f(11) = 755.641034  | 2 sqrt(oppose(f(11)) = 54.977851 | zz_10 = 49.7738324776723
f(12) = 854.247981  | 2 sqrt(oppose(f(12)) = 58.455042 | zz_11 = 52.9703214777145
f(13) = 955.245024  | 2 sqrt(oppose(f(13)) = 61.814077 | zz_12 = 56.4462476970634
f(14) = 1058.447928 | 2 sqrt(oppose(f(14)) = 65.067593 | zz_13 = 59.3470440026024
f(15) = 1163.698854 | 2 sqrt(oppose(f(15)) = 68.226061 | zz_14 = 60.8317785246098
f(16) = 1270.861057 | 2 sqrt(oppose(f(16)) = 71.298276 | zz_15 = 65.1125440480816
f(17) = 1379.814920 | 2 sqrt(oppose(f(17)) = 74.291720 | zz_16 = 67.0798105294942
f(18) = 1490.454927 | 2 sqrt(oppose(f(18)) = 77.212821 | zz_17 = 69.546401711174
f(19) = 1602.687302 | 2 sqrt(oppose(f(19)) = 80.067154 | zz_18 = 72.0671576744819
f(20) = 1716.428158 | 2 sqrt(oppose(f(20)) = 82.859596 | zz_19 = 75.7046906990839
f(21) = 1831.602006 | 2 sqrt(oppose(f(21)) = 85.594439 | zz_20 = 77.1448400688748
f(22) = 1948.140556 | 2 sqrt(oppose(f(22)) = 88.275490 | zz_21 = 79.3373750202494
f(23) = 2065.981730 | 2 sqrt(oppose(f(23)) = 90.906143 | zz_22 = 82.910380854086
f(24) = 2185.068859 | 2 sqrt(oppose(f(24)) = 93.489440 | zz_23 = 84.7354929805171
f(25) = 2305.349994 | 2 sqrt(oppose(f(25)) = 96.028121 | zz_24 = 87.4252746131252
```

```
f(26) = 2426.777351 | 2 sqrt(oppose(f(26)) = 98.524664  | zz_25 = 88.8091112076345
f(27) = 2549.306822 | 2 sqrt(oppose(f(27)) = 100.981321 | zz_26 = 92.4918992705585
f(28) = 2672.897569 | 2 sqrt(oppose(f(28)) = 103.400146 | zz_27 = 94.6513440405199
f(29) = 2797.511672 | 2 sqrt(oppose(f(29)) = 105.783017 | zz_28 = 95.8706342282453
f(30) = 2923.113829 | 2 sqrt(oppose(f(30)) = 108.131657 | zz_29 = 98.8311942181937
f(31) = 3049.671093 | 2 sqrt(oppose(f(31)) = 110.447654 | zz_30 = 101.317851005731
f(32) = 3177.152642 | 2 sqrt(oppose(f(32)) = 112.732473 | zz_31 = 103.725538040478
f(33) = 3305.529584 | 2 sqrt(oppose(f(33)) = 114.987470 | zz_32 = 105.446623052326
f(34) = 3434.774777 | 2 sqrt(oppose(f(34)) = 117.213903 | zz_33 = 107.168611184276
f(35) = 3564.862676 | 2 sqrt(oppose(f(35)) = 119.412942 | zz_34 = 111.02953554317
f(36) = 3695.769198 | 2 sqrt(oppose(f(36)) = 121.585677 | zz_35 = 111.874659176993
f(37) = 3827.471596 | 2 sqrt(oppose(f(37)) = 123.733126 | zz_36 = 114.320220915453
f(38) = 3959.948357 | 2 sqrt(oppose(f(38)) = 125.856241 | zz_37 = 116.226680320858
f(39) = 4093.179096 | 2 sqrt(oppose(f(39)) = 127.955916 | zz_38 = 118.790782865976
f(40) = 4227.144477 | 2 sqrt(oppose(f(40)) = 130.032988 | zz_39 = 121.370125002421
f(41) = 4361.826130 | 2 sqrt(oppose(f(41)) = 132.088245 | zz_40 = 122.946829293553
f(42) = 4497.206581 | 2 sqrt(oppose(f(42)) = 134.122430 | zz_41 = 124.256818554346
f(43) = 4633.269189 | 2 sqrt(oppose(f(43)) = 136.136243 | zz_42 = 127.516683879596
f(44) = 4769.998088 | 2 sqrt(oppose(f(44)) = 138.130346 | zz_43 = 129.578704199956
f(45) = 4907.378131 | 2 sqrt(oppose(f(45)) = 140.105362 | zz_44 = 131.087688530933
f(46) = 5045.394846 | 2 sqrt(oppose(f(46)) = 142.061886 | zz_45 = 133.497737202998
f(47) = 5184.034390 | 2 sqrt(oppose(f(47)) = 144.000478 | zz_46 = 134.756509753374
f(48) = 5323.283510 | 2 sqrt(oppose(f(48)) = 145.921671 | zz_47 = 138.116042054533
f(49) = 5463.129504 | 2 sqrt(oppose(f(49)) = 147.825972 | zz_48 = 139.736208952121
f(50) = 5603.560189 | 2 sqrt(oppose(f(50)) = 149.713863 | zz_49 = 141.123707404021
f(51) = 5744.563871 | 2 sqrt(oppose(f(51)) = 151.585802 | zz_50 = 143.111845807621
f(52) = 5886.129311 | 2 sqrt(oppose(f(52)) = 153.442228 | zz_51 = 146.000982486766
f(53) = 6028.245707 | 2 sqrt(oppose(f(53)) = 155.283556 | zz_52 = 147.42276534256
f(54) = 6170.902661 | 2 sqrt(oppose(f(54)) = 157.110186 | zz_53 = 150.053520420785
f(55) = 6314.090162 | 2 sqrt(oppose(f(55)) = 158.922499 | zz_54 = 150.925257612241
f(56) = 6457.798562 | 2 sqrt(oppose(f(56)) = 160.720858 | zz_55 = 153.024693811199
f(57) = 6602.018559 | 2 sqrt(oppose(f(57)) = 162.505613 | zz_56 = 156.112909294238
f(58) = 6746.741176 | 2 sqrt(oppose(f(58)) = 164.277097 | zz_57 = 157.597591817594
f(59) = 6891.957747 | 2 sqrt(oppose(f(59)) = 166.035632 | zz_58 = 158.849988171421
f(60) = 7037.659899 | 2 sqrt(oppose(f(60)) = 167.781523 | zz_59 = 161.188964137596
f(61) = 7183.839537 | 2 sqrt(oppose(f(61)) = 169.515068 | zz_60 = 163.030709687182
f(62) = 7330.488834 | 2 sqrt(oppose(f(62)) = 171.236548 | zz_61 = 165.5370691879
f(63) = 7477.600214 | 2 sqrt(oppose(f(63)) = 172.946237 | zz_62 = 167.184439978175
f(64) = 7625.166341 | 2 sqrt(oppose(f(64)) = 174.644397 | zz_63 = 169.094515415569
f(65) = 7773.180110 | 2 sqrt(oppose(f(65)) = 176.331280 | zz_64 = 169.911976479412
f(66) = 7921.634633 | 2 sqrt(oppose(f(66)) = 178.007131 | zz_65 = 173.411536519592
f(67) = 8070.523232 | 2 sqrt(oppose(f(67)) = 179.672182 | zz_66 = 174.754191523366
f(68) = 8219.839426 | 2 sqrt(oppose(f(68)) = 181.326660 | zz_67 = 176.44143429771
f(69) = 8369.576929 | 2 sqrt(oppose(f(69)) = 182.970784 | zz_68 = 178.3774077761
f(70) = 8519.729633 | 2 sqrt(oppose(f(70)) = 184.604763 | zz_69 = 179.916484020257
f(71) = 8670.291606 | 2 sqrt(oppose(f(71)) = 186.228801 | zz_70 = 182.207078484366
f(72) = 8821.257084 | 2 sqrt(oppose(f(72)) = 187.843095 | zz_71 = 184.874467848387
f(73) = 8972.620462 | 2 sqrt(oppose(f(73)) = 189.447834 | zz_72 = 185.598783677707
f(74) = 9124.376290 | 2 sqrt(oppose(f(74)) = 191.043202 | zz_73 = 187.228922583502
f(75) = 9276.519263 | 2 sqrt(oppose(f(75)) = 192.629377 | zz_74 = 189.416158656017
f(76) = 9429.044219 | 2 sqrt(oppose(f(76)) = 194.206531 | zz_75 = 192.026656360714
f(77) = 9581.946131 | 2 sqrt(oppose(f(77)) = 195.774831 | zz_76 = 193.079726603846
f(78) = 9735.220105 | 2 sqrt(oppose(f(78)) = 197.334438 | zz_77 = 195.265396679529
f(79) = 9888.861370 | 2 sqrt(oppose(f(79)) = 198.885508 | zz_78 = 196.876481840958
f(80) = 10042.865275| 2 sqrt(oppose(f(80)) = 200.428194 | zz_79 = 198.015309676252
```

```
f(81) = 10197.227289  | 2 sqrt(oppose(f(81)) = 201.962643   | zz_80 = 201.264751943704
f(82) = 10351.942989  | 2 sqrt(oppose(f(82)) = 203.488997   | zz_81 = 202.493594514141
f(83) = 10507.008062  | 2 sqrt(oppose(f(83)) = 205.007396   | zz_82 = 204.189671803105
f(84) = 10662.418300  | 2 sqrt(oppose(f(84)) = 206.517973   | zz_83 = 205.394697202163
f(85) = 10818.169591  | 2 sqrt(oppose(f(85)) = 208.020860   | zz_84 = 207.906258887806
f(86) = 10974.257924  | 2 sqrt(oppose(f(86)) = 209.516185   | zz_85 = 209.576509716856
f(87) = 11130.679380  | 2 sqrt(oppose(f(87)) = 211.004070   | zz_86 = 211.690862595365
f(88) = 11287.430129  | 2 sqrt(oppose(f(88)) = 212.484636   | zz_87 = 213.347919359713
f(89) = 11444.506429  | 2 sqrt(oppose(f(89)) = 213.958000   | zz_88 = 214.547044783491
f(90) = 11601.904622  | 2 sqrt(oppose(f(90)) = 215.424276   | zz_89 = 216.169538508264
f(91) = 11759.621132  | 2 sqrt(oppose(f(91)) = 216.883574   | zz_90 = 219.067596349021
f(92) = 11917.652461  | 2 sqrt(oppose(f(92)) = 218.336002   | zz_91 = 220.714918839314
f(93) = 12075.995185  | 2 sqrt(oppose(f(93)) = 219.781666   | zz_92 = 221.430705554693
f(94) = 12234.645957  | 2 sqrt(oppose(f(94)) = 221.220668   | zz_93 = 224.007000254604
f(95) = 12393.601500  | 2 sqrt(oppose(f(95)) = 222.653107   | zz_94 = 224.983324669582
f(96) = 12552.858605  | 2 sqrt(oppose(f(96)) = 224.079081   | zz_95 = 227.421444279679
f(97) = 12712.414131  | 2 sqrt(oppose(f(97)) = 225.498684   | zz_96 = 229.337413305525
f(98) = 12872.265001  | 2 sqrt(oppose(f(98)) = 226.912009   | zz_97 = 231.250188700499
f(99) = 13032.408202  | 2 sqrt(oppose(f(99)) = 228.319147   | zz_98 = 231.98723525318
f(100) = 13192.840780 | 2 sqrt(oppose(f(100)) = 229.720184  | zz_99 = 233.693404178908
f(101) = 13353.559842 | 2 sqrt(oppose(f(101)) = 231.115208  | zz_100 = 236.524229665816
f(102) = 13514.562551 | 2 sqrt(oppose(f(102)) = 232.504301  | zz_101 = 237.769820480925
f(103) = 13675.846126 | 2 sqrt(oppose(f(103)) = 233.887547  | zz_102 = 239.555477573328
f(104) = 13837.407840 | 2 sqrt(oppose(f(104)) = 235.265024  | zz_103 = 241.049157796217
f(105) = 13999.245019 | 2 sqrt(oppose(f(105)) = 236.636810  | zz_104 = 242.823271934223
f(106) = 14161.355040 | 2 sqrt(oppose(f(106)) = 238.002984  | zz_105 = 244.070898497078
f(107) = 14323.735327 | 2 sqrt(oppose(f(107)) = 239.363617  | zz_106 = 247.136990074898
f(108) = 14486.383356 | 2 sqrt(oppose(f(108)) = 240.718785  | zz_107 = 248.101990060148
f(109) = 14649.296646 | 2 sqrt(oppose(f(109)) = 242.068558  | zz_108 = 249.573689644707
f(110) = 14812.472765 | 2 x sqrt(oppose(f(110)) = 243.413005| zz_109=251.014947795016
f(111) = 14975.909323 | 2 x sqrt(oppose(f(111)) = 244.752196| zz_110=253.069986747999
```



S'enhardir : il se passe quoi sur la droite critique ?[1], Denise Vella-Chemla, 23 novembre 2024

Quel est notre objectif courant ? On cherche une opération qui permettrait de rassembler certains termes, par paquets (de 2 peut-être ?), dans la somme bien connue

$$\sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Dans cette vaine tentative, on trouve dans le site de Gérard Villemin comment trouver la partie réelle et la partie imaginaire d'un entier élevé à une puissance complexe "directement" ainsi :

$$\begin{aligned} n^{\frac{1}{2}+ib} &= (\ \cosh\ (a\ln n)\ +\ \sinh\ (a\ln n))\ .\ (\cos(b\ln n)+i\sin(b\ln n)) \\ &= (\ \cos\ (i\,a\ln n)\ -\ i\ \sin\ (i\,a\ln n))\ .\ (\cos(b\ln n)+i\sin(b\ln n)) \end{aligned}$$

On vérifie cela par programme au cas où quelque chose apparaisse. Voici le programme utilisé :

```
import mpmath ; from mpmath import * ; import math ; from math import cos,sin,cosh,sinh,log
lesa = [0.48,0.49,0.5,0.51,0.52]
lesb = [14.11,14.12,14.13,14.14,14.15]
for n in range(1,25):
    #for a in lesa:
    for a in [0.5]:
        #for b in lesb:
        for b in [14.13]:
            res = n**(a+1j*b)
            print(n,' --> ', res)
            print('lesh = ',cosh(a*log(n))+sinh(a*log(n)))
            print('le cos = ',cos(b*log(n)))
            print('le sin = ',sin(b*log(n)))
            print('du coup, partie reelle = ',(cosh(a*log(n))+sinh(a*log(n)))*cos(b*log(n)))
            print(' et partie imaginaire = ',(cosh(a*log(n))+sinh(a*log(n)))*sin(b*log(n)))
        print('')
    print('')
```

Le résultat du programme est fourni en annexe. On voit apparaître les racines carrées comme parties réelles en sommant côté hyperbolique (le cosh et le sinh), ce qui est normal, on a $\exp\left(\frac{1}{2}\ln x\right) = \sqrt{x}$ par exemple.

On réalise par cette expérimentation l'existence de "nombres bases" qui permettent de calculer les racines carrées, ou les racines cubiques en les élevant à des puissances correspondant aux logarithmes népériens. On a par exemple

$$\begin{aligned} \text{Base_racine_2} &= \exp(1/2) = 1.6487212707... \\ \text{Base_racine_3} &= \exp(1/3) = 1.39561242509... \end{aligned}$$

On a $\text{Base_racine_2}^{\ln n} = \sqrt{n}$, ou bien $\text{Base_racine_3}^{\ln n} = \sqrt[3]{n}$, etc.

[1] ou on ne nous dit pas tout ;-) !

Le nombre base Base_racine_$k = \exp\left(\frac{1}{k}\right)$, élevé à la puissance le logarithme népérien d'un nombre n permet d'obtenir la racine k-ième de ce nombre n.

$$\text{Base_racine_}k^{\ln n} = \sqrt[k]{n}.$$

Le programme est fourni ci-après. Il permet d'observer cette propriété des nombres bases.

D'autre part, le programme calcule pour chaque partie imaginaire z d'un zéro non trivial de la fonction ζ de Riemann la fonction suivante :

$$f(z) = \exp\left(W\left(-\left(\left(\frac{z}{2}\right)^2\right)\left(\frac{2\pi}{180}\right)\right)\right)$$

Comme on réalise qu'il y a comme un tempo de valse $[1, 1, 2, 3, 3, 4, 5, 5, 6, \text{etc.}]$, on met en regard des images obtenues par la fonction f des multiples de $2/3$ avec un tout petit (shift) décalage pour être raccord en fin de liste. La fonction qui a dû être utilisée $W(z)$ s'appelle fonction de Lambert, elle permet de trouver la solution y, lorsqu'on connaît x, d'une équation de la forme $y \ln y = x$.

```
import math ; from math import exp, pi, log,sqrt ; from scipy.special import lambertw

zeros = [  14.134725141734693790457251983562 5,  21.022039638771554992628479593896 9,
           25.010857580145688763213790992562 8,  30.424876125859513210311897530584 0,
           32.935061587739189690662368964074 7,  37.586178158825671257217763480705 3,
           40.918719012147495187398126914633 4,  43.327073280914999519496122165406 8,
           48.005150881167159727942472749427 7,  49.773832477672302181916784678563 8,
           52.970321477714460644147296608880 8,  56.446247697063394804367759476706 0,
           59.347044002602353079653648674992 2,  60.831778524609809844259901824524 1,
           65.112544048081606660875054253183 6,  67.079810529494173714478828896522 1,
           69.546401711173979252926857526554 7,  72.067157674481907582522107969826 1,
           75.704690699083933168326916762030 5,  77.144840068874805372682664856304 7,
           79.337375020249367922763592877116 1,  82.910380854086030183164837494770 6,
           84.735492980517050105735311206827 6,  87.425274613125229406531667850919 1,
           88.809111207634465423682348079509 5,  92.491899270558484296259725241810 5,
           94.651344040519886966597925815208 0,  95.870634228245309758741029219246 7,
           98.831194218193692233324420138622 4]

print('exp(0.5)**ln(2) = ',exp(0.5)**log(2))
print('sqrt(2) = ',sqrt(2))
print('exp(0.5)**ln(3) = ',exp(0.5)**log(3))
print('sqrt(3) = ',sqrt(3))
print('exp(0.5)**ln(5) = ',exp(0.5)**log(5))
print('sqrt(5) = ',sqrt(5))
print('la base des racines carrees est :  ',exp(0.5),' :  elevee a la puissance
log(n), elle fournit la racine carree de n.')
print('')
print('exp(1/3)**log(2) = ',exp(1/3)**log(2))
print('sqrt[3](2) = ',2**(1/3))
print('exp(1/3)**log(3) = ',exp(1/3)**log(3))
print('sqrt[3](3) = ',3**(1/3))
print('exp(1/3)**log(5) = ',exp(1/3)**log(5))
print('sqrt[3](5) = ',5**(1/3))
print('la base des racines cubiques est :  ',exp(1/3),' :  elevee a la puissance
log(n), elle fournit la racine cubique de n.')
```

```
premier = 1
for z in zeros:
     print(z,' --> ',exp(lambertw(-((z/2)**2)*(2*pi)/180)),' ',premier*(2/3+0.08))
     premier = premier+1
```

Voici son résultat :

```
 14.134725141734695   -->   1.0772375996941315   0.7466666666666666
 21.022039638771556   -->   1.918950321922641    1.4933333333333332
 25.01085758014569    -->   2.485787905112672    2.2399999999999998
 30.424876125859512   -->   3.3427514619545198   2.9866666666666664
 32.93506158773919    -->   3.7730944772557673   3.733333333333333
 37.586178158825675   -->   4.623993042930546    4.4799999999999995
 40.9187190121475     -->   5.2754106660147295   5.226666666666667
 43.327073280915      -->   5.767411052076091    5.973333333333333
 48.00515088116716    -->   6.773033808741858    6.719999999999999
 49.7738324776723     -->   7.170157261188014    7.466666666666666
 52.970321477714464   -->   7.911057195740718    8.213333333333333
 56.44624769706339    -->   8.750192709322919    8.959999999999999
 59.34704400260235    -->   9.476820016840236    9.706666666666665
 60.83177852460981    -->   9.857909171062472    10.453333333333333
 65.1125440480816     -->   10.991060813218892   11.2
 67.07981052949417    -->   11.528786717393535   11.946666666666665
 69.54640171117398    -->   12.217950949632758   12.693333333333332
 72.0671576744819     -->   12.939310177227325   13.439999999999998
 75.70469069908393    -->   14.010383679015998   14.186666666666666
 77.1448400688748     -->   14.444197041546738   14.933333333333332
 79.33737502024937    -->   15.115206731375853   15.679999999999998
 82.91038085408603    -->   16.235821766491938   16.426666666666666
 84.73549298051705    -->   16.82112136372026    17.173333333333332
 87.42527461312523    -->   17.69948257769329    17.919999999999998
 88.80911120763446    -->   18.15866459715959    18.666666666666664
 92.49189927055849    -->   19.40463662233388    19.41333333333333
 94.65134404051989    -->   20.151331589735214   20.159999999999997
 95.87063422824531    -->   20.578169388811915   20.906666666666666
 98.83119421819369    -->   21.630211644248604   21.653333333333332
```

Annexe : résultat du premier programme, pour vérifier les formules avec cosinus et sinus hyperboliques

```
1 --> (1+0j)
lesh = 1.0
le cos = 1.0
le sin = 0.0
du coup, partie reelle = 1.0
et partie imaginaire = 0.0
```

```
2 --> (-1.3188208179886864-0.5105993047778777j)
lesh = 1.414213562373095
le cos = -0.9325471435697897
le sin = -0.3610482308775741
du coup, partie reelle = -1.3188208179886864
et partie imaginaire = -0.5105993047778777

3 --> (-1.7026318514933363+0.31787541314227746j)
lesh = 1.7320508075688772
le cos = -0.9830149577905086
le sin = 0.18352545534645742
du coup, partie reelle = -1.7026318514933363
et partie imaginaire = 0.31787541314227746

4 --> (1.4785766999206957+1.3467779855832307j)
lesh = 2.0
le cos = 0.7392883499603479
le sin = 0.6733889927916153
du coup, partie reelle = 1.4785766999206957
et partie imaginaire = 1.3467779855832307

5 --> (-1.6357872631371633-1.5245327250532306j)
lesh = 2.23606797749979
le cos = -0.7315463034206066
le sin = -0.681791761428404
du coup, partie reelle = -1.6357872631371633
et partie imaginaire = -1.5245327250532306

6 --> (2.407773296076462+0.4501419272863697j)
lesh = 2.449489742783178
le cos = 0.9829693319477565
le sin = 0.183769672280769
du coup, partie reelle = 2.407773296076462
et partie imaginaire = 0.4501419272863697

7 --> (-1.883459943740704+1.8581115790835234j)
lesh = 2.6457513110645907
le cos = -0.7118809450699439
le sin = 0.702300163780647
du coup, partie reelle = -1.883459943740704
et partie imaginaire = 1.8581115790835234

8 --> (-1.262313829719481-2.531119079636306j)
lesh = 2.82842712474619
le cos = -0.44629533449010284
le sin = -0.8948857326007423
du coup, partie reelle = -1.2623138297194807
et partie imaginaire = -2.5311190796363054

9 --> (2.7979104434392528-1.0824496064452904j)
lesh = 3.0
le cos = 0.9326368144797509
le sin = -0.36081653548176346
du coup, partie reelle = 2.7979104434392528
et partie imaginaire = -1.0824496064452904
```

```
10 --> (1.3788849469027102+2.845817334827573j)
lesh = 3.16227766016838
le cos = 0.4360417063532902
le sin = 0.899926458284515
du coup, partie reelle = 1.3788849469027105
et partie imaginaire = 2.8458173348275735

11 --> (-2.5887751822714606+2.0732204551507216j)
lesh = 3.3166247903554
le cos = -0.7805450860162132
le sin = 0.6250994870386172
du coup, partie reelle = -2.5887751822714606
et partie imaginaire = 2.0732204551507216

12 --> (-2.9455793927390714-1.8230639157942106j)
lesh = 3.4641016151377544
le cos = -0.8503155276586587
le sin = -0.5262732212668404
du coup, partie reelle = -2.9455793927390714
et partie imaginaire = -1.8230639157942106

13 --> (0.4116436689178993-3.5819756405983294j)
lesh = 3.6055512754639896
le cos = 0.114169411961816
le sin = -0.993461295356942
du coup, partie reelle = 0.41164366891789933
et partie imaginaire = -3.58197564059833

14 --> (3.432696664132815-1.4888228947901916j)
lesh = 3.741657386773941
le cos = 0.9174267735647724
le sin = -0.39790465584927737
du coup, partie reelle = 3.4326966641328145
et partie imaginaire = -1.4888228947901914

15 --> (3.269754966309667+2.0757414242369565j)
lesh = 3.8729833462074166
le cos = 0.8442471020464223
le sin = 0.5359541311401731
du coup, partie reelle = 3.2697549663096668
et partie imaginaire = 2.075741424236956

16 --> (0.37237811509675045+3.9826290988989914j)
lesh = 4.0
le cos = 0.09309452877418761
le sin = 0.9956572747247479
du coup, partie reelle = 0.37237811509675045
et partie imaginaire = 3.9826290988989914

17 --> (-2.8506298260430993+2.9789108068006147j)
lesh = 4.123105625617661
le cos = -0.6913792866065762
le sin = 0.722491994454874
du coup, partie reelle = -2.8506298260430993
et partie imaginaire = 2.9789108068006147
```

```
18 --> (-4.242640556183696-0.0010540518471141614j)
lesh = 4.242640687119285
le cos = -0.9999999691381858
le sin = -0.0002484424029388766
du coup, partie reelle = -4.242640556183696
et partie imaginaire = -0.0010540518471141614

19 --> (-3.1467916150920603-3.0162398000136372j)
lesh = 4.358898943540673
le cos = -0.7219235077140753
le sin = -0.691972867249725
du coup, partie reelle = -3.14679161509206
et partie imaginaire = -3.0162398000136363

20 --> (-0.36542982089876647-4.457180840620885j)
lesh = 4.47213595499958
le cos = -0.08171259205352151
le sin = -0.9966559347637954
du coup, partie reelle = -0.36542982089876647
et partie imaginaire = -4.457180840620885

21 --> (2.6161909053591517-3.7623855659296885j)
lesh = 4.582575694955841
le cos = 0.5708996598220649
le sin = -0.8210198404515269
du coup, partie reelle = 2.616190905359152
et partie imaginaire = -3.7623855659296894

22 --> (4.4727155265233-1.4123794882386964j)
lesh = 4.690415759823431
le cos = 0.9535861543096288
le sin = -0.3011203186584605
du coup, partie reelle = 4.4727155265233005
et partie imaginaire = -1.4123794882386966

23 --> (4.548988332160371+1.5187841037714367j)
lesh = 4.795831523312719
le cos = 0.9485296366328896
le sin = 0.3166883774771006
du coup, partie reelle = 4.548988332160371
et partie imaginaire = 1.5187841037714367

24 --> (2.953836256212608+3.9083054347739865j)
lesh = 4.898979485566357
le cos = 0.6029493009544873
le sin = 0.7977795061785525
du coup, partie reelle = 2.9538362562126084
et partie imaginaire = 3.9083054347739874
```

Régression logarithmique pour parties imaginaires des 28 premiers zéros de ζ
Denise Vella-Chemla, 23 novembre 2024

On utilise la librairie python `limfit`, qui permet d'effectuer une régression logarithmique pour trouver par une formule de la forme $y = a \ln (x + b) + c$ les parties imaginaires des zéros non triviaux de la fonction ζ de Riemann.

On utilise le programme fourni un peu plus loin.

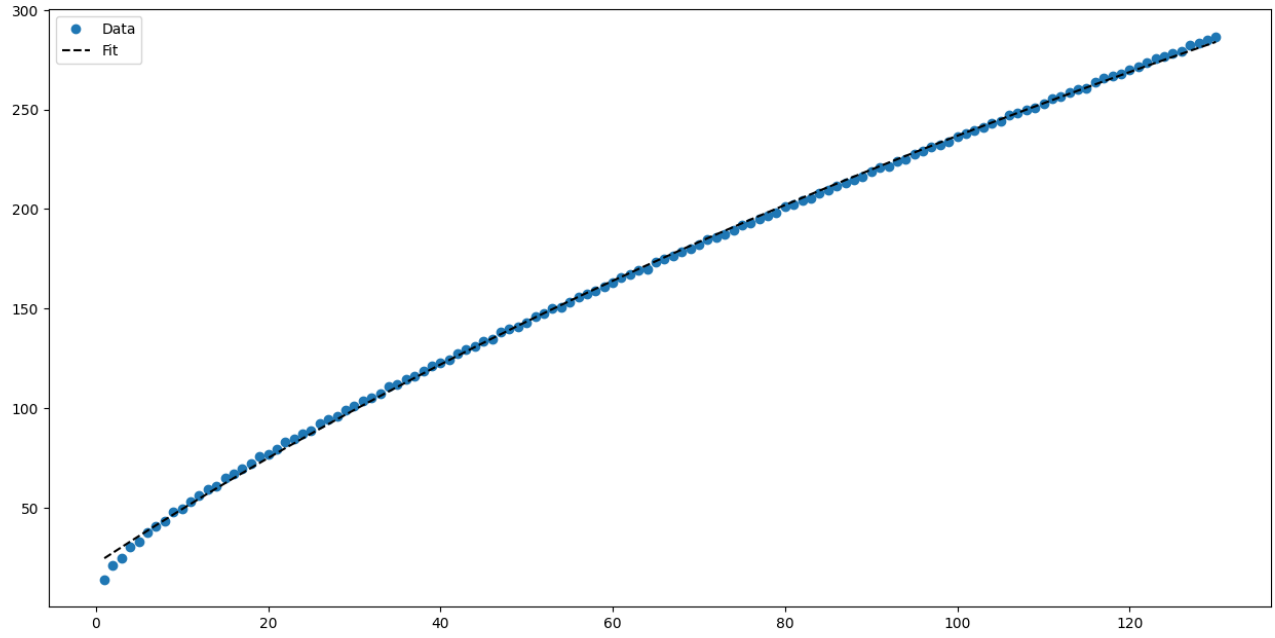
Ce programme dessine initialement le graphique de corrélation ci-après, il fournit en sortie les éléments caractéristiques de la régression logarithmique effectuée, qui sont reportés ci-dessous, puis on fait imprimer au programme, en dernier lieu, les valeurs trouvées en utilisant la fonction

$$f(x) = 402 \ln (x + 147) - 1978$$

à des fins de vérification.

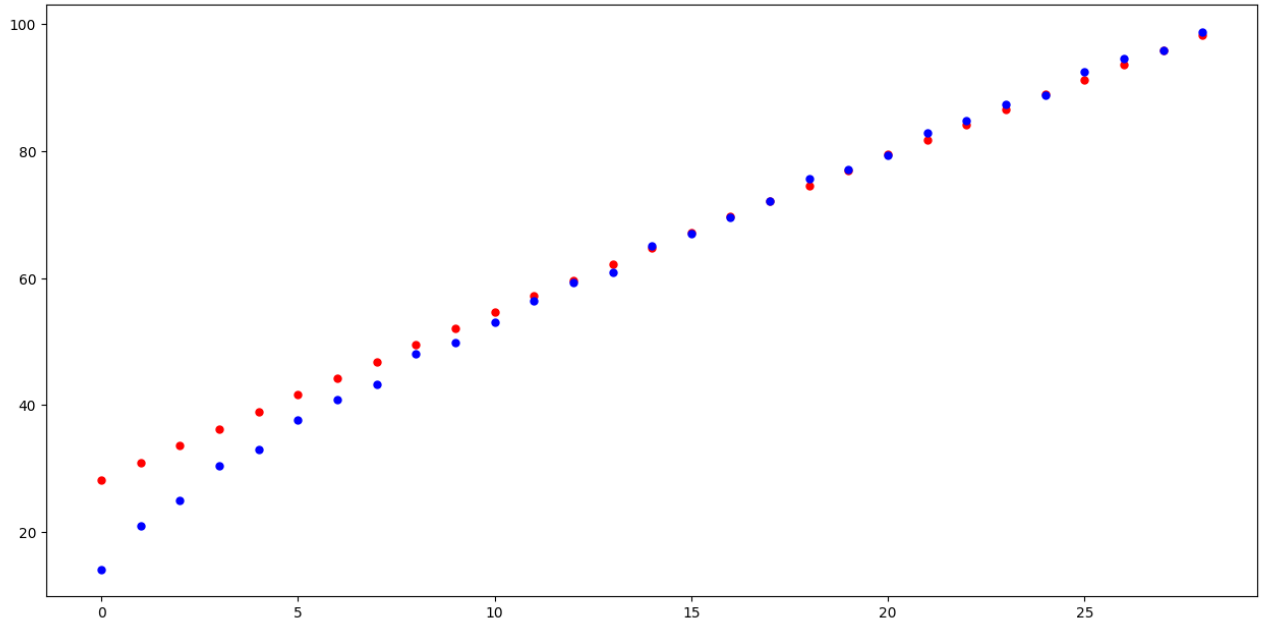
```
"""
Soit (z_k)_{1≤k≤130} la liste des parties imaginaires des 130 premiers zeros non triviaux de la
fonction zeta de Riemann.
On souhaite ajuster ces donnees a un modele logarithmique de parametres a,b,c reels, avec b0,
soit :

                        y_k = f(x_k) = a ln(x_k + b) + c,    x_k = k,    1 ≤ k ≤ 130.

"""

import lmfit
import matplotlib.pyplot as plt
import numpy as np

z = np.array([  14.134725141734693790457251983562 5,  21.022039638771554992628479593896 9,
                25.010857580145688763213790992562 8,  30.424876125859513210311897530584 0,
                32.935061587739189690662368964074 7,  37.586178158825671257217763480705 3,
                40.918719012147495187398126914633 4,  43.327073280914999519496122165406 8,
                48.005150881167159727942472749427 7,  49.773832477672302181916784678563 8,
                52.970321477714460644147296608880 8,  56.446247697063394804367759476706 0,
                59.347044002602353079653648674992 2,  60.831778524609809844259901824524 1,
                65.112544048081606660875054253183 6,  67.079810529494173714478828896522 1,
                69.546401711173979252926857526554 7,  72.067157674481907582522107969826 1,
                75.704690699083933168326916762030 5,  77.144840068874805372682664856304 7,
                79.337375020249367922763592877116 1,  82.910380854086030183164837494770 6,
                84.735492980517050105735311206827 6,  87.425274613125229406531667850919 1,
                88.809111207634465423682348079509 5,  92.491899270558484296259725241810 5,
                94.651344040519886966597925815208 0,  95.870634228245309758741029219246 7,
                98.831194218193692233324420138622 4]

def f(x, a, b, c):
     return a*np.log(x+b) + c
```

```
model = lmfit.Model(f)
params = model.make_params(a=1, b=dict(value=0.1, min=0.001), c=0.1)
x = np.arange(1, len(z)+1)
r = model.fit(z, params, x=x)
y = r.best_fit
print(r.fit_report())
_, ax = plt.subplots(figsize=(15, 5))
plt.plot(x, z, "o", label="Data")
plt.plot(x, y, "k--", label="Fit")
plt.legend()
plt.show()
print('Verification')
import math
from math import log

for x in range(29):
      res1 = 402*log(x+147)-1978
      res2 = z[x]
      print(x,' --> ',res1,' ',res2)
      plt.scatter(x,res1,s=25,color='red')
      plt.scatter(x,res2,s=25,color='blue')
plt.show()
```

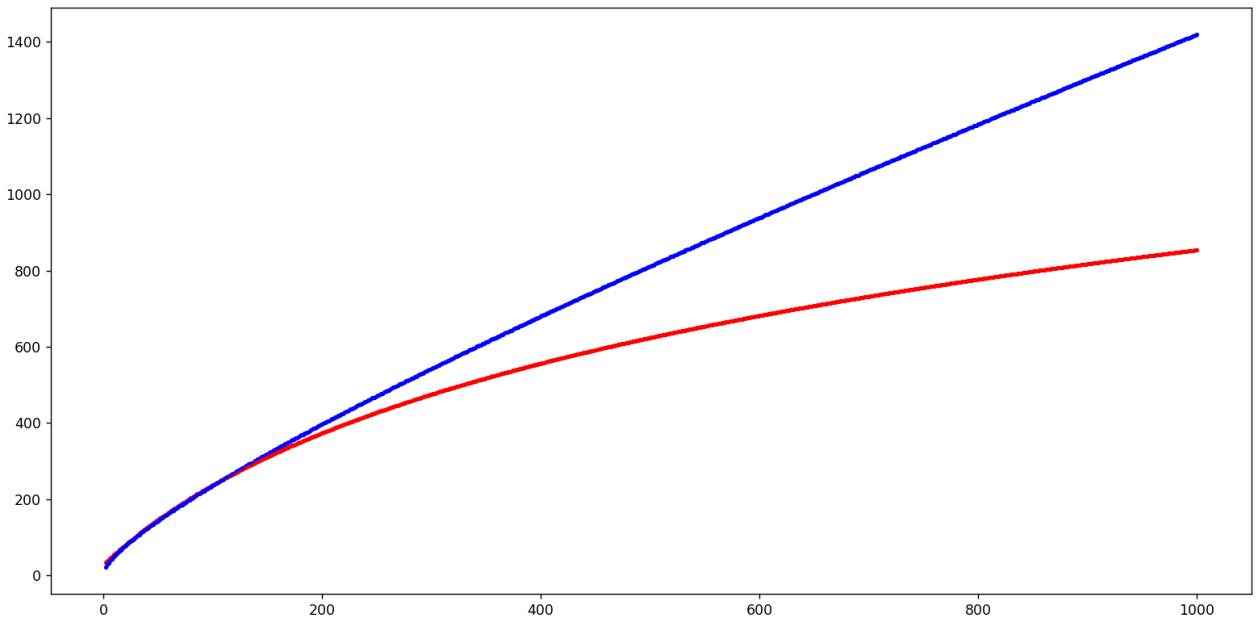


```
[[Model]]
Model(f)
[[Fit Statistics]]
fitting method = leastsq
function evals = 102
data points = 130
variables = 3
chi-square = 457.447882
reduced chi-square = 3.60195183
Akaike info crit = 169.556706
Bayesian info crit = 178.159310
R-squared = 0.99936890
[[Variables]]
a:  402.423515 +/- 10.6902515 (2.66%) (init = 1)
b:  141.683692 +/- 5.22597956 (3.69%) (init = 0.1)
c:  -1971.54485 +/- 67.3104952 (3.41%) (init = 0.1)
[[Correlations]] (unreported correlations are < 0.100)
C(a, c) = -0.9999
C(b, c) = -0.9975
C(a, b) = +0.9965

  0  -->  28.153899885051942  14.134725142
  1  -->  30.879334053174034  21.022039639
  2  -->  33.58641499007467   25.01085758
  3  -->  36.27538822669476   30.424876126
  4  -->  38.94649439959949   32.935061588
  5  -->  41.59996938020322   37.586178159
  6  -->  44.236044399759066  40.918719012
  7  -->  46.85494617027916   43.327073281
  8  -->  49.4568970015373    48.005150881
  9  -->  52.04211491431397   49.773832478
 10  -->  54.61081375001959   52.970321478
 11  -->  57.163203276840704  56.446247697
 12  -->  59.699489292533144  59.347044003
 13  -->  62.21987372399826   60.831778525
 14  -->  64.72455472375418   65.112544048
 15  -->  67.21372676341821   67.079810529
 16  -->  69.68758072431842   69.546401711
 17  -->  72.1463039853279    72.067157674
 18  -->  74.59008050803322   75.704690699
 19  -->  77.01909091933067   77.144840069
 20  -->  79.43351259153587   79.33737502
 21  -->  81.83351972010996   82.910380854
 22  -->  84.21928339907572   84.735492981
 23  -->  86.59097169420556   87.425274613
 24  -->  88.94874971406944   88.809111208
 25  -->  91.29277967900816   92.491899271
 26  -->  93.62322098810728   94.651344041
 27  -->  95.9402302842409    95.870634228
 28  -->  98.24396151725296   98.831194218
```

Vérification : on applique la formule pour la vérifier en plottant les parties imaginaires effectives des premiers zéros non triviaux de ζ (en bleu) et les valeurs calculées par la formule logarithmique (en rouge). Une seule couleur apparaît quand les zéros se chevauchent.



Mais en allant jusqu'à 1000 zéros, on obtient le graphique ci-dessous, la régression logarithmique $y = 402 \ln(x + 147) - 1978$ n'est pas une bonne idée du tout.



Une petite découverte tout extraordinaire concernant les exposants complexes de partie réelle $\frac{1}{2}$ et l'inversion, (ou les complexes, c'est pas simple), Denise Vella-Chemla, 21 novembre 2024

Quel est mon objectif courant ? Je cherche à trouver une opération qui me permettrait de rassembler certains termes, par paquets (de 4 idéalement), dans la somme bien connue

$$\sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Ce faisant, en cherchant si éventuellement il y aurait un lien entre deux termes, le terme concernant n et le terme concernant $\frac{1}{n}$ (qui ne sont d'ailleurs pas tous les deux dans la somme ci-dessus), j'ai réalisé qu'il semblerait qu'une certaine propriété soit vérifiée lorsque l'exposant choisi est de partie réelle 0.5 et seulement dans ce cas. Expliquons cette propriété algébriquement :

$$\frac{1}{n^{\frac{1}{2}+ib}} \times n = n^{\frac{1}{2}-ib}$$

qu'on peut énoncer ainsi "si on sait à quoi est égale une fraction de numérateur 1 et de dénominateur d'exposant complexe, dont la partie réelle est $\frac{1}{2}$, on obtient à quoi est égal le produit de la fraction obtenue en inversant le nombre entier au dénominateur, par le nombre entier en question, en "faisant monter" le nombre entier au numérateur, et en l'élevant à la puissance conjuguée de la puissance initiale.

Si la partie réelle de l'exposant est un nombre réel entre 0 et 1, alors il faut prendre son complémentaire et conjuguer également, ainsi :

$$\frac{1}{n^{\frac{1}{3}+ib}} \times n = n^{\frac{2}{3}-ib.}$$

Voici le programme utilisé :

```
import mpmath
from mpmath import *

print('On note f(x) = 1/(x**(0.5+bi)).')
print('aux parties imaginaires (variable b) entieres, que donne l inversion ?')
x = 5
print('x = ',x)
print('f(5) = ',1/(x**(0.5+3*1j)))
print('(x f(x)).real = ',5*((1/(x**(0.5+3*1j))).real))
print('(x f(x)).imag = ',5*((1/(x**(0.5+3*1j))).imag))
y=1/5
print('f(1/5) = ',1/(y**(0.5+3*1j)))
print('')
print('aux zeros non triviaux l inversion a aussi ce comportement (on teste avec
                le troisieme et le quatrieme zero et pour les entiers de 1 a 4)')
for k in range(1,5):
     print('k = ',k)
     print('k-ieme zero = ',zetazero(k))
     for x in range(1,5):
          print('x = ',x)
          print('f(',x,') = ',1/(x**zetazero(k)))
          print('partie reelle fois', x,' = ',(x*(1/(x**zetazero(k)))).real)
```

```
          print('partie imaginaire fois', x,' = ',(x*(1/(x**zetazero(k)))).imag)
          print('f(',1/x,') = ',1/((1/x)**zetazero(k)))
          print('')
print('')
print('tandis qu avec un complexe en exposant qui ne serait pas un zero, ce
comportement n a pas l air de se produire :  prenons d abord
un complexe de partie imaginaire plus grande que 1 :  k = 0.24565 + 7.25689575 i.')
k=0.24565+7.25689575*1j
for x in range(1,5):
     print('x = ',x)
     print('f(x) = ',1/(x**k))
     print('(f(x).real) fois x = ',x*((1/(x**k)).real))
     print('(f(x).imag) fois x = ',x*((1/(x**k)).imag))
     print('f(1/x) = ',1/((1/x)**k))
     print('')

print('')
print('puis avec un complexe en exposant, ce complexe n etant pas un zero, ce
comportement n a pas l air de se produire avec
un complexe de partie imaginaire plus petite que 1 :  k = 0.24565 + 0.725689575 i.')
k=0.24565+0.725689575*1j
for x in range(1,5):
     print('x = ',x)
     print('f(x) = ',1/(x**k))
     print('(f(x).real) fois x = ',x*((1/(x**k)).real))
     print('(f(x).imag) fois x = ',x*((1/(x**k)).imag))
     print('f(1/x) = ',1/((1/x)**k))
     print('')

print('')
print('')
print('Refaisons les memes tests mais en multipliant les memes nombres x par -i')
print('x = -5 i')
x = -5*1j
print('f(-5 i) = ',1/(x**(0.5+3*1j)))
print('(f(x).real) fois x = ',(-5*1j)*((1/(x**(0.5+3*1j))).real))
print('(f(x).imag) fois x = ',(-5*1j)*((1/(x**(0.5+3*1j))).imag))
y=1/(-5*1j)
print('f(1/(-5*1j)) = ',1/(y**(0.5+3*1j)))
print('')
print('tandis qu aux zeros non triviaux, a nouveau, l inversion n a pas ce
comportement, pourquoi ?')
print('(tests pour le troisieme et le quatrieme zero et les entiers de 1 a 4)')
for k in range(3,4):
     print(k,' ::::')
     print(zetazero(k))
     for x in range(1,5):
          xprime = -x*1j
          print('x = ',xprime)
          print('f(x) = ',1/(xprime**zetazero(k)))
          print('(f(x).real) fois x = ',xprime*(1/(xprime**zetazero(k))).real)
          print('(f(x).imag) fois x = ',xprime*(1/(xprime**zetazero(k))).imag)
          print('f(1/x) = ',1/((1/xprime)**zetazero(k)))
          print('')
```

```
print('')
print('et avec un complexe en exposant, ce complexe n etant pas, un zero, est-ce-que
cela marche, on le prend
de partie imaginaire plus grande que 1.  ')
print('on prend comme exposant k = 0.24565 + 7.25689575 i et on calcule les termes
correspondant aux entiers de 1 a 4.')
k=0.24565+7.25689575*1j
for x in range(1,5):
     xprime = -x*1j
     print('x = ',xprime)
     print('f(x) = ',1/(xprime**k))
     print('(f(x).real) fois x = ',xprime*((1/(xprime**k)).real))
     print('(f(x).imag) fois x = ',xprime*((1/(xprime**k)).imag))
     print('f(1/x) = ',1/((1/xprime)**k))
     print('')

print('')
print('et avec un complexe en exposant, ce complexe n etant pas un zero, est-ce-que
cela marche, on le prend de partie imaginaire plus petite que 1.  ')
print('on prend comme exposant k = 0.24565 + 0.725689575 i et on calcule les termes
correspondant aux entiers de 1 a 4.')
k=0.24565+0.725689575*1j
for x in range(1,5):
     xprime = -x*1j
     print('x = ',xprime)
     print('f(x) = ',1/(xprime**k))
     print('(f(x).real) fois x = ',xprime*((1/(xprime**k)).real))
     print('(f(x).imag) fois x = ',xprime*((1/(xprime**k)).imag))
     print('f(1/x) = ',1/((1/xprime)**k))
     print('')
```

Voici le résultat du programme. On voit qu'en multipliant la partie réelle et la partie imaginaire de l'image de x par x, on obtient la partie réelle et la partie imaginaire de l'image de $\frac{1}{x}$, et ce lorsque l'exposant de la puissance de x calculée au dénominateur est de partie réelle $\frac{1}{2}$, mais que cela ne soit pas le cas lorsque l'exposant choisi n'est pas de partie réelle $\frac{1}{2}$.

```
On note f(x) = 1/(x^(0.5 + bi)).
aux parties imaginaires (variable b) entieres, que donne l inversion ?
x = 5
f(5) = (0.051727089275033826+0.44421200820681633j)
(x f(x)).real = 0.2586354463751691
(x f(x)).imag = 2.2210600410340815
f(1/5) = (0.2586354463751692-2.221060041034082j)

aux zeros non triviaux l inversion a aussi ce comportement (on teste avec le troisieme
et le quatrieme zero et pour les entiers de 1 a 4)
k = 3
k-ieme zero = (0.5 + 25.0108575801457j)
x = 1
f( 1 ) = (1.0 + 0.0j)
partie reelle fois 1 = 1.0
partie imaginaire fois 1 = 0.0
f( 1.0 ) = (1.0 + 0.0j)
```

```
x = 2
f( 2 ) = (0.0405979914536856 + 0.705940367941887j)
partie reelle fois 2 = 0.0811959829073712
partie imaginaire fois 2 = 1.41188073588377
f( 0.5 ) = (0.0811959829073712 - 1.41188073588377j)

x = 3
f( 3 ) = (-0.403443856705977 - 0.412996837541815j)
partie reelle fois 3 = -1.21033157011793
partie imaginaire fois 3 = -1.23899051262545
f( 0.3333333333333333 ) = (-1.21033157011793 + 1.23899051262544j)

x = 4
f( 4 ) = (-0.496703606179853 + 0.0573195220490328j)
partie reelle fois 4 = -1.98681442471941
partie imaginaire fois 4 = 0.229278088196131
f( 0.25 ) = (-1.98681442471941 - 0.229278088196131j)

tandis qu avec un complexe en exposant qui ne serait pas un zero, ce comportement n a
pas l air de se produire :  prenons d abord
un complexe de partie imaginaire plus grande que 1 :  k = 0.24565 + 7.25689575 i.
x = 1
f(x) = (1+0j)
(f(x).real) fois x = 1.0
(f(x).imag) fois x = 0.0
f(1/x) = (1+0j)

x = 2
f(x) = (0.2634808329349642+0.8012250856106742j)
(f(x).real) fois x = 0.5269616658699284
(f(x).imag) fois x = 1.6024501712213484
f(1/x) = (0.3703778996647515-1.1262908996512908j)

x = 3
f(x) = (-0.0902854501368382-0.7581184170019675j)
(f(x).real) fois x = -0.2708563504105165
(f(x).imag) fois x = -2.274355251005902
f(1/x) = (-0.1548914481122055+1.3006088940354603j)

x = 4
f(x) = (-0.5725394884877297+0.42221490585017685j)
(f(x).real) fois x = -2.290157953950919
(f(x).imag) fois x = 1.6888596234007074
f(1/x) = (-1.131351402077241-0.8343065156487368j)

puis avec un complexe en exposant, ce complexe n etant pas un zero, ce comportement n
a pas l air de se produire avec un complexe
de partie imaginaire plus petite que 1 :  k = 0.24565 + 0.725689575 i.
x = 1
f(x) = (1+0j)
(f(x).real) fois x = 1.0
(f(x).imag) fois x = 0.0
f(1/x) = (1+0j)
```

```
x = 2
f(x) = (0.7389641063024541-0.406590502511495j)
(f(x).real) fois x = 1.4779282126049083
(f(x).imag) fois x = -0.81318100502299
f(1/x) = (1.0387699574621443+0.5715487334177909j)

x = 3
f(x) = (0.5334218815666942-0.5462198211066936j)
(f(x).real) fois x = 1.6002656447000827
(f(x).imag) fois x = -1.638659463320081
f(1/x) = (0.9151251676253258+0.9370809909080206j)

x = 4
f(x) = (0.3807521136708347-0.6009115746389452j)
(f(x).real) fois x = 1.523008454683339
(f(x).imag) fois x = -2.4036462985557807
f(1/x) = (0.7523750698544241+1.1874153069998825j)

Refaisons les memes tests mais en multipliant les memes nombres x par -i
x = -5 i
f(-5 i) = (-0.002493121507229911 3+0.0031502775535258124j)
(f(x).real) fois x = 0.012465607536149557j
(f(x).imag) fois x = -0.015751387767629063j
f(1/(-5*1j)) = (-154.46941829967753-195.1856497023865j)

tandis qu aux zeros non triviaux, a nouveau, l inversion n a pas ce comportement,
pourquoi ?
(tests pour le troisieme et le quatrieme zero et les entiers de 1 a 4)
3 ::::
(0.5 + 25.0108575801457j)
x = (-0-1j)
f(x) = (6.12877483831982e-18 + 6.12877483831982e-18j)
(f(x).real) fois x = (0.0 - 6.12877483831982e-18j)
(f(x).imag) fois x = (0.0 - 6.12877483831982e-18j)
f(1/x) = (8.15823738333114e+16 - 8.15823738333114e+16j)

x = (-0-2j)
f(x) = (-4.0777336158888e-18 + 4.57536551290414e-18j)
(f(x).real) fois x = (0.0 + 8.1554672317776e-18j)
(f(x).imag) fois x = (0.0 - 9.15073102580828e-18j)
f(1/x) = (-1.08560420971608e+17 - 1.21808743034233e+17j)

x = (-0-3j)
f(x) = (5.85480685776386e-20 - 5.00378118388623e-18j)
(f(x).real) fois x = (0.0 - 1.75644205732916e-19j)
(f(x).imag) fois x = (0.0 + 1.50113435516587e-17j)
f(1/x) = (2.33806456131524e+15 + 1.99821509792555e+17j)

x = (-0-4j)
f(x) = (-3.39548300813643e-18 - 2.69288611917917e-18j)
(f(x).real) fois x = (0.0 + 1.35819320325457e-17j)
(f(x).imag) fois x = (0.0 + 1.07715444767167e-17j)
f(1/x) = (-1.80794087837878e+17 + 1.43383986431871e+17j)
```

```
et avec un complexe en exposant, ce complexe n etant pas, un zero, est-ce-que cela
marche, on le prend de partie imaginaire plus grande que 1.
on prend comme exposant k = 0.24565 + 7.25689575 i et on calcule les termes
correspondant aux entiers de 1 a 4.
x = (-0-1j)
f(x) = (1.0381597687163496e-05+4.217323869240799e-06j)
(f(x).real) fois x = -1.0381597687163496e-05j
(f(x).imag) fois x = -4.217323869240799e-06j
f(1/x) = (82680.13145845963-33587.20906155622j)

x = (-0-2j)
f(x) = (-6.43673672370867e-07+9.429180501497222e-06j)
(f(x).real) fois x = 1.287347344741734e-06j
(f(x).imag) fois x = -1.8858361002994443e-05j
f(1/x) = (-7206.074477126351-105561.83959145554j)

x = (-0-3j)
f(x) = (2.2599236754083294e-06-8.251243388450916e-06j)
(f(x).real) fois x = -6.7797710262249885e-06j
(f(x).imag) fois x = 2.475373016535275e-05j
f(1/x) = (30877.377539580117+112736.88578448542j)

x = (-0-4j)
f(x) = (-7.724491629885193e-06+1.9686808391779328e-06j)
(f(x).real) fois x = 3.089796651954077e-05j
(f(x).imag) fois x = -7.874723356711731e-06j
f(1/x) = (-121562.31001197151-30981.636326833974j)

et avec un complexe en exposant, ce complexe n etant pas un zero, est-ce-que cela
marche, on le prend de partie imaginaire plus petite que 1.
on prend comme exposant k = 0.24565 + 0.725689575 i et on calcule les termes correspondant aux
entiers de 1 a 4.
x = (-0-1j)
f(x) = (0.2963301415622044+0.12037840579499894j)
(f(x).real) fois x = -0.29633014156220444j
(f(x).imag) fois x = -0.12037840579499894j
f(1/x) = (2.8966066597155-1.1766905994560581j)

x = (-0-2j)
f(x) = (0.26792205473371544-0.03152970011066358j)
(f(x).real) fois x = -0.5358441094674309j
(f(x).imag) fois x = 0.06305940022132717j
f(1/x) = (3.681443998440965+0.4332410236268577j)

x = (-0-3j)
f(x) = (0.2238220529554892-0.09764892119346115j)
(f(x).real) fois x = -0.6714661588664677j
(f(x).imag) fois x = 0.29294676358038346j
f(1/x) = (3.753412047947218+1.6375358568866025j)

x = (-0-4j)
f(x) = (0.18516510512298576-0.13223387953235452j)
(f(x).real) fois x = -0.740660420491943j
(f(x).imag) fois x = 0.5289355181294181j
f(1/x) = (3.5765550673412307+2.5541624141411896j)
```

Résumé des petits résultats de novembre dans le plan complexe, Denise Vella-Chemla, 24 novembre 2024

1) J'avais oublié l'égalité suivante et je l'ai redécouverte par programme, c'est ballot.

$$\frac{1}{n^{a+ib}} \times n = n^{(1-a)-ib}$$

2) On peut calculer directement la partie réelle et la partie imaginaire de n^{a+ib} en appliquant ces formules :

$$\begin{array}{rcccccccc} n^{\frac{1}{2}+ib} & = & (& \cosh & (a \ln n) & + & \sinh & (a \ln n)) & . \quad (\cos(b \ln n) + i \sin(b \ln n)) \\ & = & (& \cos & (i\ a \ln n) & - \ i & \sin & (i\ a \ln n)) & . \quad (\cos(b \ln n) + i \sin(b \ln n)) \end{array}$$

Pour $\frac{1}{n^{a+ib}}$, la partie réelle est $n^{-a} \cos(b \ln n)$ et la partie imaginaire est $-(n^{-a}) \sin(b \ln n)$.

3) Il existe des nombres bases qui permettent de calculer les racines k-ièmes de n en prenant la puissance d'un de ces nombres (constantes spéciales) élevé à l'exposant le logarithme de n. On a ainsi

$$\text{Base_racine_}k^{\ln n} = \sqrt[k]{n}.$$

avec par exemple

$$\begin{array}{l} \text{Base_racine_2} = \exp(1/2) = 1.6487212707... \\ \text{Base_racine_3} = \exp(1/3) = 1.39561242509... \\ \ ... \\ \text{Base_racine_2}^{\ln n} = \sqrt{n} \\ \text{Base_racine_3}^{\ln n} = \sqrt[3]{n}... \end{array}$$

4) On peut "presque" calculer les parties imaginaires des zéros non triviaux de la fonction ζ en calculant, pour n entier à partir de 2,

$$2 \times \sqrt{-\left(n \ln n \frac{180}{2\pi}\right)}$$

5) On trouve comme un rythme de valse [1,1,2,3,3,4,5,5,6,7,7,8,...] en appliquant la fonction ci-dessous aux parties imaginaires des zéros de ζ (avec $z_k = b_k$ dans $Z_k = 0.5 + i\ b_k$, Z_k un zéro de ζ) ; le rythme s'observe dans les *parties entières* des images :

$$f(z_k) = \exp\left(W\left(-\left(\left(\frac{z_k}{2}\right)^2\right)\left(\frac{2\pi}{180}\right)\right)\right.$$

avec $W(z)$ la fonction de Lambert. On obtient une "valse" similaire en utilisant la fonction plus simple $g(k) = (2/3 + 4/5)\, k$.

Bon tempo ou bon, tant pis...
Denise Vella-Chemla, 24 novembre 2024

Lors de sa conférence en l'honneur des 25 ans du Séminaire nord-atlantique de Géométrie noncommutative [1], mais également des 60 ans de Piotr Hajac, un chercheur de Varsovie [2], Alain Connes a parlé de trouver le bon tempo, et c'est bien ce dont il s'agit quand on essaie de comprendre pourquoi les parties imaginaires des zéros non triviaux de la fonction ζ de Riemann adviennent sur la droite critique à tel ou tel rythme.

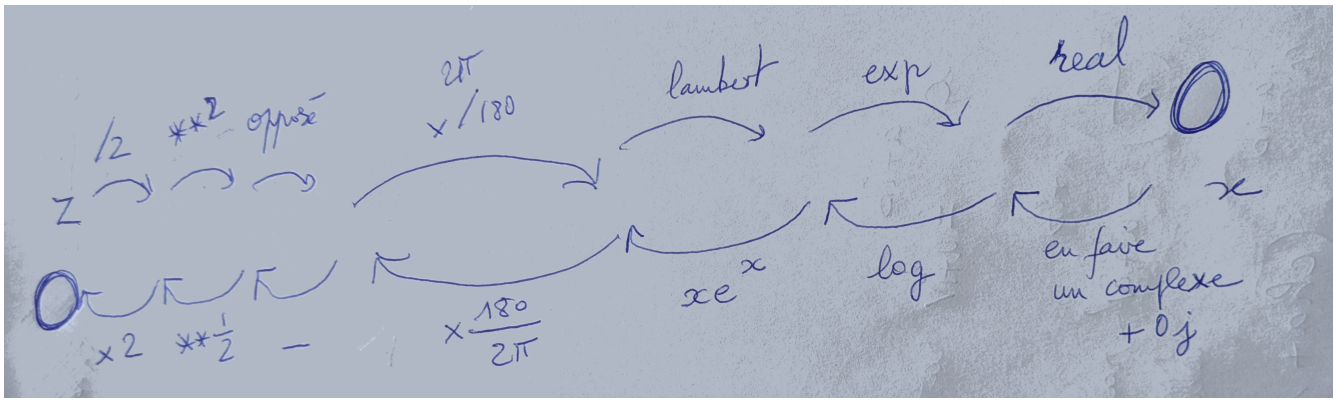
En compulsant les articles notamment d'Alain Connes et Henri Moscovici, j'ai fini par mettre hier au point une fonction, qui semble avoir presque trouvé ce tempo. Voici le programme utilisé pour "voir" cette fonction à l'œuvre.

```
import cmath
import math
from scipy.special import lambertw

"""
print('les zeros du cosinus hyperbolique sont ')
for n in range(100):
     print('i pi (n + 0.5)',1j*pi*(n+0.5))
"""

def f(z):
     return((cmath.exp(lambertw(-((z/2)**2)*(2*cmath.pi)/180))).real)

def frecipro(x):
     return(2*((-((cmath.log(x+0*1j)*cmath.exp(cmath.log(x+0*1j)))*180/(2*cmath.pi)))**0.5))

for k in range(1,10000):
     print(k,' --> ',f(k))
for k in range(1,1000):
     print(k,' --> ',frecipro(k))
for x in range(2,1000):
     res1 = -frecipro(x).imag
     res2 = zetazero(x-1).imag
     print(x,' --> ',res1,' ',res2)
     plt.scatter(x,res1,s=25,color='red')
     plt.scatter(x,res2,s=25,color='blue')
plt.show()
```

Trouver la réciproque de cette fonction donne un peu de peine, il faut savoir que la réciproque de la fonction de Lambert est xe^x et tout bien réciproquer (sic !) dans le bon ordre. Des extraits du résultat du calcul de la fonction f et de sa réciproque $frecipro$ sont fournis en annexe. Ci-dessous, l'image de la recherche de la fonction réciproque, étape par étape.

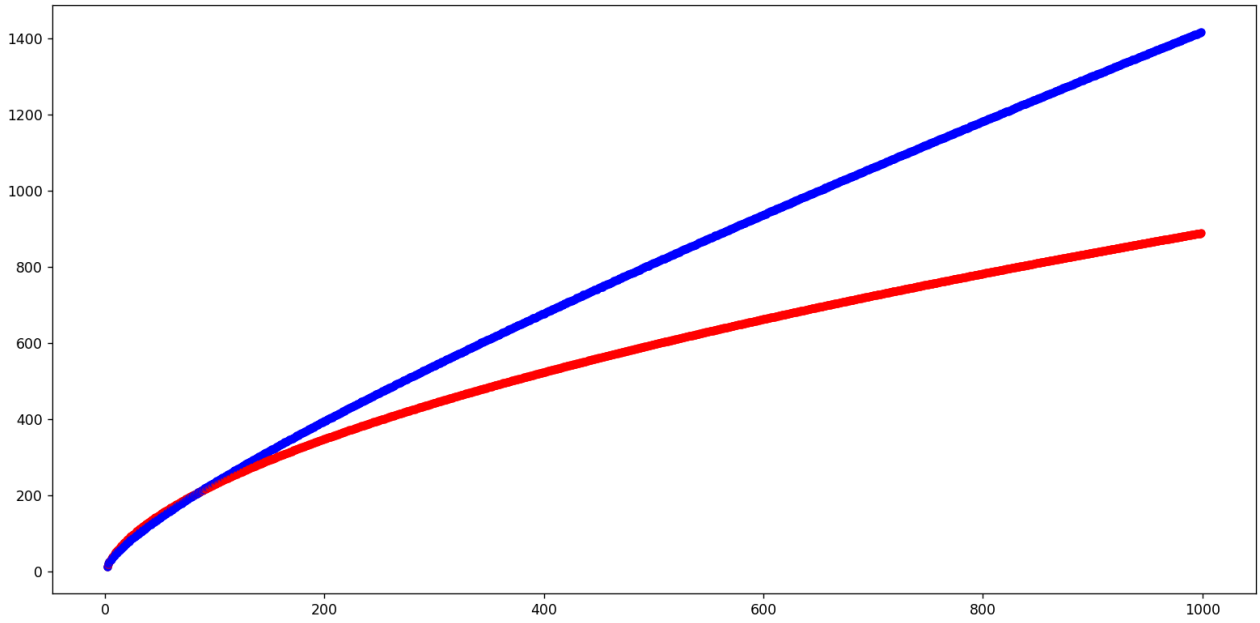
[1] North Atlantic Noncommutative Geometry Seminar https://www.mimuw.edu.pl/en/seminars/north-atlantic-noncommutative-geometry-seminar/.

[2] visionnable ici : https://www.youtube-nocookie.com/embed/1yvSeCmcsJU.



Ce qui est agréable à regarder, concernant la fonction elle-même, c'est qu'elle semble avoir un rythme, un tempo donc, qui s'accélère. Les parties imaginaires des images des entiers successifs, séparées, dans le bas de la droite des entiers, d'un espacement approximatif de 6.5 vont petit à petit s'espacer de plus en plus : on voit un espacement de 1 environ aux alentours de 100, de 0.5 aux alentours de 500, etc. Ce comportement est provoqué par la définition même de cette fonction réciproque de la fonction de Lambert, qui est $x\,e^x$.

Mais quand on teste la fonction, si au début, on a l'impression que c'est une bonne idée, on se rend bien vite compte que non.



Annexe : images des entiers successifs par f et par $frecipro$

Le résultat complet du programme est à trouver ici : https://denisevellachemla.eu/reszerosdecosh.pdf. On en fournit quelques extraits ci-après.

