# Vers une preuve de la conjecture de Goldbach

Denise Vella

Octobre 2005

*Résumé* : dans cet article, nous fournissons une preuve de la Conjecture de Goldbach, qui s'énonce de la façon suivante *"tout entier naturel pair supérieur ou égal à 4 est la somme de deux nombres premiers"*. La conjecture de Goldbach est équivalente à *"tout nombre entier supérieur ou égal à 2 est la moyenne de deux nombres premiers"*. Nous introduisons un treillis sur les nombres entiers naturels qui illustre au mieux un tel énoncé. La preuve que nous fournissons utilise les propriétés de l'arithmétique modulaire.

## 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].

Nous allons ici prouver la conjecture de Goldbach en utilisant un raisonnement qui utilise des calculs en arithmétique modulaire.

Préalablement, nous présentons un treillis sur les nombres entiers naturels qui nous a permis de trouver les idées qui sous-tendent la démonstration et qui en permet une meilleure appréhension. Nous fournissons également quelques exemples qui étayent notre propos. Nous étudions ensuite une approche informatique de ce problème. Enfin, nous fournissons les conséquences de la preuve de la conjecture.

## 2 Un curieux treillis

Il s'agit de prouver la conjecture de Goldbach, qui peut s'énoncer ainsi : *tout entier supérieur ou égal à 3 est à égale distance de deux nombres premiers*[2].

D'une autre manière, cela revient à prouver que l'application f définie ci-dessous est surjective.

$$\begin{aligned} f : \mathcal{P} - \{2\} \times \mathcal{P} - \{2\} &\to \mathcal{N} - \{0,1,2,3\}, \\ (P_i, P_j) &\mapsto (P_i + P_j)/2, \end{aligned}$$

[1] Les recherches présentées ici ont commencé il y a deux ans lorsque j'ai lu le roman de Doxiadis "Oncle Pétros et la Conjecture de Goldbach".

[2] Dans la mesure où 2 n'intervient pas dans les décompositions Goldbach, étant le seul nombre premier pair, nous en faisons un cas à part.

Nous notons $\mathcal{N}$ et $\mathcal{P}$ l'ensemble des entiers naturels et l'ensemble des nombres premiers.

Comment se fait-il qu'une telle application ne "rate" jamais d'entiers ?

Considérons le treillis (ou crible) de la figure **??** que nous appellerons dans la suite le treillis Goldbach.

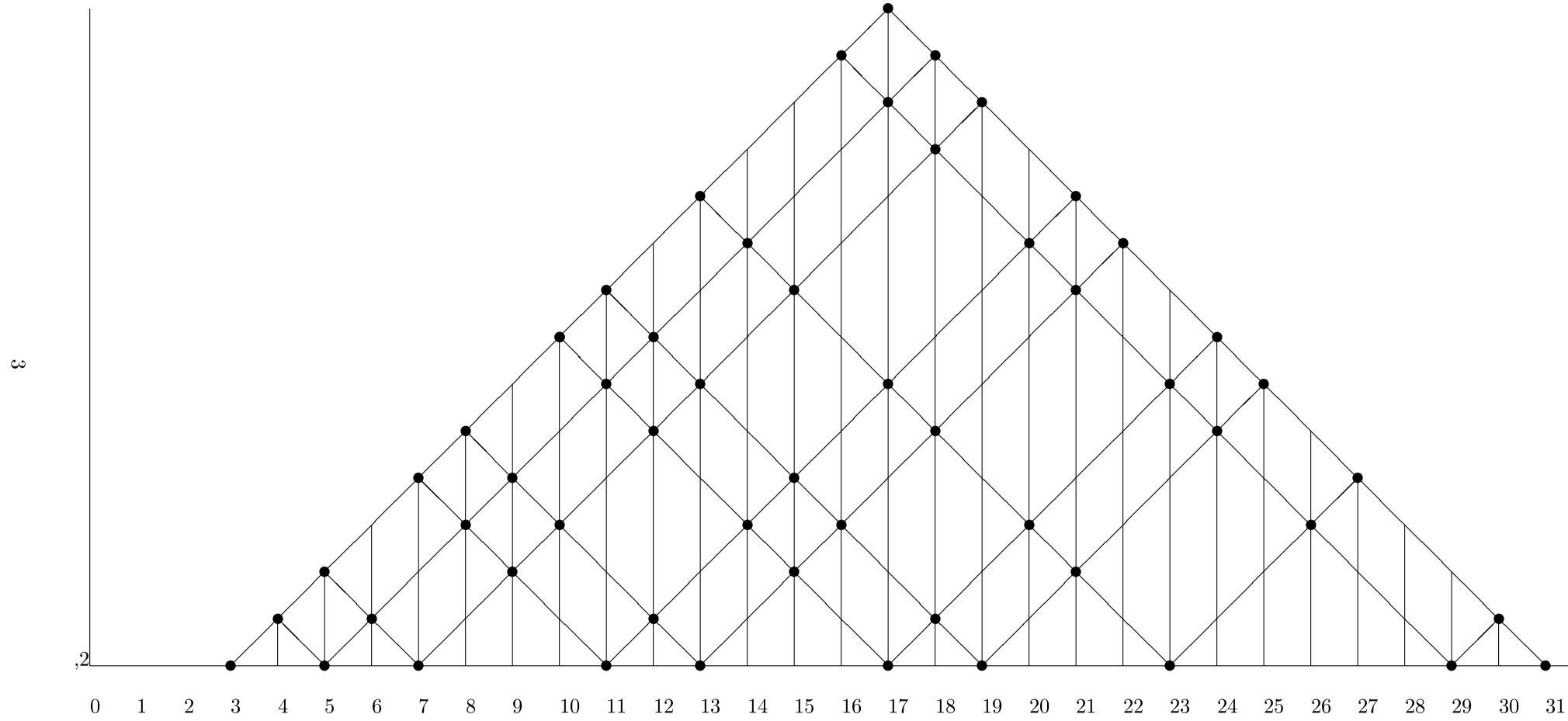



Figure 1: Le treillis Goldbach

Nous avons remplacé les lignes du treillis par des flèches pour le nombre 13 pour que soit plus explicite ce que nous entendons par *"diagonale ascendante"* et *"diagonale descendante"*.

Ce treillis se lit de la façon suivante : il y a un noeud au croisement de la diagonale ascendante correspondant à $P_i$, de la diagonale descendante correspondant à $P_j$, et de la verticale correspondant à $x$ si et seulement si $x = (P_i + P_j)/2$.
Nous appellerons un tel croisement un tri-croisement.

Par exemple, et pour ne pas surcharger le dessin, nous avons fait apparaître les verticales des entiers 4, 5, 7, 11, 12, 14 et 15.

Observons la diagonale ascendante d'un $P_i$ quelconque : elle se prolonge à l'infini et croise les diagonales descendantes de tous les $P_j$ qui sont supérieurs à $P_i$. Donc tout nombre premier intervient dans une infinité de décompositions Goldbach.

Par exemple, en ce qui concerne le nombre premier 3, on voit qu'il intervient dans l'une des décompositions Goldbach d'une infinité d'entiers naturels [3].
3 intervient dans l'une des décompositions Goldbach des entiers 3, 4, 5, 7, 8, 10, 11, 13, 16, 17...

$2\times11 = 3 + 19$
$2\times13 = 3 + 23$
$2\times16 = 3 + 29$
$2\times17 = 3 + 31$

Un entier naturel pourrait-il passer au travers des mailles du treillis Goldbach ? Démontrons maintenant que cela est impossible.

# 3 Preuve de la conjecture

Un nombre entier naturel peut être soit premier, soit composé.

Les nombres premiers correspondent au cas trivial : quand $x$ est premier, $2x$ est trivialement décomposable en somme de deux nombres premiers, en l'occurrence tous deux identiques à $x$.

Intéressons-nous maintenant aux nombres composés.
Soit $P_i$ le plus grand nombre premier inférieur à $x$ ($P_i < x < P_{i+1}$). Regardons le treillis Goldbach $\mathcal{T}$ de base $2x$.

[3] 3 intervient dans une des décompositions Goldbach de Pi(m) entiers naturels (Pi(m) étant la notation habituelle utilisée pour désigner le nombre de nombres premiers inférieurs ou égaux à m).

Prouvons que ce treillis "couvre" $x$. On dira qu'un treillis couvre $x$ s'il contient une décomposition Goldbach de $x$.

$x$ admet dans sa décomposition en facteurs premiers un certain nombre de $P_j \leq P_i$ (et $> 2$). $x$ ne peut pas admettre dans sa décomposition en facteurs premiers tous les $P_j \leq P_i$. Cela serait en contradiction avec le fait que $x$ est inférieur à $P_{i+1}$, lui-même très inférieur au produit de tous les $P_j$ inférieurs à $P_i$ (résultat de Tchebychev, qui a démontré le postulat de Bertrand : il y a toujours un nombre premier entre $n$ et $2n$).

- Premier cas : considérons l'un des $P_j$ intervenant dans la factorisation de $x$ et qui soit différent de 2 et de $P_j$.

  Un tel $P_j$ vérifie $2x - P_j \equiv 0 \pmod{P_j}$. Il ne nous permet donc pas de trouver une décomposition de $2x$ car $2x - P_j$ est non premier.

  Illustrons cela sur le schéma de la figure 1 :

  $15 = 3 \times 5$ et donc il n'y a pas de tri-croisement sur les diagonales ascendantes de 3 et 5 pour la verticale correspondant à 15.

- Deuxième cas : intéressons-nous maintenant à un $P_j$ qui ne serait pas un facteur de la décomposition en facteurs premiers de $x$. Alors, deux sous-cas se présentent :

  - cas 2a : soit le $P_j$ en question est tel qu'il existe un $P_k$ pour lequel :

    $$2x \equiv P_j \pmod{P_k}$$

    ; auquel cas, $P_j$ ne peut pas intervenir non plus dans une décomposition Goldbach de $2x$. En effet, $2x - P_j \equiv 0 \pmod{P_k}$, donc $2x - P_j$ n'est pas premier.
    Dans l'exemple que nous étudierons au paragraphe 5, cela correspondra aux cases $(2x, 5) = 3, (13, 5) = 3$ donc $(2x - 13, 5) = 0$.

  - cas 2b : soit le nombre premier $P_j$ en question est tel que, pour tout k :

    $$2x \not\equiv P_j \pmod{P_k}$$

    Alors $2x - P_j$ est premier et la paire d'entiers constituée des deux entiers $P_j$ et $2x - P_j$ est une décomposition Goldbach de $2x$.

    Pourquoi un tel $P_j$ existe-t-il forcément ?

    Il est tel que le système constitué des équations diophantiennes de la forme $2x - P_j \not\equiv 0(P_k)$ (quelque soit $P_k \leq P_i$) admet comme solution un $P_j$ inférieur à $P_i$.

    Rappelons que nous sommes dans le cas où $P_j$ ne divise pas $x$.
    L'équation

    $$-P_j.k + 2x.k' + P_j^2 - (P_j - P_j')^2 = 0$$

d'inconnues k et k' a une solution puisque $2x$ et $P_j$ sont premiers entre eux.
Posons :

$$a = P_j.k + (P_j - P'_j)^2$$
$$a = 2x.k' + P_j^2$$

Montrons qu'il existe un nombre premier $P'_j$ tel que $a = P'^2_j$.
On transforme

$$a = P_j.k + (P_j - P'_j)^2$$

en

$$a = (P_j - P'_j)^2 \pmod{P_j}.$$

D'où on tire $a = P'^2_j$ que l'on réintroduit dans

$$a = 2x.k' + P_j^2$$

que l'on avait précédemment transformé en

$$a = P_j^2 \pmod{2x}.$$

De là, on tire : $2x = P_j + P'_j$, ce qu'il fallait démontrer.

$P_j$ et $2x - P_j$ sont tous les deux premiers et permettent d'obtenir une décomposition Goldbach de $2x$.
*exemple :* on cherche à trouver la décomposition $28 = 11 + 17$.
Cela revient à résoudre l'équation $-17k + 28k' + 253 = 0$.
Cette équation en k et k' a comme solution $k = 5, k' = 6$.
$p_1 = \sqrt{28k' + 17^2} = \sqrt{121} = 11$
$p_2 = 28 - 11 = 17$.

On en conclut que $2x$ est toujours couvert par un $P_j$ dont $x$ n'est pas multiple.

# 4 Illustration par un exemple

Intéressons-nous au nombre $x = 14$. Ci-dessous, lisons le tableau[4] qui fournit les résultats des opérations de congruence appliquées aux différents nombres qui présentent un intérêt pour trouver la décomposition Goldbach de 14.

[4] La case $(x, z)$ du tableau contient le nombre $y$ si $x \equiv y \pmod{z}$

| *modulo* | 3 | 5 | 7 | 11 | 13 |
|---|---|---|---|---|---|
| 3 | **0** | 3 | 3 | 3 | 3 |
| 5 | 2 | **0** | 5 | 5 | 5 |
| 7 | 1 | 2 | **0** | 7 | 7 |
| 11 | 2 | 1 | 4 | **0** | 11 |
| 13 | 1 | 3 | 6 | 2 | **0** |
| | | | | | |
| 14 | 2 | 4 | 0 | 3 | 1 |
| 28 | 1 | 3 | 0 | 6 | 2 |
| | | | | | |
| -13 | 2 | 2 | 1 | 9 | **0** |
| -11 | 1 | 4 | 3 | **0** | 2 |
| -7 | 2 | 3 | **0** | 4 | 6 |
| -5 | 1 | **0** | 2 | 6 | 8 |
| -3 | **0** | 2 | 4 | 8 | 10 |
| | | | | | |
| 2x-13 | 0 | 0 | 1 | 4 | 2 |
| 2x-11 | 2 | 2 | 3 | 6 | 4 |
| 2x-7 | 0 | 1 | 0 | 10 | 8 |
| 2x-5 | 2 | 3 | 2 | 1 | 10 |
| 2x-3 | 1 | 0 | 4 | 3 | 12 |

La ligne 6 correspond à $x$, la ligne 7 correspond à $2x$.
Les lignes (1) à (5) seront appelées partie A du tableau, les lignes (8) à (12) partie B, et les lignes (13) à (17) partie C.
Le système d'équations diophantiennes auquel il a été fait référence au paragraphe 3b est le suivant dans le cas de $x = 14$ :

$$\begin{aligned} 2x - 11 &= 3a + 2, \\ 2x - 11 &= 5b + 2, \\ 2x - 11 &= 7c + 3, \\ 2x - 11 &= 11d + 6, \\ 2x - 11 &= 13e + 4. \end{aligned}$$

Ce système a comme solution pour $x = 14$ le quintuplet $(a = 5, b = 3, c = 2, d = 1, e = 1)$.
On voit que les parties A et B du tableau ont toutes les deux leurs diagonales remplies de zéros (en gras dans le tableau) car chaque nombre premier est égal à 0 modulo lui-même.
D'autre part, $x = 14 = 2 \times 7$.
On voit un zéro à l'intersection de la ligne $2x - 7$ et de la colonne 7.

Pourquoi a-t-on un zéro dans la case $(2x - 13, 3)$ ? Prenons les cases $(2x, 3)$ et $(13, 3)$. Elles contiennent toutes deux un 1. Nous sommes dans le cas 2a du paragraphe 4 ci-dessus.

A quelle condition une ligne de la partie C du tableau correspond-elle à un nombre premier ?

Pour que $2x - P_j$ soit premier, il faut que toutes les cases de la ligne corre-

spondant à $2x - P_j$ soient non nulles. Les deux nombres premiers $P_j$ et $2x - P_j$ constituent alors une décomposition Goldbach de $2x$.

On voit que dans notre exemple, 28 a deux décompositions : 11 et $2x - 11 = 17$ d'une part, 5 et $2x - 5 = 23$, d'autre part.
De même, on voit sur la verticale de 15 les trois décompositions de 30 ($13 + 17$, $11 + 19$ et $7 + 23$).

# 5 Goldbach for children

## 5.1 Les billes

Imaginons que l'on a un nombre pair de billes.
On peut séparer ces billes en mettant le même nombre de billes dans deux sacs différents.
Imaginons maintenant que l'on fasse passer les billes une par une d'un sac à l'autre (en faisant toujours passer les billes de droite à gauche par exemple). Alors, la conjecture de Goldbach déclare qu'à un moment donné, et ce avant que l'on ait vidé tout le sac de droite, il y aura un nombre premier de billes dans chacun des sacs.

## 5.2 Les Lego

Considérons un nombre $x$ que l'on veut placer exactement entre deux nombres premiers. Ce nombre $x$ est à deux distances $\Delta_{gauche}$ et $\Delta_{droite}$ des nombres premiers qui l'entourent. Représentons ces distances par des briques du célèbre jeu de Lego.

Considérons la suite des $\Delta_i$, qui donne l'écart entre deux nombres premiers $P_i$ et $P_{i+1}$ consécutifs. Voyons ces $\Delta_i$ comme des briques Lego que nous allons assembler à droite et à gauche des briques initiales et dans l'ordre dans lequel elles apparaissent pour avoir deux suites de briques de même longueur.

Les briques de longueur 2 peuvent être vues comme permettant en quelque sorte d' "affiner" nos deux séries de briques droite et gauche pour qu'elles soient de plus en plus proches l'une de l'autre.

# 6 Utilisons l'outil informatique

Dans le domaine des nombres premiers, les ordinateurs sont utilisés pour établir des records tels que *"le plus grand nombre premier trouvé à ce jour possède plus de 7 millions de chiffres, et s'appelle peut-être Mersenne 42"* ou bien *"jusqu'à* $2 \times 10^{17}$*, la conjecture de Goldbach est vraie"* (résultat établi par Oliveira et Silva en février 2005).

## 6.1 Par de multiples détours

Les recherches que nous avions entamées il y a deux ans suite à la lecture de [**?**], puis abandonnées, ont pris un nouvel essor en septembre 2005, avec la sortie

en France de la traduction du livre de Marcus Du Sautoy [7], un livre de vulgarisation scientifique. Elles ont été ensuite enrichies par la lecture du livre de Jean-Paul Delahaye [**?**] puis totalement réorientées en parcourant le livre de [**?**]

Au tout début, nous réfléchissions à une manière élégante d'implémenter les horloges modulaires Gaussiennes. On peut voir l'horloge modulaire de $n$ comme un polygone régulier à $n$ côtés sur le cercle unité. Prenons comme convention que tous les polygones ont en commun le sommet correspondant à midi. Deux nombres sont premiers entre eux si leurs polygones réguliers respectifs n'ont aucun sommet commun hormis le sommet midi. Cette idée des polygones réguliers nous a fait faire un détour par les fractions à coefficients entiers. 4 n'est pas premier car $2/4 = 1/2$. Cela nous a amenée naturellement a nous rendre compte qu'un nombre était premier si toutes les fractions de $1/n$ à $(n-1)/n$ étaient non réductibles.

La considération des fractions entières $1/5$, $2/5$, $3/5$, $4/5$, nous a fait dériver vers les sinusoïdes. En effet, les sinusoïdes sont des fonctions qui passent régulièrement par zéro. La sinusoïde $\sin(5\pi x)$ s'annule justement pour les 4 fractions qui nous intéressent sur l'intervalle $]0,1[$. Un nombre $n$ est ainsi premier si sa sinusoïde s'annule exactement $n-1$ fois dans l'intervalle $]0,1[$ et ce, jamais sur un point pour lequel s'annule la sinusoïde d'un nombre premier inférieur à lui.

Nous avons vite abandonné cette voie de recherche : le fait d'assimiler un nombre premier $p$ à sa sinusoïde $\sin(p\pi x)$ semblait ne pas présenter d'intérêt ; en effet, même si cela a l'avantage de restreindre l'étude à l'intervalle $]0,1[$, dans la mesure où il y a une infinité de sinusoïdes qui s'annulent dans cet intervalle, on ne fait que transformer un problème sur des données infiniment grandes en un problème sur des données infiniment petites.

Cette vision *"ondulatoire"* des nombres premiers est cependant à rapprocher de la méthode du crible d'Érathostène, et pourrait expliquer la raréfaction des nombres premiers. Un nombre est premier s'il n'existe pas de nombre premier dont il soit le multiple. Le crible d'Érathostène élimine ainsi successivement les multiples de 2, puis de 3, puis de 5, etc.

Mettons-nous à la place d'un nombre (par exemple 17) qui regarde passer les filtres des nombres premiers qui vont éliminer peu à peu tous les nombres qui sont leurs composés.

Le filtre de 2 passe, 17 le traverse avec succès étant impair, 17 traverse également avec succès le filtre de 3, celui de 5, celui de 7, puis celui de 11, et enfin celui de 13. Du côté des sinusoïdes, de plus en plus de points de l'intervalle $]0,1[$ ont été touchés par les nombres premiers de 3 à 13. 17 a en quelque sorte de moins en moins de place pour pouvoir faire passer sa propre sinusoïde. Les zéros de la sinusoïde de 17 réussissent tout de même à s'intercaler entre les zéros des autres sinusoïdes.

Partant de là, plus un nombre est grand, plus il a de filtres à traverser, et moins il semblerait probabilistiquement parlant qu'il ait de chance d'être pre-

mier. Dit autrement, moins sa sinusoïde n'a d'espace pour intercaler ses zéros sur l'intervalle ]0,1[. Cette raréfaction des nombres premiers a été démontrée (par Legendre, Euler ou encore Hadamar et la Vallée-Poussin).

En consultant la bibliographie abondante du domaine des nombres premiers, nous nous sommes aperçue que Mikolas avait prouvé le lien entre les fractions (suites de Farey) et les nombres premiers en 1949. Nous n'avions qu'un demi-siècle de retard ! Ces recherches présentent cependant un intérêt certain : dans l'article [**?**], il est fait référence à une façon d'associer à chaque fraction non réductible de l'arbre de Stern-Brocot, (et par extension à chaque fraction d'une suite de Farey, et par similitude à chaque nombre premier) un mot appartenant à un langage basé sur un alphabet binaire $\{L,\ R\}$ selon la position des fractions dans l'arbre de Stern-Brocot ($L$ signifiant que la fraction est fille gauche de son père et $R$ signifiant qu'elle en est fille droite). Cette voie serait à explorer pour trouver un programme qui s'arrête et qui prouve la conjecture de Goldbach. Enfin, concernant les propriétés étranges des fractions entières faisant intervenir des nombres premiers, on consultera la référence [**?**] qui présente de nombreux résultats très intéressants.

Avant de démontrer la conjecture, nous avons implémenté un programme qui calcule les moyennes des nombres premiers deux à deux jusqu'à un nombre premier donné. On se rend compte que ce programme engendre tous les entiers naturels "assez loin" (en fait, jusqu'à $10^6$, le ratio le plus faible que l'on ait trouvé entre le plus petit entier naturel non engendré par un treillis de base allant jusqu'à un certain nombre premier a été 22/29 (proche de 0.75). Le premier nombre non couvert par un treillis de base approximative $2x$ semble toujours supérieur à 3/4 de $x$. Il faudrait exprimer de façon précise la limite de la fonction qui à $x$ associe le rapport entre $x$ et le plus petit entier naturel non engendré par le treillis de base approximative $2x$ mais nous n'avons pas les compétences mathématiques nécessaires au développement de tels résultats.

## 6.2 Conséquences de la preuve

Il fallait pour se convaincre "travailler à l'aveugle". Nous avons choisi dans la suite des $\Delta_i$ que nous avions obtenue par programme un $\Delta_i$ au hasard.

Quelle est la procédure à suivre pour trouver la décomposition Goldbach d'un entier compris entre $P_i$ et $P_{i+1}$, qui se trouve à distance $\Delta_{gauche}$ de $P_i$ et $\Delta_{droit}$ de $P_{i+1}$ ?

Soit la suite définie de la façon suivante :

$\mathrm{S}_0 = \Delta_{droit} - \Delta_{gauche}$.

$$\mathrm{S}_{i+1} = \begin{cases} \mathrm{S}_i - \Delta_{i-1} & si\ \mathrm{S}_i > 0 \\ \mathrm{S}_i + \Delta_{i+1} & si\ \mathrm{S}_i < 0. \end{cases}$$

Cette suite est telle que l'un de ses $S_i$ est nul. Lorsque $S_i$ s'annule, on vient de trouver une décomposition Goldbach de x.

exemple : considérons les nombres premiers suivants et les $\Delta_i$ qui les séparent.

1217 1223 1229 1231 1237 1249 1259

sauts : 6 6 2 6 12 10

Considérons le nombre 1238 : il est à 1 de 1237 et à 11 de 1249.

Calculons les termes de la suite :

$$\begin{aligned} S_0 &= 11 - 1 = 10 \\ S_1 &= 10 - 6 = 4 \\ S_2 &= 4 - 2 = 2 \\ S_3 &= 2 - 6 = -4 \\ S_4 &= 4 + 10 = 6 \\ S_5 &= 6 - 6 = 0 \end{aligned}$$

Donc $2 \times 1238 = 1217 + 1259$ que l'on vérifie aisément.

Notre preuve de la conjecture a les conséquences suivantes :
Toute série de la forme :

$$\begin{aligned} &S_O = 3, \\ &S_1 = S_0 + \Delta_k, \\ &S_{i+1} = S_i + \Delta_{k-1} \end{aligned}$$

suffisamment longue contient un nombre premier. Dit autrement, le symétrique de la partie gauche du treillis "attrape" des nombres premiers dans sa partie droite.

Toute série de la forme :

$$\begin{aligned} &S_0 = 2x, \\ &S_1 = S_0 - P_1, \\ &S_{i+1} = S_i - P_{i+1} \end{aligned}$$

suffisamment longue contient un nombre premier. Dit autrement, le symétrique de la partie droite du treillis "attrape" des nombres premiers dans sa partie gauche.

## 6.3 Anecdotes

Pourrions-nous gagner de l'argent avec ça ? Comme tout le monde, nous ne verrions pas d'inconvénient à gagner de l'argent via l'EFF, en trouvant des nombres premiers encore et toujours plus grands !

Cependant, on voit bien que les idées sous-jacentes à notre preuve ne nous permettent de trouver des nombres premiers ultérieurs qu'à condition de connaître les $\Delta_i$ séparant tous les nombres premiers précédents. Or, les méthodes actuelles ont trouvé des nombres premiers très très grands en faisant des sauts par-dessus de nombreux premiers. Donc il ne semble pas que nos découvertes nous permettent d'obtenir dans l'immédiat une retraite bien méritée !

Enfin, une considération très esthétique : si on observe attentivement la lettre de Goldbach, on y lit :

$4 = 1+1+1+1 = 1+1+2 = 1+3$

$5 = 2+3 = 1+1+3 = 1+1+1+2 = 1+1+1+1+1$

$6 = 1+5 = 1+2+3 = 1+1+1+3 = 1+1+1+1+2 = 1+1+1+1+1+1$

Il n'est fait aucunement référence à la multiplication ou à l'élévation à la puissance, qui sont des éléments essentiels de la factorisation en produit de facteurs premiers.
Nous préfèrerons donc désormais la formulation *"tout entier naturel supérieur à 2 est à égale distance de deux nombres premiers"* au théorème essentiel de l'arithmétique.

# 7 Notes et remerciements

L'auteur est titulaire d'un diplôme de troisième cycle universitaire en Intelligence Artificielle obtenu en 1987 à l'Université des Sciences de Montpellier. Elle a été pendant 7 ans ingénieur en informatique dans la société Thalès. Elle dédie ces travaux à ses parents.

# 8 Conclusion et travaux à venir

According to Hardy, "It is comparatively easy to make clever guesses ; indeed there are theorems, like "Goldbach's Theorem", which have never been proved and which any fool could have guessed."

Il serait intéressant d'écrire un programme basé sur la logique qui s'appuierait sur nos travaux. Utiliser des outils informatiques de preuve de programme pourrait fournir une preuve informatique de la conjecture de Goldbach.

# References


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

[2] H. Cohen. *Les nombres premiers*. Éd. La recherche n°278, vol.26, p.760, juillet-août 1995.

[3] F. Casiro. *La conjecture de Goldbach, un défi en or*. Éd. Tangente n°78, décembre 2000, janvier 2001.

[4] J.P. Delahaye. *Merveilleux nombres premiers, voyage au coeur de l'arithmétique*. Éd. Belin Pour la Science, 2000.

[5] J.P. Delahaye. *Les fractions et leurs mystères*. Éd. Pour la science n°246, p.100, avril 1998.

[6] K. Devlin. *The Millenium problems : the seven greatest unsolved mathematical puzzles of our time*. Éd. Basic Books, 2002.

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

[8] M. Du Sautoy. *The music of the primes*. Éd. Fourth Estate, 2003.

[9] J. Gibbons, D. Lester, R. Bird. *Functional Pearl, enumerating the rationals*.
http://web.comlab.ox.ac.uk/oucl/work/jeremy.gibbons/publications/rationals.pdf.

[10] D.A. Goldston, S.W. Graham, J. Pintz, C.Y. Yildirim. *Small gaps between primes or almost primes*. arXiv.org.math/0506067 (20 septembre 2005).

[11] B. Mazur. *Pourquoi les nombres premiers*. Éd.Les dossiers de la recherche, n°20, août 2005.

[12] M. Mikolas. *Farey series and their connection with the prime number problem. I*. Éd. Acta Univ. Szeged. Sect. Sci. Math. vol.13, p.93, 1949.

[13] M. Mikolas. *Farey series and their connection with the prime nomber problem. II*. Éd. Acta Univ. Szeged. Sect. Sci. Math. vol.14, p.5, 1951.

[14] A. Odlyzko, M. Rubinstein, M. Wolf. *Jumping champions*. Éd. 1997.

[15] D. Vella-Chemla, D. Diaz. *"Using clp(FD) to Support Air Traffic Flow Management"*. Éd. Proceedings of International Logic Programming Symposium, 1994.

[16] M. Wolf. *On the twin and cousin primes*. Éd. IFTUWr 909/96, août 1996.

[17] *Revue trimestrielle - Pour la Science, les génies de la science", Riemann, le géomètre de la nature*. Éd. Août-Novembre 2002.

[18] *Les dossiers de la recherche, n° 20, Mathématiques, nouveaux défis et vieux casse-tête*. Éd. août-octobre 2005.

[19] *Dossier Hors-série Pour la science, Les mathématiciens*. Éd. janvier 1994.

[20] *Numéro spécial La recherche, Les nombres*. Éd. n°278, juillet-août 1994.

# Vers une preuve de la conjecture de Goldbach

Denise Vella

Octobre 2005

## 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 Preuve de la conjecture

Construisons un tableau pour un nombre premier donné $p$ de la façon suivante : ce tableau doit être un tableau de $4p + 2$ lignes et $3p$ colonnes.

Toutes les lignes paires de ce tableau sont identiques : elles contiennent les nombres de 1 à $p$ dans cet ordre dans les colonnes $p + 1$ à $2p$. Toutes les autres colonnes des lignes paires contiennent des zéros. Un nombre $n$ compris entre 1 et $p$ est à la position $p + n$ dans une ligne paire.

Toutes les lignes impaires de ce tableau sont différentes : elles contiennent les nombres de $p$ à 1 (dans l'ordre décroissant) à partir d'une certaine position $i$ dans la ligne, $i$ variant de 1 à $2p + 1$ (la ligne $2l + 1$, par exemple, contient le nombre $p$ à la position $l+1$). Toutes les autres colonnes des lignes impaires contiennent des zéros. Un nombre $n$ compris entre 1 et $p$ est à la position $p + n - l$ dans la ligne $2l - 1$.

Si l'on se préoccupe des lignes deux par deux, une impaire (d'indice $2l - 1$) et la paire qui la suit (d'indice $2l$), on voit que si l'on additionne les éléments de la ligne du haut à ceux de la ligne du bas, deux à deux, colonne par colonne, lorsque ces éléments sont tous deux non nuls, on obtient comme résultat de toutes les sommes successives le nombre $l$.

Notre problème consiste à trouver une décomposition Goldbach d'un nombre pair $2x$ supérieur ou égal à 6 et inférieur ou égal à $p$ dans notre tableau.

Nous allons trouver une telle décomposition de $2x$ dans les lignes successives $4x - 1$ et $4x$ de notre tableau.

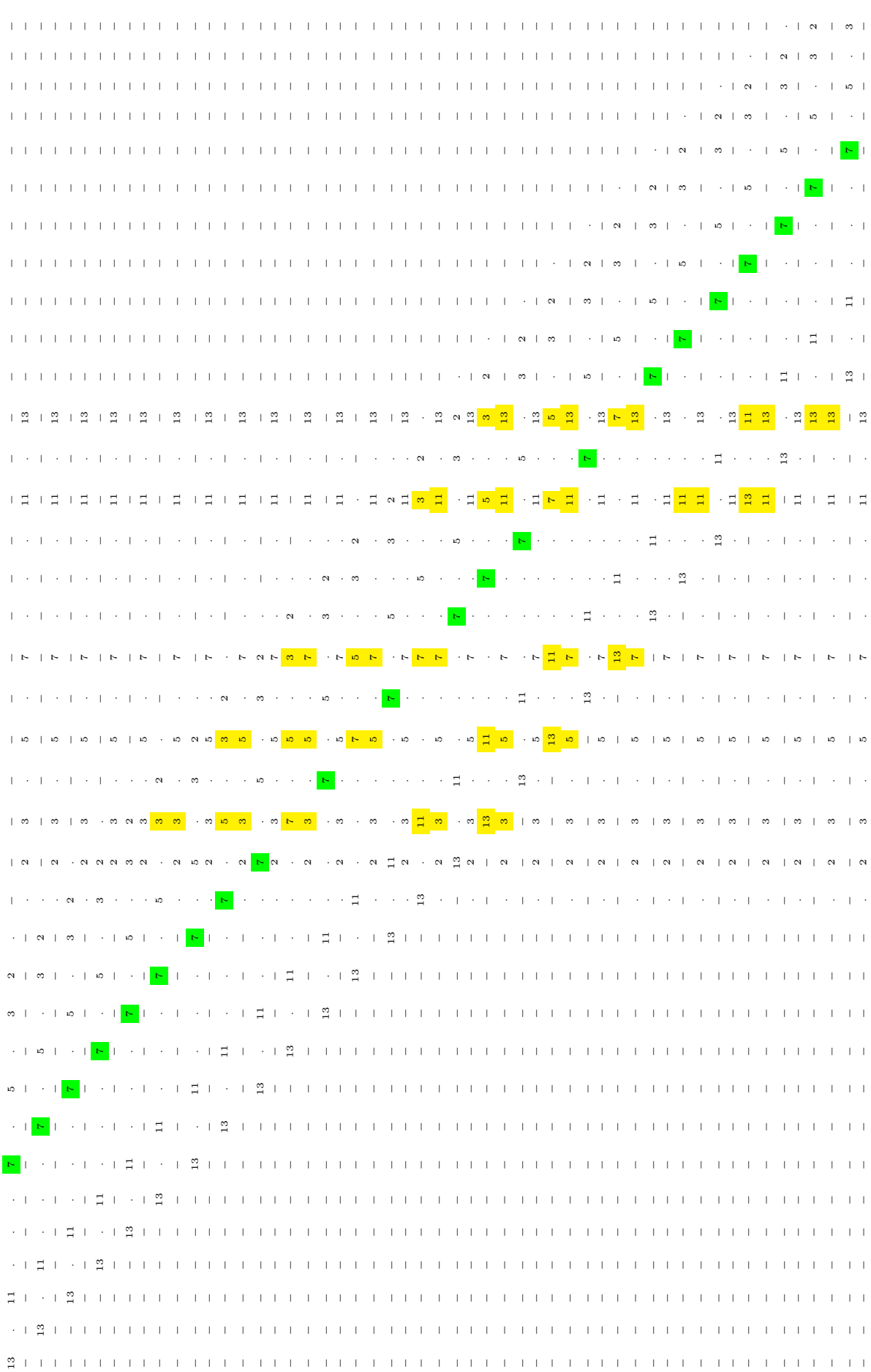
[1] Les recherches présentées ici ont été déclenchées par la lecture du roman de Doxiadis "Oncle Pétros et la Conjecture de Goldbach".

Intéressons-nous à deux nombres premiers $p_i$ et $p_j$ qui sont dans la même colonne dans les deux lignes en question. $p_i$ est à la position $p - p_i + 2x$ dans la ligne $4x - 1$ et $p_j$ est à la position $p + p_j$ dans la ligne $4x$.
Puisqu'ils sont dans la même colonne, $p - p_i + 2x = p + pj$ et donc $2x = p_i + p_j$, ce qu'il fallait démontrer.
Pourquoi deux tels nombres premiers existent-ils ?
Le nombre premier $p_j$ est resté en position fixe dans toutes les lignes paires. Le nombre premier $p_i$, quant à lui, a parcouru toutes les colonnes, de sa colonne initiale dans la première ligne $(p - p_i + 1)$, à sa colonne finale dans l'avant-dernière ligne $(3p - p_i + 1)$. Il atteindra la position $p - p_i + 2x = p + p_j$ justement dans la ligne $4x$ qui nous intéresse.

# 3 Voyons un exemple

Considérons le nombre premier 13. Nous allons construire un tableau qui va nous fournir des décompositions Goldbach des nombres pairs de 6 à 12.
Pour que ce tableau soit plus lisible, on a remplacé les zéros par des tirets et on a supprimé les nombres composés. On a également visualisé la "promenade" du nombre 7 dans les lignes impaires en vert ainsi que les décompositions Goldbach des nombres pairs successifs en jaune.

Dans la ligne 23, 5 est dans la colonne 20 (= 13-5+12). Dans la ligne 24, 7 est dans la même colonne 20 (= 13+7). Dans les lignes 23 et 24, se trouve donc une des décompositions de 12=5+7.



Dans le tableau, on trouve également des décompositions Goldbach de nombres pairs compris entre $p$ et $2p$. Cependant, il est possible que de tels nombres n'aient aucune décomposition dans le tableau. Cela signifiera que leurs décompositions Goldbach font intervenir des nombres premiers supérieurs à $p$.

Par exemple, le nombre 44 n'a pas de décomposition Goldbach apparaissant dans le tableau associé au nombre premier 29.
Considérons le sous-tableau constitué des cases qui nous intéressent pour trouver une décomposition Goldbach de 44. Dans ce sous-tableau, les colonnes ne coincident jamais et donc on ne peut trouver de décomposition Goldbach de 44 dans le tableau associé au nombre premier 29.

| *pos* | 87 | 88 |
|---|---|---|
| 3 | 70 | 32 |
| 5 | 68 | 34 |
| 7 | 66 | 36 |
| 11 | 62 | 40 |
| 13 | 60 | 42 |
| 17 | 56 | 46 |
| 19 | 54 | 48 |
| 23 | 50 | 52 |
| 29 | 44 | 58 |

# 4 Conclusion

Nous pourrons donc désormais utiliser la formulation *"tout entier naturel supérieur à 2 est à égale distance de deux nombres premiers"*[2].

[2]According to Hardy, "It is comparatively easy to make clever guesses ; indeed there are theorems, like "Goldbach's Theorem", which have never been proved and which any fool could have guessed."

# References


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

[2] H. Cohen. *Les nombres premiers*. Éd. La recherche n°278, vol.26, p.760, juillet-août 1995.

[3] F. Casiro. *La conjecture de Goldbach, un défi en or*. Éd. Tangente n°78, décembre 2000, janvier 2001.

[4] J.P. Delahaye. *Merveilleux nombres premiers, voyage au coeur de l'arithmétique*. Éd. Belin Pour la Science, 2000.

[5] K. Devlin. *The Millenium problems : the seven greatest unsolved mathematical puzzles of our time*. Éd. Basic Books, 2002.

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

[7] M. Du Sautoy. *The music of the primes*. Éd. Fourth Estate, 2003.

[8] B. Mazur. *Pourquoi les nombres premiers*. Éd.Les dossiers de la recherche, n°20, août 2005.

[9] D. Vella-Chemla, D. Diaz. *"Using clp(FD) to Support Air Traffic Flow Management"*. Éd. Proceedings of International Logic Programming Symposium, 1994.

[10] *Revue trimestrielle - Pour la Science, les génies de la science", Riemann, le géomètre de la nature*. Éd. Août-Novembre 2002.

[11] *Les dossiers de la recherche, n° 20, Mathématiques, nouveaux défis et vieux casse-tête*. Éd. août-octobre 2005.

[12] *Dossier Hors-série Pour la science, Les mathématiciens*. Éd. janvier 1994.

[13] *Numéro spécial La recherche, Les nombres*. Éd. n°278, juillet-août 1994.

# Vers une preuve de la conjecture de Goldbach

Denise Vella

Novembre 2005

## 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 Tentative de preuve de la conjecture

On prouve la conjecture par récurrence :
1) elle est vraie pour les petits nombres pairs (en fait, elle a été vérifiée par Oliveira et Silva jusqu'à $2 \times 10^{17}$ en février 2005).

2) il s'agit de prouver que si la conjecture est vérifiée par tous les nombres pairs jusqu'à un nombre premier $p_i$, elle est vérifiée par tous les nombres pairs compris entre $p_i$ et $p_{i+1}$.
On va trouver les décompositions Goldbach des nombres pairs compris entre $p_i$ et $p_{i+1}$, à partir de celles des nombres pairs inférieurs à $p_{i-1}$.

Construisons un tableau de deux lignes (que l'on appellera tableau du nombre premier $p_{i-1}$) de la façon suivante :
- la première ligne contient les nombres de $p_{i-1}$ à $(p_{i-1}+1)/2$ dans l'ordre décroissant,
- la deuxième ligne contient les nombres de 0 à $(p_{i-1}-1)/2$ dans l'ordre croissant.

Définissons une relation $sym_{p_{i-1}}$ entre deux couples de colonnes $(c1, c2)$ et $(c3, c4)$ contenant chacune un nombre premier. Nous dirons que :

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

$$(c1, c2)sym(c3, c4) \iff \begin{cases} c1 \text{ contient } p1 \text{ premier et } np1 \text{ composé} \\ c2 \text{ contient } p2 \text{ premier et } np2 \text{ composé} \\ c3 \text{ contient } p3 \text{ premier et } np3 \text{ composé} \\ c4 \text{ contient } p4 \text{ premier et } np4 \text{ composé} \\ (p1 + p2) + (p3 + p4) + (np1 + np2) + (np3 + np4) = 4p_{i-1} \\ p1 + p2 + p3 + p4 = 2p_{i-1} \\ p1 + p2 = np3 + np4 \\ p3 + p4 = np1 + np2 \end{cases}$$

Reste alors à démontrer que quel que soit $p_{i-1}$ premier, il existe toujours deux couples de colonnes dans le tableau de $p_{i-1}$ en relation selon $sym_{p_{i-1}}$.

Une fois cela démontré, l'hypothèse de récurrence nous garantit l'existence de $p3$ et $p4$ comme constituant une des décompositions Goldbach de $2b$ inférieur à $p_{i-1}$. La relation $sym_{p_{i-1}}$ garantit quant à elle l'existence de couples de colonnes reliés par $sym_{p_{i-1}}$ qui nous fournissent une décomposition Goldbach pour $2a$ compris entre $p_{i-1}$ et $p_i$ qui est "symétrique" d'une décomposition Goldbach de $2b$ inférieur à $p_{i-1}$. Donc, quel que soit $2a$ compris entre $p_{i-1}$ et $p_i$, il existe $p_1$ et $p_2$ premiers tels que $2a = p_1 + p_2$.

# 3 Voyons un exemple

Il s'agit de trouver les décompositions Goldbach des nombres pairs compris entre 23 et 29, soient 24, 26 et 28.

| 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |

Nous allons trouver ces décompositions à partir des décompositions de leur symétrique par rapport au nombre premier précédent 23, dans le tableau correspondant à 23, par le principe de symétrie découlant de la loi de réciprocité.

| 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |

$24 = 17 + 7$ car $(19 + 3) + (20 + 4) + (17 + 7) + (16 + 6) = 4 \times 23$.
$26 = 19 + 7$ car $(17 + 3) + (20 + 6) + (19 + 7) + (16 + 4) = 4 \times 23$.
$28 = 17 + 11$ car $(13 + 5) + (18 + 10) + (17 + 11) + (12 + 6) = 4 \times 23$.

# 4 Conclusion

Quand pourra-t-on utiliser la formulation *"tout entier naturel supérieur à 2 est le milieu de deux nombres premiers"* ?[2].

[2] According to Hardy, "It is comparatively easy to make clever guesses ; indeed there are theorems, like "Goldbach's Theorem", which have never been proved and which any fool could have guessed."

# References


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

[2] F. Casiro. *La conjecture de Goldbach, un défi en or*. Éd. Tangente n°78, décembre 2000, janvier 2001.

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

[4] M. Du Sautoy. *The music of the primes*. Éd. Fourth Estate, 2003.

[5] D. Vella-Chemla, D. Diaz. *"Using clp(FD) to Support Air Traffic Flow Management"*. Éd. Proceedings of International Logic Programming Symposium, 1994.

# Vers une preuve de la conjecture de Goldbach

Denise Vella

Décembre 2005

## 1 Rappels

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

Euclide a démontré qu'il existe une infinité de nombres premiers. De ce fait, on peut ajouter deux à deux les nombres premiers, en infinité, et obtenir ce faisant une infinité de nombres pairs qui vérifient la conjecture de Goldbach. En particulier, pour tout nombre pair supérieur ou égal à 6, il existe un nombre fini de nombres pairs inférieurs à lui qui vérifient la conjecture, et il existe un nombre infini de nombres pairs supérieurs à lui qui vérifient la conjecture également.

Tout nombre entier positif est décomposable en une somme de quatre carrés au plus (Théorème de Lagrange).

Gauss, pour démontrer la loi de réciprocité quadratique, distingue les nombres premiers selon qu'ils sont de la forme $4n+1$ ou de la forme $4n+3$. Un nombre premier impair de la forme $4n+1$ se décompose de manière unique comme somme de deux carrés d'entiers. Il est important de noter que si tout nombre premier est de l'une de ces deux formes, la réciproque n'est pas vraie. 9 est de la forme $4n+1$ sans être premier, et 15 est de la forme $4n+3$ sans être premier non plus.

Quel est le contenu de la loi de réciprocité quadratique ? Voyons un exemple. On s'intéresse aux restes modulo un nombre $p$ des carrés des nombres de 1 à $p-1$. Si $p$ est premier, il y a une sorte de "symétrie-miroir" entre les nombres, le reste du carré de 1 modulo $p$ est égal au reste du carré de $p-1$ modulo $p$, celui de 2 est égal à celui de $p-2$, celui de 3 à celui de $p-3$... Et dans ce cas, il y a exactement $(p-1)/2$ restes différents. Illustrons cela sur un exemple. Modulo 19 qui est premier, on a le tableau des restes suivants :

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 19 | 18 | 17 | $\overline{16}$ | 15 | 14 | 13 | 12 | 11 | 10 |
| 0 | $\overline{1}$ | 2 | 3 | $\overline{4}$ | 5 | $\overline{6}$ | 7 | 8 | $\overline{9}$ |
| 0 | 1 | 4 | 9 | 16 | 6 | 17 | 11 | 7 | 5 |

[1] Les recherches présentées ici ont commencé il y a deux ans lorsque j'ai lu le roman de Doxiadis "Oncle Pétros et la Conjecture de Goldbach".

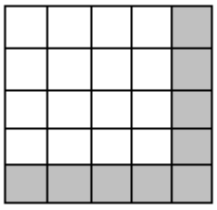
Sont colorés en rouge les nombres premiers de la forme $4n+1$. Sont colorés en vert les nombres premiers de la forme $4n+3$. Dans la troisième ligne du tableau sont fournis les restes modulo 19 des carrés des deux nombres au-dessus de lui (ils ont en effet même reste, comme on l'a vu). Enfin, sont surmontés d'un trait les nombres qui sont appelés "résidus quadratiques" de 19 (ce qui signifie "auxquels est congru le carré d'un nombre modulo 19"). Comme 19 est premier, il y a un seul résidu quadratique dans chaque colonne.
La loi s'exprime de la façon suivante :
Soient $p$ et $q$ des entiers premiers impairs.
- Si l'un (au moins) est de la forme $4n+1$, alors $p$ est résidu quadratique de $q$ si et seulement si $q$ l'est de $p$ ;
- Si $p$ et $q$ sont tous deux de la forme $4n+3$, alors $p$ est résidu quadratique de $q$ si et seulement si $q$ n'est pas résidu quadratique de $p$.

Euler a prouvé qu'un nombre impair supérieur à 1 qui est somme de deux carrés d'une seule façon est un nombre premier si les deux carrés sont premiers entre eux. Cela constitue une autre façon (que les divisions successives par des nombres premiers inférieurs du crible d'Erathostène, par exemple) de démontrer qu'un nombre est premier. Il a également montré qu'un entier impair de la forme $4n+3$ ne peut jamais être un carré.

Le carré d'un nombre pair est un nombre pair, le carré d'un nombre impair est un nombre impair.

Enfin, un nombre premier est la somme de deux nombres qui sont toujours premiers entre eux (sinon, il serait composé). Tandis que pour tout entier quelconque, il existe au moins une décomposition en une somme de deux nombres premiers entre eux.

Faisons maintenant un petit détour par la géométrie pythagoricienne. On peut obtenir le carré du successeur d'un nombre $(n+1)^2$ en ajoutant au carré de ce nombre $n^2$ le $n^{ième}$ nombre impair. On peut représenter cela par un dessin géométrique qui fait apparaître le nombre impair. La forme correspondante, en grisé, était appelé "gnomon" par les Grecs.



Après ces rappels concernant les nombres premiers ou la géométrie grecque, intéressons-nous maintenant aux nombres pairs, censés vérifier la conjecture de Goldbach.

# 2 Etude d'exemples

Les nombres pairs sont de deux formes, soit de la forme $4n$, soit de la forme $4n+2$.

Si un nombre pair de la forme $4x$ vérifie la conjecture de Goldbach, il est la somme d'un nombre premier de la forme $4n+1$ et d'un nombre premier de la forme $4n+3$.
$4x = (4n+3) + (4n'+1) = 4(n+n'+1)$.
De plus, $n+n' = x-1$. (a)

Si un nombre pair de la forme $4x+2$ vérifie la conjecture de Goldbach, il est soit la somme de deux nombres premiers de la forme $4n+1$, soit la somme de deux nombres premiers de la forme $4n+3$.
Dans le premier cas,
$4x+2 = (4n+1) + (4n'+1) = 4(n+n') + 2$.
De plus, $n+n' = x$.
Dans le deuxième cas,
$4x+2 = (4n+3) + (4n'+3) = 4(n+n''+1) + 2$.
De plus, $n+n' = x-1$.
On retrouve ici l'égalité (a) ci-dessus. Les deux cas sont peut-être à étudier de la même façon.

## 2.1 Les $4x+2$

Etudions d'abord les nombres pairs de la forme $4n+2$ de 6 à 98, et l'une de leurs décompositions Goldbach. Chacun de tels nombres pairs vérifie trivialement la conjecture de Goldbach lorsqu'il est le double d'un nombre premier. Lorsque ce n'est pas le cas, décomposons ce nombre comme somme de quatre carrés et retrouvons les deux nombres premiers composant la somme, ces deux nombres premiers étant chacun somme de deux carrés parmi les quatre.

$$
\begin{aligned}
6 &= 3+3 \ (\textit{double d'un premier}) \\
10 &= 5+5 \ (\textit{idem}) \\
14 &= 7+7 \ (\textit{idem}) \\
18 &= (4+1)+(4+9) \\
&= 5+13 \\
22 &= (4+1)+(16+9) \\
&= 5+17 \\
26 &= 13+13 \ (\textit{double d'un premier}) \\
30 &= (9+4)+(16+1) \\
&= 13+17 \\
34 &= 17+17 \ (\textit{double d'un premier}) \\
38 &= 19+19 \ (\textit{idem}) \\
42 &= (4+1)+(36+1) \\
&= 5+37 \\
46 &= 23+23 \ (\textit{double d'un premier}) \\
50 &= (9+4)+(36+1) \\
&= 13+37 \\
54 &= (9+4)+(36+4) \\
&= 13+41 \\
58 &= 29+29 \ (\textit{double d'un premier}) \\
62 &= 31+31 \ (\textit{idem}) \\
66 &= (9+4)+(49+4) \\
&= 13+53 \\
70 &= (16+1)+(49+4) \\
&= 17+53 \\
74 &= 37+37 \ (\textit{double d'un premier}) \\
78 &= (4+1)+(64+9) \\
&= 5+73 \\
82 &= (25+4)+(49+4) \\
&= 29+53 \\
86 &= (9+4)+(64+9) \\
&= 13+73 \\
90 &= (16+1)+(64+9) \\
&= 17+73 \\
94 &= (4+1)+(64+25) \\
&= 5+89 \\
98 &= (36+1)+(36+25) \\
&= 37+61
\end{aligned}
$$

Admettons qu'il existe une décomposition de ce nombre sous la forme d'une somme de 4 carrés et que deux de ces carrés correspondent à un $p1$ premier.

$$a^2 + b^2 + c^2 + d^2 = (4n + 1) + (4n' + 1) = p_1 + p_2$$

Il faut démontrer que $p_2$ est premier. Il l'est si et seulement si $c^2$ et $d^2$ sont premiers entre eux, soit si $c$ et $d$ le sont. On sait simplement que $c^2$ et $d^2$ sont l'un le carré d'un pair et l'autre le carré d'un impair.
Problème : le théorème de Lagrange pose l'existence pour chaque entier positif d'une décomposition sous la forme d'une somme de 4 carrés, mais cette décomposition n'est pas unique. De plus, on a vu que les formes $4n + 1$ ou $4n + 3$ ne garantissent pas la primarité. Enfin, la décomposition garantit 4 carrés *au plus*, ce qui peut poser problème. Peut-être faudrait-il distinguer les quatre cas : un seul carré, deux carré, trois carrés et quatre carrés.

Le $4n+2$ peut aussi être tel qu'il n'a que des décompositions comme somme de 2 nombres de la forme $4n + 3$ (comme 38, par exemple).

$$a^2 + b^2 + c^2 + d^2 = (4n + 3) + (4n' + 3) = p_1 + p_2$$

Il faut montrer que $p_1$ et $p_2$ sont tous les deux premiers. Le seul élément que l'on a est (Euler), un $4n + 3$ n'est jamais un carré unique.

## 2.2 Les $4x$

Intéressons-nous maintenant aux nombres pairs de la forme $4n$.
Ils se décomposent également comme somme de quatre carrés. Mais leurs différentes décompositions Goldbach, comme on l'a vu, font intervenir un nombre premier de chacune des deux sortes qui avaient été distinguées par Gauss.

$$8 = 4 \times 2 = (4 \times 0 + 3) + (4 \times 1 + 1) = 3 + 5 \tag{1}$$

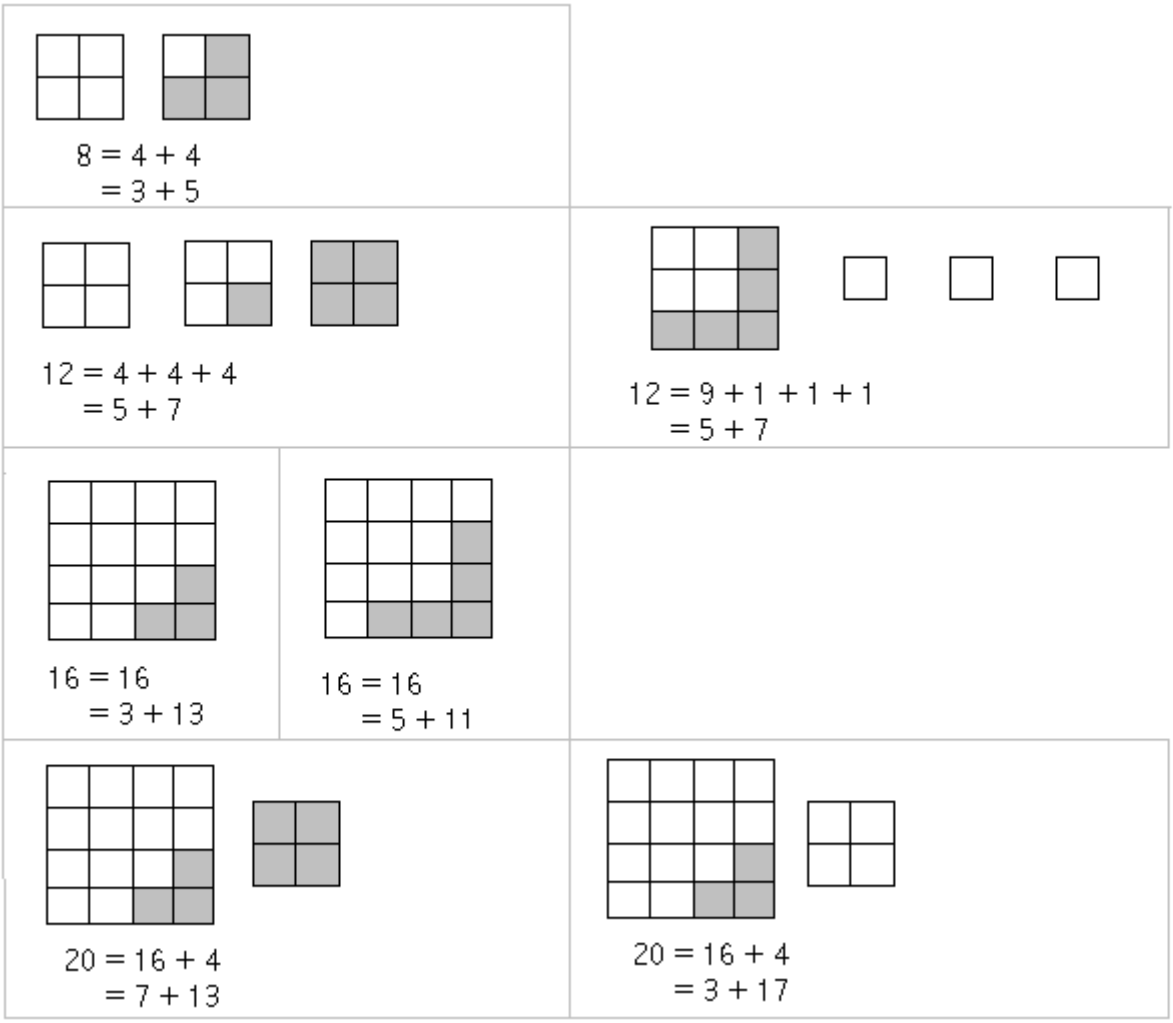
Résoudre la conjecture de Goldbach est équivalent à démontrer que quelque soit $x$, il existe $a$ et $b$ tels que $a+b = x-1$ et $4a+3$ est premier et $4b+1$ est premier.

Nous allons représenter les décompositions Goldbach en grisant des cases dans les sommes de carrés et voir que ces décompositions peuvent toujours faire appel à des aires en forme de gnomon.

Choisissons de toutes les manières possibles $a$ et $b$ tels que $a + b = x - 1$. Pourquoi existe-t-il toujours $4a+1$ et $4b+3$ premiers entre eux et premiers tout court ?
On sait en vertu du théorème de Lagrange que $4x$ est décomposable sous la forme de 4 carrés au plus.

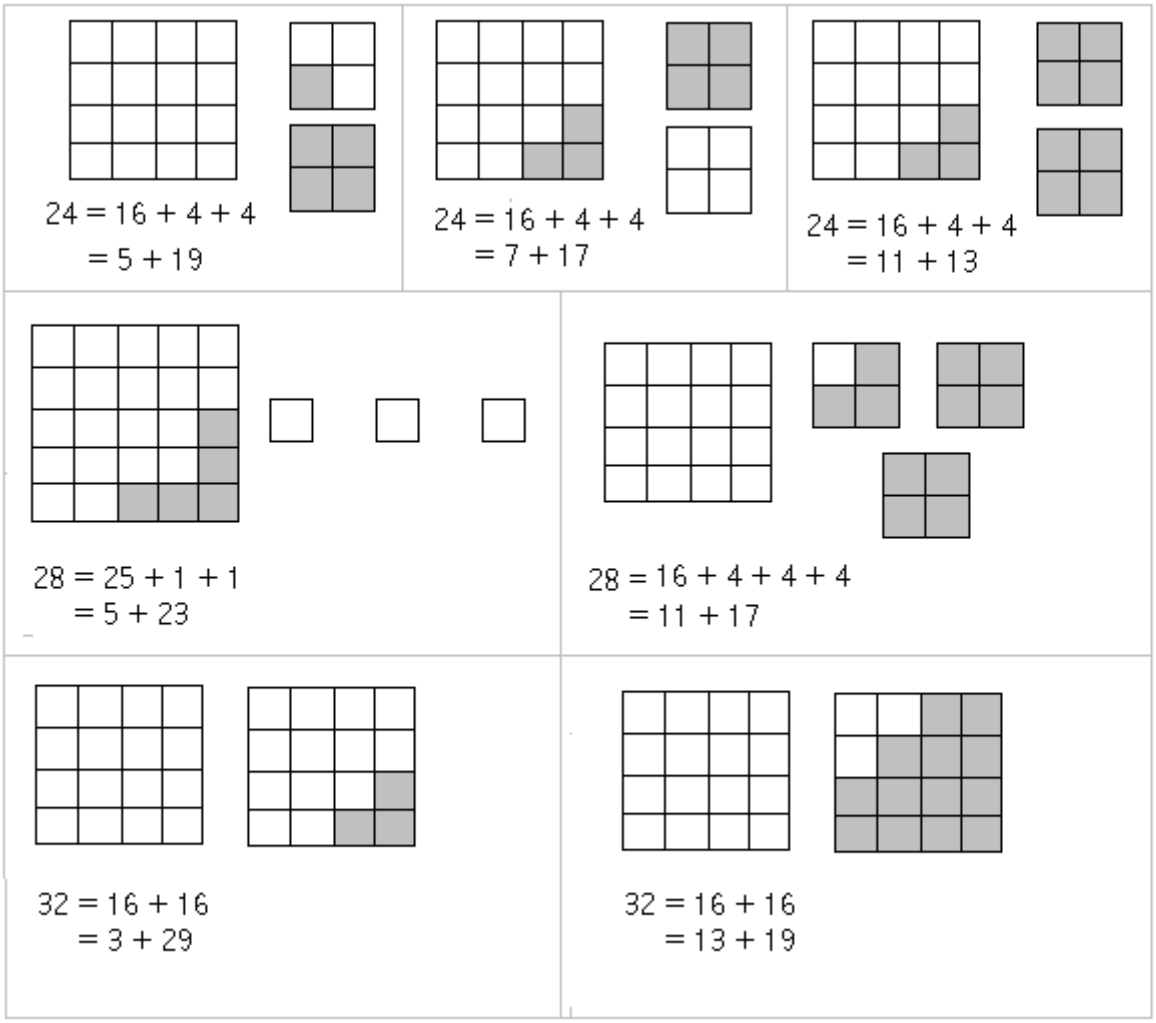
$$4x = a^2 + b^2 + c^2 + d^2 = (4n + 1) + (4n' + 3) = p_1 + p_2$$

Il faut démontrer que $c^2 + d^2$ est premier ; pour ça, il faut que $c$ et $d$ soient premiers entre eux. Est-ce que ce cas peut être regroupé avec le premier cas ci-dessus. Dit autrement, si une équation de la forme $4x = 4a + 3 + b^2 + c^2$ a toujours une solution, telle que $4a + 3$ est un nombre premier et $b^2 + c^2$ est également un nombre premier, alors la conjecture de Goldbach est vraie.




## 3 Tentatives précédentes infructueuses

- treillis Goldbach : un treillis de largeur $2x$ ne rate aucun des nombres pairs jusqu'à $x$. Moyenne arithmétique de deux premiers. Programme informatique de calcul des ratages, ratio qui tend vers 1 à l'infini ;
- arithmétique modulaire et élimination par modulo ;
- si les $2x - p_i$ avec $p_i$ premier étaient tous simultanément composés, et que Goldbach est vraie, on devrait aboutir à une contradiction ;
- les entiers de $2x - 1$ à 1 "se promenant" dans un tableau (voir les danses à la cour) face aux nombres de 1 à $2x - 1$, les nombres premiers se retrouvent en face les uns des autres une fois sur deux ;
- la suite des écarts entre nombres premiers pourrait-elle être une séquence fractale d'entiers ?
- divisibilité des factorielles dans la mesure où les décompositions Goldbach d'un nombre pair donné se voient toutes simultanément dans un tableau de 2 lignes




contenant dans la première ligne les nombres de 1 à $2x-1$ et dans la deuxième ligne les nombres de $2x-1$ à 1. (voir "Théorie des nombres" de Lucas sur Gallica pour la divisibilité des factorielles)
- somme des nombres premiers, somme des nombres composés inférieurs à $2x$ ;
- récurrence de nombre premier en nombre premier en utilisant un théorème à démontrer : "qqs p premier, il existe p1, p2, p3, p4 premiers, tels que 2p = p1+p2+p3+p4".
- réglettes de crible additif et tracé de droite pour encadrer $2x$ s'il est non Goldbach pour aboutir à une contradiction.
- mettre face à face deux cribles multiplicatifs (voir Matiiassevitch) reliés par un crible additif (voir Thérèse Eveilleau) et la décomposition Goldbach d'un nombre est une droite reliant deux nombres premiers dans chacun des deux cribles de Matiassevitch ;
- descente infinie : si tous les $2x-p_i$ étaient composés, ils auraient au moins deux facteurs chacun et seraient donc obligés d'en partager certains, et on obtiendrait

peut-être un nombre entier plus petit ne vérifiant pas Goldbach non plus...
- approche combinatoire : avec $\Pi(n)$ nombres premiers, je peux générer $2\Pi(n)-1$ nombres pairs différents au minimum alors qu'il faudrait que j'en génère $p_{\Pi}(n)-2$ toujours légèrement supérieur au nombre ci-dessus.
- il faut démontrer que toute décomposition Goldbach fait intervenir un premier inférieur à 2n+1;

# 4 Conclusion

Donc, *tout nombre pair supérieur à* 2 *est la somme de deux nombres premiers"* et *tout nombre entier supérieur à 3 est la moyenne arithmétique de deux nombres premiers.*

# Un lien entre la conjecture de Goldbach et le totient d'Euler

Denise Vella

Janvier 2006

## 1 Enoncé de la conjecture de Goldbach

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

## 2 Calculs utiles

On constate d'abord que les décompositions Goldbach d'un nombre pair $2x$ se lisent toutes simultanément dans un tableau construit de la sorte :

| $2x$ | $2x-1$ | $2x-2$ | $2x-3$ | ... | ... | 2 | 1 |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | ... | ... | $2x-2$ | $2x-1$ |

Le tableau est construit de telle façon que la somme des contenus des deux cases de chaque colonne soit toujours égale à $2x$ et lorsque les deux éléments sont des nombres premiers, on appelera cette somme une décomposition Goldbach de $2x$.

Par exemple, les décompositions Goldbach des nombres 12 et 20 sont colorées en vert.

| 12 | 11 | 10 | 9 | 8 | 7 | 6 |
|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 |

| 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

L'idée consiste alors à s'intéresser non plus aux sommes des deux nombres de chaque colonne mais à leur produit. Les décompositions Goldbach sont alors représentées par des nombres que l'on dit 2-presque-premiers, c'est à dire égaux

[1] Les recherches présentées ici ont commencé il y a deux ans lorsque j'ai lu le roman de Doxiadis "Oncle Pétros et la Conjecture de Goldbach".

au produit de deux nombres premiers.

On peut présenter ces produits par colonne dans un tableau et colorer dans ce tableau les nombres 2-presque-premiers qui sont autant de décompositions Goldbach de nombres pairs en colonne 1. Est fourni après la bibliographie un graphique qui présente les décompositions Goldbach des premiers nombres pairs.

| | | *-1* | *-4* | *-9* | *-16* | *-25* | *-36* | *-49* | *-64* | *-81* | *-100* | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *2* | 1 | | | | | | | | | | | |
| *4* | 4 | 3 | | | | | | | | | | |
| *6* | 9 | 8 | 5 | | | | | | | | | |
| *8* | 16 | 15 | 12 | 7 | | | | | | | | |
| *10* | 25 | 24 | 21 | 16 | 9 | | | | | | | |
| *12* | 36 | 35 | 32 | 27 | 20 | 11 | | | | | | |
| *14* | 49 | 48 | 45 | 40 | 33 | 24 | 13 | | | | | |
| *16* | 64 | 63 | 60 | 55 | 48 | 39 | 28 | 15 | | | | |
| *18* | 81 | 80 | 77 | 72 | 65 | 56 | 45 | 32 | 17 | | | |
| *20* | 100 | 99 | 96 | 91 | 84 | 75 | 64 | 51 | 36 | 19 | | |
| *22* | 121 | 120 | 117 | 112 | 105 | 96 | 85 | 72 | 57 | 40 | 21 | |
| *24* | 144 | 143 | 140 | 135 | 128 | 119 | 108 | 95 | 80 | 63 | 44 | ... |
| *26* | 169 | 168 | 165 | 160 | 153 | 144 | 133 | 120 | 105 | 88 | 69 | ... |
| *28* | 196 | 195 | 192 | 187 | 180 | 171 | 160 | 147 | 132 | 115 | 96 | ... |

Comment obtient-on le contenu des cases de ce tableau, qui sont en fait des différences de carrés ?

$$c(i,j) = i^2 - (j-1)^2$$

Si l'on excepte les nombres de la première colonne [2] (correspondant aux nombres pairs qui sont des doubles de nombres premiers, et qui vérifient trivialement la conjecture de Goldbach), les nombres colorés (correspondant aux décompositions Goldbach) ont toujours au-dessus d'eux leur totient d'Euler, alors que cela n'est pas le cas des nombres non colorés.

Le fait que la conjecture de Goldbach soit vraie ou pas serait donc lié au fait qu'il existe ou pas, pour tout x, une solution à l'équation :

$$\varphi((x+1)^2 - a^2) = x^2 - a^2$$

Dit autrement, il faudrait démontrer que, quelque soit $x$, il existe $y = pq$, $p$ et $q$ premiers, tel que $\varphi(y)$ appartient à la partie de $\aleph$ suivante :
$P(n) = \{x^2 - i^2, i < x - 1\}$. Si c'est le cas, $(x+1)^2 - a^2 = pq$ et $2x = p + q$.

[2] dans le cas des nombres de la première colonne, dans la case au-dessus de chaque nombre coloré on trouve le nombre $\varphi(n) - 2\sqrt{n} + 1$

# 3 Conclusion

Les deux énoncés *tout nombre pair supérieur à* 2 *est la somme de deux nombres premiers"* et *tout nombre entier supérieur à 3 est la moyenne arithmétique de deux nombres premiers* deviendront peut-être des théorèmes...

# References


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

[2] M. Guinot. *Ce "diable d'homme" d'Euler*. Éd. Aleas, 2000.

[3] F. Casiro. *La conjecture de Goldbach, un défi en or*. Éd. Tangente n°78, décembre 2000, janvier 2001.

[4] J.P. Delahaye. *Merveilleux nombres premiers, voyage au coeur de l'arithmétique*. Éd. Belin Pour la Science, 2000.

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

[6] M. Du Sautoy. *The music of the primes*. Éd. Fourth Estate, 2003.

