Deux approches de la conjecture de Goldbach

Denise Vella

Mai 2006

1 Introduction

Dans une lettre à Euler du 7 juin 1742, Goldbach énonce *"il semble que tout nombre supérieur à* 2 *soit la somme de trois nombres premiers"*. Euler reformule cette conjecture en une forme équivalente qui est *"tout nombre entier naturel pair supérieur à 2 est la somme de deux nombres premiers"*[1].

2 Approche utilisant le nombre de facteurs de la factorisation d'une factorielle

Etudions quelques exemples. On cherche les sommes de deux nombres premiers valant 12 (on les appellera *décompositions Goldbach de* 12). Pour cela, on va disposer les nombres impairs dont la somme vaut 12 par colonnes ayant même total dans un tableau.

9	7
3	5

Calculons maintenant le nombre de facteurs du produit de ces nombres : 3.5.7.9. La factorisation de ce produit a 5 facteurs (potentiellement égaux). Or, le tableau contient quatre nombres disposés dans deux colonnes. Puisque $5 \leq 4+2$, il y a forcément deux nombres premiers dans une même colonne (en l'occurrence 5 et 7). Recherchons les décompositions Goldbach de 14. Les nombres sont alors disposés comme suit dans le tableau.

11	9	7
3	5	

La factorisation du produit des 5 nombres impairs fait intervenir 6 facteurs. $6 \leq 5 + 2$. Les 2 colonnes ne peuvent donc pas contenir chacune un composé.

Généralisons : si on a $2n$ nombres impairs (resp. $2n + 1$ dans un cas sur deux, quand on cherche les décompositions Goldbach du double d'un nombre impair) disposés dans n colonnes, et que la factorisation du produit de ces nombres impairs fait intervenir moins de $3n$ (resp. $3n+1$ dans le cas du double d'un impair) facteurs premiers, alors deux nombres premiers se retrouveront dans la même colonne et constitueront une décomposition Goldbach du nombre pair égal au total de chaque colonne (qui est $4n + 2$).

[1] Les recherches présentées ici ont été déclenchées par la lecture du roman de Doxiadis "Oncle Pétros et la Conjecture de Goldbach".

Problème : pour résoudre la conjecture, il faudrait donc :
1) être capable de trouver le nombre de facteurs du produit des $2n$ (ou $2n+1$) premiers nombres entiers impairs (on ne compte pas 1) ;
2) être capable de démontrer que ce nombre est toujours inférieur à $3n$ (ou $3n+1$).
Continuons par l'exemple : voyons les factorisations des nombres de 2 à 20 (ces factorisations nous intéressent pour trouver les décompositions Goldbach de 22).

2	2									
3				3						
4	2	2								
5						5				
6	2			3						
7							7			
8	2	2	2							
9				3	3					
10	2					5				
11								11		
12	2	2		3						
13									13	
14	2						7			
15				3		5				
16	2	2	2	2						
17										17
18	2			3	3					
19										19
20	2	2				5				

Le nombre de facteurs de la factorielle de 20 se décompose de la façon suivante (en les comptant colonne par colonne)[2] :

$10 + 5 + 2 + 1 = 18$ facteurs 2
$6 + 2 = 8$ facteurs 3
4 facteurs 5
2 facteurs 7
1 facteur 11
1 facteur 13
1 facteur 17
1 facteur 19
Soit un total de : 36 facteurs.

Voyons maintenant le nombre de facteurs du produit des nombres entiers pairs de 2 à 20. On peut obtenir ce nombre de facteurs en ajoutant 10 (le nombre de facteurs 2) au nombre de facteurs de la factorielle de 10. On obtient $10+15 = 25$. Par soustraction, on obtient le nombre de facteurs du produit des nombres impairs compris entre 3 et 19, en l'occurrence $36 - 25 = 11$ facteurs pour le produit des 10 premiers nombres entiers impairs (on oublie 1). Ce nombre étant inférieur à $3 \times 4 + 1 = 13$ correspondant au nombre de facteurs assurant la