```
 1  -->  0.9912348268801342
 2  -->  0.9644540357471738
 3  -->  0.9180025427227111
 4  -->  0.8482243107574337
 5  -->  0.7466135076004062
 6  -->  0.5838866863880804
 7  -->  0.3481077986242361
 8  -->  0.3056143726364006
 9  -->  0.25859059087137415
10  -->  0.2071778721224076
11  -->  0.15150031731965438
12  -->  0.09166789462909816
13  -->  0.027778873206799243
14  -->  -0.04007828248811789
15  -->  -0.11182341456840304
16  -->  -0.18738347028476096
17  -->  -0.26669152656999356
18  -->  -0.3496859892935394
19  -->  -0.436309929400325
20  -->  -0.5265105275876397
21  -->  -0.6202386059793928
22  -->  -0.7174482302212594
23  -->  -0.8180963690934133
24  -->  -0.9221426014911805
25  -->  -1.0295488627128189
26  -->  -1.140279223595692
27  -->  -1.2542996972831746
28  -->  -1.3715780693750057
29  -->  -1.4920837479792026
30  -->  -1.6157876307921266
31  -->  -1.7426619868207462
32  -->  -1.8726803507543799
33  -->  -2.005817428312508
34  -->  -2.1420490111561543
35  -->  -2.281351900164793
36  -->  -2.423703836057907
37  -->  -2.5690834364876456
38  -->  -2.71747013885181
39  -->  -2.8688441481796096
40  -->  -3.0231863895294113
41  -->  -3.1804784644112702
42  -->  -3.340702610809375
43  -->  -3.5038416664328578
44  -->  -3.6698790348689867
45  -->  -3.838798654351816
46  -->  -4.010584968893243
47  -->  -4.185222901552433
48  -->  -4.362697829644998
49  -->  -4.54299556171524
50  -->  -4.726102316113952
51  -->  -4.912004701041146
52  -->  -5.100689695927654
53  -->  -5.29214463404265
54  -->  -5.486357186225385
55  -->  -5.683315345649647
```

```
 56  -->  -5.8830074135382615
 57  -->  -6.08542198575295
 58  -->  -6.290547940191839
 59  -->  -6.498374424933205
 60  -->  -6.708890847069639
 61  -->  -6.922086862181849
 62  -->  -7.137952364405712
 63  -->  -7.356477477050363
 64  -->  -7.577652543728509
 65  -->  -7.801468119963704
 66  -->  -8.027914965242005
 67  -->  -8.256984035478203
 68  -->  -8.488666475869238
 69  -->  -8.722953614109562
 70  -->  -8.95983695394518
 71  -->  -9.199308169044896
 72  -->  -9.441359097169006
 73  -->  -9.685981734617023
 74  -->  -9.933168230937522
 75  -->  -10.182910883884384
 76  -->  -10.435202134604795
 77  -->  -10.690034563045531
 78  -->  -10.947400883564793
 79  -->  -11.207293940738156
 80  -->  -11.469706705347306
 81  -->  -11.734632270541857
 82  -->  -12.002063848164369
 83  -->  -12.271994765229948
 84  -->  -12.544418460552015
 85  -->  -12.819328481506654
 86  -->  -13.096718480928091
 87  -->  -13.37658221412866
 88  -->  -13.658913536036852
 89  -->  -13.943706398447485
 90  -->  -14.23095484737837
 91  -->  -14.520653020528178
 92  -->  -14.812795144830618
 93  -->  -15.107375534100303
 94  -->  -15.404388586765734
 95  -->  -15.703828783685484
 96  -->  -16.005690686043554
 97  -->  -16.309968933320334
 98  -->  -16.616658241335497
 99  -->  -16.925753400359895
100  -->  -17.237249273292928
101  -->  -17.551140793902906
102  -->  -17.867422965127293
103  -->  -18.186090857430333
...
```

```
 990  -->  -1053.2890600685012
 991  -->  -1055.212982768467
 992  -->  -1057.138497669953
 993  -->  -1059.0656045282565
 994  -->  -1060.9943030989818
 995  -->  -1062.9245931380528
 996  -->  -1064.8564744017012
 997  -->  -1066.7899466464721
 998  -->  -1068.725009629221
 999  -->  -1070.6616631071133
1000  -->  -1072.5999068376248
1001  -->  -1074.5397405785397
1002  -->  -1076.4811640879486
1003  -->  -1078.424177124251
1004  -->  -1080.3687794461532
1005  -->  -1082.3149708126655
1006  -->  -1084.2627509831066
1007  -->  -1086.212119717097
1008  -->  -1088.16307677456
1009  -->  -1090.115621915727
1010  -->  -1092.0697549011256
 ...
1989  -->  -3737.5076391823313
1990  -->  -3740.9338999148313
1991  -->  -3744.3615984337125
1992  -->  -3747.7907346374673
1993  -->  -3751.221308424673
1994  -->  -3754.653319693938
1995  -->  -3758.0867683439715
1996  -->  -3761.521654273504
1997  -->  -3764.9579773813775
1998  -->  -3768.3957375664536
1999  -->  -3771.834934727687
2000  -->  -3775.27556876408
2001  -->  -3778.7176395747015
2002  -->  -3782.1611470586963
2003  -->  -3785.6060911152476
2004  -->  -3789.052471643631
2005  -->  -3792.5002885431563
2006  -->  -3795.9495417132216
2007  -->  -3799.400231053265
2008  -->  -3802.8523564627976
2009  -->  -3806.305917841411
2010  -->  -3809.760915088721
2011  -->  -3813.217348104442
2012  -->  -3816.6752167883355
2013  -->  -3820.1345210402137
2014  -->  -3823.5952607599766
2015  -->  -3827.0574358475747
2016  -->  -3830.521046203009
2017  -->  -3833.98609172636
2018  -->  -3837.4525723177603
2019  -->  -3840.9204878774153
2020  -->  -3844.389838305574
2021  -->  -3847.8606235025686
2022  -->  -3851.3328433687793
2023  -->  -3854.806497804648
2024  -->  -3858.2815867106797
 ...
```

```
 4990  -->  -20167.625249904388
 4991  -->  -20175.070099202432
 4992  -->  -20182.516220011603
 4993  -->  -20189.96361229951
 4994  -->  -20197.412276033723
 4995  -->  -20204.862211181917
 4996  -->  -20212.31341771169
 4997  -->  -20219.76589559067
 4998  -->  -20227.219644786517
 4999  -->  -20234.674665266917
 5000  -->  -20242.130956999485
 5001  -->  -20249.58851995189
 5002  -->  -20257.04735409184
 5003  -->  -20264.507459387005
 5004  -->  -20271.968835805073
 5005  -->  -20279.431483313765
 5006  -->  -20286.89540188079
 5007  -->  -20294.360591473825
 5008  -->  -20301.827052060602
 5009  -->  -20309.294783608908
 5010  -->  -20316.763786086394
  ...
 9990  -->  -72754.41433297312
 9991  -->  -72767.92075381812
 9992  -->  -72781.428342346
 9993  -->  -72794.93709854277
 9994  -->  -72808.44702239452
 9995  -->  -72821.9581138876
 9996  -->  -72835.47037300812
 9997  -->  -72848.98379974208
 9998  -->  -72862.49839407588
 9999  -->  -72876.01415599539
 ....
----------------------------------------
frecipro
----------------------------------------
  1  -->  0j
  2  -->  (7.717646788486349e-16   -  12.603873694619013j)
  3  -->  (1.189980990450552e-15   -  19.433864380800458j)
  4  -->  (1.5435293576972698e-15  -  25.207747389238026j)
  5  -->  (1.859427655588307e-15   -  30.36675810336357j)
  6  -->  (2.1491793023901847e-15  -  35.09876160026756j)
  7  -->  (2.419176648194077e-15   -  39.50815287931838j)
  8  -->  (2.6734712705058265e-15  -  43.661099222521976j)
  9  -->  (2.9148462302155932e-15  -  47.60305146341007j)
 10  -->  (3.1453212888868673e-15  -  51.36699481151239j)
 11  -->  (3.3664224815068552e-15  -  54.97785130946637j)
 12  -->  (3.579338998300489e-15   -  58.45504190747184j)
 13  -->  (3.78502056644971e-15    -  61.814076827457335j)
 14  -->  (3.984241000110738e-15   -  65.06759341362296j)
 15  -->  (4.1776413689147936e-15  -  68.22606112755825j)
 16  -->  (4.365760303153023e-15   -  71.29827646947079j)
 17  -->  (4.549055863290198e-15   -  74.29172013444902j)
 18  -->  (4.727921696397809e-15   -  77.2128208670381j)
 19  -->  (4.9026992156546346e-15  -  80.06715436757904j)
 20  -->  (5.0736869449970256e-15  -  82.85959590192901j)
```

```
21  -->  (5.2411478007148705e-15  -  85.59443921894805j)
22  -->  (5.405314843993018e-15   -  88.27549049662986j)
23  -->  (5.5663958816368065e-15  -  90.90614347765165j)
24  -->  (5.724577186459236e-15   -  93.4894402279075j)
25  -->  (5.880026535966167e-15   -  96.02812076200371j)
26  -->  (6.032895716870378e-15   -  98.52466394507731j)
27  -->  (6.183322606504471e-15   -  100.9813214848484j)
28  -->  (6.331432915792723e-15   -  103.40014639651062j)
```

Décalages, Denise Vella-Chemla, 27 novembre 2024

On fournit pour rappel, dans le tableau ci-dessous, quelques nombres de zéros de la fonction ζ jusqu'à tel nombre n.

n	$\#\{Z = s + it$ est un zéro non trivial de la fonction ζ de Riemann tel que $t \leq n\}$
100	236
200	396
500	811
1000	1419
2000	2515
5000	5447
10000	9877
20000	18046
50000	40433
100000	74920
200000	139501
500000	319387
1000000	600269
2000000	1132490

On trouve dans la littérature que Backlund a donné une formule exacte pour $N(t)$ qui est :

$$N(t) = \frac{1}{\pi}\theta(t) + 1 + S(t) \quad (1)$$

avec $\theta(t) = \arg\Gamma\left(\frac{1}{4} + \frac{i}{2}t\right) - t\log(\sqrt{\pi})$ la fonction de Riemann-Siegel et $S(t) = \frac{1}{\pi}\arg\zeta\left(\frac{1}{2} + it\right)$.
On teste ces formules avec le programme ci-dessous et on obtient les graphiques ci-après.

```
import mpmath
from mpmath import siegeltheta,zeta,arg
import math
from math import pi, e
import matplotlib.pyplot as plt
import time

def S(t):
     return(arg(zeta(1/2+1j*t))/pi)

def backlund(t):
     return((siegeltheta(t)/pi)+1+S(t))

def leclair(n):
     return((2*pi*(n-11/8))/lambertw((n-11/8)/e).real)
```

```
nmax = 25000
t1 = time.time()
fic = open("zeros25000",'r')
zeros = fic.readlines()
zeros = map(float,zeros)
k = 0
for k in range(nmax):
     res1 = backlund(k)
     plt.scatter(k,res1,s=4,color='red')
plt.legend(['Backlund N(t) = (Riemann-Siegel(t)/pi)+1+arg(zeta(zero(t)))/pi '])
plt.show()
t2 = time.time()
print('exec.  en ',t2-t1,' s.')
```

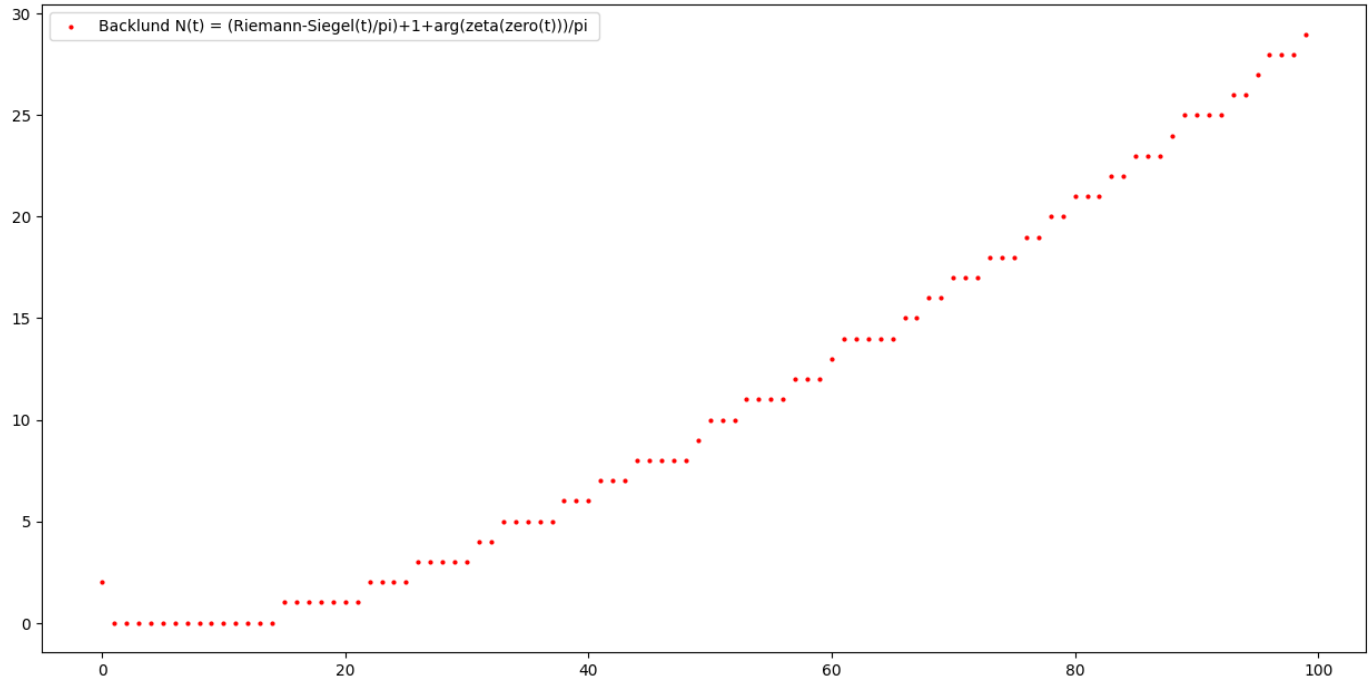


FIGURE 1

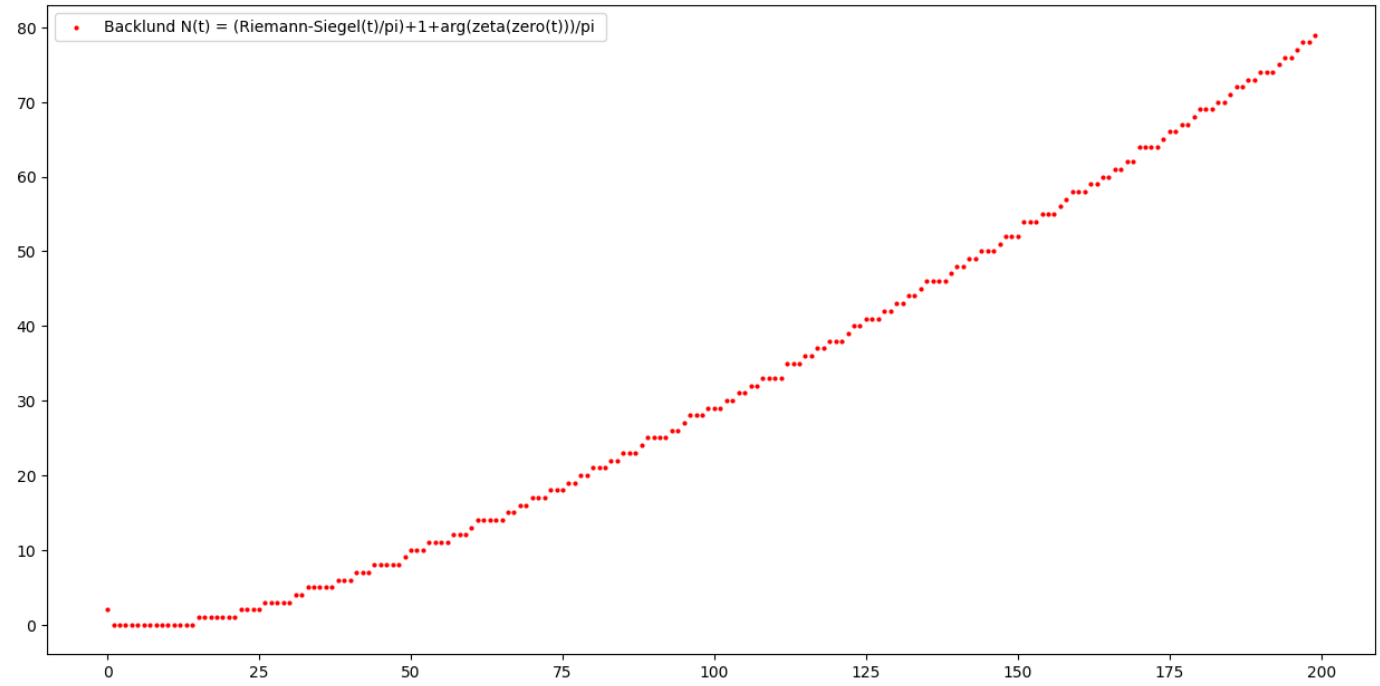


FIGURE 2

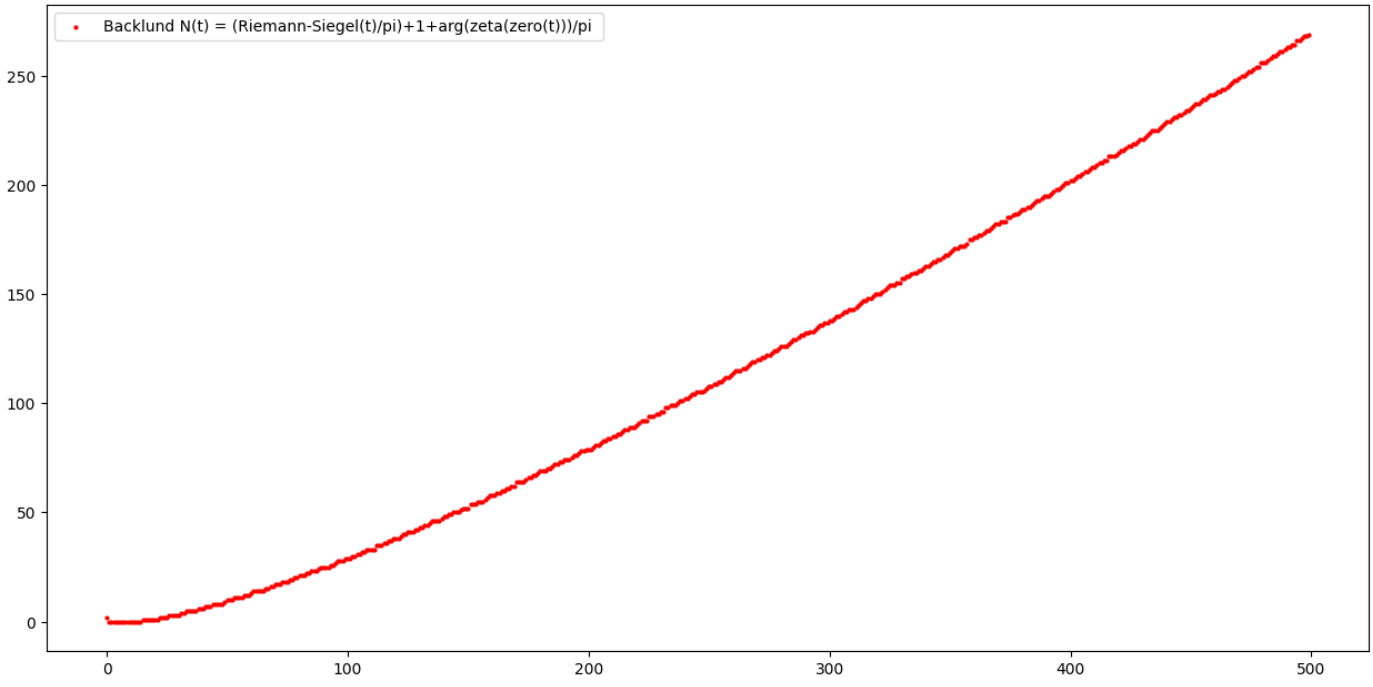


FIGURE 3

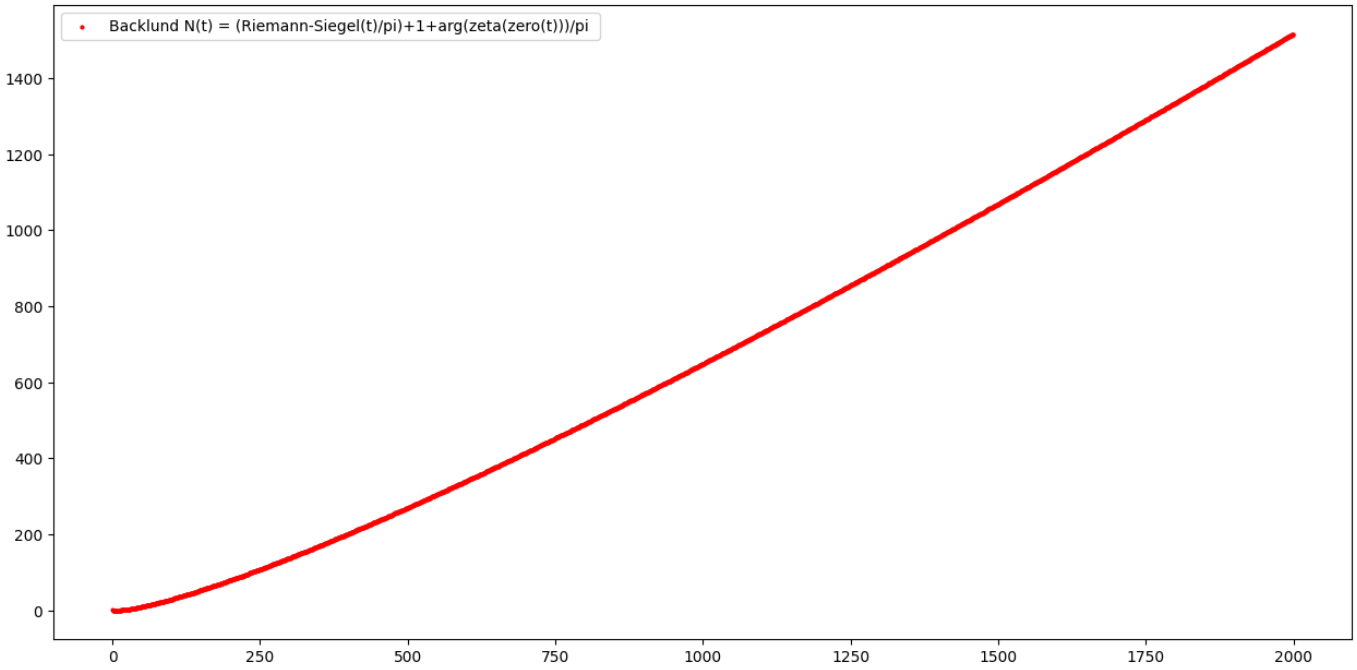


FIGURE 4

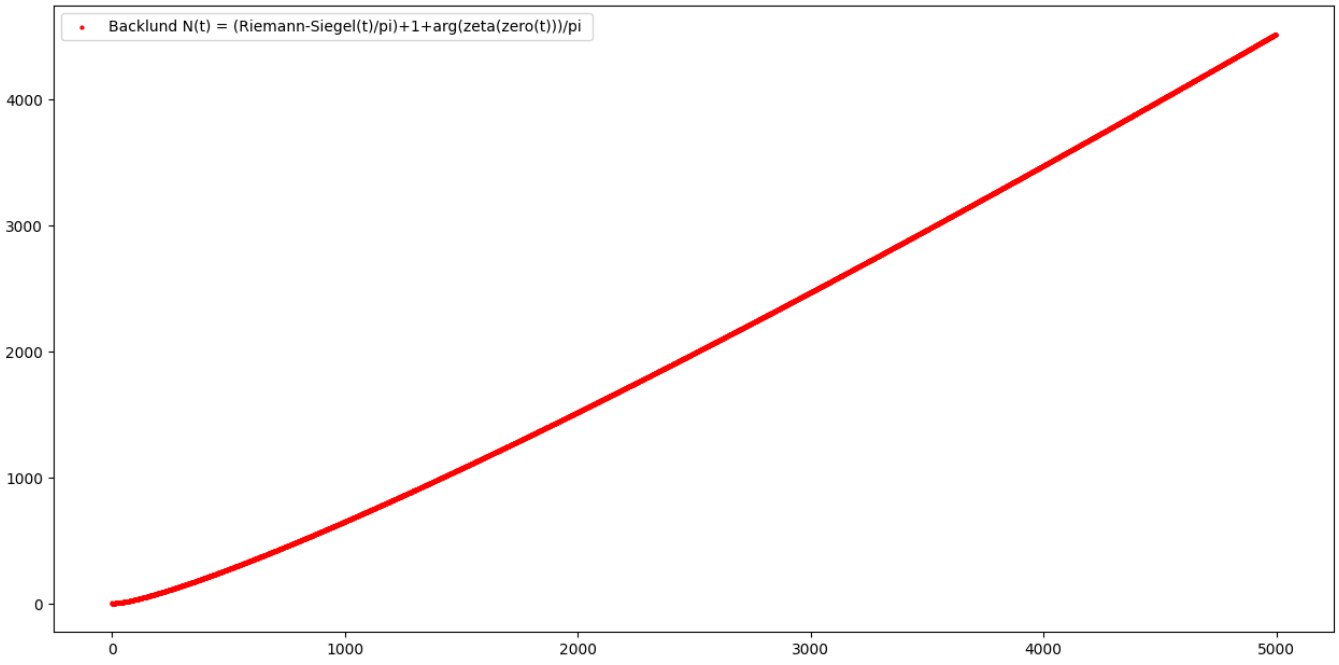


FIGURE 5

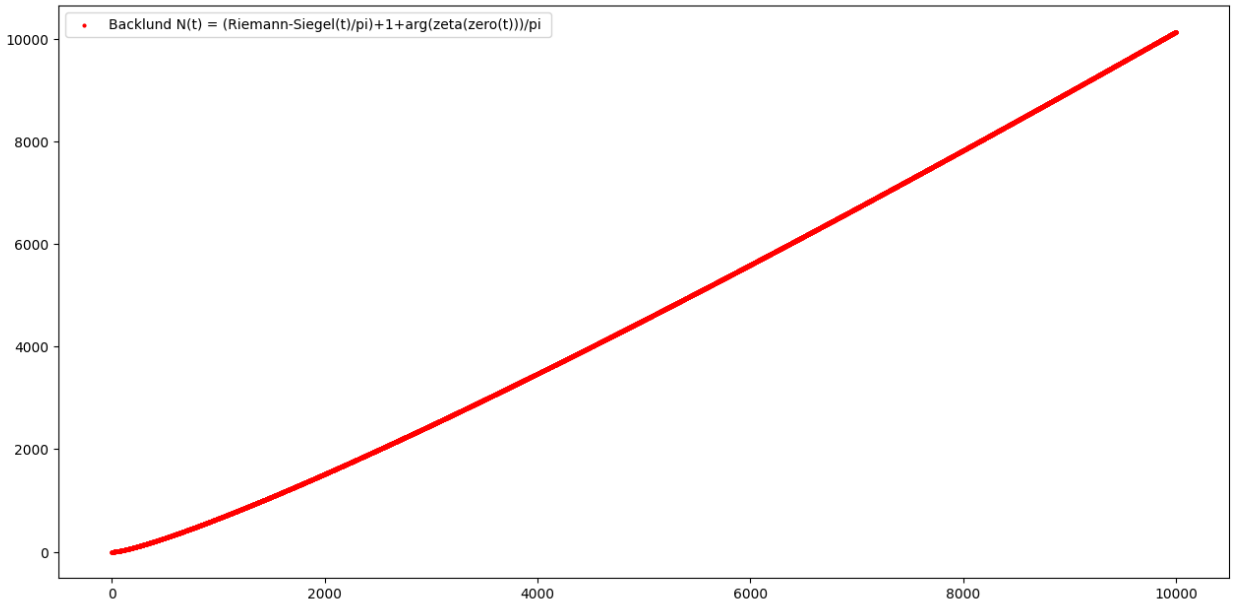


FIGURE 6

On teste également la formule fournie par França, LeClair et Mussardo [1]

$$N(t) = \frac{2\pi\left(n - \frac{11}{8}\right)}{W\left(\frac{n - \frac{11}{8}}{e}\right)} \tag{2}$$

pour calculer les zéros de ζ par le programme ci-dessous

[1] Voir les différentes références de leur travail autour de la fonction ζ de Riemann :
(https://arxiv.org/pdf/1307.8395,
https://arxiv.org/pdf/1407.4358,
https://arxiv.org/pdf/1410.3520,
https://arxiv.org/pdf/1502.06003 *,
https://arxiv.org/pdf/1509.03643,
https://arxiv.org/pdf/1809.06158,
https://arxiv.org/pdf/2101.10336,
https://arxiv.org/pdf/2406.01828).

```
from scipy.special import lambertw
import math
from math import pi, e
import matplotlib.pyplot as plt
import time

def fleclair(n):
     return((2*pi*(n-11/8))/lambertw((n-11/8)/e).real)

t1 = time.time()
fic = open("zeros25000",'r')
zeros = fic.readlines()
zeros = map(float,zeros)
k = 0
for zz in zeros:
     res1 = fleclair(k)
     plt.scatter(k,res1,s=4,color='red')
     plt.scatter(k,zz,s=4,color='blue')
     k = k+1
plt.legend(['fct de LeClair :  f(n)=2 pi (n-11/8)/W((n-11/8)/e) ','zeros de zeta'])
plt.show()
t2 = time.time()
print('exec.  en ',t2-t1,' s.')
```

et on obtient seulement jusqu'à 25000, les correspondances impressionnantes ci-dessous

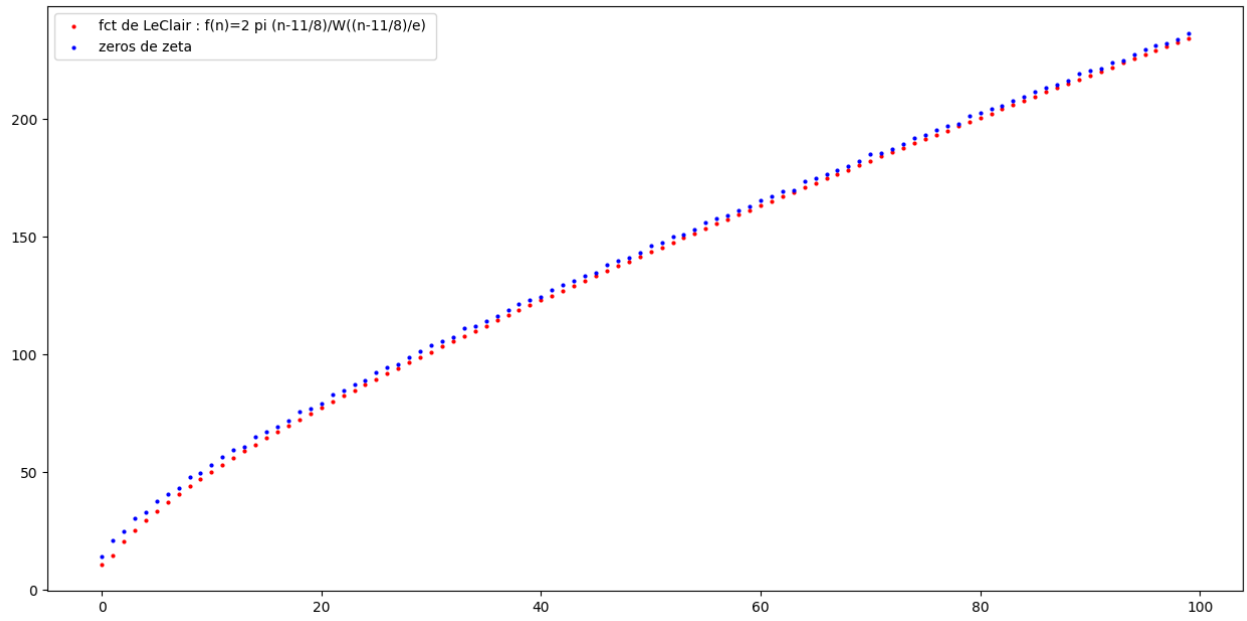


FIGURE 7

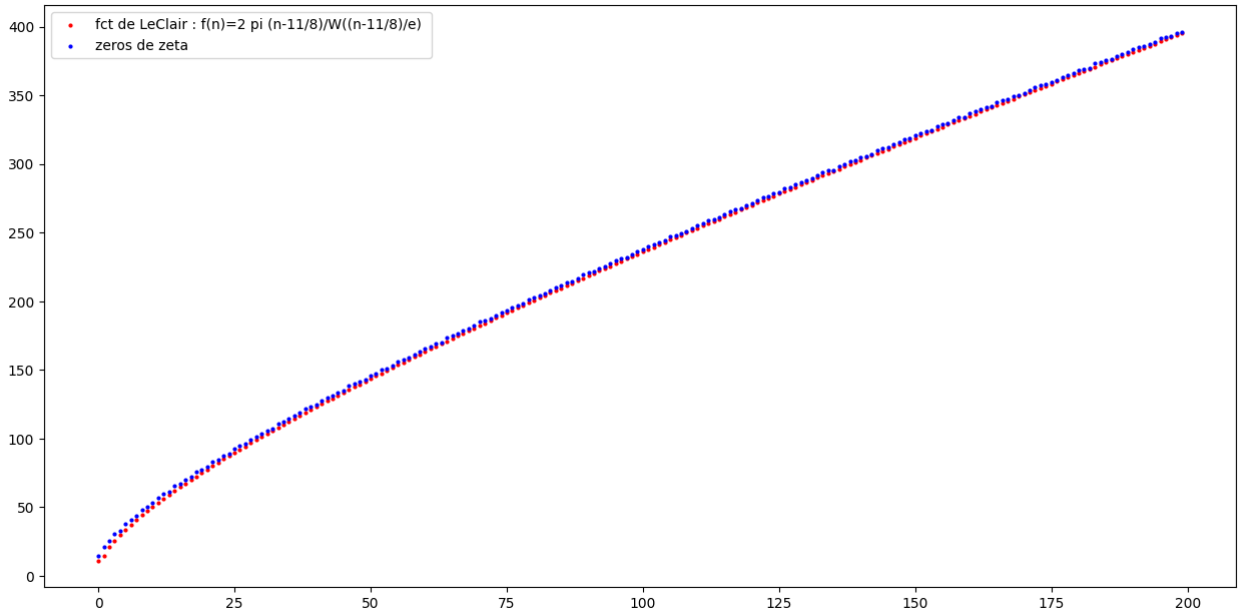


FIGURE 8

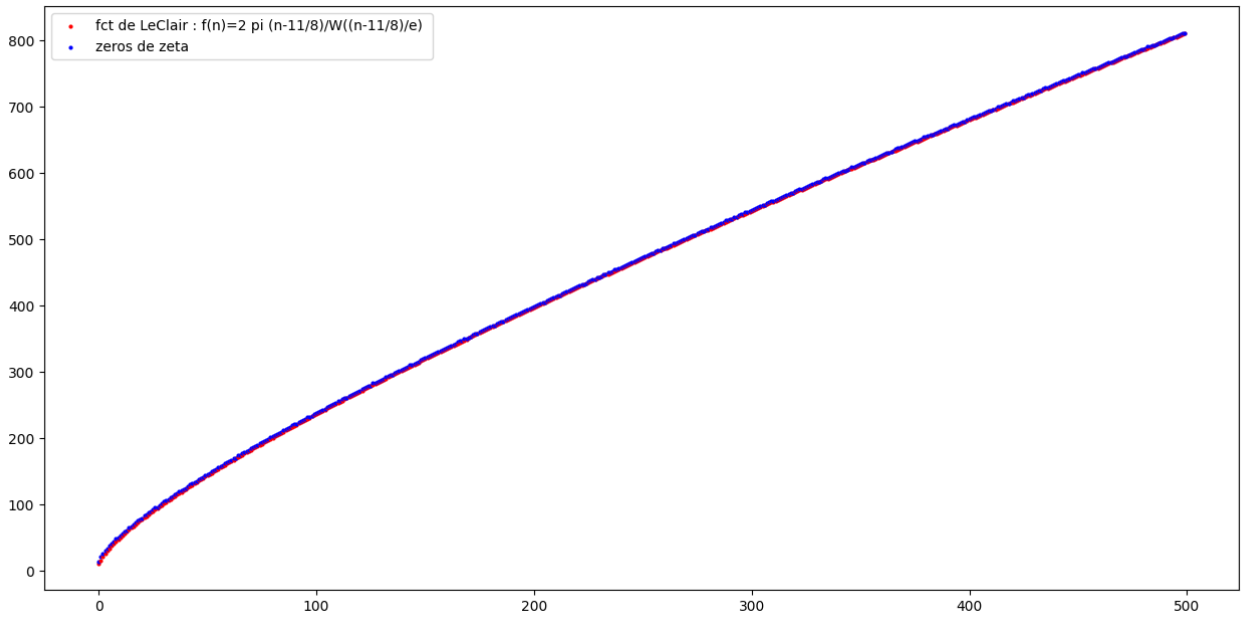


FIGURE 9

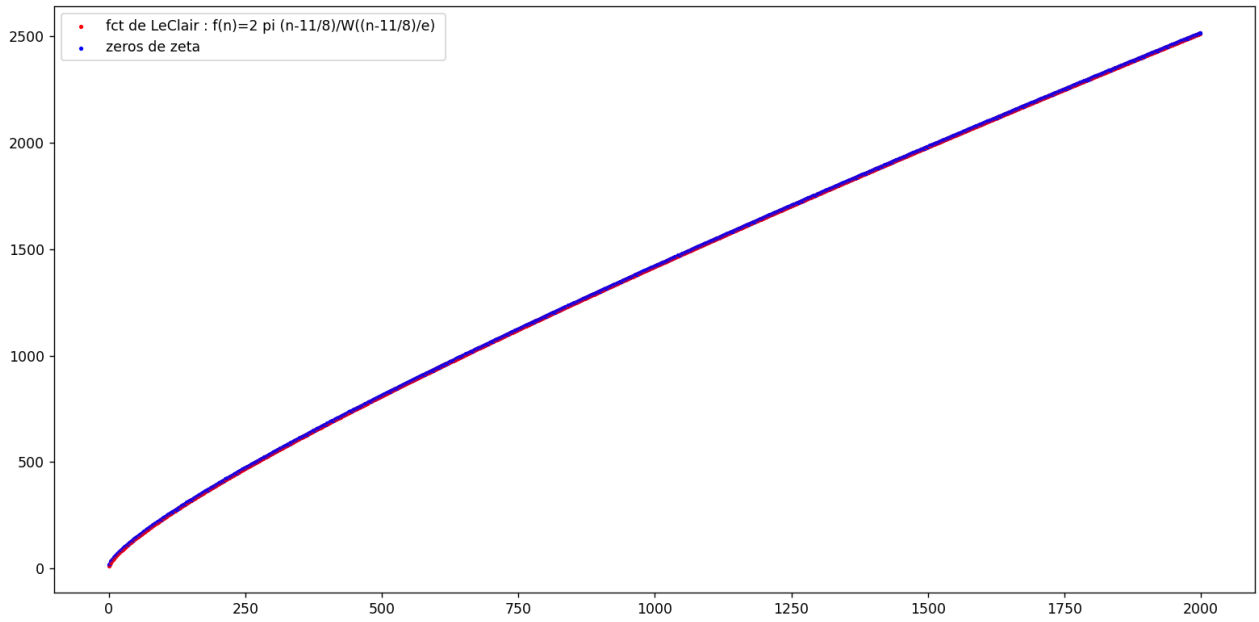


FIGURE 10

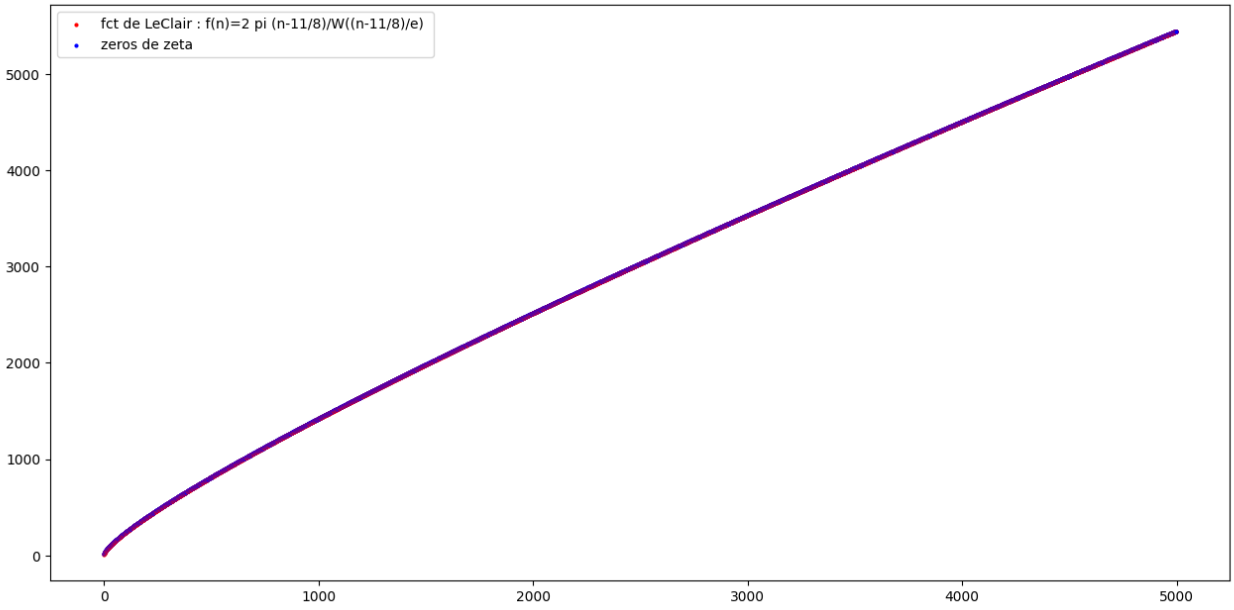


FIGURE 11

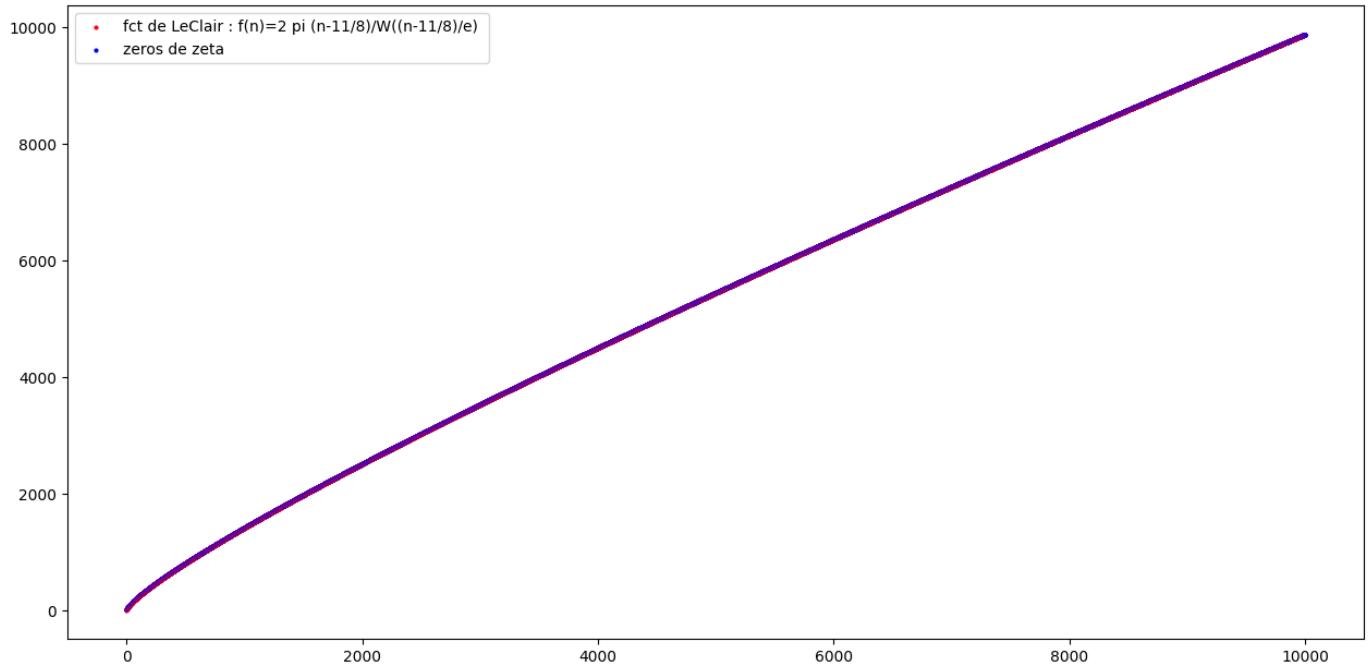
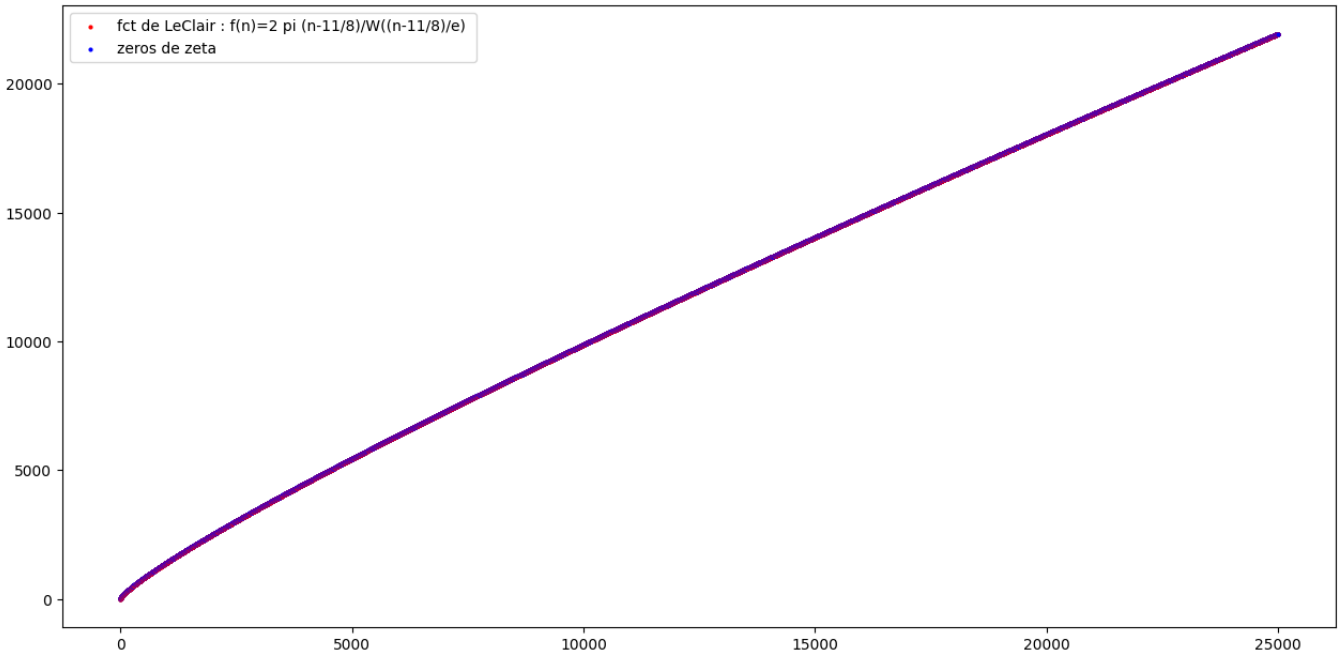


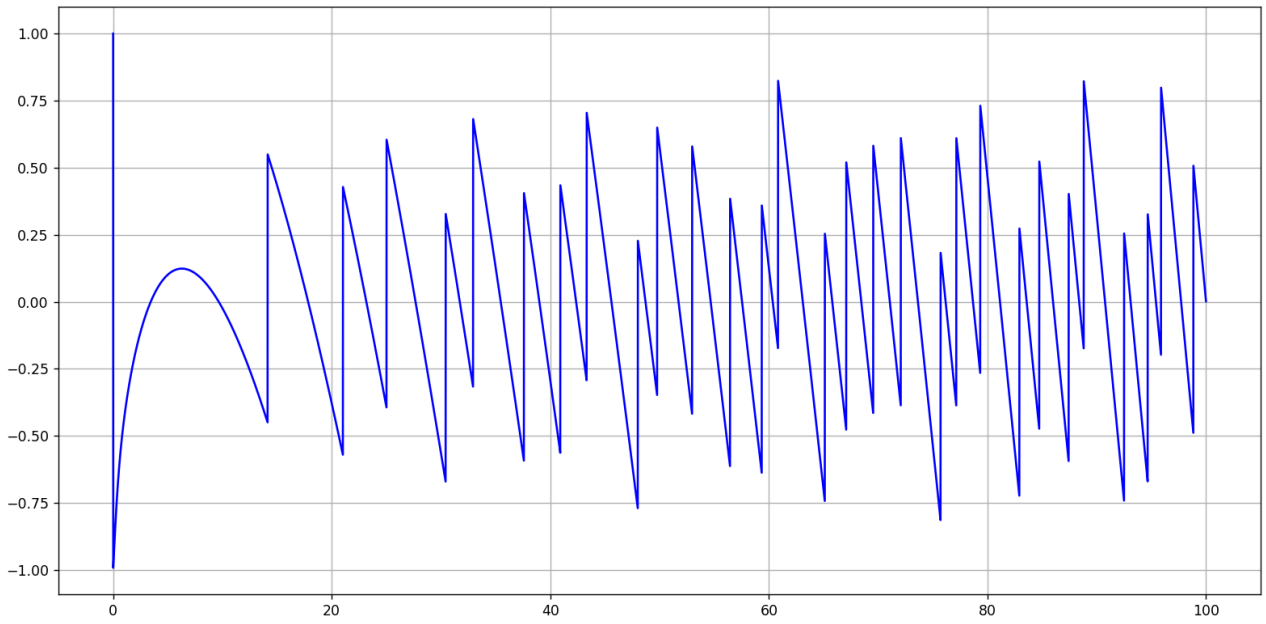
FIGURE 12



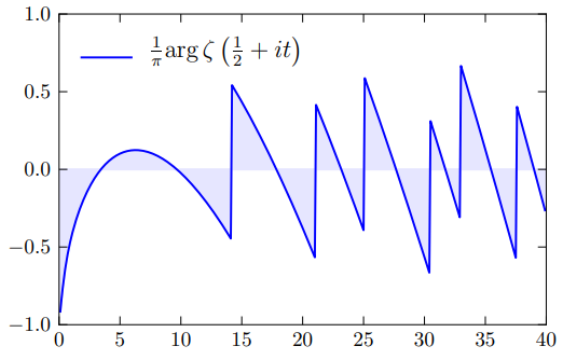
On utilise le programme `python` suivant pour vérifier les pics vers des minima locaux sur les abscisses correspondant aux parties imaginaires des zéros non triviaux de ζ :

```
import mpmath
from mpmath import zeta,arg
from math import pi,e
import matplotlib.pyplot as plt

lesx = []
lesy = []
for k in range(10000):
     lesx.append(k*0.01)
for xx in lesx:
     y = (1/pi)*arg(zeta(0.5+1j*xx))
     lesy.append(y)
plt.grid(True)
plt.plot(lesx,lesy,color='blue')
plt.show()
```

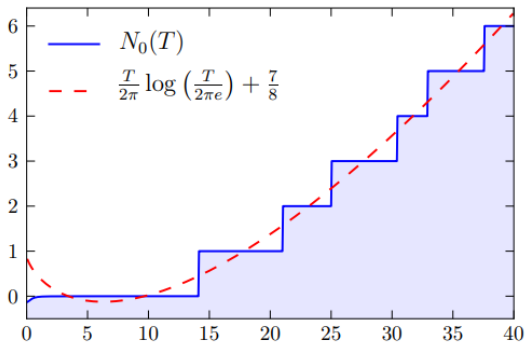
et le programme affiche le graphique prévu :



L'extrait correspondant dans l'un des articles de LeClair et al. est ci-dessous :



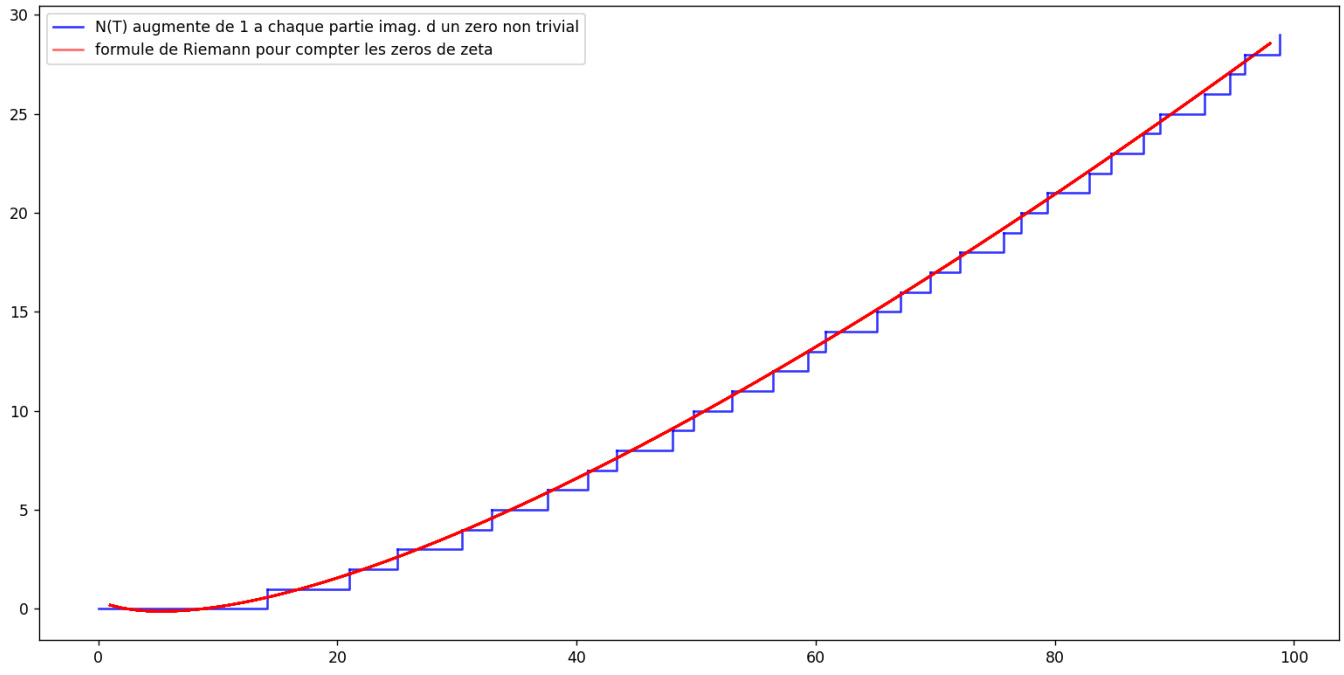
(a)



(b)

FIG. 1: (a) A plot of $\frac{1}{\pi}\arg\zeta\left(\frac{1}{2}+it\right)$ as a function of t showing its rapid oscillation. The jumps occur on a Riemann zero. (b) The function $N_0(T)$ in (14), which is indistinguishable from a manual counting of zeros. The dashed line is the smooth part without the $\arg\zeta$ term.

On programme également le second graphique :



Le problème est qu'en regardant les fonctions sur les 6 premières figures de la présente note (courbes rouges des Fig. 1 à 6) et celles des 6 figures suivantes (Fig. 7 à 12), alors qu'elles devraient normalement permettre d'obtenir sensiblement les mêmes résultats, on dirait que l'une serait plutôt la réciproque de l'autre. Mais on ne parvient pas à "réciproquer" une fonction telle que la fonction $N(t)$ définie par l'égalité (1).

On utilise le programme ci-dessous, pour calculer la formule fournie par Riemann dans son article [2] : cette formule fournit le nombre de zéros de ζ tel qu'il peut être calculé en se positionnant sur les lignes des fichiers fournis par Odlyzsko ici

https://www-users.cse.umn.edu/ odlyzko/zeta_tables/index.html

(avec l'éditeur libre Gnu-Emacs, au hasard ;-) numérotées 100, 200, 500, etc, jusqu'à 2 millions.

$$f(T) = \frac{T}{2\pi}\left(\log\left(\frac{T}{2\pi}\right) - 1\right) + \frac{7}{8}$$

```
import math
from math import pi,e,log
import time

def N0(T):
     return((T/(2*pi))*((log(T/(2*pi))-1))+7/8

nmax = 2000000
t1 = time.time()
for k in range(1,nmax):
     print(k,' --> ',N0(k))
t2 = time.time()
print('exec.  en ',t2-t1,' s.')
```

Le résultat de l'application de cette formule est à trouver dans le fichier à l'adresse

https://denisevellachemla.eu/resultat-calcul-N-formule-Riemann.txt.

Trouver dans ce fichier les nombres de zéros tels qu'ils sont fournis dans la table en tête de cette note peut se faire en utilisant un "Search" dans un fichier, en l'occurrence par exemple, "search" de la suite de caractères "811 −" pour trouver que 811 a pour image 100 (et non pour antécédent 100).

On teste également par le programme `python` ci-dessous que très peu loin à droite de la droite critique (sur la droite de partie réelle 0.500001), la formule de Riemann-Siegel appliquée aux parties imaginaires des zéros non triviaux de ζ calcule bien des multiples de π (on effectue le calcul pour un zéro sur 1000 pour que le fichier résultant ne soit pas trop lourd).

[2] et démontrée asymptotiquement par Alain Connes pour l'opérateur qu'il a mis au point avec Henri Moscovici, voir cet article https://arxiv.org/pdf/2402.13082 .

