Conjecture de Goldbach et polynômes symétriques

Denise Vella

Août 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"*.

2 Solutions d'équations polynômiales ?

L'article "le théorème de Noël" du livre de Ian Gordon [**?**] présente le domaine de la "géométrie des nombres", dont Minkowski est à l'origine.
L'exemple suivant est présenté : dans $\mathbb{Z}_{17}$, l'équation polynômiale $(x-4y)(x+4y)=0$, équivalente à $x^2-16y^2=0$, est également équivalente à $x^2+y^2=0$ puisque $-16 \equiv 1\ (mod\ 17)$.
Ailleurs, on trouve un exemple similaire : dans $\mathbb{Z}_4$, le monôme $x+2$ est un diviseur de x^2 car $(x+2)^2 = x^2\ (mod\ 4)$ dans la mesure où le module 4 a fait disparaître le $4x+4$ du développement de $(x+2)^2$.
On peut imaginer que les nombres premiers qui fournissent une décomposition Goldbach d'un nombre pair sont les solutions d'une équation polynômiale particulière dans l'anneau $\mathbb{Z}_{2a}$ du nombre pair considéré. Par exemple, en sachant que $30 = 7+23 = 11+19 = 13+17$, on peut voir à quoi équivaut le développement du polynôme à trois indéterminées $(x-7)(y-11)(z-13)$ [1] dans $\mathbb{Z}_{30}$. On découvre alors parfois des similitudes entre certaines décompositions, qu'on présentera ici.[2]

3 Multiplication modulo $2a$

Observons quelques tables de multiplication dans $\mathbb{Z}_{2a}$. On ne s'intéresse qu'aux éléments inversibles, c'est à dire aux nombres premiers à $2a$.

[1] ou bien le polynôme à une seule indéterminée $(x-7)(x-11)(x-13)$

[2] On laissera de côté les nombres pairs doubles d'un nombre premier qui vérifient trivialement la conjecture (de tels nombres inférieurs à 100 sont 6, 10, 14, 22, 26, 34, 38, 46, 58, 62, 74, 82, 86, 94).

Dans $\mathbb{Z}_8$,

	1	3	5	7
1	1	3	−3	−1
3	3	1	−1	−3
5	−3	−1	1	3
7	−1	−3	3	1

Dans $\mathbb{Z}_{20}$,

	1	3	7	9	11	13	17	19
1	1	3	7	9	−9	−7	−3	−1
3	3	9	1	7	−7	-1	−9	−3
7	7	1	9	3	−3	−9	-1	−7
9	9	7	3	1	-1	−3	−7	−9
11	−9	−7	−3	-1	1	3	7	9
13	−7	-1	−9	−3	3	9	1	7
17	−3	−9	-1	−7	7	1	9	3
19	−1	−3	−7	−9	9	7	3	1

Ces tables présentent de multiples symétries : d'une part, par rapport aux diagonales parce que la multiplication est commutative, et parce que
$pq \equiv (2a-p)(2a-q)\ (mod\ 2a)$.
D'autre part, on voit des "sortes de symétries" verticale et horizontale par rapport aux lignes centrales de la table car $p(2x-q) = -pq$. Pour visualiser ces symétries, on matérialisera les axes de symétrie vertical et horizontal, en annexe 1. D'autre part, comme on a l'impression que c'est l'élément neutre de la multiplication 1 et son opposé pour l'addition −1 qui sont importants (cases colorées en bleu sur la précédente table), on ne remplira que les cases contenant ces valeurs.

Dana la table de 8, les racines de l'unité permettent d'obtenir des décompositions Goldbach de 8. Dans la table de 20, les nombres premiers dont le produit est égal à l'unité (en bleu dans la table), permettent tous de trouver des décompositions Goldbach de 20.

4 Analyse de cas triés par similitude

En annexe 2, on fournit toutes les décompositions Goldbach des nombres de 1 à 100, de 200 et de 500.

On essaie alors de trouver des similitudes entre les cas correspondant aux nombres pairs qui admettent le même nombre de décompositions[3].

[3]On n'arrive absolument pas, malgré de nombreuses tentatives, à trouver une formule qui fournirait le nombre de décompositions Goldbach de $2a$ en fonction du nombre de diviseurs de a, de leur type pair ou impair, de leur type *4n+1* ou *4n+3* classique dans le domaine, de la présence de carrés dans la décomposition, etc)

4.1 Une seule décomposition Goldbach

8 et 12 admettent une décomposition chacun seulement. $8 = 3+5$ et $12 = 5+7$. Ces cas présentent la similitude suivante : 3 et 5 sont racines de l'unité dans $\mathbb{Z}_8$, et 5 et 7 sont racines de l'unité dans $\mathbb{Z}_{12}$.

4.2 Deux décompositions Goldbach

Etudions alors les nombres qui admettent deux décompositions Goldbach, i.e. $16, 18, 20, 28, 32, 68$.

Dans $\mathbb{Z}_{16}$, $3 * 11 = 5 * 13 = 1$.
Dans $\mathbb{Z}_{18}$, $5 * 11 = 7 * 13 = 1$.
Dans $\mathbb{Z}_{20}$, $3 * 7 = 13 * 17 = 1$.
Dans $\mathbb{Z}_{28}$, $5 * 17 = 11 * 23 = 1$.

Cependant, ce ne sont pas les seuls produits de nombres premiers égaux à l'unité. Dans $\mathbb{Z}_{16}$, 7 est racine de l'unité sans fournir de décomposition. Dans $\mathbb{Z}_{18}$, il en est de même de 17. Dans $\mathbb{Z}_{20}$, c'est le cas de 11. Dans $\mathbb{Z}_{28}$, non seulement 13 est racine de l'unité sans fournir de solution mais le produit $3 * 19$ égale l'unité alors que ni 3, ni 19 ne participent à une solution.

Pour le nombre 32 qui a également 2 décompositions, 3 et 13 qui permettent chacun d'en trouver une ont même carré (modulo 32).

4.3 Trois décompositions Goldbach

Heureusement, on arrive alors au "merveilleux" cas 24, similaire aux cas $30, 40, 44, 52$ admettant chacun trois décompositions Goldbach.

