Résoudre un système d'équations algébriques pour trouver un décomposant de Goldbach d'un nombre pair

Denise Vella-Chemla

27/10/2011

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers. On rappelle qu'un nombre premier impair p est un décomposant de Goldbach de n un nombre pair supérieur ou égal à 6 si p est incongru* à n selon tout module premier impair p' inférieur à $\sqrt{n}$. En effet, dans le cas contraire, le complémentaire à n de p est composé.

Exemple : 19 est un décomposant de Goldbach de 98 car 19 est incongru à 98 selon 3, 5 et 7. Par contre, 3 n'est pas un décomposant de Goldbach de 98 car $3 \equiv 98 \ (mod\ 5)$ (ce qui correspond au fait que 5 divise $98-3$). 5 n'est pas un décomposant de Goldbach de 98 car $5 \equiv 98 \ (mod\ 3)$. 7 n'est pas un décomposant de Goldbach de 98 car $7 \equiv 98 \ (mod\ 7)$ (ce qui correspond au fait que 7 divise $98-7$, 7 est diviseur de 98). 11 n'est pas un décomposant de Goldbach de 98 car $11 \equiv 98 \ (mod\ 3)$. 13 n'est pas un décomposant de Goldbach de 98 car $13 \equiv 98 \ (mod\ 5)$. 17 n'est pas un décomposant de Goldbach de 98 car $17 \equiv 98 \ (mod\ 3)$.

2 Modéliser la recherche des décomposants de Goldbach par des équations algébriques

Chercher un décomposant de Goldbach p d'un nombre pair n revient donc simplement à chercher un nombre qui vérifie les conditions suivantes : d'une part, il est premier et d'autre part, son complémentaire à n est premier.

Lors de ces recherches autour de la conjecture de Goldbach, comme il s'agit de trouver les solutions entières d'équations, on a longuement buté sur un extrait de Galois qui écrit : *"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 $x^{p-1} = 1$"*. Récemment, on a pu trouver sur la toile la référence [2] dans laquelle Libri explique sa méthode simple pour trouver les solutions entières d'une équation polynomiale et qui est fournie en annexe.
On réalise à ces lectures que les nombres premiers 3, 5, 7 *et* 11, par exemple, sont tous racines de l'équation polynomiale

$$(x-3)(x-5)(x-7)(x-11) = 0.$$

En développant le produit, on obtient l'équation polynomiale suivante :

$$x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0.$$

Les coefficients s'obtiennent ainsi :

$$26 = 3+5+7+11.$$
$$236 = 3.5 + 3.7 + 3.11 + 5.7 + 5.11 + 7.11.$$
$$886 = 3.5.7 + 3.5.11 + 3.7.11 + 5.7.11.$$
$$1155 = 3.5.7.11.$$

*On utilise le terme proposé par Gauss dans les Recherches Arithmétiques.

Plus généralement, pour exprimer que x, le nombre à chercher, est premier, on utilise une équation polynomiale de la forme suivante :

$$x^{\pi(n-2)-1} - \sigma_1.x^{\pi(n-2)-2} + \sigma_2.x^{\pi(n-2)-3} - \sigma_3.x^{\pi(n-2)-1} \ldots = 0$$

La plus grande puissance de x est $\pi(n-2)-1$ parce que la décomposition $1+(n-1)$ n'est jamais considérée comme une décomposition de Goldbach[†], le -1 servant à éliminer le nombre premier 2. Les nombres σ_i désignent respectivement les sommes de produits de i nombres premiers pris parmi tous les nombres premiers impairs considérés. Par exemple, $\sigma_1 = p_1 + p_2 + p_3 + p_4 ... = 3 + 5 + 7 + 11...$, $\sigma_2 = p_1p_2 + p_1p_3 + ... + p_2p_3 + p_2p_4 + ...$ et le dernier sigma est le produit de tous les nombres premiers impairs inférieurs à $n-2$.

Pour exprimer que $n-x$, le complémentaire du nombre à chercher doit être l'un des nombres premiers $3,\ 5,\ 7$ *ou* 11, on utilise la même équation polynomiale en remplaçant x par $n-x$:

$$((n-x)-3)((n-x)-5)((n-x)-7)((n-x)-11) = 0.$$

En développant le produit, on obtient l'équation polynomiale suivante :

$$(n-x)^4 - 26(n-x)^3 + 236(n-x)^2 - 886(n-x) + 1155 = 0.$$

L'élévation aux différentes puissances du monome $n-x$ donne les résultats ci-dessous :

$$\begin{array}{l}(n-x)^4 = x^4 - 4nx^3 + 6n^2x^2 - 4n^3x + n^4.\\ (n-x)^3 = -x^3 + 3nx^2 - 3n^2x + n^3.\\ (n-x)^2 = n^2 - 2nx + x^2.\end{array}$$

On reconnaît les coefficients du binôme C_i^j dans l'élévation de $n-x$ à la puissance i.