[2]Lucas fait état de résultats dans sa théorie des nombres concernant la divisibilité des factorielles. Par exemple, le plus grand exposant de la puissance d'un nombre premier p contenue dans le produit $n!$ des n premiers nombres a pour limite supérieure $\frac{n}{p-1}$ (p.362).

présence de 2 nombres premiers dans une même colonne (ici 9 impairs de 3 à 19 à placer dans 4 colonnes selon la méthode vue plus haut), on est assuré que le nombre 22 a au moins une décomposition Goldbach.
Il faut être capable de prouver que, quelque soit x :

$$NbFact(\prod_{i=2}^{x}(2i-1)) \leq \lfloor \frac{3}{2}(x-2) \rfloor$$

La fonction *NbFact* renvoie pour x entier le nombre de facteurs (potentiellement égaux) que contient la factorisation de x.
L'inégalité est plus lisible si on l'écrit :

$$NbFact((2x)!) - NbFact(x!) - x \leq \lfloor \frac{3}{2}(x-1) \rfloor$$

Notons les premières valeurs des deux membres de l'inégalité dans un tableau. On appellera le terme à gauche de l'inégalité NFFPI (pour Nombre de Facteurs de la Factorisation du Produit des Impairs !) en entête de la colonne 4.

x	$NbFact((2x)!)$	$NbFact(x!)$	$NFFPI$	$\frac{3}{2}(x-1)$
4	11	4	3	4
5	15	5	5	6
6	19	7	6	7
7	22	8	7	9
8	28	11	9	10
9	32	13	10	12
10	36	15	11	13
11	40	16	13	15
12	45	19	14	16
13	49	20	16	18
14	55	22	19	19
15	59	24	20	21
16	65	28	21	22
17	69	29	23	24
18	75	32	25	25
19	78	33	26	27
20	83	36	27	28
21	87	38	28	30
22	91	40	29	31
23	96	41	32	33
24	102	45	32	34
25	107	47	35	36

Malheureusement, il suffit d'effectuer le calcul pour la factorielle de 100 à peine pour se rendre compte que l'idée ne tient pas.
$NbFact(100!) - NbFact(50!) - 50 = 81 > 73$.
Etudions ce qui se produit pour les décompositions Goldbach de 100 : il y a 14 nombres premiers impairs de 3 à 50 et 10 nombres impairs non premiers dans le même intervalle. "En face", il y a 10 nombres premiers dont on aurait pu imaginer qu'ils se soient justement et très "malencontreusement" positionnés en face des composés, ce qui aurait fait échouer la conjecture.

Les premiers sont parfois symétriques les uns des autres autour de x non pas à cause du fait qu'ils sont un rien si nombreux qu'il ne pourrait en être autrement mais bel et bien à cause de contraintes fortes pesant sur leurs positions, qui fait qu'au moins l'un d'entre eux "se positionne en face d'un nombre premier inférieur à x".

Autre idée : trouver selon un raisonnement un peu similaire que le nombre de facteurs du produit $Produit(2x - p_i)$ quel que soit i inférieur à $\Pi(x)$ est inférieur à $2\Pi(x)$, ce qui nous garantirait que l'un au moins des $2x - p_i$ serait premier. On a écrit *Produit* au lieu de la notation habituelle du produit par la lettre Π pour éviter de confondre les deux acceptions mathématiques possibles du symbole. Dit autrement, ceux qui sont "en face des premiers plus petits que x" ne peuvent pas être tous composés simultanément. Malheureusement, autant on sait calculer le nombre de facteurs d'un produit, en utilisant la formule $NbFact(xy) = NbFact(x) + NbFact(y)$ (qui se décline en particulier pour p premier par $NbFact(px) = NbFact(x) + 1$), autant on ne sait pas trouver le nombre de facteurs d'une somme, ce qui nous permettrait de trouver le nombre de facteurs de chacun des $2x - p_i$.