24 possède les trois décompositions $5 + 19 = 7 + 17 = 11 + 13$.
5, 7, 11, 13, 17 et 19 sont tous racines de l'unité et $5 * 7 * 11 = 1$. Ce qui est merveilleux, c'est que les trois nombres 5, 7 et 11 se comportent un peu comme les trois sommets d'un triangle, le produit de deux sommets étant toujours égal au troisième sommet :

$$5 * 7 \equiv 11 \ (mod\ 24)$$
$$5 * 11 \equiv 7 \ (mod\ 24)$$
$$7 * 11 \equiv 5 \ (mod\ 24)$$

Dans le cas 30, on a aussi le même genre de configuration triangulaire mais les trois sommets ne sont pas équivalents comme on va le voir. Deux sommets seulement sur trois occupent des positions "symétriques" en quelque sorte. 30 possède les trois décompositions $7 + 23 = 11 + 19 = 13 + 17$. Or,

$$7 * 13 \equiv 1 \ (mod\ 30)$$
$$17 * 23 \equiv 1 \ (mod\ 30)$$
$$11^2 \equiv 1 \ (mod\ 30) \ (11\ est\ racine\ de\ l'unité).$$

D'autre part, on a les égalités modulaires suivantes :

$$7^2 * 19 \equiv 1 \ (mod\ 30)$$
$$13^2 * 19 \equiv 1 \ (mod\ 30)$$
$$7 * 11 \equiv 17 \ (mod\ 30)$$
$$7 * 19 \equiv 13 \ (mod\ 30)$$
$$11 * 13 \equiv 23 \ (mod\ 30)$$
$$11 * 17 \equiv 7 \ (mod\ 30)$$

Pour ce qui est du cas 40 ($= 3 + 37 = 11 + 29 = 17 + 23$), le produit de trois solutions égale l'unité : $3 * 11 * 17 = 1$ comme dans le cas 24 et 11 et 39 sont racines de l'unité. C'est comme si le sommet $(11, 19)$ "envoyait" $(7, 23)$ sur $(13, 17)$ et inversement "renvoyait" $(13, 17)$ sur $(7, 23)$. Comme dans le cas précédent, l'une des solutions occupe une position différente des deux autres : 11 est racine de l'unité et les égalités modulaires sont :

$$3 * 17 \equiv 11 \ (mod\ 40)$$
$$3 * 23 \equiv 29 \ (mod\ 40)$$
$$37 * 17 \equiv 29 \ (mod\ 40)$$
$$37 * 23 \equiv 11 \ (mod\ 40)$$

Ici, le sommet $(3, 37)$ envoie $(17, 23)$ sur $(11, 29)$ mais pas l'inverse.

Pour 44 ($= 3 + 41 = 7 + 37 = 13 + 31$),

$$7 * 13 \equiv 3 \ (mod\ 44)$$
$$7 * 31 \equiv 41 \ (mod\ 44)$$
$$37 * 13 \equiv 41 \ (mod\ 44)$$
$$37 * 31 \equiv 3 \ (mod\ 44)$$

Pour 52 ($= 5 + 47 = 11 + 41 = 23 + 29$)

$$5 * 23 \equiv 11 \ (mod\ 52)$$
$$5 * 29 \equiv 41 \ (mod\ 52)$$
$$47 * 23 \equiv 41 \ (mod\ 52)$$
$$47 * 29 \equiv 11 \ (mod\ 52)$$

4.4 Quatre décompositions Goldbach

Occupons-nous maintenant des nombres 36, 42, 50, 80, 88, 92 qui ont chacun 4 décompositions Goldbach, pour essayer de trouver des similitudes.

Pour 36 ($= 5 + 31 = 7 + 29 = 13 + 23 = 17 + 19$),

$$5 * 29 \equiv 1 \ (mod\ 36)$$
$$17^2 \equiv 1 \ (mod\ 36)$$
$$13^3 \equiv 1 \ (mod\ 36)$$

On arrive à trouver des produits qui "envoient" les solutions les unes sur les autres, mais parfois, cela n'est pas le cas :

$$13 * 5 \equiv 29 \ (mod\ 36)$$
$$13 * 29 \equiv 17 \ (mod\ 36)$$
$$13 * 17 \equiv 5 \ (mod\ 36)$$
$$13 * 7 \equiv 19 \ (mod\ 36)$$

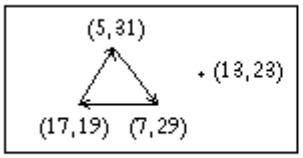
mais $17 * 7 \equiv 11$ et $17 * 5 \equiv 13$.

Pour 42 ($= 5 + 37 = 11 + 31 = 13 + 29 = 19 + 23$), on a les trois mêmes sortes de congruences :

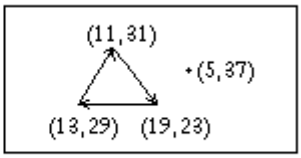
$$11 * 23 \equiv 1 \ (mod\ 42)$$
$$13^2 \equiv 1 \ (mod\ 42)$$
$$37^3 \equiv 1 \ (mod\ 42)$$

$$5 * 11 \equiv 13 \ (mod\ 42)$$
$$5 * 13 \equiv 23 \ (mod\ 42)$$
$$5 * 23 \equiv 31 \ (mod\ 42)$$
$$5 * 31 \equiv 29 \ (mod\ 42)$$
$$5 * 29 \equiv 19 \ (mod\ 42)$$
$$5 * 19 \equiv 11 \ (mod\ 42)$$

On peut obtenir la même chose avec 37, complémentaire de 5 à 42. C'est un peu comme si trois des solutions sur quatre étaient disposées en triangle, la quatrième étant extérieure au triangle et le sommet extérieur "agirait" sur les sommets du triangle pour faire subir une rotation au triangle, comme cela est présenté sur le petit dessin ci-après. La permutation des trois sommets du



Cas36 à 4 décompositions G.



Cas 42 à 4 décompositions G.

triangle, alors que le quatrième sommet reste fixe se note :

$$\begin{pmatrix} a & b & c & d \\ c & a & b & d \end{pmatrix}$$

En fait, on trouve dans l'article [**?**] qu'il vaut mieux géométriquement parlant voir cette permutation comme celle du groupe $A4$ des permutations paires sur 4 éléments, qui conserve le tétraèdre régulier a, b, c, d, et qui consiste en une rotation d'angle $2\Pi/3$ autour de l'axe du tétraèdre passant par d.

Pour 50 ($= 3 + 47 = 7 + 43 = 13 + 37 = 19 + 31$), $3 * 7 * 31 \equiv 1 \ (mod\ 50)$, $13^2 \equiv 37^2 \equiv 19 \ (mod\ 50), 13 * 19 \equiv 47 \ (mod\ 50), 19 * 3 \equiv 7 \ (mod\ 50)$.
Pour 80 ($= 7 + 73 = 13 + 67 = 19 + 61 = 37 + 43$), $13 * 37 \equiv 1 \ (mod\ 80), 13^2 \equiv 37 \ (mod\ 80), 13 * 19 \equiv 7 \ (mod\ 80)$.
Pour 88 ($= 5 + 83 = 17 + 71 = 29 + 59 = 41 + 47$), $5 * 17 * 29 \equiv 1 \ (mod\ 88), 29^2 * 41^2 \equiv 1 \ (mod\ 88)$.
Pour 92 ($= 3 + 89 = 13 + 79 = 19 + 73 = 31 + 61$), $3 * 31 \equiv 1 \ (mod\ 92), 3^2 * 19 \equiv 79 \ (mod\ 92)$.
Mais pour ces quatre derniers cas, on n'arrive pas à retrouver de permutations triangulaires des solutions.