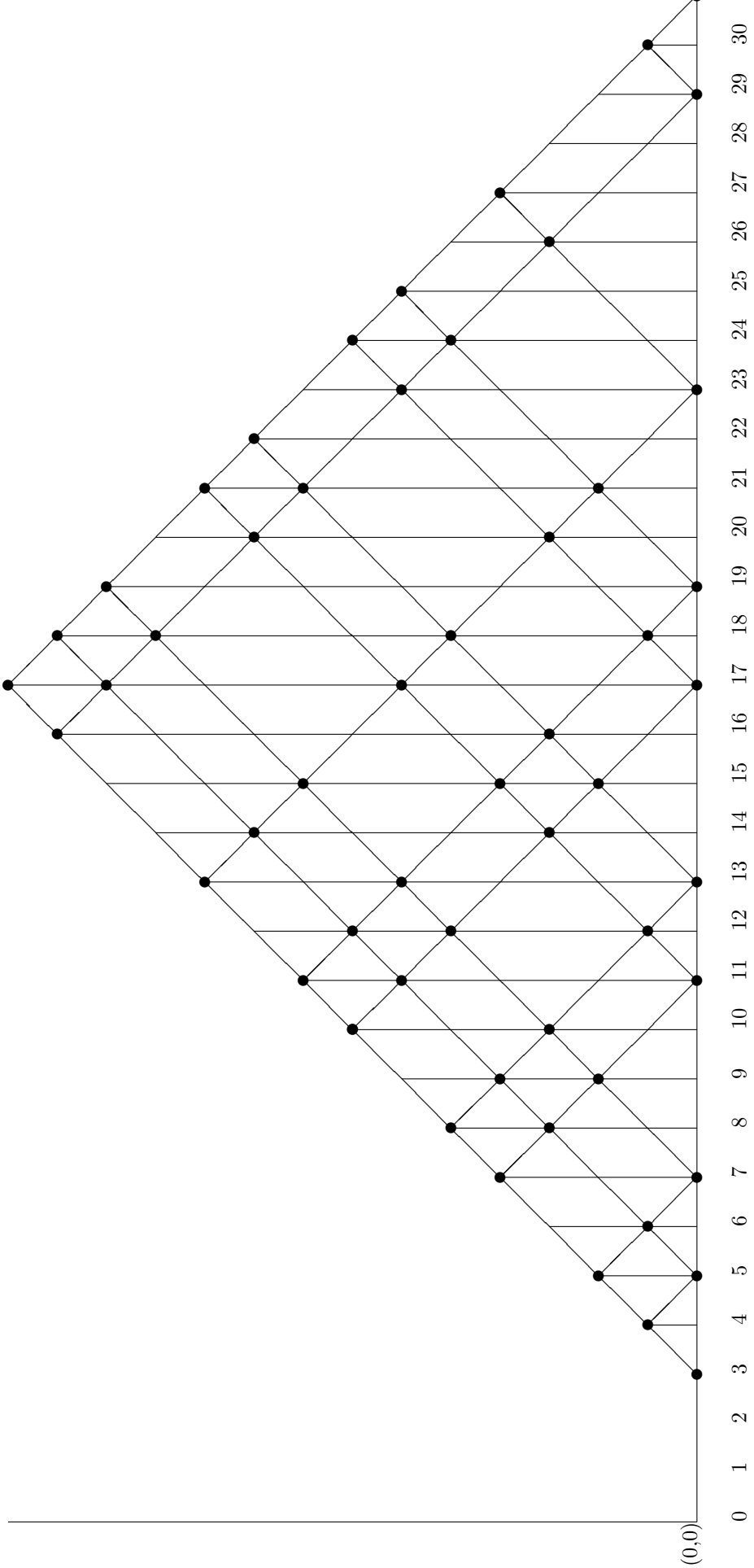



Figure 1: Le treillis Goldbach

# Fractales, symétrie et conjecture de Goldbach

Denise Vella

Février 2006

## 1 Introduction

Dans cette note, nous utilisons la théorie fractale de Mandelbrot pour étudier certaines propriétés des nombres entiers naturels. Nous mettons en évidence les symétries que l'on trouve dans certaines séquences fractales d'entiers. Ces symétries ont vraisemblablement pour conséquence que tout entier naturel supérieur à 4 est la moyenne de deux nombres premiers.

## 2 Séquences fractales de valuations p-adiques

### 2.1 Définitions

On appelle valuation p-adique ($p$ premier) d'un entier $n$ l'exposant de $p$ dans la factorisation de $n$. On a l'habitude de noter cette valuation $v_p(n)$.

On peut définir $v_p(n)$ de la façon suivante :

$$v_p(n) = \begin{cases} 0 & \text{si} \quad n \not\equiv 0 \pmod{p} \\ v_p(n/p) + 1 & \text{sinon.} \end{cases}$$

Voici la séquence des valuations 2-adiques des nombres entiers de 1 à 100 :

0 1 0 2 0 1 0 3 0 1 0 2 0 1 0 4
0 1 0 2 0 1 0 3 0 1 0 2 0 1 0 5
0 1 0 2 0 1 0 3 0 1 0 2 0 1 0 4
0 1 0 2 0 1 0 3 0 1 0 2 0 1 0 6
0 1 0 2 0 1 0 3 0 1 0 2 0 1 0 4
0 1 0 2 0 1 0 3 0 1 0 2 0 1 0 5
0 1 0 2 0

La séquence des valuations 3-adiques des mêmes nombres est [1] :

0 0 1 0 0 1 0 0 2
0 0 1 0 0 1 0 0 2
0 0 1 0 0 1 0 0 3
0 0 1 0 0 1 0 0 2
0 0 1 0 0 1 0 0 2
0 0 1 0 0 1 0 0 3
0 0 1 0 0 1 0 0 2
0 0 1 0 0 1 0 0 2
0 0 1 0 0 1 0 0 4
0 0 1 0 0 1 0 0 2
0 0 1 0 0 1 0 0 2
0

On appelle *séquence fractale d'entiers* une séquence d'entiers qui s"'autocontient". Cette notion a été définie précisément par Mandelbrot [1]. On peut dire que d'un point de vue mathématique, les fractales sont des objets construits par récurrence d'une homothétie interne, ce que l'on appelle l"'auto-similarité". Avant Mandelbrot, Peano, Sierpinski, ou Hilbert avaient inventé des courbes fractales. Chaque partie de ces courbes a une structure identique à la structure du tout.

Cette notion de "fractale" est esthétique par sa "beauté naturelle" au sens où elle permet de représenter des objets naturels tels une courbe littorale accidentée, la structure d'un arbre, etc. Enfin, Kimberling [2] a introduit la notion de "séquence fractale d'entiers" qui sera utilisée ici.

D'abord, il faut constater que les séquences constituées des valuations p-adiques des entiers sont autant de séquences fractales d'entiers : si l'on supprime de l'une de ces séquences tous ses éléments nuls et que l'on retranche 1 aux éléments restant, on obtient la séquence initiale avant transformation.

Considérons maintenant la séquence obtenue en additionnant les éléments de la séquence p-adique et de la séquence q-adique (p et q premiers). On constate que cette séquence est également fractale. Si l'on ne conserve de cette séquence que les éléments d'indices multiples du produit $pq$ et qu'on leur retranche 2, on trouve à nouveau la séquence initiale des sommes.

[1] Il est démontré que $v_p(a+b) \geqslant v_p(a) + v_p(b)$.

Considérons alors la séquence obtenue en additionnant les éléments de $i$ séquences $p_i$-adiques différentes (les $p_i$ étant premiers). Cette séquence est fractale. Si l'on ne conserve de cette séquence que les éléments d'indices multiples de $\prod {p_i}^{\,2}$ et qu'on leur retranche $i$, on obtient à nouveau la séquence initiale des sommes.

Considérons enfin la séquence obtenue en additionnant les éléments des séquences p-adiques associées à tous les nombres premiers inférieurs à un nombre donné $n$. D'une part, cette séquence est fractale. D'autre part, les $log(n)$ premiers éléments de cette séquence qui ont pour valeur 1 sont d'indices premiers. Cette séquence est représentée graphiquement dans l'annexe 6.

## 2.2 Représentation graphique

Dans le schéma suivant, les couleurs noir, rouge, vert, orange et cyan montrent les valuations p-adiques associées aux nombres premiers 2, 3, 5, 7 et 11 pour les entiers naturels de 1 à 80.

[2] Ce produit de nombres premiers est parfois appellé primorielle et sera à nouveau utilisé dans l'annexe 4.

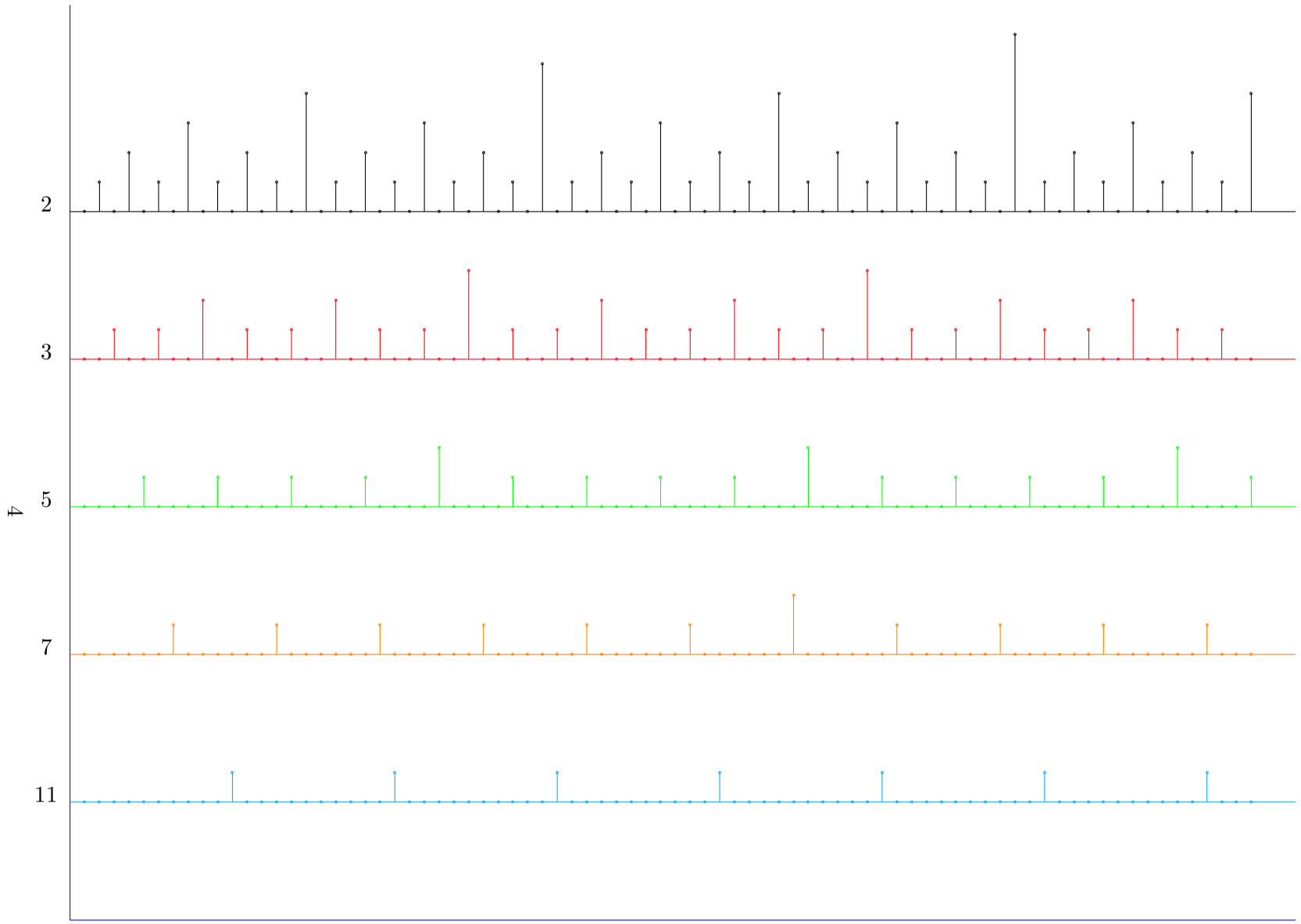



Figure 1 : Séquences fractales de valuations p-adiques

Nous fournissons en annexe l'extrait d'un article de Laisant qui présente la notion de valuation p-adique d'une manière très intuitive.

On peut représenter graphiquement l'"empilement" des factorisations des nombres entiers successifs. On construit ainsi une courbe constituée des points dont les coordonnées sont définies ainsi : l'abscisse d'un nombre premier est son "rang" (2 a pour rang 1, 3 a pour rang 2, 5 a pour rang 3, etc) ; et l'ordonnée d'un nombre premier $p$ est la somme des valuations p-adiques des $n$ premiers entiers. La courbe obtenue est une hyperbole d'équation $xy = nlog(n)$. Cette courbe est fournie en annexe.

### 2.3 Sous-séquences palindromes

En observant les différents graphiques présentés au paragraphe précédent, on constate que les séquences de valuations p-adiques contiennent des sous-séquences palindromes (identiques à elle-même, qu'on les lise de droite à gauche ou de gauche à droite).

Par exemple, considérons la séquence des valuations 2-adiques des nombres de 1 à 7. Cette séquence est $[0, 1, 0, 2, 0, 1, 0]$. Elle est palindrome. Au milieu de cette séquence, on trouve le nombre 4 de valuation 2-adique 2. Autour de lui, les nombres 3 et 5 tous deux de valuation 2-adique 0, ou bien les nombres 2 et 6 tous deux de valuation 2-adique 1, ou enfin, les nombres 1 et 7 tous deux de valuation 2-adique 0 également.

Considérons alors la séquence des valuations 3-adiques des nombres de 1 à 17 ([0,0,1,0,0,1,0,0,2,0,0,1,0,0,1,0,0]). De part et d'autre du nombre 9 de valuation 3-adique 2, on trouve systématiquement des couples de nombres de même valuation 3-adique.

Expliquons cela autrement : on peut centrer autour de tout nombre de valuation p-adique non-nulle une fenêtre contenant une sous-séquence palindrome. Cela n'est pas le cas pour les nombres de valuation p-adique nulle. Une fenêtre centrée autour d'eux ne contient jamais une sous-séquence palindrome.

Sur la figure 2 apparaissent 4 fenêtres colorées contenant des séquences palindromes de valuations 2 ou 3-adiques.

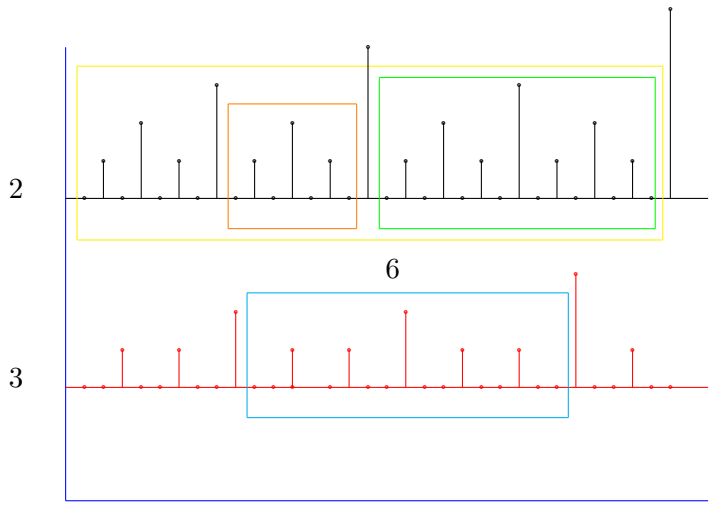
De façon plus générale, toute sous-séquence de longueur impaire centrée autour d'un élément de valuation p-adique non-nulle $i$ et contenant à gauche et à droite de cet élément central $i-1$ éléments est palindrome selon $p$. Tout couple d'entiers de cette séquence dont ce nombre central est la moyenne est constitué de deux nombres de même valuation p-adique.

### 2.4 Conséquences

Cette propriété de "symétrie" (autour des nombres au centre des fenêtres) a des conséquences intéressantes. Tout nombre de valuation p-adique $k$ non nulle est moyenne soit de deux nombres de valuations p-adique toutes deux non nulles, soit de valuations p-adiques toutes deux nulles. Tandis que tout nombre de valuation p-adique nulle ne peut jamais être moyenne de deux nombres qui seraient simultanément de valuations p-adiques non nulles.

On peut s'intéresser aussi à des fenêtres encadrant des sous-séquences palindromes mais qui ne sont pas centrées sur un nombre de valuation p-adique non nulle. Par exemple, les séquences palindromes des valuations 5-adiques des nombres de 11 à 24 (resp. de 11 à 14 ou de 6 à 14) sont [0,0,0,0,1,0,0,0,0,1,0,0,0,0] (resp. [0,0,0,0] ou [0,0,0,0,1,0,0,0,0]). La position des nombres dans les fenêtres permet de faire certaines déductions : par exemple, si l'on ajoute les nombres 14 et 6 que l'on peut considérer comme étant situés aux deux extrémités d'une fenêtre centrée sur 10 dans la ligne de 5, on sait que l'on obtiendra un nombre de dimension 5-adique non nulle (en l'occurrence 20). De même pour 14 et 11 qui sont situés l'un avant une crête (14 est un $5a-1$), et l'autre après une crête (11 est un $5b+1$) dans la séquence des valuations 5-adiques.

Figure 2 : Exemples de fenêtres centrées sur des multiples



On peut résumer ce que l'on vient d'étudier concernant les symétries dans le tableau suivant, qui fournit la connaissance que l'on peut avoir des valuations p-adiques de $x + y$ et $x - y$ connaissant celles de $x$ et $y$.

| p | x | y | x+y | x-y |
|---|---|---|---|---|
| 2 | 0 | 0 | $\neq 0$ | $\neq 0$ |
| 2 | 0 | $\neq 0$ | 0 | 0 |
| 2 | $\neq 0$ | 0 | 0 | 0 |
| 2 | $\neq 0$ | $\neq 0$ | $\neq 0$ | $\neq 0$ |
| 3 | 0 | 0 | ? | ? |
| 3 | 0 | $\neq 0$ | ? | ? |
| 3 | $\neq 0$ | 0 | 0 | 0 |
| 3 | $\neq 0$ | $\neq 0$ | $\neq 0$ | $\neq 0$ |
| p | 0 | 0 | ? | ? |
| p | 0 | $\neq 0$ | ? | ? |
| p | $\neq 0$ | 0 | 0 | 0 |
| p | $\neq 0$ | $\neq 0$ | $\neq 0$ | $\neq 0$ |

Ce tableau, bien que contenant quelques informations, ne nous sera pas d'une grande utilité par rapport à notre objectif initial et obsédant qui est de comprendre (voire démontrer !) la conjecture de Goldbach dont nous parlerons au paragraphe suivant.

Pour revenir aux symétries, on peut surtout constater qu'elles existent entre les nombres premiers eux-mêmes qui sont à des positions déterminées autour des puissances des nombres premiers inférieurs.

Montrons quelques exemples pour illustrer cela : intéressons-nous d'abord aux puissances de 2 et observons les symétries. Dans le tableau de nombres ci-après, les puissances de 2 sont écrites en bleu, chaque ligne traitant de l'intervalle entre une puissance de 2 et la puissance de 2 suivante. Les flèches entre les nombres - avec des petits nombres au-dessus fournissant les écarts - montrent les symétries (l'écart entre un nombre premier et la puissance de 2 inférieure est le même que l'écart entre la puissance de 2 supérieure et son nombre premier symétrique). Enfin, les nombres entre parenthèses sont ceux qui ont "échappé" aux symétries.

$$
\begin{array}{lllllllllllll}
2 & \overset{1}{\rightarrow} & 3 & \overset{1}{\leftarrow} & 4 & & & & & & & & \\
4 & \overset{1}{\rightarrow} & 5 & 7 & \overset{1}{\leftarrow} & 8 & & & & & & & \\
8 & \overset{3}{\rightarrow} & 11 & 13 & \overset{3}{\leftarrow} & 16 & & & & & & & \\
16 & \overset{1}{\rightarrow} & 17 & \overset{3}{\rightarrow} & 19 & (23) & 29 & \overset{3}{\leftarrow} & 31 & \overset{1}{\leftarrow} & 32 & & \\
32 & \overset{5}{\rightarrow} & 37 & (41) & \overset{11}{\longrightarrow} & 43 & (47) & 53 & \overset{11}{\longleftarrow} & 59 & \overset{5}{\leftarrow} & (61) & 64 \\
64 & (67) & (71) & (73) & \overset{15}{\longrightarrow} & 79 & \overset{19}{\longrightarrow} & 83 & (87) & \overset{25}{\longrightarrow} & 89 & (97) & \\
 & & (101) & 103 & \overset{25}{\longleftarrow} & (107) & 109 & \overset{19}{\longleftarrow} & 113 & \overset{15}{\longleftarrow} & (127) & 128 & \ldots
\end{array}
$$

Procédons de la même façon pour les puissances de 3 (mais en rouge !).

$$
\begin{array}{lllllllllllll}
3 & \overset{2}{\rightarrow} & 5 & 7 & \overset{2}{\leftarrow} & 9 & & & & & & & \\
9 & (11) & \overset{4}{\rightarrow} & 13 & \overset{8}{\rightarrow} & 17 & 19 & \overset{8}{\leftarrow} & 23 & \overset{4}{\leftarrow} & 27 & & \\
27 & \overset{2}{\rightarrow} & 29 & (31) & \overset{10}{\longrightarrow} & 37 & \overset{14}{\longrightarrow} & 41 & (43) & \overset{20}{\longrightarrow} & 47 & (53) & \\
 & & & (59) & 61 & \overset{20}{\longleftarrow} & 67 & \overset{14}{\longleftarrow} & 71 & \overset{10}{\longleftarrow} & (73) & 79 & \overset{2}{\leftarrow} & 81 & \ldots
\end{array}
$$

On voit que les nombres premiers jumeaux[3] $[3, 5]$ sont symétriques des jumeaux $[5, 7]$ dans les puissances de 3. De même, les jumeaux $[29, 31]$ sont symétriques des jumeaux $[5, 7]$ dans les puissances de 3 (même si cela n'est pas apparu ci-dessus car on ne se préoccupait simplement à chaque fois que des puissances successives) : ($29 = 27 + 2$, $31 = 27 + 4$ tandis que $7 = 9 - 2$ et $5 = 9 - 4$). L'infinitude des nombres premiers jumeaux est peut-être à chercher par là.

La maîtrise de la notion de *dimension fractale* permettrait sûrement d'avoir une compréhension précise des interactions qui existent entre les différentes structures fractales mises en évidence ci-dessus et des symétries qui en découlent.

De façon totalement anecdotique, j'ai été très surprise par la chose suivante : j'ai programmé la tortue Logo (langage de programmation graphique) de façon à ce qu'elle dessine les éléments de la séquence fractale générale, en avançant de leur valeur, et qu'elle tourne entre chaque valeur d'un angle de un degré. La tortue a dessiné... une spirale ! Si on fait de même avec les valeurs d'une seule des séquences p-adiques, on obtient... un cercle. Tout cela est troublant.

[3] Des nombres premiers sont dits *jumeaux* si une différence de 2 les sépare.

# 3 Conjecture de Goldbach

## 3.1 Rappel de son énoncé

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

## 3.2 Justification

Dès que l'on "s'attaque" à la conjecture de Goldbach, on est frappé par l'aspect symétrique du problème. Pourquoi y-a-t-il toujours deux nombres premiers, en symétrie-miroir (à égale distance de part et d'autre) d'un nombre (supérieur ou égal à 3) ? [4] Au début, j'avais en tête l'image d'un papier que l'on plierait autour du nombre $x$, à la recherche de la décomposition Goldbach de $2x$, un peu comme un éventail, mais irrégulièrement, chaque pliure coïncidant avec un nombre premier. C'est la lecture du fait que la courbe fractale du dragon correspondait au dessin que ferait la tranche d'un papier plié en se dépliant qui m'a amenée à faire ce lien entre les valuations p-adiques et les séquences fractales d'entiers. Laisant parle de cet aspect "symétrique" de la conjecture de Goldbach dans une communication de 1897 dont le texte est fourni en annexe.

Sur le schéma de la figure 1, trouver une décomposition Goldbach d'un nombre consiste à trouver deux droites à égale distance de part et d'autre d'un même point d'abscisse $x$ telles que ces droites croisent les différents graphiques colorés correspondant à chaque nombre premier en des points tous d'ordonnée nulle sauf un d'ordonnée 1. Si la conjecture de Goldbach est vraie, on peut toujours trouver deux telles droites.

La conjecture est trivialement vérifiée pour les doubles de nombres premiers. Les deux droites sont confondues.

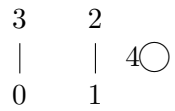
Quant aux nombres pairs qui ne sont pas double d'un premier, comment se fait-il qu'ils aient toujours au moins une décomposition Goldbach ?

[4] Est fournie en annexe 5 une représentation graphique d'une sorte de crible qui fournit les décompositions Goldbach des premiers entiers.

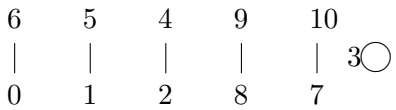
Pour l'expliquer, il faut découvrir d'où provient la "symétrie". Et pour cela, il faut faire un détour par les modulos.

Les séquences constituées des nombres qui sont les restes des entiers modulo un nombre premier ne sont pas fractales mais périodiques. La période est toujours la suite des nombres de 0 à $p-1$ qui se répète indéfiniment.

Cherchons par exemple les décompositions Goldbach de 28, constituées de deux nombres de part et d'autre de 14. Les nombres symétriques autour de 14 ont leurs restes modulo 5 (par exemple) qui obéissent au petit schéma symétrique suivant :




Modulo 11 (toujours pour 28, ou plus exactement 14), le schéma "symétrique" est :




Observons maintenant un tableau des modulos, dans lequel on a mis entre parenthèses les décompositions non Goldbach [5]. On a également coloré en vert les 0 qui sont des décompositions impossibles (tout facteur premier de $x$ ne peut permettre d'obtenir une décomposition Goldbach de $2x$).

| *mod* | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | (2) | 0 | 1 | 2 | 0 | (1) | 2 | 0 | 1 | 2 | 0 | 1 | (2) | 0 | 1 |
| 5 | | | 0 | 1 | (2) | 3 | 4 | 0 | 1 | 2 | (3) | 4 | 0 | (1) | 2 | 3 | (4) | 0 | 1 | (2) | 3 | 4 | 0 | 1 | (2) | (3) |
| 7 | | | | | 0 | (1) | 2 | 3 | (4) | 5 | 6 | 0 | 1 | (2) | (3) | 4 | 5 | (6) | 0 | 1 | (2) | 3 | 4 | (5) | 6 | 0 |
| 11 | | | | | | | | | 0 | 1 | 2 | 3 | 4 | (5) | 6 | (7) | (8) | 9 | 10 | 0 | (1) | 2 | (3) | 4 | 5 | (6) |
| 13 | | | | | | | | | | | 0 | (1) | 2 | 3 | (4) | 5 | (6) | (7) | 8 | 9 | (10) | (11) | 12 | 0 | 1 | 2 |
| 17 | | | | | | | | | | | | | | | 0 | 1 | (2) | 3 | (4) | (5) | 6 | 7 | (8) | (9) | 10 | (11) |
| 19 | | | | | | | | | | | | | | | | | 0 | (1) | 2 | (3) | (4) | 5 | 6 | (7) | (8) | 9 |
| 23 | | | | | | | | | | | | | | | | | | | | | 0 | (1) | (2) | 3 | 4 | (5) |
| 29 | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 31 | | | | | | | | | | | | | | | | | | | | | | | | | | |

[5] Ce tableau est le pendant de la représentation graphique fournie en annexe 5.

On voit que les décompositions non-Goldbach proviennent de la présence "en face" d'un nombre premier d'un nombre composé. Le nombre $\Pi(x)$ peut être calculé par la formule de Legendre (cf. Annexe 5). On cherchera selon le même principe une formule qui fournit le nombre de décompositions Goldbach. Elle doit mesurer la façon dont les nombres symétriques autour d'un nombre peuvent être simultanément premiers.

Au début de ces recherches, je cherchais une "généralisation" de l'énoncé de la conjecture "tout nombre pair est la somme de deux nombres premiers". Cet énoncé plus général aurait été de la forme "tout nombre multiple de $k$ (au lieu de pair) est la somme de $k$ (au lieu de 2) nombres premiers". Les découvertes présentées ici m'amènent au contraire à la conclusion que c'est la conjecture qui est la généralisation d'énoncés plus contraints, chacun de ces énoncés traitant d'un nombre premier seulement.

# 4 Conclusion

La répartition des nombres premiers au sein des entiers naturels semble chaotique. Pourtant, les différentes étapes (chacune correspondant à un nombre premier) de l'algorithme du crible d'Erathostène présentent chacune leur régularité propre. Il s'agirait donc d'un *chaos déterministe*. Cette régularité provient des différentes séquences fractales qui ont été mises ici en évidence. Nous avons également noté l'existence de séquences palindromes de valuations p-adiques, la structure symétrique de ces séquences les rend également régulières (même si non périodiques). On retrouve de telles fractales, de telles symétries, dans la nature. Pour illustrer cela, je citerai une anecdote : un jour, un enfant me proposa de me "montrer l'infini"... Il sortit un miroir de poche et le plaça face à un miroir accroché au mur. La suite de miroirs de plus en plus petits semblait ne jamais s'arrêter et l'enfant était émerveillé. La découverte de toutes ces symétries-miroir dans les séquences d'entiers est aussi fascinante. Les entiers *naturels* ont ainsi une structure aussi *naturelle* que peut l'être celle des structures fractales.

## Annexe 1 : extrait du texte de Laisant sur la figuration des nombres composés

A ces remarques sur les décompositions des nombres en facteurs, nous croyons devoir en ajouter une sur un mode de figuration fort simple et qui n'a cependant pas été signalé jusqu'ici, du moins à notre connaissance. Il y aurait peut-être lieu d'en tirer parti pour l'enseignement des premiers principes élémentaires relatifs à la décomposition des nombres en facteurs premiers, à la formation du plus grand commun diviseur et à celle du plus petit commun multiple de deux ou plusieurs nombres.
Voici en quoi consiste cette figuration. Supposons que, un quadrillage indéfini étant tracé à la droite d'une ligne verticale, nous numérotions les bandes horizontales successives 2, 3, 5, 7, 11, 13, 17..., en les affectant aux nombres premiers successifs. Si un nombre composé contient un facteur premier $a$ à l'exposant $i$, on comptera $i$ cases, à partir de la droite verticale, dans la bande qui représente le facteur $a$. L'ensemble des cases ainsi déterminées, et que l'on pourra limiter par le tracé du contour extérieur, figurera le nombre en question. Il est évident que ce tracé peut suivre parfois la ligne verticale origine, lorsque certains facteurs premiers font défaut, c'est à dire ont l'exposant zéro.
Nous nous bornons à donner comme exemple la figuration des nombres $360 = 2^3.3^2.5$ et $16500 = 2^2.3.5^3.11$ (fig. 1 et 2).

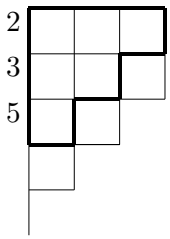



FIG. 1 – N = 360

Ce mode de représentation met en relief d'une façon saisissante la formation des diviseurs, ou, ce qui revient au même, la décomposition en deux facteurs, dont nous avons parlé ci-dessus. Le nombre des diviseurs est

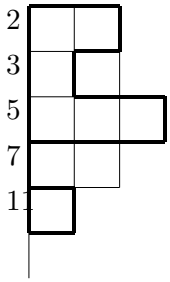



FIG. 2 – N = 16500

évidemment égal au nombre des chemins différents qu'on peut suivre pour aller de la base inférieure à la base supérieure de la figure formée, en suivant toujours les lignes du quadrillage.
Le plus grand commun diviseur de deux nombres se trouve représenté par la partie commune des figures qui représentent ces deux nombres ; le plus petit commun multiple, par la figure limitée au contour extérieur dessinée par l'ensemble des deux figures. Nous donnons comme exemple (fig.3) le plus grand commun diviseur D des deux nombres $N = 1890 = 2.3^3.5.7$ et $N' = 660 = 2^2.3.5.11$, leur plus grand commun diviseur $D = 2.3.5 = 30$ et leur plus petit commun multiple $p = 2^2.3^2.5.7.11 = 41580$, en figurant les deux nombres au moyen de carrés colorés.

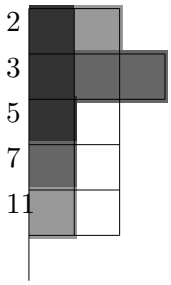



FIG. 3 – pgcd et ppcm

On comprend qu'en représentant par diverses valeurs plusieurs nombres, on peut ainsi figurer leurs diviseurs ou leurs multiples, soit d'ensemble, soit deux à deux. Par exemple, si trois nombres A, B, C sont figurés A en rouge, B en bleu et C en jaune, les plus grands communs diviseurs seront figurés celui de A et B par la partie violette, celui de B et C par la partie verte, celui de A et C par la partie orangée.

Un assez grand nombre de propriétés connues peuvent avec cette figuration prendre un caractère intuitif. Il suffit pour cela de remarquer que, lorsqu'un nombre A est multiple d'un autre nombre B, le contour de la figuration de A contient le contour de la figuration de B, et aussi que, lorsque plusieurs nombres sont premiers entre eux deux à deux, les figurations des deux quelconques de ces nombres n'ont aucune partie commune.

Au fond, ce mode de figuration est en quelque sorte un système de numérotation dans lequel l'ordre d'un chiffre, à partir de la gauche par exemple, représenterait l'exposant. Ainsi, dans les exemples cités plus haut, les divers nombres s'écriraient comme suit : 360 s'écrirait 321, 16500 s'écrirait 21301, 1890 s'écrirait 1311, 660 s'écrirait 21101, 30 s'écrirait 111, 41580 s'écrirait 23111. Le produit de deux nombres, dans ce système, s'obtiendrait par l'addition des chiffres de même rang (et il est bien entendu qu'ici nous désignons par le mot *chiffres* des nombres qui peuvent devenir aussi grands qu'on voudra). La formation du plus petit commun multiple ou du plus grand commun diviseur est évidente ; et il apparaît non moins clairement, par exemple, que le produit de deux nombres est également le produit de leur plus petit commun multiple par leur plus grand commun diviseur.
Tout nombre représenté par l'unité précédée d'un nombre quelconque de zéros est un nombre premier, et réciproquement.
Tout nombre dont les chiffres sont pairs est un carré.
Nous croyons devoir borner là ces observations, trop simples pour mériter d'être plus complètement développées.

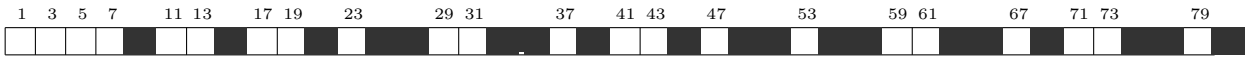
## Annexe 2 : extrait de la communication de Laisant “Sur un procédé de vérification expérimentale du théorème de Goldbach”

Ce fameux théorème empirique : *Tout nombre pair est la somme de deux nombres premiers*, dont la démonstration semble dépasser les possibilités scientifiques actuelles, a fait l'objet de nombreux travaux et de certaines contestations. Lionnet a tenté d'établir que la proposition devait probablement être inexacte. M. Georg Cantor l'a vérifiée numériquement jusqu'à 1000, en donnant pour chaque nombre pair toutes les décompositions en deux nombres premiers, et il a remarqué que le nombre de ces décompositions ne cesse de croître en moyenne, tout en présentant de grandes irrégularités.

Voici un procédé qui permettrait de faire sans calculs la vérification expérimentale dont il s'agit, et d'avoir pour chaque nombre pair, à la seule inspection d'une figure, toutes les décompositions.

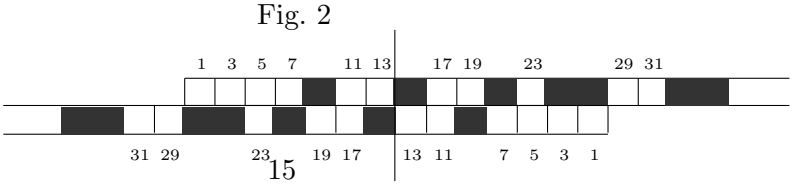
Supposons que sur une bande formée de carrés accolés, représentant les nombres impairs successifs, on ait construit le crible d'Erathostène, en ombrant les nombres composés, jusqu'à une limite quelconque $2n - 1$.

Fig. 1




Si l'on a construit deux réglettes pareilles, et si l'on place la seconde au dessous de la première en la retournant et en faisant correspondre la case 1 à $2n - 1$, il est évident que si le théorème de Goldbach est vrai pour $2n$, il y aura quelque part deux cases blanches en correspondance ; et tous les couples de cases blanches donneront les diverses décompositions. On les aura même en lisant la moitié de la figure, à cause de la symétrie par rapport au milieu. Ainsi la vérification relative au nombre 28 donnera la figure 2 et montrera qu'on a les décompositions $28 = 5 + 23 = 11 + 17$.

Fig. 2



On comprend que les réglettes étant construites à l'avance, et un simple glissement permettant de passer d'un nombre à un autre, les vérifications sont très rapides.

## Annexe 3 : L"'empilement" des valuations p-adiques"

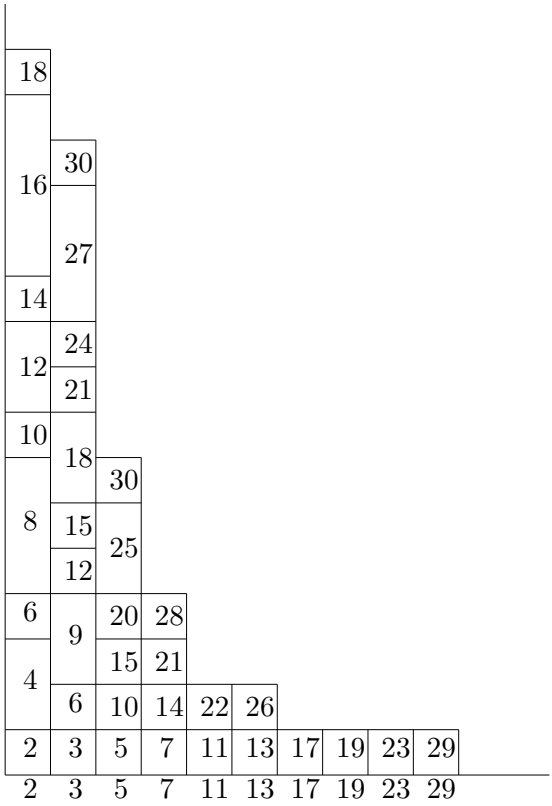



FIG. 4 – Courbe hyperbolique d'équation $xy = nlog(n)$

## Annexe 4 : Calcul de $\Pi(x)$

Pour calculer $\Pi(100)$[6], connaissant les nombres premiers inférieurs à sa racine carrée 10, et qui sont 2, 3, 5, 7, on doit faire le calcul suivant :

$$\frac{100}{2} + \frac{100}{3} - \frac{100}{2\times3} + \frac{100}{5} - \frac{100}{2\times5} - \frac{100}{3\times5} + \frac{100}{7} - \frac{100}{2\times7} - \frac{100}{3\times7} - \frac{100}{5\times7} - 5$$

En ramenant au même dénominateur, on doit calculer :

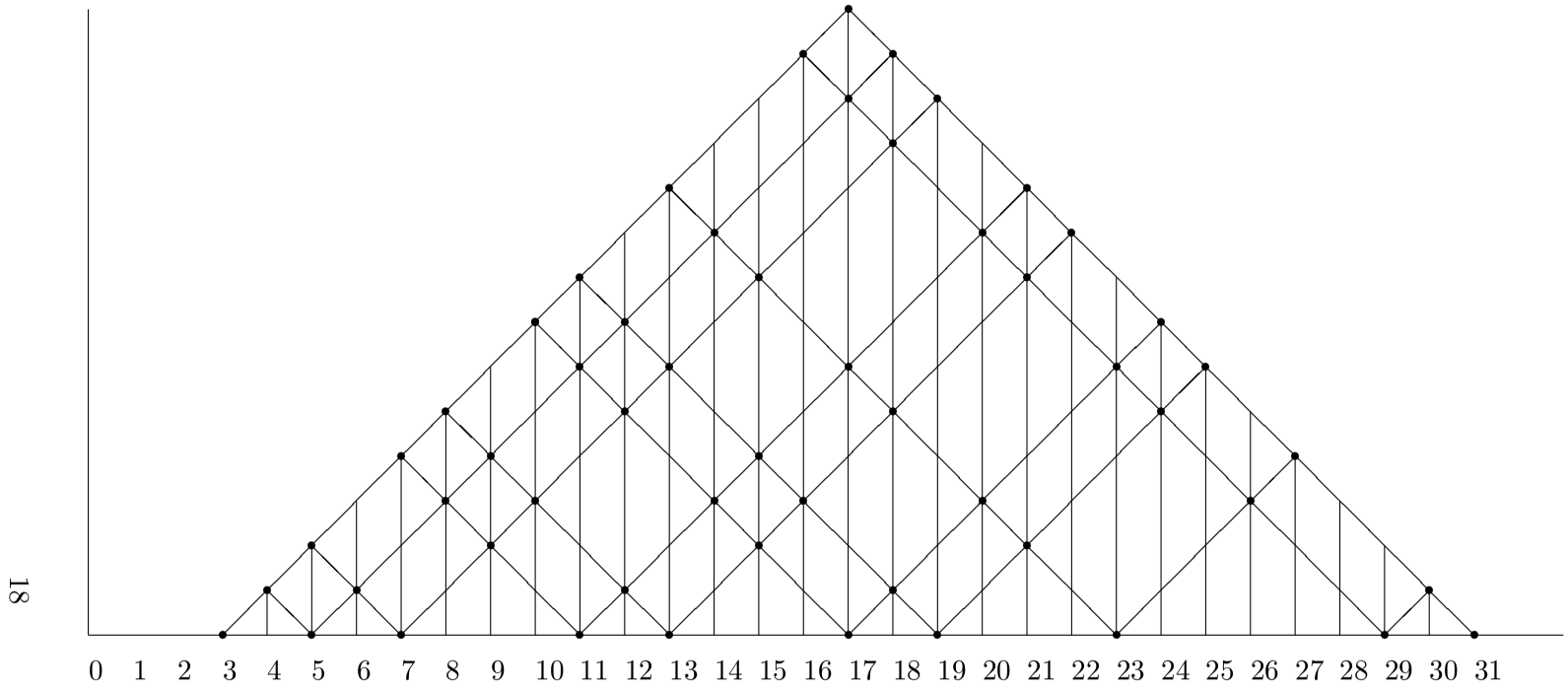
$$100 \times \frac{3\times5\times7+2\times5\times7-5\times7+2\times3\times7-3\times7-2\times7+2\times3\times5-3\times5-2\times5-2\times3)}{2\times3\times5\times7} - 5 = 25$$

Cette méthode de calcul contenant au dénominateur une "primorielle" (sorte de factorielle dans laquelle n'interviennent que des nombres premiers) et au numérateur des produits combinatoires est rédhibitoire du fait de la taille des nombres à calculer.[7]

## Annexe 5 : le crible Goldbach

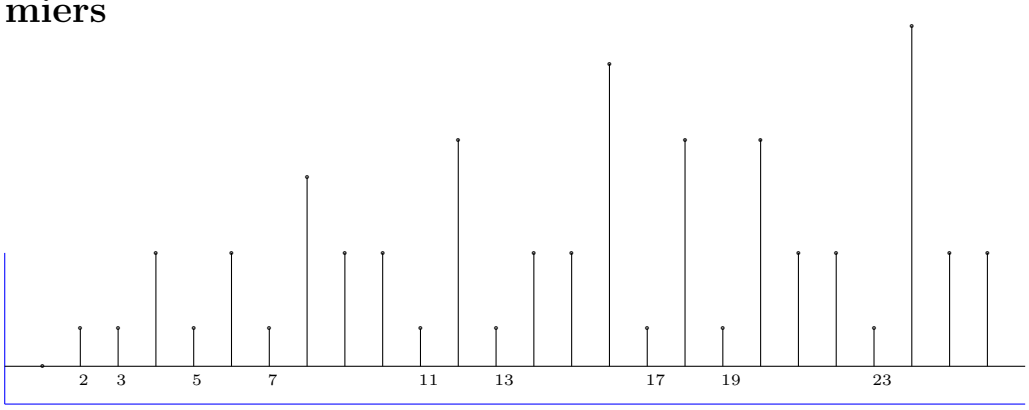
[6] $\Pi(x)$ est le nombre de nombres premiers inférieurs ou égaux à $x$

[7] J'étais très fière d'avoir trouvé cette formule, mais je me suis rendue compte en fouillant la toile que Legendre l'avait trouvée aussi ! !




*Décompositions Goldbach sous la forme* $x = \frac{p1+p2}{2}$

## Annexe 6 : la séquence fractale des nombres premiers




La séquence fractale des nombres premiers (de dimension fonction de la primorielle ?)

# 5 Bibliographie

# Références


[1] B. Mandelbrot. *Les objets fractals : forme, hasard et dimension*. Éd. Collection Champs, Flammarion, Paris, 1995.

[2] C. Kimberling. *Fractal sequences and interspersions*. Éd. Ars Combinatoria 45, p.157, 1997.

[3] 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.

[4] C.A. Laisant. *Remarques arithmétiques sur les nombres composés*. Éd. Bulletin de la S.M.F., n°16, p.150, 6/6/1888.

[5] 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.

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

[7] M. Guinot. *Ce "diable d'homme" d'Euler*. Éd. Aleas, 2000.

[8] F. Casiro. *La conjecture de Goldbach, un défi en or*. Éd. Tangente n°78, décembre 2000, janvier 2001.

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

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

[11] *les Fractales*. Éd. Tangente, HS n°18, 2004.

# Représentation de la combinatoire associée à la conjecture de Goldbach par des graphes

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 Peuvent-ils être tous composés ?

Soit un nombre pair $2x$ qui ne vérifierait pas la conjecture de Goldbach. Il n'existerait alors aucune décomposition additive de ce nombre pair $2x$ comme somme de deux nombres premiers, l'un inférieur à $x$ et l'autre supérieur à $x$. Appelons $p_1$, $p_2$,..., $p_{\Pi(x)}$ les nombres premiers inférieurs à $x$. Il faudrait alors que tous les nombres de la forme $2x - p_i$ ($p_i$ premier impair inférieur à $x$) soient composés. Ces nombres composés devraient avoir chacun au moins deux diviseurs premiers impairs inférieurs à $x$.

Etudions d'abord un cas d'école, où seulement trois nombres premiers seraient inférieurs à $x$, nous les appellerons $p_1 = a$, $p_2 = b$ et $p_3 = c$. Il s'agit vraiment d'un cas d'école puisque la conjecture a été vérifiée par ordinateur jusqu'à $3.10^{17}$ en décembre 2005 par l'équipe portugaise d'Oliveira et Silva. Représentons pour ce cas d'école tous les graphes possibles de divisibilité qui représenteraient le fait que tous les $2x - p_i$ ($p_i \in [a, b, c]$) aient au moins deux diviseurs premiers impairs différents chacun, à choisir parmi $a$, $b$ ou $c$. Le nombre total de tels graphes est 27 ($= 3^3$).

Expliquons d'abord comment lire un graphe : à gauche, les sommets représentent les nombres premiers $p_i$ inférieurs à $x$. A droite, les sommets représentent leur "correspondant", égal à $2x - p_i$ pour chacun d'entre eux. On prend l'habitude de disposer les sommets à des distances égales alors que les nombres premiers ne sont pas également espacés en réalité, ce pour des raisons de lisibilité.

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

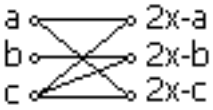



Figure 1 : un exemple

Par exemple, le graphe ci-dessus se lit : $2x-a$ est divisible par $a$ et $c$, $2x-b$ est divisible par $b$ et $c$ et $2x-c$ est divisible par $a$ et $c$. Appelons $d_1$ l'écart entre $p_1 = a$ et $p_2 = b$ et appelons $d_2$ l'écart entre $p_2 = b$ et $p_3 = c$. On retrouve ces écarts $d_1$ entre $2x-a$ et $2x-b$ et $d_2$ entre $2x-b$ et $2x-c$.

On gardera en mémoire le fait que les écarts entre les nombres premiers se retrouvent "en face". Si les écarts sont à gauche de haut en bas $d_1$ entre $p_1$ et $p_2$, $d_2$ entre $p_2$ et $p_3$, on retrouvera "en face" les mêmes écarts, $d_1$ entre $2x-p_1$ et $2x-p_2$ et $d_2$ entre $2x-p_2$ et $2x-p_3$.

Etudions toutes les possibilités que chacun des $2x-p_i$ soit divisible par au moins 2 nombres premiers impairs $p_i$ différents sur la figure 2, page suivante.

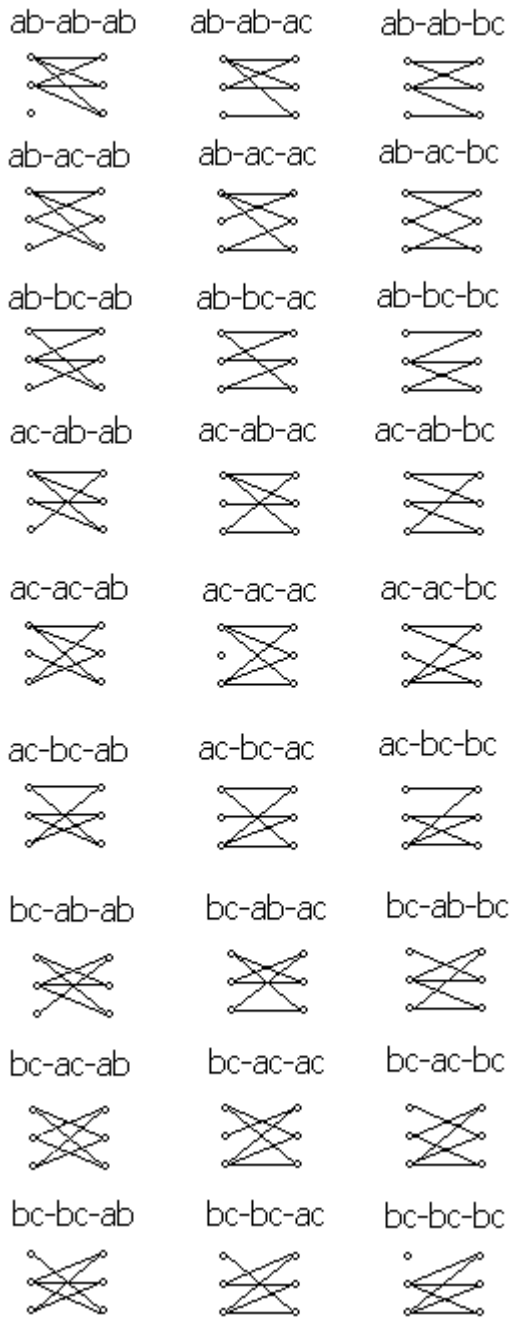



Figure 2 : combinatoire des différentes possibilités de divisibilité par deux nombres premiers impairs différents

:

Un graphe aboutit à une contradiction s'il contient l'une des configurations d'arcs présentées dans la figure 3.

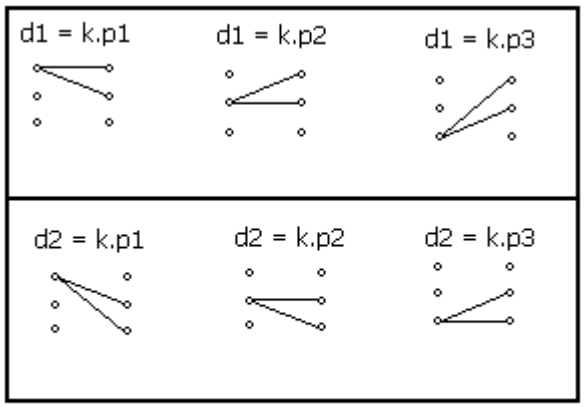


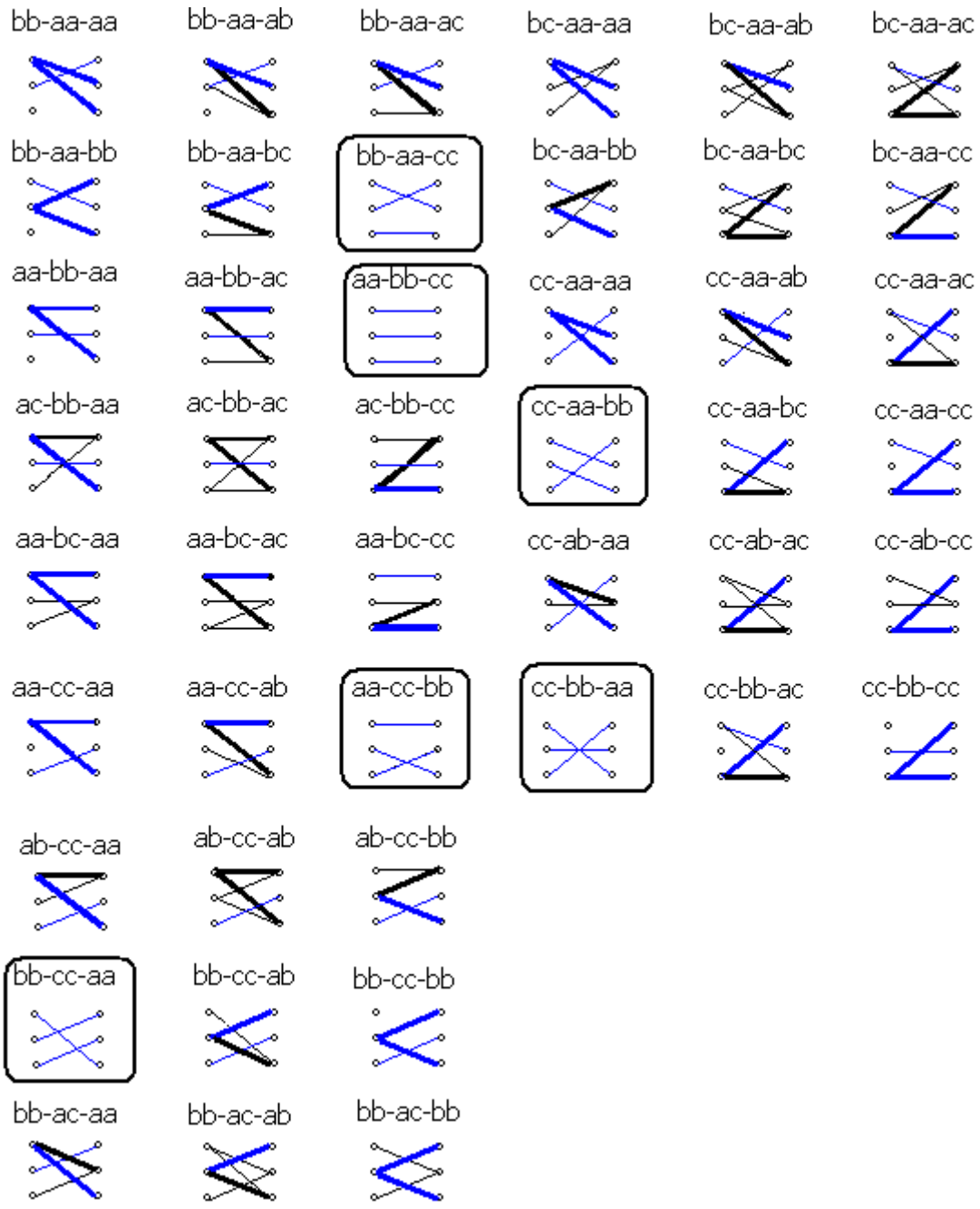

*Figure 3 : impossibilités dans le cas de 3 premiers*

Expliquons le cas du graphe qu'on appelle $d1 = k.p_1$. Si $2x - a$ et $2x - b$, qui sont séparés par l'écart $d1$ sont tous les deux divisibles par $p_1 = a$, cet écart existant également entre $p_1 = a$ et $p_2 = b$, alors $p_2$ ne pourrait pas être premier, ce qui est contradiction avec nos hypothèses. On peut faire un raisonnement similaire pour le graphe nommé $d2 = k.p_2$.
Pour les 3 configurations correspondant aux cas appelés $d_i = k.p_j$ avec $j > i$, l'impossibilité vient du fait qu'entre un nombre premier et le nombre premier précédent, l'écart ne peut être un multiple de n'importe quel nombre premier supérieur (par définition, un nombre est premier s'il y a un écart de taille lui-même entre zéro et lui, et il ne pourrait y avoir d'écart multiple de lui entre deux nombres premiers qui lui seraient inférieurs). Quant à la configuration $d_2 = k.p_1$, si $2x - p_2$ et $2x - p_3$, tous deux impairs, sont tous les deux divisibles par $p_1$, l'écart entre eux est forcément strictement supérieur à $2.p_1$. Or, le postulat de Bertrand, prouvé par Tchebychev, affirme qu'il y a toujours un nombre premier entre un nombre et son double. Cela est en particulier valable si le nombre en question est premier. On a donc $d_2 < p_2 < 2.p_1$. $d_2$ ne pouvant être simultanément strictement inférieur et strictement supérieur à $2.p_1$, on aboutit là-encore à une contradiction ; ce cas est à rapprocher des cas de contradictions concernant $d_2$ que l'on a déjà trouvés précédemment ;

On voit que l'on aboutit à une impossibilité dès que $d_i = k.p_j, \forall i, \forall j$.

Problème : on n'a pas envisagé les possibilités pour les $2x - p_i$ d'être divisibles par un carré de premier impair, ce qui les rendrait également composés. La combinatoire augmente alors considérablement : on passe de 3 possibilités d'associations pour chacun des 3 sommets à droite à 6 chacun : $aa$, $ab$, $ac$, $bb$, $bc$ et $cc$. Ce qui fait un total de 216 ($= 6^3$) minis-graphes à étudier. Sur ces 216, 189 contiennent des arcs contradictoires. Pour les 27 restant, dessinés sur la figure ci-après, on va pouvoir éliminer certains, grâce à la découverte de nouvelles contradictions mais on restera ennuyée par les autres.

Les arcs correspondant à la divisibilité par un carré de premier impair sont dessinés en bleu.




Les quatre configurations d'arcs page suivante sont elles-aussi impossibles :

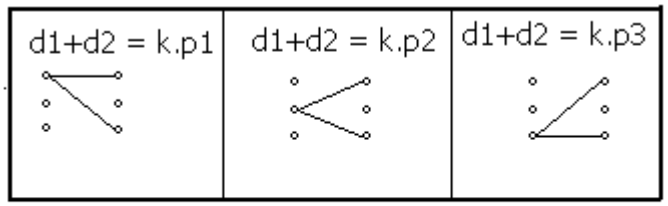



*Figure 5 : impossibilités sur d1+d2*

- Pour le cas $d_1 + d_2 = k.p_1$, ce qui aurait pour conséquence $p_3$ non premier ;
- Pour le cas $d1 + d2 = k.p_2$, si $2x - p_1$ et $2x - p_3$, tous deux impairs, sont tous les deux divisibles par $p_1$, l'écart entre eux est forcément strictement supérieur à $4.p_1$ (il y a $2x - p_2$ entre eux deux). Comme conséquence de Tchebychev, on a cette fois-ci que $d_1 + d_2 < p_1 + p_2 < 3.p_1$. On est face à un nouveau cas de contradiction.
- Pour le cas $d1 + d2 = k.p_3$ : il ne peut y avoir entre un nombre premier $p$ et un nombre premier inférieur à $p$ un écart multiple de $p$ ;

On a épaissi les arcs de ces configurations impossibles, dans les 45 cas pour lesquels on n'avait pas encore conclu. Il reste encore les 6 cas pour lesquels chacun des $2x - p_i$ est divisible par un carré de premier impair. On a entouré les graphes correspondant dans la figure de la page 5. Il faut comprendre pourquoi ces cas sont impossibles.

Pour résumer, dès que deux sommets de la partie droite d'un graphe sont reliés à un même sommet de la partie gauche du graphe, on aboutit à une contradiction. Les configurations d'arcs impossibles sont :

- soit de la forme $d_i = k.p_j$ ;
- soit de la forme $\Sigma d_i = k.p_j$.

# 3 Extension à quatre ou cinq sommets

Pour 4 sommets, les possibilités pour chaque élément de l'ensemble d'arrivée d'être associé à deux éléments différents de l'ensemble de départ peuvent se dénoter comme suit : *ab, ac, ad, bc, bd, cd.* Cela engendre $6^4 = 1296$ graphes possibles sans étudier les carrés de premiers impairs, qu'il est hors de question de dessiner ! Si on prend également en compte la possibilité d'être divisible par les carrés de nombres premiers impairs, on arrive à $10^4 = 10000$ graphes possibles. Certaines impossibilités proviennent des portions de graphes représentées sur la *figure 4*:

Pourquoi ces configurations “couvrent-elles” tous les graphes (hors cas de multiples de carrés de premiers d'impairs) que l'on peut envisager, qui feraient que tous les $2x - p_i$ soient simultanément composés ? Observons une colonne de graphes telle que celle contenant les 3 configurations $d_1 = k.p_3, d_2 = k.p_3, d_3 = k.p_3$. Les graphes qui seront couverts par la première configuration $d1 = k.p_3$ devront avoir un $c$ dans le premier couple et un $c$ dans le deuxième couple. Les graphes qui seront couverts par la deuxième configuration $d_2 = k.p_3$ devront avoir un $c$ dans le deuxième couple et un $c$ dans le troisième couple. Les graphes qui seront couverts par la troisième configuration $d_3 = k.p_3$ devront avoir un $c$ dans le troisième couple et un $c$ dans le quatrième couple. Tous les graphes (hors cas des carrés de premiers impairs) sont donc “couverts” par ces 3 configurations à peine et aboutissent ainsi tous à une contradiction.

Pour 5 sommets, les possibilités pour chaque élément de l'ensemble d'arrivée d'être associé à deux éléments de l'ensemble de départ peuvent se dénoter comme suit : *ab, ac, ad, ae, bc, bd, be, cd, ce, de.* Dans l'ensemble de ces possibilités, chaque lettre apparaît $\frac{2}{5}$ fois. Le nombre 10 d'associations possibles est égal à $\frac{5\times4}{2}$. Cela engendre $10^5 = 10000$ graphes possibles. Si l'on ajoute les cas de divisibilité par des carrés de nombres premiers impairs, on arrive à $15^5$ graphes.

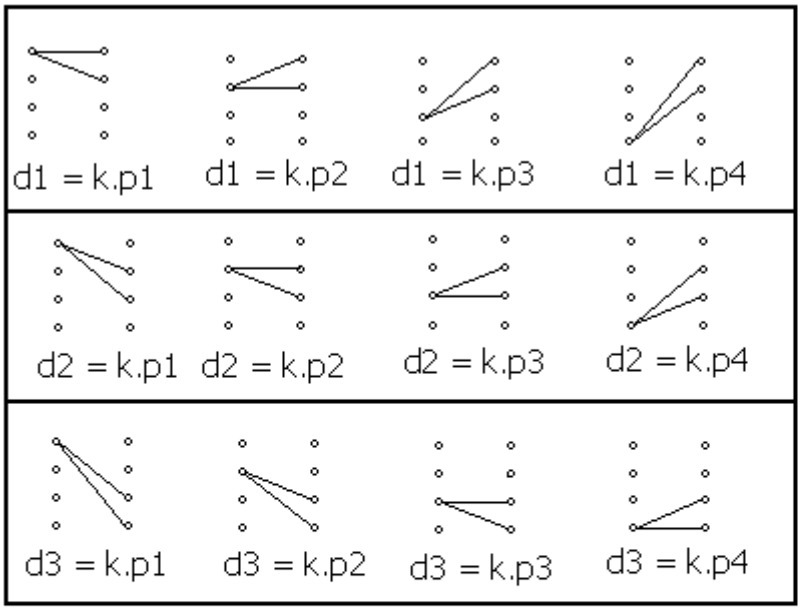



*Figure 4 : certaines impossibilités sur les di dans le cas de 4 premiers impairs*

## 4 Généralisation à $n$ sommets

Si l'on s'intéresse aux graphes contenant $2n$ sommets. Chacun des $n$ sommets droits du graphe a $\frac{n(n-1)}{2}$ possibilités différentes d'être divisible par 2 nombres premiers différents parmi les $n$ sommets gauches du graphe. Cela amène à un nombre de $(\frac{n(n-1)}{2})^n$ graphes possibles qui conduisent tous à une contradiction, car une diagonale "couvre" tous les graphes. Quand on ajoute les possibilités de divisibilité par des carrés de premiers impairs, le nombre de graphes s'élève à $(\frac{n(n+1)}{2})^n$.

Les $n-1$ premiers graphes associent chacun le sommet $p_i$ à gauche avec les deux sommets à droite qui sont aux positions $i$ et $i+1$ en partant du haut. Ils correspondent aux contradictions de la forme $d_i = k.p_i$.

Les $\frac{n(n-1)}{2}$ graphes suivants correspondent aux contradictions de la forme $d_i = k.p_j$ avec $j > i$. La *ième* ligne de graphes contient $n - i + 1$ graphes. Chaque graphe de cette ligne associe tous les nombres premiers de $p_{i+1}$ à $p_{\Pi(x)}$ à gauche avec les nombres aux positions $i$ et $i+1$ en partant du haut à droite.

D'autres graphes correspondent aux contradictions $d_i = k.p_j$ avec $j < i$. D'autres enfin correspondent aux contradictions $\Sigma d_i = k.p_j$ avec $j < i$.

## 5 Conclusion

Les $2x-p_i$ ne peuvent pas avoir chacun deux diviseurs premiers impairs différents simultanément : on aboutit à des contradictions avec les hypothèses. Si l'on arrive à résoudre les cas faisant intervenir seulement des carrés de premiers impairs, on pourra peut-être conclure que l'un au moins des $2x - p_i$ est premier et fournit avec $p_i$ une décomposition Goldbach de $2x$. Pourra-t-on alors enfin utiliser la formulation *"tout entier naturel supérieur à 2 est le milieu de deux nombres premiers"* ?

## References


[1] P. Damphousse. *L'arithmétique ou l'art de compter*. Éd. Le Pommmier, 2002.

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

[3] 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.

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

[5] 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.

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

# 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 $\Pi$ 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 $NbFact(x!) - NbFact((x/2)!)$.

Peut-être faut-il utiliser la formule :

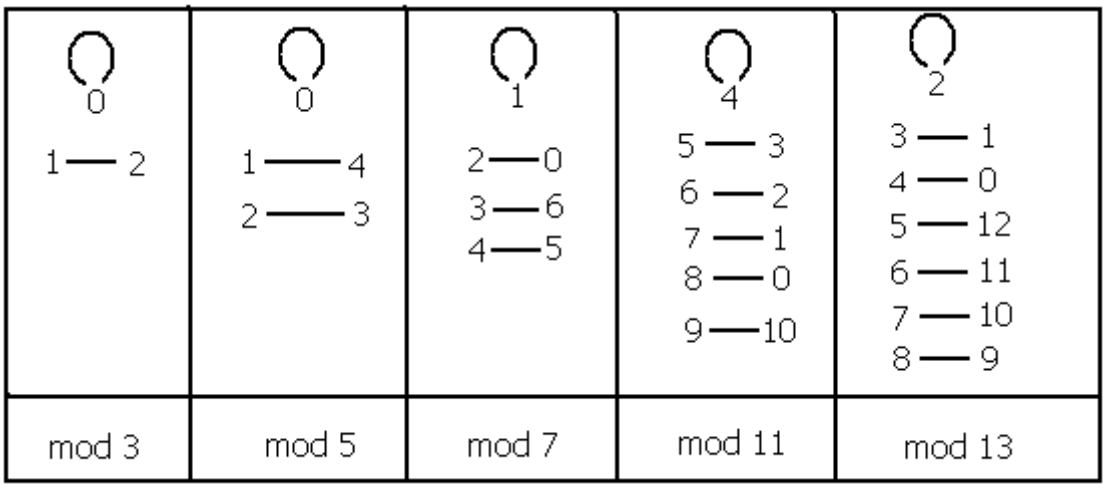
$$
\begin{aligned}
& x \left( \frac{1}{2} + \frac{1}{2^2} + ... + \frac{1}{2^{x_2}} \right) \\
+ \; & x \left( \frac{1}{3} + \frac{1}{3^2} + ... + \frac{1}{3^{x_3}} \right) \\
& \qquad ... \\
+ \; & x \left( \frac{1}{p_i} + \frac{1}{p_i^2} + ... + \frac{1}{p_i^{x_i}} \right) \\
- \; & x/2 \left( \frac{1}{2} + \frac{1}{2^2} + ... + \frac{1}{2^{y_2}} \right) \\
- \; & x/2 \left( \frac{1}{3} + \frac{1}{3^2} + ... + \frac{1}{3^{y_3}} \right) \\
& \qquad ... \\
- \; & x/2 \left( \frac{1}{p_i} + \frac{1}{p_i^2} + ... + \frac{1}{p_i^{y_i}} \right) \\
+ \; & 3x/2
\end{aligned}
$$

dans laquelle $p_i$ est le plus grand nombre premier inférieur à $x$, les nombres $x_2$, $x_3$, $x_i$ (resp. les nombres $y_2$, $y_3$, $y_i$) sont les puissances maximales des facteurs premiers 2, 3, ou $p_i$ dans la factorisation de $x$ (resp. de $x/2$).
Si le nombre de facteurs du produit des impairs compris entre $x$ et $2x$ était toujours inférieur à $x$, cela garantirait que les $2x - p_i$ ($p_i$ impair) ne peuvent être tous simultanément composés, et a fortiori que les $2x - p_i$ ($p_i$ premier) ne peuvent être tous simultanément composés, et impliquerait la conjecture. Il reste à trouver une ruse pour prouver que cela est toujours vrai, ou bien trouver un contre-exemple qui stopperait cette tentative aussi net que les précédentes. Contre-exemple trouvé dès 300 : le nombre de facteurs du produit des impairs compris entre 300 et 600 est 304 qui n'est pas inférieur à 300.

Il y a un phénomène qui peut surprendre : quand on calcule le nombre de décompositions Goldbach des entiers successifs, ce nombre semble régulièrement croître globalement. Mais comment cela n'est-il pas en contradiction avec le fait que les nombres premiers se raréfient de plus en plus ? Doit-on imaginer une espèce de "milieu de l'infini" (!) à partir duquel la tendance s'inverserait faisant alors décroître le nombre de décompositions Goldbach (comme selon une symétrie-miroir) pour tendre à l'infini vers les nombres de décompositions des premiers nombres entiers pairs ? Ou bien doit-on ne pas voir de contradiction entre l'augmentation du nombre de décompositions Goldbach et la raréfaction des nombres premiers, et imaginer que les nombres premiers sont en quelque sorte de "plus en plus rentables", c'est à dire qu'une proportion de plus en plus grande d'entre eux permettrait d'obtenir des décompositions Goldbach, ce qui ferait que même si les nombres premiers se raréfient le nombre de décompositions Goldbach quant à lui, augmente. Mystère...

# 3 Approche utilisant une vision ensembliste et relationnelle du problème

Dans une note précédente, on avait dessiné un maillage géométrique qui faisait apparaître les décompositions Goldbach et on avait vu que l'on pouvait représenter les relations symétriques liant les restes modulaires des nombres de part et d'autre d'un entier par des graphes symétriques. Par exemple, si l'on cherche les décompositions de 30, on a les 5 petits graphes de symétrie de la figure ci-dessous, correspondant aux nombres premiers inférieurs à 15 (moitié de 30).




On voit sur ces graphes que les nombres qui ne permettent pas d'obtenir de décompositions Goldbach sont toujours congrus à $(2x \ mod \ p)(modulo \ p)$ (en effet, ces nombres doivent être ajoutés à un composé pour trouver $2x$, qu'ils soient eux-mêmes premiers ou pas). Il faudrait tenir un raisonnement similaire à celui vu dans la première section, qui assurerait que même si certains nombres premiers sont éliminés du fait de leur "appariement à 0", l'ensemble résultant de l'élimination par modulo ne se retrouvera jamais complètement vide.

Ecrivons les nombres impairs de 3 à 15. Eliminons ceux qui sont congrus soit à $0\,(mod\ 3)$, soit à $0\,(mod\ 5)$, soit à $2\,(mod\ 7)$, soit à $8\,(mod\ 11)$, soit à $4\,(mod\ 13)$. 3, 5, 9 et 15 se trouvent éliminés par ce processus. Les nombres qui subsistent ont forcément un nombre premier en face. Mais sont-ils premiers eux-mêmes ? On doit constater que les différents ensembles de nombres éliminés ne sont pas disjoints 2 à 2. Par exemple, 9 est éliminé parce qu'il est congru à 0 (mod 3) mais également parce qu'il est congru à 2 (mod 7). Les 3 nombres premiers restant 7, 11 et 13 fournissent chacun l'une des décompositions Goldbach recherchées de 30.

Pourquoi est-il impossible d'éliminer tous les nombres premiers inférieurs à $x$ par cette méthode ?

Plaçons nous dans le "pire des cas", où chacun des nombres premiers éliminerait un maximum de nombres impairs et où tous les ensembles de nombres ainsi

éliminés seraient disjoints. Chaque nombre premier élimine $x/2p$ nombres impairs dans l'ensemble des impairs compris entre 3 et $x$. Puisqu'on s'est placé dans la "pire" hypothèse où les ensembles sont disjoints, le nombre total d'impairs éliminés est $\Sigma_{p_i \leq x} \frac{1}{2p_i}$. Si ce nombre est toujours inférieur à $x/2$, on est assuré qu'il restera un impair. Encore faut-il qu'il soit premier... On sait que les chances qu'a un nombre inférieur à $x$ d'être premier sont égales au produit de $x$ par le produit des $p-1/p$ avec $p$ premier. Mais à nouveau, on est complètement bloqué quant à la façon de poursuivre dans cette voie.