Dernière piste basée sur le calcul d'un nombre de facteurs :
Pour montrer que les $2x - p_i$ (p_i impair inférieur à x) ne peuvent pas être tous composés simultanément, il faudrait montrer que le nombre de facteurs du produit des nombres compris entre x (non compris) et $2x$ est toujours strictement inférieur au résultat de l'expression suivante $NbFact(x!) - NbFact((x/2)!) + 3x/2$ (si tous les $2x - p_i$ (p_i impair) étaient composés, ils auraient au moins deux facteurs chacun, ce qui entraînerait un total d'au moins x facteurs, auquel il faut ajouter le nombre de facteurs 2 de la première colonne égal à $x/2$ auquel il faut ajouter le nombre de facteurs des nombres compris entre $x/2$ et x, ce dernier étant égal à $NbFact(x!) - NbFact((x/2)!)$.

• S'octroyer le droit de conjecturer aussi. Conjecturons, conjecturons donc : je crois que du fait que ζ s'appuie sur Γ, il faut chercher pour comprendre ζ du côté de la divisibilité des factorielles (Γ est l'extension de la factorielle au plan complexe). J'ai lu dans la Théorie des nombres de Lucas un théorème intéressant sur la divisibilité des factorielles. Pour trouver l'exposant de 7 dans la factorielle de 10000, il divise itérativement 10000 par 7 et il ajoute les quotients. Cela a comme conséquence qu'un nombre premier est le seul nombre dont on soit sûr qu'il apparaît à puissance de 1 dans la factorisation de sa factorielle, les premiers plus petits que lui peuvent apparaître à puissance plus grande (par exemple dans la factorisation de 7!, 3 est dans 3 mais aussi caché dans 6). Peut-être que cette propriété mise au jour par Lucas permettrait de plaquer un ordre total sur les nombres, ce que ne permet pas la divisibilité qui plaque un ordre partiel sur eux. C'est peut-être aussi cette propriété qui aurait pour conséquence l'alignement des zéros...

Valuations p-adiques dans les factorisations des factorielles (Denise Vella-Chemla, 13.7.2017)

Lucas consacre dans sa théorie des nombres un paragraphe à la divisibilité des factorielles. Il fournit une procédure pour trouver la puissance d'un nombre premier p dans la factorisation de la factorielle d'un nombre entier n. Prenons un exemple ; pour connaître la puissance de 7 dans la factorielle de 10000, on divise successivement 10000 par 7, en obtenant comme quotients successifs 1428, 204, 29 et 4 et on ajoute ces quotients pour obtenir la valuation p-adique de 7 dans 10000 ! et qui est 1428+204+29+4=1665.

En réfléchissant un peu à cette idée, on réalise qu'un nombre premier p est à puissance 0 dans la factorisation de la factorielle de tout nombre qui lui est inférieur, à puissance 1 dans toute factorisation de la factorielle d'un entier de l'intervalle $[p, 2p[$ et à puissance supérieure à 1 pour les factorielles des nombres supérieurs ou égaux à $2p$.

Un nombre composé se distingue d'un nombre premier par le fait qu'il est à puissance au moins 2 dans la factorisation de sa propre factorielle (par exemple, 6 dans la factorielle de 6 apparaît "en tant que lui-même" mais également comme produit de ses 2 sous-facteurs 2 et 3 qui sont dans la factorielle l'un et l'autre séparément).

Cette propriété qu'un nombre premier p apparaît à puissance de 1 dans la factorisation de sa factorielle fournit une fonction qui permet de distinguer les nombres premiers des nombres composés (cette fonction associe à un nombre sa factorielle, puis extrait du nombre obtenu la valuation p-adique du nombre en question) ; les nombres premiers sont les seuls antécédents de 1 par cette fonction.

Ces propriétés permettent à nouveau d'illustrer ce que l'on peut entendre par "coïncidence de fonctions" : représentons le début de la droite numérique ainsi que les premiers nombres premiers. Représentons par des intervalles de valeurs ce qui a été énoncé ci-dessus. La deuxième ligne montre que la valuation p-adique de 3 dans les factorisations des factorielles des nombres compris entre 3 inclus et 6 exclus vaut 1 (et 0 pour des nombres inférieurs à 3 et plus que 1 pour des nombres supérieurs ou égaux à 6).