4.5 Cinq décompositions Goldbach

Etudions maintenant les nombres qui admettent 5 décompositions Goldbach chacun (48, 54, 64, 70 et 76).
Pour 48 ($= 5+43 = 7+41 = 11+37 = 17+31 = 19+29$),

$$5 * 7 * 11 \equiv 1 \ (mod\ 48)$$
$$5 * 29 \equiv 1 \ (mod\ 48)$$
$$5 * 11 \equiv 7 \ (mod\ 48)$$
$$5 * 17 \equiv 37 \ (mod\ 48)$$
$$7^2 \equiv 1 \ (mod\ 48)$$
$$(et\ donc\ 41^2 \equiv 1 \ (mod\ 48))$$
$$17^2 \equiv 1 \ (mod\ 48)$$
$$(et\ donc\ 31^2 \equiv 1 \ (mod\ 48))$$
$$5^2 * 7 \equiv 31 \ (mod\ 48)$$
$$41^2 * 7 \equiv 31 \ (mod\ 48)$$
$$19^2 * 7 \equiv 31 \ (mod\ 48)$$

Pour 54 ($= 7+47 = 11+43 = 13+41 = 17+37 = 23+31$),

$$7 * 31 \equiv 1 \ (mod\ 54)$$
$$23 * 47 \equiv 1 \ (mod\ 54)$$
$$7 * 11 * 13 * 17 * 31 \equiv 1 \ (mod\ 54)$$
$$5^2 * 43 \equiv 1 \ (mod\ 54)$$
$$13^2 * 31 \equiv 1 \ (mod\ 54)$$

Pour 64 ($= 3+61 = 5+59 = 11+53 = 17+47 = 23+41$),

$$5 * 11 * 17 * 23 \equiv 1 \ (mod\ 64)$$
$$5^2 * 41 \equiv 1 \ (mod\ 64)$$

Pour 70 ($= 3+67 = 11+59 = 17+53 = 23+47 = 29+41$),

$$3 * 11 * 17 \equiv 1 \ (mod\ 70)$$
$$3 * 47 \equiv 1 \ (mod\ 70)$$
$$23 * 67 \equiv 1 \ (mod\ 70)$$
$$29^2 \equiv 1 \ (mod\ 70)$$

Pour 76 ($= 3+73 = 5+71 = 17+59 = 23+53 = 29+47$),

$$5 * 59 * 53 * 47 \equiv 1 \ (mod\ 76)$$
$$3^2 * 17 \equiv 1 \ (mod\ 76)$$

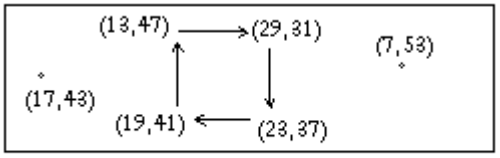
Pour les 5 nombres dont on vient de fournir les congruences qui semblent pertinentes, on n'a pas trouvé de représentation géométrique illustrative.

4.6 Six décompositions Goldbach

Voyons ce qui se passe pour les nombres qui admettent 6 décompositions Goldbach chacun (60, 66, 72 et 100).
Pour 60 ($= 7+53 = 13+47 = 17+43 = 19+41 = 23+37 = 29+31$),

$$7 * 13 * 17 * 23 \equiv 1 \ (mod\ 60)$$
$$19^2 \equiv 1 \ (mod\ 60)$$
$$29^2 \equiv 1 \ (mod\ 60)$$

Cette fois-ci, on peut voir quatre solutions disposées en carré, la cinquième et la sixième étant extérieures au carré et "amenant par la multiplication" un sommet sur le suivant, selon le schéma ci-après :



Cas 60 à 6 décompositions G.

L'un des sommets extérieurs fait tourner le carré dans un sens, tandis que l'autre sommet extérieur le fait tourner dans l'autre sens.

La permutation des quatre sommets en carré, alors que le cinquième sommet reste fixe se note

$$\begin{pmatrix} a & b & c & d & e & f \\ d & a & b & c & e & f \end{pmatrix}$$

dans un sens et

$$\begin{pmatrix} a & b & c & d & e & f \\ b & c & d & a & e & f \end{pmatrix}$$

dans l'autre sens.

$$\begin{aligned} 7 * 13 &\equiv 31 \ (mod\ 60) \\ 7 * 31 &\equiv 37 \ (mod\ 60) \\ 7 * 37 &\equiv 19 \ (mod\ 60) \\ 7 * 19 &\equiv 13 \ (mod\ 60) \end{aligned}$$

$$\begin{aligned} 17 * 13 &\equiv 41 \ (mod\ 60) \\ 17 * 19 &\equiv 23 \ (mod\ 60) \\ 17 * 23 &\equiv 31 \ (mod\ 60) \\ 17 * 29 &\equiv 13 \ (mod\ 60) \end{aligned}$$

Pour les 3 nombres qui suivent, on n'arrive pas à trouver de dessin pour conforter l'intuition.

Pour 66 $(= 5 + 61 = 7 + 59 = 13 + 53 = 19 + 47 = 23 + 43 = 29 + 37)$,

$$\begin{aligned} 5 * 13 * 19 * 23 * 29 &\equiv 1 \ (mod\ 66) \\ 5 * 53 &\equiv 1 \ (mod\ 66) \\ 7 * 19 &\equiv 1 \ (mod\ 66) \end{aligned}$$

Pour 72 $(= 5 + 67 = 11 + 61 = 13 + 59 = 19 + 53 = 29 + 43 = 31 + 41)$,

$$\begin{aligned} 5 * 11 * 19 * 29 * 31 &\equiv 1 \ (mod\ 72) \\ 5 * 29 &\equiv 1 \ (mod\ 72) \\ 11 * 59 &\equiv 1 \ (mod\ 72) \\ 19^2 &\equiv 1 \ (mod\ 72) \end{aligned}$$

Pour 100 $(= 3 + 97 = 11 + 89 = 17 + 83 = 29 + 71 = 41 + 59 = 47 + 53)$,

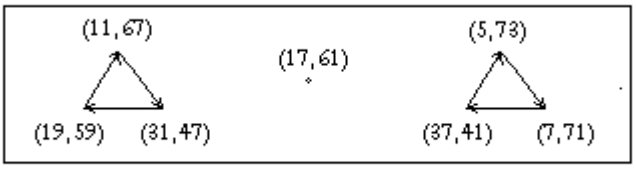
$$\begin{aligned} 3 * 11 * 17 * 41 &\equiv 1 \ (mod\ 100) \\ 17 * 53 &\equiv 1 \ (mod\ 100) \\ 47 * 83 &\equiv 1 \ (mod\ 100) \end{aligned}$$

4.7 Sept décompositions Goldbach

Etudions les nombres qui admettent 7 décompositions Goldbach chacun : 78 et 96.
Pour 78 ($= 5+73 = 7+71 = 11+67 = 17+61 = 19+59 = 31+47 = 37+41$),

$$5 * 7 * 11 * 19 * 31 * 37 \equiv 1 \ (mod\ 78)$$
$$17^6 \equiv 1 \ (mod\ 78)$$

Ce qui est intéessant dans le cas 78, c'est qu'on va à nouveau avoir une "belle" configuration : 5 est inverse de 47 (et donc 31 de 73), d'une part, et d'autre part, 7 est inverse de 67 (et complémentairement, 11 de 71). 17 est comme extérieur à deux triangles, sur les sommets desquels il opère une rotation. Expliquons cela sur le petit dessin suivant :