Si on développe et qu'on regroupe ensemble les coefficients concernant une même puissance de x, on obtient :

$$x^4 + (-4n+26)x^3 + (6n^2-78n+236)x^2 + (-4n^3+78n^2-472n+886)x + (n^4-26n^3+236n^2-886n+1155) = 0$$

On reconnaît dans la dernière parenthèse le polynôme initial dans lequel x a été remplacé par n. Puis pour les coefficients des puissances supérieures de x, on voit qu'on dérive successivement le polynôme initial puis les polynômes obtenus, qu'on prend l'opposé du résultat à chaque fois et qu'on divise successivement les résultats intermédiaires par 2, 3, etc.

Le polynôme initial est :

$$n^4 - 26n^3 + 236n^2 - 886n + 1155$$

On le dérive et on en prend l'opposé :

$$-4n^3 + 78n^2 - 472n + 886$$

On dérive ce dernier, on en prend l'opposé et on divise le résultat par 2 :

$$6n^2 - 78n + 236$$

On dérive ce dernier, on en prend l'opposé et on divise le résultat par 3 :

$$-4n + 26$$

Les coefficients d'expression $\frac{(-1)^n P^{(n)}(x)}{n!}$ sont appelés coefficients du développement de Taylor.

Les résultats de la théorie de Galois sur la résolubilité des équations polynomiales ne pourraient-ils pas être utilisés ici pour montrer que notre système de deux équations admet toujours une solution en x au moins ?...[‡]

[†] même si Cantor la comptait comme telle.

[‡] En annexe, on fournit les équations polynomiales de degré 5 qui permettent laborieusement de trouver les décomposants de Goldbach des nombres 14 et 16 qui ont comme nombres premiers impairs inférieurs à eux les nombres premiers $3, 5, 7, 11$ et 13 (!).

3 Exemples

Traitons les exemples $n = 8$ et $n = 10$. Il n'y a que trois nombres premiers impairs inférieurs à n, 3, 5 *et* 7.
L'équation polynomiale $(x-3)(x-5)(x-7) = 0$ se développe en $x^3 - 15x^2 + 71x - 105 = 0$.
L'équation polynomiale portant sur $n - x$ se développe quant à elle en :
$-x^3 + (3n-15)x^2 + (-3n^2 + 30n - 71)x + (n^3 - 15n^2 + 71n - 105) = 0$.
Si on remplace n par 8, on aboutit au système :

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 9x^2 - 23x + 15 = 0 \end{cases}$$

3 et 5 sont les seules solutions de ce système. Ce sont les décomposants de Goldbach de 8.

Si on remplace n par 10, on aboutit au système :

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 15x^2 - 71x + 105 = 0 \end{cases}$$

Les deux équations sont équivalentes, 3 et 5 et 7 sont solutions de ce système, et sont décomposants de Goldbach de 10.

4 Passer d'un degré au degré supérieur

Considérons d'abord les deux premières équations des deux systèmes pour les degrés 4 et 5. On passe de l'équation :

$$x^4 - \sigma_{1,4}x^3 + \sigma_{2,4}x^2 - \sigma_{3,4}x + \sigma_{4,4} = 0$$

à l'équation :

$$x^5 - \sigma_{1,5}x^4 + \sigma_{2,5}x^3 - \sigma_{3,5}x^2 + \sigma_{4,5}x - \sigma_{5,5} = 0$$

Les coefficients de l'équation de degré 5 ont été obtenus ainsi à partir de ceux de l'équation de degré 4.

$$\begin{array}{ll} \sigma_{1,5} = \sigma_{1,4} & +p_5 \\ \sigma_{2,5} = \sigma_{2,4} & +\sigma_{1,4}.p_5 \\ \sigma_{3,5} = \sigma_{3,4} & +\sigma_{2,4}.p_5 \\ \sigma_{4,5} = \sigma_{4,4} & +\sigma_{3,4}.p_5 \\ \sigma_{5,5} = & \sigma_{4,4}.p_5 \end{array}$$