```
import mpmath
from mpmath import siegeltheta,zeta,arg
import math
from math import pi, e
import matplotlib.pyplot as plt
import time

fic = open("zeros2millions",'r')
zeros = fic.readlines()
zeros = map(float,zeros)
indice = 0
for z in zeros:
     if indice%1000 == 0:
          print(z,' --> ',siegeltheta(z)+arg(zeta(0.500001+1j*z)))
          print(indice,' --> ',((indice+1)-1.5)*pi)
     indice = indice+1
```

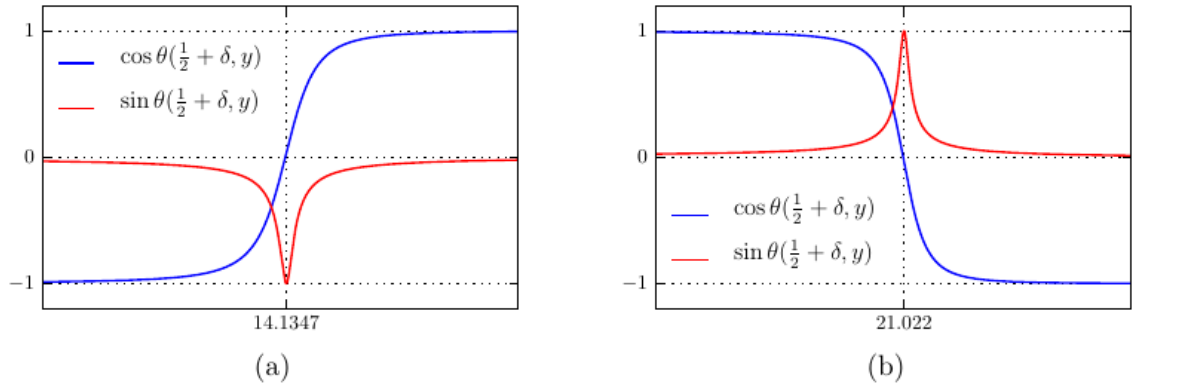
Le résultat de ce programme qui montre que l'égalité (3) ci-dessous est presque vérifiée

$$\theta(y_n) + \lim_{\delta \to 0^+} \arg\left(\zeta\left(\frac{1}{2} + \delta + i\, y_n\right)\right) = \left(n - \frac{3}{2}\right)\pi \tag{3}$$

est à lire à cette adresse :

https://denisevellachemla.eu/res-multiples-de-pi.pdf.

On souhaite maintenant, car cela est intrigant, tester le dessin ci-dessous, extrait de l'un des articles dont les références ont été fournies :



(a) (b)

FIG. 1: Exactly on a zero we have $\cos\theta = 0$ and $\sin\theta = \pm 1$. This is illustrated for the first (a) and second (b) Riemann zeros, respectively. We plot $\cos\theta\left(\frac{1}{2}+\delta, y\right)$ and $\sin\theta\left(\frac{1}{2}+\delta, y\right)$ versus y, for $0 < \delta \ll 1$.

Ce dessin indique que sur les zéros, du moins sur leur partie imaginaire, ont lieu des événements très particuliers : annulation de cosinus et minimisation ou maximisation de sinus.

On teste ceci par le programme ci-dessous :

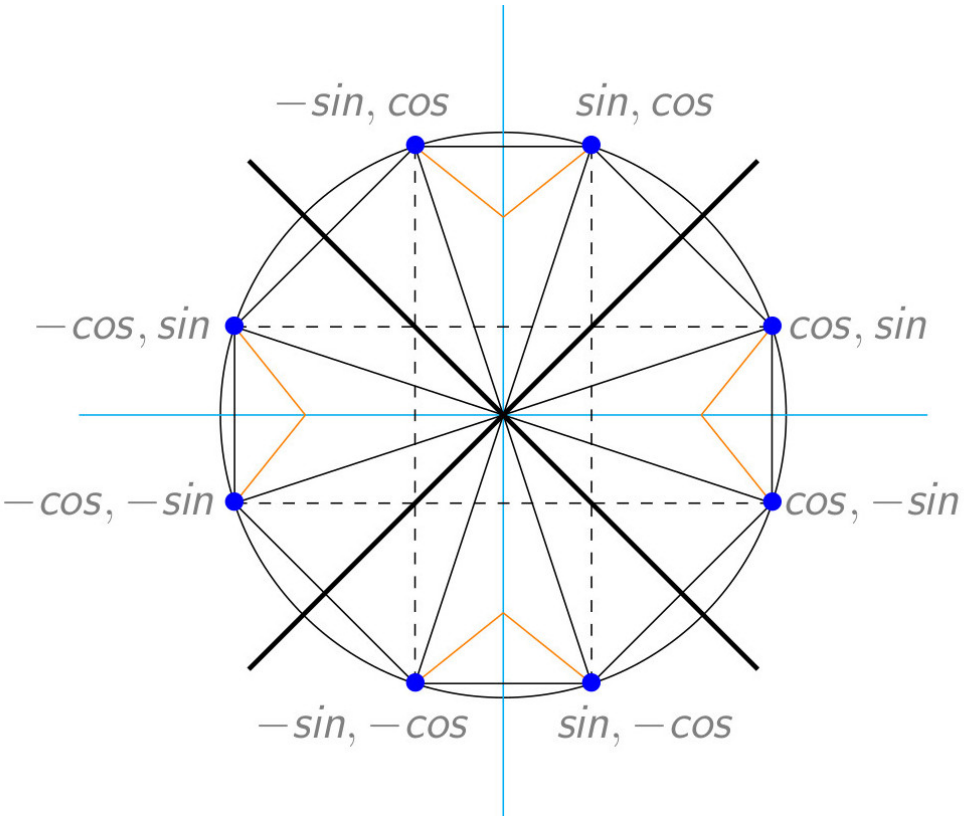
```
import mpmath
from mpmath import siegeltheta,cos,sin
import matplotlib.pyplot as plt

fic = open("zeros2millions",'r')
zeros = fic.readlines()
zeros = map(float,zeros)
indice = 0
for z in zeros:
     print(indice,' ',z,' --> le cos = ',cos(siegeltheta(0.500001+1j*z)),' le sin = ',
                sin(siegeltheta(0.500001+1j*z)))
     indice = indice+1
```

On constate, voir ci-dessous les 28 premières valeurs, pour les 28 premiers zéros, notamment à partir du troisième zéro (et voir les résultats du programme testé pour 2 millions de zéros ici
https://denisevellachemla.eu/resles2millionsdezeroscosetsin.txt),

qu'il ne se passe pas tout à fait ce qui est énoncé dans l'article, mais qu'effectivement, aux zéros, le cosinus complexe et le sinus complexe s'échangent "presque", i.e. les parties entières des nombres réels ainsi que les 2 premières décimales des nombres obtenus sont égales (on n'écrit que les 2 premiers chiffres après la virgule pour les parties imaginaires des zéros non triviaux de ζ pour que le tableau entre dans la page).

z_k	$\cos(\theta(0.500001 + i\ z_k)$	$\sin(\theta(0.500001 + i\ z_k)$
14.13	$(0.293388937669013 + 1.13029869698163j)$	$(1.49685640683923 - 0.221542382048759j)$
21.02	$(-3.65067833260755 - 5.55158585205924j)$	$(5.61453043670892 - 3.60975052325182j)$
25.01	$(51.8388221640843 + 71.4168263447541j)$	$(-71.4214116762003 + 51.8354940559466j)$
30.42	$(1279.73552271554 - 4113.64685890455j)$	$(4113.64696972589 + 1279.73548823956j)$
32.93	$(24841.8641073917 + 26496.1795441578j)$	$(-26496.1795542006 + 24841.8640979759j)$
37.58	$(-869400.988764962 - 2041151.68295039j)$	$(2041151.6829506 - 869400.988764874j)$
40.91	$(30840719.7915146 + 28754620.4954137j)$	$(-28754620.4954137 + 30840719.7915146j)$
43.32	$(-387072960.34808 + 249779472.513394j)$	$(-249779472.513394 - 387072960.34808j)$
48.00	$(43178983996.6938 - 9403272567.82428j)$	$(9403272567.82428 + 43178983996.6938j)$
49.77	$(104422162981.218 + 268200880066.318j)$	$(-268200880066.318 + 104422162981.218j)$
52.97	$(-5783591004856.14 - 5132458416844.01j)$	$(5132458416844.01 - 5783591004856.14j)$
56.44	$(291839841072518.0 + 50806726623293.6j)$	$(-50806726623293.6 + 291839841072518.0j)$
59.34	$(-7.26756835888617e+15 + 5.42279106626694e+15j)$	$(-5.42279106626694e+15 - 7.26756835888617e+15j)$
60.83	$(-3.56012563984149e+16 - 2.31911008361045e+16j)$	$(2.31911008361045e+16 - 3.56012563984149e+16j)$
65.11	$(4.61580677618116e+18 + 4.4928653739874e+18j)$	$(-4.4928653739874e+18 + 4.61580677618116e+18j)$
67.07	$(-4.37421017348352e+19 + 4.75817723092702e+19j)$	$(-4.75817723092702e+19 - 4.37421017348352e+19j)$
69.54	$(-7.10014608270834e+20 - 1.09057332806705e+21j)$	$(1.09057332806705e+21 - 7.10014608270834e+20j)$
72.06	$(2.39156360313659e+22 - 6.59809515156994e+21j)$	$(6.59809515156994e+21 + 2.39156360313659e+22j)$
75.70	$(-2.09210515573582e+24 + 1.18322703834867e+24j)$	$(-1.18322703834867e+24 - 2.09210515573582e+24j)$
77.14	$(-1.03304355079634e+25 - 9.61656561252754e+24j)$	$(9.61656561252754e+24 - 1.03304355079634e+25j)$
79.33	$(1.74491206884717e+26 - 1.52662029971126e+26j)$	$(1.52662029971126e+26 + 1.74491206884717e+26j)$
82.91	$(-1.08377054037024e+28 + 1.70145786519358e+28j)$	$(-1.70145786519358e+28 - 1.08377054037024e+28j)$
84.73	$(-1.86371342211539e+29 - 7.92302814453351e+28j)$	$(7.92302814453351e+28 - 1.86371342211539e+29j)$
87.42	$(6.21390260752283e+30 - 5.20020790876873e+30j)$	$(5.20020790876873e+30 + 6.21390260752283e+30j)$
88.80	$(3.89806768717041e+31 + 1.94114160950907e+31j)$	$(-1.94114160950907e+31 + 3.89806768717041e+31j)$
92.49	$(-5.54122808234602e+33 - 5.74915262473488e+32j)$	$(5.74915262473488e+32 - 5.54122808234602e+33j)$
94.65	$(2.93741347642162e+34 - 1.0052904554354e+35j)$	$(1.0052904554354e+35 + 2.93741347642162e+34j)$
95.87	$(5.64649058275168e+35 - 2.92179827134397e+35j)$	$(2.92179827134397e+35 + 5.64649058275168e+35j)$
98.83	$(-1.47267877047931e+37 + 3.00620553960502e+37j)$	$(-3.00620553960502e+37 - 1.47267877047931e+37j)$

Le cosinus et le sinus s'échangent comme ils le font sur le schéma ci-dessous, quand ils concernent deux angles en complémentarité adéquate par rapport à $\frac{\pi}{2}$.



Pour finir sur une note gaie, par curiosité et pour le fun, on utilise les 3 fonctions $d_1(n), d_2(n)$ et $d_3(n)$ (on a remplacé 2π par 6 et $2\pi\, e$ par 17 pour d_1, et utilisé 5π ou 6π au dénominateur pour $d_2(n)$ et $d_3(n)$) :

$$d_1(T) = \frac{T}{6} \log\left(\frac{T}{17}\right) + 1$$

$$d_2(T) = \frac{T}{2\pi} \log\left(\frac{T}{5\pi}\right) + 1$$

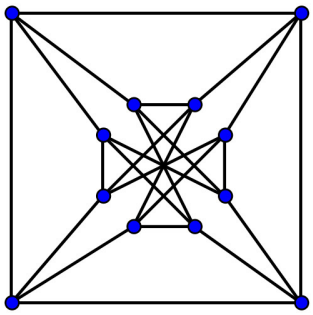
$$d_3(T) = \frac{T}{2\pi} \log\left(\frac{T}{6\pi}\right) + 1$$

Les valeurs du tableau fournies en début de note sont ainsi modifiées :

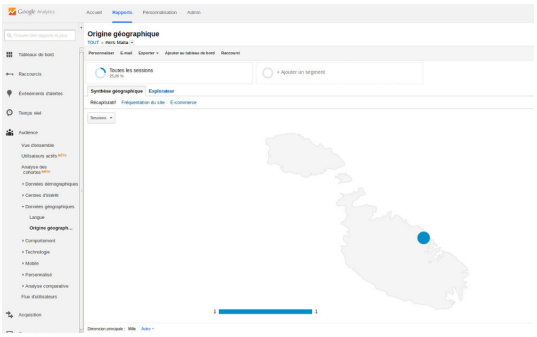
n	$\#\{Z = s + it$ est un zéro non trivial de la fonction ζ de Riemann tel que $t \leq n\}$	$d_1(n)$	$d_2(n)$	$d_3(n)$
100	236	104	102	95
200	396	208	204	192
500	811	523	510	486
1000	1419	1047	1018	976
2000	2515	2095	2032	1959
5000	5447	5238	5071	4913
10000	9877	10478	10130	9843
20000	18046	20956	20239	19715
50000	40433	52389	50537	49364
100000	74920	104776	100996	98822
200000	139501	209545	201856	197808
500000	319387	523846	504254	494986
1000000	600269	1047662	1007995	990577
2000000	1132490	2096375	2016138	1983276

Les valeurs pour tous les nombres jusqu'à 2.10^6 sont consultables ici
https://denisevellachemla.eu/resmondeliden.txt [3] [4].

La croix des chevaliers de l'Ordre de Malte



dessin géométrique d'un graphe spécial



une visite à mon site depuis l'île de Malte

[3] Comme on s'y attendait bien sûr, le rapport $\frac{d(T)}{T}$, pour la fonction $d_1(n)$, qui vaut 1.04 pour la première ligne du tableau et 1.0481875 pour la dernière ligne du tableau tendra inévitablement vers $2^{\frac{1}{12}} = 1,059463$ qui est l'intervalle d'un demi-ton dans la gamme tempérée.

[4] et ici https://denisevellachemla.eu/resmondeliden2.txt et ici https://denisevellachemla.eu/resmondeliden3.txt pour les deux dernières colonnes $d_2(n)$ et $d_3(n)$.

Formulaire résumé, Denise Vella-Chemla, 4 décembre 2024

1) Fonction qui s'annule sur les nombres premiers

$$f_1(x) = \sum_{b=2}^{x-1} \sum_{o=1}^{b} \cos\left(\frac{2\pi\ x\ o}{b}\right).$$

J'ai trouvé cette formule en juillet 2014 lien 1.

Victor Varyn a démontré qu'elle s'annule bien sur les nombres premiers et eux seuls en juillet 2017 lien 2.

On peut utiliser à la place des sommes de cosinus des produits de sinus lien 3 (mai 2009).

J'ai retrouvé "mon" produit de sinus dans un article de 1951 de Redheffer lien 4 (je l'ai retrouvé en septembre 2021).

2) Fonction qui s'annule sur les zéros de ζ

La fonction de van der Pol [1]

$$f_2(t) = \left| \left(\int_0^t -\exp\left(-\frac{x}{2}\right)\ (\exp(x) \bmod 1) \cos(-x\ t)\ dx \right)^2 \right.$$
$$\left. + \left(\int_0^t -\exp\left(-\frac{x}{2}\right)\ (\exp(x) \bmod 1) \sin(-x\ t)\ dx \right)^2 \right|.$$

3) Fonction qui fournit les valeurs des parties imaginaires des zéros non triviaux de ζ

La fonction de França, LeClair et Mussardo (W est la fonction de Lambert, i.e. la réciproque de la fonction : $W^{\leftarrow}(z) = z\ e^z$, avec z complexe.)

$$f_3(t) = \frac{2\pi(t - \frac{11}{8})}{W\left(\frac{t - \frac{11}{8}}{e}\right)}$$

Pour des tests de programmation de cette fonction, se reporter à lien 10.

4) Fonction qui compte les nombres premiers

Dans Around Wilson's Theorem, d'A. Connes, on trouve par exemple

$$f_4(x) = \pi(x) = \left\lfloor \sum_{k=1}^{x} \sin^2\left(\frac{\pi\Gamma(k)}{2k}\right) \right\rfloor.$$

[1] voir lien 5 , lien 6 , lien 7 , lien 8 et lien 9.

5) Fonctions qui comptent les zéros non triviaux de ζ sur la droite critique

a) Formule de Riemann [2] [3], à laquelle on ajoute $\frac{7}{8}$.

$$f_5(T) = \frac{T}{2\pi}\left(\log\left(\frac{T}{2\pi} - 1\right)\right) + \frac{7}{8}.$$

b) Formule de Backlund qui compte les zéros non triviaux sur la droite critique

$$f_6(t) = \frac{1}{\pi}\arg\Gamma\left(\frac{1}{2} + \frac{t}{2}i\right) + 1 + \frac{1}{\pi}\arg\zeta\left(\frac{1}{2} + it\right)$$

Pour des tests de programmation de ces fonctions, se reporter à lien 10.

6) Opérateur dont le spectre serait l'ensemble des nombres premiers

J'ai cherché à programmer l'opérateur dont il est question à la page 7/47 (ou bien 417/457 de la publication originale) de l'article *Hecke algebras, Type III factors and Phase transitions with spontaneous symmetry breaking in number theory* de J.-B. Bost et A. Connes (lien 12), mais je n'ai pas compris / trouvé la définition de l'opérateur utilisé [4] .

7) Opérateur dont le spectre serait l'ensemble des (parties imaginaires des) zéros de ζ

J'ai également cherché à programmer l'opérateur dont il est question dans l'article *The UV Prolate spectrum matches the zeros of zeta* de H. Moscovici et A. Connes mais je n'ai pas compris / trouvé la définition de l'opérateur utilisé [5] .

8) Opérateur qui a un comportement particulier qui permet de distinguer les nombres premiers des nombres composés

Voir la matrice multi-circulante à multiples matrices de permutations sur sa diagonale lien 16 .

9) petite remarque en passant sur l'utilité des exponentielles et des logarithmes pour calculer "directement" les carrés, les cubes, les puissances

$$\exp(x)^{\ln(y)} = y^x.$$

[2] Voir lien 11, extrait de lien 17, et se reporter à la page de l'Institut Clay concernant le manuscrit de Riemann lien 18.

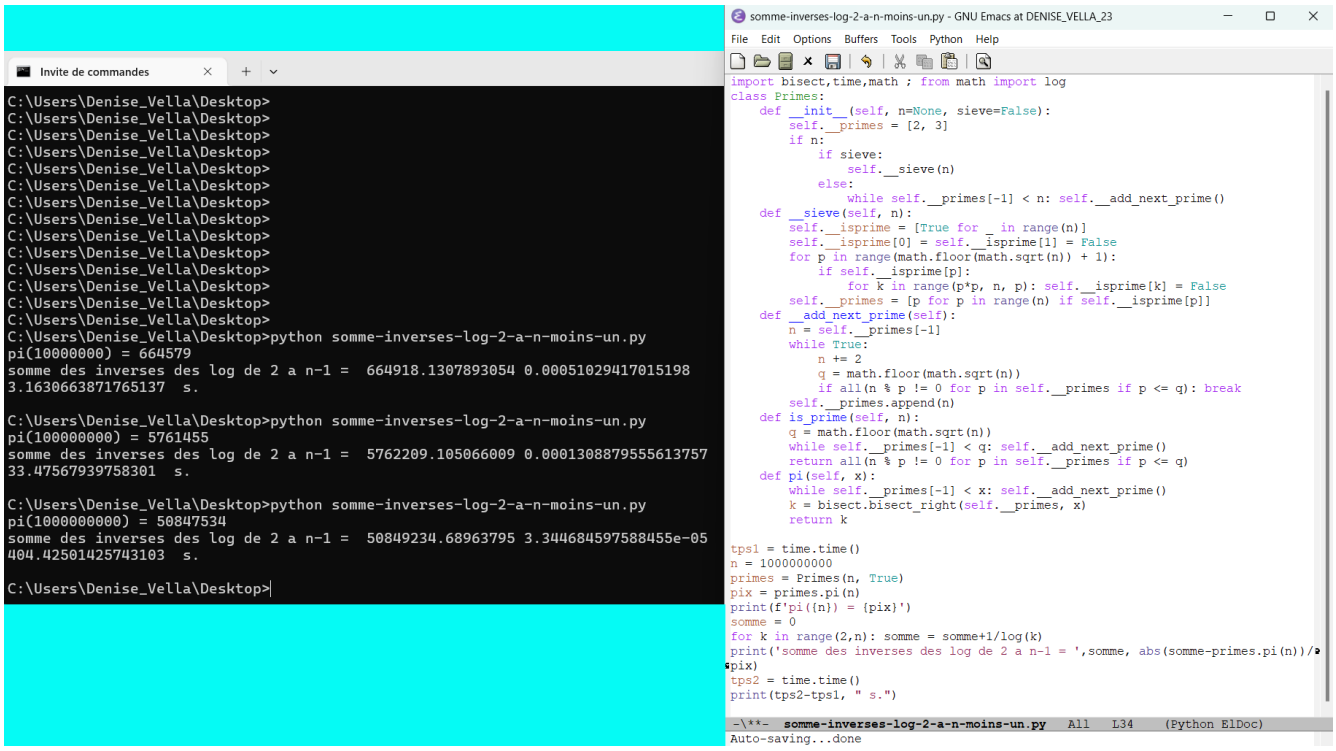
[3] On trouve parfois $\log\left(\frac{T}{2\pi} - 1\right)$ abrégé en $\log\left(\frac{T}{2\pi\, e}\right)$.

[4] voir p. 6 de cette traduction lien 13 .

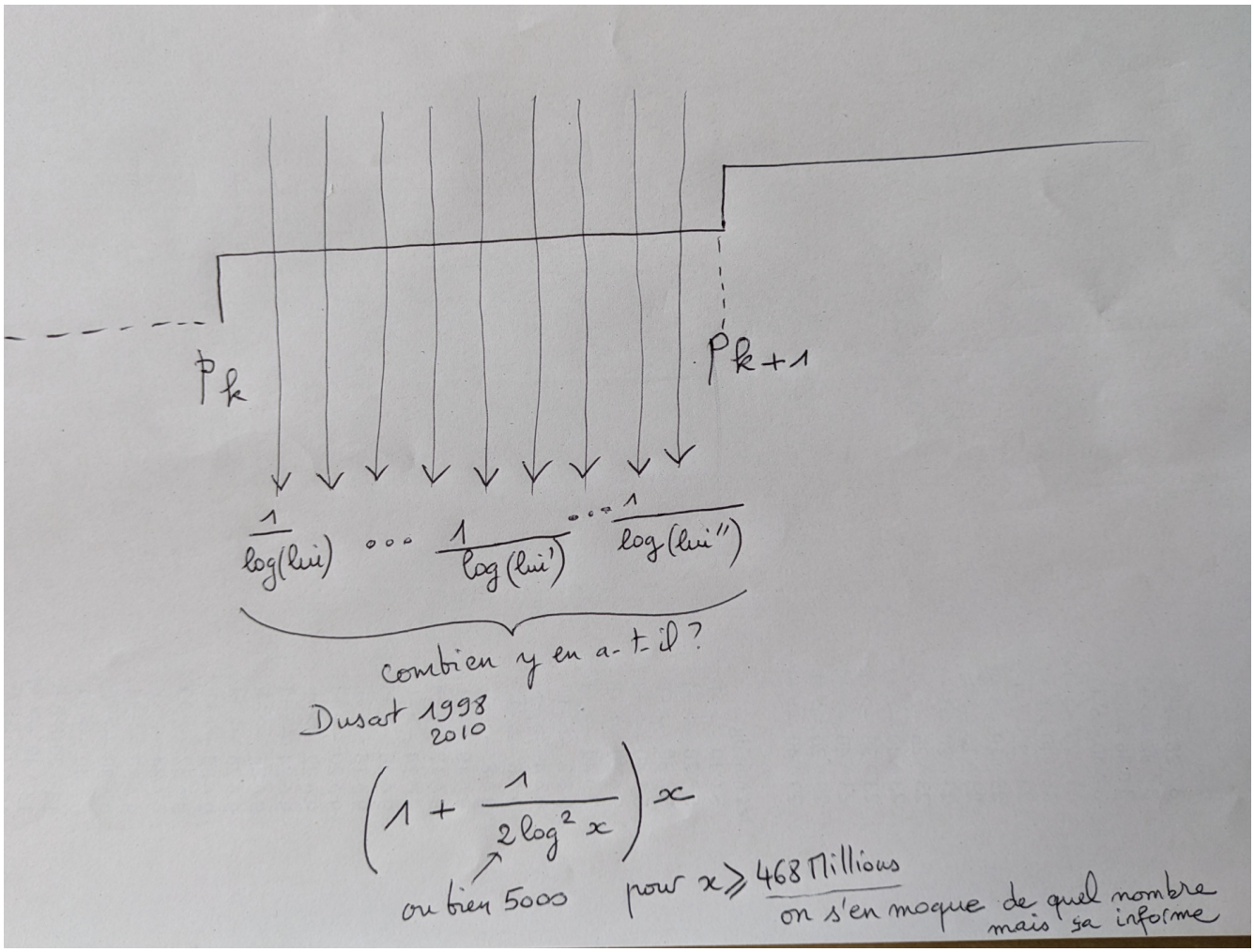
[5] voir lien 14 et traduction d'une version postée sur arxiv (et peut-être modifiée depuis) lien 15.

10) enfin comprendre un peu quel est le problème

La formule de Riemann pour calculer le nombre de nombres premiers inférieurs à un certain nombre utilise le logarithme intégral, qui est, pour le dire rapidement, une intégrale de l'inverse du logarithme. Quand on n'aime pas trop les réels et les intégrales, on remplace cette intégrale par une somme pour les entiers de 2 à $x-1$ de l'inverse de leur logarithme (à la recherche de $\pi(x)$, le nombre de nombres premiers jusqu'à x), et on obtient sensiblement le même résultat qu'avec la fonction li. Quand on observe la différence entre cette somme des inverses des logarithmes des entiers (de 2 à $x-1$) et le nombre de nombres premiers (jusqu'à x), on voit que cette différence entre eux deux devient de plus en plus petite, vraiment, mais il faudrait être sûr qu'elle ne va pas se remettre à grandir, loin, très loin, très très loin.



Tant qu'on n'avait pas compris de quoi il retournait, on se disait "c'est simple, il suffit de montrer qu'une somme d'inverses de logarithmes entre deux nombres premiers est toujours inférieure à 1" (puisque c'est de 1 que $\pi(x)$ augmente lors du passage d'un nombre premier au nombre premier suivant), en ayant à l'esprit le dessin ci-dessous.



Dusart en 1998 puis en 2010 [6] a démontré que le nombre premier suivant immédiatement x est au maximum à distance $\left(\frac{x}{2\log^2 x}\right)$ de x.

Alors on remplace la somme cumulée des $\frac{1}{\log k}$ par le plus grand d'entre ces ratios sur l'intervalle (qui est le premier d'entre eux, puisque l'inverse du logarithme décroît), multiplié par ce nombre de nombres qu'a fourni Dusart, pour voir comment cette majoration de la somme cumulée se conduit, et pour voir si elle est très inférieure à 1, ce qui tranquilliserait.

Mais pas du tout : de 2 à 20, elle décroît de 0.00120111228282827621 à 0.00014878220705519027, mais ensuite elle croît, très très lentement, c'est sûr (elle vaut à peine 0.1 et quelques pour 1 421 822, 0.2 pour 3 401 984, etc., et n'a pas encore atteint 0.5 à 10 000 000), mais elle croît : ça coince donc.

[6] où le 2 de la formule devant le log au dénominateur est devenu 5000.

Reprise du travail sur les fonctions sphéroïdales prolates, pour réussir à trouver par programme les résultats de Richard-Jung, Ramis, Thomann et Fauvet, Denise Vella-Chemla, 14 décembre 2024

Je cherche depuis longtemps à comprendre l'approche qu'a Alain Connes de l'hypothèse de Riemann et la vision qu'il a de l'ensemble des nombres premiers. Informaticienne de formation, je comprends en programmant ; en faisant cela, je suis le conseil du Professeur Donald Ervin Knuth, que j'admire entre tous, et qui dit qu'on ne comprend bien une notion que le jour où on arrive à l'enseigner à une machine. Qu'on ne se leurre pas, je suis loin de toute compréhension ici, vraiment, mais le fait d'avoir un programme qui commence à se rapprocher doucement de l'objectif fait le plus grand bien, surtout quand on a vraiment le sentiment d'avoir lutté pour l'écrire.

Donc voici : il s'agit de voir les zéros de la fonction ζ de Riemann comme les valeurs propres d'un opérateur. C'est-à-dire qu'on dispose d'un certain nombre de valeurs, les parties imaginaires des zéros non triviaux de la fonction ζ, et on cherche une fonction qui enverrait les entiers sur ces valeurs. Alain Connes a pensé à l'opérateur prolate en 1997 pour permettre d'atteindre les zéros de ζ parce que cet opérateur a notamment comme propriété intéressante de permettre de limiter et une fonction et sa transformée de Fourier, c'est ce que j'ai entendu à plusieurs reprises : il permet de limiter la bande passante à la fois de la coordonnée temporelle et de la coordonnée fréquentielle d'un signal ; habituellement, cela n'est pas possible.

Les références souvent citées concernant les fonctions prolate sont les articles de Slepian, Landau et Pollack. Une femme a travaillé avec eux, il s'agit d'Estelle Sonnenblick. Non seulement, elle a fourni toute une série de tableaux de référence pour les valeurs propres λ_n et les χ_n correspondantes, et Slepian écrit qu'il a une dette à son égard d'avoir effectué tous ces calculs sur ordinateur, mais elle fournit également des fonctions d'approximation de ces valeurs.

Ci-après un graphique que l'on voit fréquemment associé aux fonctions sphéroïdales prolates.

On teste les fonctions d'approximation de l'article de Sonnenblick et Slepian [4] par le programme fourni en annexe 1, c'est à dire qu'on vérifie en les comparant aux valeurs des tableaux qui sont fournis dans ce même article que les approximations sont assez correctes. Alors on utilise les fonctions d'approximation pour calculer les valeurs dont Alain Connes, qui les a fournies récemment dans une conférence [1], a expliqué qu'elles provenaient d'un article de Richard-Jung, Ramis, Thomann, et Fauvet : Richard-Jung et al. ont trouvé des polynômes pour calculer les fonctions prolates plus simplement car ces fonctions sont très complexes à calculer.

Voici les valeurs fournies des 31-ièmes valeurs propres obtenues par les fonctions de Richard-Jung, Ramis, Thomann, Fauvet [5], à lire par ligne, elles sont croissantes.

[1] Il s'agit d'une conférence donnée le 20 novembre 2024, pendant le Séminaire Nord-Atlantique de Géométrie non-commutative, qui a été organisé par les chercheurs de l'IMPAN à Varsovie - et qui a été l'occasion de fêter l'anniversaire de Piotr Hajac.

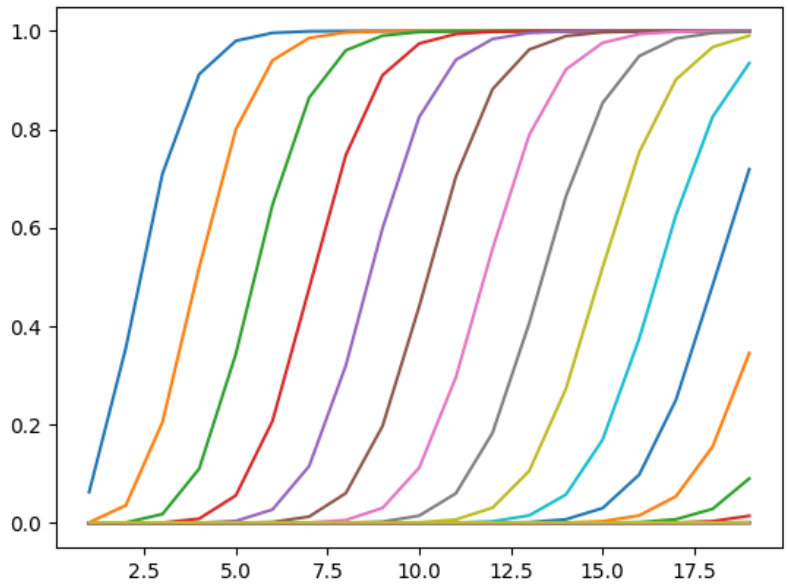
Les 14 premières 31-ièmes valeurs propres :

−39.383216574467	−94.280833772513	−152.569476972276	−214.006491323911
−278.401004621174	−324.597681671966	−415.466848582142	−487.898087149855
−562.795870371439	−640.076470907495	−719.665701171603	−801.497217687773
−885.511220599887	−971.653437429483		

Les 31-ièmes valeurs propres, de la 74$^{\text{ième}}$ à la 78$^{\text{ième}}$:

−9104.33317141284	−9281.09333576484	−9459.04366446659	9638.178978345020
−9818.49419143022			

Ces valeurs propres avaient préalablement été calculées à la main par Alain Connes et Henri Moscovici avec l'outil Mathematica, du moins leur partie entière approximative, car il s'agissait des valeurs sur lesquelles deux fonctions (à retrouver) étaient en phase ou en opposition de phase.



Voici les valeurs correspondantes (les 31-ièmes valeurs propres) calculées par les formules d'approximation fournies dans l'article d'Estelle Sonnenblick.

Les 14 premières 31-ièmes valeurs propres, approximées par Estelle Sonnenblick :

30.243951612903224	91.21975806451613	151.15927419354838	210.0383064516129
267.83266129032256	324.5181451612903	380.070564516129	434.4657258064516
487.679435483871	539.6875	590.4657258064516	639.9899193548387
688.2358870967741	735.179435483871		

Les 31-ièmes valeurs propres, de la 74$^{\text{ième}}$ à la 78$^{\text{ième}}$, approximées par Estelle Sonnenblick :

991.6260080645161	991.6260080645161	991.6260080645161	991.6260080645161
991.6260080645161			

Le passage de ces valeurs propres aux valeurs des zéros de ζ s'effectue en leur appliquant la fonction :

$$f(x) \ : \ x \mapsto \begin{cases} \mathfrak{I}(2\sqrt{-x}) & \text{si } x > 0 \\ \mathfrak{I}(2\sqrt{x}) & \text{si } x < 0 \end{cases}$$

On reporte les valeurs calculées par l'approximation d'Estelle Sonnenblick et celles calculées par Richard-Yung, Ramis, Thomann et Fauvet dans un tableau avec calcul de la fonction f pour les comparer entre elles et les comparer aux parties imaginaires des zéros non triviaux de ζ.

Les 14 premières 31-ième valeurs propres par les deux formules :

n	$a = \chi_n$ (Sonnenblick et al.)	$f(a)$	$b = \chi_n$ (Richard et al.)	$f(b)$	$\zeta(x)$
1	30.243951612903224	10.998900238278956	−39.383216574467	12.551209754357068	14.134725142
2	91.21975806451613	19.101807041692798	−94.280833772513	19.419663619384657	21.022039639
3	151.15927419354838	24.589369588791687	−152.569476972276	24.703803510575128	25.01085758
4	210.0383064516129	28.98539676813915	−214.006491323911	29.257921411057964	30.424876126
5	267.83266129032256	32.731187652776825	−278.401004621174	33.370705993201526	32.935061588
6	324.5181451612903	36.028774342810514	−342.597681671966	37.01878883334602	37.586178159
7	380.070564516129	38.99079709450059	−415.466848582142	40.76600782917758	40.918719012
8	434.4657258064516	41.68768287187243	−487.898087149855	44.176830449902354	43.327073281
9	487.679435483871	44.16693041106076	−562.795870371439	47.44663825273352	48.005150881
10	539.6875	46.46235034950342	−640.076470907495	50.59946525043501	49.773832478
11	590.4657258064516	48.599001051727456	−719.665701171603	53.65317143176545	52.970321478
12	639.9899193548387	50.59604408863755	−801.497217687773	56.62145238998283	56.446247697
13	688.2358870967741	52.468500534959986	−885.511220599887	59.515081134108755	59.347044003
14	735.179435483871	54.22838502053592	−971.653437429483	62.34271208182984	60.831778525

Les 31-ièmes valeurs propres de la 74$^{\text{ième}}$ *à la 78*$^{\text{ième}}$ *par les deux formules :*

n	$a = \chi_n$ (Sonnenblick et al.)	$f(a)$	$b = \chi_n$ (Richard et al.)	$f(b)$	$\zeta(x)$
74	991.6260080645161	62.98018761688524	−9104.33317141284	190.83325885613166	189.416158656
75	991.6260080645161	62.98018761688524	−9281.09333576484	192.6768625005591	192.026656361
76	991.6260080645161	62.98018761688524	−9459.04366446659	194.51522988667585	193.079726604
77	991.6260080645161	62.98018761688524	−9638.178978345020	196.34845533739266	195.265396680
78	991.6260080645161	62.98018761688524	−9818.49419143022	198.17663022092407	196.876481841

On obtient des valeurs qui semblent au début similaires à celles de Richard-Jung et al. avec le programme de résolution simple de Sturm-Liouville [2] et le calcul des valeurs propres fourni ci-dessous ; les valeurs semblent s'éloigner très vite de celles de Richard et al.

[2]Le calcul utilise une matrice proposé par Li-Lian Wang dans [7] (définie en (2.19)) ainsi que les formules (2.20) et (2.21) pour le calcul des fonctions prolate. Je remercie Jacques Chemla d'avoir programmé cet opérateur.

```
import matplotlib.pyplot as plt
import numpy as np
import math
from math import pi

def solve_Sturm_Liouville(c, n):
     N = int(1.1*c+n+20)
     A = np.zeros((N, N))
     for k in range(N):
          A[k, k] = k*(k+1) + (2*k*(k+1) - 1) / ((2*k+3)*(2*k-1)) * c**2
          if k+2 in range(N):
               A[k, k+2] = A[k+2, k] = (k+1)*(k+2) / ((2*k+3) * np.sqrt((2*k+1)*(2*k+5))) *
c**2
     chi, beta = np.linalg.eigh(A)
     return chi, beta, A

def prolate(c, n):
     chi, beta, A = solve_Sturm_Liouville(c, n)
     coef = np.diag([np.sqrt(k + 1/2) for k in range(len(beta))]) @ beta
     psi = [np.polynomial.Legendre(coef[:, k]) for k in range(n+1)]
     lmb = [(-1)**(k//2) * np.sqrt(2) * (
          beta[0, k] / psi[k](0) if k % 2 == 0 else
          beta[1, k] / psi[k].deriv()(0) * c / np.sqrt(3)
     ) for k in range(n+1)]
     return lmb, psi, chi, beta, A

with open("zeros200", 'r') as f:
     lines = f.readlines()
     zeros = [float(line) for line in lines]

c = 32
n = 64
lmb, psi, chi, beta, A = prolate(c, n)
for k in range(len(chi)):
     res1 = chi[k]
     res2 = 2*(res1**0.5)
     print(' ',res1, ' ',res2)
     plt.scatter(res1,res2,s=4,color='blue')
     plt.scatter(res1,zeros[k],s=4,color='red')
plt.show()
```

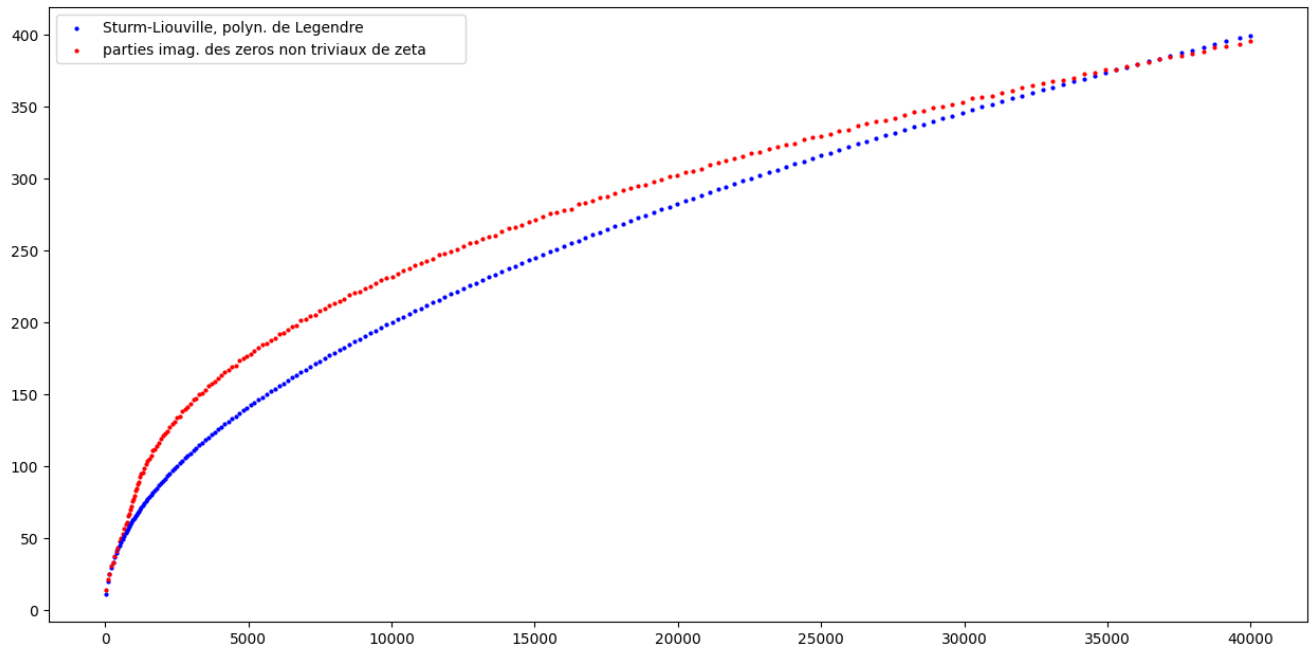
Les premières valeurs propres fournies sont les suivantes :

31.243897105576774	94.21896027377812	156.1552259401503
217.02479690312134	276.7971243661913	335.4385620950815
392.91180818935726	449.17519504826606	504.18176959991
557.8780759336684	610.2025019024709	661.0829609105459
710.4335062292904	758.149104360807	804.0968939761898
848.0998392527229	889.9026608776077	929.1041044387448
965.1026164111247	997.4723147032043	1027.3206204218318

On fournit les valeurs propres calculées par résolution de l'équation de Sturm-Liouville (en utilisant la matrice tridiagonale fournie en (19) dans [7] et les fonctions (20) et (21) de l'article en question.) en annexe 2 jusqu'à la $200^{\text{ième}}$ en les mettant en regard des parties imaginaires des zéros non triviaux

de ζ et on constate que si les valeurs diffèrent assez vite au début, elles ont tendance à se rapprocher petit à petit sur la durée.

Voici le comportement relatif des valeurs propres calculées par Sturm-Liouville et des parties imaginaires des zéros non triviaux de ζ.



On note ici qu'on a trouvé dans un article de França, LeClair [8] [3] une autre manière d'approximer les parties imaginaires des zéros non triviaux de ζ

$$g(t) = \frac{2\pi\left(t - \frac{11}{8}\right)}{W\left(\frac{t - \frac{11}{8}}{e}\right)}$$

avec W la fonction de Lambert, i.e. la réciproque de la fonction $W^{\leftarrow}(z) = ze^z$, avec z complexe. On a également trouvé dans cet article la fonction de Backlund

$$\frac{1}{\pi}\arg\Gamma\left(\frac{1}{2} + \frac{t}{2}\,i\right) + 1 + \frac{1}{\pi}\arg\zeta\left(\frac{1}{2} + it\right)$$

qui permet de rapidement calculer le nombre de zéros inférieurs à une grandeur donnée, mais qui ne semble pas découler de concepts théoriques puissants, comme ceux de la géométrie non-commutative d'Alain Connes ou ceux de la théorie quantique (on a omis de dire que la vision "opérateur issu de la physique" pour les zéros de ζ (ou les nombres premiers) consiste en fait à transposer le problème dans la théorie quantique et à compter des états quantiques dont l'énergie est bornée par une certaine grandeur).

[3] Giuseppe Mussardo a également travaillé sur ce sujet avec eux.

Références

[1] Alain Connes : Support de la conférence du 20 novembre 2024 : *From classfield theory to zeta spectral triples*, 20 novembre 2024, Séminaire Nord-Atlantique de Géométrie non-commutative 20241120-slides-Alain-Connes-anniv-Piotr.pdf (travail conjoint avec Caterina Consani et Henri Moscovici).

[2] Alain Connes, Matilde Marcolli : traduction en français du § 3.3 du livre *Noncommutative geometry, quantum field and motives*, American Mathematical Society Colloquium Publications, American Mathematical Society, 2008, vol. 55, p. https://denisevellachemla.eu/ACMM-zeta-quantique.pdf.

[3] Alain Connes, Henri Moscovici, *The UV prolate spectrum matches the zeros of zeta*, PNAS 2022, Vol. 119, n° 22, https://www.pnas.org/doi/10.1073/pnas.2123174119.

[4] David Slepian, Estelle Sonnenblick, *Eigenvalues Associated with Prolate Spheroidal Wave Functions of Zero Order*, The Bell System Technical Journal, octobre 1965, p. 1745-1759 https://denisevellachemla.eu/David-Slepian-Estelle-Sonnenblick-original.pdf.

[5] Françoise Richard-Jung, Jean-Pierre Ramis, Jean Thomann, and Frédéric Fauvet, *New Characterizations for the Eigenvalues of the Prolate Spheroidal Wave Equation*, Studies in applied mathematics, p. 1–40, 2016, Wiley Periodicals. https://denisevellachemla.eu/Richard-Jung-Ramis-Thomann-Fauvet-2016.pdf.

[6] Denise. Vella-Chemla, *Décalages*, 2024, https://denisevellachemla.eu/decalages.pdf.

[7] Li. Lian. Wang, *Analysis of spectral approximations using prolate spheroidal wave functions*, Mathematics of computation, Volume 79, Number 270, April 2010, p. 807–827.

[8] Guilherme França, André LeClair, *Transcendental equations satisfied by the individual zeros of Riemann ζ, Dirichlet and modular L-functions* https://arxiv.org/pdf/1502.06003.

Annexe 1 : extrait du programme fournissant l'approximation d'Estelle Sonnenblick

```
import numpy as np
import math ; from math import log,pi,exp
import matplotlib.pyplot as plt

def bchapo(n,c):
     res = ((n*pi/2) - c +(pi/4))/((0.5772156649/2)+(2*log(2))+(0.5*log(c)))
     return(res)

def approximelambda(n,c):
     res = 1/(1+exp(pi*bchapo(n,c)))
     return(res)
```

```
def approximechi(n,c):
     # je ne sais pas ce que signifie n grand et c grand dans l'article de
     # Estelle Sonnenblick (je prends n > 20 ?  et c > 50 ?)
     if n <= 30 and c <= 20:
          res = n*(n+1)+0.5*(1+(1/((2*n-1)*(2*n+3))))*c*c
     else:
          if n <= 30 and c > 20:
               res = (2*n+1)*c-((2*n*n+2*n+3)/4)-(((2*n+1)*(n*n+n+3))/(16*c))
          else:
               res = c*c+2*b*c+((b*b-1)/2)-((b*b-b)/(8*c))
     return(res)

for n in range(6):
     print('n = ',n)
     for c in range(1,6):
          print(approximechi(n,c),' ',end='')
     print('')

print('formule d approximation des lambda de l article d Estelle Sonnenblick ')
for x in range(1,20):
     lesy = []
     for y in range(1,20):
          print('lambda[',x,',',y,'] = ',lllambda[x,y],' approxime par ',approximelambda(x,y))
          lesy.append(lllambda[x,y])
     plt.plot(range(1,20),lesy)
plt.show()

print('formule d approximation des chi de l article d Estelle Sonnenblick ')
for x in range(1,20):
     for y in range(1,20):
          print('chi[',x,',',y,'] = ',chi[x,y],' approxime par ',approximechi(x,y))

print('la trentieme ligne')
for y in range(1,20):
     print('chi[30',',',y,'] = ',chi[30,y],' approxime par ',approximechi(30,y))

print('la trente-et-une-ieme colonne')
for y in range(0,20):
     print('chi[',y,',31] = ',chi[y,31],' approxime par ',approximechi(y,31))
for y in range(74,79):
     print('chi[',y,',31] = ',chi[y,31],' approxime par ',approximechi(y,31))
```

Le résultat de ce programme est stocké ici
https://denisevellachemla.eu/res-approxime-Slepian-Sonnenblick.pdf.

Annexe 2 : Calcul des 200 premiers zéros par résolution de l'équation différentielle de Sturm-Liouville

$31^{ièmes}$ valeurs propres de la $1^{ière}$ à la $50^{ième}$

$vp[31](x)$ Sturm − Liouville	$2\sqrt{vp[31](x)}$	$\zeta(x)$
31.24389710557676	11.17924811524939	14.134725142
94.21896027377296	19.413290321197277	21.022039639
156.15522594015044	24.992416925151552	25.010857580
217.02479690312396	29.46352300069521	30.424876126
276.79712436619167	33.27444210598829	32.935061588
335.4385620950778	36.62996380533717	37.586178159
392.91180818935743	39.64400626522791	40.918719012
449.1751950482668	42.387507359988355	43.327073281
504.18176959991007	44.90798457289795	48.005150881
557.8780759336698	47.23888550479022	49.773832478
610.2025019024709	49.40455452293729	52.970321478
661.0829609105472	51.423067232927565	56.446247697
710.4335062292903	53.30791709415367	59.347044003
758.1491043608085	55.0690150397048	60.831778525
804.0968939761894	56.71320459914744	65.112544048
848.0998392527224	58.244307507351216	67.079810529
889.9026608776078	59.66247265669125	69.546401711
929.1041044387441	60.96241807667226	72.067157674
965.1026164111245	62.1322015193772	75.704690699
997.4723147032058	63.1655702009633	77.144840069
1027.3206204218318	64.10368539863623	79.337375020
1057.7944588950675	65.04750445313233	82.910380854
1091.6948174573263	66.08161067823109	84.735492981
1129.675352045166	67.22128686793093	87.425274613
1171.2542652317939	68.44718446311123	88.809111208
1215.938430693059	69.74061745333373	92.491899271
1263.4224950736593	71.08930988759587	94.651344041
1313.5197100023847	72.4850249362552	95.870634228
1366.1058648582025	73.92173874735909	98.831194218
1421.092116378637	75.39475091486507	101.317851006
1478.4117719166898	76.9002411417985	103.725538040
1538.013113139856	78.43502057473705	105.446623052
1599.8550795064298	79.99637690561816	107.168611184
1663.90447608521	81.5819704612535	111.029535543
1730.1340732493504	83.18976074612429	111.874659177
1798.5212638337655	84.81795243540758	114.320220915
1869.0470859867453	86.46495442632802	116.226680321
1941.6954950439238	88.12934800720868	118.790782866

$31^{ièmes}$ valeurs propres de la 150$^{\text{ième}}$ à la 200$^{\text{ième}}$

$vp[31](x)$ Sturm − Liouville	$2\sqrt{vp[31](x)}$	$\zeta(x)$
22863.472066686627	302.4134392958529	321.160134309
23163.452565570347	304.39088399996706	322.144558672
23465.43344945751	306.36862404272085	323.466969558
23769.414708278193	308.3466536758795	324.862866052
24075.396332289667	310.3249672990536	327.443901262
24383.378312063665	312.3035594549871	329.033071680
24693.360638474278	314.2824248250244	329.953239728
25005.343302686408	316.26155822474794	331.474467583
25319.32629614474	318.24095459977957	333.645378525
25635.309610563105	320.2206090217374	334.211354833
25953.293237914426	322.2005166843432	336.841850428
26273.277170421094	324.1806728996724	338.339992851
26595.261400545613	326.1610730945409	339.858216725
26919.245920981863	328.141712807024	341.042261111
27245.23072464659	330.12258768310045	342.054877510
27573.21580467125	332.1036934734165	344.661702940
27903.20115439433	334.08502603016694	346.347870566
28235.18676735384	336.0665813040853	347.272677584
28569.172637280182	338.0483553415409	349.316260871
28905.1587580894	340.0303442817385	350.408419349
29243.145123876453	342.01254435401313	351.878649025
29583.131728909146	343.9949518752224	353.488900489
29925.118567621936	345.97756324722525	356.017574977
30269.105634610183	347.960374954449	357.151302252
30615.092924624663	349.94338356153935	357.952685102
30963.080432566177	351.92658571108933	359.743754953
31313.06815348044	353.90997812144514	361.289361696
31665.056082553197	355.89355758458566	363.331330579
32019.044215105438	357.87732096407245	364.736024114
32375.032546588904	359.861265193068	366.212710288
32733.02107258179	361.8453872724194	367.993575482
33093.00978878441	363.82968426880404	368.968438096
33454.99869101528	365.8141533129372	370.050919212
33818.98777520718	367.79879159783644	373.061928372
34184.977037403485	369.78359637714317	373.864873911
34552.96647375451	371.7685649634972	375.825912767
34922.9560805142	373.7536947269643	376.324092231
35294.94585403642	375.7389830935109	378.436680250
35668.93579078962	377.724427543624	379.872975347
36044.925887283185	379.7100256105081	381.484468617
36422.916144412615	381.69577490149203	383.443529450

Parties imaginaires des zéros non triviaux de zeta, fonction de Lambert, Denise Vella-Chemla, décembre 2024

On a la curiosité de simplifier encore le calcul des parties imaginaires des zéros non triviaux de la fonction ζ de Riemann par la formule trouvé dans un article de França et LeClair, modifié en 2024, téléchargeable sur arxiv ici

https://arxiv.org/pdf/1407.4358,

qu'on simplifie au maximum : on utilise le programme suivant pour calculer la fonction

$$x \mapsto \frac{2\,\pi\,x}{W\left(\frac{x}{e}\right)}$$

jusqu'à 2 millions. L'erreur va diminuant jusque là, on ne sait pas si elle finira par croître, plus loin. Le fichier contenant les 2 millions de premiers zéros de ζ a été téléchargé sur le site d'Andrew Odlyzsko ici

https://www-users.cse.umn.edu/ odlyzko/zeta_tables/index.html.

Programme python de test de l'obtention des parties imaginaires des zéros non triviaux de ζ en utilisant la fonction de Lambert $W(x)$

```
import math
from math import log,exp,pi,e
import scipy
from scipy.special import lambertw

with open("zeros2millions", 'r') as f:
     lines = f.readlines()
     zeros = [float(line) for line in lines]

print('k |2pi k/Lambert(k/e) | zeta(k) | erreur |')
for k in range(1,2000000):
     res1 = 2*pi*k/lambertw(k/e)
     print(':5d :9.5f :14.5f :8.5f'.format(k,res1.real,zeros[k],
                                          abs(res1-zeros[k])/zeros[k]))
```

Résultat du programme ci-dessus pour les 100 premiers zéros de ζ

Python se plaint pour le premier zéro en écrivant : *RuntimeWarning: invalid value encountered in scalar divide* $res1 = 2 * pi * k/lambertw(k/e)$.

k	$2\pi k/W(k/e)$	$\zeta(k)$	erreur
0	nan	14.13473	nan
1	22.56368	21.02204	0.07333
2	27.13794	25.01086	0.08505
3	31.23136	30.42488	0.02651
4	35.01238	32.93506	0.06307
5	38.56829	37.58618	0.02613
6	41.95147	40.91872	0.02524
7	45.19633	43.32707	0.04314
8	48.32696	48.00515	0.00670
9	51.36105	49.77383	0.03189
10	54.31201	52.97032	0.02533

k	$2\pi k/W(k/e)$	$\zeta(k)$	erreur
11	57.19037	56.44625	0.01318
12	60.00451	59.34704	0.01108
13	62.76130	60.83178	0.03172
14	65.46641	65.11254	0.00543
15	68.12461	67.07981	0.01558
16	70.73997	69.54640	0.01716
17	73.31597	72.06716	0.01733
18	75.85564	75.70469	0.00199
19	78.36160	77.14484	0.01577
20	80.83619	79.33738	0.01889
21	83.28146	82.91038	0.00448
22	85.69926	84.73549	0.01137
23	88.09121	87.42527	0.00762
24	90.45882	88.80911	0.01858
25	92.80341	92.49190	0.00337
26	95.12620	94.65134	0.00502
27	97.42829	95.87063	0.01625
28	99.71071	98.83119	0.00890
29	101.97438	101.31785	0.00648
30	104.22016	103.72554	0.00477
31	106.44884	105.44662	0.00950
32	108.66114	107.16861	0.01393
33	110.85776	111.02954	0.00155
34	113.03931	111.87466	0.01041
35	115.20638	114.32022	0.00775
36	117.35953	116.22668	0.00975
37	119.49927	118.79078	0.00596
38	121.62608	121.37013	0.00211
39	123.74041	122.94683	0.00645
40	125.84268	124.25682	0.01276
41	127.93330	127.51668	0.00327
42	130.01265	129.57870	0.00335
43	132.08107	131.08769	0.00758
44	134.13892	133.49774	0.00480
45	136.18649	134.75651	0.01061
46	138.22411	138.11604	0.00078
47	140.25206	139.73621	0.00369
48	142.27061	141.12371	0.00813
49	144.28002	143.11185	0.00816
50	146.28053	146.00098	0.00191
51	148.27240	147.42277	0.00576
52	150.25583	150.05352	0.00135
53	152.23105	150.92526	0.00865

k	$2\pi k/W(k/e)$	$\zeta(k)$	erreur
54	154.19826	153.02469	0.00767
55	156.15766	156.11291	0.00029
56	158.10944	157.59759	0.00325
57	160.05377	158.84999	0.00758
58	161.99084	161.18896	0.00497
59	163.92080	163.03071	0.00546
60	165.84382	165.53707	0.00185
61	167.76006	167.18444	0.00344
62	169.66965	169.09452	0.00340
63	171.57274	169.91198	0.00977
64	173.46948	173.41154	0.00033
65	175.35998	174.75419	0.00347
66	177.24438	176.44143	0.00455
67	179.12280	178.37741	0.00418
68	180.99535	179.91648	0.00600
69	182.86216	182.20708	0.00360
70	184.72334	184.87447	0.00082
71	186.57898	185.59878	0.00528
72	188.42920	187.22892	0.00641
73	190.27409	189.41616	0.00453
74	192.11374	192.02666	0.00045
75	193.94827	193.07973	0.00450
76	195.77774	195.26540	0.00262
77	197.60226	196.87648	0.00369
78	199.42191	198.01531	0.00710
79	201.23677	201.26475	0.00014
80	203.04692	202.49359	0.00273
81	204.85243	204.18967	0.00325
82	206.65339	205.39470	0.00613
83	208.44987	207.90626	0.00261
84	210.24194	209.57651	0.00318
85	212.02967	211.69086	0.00160
86	213.81312	213.34792	0.00218
87	215.59237	214.54704	0.00487
88	217.36747	216.16954	0.00554
89	219.13849	219.06760	0.00032
90	220.90549	220.71492	0.00086
91	222.66853	221.43071	0.00559
92	224.42767	224.00700	0.00188
93	226.18296	224.98332	0.00533
94	227.93445	227.42144	0.00226
95	229.68220	229.33741	0.00150
96	231.42627	231.25019	0.00076

k	$2\pi k/W(k/e)$	$\zeta(k)$	erreur
97	233.16670	231.98724	0.00508
98	234.90354	233.69340	0.00518
99	236.63684	236.52423	0.00048
100	238.36666	237.76982	0.00251

Résultat du programme ci-dessus en sautant de 10000 en 10000

k	$2\pi k/W(k/e)$	$\zeta(k)$	erreur
1	22.56368	21.02204	0.07333
10001	9879.65707	9879.03673	0.00006
20001	18048.41868	18047.99999	0.00002
30001	25756.64629	25756.39196	0.00001
40001	33191.72719	33191.34319	0.00001
50001	40435.32219	40434.98023	0.00001
60001	47532.86606	47532.50090	0.00001
70001	54513.11769	54512.56194	0.00001
80001	61395.82265	61395.85156	0.00000
90001	68195.32380	68195.19509	0.00000
100001	74922.48085	74922.59418	0.00000
110001	81585.78248	81585.87830	0.00000
120001	88192.03383	88192.10598	0.00000
130001	94746.80367	94746.68559	0.00000
140001	101254.72730	101254.70645	0.00000
150001	107719.71887	107719.30879	0.00000
160001	114145.12437	114144.89073	0.00000
170001	120533.83460	120533.66746	0.00000
180001	126888.37036	126888.50832	0.00000
190001	133210.94780	133210.65431	0.00000
200001	139503.52940	139503.24650	0.00000
210001	145767.86430	145767.64097	0.00000
220001	152005.52056	152005.45867	0.00000
230001	158217.91134	158217.97828	0.00000
240001	164406.31630	164406.12285	0.00000
250001	170571.89923	170571.85741	0.00000
260001	176715.72285	176715.35385	0.00000
270001	182838.76106	182838.87806	0.00000
280001	188941.90947	188941.72250	0.00000
290001	195025.99423	195025.50674	0.00000
300001	201091.77965	201091.34799	0.00000
310001	207139.97475	207140.01038	0.00000
320001	213171.23890	213170.84904	0.00000

k	$2\pi k/W(k/e)$	$\zeta(k)$	erreur
330001	219186.18676	219186.18476	0.00000
340001	225185.39261	225185.04899	0.00000
350001	231169.39405	231169.02030	0.00000
360001	237138.69538	237138.26425	0.00000
370001	243093.77052	243093.40254	0.00000
380001	249035.06562	249034.78222	0.00000
390001	254963.00135	254962.81145	0.00000
400001	260877.97502	260877.77142	0.00000
410001	266780.36240	266780.38777	0.00000
420001	272670.51938	272670.58651	0.00000
430001	278548.78351	278548.54962	0.00000
440001	284415.47531	284415.40621	0.00000
450001	290270.89952	290270.67490	0.00000
460001	296115.34621	296115.00624	0.00000
470001	301949.09178	301948.75496	0.00000
480001	307772.39990	307771.85195	0.00000
490001	313585.52233	313585.33992	0.00000
500001	319388.69972	319388.65016	0.00000
510001	325182.16229	325182.11046	0.00000
520001	330966.13047	330965.78541	0.00000
530001	336740.81552	336740.48966	0.00000
540001	342506.42009	342506.07911	0.00000
550001	348263.13867	348262.78609	0.00000
560001	354011.15811	354010.84011	0.00000
570001	359750.65805	359750.51936	0.00000
580001	365481.81130	365481.98893	0.00000
590001	371204.78421	371204.57638	0.00000
600001	376919.73705	376919.43116	0.00000
610001	382626.82429	382626.49448	0.00000
620001	388326.19493	388326.15656	0.00000
630001	394017.99277	394017.68117	0.00000
640001	399702.35667	399702.23199	0.00000
650001	405379.42080	405379.13884	0.00000
660001	411049.31486	411049.17763	0.00000
670001	416712.16430	416711.82640	0.00000
680001	422368.09053	422367.53258	0.00000
690001	428017.21108	428016.90685	0.00000
700001	433659.63981	433659.44198	0.00000
710001	439295.48706	439295.51621	0.00000
720001	444924.85980	444924.82418	0.00000
730001	450547.86182	450547.75865	0.00000
740001	456164.59379	456164.48468	0.00000

k	$2\pi k/W(k/e)$	$\zeta(k)$	erreur
750001	461775.15347	461774.88004	0.00000
760001	467379.63579	467379.65372	0.00000
770001	472978.13299	472977.63874	0.00000
780001	478570.73471	478570.15765	0.00000
790001	484157.52811	484157.40140	0.00000
800001	489738.59797	489738.18914	0.00000
810001	495314.02677	495313.65048	0.00000
820001	500883.89480	500883.83464	0.00000
830001	506448.28023	506448.22239	0.00000
840001	512007.25918	512006.90040	0.00000
850001	517560.90585	517561.03474	0.00000
860001	523109.29251	523109.28876	0.00000
870001	528652.48964	528652.37676	0.00000
880001	534190.56597	534190.15276	0.00000
890001	539723.58853	539723.73655	0.00000
900001	545251.62274	545251.18121	0.00000
910001	550774.73243	550774.48683	0.00000
920001	556292.97993	556292.75192	0.00000
930001	561806.42610	561806.31406	0.00000
940001	567315.13039	567314.78890	0.00000
950001	572819.15089	572819.08058	0.00000
960001	578318.54435	578318.07787	0.00000
970001	583813.36626	583812.89582	0.00000
980001	589303.67087	589303.24895	0.00000
990001	594789.51124	594789.13354	0.00000
1000001	600270.93927	600270.74787	0.00000
1010001	605748.00573	605747.54049	0.00000
1020001	611220.76031	611220.62865	0.00000
1030001	616689.25166	616688.72506	0.00000
1040001	622153.52740	622153.26585	0.00000
1050001	627613.63416	627613.41935	0.00000
1060001	633069.61761	633069.33843	0.00000
1070001	638521.52251	638521.70983	0.00000
1080001	643969.39268	643969.18514	0.00000
1090001	649413.27110	649413.09778	0.00000
1100001	654853.19988	654852.46934	0.00000
1110001	660289.22031	660289.22603	0.00000
1120001	665721.37288	665720.95905	0.00000
1130001	671149.69728	671149.49521	0.00000
1140001	676574.23248	676573.90360	0.00000
1150001	681995.01667	681994.76397	0.00000
1160001	687412.08736	687411.78506	0.00000

k	$2\pi k/W(k/e)$	$\zeta(k)$	erreur
1170001	692825.48134	692825.32909	0.00000
1180001	698235.23472	698235.19704	0.00000
1190001	703641.38297	703641.24282	0.00000
1200001	709043.96090	709043.92301	0.00000
1210001	714443.00270	714442.50436	0.00000
1220001	719838.54194	719838.27397	0.00000
1230001	725230.61161	725230.18472	0.00000
1240001	730619.24413	730619.05953	0.00000
1250001	736004.47132	736004.41822	0.00000
1260001	741386.32450	741386.63848	0.00000
1270001	746764.83441	746764.54735	0.00000
1280001	752140.03129	752140.00995	0.00000
1290001	757511.94487	757511.86133	0.00000
1300001	762880.60437	762880.44858	0.00000
1310001	768246.03855	768246.09762	0.00000
1320001	773608.27567	773608.09124	0.00000
1330001	778967.34355	778967.01138	0.00000
1340001	784323.26953	784322.85604	0.00000
1350001	789676.08055	789675.84188	0.00000
1360001	795025.80309	795025.40398	0.00000
1370001	800372.46322	800372.30529	0.00000
1380001	805716.08659	805716.03043	0.00000
1390001	811056.69847	811056.46364	0.00000
1400001	816394.32372	816394.18397	0.00000
1410001	821728.98683	821728.59790	0.00000
1420001	827060.71190	827060.42527	0.00000
1430001	832389.52267	832389.20015	0.00000
1440001	837715.44254	837715.11634	0.00000
1450001	843038.49453	843038.31553	0.00000
1460001	848358.70134	848358.44305	0.00000
1470001	853676.08532	853675.80764	0.00000
1480001	858990.66852	858990.43584	0.00000
1490001	864302.47262	864302.15119	0.00000
1500001	869611.51904	869611.24708	0.00000
1510001	874917.82886	874917.47179	0.00000
1520001	880221.42286	880221.35373	0.00000
1530001	885522.32153	885522.12472	0.00000
1540001	890820.54509	890820.43951	0.00000
1550001	896116.11344	896116.04094	0.00000
1560001	901409.04624	901408.72559	0.00000
1570001	906699.36286	906698.86174	0.00000
1580001	911987.08240	911986.96392	0.00000
1590001	917272.22371	917272.07451	0.00000
1600001	922554.80538	922554.83112	0.00000

k	$2\pi k/W(k/e)$	$\zeta(k)$	erreur
1610001	927834.84574	927834.29171	0.00000
1620001	933112.36291	933112.10103	0.00000
1630001	938387.37472	938386.95239	0.00000
1640001	943659.89880	943659.67606	0.00000
1650001	948929.95253	948929.75814	0.00000
1660001	954197.55308	954197.13337	0.00000
1670001	959462.71738	959462.19987	0.00000
1680001	964725.46215	964725.24207	0.00000
1690001	969985.80390	969985.33118	0.00000
1700001	975243.75891	975243.30147	0.00000
1710001	980499.34328	980498.83436	0.00000
1720001	985752.57289	985752.62638	0.00000
1730001	991003.46343	991003.27164	0.00000
1740001	996252.03039	996252.01168	0.00000
1750001	1001498.28907	1001498.15467	0.00000
1760001	1006742.25457	1006742.06544	0.00000
1770001	1011983.94183	1011983.66595	0.00000
1780001	1017223.36559	1017223.14191	0.00000
1790001	1022460.54041	1022460.37458	0.00000
1800001	1027695.48069	1027695.67711	0.00000
1810001	1032928.20064	1032928.00372	0.00000
1820001	1038158.71432	1038158.58525	0.00000
1830001	1043387.03560	1043386.82934	0.00000
1840001	1048613.17821	1048612.93420	0.00000
1850001	1053837.15571	1053836.87447	0.00000
1860001	1059058.98149	1059058.60937	0.00000
1870001	1064278.66881	1064278.34762	0.00000
1880001	1069496.23075	1069496.33222	0.00000
1890001	1074711.68027	1074711.41306	0.00000
1900001	1079925.03016	1079924.78216	0.00000
1910001	1085136.29306	1085135.70400	0.00000
1920001	1090345.48150	1090345.37228	0.00000
1930001	1095552.60783	1095552.09859	0.00000
1940001	1100757.68429	1100757.75763	0.00000
1950001	1105960.72297	1105960.54403	0.00000
1960001	1111161.73584	1111161.70085	0.00000
1970001	1116360.73473	1116360.55604	0.00000
1980001	1121557.73133	1121557.25561	0.00000
1990001	1126752.73722	1126752.41390	0.00000

Le fichier résultat complet pour les 2 millions de premiers zéros est téléchargeable à cette adresse https://denisevellachemla.eu/pix-par-W-de-x-2-millions.txt.

On trouve dans cet article d'István Mezö https://arxiv.org/pdf/2012.02480 une expression de la fonction de Lambert par une intégrale qu'on teste jusqu'à 2024, on fournit les fonctions de calcul

correspondantes, qu'on a ajoutées à notre programme pour effectuer la comparaison :

```
def cotan(x):
     return -tan(x+pi/2)

def lambertintegrale(x):
     return((1/pi)*quad(lambda t:log(1+(x*(sin(t)/t))*exp(t*cotan(t))),0,pi)[0])
```

k	$\dfrac{2\pi\ k}{W\left(\dfrac{k}{e}\right)}$	$\left(\dfrac{1}{\pi}\right)\displaystyle\int_0^{\pi}\log\left(1+k\ \dfrac{\sin(k)}{k}\right)\ \exp(t\ \cot(\mathrm{t}))$	$\zeta(k)$
1965	2480.11374	2480.11374	2479.97735
1966	2481.16472	2481.16472	2480.43361
1967	2482.21563	2482.21563	2481.35677
1968	2483.26646	2483.26646	2482.68341
1969	2484.31722	2484.31722	2484.50324
1970	2485.36790	2485.36790	2485.08759
1971	2486.41851	2486.41851	2485.78562
1972	2487.46905	2487.46905	2487.33384
1973	2488.51951	2488.51951	2488.11383
1974	2489.56990	2489.56990	2489.26116
1975	2490.62021	2490.62021	2490.05109
1976	2491.67045	2491.67045	2491.10552
1977	2492.72062	2492.72062	2491.90747
1978	2493.77071	2493.77071	2493.48930
1979	2494.82073	2494.82073	2494.86618
1980	2495.87067	2495.87067	2495.84684
1981	2496.92054	2496.92054	2496.48534
1982	2497.97034	2497.97034	2497.64847
1983	2499.02006	2499.02006	2497.96997
1984	2500.06971	2500.06971	2499.86204
1985	2501.11928	2501.11928	2500.56439
1986	2502.16879	2502.16879	2501.57774
1987	2503.21821	2503.21821	2503.18523
1988	2504.26757	2504.26757	2504.00893
1989	2505.31685	2505.31685	2504.77215
1990	2506.36606	2506.36606	2506.30535
1991	2507.41519	2507.41519	2507.15189
1992	2508.46425	2508.46425	2507.87104
1993	2509.51324	2509.51324	2508.76605
1994	2510.56216	2510.56216	2509.65300
1995	2511.61100	2511.61100	2511.66019
1996	2512.65977	2512.65977	2512.53822
1997	2513.70846	2513.70846	2513.57952
1998	2514.75709	2514.75709	2514.25986
1999	2515.80564	2515.80564	2515.28648

k	$\frac{2\pi\ k}{W\left(\frac{k}{e}\right)}$	$\left(\frac{1}{\pi}\right)\int_0^{\pi}\log\left(1+k\ \frac{\sin(k)}{k}\right)\ \exp(t\ \cot(\mathrm{t}))$	$\zeta(k)$
2000	2516.85411	2516.85411	2516.57105
2001	2517.90252	2517.90252	2517.14693
2002	2518.95085	2518.95085	2518.55285
2003	2519.99911	2519.99911	2519.63425
2004	2521.04729	2521.04729	2520.40232
2005	2522.09540	2522.09540	2521.88518
2006	2523.14344	2523.14344	2523.26348
2007	2524.19141	2524.19141	2523.96706
2008	2525.23931	2525.23931	2524.64205
2009	2526.28713	2526.28713	2525.68799
2010	2527.33488	2527.33488	2526.86881
2011	2528.38256	2528.38256	2527.41879
2012	2529.43016	2529.43016	2529.37804
2013	2530.47770	2530.47770	2530.27367
2014	2531.52516	2531.52516	2531.54396
2015	2532.57254	2532.57254	2531.96938
2016	2533.61986	2533.61986	2533.06732
2017	2534.66710	2534.66710	2534.40861
2018	2535.71428	2535.71428	2535.50589
2019	2536.76138	2536.76138	2536.09188
2020	2537.80840	2537.80840	2536.86749
2021	2538.85536	2538.85536	2538.55983
2022	2539.90224	2539.90224	2539.99841
2023	2540.94906	2540.94906	2540.53166
2024	2541.99580	2541.99580	2541.99873

Nombre de nombres premiers inférieurs à une grandeur donnée et fonction de Lambert, Denise Vella-Chemla, 24 décembre 2024

On souhaite simplifier au maximum l'expression trouvée pour le nombre de nombres premiers qui ferait appel à la fonction de Lambert : on utilise ce programme, qui calcule la fonction

$$f(x) = \exp(\mathrm{W}(x))$$

et la compare à la fonction qui compte le nombre de nombres premiers jusqu'à une certaine grandeur, dont on fournit les valeurs en dernière colonne du tableau.