Cas 78 à 7 décompositions Goldbach

La permutation des deux triangles, alors que le septième sommet reste fixe se note :

$$\begin{pmatrix} a & b & c & d & e & f & g \\ c & a & b & d & g & e & f \end{pmatrix}$$

L'action de 17 sur le premier triangle correspond aux calculs modulaires suivants :

$$17 * 11 \equiv 31 \ (mod\ 78)$$
$$17 * 31 \equiv 59 \ (mod\ 78)$$
$$17 * 59 \equiv 67 \ (mod\ 78)$$
$$17 * 67 \equiv 47 \ (mod\ 78)$$
$$17 * 47 \equiv 19 \ (mod\ 78)$$
$$17 * 19 \equiv 11 \ (mod\ 78)$$

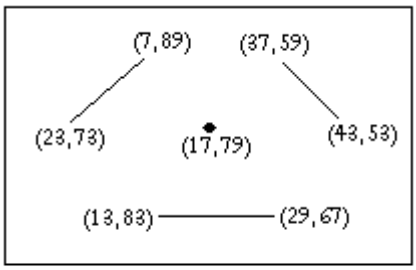
L'action de 17 sur le deuxième triangle correspond aux calculs modulaires suivants :

$$17 * 5 \equiv 7 \ (mod\ 78)$$
$$17 * 7 \equiv 41 \ (mod\ 78)$$
$$17 * 41 \equiv 73 \ (mod\ 78)$$
$$17 * 73 \equiv 71 \ (mod\ 78)$$
$$17 * 71 \equiv 37 \ (mod\ 78)$$
$$17 * 37 \equiv 5 \ (mod\ 78)$$

Pour 96 ($= 7+89 = 13+83 = 17+79 = 23+73 = 29+67 = 37+59 = 43+53$),

$$7 * 37 * 43 \equiv 1 \ (mod\ 96)$$
$$13^8 \equiv 1 \ (mod\ 96)$$
$$17^2 \equiv 1 \ (mod\ 96)$$
$$23^4 \equiv 1 \ (mod\ 96)$$
$$29^8 \equiv 1 \ (mod\ 96)$$

Ici, au lieu d'avoir deux triangles et un point au milieu, on a trois doublons et un point au milieu :



Cas 96 à 7 décompositions G.

La permutation des trois doublons du triangle, alors que le septième sommet reste fixe se note :

$$\begin{pmatrix} a & b & c & d & e & f & g \\ b & a & d & c & f & e & g \end{pmatrix}$$

$$7 * 7 \equiv 23 \ (mod\ 96)$$
$$17 * 23 \equiv 7 \ (mod\ 96)$$
$$17 * 37 \equiv 53 \ (mod\ 96)$$
$$17 * 43 \equiv 59 \ (mod\ 96)$$
$$17 * 13 \equiv 29 \ (mod\ 96)$$
$$17 * 29 \equiv 13 \ (mod\ 96)$$

4.8 Huit décompositions Goldbach

Enfin, étudions les nombres qui admettent 8 décompositions Goldbach, 84 et 200. Pour 84 ($= 5 + 79 = 11 + 73 = 13 + 71 = 17 + 67 = 31 + 53 = 37 + 47 = 41 + 43$),

$$5 * 17 \equiv 1 \ (mod\ 84)$$
$$11 * 23 \equiv 1 \ (mod\ 84)$$
$$13^2 \equiv 1 \ (mod\ 84)$$
$$(et\ donc\ 71^2 \equiv 1 \ (mod\ 84))$$
$$41^2 \equiv 1 \ (mod\ 84)$$
$$(et\ donc\ 43^2 \equiv 1 \ (mod\ 84))$$

Pour 200 ($= 3+197 = 7+193 = 19+181 = 37+163 = 43+157 = 61+139 = 73 + 127 = 97 + 103$), $3 * 7 * 181 \equiv 1 \ (mod\ 200)$.

Pour 500, $13 * 37 * 421 \equiv 1 \ (mod\ 500)$.

4.9 Résumé

Résumons les résultats dans un tableau afin de trouver une généralisation (dans la première colonne, on fournit le nombre de décompositions Goldbach, dans la deuxième colonne, on fournit une puissance de solution quand cette puissance est congrue à l'unité, ou un produit de puissances de solutions quand ce produit est

congru à l'unité et dans la troisième colonne, on fournit un produit de puissances inférieures de solutions quand il existe) :

Nombre de D.G.	$2a$	*solution à puissances élevées*	*solution simplifiée*
1	8	3^2	
	12	5^2	
2	16	$3 * 11$	
	18	$5 * 11$	
	20	$3 * 7$	
	28	$5 * 17$	
	32	$3^4 * 13^4$	
	68	$7^4 * 31^4$	
3	24	$7^2 * 5^2$	7^2 *et* 5^2
	30	$7^2 * 13^2$	
	40	$3^2 * 17^2$	
	44	$3^2 * 7^2$	
	52	$23^3 * 29^3$ *et* $5^2 * 47^2$	
	56	$3 * 19$	
	98	$19^2 * 31^2$	$19 * 31$
4	36	$5^2 * 7^2$	$5 * 29$
	42	$5^2 * 11^2$	
	50	$3^2 * 31^2$	
	80	$13^2 * 37^2$	$13 * 37$
	88	$29^2 * 41^2$	
	92	$3^2 * 31^2$	$89 * 61$
5	48	$5^2 * 11^2$	
	54	$7^2 * 23^2$	$7 * 23$
	64	$3^2 * 11^2$	
	70	$3^2 * 23^2$	
	76	$17^2 * 5$	
	136	$89^3 * 53^2$	
6	60	$7^3 * 43^3$	$7 * 43$
	66	$5^3 * 53^3$	$5 * 53$
	72	$5^3 * 53^3$	
	100	$17^3 * 53^3$	$17 * 53$
7	78	$5^4 * 61^3$	
8	84	$5^4 * 11^4$	
	200	$3^4 * 19^4$	
9	90	$11^2 * 31^2$	

Note spécifique pour le cas 52 : 23 et 29, les éléments du premier produit ne sont pas constitutifs de 2 décompositions Goldbach différentes, mais sont complémentaires (ils constituent ensemble une décomposition) ; de même de 5 et 47.

5 Polynômes symétriques

Ici, on recopie la définition trouvée dans [**?**].

Notons $\mathfrak{S}_n$ le groupe des permutations de $\{1, 2, ..., n\}$ appelé *groupe symétrique de degré n*. A tout $\sigma \in \mathfrak{S}_n$ et tout polynôme $f \in A[X_1, ..., X_n]$, on associe le polynôme que l'on notera f_σ, dans $A[X_1, ..., X_n]$, tel que

$$f_\sigma(X_1, ..., X_n) = f(X_{\sigma(1)}, ..., X_{\sigma(n)}).$$

Quels que soient σ, τ, dans $\mathfrak{S}_n$, on a

$$\begin{aligned} f_{\tau o \sigma}(X_1, ..., X_n) &= f(X_{\tau o \sigma(1)}, ..., X_{\tau o \sigma(n)}) \\ &= (f_\sigma)_\tau(X_1, ..., X_n) \end{aligned}$$

et pour l'élément unité e du groupe $\mathfrak{S}_n$, $f_e = f$.
On en déduit que le groupe $\mathfrak{S}_n$ opère sur $A[X_1, ..., X_n]$ par l'application

$$\begin{array}{ccc} \mathfrak{S}_n \times A[X_1, ..., X_n] & \longrightarrow & A[X_1, ..., X_n] \\ (\sigma, f) & \longmapsto & f_\sigma. \end{array}$$

définition : Un polynôme $f \in A[X_1, ..., X_n]$ est dit *symétrique* si

$$\forall \sigma \in \mathfrak{S}_n, f_\sigma = f.$$

Ajoutons deux extraits de [**?**].