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	8	19	20	21	22	23
2	0	[	1	[							>1												
3		0	[	1		[							>1										
5			0		[		1			[						>1							

203. Divisibilité des factorielles. — Nous commencerons par résoudre le problème suivant : *Déterminer le plus grand exposant de la puissance d'un nombre a qui ne surpasse pas un nombre donné n.*

Une première méthode, directe, consiste à calculer le Tableau des puissances successives de a, jusqu'à ce que l'on obtienne un exposant α tel que l'on ait

$$a^{\alpha} \leqslant n < a^{\alpha+1},$$

et l'exposant cherché est α; on peut déterminer ainsi, par exemple, le plus grand exposant de la puissance de 2 contenue dans un nombre donné (n° 189, Remarque II).

Mais, au lieu d'employer les multiplications successives par a, on peut aussi employer les divisions successives par a. Cette méthode repose sur le théorème suivant : *Si q désigne le quotient par défaut de la division de n par a, et si q' désigne le quotient par défaut de la division de q par b, le nombre q' est égal*

au quotient par défaut de la division de n par le produit ab. En effet, on a par définition,

$$n = aq + r, \qquad q = bq' + s,$$

r désignant l'une des valeurs 0, 1, 2, ..., $(a-1)$, et s l'une des valeurs 0, 1, 2, ..., $(b-1)$. On déduit

$$n = abq' + (as + r);$$

mais le nombre non négatif $(as + r)$ est au plus égal à

$$a(b-1) + (a-1) \quad \text{ou} \quad (ab-1);$$

donc q' est le quotient exact, ou approché par défaut, de la division de n par ab.

On désigne habituellement le plus grand nombre entier contenu dans $\frac{n}{a}$ par la notation $\mathrm{E}\frac{n}{a}$, que l'on prononce *entier de n par a* : on a donc

$$\mathrm{E}\frac{\mathrm{E}\frac{n}{a}}{b} = \mathrm{E}\frac{n}{ab},$$

et cette formule s'applique, en général, à l'entier de $\frac{n}{abc\ldots}$.

Cela posé, nous résoudrons le problème suivant : *Déterminer le plus grand exposant de la puissance d'un nombre premier p contenue dans le produit n! des n premiers nombres.* Les entiers qui contiennent p en facteur dans la factorielle $n!$ sont tous les multiples de p

$$p, 2p, 3p, \ldots, \mathrm{E}\frac{n}{p}p, \qquad \text{en nombre } \mathrm{E}\frac{n}{p};$$

par suite, l'exposant de p dans cette factorielle est égal à l'exposant de p dans le produit

$$1.2.3\ldots.\mathrm{E}\frac{n}{p},$$

augmenté du dernier facteur. En répétant le même raisonnement sur cette nouvelle factorielle, et en appliquant le théorème précédent, il en résulte que l'exposant du nombre premier p dans la

factorielle $n!$ est égal à la somme

$$\mathrm{E}\frac{n}{p} + \mathrm{E}\frac{n}{p^2} + \mathrm{E}\frac{n}{p^3} + \dots.$$

Lorsque n est une puissance de p, les quotients de n par $p, p^2, p^3, \dots$, sont tous entiers, et l'on trouve pour l'exposant cherché

$$\frac{n-1}{p-1}.$$

Si l'on écrit le nombre n dans le système de numération de base p, en supposant

$$n = a + bp + cp^2 + dp^3 + \dots,$$

on trouve facilement que l'exposant cherché a pour valeur

$$\frac{n-(a+b+c+\dots)}{p-1},$$

et a pour limite supérieure

$$\frac{n}{p-1}.$$

Exemple I. — Quel est l'exposant de 7 dans le produit des 10000 premiers nombres?

On dispose le calcul de la manière suivante :

10000	7						
30	1428	7					
20	028	204	7				
60	0	64	29	7			
4		1	1	4			

et le nombre cherché est

$$1428 + 204 + 29 + 4 = 1665.$$

Exemple II. — Le produit des 1000 premiers nombres se termine par 249 zéros.

Exemple III. — Trouver le plus grand exposant de la puissance du nombre premier p contenue dans le nombre combinatoire C_m^n.