```
import math
from math import log,exp,pi,e
import scipy
from scipy.special import lambertw

for x in range(1,30):
puiss = 10**x
print(x,' --> ',exp(lambertw(puiss)),' ',log(puiss))
```

On voit qu'il semble suffire de calculer le nombre de nombres premiers jusqu'à $\frac{x}{\ln(x)}$ et de le soustraire à l'exponentielle de l'image par la fonction de Lambert de x pour obtenir de façon vraiment assez précise le nombre de nombres premiers inférieurs à x.

x	$f(x)$	$\ln(x)$	$\frac{x}{\ln(x)}$	$\pi\left(\frac{x}{\ln(x)}\right)$	$f(x) - \pi\left(\frac{x}{\ln(x)}\right)$	$\pi(x)$
10^2	29.536	4.605	21.714	8	21	25
10^3	190.490	6.907	144.764	34	156	168
10^4	1382.772	9.210	1085.736	180	1202	1229
10^5	10770.556	11.512	8685.889	1081	9689	9592
10^6	87847.539	13.815	72382.413	7163	80684	78498
10^7	739954.524	16.118	620420.688	50644	689310	664579
10^8	6382029.546	18.420	5428681.023	376205	6005824	5761455
10^9	56048389.142	20.723	48254942.433	2902459	53145930	50847534
10^{10}	499283891.760	23.025	434294481.903	23063876	476220015	455052511
10^{11}	4499007864.959	25.328	3948131653.665	187615079	4311392785	4118054813
10^{12}	40924895425.762	27.631	36191206825.270			37607912018
10^{13}	375223433706.592	29.933	334072678387.116			346065536839
10^{14}	3463410382716.749	32.236	3102103442166.084			3204941750802
10^{15}	32152769680485.887	34.538	28952965460216.790			29844570422669
10^{16}	299987153634086.940	36.841	271434051189532.380			279238341033925
10^{17}	2811170013516462.000	39.143	2554673422960305.000			2623557157654233
10^{18}	$2.644e+16$	41.446	$2.412e+16$			24739954287740860
10^{19}	$2.496e+17$	43.749	$2.285e+17$			234057667276344607

Tableau de l'erreur relative entre $f(x) - \pi\left(\frac{x}{\ln(x)}\right)$ *et* $\pi(x)$

x	$\frac{\text{der.colonne} - \text{avant} - \text{der}}{\text{der.colonne}}$
10^2	0.16
10^3	0.071
10^4	0.0219
10^5	0.010
10^6	0.027
10^7	0.037
10^8	0.042
10^9	0.045
10^{10}	0.046
10^{11}	0.0469

L'erreur qui semble initialement décroître est décevante à partir de 10^6, la tentative de simplifier l'expression pour $\pi(x)$ était un nouveau coup d'épée dans l'eau.

Ci-dessous l'image d'une page d'une page extraite d'une référence bibliographique très illustrante de la fonction de Lambert.

6 A Final Pair of Expansions

The iterations (76–77) may be used to show that $W(z)$ can be written as

$$W(z) = \cfrac{z}{\exp\cfrac{z}{\exp\cfrac{z}{\exp\cfrac{z}{\ddots}}}} \tag{98}$$

or

$$W(z) = \ln\cfrac{z}{\ln\cfrac{z}{\ln\cfrac{z}{\ddots}}} \tag{99}$$

according as $|W(z)| < 1$ or $|W(z)| > 1$. These curious formulae are just the iterated exponential in disguise, and indeed are naturally discovered from rewriting $W(z) = z/\exp W(z)$ and $W(z) = \ln(z/W(z))$ as iterations.

Tautologies, matrices, rotations, décembre 2024

Cette manière de voir les nombres premiers me semble naturelle : plutôt que d'éliminer, selon l'instruction compliquée, qu'on doit appliquer lorsqu'on met en œuvre le crible d'Eratosthène, "tous les multiples du premier nombre qui n'a pas été barré", je préfère tout ramener sur le cercle unité, et éliminer les nombres n qui sont égaux à 1, quand on tourne n fois d'un angle plus petit $2\pi/d$, le retour sur le nombre 1 ayant lieu lorsque n est un multiple (sous-entendu entier) de d.

Ci-dessous, deux programmes python qui correspondent à cette façon de voir, l'un utilisant des points du cercle unité et l'autre utilisant les matrices de rotation correspondantes, selon l'idée de la Commission Lichnérowicz et qu'on trouve à cette page du site de Gérard Villemin :

http://villemin.gerard.free.fr/Wwwgvmm/Type/aaaCompl/Matrice.htm.

L'idée consiste à représenter les nombres complexes par des matrices 2×2.

Programme utilisant des exponentielles de norme 1

```
import mpmath
from mpmath import exp,pi
import math
from math import sqrt,floor

def premier(atester):
     k = 2
     if atester in [0, 1]:  return False
     if atester in [2, 3, 5, 7]:  return True
     while True:
          if k * k > atester:  return True
          else:
               if atester % k == 0:  return False
               else:  k = k + 1

epsilon = 1e-6
n = 98
for x in range(3,n//2+1,2):
     if x > sqrt(n):
          bool = True
          for p in range(3,floor(sqrt(n))+1):
               if premier(p):
                    if (abs(exp(2*pi*1j*n/p).real-exp(2*pi*1j*x/p).real) < epsilon)
                   and (abs(exp(2*pi*1j*n/p).imag-exp(2*pi*1j*x/p).imag) < epsilon):
                         bool = False
                    if abs(exp(2*pi*1j*x/p).real-1) < epsilon:
                         bool = False
          if bool:
               print(x, ' est un decomposant de Goldbach de ',n)
```

Programme utilisant des matrices de rotations

```
import numpy as np
from numpy import cos,sin,pi
import math
from math import floor, sqrt

def premier(atester):
     k = 2
     if atester in [0, 1]:  return False
     if atester in [2, 3, 5, 7]:  return True
     while True:
          if k * k > atester:  return True
          else:
               if atester % k == 0:  return False
               else:  k = k + 1

def matricesegales(M1,M2,epsilon):
     return((abs(M1[0,0]-M2[0,0])<epsilon) and
            (abs(M1[0,1]-M2[0,1])<epsilon) and
            (abs(M1[1,0]-M2[1,0])<epsilon) and
            (abs(M1[1,1]-M2[1,1])<epsilon))

epsilon = 1e-6
n = 98
for x in range(3,n//2+1,2):
     if x > sqrt(n):
          bool = True
          for p in range(3,floor(sqrt(n))+1):
               if premier(p):
                    Mnp = np.array([[cos(2*pi*n/p),-sin(2*pi*n/p)],
                                    [sin(2*pi*n/p),cos(2*pi*n/p)]])
                    Mxp = np.array([[cos(2*pi*x/p),-sin(2*pi*x/p)],
                                    [sin(2*pi*x/p),cos(2*pi*x/p)]])
                    if matricesegales(Mnp,Mxp,epsilon):
                         bool = False
                    if matricesegales(Mxp,np.array([[1,0],[0,1]]),epsilon):
                         bool = False
          if bool:
               print(x, ' est un decomposant de Goldbach de ',n)
```

Sur une idée de Michael Atiyah

Alain Connes

In memoriam Michael Atiyah,
avec admiration et gratitude

"In the broad light of day mathematicians check their equations and their proofs, leaving no stone unturned in their search for rigour. But, at night, under the full moon, they dream, they float among the stars and wonder at the miracle of the heavens. They are inspired. Without dreams there is no art, no mathematics, no life." [1]

(Michael Atiyah, Les Déchiffreurs 2008, Notices de l'AMS, 2010).

1 Introduction

Le théorème de Feit–Thompson sur la résolubilité des groupes finis d'ordre impair venait souvent à l'esprit de Michael Atiyah pendant sa participation à la conférence de Shanghai de 2017 au sujet de la géométrie non-commutative. La présence vivante de Michael parmi nous, et son inextinguible enthousiasme pour toutes les mathématiques – anciennes, nouvelles, et encore à créer – furent des points forts de cette rencontre.

L'idée de Michael que nous allons examiner dans cette note a été conçue par lui durant son voyage vers Shanghai. C'est une nouvelle stratégie pour FT, basée sur le processus itératif qu'il a esquissé.

5. The Iterative Process

Having started the Artin process of using the conjugation action of G on its non-empty subsets we now plan to iterate this process N times. As explained at the end of Section 3, the purpose of the iteration is to handle groups of any odd exponent $n \leq N$. The index j increases with the exponent n but eventually stops at N.

Our iterative process will produce a finite sequence, indexed by j (with $1 \leq j \leq N$), of

$$\text{odd integers } N_j, \text{ with } N_1 = N = |G|, \quad N_{j+1} = 2^{N_j} - 1 \tag{5.1}$$

$$\text{sets } S_j \text{ with } |S_j| = N_j, S_1 = G, \quad S_{j+1} = (2^{S_j})^* \tag{5.2}$$

$$\text{real fields } k_j \text{ with } k_1 = \mathbb{Q} \text{ and } k_{j+1} = N_j \times N_j \text{ matrices over } k_j \tag{5.3}$$

Figure 1 : Extrait des notes de Michael Atiyah [3]

Son idée est d'utiliser ce processus pour construire un caractère non trivial du groupe fini G. Prise trop à la lettre, cette idée ne peut pas fonctionner parce qu'elle s'appliquerait au groupe des permutations de G qui commute avec l'involution $g \mapsto g^{-1}$ et ce groupe n'a que des caractères d'ordre

Traduction : Denise Vella-Chemla, décembre 2024, de l'article Arxiv https://arxiv.org/pdf/1901.10761 .

[1] "Au grand jour, les mathématiciens vérifient leurs équations et leurs preuves, retournant chaque pierre dans leur recherche de rigueur. Mais, la nuit, sous la pleine lune, ils rêvent, ils flottent parmi les étoiles et s'émerveillent devant le miracle des cieux. Ils sont inspirés. Sans rêves, il n'y a pas d'art, pas de mathématiciens, pas de vie."

pair.

Le but du présent article, comme un hommage à une imagination lumineuse qui ne s'est jamais atténuée, est de prendre au sérieux la proposition de Michael Atiyah et de montrer que, en la comprenant dans un sens plus large, on aboutit à une idée très intéressante.

Mon point de départ est d'étudier plus généralement les itérations de la transformation qui remplace une représentation π d'un groupe fini G sur un espace vectoriel de dimension finie E par la différence $\wedge\pi - 1$, où $\wedge\pi$ est l'action de G sur la somme des puissances extérieures $\wedge^n E$ et 1 est la représentation triviale.

On montre d'abord, dans le § 2 (Proposition 2.1) que l'opération $\pi \mapsto \wedge\pi$ s'étend aux représentations virtuelles si et seulement si le groupe G est d'ordre impair. On discute brièvement dans le § 3 de ce qui ne va pas quand le groupe fini est d'ordre pair. Dans le cas impair, on montre dans le lemme 4.1 que l'opération wedge $\wedge : R(G)_{\mathbb{Z}} \to R(G)_{\mathbb{C}}$ est donnée par la formule :

$$\wedge(x) = e^{\Sigma_1^k c_j \psi_j(x)}, \;\; c_j = (-1)^{j+1} \frac{H(j/k)}{k} \tag{1}$$

où k est l'ordre impair de G, les ψ_j sont les opérations de Adams et la fonction $H(u)$ est la somme alternée $\sum \frac{(-1)^n}{n+u}$. Cela permet d'étendre l'opération wedge à des fonctions à valeurs complexes sur le groupe G et ainsi de donner un sens à l'opération $\Psi(f) := \wedge f - 1$ sur de telles fonctions. On peut alors tester l'idée d'Atiyah d'utiliser l'itération de Ψ.

Evidemment, les caractères uni-dimensionnels, *i.e.* les morphismes $\chi : G \to \mathbb{C}^*$, sont les points fixes de Ψ puisque $\wedge\chi = 1 + \chi$. On étudie la transformation Ψ dans le cas non trivial le plus simple, le groupe non commutatif fini d'ordre impair le plus petit, qui est d'ordre 21. On détermine d'abord, dans le § 5 la transformation linéaire T sur la classe des fonctions pour lesquelles le wedge est la composition de l'exponentielle avec T. On trouve que T a un noyau non trivial. Dans le § 6, on peut finalement étudier les itérations de l'application Ψ dans notre exemple concret. Comme attendu lorsqu'on prend comme point de départ la représentation ρ donnée par l'action de G sur elle-même par conjugaison, l'itération $\Psi^{\circ n}(\rho)$ explose très rapidement et ne converge nulle part, rendant ainsi difficile d'imaginer qu'une telle itération puisse être utilisée pour prouver l'existence d'un caractère uni-dimensionnel non trivial. On montre dans le § 6, par un calcul effectif, que pour une classe complète de données initiales, les itérations de l'application Ψ convergent effectivement joliment vers un des deux caractères non triviaux du groupe G. Disons de façon plus détaillée que le groupe G a 4 classes de conjugaison non-triviales habituellement dénotées $7A$, $7B$ qui sont d'ordre 7 et de taille 3 et $3A$, $3B$ qui sont d'ordre 3 et de taille 7. On teste d'abord l'itération de Ψ sur les fonctions centrales f qui valent 1 excepté sur les classes $3A$, $3B$ sur lesquelles elles prennent des valeurs conjuguées. Ainsi, f est à valeur complexe et elle remplit la condition $f(g^{-1}) = \overline{f(g)}$. De telles fonctions dépendent d'un seul nombre complexe $z = f(3A)$ et l'analyse de Ψ devient l'itération d'une transformation du plan complexe qui est donnée explicitement dans le lemme 6.2.

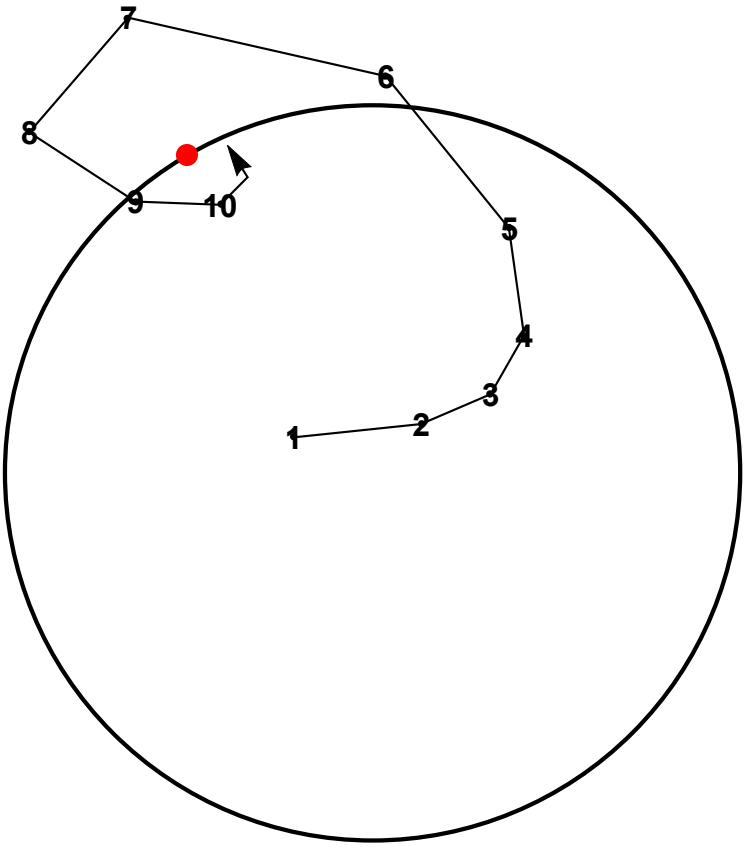


FIGURE 2 : Itération de la transformation $\Psi =$ wedge moins un.

L'itération concrète de cette transformation avec une donnée initiale proche de l'origine montre qu'en démarrant à partir d'un point sur l'axe réel, on converge vers le caractère de la représentation triviale, mais qu'en commençant à partir d'un point dans le demi-plan supérieur, on converge vers le caractère uni-dimensionnel non trivial de G (et vers son conjugué si on démarre à partir d'un point dans le demi-plan inférieur).

Pourtant, en étudiant plus avant le comportement de la transformation Ψ sur les fonctions non triviales sur les autres classes de conjugaison, on trouve un point fixe attracteur qui ne correspond pas à un caractère uni-dimensionnel. On montre dans le § 7 que les points fixes pour les autres classes de conjugaison sont les solutions d'une équation de Lambert $we^w = u$ dans laquelle la valeur $u = -\frac{6}{7}2^{-\frac{5}{7}} \log 2 \sim -0.362124$ s'avère appartenir à l'intervalle $[-1/e, 0)$ où deux solutions réelles existent. Alors que l'une d'elles correspond au caractère de la représentation triviale, l'autre ne provient pas d'un caractère. De plus, elle est le point fixe qui ne correspond pas à un caractère qui est un attracteur et cela rend assez difficile de conjecturer une relation précise entre les points fixes et les caractères des représentations uni-dimensionnelles.

Incidemment, il s'avère, de façon intéressante, qu'à la fois l'itération de l'exponentiation et l'équation de Lambert ont été étudiées par L. Euler [7,8] et on peut considérer la détermination des points fixes de l'opération $\Psi =$ wedge moins un, pour les groupes finis d'ordre impair, comme une variation de ces développements initiaux.

2 Imparité et wedge

On caractérise les groupes finis impairs *i.e.* les groupes dont l'ordre est un nombre entier impair, en fonction de la structure de λ-anneau de l'anneau de représentation $R(G)_{\mathbb{Z}}$. L'opération $\pi \mapsto \wedge\pi$ a du sens pour des représentations finies dimensionnelles et l'objectif est de voir si cette application s'étend à la représentation virtuelle en respectant la loi $\wedge(\pi_1 \oplus \pi_2) = \wedge(\pi_1) \otimes \wedge(\pi_2)$.

Proposition 2.1. *Soit G un groupe fini, les conditions suivantes sont équivalentes.*

1. *L'ordre de G est impair.*
2. *L'application $\wedge$ s'étend aux représentations virtuelles comme un morphisme du groupe additif $R(G)_{\mathbb{Z}}$ au monoïde multiplicatif $R(G)_{\mathbb{C}}$.*

Preuve. Supposons d'abord que l'application $\wedge$ s'étend à un morphisme. On a $\wedge(0) = 1$ et par conséquent,

$$\wedge(\pi) \wedge (-\pi) = 1 \in R(G)_{\mathbb{C}}$$

En passant à l'anneau $C(G)$ des fonctions centrales par l'application de Brauer, on obtient que le caractère de $\wedge(\pi)$ est inversible dans $C(G)$ et par conséquent, qu'il ne s'évanouit pas. Ainsi, par le lemme 2.2 (ci-dessous), il découle que G est d'ordre impair. Supposons maintenant que G est d'ordre impair.

Par construction, le groupe additif $R(G)_{\mathbb{Z}}$ s'obtient par symétrisation du monoïde additif des représentations finies dimensionnelles de G. Donc l'existence de l'extension est automatique si l'application $\wedge$ atterrit sur les éléments inversibles du monoïde multiplicatif $R(G)_{\mathbb{C}}$. Ce monoïde est le même que le monoïde de la classe des fonctions à valeurs complexes $C(G)$ selon le produit terme à terme. Un élément dans $C(G)$ est inversible ssi il ne s'évanouit pas et par conséquent, on obtient l'existence de l'extension en utilisant le lemme 2.2. □

Lemme 2.2. *Soit G un groupe fini, les conditions suivantes sont équivalentes*

1. *L'ordre de G est impair.*
2. *Pour toute représentation finie dimensionnelle π de G, les caractères de $\wedge\pi$ ne s'évanouissent pas :*

$$\mathrm{Tr}(\wedge\pi(g)) \neq 0\,,\ \forall g \in G$$

Preuve. Si G est d'ordre pair, il contient un élément g d'ordre 2 et $\lambda(g)$ a la valeur propre -1 dans la représentation régulière, de telle façon que

$$\mathrm{Tr}(\wedge\pi(g)) = \prod(1+\alpha) = 0$$

Si G est d'ordre impair, n'importe quel élément $g \in G$ est d'ordre impair et par conséquent, -1 ne peut pas être une valeur propre de $\pi(g)$ puisque $(-1)^k \neq 1$ pour k impair. Par conséquent,

$$\mathrm{Tr}(\wedge\pi(g)) = \prod(1+\alpha) \neq 0$$

Donc on obtient la conclusion souhaitée. □

3 Euler et les séries divergentes

On explique brièvement ce qui ne va pas dans le cas pair. Il est intéressant de noter qu'étendre l'application $\wedge$ achoppe sur la sommation des séries divergentes. Pour être plus précis, on a par construction

$$\wedge = \sum_0^\infty \lambda_j \tag{2}$$

où les λ_j sont les opérations lambda qui font partie de la structure de l'anneau de représentation. Dans le cas le plus simple, *i.e.* quand le groupe G est réduit à un élément, les opérations λ_j sont données par les coefficients binomiaux

$$\lambda_j(x) := \frac{1}{j!}\prod_0^{j-1}(x-k) \tag{3}$$

Par conséquent, quand on applique (2) à des nombres négatifs $x \in \mathbb{Z}$, on obtient les sommes infinies

$$\wedge(-1) = 1 + (-1) + 1 + (-1) + 1 + \dots$$

$$\wedge(-2) = 1 - 2 + 3 - 4 + 5 + \dots$$

pour lesquelles Leibniz et Euler donnent les valeurs $\frac{1}{2}$ et $\frac{1}{4}$ respectivement (voir [6, 4]).

. For
this reason, if we employ this definition of sum, that is to say,
the sum of a series is that quantity which generates the series,
all doubts with respect to divergent series vanish and no further
controversy remains on this score, inasmuch as this definition is
applicable equally to convergent or divergent series. Accordingly
Leibniz, without any hesitation, accepted for the series
1 - 1 + 1 - 1 + etc., the sum *1/2*, which arises out of the expan-
sion of the fraction *1/1+1*, and for the series
1 - 2 + 3 - 4 + 5 - 6 + 7 - 8 etc. the sum *1/4*, which arises out
of the expansion of the formula $1/(1+1)^2$.

FIGURE 3 : Euler et les séries divergentes.

Ces valeurs donnent la réponse correcte $\wedge(-j) = 2^{-j}$ grâce aux signes alternés. Ce que la proposition 2.1 montre, c'est qu'on ne peut pas définir ces sommes de séries infinies quand tous les signes sont identiques puisque l'extension de l'application $\wedge$ n'est pas possible à moins que le groupe ne soit impair. Pour voir concrètement ce qui arrive dans le cas pair, considérons le groupe cyclique C d'ordre 2. Les éléments de $R(G)_\mathbb{Z}$ sont de la forme $n + m\chi$ où $\chi^2 = 1$ et $n, m \in \mathbb{Z}$. La structure du λ-anneau est telle que

$$\lambda_j(m\chi) := \frac{1}{j!}\prod_0^{j-1}(m-k)\chi^j \tag{4}$$

alors que l'application de Brauer envoie en particulier $\chi \mapsto -1$ par évaluation sur la classe de conjugaison non triviale. Par conséquent, sur cette classe, on obtient les sommes infinies

$$\wedge(-\chi) \mapsto 1 + 1 + 1 + \dots$$

$$\wedge(-2\chi) = 1 + 2 + 3 + 4 + 5 + \dots$$

et Euler énonce clairement que de telles sommes sont infinies, alors que leurs analogues alternées ne le sont pas.

4 Wedge en fonction des opérations de Adams

Quand l'ordre de G est impair, il est possible d'écrire une formule pour l'opération $\wedge$ comme une exponentielle d'une combinaison linéaire d'opérations de Adams dans l'anneau de représentation $R(G)_{\mathbb{Z}}$.

On utilise, pour $u > 0$, la notation suivante pour la fonction de Hurwitz

$$H(u) = \sum_{m=0}^{\infty} \frac{(-1)^m}{m+u}$$

où la somme est convergente et peut être calculée pour des valeurs rationnelles de u, comme

$$H(2/3) = \frac{\pi}{\sqrt{3}} - \log(2)$$

En général, on a avec k un entier impair et $j \in \{1, \ldots, k\}$,

$$H(j/k) = (-1)^{j+1} \sum_{|v|<k/2} \left(\cos\left(\frac{2\pi jv}{k}\right) \log\left(2\cos(\frac{\pi v}{k}\right) + \frac{\pi v}{k} \sin\left(\frac{2\pi jv}{k}\right)\right)$$

Théorème 4.1. *Soit G un groupe fini d'ordre impair k. Soit ψ_j les endomorphismes de Adams de l'anneau de représentation $R(G)_{\mathbb{Z}}$. Alors l'opération wedge $\wedge : R(G)_{\mathbb{Z}} \to R(G)_{\mathbb{C}}$ est donnée par la formule :*

$$\wedge(x) = e^{\sum_1^k c_j \psi_j(x)}, \;\; c_j = (-1)^{j+1} \frac{H(j/k)}{k} \tag{5}$$

Preuve. Les deux côtés définissent des morphismes du groupe additif $R(G)_{\mathbb{Z}}$ vers le monoïde multiplicatif $R(G)_{\mathbb{C}}$. Par conséquent, il suffit de vérifier l'égalité (5) quand $x = \pi$ est une représentation effective de G. On évalue la fonction de classe associée aux deux côtés sur un élément du groupe $g \in G$. En exprimant la trace en fonction des valeurs propres α_j de $\pi(g)$, le côté gauche donne $\prod(1+\alpha_j)$. Pour le côté droit, la formule est l'exponentielle calculée point par point dans l'anneau de classe $C(G)$ de l'expression obtenue en remplaçant $\psi_j(x)$ par $\sum \alpha_i^j$. Par conséquent, puisque l'exponentielle transforme l'addition en produit, il suffit de montrer que pour tout $\alpha \in \mathbb{C}$ avec $\alpha^k = 1$, on a

$$1 + \alpha = e^{\sum_1^k c_j \alpha^j}$$

Pour voir cela, considérons pour $0 < t < 1$ la formule

$$\log(1+\alpha t) = \sum_1^{\infty} (-1)^{j+1} \frac{\alpha^j t^j}{j}$$

En utilisant $\alpha^k = 1$, on réécrit le côté droit comme

$$\sum_1^k (-1)^{j+1} \alpha^j t^j \left(\sum_0^{\infty} (-1)^u \frac{t^{ku}}{j+ku} \right)$$

En appliquant l'exponentielle aux deux côtés (encore pour $t < 1$), on a

$$1 + t\alpha = \exp\left(\sum_1^k (-1)^{j+1}\alpha^j t^j \left(\sum_0^\infty (-1)^u \frac{t^{ku}}{j+ku}\right)\right)$$

Maintenant, quand $t \to 1$, on a la convergence

$$\lim_{t\to 1}\left(\sum_0^\infty (-1)^u \frac{t^{ku}}{j+ku}\right) = \frac{1}{k}H(j/k).$$

En effet, on a $j \geq 1$ et

$$\frac{t^{2kv}}{j+2kv} - \frac{t^{2kv+k}}{j+2kv+k} = \frac{t^{2kv}k}{(j+2kv)(j+2kv+k)} + \frac{t^{2kv}\left(1-t^k\right)}{(j+2kv+k)}$$

où l'on contrôle le comportement de la série faisant intervenir le dernier terme quand $t \to 1$ parce qu'on a $(1-t^k)|\log(1-t^{2k})| \to 0$ quand $t \to 1$.

Donc, la continuité de l'exponentielle permet de passer à la limite quand $t \to 1$ et fournit l'égalité requise. □

Corollaire 4.2. *Soit G un groupe fini d'ordre impair k. L'extension canonique de l'opération wedge $\wedge$: $R(G)_{\mathbb{C}} \to R(G)_{\mathbb{C}}$ (donnée par la formule (5)) a un noyau non trivial donné par les fonctions centrales $f(g)$ telles que*

$$\sum_1^k (-1)^j H(j/k) f(g^j) \in 2\pi ik\mathbb{Z}, \ \forall g \in G.$$

Preuve. La condition découle de (5). La transformation

$$T(f)(g) := \sum_1^k (-1)^j H(j/k) f(g^j) \tag{6}$$

est une application linéaire $T : R(G)_{\mathbb{C}} \to R(G)_{\mathbb{C}}$ sur les fonctions centrales. Si le noyau de T est trivial alors T est surjective et l'image inverse du réseau $(2\pi ik\mathbb{Z})^c$, où c est le nombre de classes, est non triviale. Par conséquent, dans toutes les cas, le noyau de $\wedge : R(G)_{\mathbb{C}} \to R(G)_{\mathbb{C}}$ est non trivial. □

5 Le premier groupe impair non abélien

On peut se demander si l'application linéaire (6) est toujours injective. Cela n'est pas le cas en général. On étudie l'exemple non abélien le plus simple. Le premier groupe non abélien d'ordre impair est d'ordre 21 et est le produit semi-direct du groupe cyclique $C(7)$ par le groupe cyclique $C(3)$ agissant non trivialement. C'est un sous-groupe d'indice 2 dans le groupe affine de $\mathbb{F}_7$. C'est un sous-groupe transitif du groupe de permutations sur 7 lettres et on le dénote TransitiveGroup(7,3).

Ce groupe a 5 classes de conjugaison, les 4 classes non triviales, étiquetées $\gamma_2, \gamma_3, \gamma_4, \gamma_5$ (ou simplement $2, 3, 4, 5$ quand aucune confusion ne peut se produire) sont de la forme :

$$\gamma_2 = 7A, \gamma_3 = 7B,\ \gamma_4 = 3A,\ \gamma_5 = 3B,$$

où les classes $7A$ et $7B$ sont d'ordre 7 et de taille 3, et les classes $3A$ et $3B$ sont d'ordre 3 et de taille 7. L'action de l'inversion $j : g \mapsto g^{-1}$ échange simplement $3A$ et $3B$ d'une part, et $7A$ et $7B$ d'autre part. L'action de G sur lui-même par conjugaison commute avec l'inversion et se réduit (en plus de la représentation triviale) à la somme de deux copies des représentations de G par des permutations des ensembles à 3 et à 7 éléments. La représentation par des permutations sur l'ensemble à trois éléments $7A$ se fait par des permutations cycliques en utilisant le morphisme

$$G = C(7) \rtimes C(3) \to C(3)$$

La représentation par des permutations sur l'ensemble à sept éléments $3A$ est fidèle et elle donne

$$G \simeq \text{TransitiveGroup}(7, 3)$$

(dans la notation standard de théorie des groupes).

L'action des 21 applications puissance $g \mapsto g^n$, $n = 1, \ldots, 21$, sur la classe de conjugaison 2 est donnée par

$$\{2, 2, 3, 2, 3, 3, 1, 2, 2, 3, 2, 3, 3, 1, 2, 2, 3, 2, 3, 3, 1\}$$

Sur la classe de conjugaison 3, elle est donnée par

$$\{3, 3, 2, 3, 2, 2, 1, 3, 3, 2, 3, 2, 2, 1, 3, 3, 2, 3, 2, 2, 1\}$$

Ces classes sont d'ordre 7 et par conséquent, l'exposant pertinent dans (5) se réduit sur la classe 2 à

$$\frac{1}{7}u(1)H(1) + \frac{1}{7}u(2)\left(H\left(\frac{1}{7}\right) - H\left(\frac{2}{7}\right) - H\left(\frac{4}{7}\right)\right) + \frac{1}{7}u(3)\left(H\left(\frac{3}{7}\right) + H\left(\frac{5}{7}\right) - H\left(\frac{6}{7}\right)\right)$$

et sur la classe 3 à la même expression avec $u(2)$ et $u(3)$ échangés.

Mais on a

$$-H\left(\frac{1}{7}\right) + H\left(\frac{2}{7}\right) + H\left(\frac{4}{7}\right) = -H\left(\frac{3}{7}\right) - H\left(\frac{5}{7}\right) + H\left(\frac{6}{7}\right)$$

En fait, de façon plus précise, on a

$$H\left(\frac{1}{7}\right) + H\left(\frac{6}{7}\right) = \frac{\pi}{\sin(\frac{\pi}{7})}, H\left(\frac{2}{7}\right) + H\left(\frac{5}{7}\right) = \frac{\pi}{\cos(\frac{3\pi}{14})}, H\left(\frac{3}{7}\right) + H\left(\frac{4}{7}\right) = \frac{\pi}{\cos\left(\frac{\pi}{14}\right)}$$

et l'égalité ci-dessus découle de

$$\frac{1}{\sin(\frac{\pi}{7})} = \frac{1}{\cos(\frac{3\pi}{14})} + \frac{1}{\cos\left(\frac{\pi}{14}\right)}$$

En fait, on trouve que dans les deux cas, la somme se réduit à

$$\frac{\log 2}{7}\, u(1) + \frac{3}{7}\log 2\,(u(2) + u(3))$$

Donc cela signifie que le $\wedge(u)$ dépend seulement de la somme $u(2)+u(3)$ de la fonction centrale u, *i.e.* la somme de leurs valeurs sur les classes $7A$ et $7B$. La table de caractères pour G est la suivante

classe	1	7A	7B	3A	3B
taille	1	3	3	7	7
ρ_1	1	1	1	1	1
ρ_2	1	1	1	j^2	j
ρ_3	1	1	1	j	j^2
ρ_4	3	$\frac{-1-\sqrt{-7}}{2}$	$\frac{-1+\sqrt{-7}}{2}$	0	0
ρ_5	3	$\frac{-1+\sqrt{-7}}{2}$	$\frac{-1-\sqrt{-7}}{2}$	0	0

où $j := e^{\frac{2\pi i}{3}}$. On voit sur cette table que les caractères des représentations ρ_4 et ρ_5 ont la même somme sur les classes $7A$ et $7B$. Par conséquent, on obtient le

Lemme 5.1. *Les représentations irréductibles ρ_4 et ρ_5 du groupe $G = C(7) \rtimes C(3)$ deviennent isomorphes après avoir appliqué le wedge, $\wedge\rho_4 = \wedge\rho_5$.*

Preuve. En effet, l'application T de (6) prend la même valeur sur ρ_4 et ρ_5 et le caractère de $\wedge\rho_j$ est une fonction de $T\rho_j$ de telle façon que les $\wedge\rho_j$ ont le même caractère et par conséquent sont égaux. □

En fait, calculons les caractères de $\wedge\rho_j$. Sur les classes $7A$ et $7B$, ils vérifient l'égalité $u(2)+u(3) = -1$ et par conséquent, on obtient, puisque $u(1) = 3$,

$$\frac{\log 2}{7}\, u(1) + \frac{3}{7}\log 2\,(u(2)+u(3)) = 0$$

Après avoir pris l'exponentielle, cela donne la même contribution que $2\rho_1 + \rho_4 + \rho_5$ puisque le dernier est égal à $2-1=1$ sur les classes $7A$ et $7B$. Les réponses concordent pour la classe de conjugaison triviale où elles donnent toutes les deux 8. Il reste à voir ce qu'elles donnent sur les classes $3A$ et $3B$. Ces classes sont d'ordre 3 et l'action de la fonction puissance sur la classe 4 est de la forme

$$\{4,5,1,4,5,1,4,5,1,4,5,1,4,5,1,4,5,1,4,5,1\}$$

donc la somme pertinente se réduit sur la classe 4 à

$$\frac{1}{3}u(1)H(1) + \frac{1}{3}u(4)H\left(\frac{1}{3}\right) - \frac{1}{3}u(5)H\left(\frac{2}{3}\right)$$

et sur la classe 5 à la même expression avec $u(4)$ et $u(5)$ échangés. Mais on a

$$H(1/3) = \frac{\pi}{\sqrt{3}} + \log(2),\ H(2/3) = \frac{\pi}{\sqrt{3}} - \log(2)$$

À la fois pour ρ_4 et pour ρ_5, on a $u(1)=3$, $u(4)=0$ et $u(5)=0$. Donc dans les deux cas, on a

$$\frac{1}{3}u(1)H(1) + \frac{1}{3}u(4)H\left(\frac{1}{3}\right) - \frac{1}{3}u(5)H\left(\frac{2}{3}\right) = \frac{1}{3}u(1)H(1) = \log 2$$

et après avoir prix l'exponentiation, cela donne 2. Ainsi nous avons montré

$$\wedge\rho_j = 2\rho_1 + \rho_4 + \rho_5\,,\ \forall j = 4,5 \tag{7}$$

et cela correspond dans chaque cas à la décomposition de $\wedge$ comme $\sum \wedge^j$.

On a ainsi calculé la matrice T agissant sur les vecteurs colonne comme étant

$$T = \begin{pmatrix} \log(2) & 0 & 0 & 0 & 0 \\ \frac{\log(2)}{7} & \frac{3\log(2)}{7} & \frac{3\log(2)}{7} & 0 & 0 \\ \frac{\log(2)}{7} & \frac{3\log(2)}{7} & \frac{3\log(2)}{7} & 0 & 0 \\ \frac{\log(2)}{3} & 0 & 0 & \frac{1}{3}\left(\log(2) + \frac{\pi}{\sqrt{3}}\right) & \frac{1}{3}\left(\log(2) - \frac{\pi}{\sqrt{3}}\right) \\ \frac{\log(2)}{3} & 0 & 0 & \frac{1}{3}\left(\log(2) - \frac{\pi}{\sqrt{3}}\right) & \frac{1}{3}\left(\log(2) + \frac{\pi}{\sqrt{3}}\right) \end{pmatrix}$$

Ses valeurs propres sont

$$\left\{\frac{2\pi}{3\sqrt{3}}, \log(2), \frac{6\log(2)}{7}, \frac{2\log(2)}{3}, 0\right\}$$

Ses vecteurs propres sont les lignes de la matrice :

$$\begin{pmatrix} 0 & 0 & 0 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & -1 & 1 & 0 & 0 \end{pmatrix}$$

6 Itération de $\Psi =$ wedge -1

Le calcul ci-dessus restreint à la classe des fonctions qui prennent les mêmes valeurs sur les classes $2 = 7A$ et $3 = 7B$ et les mêmes valeurs sur $4 = 3A$ et $5 = 3B$ donne les résultats suivants.

Lemme 6.1. *Soit $G = C(7) \rtimes C(3)$. Soit $f \in R(G)$ une fonction classe qui est réelle et invariante sous $g \mapsto g^{-1}$. Alors, pour les trois valeurs de f sur la classe triviale 1, la classe $2 = 7A$ et la classe $4 = 3A$, on a*

$$\wedge(f)(1) = 2^{f(1)},\ \wedge(f)(2) = 2^{\frac{1}{7}f(1)+\frac{6}{7}f(2)},\ \wedge(f)(4) = 2^{\frac{1}{3}f(1)+\frac{2}{3}f(4)} \tag{8}$$

Preuve. La formule pour $\wedge f(2)$ vient de l'expression ci-dessus

$$\frac{\log 2}{7}\,u(1) + \frac{3}{7}\log 2\,(u(2) + u(3))$$

avec $u(2) = u(3) = f(2)$. La formule pour $\wedge f(4)$ provient de

$$\frac{1}{3}u(1)H(1) + \frac{1}{3}u(4)H\left(\frac{1}{3}\right) - \frac{1}{3}u(5)H\left(\frac{2}{3}\right)$$

avec $u(4) = u(5) = f(4)$ alors $H\left(\frac{1}{3}\right) - H\left(\frac{2}{3}\right) = 2\log 2$. □

Pour l'action du groupe sur lui-même par conjugaison, le caractère associe à $g \in G$ l'ordre de son commutant. Ici, cela donne 21 pour la classe 1, 7 pour les classes $2 = 7A$, $3 = 7B$, et 3 pour $4 = 3A$ et $5 = 3B$. Quand on commence à itérer le wedge -1 sur son point de départ, il devient immédiatement hors de portée puisque après deux étapes, il ressemble, pour les paires $(f(1), f(4))$ à :

$$\{21, 3\},\ \{2097151, 511\},\ \{2.272148509580683 \times 10^{631305}, 4.674093841761078 \times 10^{210537}\}$$

Pourtant, nous allons expliquer maintenant que cela se produit à cause d'un mauvais choix du point de départ. On élimine la condition $u(4) = u(5)$ et on impose les conditions $u(1) = u(2) = u(3) = 1$ qui sont par construction stables par la transformation $h \mapsto \wedge h - 1$. On définit $u(4) = x + iy$ un nombre complexe et on remplace la condition $u(4) = u(5)$ par $\overline{u(4)} = u(5)$. Alors on a le

Lemme 6.2. *La condition $\overline{u(4)} = u(5)$ est invariante par $h \mapsto \wedge h - 1$ et, en fonction des variables réelles (x, y), $u(4) = x + iy$, la transformation $h \mapsto \wedge h - 1$ est donnée par*

$$\Phi(x, y) := \left(2^{\frac{1}{3}(2x+1)} \cos\left(\frac{2\pi y}{3\sqrt{3}}\right) - 1, 2^{\frac{1}{3}(2x+1)} \sin\left(\frac{2\pi y}{3\sqrt{3}}\right)\right)$$

Preuve. On a, par définition, en utilisant $u(1) = 1$, que les composants pour $v = \wedge u - 1$ sont

$$v(4) = \exp\left(\frac{1}{3}H(1) + \frac{1}{3}u(4)H\left(\frac{1}{3}\right) - \frac{1}{3}u(5)H\left(\frac{2}{3}\right)\right) - 1$$

$$v(5) = \exp\left(\frac{1}{3}H(1) + \frac{1}{3}u(5)H\left(\frac{1}{3}\right) - \frac{1}{3}u(4)H\left(\frac{2}{3}\right)\right) - 1$$

On a

$$H(1) = \log(2),\ H(1/3) = \frac{\pi}{\sqrt{3}} + \log(2),\ H(2/3) = \frac{\pi}{\sqrt{3}} - \log(2)$$

par conséquent, les exponentiations donnent respectivement $\frac{\log 2}{3}(2x + 1) + \frac{2i\pi y}{3\sqrt{3}}$ et son conjugué complexe. Donc on obtient la formule requise. □

Le jacobien de Φ est donné par

$$J(x, y) = \frac{1}{3}2^{\frac{2(x+2)}{3}} \begin{pmatrix} \log(2)\cos\left(\frac{2\pi y}{3\sqrt{3}}\right) & -\frac{\pi}{\sqrt{3}}\sin\left(\frac{2\pi y}{3\sqrt{3}}\right) \\ \log(2)\sin\left(\frac{2\pi y}{3\sqrt{3}}\right) & \frac{\pi}{\sqrt{3}}\cos\left(\frac{2\pi y}{3\sqrt{3}}\right) \end{pmatrix}$$

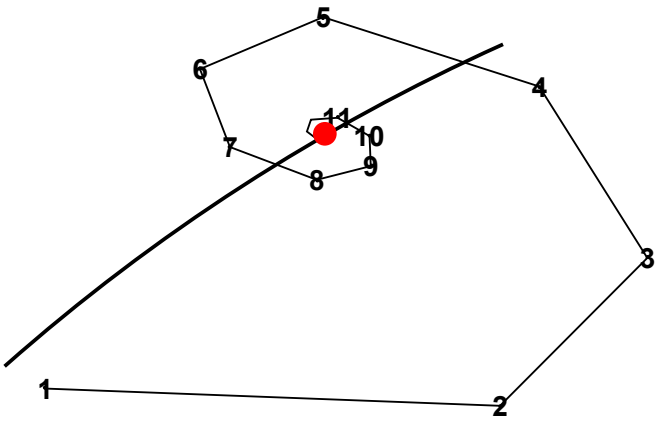
Quand on l'évalue sur le premier point fixe $P = (-1/2, \sqrt{3}/2)$, on obtient

$$(J(P)^* J(P))^{\frac{1}{2}} = \frac{1}{3}\begin{pmatrix} \log(2) & 0 \\ 0 & \frac{\pi}{\sqrt{3}} \end{pmatrix}$$

et on a la décomposition polaire

$$J(P) = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} . (J(P)^* J(P))^{\frac{1}{2}}$$

Il découle de cela, puisqu'à la fois les valeurs propres de $(J(P)^* J(P))^{\frac{1}{2}}$ sont < 1 que P est un point fixe attracteur.



En fait, le jacobien de la transformation Ψ au point fixe $1 \in \mathbb{C}$, est

$$\begin{pmatrix} \frac{4\log(2)}{3} & 0 \\ 0 & \frac{4\pi}{3\sqrt{3}} \end{pmatrix}$$

On a $\frac{4\log(2)}{3} < 1$, $\frac{4\pi}{3\sqrt{3}} > 1$ et cela montre que dès qu'on dévie dans le domaine complexe, par une légère perturbation, de la représentation triviale, on finit par atterrir dans le domaine d'attraction de l'un des deux caractères non triviaux. Par conséquent, on a le

Fait 6.3. *Les itérations $\Psi^{\circ n}(1 \pm i\epsilon)$ d'une petite perturbation complexe de la représentation triviale des classes 3A,3B, comme ci-dessus convergent, lorsque $n \to \infty$ vers un caractère non trivial de G.*

7 Tous les points fixes ne donnent pas des caractères

Ce très joli comportement de l'itération sur l'application Ψ n'est cependant pas vrai en général et il suffira de le démontrer en regardant son comportement sur les deux autres classes de conjugaison $7A$ et $7B$. Dans ce cas comme nous le verrons ci-dessous, on obtient après une itération la même valeur pour $u(2)$ et $u(3)$ qui est donnée, avec $u(1) = 1$, par

$$v(2) = v(3) = 2^{\frac{1}{7}+\frac{3}{7}(u(2)+u(3))} - 1$$

Par conséquent, dans ce cas, la transformation $\Psi = \wedge - 1$ prend la forme :

$$\Psi(z) = 2^{\frac{1}{7}+\frac{6}{7}z} - 1$$

L'équation du point fixe $\Psi(z) = z$ est équivalente à $we^w = -\frac{6}{7}2^{-\frac{5}{7}}\log 2$ où on laisse $w = -\frac{6}{7}(1+z)\log 2$. La valeur numérique $u = -\frac{6}{7}2^{-\frac{5}{7}}\log 2 \sim -0.362124$ est légèrement plus grande que $-1/e \sim -0.367879$ et par conséquent, on tombe dans le domaine dans lequel il existe deux solutions pour l'équation de Lambert $we^w = u$ (voir [8, 5]). Ce sont $W(u)$ et $W_{-1}(u)$ comme on le montre dans la figure 4.

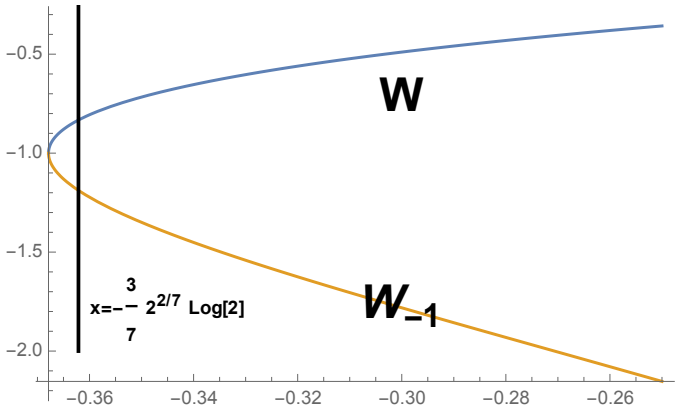


FIGURE 4 : Les deux branches de la fonction de Lambert dans l'intervalle $[-1/e, 0)$.

La solution évidente $z = 1$ correspond à $W_{-1}(u)$ mais la branche principale de la fonction de Lambert $W(u)$ donne une autre solution réelle non triviale $z \sim 0.401664$. Cette solution ne correspond pas de manière évidente à un caractère et de plus, elle ne peut avoir lieu sur la base de sa nature comme un point fixe de Ψ parce qu'elle s'avère être un attracteur. De plus, le problème qui survient est que le point fixe naturel 1 n'est pas un attracteur. En fait, la dérivée de $\Psi(z)$ en $z = 1$ est $\frac{12\log(2)}{7}$ qui est > 1. Par conséquent, 1 est un point fixe répulsif alors qu'en fait, l'autre $z = -\frac{7W\left(\frac{1}{7}(-3)2^{2/7}\log(2)\right)}{6\log(2)} - 1$ qui est ~ 0.401664 est un attracteur. Ce point fixe donne une solution de l'équation $\wedge f = 1 + f$ qui, bien qu'elle soit réelle (*i.e.* on a $f(g^{-1}) = \overline{f(g)}$ pour tout $g \in G$), et a pour dimension 1 (*i.e.* $f(1) = 1$) ne correspond pas à une représentation effective de dimension 1.

Notons également que l'équation de Lambert $we^w = u$ admet un nombre infini de solutions complexes données par les différentes branches complexes W_k, $k \notin \{-1, 0\}$, de la fonction de Lambert (voir [5]).

8 Conclusion

De l'analyse ci-dessus, on conclut qu'indubitablement, il vaut la peine d'investiguer en grand détail les points fixes de l'application $\Psi := \wedge - 1$ sur l'anneau de représentation complexifié des groupes finis d'ordre impair. En particulier, le lien avec les formes généralisées de l'équation de Lambert devrait être exploré. Mais il n'est toujours pas clair du tout de savoir si cette approche devrait mener à la construction d'un caractère non trivial uni-dimensionnel. Une raison d'être sceptique est que seule la loi de puissance des classes de conjgaison est utilisée pour dériver la formule pour Ψ, alors que la compatibilité avec la loi de puissance ne suffit pas à sélectionner des caractères parmi les fonctions de classe unitaire comme on le voit dans l'exemple le plus simple du groupe abélien impair $C(3) \times C(3)$.

Références bibliographiques

[1] M. F. Atiyah, *Characters and cohomology of finite groups*. Inst. Hautes Études Sci. Publ. Math. No. 9 1961 23–64.

[2] M. F. Atiyah, G. Segal, *Equivariant K-theory and completion*. J. Differential Geometry 3 1969 1–18.

[3] M. F. Atiyah, *Groups of odd order*. Notes non publiées.

[4] E. J. Barbeau, P. J. Leah, *Euler's 1760 paper on divergent series*. Historia Math. 3 (1976), no. 2, 141–160.

[5] R. Corless, G. Gonnet, D. Hare, J. Jeffrey, D. Knuth, *On the Lambert W function*. Adv. Comput. Math. 5 (1996), no. 4, 329–359.

[6] L. Euler, *De seriebus divergentibus*, Novi commentarii academiae scientiarum Petropolitanae 5 (1754/55), 205–237 (= Opera Omnia (1) 14, 585–617).

[7] L. Euler, *De formulis exponentialibus replicatis*, Leonhardi Euleri Opera Omnia, Ser. 1, Opera Mathematica 15 (1927) 268-297 (original date 1777).

[8] L. Euler, *De serie Lambertina plurimisque eius insignibus proprietatibus*, Leonhardi Euleri Opera Omnia, Ser. 1, Opera Mathematica, 6, (1921) 350–369 (original date 1779).

Produit eulérien pour enfants, ou mais pourquoi prennent-ils l'inverse de l'inverse de l'inverse..., Denise Vella-Chemla, 31 décembre 2024

On veut calculer

$$(1-2)(1-3)(1-4)(1-5)$$

On calcule les facteurs un par un, ça donne

$$(-1).(-2).(-3).(-4) = 24$$

Ou bien, on développe le produit du premier par le deuxième, et le produit du troisième par le quatrième, et on voit si on retombe sur ses pattes.

$$(1-2-3+6)(1-4-5+20) = 2 \times 12 = 24$$

Ou bien, on développe la totalité du produit, on est patient, le 1 apparaître une fois, en positif, les nombres 2, 3, 4 et 5 une fois, en négatif, etc. On obtient (on voit bien par ligne que le nombre de facteurs correspond au coefficient binomial (1,4,6,4,1 ici) car il s'agit de choisir tant de nombres parmi tant d'autres pour construire les produits)

$$\begin{array}{llllll} +1 & & & & & \\ -2 & -3 & -4 & -5 & & \\ +2\times 3 & +2\times 4 & +2\times 5 & +3\times 4 & +3\times 5 & +4\times 5 \\ -2\times 3\times 4 & -2\times 3\times 5 & -2\times 4\times 5 & -3\times 4\times 5 & & \\ +2\times 3\times 4\times 5 & & & & & \end{array}$$

Ce qui donne

$$+1-14+71-154+120 = -168+192 = 24.$$

Ouf !

La phrase latine qui intéresse beaucoup les mathématiciens car elle définit la fonction zeta dite "de Riemann" (dont on dit que sa compréhension est "le graal des mathématiciens") est celle qui montre l'égalité entre une somme infinie calculée sur les entiers par un produit infini calculé sur les nombres premiers, la voici :

> "*Si ex serie numerorum primorum sequens formetur expressio* $\prod_p \frac{p^s}{p^s-1}$ *erit eius valor aequalis summae huius seriei* $\sum_{n=1}^{\infty} \frac{1}{n^s}$."

La petite fonction qui envoie les parties imaginaires des zéros non triviaux de ζ vers des nombres "presque" successifs

Denise Vella-Chemla

26 décembre 2024

On teste par le programme suivant, pour les 2 millions de premiers zéros non triviaux de la fonction ζ de Riemann, que les parties imaginaires de ces zéros sont bien envoyées par la fonction de comptage vers les nombres "presque" successifs, i.e. des nombres réels séparés chacun du suivant par un écart compris entre 0 et 1 [1].

La fonction de comptage a, à une constante près, pour définition :

$$f(T) = \frac{T}{2\pi}\left(\ln\left(\frac{T}{2\pi\, e}\right)\right)$$

```
import math
from math import pi,log,e

with open("zeros2millions", 'r') as f:
     lines = f.readlines()
     zeros = [float(line) for line in lines]

for n in range(len(zeros)-1):
     print(n,' ',zeros[n],' ',(zeros[n+1]/(2*pi))*log(zeros[n+1]/(2*pi*e)))
```

Ci-dessous le résultat de ce programme jusqu'à 100 [2] .

n	$\mathfrak{Im}(\zeta_n)$	$f(\mathfrak{Im}(\zeta_{n+1}))$	n	$\mathfrak{Im}(\zeta_n)$	$f(\mathfrak{Im}(\zeta_{n+1}))$
0	14.134725142	0.694895689662535	10	52.970321478	10.7392197558459
1	21.022039639	1.51833268588623	11	56.446247697	11.7644535438555
2	25.01085758	2.79584647536906	12	59.347044003	12.2980090797995
3	30.424876126	3.44206964858738	13	60.831778525	13.8681602815966
4	32.935061588	4.71837876181937	14	65.112544048	14.6049466761078
5	37.586178159	5.6899670378981	15	67.079810529	15.5416859568015
6	40.918719012	6.4192280671934	16	69.546401711	16.5133799857929
7	43.327073281	7.89568039084821	17	72.067157674	17.9401819521021
8	48.005150881	8.47320303179638	18	75.704690699	18.5128358719339
9	49.773832478	9.54208818578511	19	77.144840069	19.3928547789907

[1] En fait, l'écart entre les images de deux parties imaginaires de deux zéros successifs (rangés dans l'ordre croissant des parties imaginaires) a été au maximum égal à 3.3 environ pour les 2 millions de premiers zéros, et non pas à 1, mais dans tous les cas, l'écart reste toujours très très petit par rapport au nombre considéré.

[2] et à cet adresse

https://denisevellachemla.eu/entre0et1.txt ,

l'exécution avec les zéros non triviaux de ζ de partie imaginaire inférieure à 2 millions fournis par Odlyzsko.

n	$\mathfrak{Im}(\zeta_n)$	$f(\mathfrak{Im}(\zeta_{n+1}))$	n	$\mathfrak{Im}(\zeta_n)$	$f(\mathfrak{Im}(\zeta_{n+1}))$
20	79.33737502	20.8475020524276	61	167.184439978	61.6984559369902
21	82.910380854	21.600069144213	62	169.094515416	62.1271444444692
22	84.735492981	22.7205417605702	63	169.911976479	63.9694035692432
23	87.425274613	23.3021589295633	64	173.41153652	64.6792079573964
24	88.809111208	24.8665888629723	65	174.754191523	65.5735076120176
25	92.491899271	25.7948264335012	66	176.441434298	66.6028057110773
26	94.651344041	26.322413725083	67	178.377407776	67.4234734608378
27	95.870634228	27.6136597251497	68	179.91648402	68.6487411487072
28	98.831194218	28.7091385850354	69	182.207078484	70.0813332073192
29	101.317851006	29.7790866652396	70	184.874467848	70.4714073780431
30	103.72553804	30.5493808703319	71	185.598783678	71.350947873569
31	105.446623052	31.3245538549383	72	187.228922584	72.5346151339257
32	107.168611184	33.078495631911	73	189.416158656	73.9525970335719
33	111.029535543	33.4652954705481	74	192.026656361	74.5262116161171
34	111.874659177	34.5902881052207	75	193.079726604	75.719672958394
35	114.320220915	35.4730710131554	76	195.26539668	76.6018838013679
36	116.226680321	36.6682086217569	77	196.876481841	77.2267590641179
37	118.790782866	37.879337085695	78	198.015309676	79.0154396127439
38	121.370125002	38.623986107933	79	201.264751944	79.6940486909973
39	122.946829294	39.2451198593009	80	202.493594514	80.6326289177557
40	124.256818554	40.8002822690803	81	204.189671803	81.3008329480505
41	127.51668388	41.790866980748	82	205.394697202	82.6971391696362
42	129.5787042	42.5190899316302	83	207.906258888	83.6283945340186
43	131.087688531	43.6878796199309	84	209.576509717	84.8102971609292
44	133.497737203	44.3011014007152	85	211.690862595	85.7389266964766
45	134.756509753	45.9468415556906	86	213.34791936	86.4122057823626
46	138.116042055	46.7451839583626	87	214.547044783	87.3248925751132
47	139.736208952	47.4312561383973	88	216.169538508	88.9599243352489
48	141.123707404	48.4181040360562	89	219.067596349	89.8920390429968
49	143.111845808	49.8599978194783	90	220.714918839	90.2976677989138
50	146.000982487	50.5729251200248	91	221.430705555	91.7606662793508
51	147.422765343	51.8978090115362	92	224.007000255	92.3163259969592
52	150.053520421	52.3384532843791	93	224.98332467	93.7068816956505
53	150.925257612	53.4029529442674	94	227.42144428	94.8025556889906
54	153.024693811	54.97711765745	95	229.337413306	95.8989445808808
55	156.112909294	55.7373818516436	96	231.2501887	96.3220875071878
56	157.597591818	56.3804305894168	97	231.987235253	97.3030374373686
57	158.849988171	57.5855873368141	98	233.693404179	98.9349673409935
58	161.188964138	58.538351594387	99	236.524229666	99.6547445742907
59	163.030709687	59.8402435745758	100	237.769820481	100.688414763251
60	165.537069188	60.699241612539			

Référence

[1] Alain Connes, Henri Moscovici, *The UV prolate spectrum matches the zeros of zeta*, PNAS, Vol. 119, n° 22, 24 mai 2022. https://doi.org/10.1073/pnas.2123174119, et article en ligne https://www.pnas.org/doi/epub/10.1073/pnas.2123174119.

Pour se faire une autre idée, on note ci-dessous une petite fonction qui trouve "presque" les valeurs des parties imaginaires des zéros non triviaux de ζ en prenant "certains" multiples de $\frac{\pi}{4}$.