D'un point de vue bibliographique, Erdös a introduit la notion d'ensemble de congruences couvrantes. Ici, il faudrait restreindre la notion et parler d'ensemble de congruences couvrant au moins un premier inférieur à $x$. L'ensemble de congruences correspondant à notre exemple s'écrit $\{(3,0),(5,0),(7,2),(11,8),(13,4)\}$. Cet ensemble couvre au moins un premier inférieur à 15.

Pour prouver la conjecture, il faudrait être capable de prouver que l'ensemble de congruences $\bigcup (p_i, 2x \ mod \ p_i)$ ($p_i$ premier inférieur à $x$) couvre toujours un nombre premier inférieur à $x$.

# 4 Personnages

Des éléments de la biographie de trois personnages m'ont marquée pendant ces recherches : il s'agit de Leonhard Euler, Sophie Germain et Paul Erdös. L'article *"Découverte d'une loi toute extraordinaire des nombres par rapport à la somme de leurs diviseurs"* [5] est impressionnant. L'émerveillement du mathématicien devant la "magie" des nombres s'en dégage de façon intemporelle. J'ai programmé le calcul récursif de la somme des diviseurs mais la formule reste hermétiquement incompréhensible[3]. La deuxième personne dont la destinée est très émouvante est Sophie Germain, contrainte de se déguiser en homme pour accéder à une once de considération. Cette considération est loin d'être acquise par les femmes encore aujourd'hui ! Enfin, j'ai été émue par le personnage de Paul Erdös, le Peter Pan mathématicien errant. Terminons par l'une de ses phrases : *"Je sais que les nombres sont beaux. S'ils ne le sont pas, rien ne l'est."*

# 5 Interrogation

Il faut être très prudent et méfiant quand on a une "impression de convergence" lors de calculs par programme informatique. J'ai donc l'impression que la somme des inverses des primorielles converge vers 1.70523.... On peut trouver sur la toile une constante assez proche de celle-ci : c'est la constante de Niven, qui a travaillé sur l'exposant moyen des factorisations des entiers.

# 6 Conclusion

J'aimerais tellement (méthode incantatoire... !) utiliser la formulation *"tout entier naturel supérieur à 2 est le milieu de deux nombres premiers"*.

[3] Il y a peut-être une formule récursive semblable qui lie entre elles les décompositions Goldbach ou leurs nombres.

# References


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

[2] B. Danchilla. *Summer 2003 Project : Open conjectures in number theory.* Éd. Note bibliographique, 2004.

[3] J.F. Gold, D.H. Tucker. *On a conjecture of Erdös.* Éd. Proceedings NCUR VIII, Vol.2, p.794-798, 1994.

[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. Guinot. *Ce "diable d'homme" d'Euler.* Éd. Aleas, 2000.

[6] 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.

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

# Conjecture de Goldbach et recherche d'un sous-graphe d'ordre maximal dans un graphe à arêtes colorées

Denise Vella

Juin 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 Etude d'exemples

### 2.1 x=14

Pour trouver une décomposition Goldbach de $28 = 2.14$, on peut apparier l'un des 5 nombres premiers inférieurs à 14, (3, 5, 7, 11 ou 13) à son complémentaire à 28 (25, 23, 21, 17 ou 15) lorsque celui-ci est premier. Seuls 17 et 23 sont premiers, ce qui fournit 2 décompositions Goldbach de 28.

On peut représenter les propriétés de divisibilité qui lient ces différents nombres sur le graphe biparti suivant, composé à gauche des nombres premiers $p_i$ inférieurs à $x$ et à droite des $2x - p_i$ correspondant.

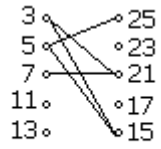



Figure 1 : x=14

Quand un nombre premier divise deux nombres, il divise également l'écart qui les sépare. Sur notre exemple, 3 divise 15 et 21 "parce qu"' il divise l'écart qui sépare 15 de 21, en l'occurrence 6. Or, cet écart est également celui qui sépare les complémentaires à $2x$ de 15 et 21 qui sont 7 et 13.

Intéressons-nous alors au graphe complet dont les sommets sont les nombres premiers inférieurs à $x$. Associons une couleur à chaque nombre premier. On colorie dans le graphe complet un arc entre deux nombres $x$ et $y$ de la couleur d'un nombre premier impair $p$ si $p$ divise l'écart entre $x$ et $y$ ; la couleur rouge (resp. jaune) correspond à la divisibilité par 3 (resp. 5).

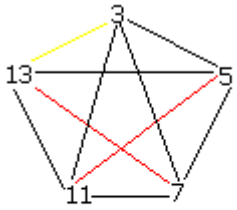



Fig. 2 : divisibilité des écarts entre premiers

Les arêtes de divisibilité entre les $p_i$ et les $2x - p_i$ qu'on avait représenté dans la figure 1 se retrouvent dans le graphe de la figure 2. On va épaissir les arêtes du graphe de la figure 2 correspondant aux arcs du graphe de la figure 1. Par exemple, épaissir l'arête jaune entre 3 et 13 représente le fait que 5 divise à la fois le complémentaire de 3 et le complémentaire de 13. Enfin, on supprime du graphe complet les arêtes correspondant aux écarts qui sont des puissances de 2 car ils ne nous intéressent pas.

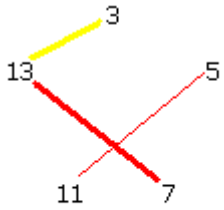



Fig. 3 : arcs étudiés si x = 14

Les sommets 5 et 11 ne sont pas "touchés" par des arêtes épaissies. Ils permettent chacun de trouver une décomposition Goldbach de 28.

Le fait de trouver une décomposition Goldbach de $x$ semble donc lié au fait de trouver un sous-graphe du graphe de divisibilité des écarts, respectant certaines contraintes, et qui soit recouvrant[1] ou pas.

## 2.2 Deux autres exemples

Représentons d'abord ci-dessous les graphes de divisibilité pour les cas $x = 21$ et $x = 28$.

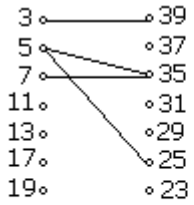



Fig. 4 : x=21

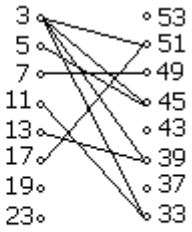



Fig. 4 bis : x=28

Représentons ci-après les sous-graphes des graphes complets de divisibilité des écarts entre premiers pour les cas $x = 21$ et $x = 28$, dans lesquels on a épaissi les arêtes obligatoirement utilisables du fait de la valeur de $x$.

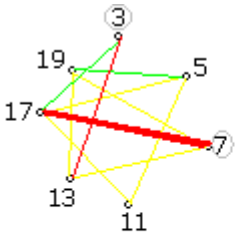



Fig. 5 : x=21

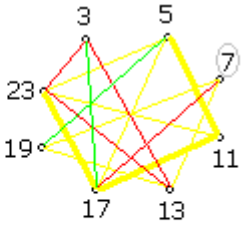



Fig. 5 bis : x=28

On a entouré en gris les sommets associés aux nombres premiers impairs qui divisent $x$. Les sommets qui ne sont ni entourés, ni extrémités d'arêtes épaissis permettent de trouver des décompositions Goldbach de 42 ($42 = 5 + 37 = 11 + 31 = 13 + 29 = 19 + 23$) et de 56 ($56 = 3 + 53 = 13 + 43 = 19 + 37$).

[1] Un sous-graphe d'un graphe est recouvrant s'il en contient tous les sommets.

# 3 Matrice de divisibilité des écarts

La représentation par des graphes est très vite illisible. On utilisera donc plutôt une représentation par matrice ; dans celle ci-dessous, $p$ nombre premier impair se trouve dans la case $(i, j)$, $j$ étant supérieur strictement à $i$ si $p|j - i$ :

| | **3** | **5** | **7** | **11** | **13** | **17** | **19** | **23** |
|---|---|---|---|---|---|---|---|---|
| **3** | X | | | | | | | |
| **5** | | X | | | | | | |
| **7** | | | X | | | | | |
| **11** | | 3 * | | X | | | | |
| **13** | 5 | | 3 | | X | | | |
| **17** | 7 | 3 | 5 ** | 3 * | | X | | |
| **19** | | 7 | 3 | | 3 | | X | |
| **23** | 5 | 3 | | 3 | 5 | 3 * | | X |

Le fait de fixer $x$, à la recherche des décompositions Goldbach de $2x$ consiste à "être contraint" d'utiliser certaines cases de la matrice.

La case marquée de deux étoiles correspond à l'arête à épaissir dans le graphe 5. Les trois cases marquées d'une étoile correspondent aux arêtes à épaissir dans le graphe 5 bis.

# 4 Les arêtes de transitivité

Etudions à nouveau le graphe de la figure 5 bis correspondant au cas $x = 28$. On appellera "arête de transitivité" une arête d'une certaine couleur reliant deux sommets $x$ et $z$ et tel qu'il existe un sommet $y$ relié à $x$ et à $z$ par deux arêtes de la même couleur que l'arête reliant $x$ à $z$. Ces arêtes sont "redondantes" avec les arêtes non transitives. On éliminera ainsi du graphe les arêtes $(3, 23)$ (redondante avec $(3, 13)$ et $(13, 23)$), $(5, 17)$ (redondante avec $(5, 11)$ et $(11, 17)$), $(5, 23)$ (redondante avec $(5, 17)$ et $(17, 23)$), , $(11, 23)$ (redondante avec $(11, 17)$ et $(17, 23)$), , $(7, 19)$ (redondante avec $(7, 13)$ et $(13, 19)$). Eliminons les arêtes redondantes du graphe de la figure 5 bis. On obtient le graphe beaucoup plus lisible suivant :

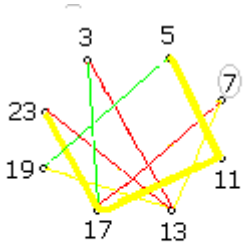



Fig. 5 bis : x=28

# 5 Les croisements

Certains croisements ont pour conséquence des impossibilités d'épaissir simultanément certaines arêtes.

Revenons à notre cas initial. 3 divise l'écart entre 5 et 11 mais 3 divise également l'écart entre 7 et 13. Cependant, on n'aura pas le droit d'utiliser simultanément ces deux arêtes lors de la recherche d'un sous-graphe d'ordre maximal. Ce sont des arêtes mutuellement exclusives : si 3 divise le correspondant de 5 alors il divise le correspondant de 11 et réciproquement. Si 3 divise le correspondant de 7, alors il divise le correspondant de 13 et réciproquement. Mais une chose est sûre, 3 ne peut diviser simultanément le correspondant de 3 et le correspondant de 5 puisque 3 et 5 sont séparés seulement d'un écart de 2.

Dans le graphe 5 bis initial, par contre, il y avait un croisement entre les arêtes rouges (5, 17) et (11, 23) ; ces arêtes pourraient cependant être épaissies simultanément sans qu'il y ait de contradiction car il s'agit d'arêtes de transitivité.

Il est à noter que cette notion de croisement est liée ici au fait que l'on a implicitement disposé les sommets sur un cercle et considéré que les arêtes devaient passer à l'intérieur du cercle. On pourrait éviter les "croisements" en dessinant les arêtes à l'extérieur du cercle, permettant ainsi au graphe d'être "planaire" (terme employé dans la littérature). La contrainte de planarité est à appliquer ici à des arêtes monochromes. Il faudra étudier précisément ces croisements pour savoir si on n'a jamais le droit de les utiliser dans le cas où il ne s'agit pas d'arcs de transitivité dans la recherche d'un sous-graphe multicolore recouvrant et planaire mono-chromatiquement.

# 6 Sommets n'appartenant pas à un sous-graphe d'ordre maximal

Dans les quatre cas qui ont été étudiés, les sommets qui ne divisaient pas $x$ et qui n'appartenaient pas au sous-graphe d'ordre maximal permettaient d'obtenir des décompositions Goldbach. Est-ce toujours le cas ? Prouver la conjecture de Goldbach est il équivalent à prouver qu'un sous-graphe d'ordre maximal n'est jamais recouvrant ? Les résultats déjà connus en théorie des graphes sur la recherche de sous-graphes respectant certaines contraintes nous permettraient-ils de conclure quant à la prouvabilité de la conjecture de Goldbach ?

# 7 Conclusion

Il semblerait qu'il y ait autant de décompositions Goldbach de $2x$ que de sommets non diviseurs premiers impairs de $x$ et n'appartenant pas à un sous-graphe d'ordre maximal du graphe des nombres premiers inférieurs à $x$. Quand pourra-t-on enfin utiliser la formulation *"tout entier naturel supérieur à 2 est le milieu de deux nombres premiers"* ?...

# References


[1] O. Cogis, C. Robert. *Au-delà des ponts de Königsberg, Théorie des graphes. Problèmes, théorèmes, algorithmes.* Éd. Vuibert, 2003.

[2] P. Damphousse. *L'arithmétique ou l'art de compter.* Éd. Le Pommmier, 2002.

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

[6] 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.

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

# 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 :

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

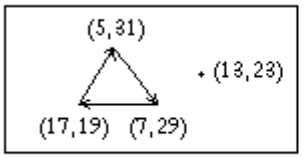
mais $17 * 7 \equiv 11$ et $17 * 5 \equiv 13$.

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

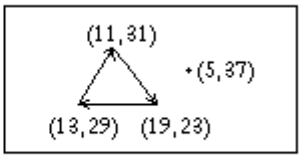
$$11 * 23 \equiv 1 \ (mod\ 42)$$
$$13^2 \equiv 1 \ (mod\ 42)$$
$$37^3 \equiv 1 \ (mod\ 42)$$

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

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

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

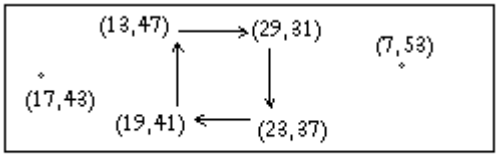
Pour les 5 nombres dont on vient de fournir les congruences qui semblent pertinentes, on n'a pas trouvé de représentation géométrique illustrative.

## 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.

$$7 * 13 \equiv 31 \ (mod\ 60)$$
$$7 * 31 \equiv 37 \ (mod\ 60)$$
$$7 * 37 \equiv 19 \ (mod\ 60)$$
$$7 * 19 \equiv 13 \ (mod\ 60)$$

$$17 * 13 \equiv 41 \ (mod\ 60)$$
$$17 * 19 \equiv 23 \ (mod\ 60)$$
$$17 * 23 \equiv 31 \ (mod\ 60)$$
$$17 * 29 \equiv 13 \ (mod\ 60)$$

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

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

$$5 * 13 * 19 * 23 * 29 \equiv 1 \ (mod\ 66)$$
$$5 * 53 \equiv 1 \ (mod\ 66)$$
$$7 * 19 \equiv 1 \ (mod\ 66)$$

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

$$5 * 11 * 19 * 29 * 31 \equiv 1 \ (mod\ 72)$$
$$5 * 29 \equiv 1 \ (mod\ 72)$$
$$11 * 59 \equiv 1 \ (mod\ 72)$$
$$19^2 \equiv 1 \ (mod\ 72)$$

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

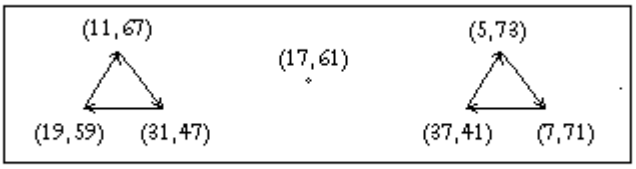
$$3 * 11 * 17 * 41 \equiv 1 \ (mod\ 100)$$
$$17 * 53 \equiv 1 \ (mod\ 100)$$
$$47 * 83 \equiv 1 \ (mod\ 100)$$

## 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 :

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

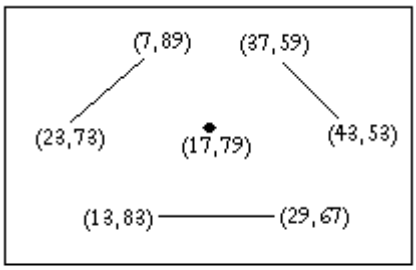
L'action de 17 sur le deuxième triangle correspond aux calculs modulaires suivants :

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

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 $f_\sigma$, dans $A[X_1, ..., X_n]$, tel que

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

Quels que soient $\sigma, \tau$, 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 $\lambda$ 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 $\sigma_1$ de trois inconnues, la somme $\sigma_2$ des doubles produits et le produit $\sigma_3$ 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 $\sigma_1$ 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 $\sigma_1$ 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 $p^\nu$ 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 $p^\nu$, 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 $p^\nu$ 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.

# Esthétique des décompositions Goldbach de certains nombres pairs

Denise Vella

Septembre 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"*.

Je "cotoie" les décompositions Goldbach des nombres inférieurs à 100 depuis un an. J'ai essayé d'approcher la conjecture de multiples manières, toutes infructueuses. Si les exemples qui vont être présentés ici sont le résultat de coïncidences, leur multitude reste troublante. En tant qu'amatrice, je leur trouve même une certaine beauté, ce qui explique le titre de cette note. Dans la suite, on appellera "nombre premier décomposant $2a$" un nombre premier inférieur à $a$ fournissant une décomposition Goldbach de $2a$ (c'est à dire un nombre premier $p$ inférieur à $a$ tel que $q = 2a - p$ est également premier).

## 2 Solutions d'équations polynômiales ?

L'article "le théorème de Noël" du livre de Ian Gordon [12] présente le domaine de la "géométrie des nombres", dont Minkowski est à l'origine.
On y trouve l'exemple suivant : 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'équations polynômiales particulières dans l'anneau $\mathbb{Z}_{2a}$ du nombre pair considéré. Le travail présenté ici consiste à rechercher quelles peuvent être ces équations polynômiales. On essaie alors de trouver des similitudes entre les cas correspondant aux nombres pairs qui admettent le même nombre de décompositions.

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

On étudiera d'abord 6 cas particulièrement "esthétiques" du fait de l'intuition géométrique que l'on peut en avoir. Ensuite, on présentera certains "calculs troublants".

# 3 Huit merveilleux cas géométriques

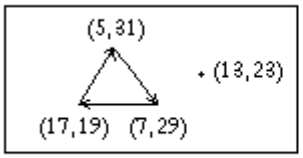
## 3.1 Nombre pair 24 : 3 décompositions Goldbach

24 possède les trois décompositions $5 + 19 = 7 + 17 = 11 + 13$[1].
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 :

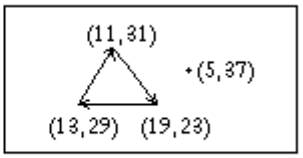
$$5 * 7 \equiv 11 \ (mod\ 24)$$
$$5 * 11 \equiv 7 \ (mod\ 24)$$
$$7 * 11 \equiv 5 \ (mod\ 24)$$

## 3.2 Nombres pairs 36 ou 42 : 4 décompositions Goldbach

Pour 36 ou 42, les solutions sont comme disposées aux 4 sommets de tétraèdres auxquels on ferait subir des rotations de $2\Pi/3$ selon un axe passant par l'un des sommets du tétraèdre. On a représenté cela sur les deux schémas ci-après (la base du tétraèdre est représentée par un triangle tandis que le sommet "selon" lequel s'effectue la rotation est le point extérieur au triangle).



Cas36 à 4 décompositions G.



Cas 42 à 4 décompositions G.

Pour 42 par exemple,

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

C'est dans l'article [2] qu'on a trouvé qu'il s'agit de la permutation 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

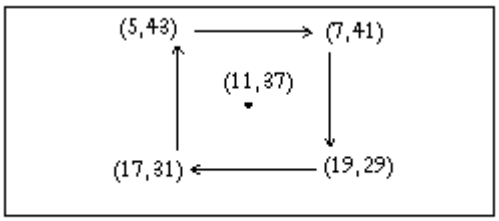
[1] Les 6 cas pour lesquels on a trouvé des configurations "esthétiques" des solutions sont systématiquement les *plus petits* nombres pairs (non compris les doubles de nombres premiers) qui ont 3, 4, 6 ou 7 décompositions.

passant par $d$. La permutation des trois sommets du triangle, alors que le quatrième sommet reste fixe se note :

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

### 3.3 Nombre pair 48 : 5 décompositions Goldbach

On est en présence d'une pyramide à base carrée. C'est la solution $11 + 37$ qui est sur l'axe de rotation d'angle $2\Pi/4$.




Cas 48 à 3 décompositions G.

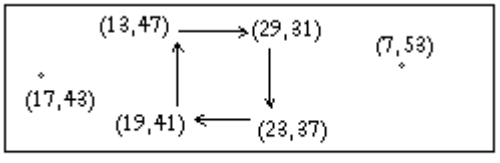
$$11 * 5 \equiv 7 \ (mod\ 48)$$
$$11 * 7 \equiv 29 \ (mod\ 48)$$
$$11 * 19 \equiv 17 \ (mod\ 48)$$
$$11 * 17 \equiv 43 \ (mod\ 48)$$

### 3.4 Nombres pairs 60 et 66 : 6 décompositions Goldbach

Pour 60 ($= 7 + 53 = 13 + 47 = 17 + 43 = 19 + 41 = 23 + 37 = 29 + 31$), on est en présence d'un octaèdre.

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

Cette fois-ci, on peut voir quatre solutions disposées en carré (la face "interne" de l'octaèdre), 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

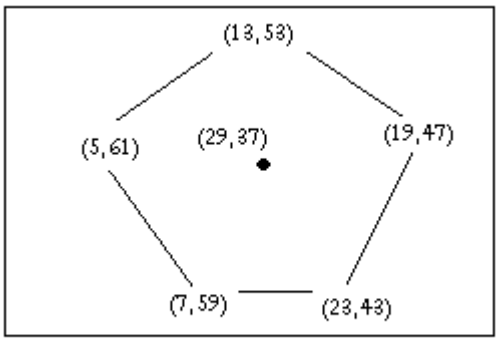
$$\begin{pmatrix} a & b & c & d & e & f \\ b & c & d & a & e & f \end{pmatrix}$$

dans l'autre sens.

$$7 * 13 \equiv 31 \ (mod\ 60)$$
$$7 * 31 \equiv 37 \ (mod\ 60)$$
$$7 * 37 \equiv 19 \ (mod\ 60)$$
$$7 * 19 \equiv 13 \ (mod\ 60)$$

$$17 * 13 \equiv 41 \ (mod\ 60)$$
$$17 * 19 \equiv 23 \ (mod\ 60)$$
$$17 * 23 \equiv 31 \ (mod\ 60)$$
$$17 * 29 \equiv 13 \ (mod\ 60)$$

Quant au nombre pair 66, on a une sorte de pyramide à base pentagonale et c'est la solution 29+37 qui appartient à l'axe de rotation de la pyramide qui subit une rotation de 2Π/5.




Cas 66 à 6 décompositions G.

La permutation des cinq sommets du pentagone, alors que le sixième sommet reste fixe se note

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

Les congruences correspondant à cette permutation sont :

$$29 * 5 \equiv 13 \ (mod\ 66)$$
$$29 * 13 \equiv 19 \ (mod\ 66)$$
$$29 * 19 \equiv 23 \ (mod\ 66)$$
$$29 * 23 \equiv 7 \ (mod\ 66)$$
$$29 * 7 \equiv 5 \ (mod\ 66)$$

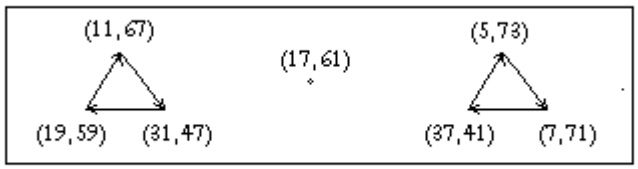
### 3.5 Nombres pairs 78 et 96 : 7 décompositions Goldbach

Ici, la configuration géométrique est connue sous le nom de "bipyramide" (on préfèrera noeud papillon rotatif !)

Pour 78 (= 5+73 = 7+71 = 11+67 = 17+61 = 19+59 = 31+47 = 37+41),

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

C'est encore 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 :

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

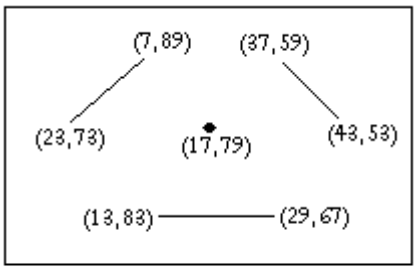
L'action de 17 sur le deuxième triangle correspond aux calculs modulaires suivants :

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

Enfin, pour le nombre pair 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 :

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

$$\begin{aligned} 17 * 7 &\equiv 23 \ (mod\ 96) \\ 17 * 23 &\equiv 7 \ (mod\ 96) \\ 17 * 37 &\equiv 53 \ (mod\ 96) \\ 17 * 43 &\equiv 59 \ (mod\ 96) \\ 17 * 13 &\equiv 29 \ (mod\ 96) \\ 17 * 29 &\equiv 13 \ (mod\ 96) \end{aligned}$$

# 4 Polynômes symétriques

On appelle *polynôme symétrique* un polynôme invariant par permutation de ses racines. Dans la suite, on appellera $\sigma_1$ la somme des racines, $\sigma_2$ la somme de tous les produits 2 à 2 des racines, ... $\sigma_i$ la somme de tous les produits de $i$ racines. Voici ce que l'on a découvert en effectuant toutes sortes 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. Développons le polynôme à une inconnue qui fait intervenir les trois solutions Goldbach.

$$\begin{aligned} (x-5)(x-7)(x-11) &= x^3 - 23x^2 + 167x - 385 \\ &= x^3 + x^2 - x - 1 \\ &= (x+1)^2(x-1) \end{aligned}$$

Ce polynôme s'annule si $x$ vaut 1 ou $-1$. Si au lieu d'une indéterminée, on écrit le polynôme à trois indéterminées.

$$(x-5)(y-7)(z-11) = xyz - 5yz - 7xz - 11xy + 55y + 77x + 35z - 385$$

Il s'annule si $x = y = z = 1$.

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 $\sigma_1$ 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 $\sigma_1$ 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).

Ces multiples exemples nous confortent dans l'idée qu'il faut creuser du côté des polynômes symétriques.

# 5 Derniers émerveillements

On travaille souvent sur le cas 98 car il n'a que 3 décompositions sur 19, 31 et 37. On se rend compte dans un premier temps du fait que si l'on ajoute les deux premières racines 19 et 31 ensemble ainsi qu'à leurs carrés respectifs, on obtient 1372 qui est divisible par 98. La troisième racine quant à elle a son carré qui est très proche de 1372 (1369). On n'a pas un traitement "équitable" des trois racines puisqu'on a d'abord trouvé une relation entre deux d'entre elles seulement, puis on a trouvé une propriété liant la troisième aux deux premières.

C'est insatisfaisant, on poursuit les calculs. Ce sera la somme des puissances 4èmes des racines ajoutée à la somme des carrés des racines qui sera "quasiment" divisible par 98 ($19^4+31^4+37^4+19^2+31^2+37^2 = 2930694$ tandis que $29905 \times 98 = 2930690$).

On essaye ainsi de trouver des polynômes symétriques qui relient *toutes* les solutions ensemble. Les résultats sont présentés dans le tableau ci-dessous.

| *Nombre pair* 2a | *Nombres premiers décomposants* | *polynôme divisible(ou"presque") par* 2a |
|---|---|---|
| 6 | $3$ | $\Sigma x + \Sigma x^2$ |
| 8 | $3$ | $\Sigma x + \Sigma x^2 + \Sigma x^3 + \Sigma x^4$ |
| 10 | $3, 5$ | $\Sigma x + \Sigma x^3$ |
| 12 | $5$ | $\Sigma x + \Sigma x^2 + \Sigma x^3 + \Sigma x^4$ |
| 14 | $3, 7$ | $\Sigma x + \Sigma x^4$ |
| 16 | $3, 5$ | $\Sigma x + \Sigma x^3$ |
| 18 | $5, 7$ | $\Sigma x^3$ |
| 20 | $3, 7$ | $\Sigma x + \Sigma x^3$ |
| 22 | $3, 5, 11$ | $\Sigma x^2$ |
| 24 | $5, 7, 11$ | $\Sigma x + \Sigma x^2$ |
| 26 | $3, 7, 13$ | $\Sigma x^4$ |
| 28 | $5, 11$ | $\Sigma x^3$ |
| 30 | $7, 11, 13$ | $\Sigma x^3$ |
| 32 | $3, 13$ | $\Sigma x + \Sigma x^3$ |
| 34 | $3, 5, 11, 17$ | $\Sigma x^3 + \Sigma x^4$ |
| 36 | $5, 7, 13, 17$ | $\Sigma x^3 + \Sigma x^4$ |
| 38 | $7, 19$ | $\Sigma x + \Sigma x^2 + \Sigma x^3$ |
| 40 | $3, 11, 17$ | $\Sigma x + \Sigma x^2 + \Sigma x^3$ |
| 42 | $5, 11, 13, 19$ | $\Sigma x^2$ |
| 44 | $3, 7, 13$ | $\Sigma x + \Sigma x^2 + \Sigma x^3$ |
| 46 | $3, 5, 17, 23$ | $\Sigma x^2 + \Sigma x^4$ |
| 48 | $5, 7, 11, 17, 19$ | $\Sigma x + \Sigma x^3 + \Sigma x^4$ |
| 50 | $3, 7, 13, 19$ | $\Sigma x^2 + \Sigma x^4$ |
| 52 | $5, 11, 23$ | $\Sigma x^2$ |
| 54 | $7, 11, 13, 17, 23$ | $\Sigma x^3$ |
| 56 | $3, 13, 19$ | $\Sigma x + \Sigma x^2 + \Sigma x^3 + \Sigma x^4$ |
| 58 | $5, 11, 17, 29$ | $\Sigma x^2$ |
| 60 | $7, 13, 17, 19, 23, 29$ | $\Sigma x + \Sigma x^2 + \Sigma x^3 + \Sigma x^4$ |
| 62 | $3, 19, 31$ | $\Sigma x^2 + \Sigma x^3$ |
| 64 | $3, 5, 11, 17, 23$ | $\Sigma x^3$ |
| 66 | $5, 7, 13, 19, 23, 29$ | $\Sigma x + \Sigma x^4$ |
| 68 | $7, 31$ | $\Sigma x^2 + \Sigma x^3$ |
| 70 | $3, 11, 17, 23, 29$ | $\Sigma x^3 + \Sigma x^4$ |
| 72 | $5, 11, 13, 19, 29, 31$ | $\Sigma x + \Sigma x^3$ |
| 74 | $3, 7, 13, 31, 37$ | $\Sigma x^4$ |
| 76 | $3, 5, 17, 23, 29$ | $\Sigma x$ |
| 78 | $5, 7, 11, 17, 19, 31, 37$ | $\Sigma x^2 + \Sigma x^3$ |
| 80 | $7, 13, 19, 37$ | $\Sigma x + \Sigma x^4$ |
| 82 | $3, 11, 23, 29, 41$ | $\Sigma x^3 + \Sigma x^4$ |

| *Nombre pair* 2a | *Nombres premiers décomposants* | *polynôme divisible(ou"presque") par* 2a |
|---|---|---|
| 84 | $5, 11, 13, 17, 23, 31, 37, 41$ | $\Sigma x^3$ |
| 86 | $3, 7, 13, 19, 43$ | $\Sigma x$ |
| 88 | $5, 17, 29, 41$ | $\Sigma x^3 + \Sigma x^4$ |
| 90 | $7, 11, 17, 19, 23, 29, 31, 37, 43$ | $\Sigma x + \Sigma x^2 + \Sigma x^3$ |
| 92 | $3, 13, 19, 31$ | $\Sigma x + \Sigma x^2$ |
| 94 | $5, 11, 23, 41, 47$ | $\Sigma x + \Sigma x^3$ |
| 96 | $7, 13, 17, 23, 29, 37, 43$ | $\Sigma x + \Sigma x^3$ |
| 98 | $19, 31, 37$ | $\Sigma x^2 + \Sigma x^4$ |
| 100 | $3, 11, 17, 29, 41, 47$ | $\Sigma x + \Sigma x^2 + \Sigma x^3$ |
| 128 | $19, 31, 61$ | $\Sigma x^2 + \Sigma x^3$ |

# 6 Conclusion

Tous ces résultats sont étranges, même si 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. A feuilleter ces cours et ces ouvrages, 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."*.

## Annexe 1 : 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 2 : 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'inégalité $N \leq q+1+2g\sqrt{q}$ (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 d'une revue de vulgarisation mathématique

  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 $x^{13} - 1 = 0$ 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 $p^\nu$ 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 $p^\nu$, 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 $p^\nu$ 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] E. Galois. *Oeuvres mathématiques*. Éd. Gallica.

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

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

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

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

[10] 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.

[11] J. Sivardière. *Description de la symétrie : des groupes de symétrie aux structures fractales*. Éd. Grenoble Sciences, 2004.

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

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

[14] G. Verriest. *Leçons sur la théorie des équations selon Galois*. Éd. Jacques Gabay.

[15] H. Weil. *Symétrie et mathématiques modernes*. Éd. Champs Flammarion

# Résultats trouvés sur les différents groupes avec l'outil GAP

D. Vella

Octobre 2006

## 1 Les groupes cycliques

- 8
  groupe C2
  nombre de décompositions Goldbach : 1
  Sur les éléments : 1, 3.
  générateur du groupe : 3.
  Décomposant Goldbach de 8 : 3.

- 12
  groupe C2
  nombre de décompositions Goldbach : 1
  sur les éléments : 1, 5.
  générateur du groupe : 5.
  Décomposant Goldbach de 12 : 5.

- 16
  groupe C4
  nombre de décompositions Goldbach : 2
  sur les éléments : 1, 3, 5, 7.
  générateurs du groupe : 3, 5.
  Décomposants Goldbach de 16 : 3, 5.

- 18
  groupe C3
  nombre de décompositions Goldbach : 2
  sur les éléments : 1, 5, 7.
  générateurs du groupe : 5, 7.
  Décomposants Goldbach de 18 : 5, 7.

- 20
  groupe C4
  nombre de décompositions Goldbach : 2
  sur les éléments : 1, 3, 7, 9.
  générateurs du groupe : 3, 7.
  Décomposants Goldbach de 20 : 3, 7.

- 28
  Groupe C6
  nombre de décompositions Goldbach : 2
  sur les éléments : 1, 3, 5, 9, 11, 13.
  générateurs du groupe : 5, 11.
  Décomposants Goldbach de 28 : 5, 11.

- 30
  Groupe C4
  nombre de décompositions Goldbach : 3
  sur les éléments : 1, 7, 11, 13.
  générateurs du groupe : 7, 13.
  Décomposants Goldbach de 30 : 7, 11, 13.

- 32
  Groupe C8
  nombre de décompositions Goldbach : 2
  sur les éléments : 1, 3, 5, 7, 9, 11, 13, 15.
  générateurs du groupe : 3, 5, 11, 13.
  Décomposants Goldbach de 32 : 3, 13.

  Complémentaire : C4xC2

- 36
  Groupe C6
  nombre de décompositions Goldbach : 4
  sur les éléments : 1, 5, 7, 11, 13, 17.
  générateurs du groupe : 5, 7.
  Décomposants Goldbach de 36 : 5, 7, 13, 17.

- 42
  Groupe C6
  nombre de décompositions Goldbach : 4
  sur les éléments : 1, 5, 11, 13, 17, 19.
  générateurs du groupe : 11, 19.
  Décomposants Goldbach de 42 : 5, 11, 13, 19.

- 44
  Groupe C10
  nombre de décompositions Goldbach : 3
  sur les éléments : 1, 3, 5, 7, 9, 13, 15, 17, 19, 21.
  générateurs du groupe : 3, 13, 15, 17.
  Décomposants Goldbach de 44 : 3, 7, 13.

- 50
  Groupe C10
  nombre de décompositions Goldbach : 4
  sur les éléments : 1, 3, 7, 9, 11, 13, 17, 19, 21, 23.
  générateurs du groupe : 3, 13, 17, 23.
  Décomposants Goldbach de 50 : 3, 7, 13, 19.

- 52
  Groupe C12
  nombre de décompositions Goldbach : 3
  sur les éléments : 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.
  générateurs du groupe : 7, 11, 15, 19.
  Décomposants Goldbach de 52 : 5, 11, 23.

- 54
  Groupe C9
  nombre de décompositions Goldbach : 5
  sur les éléments : 1, 5, 7, 11, 13, 17, 19, 23, 25.
  générateurs du groupe : 5, 7, 11, 13, 23, 25.
  Décomposants Goldbach de 54 : 7, 11, 13, 17, 23.

  Complémentaire : C9

- 64
  Groupe C16
  nombre de décompositions Goldbach : 5
  sur les éléments : 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31.
  générateurs du groupe : 3, 5, 11, 13, 19, 21, 27, 29.
  Décomposants Goldbach de 64 : 3, 5, 11, 17, 23.

- 66
  Groupe C10
  nombre de décompositions Goldbach : 6
  sur les éléments : 1, 5, 7, 13, 17, 19, 23, 25, 29, 31.
  générateurs du groupe : 5, 7, 13, 19.
  Décomposants Goldbach de 66 : 5, 7, 13, 19, 23, 29.

- 68
  Groupe C16
  nombre de décompositions Goldbach : 2
  sur les éléments : 1, 3, 5, 7, 9, 11, 13, 15, 19, 21, 23, 25, 27, 29, 31, 33.
  générateurs du groupe : 3, 5, 7, 11, 23, 27, 29, 31.
  Décomposants Goldbach de 68 : 7, 31.

- 70
  Groupe C12
  nombre de décompositions Goldbach : 5
  sur les éléments : 1, 3, 9, 11, 13, 17, 19, 23, 27, 29, 31, 33.
  générateurs du groupe : 3, 17, 23, 33.
  Décomposants Goldbach de 68 : 3, 11, 17, 23, 29.

- 76
  Groupe C18
  nombre de décompositions Goldbach : 5
  sur les éléments : 1, 3, 5, 7, 9, 11, 13, 15, 17, 21, 23, 25, 27, 29, 31, 33, 35, 37.
  générateurs du groupe : 13, 23, 25, 29, 33, 35.
  Décomposants Goldbach de 68 : 3, 5, 17, 23, 29.

- 78
  Groupe C12
  nombre de décompositions Goldbach : 7
  sur les éléments : 1, 5, 7, 11, 17, 19, 23, 25, 29, 31, 35, 37.
  générateurs du groupe : 7, 11, 19, 37.
  Décomposants Goldbach de 68 : 5, 7, 11, 17, 19, 31, 37.

- 90
  Groupe C12
  nombre de décompositions Goldbach : 9
  sur les éléments : 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43.
  générateurs du groupe : 7, 13, 23, 43.
  Décomposants Goldbach de 68 : 7, 11, 17, 19, 23, 29, 31, 37, 43.

- 92
  Groupe C22
  nombre de décompositions Goldbach : 4
  sur les éléments : 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45.
  générateurs du groupe : 3, 5, 17, 21, 27, 31, 33, 35, 37, 39.
  Décomposants Goldbach de 68 : 3, 13, 19, 31.

- 98
  Groupe C21
  nombre de décompositions Goldbach : 3
  sur les éléments : 1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27, 29, 31, 33, 37, 39, 41, 43, 45, 47.
  générateurs du groupe : 3, 5, 9, 11, 17, 23, 25, 33, 37, 39, 45, 47.
  Décomposants Goldbach de 68 : 19, 31, 37

## 2 Groupes non cycliques

- 24
  gr24 := Group([(),
  (1,2)(3,4),
  (1,3)(2,4),
  (1,4)(2,3)]);

  Groupe C2xC2
  nombre de décompositions Goldbach : 3
  sur les éléments : 1, 5, 7, 11.
  générateurs du groupe : ???
  Décomposants Goldbach de 24 : 5, 7, 11.

- 40
  gr40 := Group([(),
  (1,2,4,6)(3,5,7,8),
  (1,3,4,7)(2,8,6,5),
  (1,4)(2,6)(3,7)(5,8),
  (1,5)(2,3)(4,8)(6,7),
  (1,6,4,2)(3,5,7,8) *****,
  (1,7,4,3)(2,5,6,8) *****,
  (1,8)(2,7)(3,6)(4,5)]);

  Groupe C4xC2
  nombre de décompositions Goldbach : 3
  sur les éléments : 1, 3, 7, 9, 11, 13, 17, 19.
  générateurs du groupe : ???
  Décomposants Goldbach de 40 : 3, 11, 17.

- 48
  gr48 := Group([(),
  (1,2,8,7)(3,5,6,4),
  (1,3)(2,5)(4,7)(6,8),
  (1,4,8,5)(2,3,7,6),
  (1,5,8,4)(2,6,7,3) *****,
  (1,6)(2,4)(3,8)(5,7),
  (1,7,8,2)(3,4,6,5) *****,
  (1,8)(2,7)(3,6)(4,5)]);

  Groupe C4xC2
  nombre de décompositions Goldbach : 5
  sur les éléments : 1, 5, 7, 11, 13, 17, 19, 23.
  générateurs du groupe :
  Décomposants Goldbach de 48 : 5, 7, 11, 17, 19

- 56
  gr56 := Group([(),
  (1,2,4,12,11,9)(3,7,5,10,6,8),
  (1,3,11,6,4,5)(2,7,9,8,12,10),
  (1,4,11)(2,12,9)(3,5,6)(7,10,8),
  (1,5,4,6,11,3)(2,10,12,8,9,7) *****,
  (1,6)(2,8)(3,4)(5,11)(7,12)(9,10),
  (1,7)(2,5)(3,9)(4,10)(6,12)(8,11),
  (1,8,4,7,11,10)(2,3,12,5,9,6),
  (1,9,11,12,4,2)(3,8,6,10,5,7),
  (1,10,11,7,4,8)(2,6,9,5,12,3) *****,
  (1,11,4)(2,9,12)(3,6,5)(7,8,10) *****,
  (1,12)(2,11)(3,10)(4,9)(5,8)(6,7)]);

  Groupe C6xC2
  nombre de décompositions Goldbach : 3
  sur les éléments : 1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27.
  générateurs du groupe :
  Décomposants Goldbach de 56 : 3, 13, 19

- 60
  gr60 := Group([(),
  (1,2,3,5)(4,8,7,6),
  (1,3)(2,5)(4,7)(6,8),
  (1,4,3,7)(2,8,5,6),
  (1,5,3,2)(4,6,7,8) *****,
  (1,6)(2,4)(3,8)(5,7),
  (1,7,3,4)(2,6,5,8) *****,
  (1,8)(2,7)(3,6)(4,5)]);

  Groupe C4xC2
  nombre de décompositions Goldbach : 6
  sur les éléments : 1, 7, 11, 13, 17, 19, 23, 29.
  générateurs du groupe :
  Décomposants Goldbach de 60 : 7, 13, 17, 19, 23, 29

- 72
  gr72 := Group([(),
  (1,2,9,7,8,10)(3,12,11,4,6,5),
  (1,3,8,6,9,11)(2,12,10,5,7,4),
  (1,4,8,12,9,5)(2,6,10,11,7,3),
  (1,5,9,12,8,4)(2,3,7,11,10,6) *****,
  (1,6)(2,5)(3,9)(4,10)(7,12)(8,11),
  (1,7)(2,8)(3,4)(5,11)(6,12)(9,10),
  (1,8,9)(2,10,7)(3,6,11)(4,5,12),
  (1,8,9)(2,7,10)(3,11,6)(4,5,12) *****,
  (1,10,8,7,9,2)(3,5,6,4,11,12) *****,
  (1,11,9,6,8,3)(2,4,7,5,10,12) *****,
  (1,12)(2,11)(3,10)(4,9)(5,8)(6,7)]);

Groupe C6xC2
nombre de décompositions Goldbach : 6
sur les éléments : 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35.
générateurs du groupe :
Décomposants Goldbach de 72 : 5, 11, 13, 19, 29, 31.

- 80
gr80 := Group([(),
(1,2,4,11)(3,9,7,12)(5,14,8,10)(6,16,15,13),
(1,3,13,10)(2,9,6,5)(4,7,16,14)(8,11,12,15),
(1,4)(2,11)(3,7)(5,8)(6,15)(9,12)(10,14)(13,16),
(1,5,16,12)(2,14,15,3)(4,8,13,9)(6,7,11,10),
(1,6,4,15)(2,16,11,13)(3,5,7,8)(9,14,12,10),
(1,7,13,14)(2,12,6,8)(3,16,10,4)(5,11,9,15),
(1,8,16,10)(2,10,15,7)(3,11,14,6)(4,5,13,12),
(1,9,16,8)(2,7,15,10)(3,6,14,11)(4,12,13,5),
(1,10,13,3)(2,5,6,9)(4,14,16,7)(8,15,12,11) *****,
(1,11,4,2)(3,12,7,9)(5,8,10,14)(6,13,15,16) *****,
(1,12,16,5)(2,3,15,14)(4,9,13,8)(6,10,11,7) *****,
(1,13)(2,6)(3,10)(4,16)(5,9)(7,14)(8,12)(11,15),
(1,14,13,7)(2,8,6,12)(3,4,10,16)(5,15,9,11) *****,
(1,15,4,6)(2,13,11,16)(3,8,7,5)(9,10,12,14) *****,
(1,16)(2,15)(3,14)(4,13)(5,12)(6,11)(7,10)(8,9)]);

Groupe C4xC4
nombre de décompositions Goldbach : 4
sur les éléments : 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39.
générateurs du groupe :
Décomposants Goldbach de 80 : 7, 13, 19, 37.

- 84
gr84 := Group([(), (1,2,8,12,11,5)(3,9,7,10,4,6),
(1,3,11,4,8,7)(2,9,5,6,12,10),
(1,4)(2,6)(3,8)(5,10)(7,11)(9,12),
(1,5,11,12,8,2)(3,6,4,10,7,9) *****,
(1,6,8,9,11,10)(2,3,12,7,5,4),
(1,7,8,4,11,3)(2,10,12,6,5,9) *****,
(1,8,11)(2,12,5)(3,7,4)(6,9,10),
(1,9)(2,7)(3,5)(4,12)(6,11)(8,10),
(1,10,11,9,8,6)(2,4,5,7,12,3) *****,
(1,11,8)(2,5,12)(3,4,7)(6,10,9) *****,
(1,12)(2,11)(3,10)(4,9)(5,8)(6,7)]);

Groupe C6xC2
nombre de décompositions Goldbach : 8
sur les éléments : 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41.
générateurs du groupe :
Décomposants Goldbach de 84 : 5, 11, 13, 17, 23, 31, 37, 41.

- 88
  gr88 := Group([(),
  (1,2,5,13,4,10,12,6,18,14)(3,7,20,19,16,8,17,11,9,15),
  (1,3,12,17,5,20,18,9,4,16)(2,7,6,11,13,19,14,15,10,8),
  (1,4,18,5,12)(2,10,14,13,6)(3,16,9,20,17)(7,8,15,19,11),
  (1,5,4,12,18)(2,13,10,6,14)(3,20,16,17,9)(7,19,8,11,15) *****,
  (1,6,4,2,18,10,5,14,12,13)(3,11,16,7,9,8,20,15,17,19) *****,
  (1,7,18,15,12,11,4,8,5,19)(2,20,14,3,6,9,10,17,13,16),
  (1,8,12,7,5,11,18,19,4,15)(2,17,6,20,13,9,14,16,10,3) *****,
  (1,9,5,3,4,20,12,16,18,17)(2,15,13,7,10,19,6,8,14,11) *****,
  (1,10)(2,12)(3,8)(4,14)(5,6)(7,17)(9,19)(11,20)(13,18)(15,16),
  (1,11)(2,9)(3,13)(4,7)(5,15)(6,16)(8,18)(10,20)(12,19)(14,17),
  (1,12,5,18,4)(2,6,13,14,10)(3,17,20,9,16)(7,11,19,15,8),
  (1,13,12,14,5,10,18,2,4,6)(3,19,17,15,20,8,9,7,16,11) *****,
  (1,14,18,6,12,10,4,13,5,2)(3,15,9,11,17,8,16,19,20,7,3) *****,
  (1,15,4,19,18,11,5,7,12,8)(2,3,10,16,14,9,13,20,6,17) *****,
  (1,16,4,9,18,20,5,17,12,3)(2,8,10,15,14,19,13,11,6,7) *****,
  (1,17,18,16,12,20,4,3,5,9)(2,11,14,8,6,19,10,7,13,15) *****,
  (1,18,12,4,5)(2,14,6,10,13)(3,9,17,16,20)(7,15,11,8,19),
  (1,19,5,8,4,11,12,15,18,7)(2,16,13,17,10,9,6,3,14,20),
  (1,20)(2,19)(3,18)(4,17)(5,16)(6,15)(7,14)(8,13)(9,12)(10,11)]);

  Groupe C10xC2
  nombre de décompositions Goldbach : 4
  sur les éléments : 1, 3, 5, 7, 9, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 35, 37, 39, 41, 43
  générateurs du groupe :
  Décomposants Goldbach de 88 : 5, 17, 29, 41.

- 96
  gr96 := Group([(),
  (1,2,9,10,16,15,8,7)(3,12,6,4,14,5,11,13),
  (1,3,16,14)(2,12,15,5)(4,7,13,10)(6,8,11,9),
  (1,4,9,5,16,13,8,12)(2,14,10,11,15,3,7,6),
  (1,5,8,4,16,12,9,13)(2,11,7,14,15,6,10,3) *****,
  (1,6)(2,4)(3,8)(5,10)(7,12)(9,14)(11,16)(13,15),
  (1,7,8,15,16,10,9,2)(3,13,11,5,14,4,6,12) *****,
  (1,8,16,9)(2,7,15,10)(3,11,14,6)(4,12,13,5),
  (1,9,16,8)(2,10,15,7)(3,6,14,11)(4,5,13,12) *****,
  (1,10,8,2,16,7,9,15)(3,4,11,12,14,13,6,5) *****,
  (1,11)(2,13)(3,9)(4,15)(5,7)(6,16)(8,14)(10,12),
  (1,12,8,13,16,5,9,4)(2,6,7,3,15,11,10,14) *****,
  (1,13,9,12,16,4,8,5)(2,3,10,6,15,14,7,11) *****,
  (1,14,16,3)(2,5,15,12)(4,10,13,7)(6,9,11,8) *****,
  (1,15,9,7,16,2,8,10)(3,5,6,13,14,12,11,4) *****,
  (1,16)(2,15)(3,14)(4,13)(5,12)(6,11)(7,10)(8,9)]);

  Groupe C8xC2
  nombre de décompositions Goldbach : 7
  sur les éléments : 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47.

générateurs du groupe :
Décomposants Goldbach de 96 : 7, 13, 17, 23, 29, 37, 43.

# 3 Conclusion

Sur les 47 nombres pairs de 6 à 100, il y a 14 doubles de nombres premiers, 23 nombres auxquels ont été associés des groupes cycliques et 10 auxquels ont été associés des groupes non cycliques. Les nombres auxquels sont associés des groupes cycliques sont systématiquement de trois formes : soit ce sont des puissances de 2, soit ce sont des nombres de la forme $4n + 2$, soit ce sont des nombres de la forme $4p$ avec p premier. Enfin, on remarque que pour les nombres auxquels on associe des groupes cycliques, l'intersection entre l'ensemble des générateurs du groupe et l'ensemble des nombres premiers permettant de fournir des décompositions Goldbach du nombre pair considéré est systématiquement non vide.

# Conjecture de Goldbach et Théorie des groupes

Denise Vella

Octobre 2006

## 1 Introduction

Dans une note précédente, ont été présentés quelques cas de nombres pairs dont les décompositions Goldbach étaient en relation entre elles de la même façon que le sont entre eux les éléments d'un groupe.

Ces cas présentaient un certain caractère "esthétique" car les éléments des groupes peuvent être perçus géométriquement comme les sommets de polyèdres et leurs relations appréhendées comme des transformations telles que différentes symétries et/ou rotations.

Par l'étude de certaines tables d'opérations (tables de Cayley), on essaiera de voir ici si les nombres premiers qui participent aux décompositions Goldbach d'un nombre pair $2a$ sont des éléments particuliers de certains groupes[1].

## 2 Digression par le cas 84 et introduction d'une nouvelle opération

Dans la note précédente, à la recherche de "beaux" polyèdres, on s'était rendu compte que de tels polyèdres existaient pour les plus petits nombres ayant un nombre de décompositions Goldbach donné (en l'occurrence $24, 36, 42, 48, 60, 66, 78, 96$, écrits en bleu dans l'annexe 1). Mais le nombre 84, plus petit nombre à 8 décompositions montrait une certaine "résistance" (!) au fait de fournir des polyèdres.

Pour trouver les polyèdres, on prend les nombres premiers inférieurs à $a$ fournissant une décomposition Goldbach de $2a$ et on trouve les résultats de tous produits de deux d'entre eux modulo $2a$. Pour 84, l'ensemble $E$ des nombres premiers fournissant une décomposition Goldbach de 84 est

$$\{5, 11, 13, 17, 23, 31, 37, 41\}.$$

[1]Nous n'étudierons que des nombres pairs qui ne sont pas doubles d'un nombre premier, car pour ces nombres-là, la conjecture de Goldbach est trivialement vérifiée.

Les produits modulo 84 de deux éléments de $E$ sont les suivants :

| | | | | | | |
|---|---|---|---|---|---|---|
| $5 \times 11 = 55\ (29)$ | | | | | | |
| $5 \times 13 = 65\ (19)$ | $11 \times 13 = 59$ | | | | | |
| $5 \times 17 = 1$ | $11 \times 17 = 19$ | $13 \times 17 = 53\ (31)$ | | | | |
| $5 \times 23 = 31$ | $11 \times 23 = 1$ | $13 \times 23 = 47\ (37)$ | $17 \times 23 = 55\ (29)$ | | | |
| $5 \times 31 = 71\ (13)$ | $11 \times 31 = 5$ | $13 \times 31 = 67\ (17)$ | $17 \times 31 = 23$ | $23 \times 31 = 41$ | | |
| $5 \times 37 = 17$ | $11 \times 37 = 71\ (13)$ | $13 \times 37 = 61\ (23)$ | $17 \times 37 = 41$ | $23 \times 37 = 11$ | $31 \times 37 = 55\ (29)$ | |
| $5 \times 41 = 37$ | $11 \times 41 = 31$ | $13 \times 41 = 29$ | $17 \times 41 = 25\ (59)$ | $23 \times 41 = 19$ | $31 \times 41 = 11$ | $37 \times 41 = 5$ |

Parfois, le produit modulo $2a$ est un élément de $E$, parfois non. Ce qu'il semble intéressant de constater, c'est que lorsque le produit n'est pas l'un des nombres premiers initiaux, trois cas se présentent :

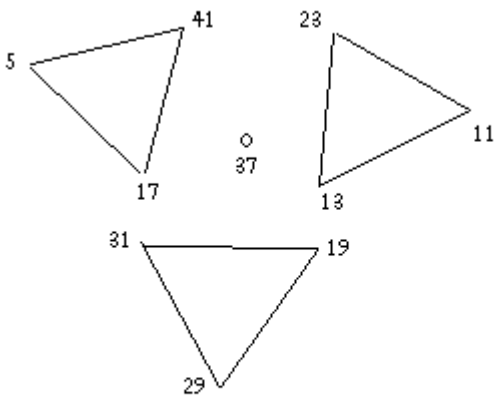
- soit le produit fournit directement un nombre premier compris entre $a$ et $2a$ (et donc n'appartenant pas à $E$) ;
- soit le produit fournit un nombre composé compris entre $a$ et $2a$ dont le complémentaire à $2a$ est un nombre premier inférieur à $a$ même si ce nombre premier n'appartient pas à $E$ ;
- soit le produit fournit un nombre composé inférieur à $a$ dont le complémentaire à $2a$ est un nombre premier compris entre $a$ et $2a$.

Bref, il semblerait que dans tous les cas de figures on "atterrisse" sur des nombres premiers, à droite ou à gauche de $a$.

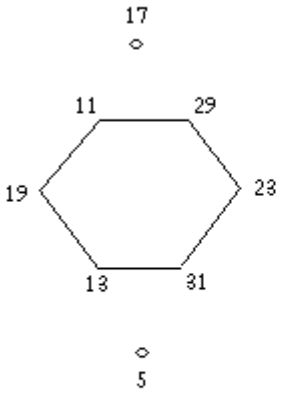
La multiplication entre eux des nombres premiers appartenant à $E$ (nombres premiers fournissant des décompositions) faisant "sortir" de $E$, on va utiliser une autre opération que la multiplication. C'est ce que l'on a indiqué au niveau des produits en mettant entre parenthèses le complémentaire à 84, qui est l'image d'un couple par cette nouvelle opération.

Cette nouvelle opération $m(x, y)$ est définie de la façon suivante :
Si $x.y > 2a$, posons $res = x.y$ $(modulo\ 2a)$.
Si $a < res < 2a$, $m(x, y) = 2a - res$, sinon $m(x, y) = res$.

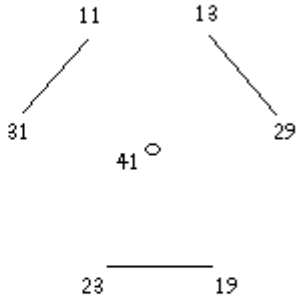
On trouve finalement, pour le nombre pair 84, par ce biais du changement d'opération, 3 tétraèdres sur 37 $(37, 5, 17, 41)$, $(37, 19, 29, 31)$ et $(37, 11, 13, 23)$, une bipyramide à base hexagonale, et une structure similaire à celle présentée pour le cas 96 dans la note précédente, de centre 41 et de doublons $(11, 31), (13, 29)$ et $(23, 19)$ (on l'appellera "septon"). $\varphi(84) = 24$.




3 tétraèdres d'axe passant par 37




Une bipyramide à base hexagonale




Un "septon" de centre 41

On présente ces structures sur le dessin ci-dessus.
On peut également présenter les résultats dans la table de $m$ suivante.

| | 1 | 5 | 11 | 13 | 17 | 19 | 23 | 25 | 29 | 31 | 37 | 41 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 5 | 11 | 13 | 17 | 19 | 23 | 25 | 29 | 31 | 37 | 41 |
| 5 | 5 | 25 | 29 | 19 | 1 | 11 | 31 | 41 | 23 | 13 | 17 | 37 |
| 11 | 11 | 29 | 37 | 25 | 19 | 41 | 1 | 23 | 17 | 5 | 13 | 31 |
| 13 | 13 | 19 | 25 | 1 | 31 | 5 | 37 | 11 | 41 | 17 | 23 | 29 |
| 17 | 17 | 1 | 19 | 31 | 37 | 13 | 29 | 5 | 11 | 23 | 41 | 25 |
| 19 | 19 | 11 | 41 | 5 | 13 | 25 | 17 | 29 | 37 | 1 | 31 | 23 |
| 23 | 23 | 31 | 1 | 37 | 29 | 17 | 25 | 13 | 5 | 41 | 11 | 19 |
| 25 | 25 | 41 | 23 | 11 | 5 | 29 | 13 | 37 | 31 | 19 | 1 | 17 |
| 29 | 29 | 23 | 17 | 41 | 11 | 37 | 5 | 31 | 1 | 25 | 19 | 13 |
| 31 | 31 | 13 | 5 | 17 | 23 | 1 | 41 | 19 | 25 | 37 | 29 | 11 |
| 37 | 37 | 17 | 13 | 23 | 41 | 31 | 11 | 1 | 19 | 29 | 25 | 5 |
| 41 | 41 | 37 | 31 | 29 | 25 | 23 | 19 | 17 | 13 | 11 | 5 | 1 |

Cette table admet entre autres les 3 sous-tables de groupes suivantes correspondant aux trois tétraèdres.
Tétraèdre (37, 11, 13, 23)

| | 11 | 13 | 23 | 25 | 1 | 37 |
|---|---|---|---|---|---|---|
| 11 | 37 | 25 | 1 | 23 | 11 | 13 |
| 13 | 25 | 1 | 37 | 11 | 13 | 23 |
| 23 | 1 | 37 | 25 | 13 | 23 | 11 |
| 25 | 23 | 11 | 13 | 37 | 25 | 1 |
| 1 | 11 | 13 | 23 | 25 | 1 | 37 |
| 37 | 13 | 23 | 11 | 1 | 37 | 25 |

Tétraèdre (37, 5, 17, 41)

| | 41 | 17 | 5 | 1 | 25 | 37 |
|---|---|---|---|---|---|---|
| 41 | 1 | 25 | 37 | 41 | 17 | 5 |
| 17 | 25 | 37 | 1 | 17 | 5 | 41 |
| 5 | 37 | 1 | 25 | 5 | 41 | 17 |
| 1 | 41 | 17 | 5 | 1 | 25 | 37 |
| 25 | 17 | 5 | 41 | 25 | 37 | 1 |
| 37 | 5 | 41 | 17 | 37 | 1 | 25 |

Tétraèdre (37, 31, 29, 19)

| | 19 | 29 | 31 | 37 | 1 | 25 |
|---|---|---|---|---|---|---|
| 19 | 25 | 37 | 1 | 31 | 19 | 29 |
| 29 | 37 | 1 | 25 | 19 | 29 | 31 |
| 31 | 1 | 25 | 37 | 29 | 31 | 19 |
| 37 | 31 | 19 | 29 | 25 | 37 | 1 |
| 1 | 19 | 29 | 31 | 37 | 1 | 25 |
| 25 | 29 | 31 | 19 | 1 | 25 | 37 |

# 3 L'ensemble des unités muni de la multiplication est un groupe

Pour un entier naturel $m$ donné, l'ensemble des entiers inversibles modulo $m$ forment, dans l'anneau $\mathbb{Z}/m\mathbb{Z}$, un groupe commutatif pour la multiplication. Cet ensemble contient $\varphi(m)$ éléments, où $\varphi$ est l'indicateur d'Euler.

Quand on travaille sur la conjecture de Goldbach, et qu'on cherche les décompositions d'un nombre pair $2a$, on prend l'habitude[2] de n'étudier que le quart haut-gauche de la table de multiplication, en ne s'intéressant qu'aux éléments inversibles inférieurs ou égaux à $a$. En fait, $\varphi(2a)$ est égal à $\varphi(a)$ si $a$ est impair tandis que $\varphi(2a)$ est égal au double de $\varphi(a)$ si $a$ est pair.

Les tables correspondant aux groupes des ensembles des unités munis de la multiplication sont fournies en annexe.

# 4 Etude de tables opératoires

Pour $\mathbb{Z}/8\mathbb{Z}$, $\varphi(8) = 4$ ; à l'opération $m$ qui a été définie correspond la table suivante.

| | 1 | 3 |
|---|---|---|
| 1 | 1 | 3 |
| 3 | 3 | 1 |

On reconnaît la table du groupe appelé habituellement $Z2$. 3 est premier et fournit une décomposition Goldbach de 8.

[2] Je ne sais pas si cela est légitime.

Pour $\mathbb{Z}/12\mathbb{Z}$, $\varphi(12) = 4$ ; la table de $m$ est :

| | 1 | 5 |
|---|---|---|
| 1 | 1 | 5 |
| 5 | 5 | 1 |

On obtient à nouveau table du groupe $Z2$ et le même nombre de décompositions (une seule). 5 est premier et fournit une décomposition Goldbach de 12.

Pour $\mathbb{Z}/16\mathbb{Z}$, $\varphi(16) = 8$ ; la table de $m$ est :

| | 1 | 3 | 5 | 7 |
|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 |
| 3 | 3 | 7 | 1 | 5 |
| 5 | 5 | 1 | 7 | 3 |
| 7 | 7 | 5 | 3 | 1 |

On obtient la table du groupe $D4$ et il y a deux décompositions différentes, l'une sur 3 et l'autre sur 5.

Pour $\mathbb{Z}/18\mathbb{Z}$, $\varphi(18) = 6$ ; la table de $m$ est :

| | 1 | 5 | 7 |
|---|---|---|---|
| 1 | 1 | 5 | 7 |
| 5 | 5 | 7 | 1 |
| 7 | 7 | 1 | 5 |

On obtient la table du groupe $Z3$ et il y a deux décompositions différentes, l'une sur 5 et l'autre sur 7.

Pour $\mathbb{Z}/20\mathbb{Z}$, $\varphi(20) = 8$ ; la table de $m$ est :

| | 1 | 3 | 7 | 9 |
|---|---|---|---|---|
| 1 | 1 | 3 | 7 | 9 |
| 3 | 3 | 9 | 1 | 7 |
| 7 | 7 | 1 | 9 | 3 |
| 9 | 9 | 7 | 3 | 1 |

On obtient à nouveau la table du groupe $D4$ et il y a deux décompositions différentes, l'une sur 3 et l'autre sur 7.

Pour $\mathbb{Z}/24\mathbb{Z}$, $\varphi(24) = 8$ ; la table de $m$ est :

| | 1 | 5 | 7 | 11 |
|---|---|---|---|---|
| 1 | 1 | 5 | 7 | 11 |
| 5 | 5 | 1 | 11 | 7 |
| 7 | 7 | 11 | 1 | 5 |
| 11 | 11 | 7 | 5 | 1 |

On obtient la table du groupe $Z2 \times Z2$ et il y a trois décompositions différentes, sur 5, 7 et 11.

Pour $\mathbb{Z}/28\mathbb{Z}$, $\varphi(28) = 12$ ; la table de $m$ est :

| | 1 | 3 | 5 | 9 | 11 | 13 |
|---|---|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 9 | 11 | 13 |
| 3 | 3 | 9 | 13 | 1 | 5 | 11 |
| 5 | 5 | 13 | 3 | 11 | 1 | 9 |
| 9 | 9 | 1 | 11 | 3 | 13 | 5 |
| 11 | 11 | 5 | 1 | 13 | 9 | 3 |
| 13 | 13 | 11 | 9 | 5 | 3 | 1 |

On obtient la table du groupe $Z3 \times Z3$ et il y a deux décompositions différentes, l'une sur 5 et l'autre sur 11.

Pour $\mathbb{Z}/30\mathbb{Z}$, $\varphi(30) = 8$ ; la table de $m$ est :

| | 1 | 7 | 11 | 13 |
|---|---|---|---|---|
| 1 | 1 | 7 | 11 | 13 |
| 7 | 7 | 11 | 13 | 1 |
| 11 | 11 | 13 | 1 | 7 |
| 13 | 13 | 1 | 7 | 11 |

On obtient la table du groupe $Z4$ et il y a trois décompositions différentes, sur 7, 11 et 13.

Pour $\mathbb{Z}/32\mathbb{Z}$, $\varphi(32) = 16$ ; la table de $m$ est :

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

32 admet seulement deux décompositions Goldbach différentes, sur 3 et 13. Je crois que la table ci-dessus est celle du groupe $Z2 \times Z2 \times Z2 \times Z2$ : on peut en effet intervertir les colonnes et obtenir la table suivante qui est "coupable" en petits carrés de 2 sur 2.

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

Pour $\mathbb{Z}/36\mathbb{Z}$, $\varphi(36) = 12$ ; la table de $m$ est :

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

Il y a 4 décompositions différentes, sur 5, 7, 13 et 17.

Pour $\mathbb{Z}/40\mathbb{Z}$, $\varphi(40) = 16$ ; la table de $m$ est :

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

Il y a 3 décompositions différentes, sur 3, 11 et 17.

Pour $\mathbb{Z}/42\mathbb{Z}$, $\varphi(42) = 12$ ; la table de $m$ est :

| | 1 | 5 | 11 | 13 | 17 | 19 |
|---|---|---|---|---|---|---|
| 1 | 1 | 5 | 11 | 13 | 17 | 19 |
| 5 | 5 | 17 | 13 | 19 | 1 | 11 |
| 11 | 11 | 13 | 5 | 17 | 19 | 1 |
| 13 | 13 | 19 | 17 | 1 | 11 | 5 |
| 17 | 17 | 1 | 19 | 11 | 5 | 13 |
| 19 | 19 | 11 | 1 | 5 | 13 | 17 |

Il y a 4 décompositions différentes, sur 5, 11, 13 et 19.

Pour $\mathbb{Z}/44\mathbb{Z}$, $\varphi(44) = 20$ ; la table de $m$ est :

| | 1 | 3 | 5 | 7 | 9 | 13 | 15 | 17 | 19 | 21 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 | 9 | 13 | 15 | 17 | 19 | 21 |
| 3 | 3 | 9 | 15 | 21 | 17 | 5 | 1 | 7 | 13 | 19 |
| 5 | 5 | 15 | 19 | 9 | 1 | 21 | 13 | 3 | 7 | 17 |
| 7 | 7 | 21 | 9 | 5 | 19 | 3 | 17 | 13 | 1 | 15 |
| 9 | 9 | 17 | 1 | 19 | 7 | 15 | 3 | 21 | 5 | 13 |
| 13 | 13 | 5 | 2 | 3 | 15 | 7 | 19 | 1 | 17 | 9 |
| 15 | 15 | 1 | 13 | 17 | 3 | 19 | 5 | 9 | 21 | 7 |
| 17 | 17 | 7 | 3 | 13 | 21 | 1 | 9 | 19 | 15 | 5 |
| 19 | 19 | 13 | 7 | 1 | 5 | 17 | 21 | 15 | 9 | 3 |
| 21 | 21 | 19 | 17 | 15 | 13 | 9 | 7 | 5 | 3 | 1 |

Il y a 3 décompositions différentes, sur 3, 7 et 13.

Pour $\mathbb{Z}/48\mathbb{Z}$, $\varphi(48) = 16$ ; la table de $m$ est :

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

Il y a 5 décompositions différentes, sur 5, 7, 11, 17 et 19.

Pour $\mathbb{Z}/50\mathbb{Z}$, $\varphi(50) = 20$ ; la table de $m$ est :

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

Il y a 4 décompositions différentes, sur 3, 7, 13 et 19.

Pour $\mathbb{Z}/52\mathbb{Z}$, $\varphi(52) = 24$ ;

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

Il y a 3 décompositions différentes, sur 5, 11 et 23.

Pour $\mathbb{Z}/54\mathbb{Z}$, $\varphi(54) = 18$ ; la table de $m$ est :

| | 1 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 25 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 25 |
| 5 | 5 | 25 | 19 | 1 | 11 | 23 | 13 | 7 | 17 |
| 7 | 7 | 19 | 5 | 23 | 17 | 11 | 25 | 1 | 13 |
| 11 | 11 | 1 | 23 | 13 | 19 | 25 | 7 | 17 | 5 |
| 13 | 13 | 11 | 17 | 19 | 7 | 5 | 23 | 25 | 1 |
| 17 | 17 | 23 | 11 | 25 | 5 | 19 | 1 | 13 | 7 |
| 19 | 19 | 13 | 25 | 7 | 23 | 1 | 17 | 5 | 11 |
| 23 | 23 | 7 | 1 | 17 | 25 | 13 | 5 | 11 | 19 |
| 25 | 25 | 17 | 13 | 5 | 1 | 7 | 11 | 19 | 23 |

Il y a 5 décompositions différentes, sur 7, 11, 13, 17 et 23.

Pour $\mathbb{Z}/56\mathbb{Z}$, $\varphi(56) = 24$ ; la table de $m$ est :

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

Il y a 3 décompositions différentes, sur 3, 13 et 19.

Pour $\mathbb{Z}/60\mathbb{Z}$, $\varphi(60) = 16$ ; la table de $m$ est :

| | 1 | 7 | 11 | 13 | 17 | 19 | 23 | 29 |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 7 | 11 | 13 | 17 | 19 | 23 | 29 |
| 7 | 7 | 11 | 17 | 29 | 1 | 13 | 19 | 23 |
| 11 | 11 | 17 | 1 | 23 | 7 | 29 | 13 | 19 |
| 13 | 13 | 29 | 23 | 11 | 19 | 7 | 1 | 17 |
| 17 | 17 | 1 | 7 | 19 | 11 | 23 | 29 | 13 |
| 19 | 19 | 13 | 29 | 7 | 23 | 1 | 17 | 11 |
| 23 | 23 | 19 | 13 | 1 | 29 | 17 | 11 | 7 |
| 29 | 29 | 23 | 19 | 17 | 13 | 11 | 7 | 1 |

Il y a 6 décompositions différentes, sur 7, 13, 17, 19, 23 et 29.