- Cas du degré 2 :
  Un polynôme de degré 2 possède deux racines a et b (avec éventuellement $a = b$ dans le cas où P serait de discriminant nul). Comme vu précédemment, on peut alors factoriser P sous la forme

  $$P = \lambda(x - a)(x - b).$$

  et en développant :

  $$P = \lambda[x^2 - (a + b)x + ab]$$

  Cette relation détermine les coefficients du polynôme P au coefficient de proportionnalité λ près. On ne peut pas préciser mieux ce dernier, sauf si par exemple on connaît le coefficient de la plus grande puissance de x. La résolution des systèmes somme / produit est une application courante du résultat ci-dessus : si l'on connaît la somme S et le produit P de deux inconnues, on peut affirmer que celles-ci sont les racines de l'équation algébrique :

  $$x^2 - Sx + P = 0$$

  et réciproquement. En résolvant cette dernière, on résoud le système étudié.

- Cas du degré 3 :
  Un polynôme de degré 3 possède trois racines a, b et c comptées avec multiplicité. Par la factorisation de P, on obtient :

  $$P = \lambda(x-a)(x-b)(x-c).$$

  Pour développer cette expression, il est usuel d'introduire les quantités suivantes appelées *expressions symétriques élémentaires* :

  $$\begin{cases} \sigma_1 = a+b+c \\ \sigma_2 = ab+bc+ca \\ \sigma_3 = abc \end{cases}$$

  et on observe :

  $$P = \lambda[x^3 - \sigma_1 x^2 + \sigma_2 x - \sigma_3].$$

  En application de ce résultat, nous pouvons résoudre les systèmes à partir desquels il est possible de déterminer la somme σ_1 de trois inconnues, la somme σ_2 des doubles produits et le produit σ_3 de ces inconnues.

Enfin, dernier extrait : Si une fonction rationnelle de a, b, c, etc. est invariable par permutation de a, b, c, etc. alors elle s'exprime rationnellement en fonction des fonctions symétriques de ces lettres c'est à dire :

$$\begin{cases} \sigma_1 = a+b+c+etc. \\ \sigma_2 = ab+bc+etc. \\ \sigma_3 = abc+etc. \\ \quad ... \\ \sigma_n = abc... \end{cases}$$

où la première ligne coomprend la somme de toutes les racines, la seconde la somme des produits deux à deux, etc.

En annexe 4 sont fournis d'autres extraits.

Voici ce que l'on a découvert en effectuant cette sorte de calculs avec les nombres premiers permettant de trouver des décompositions Goldbach d'un nombre pair. Prenons trois des nombres premiers permettant de trouver les trois décompositions Goldbach de 24, qui sont 5, 7 et 11. Calculons, soit le polynôme à une seule inconnue, soit le polynôme à trois inconnues.

$$\begin{aligned} (x-5)(x-7)(x-11) &= x^3 - 23x^2 + 167x - 385 \\ &= x^3 + x^2 - x - 1 \\ &= (x+1)^2(x-1) \\ (x-5)(y-7)(z-11) &= xyz - 5yz - 7xz - 11xy + 55y + 77x + 35z - 385 \\ &= 1 - 23 + 167 - 385 \\ &= 0 \end{aligned}$$

De la même façon, pour le nombre 30 dont deux solutions sont 7 et 11,

$$\begin{aligned} (x-7)(x-11) &= xy - 7y - 11x + 77 \\ &\equiv xy - 7y - 11x + 17 \ (mod\ 30) \end{aligned}$$

Si $x = y = 1$, le polynôme s'annule.

De la même façon, pour le nombre 36 dont les solutions sont 5, 7, 13 et 17,

$$\begin{cases} \sigma_1 = 42 \\ \sigma_2 = 616 \\ \sigma_3 = 3702 \\ \sigma_4 = 7735 \end{cases}$$

La somme de ces nombres est -1 (mod 36). Ce qui est amusant, c'est que $\sigma_4 - \sigma_3 + \sigma_2 - \sigma_1$ est aussi congru à -1.

De la même façon, pour le nombre 40 dont les solutions sont 3, 11 et 17,

$$\begin{cases} \sigma_1 = 31 \\ \sigma_2 = 271 \\ \sigma_3 = 561 \end{cases}$$

$$31 - 271 + 561 = 1 \ (mod\ 40).$$

Pour le cas 42, les racines dont le produit vaut 1 sont $5, 11, 13$ et 23. Le calcul des fonctions symétriques élémentaires donne :

$$\begin{cases} \sigma_1 = 52 \\ \sigma_2 = 930 \\ \sigma_3 = 6764 \\ \sigma_4 = 16445 \end{cases}$$

La somme de tous ces nombres est congrue à -1 (modulo 42).

Pour le cas 48, les racines dont le produit est 1 sont $5, 7$ et 11. Le calcul des fonctions symétriques élémentaires donne :

$$\begin{cases} \sigma_1 = 23 \\ \sigma_2 = 167 \\ \sigma_3 = 385 \end{cases}$$

La somme de tous ces nombres est congrue e à -1 (modulo 48).

Pour le cas 50, les racines dont le produit vaut 1 sont $3, 7, 13$ et 19. Le calcul des fonctions symétriques élémentaires donne :

$$\begin{cases} \sigma_1 = 42 \\ \sigma_2 = 588 \\ \sigma_3 = 3142 \\ \sigma_4 = 5187 \end{cases}$$

Or, on n'a pas directement la congruence à l'unité. Si on veut l'obtenir, il faut remplacer σ_1 par $16 = 3+7-13+19$ et faire alors le calcul $16+588-3142+587$ et on trouve une congruence à -1 (modulo 50).

Pour le cas 52, les racines dont le produit vaut 1 sont $5, 11$ et 23. Le calcul des fonctions symétriques élémentaires donne :

$$\begin{cases} \sigma_1 = 39 \\ \sigma_2 = 423 \\ \sigma_3 = 1265 \end{cases}$$

La somme de tous ces nombres n'est pas égale à 1. Si on veut obtenir la congruence à l'unité, il faut remplacer σ_1 par 29 en affectant la racine 5, et elle seule, du signe $-$.

Pour le cas 64, les racines dont le produit vaut 1 sont $5, 11, 17, 23$. Le calcul des fonctions symétriques élémentaires donne :

$$\begin{cases} \sigma_1 = 56 \\ \sigma_2 = 1086 \\ \sigma_3 = 8456 \\ \sigma_4 = 21505 \end{cases}$$

La somme de tous ces nombres est égale à -1 (modulo 64).