```
from math import pi

with open('zeros30', 'r') as f:
     lines = f.readlines()
     zeros = [float(line) for line in lines]

combien = [18,28,32,39,42,48,52,56,62,63,67,72,76,77,83,86,89,92,96,99,101,105,108,
           112,113,118,120,122,125]
for k in range(29):
     print(':2.9f :3d :2.9f'.format(zeros[k],combien[k],combien[k]*pi/4))
```

k	$\zeta[k]$	k'	$k'\frac{\pi}{4}$
1	14.134725142	18	14.137166941
2	21.022039639	28	21.991148575
3	25.010857580	32	25.132741229
4	30.424876126	39	30.630528373
5	32.935061588	42	32.986722863
6	37.586178159	48	37.699111843
7	40.918719012	52	40.840704497
8	43.327073281	56	43.982297150
9	48.005150881	62	48.694686131
10	49.773832478	63	49.480084294
11	52.970321478	67	52.621676948
12	56.446247697	72	56.548667765
13	59.347044003	76	59.690260418
14	60.831778525	77	60.475658582
15	65.112544048	83	65.188047562
16	67.079810529	86	67.544242052
17	69.546401711	89	69.900436542
18	72.067157674	92	72.256631033
19	75.704690699	96	75.398223686
20	77.144840069	99	77.754418176
21	79.337375020	101	79.325214503
22	82.910380854	105	82.466807157
23	84.735492981	108	84.823001647
24	87.425274613	112	87.964594301
25	88.809111208	113	88.749992464
26	92.491899271	118	92.676983281
27	94.651344041	120	94.247779608
28	95.870634228	122	95.818575934
29	98.831194218	125	98.174770425

Opérateur d'onde prolate infrarouge et ultraviolet pour zeta

Alain Connes

Merci beaucoup pour votre invitation et pour cette occasion de participer à cette grande conférence, qui est un hommage à Krzysztof Gawedzki qui était un merveilleux mathématicien et physicien.

Et ce que je souhaite expliquer, c'est un lien surprenant entre la physique, quand je parle de physique, je veux dire que je vais parler du sphéroïde prolate qui est un ellipsoïde mais vous pouvez le considérer comme un volume en dimension trois, je veux dire qu'il est plein, entre ce volume donc, et la fonction zeta de Riemann. Et quand vous regardez les zéros de la fonction zeta de Riemann, quand vous en dessinez le graphe, ce que vous trouvez bien sûr, c'est une très forte similarité avec ce que serait, si vous voulez, le spectre d'un opérateur de Dirac. Et quand vous pensez aux zéros de façon spectrale, vous trouvez qu'il y a deux régimes qui doivent être compris, si vous voulez : il y a le régime ultraviolet, dans lequel la fonction de comptage des zéros de la fonction zeta de Riemann est une fonction très étrange : elle est donnée par une formule que l'on doit à Riemann et qui est cette formule dans laquelle vous avez, si vous voulez, un terme de la forme E sur 2 pi fois log de E sur 2 pi moins E sur 2 pi et alors, il y a un écart logarithmique qui advient. Donc, ça, c'est pour la partie ultraviolette. Et pour la partie infrarouge, ce que vous obtenez est vraiment surprenant parce que le premier zéro est aux alentours de 14 et quelques, et alors, ok, les zéros se comportent d'une manière très précise que l'on doit comprendre. Et ce qu'on va voir, c'est qu'à la fois dans l'ultraviolet et dans l'infrarouge, le sphéroïde prolate va jouer un rôle crucial.

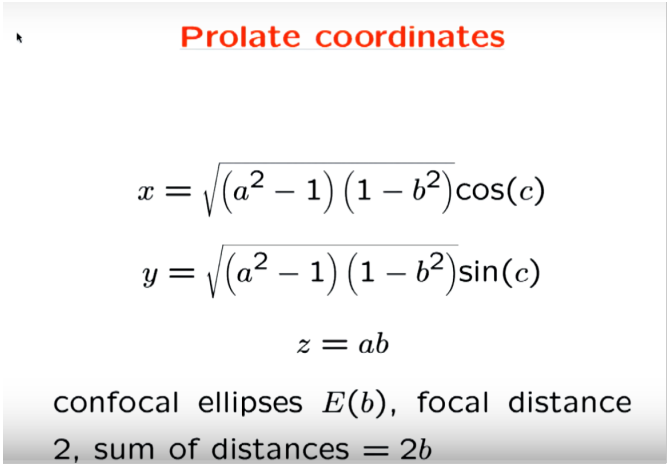


FIGURE 1

Donc je vais parler de deux papiers, écrits en collaboration, très récents, l'un qui a été publié dans les Proceedings de l'Académie des sciences, avec Henri Moscovici, sur le spectre prolate ultraviolet, et le second, en collaboration avec Katia Consani, et qui considère cette fois le comportement infrarouge.

Ok, donc on verra des résultats assez précis, mais d'une manière ou d'une autre, commençons par la physique. Commençons à partir du sphéroïde prolate. Donc si vous voulez, le sphéroïde prolate

Transcription de la vidéo derrière ce lien https://www.youtube-nocookie.com/embed/Yfu9$_f M - jzQ$, Denise Vella-Chemla, janvier 2025.

est compris au moyen d'un système spécifique de coordonnées qu'on appelle les coordonnées prolate et quand vous les regardez, ces coordonnées ont l'air un peu étranges. Je veux dire que ce sont ces coordonnées a, b, c (voir Fig. 1). c est une coordonnée évidente à cause de, si vous voulez, l'invariance de rotation du sphéroïde. Mais les autres, je veux dire le terme que l'on voit devant le cosinus et le sinus pour x et y semble très étrange. Si vous y pensez un peu, ce que vous trouverez c'est qu'en fait, il décrit une famille d'ellipses confocales donc ça ressemble à ça ; vraiment ce que vous avez est là : vous avez deux points focaux ; vous en avez un qui est le point (0,0,1) et l'autre qui est le point (0,0,-1) ; ils sont donc tous les deux sur l'axe des z si vous voulez, et le paramètre b qui apparaît dans les coordonnées est en fait là pour vérifier que $2b$ est la somme de la distance entre les points focaux. Vous savez qu'une ellipse est définie par le fait que la somme des distances aux deux points focaux est constante et que cette constante est $2b$. Donc c'est le rôle du paramètre b et le paramètre a est juste un paramètre angulaire. Donc ce qui se passe alors, c'est la chose suivante : ce qui se passe, c'est que quand vous calculez le Laplacien en ces coordonnées, le Laplacien ordinaire ok, vous trouvez une expression qui alors vous permettra de gérer l'équation de Helmholtz pour le sphéroïde en dimension 3, le sphéroïde prolate (on l'appelle prolate parce qu'il est allongé dans la direction de l'axe de symétrie).

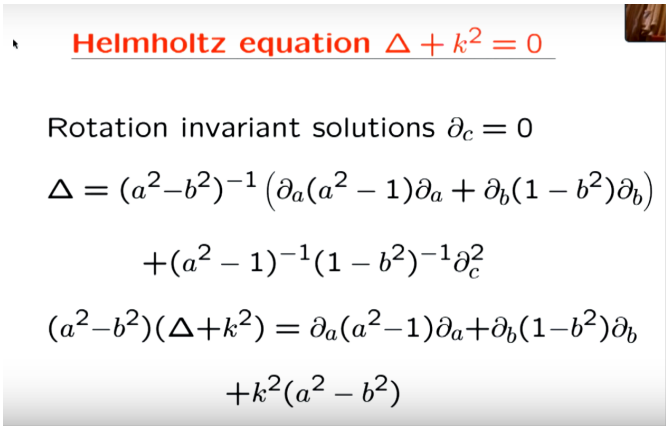


FIGURE 2

Ok, donc je veux dire que quand vous regardez le Laplacien, il a cette forme, ok, et si vous regardez les solutions invariantes par rotation, les choses se simplifient un peu parce que vous avez la différentielle par rapport à la variable c, la variable angulaire c, qui est nulle, et alors, ce que vous obtenez quand vous écrivez l'équation de Helmholtz, vous trouvez qu'il y a ce qu'on appelle une séparation de variables ; notamment, l'équation se sépare si vous voulez en une somme de deux termes, un dans lequel n'intervient que la variable a, et l'autre dans lequel n'intervient que la variable b. Et quand vous regardez cela d'un petit peu plus près, ce que vous trouvez c'est qu'en fait, pour résoudre l'équation de Helmholtz, qu'est-ce que vous devez faire ? Vous devez résoudre à la fois l'équation angulaire et l'équation radiale. Donc comme équations, comme équations différentielles, elles sont identiques, mais les variables que vous utilisez sont les variables a et b et la variable a est comprise entre -1 et 1. C'est si vous voulez la partie angulaire. Et la variable b est plus grande que 1, elle va jusqu'à l'infini, et c'est la partie radiale. Maintenant, à quoi ressemblent les solutions, elles sont produit de deux fonctions, une fonction qui ne dépend que de a et une fonction qui ne dépend que de b, par exemple $\phi(a)$ et $\psi(b)$, mais elles doivent être, si vous voulez, vecteurs propres pour la même valeur propre pour l'équation différentielle. Et c'est parce qu'elles le sont pour la

même valeur propre, si vous voulez, que les termes vont s'annuler et qu'elles vous donneront une solution de l'équation de Helmholtz.

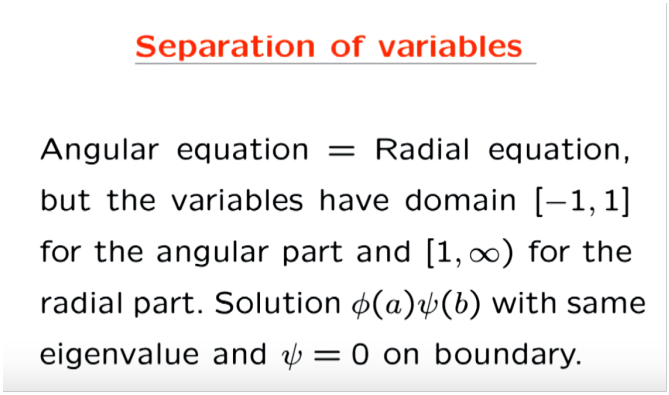


FIGURE 3

De plus, bien sûr, puisque vous voulez avoir une condition de Dirichlet au bord, vous devez avoir que $\psi(b) = 0$.

Donc ce qui se passe, en fait, peut être énoncé comme ça, si vous voulez : c'est qu'il y a un opérateur, un opérateur différentiel du second ordre, qui provient de ce Laplacien et qui a la forme suivante modulo une mise à l'échelle facile qui est un changement de variables ; cet opérateur, on l'appellera W_λ car il dépend du paramètre λ ; λ est relié à k par une équation très simple : $k = 2\pi\lambda^2$, et l'opérateur W_λ ressemble à ça : c'est une différentiation fois lambda au carré moins x au carré fois une différentiation plus un terme additionnel qui est $(2\pi\lambda x)^2$, ok.

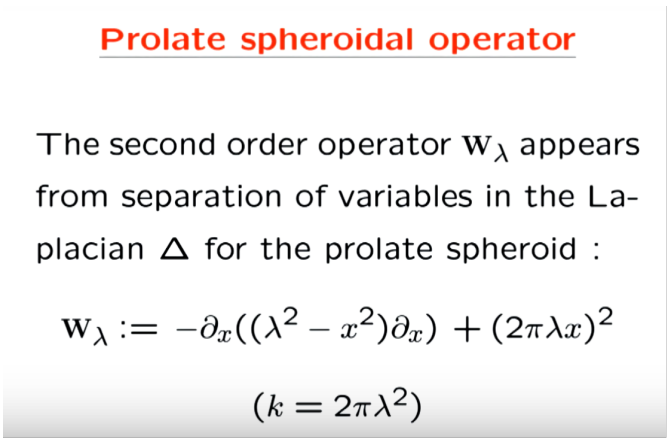


FIGURE 4

Maintenant, cet opérateur a été utilisé d'une manière assez remarquable par Slepian et ses collaborators, qui travaillaient aux laboratoires Bell et je reviendrai ultérieurement à leur motivation, quand je traiterai le problème de l'infrarouge. Mais en quelque sorte, leur découverte principale, qui est décrite dans plusieurs articles, est la suivante : c'est qu'en fait, cet opérateur différentiel commute avec ce qu'on appelle la transformation de Fourier tronquée. Et pour comprendre cela, je veux dire c'est un peu surprenant parce que ce que vous devez comprendre en quelque sorte,

c'est que ces opérateurs différentiels, le premier que j'ai montré précédemment, le W_λ, en fait, commute avec un opérateur de projection. Donc cela semble très étrange parce que vous connaissez l'opérateur de projection sur l'intervalle $[-\lambda, \lambda]$, c'est une fonction qui est discontinue, je veux dire qu'elle prend la valeur 1 entre $-\lambda$ et λ et elle prend la valeur 0 partout ailleurs, donc je veux dire qu'au premier abord, il semble très étrange que l'opérateur différentiel puisse commuter avec une telle fonction, mais si vous y pensez un peu plus avant, vous trouverez qu'en fait, ça n'est pas si surprenant parce que le cas le plus simple à considérer serait seulement celui de l'opérateur $x\partial_x$ et il suffit de comprendre qu'il commute avec la projection sur des fonctions qui ont leur support sur les entiers positifs.

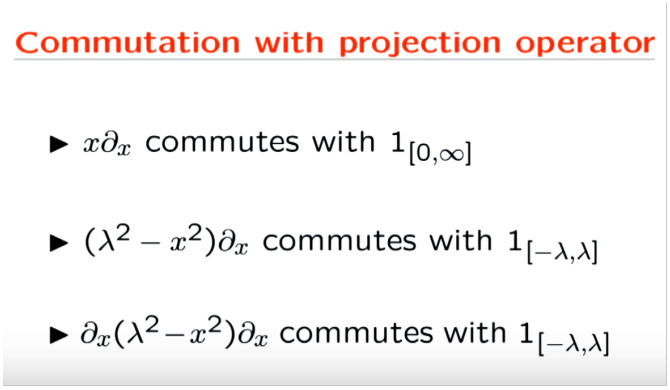


FIGURE 5

Maintenant, pourquoi est-ce que cela est évident ?

C'est évident, si vous voulez, parce que l'opérateur $x\partial_x$ engendre le semi-groupe du groupe des opérateurs de mise à l'échelle, le groupe qui remplace une fonction f de x par $f(\lambda x)$ et donc, je veux dire, de façon évidente vous savez, pour λ positif, bien sûr. Donc évidemment qu'il préserve les fonctions qui ont leur support dans $[0, \infty)$ et il commute avec cette projection.

Donc en fait, ce qui se passe, c'est que le premier morceau de l'opérateur qui est $\partial_x((\lambda^2 - x^2)\partial_x)$ commute avec $(2\pi\lambda x)^2$ (il commute bien sûr avec la multiplication par une fonction). Donc ce qui se passe, c'est que non seulement cet opérateur commute avec P_λ mais en fait, un calcul direct vous montre qu'il commute avec la transformation de Fourier, ça n'est pas difficile à voir je veux dire, il y a une partie de l'opérateur qui est l'oscillateur harmonique, qui commute avec la transformation de Fourier. Donc il commute avec la transformation de Fourier, et parce qu'il commute avec la transformation de Fourier *et* avec la projection P_λ, il commute également avec la transformée de Fourier de P_λ. Notamment, si vous voulez, il commute avec l'opérateur $\widehat{P_\lambda}$, qui est obtenu en conjuguant P_λ par la transformation de Fourier. Donc, c'est ce que Slepian et ses collaborateurs ont découvert, et je veux dire que dans les années 90, quand j'ai commencé à m'intéresser aux zéros de zeta, ce que j'ai trouvé, j'avais utilisé cette projection P_λ et $\widehat{P_\lambda}$ pour faire un cutoff. Et en fait, dans mon cours en 98, j'avais traité le problème de la façon d'utiliser cet opérateur W_λ, qui est normalement seulement traité dans l'intervalle $[-\lambda, \lambda]$, dans lequel il est auto-adjoint, comme on peut le voir facilement, la manière d'utiliser cet opérateur, donc, sur la droite des réels complète.

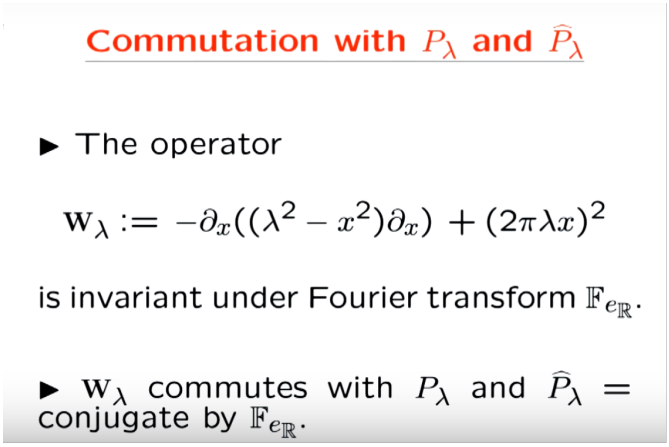


FIGURE 6

Et quand on l'utilise sur la totalité de la droite réelle, donc ce que j'avais trouvé à cette époque, je veux dire en 98, c'était que si vous prenez pour domaine minimal de cet opérateur l'espace de Schwartz des fonctions de Schwartz qui ont une décroissance rapide, elles et leurs dérivées, alors vous trouvez que l'opérateur est symétrique, bien sûr, mais il n'est pas auto-adjoint, et en fait, il a des indices de déficiences au sens de von Neumann, qui sont tous les deux égaux à 4. Et il a en fait une unique extension auto-adjointe W_λ qui doit respecter la contrainte de commuter avec la projection P_λ et avec $\widehat{P_\lambda}$. C'est là que je me suis arrêté en 98, et c'est de là que nous sommes repartis, il y a 2 ans avec Henri Moscovici, et que nous avons commencé notre collaboration. Et nous avons fait quelque chose que je n'avais pas osé faire en 98, principalement nous avons vraiment regardé précisément l'opérateur W_λ spectralement.

Et ce que je vous expliquerai maintenant c'est que si vous voulez, quand vous regardez cet opérateur W_λ spectralement, qu'est-ce que vous trouvez ? Bon, bien sûr, vous trouvez qu'il commute avec Fourier mais il est en quelque sorte presque construit ainsi de manière ad hoc, mais à notre grande surprise avec Henri, ce qu'on a trouvé, c'est que l'opérateur auto-adjoint W_λ, sur la droite réelle complète maintenant, pas seulement dans l'intervalle $[-\lambda, \lambda]$, a un spectre discret.

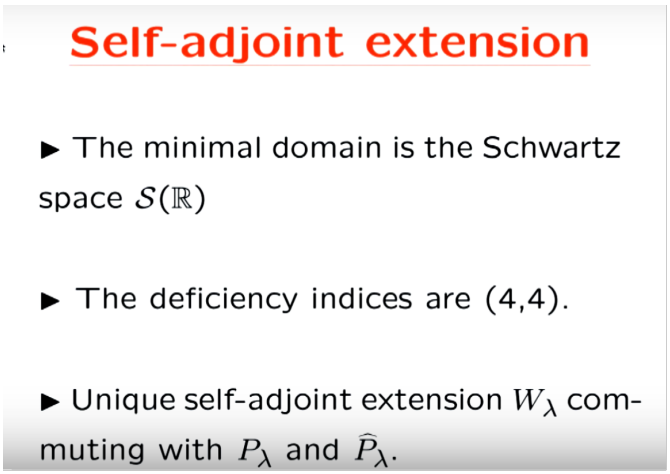


FIGURE 7

Et ce que j'expliquerai ultérieurement, c'est que ce spectre discret s'adaptera parfaitement au comportement ultraviolet des zéros de zeta. Et ce qui se passe, c'est qu'apparemment, personne n'a

regardé ce spectre parce que ce spectre s'avère avoir à la fois une partie positive et une partie négative. Et la raison pour laquelle les gens ne se sont intéressés qu'à la partie positive du spectre, c'est qu'ils voulaient s'adapter à la séparation des variables et qu'ils voulaient correspondre au spectre qui correspond à l'intervalle et qui est positif par construction. Donc personne ne regardait la partie négative du spectre, et comme nous le verrons, je veux dire, très grossièrement, la partie positive du spectre correspondra aux zéros triviaux et la partie négative correspondra maintenant aux zéros non triviaux et au comportement ultraviolet des zéros, il ne donne pas les positions exactes des zéros mais il donne le comportement ultraviolet.

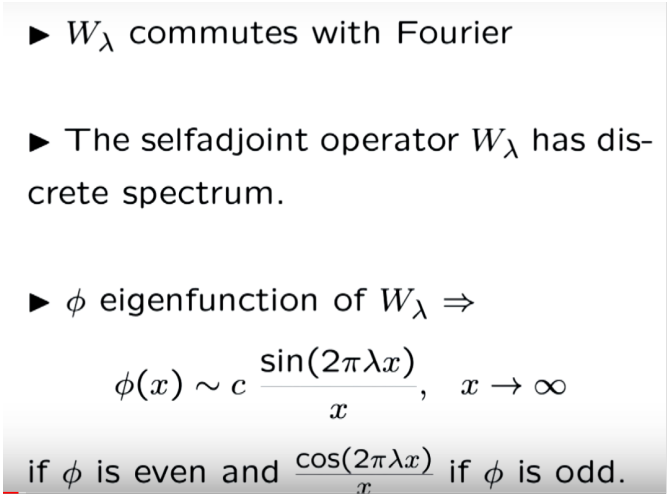


FIGURE 8

Donc, je veux dire, pour trouver l'extension auto-adjointe, on doit donner une condition aux bornes à l'infini, et la condition aux bornes à l'infini est en fait la contrainte, si vous voulez, que quand vous regardez la partie paire du spectre, donc la fonction paire, qui est celle à laquelle nous nous restreindrons, alors la fonction doit se comporter comme un sinus, elle doit avoir ce comportement oscillant d'avoir beaucoup de zéros bien sûr, lorsqu'on va vers l'infini et être équivalente à $\frac{\sin(2\pi\lambda x)}{x}$ lorsque x tend vers l'infini. Dans le cas impair, vous devez remplacer le sinus par un cosinus.

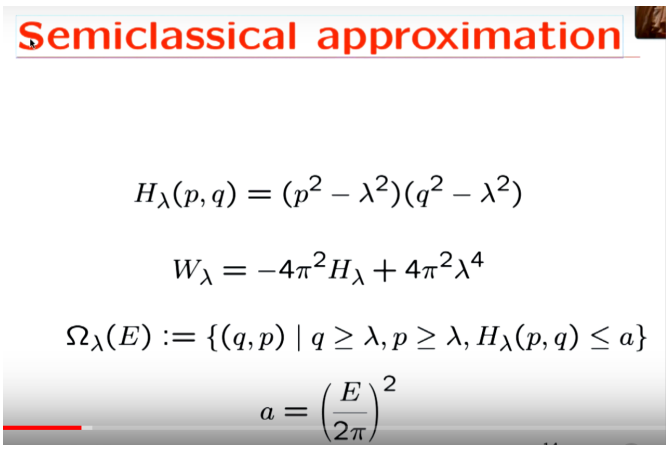


FIGURE 9

Ok. Donc si vous voulez comprendre le spectre de cet opérateur comme un physicien par exemple, il est très naturel de regarder l'approximation semi-classique, et d'exprimer l'opérateur W_λ en fonction d'un hamiltonien que vous écrivez classiquement parce que, ok, à ce stade, vous ne vous préoccupez pas de la non-commutativité de p et q ; donc ce que vous écrivez, c'est que W_λ est en fait exprimé par $-4\pi^2 H_\lambda$ où H_λ est écrit ci-dessus, c'est $(p^2-\lambda^2)(q^2-\lambda^2)+\text{Cte}$, le plus constante n'étant pas important. Et alors, quand vous voulez regarder le comportement du spectre, vous devez calculer l'aire d'une surface et en calculant cette aire, si vous voulez, l'aire qui est bornée par la valeur de H_λ, en calculant cette aire, en fait, vous pourrez estimer le nombre de valeurs propres de l'opérateur. Et quand vous faites ça, ok, vous trouvez cette image :

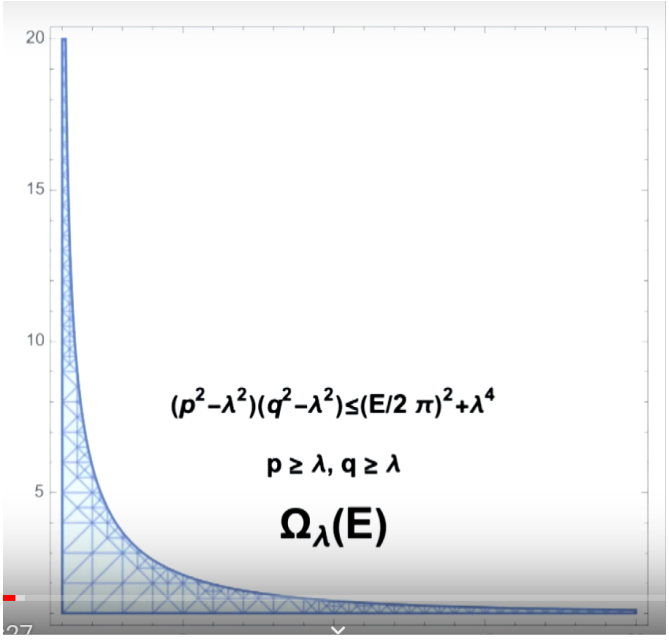


FIGURE 10

Donc vous trouvez une image dans laquelle, si vous voulez, la chose qui ressemble à une hyperbole est définie par la manière dont $(p^2-\lambda^2)(q^2-\lambda^2)$ égale $(E/(2\pi)^2+\lambda^4$, ok, et également, on a ces deux conditions que $p>\lambda$ et $q>\lambda$; c'est à cause de la positivité de l'opérateur. Ok, c'est donc ce que vous avez, et vous faites le calcul de l'aire, ok.

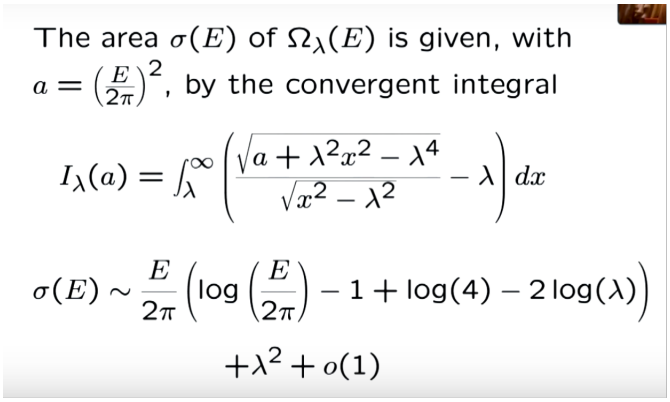


FIGURE 11

J'ai effectué ce calcul difficile donc on obtient une intégrale de λ à l'infini d'une certaine racine carrée et etc, et ce que vous trouvez, c'est que cette intégrale a son résultat qui est donné par des intégrales elliptiques, non pas par des fonctions elliptiques, mais par des intégrales elliptiques, au sens de Legendre. Et alors, quand vous les développez avec l'idée correcte que l'opérateur en question ne sera pas l'opérateur de Dirac mais qu'il sera plutôt comme le laplacien, donc vous travaillez avec le carré de l'opérateur de Dirac, et alors, vous trouvez de façon surprenante que la formule que vous obtenez pour le nombre des valeurs propres commence à sacrément ressembler à la formule de Riemann. C'est $\frac{E}{2\pi}\left(\log\frac{E}{2\pi}\right)$ moins un terme d'ordre 1, donc vous devez adapter le λ, de façon à ce que ça fasse -1, et ensuite, plus λ^2 plus un petit o(1).

Ok. D'un autre côté, on sait que lorsqu'on effectue une approximation semi-classique, on doit faire très attention au fait que cela nous permet de nous faire une première idée, mais qu'il nous faut travailler beaucoup plus pour vraiment obtenir une estimation, et on peut voir que, vous savez, cela ne pourrait pas être complètement correct de cette manière parce qu'on n'obtient pas le terme en $\mathrm{O}(\log E)$.

Donc en fait, on doit pousser l'analyse beaucoup plus loin,

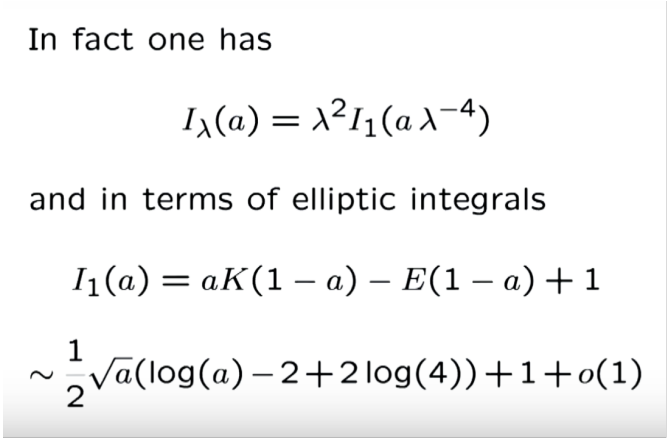


FIGURE 12

et ok, donc ça, c'est facile

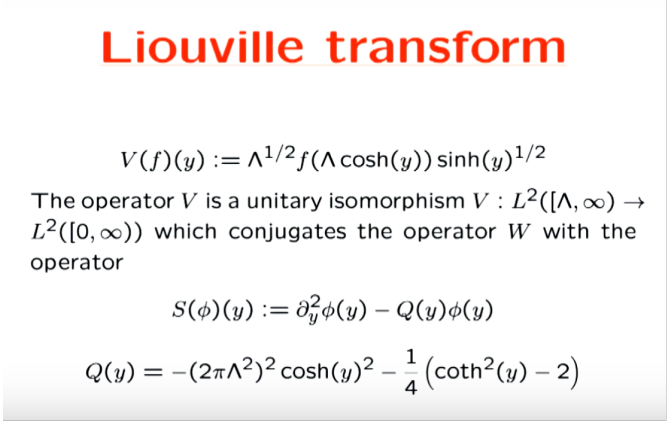


FIGURE 13

Donc ce qu'on doit faire, avant tout, on doit effectuer une transformation de Liouville pour transformer l'opérateur, cet opérateur prolate, en un opérateur de Sturm-Liouville usuel, si vous voulez, et ce faisant, on obtient un potentiel qui est très difficile à comprendre, parce qu'il n'est ni positif ni négatif. Vous obtenez cet étrange potentiel $Q(y)$ et alors

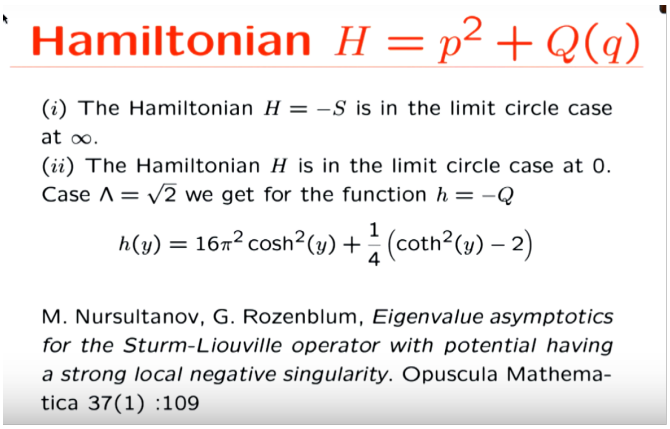


FIGURE 14

vous devez appliquer cet hamiltonien maintenant, qui est vous savez de force p^2 parce que vous le mettez sous cette forme, ok, et il a ce potentiel, et alors, on doit appliquer des estimées assez difficiles sur les valeurs propres asymptotiques à partir de l'opérateur de Sturm-Liouville. Bon, pour le potentiel qui avait, si vous voulez, une singularité.

Donc je veux dire, ces estimées existent, vous faites les calculs, et quand vous faites les calculs, ce que vous obtenez

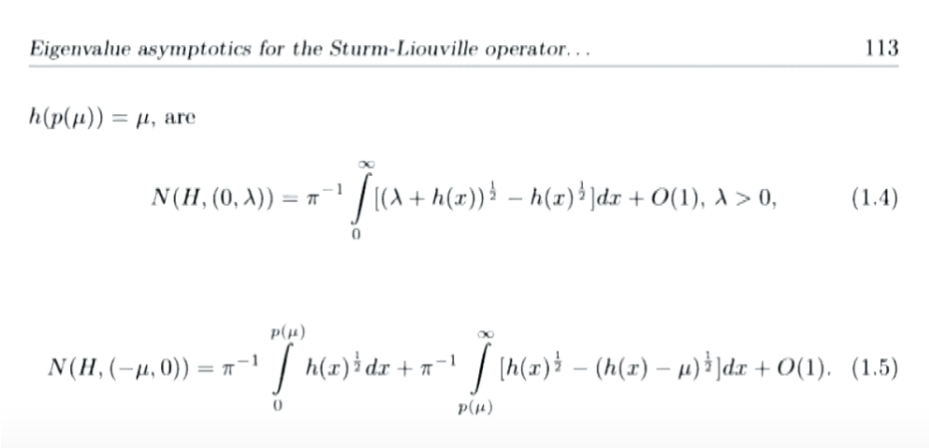


FIGURE 15

donc il y a des formules, si vous voulez, pour chaque variable, qui existent pour calculer ce nombre de valeurs propres, et quand vous effectuez ces calculs

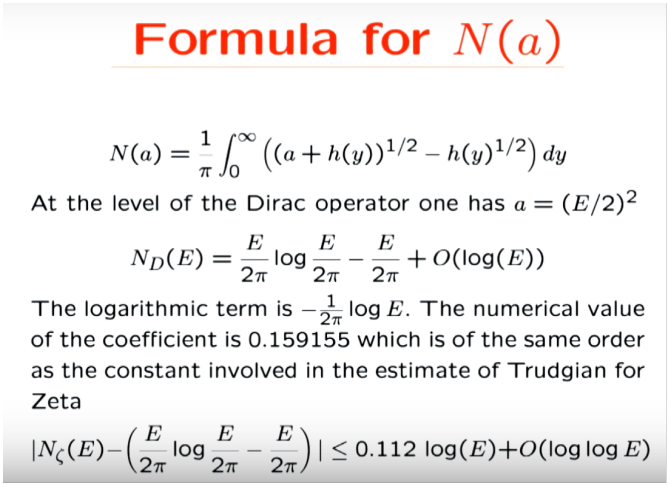


FIGURE 16

ce que vous trouvez maintenant, ce sont des intégrales beaucoup plus compliquées. Pourtant, le fait surprenant est que vous trouvez la formule correcte $\frac{E}{2\pi}\left(\log\frac{E}{2\pi}\right) - \frac{E}{2\pi}$ mais vous trouvez qu'il y a un terme additionnel en $O(\log E)$ comme vous vous y attendez. Et quand vous le calculez, vous trouvez que le terme relatif est en fait $\frac{-1}{2\pi}\log E$. Et quand vous regardez la valeur numérique de ce coefficient, vous trouvez qu'il est du même ordre que la constante qui est le 1 de la formule de Riemann pour la fonction zeta pour la différence entre la formule de Riemann et quelque chose en $o(1)$ [1].

Donc, il y a ce fait très alléchant et alors, bien sûr, vous savez, ce n'était pas parce que je prenais le laplacien

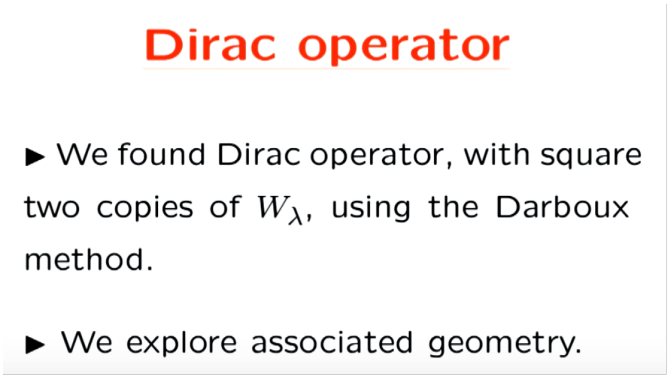


FIGURE 17

donc on devait trouver l'opérateur de Dirac, on devait trouver la sorte de racine carrée, si vous voulez, la sorte de racine carrée de l'opérateur de Dirac de cet opérateur sphéroïdal prolate. Et alors, on voulait explorer la géométrie associée.

Alors, comment avons-nous trouvé l'opérateur de Dirac de la racine carrée, si vous voulez, de cet opérateur sphéroïdal prolate. Bien, on l'a fait en utilisant la méthode de Darboux.

[1] à revoir ?

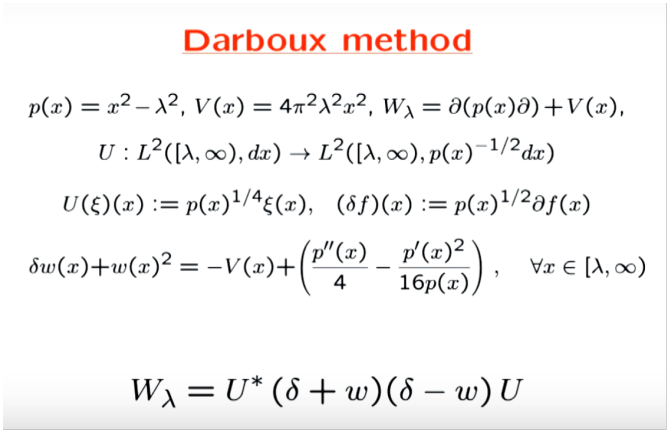


FIGURE 18

La méthode de Darboux est une méthode très générale qui est assez ancienne et qui permet lorsque vous avez un opérateur du second ordre de l'écrire non pas comme un carré, mais comme un produit de quelque chose de la forme de l'opérateur d'ordre un plus W et l'opérateur d'ordre un, le même opérateur d'ordre un moins W. Donc on peut faire ça, mais pour faire ça, il fallait qu'on résolve une équation de Ricatti. Donc on devait trouver une solution d'une équation non-linéaire qui est $\delta W + W^2$ égale une certaine fonction du potentiel, qui vous est donné depuis le début. Et on peut le faire dans notre cas, parce que ce qu'on doit faire, c'est trouver la solution de l'opérateur prolate qui ne s'évanouit pas.

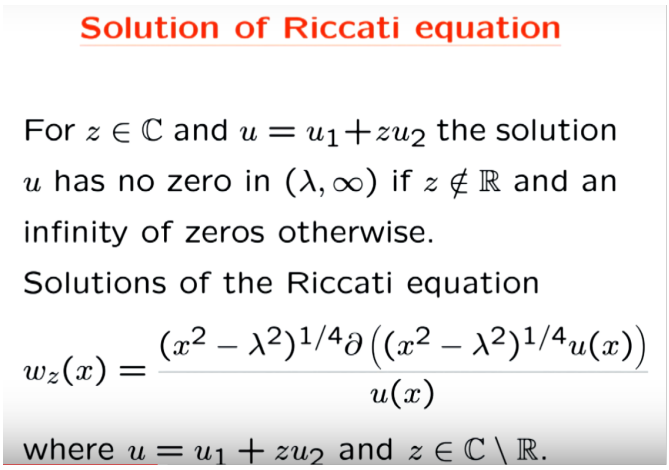


FIGURE 19

Maintenant, bien sûr, comme je vous l'ai montré, je veux dire, les solutions ordinaires s'évanouissent, mais quand vous combinez deux solutions indépendantes avec des coefficients complexes, alors vous trouvez qu'elles ne s'évanouissent nulle part.

Donc quand la combinaison ne s'évanouit nulle part, ce que vous pouvez faire consiste à résoudre l'équation de Ricatti par une sorte de dérivée logarithmique que j'ai notée comme ça $w_z(x)$ et pour chaque nombre complexe qui n'est pas dans les réels, vous trouvez une solution de l'équation de Ricatti et vous trouvez l'opérateur de Dirac correspondant.

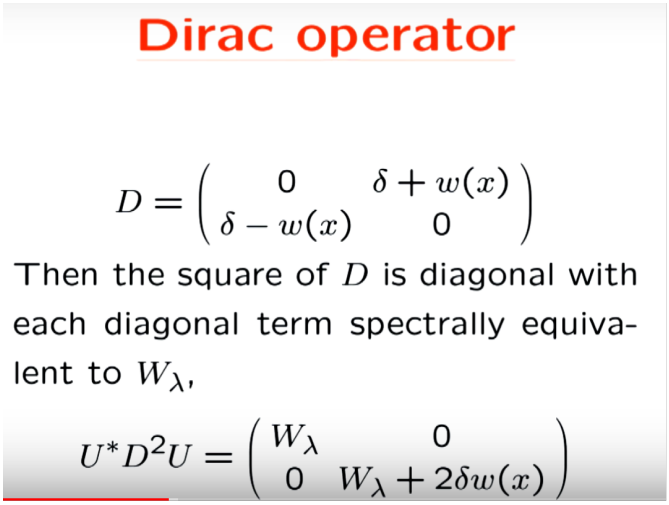


FIGURE 20

Et tous ces opérateurs de Dirac sont isospectraux, ce qui signifie que vous vous moquez duquel choisir pour considérer son spectre. Donc je veux dire, voici ce qu'on a trouvé, on a trouvé l'opérateur de Dirac, et quand on l'élève au carré, c'est bien sûr une matrice 2×2 parce qu'il agit un peu comme des spineurs, ok, donc c'est une matrice 2×2 et quand vous l'élevez au carré, vous trouvez deux copies de l'opérateur prolate, notamment en premier l'opérateur prolate lui-même et ensuite, quelque chose qui est isospectral à l'opérateur prolate, ok (dont il diffère par une paire d'opérateurs prolate).

Donc, c'est ce que nous avons trouvé, et alors, si vous voulez, par les précédents calculs, à cause, bien sûr, de cet opérateur de Dirac ayant son carré qui est deux copies de l'opérateur prolate, vous pouvez calculer son spectre, vous pouvez calculer le nombre de valeurs propres, et alors vous trouvez, pour celui-là, vous trouvez exactement l'estimation correcte pour le nombre de valeurs propres.

Et je vous montrerai très rapidement comment vous faites les calculs concrets et comment vous les comparez aux zéros de zeta.

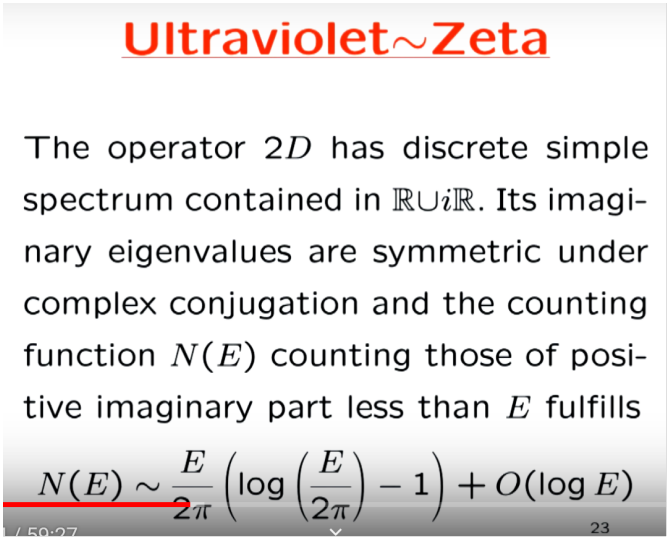


FIGURE 21

Mais comment on fait ça, ok ? On fait ça, si vous voulez, en calculant les valeurs négatives de l'opérateur prolate, et en calculant ces valeurs propres : ce que vous faites si vous voulez, vous développez la solution qui satisfait une condition aux bornes égale à λ, et vous développez la solution pour la valeur propre qui vaut -65 et vous développez la solution qui satisfait la condition aux bornes à l'infini. Et vous essayez de les faire coïncider, bien sûr ici, elles ne coïncident pas, mais vous faites varier la valeur -65, et vous continuez, ok, vous pouvez voir par exemple que sur -38, ça coïncide, excepté qu'il y a un changement de signe mais bien sûr, on ne le voit pas puisqu'on peut toujours multiplier l'une des deux par -1, donc on a une valeur propre à -38 pour W_λ et le fait qu'elles soient de signes opposés vous dit que la fonction sera son opposée quand vous effectuerez la transformation de Fourier.

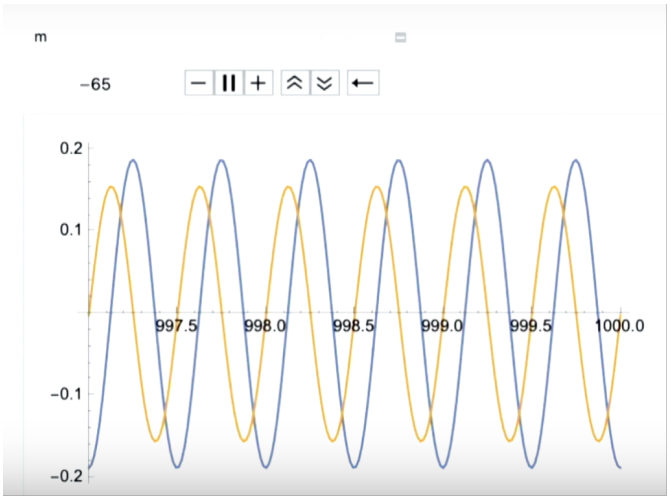


FIGURE 22

Maintenant, pour la valeur -93, vous pouvez voir qu'il y a une coïncidence exacte et cette fois, la fonction sera sa propre transformée de Fourier. Donc vous continuez comme ça, vous continuez, -150, c'est la suivante, les deux sinusoïdes, si vous voulez, les deux parties oscillantes, elles bougent l'une par rapport à l'autre, donc au bout d'un moment, elles coïncident ou bien elles sont en opposition de phase.

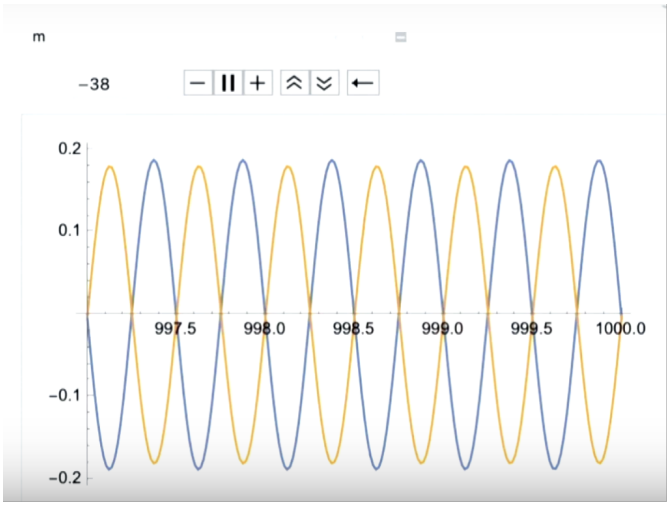


FIGURE 23

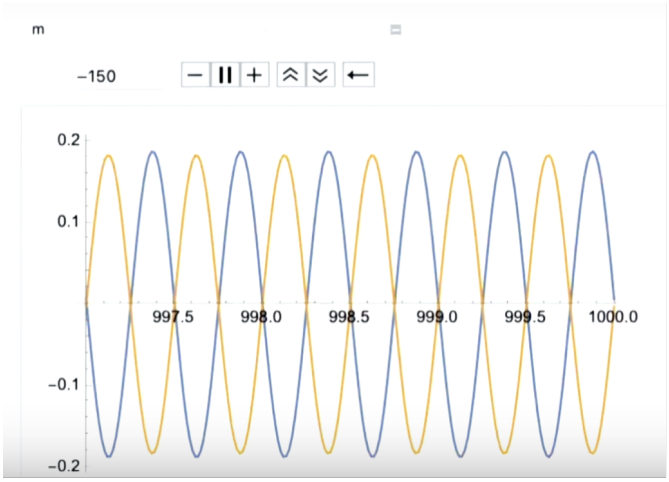
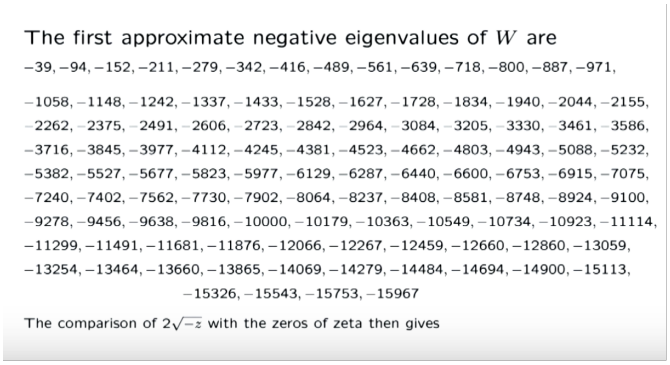


FIGURE 24


The first approximate negative eigenvalues of W are

$-39, -94, -152, -211, -279, -342, -416, -489, -561, -639, -718, -800, -887, -971,$

$-1058, -1148, -1242, -1337, -1433, -1528, -1627, -1728, -1834, -1940, -2044, -2155,$
$-2262, -2375, -2491, -2606, -2723, -2842, -2964, -3084, -3205, -3330, -3461, -3586,$
$-3716, -3845, -3977, -4112, -4245, -4381, -4523, -4662, -4803, -4943, -5088, -5232,$
$-5382, -5527, -5677, -5823, -5977, -6129, -6287, -6440, -6600, -6753, -6915, -7075,$
$-7240, -7402, -7562, -7730, -7902, -8064, -8237, -8408, -8581, -8748, -8924, -9100,$
$-9278, -9456, -9638, -9816, -10000, -10179, -10363, -10549, -10734, -10923, -11114,$
$-11299, -11491, -11681, -11876, -12066, -12267, -12459, -12660, -12860, -13059,$
$-13254, -13464, -13660, -13865, -14069, -14279, -14484, -14694, -14900, -15113,$
$-15326, -15543, -15753, -15967$

The comparison of $2\sqrt{-z}$ with the zeros of zeta then gives

FIGURE 25

Donc vous calculez comme ça les premières valeurs propres négatives de W, vous en dessinez le graphe, ok, c'est beaucoup de travail, et maintenant, ok, vous passez à l'opérateur de Dirac correspondant et vous le comparez avec les zéros de zeta. Donc vous voyez, le premier zéro est 12.49 au lieu de 14, yeah, et vous continuez comme ça, vous les comparez, et à chaque fois, le $n^{\text{ième}}$ zéro de votre fonction est très proche du $n^{\text{ième}}$ zéro de zeta, vous ne changez pas d'indice, non, le $n^{\text{ième}}$ d'un côté correspond au $n^{\text{ième}}$ de l'autre. Donc vous continuez et quand vous dessinez les deux graphes, les points rouges représentent les zéros de zeta et les points bleus représentent ce que nous avons obtenu spectralement et quand vous voyez une seule couleur, c'est que l'un cache l'autre, i.e. ils sont vraiment très très proches l'un de l'autre.

102.098	101.318
104.365	103.726
106.621	105.447
108.885	107.169
111.068	111.03
113.225	111.875
115.412	114.32
117.661	116.227
119.766	118.791
121.918	121.37
124.016	122.947
126.127	124.257
128.25	127.517
130.307	129.579
132.378	131.088
134.507	133.498
136.558	134.757
138.607	138.116
140.613	139.736
142.66	141.124
144.665	143.112
146.724	146.001
148.688	147.423
150.692	150.054
152.617	150.925
154.622	153.025
156.576	156.113
158.581	157.598
160.499	158.85
162.481	161.189

FIGURE 26

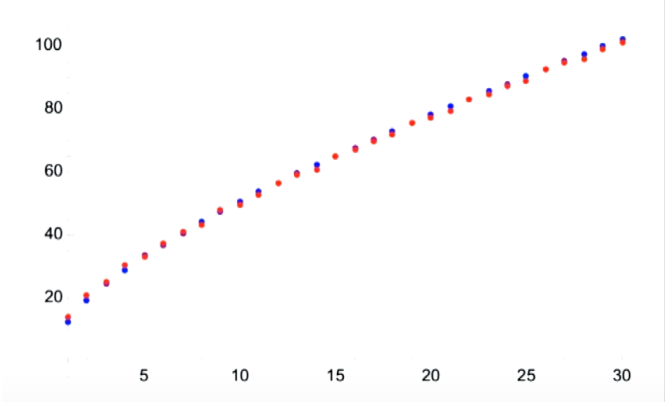


FIGURE 27

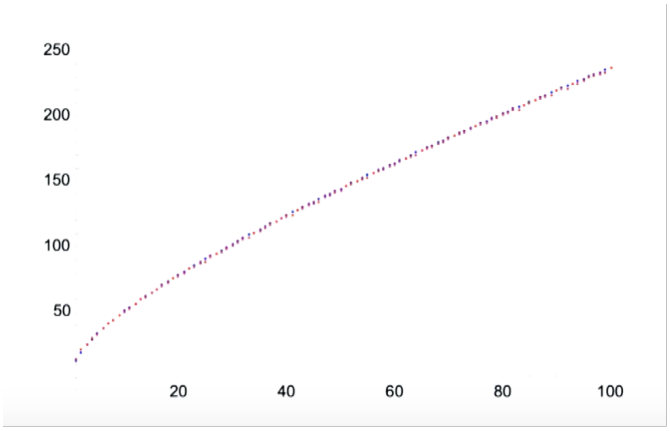


FIGURE 28

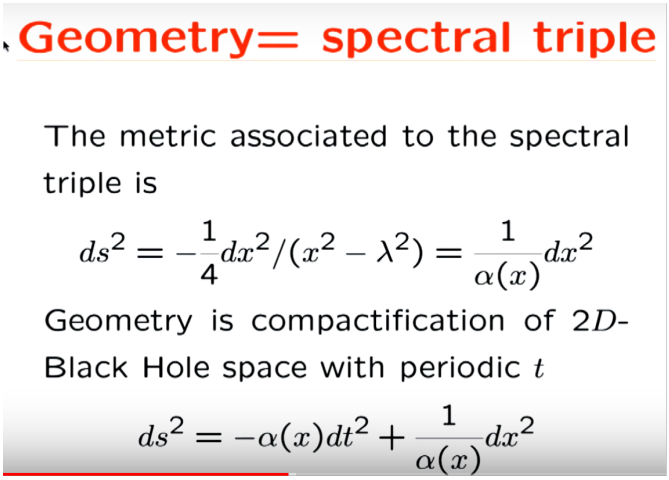


FIGURE 29

Donc on a continué jusqu'aux 60 premières valeurs propres, jusqu'aux 100 premières valeurs propres, et etc. Et bien sûr, donc cela dit vraiment que l'opérateur auto-adjoint, W_λ, parce que je veux dire, rappelez-vous, ok, je veux dire que c'est un indice extrêmement alléchant du fait qu'il devrait exister un opérateur qui les fournit exactement. L'étape suivante, bien sûr, serait de gérer la seconde partie, je veux dire avec des valeurs précises, et la partie infrarouge du spectre. Mais avant que je fasse cela, ce qui est vraiment assez important c'est qu'en géométrie non-commutative, la géométrie est donnée de façon spectrale. Quand vous parlez d'une géométrie, vous pouvez la définir au moyen de l'opérateur de Dirac, ou de ce qui remplace l'opérateur de Dirac, et ce qui remplace les fonctions, bien sûr, et etc., donc là, il n'est pas difficile de trouver ce que sont les fonctions et, je veux dire, sur cette moitié de droite, et de regarder la métrique : la métrique s'obtient à partir du symbole de l'opérateur de Dirac et ici, la métrique que vous trouvez est donnée par un dx^2, il y a une force sur $x^2 - \lambda^2$. Mais ce qui est assez surprenant, c'est que quand vous regardez le spectre comme je l'ai dit précédemment, il y a donc des valeurs négatives pour le laplacien mais il y a aussi des valeurs positives. Donc cela signifie que lorsque vous passez à l'opérateur de Dirac, il aura des valeurs propres purement imaginaires, comme pour les zéros de zeta, mais il aura aussi des valeurs propres réelles. Et ce que nous avons vérifié, avec Henri, c'est que vous savez que ces valeurs réelles ont exactement le même comportement que les zéros triviaux de zeta. Mais le fait que vous ayez à la fois les deux choses, notamment les valeurs propres négatives et les valeurs propres positives, cela vous dit que vous n'êtes pas en train de traiter un problème de Riemann, mais plutôt que vous

êtes en train de traiter un problème de Lorentz, je veux dire avec une métrique de type Minkowski.

Et donc, je veux dire que nous avons utilisé pour avoir une première idée de la géométrie qui est derrière cela, on a utilisé pour la voir, simplement, comme une compaxification d'une géométrie lorentzienne bi-dimensionnelle. Et ok, il s'avère, vous savez, qu'il y a un moyen de faire cela, quand vous rendez la variable t-periodique, et cela correspond à un trou noir en deux dimensions.

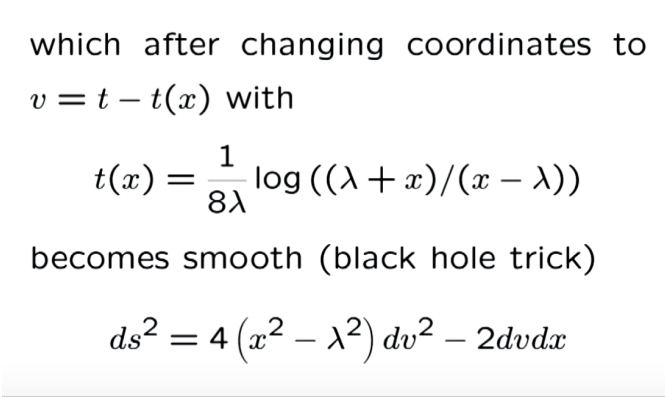


FIGURE 30

Ok et je veux dire, vous pouvez appliquer la ruse habituelle, qui consiste à voir que la métrique du trou noir est en fait lisse.

Donc vous pouvez vraiment réécrire la métrique par un changement adéquant des variables pour la rendre lisse. Et je veux dire qu'il y a, si vous voulez, une manière de plonger cela dans l'espace de Minkowski à trois dimensions, et quand vous faites cela, ce plongement, ce qui est assez intéressant, c'est que pour construire le plongement, vous devez à nouveau utiliser des intégrales elliptiques. Et cela vous donnera ce dessin :

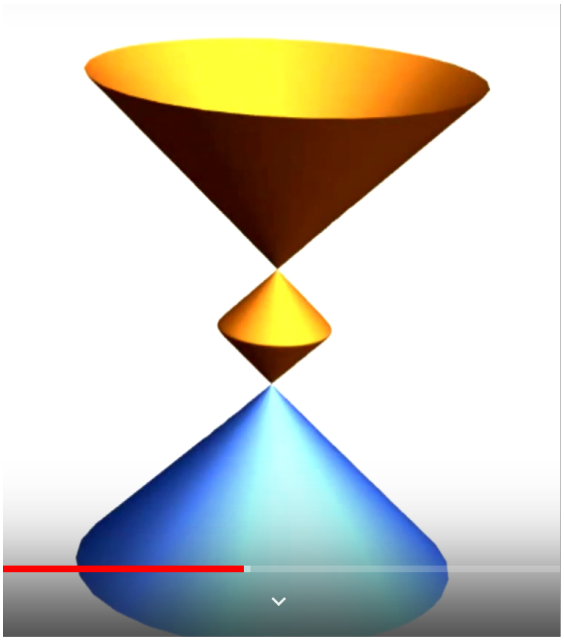


FIGURE 31

Donc si vous voulez, la partie qui est au-dessus et qui ressemble à un cône correspond à la partie intéressante de l'opérateur prolate. La partie qui est entre les deux correspond à ce qui se passe sur l'intervalle, et la partie qui est en-dessous correspond, bien sûr, à la partie symétrique de la partie supérieure. Et quand vous regardez les géodésiques, elles ont la bonne forme supposée.

Qui utilise des automorphismes intérieurs sans en avoir conscience, Denise Vella-Chemla, début novembre 2024

On revient à une note de 2018 appelée *Palindromes* '[1], dans laquelle intervenait un automorphisme intérieur dont on avait vu qu'il permettait de distinguer les nombres impairs des nombres pairs. Il permettait également de distinguer les nombres premiers[2] des nombres composés, ce à quoi on n'avait pas été suffisamment attentive.

On rappelle les définitions : on définit l'ensemble E_n ainsi :

$$E_n = \{a+b \mid a \text{ impair}, \ \ b \text{ impair}, \ \ a \in \mathcal{P}, \quad 3 \leq a \leq \frac{n}{2}, \ \ 6 \leq a+b \leq n\}.$$

La définition de l'automorphisme intérieur est :

$$\begin{array}{rccl} f_n : & E_n & \rightarrow & E_n \\ & & & \\ & a+b_1 & \mapsto & a+b_2 \iff b_1+b_2 = n \end{array}$$

Exemples : l'automorphisme intérieur f_{22} qui travaille sur l'ensemble de toutes les décompositions additives des lignes au-dessus ou sur la ligne du nombre pair 22 (se reporter à l'article initial) lie bijectivement les décompositions additives suivantes :

$$\begin{array}{rccc} f_{22} : & 3+7 & \mapsto & 3+15 \\ & 7+9 & \mapsto & 7+13 \end{array}$$

Les points fixes de f_{22} sont les décompositions additives $3+11, 5+11, 7+11$ et $11+11$.

f_n a 0 point fixe si n est de la forme $4k$ et $\pi\left(\frac{n}{2}\right)$ points fixes si n est de la forme $4k+2$.

Voici le programme python de cette bonne idée :

```
def premier(atester):
     if atester in [0, 1]:  return False
     if atester in [2, 3, 5, 7]:  return True
     k = 2
     while True:
          if k * k > atester:  return True
          else:
               if atester % k == 0:  return False
               else:  k = k + 1
```

[1] https://denisevellachemla.eu/palindromes.pdf

[2] $\mathcal{P}$ désigne l'ensemble des nombres premiers.