Pour $\mathbb{Z}/64\mathbb{Z}$, $\varphi(64) = 32$ ;

| | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 | 21 | 23 | 25 | 27 | 29 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 | 21 | 23 | 25 | 27 | 29 | 31 |
| 3 | 3 | 9 | 15 | 21 | 27 | 31 | 25 | 19 | 13 | 7 | 1 | 5 | 11 | 17 | 23 | 29 |
| 5 | 5 | 15 | 25 | 29 | 19 | 9 | 1 | 11 | 21 | 31 | 23 | 13 | 3 | 7 | 17 | 27 |
| 7 | 7 | 21 | 29 | 15 | 1 | 13 | 27 | 23 | 9 | 5 | 19 | 31 | 17 | 3 | 11 | 25 |
| 9 | 9 | 27 | 19 | 1 | 17 | 29 | 11 | 7 | 25 | 21 | 3 | 15 | 31 | 13 | 5 | 23 |
| 11 | 11 | 31 | 9 | 13 | 29 | 7 | 15 | 27 | 5 | 17 | 25 | 3 | 19 | 23 | 1 | 21 |
| 13 | 13 | 25 | 1 | 27 | 11 | 15 | 23 | 3 | 29 | 9 | 17 | 21 | 5 | 31 | 7 | 19 |
| 15 | 15 | 19 | 11 | 23 | 7 | 27 | 3 | 31 | 1 | 29 | 5 | 25 | 9 | 21 | 13 | 17 |
| 17 | 17 | 13 | 21 | 9 | 25 | 5 | 29 | 1 | 31 | 3 | 27 | 7 | 23 | 11 | 19 | 15 |
| 19 | 19 | 7 | 31 | 5 | 21 | 17 | 9 | 29 | 3 | 23 | 15 | 11 | 27 | 1 | 25 | 13 |
| 21 | 21 | 1 | 23 | 19 | 3 | 25 | 17 | 5 | 27 | 15 | 7 | 29 | 13 | 9 | 31 | 11 |
| 23 | 23 | 5 | 13 | 31 | 15 | 3 | 21 | 25 | 7 | 11 | 29 | 17 | 1 | 19 | 27 | 9 |
| 25 | 25 | 11 | 3 | 17 | 31 | 19 | 5 | 9 | 23 | 27 | 13 | 1 | 15 | 29 | 21 | 7 |
| 27 | 27 | 17 | 7 | 3 | 13 | 23 | 31 | 21 | 11 | 1 | 9 | 19 | 29 | 25 | 15 | 5 |
| 29 | 29 | 23 | 17 | 11 | 5 | 1 | 7 | 13 | 19 | 25 | 31 | 27 | 21 | 15 | 9 | 3 |
| 31 | 31 | 29 | 27 | 25 | 23 | 21 | 19 | 17 | 15 | 13 | 11 | 9 | 7 | 5 | 3 | 1 |

Il y a 5 décompositions différentes, sur 3, 5, 11, 17 et 23.

Pour $\mathbb{Z}/66\mathbb{Z}$, $\varphi(66) = 20$ ; la table de $m$ est :

| | 1 | 5 | 7 | 13 | 17 | 19 | 23 | 25 | 29 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 5 | 7 | 13 | 17 | 19 | 23 | 25 | 29 | 31 |
| 5 | 5 | 25 | 31 | 1 | 19 | 29 | 17 | 7 | 13 | 23 |
| 7 | 7 | 31 | 17 | 25 | 13 | 1 | 29 | 23 | 5 | 19 |
| 13 | 13 | 1 | 25 | 29 | 23 | 17 | 31 | 5 | 19 | 7 |
| 17 | 17 | 19 | 13 | 23 | 25 | 7 | 5 | 29 | 31 | 1 |
| 19 | 19 | 29 | 1 | 17 | 7 | 31 | 25 | 13 | 23 | 5 |
| 23 | 23 | 17 | 29 | 31 | 5 | 25 | 1 | 19 | 7 | 13 |
| 25 | 25 | 7 | 23 | 5 | 29 | 13 | 19 | 31 | 1 | 17 |
| 29 | 29 | 13 | 5 | 19 | 31 | 23 | 7 | 1 | 17 | 25 |
| 31 | 31 | 23 | 19 | 7 | 1 | 5 | 13 | 17 | 25 | 29 |

Il y a 6 décompositions différentes, sur 5, 7, 13, 19, 23 et 29.

Pour $\mathbb{Z}/68\mathbb{Z}$, $\varphi(68) = 32$ ;

| | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 19 | 21 | 23 | 25 | 27 | 29 | 31 | 33 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 19 | 21 | 23 | 25 | 27 | 29 | 31 | 33 |
| 3 | 3 | 9 | 15 | 21 | 27 | 33 | 29 | 23 | 11 | 5 | 1 | 7 | 13 | 19 | 25 | 31 |
| 5 | 5 | 15 | 25 | 33 | 23 | 13 | 3 | 7 | 27 | 31 | 21 | 11 | 1 | 9 | 19 | 29 |
| 7 | 7 | 21 | 33 | 19 | 5 | 9 | 23 | 31 | 3 | 11 | 25 | 29 | 15 | 1 | 13 | 27 |
| 9 | 9 | 27 | 23 | 5 | 13 | 31 | 19 | 1 | 33 | 15 | 3 | 21 | 29 | 11 | 7 | 25 |
| 11 | 11 | 33 | 13 | 9 | 31 | 15 | 7 | 29 | 5 | 27 | 19 | 3 | 25 | 21 | 1 | 23 |
| 13 | 13 | 29 | 3 | 23 | 19 | 7 | 33 | 9 | 25 | 1 | 27 | 15 | 11 | 31 | 5 | 21 |
| 15 | 15 | 23 | 7 | 31 | 1 | 29 | 9 | 21 | 13 | 25 | 5 | 33 | 3 | 27 | 11 | 19 |
| 19 | 19 | 11 | 27 | 3 | 33 | 5 | 25 | 13 | 21 | 9 | 29 | 1 | 31 | 7 | 23 | 15 |
| 21 | 21 | 5 | 31 | 11 | 15 | 27 | 1 | 25 | 9 | 33 | 7 | 19 | 23 | 3 | 29 | 13 |
| 23 | 23 | 1 | 21 | 25 | 3 | 19 | 27 | 5 | 29 | 7 | 15 | 31 | 9 | 13 | 33 | 11 |
| 25 | 25 | 7 | 11 | 29 | 21 | 3 | 15 | 33 | 1 | 19 | 31 | 13 | 5 | 23 | 27 | 9 |
| 27 | 27 | 13 | 1 | 15 | 29 | 25 | 11 | 3 | 31 | 23 | 9 | 5 | 19 | 33 | 21 | 7 |
| 29 | 29 | 19 | 9 | 1 | 11 | 21 | 31 | 27 | 7 | 3 | 13 | 23 | 33 | 25 | 15 | 5 |
| 31 | 31 | 25 | 19 | 13 | 7 | 1 | 5 | 11 | 23 | 29 | 33 | 27 | 21 | 15 | 9 | 3 |
| 33 | 33 | 31 | 29 | 27 | 25 | 23 | 21 | 19 | 15 | 13 | 11 | 9 | 7 | 5 | 3 | 1 |

Il y a 2 décompositions différentes, sur 7 et 31.

Pour $\mathbb{Z}/70\mathbb{Z}$, $\varphi(70) = 24$ ; la table de $m$ est :

| | 1 | 3 | 9 | 11 | 13 | 17 | 19 | 23 | 27 | 29 | 31 | 33 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 3 | 9 | 11 | 13 | 17 | 19 | 23 | 27 | 29 | 31 | 33 |
| 3 | 3 | 9 | 27 | 33 | 31 | 19 | 13 | 1 | 11 | 17 | 23 | 29 |
| 9 | 9 | 27 | 11 | 29 | 23 | 13 | 31 | 3 | 33 | 19 | 1 | 17 |
| 11 | 11 | 33 | 29 | 19 | 3 | 23 | 1 | 27 | 17 | 31 | 9 | 13 |
| 13 | 13 | 31 | 23 | 3 | 29 | 11 | 33 | 19 | 1 | 27 | 17 | 9 |
| 17 | 17 | 19 | 13 | 23 | 11 | 9 | 27 | 29 | 31 | 3 | 33 | 1 |
| 19 | 19 | 13 | 31 | 1 | 33 | 27 | 11 | 17 | 23 | 9 | 29 | 3 |
| 23 | 23 | 1 | 3 | 27 | 19 | 29 | 17 | 31 | 9 | 33 | 13 | 11 |
| 27 | 27 | 11 | 33 | 17 | 1 | 31 | 23 | 9 | 29 | 13 | 3 | 19 |
| 29 | 29 | 17 | 19 | 31 | 27 | 3 | 9 | 33 | 13 | 1 | 11 | 23 |
| 31 | 31 | 23 | 1 | 9 | 17 | 33 | 29 | 13 | 3 | 11 | 19 | 27 |
| 33 | 33 | 29 | 17 | 13 | 9 | 1 | 3 | 11 | 19 | 23 | 27 | 31 |

à revoir

Il y a 5 décompositions différentes, sur 3, 11, 17, 23 et 29.

Pour $\mathbb{Z}/72\mathbb{Z}$, $\varphi(72) = 24$ ; la table de $m$ est :

| | 1 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 25 | 29 | 31 | 35 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 25 | 29 | 31 | 35 |
| 5 | 5 | 25 | 35 | 17 | 7 | 13 | 23 | 29 | 19 | 1 | 11 | 31 |
| 7 | 7 | 35 | 23 | 5 | 19 | 25 | 11 | 17 | 31 | 13 | 1 | 29 |
| 11 | 11 | 17 | 5 | 23 | 1 | 29 | 7 | 35 | 13 | 31 | 19 | 25 |
| 13 | 13 | 7 | 19 | 1 | 25 | 5 | 31 | 11 | 35 | 17 | 29 | 23 |
| 17 | 17 | 13 | 25 | 29 | 5 | 1 | 35 | 31 | 7 | 11 | 23 | 19 |
| 19 | 19 | 23 | 11 | 7 | 31 | 35 | 1 | 5 | 29 | 25 | 13 | 17 |
| 23 | 23 | 29 | 17 | 35 | 11 | 31 | 5 | 25 | 1 | 19 | 7 | 13 |
| 25 | 25 | 19 | 31 | 13 | 35 | 7 | 29 | 1 | 23 | 5 | 17 | 11 |
| 29 | 29 | 1 | 13 | 31 | 17 | 11 | 25 | 19 | 5 | 23 | 35 | 7 |
| 31 | 31 | 11 | 1 | 19 | 29 | 23 | 13 | 7 | 17 | 35 | 25 | 5 |
| 35 | 35 | 31 | 29 | 25 | 23 | 19 | 17 | 13 | 11 | 7 | 5 | 1 |

Il y a 6 décompositions différentes, sur 5, 11, 13, 19, 29 et 31.

Pour $\mathbb{Z}/76\mathbb{Z}$, $\varphi(76) = 36$ ;

| | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 21 | 23 | 25 | 27 | 29 | 31 | 33 | 35 | 37 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 21 | 23 | 25 | 27 | 29 | 31 | 33 | 35 | 37 |
| 3 | 3 | 9 | 15 | 21 | 27 | 33 | 37 | 31 | 25 | 13 | 7 | 1 | 5 | 11 | 17 | 23 | 29 | 35 |
| 5 | 5 | 15 | 25 | 35 | 31 | 21 | 11 | 1 | 9 | 29 | 37 | 27 | 17 | 7 | 3 | 13 | 23 | 33 |
| 7 | 7 | 21 | 35 | 27 | 13 | 1 | 15 | 29 | 33 | 5 | 9 | 23 | 37 | 25 | 11 | 3 | 17 | 31 |
| 9 | 9 | 27 | 31 | 13 | 5 | 23 | 35 | 17 | 1 | 37 | 21 | 3 | 15 | 33 | 25 | 7 | 11 | 29 |
| 11 | 11 | 33 | 21 | 1 | 23 | 31 | 9 | 13 | 35 | 3 | 25 | 29 | 7 | 15 | 37 | 17 | 5 | 27 |
| 13 | 13 | 37 | 11 | 15 | 35 | 9 | 17 | 33 | 7 | 31 | 5 | 21 | 29 | 3 | 23 | 27 | 1 | 25 |
| 15 | 15 | 31 | 1 | 29 | 17 | 13 | 33 | 3 | 27 | 11 | 35 | 5 | 25 | 21 | 9 | 37 | 7 | 23 |
| 17 | 17 | 25 | 9 | 33 | 1 | 35 | 7 | 27 | 15 | 23 | 11 | 31 | 3 | 37 | 5 | 29 | 13 | 21 |
| 21 | 21 | 13 | 29 | 5 | 37 | 3 | 31 | 11 | 23 | 15 | 27 | 7 | 35 | 1 | 33 | 9 | 25 | 17 |
| 23 | 23 | 7 | 37 | 9 | 21 | 25 | 5 | 35 | 11 | 27 | 3 | 33 | 13 | 17 | 29 | 1 | 31 | 15 |
| 25 | 25 | 1 | 27 | 23 | 3 | 29 | 21 | 5 | 31 | 7 | 33 | 17 | 9 | 35 | 15 | 11 | 37 | 13 |
| 27 | 27 | 5 | 17 | 37 | 15 | 7 | 29 | 25 | 3 | 35 | 13 | 9 | 31 | 23 | 1 | 21 | 33 | 11 |
| 29 | 29 | 11 | 7 | 25 | 33 | 15 | 3 | 21 | 37 | 1 | 17 | 35 | 23 | 5 | 13 | 31 | 27 | 9 |
| 31 | 31 | 17 | 3 | 11 | 25 | 37 | 23 | 9 | 5 | 33 | 29 | 15 | 1 | 13 | 27 | 35 | 21 | 7 |
| 33 | 33 | 23 | 13 | 3 | 7 | 17 | 27 | 37 | 29 | 9 | 1 | 11 | 21 | 31 | 35 | 25 | 15 | 5 |
| 35 | 35 | 29 | 23 | 17 | 11 | 5 | 1 | 7 | 13 | 25 | 31 | 37 | 33 | 27 | 21 | 15 | 9 | 3 |
| 37 | 37 | 35 | 33 | 31 | 29 | 27 | 25 | 23 | 21 | 17 | 15 | 13 | 11 | 9 | 7 | 5 | 3 | 1 |

Il y a 5 décompositions différentes, sur 3, 5, 17, 23 et 29.

Pour $\mathbb{Z}/78\mathbb{Z}$, $\varphi(78) = 24$ ; la table de $m$ est :

| | 1 | 5 | 7 | 11 | 17 | 19 | 23 | 25 | 29 | 31 | 35 | 37 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 25 | 29 | 31 | 35 |
| 5 | 5 | 25 | 35 | 23 | 7 | 17 | 37 | 31 | 11 | 1 | 19 | 29 |
| 7 | 7 | 35 | 29 | 1 | 37 | 23 | 5 | 19 | 31 | 17 | 11 | 25 |
| 11 | 11 | 23 | 1 | 35 | 31 | 25 | 19 | 37 | 7 | 29 | 5 | 17 |
| 17 | 17 | 7 | 37 | 31 | 23 | 11 | 1 | 35 | 25 | 19 | 29 | 5 |
| 19 | 19 | 17 | 23 | 25 | 11 | 29 | 31 | 7 | 5 | 35 | 37 | 1 |
| 23 | 23 | 37 | 5 | 19 | 1 | 31 | 17 | 29 | 35 | 11 | 25 | 7 |
| 25 | 25 | 31 | 19 | 37 | 35 | 7 | 29 | 1 | 23 | 5 | 17 | 11 |
| 29 | 29 | 11 | 31 | 7 | 25 | 5 | 35 | 23 | 17 | 37 | 1 | 19 |
| 31 | 31 | 1 | 17 | 29 | 19 | 35 | 11 | 5 | 37 | 25 | 7 | 23 |
| 35 | 35 | 19 | 11 | 5 | 29 | 37 | 25 | 17 | 1 | 7 | 23 | 31 |
| 37 | 37 | 29 | 25 | 17 | 5 | 1 | 7 | 11 | 19 | 23 | 31 | 35 |

Il y a 7 décompositions différentes, sur 5, 7, 11, 17, 19, 31 et 37.

Pour $\mathbb{Z}/80\mathbb{Z}$, $\varphi(80) = 32$ ;

| | 1 | 3 | 7 | 9 | 11 | 13 | 17 | 19 | 21 | 23 | 27 | 29 | 31 | 33 | 37 | 39 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 3 | 7 | 9 | 11 | 13 | 17 | 19 | 21 | 23 | 27 | 29 | 31 | 33 | 37 | 39 |
| 3 | 3 | 9 | 21 | 27 | 33 | 39 | 29 | 23 | 17 | 11 | 1 | 7 | 13 | 19 | 31 | 37 |
| 7 | 7 | 21 | 31 | 17 | 3 | 11 | 39 | 27 | 13 | 1 | 29 | 37 | 23 | 9 | 19 | 33 |
| 9 | 9 | 27 | 17 | 1 | 19 | 37 | 7 | 11 | 29 | 33 | 3 | 21 | 39 | 23 | 13 | 31 |
| 11 | 11 | 33 | 3 | 19 | 39 | 17 | 27 | 31 | 9 | 13 | 23 | 1 | 21 | 37 | 7 | 29 |
| 13 | 13 | 39 | 11 | 37 | 17 | 9 | 19 | 7 | 33 | 21 | 31 | 23 | 3 | 29 | 1 | 27 |
| 17 | 17 | 29 | 39 | 7 | 27 | 19 | 31 | 3 | 37 | 9 | 21 | 13 | 33 | 1 | 11 | 23 |
| 19 | 19 | 23 | 27 | 11 | 31 | 7 | 3 | 39 | 1 | 37 | 33 | 9 | 29 | 13 | 17 | 21 |
| 21 | 21 | 17 | 13 | 29 | 9 | 33 | 37 | 1 | 39 | 3 | 7 | 31 | 11 | 27 | 23 | 19 |
| 23 | 23 | 11 | 1 | 33 | 13 | 21 | 9 | 37 | 3 | 31 | 19 | 27 | 7 | 39 | 29 | 17 |
| 27 | 27 | 1 | 29 | 3 | 23 | 31 | 21 | 33 | 7 | 19 | 9 | 17 | 37 | 11 | 39 | 13 |
| 29 | 29 | 7 | 37 | 21 | 1 | 23 | 13 | 9 | 31 | 27 | 17 | 39 | 19 | 3 | 33 | 11 |
| 31 | 31 | 13 | 23 | 39 | 21 | 3 | 33 | 29 | 11 | 7 | 37 | 19 | 1 | 17 | 27 | 9 |
| 33 | 33 | 19 | 9 | 23 | 37 | 29 | 1 | 13 | 27 | 39 | 11 | 3 | 17 | 31 | 21 | 7 |
| 37 | 37 | 31 | 19 | 13 | 7 | 1 | 11 | 17 | 23 | 29 | 39 | 33 | 27 | 21 | 9 | 3 |
| 39 | 39 | 37 | 33 | 31 | 29 | 27 | 23 | 21 | 19 | 17 | 13 | 11 | 9 | 7 | 3 | 1 |

Il y a 4 décompositions différentes, sur 7, 13, 19 et 37.

Pour $\mathbb{Z}/88\mathbb{Z}$, $\varphi(88) = 40$ ;

| | 1 | 3 | 5 | 7 | 9 | 13 | 15 | 17 | 19 | 21 | 23 | 25 | 27 | 29 | 31 | 35 | 37 | 39 | 41 | 43 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 | 9 | 13 | 15 | 17 | 19 | 21 | 23 | 25 | 27 | 29 | 31 | 35 | 37 | 39 | 41 | 43 |
| 3 | 3 | 9 | 15 | 21 | 27 | 39 | 43 | 37 | 31 | 25 | 19 | 13 | 7 | 1 | 5 | 17 | 23 | 29 | 35 | 41 |
| 5 | 5 | 15 | 25 | 35 | 43 | 23 | 13 | 3 | 7 | 17 | 27 | 37 | 41 | 31 | 21 | 1 | 9 | 19 | 29 | 39 |
| 7 | 7 | 21 | 35 | 39 | 25 | 3 | 17 | 31 | 43 | 29 | 15 | 1 | 13 | 27 | 41 | 19 | 5 | 9 | 23 | 37 |
| 9 | 9 | 27 | 43 | 25 | 7 | 29 | 41 | 23 | 5 | 13 | 31 | 39 | 21 | 3 | 15 | 37 | 19 | 1 | 17 | 35 |
| 13 | 13 | 39 | 23 | 3 | 29 | 7 | 19 | 43 | 17 | 9 | 35 | 27 | 1 | 25 | 37 | 15 | 41 | 21 | 5 | 31 |
| 15 | 15 | 43 | 13 | 17 | 41 | 19 | 39 | 9 | 21 | 37 | 7 | 23 | 35 | 5 | 25 | 3 | 27 | 31 | 1 | 29 |
| 17 | 17 | 37 | 3 | 31 | 23 | 43 | 9 | 25 | 29 | 5 | 39 | 15 | 19 | 35 | 1 | 21 | 13 | 41 | 7 | 27 |
| 19 | 19 | 31 | 7 | 43 | 5 | 17 | 21 | 29 | 9 | 41 | 3 | 35 | 15 | 23 | 27 | 39 | 1 | 37 | 13 | 25 |
| 21 | 21 | 25 | 17 | 29 | 13 | 9 | 37 | 5 | 41 | 1 | 43 | 3 | 39 | 7 | 35 | 31 | 15 | 27 | 19 | 23 |
| 23 | 23 | 19 | 27 | 15 | 31 | 35 | 7 | 39 | 3 | 43 | 1 | 41 | 5 | 37 | 9 | 13 | 29 | 17 | 25 | 21 |
| 25 | 25 | 13 | 37 | 1 | 39 | 27 | 23 | 15 | 35 | 3 | 41 | 9 | 29 | 21 | 17 | 5 | 43 | 7 | 31 | 19 |
| 27 | 27 | 7 | 41 | 13 | 21 | 1 | 35 | 19 | 15 | 39 | 5 | 29 | 25 | 9 | 43 | 23 | 31 | 3 | 37 | 17 |
| 29 | 29 | 1 | 31 | 27 | 3 | 25 | 5 | 35 | 23 | 7 | 37 | 21 | 9 | 39 | 19 | 41 | 17 | 13 | 43 | 15 |
| 31 | 31 | 5 | 21 | 41 | 15 | 37 | 25 | 1 | 27 | 35 | 9 | 17 | 43 | 19 | 7 | 29 | 3 | 23 | 39 | 13 |
| 35 | 35 | 17 | 1 | 19 | 37 | 15 | 3 | 21 | 39 | 31 | 13 | 5 | 23 | 41 | 29 | 7 | 25 | 43 | 27 | 9 |
| 37 | 37 | 23 | 9 | 5 | 19 | 41 | 27 | 13 | 1 | 15 | 29 | 43 | 31 | 17 | 3 | 25 | 39 | 35 | 21 | 7 |
| 39 | 39 | 29 | 19 | 9 | 1 | 21 | 31 | 41 | 37 | 27 | 17 | 7 | 3 | 13 | 23 | 43 | 35 | 25 | 15 | 5 |
| 41 | 41 | 35 | 29 | 23 | 17 | 5 | 1 | 7 | 13 | 19 | 25 | 31 | 37 | 43 | 39 | 27 | 21 | 15 | 9 | 3 |
| 43 | 43 | 41 | 39 | 37 | 35 | 31 | 29 | 27 | 25 | 23 | 21 | 19 | 17 | 15 | 13 | 9 | 7 | 5 | 3 | 1 |

Il y a 4 décompositions différentes, sur 5, 17, 29 et 41.

Pour $\mathbb{Z}/90\mathbb{Z}$, $\varphi(90) = 24$ ; la table de $m$ est :

| | 1 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 |
| 7 | 7 | 41 | 13 | 1 | 29 | 43 | 19 | 23 | 37 | 11 | 17 | 31 |
| 11 | 11 | 13 | 31 | 37 | 7 | 29 | 17 | 41 | 19 | 43 | 1 | 23 |
| 13 | 13 | 1 | 37 | 11 | 41 | 23 | 29 | 17 | 43 | 31 | 7 | 19 |
| 17 | 17 | 29 | 7 | 41 | 19 | 37 | 31 | 43 | 13 | 1 | 23 | 11 |
| 19 | 19 | 43 | 29 | 23 | 37 | 1 | 13 | 11 | 41 | 17 | 31 | 7 |
| 23 | 23 | 19 | 17 | 29 | 31 | 13 | 11 | 37 | 7 | 41 | 43 | 1 |
| 29 | 29 | 23 | 41 | 17 | 43 | 11 | 37 | 31 | 1 | 7 | 19 | 13 |
| 31 | 31 | 37 | 19 | 43 | 13 | 41 | 7 | 1 | 29 | 23 | 11 | 17 |
| 37 | 37 | 11 | 43 | 31 | 1 | 17 | 41 | 7 | 23 | 19 | 13 | 29 |
| 41 | 41 | 17 | 1 | 7 | 23 | 31 | 43 | 19 | 11 | 13 | 29 | 37 |
| 43 | 43 | 31 | 23 | 19 | 11 | 7 | 1 | 13 | 17 | 29 | 37 | 41 |

Il y a 9 décompositions différentes, sur 7, 11, 17, 19, 23, 29, 31, 37 et 43.

Pour $\mathbb{Z}/92\mathbb{Z}$, $\varphi(92) = 44$ ;

| | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 | 21 | 25 | 27 | 29 | 31 | 33 | 35 | 37 | 39 | 41 | 43 | 45 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 | 21 | 25 | 27 | 29 | 31 | 33 | 35 | 37 | 39 | 41 | 43 | 45 |
| 3 | 3 | 9 | 15 | 21 | 27 | 33 | 39 | 45 | 41 | 35 | 29 | 17 | 11 | 5 | 1 | 7 | 13 | 19 | 25 | 31 | 37 | 43 |
| 5 | 5 | 15 | 25 | 35 | 45 | 37 | 27 | 17 | 7 | 3 | 13 | 33 | 43 | 39 | 29 | 19 | 9 | 1 | 11 | 21 | 31 | 41 |
| 7 | 7 | 21 | 35 | 43 | 29 | 15 | 1 | 13 | 27 | 41 | 37 | 9 | 5 | 19 | 33 | 45 | 31 | 17 | 3 | 11 | 25 | 39 |
| 9 | 9 | 27 | 45 | 29 | 11 | 7 | 25 | 43 | 31 | 13 | 5 | 41 | 33 | 15 | 3 | 21 | 39 | 35 | 17 | 1 | 19 | 37 |
| 11 | 11 | 33 | 37 | 15 | 7 | 29 | 41 | 19 | 3 | 25 | 45 | 1 | 21 | 43 | 27 | 5 | 17 | 39 | 31 | 9 | 13 | 35 |
| 13 | 13 | 39 | 27 | 1 | 25 | 41 | 15 | 11 | 37 | 29 | 3 | 43 | 17 | 9 | 35 | 31 | 5 | 21 | 45 | 19 | 7 | 33 |
| 15 | 15 | 45 | 17 | 13 | 43 | 19 | 11 | 41 | 21 | 9 | 39 | 7 | 37 | 25 | 5 | 35 | 27 | 3 | 33 | 29 | 1 | 31 |
| 17 | 17 | 41 | 7 | 27 | 31 | 3 | 37 | 21 | 13 | 45 | 11 | 35 | 1 | 33 | 25 | 9 | 43 | 15 | 19 | 39 | 5 | 29 |
| 19 | 19 | 35 | 3 | 41 | 13 | 25 | 29 | 9 | 45 | 7 | 31 | 15 | 39 | 1 | 33 | 25 | 9 | 43 | 15 | 19 | 39 | 5 |
| 21 | 21 | 29 | 13 | 37 | 5 | 45 | 3 | 39 | 11 | 31 | 19 | 27 | 15 | 35 | 7 | 43 | 1 | 41 | 9 | 33 | 17 | 25 |
| 25 | 25 | 17 | 33 | 9 | 41 | 1 | 43 | 7 | 35 | 15 | 27 | 19 | 31 | 11 | 39 | 3 | 45 | 5 | 37 | 13 | 29 | 21 |
| 27 | 27 | 11 | 43 | 5 | 33 | 21 | 17 | 37 | 1 | 39 | 15 | 31 | 7 | 45 | 9 | 29 | 25 | 13 | 41 | 3 | 35 | 19 |
| 29 | 29 | 5 | 39 | 19 | 15 | 43 | 9 | 25 | 33 | 1 | 35 | 11 | 45 | 13 | 21 | 37 | 3 | 31 | 27 | 7 | 41 | 17 |
| 31 | 31 | 1 | 29 | 33 | 3 | 27 | 35 | 5 | 25 | 37 | 7 | 39 | 9 | 21 | 41 | 11 | 19 | 43 | 13 | 17 | 45 | 15 |
| 33 | 33 | 7 | 19 | 45 | 21 | 5 | 31 | 35 | 9 | 17 | 43 | 3 | 29 | 37 | 11 | 15 | 41 | 25 | 1 | 27 | 39 | 13 |
| 35 | 35 | 13 | 9 | 31 | 39 | 17 | 5 | 27 | 43 | 21 | 1 | 45 | 25 | 3 | 19 | 41 | 29 | 7 | 15 | 37 | 33 | 11 |
| 37 | 37 | 19 | 1 | 17 | 35 | 39 | 21 | 3 | 15 | 33 | 41 | 5 | 13 | 31 | 43 | 25 | 7 | 11 | 29 | 45 | 27 | 9 |
| 39 | 39 | 25 | 11 | 3 | 17 | 31 | 45 | 33 | 19 | 5 | 9 | 37 | 41 | 27 | 13 | 1 | 15 | 29 | 43 | 35 | 21 | 7 |
| 41 | 41 | 31 | 21 | 11 | 1 | 9 | 19 | 29 | 39 | 43 | 33 | 13 | 3 | 7 | 17 | 27 | 37 | 45 | 35 | 25 | 15 | 5 |
| 43 | 43 | 37 | 31 | 25 | 19 | 13 | 7 | 1 | 5 | 11 | 17 | 29 | 35 | 41 | 45 | 39 | 33 | 27 | 21 | 15 | 9 | 3 |
| 45 | 45 | 43 | 41 | 39 | 37 | 35 | 33 | 31 | 29 | 27 | 25 | 21 | 19 | 17 | 15 | 13 | 11 | 9 | 7 | 5 | 3 | 1 |

Il y a 4 décompositions différentes, sur 3, 13, 19 et 31.

Pour $\mathbb{Z}/96\mathbb{Z}$, $\varphi(96) = 32$ ; la table de $m$ est :

| | 1 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 25 | 29 | 31 | 35 | 37 | 41 | 43 | 47 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 25 | 29 | 31 | 35 | 37 | 41 | 43 | 47 |
| 5 | 5 | 25 | 35 | 41 | 31 | 11 | 1 | 19 | 29 | 47 | 37 | 17 | 7 | 13 | 23 | 43 |
| 7 | 7 | 35 | 47 | 19 | 5 | 23 | 37 | 31 | 17 | 11 | 25 | 43 | 29 | 1 | 13 | 41 |
| 11 | 11 | 41 | 19 | 25 | 47 | 5 | 17 | 35 | 13 | 31 | 43 | 1 | 23 | 29 | 7 | 37 |
| 13 | 13 | 31 | 5 | 47 | 23 | 29 | 41 | 11 | 37 | 7 | 19 | 25 | 1 | 43 | 17 | 35 |
| 17 | 17 | 11 | 23 | 5 | 29 | 1 | 35 | 7 | 41 | 13 | 47 | 19 | 43 | 25 | 37 | 31 |
| 19 | 19 | 1 | 37 | 17 | 41 | 35 | 23 | 43 | 5 | 25 | 13 | 7 | 31 | 11 | 47 | 29 |
| 23 | 23 | 19 | 31 | 35 | 11 | 7 | 43 | 47 | 1 | 5 | 41 | 37 | 13 | 17 | 29 | 25 |
| 25 | 25 | 29 | 17 | 13 | 37 | 41 | 5 | 1 | 47 | 43 | 7 | 11 | 35 | 31 | 19 | 23 |
| 29 | 29 | 47 | 11 | 31 | 7 | 13 | 25 | 5 | 43 | 23 | 35 | 41 | 17 | 37 | 1 | 19 |
| 31 | 31 | 37 | 25 | 43 | 19 | 47 | 13 | 41 | 7 | 35 | 1 | 29 | 5 | 23 | 11 | 17 |
| 35 | 35 | 17 | 43 | 1 | 25 | 19 | 7 | 37 | 11 | 41 | 29 | 23 | 47 | 5 | 31 | 13 |
| 37 | 37 | 7 | 29 | 23 | 1 | 43 | 31 | 13 | 35 | 17 | 5 | 47 | 25 | 19 | 41 | 11 |
| 41 | 41 | 13 | 1 | 29 | 43 | 25 | 11 | 17 | 31 | 37 | 23 | 5 | 19 | 47 | 35 | 7 |
| 43 | 43 | 23 | 13 | 7 | 17 | 37 | 47 | 29 | 19 | 1 | 11 | 31 | 41 | 35 | 25 | 5 |
| 47 | 47 | 43 | 41 | 37 | 35 | 31 | 29 | 25 | 23 | 19 | 17 | 13 | 11 | 7 | 5 | 1 |

Il y a 7 décompositions différentes, sur 7, 13, 17, 23, 29, 37 et 4.

Pour $\mathbb{Z}/98\mathbb{Z}$, $\varphi(98) = 42$ ;

| | 1 | 3 | 5 | 9 | 11 | 13 | 15 | 17 | 19 | 23 | 25 | 27 | 29 | 31 | 33 | 37 | 39 | 41 | 43 | 45 | 47 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 9 | 11 | 13 | 15 | 17 | 19 | 23 | 25 | 27 | 29 | 31 | 33 | 37 | 39 | 41 | 43 | 45 | 47 |
| 3 | 3 | 9 | 15 | 27 | 33 | 39 | 45 | 47 | 41 | 29 | 23 | 17 | 11 | 5 | 1 | 13 | 19 | 25 | 31 | 37 | 43 |
| 5 | 5 | 15 | 25 | 45 | 43 | 33 | 23 | 13 | 3 | 17 | 27 | 37 | 47 | 41 | 31 | 11 | 1 | 9 | 19 | 29 | 39 |
| 9 | 9 | 27 | 45 | 17 | 1 | 19 | 37 | 43 | 25 | 11 | 29 | 47 | 33 | 15 | 3 | 39 | 41 | 23 | 5 | 13 | 31 |
| 11 | 11 | 33 | 43 | 1 | 23 | 45 | 31 | 9 | 13 | 41 | 19 | 3 | 25 | 47 | 29 | 15 | 37 | 39 | 17 | 5 | 27 |
| 13 | 13 | 39 | 33 | 19 | 45 | 27 | 1 | 25 | 47 | 5 | 31 | 41 | 15 | 11 | 37 | 9 | 17 | 43 | 29 | 3 | 23 |
| 15 | 15 | 45 | 23 | 37 | 31 | 1 | 29 | 39 | 9 | 47 | 17 | 13 | 43 | 25 | 5 | 33 | 3 | 27 | 41 | 11 | 19 |
| 17 | 17 | 47 | 13 | 43 | 9 | 25 | 39 | 5 | 29 | 1 | 33 | 31 | 3 | 37 | 27 | 41 | 23 | 11 | 45 | 19 | 15 |
| 19 | 19 | 41 | 3 | 25 | 13 | 47 | 9 | 29 | 31 | 45 | 15 | 23 | 37 | 1 | 39 | 17 | 43 | 5 | 33 | 27 | 11 |
| 23 | 23 | 29 | 17 | 11 | 41 | 5 | 47 | 1 | 45 | 39 | 13 | 33 | 19 | 27 | 25 | 31 | 15 | 37 | 9 | 43 | 3 |
| 25 | 25 | 23 | 27 | 29 | 19 | 31 | 17 | 33 | 15 | 13 | 37 | 11 | 39 | 9 | 41 | 43 | 5 | 45 | 3 | 47 | 1 |
| 27 | 27 | 17 | 37 | 47 | 3 | 41 | 13 | 31 | 23 | 33 | 11 | 43 | 1 | 45 | 9 | 19 | 25 | 29 | 15 | 39 | 5 |
| 29 | 29 | 11 | 47 | 33 | 25 | 15 | 43 | 3 | 37 | 19 | 39 | 1 | 41 | 17 | 23 | 5 | 45 | 13 | 27 | 31 | 9 |
| 31 | 31 | 5 | 41 | 15 | 47 | 11 | 25 | 37 | 1 | 27 | 9 | 45 | 17 | 19 | 43 | 29 | 33 | 3 | 39 | 23 | 13 |
| 33 | 33 | 1 | 31 | 3 | 29 | 37 | 5 | 27 | 39 | 25 | 41 | 9 | 23 | 43 | 11 | 45 | 13 | 19 | 47 | 15 | 17 |
| 37 | 37 | 13 | 11 | 39 | 15 | 9 | 33 | 41 | 17 | 31 | 43 | 19 | 5 | 29 | 45 | 3 | 27 | 47 | 23 | 1 | 25 |
| 39 | 39 | 19 | 1 | 41 | 37 | 17 | 3 | 23 | 43 | 15 | 5 | 25 | 45 | 33 | 13 | 27 | 47 | 31 | 11 | 9 | 29 |
| 41 | 41 | 25 | 9 | 23 | 39 | 43 | 27 | 11 | 5 | 37 | 45 | 29 | 13 | 3 | 19 | 47 | 31 | 15 | 1 | 17 | 33 |
| 43 | 43 | 31 | 19 | 5 | 17 | 29 | 41 | 45 | 33 | 9 | 3 | 15 | 27 | 39 | 47 | 23 | 11 | 1 | 13 | 25 | 37 |
| 45 | 45 | 37 | 29 | 13 | 5 | 3 | 11 | 19 | 27 | 43 | 47 | 39 | 31 | 23 | 15 | 1 | 9 | 17 | 25 | 33 | 41 |
| 47 | 47 | 43 | 39 | 31 | 27 | 23 | 19 | 15 | 11 | 3 | 1 | 5 | 9 | 13 | 17 | 25 | 29 | 33 | 37 | 41 | 45 |

Il y a 3 décompositions différentes, sur 19, 31 et 37.

# 5 Conclusion

La théorie des groupes permettrait-elle de résoudre la conjecture de Goldbach ?...

# 6 Annexe : Nombres de 1 à 1000 classés par leur nombre de décompositions Goldbach lorsque celui-ci est inférieur à 10 (y compris nombres doubles de nombres premiers)

Les nombres bleus sont ceux pour lesquels on avait trouvé une configuration "esthétique" dans la note précédente. Les nombres vert sont des doubles de nombres premiers.

Une seule décomposition :
6, 8, 12

Deux décompositions :
10, 14, 16, 18, 20, 28, 32, 38, 68

Trois décompositions :
22, 24, 26, 30, 40, 44, 52, 56, 62, 98, 128

Quatre décompositions :
34, 36, 42, 46, 50, 58, 80, 88, 92, 122, 152

Cinq décompositions :
48, 54, 64, 70, 74, 76, 82, 86, 94, 104, 124, 136, 148, 158, 164, 188

Six décompositions :
60, 66, 72, 100, 106, 110, 116, 118, 134, 146, 166, 172, 182, 212, 248, 332

Sept décompositions :
78, 96, 112, 130, 140, 176, 178, 194, 206, 208, 218, 224, 226, 232, 272, 278, 326, 398

Huit décompositions :
84, 102, 108, 138, 142, 154, 160, 184, 190, 200, 214, 242, 256, 266, 284, 292, 296, 308, 362, 368

Neuf décompositions :
90, 132, 170, 196, 202, 220, 230, 236, 238, 244, 250, 254, 262, 268, 302, 314, 338, 346, 356, 388, 428, 458, 488

Dix décompositions :
114, 126, 162, 260, 290, 304, 316, 328, 344, 352, 358, 374, 382, 416, 542, 632

# 7 Annexe 2 : table des groupes des ensembles des unités munis de la multiplication

La table de multiplication sur l'ensemble des unités de $\mathbb{Z}/8\mathbb{Z}$ quant à elle est :

| | 1 | 3 | 5 | 7 |
|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 |
| 3 | 3 | 1 | 7 | 5 |
| 5 | 5 | 7 | 1 | 3 |
| 7 | 7 | 5 | 3 | 1 |

La table de multiplication sur l'ensemble des unités de $\mathbb{Z}/12\mathbb{Z}$ quant à elle est :

| | 1 | 5 | 7 | 11 |
|---|---|---|---|---|
| 1 | 1 | 5 | 7 | 11 |
| 5 | 5 | 1 | 11 | 7 |
| 7 | 7 | 11 | 1 | 5 |
| 11 | 11 | 7 | 5 | 1 |

La table de multiplication sur l'ensemble des unités de $\mathbb{Z}/16\mathbb{Z}$ quant à elle

est :

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

La table de multiplication sur l'ensemble des unités de $\mathbb{Z}/9\mathbb{Z}$ est :

| | 1 | 2 | 4 | 5 | 7 | 8 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 4 | 5 | 7 | 8 |
| 2 | 2 | 4 | 8 | 1 | 5 | 7 |
| 4 | 4 | 8 | 7 | 2 | 1 | 5 |
| 5 | 5 | 1 | 2 | 7 | 8 | 4 |
| 7 | 7 | 5 | 1 | 8 | 4 | 2 |
| 8 | 8 | 7 | 5 | 4 | 2 | 1 |

La table de multiplication sur l'ensemble des unités de $\mathbb{Z}/18\mathbb{Z}$ quant à elle est :

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

La table de multiplication sur l'ensemble des unités de $\mathbb{Z}/20\mathbb{Z}$ quant à elle est :

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

La table de multiplication sur l'ensemble des unités de $\mathbb{Z}/24\mathbb{Z}$ quant à elle est :

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

La table de multiplication sur l'ensemble des unités de $\mathbb{Z}/28\mathbb{Z}$ quant à elle est :

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

La table de multiplication sur l'ensemble des unités de $\mathbb{Z}/15\mathbb{Z}$ quant à elle est :

| | 1 | 2 | 4 | 7 | 8 | 11 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 4 | 7 | 8 | 11 | 13 | 14 |
| 2 | 2 | 4 | 8 | 14 | 1 | 7 | 11 | 13 |
| 4 | 4 | 8 | 1 | 13 | 2 | 14 | 7 | 11 |
| 7 | 7 | 14 | 13 | 4 | 11 | 2 | 1 | 8 |
| 8 | 8 | 1 | 2 | 11 | 4 | 13 | 14 | 7 |
| 11 | 11 | 7 | 14 | 2 | 13 | 1 | 8 | 4 |
| 13 | 13 | 11 | 7 | 1 | 14 | 8 | 4 | 2 |
| 14 | 14 | 13 | 11 | 8 | 7 | 4 | 2 | 1 |

La table de multiplication sur l'ensemble des unités de $\mathbb{Z}/30\mathbb{Z}$ quant à elle est :

| | 1 | 7 | 11 | 13 | 17 | 19 | 23 | 29 |
|---|---|---|---|---|---|---|---|---|

La table de multiplication sur l'ensemble des unités de $\mathbb{Z}/32\mathbb{Z}$ quant à elle est :

| | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 | 21 | 23 | 25 | 27 | 29 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

La table de multiplication sur l'ensemble des unités de $\mathbb{Z}/36\mathbb{Z}$ quant à elle est :

| | 1 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 25 | 29 | 31 | 35 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|

La table de multiplication sur l'ensemble des unités de $\mathbb{Z}/40\mathbb{Z}$ quant à elle est :

| | 1 | 3 | 7 | 9 | 11 | 13 | 17 | 19 | 21 | 23 | 27 | 29 | 31 | 33 | 37 | 39 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

La table de multiplication sur l'ensemble des unités de $\mathbb{Z}/42\mathbb{Z}$ quant à elle est :

| | 1 | 5 | 11 | 13 | 17 | 19 | 23 | 25 | 29 | 31 | 37 | 41 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|

La table de multiplication sur l'ensemble des unités de $\mathbb{Z}/48\mathbb{Z}$ quant à elle est :

| | 1 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 25 | 29 | 31 | 35 | 37 | 41 | 43 | 47 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

La table de multiplication sur l'ensemble des unités de $\mathbb{Z}/60\mathbb{Z}$ quant à elle est :

| | 1 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 | 47 | 49 | 53 | 59 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

# Conjecture de Goldbach et Symétrie-miroir dans les tables de congruence

Denise Vella

Décembre 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 Etude d'un exemple

Cherchons les nombres premiers qui fournissent une décomposition Goldbach du nombre pair 98.
Seuls trois nombres premiers inférieurs à 49 (la moitié de 98) permettent de trouver de telles décompositions (i.e. ont leur complémentaire à 98 qui est premier aussi) : ce sont 19, 31 et 37.
98 = 19+79 = 31+67 = 37+61.
Ces nombres premiers se retrouvent aisément dans une table de congruence : pour que $p_j = 2x - p_i$ ($p_i$ nombre premier inférieur à $x$ ici 49) soit premier, $p_i$ doit être incongru à $2x$ modulo tout nombre premier $p_k$ inférieur à $x$.
Dans un premier temps, on trouve les restes modulaires de 98 pour chacun des nombres premiers inférieurs à $x$.
On renseigne une table de congruence (dont chaque case $(p_i, p_j)$ contient le reste modulaire de $p_i$ par $p_j$). Dans cette table, on élimine dans chaque colonne d'un nombre premier $p_j$ (en coloriant la case correspondante) les $p_i$ congru à $2x$ modulo $p_j$.

Pour 98, ces restes sont :

| | | |
|---|---|---|
| $98 \equiv 2\ (mod\ 3)$ | $98 \equiv 3\ (mod\ 5)$ | $98 \equiv 0\ (mod\ 7)$ |
| $98 \equiv 10\ (mod\ 11)$ | $98 \equiv 7\ (mod\ 13)$ | $98 \equiv 13\ (mod\ 17)$ |
| $98 \equiv 3\ (mod\ 19)$ | $98 \equiv 6\ (mod\ 23)$ | $98 \equiv 11\ (mod\ 29)$ |
| $98 \equiv 5\ (mod\ 31)$ | $98 \equiv 24\ (mod\ 37)$ | $98 \equiv 16\ (mod\ 41)$ |
| $98 \equiv 12\ (mod\ 43)$ | $98 \equiv 4\ (mod\ 47)$ | |

On aboutit à la table suivante :

| | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 | 47 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 0 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 5 | 2 | 0 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 7 | 1 | 2 | 0 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 |
| 11 | 2 | 1 | 4 | 0 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 |
| 13 | 1 | 3 | 6 | 2 | 0 | 13 | 13 | 13 | 13 | 13 | 13 | 13 | 13 | 13 |
| 17 | 2 | 2 | 3 | 6 | 4 | 0 | 17 | 17 | 17 | 17 | 17 | 17 | 17 | 17 |
| 19 | 1 | 4 | 5 | 8 | 6 | 2 | 0 | 19 | 19 | 19 | 19 | 19 | 19 | 19 |
| 23 | 2 | 3 | 2 | 1 | 10 | 6 | 4 | 0 | 23 | 23 | 23 | 23 | 23 | 23 |
| 29 | 2 | 4 | 1 | 7 | 3 | 12 | 10 | 6 | 0 | 29 | 29 | 29 | 29 | 29 |
| 31 | 1 | 1 | 3 | 9 | 5 | 14 | 12 | 8 | 2 | 0 | 31 | 31 | 31 | 31 |
| 37 | 1 | 2 | 2 | 4 | 11 | 3 | 18 | 14 | 8 | 6 | 0 | 37 | 37 | 37 |
| 41 | 2 | 1 | 6 | 8 | 2 | 7 | 3 | 18 | 12 | 10 | 4 | 0 | 41 | 41 |
| 43 | 1 | 3 | 1 | 10 | 4 | 9 | 5 | 20 | 14 | 12 | 6 | 2 | 0 | 43 |
| 47 | 2 | 2 | 5 | 3 | 8 | 13 | 9 | 1 | 18 | 16 | 10 | 6 | 4 | 0 |

Les nombres premiers inférieurs à $x$ permettant d'obtenir une décomposition Goldbach de $2x$ sont ceux dont la ligne ne contient aucune case éliminée (colorée)[1].
Démontrer la conjecture de Goldbach équivaut à démontrer qu'il existe toujours un nombre premier qui ne partage avec $2x$ aucune classe de congruence selon un certain nombre premier inférieur à $x$.
La table fournie pour 98 n'est qu'une partie d'une table de congruence complète que nous allons fournir ci-dessous pour le cas 30 car seule la table complète permet de voir les régularités.

[1] remarque : les colonnes des nombres premiers supérieurs à 2x/3 ne peuvent pas contenir de cases colorées.

| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 3 | 1 | 0 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 4 | 0 | 1 | 0 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 5 | 1 | 2 | 1 | 0 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 6 | 0 | 0 | 2 | 1 | 0 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 7 | 1 | 1 | 3 | 2 | 1 | 0 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 |
| 8 | 0 | 2 | 0 | 3 | 2 | 1 | 0 | 8 | 8 | 8 | 8 | 8 | 8 | 8 |
| 9 | 1 | 0 | 1 | 4 | 3 | 2 | 1 | 0 | 9 | 9 | 9 | 9 | 9 | 9 |
| 10 | 0 | 1 | 2 | 0 | 4 | 3 | 2 | 1 | 0 | 10 | 10 | 10 | 10 | 10 |
| 11 | 1 | 2 | 3 | 1 | 5 | 4 | 3 | 2 | 1 | 0 | 11 | 11 | 11 | 11 |
| 12 | 0 | 0 | 0 | 2 | 0 | 5 | 4 | 3 | 2 | 1 | 0 | 12 | 12 | 12 |
| 13 | 1 | 1 | 1 | 3 | 1 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 13 | 13 |
| 14 | 0 | 2 | 2 | 4 | 2 | 0 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 14 |
| 15 | 1 | 0 | 3 | 0 | 3 | 1 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 16 | 0 | 1 | 0 | 1 | 4 | 2 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 17 | 1 | 2 | 1 | 2 | 5 | 3 | 1 | 8 | 7 | 6 | 5 | 4 | 3 | 2 |
| 18 | 0 | 0 | 2 | 3 | 0 | 4 | 2 | 0 | 8 | 7 | 6 | 5 | 4 | 3 |
| 19 | 1 | 1 | 3 | 4 | 1 | 5 | 3 | 1 | 9 | 8 | 7 | 6 | 5 | 4 |
| 20 | 0 | 2 | 0 | 0 | 2 | 6 | 4 | 2 | 0 | 9 | 8 | 7 | 6 | 5 |
| 21 | 1 | 0 | 1 | 1 | 3 | 0 | 5 | 3 | 1 | 10 | 9 | 8 | 7 | 6 |
| 22 | 0 | 1 | 2 | 2 | 4 | 1 | 6 | 4 | 2 | 0 | 10 | 9 | 8 | 7 |
| 23 | 1 | 2 | 3 | 3 | 5 | 2 | 7 | 5 | 3 | 1 | 11 | 10 | 9 | 8 |
| 24 | 0 | 0 | 0 | 4 | 0 | 3 | 0 | 6 | 4 | 2 | 0 | 11 | 10 | 9 |
| 25 | 1 | 1 | 1 | 0 | 1 | 4 | 1 | 7 | 5 | 3 | 1 | 12 | 11 | 10 |
| 26 | 0 | 2 | 2 | 1 | 2 | 5 | 2 | 8 | 6 | 4 | 2 | 0 | 12 | 11 |
| 27 | 1 | 0 | 3 | 2 | 3 | 6 | 3 | 0 | 7 | 5 | 3 | 1 | 13 | 12 |
| 28 | 0 | 1 | 0 | 3 | 4 | 0 | 4 | 1 | 8 | 6 | 4 | 2 | 0 | 13 |
| 29 | 1 | 2 | 1 | 4 | 5 | 1 | 5 | 2 | 9 | 7 | 5 | 3 | 1 | 14 |
| 30 | 0 | 0 | 2 | 0 | 0 | 2 | 6 | 3 | 0 | 8 | 6 | 4 | 2 | 0 |

Dans la colonne de $p_j$ sont colorés les nombres congrus à $2x$ (ici 30) modulo $p_j$. Cela a pour conséquence que dans chaque ligne $p_i$ sont colorés les nombres se trouvant dans la colonne d'un diviseur de $2x-p_i$. Par exemple, dans la deuxième ligne, on lit que 2, 4, 7 et 14 divisent 28. Dans la troisième ligne, on lit que 3 et 9 divisent 27.

Mathématiquement, cela s'écrit[2] :

$$\tau(2x - p_i) - 2 = Card\{\ p_j\ <\ x\ tel\ que\ 2x\ \equiv\ p_i\ (mod\ p_j)\}$$

Lorsqu'aucune case n'est colorée dans une ligne, le nombre $2x - p_i$ est premier. Il est obligatoire qu'au moins un nombre inférieur à $x$ ait une ligne ne contenant aucune case colorée car si tel n'était pas le cas, cela aurait pour conséquence une contradiction avec le théorème de Tchebychev (preuve du postulat de Bertrand)

[2] $\tau(n)$ désigne le nombre de diviseurs de n. 1 et n étant des diviseurs de n, on ôte 2 à $\tau(n)$

qui exprime qu'il y a toujours un nombre premier entre $x$ et $2x$. Il faut cependant prouver qu'une telle ligne sans couleur existe pour un nombre premier inférieur à $x$.

On remarque qu'on a utilisé différentes couleurs pour représenter les congruences. On voit se dégager dans ce tableau des triplets de coordonnées représentant le fait que deux cases d'une même ligne sont de la même couleur (elles vont presque toujours par deux ; lorsque ce n'est pas le cas, soit c'est dû au fait que les deux cases s'identifient, soit il s'agit de cases de la dernière ligne (vertes dans notre exemple), ou de la dernière diagonale ascendante de nombres (verts également car ils sont en correspondance (verticale cette fois) avec ceux de la dernière ligne)). Par exemple, le triplet $(k, i, j) = (9, 3, 7)$ représente le fait que les deux cases $(9, 3)$ et $(9, 7)$ sont de la même couleur (dit autrement, $3 \mid 30 - 9 \Rightarrow 7 \mid 30 - 9$)[3].

On verra d'autres propriétés de la table de congruence au paragraphe 4.

# 3 Les beautés cachées des tables de congruence

On retrouve dans la table de congruence une propriété connue : les contenus des cases de chaque ligne se retrouvent dans deux diagonales : la diagonale descendante qui débute deux lignes au-dessous et la diagonale ascendante qui débute deux lignes au-dessus (du fait de l'équivalence $i \equiv j \ (mod\ k) \Leftrightarrow i + k \equiv j \ (mod\ k)\ et\ \ i - k \equiv j \ (mod\ k)$). On illustrera ce fait par trois lignes rouges dans la ligne de 7, la diagonale ascendante de 5 et la diagonale descendante de 9 dans la table suivante.

[3]Le triplet (k,i,j) représente le fait que $i \times j = 2x - k$.

| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 3 | 1 | 0 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 4 | 0 | 1 | 0 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 5 | 1 | 2 | 1 | 0 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 6 | 0 | 0 | 2 | 1 | 0 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 7 | 1 | 1 | 3 | 2 | 1 | 0 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 |
| 8 | 0 | 2 | 0 | 3 | 2 | 1 | 0 | 8 | 8 | 8 | 8 | 8 | 8 | 8 |
| 9 | 1 | 0 | 1 | 4 | 3 | 2 | 1 | 0 | 9 | 9 | 9 | 9 | 9 | 9 |
| 10 | 0 | 1 | 2 | 0 | 4 | 3 | 2 | 1 | 0 | 10 | 10 | 10 | 10 | 10 |
| 11 | 1 | 2 | 3 | 1 | 5 | 4 | 3 | 2 | 1 | 0 | 11 | 11 | 11 | 11 |
| 12 | 0 | 0 | 0 | 2 | 0 | 5 | 4 | 3 | 2 | 1 | 0 | 12 | 12 | 12 |
| 13 | 1 | 1 | 1 | 3 | 1 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 13 | 13 |
| 14 | 0 | 2 | 2 | 4 | 2 | 0 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 14 |
| 15 | 1 | 0 | 3 | 0 | 3 | 1 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 16 | 0 | 1 | 0 | 1 | 4 | 2 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 17 | 1 | 2 | 1 | 2 | 5 | 3 | 1 | 8 | 7 | 6 | 5 | 4 | 3 | 2 |
| 18 | 0 | 0 | 2 | 3 | 0 | 4 | 2 | 0 | 8 | 7 | 6 | 5 | 4 | 3 |
| 19 | 1 | 1 | 3 | 4 | 1 | 5 | 3 | 1 | 9 | 8 | 7 | 6 | 5 | 4 |
| 20 | 0 | 2 | 0 | 0 | 2 | 6 | 4 | 2 | 0 | 9 | 8 | 7 | 6 | 5 |
| 21 | 1 | 0 | 1 | 1 | 3 | 0 | 5 | 3 | 1 | 10 | 9 | 8 | 7 | 6 |
| 22 | 0 | 1 | 2 | 2 | 4 | 1 | 6 | 4 | 2 | 0 | 10 | 9 | 8 | 7 |
| 23 | 1 | 2 | 3 | 3 | 5 | 2 | 7 | 5 | 3 | 1 | 11 | 10 | 9 | 8 |
| 24 | 0 | 0 | 0 | 4 | 0 | 3 | 0 | 6 | 4 | 2 | 0 | 11 | 10 | 9 |
| 25 | 1 | 1 | 1 | 0 | 1 | 4 | 1 | 7 | 5 | 3 | 1 | 12 | 11 | 10 |
| 26 | 0 | 2 | 2 | 1 | 2 | 5 | 2 | 8 | 6 | 4 | 2 | 0 | 12 | 11 |
| 27 | 1 | 0 | 3 | 2 | 3 | 6 | 3 | 0 | 7 | 5 | 3 | 1 | 13 | 12 |
| 28 | 0 | 1 | 0 | 3 | 4 | 0 | 4 | 1 | 8 | 6 | 4 | 2 | 0 | 13 |
| 29 | 1 | 2 | 1 | 4 | 5 | 1 | 5 | 2 | 9 | 7 | 5 | 3 | 1 | 14 |
| 30 | 0 | 0 | 2 | 0 | 0 | 2 | 6 | 3 | 0 | 8 | 6 | 4 | 2 | 0 |

Intéressons-nous maintenant aux différentes symétries-miroir que recèle chaque table de congruence. Pour cela, comparons deux tables : l'une dans laquelle on va colorer les cases $(i, j)$ telles que $i \equiv 5 \ (mod\ j)$ et l'autre dans laquelle on va colorer les cases $(i, j)$ telles que $i \equiv 23 \ (mod\ j)$. Pour la deuxième table, à notre habitude, on calcule les restes de 23 modulo chacun des nombres de 2 à 14. Les restes de 23 sont :

$$\begin{array}{l|l} 23 \equiv 1 \ (mod\ 2) & 23 \equiv 5 \ (mod\ 9) \\ 23 \equiv 2 \ (mod\ 3) & 23 \equiv 3 \ (mod\ 10) \\ 23 \equiv 3 \ (mod\ 4) & 23 \equiv 1 \ (mod\ 11) \\ 23 \equiv 3 \ (mod\ 5) & 23 \equiv 11 \ (mod\ 12) \\ 23 \equiv 5 \ (mod\ 6) & 23 \equiv 10 \ (mod\ 13) \\ 23 \equiv 2 \ (mod\ 7) & 23 \equiv 9 \ (mod\ 14) \\ 23 \equiv 7 \ (mod\ 8) & \end{array}$$

| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 3 | 1 | 0 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 4 | 0 | 1 | 0 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 5 | 1 | 2 | 1 | 0 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 6 | 0 | 0 | 2 | 1 | 0 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 7 | 1 | 1 | 3 | 2 | 1 | 0 | 7 | 7 | 7 | 7 | 7 | 7 | 7 |
| 8 | 0 | 2 | 0 | 3 | 2 | 1 | 0 | 8 | 8 | 8 | 8 | 8 | 8 |
| 9 | 1 | 0 | 1 | 4 | 3 | 2 | 1 | 0 | 9 | 9 | 9 | 9 | 9 |
| 10 | 0 | 1 | 2 | 0 | 4 | 3 | 2 | 1 | 0 | 10 | 10 | 10 | 10 |
| 11 | 1 | 2 | 3 | 1 | 5 | 4 | 3 | 2 | 1 | 0 | 11 | 11 | 11 |
| 12 | 0 | 0 | 0 | 2 | 0 | 5 | 4 | 3 | 2 | 1 | 0 | 12 | 12 |
| 13 | 1 | 1 | 1 | 3 | 1 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 13 |
| 14 | 0 | 2 | 2 | 4 | 2 | 0 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 15 | 1 | 0 | 3 | 0 | 3 | 1 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 16 | 0 | 1 | 0 | 1 | 4 | 2 | 0 | 7 | 6 | 5 | 4 | 3 | 2 |
| 17 | 1 | 2 | 1 | 2 | 5 | 3 | 1 | 8 | 7 | 6 | 5 | 4 | 3 |
| 18 | 0 | 0 | 2 | 3 | 0 | 4 | 2 | 0 | 8 | 7 | 6 | 5 | 4 |
| 19 | 1 | 1 | 3 | 4 | 1 | 5 | 3 | 1 | 9 | 8 | 7 | 6 | 5 |
| 20 | 0 | 2 | 0 | 0 | 2 | 6 | 4 | 2 | 0 | 9 | 8 | 7 | 6 |
| 21 | 1 | 0 | 1 | 1 | 3 | 0 | 5 | 3 | 1 | 10 | 9 | 8 | 7 |
| 22 | 0 | 1 | 2 | 2 | 4 | 1 | 6 | 4 | 2 | 0 | 10 | 9 | 8 |
| 23 | 1 | 2 | 3 | 3 | 5 | 2 | 7 | 5 | 3 | 1 | 11 | 10 | 9 |
| 24 | 0 | 0 | 0 | 4 | 0 | 3 | 0 | 6 | 4 | 2 | 0 | 11 | 10 |
| 25 | 1 | 1 | 1 | 0 | 1 | 4 | 1 | 7 | 5 | 3 | 1 | 12 | 11 |
| 26 | 0 | 2 | 2 | 1 | 2 | 5 | 2 | 8 | 6 | 4 | 2 | 0 | 12 |
| 27 | 1 | 0 | 3 | 2 | 3 | 6 | 3 | 0 | 7 | 5 | 3 | 1 | 13 |
| 28 | 0 | 1 | 0 | 3 | 4 | 0 | 4 | 1 | 8 | 6 | 4 | 2 | 0 |

Table de congruence de x = 14, 2x = 28 avec ses cases $(i, j)$ / $i \equiv 5\ (mod\ j)$ colorées

| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 3 | 1 | 0 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 4 | 0 | 1 | 0 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 5 | 1 | 2 | 1 | 0 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 6 | 0 | 0 | 2 | 1 | 0 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 7 | 1 | 1 | 3 | 2 | 1 | 0 | 7 | 7 | 7 | 7 | 7 | 7 | 7 |
| 8 | 0 | 2 | 0 | 3 | 2 | 1 | 0 | 8 | 8 | 8 | 8 | 8 | 8 |
| 9 | 1 | 0 | 1 | 4 | 3 | 2 | 1 | 0 | 9 | 9 | 9 | 9 | 9 |
| 10 | 0 | 1 | 2 | 0 | 4 | 3 | 2 | 1 | 0 | 10 | 10 | 10 | 10 |
| 11 | 1 | 2 | 3 | 1 | 5 | 4 | 3 | 2 | 1 | 0 | 11 | 11 | 11 |
| 12 | 0 | 0 | 0 | 2 | 0 | 5 | 4 | 3 | 2 | 1 | 0 | 12 | 12 |
| 13 | 1 | 1 | 1 | 3 | 1 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 13 |
| 14 | 0 | 2 | 2 | 4 | 2 | 0 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 15 | 1 | 0 | 3 | 0 | 3 | 1 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 16 | 0 | 1 | 0 | 1 | 4 | 2 | 0 | 7 | 6 | 5 | 4 | 3 | 2 |
| 17 | 1 | 2 | 1 | 2 | 5 | 3 | 1 | 8 | 7 | 6 | 5 | 4 | 3 |
| 18 | 0 | 0 | 2 | 3 | 0 | 4 | 2 | 0 | 8 | 7 | 6 | 5 | 4 |
| 19 | 1 | 1 | 3 | 4 | 1 | 5 | 3 | 1 | 9 | 8 | 7 | 6 | 5 |
| 20 | 0 | 2 | 0 | 0 | 2 | 6 | 4 | 2 | 0 | 9 | 8 | 7 | 6 |
| 21 | 1 | 0 | 1 | 1 | 3 | 0 | 5 | 3 | 1 | 10 | 9 | 8 | 7 |
| 22 | 0 | 1 | 2 | 2 | 4 | 1 | 6 | 4 | 2 | 0 | 10 | 9 | 8 |
| 23 | 1 | 2 | 3 | 3 | 5 | 2 | 7 | 5 | 3 | 1 | 11 | 10 | 9 |
| 24 | 0 | 0 | 0 | 4 | 0 | 3 | 0 | 6 | 4 | 2 | 0 | 11 | 10 |
| 25 | 1 | 1 | 1 | 0 | 1 | 4 | 1 | 7 | 5 | 3 | 1 | 12 | 11 |
| 26 | 0 | 2 | 2 | 1 | 2 | 5 | 2 | 8 | 6 | 4 | 2 | 0 | 12 |
| 27 | 1 | 0 | 3 | 2 | 3 | 6 | 3 | 0 | 7 | 5 | 3 | 1 | 13 |
| 28 | 0 | 1 | 0 | 3 | 4 | 0 | 4 | 1 | 8 | 6 | 4 | 2 | 0 |

Table de congruence x = 14, 2x = 28 avec ses cases (i,j) / i $\equiv 23 (mod j) colorées$

On voit que les nombres entourés dans les deux tables sont deux à deux symétriques autour de la ligne de 14 (à part le nombre coloré dans la ligne de 28).

Les différentes symétries-miroir que contient une table de congruence ont pour conséquence la propriété suivante :

$$\begin{array}{rl} \exists i, & i \nmid 2x, \\ \forall k < i, & \\ & 2 \nmid i+2 \\ & 3 \nmid i+3 \\ & 4 \nmid i+4 \\ & \dots \\ & k \nmid i+k \end{array}$$

# 4 Symétrie-miroir entre les congruents à 2x et les congruents à 0

La symétrie-miroir a été montrée ci-dessus entre les cases $(i, j)$ telles que $i \equiv 5 \ (mod\ j)$ et les cases telles que $i \equiv 23 \ (mod\ j)$. Cette symétrie existe évidemment également entre les cases $(i, j)$ telles que $i \equiv 28 \ (mod\ j)$ et celles telles que $i \equiv 0 \ (mod\ j)$ et plus généralement entre les cases telles que $i \equiv 0 \ (mod\ j)$ et celles telles que $i \equiv 2x \ (mod\ j)$.

Dessinons une dernière fois la table du cas 30 avec colorées de trois couleurs différentes les cases en question (vert pour les congrus à 0 en étant congrus à $2x$, cyan pour les autres congrus à $2x$ (non congrus à 0) et jaune pour les congrus à 0 hors congruence à $2x$), de façon à bien appréhender cette symétrie. Elle s'effectue verticalement autour de la ligne $x$ qu'on matérialise en l'encadrant par deux lignes horizontales. On isole également la ligne $2x$ par une ligne horizontale car ses éléments ne sont pas affectés par la symétrie.

| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 3 | 1 | 0 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 4 | 0 | 1 | 0 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 5 | 1 | 2 | 1 | 0 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 6 | 0 | 0 | 2 | 1 | 0 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 7 | 1 | 1 | 3 | 2 | 1 | 0 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 |
| 8 | 0 | 2 | 0 | 3 | 2 | 1 | 0 | 8 | 8 | 8 | 8 | 8 | 8 | 8 |
| 9 | 1 | 0 | 1 | 4 | 3 | 2 | 1 | 0 | 9 | 9 | 9 | 9 | 9 | 9 |
| 10 | 0 | 1 | 2 | 0 | 4 | 3 | 2 | 1 | 0 | 10 | 10 | 10 | 10 | 10 |
| 11 | 1 | 2 | 3 | 1 | 5 | 4 | 3 | 2 | 1 | 0 | 11 | 11 | 11 | 11 |
| 12 | 0 | 0 | 0 | 2 | 0 | 5 | 4 | 3 | 2 | 1 | 0 | 12 | 12 | 12 |
| 13 | 1 | 1 | 1 | 3 | 1 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 13 | 13 |
| 14 | 0 | 2 | 2 | 4 | 2 | 0 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 14 |
| 15 | 1 | 0 | 3 | 0 | 3 | 1 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 16 | 0 | 1 | 0 | 1 | 4 | 2 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 17 | 1 | 2 | 1 | 2 | 5 | 3 | 1 | 8 | 7 | 6 | 5 | 4 | 3 | 2 |
| 18 | 0 | 0 | 2 | 3 | 0 | 4 | 2 | 0 | 8 | 7 | 6 | 5 | 4 | 3 |
| 19 | 1 | 1 | 3 | 4 | 1 | 5 | 3 | 1 | 9 | 8 | 7 | 6 | 5 | 4 |
| 20 | 0 | 2 | 0 | 0 | 2 | 6 | 4 | 2 | 0 | 9 | 8 | 7 | 6 | 5 |
| 21 | 1 | 0 | 1 | 1 | 3 | 0 | 5 | 3 | 1 | 10 | 9 | 8 | 7 | 6 |
| 22 | 0 | 1 | 2 | 2 | 4 | 1 | 6 | 4 | 2 | 0 | 10 | 9 | 8 | 7 |
| 23 | 1 | 2 | 3 | 3 | 5 | 2 | 7 | 5 | 3 | 1 | 11 | 10 | 9 | 8 |
| 24 | 0 | 0 | 0 | 4 | 0 | 3 | 0 | 6 | 4 | 2 | 0 | 11 | 10 | 9 |
| 25 | 1 | 1 | 1 | 0 | 1 | 4 | 1 | 7 | 5 | 3 | 1 | 12 | 11 | 10 |
| 26 | 0 | 2 | 2 | 1 | 2 | 5 | 2 | 8 | 6 | 4 | 2 | 0 | 12 | 11 |
| 27 | 1 | 0 | 3 | 2 | 3 | 6 | 3 | 0 | 7 | 5 | 3 | 1 | 13 | 12 |
| 28 | 0 | 1 | 0 | 3 | 4 | 0 | 4 | 1 | 8 | 6 | 4 | 2 | 0 | 13 |
| 29 | 1 | 2 | 1 | 4 | 5 | 1 | 5 | 2 | 9 | 7 | 5 | 3 | 1 | 14 |
| 30 | 0 | 0 | 2 | 0 | 0 | 2 | 6 | 3 | 0 | 8 | 6 | 4 | 2 | 0 |

Considérons dans ce tableau les nombres premiers inférieurs à $x$, qui ne divisent pas $x$, et dont les lignes contiennent comme seuls éléments colorés les zéros de la diagonale, qui sont jaunes. Les trois nombres concernés ici sont 7, 11 et 13. Considérons l'un de ces nombres et appelons le $p$. Puisque la ligne de $p$ ne contient aucune case colorée à part le zéro de la diagonale, la ligne du symétrique de $p$ par rapport à $x$, qui est égal à $2x - p$, ne contient pas de case colorée non plus si ce n'est sur sa diagonale. Mais si cette ligne ne contient pas de case colorée, elle ne contient pas de 0 puisqu'on a coloré tous les zéros. Donc ce nombre n'est divisible par aucun nombre premier inférieur à $\sqrt{2x}$. Il est donc premier aussi.

Voyons maintenant pourquoi une telle ligne au moins (avec pour seul élément coloré un zéro jaune dans la diagonale) existe forcément. Intéressons-nous à la partie supérieure droite (au-dessus de la diagonale de zéros) de la partie supérieure de la table. Dans cette partie de la table, on voit que lorsque des éléments ont été entourés, ils sont égaux à l'indice de la ligne à laquelle ils

appartiennent dans la table (pour la table de 30 que l'on a étudiée, on a dû entourer les 2 de la deuxième ligne, les 3 de la troisième ligne, les 4 de la quatrième ligne, les 6 de la sixième ligne et les 8 de la huitième ligne). Ces nombres se retrouvent dans la dernière ligne de la table : ce sont les résidus de $2x$ modulo chaque indice de colonne. Il n'est pas possible de colorier un élément dans chaque ligne du tableau dans cette partie supérieure droite de la partie supérieure de la table car l'ensemble des résidus de $2x$ modulo les nombres de 2 à $x$ ne peut contenir tous les nombres de 1 à $x-1$. Il y a donc forcément dans la partie supérieure de la table un nombre premier inférieur à $x$ qui a comme seul élément coloré de sa ligne en tout et pour tout le zéro de sa diagonale.