Pour le cas 66, les racines dont le produit vaut 1 sont $5, 13, 19, 23, 29$. Le calcul des fonctions symétriques élémentaires donne :

$$\begin{cases} \sigma_1 = 89 \\ \sigma_2 = 2998 \\ \sigma_3 = 47078 \\ \sigma_4 = 335689 \\ \sigma_5 = 823745 \end{cases}$$

$\sigma_5 - \sigma_4 + \sigma_3 - \sigma_2 + \sigma_1$ vaut 1 (modulo 66).

Pour le cas 72, les racines dont le produit vaut -1 (modulo 72) sont $5, 11, 19, 29, 31$. Le calcul des fonctions symétriques élémentaires donne :

$$\begin{cases} \sigma_1 = 95 \\ \sigma_2 = 3358 \\ \sigma_3 = 54050 \\ \sigma_4 = 385441 \\ \sigma_5 = 939455 \end{cases}$$

Le calcul de ${}_5 - \sigma_4 + \sigma_3 - \sigma_2 + \sigma_1$ est congru à 1 (modulo 72).

6 Hypothèse informatique

Le nombre de permutations de k éléments est $k!$. Ici, on a deux nombres qui ont une seule décomposition Goldbach, tandis qu'on a 6 nombres qui ont deux décompositons Goldbach. Si 24 nombres ont 3 décompositions Goldbach chacun (sur les 1000000 premiers nombres, encore que !...), on aura la forte conviction qu'il y a un isomorphisme entre l'ensemble des nombres qui admettent k décompositions Goldbach et le groupe $\mathfrak{S}_k$ des permutations de k éléments. Malheureusement, après programmation sur les 1000000 de premiers nombres, le nombre de pairs qui ont respectivement 1, 2, 3, 4, 5 décompositions Goldbach semblent se fixer sur 2, 6, 8, 7, 11. On abandonne...

7 Restes des puissances

Quand on étudie les résidus des puissances des nombres premiers à $2a$, pour essayer de trouver des façons de discriminer les nombres premiers qui fournissent des décompositions Goldbach de ceux qui n'en fournissent pas, sans s'autoriser à effectuer des produits de 2 puissances de deux nombres premiers participant à des décompositions Goldbach différentes, on n'arrive strictement à rien sauf pour trois cas sur les cinquante étudiés et qui sont les nombres 74 (double de

37 qui est premier), 62 (une puissance de 2, ainsi que le double du premier 31) et 98 (quadruple de 7).

Pour le cas 74,

$$3^{18} \equiv 1$$
$$7^{9} \equiv 1$$
$$13^{18} \equiv 1$$
$$31^{4} \equiv 1$$
$$37^{27} \equiv 1$$

Les nombres 18, 9 et 4 sont tous diviseurs de $36 = 37 - 1$. Malheureusement, 12 l'est aussi et bien que $23^{12} \equiv 1$ et $29^{12} \equiv 1$, 23 et 29 ne fournissent pas de décomposition Goldbach de 74.

Pour le cas 62, les décompositions Goldbach sont fournies par les nombres 3 et 19 qui doivent être élevés à la puissance 30 pour obtenir l'unité. Les autres diviseurs de 30 ne permettent pas d'obtenir des décompositions Goldbach.

Enfin, pour le cas 98, 19 à la puissance 6 (le $p - 1$ de 7 seul diviseur premier impair de 98), ainsi que 31 à la puissance 6 permettent d'obtenir l'unité ; quant à 37, c'est à la puissance 31 qu'il faut l'élever.

Mais l'analyse d'un cas comme 58, double du premier 29, nous fait définitivement abandonner tout désir d'en passer par les puissances sans produit entre elles : les puissances permettant d'atteindre l'unité sont :

$$5^{14} \equiv 1$$
$$11^{19} \equiv 1$$
$$17^{4} \equiv 1$$
$$29^{27} \equiv 1$$

Autant on comprend les puissances 4 et 14 (qui divisent $28 = p - 1$), autant le 19 puissance de 11 est incompréhensible...

8 Diviseurs de $2a + 1$

Comme on cherche souvent des congruences à l'unité modulo $2n$, on peut se demander si un diviseur de $2n + 1$ permet toujours d'obtenir une décomposition Goldbach de $2n$. Cela est très souvent le cas (5 échecs seulement pour les nombres inférieurs à 100, ce qui est vraisemblablement énorme !). On trouvera en annexe 3 les calculs associés à cette tentative.

9 Conclusion

Tous ces résultats sont étranges, mais rien de systématique n'a été trouvé. De plus, Abel a prouvé l'impossibilité de résoudre l'équation générale de degré supérieur à 5 par radicaux. Il est vrai qu'ici, à aucun moment, il n'a été question d'équation générale. Enfin, quand on est seulement amatrice, les cours d'algèbre, de théorie des groupes, de théorie des anneaux sont totalement hermétiques, même si on aimerait beaucoup avoir une explication. Je suis informaticienne de formation. Ce qui guide ma recherche ici est une méthodologie que l'on utilise en théorie de la complexité informatique : pour prouver la NP-complétude d'un problème, on essaie de trouver un isomorphisme entre ce problème et un

problème dont la NP-complétude est prouvée. Je cherche ainsi un lien entre la conjecture et une représentation qui lui soit équivalente. En tous les cas, à feuilleter ces cours et ces ouvrages, car feuilleter est tout ce qu'on peut faire, on prend la pleine mesure de notre incompréhension. Finissons cependant humoristiquement avec cette citation de H.Poincaré in "La Science et l'Hypothèse" : *"une accumulation de faits n'est pas plus une science qu'un tas de pierre n'est une maison."*. Je dédie ce travail à mon père.

Annexe 1 : Tables de multiplication modulaires

Ici, on fournit les tables qui nous confortent dans l'idée qu'il faudrait pousser plus avant dans cette direction : celles dans lesquelles les nombres premiers dont le produit égale l'unité fournissent une décomposition Goldbach de $2a$. On rappelle que les seuls éléments inversibles sont les éléments premiers à $2a$.

Dans $\mathbb{Z}_{16}$, 2 solutions : $16 = 2^4 = 3 + 13 = 5 + 11$.

	1	3	5	7	9	11	13	15
1	1							-1
3			-1			1		
5		-1					1	
7				1	-1			
9				-1	1			
11		1					-1	
13			1			-1		
15	-1							1

Dans $\mathbb{Z}_{18}$, 2 solutions : $18 = 2 * 3^2 = 5 + 13 = 7 + 11$.

	1	5	7	11	13	17
1	1					-1
5			-1	1		
7		-1			1	
11		1			-1	
13			1	-1		
17	-1				1	

Dans $\mathbb{Z}_{24}$, 3 solutions : $24 = 2^3 * 3 = 5 + 19 = 7 + 17 = 11 + 13$.

	1	5	7	11	13	17	19	23
1	1							-1
5		1					-1	
7			1			-1		
11				1	-1			
13				-1	1			
17			-1			1		
19		-1					1	
23	-1							1

Dans $\mathbb{Z}_{28}$, 2 solutions : $28 = 2^2 * 7 = 5 + 23 = 11 + 17$.