On a

$$\mathrm{C}_m^n = \frac{m!}{n!(m-n)!},$$

Valuations p-adiques des nombres dans les factorielles (Denise Vella-Chemla, 12.8.2017)

Dans la table suivante, on fournit dans la case (i, j) la valuation i-adique de i dans la factorielle de j (ou $val_i(j!)$, pour $i \geqslant 2$). On la note $<$ si elle est inférieure à 1, 1 si elle vaut 1 et $>$ si elle est supérieure à 1.

$val_3(4!) = val_3(4.3.2.1) = val_3(2.2.3.2.1) = 1$.

$val_9(6!) = val_9(6.5.4.3.2.1) = val_9(3.2.5.2.2.3.2.1) = 1$.

$val_i(j!)$	1	2	3	4	5	6	7	8	9	10
2	$<$	1	1	$>$	$>$	$>$	$>$	$>$	$>$	$>$
3	$<$	$<$	1	1	1	$>$	$>$	$>$	$>$	$>$
4	$<$	$<$	$<$	1	1	1	1	$>$	$>$	$>$
5	$<$	$<$	$<$	$<$	1	1	1	1	1	$>$
6	$<$	$<$	1	1	1	1	1	1	$>$	$>$
7	$<$	$<$	$<$	$<$	$<$	$<$	1	1	1	1
8	$<$	$<$	$<$	1	1	1	1	1	1	1
9	$<$	$<$	$<$	$<$	$<$	1	1	1	$>$	$>$
10	$<$	$<$	$<$	$<$	1	1	1	1	1	$>$

On note que $val_{p^2}((2p)!) = 1$.

On simplifie à l'extrême en n'utilisant que 3 images. On aurait pu utiliser une fonction val' qui aurait associé aux nombres des images rationnelles ; par exemple,

$$val'_9(12!) = val_9(12.11.10.9.8.7.6.5.4.3.2) = val'_9(2.2.3.11.2.5.3.3.2.2.2.7.2.3.5.2.2.3.2) = \frac{5}{2}.$$

Les seuls nombres tels que $val_x(x!) = 1$ sont les nombres premiers.

Pour voir si un autre élément permettrait de caractériser les nombres premiers, on calcule par programme dans $\mathbb{Z}/n\mathbb{Z}$ pour n pair le produit des $n/2$ nombres compris entre 1 et $n/2$, $k(n) = \prod_{x=1}^{n/2} x \ (mod\, n)$.

$k(n)$ est nul pour les nombres pairs. Voyons dans le tableau ci-dessous sa valeur pour les nombres impairs.

n	$k(n)$	n	$k(n)$	n	$k(n)$	n	$k(n)$	n	$k(n)$
$k(1)$	1	$k(21)$	0	$k(41)$	9	$k(61)$	11	$k(81)$	0
$k(3)$	1	$k(23)$	1	$k(43)$	42	$k(63)$	0	$k(83)$	1
$k(5)$	2	$k(25)$	0	$k(45)$	0	$k(65)$	0	$k(85)$	0
$k(7)$	6	$k(27)$	0	$k(47)$	46	$k(67)$	66	$k(87)$	0
$k(9)$	6	$k(29)$	12	$k(49)$	0	$k(69)$	0	$k(89)$	34
$k(11)$	10	$k(31)$	1	$k(51)$	0	$k(71)$	1	$k(91)$	0
$k(13)$	5	$k(33)$	0	$k(53)$	23	$k(73)$	27	$k(93)$	0
$k(15)$	0	$k(35)$	0	$k(55)$	0	$k(75)$	0	$k(95)$	0
$k(17)$	13	$k(37)$	31	$k(57)$	0	$k(77)$	0	$k(97)$	22
$k(19)$	18	$k(39)$	0	$k(59)$	1	$k(79)$	78	$k(99)$	0

Cette “moitié de factorielle”[†] de n est non-nulle pour les nombres premiers (sauf les nombres 1 et 9[‡]) tandis qu’elle est nulle pour les nombres composés.

Elle est égale à 1 ou $p-1$ pour les premiers $4k+3$ et à un nombre différent de 1 ou $p-1$ pour les premiers $4k+1$.