```
def autom(n,d):
     return([d[0],n-d[1]])

decompositions = []
for n in range(6,104,2):
     print('',n,':::',end='')
     for x in range(3,n//2+1,2):
          if premier(x):
               decompositions.append([x,n-x])
     for y in range(3,n-1,2):
          nbdecompo = 0
          for d in decompositions:
               if d[1] == y:
                    nbdecompo = nbdecompo+1
          print(nbdecompo,' ',end='')
     print('')
     print('application de l automorphisme f-' ,n)
     nbptsfixesautom = 0
     for d in decompositions:
          if d[0] == autom(n,d)[0] and d[1] == autom(n,d)[1]:
               nbptsfixesautom = nbptsfixesautom+1
     print('nb pts fixes de l automorphisme :  ',nbptsfixesautom)
```

Comme on peut le constater (voir résultat du programme en annexe), et cela doit se démontrer aisément, la fonction *autom* du programme a son résultat qui non seulement est nul pour les doubles de pairs et non nul pour les doubles d'impairs, mais surtout, son résultat qui augmente strictement à chaque nombre double d'un nombre premier.

Cette idée permettrait peut-être d'obtenir une démonstration "à la Zagier" du fait que tout nombre pair a une décomposition de Goldbach (Don Zagier a écrit la preuve en une ligne du fait que tout nombre premier de la forme $4k + 1$ est de façon unique la somme de deux carrés d'entiers). La preuve de Don Zagier [1] est basée sur les notions d'involution et de nombre de points fixes.

Références

[1] Don Zagier, *A One-Sentence Proof That Every Prime* $p \equiv 1 \pmod 4$ *Is a Sum of Two Squares*, The American Mathematical Monthly, Vol. 97, n° 2 (Février 1990), p. 144.

Transcription en Latex de la version française de l'article [1] parue dans la Revue l'Enseignement mathématique
https://denisevellachemla.eu/trad-Zagier-one-sentence-proof.pdf.

Annexe : résultat du programme fourni dans le corps de l'article

```
6 ::::1
application de l automorphisme f_6
nb pts fixes de l automorphisme :  1

8 ::::1 1
application de l automorphisme f_8
nb pts fixes de l automorphisme :  0

10 ::::1 2 1
application de l automorphisme f_10
nb pts fixes de l automorphisme :  2

12 ::::1 2 2 1
application de l automorphisme f_12
nb pts fixes de l automorphisme :  0

14 ::::1 2 3 2 1
application de l automorphisme f_14
nb pts fixes de l automorphisme :  3

16 ::::1 2 3 3 2 1
application de l automorphisme f_16
nb pts fixes de l automorphisme :  0

18 ::::1 2 3 3 3 2 1
application de l automorphisme f_18
nb pts fixes de l automorphisme :  3

20 ::::1 2 3 3 3 3 2 1
application de l automorphisme f_20
nb pts fixes de l automorphisme :  0

22 ::::1 2 3 3 4 3 3 2 1
application de l automorphisme f_22
nb pts fixes de l automorphisme :  4

24 ::::1 2 3 3 4 4 3 3 2 1
application de l automorphisme f_24
nb pts fixes de l automorphisme :  0

26 ::::1 2 3 3 4 5 4 3 3 2 1
application de l automorphisme f_26
nb pts fixes de l automorphisme :  5

28 ::::1 2 3 3 4 5 5 4 3 3 2 1
application de l automorphisme f_28
nb pts fixes de l automorphisme :  0

30 ::::1 2 3 3 4 5 5 5 4 3 3 2 1
application de l automorphisme f_30
nb pts fixes de l automorphisme :  5
```

```
32 ::::1 2 3 3 4 5 5 5 5 4 3 3 2 1
application de l automorphisme f_32
nb pts fixes de l automorphisme :  0

34 ::::1 2 3 3 4 5 5 6 5 5 4 3 3 2 1
application de l automorphisme f_34
nb pts fixes de l automorphisme :  6

36 ::::1 2 3 3 4 5 5 6 6 5 5 4 3 3 2 1
application de l automorphisme f_36
nb pts fixes de l automorphisme :  0

38 ::::1 2 3 3 4 5 5 6 7 6 5 5 4 3 3 2 1
application de l automorphisme f_38
nb pts fixes de l automorphisme :  7

40 ::::1 2 3 3 4 5 5 6 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_40
nb pts fixes de l automorphisme :  0

42 ::::1 2 3 3 4 5 5 6 7 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_42
nb pts fixes de l automorphisme :  7

44 ::::1 2 3 3 4 5 5 6 7 7 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_44
nb pts fixes de l automorphisme :  0

46 ::::1 2 3 3 4 5 5 6 7 7 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_46
nb pts fixes de l automorphisme :  8

48 ::::1 2 3 3 4 5 5 6 7 7 8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_48
nb pts fixes de l automorphisme :  0

50 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_50
nb pts fixes de l automorphisme :  8

52 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_52
nb pts fixes de l automorphisme :  0

54 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_54
nb pts fixes de l automorphisme :  8

56 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 8 8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_56
nb pts fixes de l automorphisme :  0

58 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 8 8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_58
nb pts fixes de l automorphisme :  9
```

```
60 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 9 8 8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_60
nb pts fixes de l automorphisme :  0_
62 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 9 8 8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_62
nb pts fixes de l automorphisme :  10

64 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 10 9 8 8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_64
nb pts fixes de l automorphisme :  0

66 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 10 10 9 8 8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_66
nb pts fixes de l automorphisme :  10

68 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 10 10 10 9 8 8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_68
nb pts fixes de l automorphisme :  0

70 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 10 10 10 10 9 8 8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_70
nb pts fixes de l automorphisme :  10

72 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 10 10 10 10 10 9 8 8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_72
nb pts fixes de l automorphisme :  0

74 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 10 10 11 10 10 10 9 8 8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_74
nb pts fixes de l automorphisme :  11

76 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 10 10 11 11 10 10 10 9 8 8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_76
nb pts fixes de l automorphisme :  0

78 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 10 10 11 11 11 10 10 10 9 8 8 8 7 7 6 5 5 4 3 3
2 1
application de l automorphisme f_78
nb pts fixes de l automorphisme :  11

80 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 10 10 11 11 11 11 10 10 10 9 8 8 8 7 7 6 5 5 4 3
3 2 1
application de l automorphisme f_80
nb pts fixes de l automorphisme :  0

82 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 10 10 11 11 12 11 11 10 10 10 9 8 8 8 7 7 6 5 5
4 3 3 2 1
application de l automorphisme f_82
nb pts fixes de l automorphisme :  12

84 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 10 10 11 11 12 12 11 11 10 10 10 9 8 8 8 7 7 6 5
5 4 3 3 2 1
application de l automorphisme f_84
nb pts fixes de l automorphisme :  0
```

```
86 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 10 10 11 11 12 13 12 11 11 10 10 10 9 8 8 8 7 7
6 5 5 4 3 3 2 1
application de l automorphisme f_86
nb pts fixes de l automorphisme :  13

88 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 10 10 11 11 12 13 13 12 11 11 10 10 10 9 8 8 8 7
7 6 5 5 4 3 3 2 1
application de l automorphisme f_88
nb pts fixes de l automorphisme :  0

90 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 10 10 11 11 12 13 13 13 12 11 11 10 10 10 9 8 8
8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_90
nb pts fixes de l automorphisme :  13

92 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 10 10 11 11 12 13 13 13 13 12 11 11 10 10 10 9 8
8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_92
nb pts fixes de l automorphisme :  0

94 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 10 10 11 11 12 13 13 14 13 13 12 11 11 10 10 10
9 8 8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_94
nb pts fixes de l automorphisme :  14

96 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 10 10 11 11 12 13 13 14 14 13 13 12 11 11 10 10
10 9 8 8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_96
nb pts fixes de l automorphisme :  0

98 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 10 10 11 11 12 13 13 14 14 14 13 13 12 11 11 10
10 10 9 8 8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_98
nb pts fixes de l automorphisme :  14

100 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 10 10 11 11 12 13 13 14 14 14 14 13 13 12 11 11
10 10 10 9 8 8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_100
nb pts fixes de l automorphisme :  0

102 ::::1 2 3 3 4 5 5 6 7 7 8 8 8 9 10 10 10 11 11 12 13 13 14 14 14 14 14 13 13 12 11
11 10 10 10 9 8 8 8 7 7 6 5 5 4 3 3 2 1
application de l automorphisme f_102
nb pts fixes de l automorphisme :  14
```

Se rappeler de cela, Denise Vella-Chemla, début novembre 2024

Il faut que je me rappelle que Gauss voit la relation $a \equiv b$ (mod m) comme une relation d'équivalence sans restriction sur a, b, m (si ce n'est que m est "sans signe", voir image ci-dessous) alors que je l'utilise plutôt systématiquement comme si j'avais :

$$a \bmod m = b \iff \exists q \text{ tel que } \begin{array}{l} a = mq + b \\ \text{et } b \geq 0 \text{ et } b \text{ minimum} \\ \text{et } a \geq 0 \text{ et } a \text{ maximum.} \end{array}$$

i.e. je projette la classe d'équivalence dans $\mathbb{Z}$ sur l'intervalle $[0, m[$; Gauss appelle le résidu modulaire que je considère toujours le "résidu minimum positif de a modulo m".

RECHERCHES

ARITHMÉTIQUES.

SECTION PREMIÈRE.

Des Nombres congrus en général.

1. Si un nombre *a* divise la différence des nombres *b* et *c*, *b* et *c* sont dits *congrus* suivant *a*, sinon *incongrus*. *a* s'appellera le module ; chacun des nombres *b* et *c*, *résidus* de l'autre dans le premier cas, et *non résidus* dans le second.

Les nombres peuvent être positifs ou négatifs, mais entiers. Quant au module il doit évidemment être pris absolument, c'est-à-dire, sans aucun signe.

Ainsi −9 et +16 sont *congrus* par rapport au module 5; −7 est *résidu* de 15 par rapport au module 11, et *non résidu* par rapport au module 3.

Au reste 0 étant divisible par tous les nombres, il s'ensuit qu'on peut regarder tout nombre comme congru avec lui-même par rapport à un module quelconque.

2. Tous les résidus d'un nombre donné *a* suivant le module *m*, sont compris dans la formule $a + km$, *k* étant un entier indéterminé. Les plus faciles des propositions que nous allons exposer

A

FIGURE 1 : article 1 des Recherches arithmétiques de Karl Friedrich Gauss.

4. Il suit de là que chaque nombre aura un résidu, tant dans la suite $0, 1, 2, \ldots (m-1)$, que dans celle-ci $0, -1, -2, \ldots -(m-1)$; nous les appellerons résidus *minima*; et il est clair qu'à moins que 0 ne soit résidu, il y en aura toujours deux, l'un positif, l'autre négatif. S'ils sont inégaux, l'un d'eux sera $< \frac{m}{2}$; s'ils sont égaux, chacun d'eux $= \frac{m}{2}$ sans avoir égard au signe; d'où il suit qu'un nombre quelconque a un résidu qui ne surpasse pas la moitié du module, et que nous appellerons résidu *minimum absolu*.

Par exemple -13 suivant le module 5, a pour résidu *minimum* positif 2, qui est en même temps *minimum absolu*, et -3 pour résidu *minimum* négatif; $+5$, suivant le module 7, est lui-même son résidu *minimum* positif; -2 est le résidu *minimum* négatif et en même temps le *minimum absolu*.

(*) Nous avons adopté ce signe à cause de la grande analogie qui existe entre l'égalité et la congruence. C'est pour la même raison que Legendre, dans des mémoires que nous aurons souvent occasion de citer, a employé le signe même de l'égalité, pour désigner la congruence; nous en avons préféré un autre, pour prévenir toute ambiguité.

FIGURE 2 : article 4 des Recherches arithmétiques de Karl Friedrich Gauss.

De l'importance des bijections, Denise Vella-Chemla, octobre 2024

On cherche à démontrer que tout nombre pair ($n > 4$) est la somme de deux nombres premiers (impairs). $\mathcal{P}$ désigne l'ensemble des nombres premiers. On a compris (et Leila Schneps a démontré [1]) qu'un nombre premier p, inférieur à la moitié de n, qui ne partage aucun reste de division euclidienne avec n (lorsqu'on le divise par un nombre premier impair inférieur à $\sqrt{n}$) est un décomposant de Goldbach de n.

On va ci-après établir une relation entre certaines écritures simples des deux nombres 0 et n, qui devrait garantir l'existence d'un décomposant de Goldbach pour tout nombre pair.

Étudions l'exemple fétiche $n = 98$ pour fixer les idées.

Ci-dessous, dans un tableau, dans les deux colonnes de gauche, les écritures de 98, de la forme $n = 98 = r + b \times q$ avec $3 \leq r \leq \frac{n}{2}$, $1 \leq b \leq \sqrt{n}$, $b \in \mathcal{P} \cup \{1\}$ et dans les deux colonnes de droite les écritures de 0 de la forme $0 = r - b \times q$ avec $3 \leq r \leq \frac{n}{2}$, $1 \leq b \leq \sqrt{n}$, $b \in \mathcal{P} \cup \{1\}$.

98	$= 3 + 5 \times 19$	98	$= 9 + 1 \times 89$	0	$= 3 - 3 \times 1$	0	$= 11 - 1 \times 11$
	$= 5 + 3 \times 31$		$= 15 + 1 \times 83$		$= 5 - 5 \times 1$		$= 13 - 1 \times 13$
	$= 7 + 7 \times 13$		$= 19 + 1 \times 79$		$= 7 - 7 \times 1$		$= 17 - 1 \times 17$
	$= 11 + 3 \times 29$		$= 25 + 1 \times 73$		$= 9 - 3 \times 3$		$= 19 - 1 \times 19$
	$= 13 + 5 \times 17$		$= 27 + 1 \times 71$		$= 15 - 3 \times 5$		$= 23 - 1 \times 23$
	$= 17 + 3 \times 27$		$= 31 + 1 \times 67$		$= 21 - 3 \times 7$		$= 29 - 1 \times 29$
	$= 21 + 7 \times 11$		$= 37 + 1 \times 61$		$= 25 - 5 \times 5$		$= 31 - 1 \times 31$
	$= 23 + 3 \times 25$		$= 39 + 1 \times 59$		$= 27 - 3 \times 9$		$= 37 - 1 \times 37$
	$= 29 + 3 \times 23$		$= 45 + 1 \times 53$		$= 33 - 3 \times 11$		$= 41 - 1 \times 41$
	$= 33 + 5 \times 13$				$= 35 - 5 \times 7$		$= 43 - 1 \times 43$
	$= 35 + 3 \times 21$				$= 39 - 3 \times 13$		$= 47 - 1 \times 47$
	$= 41 + 3 \times 19$				$= 45 - 3 \times 15$		
	$= 43 + 5 \times 11$				$= 49 - 7 \times 7$		
	$= 47 + 3 \times 17$						
	$= 49 + 7 \times 7$						

Associons maintenant les égalités de la colonne de gauche et celles de la colonne de droite par des lettres entre parenthèses, cette bijection s'effectue entre deux égalités qui ont r en commun (dans les écritures $n = r + b \times q$ et $0 = r - b \times q$).

[1] voir https://denisevellachemla.eu/moins-deux.pdf section 1.

98	$= 3 + 5 \times 19$	(a)	0	$= 9 - 3 \times 3$	(p)
	$= 5 + 3 \times 31$	(b)		$= 15 - 3 \times 5$	(q)
	$= 7 + 7 \times 13$	(c)		$= 21 - 3 \times 7$	(g)
	$= 11 + 3 \times 29$	(d)		$= 25 - 5 \times 5$	(s)
	$= 13 + 5 \times 17$	(e)		$= 27 - 3 \times 9$	(t)
	$= 17 + 3 \times 27$	(f)		$= 33 - 3 \times 11$	(j)
	$= 21 + 7 \times 11$	(g)		$= 35 - 5 \times 7$	(k)
	$= 23 + 3 \times 25$	(h)		$= 39 - 3 \times 13$	(w)
	$= 29 + 3 \times 23$	(i)		$= 45 - 3 \times 15$	(x)
	$= 33 + 5 \times 13$	(j)		$= 49 - 7 \times 7$	(o)
	$= 35 + 3 \times 21$	(k)		----------	
	$= 41 + 3 \times 19$	(l)		$= 3 - 1 \times 3$	(a)
	$= 43 + 5 \times 11$	(m)		$= 5 - 1 \times 5$	(b)
	$= 47 + 3 \times 17$	(n)		$= 7 - 1 \times 7$	(c)
	$= 49 + 7 \times 7$	(o)		$= 11 - 1 \times 11$	(d)
	----------			$= 13 - 1 \times 13$	(e)
	$= 9 + 1 \times 89$	(p)		$= 17 - 1 \times 17$	(f)
	$= 15 + 1 \times 83$	(q)		$= 19 - 1 \times 19$	(r)
	$= 19 + 1 \times 79$	(r)		$= 23 - 1 \times 23$	(h)
	$= 25 + 1 \times 73$	(s)		$= 29 - 1 \times 29$	(i)
	$= 27 + 1 \times 71$	(t)		$= 31 - 1 \times 31$	(u)
	$= 31 + 1 \times 67$	(u)		$= 37 - 1 \times 37$	(v)
	$= 37 + 1 \times 61$	(v)		$= 41 - 1 \times 41$	(l)
	$= 39 + 1 \times 59$	(w)		$= 43 - 1 \times 43$	(m)
	$= 45 + 1 \times 53$	(x)		$= 47 - 1 \times 47$	(n)

Il faut comprendre pourquoi toute telle bijection envoie une écriture de la forme $n = r + 1 \times q$ sur une écriture de la forme $0 = r - 1 \times r$, c'est-à-dire associe deux écritures des parties basses du tableau, i.e. deux écritures qui ont toutes les deux le nombre 1 comme premier facteur dans le produit.

Disons-le autrement : on désigne les 4 parties du tableau par les termes HG pour haut-gauche, HD pour haut-droit, BG pour bas-gauche et BD pour bas-droit. La conjecture de Goldbach serait démontrée si l'on pouvait prouver qu'il y a toujours une flèche entre BG et BD. S'il existait un contre-exemple à la conjecture, on aurait une configuration dans laquelle toutes les flèches partant du bas du tableau seraient soit des flèches BG $\longleftrightarrow$ HD, soit des flèches BD $\longleftrightarrow$ HG.

Étudions ces produits un instant : les produits qui interviennent dans les égalités des deux parties hautes du tableau sont ordonnés, du plus petit au plus grand (avec seulement un palier sur $\frac{n}{2}$, qui se trouve écrit dans les deux colonnes en partie haute) ; ils vont croissant dans la colonne de droite, en descendant dans la colonne, puis vont croissant à nouveau (après $\frac{n}{2}$) dans la colonne de gauche, en remontant dans la colonne). De même, les produits qui interviennent dans les égalités des parties basses du tableau sont ordonnés de façon croissante similairement (descendre dans la colonne de droite, et remonter dans celle de gauche pour maintenir la croissance stricte).
Rappelons que les égalités sont des 4 formes suivantes :

- dans la partie HG, $n = r + b \times q$ avec $3 \leq r \leq \frac{n}{2}$, $1 \leq b \leq \sqrt{n}$, $b \in \mathcal{P} \cup \{1\}$;
- dans la partie BG, $n = r + 1 \times q$ avec $\frac{n}{2} \leq q \leq n$;
- dans la partie HD, $0 = r - b \times q$ avec $3 \leq r \leq \frac{n}{2}$, $1 \leq b \leq \sqrt{n}$, $b \in \mathcal{P} \cup \{1\}$;
- dans la partie BD, $0 = r - 1 \times q$ avec $r = q$, $r \in \mathcal{P}$, $\sqrt{n} \leq r \leq \frac{n}{2}$.

Si toutes les flèches de la bijection reliaient systématiquement une égalité de BG à une égalité de HD, alors, on devrait avoir un lien bijectif entre toute égalité de la forme

$$n = r + p \ (\times 1) \qquad (A)$$

(se trouvant dans la partie BG du tableau) et une égalité de la forme

$$0 = r - p' \times q \qquad (B).$$

(se trouvant dans la partie HD de la table). On transforme (B) en ajoutant n aux deux côtés de l'égalité en

$$\begin{aligned} 0 + n &= r - p' \times q + n \\ n &= r - p' \times q + n \qquad (B') \end{aligned}$$

Mais identifier (A) et (B'), et éliminer n et r donne

$$\begin{cases} n = r + p \ (\times 1) & (A) \\ n = r - p' \times q + n & (B') \end{cases}$$

qui amène

$$r + p = r - p' \times q + n$$

qu'on réécrit en

$$n = p + p' \times q$$

avec p un nombre premier supérieur à $\dfrac{n}{2}$.

Effectuons la transformation qui vient d'être indiquée sur toutes les égalités de la partie BG du tableau puisqu'elles sont censées *toutes* "pointer" vers HD. Ce faisant, on obtient pour chacune d'elles une égalité de la forme $n = p + p' \times q$, les nombres p couvrant certains nombres impairs supérieurs à $\dfrac{n}{2}$. On peut rassembler toutes ces égalités (celles qui étaient déjà en partie HG du

tableau et celles qui étaient en partie HG du tableau et qu'on a transformées) pour fixer les idées et comprendre d'où proviendrait la contradiction : elle proviendrait de l'ordre strictement croissant sur les produits qui doit nécessairement être respecté par les égalités. On met en regard des 3 nombres premiers permettant de trouver (dans la vraie vie) une décomposition de Goldbach de $n = 98$ un point d'interrogation :

98	$= 3 + 5 \times 19$	(a)
	$= 5 + 3 \times 31$	(b)
	$= 7 + 7 \times 13$	(c)
	$= 11 + 3 \times 29$	(d)
	$= 13 + 5 \times 17$	(e)
	$= 17 + 3 \times 27$	(f)
	$= 21 + 7 \times 11$	(g)
	$= 23 + 3 \times 25$	(h)
	$= 29 + 3 \times 23$	(i)
	$= 33 + 5 \times 13$	(j)
	$= 35 + 3 \times 21$	(k)
	$= 41 + 3 \times 19$	(l)
	$= 43 + 5 \times 11$	(m)
	$= 47 + 3 \times 17$	(n)
	$= 49 + 7 \times 7$	(o)

	$= 53 + 3 \times 15$	(x)
	$= 59 + 3 \times 13$	(w)
	$= 61 + b \times q$?	(contrad 1 ?)
	$= 67 + b' \times q'$?	(contrad 2 ?)
	$= 71 + 3 \times 9$	(t)
	$= 73 + 5 \times 5$	(s)
	$= 79 + b'' \times q''$?	(contrad 3 ?)
	$= 83 + 3 \times 5$	(q)
	$= 89 + 3 \times 3$	(p)

Posons que l'égalité (contrad 1 ?) est de la forme $98 = 61 + 3 \times k$, alors, du fait de l'ordre croissant à respecter, k devrait être strictement compris entre 9 et 13 (regarder les égalités correctement remplies au-dessus et au-dessous de celle à laquelle on s'intéresse : puisque 61 est compris entre 59 et 71). Or $61 + 3 \times 11 = 94 \neq 98$, d'où une première contradiction.

Posons que l'égalité (contrad 1 ?) est de la forme $98 = 61 + 5 \times k$, alors k, du fait de l'ordre crois-

sant à respecter, devrait être strictement compris entre 5 et 11 (regarder les égalités correctement remplies au-dessus et au-dessous de celle à laquelle on s'intéresse : puisque 61 est compris entre 43 et 73). Or $61+5\times 7 = 96 \neq 98$, d'où une seconde contradiction. Ou bien, or $61+5\times 9 = 106 \neq 98$, d'où une troisième contradiction

Posons que l'égalité (contrad 1 ?) est de la forme $98 = 61 + 7 \times k$, alors k, du fait de l'ordre croissant à respecter, devrait être strictement inférieur à 7 (la seule égalité correctement remplie au-dessus de celle à laquelle on s'intéresse faisant intervenir 7 comme premier facteur du produit est $98 = 49 + 7 \times 7$: puisque 61 est supérieur à 49). Or $61 + 7 \times k$, avec $k < 7$ ne permet pas d'atteindre 98, d'où un certain nombre d'autres contradictions.

On peut établir des raisonnements similaires pour les égalités $98 = 67 + b \times q$ et $98 = 79 + b' \times q'$ avec $b, b' \in \mathcal{P}$, $b, b' \leq \sqrt{n}$, q, q' nombres impairs compris strictement entre ceci et cela et aboutir à autant de contradictions. Il faudrait écrire méthodiquement cela de façon générale. On pense avoir fourni l'idée d'une démonstration.

Annexe : programme d'écriture des égalités et son résultat

Voici un petit programme python qui écrit les égalités :

```
import math
from math import sqrt,floor

for n in range(98,100,2):
     print('',n,':::::')
     rac = floor(sqrt(n))
     for x in range(3,n//2+1,2):
          print(":3d = :3d +".format(n,x),end='')
          k = 3
          while (n-x)%k != 0 and k <= rac:
               k = k+2
          if k>rac:
               print(" 1 x:3d.".format(n-x))
          else:
               print(":3d x:3d.".format(k,(n-x)//k))
          print(" 0 = :3d -".format(x),end='')
          k = 3
          while x%k != 0 and k <= rac:
               k = k+2
          if k>rac:
               print(" 1 x:3d.".format(x))
          else:
               print(":3d x:3d.".format(k,x//k))
          print('')
```

Voici son résultat :

```
98 ::::
 98 = 3 + 5 x 19.
  0 = 3 - 3 x 1.

 98 = 5 + 3 x 31.
  0 = 5 - 5 x 1.

 98 = 7 + 7 x 13.
  0 = 7 - 7 x 1.

 98 = 9 + 1 x 89.
  0 = 9 - 3 x 3.

 98 = 11 + 3 x 29.
  0 = 11 - 1 x 11.

 98 = 13 + 5 x 17.
  0 = 13 - 1 x 13.

 98 = 15 + 1 x 83.
  0 = 15 - 3 x 5.

 98 = 17 + 3 x 27.
  0 = 17 - 1 x 17.
```

```
 98 = 19 + 1 x 79.
  0 = 19 - 1 x 19.

 98 = 21 + 7 x 11.
  0 = 21 - 3 x 7.

 98 = 23 + 3 x 25.
  0 = 23 - 1 x 23.

 98 = 25 + 1 x 73.
  0 = 25 - 5 x 5.

 98 = 27 + 1 x 71.
  0 = 27 - 3 x 9.

 98 = 29 + 3 x 23.
  0 = 29 - 1 x 29.

 98 = 31 + 1 x 67.
  0 = 31 - 1 x 31.

 98 = 33 + 5 x 13.
  0 = 33 - 3 x 11.

 98 = 35 + 3 x 21.
  0 = 35 - 5 x 7.

 98 = 37 + 1 x 61.
  0 = 37 - 1 x 37.

 98 = 39 + 1 x 59.
  0 = 39 - 3 x 13.

 98 = 41 + 3 x 19.
  0 = 41 - 1 x 41.

 98 = 43 + 5 x 11.
  0 = 43 - 1 x 43.

 98 = 45 + 1 x 53.
  0 = 45 - 3 x 15.

 98 = 47 + 3 x 17.
  0 = 47 - 1 x 47.

 98 = 49 + 7 x 7.
  0 = 49 - 7 x 7.
```

Sauts de puces, Denise Vella-Chemla, décembre 2024

On note $\mathcal{P}$ l'ensemble des nombres premiers. Soit n un nombre pair.

Considérons un ensemble E de cardinal $\frac{n-2}{4}$ contenant des triplets défini par

$$E = \{(r, b, q) \mid 3 \leq r \leq n/2 \text{ et } n = r + b \times q \text{ et } 1 \leq b \leq \sqrt{n} \text{ et } b \in \mathcal{P} \cup \{1\}\}$$

et un ensemble F de cardinal $\frac{n-2}{4}$ contenant des triplets défini par

$$F = \{(r, b, q) \mid 3 \leq r \leq n/2 \text{ et } 0 = r - b \times q \text{ et } 1 \leq b \leq \sqrt{n} \text{ et } b \in \mathcal{P} \cup \{1\}\}$$

Voyons E comme l'union de deux sous-ensembles disjoints EH et EB, les triplets de EB étant de la forme $(r, 1, q)$ (avec r un nombre composé et q un nombre premier tel que $\frac{n}{2} \leq q \leq n$) et les triplets de EH étant de la forme (r, b, q) avec $b \neq 1$.

Similairement, voyons F comme l'union de deux sous-ensembles disjoints FH et FB, les triplets de FB étant de la forme $(r, 1, q)$ et les triplets de FH étant de la forme (r, b, q) avec $b \neq 1$.

Les triplets de l'ensemble EH peuvent être totalement ordonnés selon leur première coordonnée (r). Notons ainsi l'ordre en question [1] :

$$(r_1, b_1, q_1) < (r_2, b_2, q_2) < \ldots < (r_{\frac{n-2}{4}}, b_{\frac{n-2}{4}}, q_{\frac{n-2}{4}}),$$

avec

$$r_1 < r_2 < \ldots < r_{\frac{n-2}{4}}.$$

L'ordre croissant sur les r_i entraîne un ordre décroissant sur les produit $b_i \times q_i$ puisque toutes les formes $r_i + b_i \times q_i$ sont autant de représentations différentes du nombre n.

Les triplets de l'ensemble FB sont de la forme $(r, 1, r)$ (puisque $0 = r - 1 \times r$) avec r un nombre premier[2].

Comme il y a au moins un nombre premier entre 3 et $n/2$, l'ensemble EB n'est pas vide.

Comme il y a au moins un nombre premier entre $n/2$ et n, l'ensemble FB n'est pas vide (théorème de Tchebychev démontrant le Postulat de Bertrand).

Il existe une bijection de E dans F qui envoie chaque triplet de E sur le triplet de F qui a la même première coordonnée que lui.

On comprend aisément qu'une décomposition de Goldbach, si elle existe, associe par cette bijection un élément de EB à un élément de FB.

[1] On se place "côté n".
[2] On se place "côté 0".

Pourquoi n'est-il pas possible pour une bijection ainsi définie qu'elle envoie tout élément de EB vers un élément de FH et tout élément de FB vers un élément de EH ?

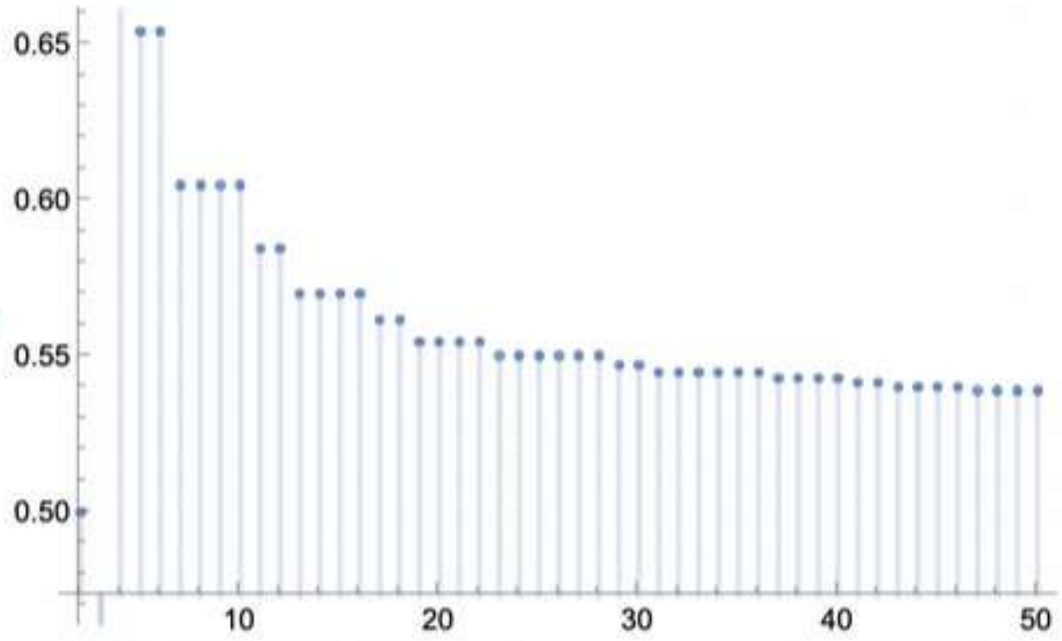
Si c'était le cas, la bijection enverrait une égalité de la forme (a) $n = r + p(\times 1)$ sur une égalité de la forme (b) $0 = r - p'$, qu'on transforme en (c) $0 + n = r - p' \times q + n$, qui, utilisée conjointement avec (a), amène $r + p = r - p' \times q + n$, qu'on réécrit en $n = p + p' \times q$, avec $p \geq \frac{n}{2}$.

Mais de telles nouvelles égalités engendrées ne pourraient s'intercaler entre les produits ordonnés dans l'ordre croissant qu'on avait mis au jour, dans la mesure où l'intervalle est déjà "plein comme un œuf" (pour sûr, il faudrait dire cela plus mathématiquement).

In[64]:=
```
wif[n_] := N[Total[Table[Sin[Pi Gamma[k] / (2 k)]^2, {k, 1, n}]]]
```

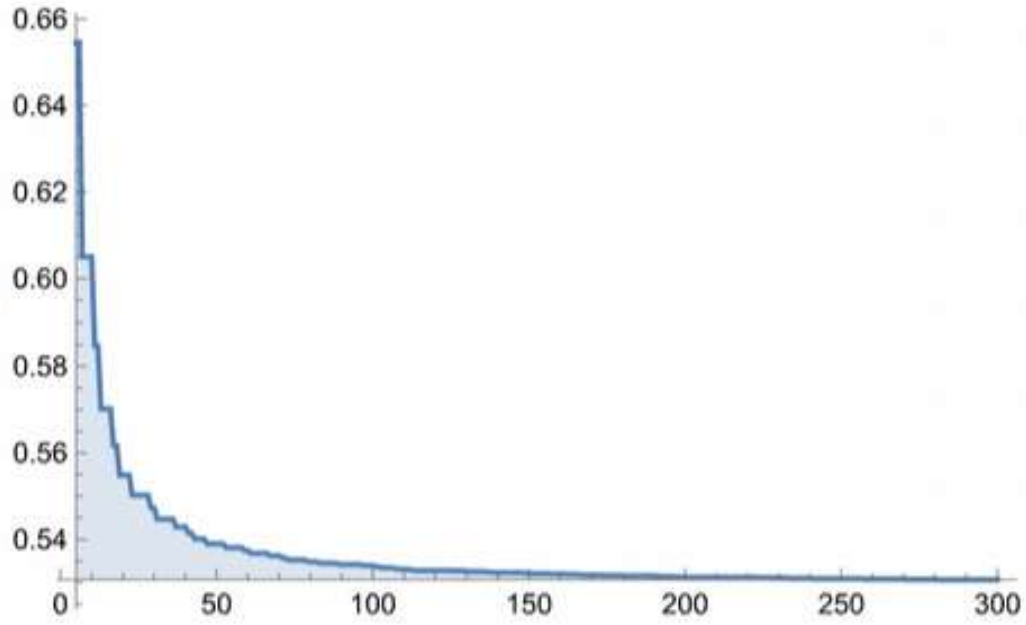
In[65]:=
```
DiscretePlot[{wif[n] - PrimePi[n]}, {n, 2, 50}]
```

Out[65]=



In[68]:=
```
DiscretePlot[{wif[n] - PrimePi[n]}, {n, 5, 300}, PlotRange → All]
```

Out[68]=



ps pour k=21 on a (k-1)!/(2k) =57926238289920000 qui est un entier et donc le sinus donne zero.

emacs27@denise-Inspiron-3501

File Edit Options Buffers Tools TeX Text Isearch Help

Repeat Forward Abort Finish Undo Replace Show Hits Help

```
racine 37
produit des p moins 2 sur p 0.02702702702702703
1408  -->  19.027027027027028
min reussi

1410
nbdg  58
racine 37
produit des p moins 2 sur p 0.02702702702702703
1410  -->  19.054054054054056
min reussi

1412
nbdg  18
racine 37
produit des p moins 2 sur p 0.02702702702702703
1412  -->  19.08108108108108
min rate

1414
nbdg  30
racine 37
produit des p moins 2 sur p 0.02702702702702703
1414  -->  19.10810810810811
min reussi

1416
nbdg  47
racine 37
produit des p moins 2 sur p 0.02702702702702703
1416  -->  19.135135135135137
min reussi

1418
```

-:--- essaimin.tex 2% L4928 (LaTeX Isearch)

I-search backward: rate

emacs27@denise-Inspiron-3501

File Edit Options Buffers Tools Python Help

Save Undo

```
import math

def prime(atester):
  k = 2 ;
  if (atester in [0,1]): return False ;
  if (atester in [2,3,5,7]): return True ;
  while (True):
    if ((k * k) > atester): return True
    else:
      if ((atester % k) == 0): return False
      else: k=k+1

for n in range(6,100002,2):
  print('')
  print(n)
  nbdg = 0
  moitie = int(n/2)
  for p in range(3, moitie+1,2):
    if prime(p) and prime(n-p):
      nbdg += 1
  print('nbdg ', nbdg)
  racine = int(math.sqrt(n))
  print('racine',racine)
  proddespmoinsdeuxsurp = 1
  for p in range(3,racine+1,2):
    proddespmoinsdeuxsurp = proddespmoinsdeuxsurp * (p-2)/p
  print('produit des p moins 2 sur p',proddespmoinsdeuxsurp)
  essaimin = proddespmoinsdeuxsurp*n/2
  print(n,' --> ',essaimin)
  if essaimin < nbdg:
    print('min reussi')
  else:
    print('min rate')
```

oubli ici du test if prime(p)

-:--- proddesunmoinsdeuxsurp.py All L13 (Python ElDoc)

Wrote /home/denise/Bureau/proddesunmoinsdeuxsurp.py

Figure 4

Troisièmement, le rectangle est penché sur la gauche de telle façon que son côté droit ait une pente de $-\sqrt{3}$. En utilisant la transformation (6), x est remplacé par $x+\frac{1}{3}\sqrt{3}y$, ce qui donne

$$|x+\sqrt{3}y-a|+|x-\frac{1}{3}\sqrt{3}y+a|=2a$$

qui est l'équation d'un parallélogramme (Fig. 5) avec un côté sur l'axe des x et un côté allant du point $(a,0)$ vers le haut à gauche jusqu'au point $(0,\sqrt{3}a)$.

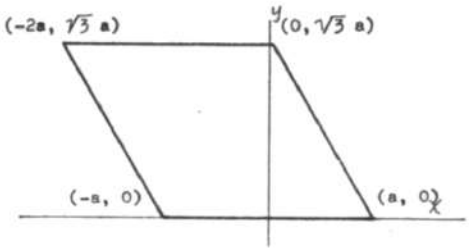


Figure 5

On ne sait pas encore si le second résultat :

$$\sum_{k=1}^{k=n} \frac{1}{\sqrt{k}} \simeq 2\sqrt{n} + \gamma'$$

est connu, est vrai et si oui, s'il est démontré. La différence entre les deux résultats des calculs, égale à $\gamma' = 1.4603046$, pourrait faire penser[1] à une constante dite Constante de Porter, dont la valeur est 1.4670780794... ; Donald E. Knuth en a donné la valeur exacte (Voir ici : https://fr.wikipedia.org/wiki/Constante_de_Porter).

Mathematical Physics. — *Sur l'intégration de quelques problèmes aux limites régis par l'équation de* FOURIER *dite „de la chaleur" au moyen de la méthode des transformations fonctionnelles simultanées.* Par S. R. DE GROOT. (Soixante-dix-neuvième publication du Fonds VAN DER WAALS, VAN DER WAALS-Laboratorium der Gemeente Universiteit, Amsterdam.) (Communicated by Prof. J. D. VAN DER WAALS JR.)

(Communicated at the meeting of June 27, 1942.)

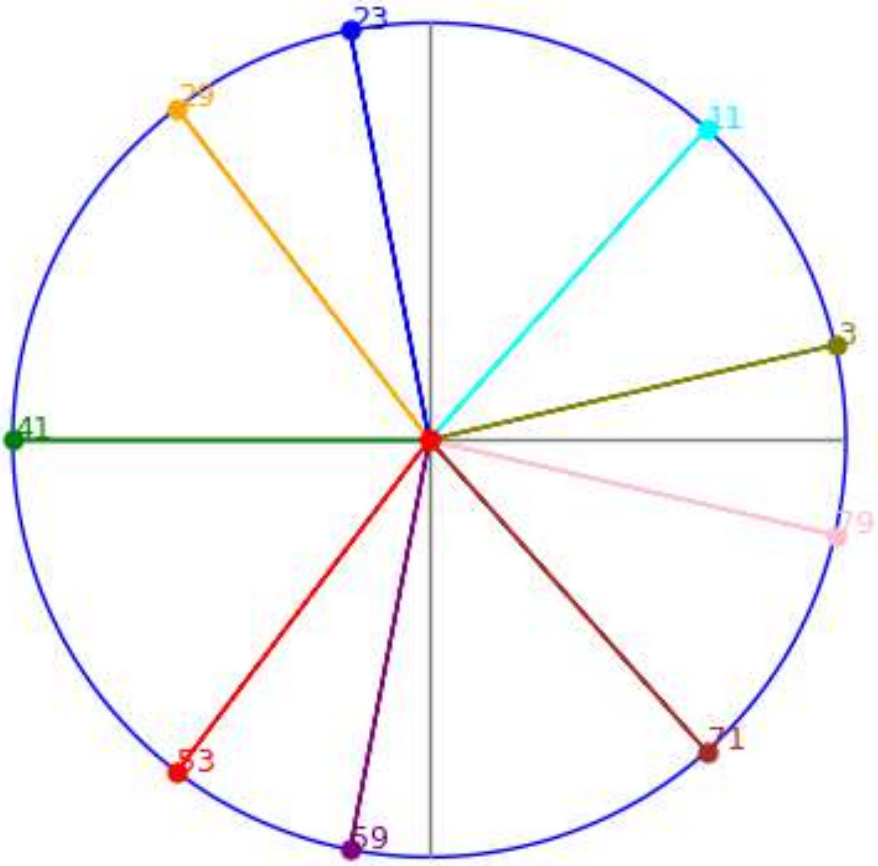
Sommaire. Quelques problèmes aux limites sur la propagation de la chaleur dans un fil ont été intégrés au moyen de la méthode des transformations fonctionnelles. Si l'on applique une transformation de FOURIER par rapport à la variable qui désigne l'abscisse et en même temps une transformation de LAPLACE à la variable du temps, la solution peut être fournie après un calcul très simple. Il est essentiel de choisir la transformation qui est adaptée aux intervalles des variables et aux conditions aux frontières.

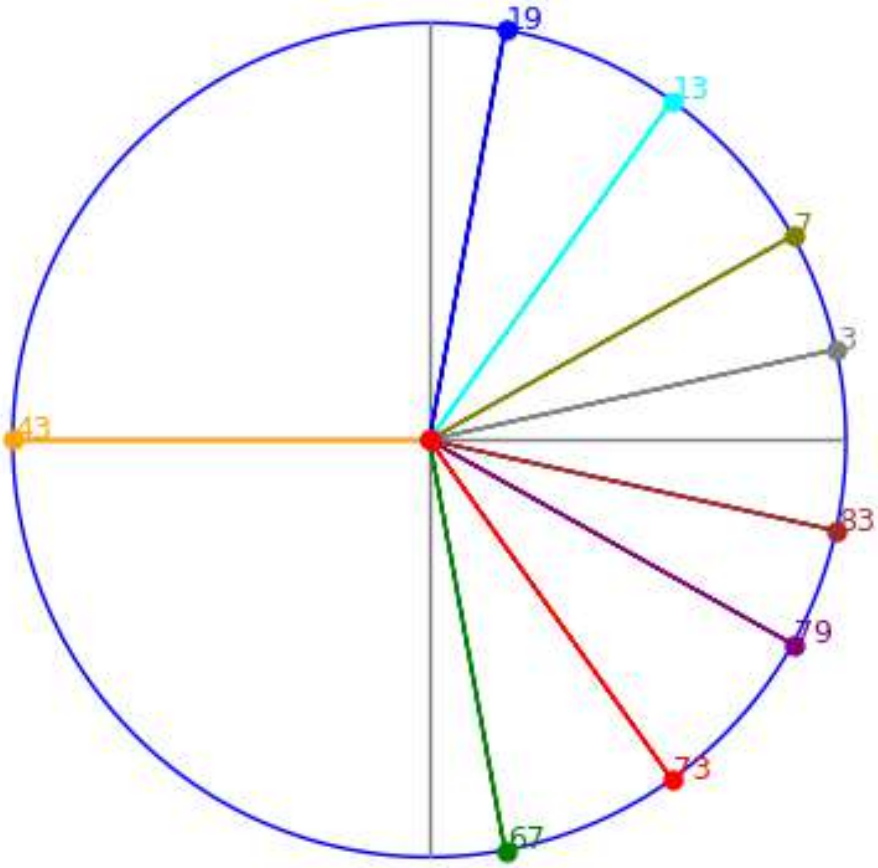
I. Conditions aux limites de première espèce.

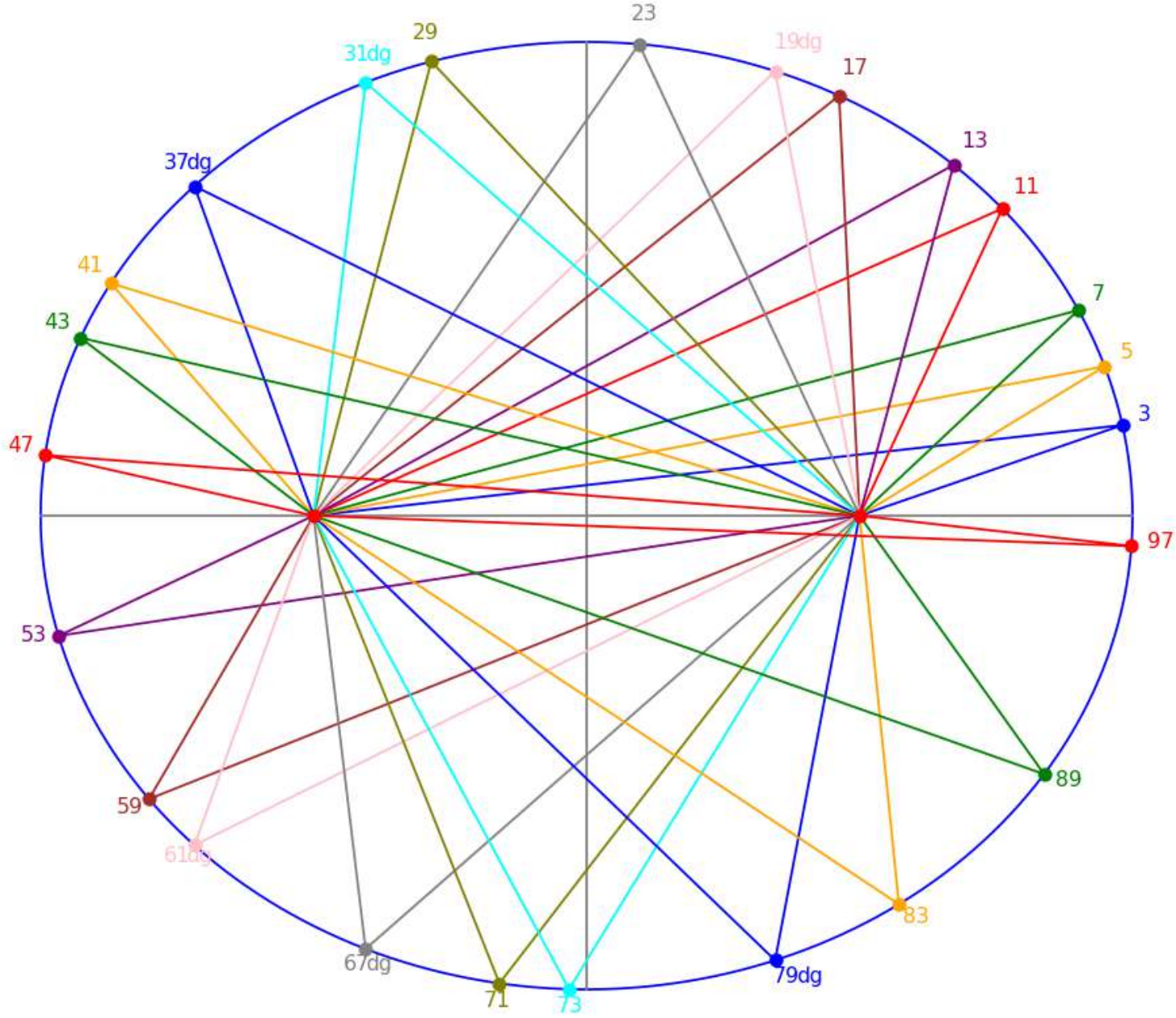
§ 1. *La transformation fonctionnelle.*

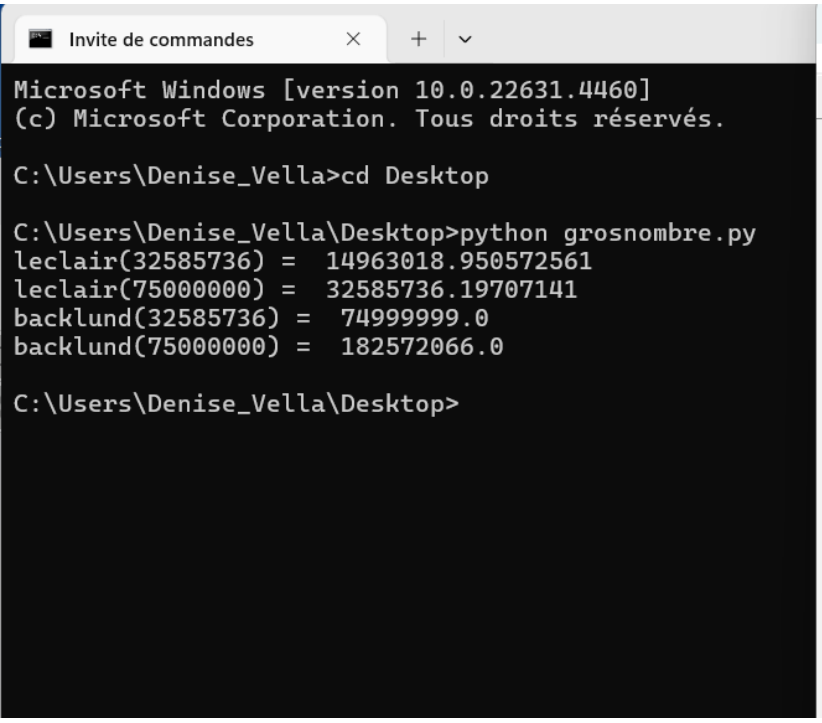
On sait que la transformation de LAPLACE donne une justification rigoureuse de la méthode opératoire de HEAVISIDE (calcul symbolique) dans les cas où cette méthode est légitime. D'autre part la théorie de la transformation de LAPLACE montre clairement les cas où il n'est pas permis d'appliquer le calcul symbolique. En outre, on peut aborder avec la transformation de LAPLACE des problèmes plus étendus qu'avec le calcul symbolique et la méthode ne le cède en rien à la méthode opératoire quant à la rapidité et la simplicité du calcul. Ces faits ont été soulignés par un grand nombre d'auteurs [1]).

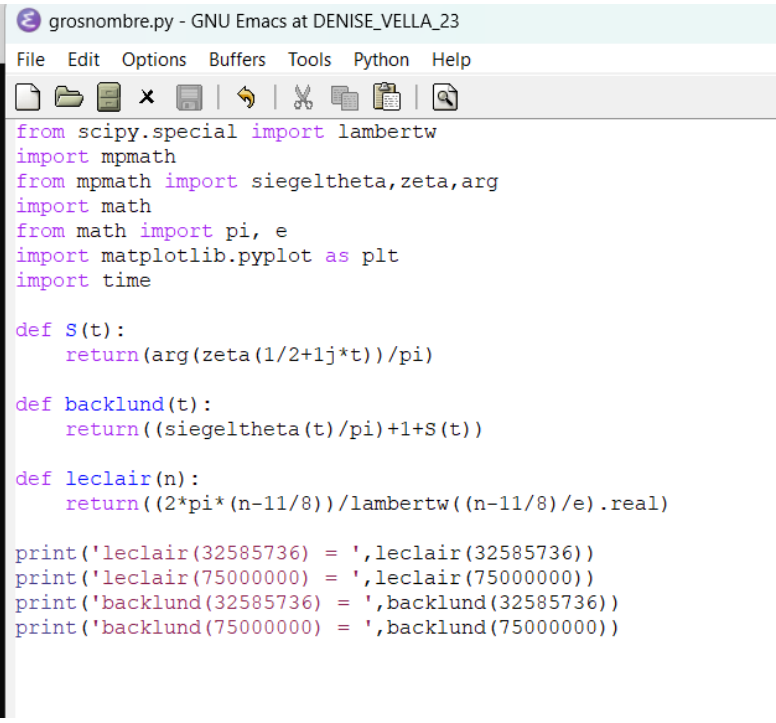
Appliquée à une équation différentielle ordinaire, la transformation de LAPLACE par rapport à la variable indépendante, la réduit en une équation algébrique, dans laquelle un paramètre a remplacé la variable indépendante. Considérons maintenant le cas des

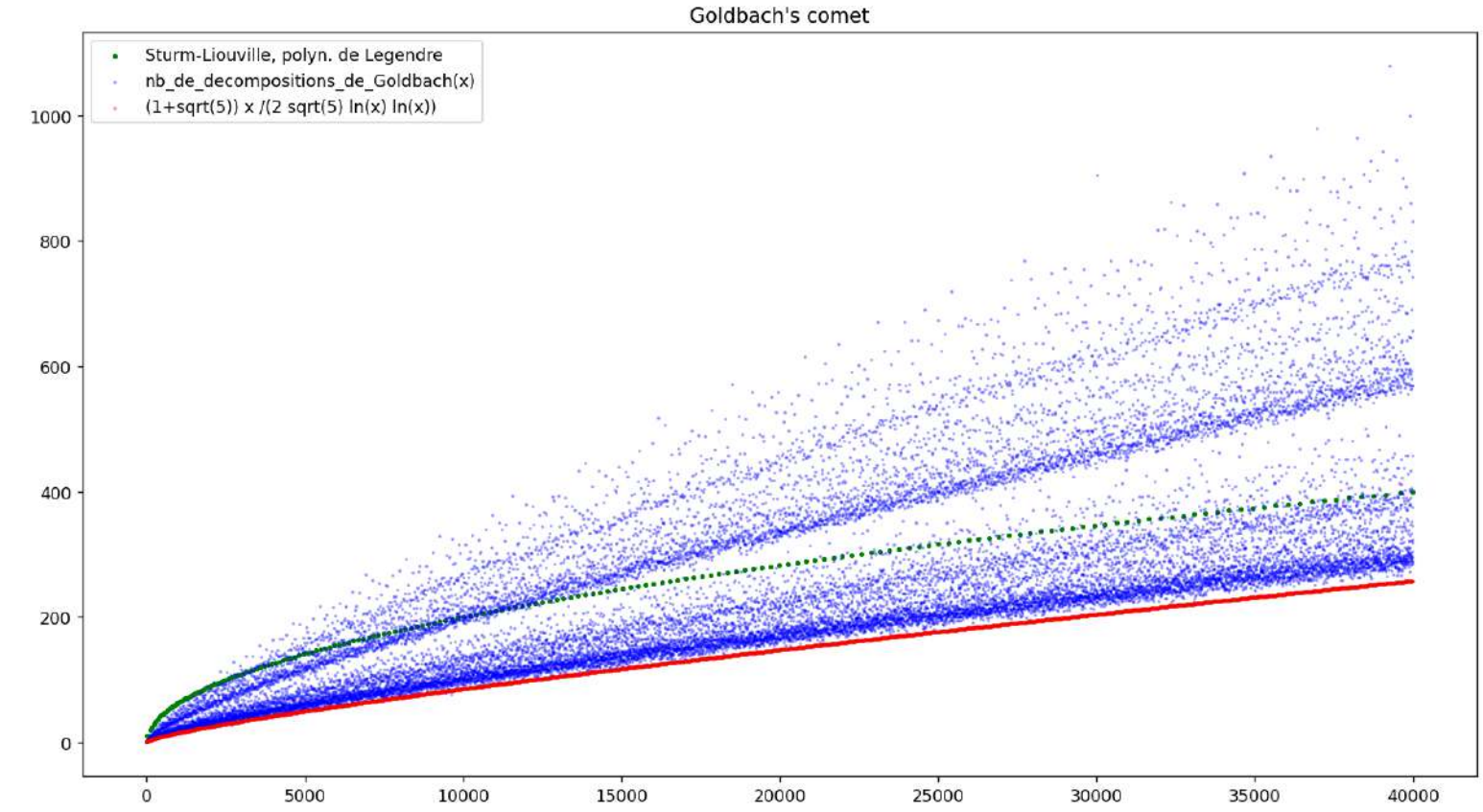

23
29
11
3
41
79
53
71
59

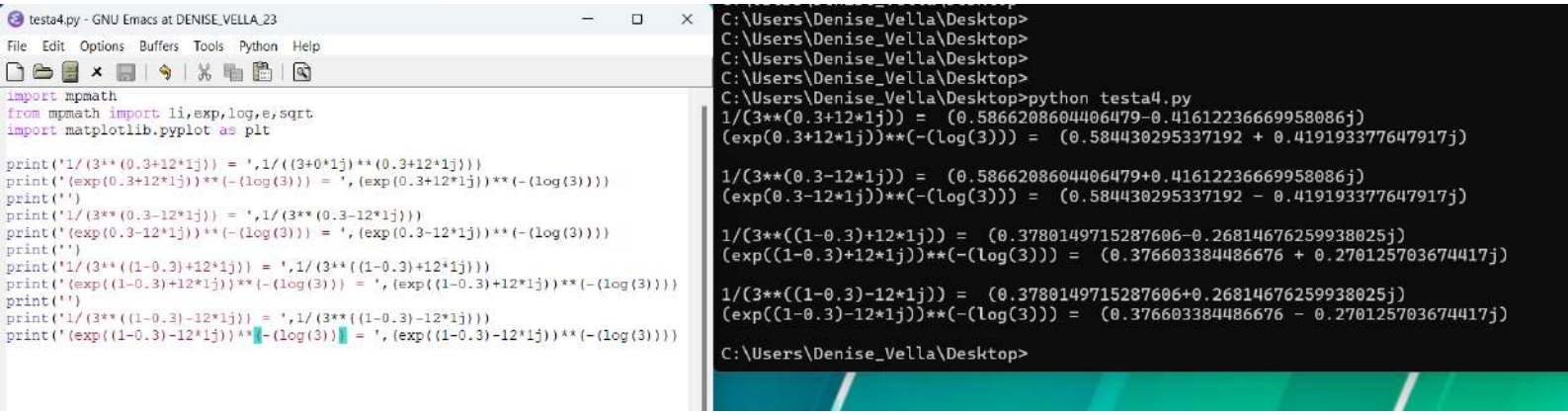

19
13
7
3
43
83
79
73
67


23
29
31dg
19dg
17
13
37dg
11
41
7
43
5
3
47
97
53
89
59
61dg
83
67dg
79dg
71
73


Invite de commandes
Microsoft Windows [version 10.0.22631.4460]
(c) Microsoft Corporation. Tous droits réservés.
C:\Users\Denise_Vella>cd Desktop
C:\Users\Denise_Vella\Desktop>python grosnombre.py
leclair(32585736) = 14963018.950572561
leclair(75000000) = 32585736.19707141
backlund(32585736) = 74999999.0
backlund(75000000) = 182572066.0
C:\Users\Denise_Vella\Desktop>


grosnombre.py - GNU Emacs at DENISE_VELLA_23
File Edit Options Buffers Tools Python Help
from scipy.special import lambertw
import mpmath
from mpmath import siegeltheta,zeta,arg
import math
from math import pi, e
import matplotlib.pyplot as plt
import time
def S(t):
return(arg(zeta(1/2+1j*t))/pi)
def backlund(t):
return((siegeltheta(t)/pi)+1+S(t))
def leclair(n):
return((2*pi*(n-11/8))/lambertw((n-11/8)/e).real)
print('leclair(32585736) = ',leclair(32585736))
print('leclair(75000000) = ',leclair(75000000))
print('backlund(32585736) = ',backlund(32585736))
print('backlund(75000000) = ',backlund(75000000))


Goldbach's comet
Sturm-Liouville, polyn. de Legendre
nb_de_decompositions_de_Goldbach(x)
(1+sqrt(5)) x /(2 sqrt(5) ln(x) ln(x))
1000
800
600
400
200
0
0
5000
10000
15000
20000
25000
30000
35000
40000


testa4.py - GNU Emacs at DENISE_VELLA_23
File Edit Options Buffers Tools Python Help
import mpmath
from mpmath import li,exp,log,e,sqrt
import matplotlib.pyplot as plt
print('1/(3**(0.3+12*1j)) = ',1/((3+0*1j)**(0.3+12*1j)))
print('(exp(0.3+12*1j))**(-(log(3))) = ',(exp(0.3+12*1j))**(-(log(3))))
print('')
print('1/(3**(0.3-12*1j)) = ',1/(3**(0.3-12*1j)))
print('(exp(0.3-12*1j))**(-(log(3))) = ',(exp(0.3-12*1j))**(-(log(3))))
print('')
print('1/(3**((1-0.3)+12*1j)) = ',1/(3**((1-0.3)+12*1j)))
print('(exp((1-0.3)+12*1j))**(-(log(3))) = ',(exp((1-0.3)+12*1j))**(-(log(3))))
print('')
print('1/(3**((1-0.3)-12*1j)) = ',1/(3**((1-0.3)-12*1j)))
print('(exp((1-0.3)-12*1j))**(-(log(3))) = ',(exp((1-0.3)-12*1j))**(-(log(3))))
C:\Users\Denise_Vella\Desktop>
C:\Users\Denise_Vella\Desktop>
C:\Users\Denise_Vella\Desktop>
C:\Users\Denise_Vella\Desktop>
C:\Users\Denise_Vella\Desktop>python testa4.py
1/(3**(0.3+12*1j)) = (0.5866208604406479-0.41612236669958086j)
(exp(0.3+12*1j))**(-(log(3))) = (0.584430295337192 + 0.4191933776479 17j)
1/(3**(0.3-12*1j)) = (0.5866208604406479+0.41612236669958086j)
(exp(0.3-12*1j))**(-(log(3))) = (0.584430295337192 - 0.4191933776479 17j)
1/(3**((1-0.3)+12*1j)) = (0.3780149715287606-0.26814676259938025j)
(exp((1-0.3)+12*1j))**(-(log(3))) = (0.376603384486676 + 0.2701257036744 17j)
1/(3**((1-0.3)-12*1j)) = (0.3780149715287606+0.26814676259938025j)
(exp((1-0.3)-12*1j))**(-(log(3))) = (0.376603384486676 - 0.2701257036744 17j)
C:\Users\Denise_Vella\Desktop>

$$\xi(t) = 4\int_1^{\infty} \frac{d\left[x^{\frac{3}{2}}\psi'(x)\right]}{dx} x^{-\frac{1}{4}} \cos\left(\frac{1}{2}t\log x\right) dx$$

Cette fonction est finie pour toutes les valeurs finies de t et peut être développée suivant les puissances de t^2 en une série qui converge très rapidement. Puisque, pour une valeur s de dont la partie réelle est plus grande que 1, $\log \zeta(x) = -\sum \log(1 - p^{-s})$ reste fini et que ce même fait a lieu pour les logarithmes des facteurs restants de $\xi(t)$, la fonction $\xi(t)$ peut seulement s'évanouir lorsque la partie imaginaire de t se trouve comprise entre $\frac{1}{2}i$ et $-\frac{1}{2}i$. Le nombre de racines de $\xi(t) = 0$ dont les parties réelles sont comprises entre 0 et T est environ égal à

$$\frac{T}{2\pi}\log\frac{T}{2\pi} - \frac{T}{2\pi}$$

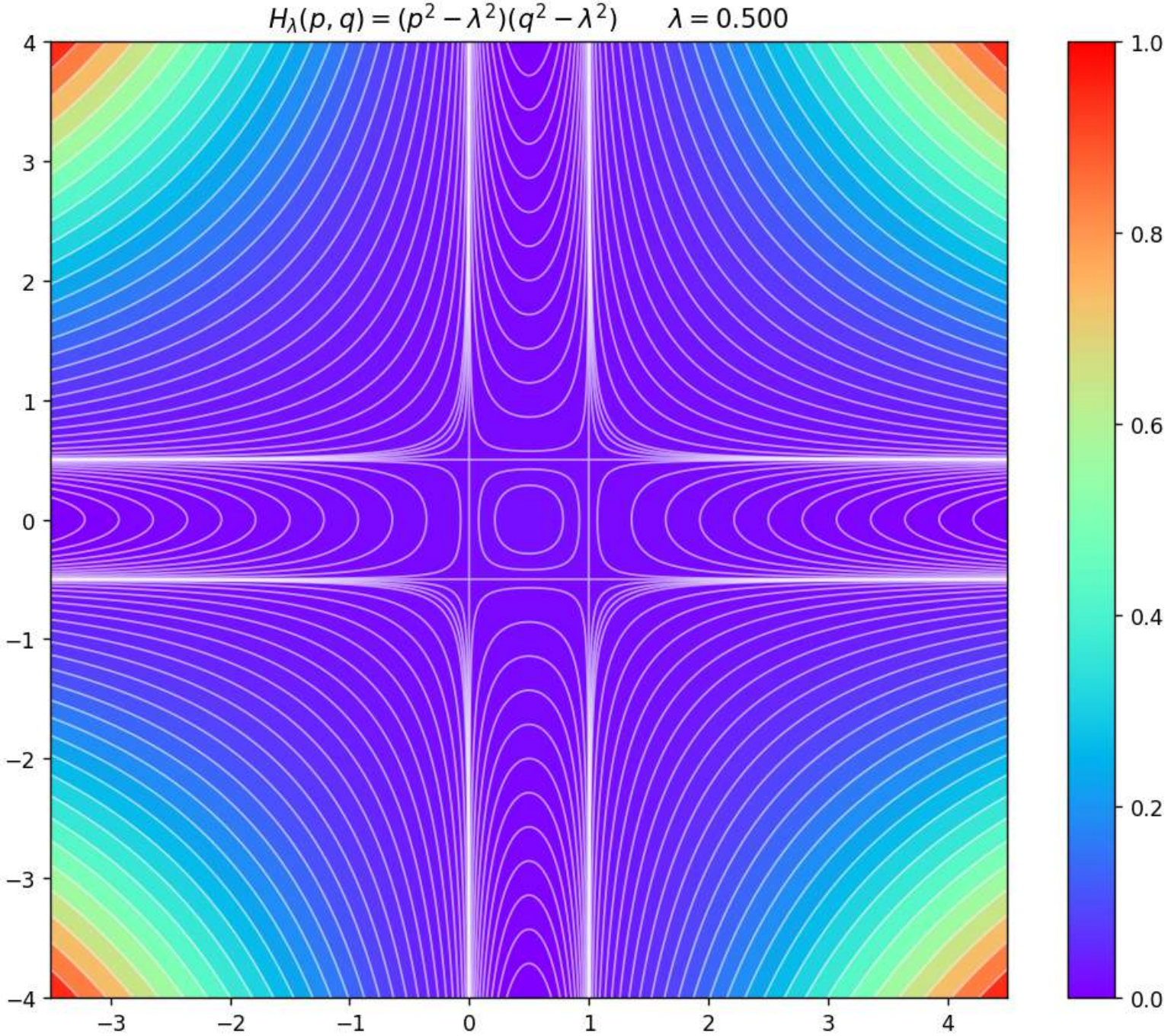
car l'intégrale $\int d \log \xi(t)$ prise le long d'un contour décrit dans le sens positif, comprenant à son intérieur l'ensemble des valeurs de t dont les parties imaginaires sont comprises entre $\frac{1}{2}i$ et $-\frac{1}{2}i$ et les parties réelles entre 0 et T est égale (abstraction faite d'une partie fractionnaire de même ordre de grandeur que la grandeur $\frac{1}{T}$) à $(T\log\frac{T}{2\pi} - T)i$; or cette intégrale est égale au nombre de racines de $\xi(t) = 0$ situées dans ce domaine, multiplié par $2\pi i$. On trouve, en effet, entre ces limites un nombre environ égal à celui-ci, de racines réelles, et il est très probable que toutes les racines sont réelles[4].

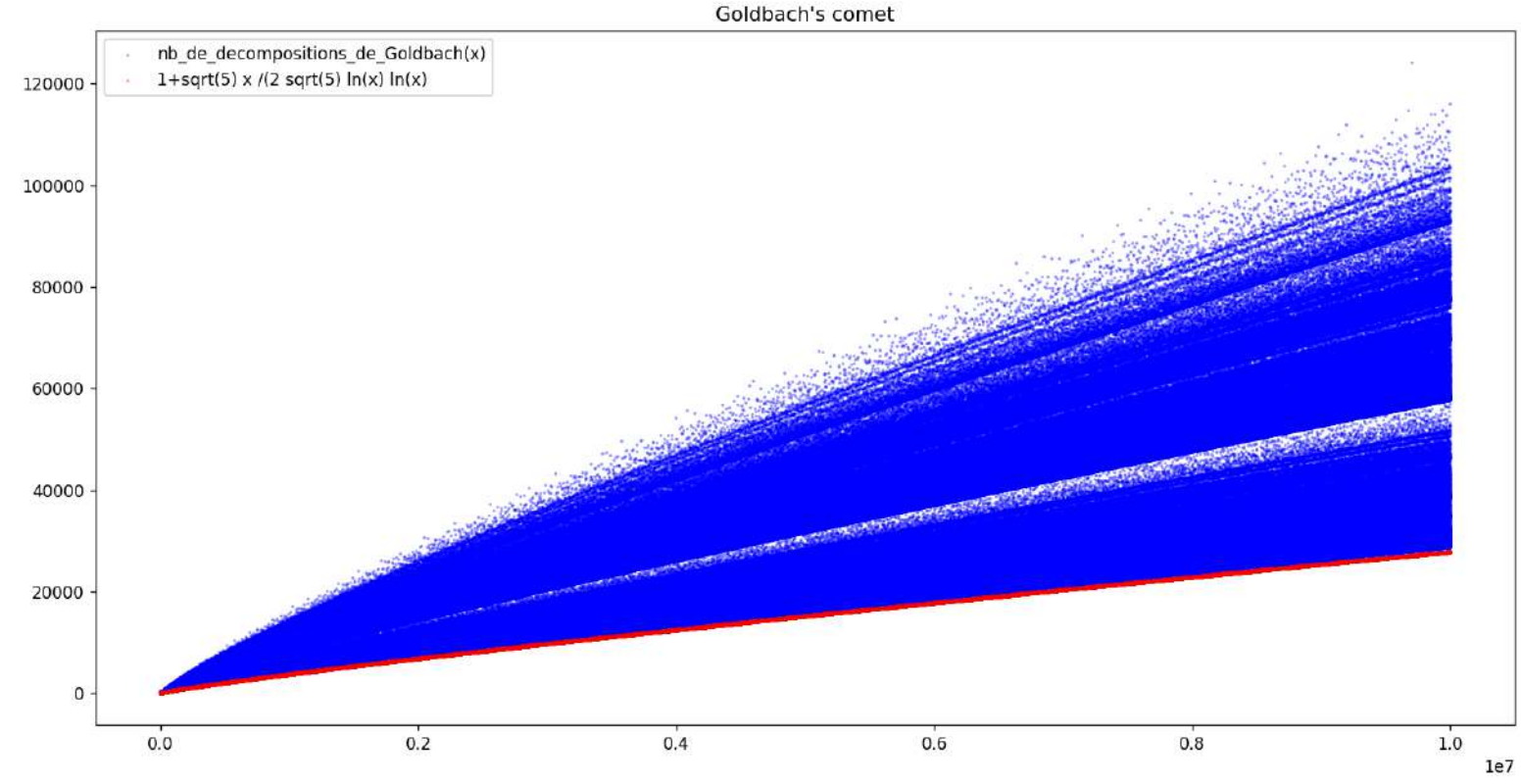
Il serait à désirer, sans doute, que l'on eût une démonstration rigoureuse de cette proposition ; néanmoins j'ai laissé cette recherche de côté pour le moment après quelques rapides essais infructueux, car elle paraît superflue pour le but immédiat de mon étude.

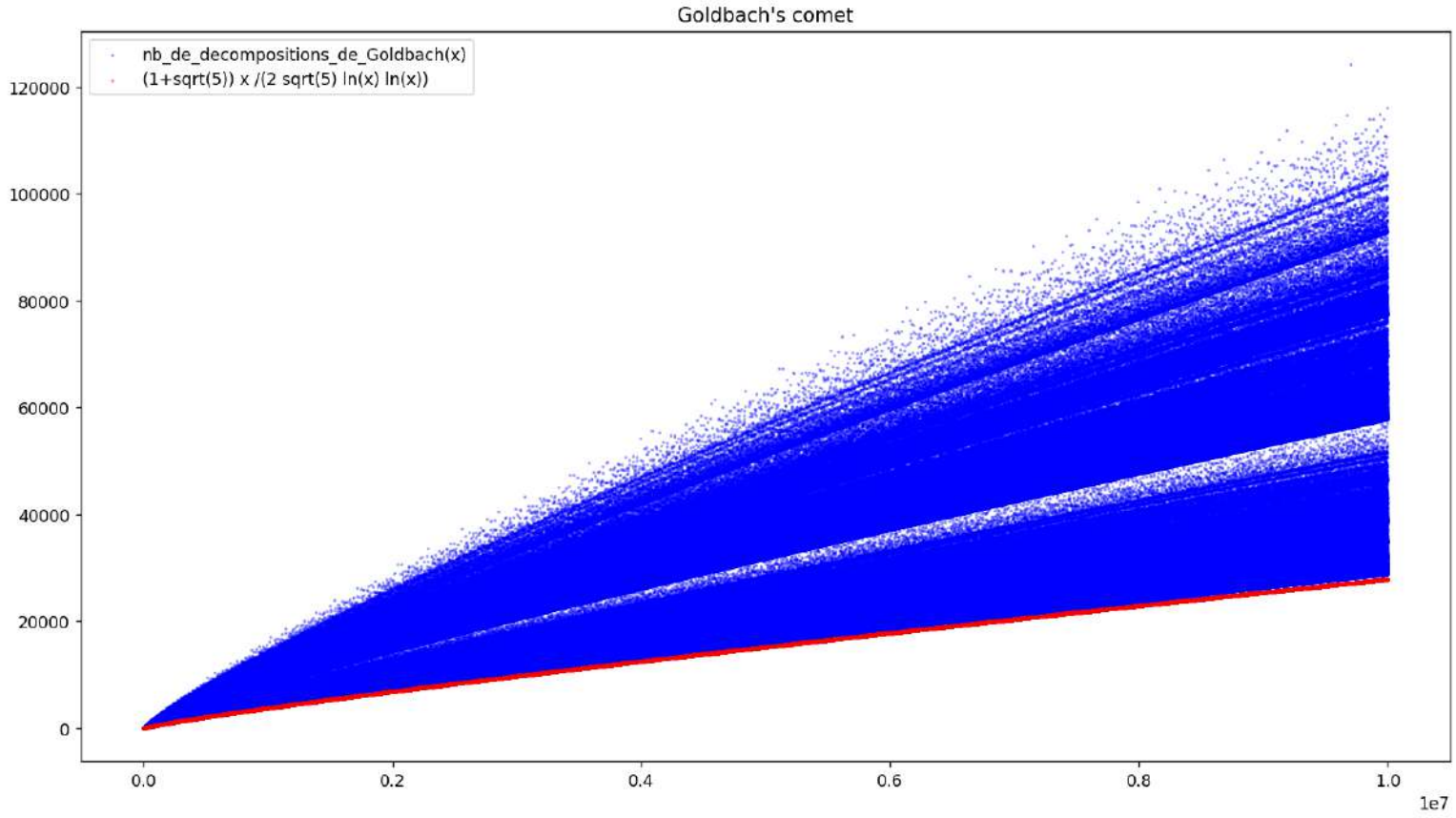
Si l'on désigne par α toute racine de l'équation $\xi(\alpha) = 0$, on peut exprimer $\log \xi(t)$ par

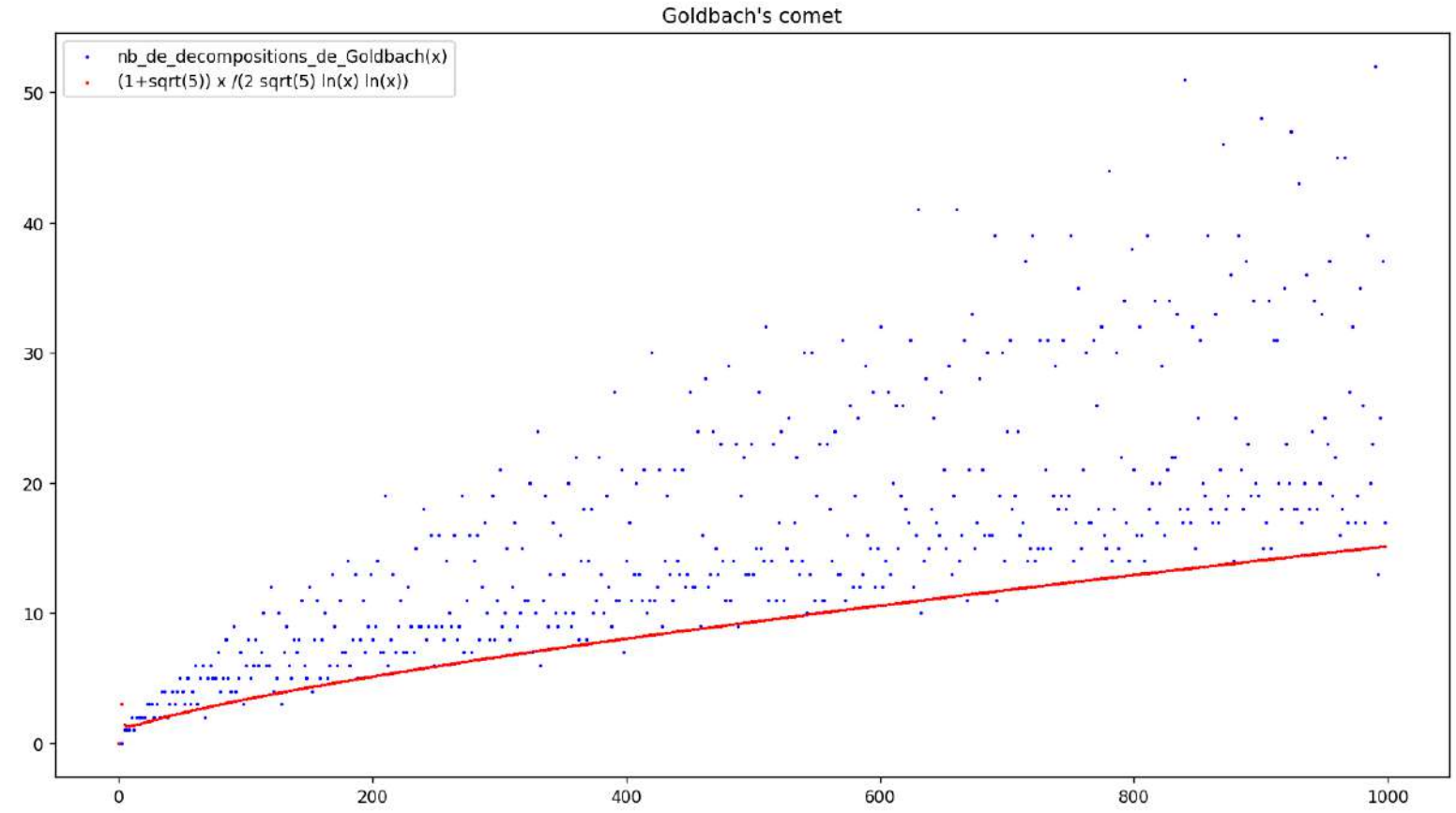
$$\sum \log\left(1 - \frac{t^2}{\alpha^2}\right) + \log \xi(0)$$

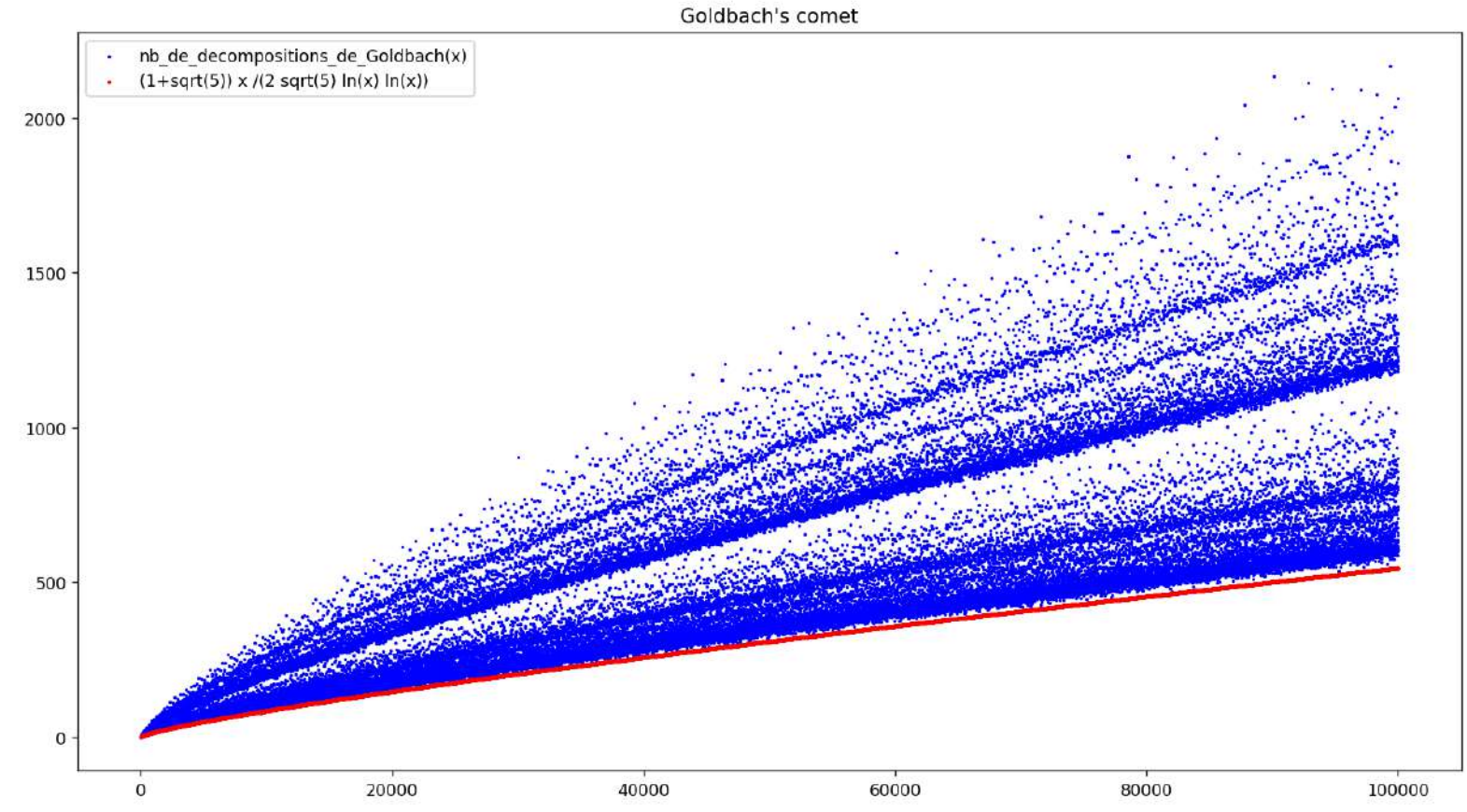
Ψ(x)=Σ_{n=1}^{infini} exp(−(n^2)πx)

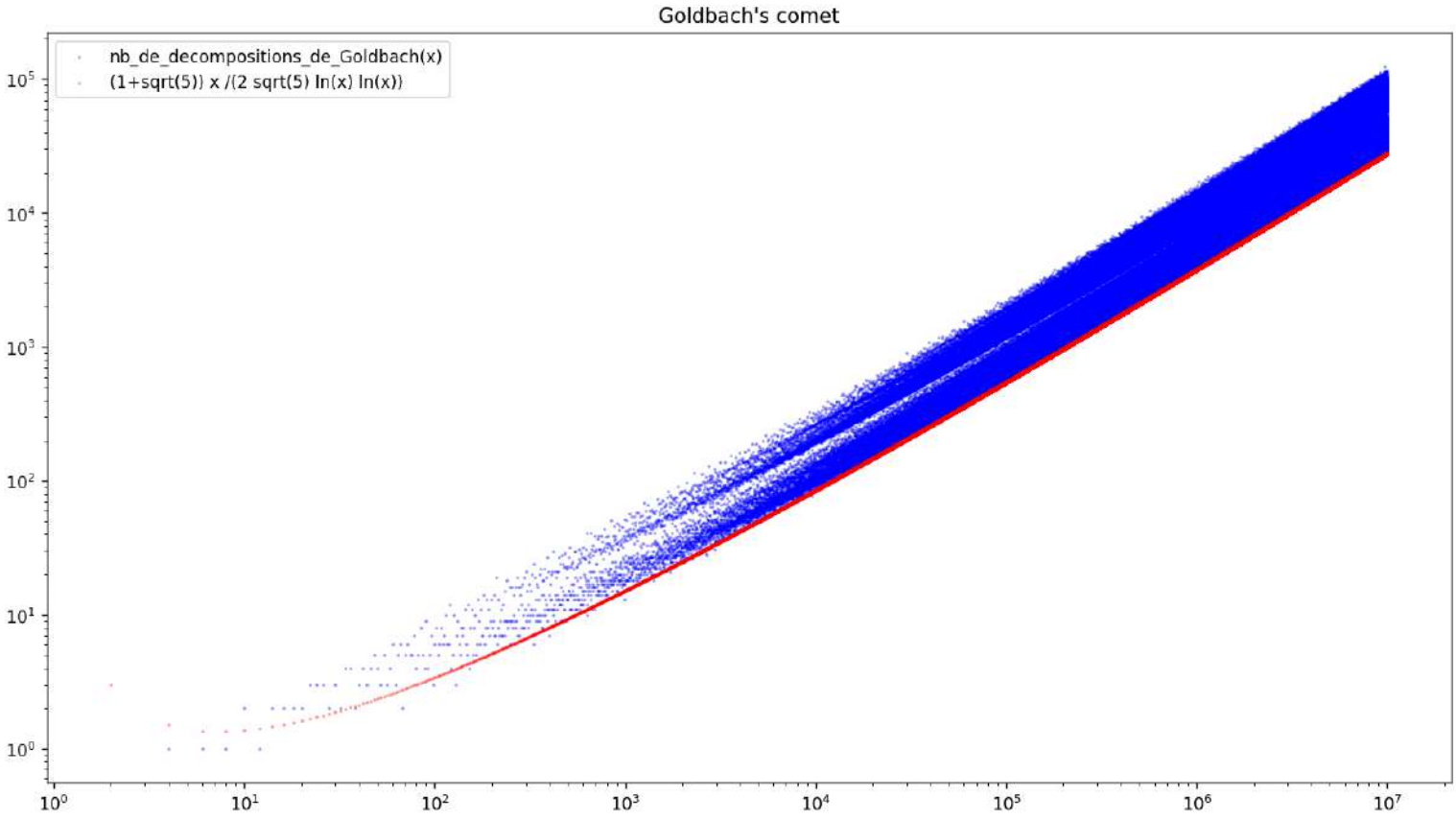

$H_\lambda(p,q) = (p^2 - \lambda^2)(q^2 - \lambda^2)$ $\lambda = 0.500$
4
3
2
1
0
−1
−2
−3
−4
−3
−2
−1
0
1
2
3
4
1.0
0.8
0.6
0.4
0.2
0.0

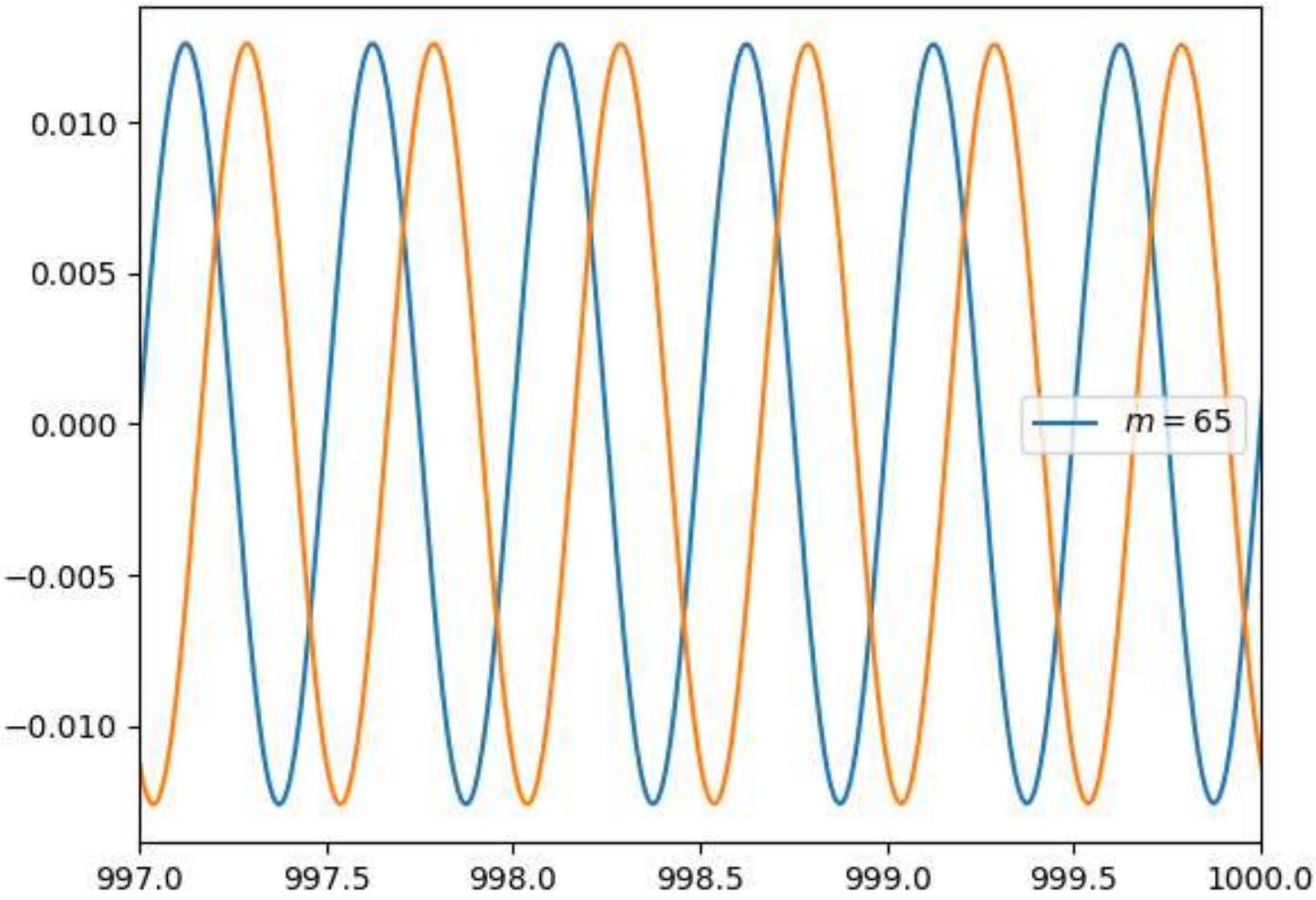

Goldbach's comet
nb_de_decompositions_de_Goldbach(x)
1+sqrt(5) x /(2 sqrt(5) ln(x) ln(x)
120000
100000
80000
60000
40000
20000
0
0.0
0.2
0.4
0.6
0.8
1.0
1e7

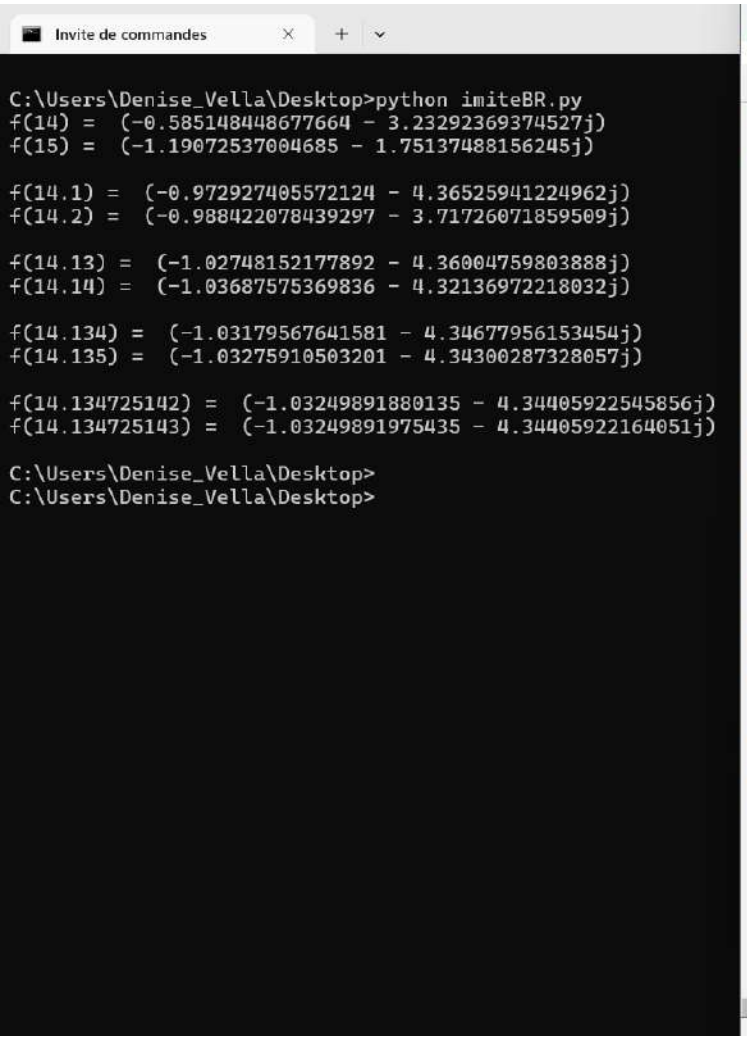

Goldbach's comet
nb_de_decompositions_de_Goldbach(x)
(1+sqrt(5)) x /(2 sqrt(5) ln(x) ln(x))
120000
100000
80000
60000
40000
20000
0
0.0
0.2
0.4
0.6
0.8
1.0
1e7

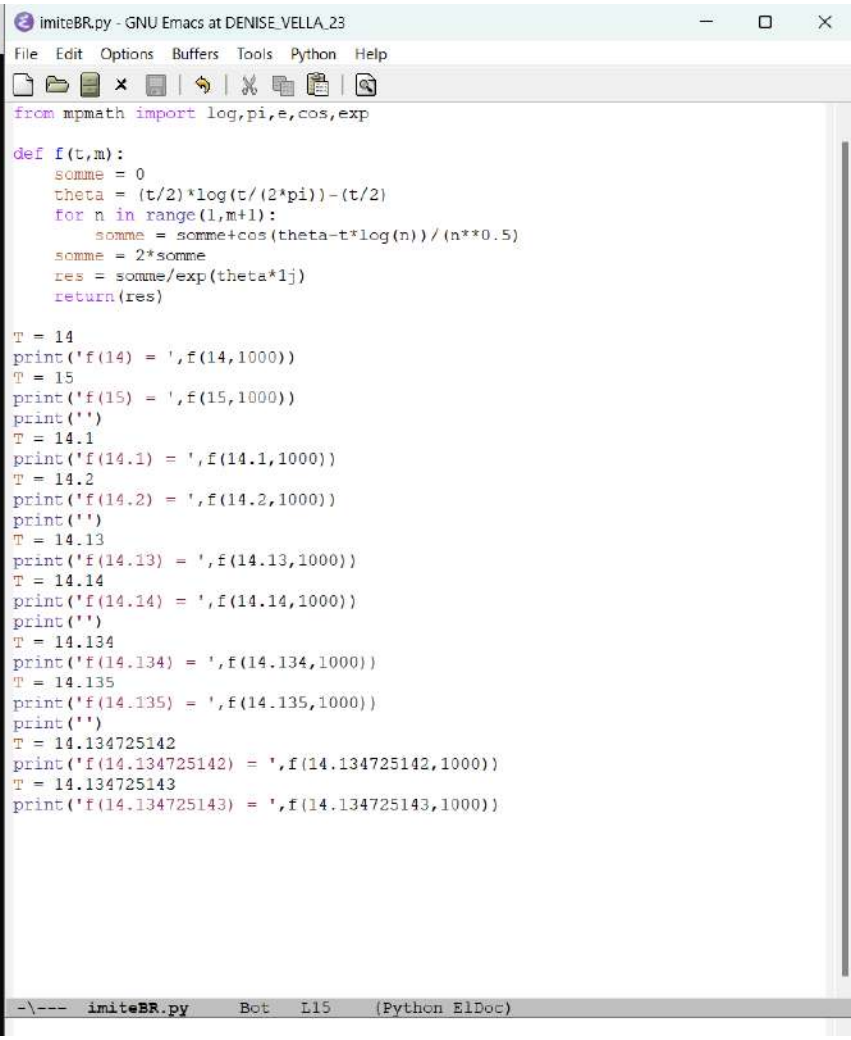

Goldbach's comet
nb_de_decompositions_de_Goldbach(x)
(1+sqrt(5)) x /(2 sqrt(5) ln(x) ln(x))
0
10
20
30
40
50
0
200
400
600
800
1000


Goldbach's comet
nb_de_decompositions_de_Goldbach(x)
(1+sqrt(5)) x /(2 sqrt(5) ln(x) ln(x))
2000
1500
1000
500
0
0
20000
40000
60000
80000
100000


Goldbach's comet
nb_de_decompositions_de_Goldbach(x)
(1+sqrt(5)) x /(2 sqrt(5) ln(x) ln(x))
10^5
10^4
10^3
10^2
10^1
10^0
10^0
10^1
10^2
10^3
10^4
10^5
10^6
10^7


0.010
0.005
0.000
−0.005
−0.010
997.0
997.5
998.0
998.5
999.0
999.5
1000.0
$m = 65$


Invite de commandes
C:\Users\Denise_Vella\Desktop>python imiteBR.py
f(14) = (-0.585148448677664 - 3.232923693745 27j)
f(15) = (-1.19072537004685 - 1.751374881562 45j)
f(14.1) = (-0.972927405572124 - 4.365259412249 62j)
f(14.2) = (-0.988422078439297 - 3.717260718595 09j)
f(14.13) = (-1.02748152177892 - 4.360047598038 88j)
f(14.14) = (-1.03687575369836 - 4.321369722180 32j)
f(14.134) = (-1.03179567641581 - 4.346779561534 54j)
f(14.135) = (-1.03275910503201 - 4.343002873280 57j)
f(14.134725142) = (-1.03249891880135 - 4.344059225458 56j)
f(14.134725143) = (-1.03249891975435 - 4.344059221640 51j)
C:\Users\Denise_Vella\Desktop>
C:\Users\Denise_Vella\Desktop>


imiteBR.py - GNU Emacs at DENISE_VELLA_23
File Edit Options Buffers Tools Python Help
from mpmath import log,pi,e,cos,exp
def f(t,m):
somme = 0
theta = (t/2)*log(t/(2*pi))-(t/2)
for n in range(1,m+1):
somme = somme+cos(theta-t*log(n))/(n**0.5)
somme = 2*somme
res = somme/exp(theta*1j)
return(res)
T = 14
print('f(14) = ',f(14,1000))
T = 15
print('f(15) = ',f(15,1000))
print('')
T = 14.1
print('f(14.1) = ',f(14.1,1000))
T = 14.2
print('f(14.2) = ',f(14.2,1000))
print('')
T = 14.13
print('f(14.13) = ',f(14.13,1000))
T = 14.14
print('f(14.14) = ',f(14.14,1000))
print('')
T = 14.134
print('f(14.134) = ',f(14.134,1000))
T = 14.135
print('f(14.135) = ',f(14.135,1000))
print('')
T = 14.134725142
print('f(14.134725142) = ',f(14.134725142,1000))
T = 14.134725143
print('f(14.134725143) = ',f(14.134725143,1000))
-\--- imiteBR.py Bot L15 (Python ElDoc)

PETIT ESSAI SUR LES LOGARITHMES

Dans les copies de Mathématiques Spéciales de Galois, plusieurs pages sont consacrées aux logarithmes. Une autre allusion aux logarithmes figure dans un cahier où le jeune mathématicien a consigné quelques premiers essais :

«On peut rattacher la théorie des logarithmes népériens aux considérations de l'arithmétique élémentaire. En effet, on sait qu'un franc placé à l'intérêt de *a* pour 1 dans un an augmente différemment suivant que les intervalles par rapport auxquels on prend les intérêts des intérêts sont plus ou moins rapprochés. Par exemple, si on prenait les intérêts de mois en mois, le franc au bout d'un an vaudrait :

$$\left(1 + \frac{a}{12}\right)^{12} \text{ franc}$$

Si on les prenait de jour en jour, le franc au bout d'un an vaudrait :

$$\left(1 + \frac{a}{365}\right)^{365} \text{ franc}$$

Or il est curieux de voir quelle est la limite que l'on ne peut dépasser, à quelque peu de distance que l'on prenne les intérêts. D'après ce qui précède, cette limite sera :

$$e^a = \lim \left(1 + \frac{a}{n}\right)^n .»$$

Un colloque international à l'IHP

Après-midi grand public à l'Institut Océanographique
- Programme de l'après-midi
- Inscription à l'après-midi grand public

Exposition à la bibliothèque de l'IHP

Et aussi…

Participez vous aussi à la fête galoisienne

- A propos du bicentenaire
- Inscrivez-vous
- Nous contacter
- Remerciements

Après-midi grand public à l'Institut Océanographique

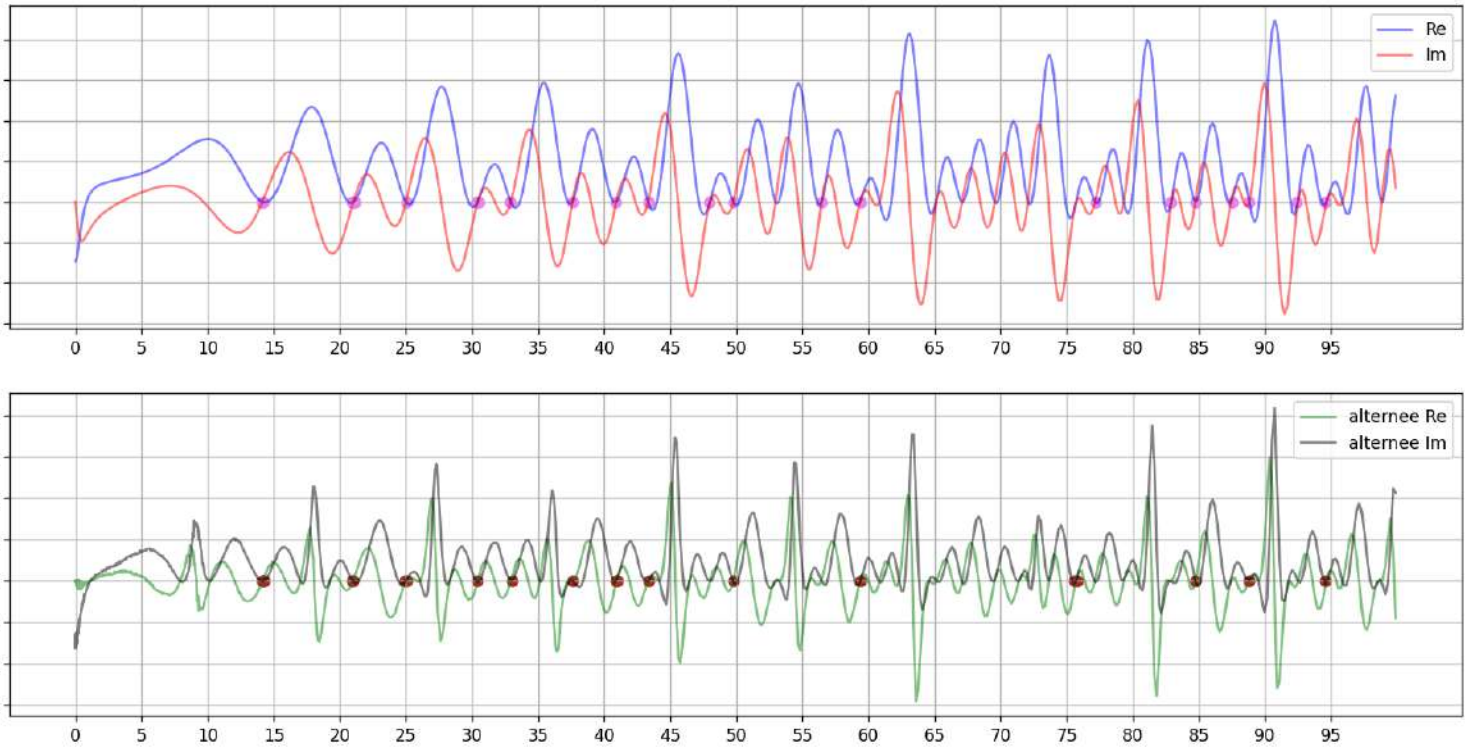
L'Institut Henri Poincaré et la Société Mathématique de France organisent ensemble une après-midi grand public à l'Institut Océanographique (195 Rue Saint-Jacques, 75005 Paris) le mercredi 26 octobre.

Des exposés mathématiques et historiques, une table ronde, une projection d'un court-métrage et un spectacle de clown agrémenteront cette après-midi. Le programme détaillé est disponible ici.

L'inscription est recommandée.

Remerciements

Nous remercions tous nos partenaires.


Re
Im
alternee Re
alternee Im

rescossinnp - GNU Emacs at DENISE_VELLA_23

File Edit Options Buffers Tools Help