	1	3	5	9	11	13	15	17	19	23	25	27
1	1											−1
3				−1					1			
5					−1			1				
9		−1									1	
11			−1							1		
13						1	−1					
15						−1	1					
17			1							−1		
19		1									−1	
23					1			−1				
25				1					−1			
27	−1											1

Dans $\mathbb{Z}_{30}$, 3 solutions : $30 = 2 * 3 * 5 = 7 + 23 = 11 + 19 = 13 + 17$.

	1	7	11	13	17	19	23	29
1	1							−1
7				1	−1			
11			1			−1		
13		1					−1	
17		−1					1	
19			−1			1		
23				−1	1			
29	−1							1

Les tables qui suivent auraient été trop grandes ; on n'en fournit que le quart haut-gauche puisque les trois autres quarts s'en déduisent par symétries et opposition. On retrouve seulement la symétrie par rapport à la diagonale.

Dans $\mathbb{Z}_{32}$, 2 solutions : $32 = 2^5 = 3 + 29 = 13 + 19$.

	1	3	5	7	9	11	13	15
1	1							
3						1		
5							1	
7					−1			
9				−1				
11		1						
13			1					
15								1

Dans $\mathbb{Z}_{40}$, 3 solutions : $40 = 2^3 * 5 = 3 + 37 = 11 + 29 = 17 + 23$.

	1	3	7	9	11	13	17	19
1	1							
3						-1		
7							-1	
9				1				
11					1			
13		-1						
17			-1					
19								1

Dans $\mathbb{Z}_{44}$, 2 solutions : $44 = 2^2 * 11 = 3 + 41 = 7 + 37 = 13 + 31$.

	1	3	5	7	9	13	15	17	19	21
1	1									
3							1			
5					1					
7									1	
9			1							
13								1		
15		1								
17						1				
19				1						
21										1

Dans $\mathbb{Z}_{48}$, 5 solutions : $48 = 2^4 * 3 = 5 + 43 = 7 + 41 = 11 + 37 = 17 + 31 = 19 + 29$.

	1	5	7	11	13	17	19	23
1	1							
5							-1	
7			1					
11					-1			
13				-1				
17						1		
19		-1						
23								1

Dans $\mathbb{Z}_{50}$, 4 solutions : $50 = 2 * 5^2 = 3 + 47 = 7 + 43 = 13 + 37 = 19 + 31$.

	1	3	7	9	11	13	17	19	21	23
1	1									
3							1			
7			-1							
9					-1					
11				-1						
13										-1
17		1								
19									-1	
21								-1		
23						-1				

Dans $\mathbb{Z}_{52}$, 3 solutions : $52 = 2^2 * 13 = 5 + 47 = 11 + 41 = 19 + 31$.

	1	3	5	7	9	11	15	17	19	21	23	25
1	1											
3								-1				
5										1		
7							1					
9											-1	
11									1			
15				1								
17		-1										
19						1						
21			1									
23					-1							
25												1

Dans $\mathbb{Z}_{56}$, 3 solutions : $56 = 2^3 * 7 = 3 + 53 = 13 + 43 = 19 + 37$.

	1	3	5	9	11	13	15	17	19	23	25	27
1	1											
3									1			
5					-1							
9											1	
11			-1									
13						1						
15							1					
17										-1		
19		1										
23								-1				
25				1								
27												1

Annexe 2 : Décompositions Goldbach des nombres pairs de 6 à 100, de 200 et de 500

6	$= 3 + 3$						
8	$= 3 + 5$						
10	$= 3 + 7$	$= 5 + 5$					
12	$= 5 + 7$						
14	$= 3 + 11$	$= 7 + 7$					
16	$= 3 + 13$	$= 5 + 11$					
18	$= 5 + 13$	$= 7 + 11$					
20	$= 3 + 17$	$= 7 + 13$					
22	$= 3 + 19$	$= 5 + 17$	$= 11 + 11$				
24	$= 5 + 19$	$= 7 + 17$	$= 11 + 13$				
26	$= 3 + 23$	$= 7 + 19$	$= 13 + 13$				
28	$= 5 + 23$	$= 11 + 17$					
30	$= 7 + 23$	$= 11 + 19$	$= 13 + 17$				
32	$= 3 + 29$	$= 13 + 19$					
34	$= 3 + 31$	$= 5 + 29$	$= 11 + 23$	$= 17 + 17$			
36	$= 5 + 31$	$= 7 + 29$	$= 13 + 23$	$= 17 + 19$			
38	$= 7 + 31$	$= 19 + 19$					
40	$= 3 + 37$	$= 11 + 29$	$= 17 + 23$				
42	$= 5 + 37$	$= 11 + 31$	$= 13 + 29$	$= 19 + 23$			
44	$= 3 + 41$	$= 7 + 37$	$= 13 + 31$				
46	$= 3 + 43$	$= 5 + 41$	$= 17 + 29$	$= 23 + 23$			
48	$= 5 + 43$	$= 7 + 41$	$= 11 + 37$	$= 17 + 31$	$= 19 + 29$		
50	$= 3 + 47$	$= 7 + 43$	$= 13 + 37$	$= 19 + 31$			
52	$= 5 + 47$	$= 11 + 41$	$= 23 + 29$				
54	$= 7 + 47$	$= 11 + 43$	$= 13 + 41$	$= 17 + 37$	$= 23 + 31$		
56	$= 3 + 53$	$= 13 + 43$	$= 19 + 37$				
58	$= 5 + 53$	$= 11 + 47$	$= 17 + 41$	$= 29 + 29$			
60	$= 7 + 53$	$= 13 + 47$	$= 17 + 43$	$= 19 + 41$	$= 23 + 37$	$= 29 + 31$	
62	$= 3 + 59$	$= 19 + 43$	$= 31 + 31$				
64	$= 3 + 61$	$= 5 + 59$	$= 11 + 53$	$= 17 + 47$	$= 23 + 41$		
66	$= 5 + 61$	$= 7 + 59$	$= 13 + 53$	$= 19 + 47$	$= 23 + 43$	$= 29 + 37$	
68	$= 7 + 61$	$= 31 + 37$					
70	$= 3 + 67$	$= 11 + 59$	$= 17 + 53$	$= 23 + 47$	$= 29 + 41$		
72	$= 5 + 67$	$= 11 + 61$	$= 13 + 59$	$= 19 + 53$	$= 29 + 43$	$= 31 + 41$	
74	$= 3 + 71$	$= 7 + 67$	$= 13 + 61$	$= 31 + 43$	$= 37 + 37$		
76	$= 3 + 73$	$= 5 + 71$	$= 17 + 59$	$= 23 + 53$	$= 29 + 47$		
78	$= 5 + 73$	$= 7 + 71$	$= 11 + 67$	$= 17 + 61$	$= 19 + 59$	$= 31 + 47$	$= 37 + 41$
80	$= 7 + 73$	$= 13 + 67$	$= 19 + 61$	$= 37 + 43$			
82	$= 3 + 79$	$= 11 + 71$	$= 23 + 59$	$= 29 + 53$	$= 41 + 41$		
84	$= 5 + 79$	$= 11 + 73$	$= 13 + 71$	$= 17 + 67$	$= 23 + 61$	$= 31 + 53$	$= 37 + 47$
	$= 41 + 43$						
86	$= 3 + 83$	$= 7 + 79$	$= 13 + 73$	$= 19 + 67$	$= 43 + 43$		
88	$= 5 + 83$	$= 17 + 71$	$= 29 + 59$	$= 41 + 47$			
90	$= 7 + 83$	$= 11 + 79$	$= 17 + 73$	$= 19 + 71$	$= 23 + 67$	$= 29 + 61$	$= 31 + 59$
	$= 37 + 53$	$= 43 + 47$					
92	$= 3 + 89$	$= 13 + 79$	$= 19 + 73$	$= 31 + 61$			
94	$= 5 + 89$	$= 11 + 83$	$= 23 + 71$	$= 41 + 53$	$= 47 + 47$		