# 5 Les Recherches arithmétiques de Gauss

C'est Gauss qui est à l'origine de l'arithmétique modulaire. Ses "Recherches arithmétiques" sont agréables à lire car l'auteur y est pédagogue pour expliquer au lecteur ses découvertes et résultats.
Le paragraphe 33 [4] de la Section Seconde "Des congruences du premier degré" explique comment résoudre un système de congruence : "Quand tous les nombres A, B, C, etc. sont premiers entre eux, leur produit est le plus petit nombre divisible par chacun d'eux ; et dans ce cas, il est évident que toutes les congruences $z \equiv a \ (mod\ A)$, $z \equiv b \ (mod\ B)$, etc. se ramènent à une seule $z \equiv r \ (mod\ R)$ qui leur équivaudra, R étant le produit des nombres A, B, C, etc. : il suit de là réciproquement qu'une seule condition $z \equiv r \ (mod\ R)$ peut être décomposée en plusieurs $z \equiv a \ (mod\ A)$, $z \equiv b \ (mod\ B)$, $z \equiv c \ (mod\ C)$, etc. si A, B, C, etc. sont les différents facteurs premiers entre eux qui composent R. Cette observation nous donne non seulement le moyen de découvrir l'impossibilité lorsqu'elle existe, mais encore une méthode plus commode et plus élégante pour déterminer les racines."
Dans le cas qui nous intéresse, il ne s'agit pas de résoudre un système de *congruences* mais un système d'*incongruences*. Résoudre ce système d'incongruences équivaut à trouver l'union des ensembles de solutions des systèmes obtenus en remplaçant chaque incongruence par une disjonction des congruences complémentaires correspondantes. Cette union devait a priori être non vide, chaque système ayant une solution, dans la mesure où les modules sont premiers entre eux ; cependant, il restait à garantir que l'une au moins des solutions trouvées est un nombre premier impair inférieur à $x$.

# 6 Les preuves élémentaires d'Erdös

Erdös a été le mathématicien voyageur. La lecture de sa biographie le rend éminemment sympathique, il était très spirituel. Surtout, Erdös cherchait les Preuves du Livre, il abordait les mathématiques artistiquement, il était en quête de démonstrations qui soient également esthétiques. Il paraît qu'il abordait les mathématiciens, du plus au moins connu, en leur disant : *"Mon cerveau est ouvert. Avez-vous un problème ?"*.

[4] Bizarrement, le paragraphe 34 est noté 43 dans l'édition Jacques Gabay dont je dispose ainsi que dans celle disponible sur Gallica. Gauss avait sûrement vu toutes les symétries-miroir des tables de congruence et l'a peut-être indiqué par un clin d'oeil en inversant les deux chiffres ; ou bien c'est tout simplement une erreur dactylographique...

Le livre “Raisonnements divins” d'Aigner et Ziegler fournit la preuve élémentaire d'Erdös du théorème de Tchebychev. Il fournit aussi sa preuve, élémentaire également, de l'infinitude des nombres premiers. Ces preuves sont dites élémentaires car elles ne nécessitent pas l'utilisation d'outils de l'analyse complexe. Erdös a aussi prouvé avec Selberg le théorème des nombres premiers, à nouveau par une méthode élémentaire. La conjecture de Goldbach devait donc elle aussi, vraisemblablement, pouvoir être démontrée de façon élémentaire. Terminons ce paragraphe par une citation d'Erdös : *“Je sais que les nombres sont beaux. S'ils ne le sont pas, rien ne l'est.”*.

# 7 La découverte merveilleuse d'Euler

Dans son article “Découverte d'une loi toute extraordinaire des nombres par rapport à la somme de leurs diviseurs”, Euler présente une formule récurrente de calcul de cette somme. Il prévient tout d'abord le lecteur : *“Cette règle, que je vais expliquer, est à mon avis d'autant plus importante q'ulle appartient à ce genre dont nous pouvons nous assurer de la vérité, sans en donner une démonstration parfaite. Néammoins, j'en apporterai de telles preuves, qu'on pourra presque les envisager comme équivalentes à une démonstration rigoureuse.” [...] “Néammoins, j'ai remarqué que cette progression suit une loi bien réglée et qu'elle est même comprise dans l'ordre des progressions que les Géomètres nomment récurrentes, de sorte qu'on peut toujours former chacun de ses termes par quelques-uns des précédents, suivant une règle constante.”. [...] “Ces choses remarquées, il ne sera pas difficile de faire l'application de cette formule à chaque nombre proposé et de se convaincre de sa vérité par autant d'exemples qu'on voudra développer. Et comme je dois avouer que je ne suis pas en état d'en donner une démonstration rigoureuse, j'en ferai voir sa justesse par un assez grand nombre d'exemples.”*.
Un programme en C++ de calcul de la somme des diviseurs d'un nombre par la méthode récursive d'Euler est fourni en annexe.
Euler fournit (sections 10, et suiv. de son article) une ébauche de démonstration ; pour faire un raisonnement similaire ici, il faut s'intéresser à la factorielle de $2x-1$ ; le développement du produit infini $(2x-1)(2x-2)(2x-3)...$ fait intervenir des puissances de 2 et des produits de $k$ entiers pris parmi $n$, ces produits pouvant être retrouvés par une fonction que l'on définira dans la section suivante.
Par exemple, $(2x-1)(2x-2)(2x-3)$ se développe en $8x^3-24x^2+22x-6)$ où $8=2^3$, $24=2^2*6$, $22=2^1*11$ et $6=3!$. Le 6 est la somme des 3 premiers entiers (6=1+2+3). Le 11 est la somme des produits de 2 parmi les 3 premiers entiers ($11=1*2+1*3+2*3$). 3! est le produit des 3 premiers entiers. Les symétries-miroir doivent pouvoir être retrouvées dans la formule de récurrence.

# 8 La géométrie des nombres de Minkowski

La géométrie des nombres est un domaine créé par Minkowski, et dont on peut lire une description sommaire dans l'article “le théorème de Noël” du livre l”'Univers des Nombres” de Ian Stewart. Ce domaine a permis d'obtenir des démonstrations esthétiques : l'article présente celle du fait qu'un nombre pre-

mier de la forme $4n + 1$ est toujours somme de deux carrés.
En suivant cette leçon, on peut “dessiner des lignes” dans les tables de congruence de la façon suivante :

| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 3 | 1 | 0 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 4 | 0 | 1 | 0 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 5 | 1 | 2 | 1 | 0 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 6 | 0 | 0 | 2 | 1 | 0 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 7 | 1 | 1 | 3 | 2 | 1 | 0 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 |
| 8 | 0 | 2 | 0 | 3 | 2 | 1 | 0 | 8 | 8 | 8 | 8 | 8 | 8 | 8 |
| 9 | 1 | 0 | 1 | 4 | 3 | 2 | 1 | 0 | 9 | 9 | 9 | 9 | 9 | 9 |
| 10 | 0 | 1 | 2 | 0 | 4 | 3 | 2 | 1 | 0 | 10 | 10 | 10 | 10 | 10 |
| 11 | 1 | 2 | 3 | 1 | 5 | 4 | 3 | 2 | 1 | 0 | 11 | 11 | 11 | 11 |
| 12 | 0 | 0 | 0 | 2 | 0 | 5 | 4 | 3 | 2 | 1 | 0 | 12 | 12 | 12 |
| 13 | 1 | 1 | 1 | 3 | 1 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 13 | 13 |
| 14 | 0 | 2 | 2 | 4 | 2 | 0 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 14 |
| 15 | 1 | 0 | 3 | 0 | 3 | 1 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 16 | 0 | 1 | 0 | 1 | 4 | 2 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 17 | 1 | 2 | 1 | 2 | 5 | 3 | 1 | 8 | 7 | 6 | 5 | 4 | 3 | 2 |
| 18 | 0 | 0 | 2 | 3 | 0 | 4 | 2 | 0 | 8 | 7 | 6 | 5 | 4 | 3 |
| 19 | 1 | 1 | 3 | 4 | 1 | 5 | 3 | 1 | 9 | 8 | 7 | 6 | 5 | 4 |
| 20 | 0 | 2 | 0 | 0 | 2 | 6 | 4 | 2 | 0 | 9 | 8 | 7 | 6 | 5 |
| 21 | 1 | 0 | 1 | 1 | 3 | 0 | 5 | 3 | 1 | 10 | 9 | 8 | 7 | 6 |
| 22 | 0 | 1 | 2 | 2 | 4 | 1 | 6 | 4 | 2 | 0 | 10 | 9 | 8 | 7 |
| 23 | 1 | 2 | 3 | 3 | 5 | 2 | 7 | 5 | 3 | 1 | 11 | 10 | 9 | 8 |
| 24 | 0 | 0 | 0 | 4 | 0 | 3 | 0 | 6 | 4 | 2 | 0 | 11 | 10 | 9 |
| 25 | 1 | 1 | 1 | 0 | 1 | 4 | 1 | 5 | 7 | 3 | 1 | 12 | 11 | 10 |
| 26 | 0 | 2 | 2 | 1 | 2 | 5 | 2 | 8 | 6 | 4 | 2 | 0 | 12 | 11 |
| 27 | 1 | 0 | 3 | 2 | 3 | 6 | 3 | 0 | 7 | 5 | 3 | 1 | 13 | 12 |
| 28 | 0 | 1 | 0 | 3 | 4 | 0 | 4 | 1 | 8 | 6 | 4 | 2 | 0 | 13 |
| 29 | 1 | 2 | 1 | 4 | 5 | 1 | 5 | 2 | 9 | 7 | 5 | 3 | 1 | 14 |
| 30 | 0 | 0 | 2 | 0 | 0 | 2 | 6 | 3 | 0 | 8 | 6 | 4 | 2 | 0 |

Les “équations” des différents segments de droites sont (si l'on considère que les éléments de la colonne $i$ ont pour abscisse $i-2$):

$y = 0\ ;\ 1 \leq x \leq 26\ ;\ x \equiv 0\ (mod\ 2)$ (*segment de droite vertical rouge*)
$y = 1\ ;\ 1 \leq x \leq 21\ ;\ x \equiv 0\ (mod\ 3)$ (*segment de droite vertical jaune*)
$y = 2\ ;\ 1 \leq x \leq 14\ ;\ x \equiv 2\ (mod\ 4)$ (*segment de droite vertical bleu*)
$y = 3\ ;\ 1 \leq x \leq 5\ ;\ x \equiv 0\ (mod\ 5)$ (*point de cordonnées* $(5,5)$)

$y = (26-x)/2\ ;\ 1 \leq x \leq 26$ (*segment de droite oblique rouge*)
$y = (24-x)/3\ ;\ 1 \leq x \leq 21$ (*segment de droite oblique jaune*)
$y = (22-x)/4\ ;\ 1 \leq x \leq 14$ (*segment de droite oblique bleu*)
$y = (20-x)/5\ ;\ 1 \leq x \leq 5$ (*point de coordonnées* $(5,5)$)

Quand on cherche un décomposant Goldbach de $2x$, on cherche une droite d'équation $x = p$ avec $p$ nombre premier impair inférieur à $x$ qui ne contienne aucun des nombres colorés. Tout d'abord, on constate qu'on peut négliger les colonnes des nombres composés (et les équations correspondantes), celles-ci étant redondantes avec les colonnes des nombres premiers les factorisant. D'autre part, les équations des droites obliques de la forme $y = (k-x)/q$ sont aussi redondantes avec les autres : si une droite ne contient aucun élément coloré à gauche de $\sqrt{2x}$, elle ne peut en contenir non plus à droite de $\sqrt{2x}$ puisqu'on a vu que les cases colorées vont deux par deux, l'une à gauche et l'autre à droite de la colonne $\sqrt{2x}$. De plus quand on essaie de résoudre le système de deux équations contenant l'équation d'une droite horizontale et l'équation d'une droite oblique, on ne peut jamais obtenir une solution entière pour $y$.

Démontrer la conjecture revient donc à démontrer qu'il existe toujours un nombre premier $p$ incongru à $2x$ selon chacun des nombres premiers inférieurs à $\sqrt{2x}$. En ce qui concerne notre exemple consistant à trouver les décompositions Goldbach de 30, les droites définies par les équations $x = 7$, $x = 11$ ou bien encore $x = 13$ sont solutions.

# 9 Equations rationnelles de droites affines dont on cherche des solutions entières

Dans la section précédente, nous avons fourni les équations qui permettent de trouver les décomposants Goldbach d'un nombre. Il s'agit d'équations dont les coefficients sont rationnels, mais dont on va ici chercher des solutions entières. On ne va s'intéresser qu'aux équations des droites qu'on a dites “obliques” au paragraphe précédent.

Nous avons vu que si $2a$ est un nombre pair donné et si $p$ est un nombre premier impair inférieur à $a$, et si quelque soit $i$ entier inférieur à $\frac{2a}{3}$, on a $\frac{2a-2i-p}{i}$ qui est non entier, alors $p$ est décomposant Goldbach de $2a$ ($2a-p$ est premier aussi).

Au contraire, si $2a$ est un nombre pair donné et si $p$ est un nombre premier impair inférieur à $a$ et s'il existe un entier $i$ inférieur à $\frac{2a}{3}$ tel que $\frac{2a-2i-p}{i}$

n'est pas un entier, alors $p$ n'est pas décomposant Goldbach de $2a$ ($2a - p$ est composé).

Montrons cela sur un exemple : soit à décomposer 48. Les nombres premiers susceptibles de fournir des décompositions Goldbach de 48 (inférieurs à 24) sont 3, 5, 7, 11, 13, 17, 19 et 23.
Les équations affines rationnelles des droites obliques dont on va chercher des solutions entières sont :

$$eq1 : y = \frac{44 - x}{2}$$

$$eq2 : y = \frac{42 - x}{3}$$

$$eq3 : y = \frac{40 - x}{4}$$

$$eq4 : y = \frac{38 - x}{5}$$

$$eq5 : y = \frac{36 - x}{6}$$

$$eq6 : y = \frac{34 - x}{7}$$

Résumons dans le tableau suivant le fait qu'$y$ est entier suivant les valeurs de $x$ fournies par l'entête de chaque ligne, un $V$ dans la case signifiant qu'$y$ est entier tandis qu'un $F$ signifie qu'il ne l'est pas. On voit ainsi que 3, 13 et 23 ne permettent d'obtenir de décompositions Goldbach de 48 tandis que les 5 autres nombres premiers le permettent.

| | $eq1$ | $eq2$ | $eq3$ | $eq4$ | $eq5$ | $eq6$ |
|---|---|---|---|---|---|---|
| 3 | $F$ | $V$ | $F$ | $V$ | $F$ | $F$ |
| 5 | $F$ | $F$ | $F$ | $F$ | $F$ | $F$ |
| 7 | $F$ | $F$ | $F$ | $F$ | $F$ | $F$ |
| 11 | $F$ | $F$ | $F$ | $F$ | $F$ | $F$ |
| 13 | $F$ | $F$ | $F$ | $V$ | $F$ | $V$ |
| 17 | $F$ | $F$ | $F$ | $F$ | $F$ | $F$ |
| 19 | $F$ | $F$ | $F$ | $F$ | $F$ | $F$ |
| 23 | $F$ | $F$ | $F$ | $V$ | $F$ | $F$ |

# 10 Conjecture des nombres premiers jumeaux

La conjecture de Goldbach et la conjecture des nombres premiers jumeaux sont liées[5]. Parmi les nombres de 6 à 100, il y a 6 nombres $2x$ qui ont pour décomposition Goldbach $(x - 1) + (x + 1)$ avec $x - 1$ et $x + 1$ deux nombres premiers jumeaux. Ce sont les nombres 8 (=3+5), 12 (=5+7), 24 (=11+13), 36 (=17+19), 60 (=29+31) et 84 (=41+43). Cela est dû au fait que les suites de fractions rationnelles correspondant à chacun ne contiennent jamais d'entiers

[5]Elles font toutes deux partie du huitième problème de Hilbert qui concerne la démonstration de l'Hypothèse de Riemann.

(pour 60 par exemple, il s'agit de la suite de fractions 27/2, 25/3, 23/4, 21/5) mais il faudra aller un peu plus avant tout de même pour être assuré de l'infinité...

# 11 Raisonner probabilistiquement

## 11.1 Congruences

Un nombre a une chance sur deux d'être divisible par 2, une chance sur 3 d'être divisible par 3, une chance sur $n$ d'être divisible par $n$.
Combien de chances un nombre a-t-il d'être divisible soit par 2 soit par 3 ?
Les probabilités concernant la divisibilité par 2 ou par 3 sont indépendantes l'une de l'autre. On appellera "addition disjointe" l'opération définie par

$$x \oplus y = x + y - xy$$

qui va nous permettre de calculer la possibilité pour un nombre d'être divisible soit par 2 soit par 3.

$$\frac{1}{2} \oplus \frac{1}{3} = \frac{1}{2} + \frac{1}{3} - \frac{1}{6} = \frac{4}{6}$$

Effectivement, de 1 à 6, il y a 4 nombres divisibles par 2 ou par 3 (2, 4 et 6 le sont par 2 et 3 et 6 le sont par 3).

L'intérêt de cette "addition disjointe" est qu'elle permet d'obtenir directement les résultats de fastidieux calculs faisant appel à des résultats combinatoires (produit de 2 nombres parmi n, de 3 nombres parmi n, etc) à cause de la propriété d'associativité.

$$\begin{aligned}((a \oplus b) \oplus c) \oplus d &= ((a + b - ab) \oplus c) \oplus d \\ &= ((a + b - ab) + c - (a + b - ab)c) \oplus d \\ &= (a + b - ab + c - ac - bc + abc) \oplus d \\ &= a + b + c + d - ab - ac - ad - bc - bd - cd + abc + abd + acd + bcd - abcd\end{aligned}$$

## 11.2 Incongruités (!)

Essayons d'étendre notre raisonnement aux problèmes d'incongruences vus plus haut.
Probabilistiquement, un nombre a une chance sur deux d'être pair ou impair.
Puisqu'il a une chance sur trois d'être *congru* à 0 ou 1 ou 2 modulo 3, il a deux chances sur trois d'être *incongru* à 0 ou 1 ou 2 modulo 3 (complémentaire d'1/3 à 1).
On utilise à nouveau l'"addition disjointe".
Avec les nombres premiers 2 et 3, l'utilisation de cette opération fournit le calcul suivant :

$$\frac{1}{2} \oplus \frac{2}{3} = \frac{1}{2} + \frac{2}{3} - \frac{2}{6} = \frac{5}{6}$$

On voit qu'un nombre a 5/6 chances d'être soit incongru à un nombre modulo 2 soit incongru à un nombre modulo 3.
Il a donc probabilistiquement seulement 1 chance sur 6 de vérifier simultanément

deux conditions de congruence l'une modulo 2 et l'autre modulo 3.

Avec les nombres premiers 2, 3, et 5,

$$\frac{5}{6} \oplus \frac{4}{5} = \frac{5}{6} + \frac{4}{5} - \frac{20}{30} = \frac{29}{30}$$

On déduit que les probabilités successives vont être 209/210, 2309/2310, 30029/30030, etc. Les dénominateurs sont les produits d'un nombre de plus en plus grand de nombres premiers successifs, et les numérateurs sont égaux aux dénominateurs auxquels on a soustrait 1. Cette suite de nombres tend très vite vers 1 sans jamais l'atteindre.

## 12 Résumé de la démonstration

Considérons une table de congruence de taille $2x$ sur $x-1$ (dont les lignes sont numérotées de 1 à $2x$ et les colonnes sont numérotées de 2 à $x$). Colorons dans cette table d'une part les cases (i,j) telles que $i \equiv 0 \ (mod\ j)$ et d'autre part les cases (i,j) telles que $i \equiv 2x \ (mod\ j)$. Il existe dans la partie supérieure de cette table une ligne d'un nombre $p$ qui contient comme seule case colorée un zéro dans sa diagonale (contraposée du théorème de Tchebychev). Ne contenant qu'un zéro sur sa diagonale, c'est la ligne d'un nombre premier. A cause de la propriété de symétrie-miroir entre les cases colorées autour de la ligne $x$, la ligne symétrique de cette ligne (ligne de $2x-p$) ne contient pas non plus de case colorée avant sa diagonale. En particulier, puisqu'on a coloré tous les zéros de la table, elle ne contient aucun zéro. C'est donc la ligne d'un nombre premier. CQFD.

## 13 Conclusion

On peut donc désormais utiliser la formulation *"tout entier naturel supérieur à 2 est la moyenne arithmétique de deux nombres premiers"*. Concluons par deux citations d'Hilbert : *"Nous devons savoir et nous saurons ; il n'y a pas d'ignorabimus en mathématiques"* et puis un conseil qu'il donne à Klein : *"Il vous faut avoir un problème. Choisissez un objectif déterminé et marchez franchement vers lui. Vous pouvez ne jamais atteindre le but mais vous trouverez sûrement quelque chose d'intéressant en chemin"*. En mathématiques, il faut garder l'âme d'un *epsilon*[6] qui s'émerveille...

## Bibliographie


M. Aigner, G.M. Ziegler. *Raisonnements divins*. Éd. Springer, 2002.

F. Casiro. *La conjecture de Goldbach, un défi en or*. Éd. Tangente n°78, décembre 2000, janvier 2001.

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


[6] C'est ainsi qu'Erdös désignait les enfants.

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.

C.F. Gauss. *Recherches arithmétiques.* 1807. Éd. Jacques Gabay, 1989.

J. Hadamard. *Essai sur la psychologie de l'invention mathématique suivi de H. Poincaré, l'invention mathématique.* Éd. Jacques Gabay, 1959.

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

O. Kerléguer, D. Dumont. *Des images pour les nombres.* Éd. ACL du Kangourou, 2001.

D. Nordon. *Les obstinations d'un mathématicien.* Éd. Belin Pour la Science, 2003.

A. Sainte Laguë. *Avec des nombres et des lignes.* Éd. Vuibert, 1937.

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

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

A. Warusfel. *Les nombres et leurs mystères.* Éd. Points Sciences, 1961.

## Annexe 1 : l'article d'Euler auquel il a été fait référence

L'article d'Euler "Découverte d'une loi toute extraordinaire des nombres par rapport à la somme de leurs diviseurs peut être trouvé au format *pdf* dans la page http://math-doc.ujf-grenoble.fr/OEUVRES/

## Annexe 2 : programme de calcul de la somme des diviseurs des entiers successifs par la méthode récurrente d'Euler

```
#include <iostream>
#include <cmath>

const int taille = 100;
int a[taille];
int h[taille];
int euler[taille];

int f(int x) { return (3 * x * x - x) / 2 ; }

int g(int x) { return (3 * x * x + x) / 2 ; }

int fh(){
    int i, y, z;

    for (i = 1 ; i < taille ; i++)
        if (i % 2 == 0) {
```

```
            y = i / 2 ;
            z = f(y) ;
            h[i] = z ; }
        else {
            y = (i-1) / 2 ;
            z = g(y) ;
            h[i] = z ; } }

int fa(){
    int i;

    for (i = 1 ; i < taille ; i++)
        if (i % 4 == 1) a[i] = 1 ;
        else if (i % 4 == 2) a[i] = 1 ;
        else if (i % 4 == 0) a[i] = -1 ;
        else if (i % 4 == 3) a[i] = -1 ; }

int calcule(){
    int x, y, somme;

    euler[0] = 1 ;
    euler[1] = 1 ;
    for (x = 1 ; x < taille ; x++) {
        somme = 0 ;
        y = 1 ;
        while (x - h[y+1] >= 0)
            if (x == h[y+1])
                somme = somme + a[y] * x;
            else
                somme = somme + a[y] * euler[x - h[y+1]];
                y++ ;}
        euler[x] = somme ;}}

int main (int argc, char* argv[]){
    int i, x;

    fa();
    fh();
    calcule();
    for (i = 1 ; i < taille ; i++)
        std::cout << " " << euler[i];}
```

# Une nouvelle vision des nombres premiers

Denise Vella

Janvier 2007

## 1 Introduction

Dans cette note, nous présentons une nouvelle façon de considérer la primarité, basée sur des découvertes associant les tables de congruence de Gauss, la géométrie des nombres de Minkowski, et les considérations de Cantor.

## 2 Les Recherches arithmétiques de Gauss

Gauss est à l'origine de l'arithmétique modulaire. Ses *Disquisitiones Arithmeticae* sont agréables à lire car l'auteur y est pédagogue pour expliquer à la lectrice ses découvertes et résultats. Il y présente la notion de congruence, qui est une relation d'équivalence, et que nous utilisons naturellement dès qu'on nous apprend la division avec reste[1].
Dans la section suivante, nous utiliserons une table de congruence. Chaque case $(i, j)$ d'une telle table contient $i \ mod \ j$, c'est à dire le nombre $k$ tel que $i \equiv k \ (mod \ j)$

## 3 Trouver des équations de droites dans une table de congruence

La géométrie des nombres est un domaine créé par Minkowski, et dont on peut lire une description sommaire dans l'article *le théorème de Noël* du livre l'*Univers des Nombres* de Ian Stewart. Ce domaine a permis d'obtenir des démonstrations esthétiques : l'article présente celle du fait qu'un nombre premier de la forme $4n + 1$ est toujours somme de deux carrés.
En suivant cette leçon, on peut colorier les cases d'une table de congruence contenant des zéros qui exprime la divisibilité tout en repérant le fait que ces zéros se trouvent appartenir à des droites affines dont on va rechercher les équations :

[1]Bizarrement, le paragraphe 34 des Recherches Arithmétiques est noté 43 dans l'édition Jacques Gabay. On imagine mal Gauss se trompant dans l'écriture d'un nombre à deux chiffres. Le "prince des mathématiques" avait sûrement vu toutes les symétries-miroir des tables de congruence que nous venons tout juste de découvrir et que nous avons présentées dans une note *Conjecture de Goldbach et propriétés de symétrie-miroir d'une table de congruence* et l'a peut-être indiqué par un clin d'oeil en inversant les deux chiffres ; ou bien c'est tout simplement une erreur dactylographique...

| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 3 | 1 | 0 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 4 | 0 | 1 | 0 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 5 | 1 | 2 | 1 | 0 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 6 | 0 | 0 | 2 | 1 | 0 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 7 | 1 | 1 | 3 | 2 | 1 | 0 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 |
| 8 | 0 | 2 | 0 | 3 | 2 | 1 | 0 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 |
| 9 | 1 | 0 | 1 | 4 | 3 | 2 | 1 | 0 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 |
| 10 | 0 | 1 | 2 | 0 | 4 | 3 | 2 | 1 | 0 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| 11 | 1 | 2 | 3 | 1 | 5 | 4 | 3 | 2 | 1 | 0 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 |
| 12 | 0 | 0 | 0 | 2 | 0 | 5 | 4 | 3 | 2 | 1 | 0 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 |
| 13 | 1 | 1 | 1 | 3 | 1 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 13 | 13 | 13 | 13 | 13 | 13 | 13 |
| 14 | 0 | 2 | 2 | 4 | 2 | 0 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 14 | 14 | 14 | 14 | 14 | 14 |
| 15 | 1 | 0 | 3 | 0 | 3 | 1 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 15 | 15 | 15 | 15 | 15 |
| 16 | 0 | 1 | 0 | 1 | 4 | 2 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 16 | 16 | 16 | 16 |
| 17 | 1 | 2 | 1 | 2 | 5 | 3 | 1 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 17 | 17 | 17 |
| 18 | 0 | 0 | 2 | 3 | 0 | 4 | 2 | 0 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 18 | 18 |
| 19 | 1 | 1 | 3 | 4 | 1 | 5 | 3 | 1 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 19 |
| 20 | 0 | 2 | 0 | 0 | 2 | 6 | 4 | 2 | 0 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

Dans cette table, la divisibilité de tout nombre par lui-même est coloriée en cyan, la divisibilité de tout nombre par sa moitié est coloriée en rouge, la divisibilité de tout nombre par son tiers en jaune, par son quart en vert, par son cinquième en bleu, par son sixième en magenta, par son septième en orange, par son huitième en bleu-turquoise, par son neuvième en gris, par son dixième en marron.

Trouvons les équations des droites de chaque couleur. Pour ça, considérons un repère cartésien : l'axe des abscisses (x) correspond à la ligne verticale des en-têtes de lignes orienté de telle façon que $+\infty$ soit en bas de la page, l'abscisse d'une case est l'en-tête de sa ligne ; l'axe des ordonnées (y) correspond à la ligne horizontale des en-têtes de colonnes si ce n'est qu'on va considérer que les cases de la colonne $i$ ont pour ordonnée $i-2$ (pour s'approcher du $\frac{1}{2}$ de l'Hypothèse de Riemann). On n'a pas de risque à faire ce changement d'ordonnée car si on ajoute ou soustrait 2 à un entier, on obtient un entier tandis que si on ajoute ou soustrait 2 à une fraction rationnelle non entière, on obtient une fraction rationnelle non entière.
L'équation de la droite rouge est (divisibilité d'un nombre par sa moitié) :

$$x = 2y + 4.$$

L'équation de la droite jaune (divisibilité d'un nombre par son tiers) :

$$x = 3y + 6.$$

Plus généralement, l'équation de la i-ème droite (divisibilité d'un nombre par son i-ème) est

$$x = iy + 2i.$$

# 4 Primarité

A chaque nombre $n$ est associé une droite d'équation $x = n$. Les équations de droite vont permettre de distinguer les nombres premiers des nombres composés mais pas tout à fait de la façon à laquelle on s'était habitué. Considérons le nombre 9.
Existe-t-il un $x$ entier tel que $9 = 2x + 4$ ? Non, car $x = \frac{5}{2}$ est une fraction rationnelle non entière.
Existe-t-il un $x$ entier tel que $9 = 3x + 6$ ? Oui, car $x = \frac{3}{3}$ est une fraction rationnelle entière.
Existe-t-il un $x$ entier tel que $9 = 4x + 8$ ? Non, car $x = \frac{1}{4}$ est une fraction rationnelle non entière.
A cause de la réponse *oui* à la deuxième question, 9 n'est pas un nombre premier. Considérons le nombre 17.
Existe-t-il un $x$ entier tel que $17 = 2x + 4$ ? Non, car $x = \frac{13}{2}$ est une fraction rationnelle non entière.
Existe-t-il un $x$ entier tel que $17 = 3x + 6$ ? Non, car $x = \frac{11}{3}$ est une fraction rationnelle non entière.
Existe-t-il un $x$ entier tel que $17 = 4x + 8$ ? Non, car $x = \frac{9}{4}$ est une fraction rationnelle non entière.
Existe-t-il un $x$ entier tel que $17 = 5x + 10$ ? Non, car $x = \frac{7}{5}$ est une fraction rationnelle non entière.
Existe-t-il un $x$ entier tel que $17 = 6x + 12$ ? Non, car $x = \frac{5}{6}$ est une fraction rationnelle non entière.
Existe-t-il un $x$ entier tel que $17 = 7x + 14$ ? Non, car $x = \frac{3}{7}$ est une fraction rationnelle non entière.
Existe-t-il un $x$ entier tel que $17 = 8x + 16$ ? Non, car $x = \frac{1}{8}$ est une fraction rationnelle non entière.
Donc 17 est premier. En généralisant, on voit qu'il s'agit d'associer à un nombre impair $p$ (les nombres pairs n'étant trivialement pas premiers) un ensemble de $\frac{p-3}{2}$ fractions rationnelles dont le numérateur est un nombre impair variant de 1 à $p - 4$ et le dénominateur est un entier variant de $\frac{p-1}{2}$ à 2.

En annexe, est fournie une table qui fournit pour chaque nombre de 9 à 45 les fractions rationnelles qui doivent lui être associées. On voit que dans l'ensemble associé à un entier impair, toute fraction rationnelle dont le dénominateur est un diviseur de ce nombre est entière.

Il en résulte une nouvelle caractérisation des nombres premiers qui est :

$$p \textit{ premier} \iff \forall\, i,\ 1 \leq i \leq \frac{p-3}{2},\ \frac{4i+2}{p-2i-1} \notin \mathbb{N}$$

On peut encore améliorer cette caractérisation car si le numérateur d'une fraction est strictement inférieur à son dénominateur, elle ne peut être entière, ce

qui est le cas dès que $i < \lceil \frac{p-3}{6} \rceil$ On se restreint donc finalement à la caractérisation suivante :

$$p\ premier \iff \forall\, i,\ \left\lceil \frac{p-3}{6} \right\rceil \leq i \leq \frac{p-3}{2},\ \frac{4i+2}{p-2i-1} \notin \mathbb{N}$$

Tout nombre impair peut donc être considéré comme établissant une correspondance biunivoque entre les entiers impairs croissant et les entiers tout court décroissants jusqu'à 2. Si cette correspondance ne donne lieu qu'à des fractions rationnelles non entières, le nombre est premier. Il est composé dans le cas contraire. Cette façon de voir les choses aurait peut-être intéressé Cantor, qui a travaillé sur la conjecture de Goldbach en 1894, en présentant une table des décompositions des nombres pairs de 6 à 1000 sous la forme de deux nombres premiers au congrès de l'AFAS.

# 5 Conjecture de Goldbach et Conjecture des nombres premiers jumeaux

La conjecture de Goldbach et la conjecture des nombres premiers jumeaux sont liées dans la mesure où elles font toutes deux partie du huitième problème de Hilbert qui concerne la démonstration de l'Hypothèse de Riemann. Une première conséquence de la nouvelle façon de considérer la primarité est qu'elle nous permet d'obtenir une formule qui permet de trouver les décomposants Goldbach d'un nombre pair et qui se note (on a laissé $prime(i)$ pour alléger l'énoncé, mais on comprend aisément qu'on peut remplacer aussi cette condition par la condition sur fractions rationnelles correspondante :

$$\begin{aligned} Goldbach(2a,i,j) \iff\ & 3 \leq i \leq a \\ & \wedge\ prime(i) \\ & \wedge\ \forall\, j,\ 2 \leq j \leq a \Rightarrow \frac{2a-2j-i}{j} \notin \mathbb{N} \end{aligned}$$

La deuxième conséquence de la nouvelle vision est que si l'union d'ensembles dépendante du nombre $p$ impair ci-dessous ne contient que des fractions rationnelles non entières, alors $p$ et $p+2$ sont des nombres premiers jumeaux.

$$\left\{ \frac{p-2}{2} \right\} \cup \bigcup_{\substack{j\ impair \\ 1 \leq j \leq p-4}} \left\{ \frac{2j}{p-j},\ \frac{2j}{p-j+2} \right\}$$

Les programmes de vérification en C++ qui permettent de vérifier que ces équations rationnelles ont bien comme solutions entières soit des nombres premiers, soit les décomposants Goldbach d'un nombre pair donné, soit les nombres premiers jumeaux peuvent être trouvés à l'adresse *http://denise.vella.chemla.free.fr*, dans l'onglet *Des notes et puis un jour l'Harmonie.*

# 6 Les preuves élémentaires d'Erdös

Erdös a été le mathématicien voyageur. La lecture de sa biographie le rend éminemment sympathique, il était très spirituel. Surtout, Erdös cherchait les

Preuves du Livre, il abordait les mathématiques artistiquement, il était en quête de démonstrations qui soient également esthétiques. Il paraît qu'il abordait les mathématiciens, du plus au moins connu, en leur disant : *"Mon cerveau est ouvert. Avez-vous un problème ?"*.
Le livre "Raisonnements divins" d'Aigner et Ziegler fournit la preuve élémentaire d'Erdös du théorème de Tchebychev. Il fournit aussi sa preuve, élémentaire également, de l'infinitude des nombres premiers. Ces preuves sont dites élémentaires car elles ne nécessitent pas l'utilisation d'outils de l'analyse complexe. Erdös a aussi prouvé avec Selberg le théorème des nombres premiers, à nouveau par une méthode élémentaire. Terminons ce paragraphe par une citation d'Erdös : *"Je sais que les nombres sont beaux. S'ils ne le sont pas, rien ne l'est."*.

# 7 Conclusion

On peut peut-être désormais utiliser la formulation *"tout entier naturel supérieur à 2 est la moyenne arithmétique de deux nombres premiers"*. Concluons par deux citations d'Hilbert : *"Nous devons savoir et nous saurons ; il n'y a pas d'ignorabimus en mathématiques"* et puis un conseil qu'il donne à Klein : *"Il vous faut avoir un problème. Choisissez un objectif déterminé et marchez franchement vers lui. Vous pouvez ne jamais atteindre le but mais vous trouverez sûrement quelque chose d'intéressant en chemin*". En mathématiques, il faut garder l'âme d'un *epsilon*[2] qui s'émerveille...

# Bibliographie


M. Aigner, G.M. Ziegler. *Raisonnements divins.* Éd. Springer, 2002.

F. Casiro. *La conjecture de Goldbach, un défi en or.* Éd. Tangente n°78, décembre 2000, janvier 2001.

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

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.

C.F. Gauss. *Recherches arithmétiques.* 1807. Éd. Jacques Gabay, 1989.

J. Hadamard. *Essai sur la psychologie de l'invention mathématique suivi de H. Poincaré, l'invention mathématique.* Éd. Jacques Gabay, 1959.

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

O. Kerléguer, D. Dumont. *Des images pour les nombres.* Éd. ACL du Kangourou, 2001.

D. Nordon. *Les obstinations d'un mathématicien.* Éd. Belin Pour la Science, 2003.

A. Sainte Laguë. *Avec des nombres et des lignes.* Éd. Vuibert, 1937.

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

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


[2] C'est ainsi qu'Erdös désignait les enfants.

A. Warusfel. *Les nombres et leurs mystères*. Éd. Points Sciences, 1961.

## Annexe 1 : un article merveilleux d'Euler

L'article d'Euler "Découverte d'une loi toute extraordinaire des nombres par rapport à la somme de leurs diviseurs peut être trouvé au format *pdf* dans la page http://math-doc.ujf-grenoble.fr/OEUVRES/

## Annexe 2 : association de fractions rationnelles aux nombres de 9 à 45

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 9 | $\frac{1}{4}$ | $\frac{3}{3}$ | $\frac{5}{2}$ | | | | | | | | | | |
| 11 | $\frac{1}{5}$ | $\frac{3}{4}$ | $\frac{5}{3}$ | $\frac{7}{2}$ | | | | | | | | | |
| 13 | $\frac{1}{6}$ | $\frac{3}{5}$ | $\frac{5}{4}$ | $\frac{7}{3}$ | $\frac{9}{2}$ | | | | | | | | |
| 15 | $\frac{1}{7}$ | $\frac{3}{6}$ | $\frac{5}{5}$ | $\frac{7}{4}$ | $\frac{9}{3}$ | $\frac{11}{2}$ | | | | | | | |
| 17 | $\frac{1}{8}$ | $\frac{3}{7}$ | $\frac{5}{6}$ | $\frac{7}{5}$ | $\frac{9}{4}$ | $\frac{11}{3}$ | $\frac{13}{2}$ | | | | | | |
| 19 | $\frac{1}{9}$ | $\frac{3}{8}$ | $\frac{5}{7}$ | $\frac{7}{6}$ | $\frac{9}{5}$ | $\frac{11}{4}$ | $\frac{13}{3}$ | $\frac{15}{2}$ | | | | | |
| 21 | $\frac{1}{10}$ | $\frac{3}{9}$ | $\frac{5}{8}$ | $\frac{7}{7}$ | $\frac{9}{6}$ | $\frac{11}{5}$ | $\frac{13}{4}$ | $\frac{15}{3}$ | $\frac{17}{2}$ | | | | |
| 23 | $\frac{1}{11}$ | $\frac{3}{10}$ | $\frac{5}{9}$ | $\frac{7}{8}$ | $\frac{9}{7}$ | $\frac{11}{6}$ | $\frac{13}{5}$ | $\frac{15}{4}$ | $\frac{17}{3}$ | $\frac{19}{2}$ | | | |
| 25 | $\frac{1}{12}$ | $\frac{3}{11}$ | $\frac{5}{10}$ | $\frac{7}{9}$ | $\frac{9}{8}$ | $\frac{11}{7}$ | $\frac{13}{6}$ | $\frac{15}{5}$ | $\frac{17}{4}$ | $\frac{19}{3}$ | $\frac{21}{2}$ | | |
| 27 | $\frac{1}{13}$ | $\frac{3}{12}$ | $\frac{5}{11}$ | $\frac{7}{10}$ | $\frac{9}{9}$ | $\frac{11}{8}$ | $\frac{13}{7}$ | $\frac{15}{6}$ | $\frac{17}{5}$ | $\frac{19}{4}$ | $\frac{21}{3}$ | $\frac{23}{2}$ | |
| 29 | $\frac{1}{14}$ | $\frac{3}{13}$ | $\frac{5}{12}$ | $\frac{7}{11}$ | $\frac{9}{10}$ | $\frac{11}{9}$ | $\frac{13}{8}$ | $\frac{15}{7}$ | $\frac{17}{6}$ | $\frac{19}{5}$ | $\frac{21}{4}$ | $\frac{23}{3}$ | $\frac{25}{2}$ |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 31 | $\frac{1}{15}$ | $\frac{3}{14}$ | $\frac{5}{13}$ | $\frac{7}{12}$ | $\frac{9}{11}$ | $\frac{11}{10}$ | $\frac{13}{9}$ | $\frac{15}{8}$ | $\frac{17}{7}$ | $\frac{19}{6}$ | $\frac{21}{5}$ | $\frac{23}{4}$ | $\frac{25}{3}$ | $\frac{27}{2}$ | |
| 33 | $\frac{1}{16}$ | $\frac{3}{15}$ | $\frac{5}{14}$ | $\frac{7}{13}$ | $\frac{9}{12}$ | $\frac{11}{11}$ | $\frac{13}{10}$ | $\frac{15}{9}$ | $\frac{17}{8}$ | $\frac{19}{7}$ | $\frac{21}{6}$ | $\frac{23}{5}$ | $\frac{25}{4}$ | $\frac{27}{3}$ | $\frac{29}{2}$ |
| 35 | $\frac{1}{17}$ | $\frac{3}{16}$ | $\frac{5}{15}$ | $\frac{7}{14}$ | $\frac{9}{13}$ | $\frac{11}{12}$ | $\frac{13}{11}$ | $\frac{15}{10}$ | $\frac{17}{9}$ | $\frac{19}{8}$ | $\frac{21}{7}$ | $\frac{23}{6}$ | $\frac{25}{5}$ | $\frac{27}{4}$ | $\frac{29}{3}$ |
| | $\frac{31}{2}$ | | | | | | | | | | | | | | |
| 37 | $\frac{1}{18}$ | $\frac{3}{17}$ | $\frac{5}{16}$ | $\frac{7}{15}$ | $\frac{9}{14}$ | $\frac{11}{13}$ | $\frac{13}{12}$ | $\frac{15}{11}$ | $\frac{17}{10}$ | $\frac{19}{9}$ | $\frac{21}{8}$ | $\frac{23}{7}$ | $\frac{25}{6}$ | $\frac{27}{5}$ | $\frac{29}{4}$ |
| | $\frac{31}{3}$ | $\frac{33}{2}$ | | | | | | | | | | | | | |
| 39 | $\frac{1}{19}$ | $\frac{3}{18}$ | $\frac{5}{17}$ | $\frac{7}{16}$ | $\frac{9}{15}$ | $\frac{11}{14}$ | $\frac{13}{13}$ | $\frac{15}{12}$ | $\frac{17}{11}$ | $\frac{19}{10}$ | $\frac{21}{9}$ | $\frac{23}{8}$ | $\frac{25}{7}$ | $\frac{27}{6}$ | $\frac{29}{5}$ |
| | $\frac{31}{4}$ | $\frac{33}{3}$ | $\frac{35}{2}$ | | | | | | | | | | | | |
| 41 | $\frac{1}{20}$ | $\frac{3}{19}$ | $\frac{5}{18}$ | $\frac{7}{17}$ | $\frac{9}{16}$ | $\frac{11}{15}$ | $\frac{13}{14}$ | $\frac{15}{13}$ | $\frac{17}{12}$ | $\frac{19}{11}$ | $\frac{21}{10}$ | $\frac{23}{9}$ | $\frac{25}{8}$ | $\frac{27}{7}$ | $\frac{29}{6}$ |
| | $\frac{31}{5}$ | $\frac{33}{4}$ | $\frac{35}{3}$ | $\frac{37}{2}$ | | | | | | | | | | | |
| 43 | $\frac{1}{21}$ | $\frac{3}{20}$ | $\frac{5}{19}$ | $\frac{7}{18}$ | $\frac{9}{17}$ | $\frac{11}{16}$ | $\frac{13}{15}$ | $\frac{15}{14}$ | $\frac{17}{13}$ | $\frac{19}{12}$ | $\frac{21}{11}$ | $\frac{23}{10}$ | $\frac{25}{9}$ | $\frac{27}{8}$ | $\frac{29}{7}$ |
| | $\frac{31}{6}$ | $\frac{33}{5}$ | $\frac{35}{4}$ | $\frac{37}{3}$ | $\frac{39}{2}$ | | | | | | | | | | |
| 45 | $\frac{1}{22}$ | $\frac{3}{21}$ | $\frac{5}{20}$ | $\frac{7}{19}$ | $\frac{9}{18}$ | $\frac{11}{17}$ | $\frac{13}{16}$ | $\frac{15}{15}$ | $\frac{17}{14}$ | $\frac{19}{13}$ | $\frac{21}{12}$ | $\frac{23}{11}$ | | | |
| | $\frac{25}{10}$ | $\frac{27}{9}$ | $\frac{29}{8}$ | $\frac{31}{7}$ | $\frac{33}{6}$ | $\frac{35}{5}$ | $\frac{37}{4}$ | $\frac{39}{3}$ | $\frac{41}{2}$ | | | | | | |

## Annexe : Citations littéraires

Des citations tirées du livre *La symphonie des nombres premiers* de Marcus du Sautoy.

Henri Poincaré : Le scientifique n'étudie pas la Nature parce qu'elle est utile ; il l'étudie parce qu'elle le réjouit. Et elle le réjouit parce qu'elle est belle. Si la nature n'était pas belle, elle ne vaudrait pas la peine d'être connue, et si la Nature ne valait pas la peine d'être connue, la vie ne vaudrait pas la peine d'être vécue.

Hardy : Je pense que la réalité mathématique existe en dehors de nous, que notre fonction est de la découvrir ou de l'observer et que les théorèmes que nous

démontrons et que nous décrivons avec grandiloquence comme nos créations sont simplement les notes de nos observations.

Gauss a coiffé Legendre sur le poteau au sujet du lien entre les nombres premiers et les logarithmes. Cela nous est révélé dans une lettre de Gauss à Encke, écrite le soir de Noël 1849[3].

Lagrange conseilla au père de Cauchy : Veillez à ce qu'il ne touche pas de livre de mathématiques avant ses 17 ans. Au lieu de cela, il suggéra de stimuler les talents littéraires de l'enfant si bien que, le jour où il reviendrait aux mathématiques, il serait capable de parler de sa propre voix mathématique, non en imitant ce qu'il aurait prélevé dans les ouvrages de l'époque.

Hardy à propos de Ramanujan : il était porteur d'un handicap insurmontable, pauvre hindou solitaire s'attaquant à la sagesse accumulée de l'Europe.

Ramanujan commençait à se dire que la priorité que Hardy accordait à la rigueur mathématique empêchait son esprit de parcourir librement le paysage mathématique.

Julia Robinson : Je souhaitais toujours à chacun de mes anniversaires et d'année en année que le dixième problème de Hilbert soit résolu. Pas par moi, mais simplement qu'il soit résolu. J'avais le sentiment que je ne pourrais accepter de mourir sans connaître la réponse.

Gauss : le problème de distinguer les nombres premiers des nombres composés et de décomposer ceux-ci en leurs facteurs premiers est connu comme un des plus importants et des plus utiles de toute l'Arithmétique. [...] En outre, la dignité de la Science semble demander que l'on recherche avec soin tous les secours nécessaires pour parvenir à la solution d'un problème si élégant et si célèbre.

[3] 157 ans sépare Noel 1849 de Noël 2006. Déduisez-en la primarité de 157 !

# Conjecture de Goldbach et propriétés de symétrie d'une table de congruence

Denise Vella

Janvier 2007

La conjecture de Goldbach énonce que tout nombre pair supérieur à 4 est la somme de deux nombres premiers.
Soit un nombre pair $2a$ dont on cherche à démontrer qu'il vérifie la conjecture de Goldbach. Posons que $a$ n'est pas un nombre premier car les doubles de premiers vérifient trivialement la conjecture.

Pour démontrer la conjecture, on va considérer une table de congruence (dont chaque case $(i, j)$ contient le reste de la division Euclidienne de $i$ par $j$, appelé habituellement $i \ mod \ j$). Les lignes de cette table seront indicées par les nombres de 1 à $2a$, tandis que ses colonnes seront indicées par les nombres de 2 à $a$. Par abus de langage, on pourra parfois dire qu'une case $(i, j)$ est "congrue à $u$" ($u$ pouvant être n'importe quel nombre inférieur à $a-1$) à la place de $i \equiv u \ (mod \ j)$.

Cette table de congruence possède deux propriétés importantes qui sont d'une part une symétrie horizontale que nous noterons $Sym_h$ et une propriété que, par abus de langage, nous appellerons symétrie verticale et que nous noterons $Sym_v$ qui est en fait une mise en correspondance bijective de certaines cases d'une même ligne.

La propriété de symétrie horizontale $Sym_h$ d'une table de congruence s'écrit

$$i \equiv k \ (mod \ j) \Leftrightarrow 2a - i \equiv 2a - k \ (mod \ j)$$

En particulier, pour $k = 0$,

$$(propriété \ Sym_h) \ \ i \equiv 0 \ (mod \ j) \Leftrightarrow 2a - i \equiv 2a \ (mod \ j)$$

La démonstration de la conjecture de Goldbach se décompose en trois étapes.

1) D'abord, il faut démontrer qu' il existe un nombre $p$ inférieur à $\lfloor a/2 \rfloor$ incongru à $2a$ selon tout module compris entre $p$ et $a$.

$$\exists \ p \ ( \ 2 \leq p < \lfloor a/2 \rfloor) \ \wedge \ ( \ \forall \ q \ (p < q \leq a) \ \Rightarrow (p \not\equiv 2a \ (mod \ q)))$$

Supposons le contraire, c'est à dire supposons que :

$$\forall \ p[\neg( \ 2 \leq p < \lfloor a/2 \rfloor) \ \vee \ ( \ \exists \ q \ (p < q \leq a) \ \wedge \ (p \equiv 2a \ (mod \ q)))]$$

Observons les résidus de $2a$ selon les modules compris entre 2 et $a$. D'abord, on a la propriété suivante qui est vérifiée par les diviseurs de $2a$.

$$d \mid 2a \ \Rightarrow \ \exists \ d', \ (d < d' \leq a) \ \wedge \ (2a \equiv d \ (mod \ d'))$$

Les autres relations de congruence que vérifie $2a$ sont :

$$(éq.\ eq_1)\ 2a \ \equiv\ 2\ (mod\ a-1)$$
$$(éq.\ eq_2)\ 2a \ \equiv\ 4\ (mod\ a-2)$$
$$(éq.\ eq_3)\ 2a \ \equiv\ 6\ (mod\ a-3)$$
$$....$$
$$(éq.\ eq_i)\ 2a \ \equiv\ 2i\ (mod\ a-i)$$

Puisque $2a$ vérifie toutes ces relations de congruence (et notamment à cause des congruences à ses diviseurs modulo, pour chacun d'eux $d$, un module $d'$ compris entre $d$ et $a$), il existe des lignes indicées par un nombre $p$ qui ne divise pas $2a$, qui est inférieur à $\lfloor a/2 \rfloor$ et qui est incongru à $2a$ selon tout module compris entre $p$ et $a$ (si ce n'est pour les 3 petits nombres pairs 8, 12 et 18 qui sont trop petits et pour lesquels il n'y a pas assez d'équations de la forme ci-dessus mais ils vérifient la conjecture malgré cela).
Cela s'écrit :

$$\exists\ p\ (2 \leq p < \lfloor a/2 \rfloor)\ \wedge\ (\ \forall\ q\ (p < q \leq a)\ \Rightarrow\ (2a\ \not\equiv\ p\ (mod\ q))).$$

Dit autrement, les nombres inférieurs à $\lfloor a/2 \rfloor$ ne peuvent pas être tous simultanément résidus de $2a$ modulo des nombres qui sont compris entre eux et $a$.

2) Maintenant, il faut montrer qu'il existe une ligne dans l'ensemble de lignes que l'on a identifié ci-dessus qui est la ligne d'un nombre premier inférieur à $\lfloor a/2 \rfloor$.

Pour cela, on va utiliser la propriété que l'on appelle "symétrie verticale" de la table de congruence et qui est en fait une mise en correspondance bijective de certaines cases d'une même ligne de la table. Cette relation lie entre eux les éléments d'un triplet constitué de deux indices de colonnes $i$ et $j$ et d'un indice de ligne $k$ lorsque $2a - k\ =\ i\ \times\ j$.

A cause de cette propriété de "symétrie verticale" $Sym_v$ qui va être explicitée ci-dessous, une ligne d'indice inférieur à $\lfloor a/2 \rfloor$, qui ne contient aucune case de congruence à $2a$ dans sa partie droite, ne peut non plus contenir de telle case de congruence à $2a$ dans sa partie gauche. Cette propriété $Sym_v$ ne s'applique qu'aux lignes d'indices inférieurs à $\lfloor 2a/3 \rfloor$ et donc a fortiori aux lignes d'indices inférieurs à $\lfloor a/2 \rfloor$[1].

$$(propriété\ Sym_v)\ i\ \not\equiv\ 2a\ (mod\ j)\ \Leftrightarrow\ i\ \not\equiv\ 2a\ (mod\ \lfloor (2a-i)/j \rfloor)$$

Dans le premier quart du haut de la table (pour les lignes dont l'indice est compris entre 1 et $\lfloor a/2 \rfloor$), la partie de la ligne qui se trouve à droite de la diagonale de zéros est systématiquement plus longue que la partie de la ligne qui se trouve à gauche de la diagonale de zéros. S'il n'y a aucun élément "congru à 2a" dans la partie droite d'une telle ligne, il n'y aura par la propriété de mise en correspondance $Sym_v$ aucun élément congru à $2a$ dans la partie gauche de la ligne et donc la ligne dans son entier ne contiendra aucun élément congru à $2a$.

[1]Il est à noter que cette propriété se retrouve en partie "haute" de la table pour les lignes d'indices compris entre $\lfloor 4a/3 \rfloor$ et $2a$ mais la mise en correspondance que l'on observe alors concerne les cases touchées par une congruence à 0.

Pour que cette ligne d'indice $i$ inférieur à $a$ soit la ligne d'un nombre premier, il faut également que les contenus des cases situées à gauche de la diagonale de 0, en plus d'être incongrus à $2a$, soient non nuls. Cette ligne contient un 1 dans la colonne du nombre premier 2. Elle contient également un nombre non nul dans toutes les colonnes des diviseurs de $2a$ car dans ces colonnes, pour les lignes d'indices inférieurs à $\lfloor 2a/3 \rfloor$, seuls les éléments des lignes dont l'indice $i$ est tel que $PGCD(i, 2a) > 1$ peuvent contenir un élément nul.

**Enfin, et malheureusement, il faut réussir à démontrer qu'il existe une ligne telle que dans les autres colonnes que sa diagonale que sont les colonnes des nombres qui ne divisent pas $2a$, cette ligne contient aussi des éléments non nuls. Et ça, ça reste à faire parce qu'il existe des composés incongrus à 2a selon tout module de 2 à $a$ (par exemple, le nombre 9 dans le cas de la recherche de décompositions pour le nombre pair 40).**

En fait, un tel nombre premier est solution entière d'un système d'équations rationnelles défini de la façon suivante : on définit d'abord la fonction $f$ suivante sur les nombres entiers compris entre 2 et $a$,

$$\begin{aligned} f : \big[2,3,...,\mathrm{a}\big] &\to \mathbb{Q}^*, \\ x &\mapsto f(x) = \frac{2a - 2x - p}{x} \end{aligned}$$

On associe alors à tout $p$ un (a-1)-uplet de nombres de la façon suivante :

$$\begin{aligned} g : \big[2,3,...,\mathrm{a}\big] &\to \mathbb{Q}^{*a-1}, \\ x &\mapsto g(x) = (f(2), f(3), ..., f(\mathrm{a})) \end{aligned}$$

Tout nombre premier qui a pour image un (a-1)-uplet ne contenant que des rationnels non entiers est décomposant Goldbach de $2a$.

**Il faut démontrer qu'un tel nombre premier (inférieur à a et incongru à 2a pour tout module de 2 à a) existe toujours.**

Peut-être faudrait-il utiliser la bijection que l'on peut établir entre toute case $(i, j)$ de la table de congruence et la fraction rationnelle $i/j$. La condition

$$p \equiv 0 \ (mod\ q)$$

se transforme alors en

$$la\ fraction\ rationnelle\ \frac{p}{q}\ est\ entière$$

tandis que la condition

$$p \equiv 2a \ (mod\ q)$$

se transforme quant à elle en

$$les\ fractions\ rationnelles\ \frac{2a}{q}\ et\ \frac{p}{q}$$
$$sont\ des\ rationnels\ non\ entiers\ qui\ ont\ même\ partie\ décimale.$$

On ordonne alors les cases de la table de congruence ainsi notées sous forme de fractions rationnelles[2] et on découvre une troisième symétrie autour de la diagonale des zéros en partie haute de la table de congruence et qui associe à toute fraction entière (par exemple 4/2) le fait que la fraction inverse (2/4) est déjà apparue antérieurement dans la table (sous la forme 1/2)[3].

3) Primarité du complémentaire $2a - p$ : une fois prouvée l'existence d'un nombre premier impair, inférieur à $\lfloor a/2 \rfloor$, ne divisant pas $2a$, et incongru à $2a$ modulo tout nombre compris entre 2 et $a$, montrons que le complémentaire de ce nombre à $2a$ est premier également. On réutilise à nouveau la propriété $Sym_h$ pour "se transporter" dans la partie inférieure de la table.

$$\exists\, p \,<\, a,\; p \nmid a,\; p \textit{ nombre premier impair } / \,\forall\, q \,\leq\, a, \quad \begin{array}{l} 2a \,\not\equiv\, p \;(mod\; q) \\ \Leftrightarrow\; 2a - p \,\not\equiv\, 0 \;(mod\; q) \\ \Leftrightarrow\; 2a - p \textit{ est premier également.} \end{array}$$

Le complémentaire du nombre premier qu'on avait identifié dans la partie supérieure de la table est donc premier lui-aussi, donc la conjecture de Goldbach est vraie pour $2a$, et donc tout nombre pair supérieur à 4 est la somme de deux nombres premiers. La conjecture de Goldbach est ainsi démontrée pour tout nombre pair et on peut désormais en utiliser une formule équivalente qui est : "Tout nombre entier supérieur ou égal à 2 est la moyenne arithmétique de deux nombres premiers.".

## Annexe : Associer aux entiers des ensembles de fractions rationnelles

Habituellement, pour savoir si un nombre est premier, on le divise par tous les nombres premiers inférieurs à sa racine et si les résultats de toutes ces divisions sont des rationnels non entiers, on en déduit que le nombre est premier.

Au début de ce travail, j'avais pour habitude d'associer à un nombre entier impair (les pairs étant trivialement non premiers) un autre ensemble de fractions rationnelles pour savoir s'il était premier. Imaginons en effet que l'on ne connaisse pas les nombres premiers inférieurs à un nombre donné. Un nombre entier impair $p$ est premier si toute fraction rationnelle dont le numérateur est un nombre $i$ variant de 1 à $\frac{p-3}{2}$ et dont le dénominateur est égal à $p - 2i$ est une fraction rationnelle non entière.
Par exemple, on associe au nombre 9 l'ensemble des fractions rationnelles $\left\{\frac{1}{7}, \frac{2}{5}, \frac{3}{3}\right\}$ et 9 n'est donc pas premier puisque la fraction rationnelle $\frac{3}{3}$ est entière. De la même façon, on associe au nombre 11 l'ensemble des fractions rationnelles $\left\{\frac{1}{9}, \frac{2}{7}, \frac{3}{5}, \frac{4}{3}\right\}$ et 11 est un nombre premier parce que toutes les fractions rationnelles de l'ensemble en question sont non entières.

[2] non pas à la Cantor qui avait travaillé sur la conjecture en 1894, mais selon l'ordre suivant : les premières dans l'ordre sont les fractions de la première ligne de la table qui se retrouvent dans la diagonale à droite de l'arbre, on les obtient en descendant toujours sur le fils droit du sommet courant, puis celles de la deuxième ligne, etc

[3] Les deux dernières pages de ce document fournissent une telle table remplie de rationnels ainsi qu'un début d'arbre binaire de rationnels.

Maintenant qu'on a étudié toutes les symétries des tables de congruence et les équations rationnelles qui permettent de trouver les nombres premiers qui sont décomposants Goldbach d'un nombre pair donné (Cf note *noel2006.pdf*, parties *La géométrie des nombres de Minkowski* et *Equations rationnelles de droites affines dont on cherche des solutions entières*), on a découvert une autre façon de caractériser les nombres premiers et qui est en quelque sorte le "pendant" de celle évidente dont on se servait initialement que l'on va expliquer ici : il s'agit d'associer à un nombre impair $p$ un ensemble de $\frac{p-3}{2}$ fractions rationnelles dont le numérateur est un nombre impair variant de 1 à $p-4$ et le dénominateur est un entier variant de $\frac{p-1}{2}$ à 2.
Cette application fait associer à 9 l'ensemble des fractions rationnelles $\left\{\frac{1}{4}, \frac{3}{3}, \frac{5}{2}\right\}$ et 9 n'est donc pas premier à nouveau parce que la fraction rationnelle $\frac{3}{3}$ est entière. De la même façon, on associe au nombre 11 l'ensemble des fractions rationnelles $\left\{\frac{1}{5}, \frac{3}{4}, \frac{5}{3}, \frac{7}{2}\right\}$ et 11 est un nombre premier parce que toutes les fractions rationnelles de l'ensemble en question sont non entières.
On trouvera en toute fin de cette note les ensembles de rationnels que l'on associe aux nombres de 9 à 45. On voit que dans l'ensemble associé à un entier impair, toute fraction rationnelle dont le dénominateur est un diviseur de ce nombre est entière.
Il en résulte une nouvelle caractérisation des nombres premiers qui est :

$$p\ premier \iff \forall\, i,\ 1 \leq i \leq \frac{p-3}{2},\ \frac{4i+2}{p-2i-1} \notin \mathbb{N}$$

On peut encore améliorer cette caractérisation car si le numérateur d'une fraction est strictement inférieur à son dénominateur, elle ne peut être entière, ce qui est le cas dès que $i < \lceil \frac{p-3}{6} \rceil$ On se restreint donc finalement à la caractérisation suivante :

$$p\ premier \iff \forall\, i,\ \left\lceil \frac{p-3}{6} \right\rceil \leq i \leq \frac{p-3}{2},\ \frac{4i+2}{p-2i-1} \notin \mathbb{N}$$

Une première conséquence de cela est la formule qui permet de trouver les décomposants Goldbach d'un nombre pair et qui se note :

$$\begin{aligned} Goldbach(2a,i,j) \iff\ & 3 \leq i \leq a \\ & \wedge\ prime(i) \\ & \wedge\ \forall\, j,\ 2 \leq j \leq a \Rightarrow \tfrac{2a-2j-i}{j} \notin \mathbb{N} \end{aligned}$$

A la suite de cela, si l'union d'ensembles dépendante du nombre $p$ impair ci-dessous ne contient que des fractions rationnelles non entières, alors $p$ et $p+2$ sont des nombres premiers jumeaux.

$$\left\{\frac{p-2}{2}\right\} \cup \bigcup_{\substack{j\ impair \\ 1 \leq j \leq p-4}} \left\{\frac{2j}{p-j}, \frac{2j}{p-j+2}\right\}$$

Les programmes de vérification en C++ qui permettent de vérifier que ces équations rationnelles ont bien comme solutions entières soit des nombres premiers, soit les décomposants Goldbach d'un nombre pair donné, soit les nombres premiers jumeaux peuvent être trouvés à l'adresse *http://denise.vella.chemla.free.fr*, dans l'onglet *Des notes et puis un jour l'Harmonie.*

Ci-dessous, les tables de congruence associées aux nombres pairs 24, 40 et 30 :

| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 3 | 1 | 0 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 4 | 0 | 1 | 0 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 5 | 1 | 2 | 1 | 0 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 6 | 0 | 0 | 2 | 1 | 0 | 6 | 6 | 6 | 6 | 6 | 6 |
| 7 | 1 | 1 | 3 | 2 | 1 | 0 | 7 | 7 | 7 | 7 | 7 |
| 8 | 0 | 2 | 0 | 3 | 2 | 1 | 0 | 8 | 8 | 8 | 8 |
| 9 | 1 | 0 | 1 | 4 | 3 | 2 | 1 | 0 | 9 | 9 | 9 |
| 10 | 0 | 1 | 2 | 0 | 4 | 3 | 2 | 1 | 0 | 10 | 10 |
| 11 | 1 | 2 | 3 | 1 | 5 | 4 | 3 | 2 | 1 | 0 | 11 |
| 12 | 0 | 0 | 0 | 2 | 0 | 5 | 4 | 3 | 2 | 1 | 0 |
| 13 | 1 | 1 | 1 | 3 | 1 | 6 | 5 | 4 | 3 | 2 | 1 |
| 14 | 0 | 2 | 2 | 4 | 2 | 0 | 6 | 5 | 4 | 3 | 2 |
| 15 | 1 | 0 | 3 | 0 | 3 | 1 | 7 | 6 | 5 | 4 | 3 |
| 16 | 0 | 1 | 0 | 1 | 4 | 2 | 0 | 7 | 6 | 5 | 4 |
| 17 | 1 | 2 | 1 | 2 | 5 | 3 | 1 | 8 | 7 | 6 | 5 |
| 18 | 0 | 0 | 2 | 3 | 0 | 4 | 2 | 0 | 8 | 7 | 6 |
| 19 | 1 | 1 | 3 | 4 | 1 | 5 | 3 | 1 | 9 | 8 | 7 |
| 20 | 0 | 2 | 0 | 0 | 2 | 6 | 4 | 2 | 0 | 9 | 8 |
| 21 | 1 | 0 | 1 | 1 | 3 | 0 | 5 | 3 | 1 | 10 | 9 |
| 22 | 0 | 1 | 2 | 2 | 4 | 1 | 6 | 4 | 2 | 0 | 10 |
| 23 | 1 | 2 | 3 | 3 | 5 | 2 | 7 | 5 | 3 | 1 | 11 |
| 24 | 0 | 0 | 0 | 4 | 0 | 3 | 0 | 6 | 4 | 2 | 0 |

| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 3 | 1 | 0 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 4 | 0 | 1 | 0 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 5 | 1 | 2 | 1 | 0 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 6 | 0 | 0 | 2 | 1 | 0 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 7 | 1 | 1 | 3 | 2 | 1 | 0 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 |
| 8 | 0 | 2 | 0 | 3 | 2 | 1 | 0 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 |
| 9 | 1 | 0 | 1 | 4 | 3 | 2 | 1 | 0 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 |
| 10 | 0 | 1 | 2 | 0 | 4 | 3 | 2 | 1 | 0 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| 11 | 1 | 2 | 3 | 1 | 5 | 4 | 3 | 2 | 1 | 0 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 |
| 12 | 0 | 0 | 0 | 2 | 0 | 5 | 4 | 3 | 2 | 1 | 0 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 |
| 13 | 1 | 1 | 1 | 3 | 1 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 13 | 13 | 13 | 13 | 13 | 13 | 13 |
| 14 | 0 | 2 | 2 | 4 | 2 | 0 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 14 | 14 | 14 | 14 | 14 | 14 |
| 15 | 1 | 0 | 3 | 0 | 3 | 1 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 15 | 15 | 15 | 15 | 15 |
| 16 | 0 | 1 | 0 | 1 | 4 | 2 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 16 | 16 | 16 | 16 |
| 17 | 1 | 2 | 1 | 2 | 5 | 3 | 1 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 17 | 17 | 17 |
| 18 | 0 | 0 | 2 | 3 | 0 | 4 | 2 | 0 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 18 | 18 |
| 19 | 1 | 1 | 3 | 4 | 1 | 5 | 3 | 1 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 19 |
| 20 | 0 | 2 | 0 | 0 | 2 | 6 | 4 | 2 | 0 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 21 | 1 | 0 | 1 | 1 | 3 | 0 | 5 | 3 | 1 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 22 | 0 | 1 | 2 | 2 | 4 | 1 | 6 | 4 | 2 | 0 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 |
| 23 | 1 | 2 | 3 | 3 | 5 | 2 | 7 | 5 | 3 | 1 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 |
| 24 | 0 | 0 | 0 | 4 | 0 | 3 | 0 | 6 | 4 | 2 | 0 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 |
| 25 | 1 | 1 | 1 | 0 | 1 | 4 | 1 | 7 | 5 | 3 | 1 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 |
| 26 | 0 | 2 | 2 | 1 | 2 | 5 | 2 | 8 | 6 | 4 | 2 | 0 | 12 | 11 | 10 | 9 | 8 | 7 | 6 |
| 27 | 1 | 0 | 3 | 2 | 3 | 6 | 3 | 0 | 7 | 5 | 3 | 1 | 13 | 12 | 11 | 10 | 9 | 8 | 7 |
| 28 | 0 | 1 | 0 | 3 | 4 | 0 | 4 | 1 | 8 | 6 | 4 | 2 | 0 | 13 | 12 | 11 | 10 | 9 | 8 |
| 29 | 1 | 2 | 1 | 4 | 5 | 1 | 5 | 2 | 9 | 7 | 5 | 3 | 1 | 14 | 13 | 12 | 11 | 10 | 9 |
| 30 | 0 | 0 | 2 | 0 | 0 | 2 | 6 | 3 | 0 | 8 | 6 | 4 | 2 | 0 | 14 | 13 | 12 | 11 | 10 |
| 31 | 1 | 1 | 3 | 1 | 1 | 3 | 7 | 4 | 1 | 9 | 7 | 5 | 3 | 1 | 15 | 14 | 13 | 12 | 11 |
| 32 | 0 | 2 | 0 | 2 | 2 | 4 | 0 | 5 | 2 | 10 | 8 | 6 | 4 | 2 | 0 | 15 | 14 | 13 | 12 |
| 33 | 1 | 0 | 1 | 3 | 3 | 5 | 1 | 6 | 3 | 0 | 9 | 7 | 5 | 3 | 1 | 16 | 15 | 14 | 13 |
| 34 | 0 | 1 | 2 | 4 | 4 | 6 | 2 | 7 | 4 | 1 | 10 | 8 | 6 | 4 | 2 | 0 | 16 | 15 | 14 |
| 35 | 1 | 2 | 3 | 0 | 5 | 0 | 3 | 8 | 5 | 2 | 11 | 9 | 7 | 5 | 3 | 1 | 17 | 16 | 15 |
| 36 | 0 | 0 | 0 | 1 | 0 | 1 | 4 | 0 | 6 | 3 | 0 | 10 | 8 | 6 | 4 | 2 | 0 | 17 | 16 |
| 37 | 1 | 1 | 1 | 2 | 1 | 2 | 5 | 1 | 7 | 4 | 1 | 11 | 9 | 7 | 5 | 3 | 1 | 18 | 17 |
| 38 | 0 | 2 | 2 | 3 | 2 | 3 | 6 | 2 | 8 | 5 | 2 | 12 | 10 | 8 | 6 | 4 | 2 | 0 | 18 |
| 39 | 1 | 0 | 3 | 4 | 3 | 4 | 7 | 3 | 9 | 6 | 3 | 0 | 11 | 9 | 7 | 5 | 3 | 1 | 19 |
| 40 | 0 | 1 | 0 | 0 | 4 | 5 | 0 | 4 | 0 | 7 | 4 | 1 | 12 | 10 | 8 | 6 | 4 | 2 | 0 |

| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 3 | 1 | 0 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 4 | 0 | 1 | 0 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 5 | 1 | 2 | 1 | 0 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 6 | 0 | 0 | 2 | 1 | 0 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 7 | 1 | 1 | 3 | 2 | 1 | 0 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 |
| 8 | 0 | 2 | 0 | 3 | 2 | 1 | 0 | 8 | 8 | 8 | 8 | 8 | 8 | 8 |
| 9 | 1 | 0 | 1 | 4 | 3 | 2 | 1 | 0 | 9 | 9 | 9 | 9 | 9 | 9 |
| 10 | 0 | 1 | 2 | 0 | 4 | 3 | 2 | 1 | 0 | 10 | 10 | 10 | 10 | 10 |
| 11 | 1 | 2 | 3 | 1 | 5 | 4 | 3 | 2 | 1 | 0 | 11 | 11 | 11 | 11 |
| 12 | 0 | 0 | 0 | 2 | 0 | 5 | 4 | 3 | 2 | 1 | 0 | 12 | 12 | 12 |
| 13 | 1 | 1 | 1 | 3 | 1 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 13 | 13 |
| 14 | 0 | 2 | 2 | 4 | 2 | 0 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 14 |
| 15 | 1 | 0 | 3 | 0 | 3 | 1 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 16 | 0 | 1 | 0 | 1 | 4 | 2 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 17 | 1 | 2 | 1 | 2 | 5 | 3 | 1 | 8 | 7 | 6 | 5 | 4 | 3 | 2 |
| 18 | 0 | 0 | 2 | 3 | 0 | 4 | 2 | 0 | 8 | 7 | 6 | 5 | 4 | 3 |
| 19 | 1 | 1 | 3 | 4 | 1 | 5 | 3 | 1 | 9 | 8 | 7 | 6 | 5 | 4 |
| 20 | 0 | 2 | 0 | 0 | 2 | 6 | 4 | 2 | 0 | 9 | 8 | 7 | 6 | 5 |
| 21 | 1 | 0 | 1 | 1 | 3 | 0 | 5 | 3 | 1 | 10 | 9 | 8 | 7 | 6 |
| 22 | 0 | 1 | 2 | 2 | 4 | 1 | 6 | 4 | 2 | 0 | 10 | 9 | 8 | 7 |
| 23 | 1 | 2 | 3 | 3 | 5 | 2 | 7 | 5 | 3 | 1 | 11 | 10 | 9 | 8 |
| 24 | 0 | 0 | 0 | 4 | 0 | 3 | 0 | 6 | 4 | 2 | 0 | 11 | 10 | 9 |
| 25 | 1 | 1 | 1 | 0 | 1 | 4 | 1 | 7 | 5 | 3 | 1 | 12 | 11 | 10 |
| 26 | 0 | 2 | 2 | 1 | 2 | 5 | 2 | 8 | 6 | 4 | 2 | 0 | 12 | 11 |
| 27 | 1 | 0 | 3 | 2 | 3 | 6 | 3 | 0 | 7 | 5 | 3 | 1 | 13 | 12 |
| 28 | 0 | 1 | 0 | 3 | 4 | 0 | 4 | 1 | 8 | 6 | 4 | 2 | 0 | 13 |
| 29 | 1 | 2 | 1 | 4 | 5 | 1 | 5 | 2 | 9 | 7 | 5 | 3 | 1 | 14 |
| 30 | 0 | 0 | 2 | 0 | 0 | 2 | 6 | 3 | 0 | 8 | 6 | 4 | 2 | 0 |