```
avec des cosinus
3+3
3+5
5+5
5+7
7+7
5+11
5+13 = 7+11
7+13
5+17 = 11+11
5+19 = 7+17 = 11+13
7+19 = 13+13
11+17
7+23 = 11+19 = 13+17
13+19
11+23 = 17+17
7+29 = 13+23 = 17+19
7+31 = 19+19
11+29 = 17+23
11+31 = 13+29 = 19+23
7+37 = 13+31
17+29 = 23+23
7+41 = 11+37 = 17+31 = 19+29
13+37 = 19+31
11+41 = 23+29
11+43 = 13+41 = 17+37 = 23+31
13+43 = 19+37
11+47 = 17+41 = 29+29
13+47 = 17+43 = 19+41 = 23+37 = 29+31
19+43 = 31+31
11+53 = 17+47 = 23+41
13+53 = 19+47 = 23+43 = 29+37
31+37
11+59 = 17+53 = 23+47 = 29+41
11+61 = 13+59 = 19+53 = 29+43 = 31+41
13+61 = 31+43 = 37+37
17+59 = 23+53 = 29+47
11+67 = 17+61 = 19+59 = 31+47 = 37+41
13+67 = 19+61 = 37+43
11+71 = 23+59 = 29+53 = 41+41
11+73 = 13+71 = 17+67 = 23+61 = 31+53 = 37+47 = 41+43
13+73 = 19+67 = 43+43
17+71 = 29+59 = 41+47
11+79 = 17+73 = 19+71 = 23+67 = 29+61 = 31+59 = 37+53 = 43+47
```

-\--- **rescossinnp** Top L18 (Fundamental)

cossinnp.py - GNU Emacs at DENISE_VELLA_23

File Edit Options Buffers Tools Python Help

```python
import numpy as np

nmax = 92
print('avec des cosinus ')
for n in range(6, nmax, 2):
    m = int(np.floor(np.sqrt(n)))
    r = np.arange(2, m+1)
    c = np.cos(np.pi*n/r)
    s = []
    for x in range(3, n//2+1):
        produit = np.prod(c - np.cos(np.pi*(n-2*x)/r))
        if abs(produit) > 1e-6:
            s += [f'{x}+{n-x}']
    print(' = '.join(s))

print('avec des sinus ')
for n in range(6, nmax, 2):
    m = int(np.floor(np.sqrt(n)))
    r = np.arange(2, m+1)
    c = np.cos(np.pi*n/r)
    s = []
    for x in range(3, n//2+1):
        produit = np.prod((-2)*np.sin(np.pi*(n-x)/r)*np.sin(np.pi*x/r))
        if abs(produit) > 1e-6:
            s += [f'{x}+{n-x}']
    print(' = '.join(s))
```

-\--- **cossinnp.py** All L15 (Python ElDoc)

(No changes need to be saved)

6 A Final Pair of Expansions

The iterations (76–77) may be used to show that $W(z)$ can be written as

$$W(z) = \cfrac{z}{\exp\cfrac{z}{\exp\cfrac{z}{\exp\cfrac{z}{\ddots}}}} \tag{98}$$

or

$$W(z) = \ln\cfrac{z}{\ln\cfrac{z}{\ln\cfrac{z}{\ddots}}} \tag{99}$$

according as $|W(z)| < 1$ or $|W(z)| > 1$. These curious formulae are just the iterated exponential in disguise, and indeed are naturally discovered from rewriting $W(z) = z/\exp W(z)$ and $W(z) = \ln(z/W(z))$ as iterations.

LECTURE SERIES

Mathematical Science Literature

November 23, 2020

8:00am ET- *Virtually*

Alain Connes
Collège de France

"Noncommutative Geometry, the Spectral Aspect"

This talk will be a survey of the spectral side of noncommutative geometry, presenting the new paradigm of spectral triples and showing its relevance for the fine structure of space-time, its large scale structure and also in number theory in connection with the zeros of the Riemann zeta function.

Talk chair: Peter Kronheimer

This lecture will be held virtually.
Click here to register

cmsa.fas.harvard.edu/literature-lecture-series/

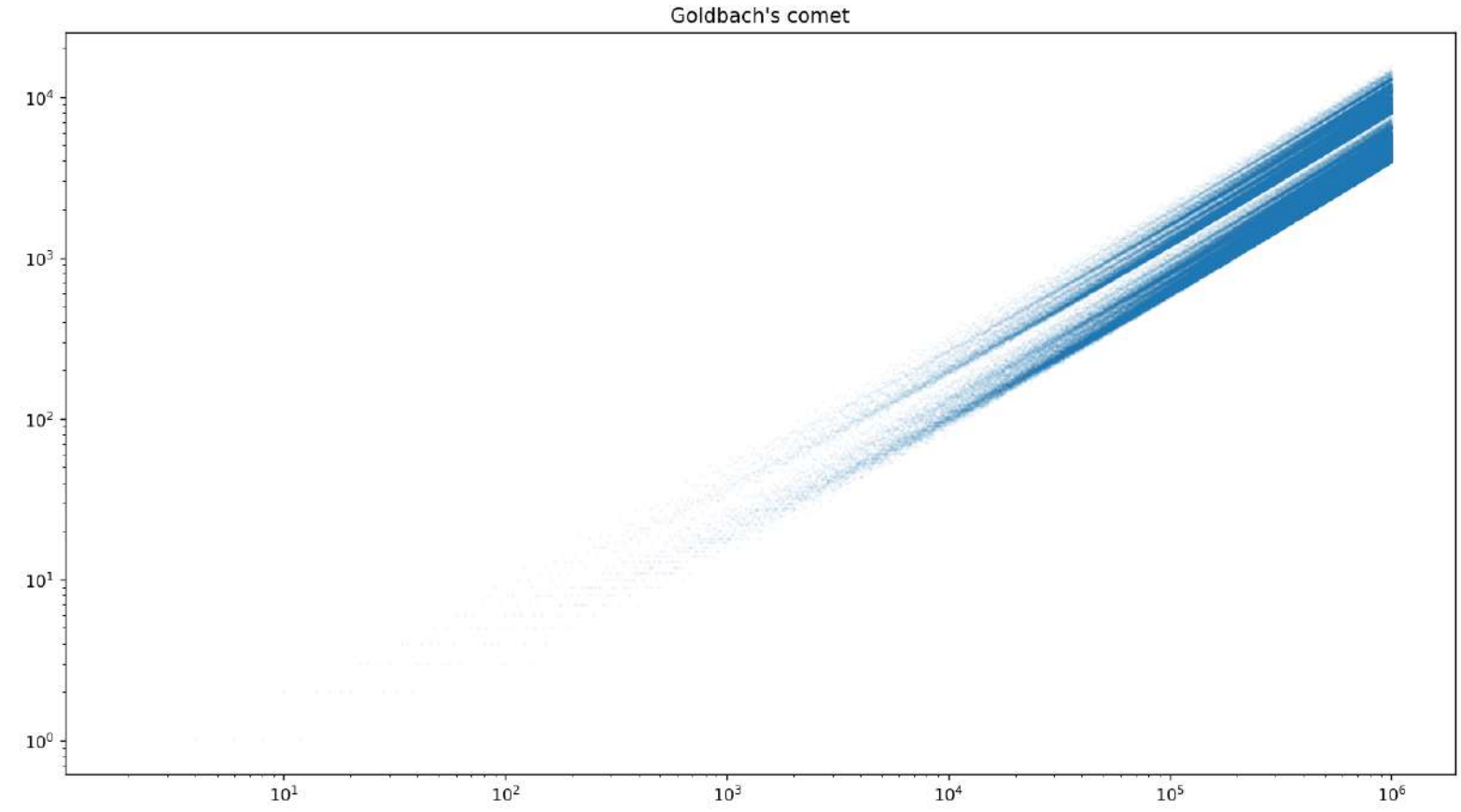
SCIENCE

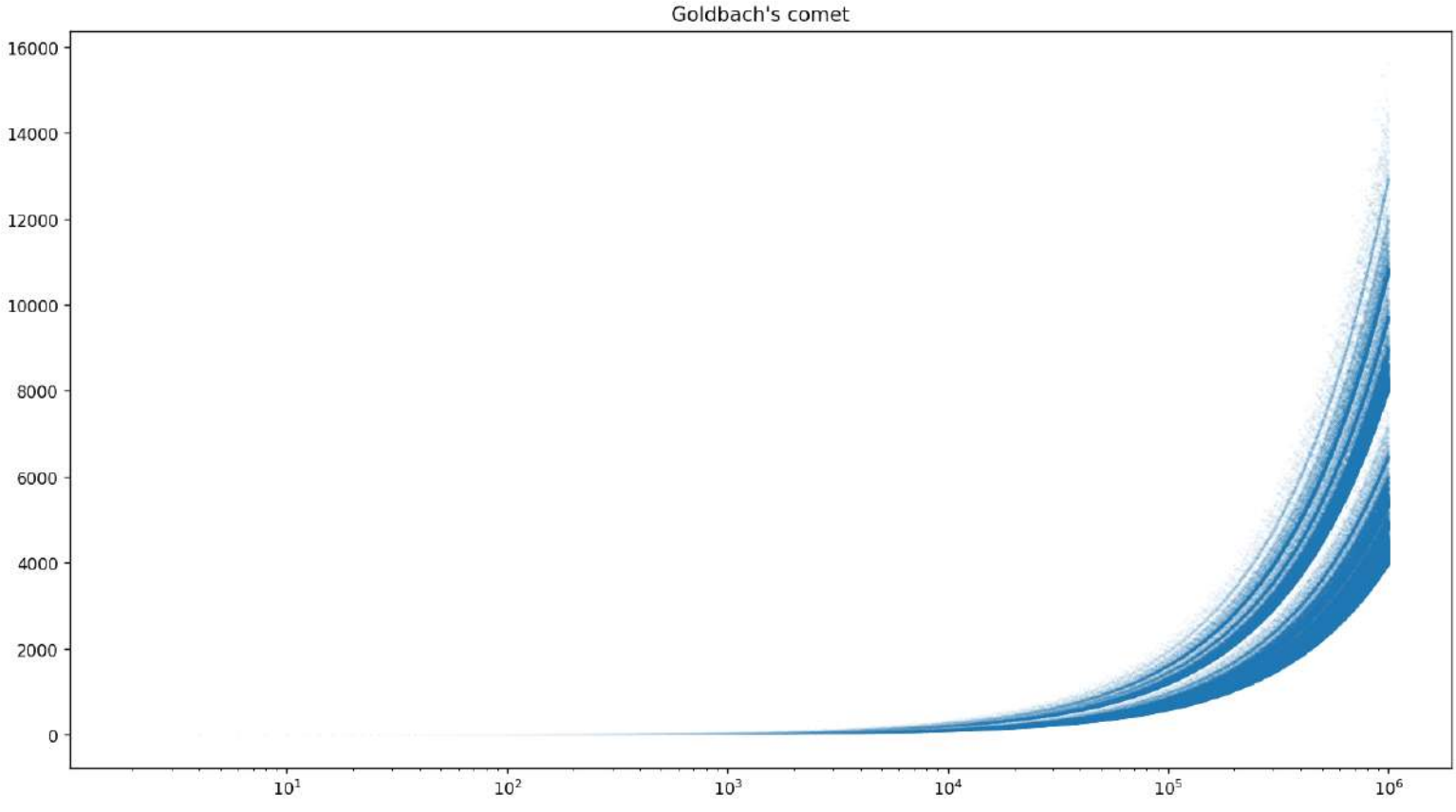
LES GÉNIES DE LA SCIENCE

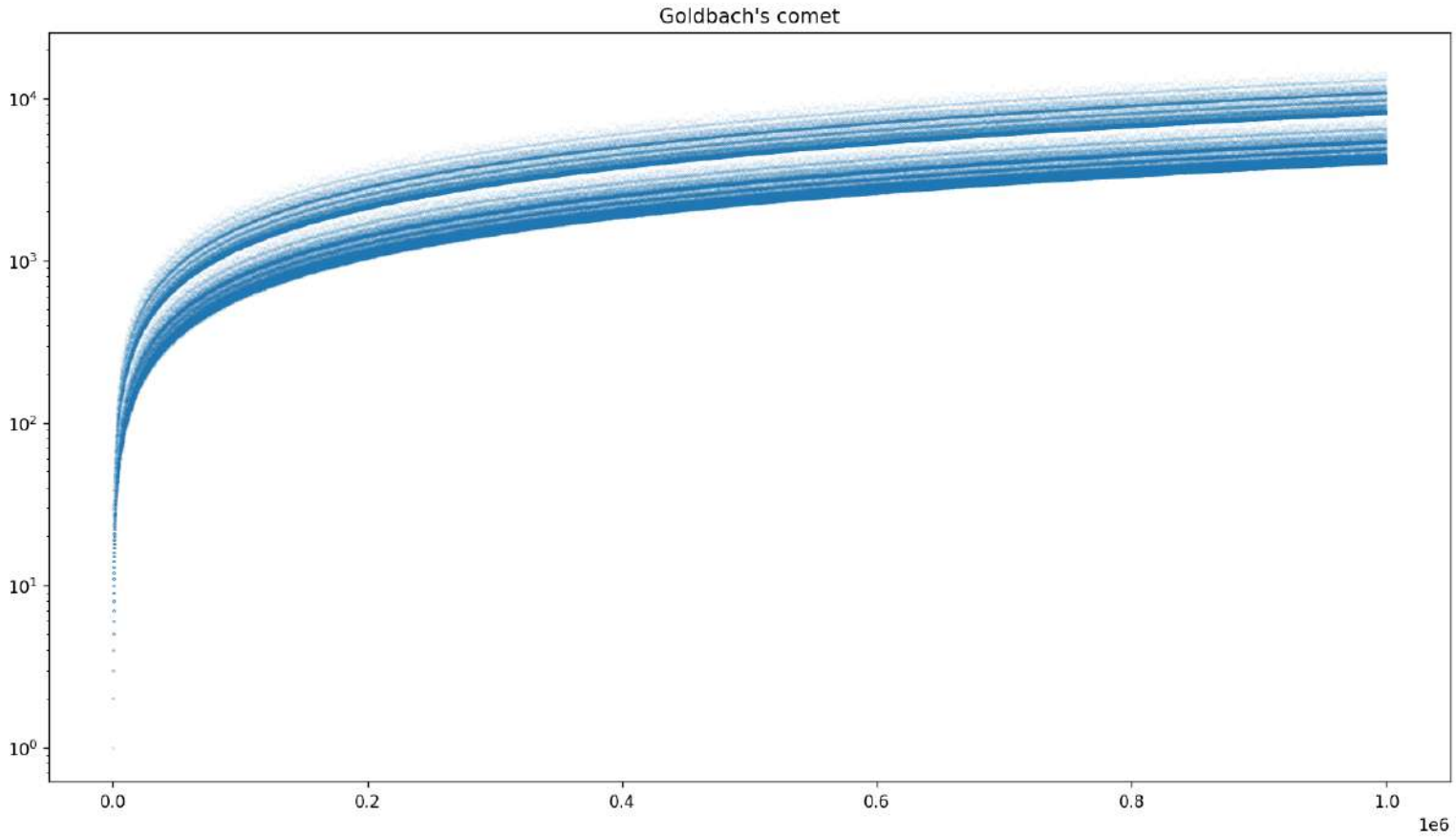
Évariste Galois

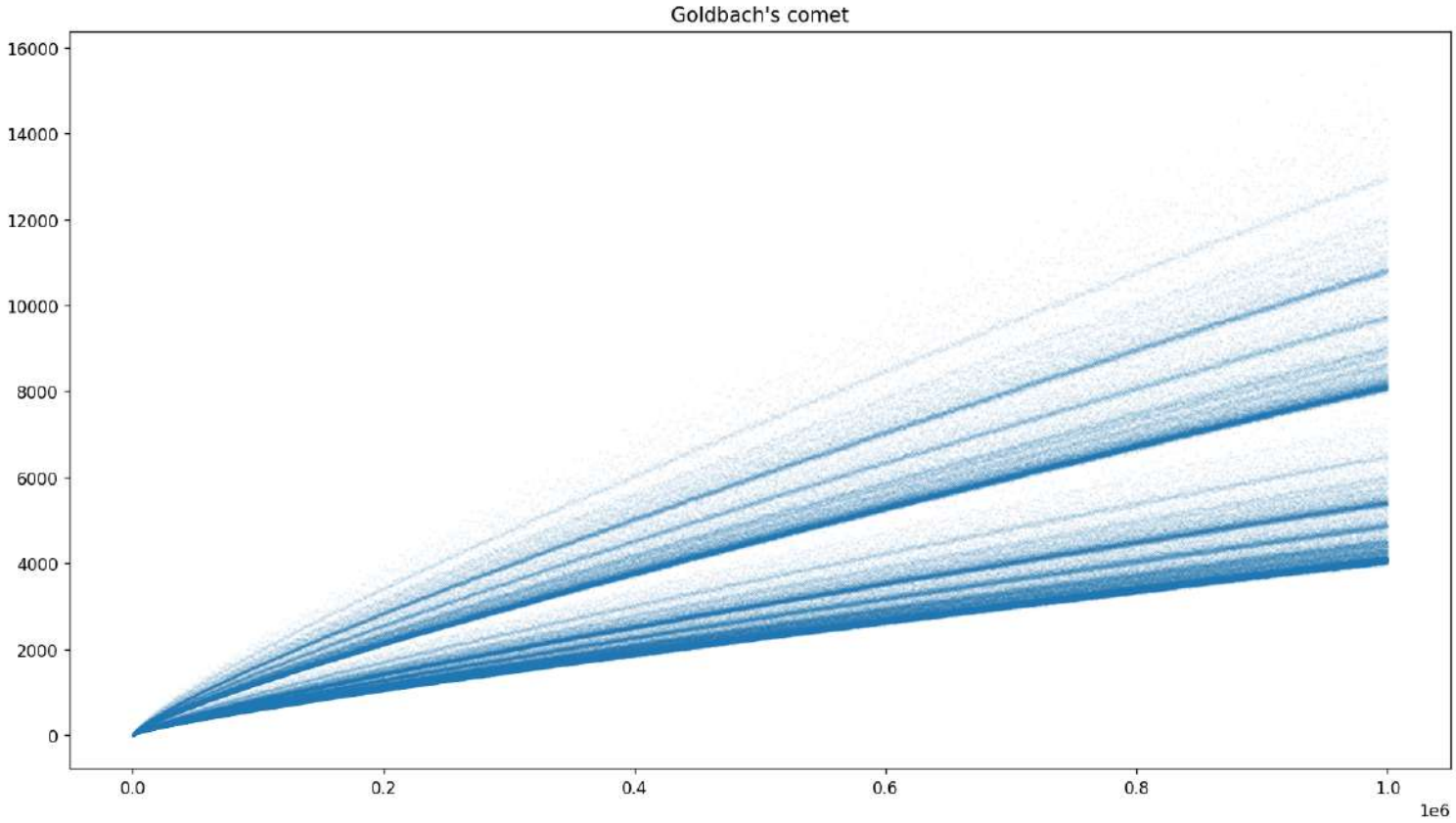
Le mathématicien maudit

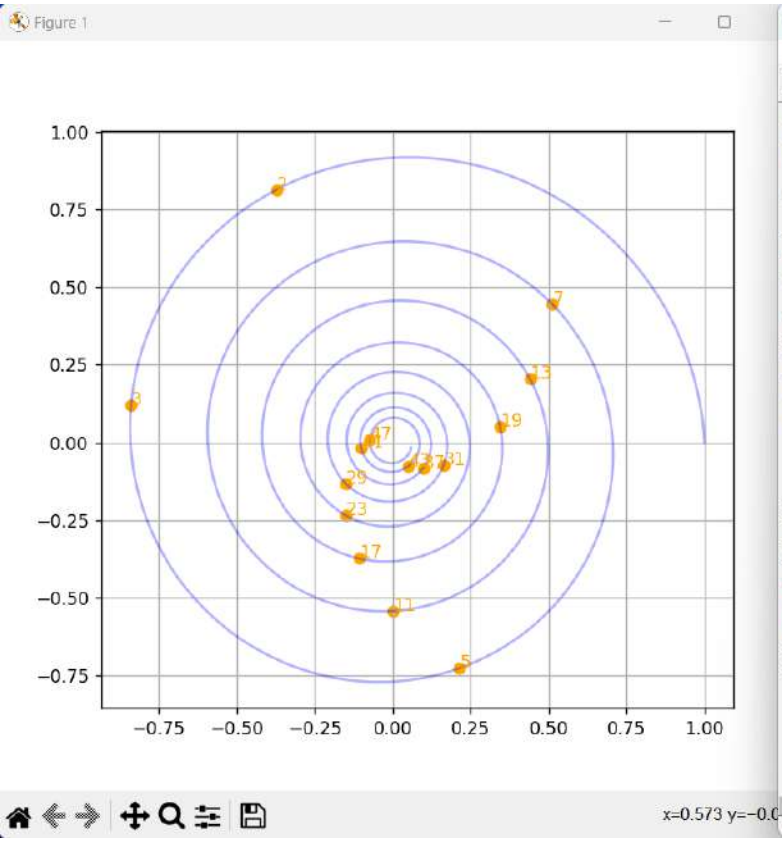
N°14


Goldbach's comet
10^4
10^3
10^2
10^1
10^0
10^1
10^2
10^3
10^4
10^5
10^6


Goldbach's comet
16000
14000
12000
10000
8000
6000
4000
2000
0
10^1
10^2
10^3
10^4
10^5
10^6


Goldbach's comet
10^4
10^3
10^2
10^1
10^0
0.0
0.2
0.4
0.6
0.8
1.0
1e6


Goldbach's comet
16000
14000
12000
10000
8000
6000
4000
2000
0
0.0
0.2
0.4
0.6
0.8
1.0
1e6



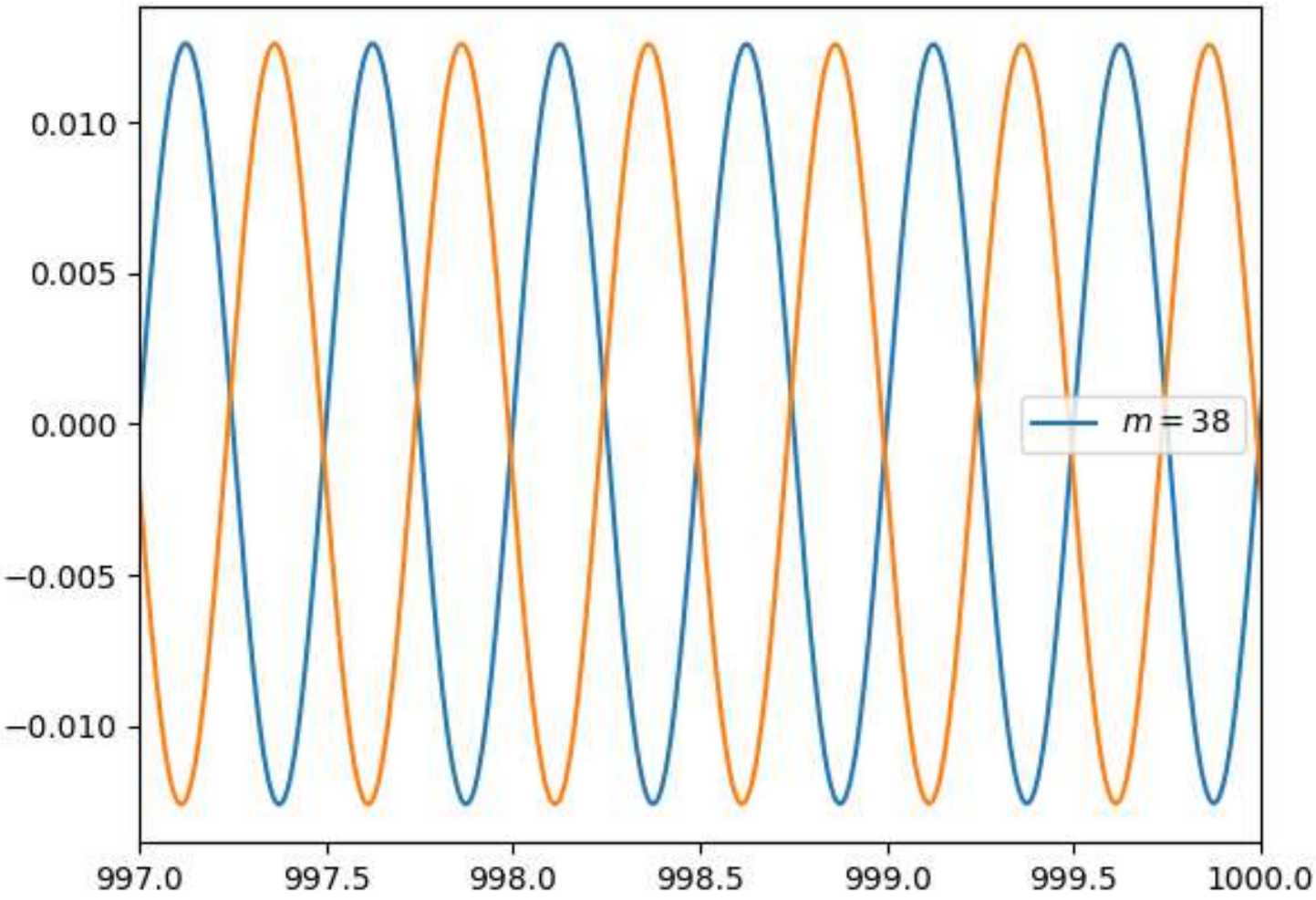
oeil-du-cyclone.py - GNU Emacs at DENISE_VELLA_23

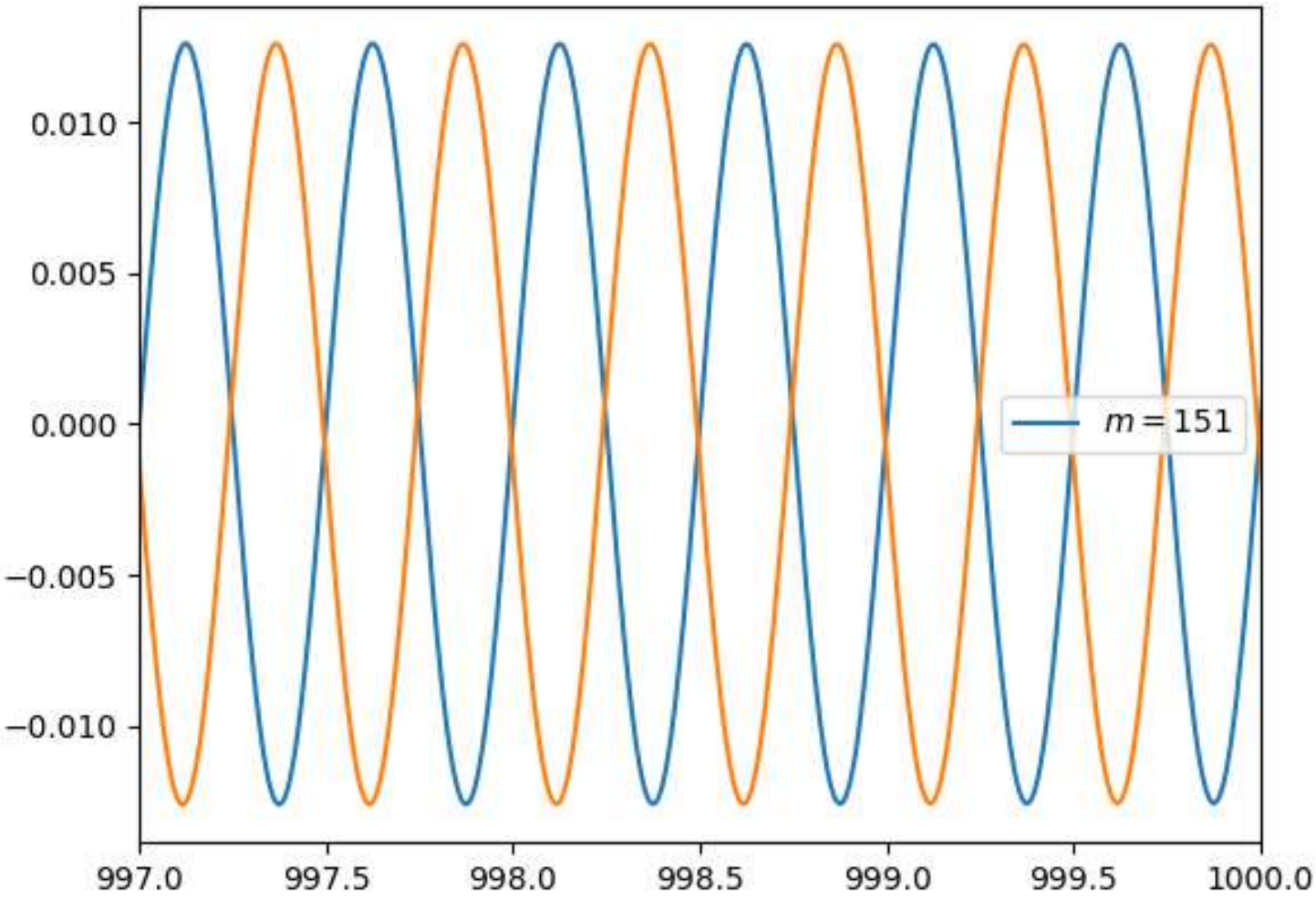
File Edit Options Buffers Tools Python Help

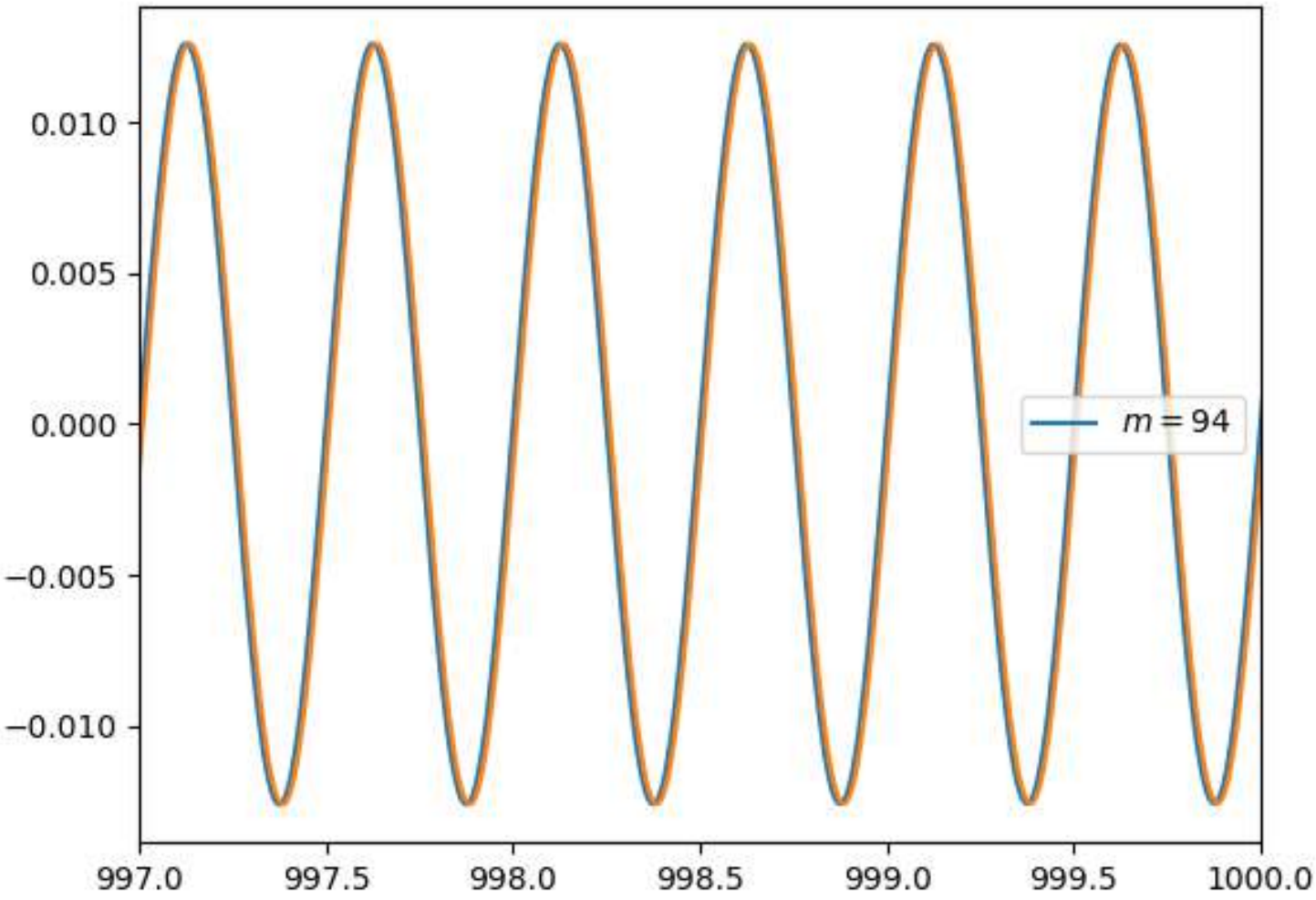
```
import matplotlib.pyplot as plt
import numpy as np
from numpy import exp,sin,cos,min,max

b = 0.05555

t = np.linspace(0,50,2024)
x = exp(-b*t)*cos(t)
y = exp(-b*t)*sin(t)