96	$= 7 + 89$	$= 13 + 83$	$= 17 + 79$	$= 23 + 73$	$= 29 + 67$	$= 37 + 59$	$= 43 + 53$
98	$= 19 + 79$	$= 31 + 67$	$= 37 + 61$				
100	$= 3 + 97$	$= 11 + 89$	$= 17 + 83$	$= 29 + 71$	$= 41 + 59$	$= 47 + 53$	
200	$= 3 + 197$	$= 7 + 193$	$= 19 + 181$	$= 37 + 163$	$= 43 + 157$	$= 61 + 139$	
	$= 73 + 127$	$= 97 + 103$					
500	$= 13 + 487$	$= 37 + 463$	$= 43 + 457$	$= 61 + 439$	$= 67 + 433$	$= 79 + 421$	
	$= 103 + 397$	$127 + 373$	$= 151 + 349$	$= 163 + 337$	$= 193 + 307$	$= 223 + 277$	$= 229 + 271$

Annexe 3 : quand un diviseur de $2n+1$ fournit une décomposition Goldbach de $2n$

$9 = 3^2$	$8 = 3 + 5$
$15 = 3 * 5$	$14 = 3 + 11$
$21 = 3 * 7$	$20 = 3 + 17 = 7 + 13$
$25 = 5 * 5$	$24 = 5 + 19$
$27 = 3^3$	$26 = 3 + 23$
$33 = 3 * 11$	$32 = 3 + 29$
$35 = 5 * 7$	$34 = 5 + 29$
$39 = 3 * 13$	38 *ratage mais double de premier*
$45 = 3^2 * 5$	$44 = 3 + 41$
$49 = 7^2$	$48 = 7 + 41$
$51 = 3 * 17$	$50 = 3 + 47$
$55 = 5 * 11$	$54 = 11 + 43$
$57 = 3 * 19$	$56 = 3 + 53 = 19 + 3$
$63 = 3^2 * 7$	$62 = 3 + 59$
$65 = 5 * 13$	$64 = 5 + 59$
$69 = 3 * 23$	68 *ratage* ($= 2^2 * 17$)
$75 = 5^2 * 3$	$74 = 3 + 71$
$77 = 7 * 11$	76 *ratage* ($= 2^2 * 19$)
$81 = 3^4$	80 *ratage* ($= 2^4 * 5$)
$85 = 5 * 17$	$84 = 5 + 79 = 17 + 67$
$87 = 3 * 29$	$86 = 3 + 83$
$91 = 7 * 13$	$90 = 7 + 83$
$93 = 3 * 31$	$92 = 3 + 89 = 31 + 61$
$95 = 5 * 19$	$94 = 5 + 89$
$99 = 3^2 * 11$	98 *ratage* ($= 2 * 7^2$)
$201 = 3 * 67$	$200 = 3 + 197$
$501 = 3 * 167$	500 *ratage* ($= 2^2 * 5^3$).

Annexe 4 : éléments épars

- Extrait d'un numéro spécial du magazine la Recherche "Nombres" n°278, juillet/août 1995.

  Quand les paramètres et les variables de l'équation sont des éléments d'un corps fini (remarque de l'auteur : mais cela n'est pas le cas pour $\mathbb{Z}_n$ lorsque n n'est pas premier car il existe des diviseurs de 0), on dit que l'équation définit une courbe sur le corps fini considéré. Ce sont des courbes *algébriques*, car leurs équations sont toujours données par des polynômes. En effet, sur un corps fini, *toutes* les fonctions sont des polynômes, ce qui simplifie grandement les calculs : il n'y a ni sinus ni cosinus (cela découle du fait que pour tout élément x d'un tel corps, on a $x^q = x$, où q est le nombre d'éléments du corps). L'un des résultats les plus importants concerne le nombre de points d'une courbe algébrique sur un corps fini, c'est-à-dire le nombre de solutions du système d'équations correspondant. Le mathématicien français André Weil a prouvé en 1940 que le nombre N de points de la courbe vérifie l'ingégalité $N \leq q+1+2g\sqrt{q}$ (où q est le nombre d'éléments du corps considéré et g est le "genre" de la

courbe, un nombre qui mesure sa complexité). La généralisation de cette inégalité a valu à Pierre Deligne la médaille Fields en 1978.

- Extrait quelconque L'équation $x^n - 1 = 0$ est équivalente à autant d'équations particulières que $n - 1$ a de facteurs premiers et les degrés des équations sont les facteurs en question. Par exemple, l'équation $x^1 3 - 1 = 0$ puisque $13 - 1 = 12 = 2 * 2 * 3$ est équivalente à deux équations du second degré et une équation du troisième degré.

  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."

Extrait des oeuvres mathématiques d'Evariste Galois trouvées sur Gallica p.405 : "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 $Fx = 0$, 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 $x^{p^\nu - 1} = 1$.

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 ...] 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.

References

[1] J. Calais. *Eléments de théorie des anneaux : anneaux commutatifs*. Éd. Ellipses.

[2] A. Connes. *Symétries*. Éd. Magazine Pour la Science, n°292, février 2001.

[3] A. Doxiadis. *Oncle Pétros et la conjecture de Goldbach*. Éd. Points Seuil 2003.

[4] L. Euler. *Découverte d'une loi toute extraordinaire des nombres par rapport à la somme de leurs diviseurs*. Éd. Commentationes arithmeticae 2, p.639, 1849.

[5] M. Gardner. *L'univers ambidextre, les symétries de la nature*. Éd. Points Sciences.

[6] C.F. Gauss. *Recherches arithmétiques*. Éd. Jacques Gabay, 1989.

[7] . *Les équations algébriques*. Éd. Bibliothèque Tangente, HS n°22.

[8] P. Hoffman. *Erdös, l'homme qui n'aimait que les nombres*. Éd. Belin, 2000.

[9] C.A. Laisant. *Sur un procédé de vérification expérimentale du théorème de Goldbach*. Éd. Bulletin de la S.M.F., n°25, p.108, 1/12/1897.

[10] I. Stewart. *L'univers des nombres*. Éd. Belin Pour la Science, 2000.

[11] G. Tenenbaum, M. Mendès France. *Les nombres premiers*. Éd. Que sais-je ?, n°571, 1997.