Ici, on va redessiner la table du cas 30 en visualisant les lignes correspondant aux 3 décomposants Goldbach : 7 (symbole ■), 11 (symbole ♠) et 13 (symbole ◄) et à leur symétrique : 23 (symbole ♦), 19 (symbole ♣) et 17 (symbole ►).
**Décomposition 30 = 7+23**

| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1■ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 0 | 2 | 2 | 2■ | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 3 | 1 | 0 | 3■ | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 4 | 0 | 1■ | 0 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 5 | 1■ | 2 | 1 | 0 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 6 | 0 | 0 | 2 | 1 | 0 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 7 | 1■ | 1■ | 3■ | 2■ | 1■ | 0 ■ | 7■ | 7■ | 7■ | 7■ | 7■ | 7■ | 7■ | 7■ |
| 8 | 0 | 2 | 0 | 3 | 2 | 1 | 0 | 8 | 8 | 8 | 8 | 8 | 8 | 8♦ |
| 9 | 1■ | 0 | 1 | 4 | 3 | 2 | 1 | 0 | 9 | 9 | 9 | 9 | 9♦ | 9 |
| 10 | 0 | 1■ | 2 | 0 | 4 | 3 | 2 | 1 | 0 | 10 | 10 | 10♦ | 10 | 10 |
| 11 | 1 | 2 | 3■ | 1 | 5 | 4 | 3 | 2 | 1 | 0 | 11♦ | 11 | 11 | 11 |
| 12 | 0 | 0 | 0 | 2■ | 0 | 5 | 4 | 3 | 2 | 1♦ | 0 | 12 | 12 | 12 |
| 13 | 1 | 1 | 1 | 3 | 1■ | 6 | 5 | 4 | 3♦ | 2 | 1 | 0 | 13 | 13 |
| 14 | 0 | 2 | 2 | 4 | 2 | 0 ■ | 6 | 5♦ | 4 | 3 | 2 | 1 | 0 | 14 |
| 15 | 1 | 0 | 3 | 0 | 3 | 1 | 7■♦ | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 16 | 0 | 1 | 0 | 1 | 4 | 2 ♦ | 0 | 7 | ■6 | 5 | 4 | 3 | 2 | 1 |
| 17 | 1 | 2 | 1 | 2 | 5♦ | 3 | 1 | 8 | 7 | ■6 | 5 | 4 | 3 | 2 |
| 18 | 0 | 0 | 2 | 3♦ | 0 | 4 | 2 | 0 | 8 | 7 | ■6 | 5 | 4 | 3 |
| 19 | 1 | 1 | 3♦ | 4 | 1 | 5 | 3 | 1 | 9 | 8 | 7 | ■6 | 5 | 4 |
| 20 | 0 | 2♦ | 0 | 0 | 2 | 6 | 4 | 2 | 0 | 9 | 8 | 7 | ■6 | 5 |
| 21 | 1♦ | 0 | 1 | 1 | 3 | 0 | 5 | 3 | 1 | 10 | 9 | 8 | 7 | 6 |
| 22 | 0 | 1 | 2 | 2 | 4 | 1 | 6 | 4 | 2 | 0 | 10 | 9 | 8 | 7 |
| 23 | 1♦ | 2♦ | 3♦ | 3♦ | 5♦ | 2 ♦ | 7♦ | 5♦ | 3♦ | 1♦ | 11♦ | 10♦ | 9♦ | 8♦ |
| 24 | 0 | 0 | 0 | 4 | 0 | 3 | 0 | 6 | 4 | 2 | 0 | 11 | 10 | 9 |
| 25 | 1♦ | 1 | 1 | 0 | 1 | 4 | 1 | 7 | 5 | 3 | 1 | 12 | 11 | 10 |
| 26 | 0 | 2♦ | 2 | 1 | 2 | 5 | 2 | 8 | 6 | 4 | 2 | 0 | 12 | 11 |
| 27 | 1 | 0 | 3♦ | 2 | 3 | 6 | 3 | 0 | 7 | 5 | 3 | 1 | 13 | 12 |
| 28 | 0 | 1 | 0 | 3♦ | 4 | 0 | 4 | 1 | 8 | 6 | 4 | 2 | 0 | 13 |
| 29 | 1 | 2 | 1 | 4 | 5♦ | 1 | 5 | 2 | 9 | 7 | 5 | 3 | 1 | 14 |
| 30 | 0 | 0 | 2 | 0 | 0 | 2 ♦ | 6 | 3 | 0 | 8 | 6 | 4 | 2 | 0 |

**Décomposition 30 = 11+29**

| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1♠ | 1 | 1 | 1 | 1 | 1 |
| 2 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2♠ | 2 | 2 | 2 | 2 | 2 | 2 |
| 3 | 1 | 0 | 3 | 3 | 3 | 3 | 3♠ | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 4 | 0 | 1 | 0 | 4 | 4 | 4♠ | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4♣ |
| 5 | 1 | 2 | 1 | 0 | 5♠ | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5♣ | 5 |
| 6 | 0 | 0 | 2 | 1♠ | 0 | 6 | 6 | 6 | 6 | 6 | 6 | 6♣ | 6 | 6 |
| 7 | 1 | 1 | 3♠ | 2 | 1 | 0 | 7 | 7 | 7 | 7 | 7♣ | 7 | 7 | 7 |
| 8 | 0 | 2♠ | 0 | 3 | 2 | 1 | 0 | 8 | 8 | 8♣ | 8 | 8 | 8 | 8 |
| 9 | 1♠ | 0 | 1 | 4 | 3 | 2 | 1 | 0 | 9♣ | 9 | 9 | 9 | 9 | 9 |
| 10 | 0 | 1 | 2 | 0 | 4 | 3 | 2 | 1♣ | 0 | 10 | 10 | 10 | 10 | 10 |
| 11 | 1♠ | 2♠ | 3♠ | 1♠ | 5♠ | 4♠ | 3♠♣ | 2♠ | 1♠ | 0 ♠ | 11♠ | 11♠ | 11♠ | 11♠ |
| 12 | 0 | 0 | 0 | 2 | 0 | 5♣ | 4 | 3 | 2 | 1 | 0 | 12 | 12 | 12 |
| 13 | 1♠ | 1 | 1 | 3 | 1♣ | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 13 | 13 |
| 14 | 0 | 2♠ | 2 | 4♣ | 2 | 0 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 14 |
| 15 | 1 | 0 | 3♠♣ | 0 | 3 | 1 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 16 | 0 | 1♣ | 0 | 1♠ | 4 | 2 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 17 | 1♣ | 2 | 1 | 2 | 5♠ | 3 | 1 | 8 | 7 | 6 | 5 | 4 | 3 | 2 |
| 18 | 0 | 0 | 2 | 3 | 0 | 4♠ | 2 | 0 | 8 | 7 | 6 | 5 | 4 | 3 |
| 19 | 1♣ | 1♣ | 3♣ | 4♣ | 1♣ | 5♣ | 3♠♣ | 1♣ | 9♣ | 8♣ | 7♣ | 6♣ | 5♣ | 4♣ |
| 20 | 0 | 2 | 0 | 0 | 2 | 6 | 4 | 2♠ | 0 | 9 | 8 | 7 | 6 | 5 |
| 21 | 1♣ | 0 | 1 | 1 | 3 | 0 | 5 | 3 | 1♠ | 10 | 9 | 8 | 7 | 6 |
| 22 | 0 | 1♣ | 2 | 2 | 4 | 1 | 6 | 4 | 2 | 0 ♠ | 10 | 9 | 8 | 7 |
| 23 | 1 | 2 | 3♣ | 3 | 5 | 2 | 7 | 5 | 3 | 1 | 11♠ | 10 | 9 | 8 |
| 24 | 0 | 0 | 0 | 4♣ | 0 | 3 | 0 | 6 | 4 | 2 | 0 | 11♠ | 10 | 9 |
| 25 | 1 | 1 | 1 | 0 | 1♣ | 4 | 1 | 7 | 5 | 3 | 1 | 12 | 11♠ | 10 |
| 26 | 0 | 2 | 2 | 1 | 2 | 5♣ | 2 | 8 | 6 | 4 | 2 | 0 | 12 | 11♠ |
| 27 | 1 | 0 | 3 | 2 | 3 | 6 | 3♣ | 0 | 7 | 5 | 3 | 1 | 13 | 12 |
| 28 | 0 | 1 | 0 | 3 | 4 | 0 | 4 | 1♣ | 8 | 6 | 4 | 2 | 0 | 13 |
| 29 | 1 | 2 | 1 | 4 | 5 | 1 | 5 | 2 | 9♣ | 7 | 5 | 3 | 1 | 14 |
| 30 | 0 | 0 | 2 | 0 | 0 | 2 | 6 | 3 | 0 | 8♣ | 6 | 4 | 2 | 0 |

**Décomposition 30 = 13+17**

| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 ◀ | 1 | 1 | 1 |
| 2 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 ◀ | 2 | 2 | 2 | 2 ▶ |
| 3 | 1 | 0 | 3 | 3 | 3 | 3 | 3 | 3 | 3 ◀ | 3 | 3 | 3 | 3 ▶ | 3 |
| 4 | 0 | 1 | 0 | 4 | 4 | 4 | 4 | 4 ◀ | 4 | 4 | 4 | 4 ▶ | 4 | 4 |
| 5 | 1 | 2 | 1 | 0 | 5 | 5 | 5 ◀ | 5 | 5 | 5 | 5 ▶ | 5 | 5 | 5 |
| 6 | 0 | 0 | 2 | 1 | 0 | 6 ◀ | 6 | 6 | 6 | 6 ▶ | 6 | 6 | 6 | 6 |
| 7 | 1 | 1 | 3 | 2 | 1 ◀ | 0 | 7 | 7 | 7 ▶ | 7 | 7 | 7 | 7 | 7 |
| 8 | 0 | 2 | 0 | 3 ◀ | 2 | 1 | 0 | 8 ▶ | 8 | 8 | 8 | 8 | 8 | 8 |
| 9 | 1 | 0 | 1 ◀ | 4 | 3 | 2 | 1 ▶ | 0 | 9 | 9 | 9 | 9 | 9 | 9 |
| 10 | 0 | 1 ◀ | 2 | 0 | 4 | 3 ▶ | 2 | 1 | 0 | 10 | 10 | 10 | 10 | 10 |
| 11 | 1 ◀ | 2 | 3 | 1 | 5 ▶ | 4 | 3 | 2 | 1 | 0 | 11 | 11 | 11 | 11 |
| 12 | 0 | 0 | 0 | 2 ▶ | 0 | 5 | 4 | 3 | 2 | 1 | 0 | 12 | 12 | 12 |
| 13 | 1 ◀ | 1 ◀ | 1 ◀▶ | 3 ◀ | 1 ◀ | 6 ◀ | 5 ◀ | 4 ◀ | 3 ◀ | 2 ◀ | 1 ◀ | 0 ◀ | 13 ◀ | 13 ◀ |
| 14 | 0 | 2 ▶ | 2 | 4 | 2 | 0 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 14 |
| 15 | 1 ◀▶ | 0 | 3 | 0 | 3 | 1 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 16 | 0 | 1 ◀ | 0 | 1 | 4 | 2 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 17 | 1 ▶ | 2 ▶ | 1 ◀▶ | 2 ▶ | 5 ▶ | 3 ▶ | 1 ▶ | 8 ▶ | 7 ▶ | 6 ▶ | 5 ▶ | 4 ▶ | 3 ▶ | 2 ▶ |
| 18 | 0 | 0 | 2 | 3 ◀ | 0 | 4 | 2 | 0 | 8 | 7 | 6 | 5 | 4 | 3 |
| 19 | 1 ▶ | 1 | 3 | 4 | 1 ◀ | 5 | 3 | 1 | 9 | 8 | 7 | 6 | 5 | 4 |
| 20 | 0 | 2 ▶ | 0 | 0 | 2 | 6 ◀ | 4 | 2 | 0 | 9 | 8 | 7 | 6 | 5 |
| 21 | 1 | 0 | 1 ▶ | 1 | 3 | 0 | 5 ◀ | 3 | 1 | 10 | 9 | 8 | 7 | 6 |
| 22 | 0 | 1 | 2 | 2 ▶ | 4 | 1 | 6 | 4 ◀ | 2 | 0 | 10 | 9 | 8 | 7 |
| 23 | 1 | 2 | 3 | 3 | 5 ▶ | 2 | 7 | 5 | 3 ◀ | 1 | 11 | 10 | 9 | 8 |
| 24 | 0 | 0 | 0 | 4 | 0 | 3 ▶ | 0 | 6 | 4 | 2 ◀ | 0 | 11 | 10 | 9 |
| 25 | 1 | 1 | 1 | 0 | 1 | 4 | 1 ▶ | 7 | 5 | 3 | 1 ◀ | 12 | 11 | 10 |
| 26 | 0 | 2 | 2 | 1 | 2 | 5 | 2 | 8 ▶ | 6 | 4 | 2 | 0 ◀ | 12 | 11 |
| 27 | 1 | 0 | 3 | 2 | 3 | 6 | 3 | 0 | 7 ▶ | 5 | 3 | 1 | 13 ◀ | 12 |
| 28 | 0 | 1 | 0 | 3 | 4 | 0 | 4 | 1 | 8 | 6 ▶ | 4 | 2 | 0 | 13 ◀ |
| 29 | 1 | 2 | 1 | 4 | 5 | 1 | 5 | 2 | 9 | 7 | 5 ▶ | 3 | 1 | 14 |
| 30 | 0 | 0 | 2 | 0 | 0 | 2 | 6 | 3 | 0 | 8 | 6 | 4 ▶ | 2 | 0 |

Ci-dessous, la table du cas du nombre pair 18 dont chaque case $(i, j)$ contient le rationnel $i/j$, qu'il soit entier ou pas.

| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|
| 1 | 0.5 | 0.3333 | 0.25 | 0.2 | 0.1666 | 0.1429 | 0.125 | 0.1111 |
| 2 | 1 | 0.6666 | 0.5 | 0.4 | 0.3333 | 0.2857 | 0.25 | 0.2222 |
| 3 | 1.5 | 1 | 0.75 | 0.6 | 0.5 | 0.4286 | 0.375 | 0.3333 |
| 4 | 2 | 1.3333 | 1 | 0.8 | 0.6666 | 0.5714 | 0.5 | 0.4444 |
| 5 | 2.5 | 1.6666 | 1.25 | 1 | 0.8333 | 0.7143 | 0.625 | 0.5555 |
| 6 | 3 | 2 | 1.5 | 1.2 | 1 | 0.8571 | 0.75 | 0.6666 |
| 7 | 3.5 | 2.3333 | 1.75 | 1.4 | 1.1666 | 1 | 0.875 | 0.7777 |
| 8 | 4 | 2.6666 | 2 | 1.6 | 1.3333 | 1.1429 | 1 | 0.8888 |
| 9 | 4.5 | 3 | 2.25 | 1.8 | 1.5 | 1.2857 | 1.125 | 1 |
| 10 | 5 | 3.3333 | 2.5 | 2 | 1.6666 | 1.4286 | 1.25 | 1.1111 |
| 11 | 5.5 | 3.6666 | 2.75 | 2.2 | 1.8333 | 1.5714 | 1.375 | 1.2222 |
| 12 | 6 | 4 | 3 | 2.4 | 2 | 1.7143 | 1.5 | 1.3333 |
| 13 | 6.5 | 4.3333 | 3.25 | 2.6 | 2.1666 | 1.8571 | 1.625 | 1.4444 |
| 14 | 7 | 4.6666 | 3.5 | 2.8 | 2.3333 | 2 | 1.75 | 1.5555 |
| 15 | 7.5 | 5 | 3.75 | 3 | 2.5 | 2.1429 | 1.875 | 1.6666 |
| 16 | 8 | 5.3333 | 4 | 3.2 | 2.6666 | 2.2857 | 2 | 1.7777 |
| 17 | 8.5 | 5.6666 | 4.25 | 3.4 | 2.8333 | 2.4286 | 2.125 | 1.8888 |
| 18 | 9 | 6 | 4.5 | 3.6 | 3 | 2.5714 | 2.25 | 2 |

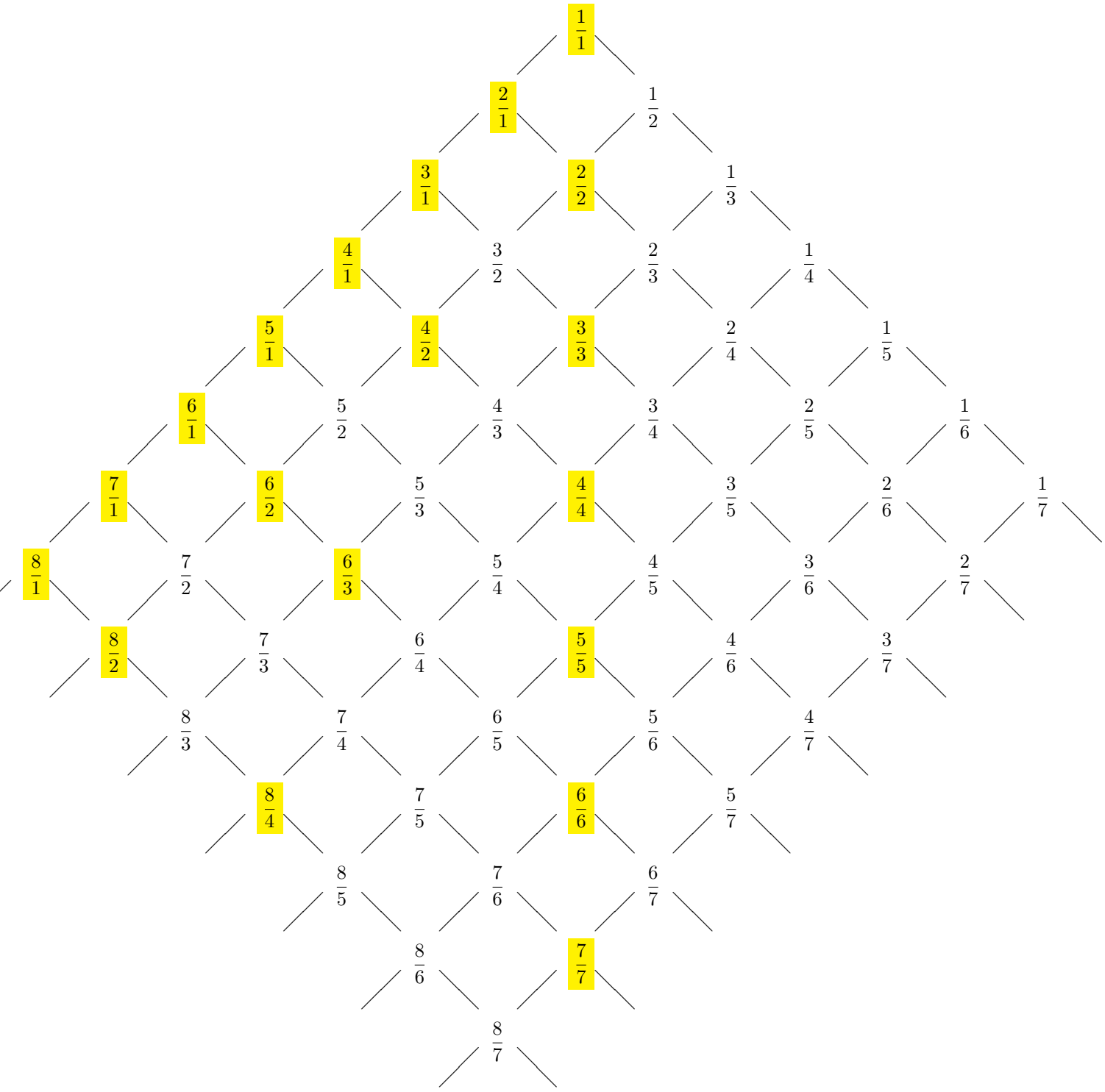
Le coloriage des congruences à 0 devient un coloriage des rationnels entiers et le coloriage des nombres congrus à $2a$ par colonne devient un coloriage des nombres rationnels qui ont même partie décimale que les nombres de la dernière ligne.

| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|
| 1 | 0.5 | 0.3333 | 0.25 | 0.2 | 0.1666 | 0.1429 | 0.125 | 0.1111 |
| 2 | 1 | 0.6666 | 0.5 | 0.4 | 0.3333 | 0.2857 | 0.25 | 0.2222 |
| 3 | 1.5 | 1 | 0.75 | 0.6 | 0.5 | 0.4286 | 0.375 | 0.3333 |
| 4 | 2 | 1.3333 | 1 | 0.8 | 0.6666 | 0.5714 | 0.5 | 0.4444 |
| 5 | 2.5 | 1.6666 | 1.25 | 1 | 0.8333 | 0.7143 | 0.625 | 0.5555 |
| 6 | 3 | 2 | 1.5 | 1.2 | 1 | 0.8571 | 0.75 | 0.6666 |
| 7 | 3.5 | 2.3333 | 1.75 | 1.4 | 1.1666 | 1 | 0.875 | 0.7777 |
| 8 | 4 | 2.6666 | 2 | 1.6 | 1.3333 | 1.1429 | 1 | 0.8888 |
| 9 | 4.5 | 3 | 2.25 | 1.8 | 1.5 | 1.2857 | 1.125 | 1 |
| 10 | 5 | 3.3333 | 2.5 | 2 | 1.6666 | 1.4286 | 1.25 | 1.1111 |
| 11 | 5.5 | 3.6666 | 2.75 | 2.2 | 1.8333 | 1.5714 | 1.375 | 1.2222 |
| 12 | 6 | 4 | 3 | 2.4 | 2 | 1.7143 | 1.5 | 1.3333 |
| 13 | 6.5 | 4.3333 | 3.25 | 2.6 | 2.1666 | 1.8571 | 1.625 | 1.4444 |
| 14 | 7 | 4.6666 | 3.5 | 2.8 | 2.3333 | 2 | 1.75 | 1.5555 |
| 15 | 7.5 | 5 | 3.75 | 3 | 2.5 | 2.1429 | 1.875 | 1.6666 |
| 16 | 8 | 5.3333 | 4 | 3.2 | 2.6666 | 2.2857 | 2 | 1.7777 |
| 17 | 8.5 | 5.6666 | 4.25 | 3.4 | 2.8333 | 2.4286 | 2.125 | 1.8888 |
| 18 | 9 | 6 | 4.5 | 3.6 | 3 | 2.5714 | 2.25 | 2 |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 9 | $\frac{1}{4}$ | $\frac{3}{3}$ | $\frac{5}{2}$ | | | | | | | | | |
| 11 | $\frac{1}{5}$ | $\frac{3}{4}$ | $\frac{5}{3}$ | $\frac{7}{2}$ | | | | | | | | |
| 13 | $\frac{1}{6}$ | $\frac{3}{5}$ | $\frac{5}{4}$ | $\frac{7}{3}$ | $\frac{9}{2}$ | | | | | | | |
| 15 | $\frac{1}{7}$ | $\frac{3}{6}$ | $\frac{5}{5}$ | $\frac{7}{4}$ | $\frac{9}{3}$ | $\frac{11}{2}$ | | | | | | |
| 17 | $\frac{1}{8}$ | $\frac{3}{7}$ | $\frac{5}{6}$ | $\frac{7}{5}$ | $\frac{9}{4}$ | $\frac{11}{3}$ | $\frac{13}{2}$ | | | | | |
| 19 | $\frac{1}{9}$ | $\frac{3}{8}$ | $\frac{5}{7}$ | $\frac{7}{6}$ | $\frac{9}{5}$ | $\frac{11}{4}$ | $\frac{13}{3}$ | $\frac{15}{2}$ | | | | |
| 21 | $\frac{1}{10}$ | $\frac{3}{9}$ | $\frac{5}{8}$ | $\frac{7}{7}$ | $\frac{9}{6}$ | $\frac{11}{5}$ | $\frac{13}{4}$ | $\frac{15}{3}$ | $\frac{17}{2}$ | | | |
| 23 | $\frac{1}{11}$ | $\frac{3}{10}$ | $\frac{5}{9}$ | $\frac{7}{8}$ | $\frac{9}{7}$ | $\frac{11}{6}$ | $\frac{13}{5}$ | $\frac{15}{4}$ | $\frac{17}{3}$ | $\frac{19}{2}$ | | |
| 25 | $\frac{1}{12}$ | $\frac{3}{11}$ | $\frac{5}{10}$ | $\frac{7}{9}$ | $\frac{9}{8}$ | $\frac{11}{7}$ | $\frac{13}{6}$ | $\frac{15}{5}$ | $\frac{17}{4}$ | $\frac{19}{3}$ | $\frac{21}{2}$ | |
| 27 | $\frac{1}{13}$ | $\frac{3}{12}$ | $\frac{5}{11}$ | $\frac{7}{10}$ | $\frac{9}{9}$ | $\frac{11}{8}$ | $\frac{13}{7}$ | $\frac{15}{6}$ | $\frac{17}{5}$ | $\frac{19}{4}$ | $\frac{21}{3}$ | $\frac{23}{2}$ |
| 29 | $\frac{1}{14}$ | $\frac{3}{13}$ | $\frac{5}{12}$ | $\frac{7}{11}$ | $\frac{9}{10}$ | $\frac{11}{9}$ | $\frac{13}{8}$ | $\frac{15}{7}$ | $\frac{17}{6}$ | $\frac{19}{5}$ | $\frac{21}{4}$ | $\frac{23}{3}$ | $\frac{25}{2}$ |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 31 | $\frac{1}{15}$ | $\frac{3}{14}$ | $\frac{5}{13}$ | $\frac{7}{12}$ | $\frac{9}{11}$ | $\frac{11}{10}$ | $\frac{13}{9}$ | $\frac{15}{8}$ | $\frac{17}{7}$ | $\frac{19}{6}$ | $\frac{21}{5}$ | $\frac{23}{4}$ | $\frac{25}{3}$ | $\frac{27}{2}$ | |
| 33 | $\frac{1}{16}$ | $\frac{3}{15}$ | $\frac{5}{14}$ | $\frac{7}{13}$ | $\frac{9}{12}$ | $\frac{11}{11}$ | $\frac{13}{10}$ | $\frac{15}{9}$ | $\frac{17}{8}$ | $\frac{19}{7}$ | $\frac{21}{6}$ | $\frac{23}{5}$ | $\frac{25}{4}$ | $\frac{27}{3}$ | $\frac{29}{2}$ |
| 35 | $\frac{1}{17}$ | $\frac{3}{16}$ | $\frac{5}{15}$ | $\frac{7}{14}$ | $\frac{9}{13}$ | $\frac{11}{12}$ | $\frac{13}{11}$ | $\frac{15}{10}$ | $\frac{17}{9}$ | $\frac{19}{8}$ | $\frac{21}{7}$ | $\frac{23}{6}$ | $\frac{25}{5}$ | $\frac{27}{4}$ | $\frac{29}{3}$ |
| | $\frac{31}{2}$ | | | | | | | | | | | | | | |
| 37 | $\frac{1}{18}$ | $\frac{3}{17}$ | $\frac{5}{16}$ | $\frac{7}{15}$ | $\frac{9}{14}$ | $\frac{11}{13}$ | $\frac{13}{12}$ | $\frac{15}{11}$ | $\frac{17}{10}$ | $\frac{19}{9}$ | $\frac{21}{8}$ | $\frac{23}{7}$ | $\frac{25}{6}$ | $\frac{27}{5}$ | $\frac{29}{4}$ |
| | $\frac{31}{3}$ | $\frac{33}{2}$ | | | | | | | | | | | | | |
| 39 | $\frac{1}{19}$ | $\frac{3}{18}$ | $\frac{5}{17}$ | $\frac{7}{16}$ | $\frac{9}{15}$ | $\frac{11}{14}$ | $\frac{13}{13}$ | $\frac{15}{12}$ | $\frac{17}{11}$ | $\frac{19}{10}$ | $\frac{21}{9}$ | $\frac{23}{8}$ | $\frac{25}{7}$ | $\frac{27}{6}$ | $\frac{29}{5}$ |
| | $\frac{31}{4}$ | $\frac{33}{3}$ | $\frac{35}{2}$ | | | | | | | | | | | | |
| 41 | $\frac{1}{20}$ | $\frac{3}{19}$ | $\frac{5}{18}$ | $\frac{7}{17}$ | $\frac{9}{16}$ | $\frac{11}{15}$ | $\frac{13}{14}$ | $\frac{15}{13}$ | $\frac{17}{12}$ | $\frac{19}{11}$ | $\frac{21}{10}$ | $\frac{23}{9}$ | $\frac{25}{8}$ | $\frac{27}{7}$ | $\frac{29}{6}$ |
| | $\frac{31}{5}$ | $\frac{33}{4}$ | $\frac{35}{3}$ | $\frac{37}{2}$ | | | | | | | | | | | |
| 43 | $\frac{1}{21}$ | $\frac{3}{20}$ | $\frac{5}{19}$ | $\frac{7}{18}$ | $\frac{9}{17}$ | $\frac{11}{16}$ | $\frac{13}{15}$ | $\frac{15}{14}$ | $\frac{17}{13}$ | $\frac{19}{12}$ | $\frac{21}{11}$ | $\frac{23}{10}$ | $\frac{25}{9}$ | $\frac{27}{8}$ | $\frac{29}{7}$ |
| | $\frac{31}{6}$ | $\frac{33}{5}$ | $\frac{35}{4}$ | $\frac{37}{3}$ | $\frac{39}{2}$ | | | | | | | | | | |
| 45 | $\frac{1}{22}$ | $\frac{3}{21}$ | $\frac{5}{20}$ | $\frac{7}{19}$ | $\frac{9}{18}$ | $\frac{11}{17}$ | $\frac{13}{16}$ | $\frac{15}{15}$ | $\frac{17}{14}$ | $\frac{19}{13}$ | $\frac{21}{12}$ | $\frac{23}{11}$ | | | |
| | $\frac{25}{10}$ | $\frac{27}{9}$ | $\frac{29}{8}$ | $\frac{31}{7}$ | $\frac{33}{6}$ | $\frac{35}{5}$ | $\frac{37}{4}$ | $\frac{39}{3}$ | $\frac{41}{2}$ | | | | | | |

Ci-dessous, un arbre binaire de fractions rationnelles que l'on a dû tronquer pour qu'il reste lisible dans la page. A gauche de la ligne verticale de fractions valant 1, sont entourées les fractions entières. Leur symétrique par rapport à la verticale des 1 sont des fractions qui existent déjà dans la table sous la forme d'une fraction de numérateur et dénominateur plus petits.


1/1
2/1 1/2
3/1 2/2 1/3
4/1 3/2 2/3 1/4
5/1 4/2 3/3 2/4 1/5
6/1 5/2 4/3 3/4 2/5 1/6
7/1 6/2 5/3 4/4 3/5 2/6 1/7
8/1 7/2 6/3 5/4 4/5 3/6 2/7
8/2 7/3 6/4 5/5 4/6 3/7
8/3 7/4 6/5 5/6 4/7
8/4 7/5 6/6 5/7
8/5 7/6 6/7
8/6 7/7
8/7

# Une approche enfantine des nombres premiers

Denise Vella

Janvier 2007

## 1 Introduction

On va présenter ici une dernière façon de caractériser les nombres premiers, qui repose sur la manière dont Gauss enfant a associé les entiers deux à deux pour découvrir la formule

$$\sum_{i=1}^{n} = \frac{n(n+1)}{2}$$

On avait pris pour habitude de considérer comme premier un nombre qui entretenait une certaine relation (être divisible par) avec d'autres nombres. Mais ce qui est également extraordinaire, c'est de voir la primarité d'un nombre comme le fait que ce nombre établit des relations d'indivisibilité entre des nombres inférieurs à lui pris deux à deux.

Dans un premier temps, illustrons cela par des exemples. Chacun des tableaux suivants est associé à un nombre entier, qui se trouve toujours être la somme des deux nombres d'une même colonne. Ce nombre est premier lorsque dans chaque colonne du tableau, le nombre de la première ligne ne divise pas celui de la deuxième ligne. Si au contraire, dans une colonne au moins, le nombre de la première ligne divise celui de la deuxième, alors on a affaire au tableau d'un nombre composé.

Tableau du nombre premier 5 :

| | | |
|---|---|---|
| 2 | 3 | 4 |
| 3 | 2 | 1 |

Tableau du nombre premier 7 :

| | | | | |
|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 |
| 5 | 4 | 3 | 2 | 1 |

Tableau du nombre premier 11 :

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

Tableau du nombre premier 13 :

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

Tableau du nombre composé 12 :

| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|
| 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

Tableau du nombre composé 15 :

| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

Si on adopte une approche basée sur les fractions rationnelles (dont le numérateur appartient à la liste d'entiers croissants de la première ligne des tableaux et dont le dénominateur appartient à la liste d'entiers décroissants de la deuxième ligne des tableaux), alors dans l'ensemble de fractions rationnelles associé à un entier impair, toute fraction dont le numérateur est un diviseur de ce nombre est entière.

Il résulte de tout cela une nouvelle caractérisation des nombres premiers qui est :

$$p \text{ impair est premier} \quad \Leftrightarrow \forall\, i,\ 2 \leq i \leq \frac{p-1}{2},\ i \nmid p-i$$

$$\Leftrightarrow \forall\, i,\ 2 \leq i \leq \frac{p-1}{2}, \frac{i}{p-i} \notin \mathbb{N}.$$

Voyons les différentes décompositions du nombre pair 40 comme somme de deux nombres impairs pour étudier, grâce à cette nouvelle manière de considérer la primarité des nombres, les décompositions qui sont des décompositions Goldbach (mettant en jeu deux nombres premiers).

décomposition 3 premier et 37 premier :

| 2 | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | | | | | | | | | | | | | | | | | |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 35 | 34 | 33 | 32 | 31 | 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 |

décomposition 5 premier et 35 composé :

| 2 | 3 | 4 | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 2 | 1 | | | | | | | | | | | | | | | | |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 33 | 32 | 31 | 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 |

décomposition 7 premier et 33 composé :

| 2 | 3 | 4 | 5 | 6 | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5 | 4 | 3 | 2 | 1 | | | | | | | | | | | | | | |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 31 | 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 |

décomposition 9 composé et 31 premier :

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | | | | | | | | | | | | |
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | | | | | | | | | | | | |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 |

décomposition 11 premier et 29 premier :

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | | | | | | | | | | |
| 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | | | | | | | | | | |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 |

décomposition 13 premier et 27 composé :

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | | | | | | | | |
| 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | | | | | | | | |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 |

décomposition 15 composé et 25 composé :

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | | | | | | |
| 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | | | | | | |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 |

décomposition 17 premier et 23 premier :

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | | | | |
| 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | | | | |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 |

décomposition 19 premier et 21 composé :

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | | |
| 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | | |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

La formule d'existence de décomposants Goldbach pour un nombre pair qui résulte de cette approche devient :

$$\begin{array}{l} Goldbach(2a,i,j) \Leftrightarrow \\ \quad \exists\, i, (\ i\ impair) \wedge (\ 3 \leq i \leq a)\ tel\ que \\ \quad\quad \forall\, y, (\ 2 \leq y \leq a), \\ \quad\quad\quad (2x = 2y + (2x-i-y) + (i-y)) \Rightarrow (y \nmid 2x-i-y) \wedge (y \nmid i-y). \end{array}$$

## 2 Conclusion

On peut peut-être désormais utiliser la formulation *"tout entier naturel supérieur à 2 est la moyenne arithmétique de deux nombres premiers"*. Concluons par deux citations d'Hilbert : *"Nous devons savoir et nous saurons ; il n'y a pas d'ignorabimus en mathématiques"* et puis un conseil qu'il donne à Klein : *"Il vous faut avoir un problème. Choisissez un objectif déterminé et marchez franchement vers lui. Vous pouvez ne jamais atteindre le but mais vous trouverez sûrement quelque chose d'intéressant en chemin"*. En mathématiques, il faut garder l'âme d'un *epsilon*[1] qui s'émerveille...

## Bibliographie


F. Casiro. *La conjecture de Goldbach, un défi en or.* Éd. Tangente n°78, décembre 2000, janvier 2001.

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

C.F. Gauss. *Recherches arithmétiques.* 1807. Éd. Jacques Gabay, 1989.

J. Hadamard. *Essai sur la psychologie de l'invention mathématique suivi de H. Poincaré, l'invention mathématique.* Éd. Jacques Gabay, 1959.

O. Kerléguer, D. Dumont. *Des images pour les nombres.* Éd. ACL du Kangourou, 2001.

D. Nordon. *Les obstinations d'un mathématicien.* Éd. Belin Pour la Science, 2003.

A. Sainte Laguë. *Avec des nombres et des lignes.* Éd. Vuibert, 1937.

A. Warusfel. *Les nombres et leurs mystères.* Éd. Points Sciences, 1961.


## Annexe : Citations littéraires

Des citations tirées du livre *La symphonie des nombres premiers* de Marcus du Sautoy.

Poincaré : Le scientifique n'étudie pas la Nature parce qu'elle est utile ; il l'étudie parce qu'elle le réjouit. Et elle le réjouit parce qu'elle est belle. Si la nature n'était pas belle, elle ne vaudrait pas la peine d'être connue, et si la Nature ne valait pas la peine d'être connue, la vie ne vaudrait pas la peine d'être vécue.

[1] C'est ainsi qu'Erdös désignait les enfants.

Hardy : Je pense que la réalité mathématique existe en dehors de nous, que notre fonction est de la découvrir ou de l'observer et que les théorèmes que nous démontrons et que nous décrivons avec grandiloquence comme nos créations sont simplement les notes de nos observations.

Gauss a coiffé Legendre sur le poteau au sujet du lien entre les nombres premiers et les logarithmes. Cela nous est révélé dans une lettre de Gauss à Encke, écrite le soir de Noël 1849[2].

Lagrange conseilla au père de Cauchy : Veillez à ce qu'il ne touche pas de livre de mathématiques avant ses 17 ans. Au lieu de cela, il suggéra de stimuler les talents littéraires de l'enfant si bien que, le jour où il reviendrait aux mathématiques, il serait capable de parler de sa propre voix mathématique, non en imitant ce qu'il aurait prélevé dans les ouvrages de l'époque.

Hardy à propos de Ramanujan : il était porteur d'un handicap insurmontable, pauvre hindou solitaire s'attaquant à la sagesse accumulée de l'Europe.

Ramanujan commençait à se dire que la priorité que Hardy accordait à la rigueur mathématique empêchait son esprit de parcourir librement le paysage mathématique.

Julia Robinson : Je souhaitais toujours à chacun de mes anniversaires et d'année en année que le dixième problème de Hilbert soit résolu. Pas par moi, mais simplement qu'il soit résolu. J'avais le sentiment que je ne pourrais accepter de mourir sans connaître la réponse.

Gauss : le problème de distinguer les nombres premiers des nombres composés et de décomposer ceux-ci en leurs facteurs premiers est connu comme un des plus importants et des plus utiles de toute l'Arithmétique. [...] En outre, la dignité de la Science semble demander que l'on recherche avec soin tous les secours nécessaires pour parvenir à la solution d'un problème si élégant et si célèbre.

[2] 157 ans sépare Noel 1849 de Noël 2006. Déduisez-en la primarité de 157 !

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 9 | $\frac{1}{4}$ | $\frac{3}{3}$ | $\frac{5}{2}$ | | | | | | | | | |
| 11 | $\frac{1}{5}$ | $\frac{3}{4}$ | $\frac{5}{3}$ | $\frac{7}{2}$ | | | | | | | | |
| 13 | $\frac{1}{6}$ | $\frac{3}{5}$ | $\frac{5}{4}$ | $\frac{7}{3}$ | $\frac{9}{2}$ | | | | | | | |
| 15 | $\frac{1}{7}$ | $\frac{3}{6}$ | $\frac{5}{5}$ | $\frac{7}{4}$ | $\frac{9}{3}$ | $\frac{11}{2}$ | | | | | | |
| 17 | $\frac{1}{8}$ | $\frac{3}{7}$ | $\frac{5}{6}$ | $\frac{7}{5}$ | $\frac{9}{4}$ | $\frac{11}{3}$ | $\frac{13}{2}$ | | | | | |
| 19 | $\frac{1}{9}$ | $\frac{3}{8}$ | $\frac{5}{7}$ | $\frac{7}{6}$ | $\frac{9}{5}$ | $\frac{11}{4}$ | $\frac{13}{3}$ | $\frac{15}{2}$ | | | | |
| 21 | $\frac{1}{10}$ | $\frac{3}{9}$ | $\frac{5}{8}$ | $\frac{7}{7}$ | $\frac{9}{6}$ | $\frac{11}{5}$ | $\frac{13}{4}$ | $\frac{15}{3}$ | $\frac{17}{2}$ | | | |
| 23 | $\frac{1}{11}$ | $\frac{3}{10}$ | $\frac{5}{9}$ | $\frac{7}{8}$ | $\frac{9}{7}$ | $\frac{11}{6}$ | $\frac{13}{5}$ | $\frac{15}{4}$ | $\frac{17}{3}$ | $\frac{19}{2}$ | | |
| 25 | $\frac{1}{12}$ | $\frac{3}{11}$ | $\frac{5}{10}$ | $\frac{7}{9}$ | $\frac{9}{8}$ | $\frac{11}{7}$ | $\frac{13}{6}$ | $\frac{15}{5}$ | $\frac{17}{4}$ | $\frac{19}{3}$ | $\frac{21}{2}$ | |
| 27 | $\frac{1}{13}$ | $\frac{3}{12}$ | $\frac{5}{11}$ | $\frac{7}{10}$ | $\frac{9}{9}$ | $\frac{11}{8}$ | $\frac{13}{7}$ | $\frac{15}{6}$ | $\frac{17}{5}$ | $\frac{19}{4}$ | $\frac{21}{3}$ | $\frac{23}{2}$ |
| 29 | $\frac{1}{14}$ | $\frac{3}{13}$ | $\frac{5}{12}$ | $\frac{7}{11}$ | $\frac{9}{10}$ | $\frac{11}{9}$ | $\frac{13}{8}$ | $\frac{15}{7}$ | $\frac{17}{6}$ | $\frac{19}{5}$ | $\frac{21}{4}$ | $\frac{23}{3}$ | $\frac{25}{2}$ |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 31 | $\frac{1}{15}$ | $\frac{3}{14}$ | $\frac{5}{13}$ | $\frac{7}{12}$ | $\frac{9}{11}$ | $\frac{11}{10}$ | $\frac{13}{9}$ | $\frac{15}{8}$ | $\frac{17}{7}$ | $\frac{19}{6}$ | $\frac{21}{5}$ | $\frac{23}{4}$ | $\frac{25}{3}$ | $\frac{27}{2}$ | |
| 33 | $\frac{1}{16}$ | $\frac{3}{15}$ | $\frac{5}{14}$ | $\frac{7}{13}$ | $\frac{9}{12}$ | $\frac{11}{11}$ | $\frac{13}{10}$ | $\frac{15}{9}$ | $\frac{17}{8}$ | $\frac{19}{7}$ | $\frac{21}{6}$ | $\frac{23}{5}$ | $\frac{25}{4}$ | $\frac{27}{3}$ | $\frac{29}{2}$ |
| 35 | $\frac{1}{17}$ | $\frac{3}{16}$ | $\frac{5}{15}$ | $\frac{7}{14}$ | $\frac{9}{13}$ | $\frac{11}{12}$ | $\frac{13}{11}$ | $\frac{15}{10}$ | $\frac{17}{9}$ | $\frac{19}{8}$ | $\frac{21}{7}$ | $\frac{23}{6}$ | $\frac{25}{5}$ | $\frac{27}{4}$ | $\frac{29}{3}$ |
| | $\frac{31}{2}$ | | | | | | | | | | | | | | |
| 37 | $\frac{1}{18}$ | $\frac{3}{17}$ | $\frac{5}{16}$ | $\frac{7}{15}$ | $\frac{9}{14}$ | $\frac{11}{13}$ | $\frac{13}{12}$ | $\frac{15}{11}$ | $\frac{17}{10}$ | $\frac{19}{9}$ | $\frac{21}{8}$ | $\frac{23}{7}$ | $\frac{25}{6}$ | $\frac{27}{5}$ | $\frac{29}{4}$ |
| | $\frac{31}{3}$ | $\frac{33}{2}$ | | | | | | | | | | | | | |
| 39 | $\frac{1}{19}$ | $\frac{3}{18}$ | $\frac{5}{17}$ | $\frac{7}{16}$ | $\frac{9}{15}$ | $\frac{11}{14}$ | $\frac{13}{13}$ | $\frac{15}{12}$ | $\frac{17}{11}$ | $\frac{19}{10}$ | $\frac{21}{9}$ | $\frac{23}{8}$ | $\frac{25}{7}$ | $\frac{27}{6}$ | $\frac{29}{5}$ |
| | $\frac{31}{4}$ | $\frac{33}{3}$ | $\frac{35}{2}$ | | | | | | | | | | | | |
| 41 | $\frac{1}{20}$ | $\frac{3}{19}$ | $\frac{5}{18}$ | $\frac{7}{17}$ | $\frac{9}{16}$ | $\frac{11}{15}$ | $\frac{13}{14}$ | $\frac{15}{13}$ | $\frac{17}{12}$ | $\frac{19}{11}$ | $\frac{21}{10}$ | $\frac{23}{9}$ | $\frac{25}{8}$ | $\frac{27}{7}$ | $\frac{29}{6}$ |
| | $\frac{31}{5}$ | $\frac{33}{4}$ | $\frac{35}{3}$ | $\frac{37}{2}$ | | | | | | | | | | | |
| 43 | $\frac{1}{21}$ | $\frac{3}{20}$ | $\frac{5}{19}$ | $\frac{7}{18}$ | $\frac{9}{17}$ | $\frac{11}{16}$ | $\frac{13}{15}$ | $\frac{15}{14}$ | $\frac{17}{13}$ | $\frac{19}{12}$ | $\frac{21}{11}$ | $\frac{23}{10}$ | $\frac{25}{9}$ | $\frac{27}{8}$ | $\frac{29}{7}$ |
| | $\frac{31}{6}$ | $\frac{33}{5}$ | $\frac{35}{4}$ | $\frac{37}{3}$ | $\frac{39}{2}$ | | | | | | | | | | |
| 45 | $\frac{1}{22}$ | $\frac{3}{21}$ | $\frac{5}{20}$ | $\frac{7}{19}$ | $\frac{9}{18}$ | $\frac{11}{17}$ | $\frac{13}{16}$ | $\frac{15}{15}$ | $\frac{17}{14}$ | $\frac{19}{13}$ | $\frac{21}{12}$ | $\frac{23}{11}$ | | | |
| | $\frac{25}{10}$ | $\frac{27}{9}$ | $\frac{29}{8}$ | $\frac{31}{7}$ | $\frac{33}{6}$ | $^2\frac{35}{5}$ | $\frac{37}{4}$ | $\frac{39}{3}$ | $\frac{41}{2}$ | | | | | | |

# Arbres de nombres et conjecture de Goldbach

Denise Vella

Juillet 2007

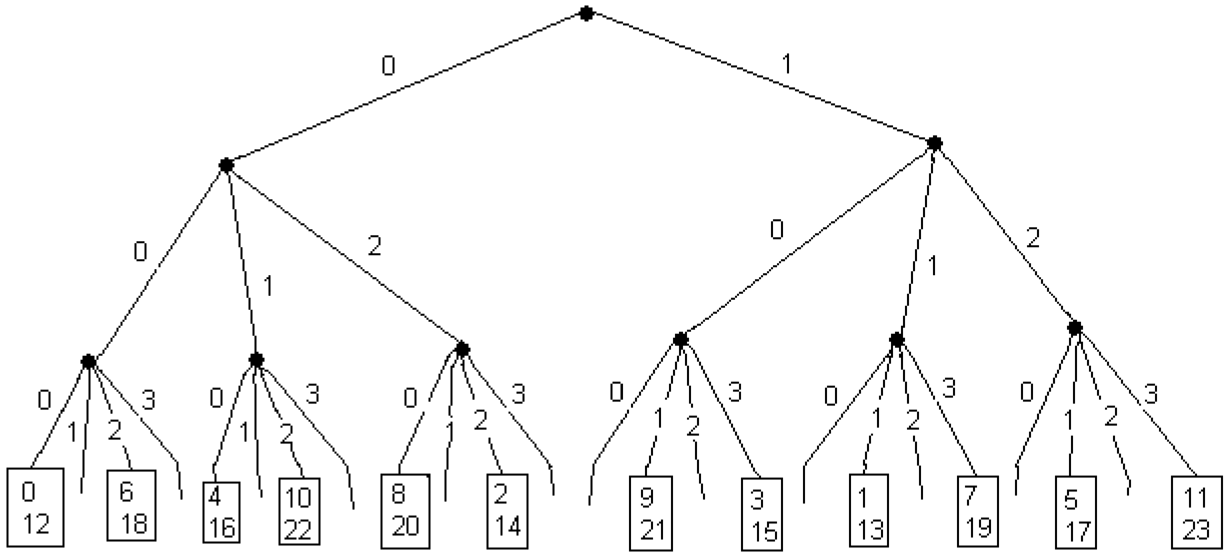
## 1 Introduction

La conjecture de Goldbach énonce que tout nombre pair supérieur ou égal à 6 est la somme de deux nombres premiers.
Dans une note précédente, on a constaté que tout nombre inférieur à $x$ et dont les restes de divisions euclidiennes par les nombres de 2 à $x$ sont différents un à un des restes de $2x$ par ces mêmes divisions a son complémentaire à $2x$ qui est premier.
En définissant des structures arborescentes qu'on appellera "arbres de restes", on "se dirigera vers" une démonstration par récurrence de la conjecture de Goldbach.

## 2 Arbres de restes

Les structures arborescentes sont très utilisées en informatique. Un arbre est un graphe connexe sans cycle. Ici, on va utiliser un arbre de classification selon les restes des divisions euclidiennes.
De la racine de l'arbre partiront systématiquement deux branches selon que le nombre à classer est pair ou impair. Les nombres pairs se retrouveront dans la partie gauche de l'arbre, et les impairs dans la partie droite. Des deux fils de la racine partiront trois branches selon le reste obtenu en divisant le nombre à classer par 3 (0, 1 ou 2). Des petits-fils de la racine partiront 4 branches, selon le reste obtenu dans une division par 4 (0, 1, 2 ou 3) et etc.
Par exemple, l'arbre de la figure ci-après est un arbre de classification des nombres de 0 à 23 selon leurs restes dans les divisions par 2, 3 et 4.

On constate différentes propriétés de l'arbre qui permettront certains raisonnements.
D'abord, toutes les feuilles de l'arbre ne sont pas "étiquetées" (ne mènent pas toutes à des nombres). Par exemple, le chemin 013 ne mène à rien : il n'existe pas de nombre qui soit à la fois de la forme $2x$, $3y$ et $4z + 3$.
Le nombre de feuilles "étiquetées" est calculable : l'arbre de niveau $n$ a $n!$ feuilles mais parmi elles, seules $PPCM(2, 3, 4, ..., n)$ sont étiquetées. Les feuilles qui sont étiquetées le sont par autant de nombres chacune.
Par exemple, l'arbre à trois niveaux a $2 \times 3 \times 4 = 24$ feuilles. Parmi elles, seules $PPCM(2, 3, 4) = 12$ sont étiquetées : une feuille sur deux est vide tandis que les feuilles étiquetées mènent à deux nombres chacune.
L'arbre à quatre niveaux quant à lui a $2 \times 3 \times 4 \times 5 = 120$ feuilles. Parmi elles,




seules $PPCM(2, 3, 4, 5) = 60$ sont étiquetées : une feuille sur deux est vide tandis que les feuilles étiquetées mènent à deux nombres chacune.
L'arbre a cinq niveaux a $2 \times 3 \times 4 \times 5 \times 6 = 720$ feuilles. Parmi elles, seules $PPCM(2, 3, 4, 5, 6) = 60$ sont étiquetées : onze feuilles sur douze sont vides tandis que les feuilles étiquetées mènent à douze nombres chacune.
Une autre propriété de l'arbre est que les nombres qui se retrouvent sur une même feuille de l'arbre constituent une progression arithmétique de nombres d'écart le PPCM des nombres de 2 au niveau de l'arbre.
Enfin, l'arbre présente une sorte de "symétrie" autour d'un axe central imaginaire. Si l'on s'intéresse à un nombre dans la partie gauche de l'arbre, auquel mène le chemin étiqueté $a_2a_3a_4$, et à son symétrique par rapport à l'axe central, auquel mène le chemin $b_2b_3b_4$, alors on a $a_2 + b_2 = 1$, $a_3 + b_3 = 2$ et $a_4 + b_4 = 3$.

## 3 Idée : les nombres associés à une même feuille de l'arbre "partagent" des décomposants Goldbach

Puisque les nombres qui sont associés à une même feuille selon un niveau donné ont le même chemin d'accès, et puisqu'on pense qu'un décomposant Goldbach d'un nombre a son chemin d'accès qui est différent de celui de ce nombre, lettre à lettre, les nombres d'une même feuille doivent "partager" des décomposants Goldbach.
On vérifie cela sur les arbres de niveau 3 et 4.
Pour l'arbre de niveau 3, cette constatation correspond à l'assertion "tout nombre pair $i$ compris entre 8 et 12 a une décomposition Goldbach en commun avec $i + 12$. Tous les nombres pairs jusqu'à 24 se voient alors attribuer au moins un

décomposant Goldbach.
Pour l'arbre de niveau 4, cette constatation correspond à l'assertion "tout nombre pair $i$ compris entre 8 et 60 a une décomposition Goldbach en commun avec $i+60$. Tous les nombres pairs jusqu'à 120 se voient alors attribuer au moins un décomposant Goldbach.
Pour l'arbre de niveau 5, cette constatation correspond à l'assertion "tout nombre pair $i$ compris entre 8 et 60 a une décomposition Goldbach en commun avec $i+60j$, pour $j$ allant de 1 à 11. Tous les nombres pairs jusqu'à 720 obéissent à la conjecture.
Pour l'arbre de niveau 6, cette constatation correspond à l'assertion "tout nombre pair $i$ compris entre 8 et 420 a une décomposition Goldbach en commun avec $i+420j$, pour $j$ allant de 1 à 11. Tous les nombres pairs jusqu'à 5040 obéissent à la conjecture de Goldbach.
Pour l'arbre de niveau 7, cette constatation correspond à l'assertion "tout nombre pair $i$ compris entre 8 et 840 a une décomposition Goldbach en commun avec $i+840j$, pour $j$ allant de 1 à 47.

Pour corroborer cette idée, j'ai fait deux tests.
Dans l'arbre 6, j'ai pris le nombre 122 au hasard, j'ai trouvé ses décomposants Goldbach et j'ai vérifié qu"il en "partageait" toujours au moins un avec les nombres de la forme $122+420j$, $j$ allant de 1 à 11.
122 a pour décomposants Goldbach les nombres premiers 13, 19, 43, 61, 79, 103 et 109. Les nombres de la forme $122+420j$ pour $j$ de 1 à 11 sont 542, 962, 1382, 1802, 2222, 2642, 3062, 3482, 3902, 4322, 4742.
Les partages de décomposants Goldbach sont les suivants :
Avec 542, 122 partage 19, 43, 79, 103 et 109.
Avec 962, 122 partage 43, 79, 103 et 109.
Avec 1382, 122 partage 61, 79 et 103.
Avec 1802, 122 partage tous ses décomposants !
Avec 2222, 122 partage 19, 43, 61, 79, et 109.
Avec 2642, 122 ne partage que 103.
Avec 3062, 122 partage 13, 43, 61 et 109.
Avec 3482, 122 partage 13, 19 et 109.
Avec 3902, 122 partage 13, 79 et 109.
Avec 4322, 122 partage 61, 79 et 103.
Avec 4742, 122 partage 13, 19, 79 et 103.

Dans l'arbre 7, j'ai vérifié que le nombre 632 partageait avec tous les nombres de la forme $632+840j$ pour $j$ allant de 1 à 47 au moins un décomposant Goldbach.

Par le "partage" des décompositions, on atteint à chaque niveau d'arbre successifs la factorielle de $n$ alors que l'arbre de niveau suivant a besoin seulement des PPCM premiers nombres pairs (toujours inférieur à la factorielle) pour en engendrer encore et encore.

# 4 Conclusion

Les petits nombres “donnent” certains de leurs décomposants Goldbach à d'autres nombres qui appartiennent à certaines progressions arithmétiques[1].

# Annexe 1 : L'arbre de niveau 5

Pour condenser l'écriture, on écrit sur une même ligne, suivi du symbole de l'ensemble vide $\emptyset$ les chemins qui n'amènent à aucun nombre. Dans la partie droite de l'arbre (chemins commençant par un 1 pour les nombres impairs), on

[1] La croissance de l'arbre des restes fait penser à la croissance d'un chou Romanesco...

a souligné les nombres premiers.

0000 : $0, 60(7), 120(7)$
0001 : $36(7), 96(7)$
0002 : $12(5), 72(5)$
0003 : $48(5), 108(5)$
0004 : $24(5), 84(5)$

0010 : $\emptyset$ 0011 : $\emptyset$ 0012 : $\emptyset$ 0013 : $\emptyset$ 0014 : $\emptyset$

0020 : $30(7), 90(7)$
0021 : $6, 66$
0022 : $42(5), 102(5)$
0023 : $18(5), 78(5)$
0024 : $54(7), 114(7)$

0030 : $\emptyset$ 0031 : $\emptyset$ 0032 : $\emptyset$ 0033 : $\emptyset$ 0034 : $\emptyset$

0100 : $40(3), 100(3)$
0101 : $16(3), 76(3)$
0102 : $52(5), 112(5)$
0103 : $28(5), 88(5)$
0104 : $4, 64$

0110 : $\emptyset$ 0111 : $\emptyset$ 0112 : $\emptyset$ 0113 : $\emptyset$ 0114 : $\emptyset$

0120 : $10(3), 70(3)$
0121 : $46(3), 106(3)$
0122 : $22(3), 82(3)$
0123 : $58(5), 118(5)$
0124 : $34(5), 94(5)$

0130 : $\emptyset$ 0131 : $\emptyset$ 0132 : $\emptyset$ 0133 : $\emptyset$ 0134 : $\emptyset$

0200 : $20(7), 80(7)$
0201 : $56(3), 116(3)$
0202 : $32(3), 92(3)$
0203 : $8, 68$
0204 : $44(3), 104(3)$

0210 : $\emptyset$ 0211 : $\emptyset$ 0212 : $\emptyset$ 0213 : $\emptyset$ 0214 : $\emptyset$

0220 : $50(3), 110(3)$
0221 : $26(3), 86(3)$
0222 : $2, 62$
0223 : $38(19), 98(19)$
0224 : $14(3), 74(3)$

0230 : $\emptyset$ 0231 : $\emptyset$ 0232 : $\emptyset$ 0233 : $\emptyset$ 0234 : $\emptyset$

1000 : ∅ 1001 : ∅ 1002 : ∅ 1003 : ∅ 1004 : ∅

1010 : 45, 105
1011 : 21, 81
1012 : 57, 117
1013 : 33, 93
1014 : 9, 69

1020 : ∅ 1021 : ∅ 1022 : ∅ 1023 : ∅ 1024 : ∅

1030 : 15, 75
1031 : 51, 111
1032 : 27, 87
1033 : 3, 63
1034 : 39, 99

1100 : ∅ 1101 : ∅ 1102 : ∅ 1103 : ∅ 1104 : ∅

1110 : 25, 85
1111 : 1, 61
1112 : 37, 97
1113 : 13, 73
1114 : 49, 109

1120 : ∅ 1121 : ∅ 1122 : ∅ 1123 : ∅ 1124 : ∅

1130 : 55, 115
1131 : 31, 91
1132 : 7, 67
1133 : 43, 103
1134 : 19, 79

1200 : ∅ 1201 : ∅ 1202 : ∅ 1203 : ∅ 1204 : ∅

1210 : 5, 65
1211 : 41, 101
1212 : 17, 77
1213 : 53, 113
1214 : 29, 89

1220 : ∅ 1221 : ∅ 1222 : ∅ 1223 : ∅ 1224 : ∅

1230 : 35, 95
1231 : 11, 71
1232 : 47, 107
1233 : 23, 93
1234 : 59, 119

# Annexe 2 : Extrait d'une biographie de Poincaré concernant la démonstration par récurrence

Le texte qui suit est extrait de la biographie "Poincaré : philosophe et mathématicien" d'Umberto Bottazzini aux éditions Belin Pour la Science.

Le raisonnement par récurrence : le terrain le plus naturel et le plus favorable pour cette étude est l'arithmétique élémentaire, c'est à dire les opérations mettant en jeu des nombres entiers. Quand nous analysons des opérations telles que l'addition et la multiplication, nous nous rendons compte qu'un type de raisonnement se "retrouve à chaque pas", c'est la démonstration "par récurrence" : "on établit d'abord un théorème pour $n$ égal à 1 ; on montre ensuite que, s'il est vrai de $n-1$, il est vrai de $n$, et on en conclut qu'il est vrai pour tous les nombres entiers." C'est là le "raisonnement mathématique par excellence", déclare Poincaré. Sa particularité est "qu'il contient, sous une forme condensée, une infinité de syllogismes", et qu'il permet de passer du particulier au général, du fini à l'infini, concept qui apparaît dès les premiers pas de l'arithmétique élémentaire et sans lequel "il n'y aurait pas de science parce qu'il n'y aurait rien de général", mais uniquement des énoncés particuliers.
D'où nous vient ce "raisonnement pas récurrence", s'interroge Poincaré ? Certainement pas de l'expérience. Celle-ci peut nous suggérer que la règle est vraie pour les dix ou les cent premiers nombres, mais elle est désarmée face à l'infinité de tous les nombres naturels. Le principe de contradiction (on dirait aujourd'hui le raisonnement par l'absurde) est aussi impuissant : il nous permet d'obtenir certaines vérités, mais non d'en enfermer une infinité en une seule formule. "Cette règle (le raisonnement par récurrence), inaccessible à la démonstration analytique et à l'expérience, est le véritable type du jugement synthétique *a priori*, conclut Poincaré. L"'irrésistible évidence" avec laquelle ce "principe" s'impose n'est autre que "l'affirmation de la puissance de l'esprit qui se sait capable de concevoir la répétition indéfinie d'un même acte dès que cet acte est une fois possible"...

# Changer l'ordre sur les entiers naturels pour comprendre le partage des décomposants Goldbach

Denise Vella

Octobre 2007

## 1 Introduction

La conjecture de Goldbach (1742) énonce que tout nombre pair supérieur ou égal à 6 est la somme de deux nombres premiers.
Cette note présente un nouvel ordre sur les entiers, basé sur un système de numération par les restes modulaires découlant du théorème des restes chinois, qui vise à faire appréhender la façon dont les nombres pairs partagent des décomposants Goldbach[1].
Je remercie Denis Guedj d'avoir fait "revivre Cantor" par son livre "Villa des hommes" paru en septembre 2007 et Nathalie Charraud pour la même raison par son livre "Infini et Inconscient : essai sur Georg Cantor".

## 2 Deux anecdotes en école élémentaire

La première anecdote est inventée ; la seconde est vécue[2].

Imaginons une maîtresse de CP qui demande à un élève de ranger un ensemble de formes géométriques selon leur couleur. Après une réalisation laborieuse de la consigne par l'élève, elle lui demande "Combien y-a-t-il de rectangles ?" L'élève est en droit de se rebeller : "Comment ? On me demande un classement. Je m'attends à une question en relation avec le classement effectué du style "combien y-a-t-il de formes de couleur bleue par exemple ?" et on me pose au lieu de cela une question qui m'oblige à littéralement "bouleverser" mon classement". Dans la suite de cette note, j'ai postulé que l'on n'arrivait pas à prouver la conjecture de Goldbach car on n'avait pas utilisé encore le bon "classement" des entiers naturels.

Deuxième exemple, vécu cette fois. Il peut arriver, en classe de CE2, lorsqu'on introduit les milliers en numération que des élèves qui ont à ranger des nombres dans l'ordre croissant écrivent par mégarde que 1236 est plus petit que 702. L'explication de ce fait peut être que l'ordre lexicographique du dictionnaire qu'ils ont acquis se "télescope" alors avec l'ordre engendré par le système de numération décimale et les élèves appliquent la règle "j'ordonne les mots (là, il

[1] On appelle décomposant Goldbach d'un nombre pair donné un nombre premier qui est terme d'une somme de deux nombres premiers de valeur égale au nombre pair en question.

[2] Après 8 années d'ingéniorat d'informatique, je me suis reconvertie professeur des écoles.

s'agit de nombres) en observant leur première lettre (là, il s'agit de chiffres) ; s'il y a égalité, je m'occupe de la deuxième lettre, etc". Et ils oublient de regarder en premier lieu et tout simplement le "nombre" de chiffres des nombres à comparer. Dans le dictionnaire, le mot "alphabet" est avant le mot "bol" par exemple, bien que comptant beaucoup plus de lettres que ce dernier car $a$ est avant $b$ dans l'ordre alphabétique et donc cela peut ne pas être choquant pour un élève que 1236 soit inférieur à 702 dans la mesure où 1 est inférieur à 7[3].

Dans la suite, on introduira un ordre lexicographique (utilisant d'ailleurs la notion de préfixe) dans un système de représentation des entiers naturels par leurs restes chinois.

## 3 Théorème des restes chinois et système de numération par n-uplets de restes

J'ai dans un premier temps voulu ordonner lexicographiquement les entiers de 0 à 210 (qui est le produit des quatre premiers nombres premiers 2, 3, 5 et 7) en les représentant chacun par leurs quatre restes dans les divisions par ces nombres premiers. J'ai obtenu l'ordre suivant, étonnant, dû au théorème des restes chinois. Les résultats sont présentés dans deux tableaux (le tableau correspondant aux nombres pairs s'obtient par complémentarité à 209), un pour les nombres pairs, et un pour les nombres impairs. Les en-têtes des lignes fournissent les restes des divisions des nombres se trouvant dans les cases du tableau par 2, 3 et 5 (ou classes d'équivalences modulo 2, 3 ou 5), et les en-têtes de colonnes fournissent le reste de la division des nombres des cases de la colonne par 7 (ou classe d'équivalence modulo 7). On a coloré les nombres premiers en bleu.

| | $(---6)$ | $(---5)$ | $(---4)$ | $(---3)$ | $(---2)$ | $(---1)$ | $(---0)$ |
|---|---|---|---|---|---|---|---|
| $(124-)$ | 0 | 89 | 179 | 59 | 149 | 29 | 119 |
| $(123-)$ | 83 | 173 | 53 | 143 | 23 | 113 | 203 |
| $(122-)$ | 167 | 47 | 137 | 17 | 107 | 197 | 77 |
| $(121-)$ | 41 | 131 | 11 | 101 | 191 | 71 | 161 |
| $(120-)$ | 125 | 5 | 95 | 185 | 65 | 155 | 35 |
| $(114-)$ | 139 | 19 | 109 | 199 | 79 | 169 | 49 |
| $(113-)$ | 13 | 103 | 193 | 73 | 163 | 43 | 133 |
| $(112-)$ | 97 | 187 | 67 | 157 | 37 | 127 | 7 |
| $(111-)$ | 181 | 61 | 151 | 31 | 121 | 1 | 91 |
| $(110-)$ | 55 | 145 | 25 | 115 | 205 | 85 | 175 |
| $(104-)$ | 69 | 159 | 139 | 129 | 9 | 99 | 189 |
| $(103-)$ | 153 | 33 | 123 | 33 | 93 | 183 | 63 |
| $(102-)$ | 27 | 117 | 207 | 87 | 177 | 57 | 147 |
| $(101-)$ | 111 | 201 | 81 | 171 | 51 | 141 | 21 |
| $(100-)$ | 195 | 75 | 165 | 45 | 135 | 15 | 105 |

L'énoncé du théorème des restes chinois (qui date du troisième siècle et a été développé par le mathématicien chinois Sun Tzu) est le suivant :

[3]Concernant le traitement de l'erreur en didactique des mathématiques, on consultera "l'âge du capitaine" de Stella Baruk [22].

*Soient k nombres entiers naturels* $m_1,\ m_2,\ ...,\ m_k$
*premiers entre eux deux à deux*
*et k entiers* $r_1,\ r_2,\ ...,\ r_k$,
*le système de congruence*
$$\begin{cases} x \equiv r_1\ (mod\ m_1) \\ x \equiv r_2\ (mod\ m_2) \\ ... \\ x \equiv r_k\ (mod\ m_k) \end{cases}$$
*admet une unique solution modulo* $M = m_1 m_2 ... m_k$

A cause du théorème des restes chinois, chaque entier est solution d'une infinité de systèmes de congruences.
Par exemple, l'entier 26 est solution du système :

$$\begin{cases} x \equiv 0\ (mod\ 2) \\ x \equiv 2\ (mod\ 3) \end{cases}$$

mais également du système :

$$\begin{cases} x \equiv 0\ (mod\ 2) \\ x \equiv 2\ (mod\ 3) \\ x \equiv 1\ (mod\ 5) \end{cases}$$

ou encore du système :

$$\begin{cases} x \equiv 0\ (mod\ 2) \\ x \equiv 2\ (mod\ 3) \\ x \equiv 1\ (mod\ 5) \\ x \equiv 5\ (mod\ 7) \\ x \equiv 4\ (mod\ 11) \\ x \equiv 0\ (mod\ 13) \\ x \equiv 9\ (mod\ 17) \\ x \equiv 7\ (mod\ 19) \\ x \equiv 3\ (mod\ 23) \\ x \equiv 26\ (mod\ 29) \\ x \equiv 26\ (mod\ 31) \\ x \equiv 26\ (mod\ 37) \end{cases}$$

On peut donc associer à tout entier plusieurs représentations par des n-uplets de restes. En l'occurence, on pourrait associer à 26 les représentations par n-uplets de restes suivantes : $(0, 2)$ ou $(0, 2, 1)$ ou $(0, 2, 1, 5, 4, 0, 9, 7, 3, 26, 26, 26)$.
Un tel système de numération[4] permet de représenter un grand nombre entier par un ensemble d'entiers plus petits et est notamment utilisé en cryptographie.