err = 0.12
plt.plot(x,y,color='blue',alpha=0.3)
lesx = [2,3,5,7,11,13,17,19,23,29,31,37,41,43,47]
lesy1 = []
lesy2 = []
for x in lesx:
    lesy1.append(exp(-b*x)*cos(x))
    lesy2.append(exp(-b*x)*sin(x))
    plt.annotate(x,xy=(exp(-b*x)*cos(x),exp(-b*x)*sin(x)),color='orange')
plt.scatter(lesy1,lesy2,color='orange')
xmin,xmax = 0,int(max(lesy1))+2
ymin,ymax = 0,int(max(lesy2))+2
minor_ticks = np.arange(xmin,xmax,1)
axes = plt.gca()
#axes.set_xticks(minor_ticks,minor = True)
#axes.set_yticks(minor_ticks,minor = True)
plt.grid()
plt.show()
```

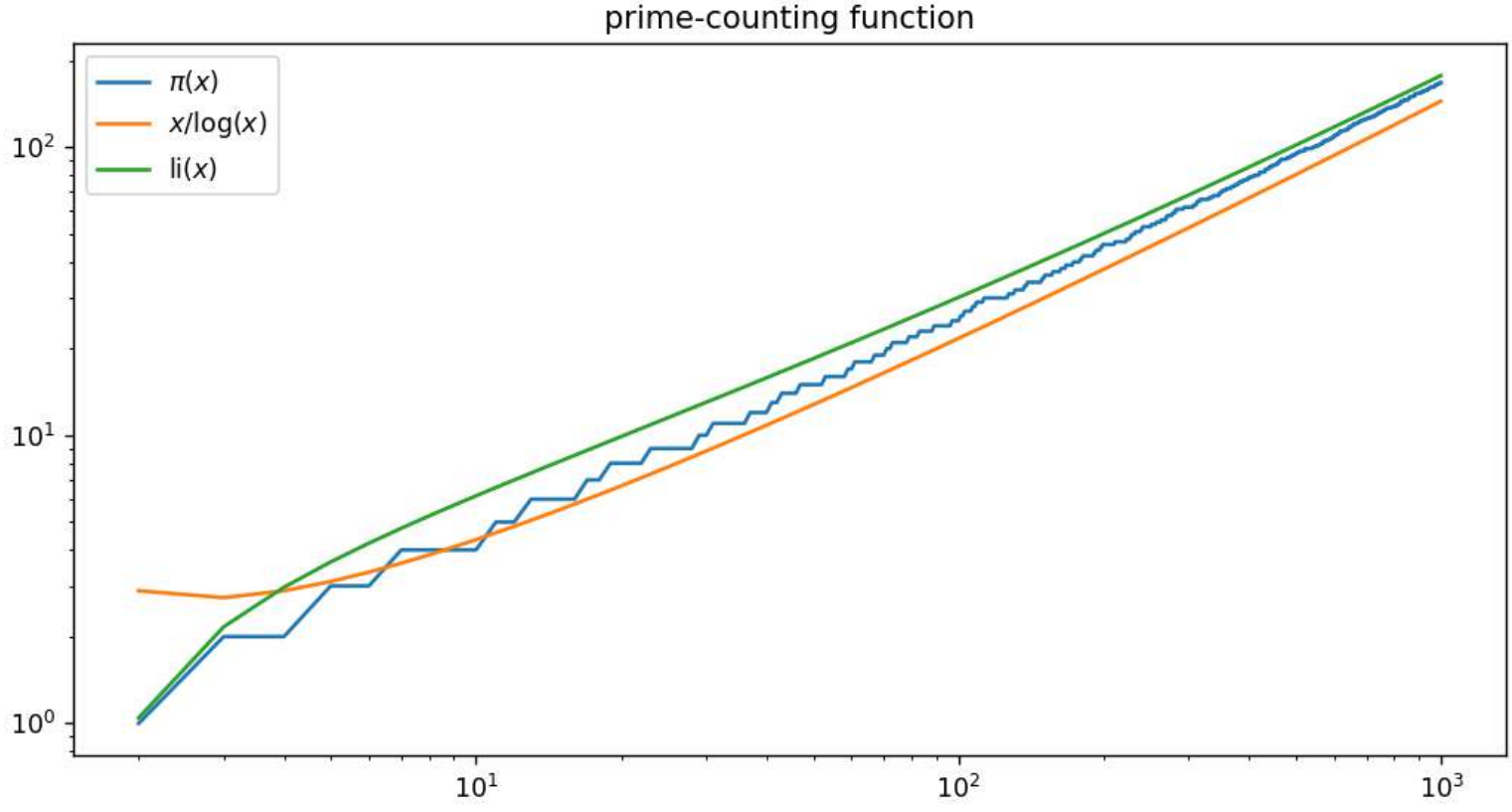
-\--- **oeil-du-cyclone.py** All L18 (Python ElDoc)

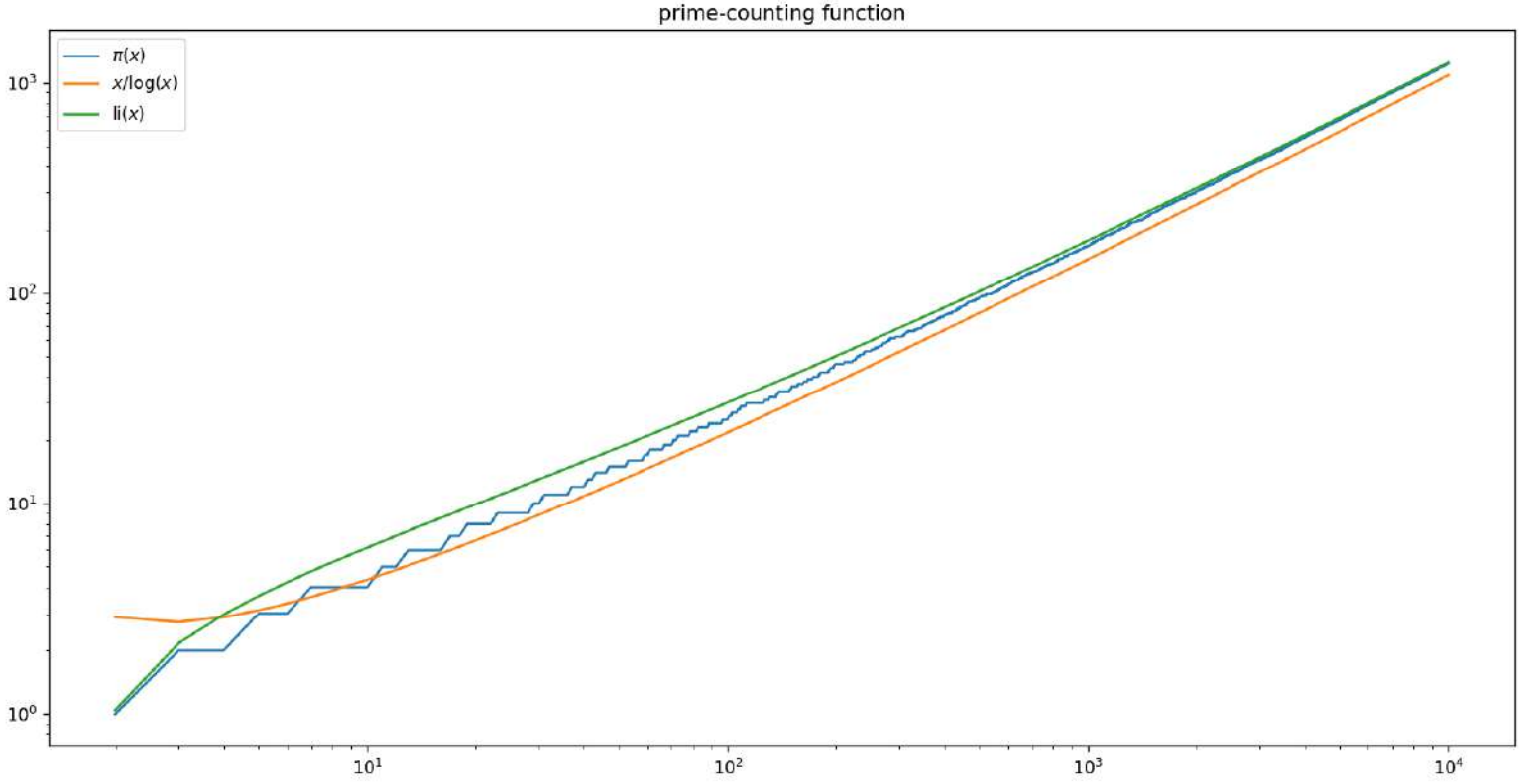
Wrote c:/Users/Denise_Vella/Desktop/oeil-du-cyclone.py

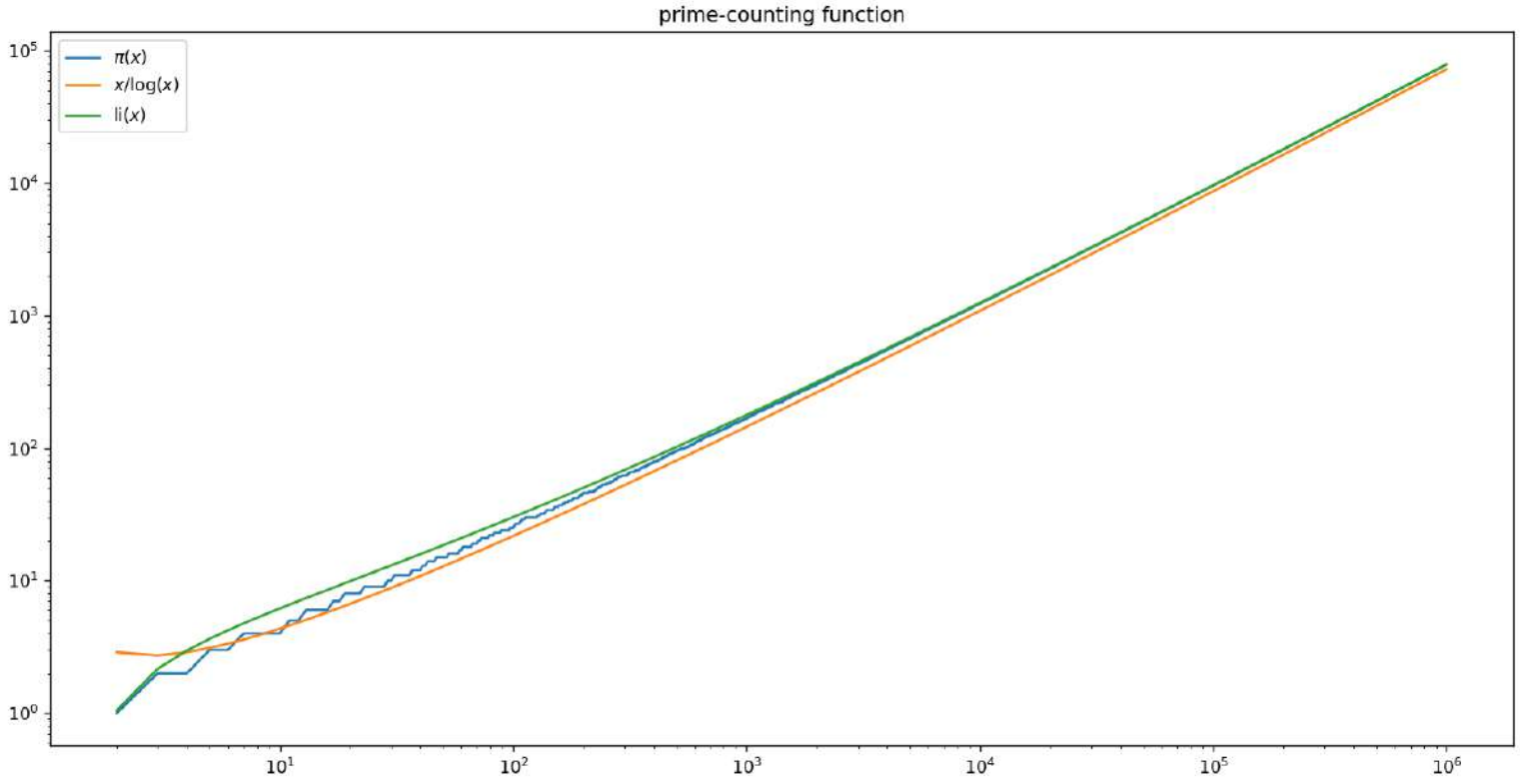

0.010
0.005
0.000
−0.005
−0.010
997.0
997.5
998.0
998.5
999.0
999.5
1000.0
$m = 38$

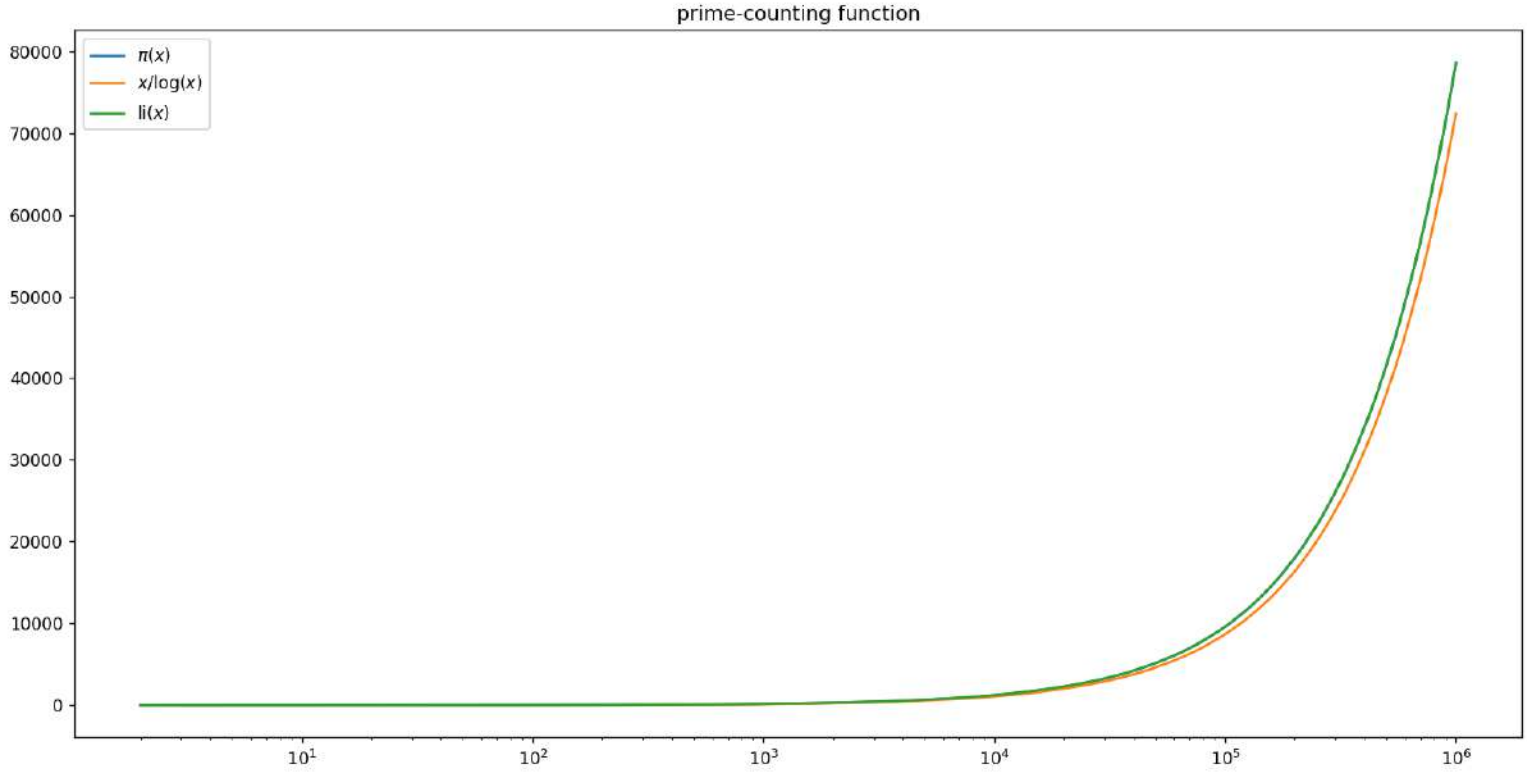

0.010
0.005
0.000
−0.005
−0.010
997.0
997.5
998.0
998.5
999.0
999.5
1000.0
$m = 151$

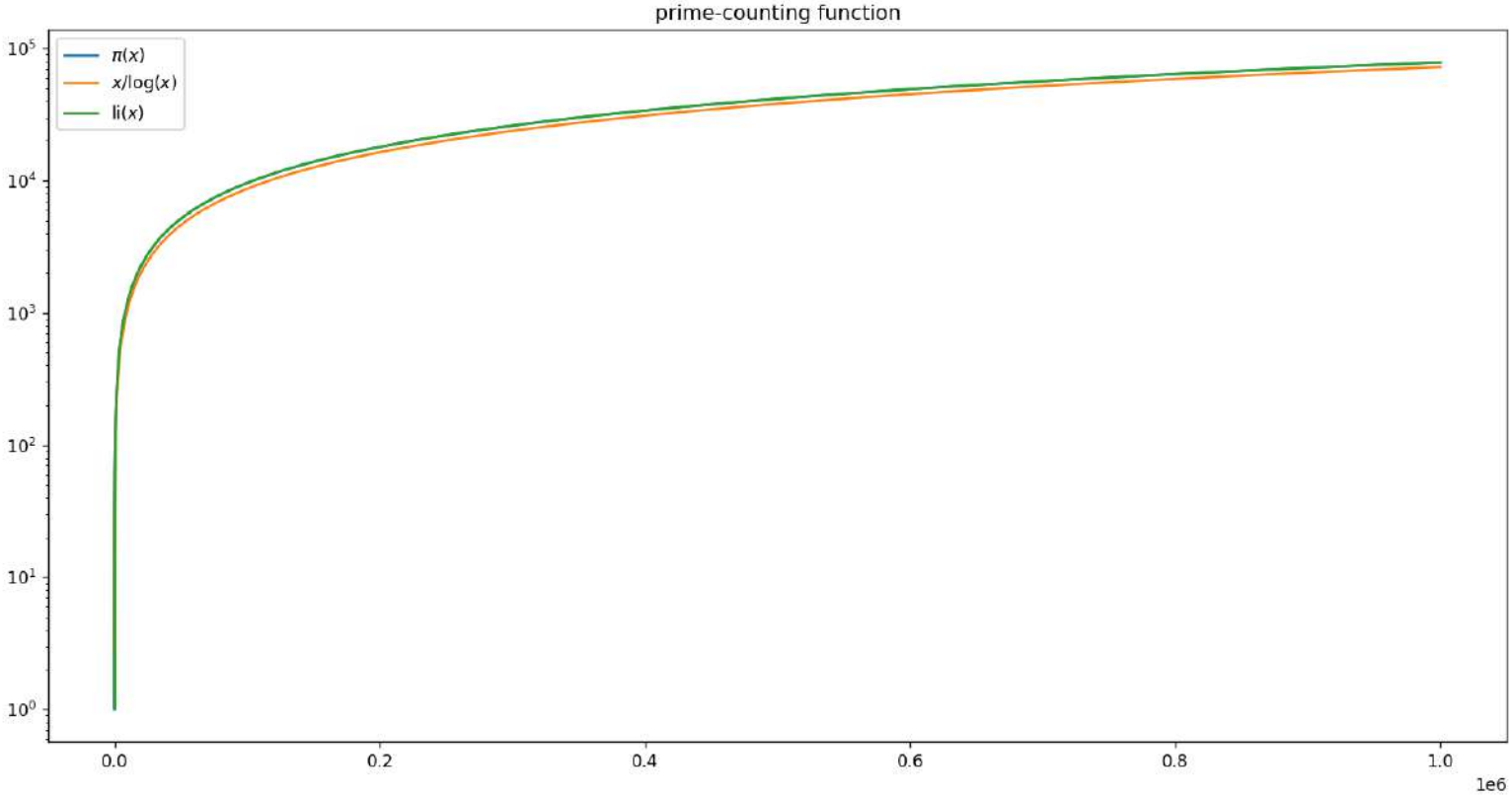

0.010
0.005
0.000
−0.005
−0.010
997.0
997.5
998.0
998.5
999.0
999.5
1000.0
$m = 94$

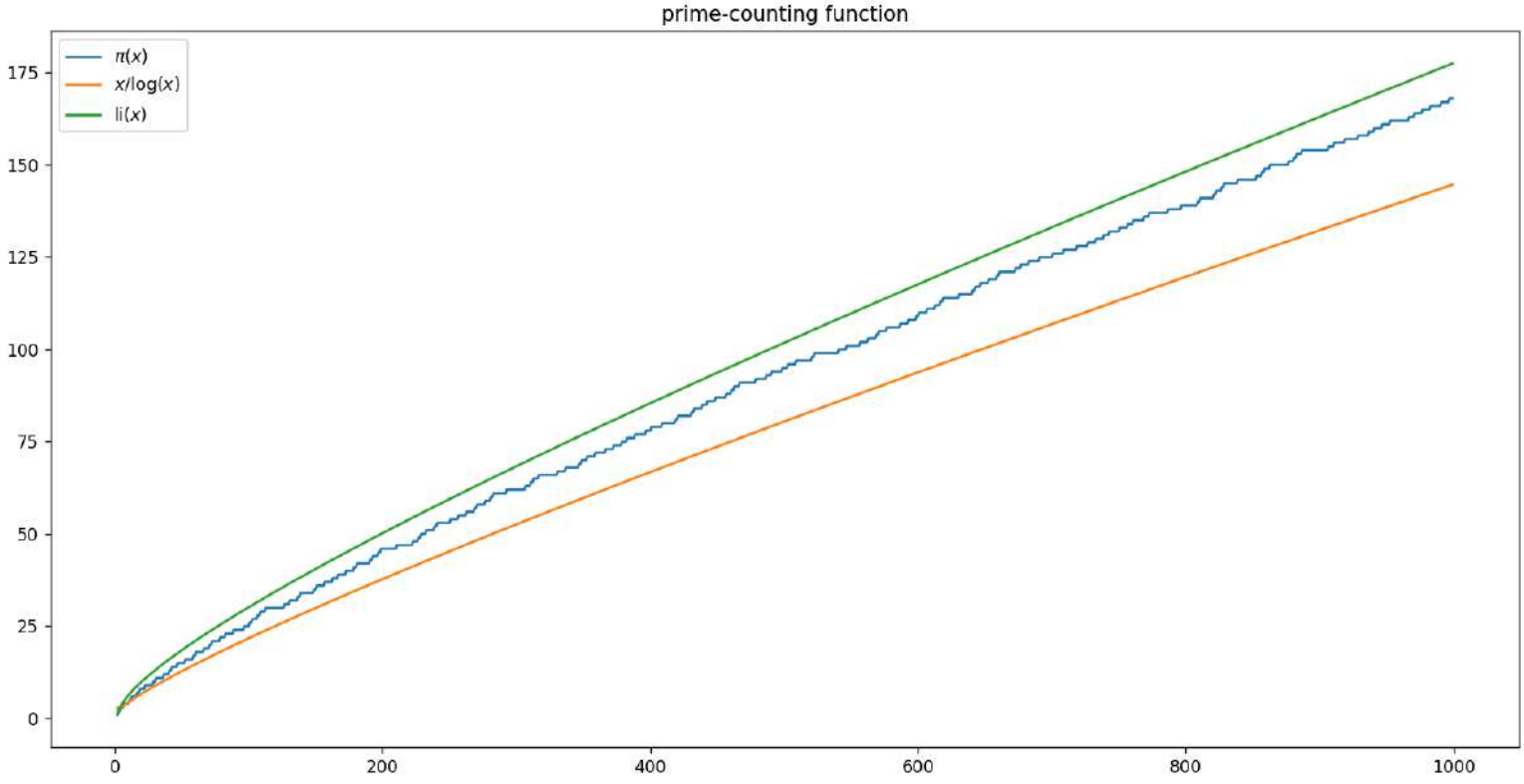

prime-counting function
π(x)
x/log(x)
li(x)
10^2
10^1
10^0
10^1
10^2
10^3

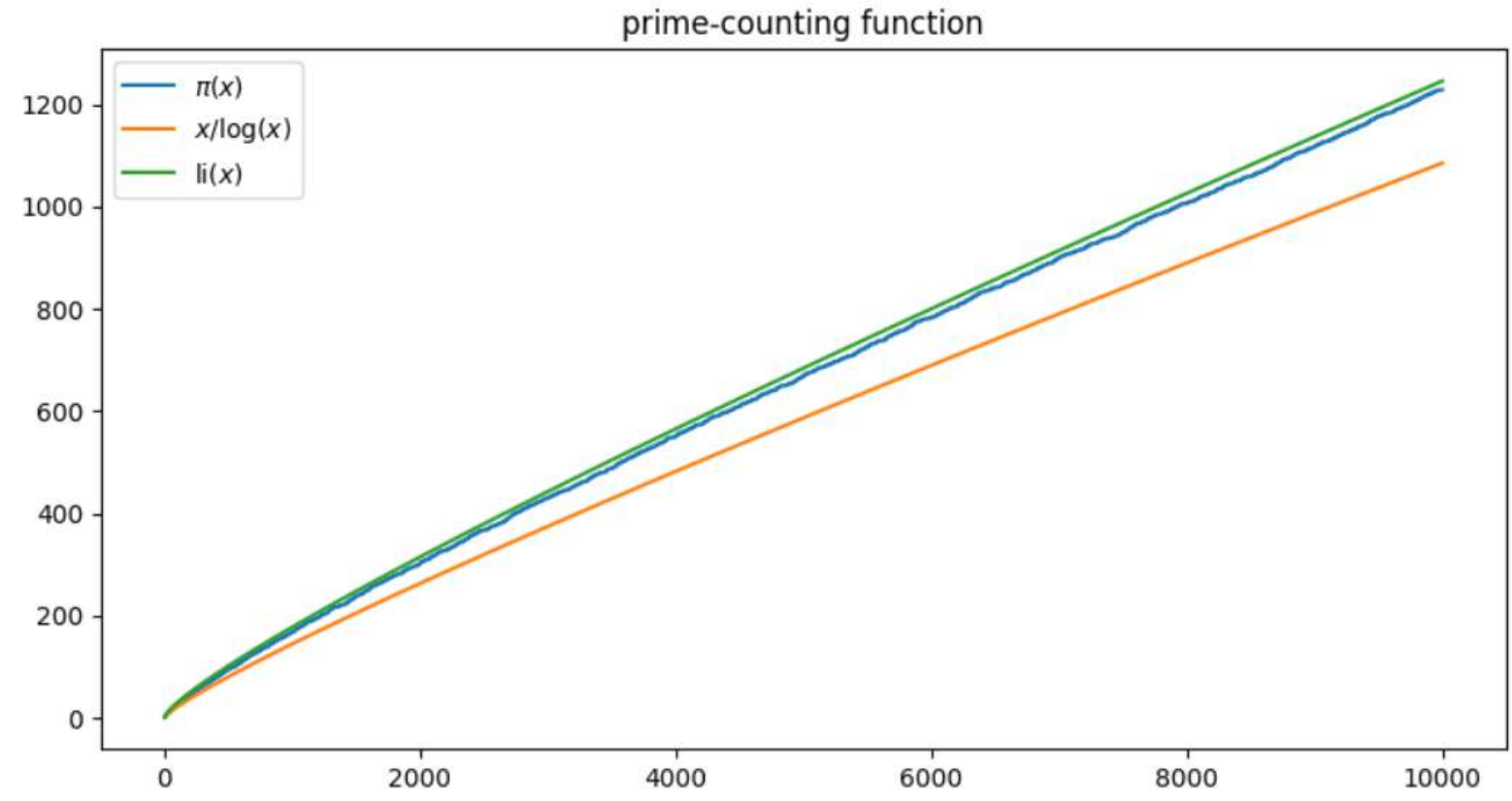

prime-counting function
π(x)
x/log(x)
li(x)
10^3
10^2
10^1
10^0
10^1
10^2
10^3
10^4

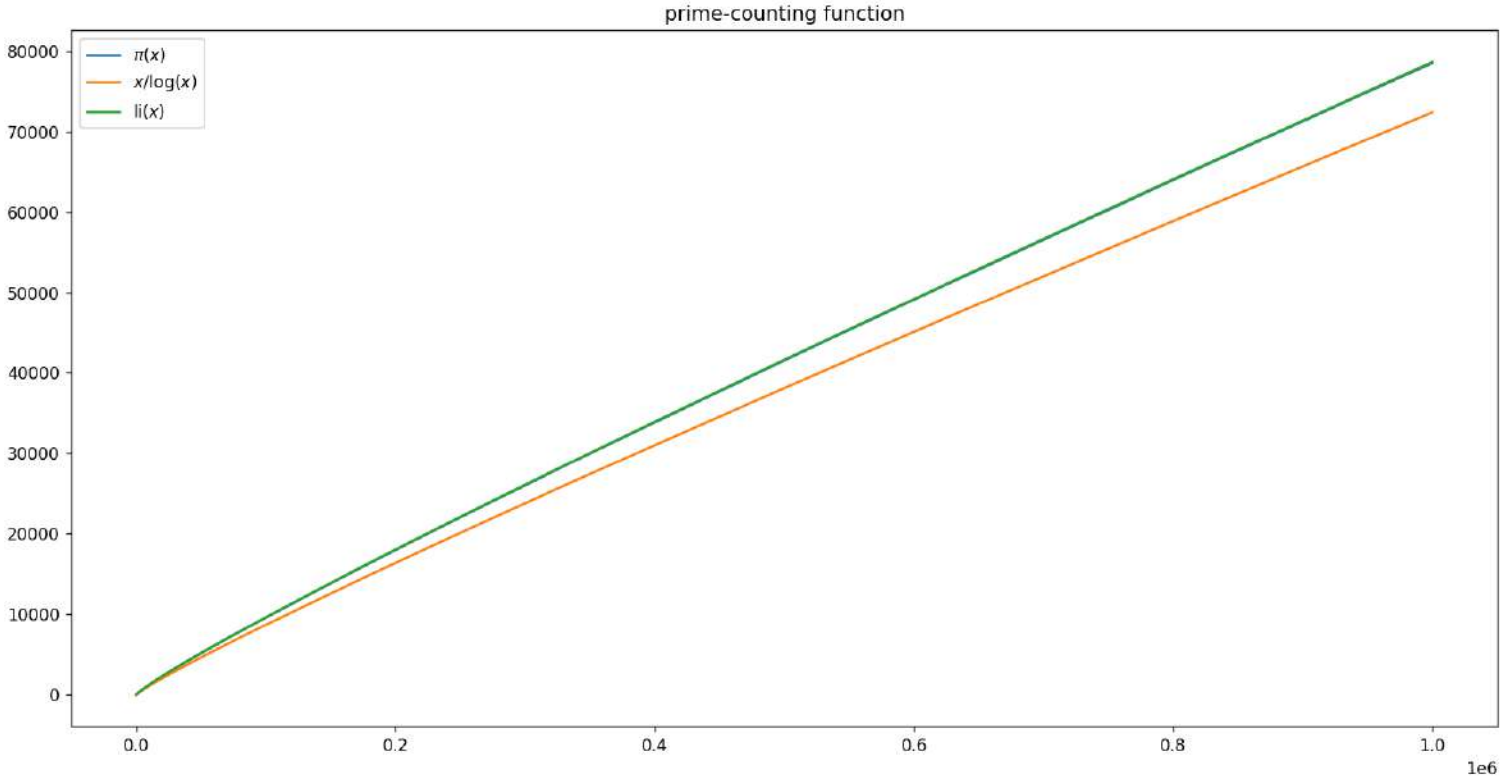

prime-counting function
π(x)
x/log(x)
li(x)
10^5
10^4
10^3
10^2
10^1
10^0
10^1
10^2
10^3
10^4
10^5
10^6


prime-counting function
π(x)
x/log(x)
li(x)
80000
70000
60000
50000
40000
30000
20000
10000
0
10¹
10²
10³
10⁴
10⁵
10⁶


prime-counting function
π(x)
x/log(x)
li(x)
10^5
10^4
10^3
10^2
10^1
10^0
0.0
0.2
0.4
0.6
0.8
1.0
1e6


prime-counting function
π(x)
x/log(x)
li(x)
175
150
125
100
75
50
25
0
0
200
400
600
800
1000


prime-counting function
π(x)
x/log(x)
li(x)
0
200
400
600
800
1000
1200
0
2000
4000
6000
8000
10000


prime-counting function
π(x)
x/log(x)
li(x)
80000
70000
60000
50000
40000
30000
20000
10000
0
0.0
0.2
0.4
0.6
0.8
1.0
1e6

Invite de commandes

```
C:\Users\Denise_Vella>cd Desktop

C:\Users\Denise_Vella\Desktop>python schisme-a-ma-facon-le-mieux-dec-2024.py
----------------- Sturm-Liouville (c = 5.50, n = 10) : N = 116 ------------------
0  -->  4.7025839022433855  --->  4.337088379197908
1  -->  14.460555877930148  --->  7.6054075177942035
2  -->  22.751451128939088  --->  9.539696248610662
3  -->  29.790071504325624  --->  10.91605633996557
4  -->  37.11996235186697  --->  12.185230790078121
5  -->  46.37664283748533  --->  13.62007971158544
6  -->  57.96375587871829  --->  15.226786381731149
7  -->  71.73495280831985  --->  16.939297837669642
8  -->  87.5920121676697  --->  18.718120863769386
9  -->  105.49514125823619  --->  20.542165539030805
10  -->  125.42599492219544  --->  22.39874951172011
------------------------- prolate (c = 5.50, n = 10) --------------------------
lambda( 0) = 1.068694704193758
lambda( 1) = 1.063992988597398
lambda( 2) = 1.006447812586847
lambda( 3) = 0.753643303365568
lambda( 4) = 0.362179480409259
lambda( 5) = 0.113779929316233
lambda( 6) = 0.027284099109160
lambda( 7) = 0.005470259037271
lambda( 8) = 0.000951448074434
lambda( 9) = 0.000146499345205
lambda(10) = 0.000020254774082

C:\Users\Denise_Vella\Desktop>
```

schisme-a-ma-facon-le-mieux-dec-2024.py - GNU Emacs at DENISE_VELLA_23

File Edit Options Buffers Tools Python Help

```
import math
from math import pi, sqrt
import matplotlib.pyplot as plt
import numpy as np

c = 5.5
n = 10
N = int (1.1*c + n + 100)
M = np.zeros((N, N))
for k in range(N):
    M[k, k] = k*(k+1) + (2*k*(k+1) - 1) / ((2*k+3)*(2*k-1)) * c**2
    if k+2 in range(N):
        M[k, k+2] = (k+1)*(k+2) / ((2*k+3) * np.sqrt((2*k+1)*(2*k+5))) * c**2
        M[k+2, k] = M[k, k+2]
chi, beta = np.linalg.eigh(M)
print(" Sturm-Liouville (c = {:.2f}, n = {:d}) : N = {:d} ".format(c, n, len(chi
)).center(80, '-'))
for k in range(n+1):
    mu, v = chi[k], beta[:, k]
    err = np.linalg.norm(M@v - mu*v)
    nrm = np.linalg.norm(v)
    print(k, ' --> ', chi[k], ' ---> ', 2*sqrt(chi[k]))
coef = np.diag([np.sqrt(k + 1/2) for k in range(len(beta))]) @ beta
psi = [np.polynomial.Legendre(coef[:, k]) for k in range(n+1)]
lmb = [(-1)**(k//2) * np.sqrt(2) * (beta[0, k] / psi[k](0) if k % 2 == 0
       else beta[1, k] / psi[k].deriv()(0) * c / np.sqrt(3))
      for k in range(n+1)]
print(" prolate (c = {:.2f}, n = {:d}) ".format(c, n).center(80, '-'))
for k, l in enumerate(lmb):
    plt.plot(lmb)
    print('lambda({:2d}) = {:.15f}'.format(k, l))

plt.show()
```

-(Unix)--- **schisme-a-ma-facon-le-mieux-dec-2024.py** All L1 (Python ElDoc)

spilog2.py - GNU Emacs at DENISE_VELLA_23

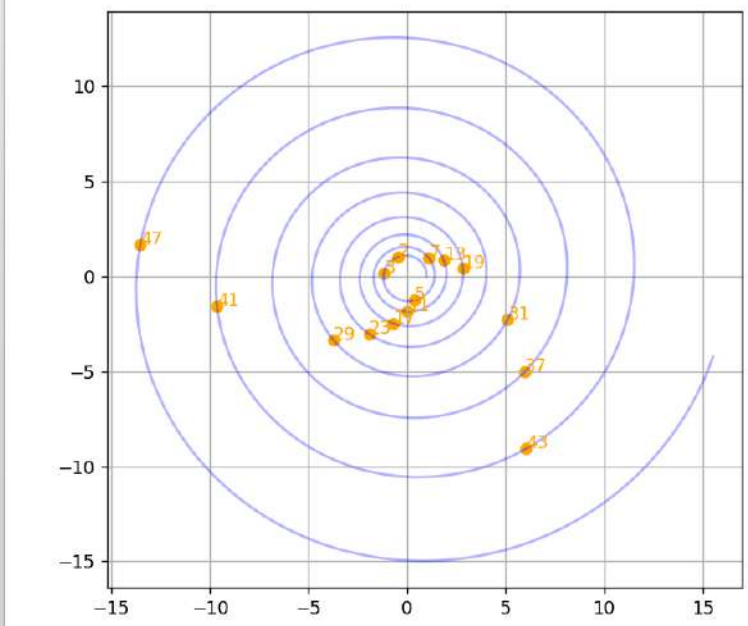
File Edit Options Buffers Tools Python Help

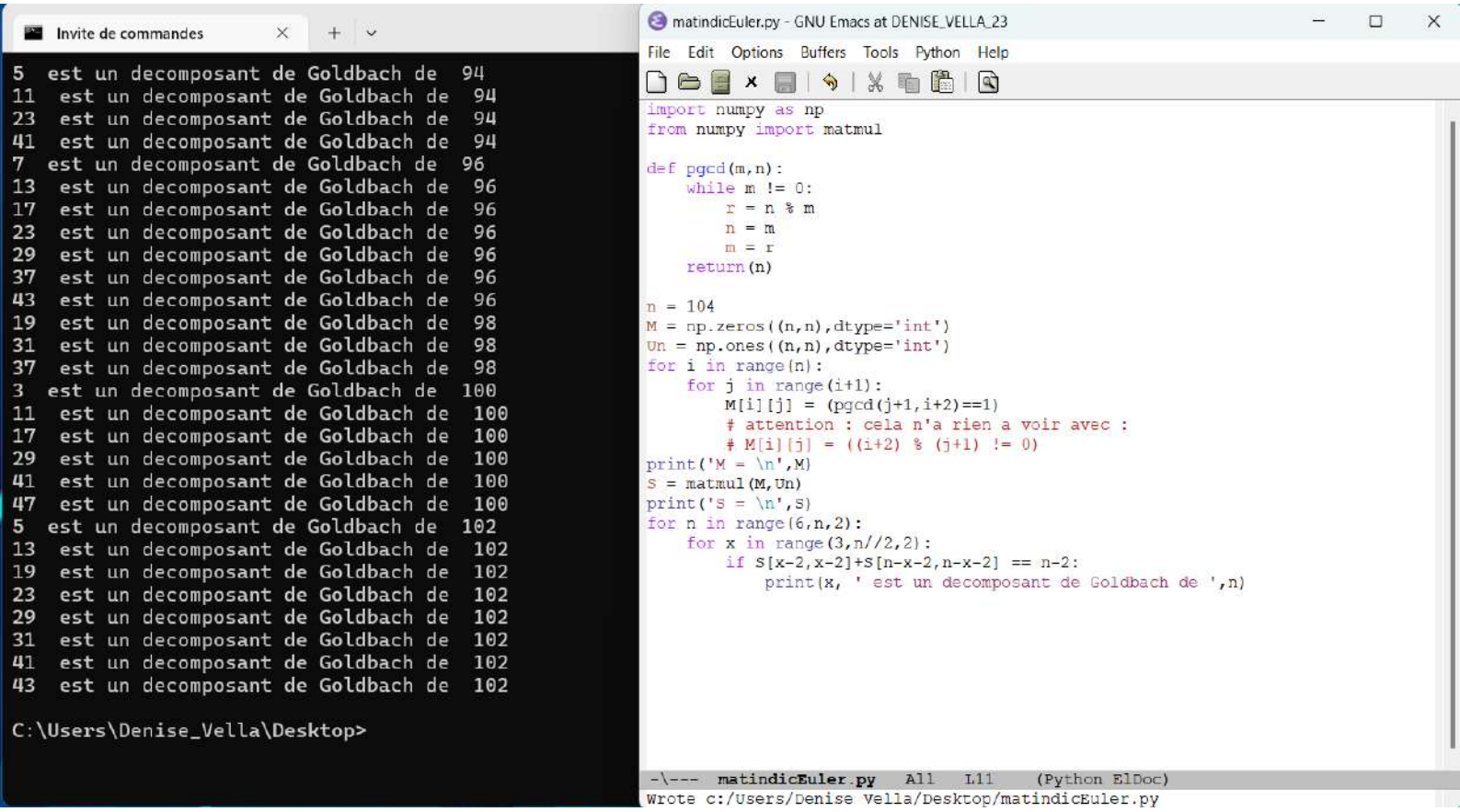
```
import matplotlib.pyplot as plt
import numpy as np
from numpy import exp,sin,cos,min,max

b = 0.05555

t = np.linspace(0,50,2024)
x = exp(b*t)*cos(t)
y = exp(b*t)*sin(t)

err = 0.12
plt.plot(x,y,color='blue',alpha=0.3)
lesx = [2,3,5,7,11,13,17,19,23,29,31,37,41,43,47]
lesy1 = []
lesy2 = []
for x in lesx:
    lesy1.append(exp(b*x)*cos(x))
    lesy2.append(exp(b*x)*sin(x))
    plt.annotate(x,xy=(exp(b*x)*cos(x),exp(b*x)*sin(x)),color='orange')
plt.scatter(lesy1,lesy2,color='orange')
xmin,xmax = 0,int(max(lesy1))+2
ymin,ymax = 0,int(max(lesy2))+2
minor_ticks = np.arange(xmin,xmax,1)
axes = plt.gca()
#axes.set_xticks(minor_ticks,minor = True)
#axes.set_yticks(minor_ticks,minor = True)
plt.grid()
plt.show()
```

1\--- **spilog2.py** All L12 (Python ElDoc)

Wrote c:/Users/Denise Vella/Desktop/spilog2.py

Figure 1

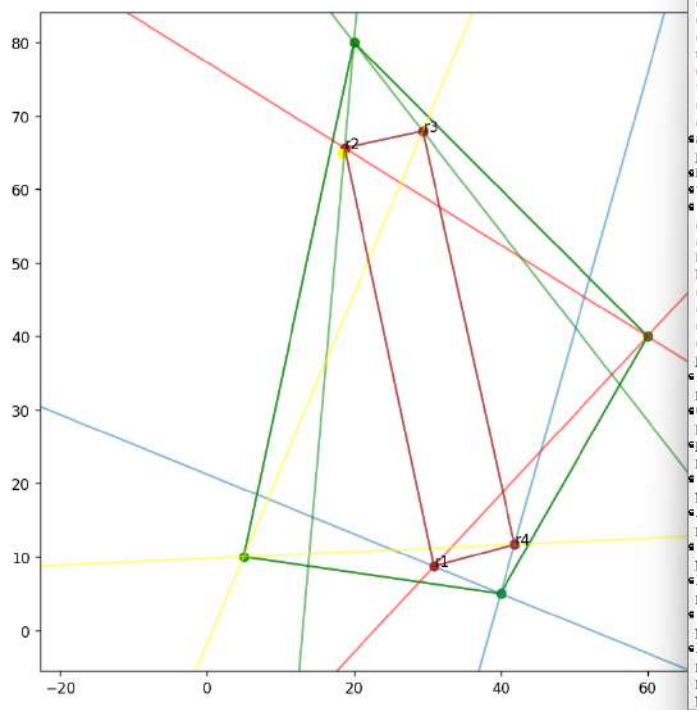



Invite de commandes
5 est un decomposant de Goldbach de 94
11 est un decomposant de Goldbach de 94
23 est un decomposant de Goldbach de 94
41 est un decomposant de Goldbach de 94
7 est un decomposant de Goldbach de 96
13 est un decomposant de Goldbach de 96
17 est un decomposant de Goldbach de 96
23 est un decomposant de Goldbach de 96
29 est un decomposant de Goldbach de 96
37 est un decomposant de Goldbach de 96
43 est un decomposant de Goldbach de 96
19 est un decomposant de Goldbach de 98
31 est un decomposant de Goldbach de 98
37 est un decomposant de Goldbach de 98
3 est un decomposant de Goldbach de 100
11 est un decomposant de Goldbach de 100
17 est un decomposant de Goldbach de 100
29 est un decomposant de Goldbach de 100
41 est un decomposant de Goldbach de 100
47 est un decomposant de Goldbach de 100
5 est un decomposant de Goldbach de 102
13 est un decomposant de Goldbach de 102
19 est un decomposant de Goldbach de 102
23 est un decomposant de Goldbach de 102
29 est un decomposant de Goldbach de 102
31 est un decomposant de Goldbach de 102
41 est un decomposant de Goldbach de 102
43 est un decomposant de Goldbach de 102
C:\Users\Denise_Vella\Desktop>
matindicEuler.py - GNU Emacs at DENISE_VELLA_23
File Edit Options Buffers Tools Python Help
import numpy as np
from numpy import matmul
def pgcd(m,n):
while m != 0:
r = n % m
n = m
m = r
return(n)
n = 104
M = np.zeros((n,n),dtype='int')
Un = np.ones((n,n),dtype='int')
for i in range(n):
for j in range(i+1):
M[i][j] = (pgcd(j+1,i+2)==1)
# attention : cela n'a rien a voir avec :
# M[i][j] = ((i+2) % (j+1) != 0)
print('M = \n',M)
S = matmul(M,Un)
print('S = \n',S)
for n in range(6,n,2):
for x in range(3,n//2,2):
if S[x-2,x-2]+S[n-x-2,n-x-2] == n-2:
print(x, ' est un decomposant de Goldbach de ',n)
-\--- matindicEuler.py All L11 (Python ElDoc)
Wrote c:/Users/Denise Vella/Desktop/matindicEuler.py

Invite de commandes - pytho

```
C:\Users\Denise_Vella\Desktop>py
anglea =  111.61477894278624
angleb =  105.25511870305778
anglec =  57.094757077012105
angled =  86.03534527714388
Norme cote 1 58.209632173537941
Norme cote 2 10.892023383982890
Norme cote 3 57.588239762670213
Norme cote 4 11.391280903551420
 115.797871936208153
```

Figure 1



toto4.py - GNU Emacs at DENISE_VELLA_23

File Edit Options Buffers Tools Python Help

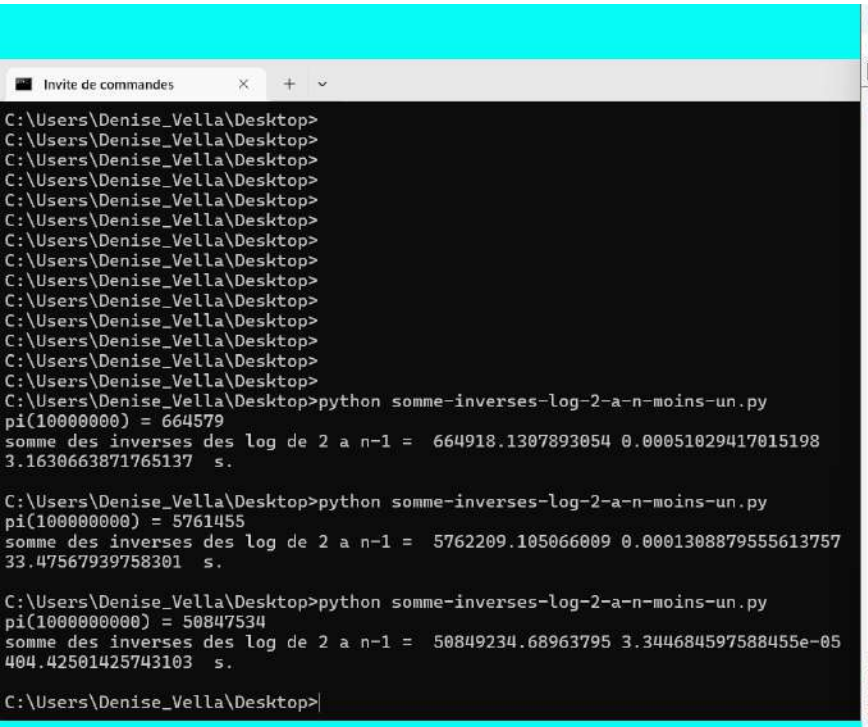
```
me(vecteur(c,d))+norme(vecteur(d,a))
c1=norme(vecteur(a,b))
c2=norme(vecteur(b,c))
c3=norme(vecteur(c,d))
c4=norme(vecteur(d,a))
un = (0,0)
deux = (0,100)
trois = (100,100)
quatre = (100,0)
anglea=angle(ab,ad) ; angleb=angle(bc,ba) ; anglec=
angle(cd,cb) ; angled=angle(da,dc)
print('anglea = ',anglea*360/(2*pi)) ; print('angle
b = ',angleb*360/(2*pi)) ; print('anglec = ',anglec
*360/(2*pi)) ; print('angled = ',angled*360/(2*pi))
 ;
aprime = add(a, rotation(ab,anglea*157.5/180))
aseconde = add(a, rotation(ab,anglea*22.5/180))
bprime = add(b, rotation(bc,angleb*22.5/180))
bseconde = add(b, rotation(bc,angleb*157.5/180))
cprime = add(c, rotation(cd,anglec*157.5/180))
cseconde = add(c, rotation(cd,anglec*22.5/180))
dprime = add(d, rotation(da,angled*22.5/180))
dseconde = add(d, rotation(da,angled*157.5/180))
plt.plot([a[0],b[0],c[0],d[0],a[0]],[a[1],b[1],c[1]
,d[1],a[1]],color='green',alpha=0.8)
plt.axline([a[0],a[1]],[aprime[0],aprime[1]],alpha=
0.5)
plt.axline([a[0],a[1]],[aseconde[0],aseconde[1]],al
pha=0.5)
plt.axline([b[0],b[1]],[bprime[0],bprime[1]],color=
'red',alpha=0.5)
plt.axline([b[0],b[1]],[bseconde[0],bseconde[1]],co
lor='red',alpha=0.5)
plt.axline([c[0],c[1]],[cprime[0],cprime[1]],color=
'green',alpha=0.5)
plt.axline([c[0],c[1]],[cseconde[0],cseconde[1]],co
lor='green',alpha=0.5)
plt.axline([d[0],d[1]],[dprime[0],dprime[1]],color=
'yellow',alpha=0.5)
plt.axline([d[0],d[1]],[dseconde[0],dseconde[1]],co
lor='yellow',alpha=0.5)
plt.xlim(-20,120)
plt.ylim(-20,120)
plt.scatter(a[0],a[1],color='green',alpha=0.8)
```

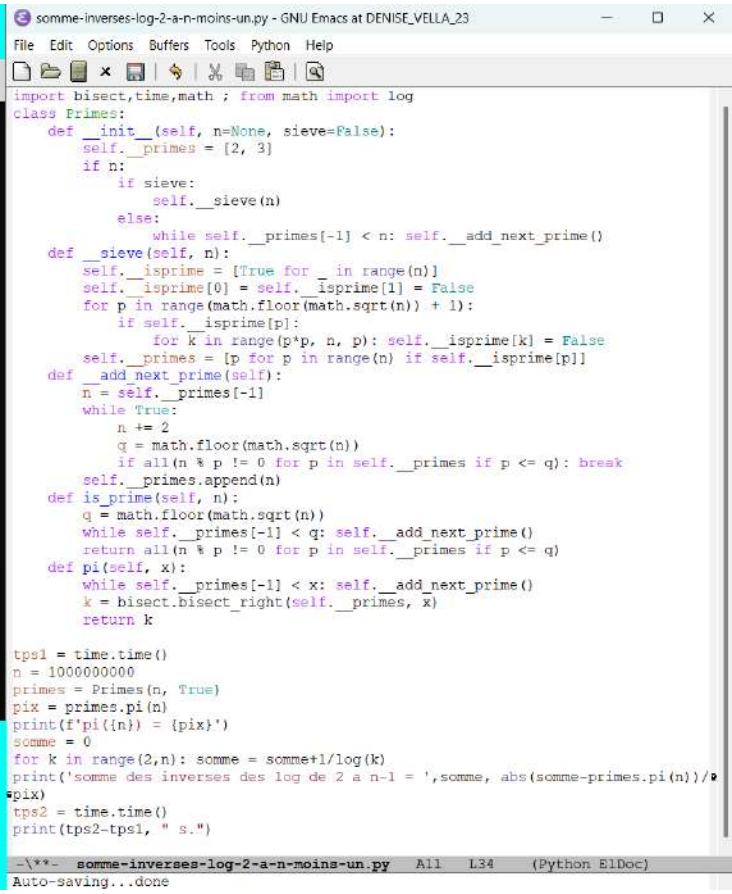
-**- **toto4.py** 34% L56 (Python ElDoc)

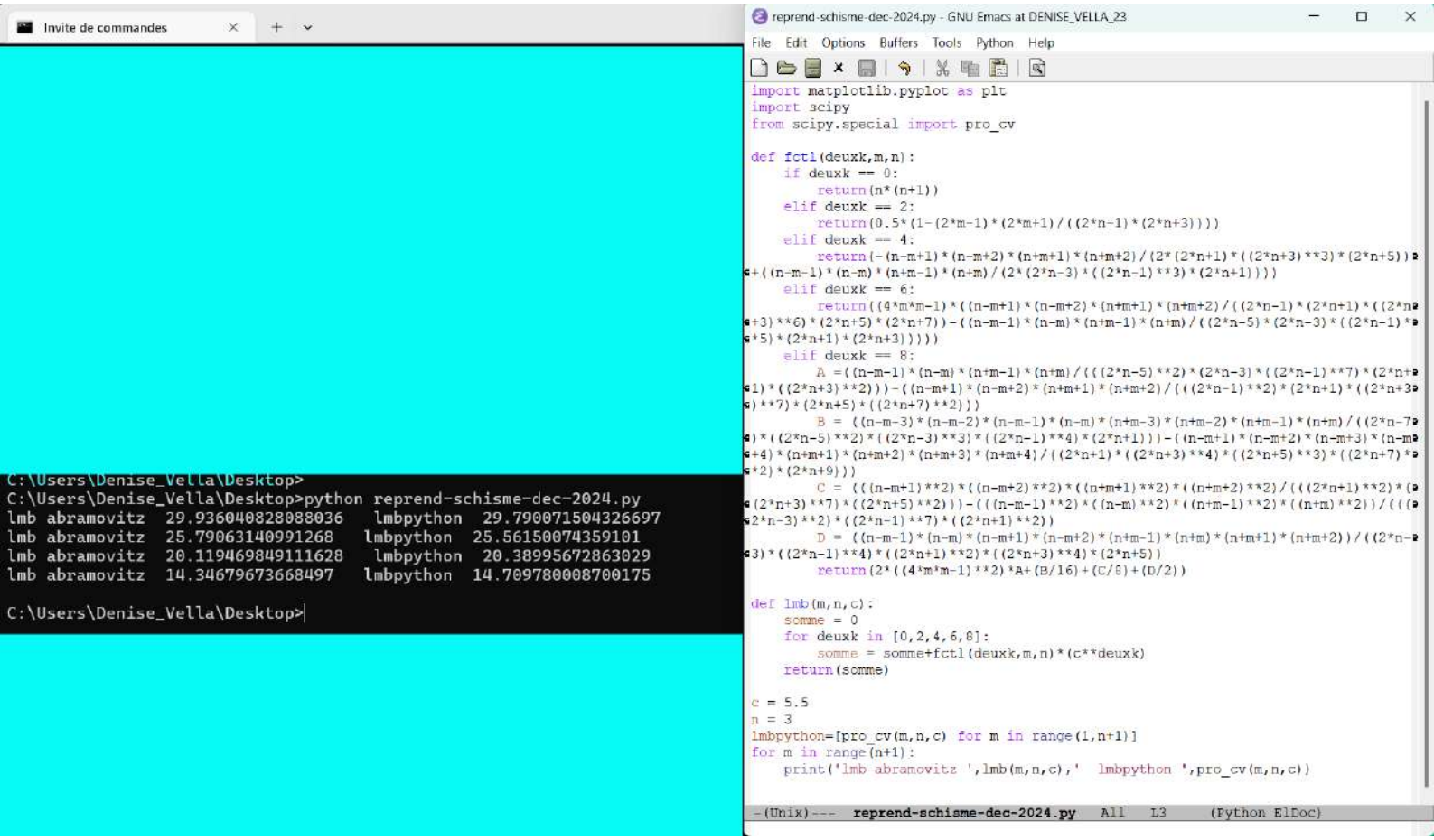
D'un autre côté, on ne devrait pas tirer de ce commentaire la conclusion que l'hypothèse de Riemann était seulement une remarque occasionnelle d'un intérêt mineur pour lui. La validité de l'hypothèse de Riemann équivaut à dire que la déviation du nombre de nombres premiers du terme moyen $\mathrm{Li}(x)$ est

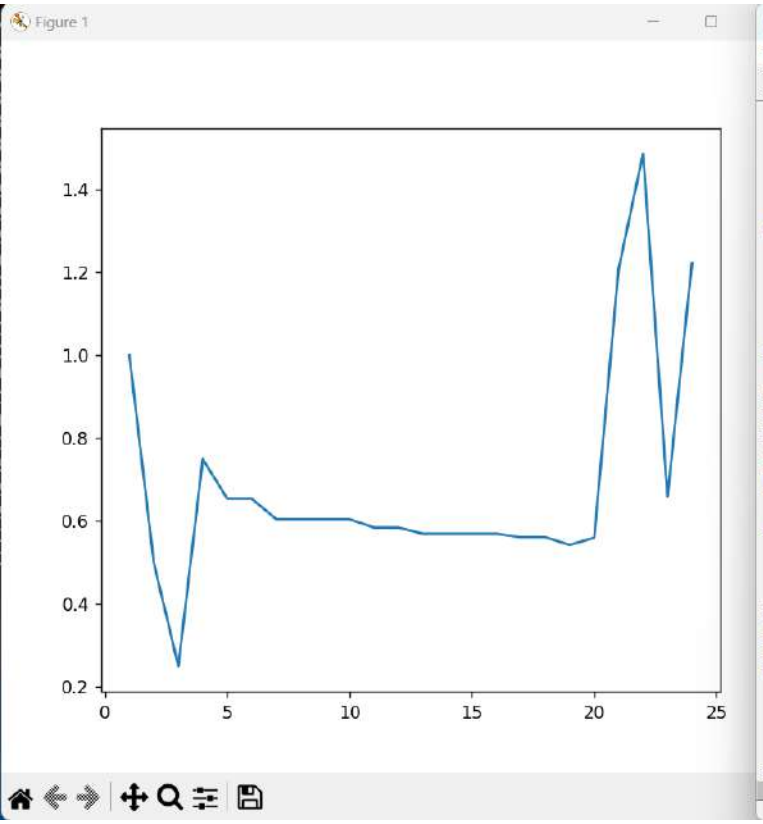
$$\pi(x) = \mathrm{Li}(x) + O(\sqrt{x}\log x);$$

Le terme d'erreur ne peut pas être beaucoup amélioré, puisqu'on sait qu'il oscille dans les deux directions d'un ordre de grandeur au moins égal à $\mathrm{Li}(\sqrt{x})\log\log\log x$ (Littlewood). Quand on voit les commentaires de Riemann à la fin de son mémoire à propos de l'approximation de $\pi(x)$ par $\mathrm{Li}(x)$, il est assez vraisemblable qu'il avait vu combien son hypothèse était centrale pour permettre d'évaluer la qualité de l'approximation de $\pi(x)$ que l'on peut obtenir à partir de cette formule.


Invite de commandes
C:\Users\Denise_Vella\Desktop>
C:\Users\Denise_Vella\Desktop>
C:\Users\Denise_Vella\Desktop>
C:\Users\Denise_Vella\Desktop>
C:\Users\Denise_Vella\Desktop>
C:\Users\Denise_Vella\Desktop>
C:\Users\Denise_Vella\Desktop>
C:\Users\Denise_Vella\Desktop>
C:\Users\Denise_Vella\Desktop>
C:\Users\Denise_Vella\Desktop>
C:\Users\Denise_Vella\Desktop>
C:\Users\Denise_Vella\Desktop>
C:\Users\Denise_Vella\Desktop>
C:\Users\Denise_Vella\Desktop>
C:\Users\Denise_Vella\Desktop>python somme-inverses-log-2-a-n-moins-un.py
pi(10000000) = 664579
somme des inverses des log de 2 a n-1 = 664918.1307893054 0.00051029417015198
3.1630663871765137 s.
C:\Users\Denise_Vella\Desktop>python somme-inverses-log-2-a-n-moins-un.py
pi(100000000) = 5761455
somme des inverses des log de 2 a n-1 = 5762209.105066009 0.0001308879555613757
33.47567939758301 s.
C:\Users\Denise_Vella\Desktop>python somme-inverses-log-2-a-n-moins-un.py
pi(1000000000) = 50847534
somme des inverses des log de 2 a n-1 = 50849234.68963795 3.344684597588455e-05
404.42501425743103 s.
C:\Users\Denise_Vella\Desktop>


somme-inverses-log-2-a-n-moins-un.py - GNU Emacs at DENISE_VELLA_23
File Edit Options Buffers Tools Python Help
import bisect,time,math ; from math import log
class Primes:
def __init__(self, n=None, sieve=False):
self.__primes = [2, 3]
if n:
if sieve:
self.__sieve(n)
else:
while self.__primes[-1] < n: self.__add_next_prime()
def __sieve(self, n):
self.__isprime = [True for _ in range(n)]
self.__isprime[0] = self.__isprime[1] = False
for p in range(math.floor(math.sqrt(n)) + 1):
if self.__isprime[p]:
for k in range(p*p, n, p): self.__isprime[k] = False
self.__primes = [p for p in range(n) if self.__isprime[p]]
def __add_next_prime(self):
n = self.__primes[-1]
while True:
n += 2
q = math.floor(math.sqrt(n))
if all(n % p != 0 for p in self.__primes if p <= q): break
self.__primes.append(n)
def is_prime(self, n):
q = math.floor(math.sqrt(n))
while self.__primes[-1] < q: self.__add_next_prime()
return all(n % p != 0 for p in self.__primes if p <= q)
def pi(self, x):
while self.__primes[-1] < x: self.__add_next_prime()
k = bisect.bisect_right(self.__primes, x)
return k
tps1 = time.time()
n = 1000000000
primes = Primes(n, True)
pix = primes.pi(n)
print(f'pi({n}) = {pix}')
somme = 0
for k in range(2,n): somme = somme+1/log(k)
print('somme des inverses des log de 2 a n-1 = ',somme, abs(somme-primes.pi(n))/p
ix)
tps2 = time.time()
print(tps2-tps1, " s.")
-**- somme-inverses-log-2-a-n-moins-un.py All L34 (Python ElDoc)
Auto-saving...done


Invite de commandes
C:\Users\Denise_Vella\Desktop>
C:\Users\Denise_Vella\Desktop>python reprend-schisme-dec-2024.py
lmb abramovitz 29.936040828088036 lmbpython 29.790071504326697
lmb abramovitz 25.79063140991268 lmbpython 25.56150074359101
lmb abramovitz 20.119469849111628 lmbpython 20.38995672863029
lmb abramovitz 14.34679673668497 lmbpython 14.709780008700175
C:\Users\Denise_Vella\Desktop>
reprend-schisme-dec-2024.py - GNU Emacs at DENISE_VELLA_23
File Edit Options Buffers Tools Python Help
import matplotlib.pyplot as plt
import scipy
from scipy.special import pro_cv
def fctl(deuxk,m,n):
if deuxk == 0:
return(n*(n+1))
elif deuxk == 2:
return(0.5*(1-(2*m-1)*(2*m+1)/((2*n-1)*(2*n+3))))
elif deuxk == 4:
return(-(n-m+1)*(n-m+2)*(n+m+1)*(n+m+2)/(2*(2*n+1)*((2*n+3)**3)*(2*n+5))+((n-m-1)*(n-m)*(n+m-1)*(n+m)/(2*(2*n-3)*((2*n-1)**3)*(2*n+1))))
elif deuxk == 6:
return((4*m*m-1)*((n-m+1)*(n-m+2)*(n+m+1)*(n+m+2)/((2*n-1)*(2*n+1)*((2*n+3)**6)*(2*n+5)*(2*n+7))-((n-m-1)*(n-m)*(n+m-1)*(n+m)/((2*n-5)*(2*n-3)*((2*n-1)*5)*(2*n+1)*(2*n+3)))))
elif deuxk == 8:
A =((n-m-1)*(n-m)*(n+m-1)*(n+m)/(((2*n-5)**2)*(2*n-3)*((2*n-1)**7)*(2*n+1)*((2*n+3)**2)))-((n-m+1)*(n-m+2)*(n+m+1)*(n+m+2)/(((2*n-1)**2)*(2*n+1)*((2*n+3)**7)*(2*n+5)*((2*n+7)**2)))
B = ((n-m-3)*(n-m-2)*(n-m-1)*(n-m)*(n+m-3)*(n+m-2)*(n+m-1)*(n+m)/(((2*n-7)*((2*n-5)**2)*((2*n-3)**3)*((2*n-1)**4)*(2*n+1)))-((n-m+1)*(n-m+2)*(n-m+3)*(n-m+4)*(n+m+1)*(n+m+2)*(n+m+3)*(n+m+4)/((2*n+1)*((2*n+3)**4)*((2*n+5)**3)*((2*n+7)*2)*(2*n+9)))
C = (((n-m+1)**2)*((n-m+2)**2)*((n+m+1)**2)*((n+m+2)**2)/(((2*n+1)**2)*((2*n+3)**7)*((2*n+5)**2)))-(((n-m-1)**2)*((n-m)**2)*((n+m-1)**2)*((n+m)**2))/(((2*n-3)**2)*((2*n-1)**7)*((2*n+1)**2))
D = ((n-m-1)*(n-m)*(n-m+1)*(n-m+2)*(n+m-1)*(n+m)*(n+m+1)*(n+m+2))/((2*n-3)*((2*n-1)**4)*((2*n+1)**2)*((2*n+3)**4)*(2*n+5))
return(2*((4*m*m-1)**2)*A+(B/16)+(C/8)+(D/2))
def lmb(m,n,c):
somme = 0
for deuxk in [0,2,4,6,8]:
somme = somme+fctl(deuxk,m,n)*(c**deuxk)
return(somme)
c = 5.5
n = 3
lmbpython=[pro_cv(m,n,c) for m in range(1,n+1)]
for m in range(n+1):
print('lmb abramovitz ',lmb(m,n,c),' lmbpython ',pro_cv(m,n,c))
-(Unix)--- reprend-schisme-dec-2024.py All L3 (Python ElDoc)



alain-wilson-2.py - GNU Emacs at DENISE_VELLA_23

File Edit Options Buffers Tools Python Help

```
            res = 0
        else:
            res = 1
        somme = somme+pow(sin((ppi/2)*res),2)
    return(somme)

def wif(n):
    somme = 0.0
    for k in range(1,n+1):
        somme = somme+pow(sin((ppi/2.0)*gamma_iterative(k)/k),2.0)
    return(somme)

import decimal

nmax = 25
format(ppi,'.100g')
print(decimal.Decimal.from_float(ppi))
nbprimes = 0
tabpremiers = []
for n in range(nmax):
    tabpremiers.append(0)
for n in range(2,nmax):
    if prime(n):
        nbprimes = nbprimes+1
    tabpremiers[n] = nbprimes
print('tabpremiers = ',tabpremiers)
lesx = []
lesy = []
for xx in range(1,nmax):
    lesx.append(xx)
    res = wif(xx)-tabpremiers[xx]
    print(res)
    lesy.append(res)
print(lesx)
```

-\--- **alain-wilson-2.py** 94% L90 (Python ElDoc)