Plus généralement, si p_i désigne le $p^{ième}$ nombre premier impair,

$$\begin{array}{ll} \sigma_{1,i} = \sigma_{1,i-1} & +p_i \\ \sigma_{2,i} = \sigma_{2,i-1} & +\sigma_{1,i-1}.p_i \\ \sigma_{3,i} = \sigma_{3,i-1} & +\sigma_{2,i-1}.p_i \\ \vdots & \\ \sigma_{i-1,i} = \sigma_{i-1,i-1} & +\sigma_{i-2,i-1}.p_i \\ \sigma_{i,i} = & +\sigma_{i-1,i-1}.p_i \end{array}$$

Considérons maintenant les deux secondes équations des deux systèmes :

Peut-être est-ce à cause de ce mécanisme de passage d'un degré au degré supérieur que les équations sont toujours résolubles ?...

Bibliographie

[1], **Evariste Galois**, *Sur la théorie des nombres*, Bulletin des Sciences mathématiques de M. Férussac, tome XIII, page 428, juin 1830. Note de J. Liouville : ce mémoire fait partie des recherches de M. Galois sur la théorie des permutations et des équations algébriques.

[2], **Guillaume Libri**, *Mémoire sur la théorie des nombres*, in *Mémoires de mathématiques*, extraits du *Journal de Mathématiques Pures et Appliquées*, publié par A.L. Crelle, Berlin, 1835, p.44.

Annexe 1 : extrait du Mémoire sur la théorie des nombres de Libri qui explique comment trouver les solutions entières d'une équation

limite n. Il faut remarquer surtout que les coefficiens des variables x, y, z, ... etc., dans le développement en série de l'intégrale qui forme le premier membre de l'équation (13.), sont tels qu'en calculant un certain nombre de termes, il ne reste à peu près que ce qu'il faut pour donner le nombre des solutions de l'équation proposée. C'est de cette considération, et de l'examen attentif de la nature de ces coefficiens (qui s'expriment aussi par des intégrales définies) que l'on pourrait déduire des considérations qui jetteraient beaucoup de lumière sur la marche de la fonction représentée par la formule (13.): mais ces recherches ne sauraient trouver place ici, et nous les exposerons dans un travail particulier.

Cet aperçu suffirait déjà pour montrer de quelle manière on pourrait réduire la théorie des nombres à l'analyse ordinaire: mais nous allons reprendre maintenant cette question dans toute sa généralité.

Étant proposée une équation à plusieurs inconnues à résoudres en nombres rationnels, fractionnaires ou entiers, on pourra toujours la préparer de manière que tous les nombres cherchés doivent être entiers et positifs: puisqu'en général, si l'équation proposée est de la forme

$$\varphi\,(x, y, z, \ldots\ \text{etc.}) = 0,$$

et que l'on cherche pour x, y, z, ... etc., des valeurs fractionnaires, en faisant

$$x = \frac{x_1}{x_2},\quad y = \frac{y_1}{y_2},\quad z = \frac{z_1}{z_2},\ \ldots\ \text{etc.},$$

on aura l'équation

$$\varphi\left(\frac{x_1}{x_2},\ \frac{y_1}{y_2},\ \frac{z_1}{z_2},\ \ldots\ \text{etc.}\right) = 0,$$

dans laquelle il ne faudra chercher pour

$$x_1,\ x_2,\ y_1,\ y_2,\ z_1,\ z_2,\ \ldots\ \text{etc.},$$

que des valeurs entières: et d'ailleurs s'il y avait des solutions négatives on les obtiendrait en changeant les signes des variables. Nous supposerons par conséquent que ces réductions soient toujours effectuées dans les équations dont nous chercherons la résolution.

Soit proposé de résoudre en nombres entiers et positifs l'équation

$$\varphi\,(x, y, z, \ldots\ \text{etc.}) = 0$$

que nous représenterons comme auparavant par $\varphi = 0$. Avec les méthodes connues on s'arrête là, et on tâche de résoudre cette équation en s'aidant de la forme particulière de ses coefficiens. Mais l'équatiou $\varphi = 0$, exprime seulement les relations qui doivent exister entre les inconnues, et n'indique pas que ces inconnues ne doivent recevoir que des valeurs entières et positives: pour exprimer cette dernière condition l'on supposera d'abord que l'on veuille trouver toutes les solutions qui s'obtiennent en donnant à x des valeurs moindres qu'une limite donnée a; à y des valeurs plus petites que b; à z des valeurs moindres que c; et ainsi de suite: $a, b, c, \ldots$ etc., étant des nombres entiers et positifs. Il est clair qu'à cet effet l'on devra donner à $x, y, z, \ldots$ etc., toutes les valeurs comprises dans les séries