On trouve dans [3] quelques points forts de l'histoire du théorème chinois des restes (notamment sa première formulation dans le traité classique de Sunzi, puis son apparition dans les Neufs Chapitres[5] ou dans le Liber Abbaci de Fibonnacci ; le théorème des restes chinois a été également présenté par Euler, ou

[4] appelé RNS dans la littérature anglo-saxonne pour Residue Numeration System.

[5] Mon nom d'épouse est Chemla ; ce nom est également celui d'une mathématicienne et épistémologue française renommée qui a réalisé un travail considérable d'analyse des Neufs Chapitres. Cela fait au moins deux personnes nommées Chemla et s'intéressant au théorème des restes chinoisn !

bien de façon plus contemporaine par Shockley, Prather, ou Weiss).
Notons ici qu'on le trouve également dans le paragraphe 38 des Recherches Arithmétiques de Gauss mais reformulé par des congruences (que Gauss a inventéees). Si l'on considère chaque congruence comme représentant un ensemble d'entiers naturels, on peut dire que chaque entier est solution d'une multitude de systèmes de congruence correspondant à différents ensembles de nombres auxquels il appartient (éventuellement "inclus" les uns dans les autres).

Une formulation m'intéresse parmi toutes celles présentées par Davis et Hersh ; elle est d'abord présentée succinctement, puis analysée précisément un peu plus loin. Il s'agit de la formulation du théorème des restes chinois par Prather, un "savant informaticien contemporain".

*Si* $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ *est la décomposition de l'entier n en facteurs premiers* $(p_i^{\alpha_i} = q_i)$
*alors le groupe cyclique* $Z_n$ *a la représentation produit* $Z_{q_1} \times Z_{q_2} \times ... \times Z_{q_r}$.

L'analyse extraite de "l'Univers mathématique" de Davis et Hersh de la formulation par Prather du théorème des restes chinois est fournie en annexe 2.

Ma formation initiale est une formation en informatique[6]. Cette formation incluait notamment un cours de théorie des langages et automates[7].
Dans cette théorie, on définit un alphabet A comme un ensemble fini non vide de symboles. On appelle monoïde libre engendré par A l'ensemble A* muni de la concaténation des mots[8]. Enfin, on appelle langage sur l'alphabet A ou langage de A* tout ensemble de mots de A*. Autrement dit, un langage sur A est un sous-ensemble de A*.

Nous avons choisi de représenter les entiers par des n-uplets de restes. Cela présente deux particularités, si l'on considère les représentations par restes comme les mots d'un langage dans la théorie des langages :

- l'alphabet d'appartenance des lettres des mots est infini, c'est $\mathbb{N}$,
- à chaque entier pourrait être associée une infinité dénombrable de mots en bijection avec $\mathbb{N}$ selon la longueur du n-uplet de représentation que l'on choisit.

Pour pallier au deuxième inconvénient, on va choisir d'associer à chaque entier un unique n-uplet le représentant, en ne s'intéressant qu'aux modules premiers inférieurs à sa racine. On considère ainsi l'unique système de congruences selon les nombres premiers inférieurs à la racine du nombre que l'on veut représenter[9].
Fournissons quelques exemples de représentations :
14 et 20 ont pour représentations (0,2).
38 a pour représentation (0, 2, 3).
76 a pour représentation (0,1,1,6).

[6] J'ai obtenu un DEA d'intelligence artificielle en 1987.
[7] Le paragraphe suivant présentant des définitions est extrait du livre [2].
[8] A* consiste à introduire le mot particulier appelé "mot vide" de longueur nulle.
[9] Delahaye présente ce "système de numération en nombres premiers" (page 72 de son livre "Merveilleux nombres premiers").

# 4 Hilbert, Cantor et la notion d'ordre sur les entiers

Dans une biographie de Hilbert, on trouve que "Hilbert affirme la résolubilité de tout problème mathématique". Il écrit "Jamais le mathématicien ne sera réduit à dire Ignorabimus". Cette conviction lui fait dire à Klein : "Il vous faut avoir un problème. Choisissez un objectif déterminé et marchez franchement vers lui. Vous pourrez ne jamais atteindre le but mais vous trouverez sûrement quelque chose d'intéressant en chemin."

La conjecture de Goldbach, comme la conjecture des nombres premiers jumeaux ou essentiellement l'hypothèse de Riemann, fait partie du huitième problème de la liste de 23 problèmes exposée en 1900 par Hilbert. Hilbert avait placé en tête de ses 23 problèmes celui de l'hypothèse du continu de Cantor[10].

Enfin, Hilbert écrit ceci de l'ordre sur les entiers : "l'ordre dit naturel des nombres d'un système est celui où l'on regarde un plus petit nombre comme précédant un plus grand qui sera de son côté regardé comme suivant le premier. Il y a, c'est facile à voir, une infinité d'autres manières d'ordonner les nombres d'un système". Hilbert dit également "Nul ne doit nous exclure du paradis que Cantor a créé".

Cantor a créé la théorie des ensembles, a inventé les nombres "transfinis". Si l'on souhaite avoir des détails sur les avancées majeures qu'il a apportées aux mathématiques, on consultera les références [4], [5], [6] et [14] ainsi que ses oeuvres sur Gallica. Il est à l'origine de l'idée de modifier l'ordre sur les entiers. Citons une phrase de Cantor illustrant sa prise de conscience du bouleversement qu'il introduit : "Ce-disant, je ne dissimule en aucune façon que par cette entreprise, j'entre en opposition, dans une certaine mesure, avec des conceptions largement répandues concernant l'infini mathématique et avec les points de vue que l'on a fréquemment adoptés sur l'essence de la grandeur numérique.".

Présentons maintenant un exemple classique de bouleversement de l'ordre sur les entiers que Cantor propose et qui va nous amener à définir un ordre qui semble pertinent pour comprendre la conjecture de Goldbach. D'ailleurs, Cantor s'est intéressé à la conjecture de Golbach en 1894 et en a publié une table de vérification jusqu'à 1000 au congrès de l'AFAS.

Si par exemple, on décide de réordonner les entiers en énumérant dans un premier temps tous les entiers pairs puis tous les entiers impairs, les entiers seront énumérés selon l'ordre suivant :

$$0, 2, 4, 6, 8, ..., 1, 3, 5, 7, ...$$

(et 1 non seulement se retrouvera à la position $\omega + 1$ où $\omega$ désigne le nombre d'éléments d'un ensemble infini dénombrable, en l'occurence l'ensemble des nombres pairs, en bijection avec $\mathbb{N}$, mais de surcroît, 1 n'aura pas de prédécesseur ; cela semble vertigineux et l'on se demande dans quelle mesure on

[10] Cohen a démontré l'indécidabilité de cette hypothèse.

peut s'acclimater à ces sortes d'ordres tant ils ne nous sont pas "naturels"). Dans [5], N. Charraud nous explique que Cantor, grâce à ses ordres, peut faire des rapprochements inattendus et démontre que divers objets peuvent se trouver comparables. Pour illustrer ses types d'ordre, il montre même comment associer un type d'ordre à une peinture ou à une symphonie. Il se place ainsi en précurseur de la numérisation de l'information qui envahit tous les champs de connaissance actuellement.

N. Charraud signale également le souci du style de présentation des résultats et de la transmission qui motive Cantor. Il insiste en effet sur "l'effort de présenter le cheminement de pensée aussi clairement que possible" et admire particulièrement les exposés d'Hermite pour leur limpidité : "Le style personnel de Cantor va avec le souci de communiquer de la façon la plus transparente possible le processus et les étapes de sa découverte".

Ce souci de limpidité se retrouve chez Hilbert, dans un extrait de sa conférence de 1900 : "On peut néammoins se demander s'il n'existe pas des attributs généraux caractérisant un bon problème de mathématiques. Un mathématicien français des temps passés a dit : "une théorie mathématique ne doit être regardée comme parfaite que si elle a été rendue tellement claire qu'on puisse la faire comprendre au premier individu rencontré dans la rue". Cette clarté, cette limpidité si énergiquement exigée ici d'une théorie mathématique, je l'exigerai encore davantage d'un problème mathématique parfait ; ce qui est clair et limpide nous attire en effet, ce qui est embrouillé nous rebute".

Il y a un an quand j'ai lu la biographie de Cantor par J.P.Belna [14], j'ai essayé d'utiliser la notion de bijection entre ensembles pour accéder à la conjecture de Goldbach ; j'étais partie de la façon suivante : l'ensemble des nombres pairs ayant l'une de leurs décompositions Goldbach faisant intervenir 3 est infini dénombrable (3+3=6, 3+5=8, 3+7=10, 3+11=14,...). De même, l'ensemble des nombres pairs faisant intervenir 5 dans l'une des décompositions Goldbach est également infini dénombrable : 5+5=10, 5+7=12, 5+11=16,...). Et de même pour chacun des ensembles de nombres pairs engendrables par chacun des nombres premiers qui sont en nombre infini. Si on fait l'union de tous ces ensembles infinis dénombrables, on obtient un ensemble infini dénombrable, qu'on peut mettre en bijection avec $\mathbb{N}$, l'ensemble des entiers naturels. Les intersections de ces ensembles sont parfois non vides : 3+7=5+5, par exemple. D'autre part, l'ensemble des nombres pairs est aussi en bijection avec l'ensemble des entiers naturels. Pour autant, cela ne me permettait pas d'assurer que l'on ne "ratait" aucun entier.

# 5 Un ordre inhabituel sur les entiers

Selon Hermann Weyl, il revient à chaque utilisateur de créer son propre ensemble de nombres selon la réalité qu'il souhaite modéliser. Une excellente présentation de la façon dont l'homme a "construit les différentes sortes de nombres" est à trouver dans l'ouvrage de Claude-Paul Bruter [1].

En ce qui concerne une justification éventuelle de la conjecture de Goldbach, citons un extrait de [3] : "l'ordre à partir du chaos n'est pas toujours arrivé à si bon compte. Suivant une conjecture non encore prouvée (1984) de Goldbach

(1690 - 1764), tout nombre pair est la somme de deux nombres premiers. Par exemple, $24 = 5 + 19$. Ceci peut se produire de plusieurs manières différentes : $24 = 7 + 17 = 11 + 13$. La liste suivante obtenue par ordinateur[11] donne la décomposition de nombres pairs en somme de deux nombres premiers, où le premier terme est le plus petit possible (et le second, le plus grand possible). Le chaos est clair. Mais quel est l'ordre sous-jacent ? La démonstration de la conjecture de Goldbach, si jamais elle arrive, peut apporter de l'ordre dans ce chaos".

Reprenons ici les mots de l'article d'Euler "Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs" : Les mathématiciens ont tâché jusqu'ici en vain à découvrir quelque ordre dans la progression des nombres premiers, et on a lieu de croire que c'est un mystère auquel l'esprit humain ne sauroit jamais pénétrer. Pour s'en convaincre, on n'a qu'à jeter les yeux sur les tables des nombres premiers, que quelques-uns se sont donnés la peine de continuer au-delà de cent mille et on s'apercevra qu'il n'y règne aucun ordre ni règle".

Si l'on observe finement la liste de décompositions fournie par Davis et Hersh[12], on constate une coïncidence troublante qui fait penser à un "motif" de nombres premiers qui se répètent (en l'occurrence 3, 5, 3, 5, 7, 13, 11, 13, 19, 17, 19, 3) et qui sont décomposants Goldbach des nombres 20902 et suivants et des nombres 20962 et suivants (je les ai positionnés en regard les uns des autres en annexe 1). Les tables de nombres premiers nous ont habitués à une présentation si chaotique, "sans schéma discernable de régularité" qu'on a beaucoup de mal à penser que la répétition d'un tel "motif" soit absolument accidentelle. On va imaginer comment un nouvel ordre sur les entiers pourrait expliquer cette coïncidence.

Choisissons comme "bon ordre" l'ordre lexicographique sur les représentations par les restes. Selon cet ordre, tous les entiers pairs sont plus petits que 1 puisque le n-uplet représentant chacun d'eux a 0 comme première coordonnée alors que celui de 1 a 1 comme première coordonnée. Mais ce qui est troublant, c'est que 6 est plus petit que 2 car 2 est congru à 2 (modulo 3) alors que 6 est congru à 0 (modulo 3). On définit la relation d'ordre suivant :

$$
\begin{array}{ll}
 & a < b \\
\iff & \textit{la représentation par restes de a est un préfixe de la représentation par restes de b} \\
 & (\textit{i.e. il y a partage de toutes les coordonnées communes}).
\end{array}
$$

Pour chercher des décomposants Goldbach partagés, on s'intéressera dans un premier temps aux préfixes les plus longs possibles, c'est à dire dont la représentation par les restes a seulement une lettre en moins que celle du mot auquel on s'intéresse.

[11] Je reproduis cette liste en annexe 1.

[12] voir annexe 1.

Ci-dessous, fournissons les représentations par restes des nombres de 6 à 100.

| | |
|---|---|
| $6 : (0)$ | $54 : (0, 0, 4, 5)$ |
| $8 : (0)$ | $56 : (0, 2, 1, 0)$ |
| $10 : (0, 1)$ | $58 : (0, 1, 3, 2)$ |
| $12 : (0, 0)$ | $60 : (0, 0, 0, 4)$ |
| $14 : (0, 2)$ | $62 : (0, 2, 2, 6)$ |
| $16 : (0, 1)$ | $64 : (0, 1, 4, 1)$ |
| $18 : (0, 0)$ | $66 : (0, 0, 1, 3)$ |
| $20 : (0, 2)$ | $68 : (0, 2, 3, 5)$ |
| $22 : (0, 1)$ | $70 : (0, 1, 0, 0)$ |
| $24 : (0, 0)$ | $72 : (0, 0, 2, 2)$ |
| $26 : (0, 2, 1)$ | $74 : (0, 2, 4, 4)$ |
| $28 : (0, 1, 3)$ | $76 : (0, 1, 1, 6)$ |
| $30 : (0, 0, 0)$ | $78 : (0, 0, 3, 1)$ |
| $32 : (0, 2, 2)$ | $80 : (0, 2, 0, 3)$ |
| $34 : (0, 1, 4)$ | $82 : (0, 1, 2, 5)$ |
| $36 : (0, 0, 1)$ | $84 : (0, 0, 4, 0)$ |
| $38 : (0, 2, 3)$ | $86 : (0, 2, 1, 2)$ |
| $40 : (0, 1, 0)$ | $88 : (0, 1, 3, 4)$ |
| $42 : (0, 0, 2)$ | $90 : (0, 0, 0, 6)$ |
| $44 : (0, 2, 4)$ | $92 : (0, 2, 2, 1)$ |
| $46 : (0, 1, 1)$ | $94 : (0, 1, 4, 3)$ |
| $48 : (0, 0, 3)$ | $96 : (0, 0, 1, 5)$ |
| $50 : (0, 2, 0, 1)$ | $98 : (0, 2, 3, 0)$ |
| $52 : (0, 1, 2, 3)$ | $100 : (0, 1, 0, 2)$ |

Voyons les relations d'ordre entre les nombres maintenant :
10, 12, 14, 16, 18, 20, 22 et 24 ont tous pour préfixes 6 ou 8 et ils partagent tous un décomposant Goldbach avec au moins l'un des deux.
26, 32, 38 et 44 ont pour préfixes 14 ou 20 et le partage d'au moins un décomposant Goldbach a systématiquement lieu.
28, 34, 40 et 46 ont pour préfixes 10, 16 ou 22 et on parvient à la même conclusion au niveau des partages de décomposants.
On va dans la section suivante essayer d'expliquer du mieux possible ce partage des décomposants.

# 6 Partage des décomposants Goldbach

Dans une note précédente, on a constaté que tout nombre inférieur à $x$ et dont les restes de divisions euclidiennes par les nombres de 2 à $x$ sont différents un à un des restes de $2x$ par ces mêmes divisions a son complémentaire à $2x$ qui est premier. Ecrivons cela en utilisant une notation en langage mathématique :

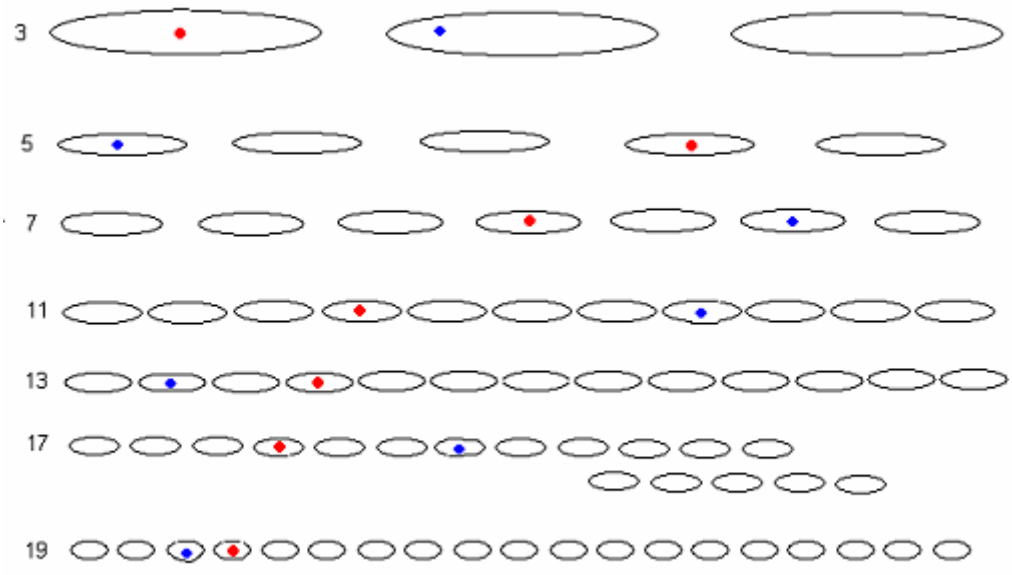
$\forall\ 2x$
$\forall\ p_1$ *premier impair inférieur ou égal à* $x$
$\forall\ q$ *premier impair inférieur ou égal à* $x$,
$2x \not\equiv p_1\ (mod\ q) \iff p_2 = 2x - p_1$ *premier impair supérieur ou égal à* $x$
$(2x = p_1 + p_2$ *est appelée une décomposition Goldbach de* $2x)$.

En effet,

$$
\begin{aligned}
& 2x \not\equiv p_1 \ (mod\ q) \\
\iff\ & 2x - p_1 \not\equiv 0 \ (mod\ q) \\
\iff\ & 2x - p_1 \textit{ est un nombre premier car il n'est divisible par aucun autre nombre premier } q
\end{aligned}
$$

On fournissait l'exemple du nombre pair 40 : les nombres impairs inférieurs à 20 qui sont incongrus à 40 selon tout nombre premier inférieur à 20 sont les nombres 3, 9, 11 et 17. Tous ces nombres ont leur complémentaire à 40 qui est premier. On constate que l'ensemble des nombres qui ont leur complémentaire à $2x$ qui est premier peut à la fois contenir des nombres premiers et des nombres composés.

L'énoncé présenté ci-dessus est vrai. Cependant, il pourrait être vrai par vacuité, c'est à dire vrai alors qu'il n'existerait aucun $p_1$ le vérifiant. Démontrer la conjecture de Goldbach consiste à démontrer que cet énoncé ne peut jamais être vrai par vacuité.
Représentons cela dans la théorie des ensembles. Ci-dessous sont dessinés les résidus possibles selon chaque nombre premier inférieur à 20 (3 classes de congruence modulo 3, 5 classes de congruence modulo 5, etc). Par convention, on dessine la classe 0 à l'extrême-gauche du dessin. Les points bleus représentent l'appartenance de 40. 3 permet de trouver une décomposition Goldbach de 40 car 3 n'est jamais dans le même ensemble de congruence que 40. Démontrer la conjecture de Goldbach consiste donc à démontrer qu'il existe toujours un nombre premier qui ne partage aucune classe de congruence avec 2x. Les nombres impairs inférieurs à 20 qui ne partagent aucune classe de congruence avec 40 ont leur complémentaire à 40 qui est premier (ce sont ici 3, 9, 11 et 17).




Un professeur a insisté sur le fait qu'il fallait que j'adopte une méthode constructiviste. J'ai donc essayé de trouver comment un nombre pair pourrait

"hériter" ses décomposants Goldbach d'autres nombres pairs plus petits que lui (et d'ailleurs, du coup, les transmettre à des nombres pairs plus grands que lui).

# 7 Descente infinie de Fermat

Quand cet été, j'ai décidé de me "fixer" définitivement sur la numération par restes pour étudier le partage des décomposants Goldbach[13], j'étais persuadée qu'il fallait suivre la recommandation de Poincaré et essayer d'établir une démonstration par récurrence. Mais le problème est que rien ne lie les décompositions Goldbach de deux entiers successifs car les décomposants devant être incongrus selon tous les modules inférieurs à $x$ au nombre pair $2x$ considéré, tout distingue deux entiers successifs représentés par leurs restes modulaires puisqu'ils n'ont aucun reste en commun ; le mode de raisonnement par récurrence semblait donc très mal adapté. Le fait de choisir plutôt comme ordre l'ordre lexicographique des représentations par restes des entiers fait que l'on ne se place plus dans l'axiomatique de Peano. Je crois qu'associé à l'idée de nouvel ordre sur les entiers, le raisonnement appelé "descente infinie de Fermat" est plus adapté à la conjecture de Goldbach.

On trouve par exemple dans [4] une présentation de ce mode de raisonnement ; il repose sur le fait qu'il n'existe pas de suite infinie strictement décroissante d'entiers positifs.

L'ensemble $\mathbb{N}$ des entiers naturels et toutes ses parties propres non vides possèdent une propriété remarquable : ils admettent un plus petit élément.
Imaginons que nous voulions démontrer qu'une certaine propriété $P(n)$ est impossible ($n$ est un entier naturel). On raisonne par l'absurde en supposant $P(n)$ vraie pour un certain entier $n$ (la partie $E$ de $\mathbb{N}$ où $P(n)$ est vraie est donc non vide). Si nous sommes capables de montrer que P est alors vraie pour un entier strictement inférieur à $n$, nous aboutirons à une contradiction. En effet, si $a$ désigne le plus petit élément de $E$, on a simultanément $P(a)$ vraie et $P(b)$ vraie avec $b < a$. L'entier $b$ appartient donc à $E$ et est strictement plus petit que le plus petit élément de $E$. D'où la contradiction.

Puisqu'il semble qu'un entier "partage" toujours ses décomposants avec des nombres entiers plus petits que lui au sens du nouvel ordre que nous avons défini sur les entiers, si un nombre pair ne vérifiait pas Goldbach, il y aurait un nombre entier plus petit que lui (au moins) qui ne la vérifierait pas non plus mais cela est impossible puisqu'il n'existe pas de suite strictement décroissante infinie d'entiers naturels. Donc la conjecture de Goldbach doit être vraie.

# 8 Les chemins empruntés, les souvenirs engrangés

Depuis deux ans, j'ai emprunté de multiples chemins, pour essayer de comprendre la conjecture de Goldbach. Au début, je l'ai lue autrement : "tout nombre entier supérieur ou égal à 2 est moyenne de deux nombres premiers (ou bien est à égale distance de deux premiers)". Peu après, j'en ai trouvé une

[13] J'avais écrit une note à Noël 2006 qui s'appelait "propriétés de symétrie d'une table de congruence" et qui utilisait déjà cette représentation.

représentation géométrique dont j'espérais qu'elle serait fructueuse. Après cela, je me suis intéressée aux séquences de valuations p-adiques, qui sont autant de séquences fractales d'entiers. En additionnant les exposants intervenant dans les factorisations des entiers successifs, j'obtenais une séquence fractale d'entiers dont les $log(n)$ premiers éléments ayant 1 pour image étaient d'indices premiers. En représentant graphiquement les empilements de valuations p-adiques, je suis "tombée" sur une courbe logarithmique (que je me suis outrancièrement expliquée par le TNP d'Hadamard et La Vallée-Poussin). J'ai découvert une note de Laisant dans le Bulletin de la SMF (tome 25 de l'année 1897) avec qui je partageais une vision, selon laquelle les nombres premiers effectuaient une sorte de danse de salon les uns en face des autres (pour Laisant, c'était des tirettes que l'on faisait coïncider [21]). Puis j'ai fait un détour par la théorie des graphes, toujours sans aucun succès. Alors, lors de l'été 2006, j'ai découvert les groupes et Galois, sous prétexte que l'on pouvait associer certaines décompositions Goldbach aux sommets de polyèdres imaginaires. Enfin, aux environs de Noël 2006, j'ai cru en avoir terminé car j'avais alors trouvé que la conjecture de Goldbach peut être reformulée de la façon suivante : quelque soit $2x$ un nombre pair, il existe une suite décroissante de $x-1$ entiers successifs et inférieurs strictement à $2x-1$ qui ne sont pas divisibles un à un par les éléments de la suite croissante des nombres entiers de 2 à $x$ mais cela restait à établir. Je trouvais qu'il suffisait (sic) d'associer à tout entier un certain nombre de fractions rationnelles dont il s'agissait de tester le caractère entier ou non...
Pendant tout ce temps, je me suis servie de l'informatique pour vérifier mes idées (autant que faire se peut dans la mesure où l'infini informatique est une poussière devant l'infini mathématique) ; j'adoptais une démarche expérimentale, par essais et erreurs. Le programme le plus intéressant intellectuellement a été celui du calcul de la somme des diviseurs des entiers, par un algorithme récursif inventé par Euler et qui est en relation avec son théorème pentagonal. L'article *"Découverte d'une loi toute extraordinaire des nombres par rapport à la somme de leurs diviseurs"* [10] décrit cet algorithme et est très impressionnant. L'émerveillement du mathématicien devant la "magie" des nombres s'en dégage de façon intemporelle. On programme donc récursivement le calcul de la somme des diviseurs mais la formule reste hermétiquement incompréhensible[14]. Tout au long de ce travail, j'ai échangé souvent avec quelques professeurs qui ont été bienveillants à mon égard et je les en remercie.

# 9 Conclusion

Citons Henri Cohen : "à la différence de l'hypothèse de Riemann, la conjecture de Goldbach n'a pas d'intérêt en soi, outre le pur défi qu'elle pose". La légende court selon laquelle Gauss aurait dit à propos de la conjecture de Goldbach ou d'une conjecture similaire qu'il pouvait en écrire de nombreuses du même genre et que cela ne présentait pas d'intérêt de résoudre de tels problèmes. Gauss a entre autres inventé le langage des congruences, a conjecturé le TNP, a prouvé le théorème fondamental de l'algèbre, a démontré de multiples façons la loi de réciprocité quadratique. Quant à Cantor, on sait qu'il s'est intéressé à la

[14]Il y a peut-être une formule récursive semblable qui lie entre elles les décompositions Goldbach de certains entiers ou les nombres de telles décompositions.

conjecture de Goldbach et on peut se demander si c'est elle qui l'a amené à définir ses types d'ordre[15]. Le travail présenté ici illustre en quelque sorte une fable dont le titre pourrait être "les géants et la fourmi" ou bien "les théoriciens et l'ingénieur" au sens où je n'ai fait qu'essayer d'utiliser les outils théoriques qu'ils avaient élaborés pour résoudre ce problème que je me suis approprié.
Je ne sais pas si les idées qui ont été présentées pourraient servir à mener à bien une démonstration de la conjecture de Goldbach. Ma promenade promet d'être encore longue et pour la première fois depuis deux ans, j'ai l'impression d'avoir enfin emprunté le bon chemin. J'aime beaucoup le titre d'un livre de Hawking qui est "Sur les épaules des géants". Par la lecture de tous ces ouvrages de vulgarisation, j'ai le sentiment d'avoir quelque peu cotoyé ces personnes éminemment intéressantes qu'ont été Cantor, Hilbert, Gauss, Galois et même si je n'aboutis pas, les avoir "rencontrées" aura été un enrichissement humain[16].
Pour terminer, je citerai une anecdote : un jour, un enfant me proposa de me "montrer l'infini"... Il sortit un miroir de poche et le plaça face à un miroir accroché au mur. La suite de miroirs de plus en plus petits semblait ne jamais s'arrêter et l'enfant était émerveillé. Je continue de partager son sentiment après deux ans de promenade autour de la conjecture de Goldbach.

## Bibliographie

(1) C.P. Bruter, *La construction des nombres*, Ed. Ellipses, 2000.
(2) T. Brugère et A. Mollard, *Mathématiques à l'usage des informaticiens*, Ed. Ellipses, 2003.
(3) P.J. Davis, R.Hersh, *l'Univers mathématique*, Ed. Gauthier-Villars, 1985
(4) *L'infini (le fini, le discret et le continu)*, Hors série n° 13, Ed. Bibliothèque Tangente, 2006.
(5) N. Charraud, *Infini et Inconscient, essai sur Georg Cantor*, Ed. Anthropos, 1994.
(6) D. Guedj, *Villa des hommes*, Ed. Robert Laffont, 2007
(7) D. Nordon, M.Mendès-France (illustrations), *Les mathématiques pures n'existent pas !*, Ed. Actes Sud, 1985.
(8) D. Nordon, *Les obstinations d'un mathématicien*, Ed. Belin Pour La Science, 2003.
(9) A. Doxiadis, *Oncle Pétros et la conjecture de Goldbach*, Ed. Points, 2002.
(10) L. Euler, *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs*, Commentatio 175 indicis Enestroemiani, Bibliothèque impartiale 3, 1751, p.10-31.
(11) P. Damphousse, *Découvrir l'arithmétique*, Ed. Ellipses, 2000.
(12) A. Astruc, *Evariste Galois*, Ed. Grandes biographies, 1999.
(13) M. Du Sautoy, *La symphonie des nombres premiers*, Ed. Eloïse d'Ormesson, 2005.
(14) J.P. Belna, *Cantor*, Ed. Les belles lettres, 2000.
(15) J.P. Delahaye, *Merveilleux nombres premiers*, Ed. Belin Pour La Science,

[15] Je suis née en 1965 et tout mon apprentissage des mathématiques en école élémentaire s'est fait par les ensembles d'une part et par la représentation des nombres dans des systèmes de numération multi-bases d'autre part, ce que l'on a appelé les "mathématiques modernes".

[16] En annexe 3, sont présentées très succinctement d'autres références trouvées çà et là qui pourraient être mises à profit pour comprendre la conjecture de Goldbach.

2000.
(16) P. Hoffman, *Erdös, l'homme qui n'aimait que les nombres*, Ed. Belin, 2000.
(17) J. Hadamard, *Essai sur la psychologie de l'invention dans le domaine mathématique*, suivi de H. Poincaré, *L'invention mathématique*, Ed. Jacques Gabay, 2000.
(18) J.J.Gray, *Le défi de Hilbert*, Ed. Dunod, 2003.
(19) Collectif, Ebbinghaus et autres auteurs, *Les Nombres*, Ed. Vuibert, 1999.
(20) S. Hawking, *Et Dieu créa les nombres*, Ed. Dunod, 2006.
(21) C. Laisant, *Sur un procédé expérimental de vérification de la conjecture de Goldbach*, Bulletin de la SMF n°25 de 1897.
(22) S. Baruk, *L'âge du capitaine*, Ed. Seuil, 1998.
(23) G. Tenenbaum, M. Mendès-France, *Les nombres premiers*, Collection Que sais-je ?, PUF, 2000
(24) C.F. Gauss, *Recherches arithmétiques*, Ed. Jacques Gabay, 1801.

Enfin, toutes les notes de recherches et une bibliographie détaillée se trouve sur un site personnel à l'adresse http://denise.vella.chemla.free.fr.

## Annexe 1 : la conjecture de Goldbach présentée dans le livre de Davis et Hersh

$20882 = 3 + 20879$ $20942 = 3 + 20939$
$20884 = 5 + 20879$ $20944 = 5 + 20939$
$20886 = 7 + 20879$ $20946 = 7 + 20939$
$20888 = 31 + 20857$ $20948 = 19 + 20929$
$20890 = 3 + 20887$ $20950 = 3 + 20947$
$20892 = 5 + 20887$ $20952 = 5 + 20947$
$20894 = 7 + 20887$ $20954 = 7 + 20947$
$20896 = 17 + 20879$ $20956 = 17 + 20939$
$20898 = 11 + 20887$ $20958 = 11 + 20947$
$20900 = 3 + 20897$ $20960 = 13 + 20947$
$20902 = 3 + 20899$ $20962 = 3 + 20959$
$20904 = 5 + 20899$ $20964 = 5 + 20959$
$20906 = 3 + 20903$ $20966 = 3 + 20963$
$20908 = 5 + 20903$ $20968 = 5 + 20963$
$20910 = 7 + 20903$ $20970 = 7 + 20963$
$20912 = 13 + 20899$ $20972 = 13 + 20959$
$20914 = 11 + 20903$ $20974 = 11 + 20963$
$20916 = 13 + 20903$ $20976 = 13 + 20963$
$20918 = 19 + 20899$ $20978 = 19 + 20959$
$20920 = 17 + 20903$ $20980 = 17 + 20963$
$20922 = 19 + 20903$ $20982 = 19 + 20963$
$20924 = 3 + 20921$ $20984 = 3 + 20981$
$20926 = 5 + 20921$ $20986 = 3 + 20983$
$20928 = 7 + 20921$ $20988 = 5 + 20983$
$20930 = 31 + 20899$ $20990 = 7 + 20983$
$20932 = 3 + 20929$ $20992 = 11 + 20981$
$20934 = 5 + 20929$ $20994 = 11 + 20983$
$20936 = 7 + 20929$ $20996 = 13 + 20983$
$20938 = 17 + 20921$ $20998 = 17 + 20981$
$20940 = 11 + 20929$ $21000 = 17 + 20983$

## Annexe 2 : le théorème chinois pour l'informaticien Prather selon Davis et Hersh

Avant d'analyser la présentation du théorème chinois des restes par Prather l'informaticien, Davis et Hersh jugent la présentation de ce théorème par Shockley (dans son Introduction à la théorie des nombres de 1967). Ils expliquent : "la présentation de Shockley peut être appelée une version à la mode de ce qui figure dans les Disquisitiones Arithmeticae de Gauss (1801). La notation Gaussienne pour les congruences est pleinement établie et se prête à un degré d'élégance inconnu jusqu'alors [...] Cette formulation peut être considérée comme un sommet dans le cadre de la théorie des nombres algébrisée de manière classique.

La différence de ton entre les formulations de Prather et Shockley est intense. Nous avons chez Prather une réécriture complète du théorème sous l'influence de la conception structuraliste des mathématiques. L'ensemble fini des entiers naturels $0, 1, 2, ..., n-1$ considéré muni de l'addition modulo $n$ (c'est à dire

négligeant les multiples de $n$) constitue ce qu'on appelle un groupe cyclique additif, noté $Z_n$. Le produit de deux tels groupes, $Z_4 \times Z_3$ par exemple, consiste en couples $(a, b)$ d'entiers où le premier est un élément de $Z_4$ et le second un élément de $Z_3$. Ainsi, les éléments de $Z_4 \times Z_3$ sont les douze couples :

| | | | |
|---|---|---|---|
| $(0,0)$ | $(1,0)$ | $(2,0)$ | $(3,0)$ |
| $(0,1)$ | $(1,1)$ | $(2,1)$ | $(3,1)$ |
| $(0,2)$ | $(1,2)$ | $(2,2)$ | $(3,2)$ |

L'addition des éléments de $Z_4 \times Z_3$ est définie comme l'addition des entiers correspondants, la première étant effectuée modulo 4 et la seconde modulo 3. Ainsi, par exemple :

$$(2,2) + (3,2) \ = \ ((2+3) \ mod \ 4, \ (2+2) \ mod \ 3) \ = \ (1,1)$$

Chaque couple $(a, b)$ peut être identifié avec l'unique nombre parmi $0, 1, ..., 11$ dont la division par 4 fournit $a$ et dont la division par 3 fournit $b$. Avec cette identification, la table ci-dessus devient :

| | | | |
|---|---|---|---|
| 0 | 9 | 6 | 3 |
| 4 | 1 | 10 | 7 |
| 8 | 5 | 2 | 11 |

Ainsi, $(1, 1) = (2, 2) + (3, 2)$ se traduit par $1 = (2 + 11) \ mod \ 12$, ce qui est un exemple particulier de l'isomorphisme des deux tables suivant leurs définitions individuelles de $+$. La présente formulation du théorème chinois affirme que ce schéma est vrai dans le cas général de l'entier $n$, pourvu que nous décomposions $n$ en ses facteurs premiers. Notons que cette formulation du théorème chinois nous donne à la fois plus et moins que la formulation précédente (par Shockley). Elle met l'accent sur la structure au détriment de l'algorithme. Elle fournit une analyse complète de l'addition modulaire dans $Z_n$, en termes d'additions plus simples dans $(Z_{q_i})$. Elle court-circuite la question de savoir comment établir l'identification de $Z_n$ et de $Z_{q_1} \times ... \times Z_{q_r}$ (quoique cette identification intervienne au coeur de la démonstration) et elle ignore totalement la question, historiquement motivante, de savoir comment, les restes étant donnés, nous pouvons promptement calculer le nombre qui engendre ces restes. En un sens, il est très étrange de voir dans le commentaire de Prather à la fin de son exposé que le théorème chinois s'est montré utile dans la conception d'unités arithmétiques rapides pour les ordinateurs. On penserait que ceci appelle la connaissance d'un algorithme concret. Mais il est vrai que l'informatique dans sa formulation théorique est dominée par un esprit d'abstraction qui n'a rien à envier aux autres branches des mathématiques dans son fanatisme."

# Annexe 3 : d'autres manières d'aborder la conjecture de Goldbach d'une grande complexité

Un extrait du livre collectif "les Nombres" aux éditions Vuibert [19], page 404, provenant de la section concernant les preuves d'indépendance logique :
"On peut mentionner la conjecture de Goldbach. Plus généralement, on peut penser à tout énoncé portant sur les nombres naturels et comprenant un ensemble fini de quantificateurs universels suivi d'un noyau sans quantificateur, ce qui

est par exemple le cas de toute équation diophantienne ou de sa négation. Tant qu'un tel problème n'est pas résolu, on peut se demander s'il est indépendant de ZFC[17]. Pour ce type de problème, un résultat d'indépendance a une signification très différente de ceux concernant l'hypothèse du continu ou l'hypothèse de Suslin : une preuve de son indépendance implique automatiquement sa vérité. Si par exemple, l'hypothèse de Riemann était fausse, il devrait y avoir un contre-exemple dont la validité pourrait être vérifiée, sur la base de ZFC. Ainsi, l'indépendance ne pourrait survenir que si la conjecture était vraie. Pour démontrer que Goldbach est vraie, il faudrait démontrer qu'elle n'est pas réfutable selon ZFC."

Un extrait du livre "le défi de Hilbert" de J.J.Gray [18]: Un autre problème, également mentionné par Hilbert, qui peut se ramener à une équation diophantienne, est la conjecture de Goldbach. Elle en devient l'affirmation qu'une certaine équation diophantienne n'a pas de solution. Si le dixième problème de Hilbert avait admis une réponse positive, la conjecture de Goldbach aurait été réfutée - une connexion que Hilbert n'avait certainement pas soupçonnée. Davis, Mattiassevitch et Robinson montrèrent que même l'hypothèse de Riemann peut être reformulée comme une question Diophantienne (ce qui ne la rend pas plus facile pour autant). Julia Robinson disait ceci à propos du dixième problème de Hilbert : "Je souhaitais toujours à chacun de mes anniversaires et d'année en année que le dixième problème de Hilbert soit résolu. Pas par moi, mais simplement qu'il soit résolu. J'avais le sentiment que je ne pourrais accepter de mourir sans connaître la réponse". On raconte d'autre part qu'Hadamard et la Vallée-Poussin qui ont prouvé indépendamment le TNP sont morts très âgés. Allez, je l'avoue, toutes ces recherches n'ont qu'un but : augmenter, autant que faire se peut, ma longévité !

Enfin, un extrait des oeuvres mathématiques d'Evariste Galois trouvées sur Gallica p.405 : "le principal avantage de la nouvelle théorie [18] 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 $p^\nu$, 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 $p^\nu$ sera

[17] mis pour axiomatique de Zermelo-Fraenkel avec l'axiome du choix.

[18] consistant à associer à une équation ce que l'on appelle son groupe de Galois.

primitive et soluble par radicaux"[19].

Pour finir, je voudrais reproduire dans cette annexe un extrait d'une superbe biographie de Galois par Alexandre Astruc, publiée aux éditions Flammarion en 1994 car je crois que l'on gagnerait à faire circuler de telles phrases.

Astruc écrit que "communiquer ses découvertes, être reconnu par ses pairs, telles sont les idées fixes de tout savant, et Galois ne fait pas exception à cette règle". Un peu plus loin, il cite intégralement la préface de Galois à ses "deux mémoires d'analyse pure". La fin de cette préface préfigure le partage actuel de la connaissance via internet notamment et cette notion de partage m'est chère.

"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 su 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[20] 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 les moindres observations pour peu qu'elles soient nouvelles, et on ajoutera : "Je ne sais pas le reste.""

[19] J'aimerais vraiment qu'un professeur m'explique dans quelle mesure ces quelques lignes ne suffisent pas, à elles seules, à prouver la conjecture de Goldbach, dans la mesure où il y est question de solutions entières et de congruences et que la conjecture est formulable en ces termes.

[20] Ici, Galois veut parler des mathématiciens qui ont dénigré son travail à l'époque.

# Une méthode pour déterminer les décomposants de Goldbach

Denise Vella

1er Novembre 2007

**Résumé**

Cette note présente une méthode de détermination de décomposants de Goldbach d'un nombre pair (i.e. nombres premiers dont ce nombre pair est la somme). Elle utilise une représentation des entiers par leurs restes selon des modules premiers. Les décomposants de Goldbach sont les nombres premiers solutions de systèmes de congruence particuliers dont le théorème des restes chinois assure l'existence.

## 1 Introduction

La conjecture de Goldbach (1742) énonce que tout nombre pair $2x$ supérieur ou égal à 4 est la somme de deux nombres premiers $p$ et $q$. Le nombre $p$ et le nombre $q$ sont appelés des décomposants de Goldbach de $2x$. Cette note présente un système de représentation des entiers naturels par leurs restes modulaires selon des modules premiers. Les décomposants de Goldbach d'un entier pair $2x$ sont les entiers inférieurs ou égaux à $x$ solutions de systèmes de congruence généralisés découlant de cette représentation.

## 2 Théorème des restes chinois et système de numération par n-uplets de restes

L'énoncé du théorème des restes chinois[1] (qui date du troisième siècle et a été développé par le mathématicien chinois Sun Tzu) est le suivant :

*Soient k nombres entiers naturels* $m_1,\ m_2,\ ...,\ m_k$
*premiers entre eux deux à deux*
*et k entiers* $r_1,\ r_2,\ ...,\ r_k$,
*le système de congruence*
$$\begin{cases} x \equiv r_1\ (mod\ m_1) \\ x \equiv r_2\ (mod\ m_2) \\ ... \\ x \equiv r_k\ (mod\ m_k) \end{cases}$$
*admet une unique solution modulo* $M = m_1 m_2 ... m_k$

Du théorème des restes chinois, il résulte que chaque entier est solution

[1] On trouve le théorème des restes chinois dans le paragraphe 36 des Recherches Arithmétiques de Gauss, reformulé dans le langage des congruences que Gauss a inventé.

d'une infinité de systèmes de congruences. Par exemple, l'entier 26 est solution du système :

$$\begin{cases} x \equiv 0 \ (mod\ 2) \\ x \equiv 2 \ (mod\ 3) \end{cases}$$

mais également du système :

$$\begin{cases} x \equiv 0 \ (mod\ 2) \\ x \equiv 2 \ (mod\ 3) \\ x \equiv 1 \ (mod\ 5) \end{cases}$$

ou encore du système :

$$\begin{cases} x \equiv 0 \ (mod\ 2) \\ x \equiv 2 \ (mod\ 3) \\ x \equiv 1 \ (mod\ 5) \\ x \equiv 5 \ (mod\ 7) \\ x \equiv 4 \ (mod\ 11) \\ x \equiv 0 \ (mod\ 13) \\ x \equiv 9 \ (mod\ 17) \\ x \equiv 7 \ (mod\ 19) \\ x \equiv 3 \ (mod\ 23) \\ x \equiv 26 \ (mod\ 29) \\ x \equiv 26 \ (mod\ 31) \\ x \equiv 26 \ (mod\ 37) \end{cases}$$

On appellera ici *n-uplet* une suite de $n$ entiers $k_i$. Associé à un entier $x$, $k_i(x)$ sera la *i-ème coordonnée* de $x$ dans ce n-uplet. Un *n-uplet de référence* $(2, p_2, ..., p_i, ..., p_n)$ est une suite croissante de $n$ nombres premiers commençant par deux et telle que l'intervalle entre un nombre premier de cette suite et son successeur ne contienne aucun nombre premier. Tout entier $x$ peut être représenté à partir d'un tel n-uplet de référence : la composante $k_i$ du n-uplet $R(x)$ de représentation de $x$ étant le reste de la division euclidienne de $x$ par $p_i$, $x$ possède $\Pi(x)$ représentations distinctes, où $\Pi(x)$ désigne la quantité de nombres premiers inférieurs à $x$.
Un tel système de numération permet ainsi de représenter un grand nombre entier par des nombres entiers plus petits : il est notamment utilisé en cryptographie.
La remarque de Claude-Paul Bruter ([3]) selon laquelle "il revient à chaque utilisateur de créer son propre ensemble de nombres selon la réalité qu'il souhaite modéliser" trouve ici son illustration.
Nous étudierons dans la suite, à titre d'exemple, le cas particulier de la décomposition de Goldbach du nombre 2308. Puisque 2308 est compris entre $2 \times 3 \times 5 \times 7 = 210$ et $2 \times 3 \times 5 \times 7 \times 11 = 2310$, le théorème chinois rappelé précédemment nous conduit à choisir $(2, 3, 5, 7)$ comme n-uplet de référence. Nous donnons ici la liste des nombres inférieurs à 210 et leur représentation dans ce n-uplet.

| | | |
|---|---|---|
| $1 : (1, 1, 1, 1)$ | $71 : (1, 2, 1, 1)$ | $141 : (1, 0, 1, 1)$ |
| $3 : (1, 0, 3, 3)$ | $73 : (1, 1, 3, 3)$ | $143 : (1, 2, 3, 3)$ |
| $5 : (1, 2, 0, 5)$ | $75 : (1, 0, 0, 5)$ | $145 : (1, 1, 0, 5)$ |
| $7 : (1, 1, 2, 0)$ | $77 : (1, 2, 2, 0)$ | $147 : (1, 0, 2, 0)$ |
| $9 : (1, 0, 4, 2)$ | $79 : (1, 1, 4, 2)$ | $149 : (1, 2, 4, 2)$ |
| $11 : (1, 2, 1, 4)$ | $81 : (1, 0, 1, 4)$ | $151 : (1, 1, 1, 4)$ |
| $13 : (1, 1, 3, 6)$ | $83 : (1, 2, 3, 6)$ | $153 : (1, 0, 3, 6)$ |
| $15 : (1, 0, 0, 1)$ | $85 : (1, 1, 0, 1)$ | $155 : (1, 2, 0, 1)$ |
| $17 : (1, 2, 2, 3)$ | $87 : (1, 0, 2, 3)$ | $157 : (1, 1, 2, 3)$ |
| $19 : (1, 1, 4, 5)$ | $89 : (1, 2, 4, 5)$ | $159 : (1, 0, 4, 5)$ |
| $21 : (1, 0, 1, 0)$ | $91 : (1, 1, 1, 0)$ | $161 : (1, 2, 1, 0)$ |
| $23 : (1, 2, 3, 2)$ | $93 : (1, 0, 3, 2)$ | $163 : (1, 1, 3, 2)$ |
| $25 : (1, 1, 0, 4)$ | $95 : (1, 2, 0, 4)$ | $165 : (1, 0, 0, 4)$ |
| $27 : (1, 0, 2, 6)$ | $97 : (1, 1, 2, 6)$ | $167 : (1, 2, 2, 6)$ |
| $29 : (1, 2, 4, 1)$ | $99 : (1, 0, 4, 1)$ | $169 : (1, 1, 4, 1)$ |
| $31 : (1, 1, 1, 3)$ | $101 : (1, 2, 1, 3)$ | $171 : (1, 0, 1, 3)$ |
| $33 : (1, 0, 3, 5)$ | $103 : (1, 1, 3, 5)$ | $173 : (1, 2, 3, 5)$ |
| $35 : (1, 2, 0, 0)$ | $105 : (1, 0, 0, 0)$ | $175 : (1, 1, 0, 0)$ |
| $37 : (1, 1, 2, 2)$ | $107 : (1, 2, 2, 2)$ | $177 : (1, 0, 2, 2)$ |
| $39 : (1, 0, 4, 4)$ | $109 : (1, 1, 4, 4)$ | $179 : (1, 2, 4, 4)$ |
| $41 : (1, 2, 1, 6)$ | $111 : (1, 0, 1, 6)$ | $181 : (1, 1, 1, 6)$ |
| $43 : (1, 1, 3, 1)$ | $113 : (1, 2, 3, 1)$ | $183 : (1, 0, 3, 1)$ |
| $45 : (1, 0, 0, 3)$ | $115 : (1, 1, 0, 3)$ | $185 : (1, 2, 0, 3)$ |
| $47 : (1, 2, 2, 5)$ | $117 : (1, 0, 2, 5)$ | $187 : (1, 1, 2, 5)$ |
| $49 : (1, 1, 4, 0)$ | $119 : (1, 2, 4, 0)$ | $189 : (1, 0, 4, 0)$ |
| $51 : (1, 0, 1, 2)$ | $121 : (1, 1, 1, 2)$ | $191 : (1, 2, 1, 2)$ |
| $53 : (1, 2, 3, 4)$ | $123 : (1, 0, 3, 4)$ | $193 : (1, 1, 3, 4)$ |
| $55 : (1, 1, 0, 6)$ | $125 : (1, 2, 0, 6)$ | $195 : (1, 0, 0, 6)$ |
| $57 : (1, 0, 2, 1)$ | $127 : (1, 1, 2, 1)$ | $197 : (1, 2, 2, 1)$ |
| $59 : (1, 2, 4, 3)$ | $129 : (1, 0, 4, 3)$ | $199 : (1, 1, 4, 3)$ |
| $61 : (1, 1, 1, 5)$ | $131 : (1, 2, 1, 5)$ | $201 : (1, 0, 1, 5)$ |
| $63 : (1, 0, 3, 0)$ | $133 : (1, 1, 3, 0)$ | $203 : (1, 2, 3, 0)$ |
| $65 : (1, 2, 0, 2)$ | $135 : (1, 0, 0, 2)$ | $205 : (1, 1, 0, 2)$ |
| $67 : (1, 1, 2, 4)$ | $137 : (1, 2, 2, 4)$ | $207 : (1, 0, 2, 4)$ |
| $69 : (1, 0, 4, 6)$ | $139 : (1, 1, 4, 6)$ | $209 : (1, 2, 4, 6)$ |

$210 : (0, 0, 0, 0)$
$211 : (1, 1, 1, 1)$
...

# 3 Les décomposants de Goldbach sont non congrus à $2x$ selon tout module

On peut formuler ainsi la conjecture de Goldbach : "tout nombre inférieur à $x$ et dont les restes de divisions euclidiennes par les nombres premiers inférieurs à $x$ sont différents un à un des restes de $2x$ par ces mêmes divisions a son complémentaire à $2x$ qui est premier". En d'autres termes :

$\forall\ 2x$
$\forall\ p_1$ *premier impair inférieur ou égal à* $x$
$\forall\ q$ *premier impair inférieur ou égal à* $x$,
$2x \not\equiv p_1\ (mod\ q) \iff p_2 = 2x - p_1$ *premier impair supérieur ou égal à* $x$
($p_1$ *et* $p_2$ *sont des décomposants de Goldbach de* $2x$).

En effet,

$$\begin{array}{ll} & 2x \not\equiv p_1 \ (mod\ q) \\ \iff & 2x - p_1 \not\equiv 0 \ (mod\ q) \\ \iff & 2x - p_1 \ est\ un\ nombre\ premier \\ & \quad car\ il\ n'est\ divisible\ par\ aucun\ autre\ nombre\ premier\ q \end{array}$$

Les décomposants de Goldbach d'un nombre pair $2x$, devant être premiers, sont a fortiori premiers à $2x$ (i.e. de plus grand diviseur commun à $2x$ égal à 1).
On notera qu'un nombre premier inférieur à $x$ étant donné, son complémentaire à $2x$ n'est pas obligatoirement un nombre premier. D'autre part, un nombre inférieur à $x$ et non congru à $2x$ selon tout module n'est pas nécessairement premier.
L'énoncé présenté ci-dessus est vrai. Cependant, il pourrait être vrai par vacuité, c'est à dire vrai alors qu'il n'existerait aucun $p_1$ le vérifiant. Démontrer la conjecture de Goldbach consisterait à démontrer que cet énoncé ne peut jamais être vrai par vacuité[2].

# 4 Remarques préliminaires au traitement de cas

Définissons d'abord la relation binaire *Congru_à* [3] entre deux n-uplets dans un même n-uplet de référence de la façon suivante :

$$(x_1, x_2, ..., x_n)\ Congru\_à\ (y_1, y_2, ...y_n)\ dans\ (p_1, p_2, ..., p_n)$$
$$\iff$$
$$\begin{cases} x_1 \equiv y_1 \ (mod\ p_1) \vee \\ x_2 \equiv y_2 \ (mod\ p_2) \vee \\ ... \vee \\ x_n \equiv y_n \ (mod\ p_n) \end{cases}$$

Cette relation est réflexive, symétrique mais elle n'est pas transitive. La relation "inverse" de cette relation, que l'on pourrait appeler *Non_congru_à*[4], est quant à elle non réflexive, symétrique et non transitive.

Définissons également une relation unaire *Contient_un_zéro* qui à un n-uplet $(x_1, x_2, ..., x_n)$ dans un n-uplet de référence $(p_1, p_2, ..., p_n)$ associe le booléen vrai si et seulement si l'une des coordonnées du n-uplet est nulle.

$$Contient\_un\_zéro((x_1, x_2, ..., x_n))\ est\ vrai$$
$$\iff$$
$$x_1 \equiv 0 \ (mod\ p_1) \vee x_2 \equiv 0 \ (mod\ p_2) \vee ... \vee x_n \equiv 0 \ (mod\ p_n)$$

Nous allons nous intéresser ici à des triplets de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, que nous noterons sans parenthèses ni virgules pour en alléger l'écriture. Trouvons d'abord pour chaque triplet quels sont les triplets qui lui sont

[2] Le corollaire de ce qui vient d'être présenté est que les facteurs premiers de $2x - p$ sont les nombres premiers du n-uplet de référence dans lequel est représenté $p$ selon lesquels $p$ et $2x$ sont congrus.
[3] i.e. sous-entendu *Congru à* selon un module
[4] i.e. sous-entendu *Non_congru_à* selon tout module

non congrus selon toutes les coordonnées.
Sont non congrus à 000 les triplets 111, 112, 121, 113, 122, 114, 123, 124.
Sont non congrus à 001 les triplets 120, 112, 113, 122, 114, 123, 110, 124.
Sont non congrus à 002 les triplets 111, 120, 121, 113, 114, 123, 110, 124.
Sont non congrus à 003 les triplets 111, 120, 112, 121, 122, 114, 110, 124.
Sont non congrus à 004 les triplets 111, 120, 112, 121, 113, 122, 123, 110.
Sont non congrus à 010 les triplets 103, 104, 121, 122, 101, 123, 102, 124.
Sont non congrus à 011 les triplets 103, 120, 104, 100, 122, 123, 102, 124.
Sont non congrus à 012 les triplets 103, 120, 104, 121, 100, 101, 123, 124.
Sont non congrus à 013 les triplets 120, 104, 121, 100, 122, 101, 102, 124.
Sont non congrus à 014 les triplets 103, 121, 100, 122, 101, 102, 123, 120.
Sont non congrus à 020 les triplets 111, 103, 112, 104, 113, 114, 101, 102.
Sont non congrus à 021 les triplets 103, 112, 104, 113, 100, 114, 110, 102.
Sont non congrus à 022 les triplets 111, 103, 104, 113, 100, 114, 101, 110.
Sont non congrus à 023 les triplets 111, 112, 104, 100, 114, 101, 110, 102.
Sont non congrus à 024 les triplets 111, 103, 112, 113, 100, 101, 110, 102.
On voit qu'à chaque triplet correspondent 8 triplets qui lui sont non congrus selon toutes les coordonnées. En effet, la fonction $\varphi(x)$, appelée fonction indicatrice d'Euler, qui compte les nombres inférieurs à $x$ et premiers à $x$, prend la valeur 8 pour $30 = 2 \times 3 \times 5$ ($\varphi(30) = 8$).
Cherchons d'autre part quels sont les triplets qui n'ont aucune coordonnée nulle. Ce sont les triplets 111, 112, 113, 114, 121, 122, 123 et 124. Eux aussi sont au nombre de 8.

Effectuons encore quelques comptages : considérons l'ensemble des nombres premiers à 98. Ils sont au nombre de 42 ($\varphi(98) = 42$). Ils vont par deux car si $p$ appartient à cet ensemble, $2x - p$ appartient aussi à cet ensemble.
98 a pour représentation $(0, 2, 3)$ selon $(2, 3, 5)$. Fournissons dans un tableau en première colonne la valeur entière de chacun des nombres en question (c'est à dire les nombres inférieurs à 98 et premiers à 98) ; en deuxième colonne, fournissons leur représentation dans $(2, 3, 5)$. En troisième colonne, on note le fait que la représentation en question vérifie une propriété que l'on appellera $c1$ qui consiste à être congru à la représentation de 98 selon une coordonnée, et en quatrième colonne, on note le fait qu'elle vérifie une propriété que l'on appellera $c2$, c'est à dire qu'elle ne contient aucune coordonnée nulle. On dira qu'un nombre a la propriété $c$ dans un n-uplet de référence $R$ si sa représentation vérifie les deux propriétés $c1$ et $c2$.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | $(1,1,1)$ | $\times$ | $\circ$ | 97 | $(1,1,2)$ | $\times$ | $\circ$ |
| 3 | $(1,0,3)$ | | | 95 | $(1,2,0)$ | | |
| 5 | $(1,2,0)$ | | | 93 | $(1,0,3)$ | | |
| 9 | $(1,0,4)$ | $\times$ | | 89 | $(1,2,4)$ | | $\circ$ |
| 11 | $(1,2,1)$ | | $\circ$ | 87 | $(1,0,2)$ | $\times$ | |
| 13 | $(1,1,3)$ | | $\circ$ | 85 | $(1,1,0)$ | $\times$ | |
| 15 | $(1,0,0)$ | $\times$ | | 83 | $(1,2,3)$ | | $\circ$ |
| 17 | $(1,2,2)$ | | $\circ$ | 81 | $(1,0,1)$ | $\times$ | |
| 19 | $(1,1,4)$ | $\times$ | $\circ$ | 79 | $(1,1,4)$ | $\times$ | $\circ$ |
| 23 | $(1,2,3)$ | | $\circ$ | 75 | $(1,0,0)$ | $\times$ | |
| 25 | $(1,1,0)$ | $\times$ | | 73 | $(1,1,3)$ | | $\circ$ |
| 27 | $(1,0,2)$ | $\times$ | | 71 | $(1,2,1)$ | | $\circ$ |
| 29 | $(1,2,4)$ | | $\circ$ | 69 | $(1,0,4)$ | $\times$ | |
| 31 | $(1,1,1)$ | $\times$ | $\circ$ | 67 | $(1,1,2)$ | $\times$ | $\circ$ |
| 33 | $(1,0,3)$ | | | 65 | $(1,2,0)$ | | |
| 37 | $(1,1,2)$ | $\times$ | $\circ$ | 61 | $(1,1,1)$ | $\times$ | $\circ$ |
| 39 | $(1,0,4)$ | $\times$ | | 59 | $(1,2,4)$ | | $\circ$ |
| 41 | $(1,2,1)$ | | $\circ$ | 57 | $(1,0,2)$ | $\times$ | |
| 43 | $(1,1,3)$ | | $\circ$ | 55 | $(1,1,0)$ | $\times$ | |
| 45 | $(1,0,0)$ | $\times$ | | 53 | $(1,2,3)$ | | $\circ$ |
| 47 | $(1,2,2)$ | | $\circ$ | 51 | $(1,0,1)$ | $\times$ | |

On constate que les troisième et quatrième colonnes sont symétriques l'une de l'autre autour du nombre 49 (moitié de 98) en ce sens que si $p$ est non congru à $2x$ selon toute coordonnée, alors la représentation de $2x-p$ ne contient aucun zéro. Les nombres $p$ vérifiant la propriété $c(p)$ sont les décomposants de Goldbach de 98. Trouver ce qui garantit l'existence d'un nombre dont la troisième et la quatrième colonne sont marquées consiste à prouver la conjecture de Goldbach.

# 5 Traitement de cas

Au paragraphe précédent, on a traité le cas du nombre pair 98 en considérant les nombres premiers à 98. Traitons maintenant ce cas en ne considérant que l'espace des représentations par les n-uplets. 98 a pour racine carrée 9.89... Il est compris entre $2\times3\times5$ et $2\times3\times5\times7$. On rappelle que sa représentation est le triplet $(0,2,3)$ selon le triplet de référence $(2,3,5)$. Considérons les nombres $p$ qui vérifient la propriété $c(p)$.
Puisque 98 a pour coordonnée 2 ($mod$ 3), on ne va conserver que les nombres ayant pour coordonnée 1 ($mod$ 3). Puisque 98 a pour coordonnée 3 ($mod$ 5), on ne va conserver que les nombres ayant pour coordonnée 1, 2 *ou* 4 ($mod$ 5). On a omis de dire que trivialement les solutions doivent être impaires (première coordonnée ($mod$ 2) égale à 1).
Ces nombres sont solutions du système de congruence généralisé par disjonction suivant :

$$\begin{cases} p \equiv 1\ (mod\ 2) \\ p \equiv 1\ (mod\ 3) \\ p \equiv 1 \vee 2 \vee 4\ (mod\ 5) \end{cases}$$

Ils ont pour représentation selon le triplet de référence $(2,3,5)$ les triplets $(1,1,1)$, $(1,1,2)$ et $(1,1,4)$.
Le premier système de la disjonction correspondant au triplet $(1,1,1)$ a pour solutions les nombres : 31, 61, ... en vertu du théorème des restes chinois.

Le deuxième système de la disjonction correspondant au triplet $(1, 1, 2)$ a pour solutions les nombres : 7, 37, 67... en vertu du théorème des restes chinois.
Le troisième système de la disjonction correspondant au triplet $(1, 1, 4)$ a pour solutions les nombres : 19, 49, 79, ... en vertu du théorème des restes chinois.
Il s'agit maintenant d"'étendre" les solutions trouvées en vérifiant qu'elles restent solutions lorsqu'on ajoute la condition de non congruence à 0 ($mod$ 7). 7 étant congru à 0 ($mod$ 7) et 98 l'étant également, 7 n'est donc pas un décomposant de Goldbach de 98. 19, 31 et 37 ne sont pas éliminés par l'extension au module 7 et sont donc décomposants de Goldbach de 98.

Supposons qu'au lieu de devoir examiner le triplet de représentation associé à 98, on ait eu à examiner un triplet quelconque. Il est possible de calculer le nombre de triplets qui vérifient la propriété $c$.
Dans le cas où le triplet serait 010, ne subsisteraient que 121, 122, 123 et 124. Pour le triplet 023, ne subsisteraient que 111, 112 et 113. On voit que le nombre de triplets appartenant à l'intersection des deux ensembles a un cardinal fonction du triplet en question. Si une coordonnée du triplet est nulle, il subsiste $p_i - 1$ possibilités pour cette coordonnée dans les triplets que l'on recherche ($p_i$ étant le nombre premier du triplet de référence selon lequel est calculée la coordonnée) tandis que si cette coordonnée est non nulle, il subsiste $p_i - 2$ possibilités ($p_i$ premier impair) pour cette coordonnée dans les triplets que l'on recherche[5].

Un problème persiste, dû au fait que les comptages présentés ci-dessus ne peuvent s'effectuer précisément que lorsque l'on se place sur un ensemble de nombres "complet", par exemple sur l'ensemble des nombres de 0 à 210 ($= 2 \times 3 \times 5$), ou bien ceux de 0 à 30030 ($= 2 \times 3 \times 5 \times 7 \times 11 \times 13$). Dans des ensembles de nombres "incomplets", on ne pourra effectuer ces comptages précisément.
Par analogie avec le terme factorielle, appelons *primorielle* $n$ le produit des $n$ nombres d'un n-uplet de référence. Le nombre pair $2x$ étant donné, la primorielle $n(x)$ est choisie de sorte que $n(x) < 2x < (n+1)(x)$. $2x$ admet une représentation $R(2x)$ dans le n-uplet de référence ainsi défini.

On va associer à $R(2x)$ l'ensemble des n-uplets vérifiant la propriété $c$. En effet, d'une part, le fait d'être non congru à $R(2x)$ selon toute coordonnée est une nécessité pour les décomposants de Goldbach de $2x$ (le complémentaire à $2x$ d'un nombre qui serait congru à $2x$ selon une coordonnée serait nécessairement composé). Le fait de n'avoir aucune coordonnée nulle garantit que l'on ne récupèrera pas des nombres composés ayant pour facteurs les nombres premiers du n-uplet de référence.
Un problème peut persister lorsque le plus grand nombre premier de $n(x)$ est inférieur au plus grand nombre premier inférieur à $\sqrt{2x}$. On verra sur des exemples qu'il faut s'assurer qu'il subsiste toujours un nombre premier qui va "conserver sa propriété $c$" en étendant ainsi l'ensemble des modules à considérer. C'est ce que fait la deuxième étape de l'algorithme, qui étend les représentations selon un n-uplet de référence contenant tous les nombres premiers inférieurs à la racine de $2x$.

[5]De ce fait, on peut vérifier que le nombre de décomposants de Goldbach des nombres pairs qui ont un nombre de facteurs premiers élevé (comme les multiples de 30, ou de 210 ou de 2310,...) subit des pics d'augmentation ponctuels.

Résumons l'algorithme :
Première étape : trouver les nombres compris entre 3 et $2x$ qui :
a) sont non congrus à $2x$ selon toute coordonnée dans le n-uplet de référence $(2, 3, ..., n(x))$ ;
b) ont une représentation ne contenant aucune coordonnée nulle.

Deuxième étape : extension éventuelle (au cas où $n(x) < \sqrt{2x}$)
Ne conserver de l'ensemble de nombres obtenus par la première étape que ceux qui "conservent leur propriété $c$" dans le n-uplet de référence $((n+1)(x), ..., plus\ grand\ nombre\ premier\ inférieur\ à \sqrt{2x})$.

Remarque : on aura noté que l'étape $I.a$ permet d'obtenir trois sortes de nombres :

- les nombres dont la représentation est un n-uplet vérifiant la propriété $c$, seuls nombres dont on va tester la représentation dans la deuxième étape ;
- les nombres dont la représentation contient un seul zéro et qui sont de deux sortes, soit de petits nombres premiers (qui peuvent d'ailleurs fournir des décompositions de Goldbach de $2x$), soit des puissances de ces petits nombres premiers qui sont donc des nombres composés et ne peuvent par conséquent fournir de décompositions de Goldbach de $2x$ ;
- les nombres composés dont la représentation contient au moins deux zéros (i.e. qui ont au moins deux facteurs premiers).

Soit $pair$ un nombre pair qui a pour représentation $(0, pair_2, pair_3, ...)$. Trouver les décomposants de Goldbach de $pair$ consiste à trouver les n-uplets $(1, x_2, x_3..., x_{n-1}, x_n)$ égaux à $(1, 1, 1, ..., 1, 1) + k(1, 1, 1, ..., 1, 1)$ et appartenant au produit cartésien $\mathbb{Z}/2\mathbb{Z} - \{0\} \times \mathbb{Z}/3\mathbb{Z} - \{0, pair_2\} \times \mathbb{Z}/5\mathbb{Z} - \{0, pair_3\} \times .....$ (c'est à dire le produit cartésien des corps premiers duquel on a enlevé les n-uplets vérifiant la propriété $c$.

Quelles sont les données numériques qui pourraient nous conforter dans l'idée qu'on n'a pas à craindre la non congruence aux nombres premiers plus grands quand on a la non congruence aux nombres premiers plus petits ?
On a vu qu'étant donné un nombre pair $2x$, il y a au minimum

$$\prod_{p_i\ premier\ impair} (p_i - 2)$$

n-uplets vérifiant la propriété $c$ (où $p_i$ est le plus grand nombre premier de la plus grande primorielle inférieure à $2x$).
Ce produit prendra les valeurs successives 1, $3 = 1 \times 3$, $15 = 1 \times 3 \times 5$, $135 = 1 \times 3 \times 5 \times 9$, etc... Ces nombres pourront être "éliminés" par des nombres premiers plus grands. Cependant, le nombre de nombres premiers plus grands qui pourraient éliminer des solutions croît bien plus lentement que le nombre de solutions potentielles [6].

Etudions un deuxième cas qui illustrera davantage le souci posé par ce que l'on pourrait appeler l' "extension" des solutions aux nombres

[6] la première quantité croît comme le produit des $p_i - 2$ ($p_i$ premier impair) alors que la seconde croît comme le nombre de nombres premiers compris entre les nombres premiers successifs et les racines des primorielles successives : elle vaudra 11 quand la première vaudra 15 puis vaudra 35 quand la première vaudra 135, puis vaudra 121 quand la première vaudra 1485, etc.

premiers plus grands. Le nombre pair à étudier est 2308 (de racine 48.04) : il est compris entre $2\times3\times5\times7$ et $2\times3\times5\times7\times11$ ; sa représentation selon le quadruplet de référence $(2,3,5,7)$ est $(0,1,3,5)$. Les quadruplets (que l'on écrit à nouveau sans parenthèse ni virgule) qui vérifient la propriété $c$ sont

1214, 1223, 1241, 1216, 1243, 1211, 1213, 1222, 1224, 1212, 1221, 1246, 1242, 1226, 1244.

Ils sont bien au nombre de 15, produit des $p_i - 2$ ($p_i$ premier impair).

Fournissons une table de congruence qui va nous permettre de voir s'ils conservent la propriété $c$, selon les modules de 11 à 47, 47 étant le plus grand nombre premier inférieur à la racine carrée de 2308.

| | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 | 47 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $71=(1,2,1,1)$ | 5 | 6 | 3 | 14 | 2 | 13 | 11 | 34 | 30 | 28 | 24 |
| $191=(1,2,1,2)$ | 4 | 9 | 4 | 1 | 7 | 17 | 5 | 6 | 27 | 19 | 3 |
| $101=(1,2,1,3)$ | 2 | 10 | 16 | 6 | 9 | 14 | 8 | 27 | 19 | 15 | 7 |
| $11=(1,2,1,4)$ | 0 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 |
| $41=(1,2,1,6)$ | 8 | 2 | 7 | 3 | 18 | 12 | 10 | 4 | 0 | 41 | 41 |
| $197=(1,2,2,1)$ | 10 | 2 | 10 | 7 | 13 | 23 | 11 | 12 | 33 | 25 | 9 |
| $107=(1,2,2,2)$ | 8 | 3 | 5 | 12 | 15 | 20 | 14 | 33 | 25 | 21 | 13 |
| $17=(1,2,2,3)$ | 6 | 4 | 0 | 17 | 17 | 17 | 17 | 17 | 17 | 17 | 17 |
| $137=(1,2,2,4)$ | 5 | 7 | 1 | 4 | 22 | 21 | 13 | 26 | 14 | 8 | 43 |
| $167=(1,2,2,6)$ | 2 | 11 | 14 | 15 | 6 | 22 | 12 | 19 | 3 | 38 | 26 |
| $29=(1,2,4,1)$ | 7 | 3 | 12 | 10 | 6 | 0 | 29 | 29 | 29 | 29 | 29 |
| $149=(1,2,4,2)$ | 6 | 6 | 13 | 16 | 11 | 4 | 25 | 1 | 26 | 20 | 8 |
| $59=(1,2,4,3)$ | 4 | 7 | 8 | 2 | 13 | 1 | 28 | 22 | 18 | 16 | 12 |
| $179=(1,2,4,4)$ | 3 | 10 | 9 | 8 | 18 | 5 | 24 | 31 | 15 | 7 | 38 |
| $209=(1,2,4,6)$ | 0 | 1 | 5 | 0 | 2 | 6 | 23 | 24 | 4 | 37 | 21 |
| $2308=(0,1,3,5)$ | 9 | 7 | 13 | 9 | 8 | 17 | 14 | 14 | 12 | 29 | 5 |

Tous les nombres premiers n'ayant pas été éliminés par cette table, certains, comme $11, 41, 71, 101, 167, 197, 179$ permettent d'obtenir des décompositions de Goldbach de 2308.