$$\begin{aligned} x &= 0,\ 1,\ 2,\ 3, \ldots \ldots \ldots a-1; \\ y &= 0,\ 1,\ 2,\ 3, \ldots \ldots \ldots b-1; \\ z &= 0,\ 1,\ 2,\ 3, \ldots \ldots \ldots c-1; \\ & \ldots \ldots \ldots \ldots \ldots \ldots \text{etc.}; \end{aligned}$$

et faire toutes les combinaisons possibles dans l'équation $\varphi = 0$. On observera que toutes ces valeurs de x se trouveront parmi les racines de l'équation

$$X = x(x-1)(x-2)\ldots\ldots(x-(a-1)) = 0;$$

et que de mêmes les valeurs de y et de z seront comprises parmi les racines des équations

$$\begin{aligned} Y &= y(y-1)(y-2)\ldots\ldots(y-(b-1)) = 0; \\ Z &= z(z-1)(z-2)\ldots\ldots(z-(c-1)) = 0; \\ & \ldots \ldots \ldots \ldots \ldots \ldots \ldots \text{etc.} \end{aligned}$$

Les équations précédentes expriment les conditions que x soit un nombre entier positif moindre que a; que y soit un nombre entier positif moindre que b; et ainsi de suite. Ces équations dont le nombre est égal à celui des inconnues, étant combinées avec l'équation $\varphi = 0$, fournissent toutes les conditions du problème; de manière qu'ayant un nombre total d'équations qui surpasse de l'unité le nombre des inconnues, le problème sera plus que déterminé; en éliminant successivement toutes les inconnues entre ces équations, on aura une autre équation de condition $F = 0$, qui comprendra les limites $a, b, c, \ldots$ etc., assignées aux variables, et les coefficiens de l'équation proposée; et qui exprimera la relation qui doit exister entre ces quantités afin que le problème soit résoluble. Lorsque l'équation de condition sera satisfaite, et que l'on sera assuré que l'équation proposé peut être résolue, on reprendra l'une des équations à une seule inconnue que l'on a obtenues par l'élimination avant de parvenir à l'équation $F = 0$. Soit $X_1 = 0$, cette équation en x seul;

en cherchant le plus grand diviseur commun entre $X=0$, et $X_1=0$, on aura une équation de la forme $X_2=0$, qui ne contiendra que l'inconnue x, et dont le degré sera égal au nombre des valeurs de x qui satisfont à l'équation proposée; et en résolvant l'équation $X_2=0$, on aura toutes les valeurs de x qui satisfont à l'équation $\varphi=0$. On pourrait trouver de même les valeurs des autres inconnues, qui résolvent l'équation proposée; et l'on voit que ce principe s'applique encore à la recherche directe des racines rationnelles d'une équation à une seule inconnue; car ce problème aussi dépend de la théorie des nombres.

Avec la méthode que nous venons d'indiquer, on a seulement les racines inégales; mais s'il y a des racines égales, elles peuvent se trouver avec facilité de la manière suivante. Nous supposerons d'abord, pour simplifier la question, qu'il s'agisse d'une équation à deux inconnues seulement; puisque la méthode est absolument la même lorsque le nombre des variables est plus grand.

Maintenant soit proposé de résoudre en nombres rationnels l'équation

$$\varphi(x,y)=0;$$

et supposons que n valeurs rationnelles de $x=a$, correspondent à une seule valeur rationnelles de $y=b$; (n étant un nombre plus grand que l'unité) en différentiant l'équation proposée par rapport à x, et cherchant le plus grand commun diviseur Δ, entre

$$\frac{d.\varphi(x,y)}{dx} \quad \text{et} \quad \varphi(x,y),$$

on aura $\Delta=F(x,y)$, et il y aura un reste $R=f(y)$ qui ne contiendra plus x, et qui par supposition devra se réduire à zéro. Si l'on fait par conséquent $f(y)=0$, on cherchera les racines rationnelles $y=b$, $y=b_1$, $y=b_2$, ... etc., de cette équation, lorsqu'il en existe, et en substituant successivement b, b_1, b_2, ... etc., pour y dans l'expression de Δ on aura les équations

$$F(x,b)=0; \quad F(x,b_1)=0; \quad F(x,b_2)=0; \;.\;.\;.\;.\; \text{etc.}$$

que l'on tâchera de réduire à la forme $(x-a)^{n-1}=0$; et on trouvera de cette manière les valeurs multiples de x que l'on cherche.

Si l'on avait identiquement $R=0$, on trouverait l'équation

$$\Delta=F(x,y)=(x-\psi(y))^{n-1}=0,$$

qui devrait exister en même tems que l'équation $\varphi(x,y)=0$, et qui en serait un facteur: l'on ne pourrait donc pas déterminer de cette manière

Annexe 2 : exemples de degrés 4 et 5

Si on résoud les équations dont on a calculé les coefficients en remplaçant n successivement par les valeurs 12 (équations de degré 4 car il y a 4 nombres premiers impairs inférieurs à 12 qui sont $3, 5, 7$ et 11) puis par les valeurs 14 et 16 pour n (équations polynomiales de degré 5 car on a rajouté le nombre premier impair 13) avec un outil tel que l'outil libre Sage qui permet la résolution d'équations polynomiales, on arrive à résoudre les systèmes ci-dessous.

Pour $n = 12$, il faut résoudre le système :

$$\left\{ \begin{array}{l} x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0 \\ x^4 + (26-4n)x^3 + (6n^2 - 78n + 236)x^2 + (-4n^3 + 78n^2 - 472n + 886)x + (n^4 - 26n^3 + 236n^2 - 886n + 1155) = 0 \end{array} \right.$$

qui se ramène au système :

$$\left\{ \begin{array}{l} x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0 \\ x^4 - 22x^3 + 164x^2 - 458x + 315 = 0 \end{array} \right.$$

Les seules valeurs de x qui conviennent sont bien 5 et 7 qui sont bien les décomposants de Goldbach de 12.

Calculons les équations pour le degré 5 (nombres premiers impairs 3, 5, 7, 11 et 13).

$$x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 10725 = 0$$

avec

$3 + 5 + 7 + 11 + 13 = 39$
$3.5 + 3.7 + 3.11 + 3.13 + 5.7 + 5.11 + 5.13 + 7.11 + 7.13 + 11.13 = 574$
$3.5.7 + 3.5.11 + 3.5.13 + 3.7.11 + 3.7.13 + 3.11.13 + 5.7.11 + 5.7.13 + 5.11.13 + 7.11.13 = 3954$
$3.5.7.11 + 3.5.7.13 + 3.5.11.13 + 3.7.11.13 + 5.7.11.13 = 12673$
$3.5.7.11.13 = 15015.$

En remplaçant x par $n-x$, on obtient le polynôme suivant dont on cherche quelles valeurs de x l'annulent.

$$\begin{array}{rrrrrrr}
 & & & & & & -x^5 \\
 & & & & +(5n & -39) & x^4 \\
 & & & +(-10n^2 & +156n & -574) & x^3 \\
 & & +(10n^3 & -234n^2 & +1722n & -3954) & x^2 \\
 & +(-5n^4 & +156n^3 & -1722n^2 & +7908n & -12673) & x^1 \\
+(n^5 & -39n^4 & +574n^3 & -3954n^2 & +12673n & -15015) &
\end{array}$$

Pour $n = 14$ ou $n = 16$, il faut résoudre le système :

$$\left\{ \begin{array}{l} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + (5n-39)x^4 + (-10n^2 + 156n - 574)x^3 + (10n^3 - 234n^2 + 1722n - 3954)x^2 + \\ \qquad (-5n^4 + 156n^3 - 1722n^2 + 7908n - 12673)x + (n^5 - 39n^4 + 574n^3 - 3954n^2 + 12673n - 15015) = 0 \end{array} \right.$$

qui se ramène dans le cas de $n = 14$ au système :

$$\left\{ \begin{array}{l} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + 31x^4 - 350x^3 + 1730x^2 - 3489x + 2079 = 0 \end{array} \right.$$

Les seules valeurs de x qui conviennent sont $3, 7$ et 11, qui sont bien les décomposants de Goldbach de 14.

Pour $n = 16$, le système final à résoudre est :

$$\left\{ \begin{array}{l} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + 41x^4 - 638x^3 + 4654x^2 + 15681x - 19305 = 0 \end{array} \right.$$

Les seules valeurs de x qui conviennent sont $3, 5, 11$ et 13, qui sont bien les décomposants de Goldbach de 16.