Le théorème des restes chinois garantit l'existence de solutions mais il ne garantit pas, d'une part que ces solutions sont inférieures à une borne fixée, en l'occurrence ici, il s'agit pour nous d'être assuré que les solutions des systèmes de congruence sont inférieures à $x$ quand on cherche les décomposants de Goldbach de $2x$. Le théorème ne garantit rien non plus quant à la primarité des solutions d'un système de congruence. On voit bien par contre ci-dessus que ces solutions des systèmes de congruences sont éléments de suites arithmétiques (i.e. $31+30k$, $7+30k'$, $19+30k''$ sont les suites arithmétiques correspondant au traitement du nombre pair 98 au paragraphe précédent). Le théorème de Dirichlet et le théorème de Linnik assurent de trouver des nombres premiers dans de telles suites arithmétiques inférieurs à certaine limite mais le problème de la borne supérieure est le bât qui blesse pour l'instant car la limite fournie par le théorème de Linnik est bien trop élevée pour garantir ce qui nous intéresse. On trouve dans [4] des éléments au sujet de deux théorèmes issus de la théorie analytique des nombres qui pourraient peut-être être utilisés ici : le théorème de Siegel-Walfisz et le théorème de Brun-Titchmarsh qui fournissent des renseignements sur la fonction de comptage des nombres

premiers $p$ inférieurs ou égaux à un nombre donné $x$ et congrus à un certain nombre modulo un certain autre (i.e. tels que $p \equiv a\ (mod\ q)$).

# 6 Descente infinie de Fermat

En matière de démonstrations "simples", on peut suivre la recommandation de Poincaré qui qualifiait la démonstration par récurrence de démonstration par excellence. Mais le mode de raisonnement par récurrence nécessite de prouver $P(n) \Rightarrow P(Succ(n))$[7]. Or les représentations choisies ici sont telles que $R(x+1)$ diffère par toutes ses coordonnées de $R(x)$. Puisqu'on a vu que les décomposants de Goldbach de $2x$ sont les nombres premiers $p$ inférieurs ou égaux à $x$ tels que $non[R(p)\ Congru\_à\ R(2x)]$, on imagine davantage relier entre elles les décompositions de Goldbach de nombres dont les représentations partagent des coordonnées plutôt que relier entre elles les décompositions de nombres dont les représentations ne partagent aucune coordonnée. Le raisonnement appelé "descente infinie de Fermat" permettrait-il d'atteindre la conjecture de Goldbach ?

Ce mode de raisonnement repose sur le fait qu'il n'existe pas de suite infinie strictement décroissante d'entiers positifs. L'ensemble $\mathbb{N}$ des entiers naturels et toutes ses parties propres non vides possèdent une propriété remarquable : ils admettent un plus petit élément.
Imaginons que nous voulions démontrer qu'une certaine propriété $P(n)$ est impossible ($n$ est un entier naturel). On raisonne par l'absurde en supposant $P(n)$ vraie pour un certain entier $n$ (la partie $E$ de $\mathbb{N}$ où $P(n)$ est vraie est donc non vide). Si nous sommes capables de montrer que P est alors vraie pour un entier strictement inférieur à $n$, nous aboutirons à une contradiction. En effet, si $a$ désigne le plus petit élément de $E$, on a simultanément $P(a)$ vraie et $P(b)$ vraie avec $b < a$. L'entier $b$ appartient donc à $E$ et est strictement plus petit que le plus petit élément de $E$. D'où la contradiction.

On a vu précédemment qu'un décomposant de Goldbach d'un nombre pair $2x$ est un nombre premier inférieur à $x$ qui ne partage avec $2x$ aucune classe de congruence[8]. S'il existait un nombre pair $2ng$ contredisant la conjecture de Goldbach, ce nombre pair "partagerait" chacune de ses classes d'équivalence selon des modules premiers inférieurs à sa racine avec des nombres premiers inférieurs à sa moitié (i.e. chaque élément du n-uplet représentant $2x$ serait commun avec l'élément correspondant du n-uplet de représentation d'un nombre premier inférieur à $x$). Mais alors, en prenant un nombre plus petit que $2ng$ et qui partage de nombreuses coordonnées avec $2ng$ (par exemple un nombre dont la représentation est un préfixe propre de la représentation de $2ng$), on construirait un nombre plus petit que $2ng$ et qui contredirait également la conjecture de Goldbach car lui aussi, par "inclusion" en quelque sorte, "partagerait" chacune de

[7] où Succ est défini par l'axiomatique de Peano.
[8] Cf en annexe 1 l'exemple du nombre pair 43532 très explicite à ce sujet.

ses classes d'équivalence selon des modules inférieurs à sa racine.

$$
\begin{array}{ll}
 & \exists\, 2x \;/\; 2x \textit{ ne vérifie pas la conjecture de Goldbach} \\
\iff & \forall\, p \textit{ premier impair inférieur ou égal à } \sqrt{2x} \\
 & \exists\, q \textit{ premier impair inférieur ou égal à } x, \\
 & \quad R(2x) \textit{ Congru\_à } R(p) \textit{ dans } n(x) \\
\Rightarrow & \exists\, 2y < 2x \;/\; R(2y) \textit{ préfixe propre de } R(2x) \textit{ et} \\
 & \forall\, p \textit{ premier impair inférieur ou égal à } \sqrt{2x} \\
 & \quad (\textit{et donc inférieur ou égal à } \sqrt{2y}) \\
 & \exists\, q \textit{ premier impair inférieur ou égal à } x, \\
 & \quad R(2y) \textit{ Congru\_à } R(p) \textit{ dans } n(x) \\
\Rightarrow & \exists\, 2y < 2x \;/\; 2y \textit{ ne vérifie pas la conjecture de Goldbach.}
\end{array}
$$

Or, cela est impossible. Donc, la conjecture de Goldbach doit être vraie.

# 7 Conclusion

La conjecture de Goldbach fait partie, avec l'hypothèse de Riemann et la conjecture des nombres premiers jumeaux, du huitième problème de la liste des 23 problèmes de Hilbert. La méthode présentée ici nous fait voir les décomposants de Goldbach d'un nombre pair sous un jour nouveau, comme solutions de systèmes de congruence particuliers. Le théorème des restes chinois ne nous permet cependant pas d'assurer qu'il existe des nombres premiers parmi de telles solutions.

Je remercie le professeur Claude-Paul Bruter, qui m'a encouragée et orientée tout au long de ce travail.

# Bibliographie

(1) C.F. Gauss, *Recherches arithmétiques*, Ed. Jacques Gabay, 1801.
(2) C.P. Bruter, *La construction des nombres*, Ed. Ellipses, 2000.
(3) C.P. Bruter, *Du nouveau du côté des nombres*, Quadrature, n°66, Octobre-Décembre 2007, p-8-14.
(4) O. Bordellès, *Thèmes d'arithmétique*, Ed. Ellipses, 2006. (5) P.J. Davis, R.Hersh, *l'Univers mathématique*, Ed. Gauthier-Villars, 1985
(6) N. Charraud, *Infini et Inconscient, essai sur Georg Cantor*, Ed. Anthropos, 1994.
(7) D. Guedj, *Villa des hommes*, Ed. Robert Laffont, 2007
(8) D. Nordon, M.Mendès-France (illustrations), *Les mathématiques pures n'existent pas !*, Ed. Actes Sud, 1985.
(9) D. Nordon, *Les obstinations d'un mathématicien*, Ed. Belin Pour La Science, 2003.
(10) A. Doxiadis, *Oncle Pétros et la conjecture de Goldbach*, Ed. Points, 2002.
(11) L. Euler, *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs*, Commentatio 175 indicis Enestroemiani, Bibliothèque impartiale 3, 1751, p.10-31.
(12) P. Damphousse, *Découvrir l'arithmétique*, Ed. Ellipses, 2000.
(13) A. Astruc, *Evariste Galois*, Ed. Grandes biographies, 1999.
(14) M. Du Sautoy, *La symphonie des nombres premiers*, Ed. Eloïse d'Ormesson, 2005.
(15) J.P. Belna, *Cantor*, Ed. Les belles lettres, 2000.
(16) P. Hoffman, *Erdös, l'homme qui n'aimait que les nombres*, Ed. Belin,

2000.
(17) J. Hadamard, *Essai sur la psychologie de l'invention dans le domaine mathématique*, suivi de H. Poincaré, *L'invention mathématique*, Ed. Jacques Gabay, 2000.
(18) J.J.Gray, *Le défi de Hilbert*, Ed. Dunod, 2003.
(19) Collectif, Ebbinghaus et autres auteurs, *Les Nombres*, Ed. Vuibert, 1999.
(20) C. Laisant, *Sur un procédé expérimental de vérification de la conjecture de Goldbach*, Bulletin de la SMF n°25 de 1897.
(21) G. Tenenbaum, M. Mendès-France, *Les nombres premiers*, Collection Que sais-je ?, PUF, 2000

# Annexe 1 : Etude d'un cas : le nombre pair 43532 de premier décomposant de Goldbach égal à 211

Etudions le cas du nombre pair 43532 de racine 208 et quelques en calculant ses restes selon les nombres premiers inférieurs ou égaux à 199, le plus grand nombre premier inférieur à sa racine.

$43532 \equiv 2 \ (mod\ 3)$
$43532 \equiv 2 \ (mod\ 5)$
$43532 \equiv 6 \ (mod\ 7)$
$43532 \equiv 5 \ (mod\ 11)$
$43532 \equiv 8 \ (mod\ 13)$
$43532 \equiv 12 \ (mod\ 17)$
$43532 \equiv 3 \ (mod\ 19)$
$43532 \equiv 16 \ (mod\ 23)$
$43532 \equiv 3 \ (mod\ 29)$
$43532 \equiv 8 \ (mod\ 31)$
$43532 \equiv 20 \ (mod\ 37)$
$43532 \equiv 31 \ (mod\ 41)$
$43532 \equiv 16 \ (mod\ 43)$
$43532 \equiv 10 \ (mod\ 47)$
$43532 \equiv 19 \ (mod\ 53)$
$43532 \equiv 49 \ (mod\ 59)$
$43532 \equiv 39 \ (mod\ 61)$
$43532 \equiv 49 \ (mod\ 67)$
$43532 \equiv 9 \ (mod\ 71)$
$43532 \equiv 24 \ (mod\ 73)$
$43532 \equiv 3 \ (mod\ 79)$
$43532 \equiv 40 \ (mod\ 83)$
$43532 \equiv 11 \ (mod\ 89)$
$43532 \equiv 76 \ (mod\ 97)$
$43532 \equiv 1 \ (mod\ 101)$
$43532 \equiv 66 \ (mod\ 103)$
$43532 \equiv 90 \ (mod\ 107)$
$43532 \equiv 41 \ (mod\ 109)$
$43532 \equiv 27 \ (mod\ 113)$
$43532 \equiv 98 \ (mod\ 127)$
$43532 \equiv 40 \ (mod\ 131)$
$43532 \equiv 103 \ (mod\ 137)$
$43532 \equiv 25 \ (mod\ 139)$
$43532 \equiv 24 \ (mod\ 149)$
$43532 \equiv 44 \ (mod\ 151)$
$43532 \equiv 43 \ (mod\ 157)$
$43532 \equiv 11 \ (mod\ 163)$
$43532 \equiv 112 \ (mod\ 167)$
$43532 \equiv 109 \ (mod\ 173)$
$43532 \equiv 35 \ (mod\ 179)$
$43532 \equiv 92 \ (mod\ 181)$
$43532 \equiv 175 \ (mod\ 191)$
$43532 \equiv 107 \ (mod\ 193)$
$43532 \equiv 192 \ (mod\ 197)$
$43532 \equiv 150 \ (mod\ 199)$

Les décomposants de Goldbach de 43532 sont donc les nombres $x$ premiers et inférieurs à 21766 solutions du système de congruence suivant :

$$\begin{cases} x \equiv r_1 \ (mod\ 2) \\ x \equiv r_2 \ (mod\ 3) \\ x \equiv r_3 \ (mod\ 5) \\ x \equiv r_4 \ (mod\ 7) \\ x \equiv r_5 \ (mod\ 11) \\ ... \\ x \equiv r_4 6 \ (mod\ 199) \end{cases} \quad avec \begin{cases} r_1 \in \mathbb{Z}/2\mathbb{Z} - \{0\} \\ r_2 \in \mathbb{Z}/3\mathbb{Z} - \{0,2\} \\ r_3 \in \mathbb{Z}/5\mathbb{Z} - \{0,2\} \\ r_4 \in \mathbb{Z}/7\mathbb{Z} - \{0,6\} \\ r_5 \in \mathbb{Z}/11\mathbb{Z} - \{0,5\} \\ ... \\ r_4 6 \in \mathbb{Z}/199\mathbb{Z} - \{0,150\} \end{cases}$$

La congruence à 2 ($mod$ 3) élimine les nombres premiers $5, 11, 17, 23, 29, 47, 53, 59, 71, 83, 89, 101, 131, 137, 149, 167, 173, 179, 191$ et $197$.
La congruence à 2 ($mod$ 5) élimine les nombres premiers $7, 37, 67, 97, 127$ et $157$.
La congruence à 6 ($mod$ 7) élimine les nombres premiers $13, 139$ et $181$.
La congruence à 8 ($mod$ 13) élimine les nombres premiers $73, 151$ et $193$.
La congruence à 12 ($mod$ 17) élimine le nombre premier $199$.
La congruence à 3 ($mod$ 19) élimine les nombres premiers $3$ et $79$.
La congruence à 3 ($mod$ 29) élimine le nombre premier $61$.
La congruence à 8 ($mod$ 31) élimine le nombre premier $163$.
La congruence à 31 ($mod$ 41) élimine les nombres premiers $31$ et $113$.
La congruence à 19 ($mod$ 53) élimine le nombre premier $19$.
La congruence à 103 ($mod$ 137) élimine le nombre premier $103$.
La congruence à 43 ($mod$ 157) élimine le nombre premier $43$.
La congruence à 109 ($mod$ 173) élimine le nombre premier $109$.

Le nombre premier le plus petit à ne pas être éliminé par toutes ces congruences est donc 211 dont la représentation par un n-uplet de 46 coordonnées est $(1, 1, 1, 1, 2, 3, 7, 2, 4, 8, 25, 26, 6, 39, 23{,}52, 34, 28, 10, 69, 65, 53, 45, 33, 17, 9, 5, 104, 102, 98, 84, 80, 74, 72, 62, 60, 54, 48, 44, 38, 32, 30, 20, 18, 14, 12)$.

La méthode présentée ici tire parti des représentations modulaires des entiers pour estimer plus rapidement si un nombre peut être décomposant de Goldbach d'un nombre pair, sans avoir à tester "précisément" sa primarité. Elle est en ceci avantageuse par rapport à une procédure qui, cherchant les décomposants de Goldbach de $2x$, consisterait à calculer pour chaque premier $p$ inférieur à $x$ si $2x - p$ est premier.

# 1 Tableaux de recherche des décomposants de Goldbach

Sont fournis ici les tableaux de décomposition Goldbach des nombres de 12 à 100.On ne fournit pas les tableaux des nombres doubles de premiers car ils vérifient trivialement la conjecture de Goldbach.
On trouvera pour chaque cas le triplet de référence, la décomposition de $2x$ dans ce triplet, et pour chaque nombre premier à $2x$ (sauf 1), sa représentation, sa propriété $c1$ (représentée par une croix) et sa propriété $c2$ (représentée par un cercle), le fait qu'il soit ou non décomposant de Goldbach de $2x$ (lettre $G$ et lettres $NG$ s'il aurait dû l'être mais ne l'est pas à cause de congruence à $2x$ ou à *null* modulo des premiers plus grands que ceux du n-uplet de référence dans lequel on se place).
A la fin du document seront fournies quelques pistes pour le comptage.

- nombre pair 12
  couple de référence = (2,3)
  12 = (0,0)

| | | | | |
|---|---|---|---|---|
| 3 | $(1,0)$ | | | |
| 5 | $(1,2)$ | $\times$ | $\circ$ | $G$ |

- nombre pair 16
  couple de référence = (2,3)
  16 = (0,1)

| | | | | |
|---|---|---|---|---|
| 3 | $(1,0)$ | $\times$ | | |
| 5 | $(1,2)$ | $\times$ | $\circ$ | $G$ |
| 7 | $(1,1)$ | | $\circ$ | |

- nombre pair 18
  couple de référence = (2,3)
  18 = (0,0)

| | | | | |
|---|---|---|---|---|
| 5 | $(1,2)$ | $\times$ | $\circ$ | $G$ |
| 7 | $(1,1)$ | $\times$ | $\circ$ | $G$ |

- nombre pair 20
  couple de référence = (2,3)
  20 = (0,2)

| | | | | |
|---|---|---|---|---|
| 3 | $(1,0)$ | $\times$ | | |
| 7 | $(1,1)$ | $\times$ | $\circ$ | $G$ |
| 9 | $(1,0)$ | $\times$ | | |

- nombre pair 24
  couple de référence = (2,3)
  24 = (0,0)

| | | | | |
|---|---|---|---|---|
| 5 | $(1,2)$ | $\times$ | $\circ$ | $G$ |
| 7 | $(1,1)$ | $\times$ | $\circ$ | $G$ |
| 11 | $(1,2)$ | $\times$ | $\circ$ | $G$ |

- nombre pair 28
  couple de référence = (2,3)
  28 = (0,1)

| | | | | |
|---|---|---|---|---|
| 3 | $(1,0)$ | $\times$ | | |
| 5 | $(1,2)$ | $\times$ | $\circ$ | $G$ |
| 9 | $(1,0)$ | $\times$ | | |
| 11 | $(1,2)$ | $\times$ | $\circ$ | $G$ |
| 13 | $(1,1)$ | | $\circ$ | |

- nombre pair 30
  triplet de référence = (2,3,5)
  30 = (0,0,0)

| | | | | |
|---|---|---|---|---|
| 7 | $(1,1,2)$ | $\times$ | $\circ$ | $G$ |
| 11 | $(1,2,1)$ | $\times$ | $\circ$ | $G$ |
| 13 | $(1,1,3)$ | $\times$ | $\circ$ | $G$ |

- nombre pair 32
  triplet de référence = (2,3,5)
  32 = (0,2,2)

| | | | | |
|---|---|---|---|---|
| 3 | $(1,0,3)$ | $\times$ | | |
| 5 | $(1,2,0)$ | | | |
| 7 | $(1,1,2)$ | | $\circ$ | |
| 9 | $(1,0,4)$ | $\times$ | | |
| 11 | $(1,2,1)$ | | $\circ$ | |
| 13 | $(1,1,3)$ | $\times$ | $\circ$ | $G$ |
| 15 | $(1,0,0)$ | $\times$ | | |

- nombre pair 36
  triplet de référence = (2,3,5)
  36 = (0,0,1)

| | | | | |
|---|---|---|---|---|
| 5 | $(1,2,0)$ | $\times$ | | |
| 7 | $(1,1,2)$ | $\times$ | $\circ$ | $G$ |
| 11 | $(1,2,1)$ | | $\circ$ | |
| 13 | $(1,1,3)$ | $\times$ | $\circ$ | $G$ |
| 17 | $(1,2,2)$ | $\times$ | $\circ$ | $G$ |

- nombre pair 40
  triplet de référence = (2,3,5)
  40 = (0,1,0)

| | | | | |
|---|---|---|---|---|
| 3 | $(1,0,3)$ | $\times$ | | |
| 7 | $(1,1,2)$ | | $\circ$ | |
| 9 | $(1,0,4)$ | $\times$ | | |
| 11 | $(1,2,1)$ | $\times$ | $\circ$ | $G$ |
| 13 | $(1,1,3)$ | | $\circ$ | |
| 17 | $(1,2,2)$ | $\times$ | $\circ$ | $G$ |
| 19 | $(1,1,4)$ | | $\circ$ | |

- nombre pair 42
  triplet de référence = (2,3,5)
  42 = (0,0,2)

| | | | | |
|---|---|---|---|---|
| 5 | $(1,2,0)$ | $\times$ | | |
| 11 | $(1,2,1)$ | $\times$ | $\circ$ | $G$ |
| 13 | $(1,1,3)$ | $\times$ | $\circ$ | $G$ |
| 17 | $(1,2,2)$ | | $\circ$ | |
| 19 | $(1,1,4)$ | $\times$ | $\circ$ | $G$ |

- nombre pair 44
  triplet de référence = (2,3,5)
  44 = (0,2,4)

| | | | | |
|---|---|---|---|---|
| 3 | $(1,0,3)$ | $\times$ | | |
| 5 | $(1,2,0)$ | | | |
| 7 | $(1,1,2)$ | $\times$ | $\circ$ | $G$ |
| 9 | $(1,0,4)$ | | | |
| 13 | $(1,1,3)$ | $\times$ | $\circ$ | $G$ |
| 15 | $(1,0,0)$ | $\times$ | | |
| 17 | $(1,2,2)$ | | $\circ$ | |
| 19 | $(1,1,4)$ | | $\circ$ | |
| 21 | $(1,0,1)$ | $\times$ | | |

- nombre pair 48
  triplet de référence = (2,3,5)
  48 = (0,0,3)

| | | | | |
|---|---|---|---|---|
| 5 | $(1,2,0)$ | $\times$ | | |
| 7 | $(1,1,2)$ | $\times$ | $\circ$ | $G$ |
| 11 | $(1,2,1)$ | $\times$ | $\circ$ | $G$ |
| 13 | $(1,1,3)$ | | $\circ$ | |
| 17 | $(1,2,2)$ | $\times$ | $\circ$ | $G$ |
| 19 | $(1,1,4)$ | $\times$ | $\circ$ | $G$ |
| 23 | $(1,2,3)$ | | $\circ$ | |

- nombre pair 50
  triplet de référence = (2,3,5)
  50 = (0,2,0)

| | | | | |
|---|---|---|---|---|
| 3 | $(1,0,3)$ | $\times$ | | |
| 7 | $(1,1,2)$ | $\times$ | $\circ$ | $G$ |
| 9 | $(1,0,4)$ | $\times$ | | |
| 11 | $(1,2,1)$ | | $\circ$ | |
| 13 | $(1,1,3)$ | $\times$ | $\circ$ | $G$ |
| 17 | $(1,2,2)$ | | $\circ$ | |
| 19 | $(1,1,4)$ | $\times$ | $\circ$ | $G$ |
| 21 | $(1,0,1)$ | $\times$ | | |
| 23 | $(1,2,3)$ | | $\circ$ | |

- nombre pair 52
  triplet de référence = (2,3,5)
  52 = (0,1,2)

| | | | | |
|---|---|---|---|---|
| 3 | $(1,0,3)$ | $\times$ | | |
| 5 | $(1,2,0)$ | $\times$ | | |
| 7 | $(1,1,2)$ | | $\circ$ | |
| 9 | $(1,0,4)$ | $\times$ | | |
| 11 | $(1,2,1)$ | $\times$ | $\circ$ | $G$ |
| 15 | $(1,0,0)$ | $\times$ | | |
| 17 | $(1,2,2)$ | | $\circ$ | |
| 19 | $(1,1,4)$ | | $\circ$ | |
| 21 | $(1,0,1)$ | $\times$ | | |
| 23 | $(1,2,3)$ | $\times$ | $\circ$ | $G$ |
| 25 | $(1,1,0)$ | | | |

- nombre pair 54
  triplet de référence = (2,3,5)
  54 = (0,0,4)

| | | | | |
|---|---|---|---|---|
| 5 | $(1,2,0)$ | $\times$ | | |
| 7 | $(1,1,2)$ | $\times$ | $\circ$ | $G$ |
| 11 | $(1,2,1)$ | $\times$ | $\circ$ | $G$ |
| 13 | $(1,1,3)$ | $\times$ | $\circ$ | $G$ |
| 17 | $(1,2,2)$ | $\times$ | $\circ$ | $G$ |
| 19 | $(1,1,4)$ | | $\circ$ | |
| 23 | $(1,2,3)$ | $\times$ | $\circ$ | $G$ |
| 25 | $(1,1,0)$ | $\times$ | | |

- nombre pair 56
  triplet de référence = (2,3,5)
  56 = (0,2,1)

| | | | | |
|---|---|---|---|---|
| 3 | $(1,0,3)$ | $\times$ | | |
| 5 | $(1,2,0)$ | | | |
| 9 | $(1,0,4)$ | $\times$ | | |
| 11 | $(1,2,1)$ | | $\circ$ | |
| 13 | $(1,1,3)$ | $\times$ | $\circ$ | $G$ |
| 15 | $(1,0,0)$ | $\times$ | | |
| 17 | $(1,2,2)$ | | $\circ$ | |
| 19 | $(1,1,4)$ | $\times$ | $\circ$ | $G$ |
| 23 | $(1,2,3)$ | | $\circ$ | |
| 25 | $(1,1,0)$ | $\times$ | | |
| 27 | $(1,0,2)$ | $\times$ | | |

- nombre pair 60
  triplet de référence = (2,3,5)
  60 = (0,0,0)

| | | | | |
|---|---|---|---|---|
| 7 | $(1,1,2)$ | $\times$ | $\circ$ | $G$ |
| 11 | $(1,2,1)$ | $\times$ | $\circ$ | $NG$ |
| 13 | $(1,1,3)$ | $\times$ | $\circ$ | $G$ |
| 17 | $(1,2,2)$ | $\times$ | $\circ$ | $G$ |
| 19 | $(1,1,4)$ | $\times$ | $\circ$ | $G$ |
| 23 | $(1,2,3)$ | $\times$ | $\circ$ | $G$ |
| 29 | $(1,2,4)$ | $\times$ | $\circ$ | $G$ |

  *explication du NG* : 60 et 11 sont tous les deux congrus à 4 (mod 7).

- nombre pair 64
  triplet de référence = (2,3,5)
  64 = (0,1,4)

| | | | | |
|---|---|---|---|---|
| 3 | $(1,0,3)$ | $\times$ | | |
| 5 | $(1,2,0)$ | $\times$ | | |
| 7 | $(1,1,2)$ | | $\circ$ | |
| 9 | $(1,0,4)$ | | | |
| 11 | $(1,2,1)$ | $\times$ | $\circ$ | $G$ |
| 13 | $(1,1,3)$ | | $\circ$ | |
| 15 | $(1,0,0)$ | $\times$ | | |
| 17 | $(1,2,2)$ | $\times$ | $\circ$ | $G$ |
| 19 | $(1,1,4)$ | | $\circ$ | |
| 21 | $(1,0,1)$ | $\times$ | | |
| 23 | $(1,2,3)$ | $\times$ | $\circ$ | $G$ |
| 25 | $(1,1,0)$ | | | |
| 27 | $(1,0,2)$ | $\times$ | | |
| 29 | $(1,2,4)$ | | $\circ$ | |
| 31 | $(1,1,1)$ | | $\circ$ | |

- nombre pair 66
  triplet de référence = (2,3,5)
  66 = (0,0,1)

| | | | | |
|---|---|---|---|---|
| 5 | $(1,2,0)$ | $\times$ | | |
| 7 | $(1,1,2)$ | $\times$ | $\circ$ | $G$ |
| 13 | $(1,1,3)$ | $\times$ | $\circ$ | $G$ |
| 17 | $(1,2,2)$ | $\times$ | $\circ$ | $NG$ |
| 19 | $(1,1,4)$ | $\times$ | $\circ$ | $G$ |
| 23 | $(1,2,3)$ | $\times$ | $\circ$ | $G$ |
| 25 | $(1,1,0)$ | $\times$ | | |
| 29 | $(1,2,4)$ | $\times$ | $\circ$ | $G$ |
| 31 | $(1,1,1)$ | | $\circ$ | |

  *explication du NG* : 66 et 17 sont tous les deux congrus à 3 (mod 7).

- nombre pair 68
  triplet de référence = (2,3,5)
  68 = (0,2,3)

| | | | | |
|---|---|---|---|---|
| 3 | $(1,0,3)$ | | | |
| 5 | $(1,2,0)$ | | | |
| 7 | $(1,1,2)$ | $\times$ | $\circ$ | $G$ |
| 9 | $(1,0,4)$ | $\times$ | | |
| 11 | $(1,2,1)$ | | $\circ$ | |
| 13 | $(1,1,3)$ | | $\circ$ | |
| 15 | $(1,0,0)$ | $\times$ | | |
| 19 | $(1,1,4)$ | $\times$ | $\circ$ | $NG$ |
| 21 | $(1,0,1)$ | $\times$ | | |
| 23 | $(1,2,3)$ | | $\circ$ | |
| 25 | $(1,1,0)$ | $\times$ | | |
| 27 | $(1,0,2)$ | $\times$ | | |
| 29 | $(1,2,4)$ | | $\circ$ | |
| 31 | $(1,1,1)$ | $\times$ | $\circ$ | $G$ |
| 33 | $(1,0,3)$ | | | |

  *explication du NG* : 68 et 19 sont tous les deux congrus à 5 (mod 7).

- nombre pair 70
  triplet de référence = (2,3,5)
  70 = (0,1,0)

| | | | | |
|---|---|---|---|---|
| 3 | $(1,0,3)$ | $\times$ | | |
| 9 | $(1,0,4)$ | $\times$ | | |
| 11 | $(1,2,1)$ | $\times$ | $\circ$ | $G$ |
| 13 | $(1,1,3)$ | | $\circ$ | |
| 17 | $(1,2,2)$ | $\times$ | $\circ$ | $G$ |
| 19 | $(1,1,4)$ | | $\circ$ | |
| 23 | $(1,2,3)$ | $\times$ | $\circ$ | $G$ |
| 27 | $(1,0,2)$ | $\times$ | | |
| 29 | $(1,2,4)$ | $\times$ | $\circ$ | $G$ |
| 31 | $(1,1,1)$ | | $\circ$ | |
| 33 | $(1,0,3)$ | $\times$ | | |

- nombre pair 72
  triplet de référence = (2,3,5)
  72 = (0,0,2)

| | | | | |
|---|---|---|---|---|
| 5 | $(1,2,0)$ | $\times$ | | |
| 7 | $(1,1,2)$ | | $\circ$ | |
| 11 | $(1,2,1)$ | $\times$ | $\circ$ | $G$ |
| 13 | $(1,1,3)$ | $\times$ | $\circ$ | $G$ |
| 17 | $(1,2,2)$ | | $\circ$ | |
| 19 | $(1,1,4)$ | $\times$ | $\circ$ | $G$ |
| 23 | $(1,2,3)$ | $\times$ | $\circ$ | $NG$ |
| 25 | $(1,1,0)$ | $\times$ | | |
| 29 | $(1,2,4)$ | $\times$ | $\circ$ | $G$ |
| 31 | $(1,1,1)$ | $\times$ | $\circ$ | $G$ |
| 35 | $(1,2,0)$ | $\times$ | | |

*explication du NG* : 72 et 23 sont tous les deux congrus à 2 (mod 7).

- nombre pair 76
  triplet de référence = (2,3,5)
  76 = (0,1,1)

| | | | | |
|---|---|---|---|---|
| 3 | $(1,0,3)$ | $\times$ | | |
| 5 | $(1,2,0)$ | $\times$ | | |
| 7 | $(1,1,2)$ | | $\circ$ | |
| 9 | $(1,0,4)$ | $\times$ | | |
| 11 | $(1,2,1)$ | | $\circ$ | |
| 13 | $(1,1,3)$ | | $\circ$ | |
| 15 | $(1,0,0)$ | $\times$ | | |
| 17 | $(1,2,2)$ | $\times$ | $\circ$ | $G$ |
| 21 | $(1,0,1)$ | | | |
| 23 | $(1,2,3)$ | $\times$ | $\circ$ | $G$ |
| 25 | $(1,1,0)$ | | | |
| 27 | $(1,0,2)$ | $\times$ | | |
| 29 | $(1,2,4)$ | $\times$ | $\circ$ | $G$ |
| 31 | $(1,1,1)$ | | $\circ$ | |
| 33 | $(1,0,3)$ | $\times$ | | |
| 35 | $(1,2,0)$ | $\times$ | | |
| 37 | $(1,1,2)$ | | $\circ$ | |

- nombre pair 78
  triplet de référence = (2,3,5)
  78 = (0,0,3)

| | | | | |
|---|---|---|---|---|
| 5 | $(1,2,0)$ | $\times$ | | |
| 7 | $(1,1,2)$ | $\times$ | $\circ$ | $G$ |
| 11 | $(1,2,1)$ | $\times$ | $\circ$ | $G$ |
| 17 | $(1,2,2)$ | $\times$ | $\circ$ | $G$ |
| 19 | $(1,1,4)$ | $\times$ | $\circ$ | $G$ |
| 23 | $(1,2,3)$ | | $\circ$ | |
| 25 | $(1,1,0)$ | $\times$ | | |
| 29 | $(1,2,4)$ | $\times$ | $\circ$ | $NG$ |
| 31 | $(1,1,1)$ | $\times$ | $\circ$ | $G$ |
| 35 | $(1,2,0)$ | $\times$ | | |
| 37 | $(1,1,2)$ | $\times$ | $\circ$ | $G$ |

*explication du NG* : 78 et 29 sont tous les deux congrus à 1 (mod 7).

- nombre pair 80
  triplet de référence = (2,3,5)
  80 = (0,2,0)

| | | | | |
|---|---|---|---|---|
| 3 | $(1,0,3)$ | $\times$ | | |
| 7 | $(1,1,2)$ | $\times$ | $\circ$ | $G$ |
| 9 | $(1,0,4)$ | $\times$ | | |
| 11 | $(1,2,1)$ | $\times$ | $\circ$ | $NG$ |
| 13 | $(1,1,3)$ | $\times$ | $\circ$ | $G$ |
| 17 | $(1,2,2)$ | | $\circ$ | |
| 19 | $(1,1,4)$ | $\times$ | $\circ$ | $G$ |
| 21 | $(1,0,1)$ | $\times$ | | |
| 23 | $(1,2,3)$ | | $\circ$ | |
| 27 | $(1,0,2)$ | $\times$ | | |
| 29 | $(1,2,4)$ | | $\circ$ | |
| 31 | $(1,1,1)$ | $\times$ | $\circ$ | $NG$ |
| 33 | $(1,0,3)$ | $\times$ | | |
| 37 | $(1,1,2)$ | $\times$ | $\circ$ | $G$ |
| 39 | $(1,0,4)$ | $\times$ | | |

  *explication des deux NG* : 80 et 11 sont tous les deux congrus à 11 (mod 23) et 80 et 31 sont tous les deux congrus à 3 (mod 7).

- nombre pair 84
  triplet de référence = (2,3,5)
  84 = (0,0,4)

| | | | | |
|---|---|---|---|---|
| 5 | $(1,2,0)$ | | | |
| 11 | $(1,2,1)$ | $\times$ | $\circ$ | $G$ |
| 13 | $(1,1,3)$ | $\times$ | $\circ$ | $G$ |
| 17 | $(1,2,2)$ | $\times$ | $\circ$ | $G$ |
| 19 | $(1,1,4)$ | | $\circ$ | |
| 23 | $(1,2,3)$ | $\times$ | $\circ$ | $G$ |
| 25 | $(1,1,0)$ | | | |
| 29 | $(1,2,4)$ | | $\circ$ | |
| 31 | $(1,1,1)$ | $\times$ | $\circ$ | $G$ |
| 37 | $(1,1,2)$ | $\times$ | $\circ$ | $G$ |
| 41 | $(1,2,1)$ | $\times$ | $\circ$ | $G$ |

- nombre pair 88
  triplet de référence = (2,3,5)
  88 = (0,1,3)

| | | | | |
|---|---|---|---|---|
| 3 | $(1,0,3)$ | | | |
| 5 | $(1,2,0)$ | $\times$ | | |
| 7 | $(1,1,2)$ | | $\circ$ | |
| 9 | $(1,0,4)$ | $\times$ | | |
| 13 | $(1,1,3)$ | | $\circ$ | |
| 15 | $(1,0,0)$ | $\times$ | | |
| 17 | $(1,2,2)$ | $\times$ | $\circ$ | $G$ |
| 19 | $(1,1,4)$ | | $\circ$ | |
| 21 | $(1,0,1)$ | $\times$ | | |
| 23 | $(1,2,3)$ | | $\circ$ | |
| 25 | $(1,1,0)$ | | | |
| 27 | $(1,0,2)$ | $\times$ | | |
| 29 | $(1,2,4)$ | $\times$ | $\circ$ | $G$ |
| 31 | $(1,1,1)$ | | $\circ$ | |
| 35 | $(1,2,0)$ | $\times$ | | |
| 37 | $(1,1,2)$ | | $\circ$ | |
| 39 | $(1,0,4)$ | $\times$ | | |
| 41 | $(1,2,1)$ | $\times$ | $\circ$ | $G$ |
| 43 | $(1,1,3)$ | | $\circ$ | |

- nombre pair 90
  triplet de référence = (2,3,5)
  90 = (0,0,0)

| | | | | |
|---|---|---|---|---|
| 7 | $(1,1,1)$ | $\times$ | $\circ$ | $G$ |
| 11 | $(1,1,1)$ | $\times$ | $\circ$ | $G$ |
| 13 | $(1,1,1)$ | $\times$ | $\circ$ | $NG$ |
| 17 | $(1,1,1)$ | $\times$ | $\circ$ | $G$ |
| 19 | $(1,1,1)$ | $\times$ | $\circ$ | $G$ |
| 23 | $(1,1,1)$ | $\times$ | $\circ$ | $G$ |
| 29 | $(1,1,1)$ | $\times$ | $\circ$ | $G$ |
| 31 | $(1,1,1)$ | $\times$ | $\circ$ | $G$ |
| 37 | $(1,1,1)$ | $\times$ | $\circ$ | $G$ |
| 41 | $(1,1,1)$ | $\times$ | $\circ$ | $NG$ |
| 43 | $(1,1,1)$ | $\times$ | $\circ$ | $G$ |

  *explication des deux NG* : 90, 13 et 1 sont tous les trois congrus à 6 (mod 7).

- nombre pair 92
  triplet de référence = (2,3,5)
  92 = (0,2,2)

| | | | | |
|---|---|---|---|---|
| 3 | $(1,0,3)$ | $\times$ | | |
| 5 | $(1,2,0)$ | | | |
| 7 | $(1,1,2)$ | | $\circ$ | |
| 9 | $(1,0,4)$ | $\times$ | | |
| 11 | $(1,2,1)$ | | $\circ$ | |
| 13 | $(1,1,3)$ | $\times$ | $\circ$ | $G$ |
| 15 | $(1,0,0)$ | $\times$ | | |
| 17 | $(1,2,2)$ | | $\circ$ | |
| 19 | $(1,1,4)$ | $\times$ | $\circ$ | $G$ |
| 21 | $(1,0,1)$ | $\times$ | | |
| 25 | $(1,1,0)$ | $\times$ | | |
| 27 | $(1,0,2)$ | | | |
| 29 | $(1,2,4)$ | | $\circ$ | |
| 31 | $(1,1,1)$ | $\times$ | $\circ$ | $G$ |
| 33 | $(1,0,3)$ | $\times$ | | |
| 35 | $(1,2,0)$ | | | |
| 37 | $(1,1,2)$ | | $\circ$ | |
| 39 | $(1,0,4)$ | $\times$ | | |
| 41 | $(1,2,1)$ | | $\circ$ | |
| 43 | $(1,1,3)$ | $\times$ | $\circ$ | $NG$ |
| 45 | $(1,0,0)$ | $\times$ | | |

  *explication du NG* : 92 et 143 sont tous les deux congrus à 1 (mod 7).

- nombre pair 96
  triplet de référence = (2,3,5)
  96 = (0,0,1)

| | | | | |
|---|---|---|---|---|
| 5 | $(1,2,0)$ | $\times$ | | |
| 7 | $(1,1,2)$ | $\times$ | $\circ$ | $G$ |
| 11 | $(1,2,1)$ | | $\circ$ | |
| 13 | $(1,1,3)$ | $\times$ | $\circ$ | $G$ |
| 17 | $(1,2,2)$ | $\times$ | $\circ$ | $G$ |
| 19 | $(1,1,4)$ | $\times$ | $\circ$ | $NG$ |
| 23 | $(1,2,3)$ | $\times$ | $\circ$ | $G$ |
| 25 | $(1,1,0)$ | $\times$ | | |
| 29 | $(1,2,4)$ | $\times$ | $\circ$ | $G$ |
| 31 | $(1,1,1)$ | | $\circ$ | |
| 35 | $(1,2,0)$ | $\times$ | | |
| 37 | $(1,1,2)$ | $\times$ | $\circ$ | $G$ |
| 41 | $(1,2,1)$ | | $\circ$ | |
| 43 | $(1,1,3)$ | $\times$ | $\circ$ | $G$ |
| 47 | $(1,2,2)$ | $\times$ | $\circ$ | $NG$ |

  *explication des deux NG* : 96, 19 et 47 sont tous les trois congrus à 5 (mod 7).

Le nombre de cercles est toujours compris entre le produit des $p_i - 1$ et $\Pi(x) - \omega(2x)$ où $\omega(n)$ est le nombre de facteurs premiers distincts de $n$ tel que

défini dans Bordellès.
Le nombre de croix est toujours supérieur au produit des $p_i - 1$ ou $p_i - 2$ suivant que la coordonnée de la représentation de $2x$ selon $p_i$ est nulle ou non nulle. Ce nombre est toujours supérieur au produit des $p_i - 2$.
Si on arrivait à prouver que la somme du produit des $p_i - 2$ et du produit des $p_i - 1$ est toujours supérieure strictement à $\frac{1}{2}\varphi(2x) - 1$ alors, en vertu du principe des tiroirs, on aurait une preuve de la conjecture (on aurait un nombre premier qui vérifie les deux propriétés $c1$ et $c2$).

# 1 Exponentielles de nombres premiers

Au sujet de la question posée sur les exponentielles de nombres premiers, j'en ai d'abord calculé quelques unes sur une calculatrice scientifique.
Le nombre ayant pour Log 3 (du moins fourni par la calculatrice) est 20,08553692.
Celui qui a 5 pour Log est 148,4131591.
Pour 7, c'est 1096,633158.
Pour 11, 59874,14172, etc.
Pour 19 et 23, la calculatrice fournit des nombres entiers.
Pour 29, ça sort du cadre : $3,93133429710^{12}$.
Alors j'ai cherché sur la toile et trouvé deux extraits de livres qui pourraient vous intéresser en pièces jointes.
Enfin, dans le livre d'Aigner et Ziegler "Raisonnement divins", dans le chapitre 6, page 37, il y a une démonstration du fait que tous ces nombres sont irrationnels, indépendamment de la primarité :
Théorème : $e^r$ est irrationnel pour tout $r \in \mathbb{Q}\backslash\{0\}$.
Tout cela me dépasse totalement, je ne suis à peu près à l'aise que dans le discret, l'entier, la combinatoire. Tout le reste est trop loin. Je sais que c'est ridicule de ne pas apprécier à ce point-là de réfléchir dans le continu (cf Kronecker) mais comme je n'ai pas d'obligation, autant m'orienter vers ce qui m'attire davantage.

# 2 Décomposants de Goldbach et découverte extraordinaire d'Euler

Dans l'article "Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs", Euler fournit une récurrence surprenante qui lie entre elles les sommes des diviseurs des entiers successifs.

$$\sigma(n) = \sigma(n-1) + \sigma(n-2) - \sigma(n-5) - \sigma(n-7) + \sigma(n-12) + \sigma(n-15) - ... \quad (1)$$

Monsieur Giard fournit sur la toile une autre récurrence, non moins surprenante, pour calculer la somme des diviseurs d'un entier.

$$\sigma(n) = \frac{12}{n^2(n-1)} \sum_{k=1}^{k=n-1} (5k(n-k) - n^2)\sigma(k)\sigma(n-k) \quad (2)$$

Un nombre premier $p$ a pour somme de diviseurs $p+1$. Donc $p$ est premier si et seulement si :

$$\frac{12}{n^2(n^2-1)} \sum_{k=1}^{k=n-1} (5k(n-k) - n^2)\sigma(k)\sigma(n-k) = 1 \quad (3)$$

Cette récurrence fonctionne effectivement. Elle manipule deux triangles de nombres, qui rappellent le triangle de Pascal.
Voici le premier triangle :
1
1 1
-1 4 -1
-5 5 5 -5
-11 4 9 4 -11
-19 1 11 11 1 -19
-29 -4 11 16 11 -4 -29
-41 -11 9 19 19 9 -11 -41
-55 -20 5 20 25 20 5 -20 -55

Le triangle ci-dessus contient les coefficients multiplicatifs
$p(n,k) = -n^2 + 5kn - 5k^2$ pour $n$ variant de 2 à 10 et pour $k$ variant dans chaque ligne de 1 à $n-1$.

Et voici le deuxième triangle :
1
3 3
4 9 4
7 12 12 7
6 21 16 21 6
12 18 28 28 18 12
8 36 24 49 24 36 8
15 24 48 42 42 48 24 15
13 45 32 84 36 84 32 45 13

Pour trouver le premier élément de chaque ligne de ce deuxième triangle, on multiplie terme à terme les éléments des lignes précédentes dans les deux triangles et on multiplie le résultat par $\frac{12}{n^2(n-1)}$.
Pour trouver les autres éléments d'une ligne, on se sert des premiers éléments de chaque ligne, en les multipliant deux à deux.
Les premiers éléments des lignes de ce deuxième triangle sont les sommes des diviseurs des entiers successifs.

La conjecture de Goldbach est vérifiée par un nombre pair $2a$ s'il existe deux nombres premiers $p$ et $q$ tels que $\sigma(p) + \sigma(q) = 2a + 2$. La récurrence fournie ci-dessus permettrait-elle d'approcher la conjecture d'une autre manière ?...
Indépendamment d'une démonstration éventuelle, la formule $\sigma(p)+\sigma(q) = 2a+2$ permet d'imaginer une sorte de "paysage de Goldbach" en trois dimensions (inspiré par le paysage associé à la fonction zeta par Riemann tel que décrit dans les livres de vulgarisation "la symphonie des nombres premiers" ou "dans la jungle des nobmres premiers").
Dans un espace à trois dimensions, on relie les points à coordonnées entières $(x, y, z)$ définis par $z = \sigma(x) + \sigma(y)$ par une surface bosselée. Quand on "se promène" sur une diagonale d'équation $x + y = 2a$, les "trous" dans lesquels on tombe (les points qui minimisent $\sigma(x) + \sigma(y)$) sont justement les solutions Goldbach de $2a$ (c'est à dire de deux premières coordonnées premières).

# 3 Cribles et coopératives agricoles

A chaque nombre, on a décidé d'associer ses restes selon les divisions par les nombres premiers inférieurs à sa racine. Ce tri des nombres par leur reste selon différents modules m'a fait retrouver un vieux souvenir, par analogie.
Quand j'étais petite, mon oncle travaillait dans une coopérative agricole de fruits en Provence. Un dimanche, il nous y a emmenés pour nous montrer le fonctionnement des "calibreuses".
C'est exactement comme cela que je vois les nombres maintenant, avec cette idée des restes selon les différentes divisions. Une calibreuse est une sorte de tapis roulant sur lequel on dépose au départ toutes les poires en vrac. Elles avancent sur le tapis roulant et au fur et à mesure, elles doivent traverser des espèces de disques en métal, qui tournent sur leur axe et qui contiennent différents trous de différentes tailles. Les poires ne peuvent pas passer par les petits trous mais peuvent passer par le premier trou de taille plus grande que leur taille. Alors, selon le disque qu'elles ont traversé, elles se retrouvent dans différents chemins et selon le même principe et par dichotomie, au bout des différents tapis, on retrouve des poires complètement triées selon un certain nombre de calibres.

Totalement indépendamment de cette anecdote, comparons maintenant le crible d'Eratosthène au "crible de Goldbach", le premier cherchant les nombres premiers inférieurs à 50 et le second cherchant les nombres premiers fournissant une décomposition de Goldbach de 100. 100 s'écrit (1,0,2) dans le triplet de référence (3,5,7) (on ne considèrera que les nombres impairs, les pairs n'étant jamais premiers).
Par la passe du crible d'Eratosthène d'élimination des multiples de 3, on élimine 9, 15, 21, 27, 33, 39 et 45.
Par la passe du crible de Goldbach d'élimination des "congrus à 1 mod 3", on élimine 7, 13, 19, 25, 31, 37, 43, 49.
Par la passe du crible d'Eratosthène d'élimination des multiples de 5, on élimine 25, 35 et 45 (15 a déjà été éliminé).
Par la passe du crible de Goldbach d'élimination des "congrus à 0 mod 5", on élimine 5, 15, 35, 45 (25 a déjà été éliminé).
Par la passe du crible d'Eratosthène d'élimination des multiples de 7, on élimine 49 (21 et 35 ont déjà été éliminés).
Par la passe du crible de Goldbach d'élimination des "congrus à 2 mod 7", on élimine 9 et 23 (37 a déjà été éliminé).
Il reste comme nombres premiers impairs inférieurs à 50 : 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.
Il reste comme nombres premiers impairs fournissant une décomposition de 100 : 3, 11, 17, 29, 41 et 47.
Les processus sont très similaires.

# 4 Pourquoi la non-congruence selon les petits premiers implique-t-elle la non-congruence selon les premiers plus grands ?

Quand on prend des nombres espacés régulièrement (selon une progression arithmétique), on parcourt les différents restes modulo un autre nombre et cela selon une certaine périodicité. Si de plus les nombres sont premiers entre eux, on parcourt tous les restes. C'est le cas dans la note que vous m'avez aidé à écrire : en ne sélectionnant que les non-congrus selon les petits, parmi eux, il y en a toujours qui sont non-congrus selon les plus grands mais je ne sais pas le démontrer.
Il me semble qu'un texte de Legendre permettrait de répondre à une telle question mais je n'en suis pas sûre : il faudrait que je comprenne précisément ce texte.

# 5 Récurrence versus descente infinie

J'aurais aimé trouvé une récurrence à cause de ce fragment de texte de Poincaré qui exprime bien ce que l'on ressent en cherchant les décomposants de Goldbach : on se dit "ça ne peut pas ne pas marcher !" et Poincaré exprime extrêmement bien ce sentiment. Le fragment est extrait de la biographie "Poincaré : philosophe et mathématicien" d'Umberto Bottazzini aux éditions Belin Pour la Science.

Le raisonnement par récurrence : le terrain le plus naturel et le plus favorable pour cette étude est l'arithmétique élémentaire, c'est à dire les opérations mettant en jeu des nombres entiers. Quand nous analysons des opérations telles que l'addition et la multiplication, nous nous rendons compte qu'un type de raisonnement se "retrouve à chaque pas", c'est la démonstration "par récurrence" : "on établit d'abord un théorème pour $n$ égal à 1 ; on montre ensuite que, s'il est vrai de $n-1$, il est vrai de $n$, et on en conclut qu'il est vrai pour tous les nombres entiers." C'est là le "raisonnement mathématique par excellence", déclare Poincaré. Sa particularité est "qu'il contient, sous une forme condensée, une infinité de syllogismes", et qu'il permet de passer du particulier au général, du fini à l'infini, concept qui apparaît dès les premiers pas de l'arithmétique élémentaire et sans lequel "il n'y aurait pas de science parce qu'il n'y aurait rien de général", mais uniquement des énoncés particuliers.
D'où nous vient ce "raisonnement pas récurrence", s'interroge Poincaré ? Certainement pas de l'expérience. Celle-ci peut nous suggérer que la règle est vraie pour les dix ou les cent premiers nombres, mais elle est désarmée face à l'infinité de tous les nombres naturels. Le principe de contradiction (on dirait aujourd'hui le raisonnement par l'absurde) est aussi impuissant : il nous permet d'obtenir certaines vérités, mais non d'en enfermer une infinité en une seule formule. "Cette règle (le raisonnement par récurrence), inaccessible à la démonstration analytique et à l'expérience, est le véritable type du jugement synthétique *a priori*, conclut Poincaré. L"'irrésistible évidence" avec laquelle ce "principe" s'impose n'est autre que "l'affirmation de la puissance de l'esprit qui se sait capable de concevoir la répétition indéfinie d'un même acte dès que cet acte est une fois possible"...

# 6 Sharol Nau

Mon tableau préféré (parmi ceux que j'ai pu voir sur la toile) de Sharol Nau s'appelle "Goldbach Hexagon Tiling - 4", à cause du fait qu'il est "presque" symétrique, ce qui finalement ne veut rien dire mathématiquement parlant, mais qui est pourtant extrêmement compréhensible, humainement parlant... On peut le voir à l'adresse http://www.bridgesmathart.org/art-exhibits/bridges06/nau.html.

J'ai essayé ici de trouver une fonction :

- dont on connaîtrait certaines caractéristiques ;
- qui aurait le même comportement que la fonction modulo ;
- et qu'on pourrait utiliser pour que les décomposants Goldbach deviennent les solutions d'une certaine inéquation.

## 1 *Rappel du cas* 40

On cherche les décomposants de Goldbach du nombre pair $2a$ égal à 40. Ils ne peuvent être congrus à 40 selon un quelconque module premier inférieur à 20 (la moitié de 40) et ils ne peuvent pas être composés.
Dans le tableau de congruence, les restes modulaires identiques à ceux de 40 sont repérés en rouge.

| $x\backslash p$ | 3 | 5 | 7 | 11 | 13 | 17 | 19 |
|---|---|---|---|---|---|---|---|
| 3 | 0 | 3 | 3 | 3 | 3 | 3 | 3 |
| 5 | 2 | 0 | 5 | 5 | 5 | 5 | 5 |
| 7 | 1 | 2 | 0 | 7 | 7 | 7 | 7 |
| 9 | 0 | 4 | 2 | 9 | 9 | 9 | 9 |
| 11 | 2 | 1 | 4 | 0 | 11 | 11 | 11 |
| 13 | 1 | 3 | 6 | 2 | 0 | 13 | 13 |
| 15 | 0 | 0 | 1 | 4 | 2 | 15 | 15 |
| 17 | 2 | 2 | 3 | 6 | 4 | 0 | 17 |
| 19 | 1 | 4 | 5 | 8 | 6 | 2 | 0 |
| 40 | 1 | 0 | 5 | 7 | 1 | 6 | 2 |

On remarque que 9 n'a aucun reste commun avec 40. Son complémentaire à 40, qui est égal à 31, est donc premier. Par contre, ce n'est pas un décomposant de Goldbach de 40 car il est composé (son reste dans la division par 3 est nul).
Les décomposants de Goldbach de 40 sont bien 3 ($40 = 3 + 37$), 11 ($40 = 11 + 29$), 17 ($40 = 17 + 23$).

## 2 $Tangente(2\pi x/p)$

Dans le tableau suivant, on met dans les cases d'indice de ligne $x$ et d'indice de colonne $p$ la valeur de $tan(2\pi x/p)$.

| $x\backslash p$ | 3 | 5 | 7 | 11 | 13 | 17 | 19 |
|---|---|---|---|---|---|---|---|
| 3 | 0 | 0.72 | −0.48 | −6.95 | 8.23 | 2.00 | 1.53 |
| 5 | 1.73 | 0 | 4.38 | −0.29 | −0.88 | −3.51 | −12.06 |
| 7 | −1.73 | −0.72 | 0 | 1.15 | 0.24 | −0.61 | −1.08 |
| 9 | 0 | −3.07 | −4.38 | −2.18 | 2.63 | 0.18 | −0.16 |
| 11 | 1.73 | 3.07 | 0.48 | 0 | −1.44 | 1.32 | 0.54 |
| 13 | −1.73 | 0.72 | −1.25 | 2.18 | 2.63 | 0.18 | −0.16 |
| 15 | 0 | 0 | 1.25 | −1.15 | 1.44 | −0.91 | −3.94 |
| 17 | 1.73 | −0.72 | −0.48 | 0.29 | −2.63 | 0 | −0.77 |
| 19 | −1.73 | −3.07 | 4.38 | 6.95 | −0.24 | 0.91 | 0 |
| 40 | −1.73 | 0 | 4.38 | 1.15 | 0.52 | −1.32 | 0.77 |
| 4 | −1.73 | −3.07 | 0.48 | −1.15 | −2.63 | 10.79 | 3.94 |
| 6 | 0 | 3.07 | −1.25 | 0.29 | −0.24 | −1.32 | −2.27 |
| 8 | 1.73 | 0.72 | 1.25 | 6.95 | 0.88 | −0.18 | −0.54 |
| 9.2 | 0.44 | −1.57 | −2.33 | −1.65 | 3.67 | 0.26 | −0.09 |

Dans ce tableau, les cases présentant le même contenu que celles de même colonne pour le nombre 40 sont repérées en rouge.

Cela nous permet d'inventer une fonction sur les réels qui permettrait (peut-être, qui sait ?) de trouver les décomposants de Goldbach.

La condition "ne pas être congru à $2a$ selon tout module inférieur à $a$" correspond à l'inéquation suivante :

$$\prod_{p=3}^{a}[tan(2\pi x/p) - tan(4\pi a/p))] \neq 0$$

(on pourrait n'effectuer le produit que sur les $p$ premiers impairs inférieurs à $a$ mais on ne sait pas qui sont ces nombres premiers alors qu'on connaît bien les nombres de 1 à $a$)

La condition "ne pas être un impair composé" correspond à l'inéquation suivante :

$$\prod_{p=3}^{a}[tan(2\pi x/p)] \neq 0$$

La condition "x n'est pas pair" correspond à l'inéquation suivante (on doit ajouter cette condition car si l'on se contente des deux conditions ci-dessus, on "attrape" aussi des pairs dans nos filets). :

$$sin(\pi x + \pi/2) - 1 \neq 0$$

On cumule les trois conditions en la grosse inéquation suivante :

$$\prod_{p=3}^{a}[tan(2\pi x/p) - tan(4\pi a/p)) \times tan(2\pi x/p) \times (sin(\pi x + \pi/2) - 1)] \neq 0$$

Les $x$ entiers qui vérifient cette inéquation sont des décomposants de Goldbach du nombre pair $2a$.

Enfin, le problème, et non des moindres, qui subsiste, est que par cette inéquation, on peut obtenir des solutions non entières (c'est pour illustrer cela que j'ai mis le nombre décimal 9.2 en bas du tableau des tangentes) et qu'il faudrait, similairement à ce qui a été fait pour les trois conditions ci-dessus, trouver une fonction qui ne s'annulerait pas sur les entiers et qui s'annulerait sur tous les autres nombres.
Dans un premier temps, j'ai pensé à la fonction $int(x)$ qui prend la valeur 1 si $x$ est entier et 0 sinon. Mais le problème d'une telle fonction est qu'elle réduirait à néant toutes les propriétés de continuité "fréquente" (à part les quelques points par ci, par là, où elle va vers $\infty$ ou $-\infty$) de la fonction tangente qui nous semblaient intéressantes à utiliser.
Alors, j'ai cherché sur la toile. Il y a un papier de Bélair qui s'appelle "définissabilité des entiers dans les corps de courbes réels archimédiens". Absolument incompréhensible pour moi...

Ces idées présentent-elles un intérêt ?
Pensez-vous que cette histoire de solutions entières annule toute possibilité de faire quoi que ce soit en suivant cette voie-là ?
Dans le cas où cette histoire de solutions entières serait surmontable par des analystes, croyez-vous qu'on pourrait trouver quelque chose sur le nombre de solutions de l'inéquation qu'on pourrait transférer au nombre de décomposants Goldbach ?

# 1 Les deux partages de décomposants les plus chouettes qu'il m'ait été donné de voir

## 1.1 122 et 1802

Voici les décompositions de 122.
122 = 13+109
122 = 19+103
122 = 43+79
122 = 61+61

Voici les décompositions de 1802.
1802 = 13+1789
1802 = 19+1783
1802 = 43+1759
1802 = 61+1741
1802 = 79+1723
1802 = 103+1699
1802 = 109+1693
1802 = 139+1663
1802 = 181+1621
1802 = 193+1609
1802 = 223+1579
1802 = 271+1531
1802 = 313+1489
1802 = 331+1471
1802 = 349+1453
1802 = 373+1429
1802 = 379+1423
1802 = 421+1381
1802 = 499+1303
1802 = 523+1279
1802 = 571+1231
1802 = 601+1201
1802 = 631+1171
1802 = 673+1129
1802 = 709+1093
1802 = 733+1069
1802 = 739+1063
1802 = 751+1051
1802 = 769+1033
1802 = 811+991
1802 = 883+919

On voit que l'ensemble des nombres premiers décomposants de 122 est inclus dans l'ensemble des nombres premiers décomposants de 1802.

Ecrivons 122, 1802, et leurs décomposants communs en écriture par les restes selon la base (2,3,5,7,11).

| | |
|---|---|
| 122 | *a pour écriture* $0-2-2-3-1$. |
| 1802 | *a pour écriture* $0-2-2-3-9$. |
| 13 | *a pour écriture* $1-1-3-6-2$. |
| 19 | *a pour écriture* $1-1-4-5-8$. |
| 43 | *a pour écriture* $1-1-3-1-10$. |
| 61 | *a pour écriture* $1-1-1-5-6$. |
| 79 | *a pour écriture* $1-1-4-2-2$. |
| 103 | *a pour écriture* $1-1-2-5-4$. |
| 109 | *a pour écriture* $1-1-4-4-10$. |

La différence de 1802 et 122 est 1680 qui est divisible par $2 \times 3 \times 5 \times 7$, la quatrième primorielle[1].

## 1.2 Toujours plus fort (!) : les décompositions de l'Univers mathématique de Davis et Hersh[2]

Voici les premières[3] décompositions des nombres de 20902 à 20924.

| | | |
|---|---|---|
| 20902 | $= 3$ | $+20899$ |
| 20904 | $= 5$ | $+20890$ |
| 20906 | $= 3$ | $+20903$ |
| 20908 | $= 5$ | $+20903$ |
| 20910 | $= 7$ | $+20903$ |
| 20912 | $= 13$ | $+20899$ |
| 20914 | $= 11$ | $+20903$ |
| 20916 | $= 13$ | $+20903$ |
| 20918 | $= 19$ | $+20899$ |
| 20920 | $= 17$ | $+20903$ |
| 20922 | $= 19$ | $+20903$ |
| 20924 | $= 3$ | $+20921$ |

Voici les premières décompositions des nombres de 20962 à 20984.

| | | |
|---|---|---|
| 20962 | $= 3$ | $+20959$ |
| 20964 | $= 5$ | $+20959$ |
| 20966 | $= 3$ | $+20963$ |
| 20968 | $= 5$ | $+20963$ |
| 20970 | $= 7$ | $+20963$ |
| 20972 | $= 13$ | $+20959$ |
| 20974 | $= 11$ | $+20963$ |
| 20976 | $= 13$ | $+20963$ |
| 20978 | $= 19$ | $+20959$ |
| 20980 | $= 17$ | $+20963$ |
| 20982 | $= 19$ | $+20963$ |
| 20984 | $= 3$ | $+20981$ |

[1] J'ai vu une notation je ne sais plus où pour la primorielle, il faut utiliser le dièse, en l'occurrence #7.

[2] Bibliographie : P.J. Davis, R.Hersh, *l'Univers mathématique*, Ed. Gauthier-Villars, 1985

[3] Celles faisant intervenir le nombre premier le plus petit possible étant donné un nombre pair.

Dingue !!!
Elles font intervenir les mêmes nombres premiers dans le même ordre !!!
Remarquons que ces deux suites de nombres pairs sont “écartées” de 60, multiple de #5.
Observons les écritures par les restes.
Là, il faut s'arracher un peu les yeux au niveau de la lisibilité : j'ai mis, entre parenthèses dans l'écriture par les restes et pour un reste donné, le nombre premier que ce reste fait éliminer (parce que ce nombre premier appartient à la classe d'équivalence correspondante).

D'abord, voici la base des premiers, jusqu'à 149, le plus grand premier inférieur à la racine de 20984.
(2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97,101,103,107,109,113,127,131,137,139,149).

Voici les écritures par les restes de la première série de nombres.
20902 : plus petit décomposant 3
0-1-2-0-2-11-9-2-18-22-8-34-33-4-34-20-16-40-65-28-24-46-69-76-47-96-96-37-83-110-74-73-78-52

20904 : plus petit décomposant 5
0-0(3)-4-2-4-0-11-4-20-24-10-36-35-6-36-22-18-42-0-30-26-48-71-78-49-98-98-39-85-112-76-75-80-54

20906 : plus petit décomposant 3
0-2-1-4-6-2-13-6-22-26-12-1-37-8-38-24-20-44-2-32-28-50-73-80-51-100-100-41-87-1-78-77-82-56

20908 : plus petit décomposant 5
0-1-3(3)-6-8-4-15-8-1-28-14-3-39-10-40-26-22-46-4-34-30-52-75-82-53-1-102-43-89-3-80-79-84-58

20910 : plus petit décomposant 7
0-0(3)-0(5)-1-10-6-0-10-3-1-16-5-0-12-42-28-24-48-6-36-32-54-77-84-55-3-1-45-91-5-82-81-86-60

20912 : plus petit décomposant 13
0-2(5,11)-2(7)-3(3)-1-8-2-12-5-3-18-7-2-14-44-30-26-50-8-38-34-56-79-86-57-5-3-47-93-7-84-83-88-62

20914 : plus petit décomposant 11
0-1(7)-4-5(5)-3(3)-10-4-14-7-5-20-9-4-16-46-32-28-52-10-40-36-58-81-88-59-7-5-49-95-9-86-85-90-64

20916 : plus petit décomposant 13
0-0(3)-1(11)-0(7)-5(5)-12-6-16-9-7-22-11-6-18-1-34-30-54-12-42-38-60-0-1-61-9-7-51-97-11-88-87-92-66

20918 : plus petit décomposant 19
0-2(5,11,17)-3(3,13)-2-7(7)-1-8-18-11-9-24-13-8-20-3-36-32-56-14-44-40-62-2-3-63-11-9-53-99-13-90-89-94-68

20920 : plus petit décomposant 17
0-1(7,13)-0(5)-4(11)-9-3(3)-10-1-13-11-26-15-10-22-5-38-34-58-16-46-42-64-4-5-65-13-11-55-101-15-92-91-96-70

20922 : plus petit décomposant 19
0-0(3)-2(7,17)-6(13)-0(11)-5(5)-12-3-15-13-28-17-12-24-7-40-36-60-18-48-44-66-6-7-67-15-13-57-103-17-94-93-98-72

20924 : plus petit décomposant 3
0-2-4-1-2-7-14-5-17-15-30-19-14-26-9-42-38-1-20-50-46-68-8-9-69-17-15-59-105-19-96-95-100-74

Et voici les écriture par les restes de la deuxième série de nombres.
20962 : plus petit décomposant 3
0-1-2-4-7-6-1-5-9-24-6-20-11-21-0-27-17-39-58-17-11-27-46-47-10-55-53-97-34-57-7-2-1-112

20964 : plus petit décomposant 5
0-0(3)-4-6-9-8-3-7-11-26-8-22-13-23-2-29-19-41-60-19-13-29-48-49-12-57-55-99-36-59-9-4-3-114

20966 : plus petit décomposant 3
0-2-1-1-0-10-5-9-13-28-10-24-15-25-4-31-21-43-62-21-15-31-50-51-14-59-57-101-38-61-11-6-5-116

20968 : plus petit décomposant 5
0-1-3(3)-3-2-12-7-11-15-1-12-26-17-27-6-33-23-45-64-23-17-33-52-53-16-61-59-103-40-63-13-8-7-118

20970 : plus petit décomposant 7
0-0(3)-0(5)-5-4-1-9-13-17-3-14-28-19-29-8-35-25-47-66-25-19-35-54-55-18-63-61-105-42-65-15-10-9-120

20972 : plus petit décomposant 13
0-2(5,11)-2(7)-0-6-3(3)-11-15-19-5-16-30-21-31-10-37-27-49-1-27-21-37-56-57-20-65-63-0-44-67-17-12-11-122

20974 : plus petit décomposant 11
0-1(7)-4-2-8-5(5)-13-17-21-7-18-32-23-33-12-39-29-51-3(3)-29-23-39-58-59-22-67-65-2-46-69-19-14-13-124

20976 : plus petit décomposant 13
0-0(3)-1(11)-4-10-7(7)-15-0-0-9-20-34-25-35-14-41-31-53-5(5)-31-25-41-60-61-24-69-67-4-48-71-21-16-15-126

20978 : plus petit décomposant 19
0-2(5,11,17)-3(3,13)-6-1-9-0-2-2-11-22-36-27-37-16-43-33-55-7(7)-33-27-43-62-63-26-71-69-6-50-73-23-18-17-128

20980 : plus petit décomposant 17
0-1(7,13)-0(5)-1-3(3)-11(11)-2-4-4-13-24-1-29-39-18-45-35-57-9-35-29-45-64-65-28-73-71-8-52-75-25-20-19-130

20982 : plus petit décomposant 19
0-0(3)-2(7,17)-3-5(5)-0(13)-4-6-6-15-26-3-31-41-20-47-37-59-11(11)-37-31-47-66-67-30-75-73-10-54-77-27-22-21-132

20984 : plus petit décomposant 3
0-2-4-5-7-2-6-8-8-17-28-5-33-0-22-49-39-0-13-39-33-49-68-69-32-77-75-12-56-79-29-24-23-134

On voit que les écritures se correspondent terme à terme dans les deux séries seulement selon les trois premières coordonnées des n-uplets (Donc vous aviez raison au sujet d'un texte que je vous avais fait parvenir en fin d'été 2007 sur le fait que la notion d'ordre (je voulais réordonner les entiers sous prétexte que j'avais lu le bouquin de Denis Guedj sur Cantor) n'a pas d'importance ici car on n'a pas partage entre des nombres qui auraient des écritures qui seraient ce que j'avais appelé "préfixes propres" les unes des autres, au sens langagier monoïdal où on peut l'entendre (sic !), c'est à dire une suite de lettres qui commence une autre suite de lettres).

On constate également que les nombres premiers qui ne peuvent participer à une décomposition Goldbach, sous prétexte qu'ils partagent une coordonnée avec $2x$ sont éliminés par des voies totalement différentes dans les deux séries et pourtant, de façon totalement déterministe, même si de façon totalement chaotique, on se retrouve avec les mêmes décomposants dans le même ordre, et ça, je trouve que c'est franchement jubilatoire de le savoir !

## 2 Probabilités et Identité de Poincaré

Je regrette infiniment de ne pas réussir à croire que ces exemples sont le résultat de bêtes coïncidences.
Donc, j'essaie de réfléchir en terme de probabilités.

Admettons que j'aie à tirer au hasard deux couples dans un ensemble de couples dont les premières coordonnées varient de 0 à 2 (au hasard, histoire de bien visualiser la congruence mod 3) et dont la deuxième coordonnée varie de 0 à 4 (histoire cette fois-ci de bien visualiser la congruence à 5).

Chacun des deux couples peut être l'un des 15 couples différents possibles :
(0,0),(0,1),(0,2),(0,3),(0,4), (1,0),(1,1),(1,2),(1,3),(1,4), (2,0),(2,1),(2,2),(2,3),(2,4).

Quelles sont mes chances de tirer deux couples qui partagent au moins une coordonnée (i.e. le premier couple s'appelant $(x_1, y_1)$ et le deuxième s'appelant

$(y_1, y_2)$, quelle est la probabilité que $(x_1 = x_2) \vee (y_1 = y_2))$ ?

J'applique l'identité de Poincaré[4] et je trouve $\frac{7}{15}$, c'est à dire $\frac{p+q-1}{pq}$.

Je recommence pour des triplets, dont la coordonnée cette fois varie de 0 à 6 (pour la congruence selon 7).
Je réapplique l'identité de Poincaré et je calcule mes chances...
Cette fois-ci, j'obtiens $\frac{57}{105}$, selon la formule $\frac{pq+pr+qr-p-q-r+1}{pqr}$.

Par programme, j'ai calculé la valeur de la probabilité pour tous les nombres premiers jusqu'à $10^9$. J'ai trouvé 0.925046.

On dirait que la probabilité tend vers 1 mais sans jamais l'atteindre... Est-ce que pour autant cela veut dire qu'on est obligé de toujours trouver un nombre premier $p$ qui ne partage aucune de ses coordonnées avec $2x$ ?...

En fait, si on voulait vraiment être en cohérence avec les exemples qui ont été vus dans la première section, et exprimer la notion que j'appelle "partage des décomposants de Goldbach", il faudrait être capable d'exprimer en termes de probabilités le fait que deux nombres, non pas sont congrus entre eux modulo un certain nombre premier, mais ne sont pas tous les deux congrus à ce même premier selon d'autres premiers, en quelque sorte être capable d'exprimer comment deux objets ne sont pas égaux à un même troisième en se moquant de la relation qui les lie entre eux, car c'est là alors qu'ils ont des chances de partager des décomposants Goldbach...

[4] P(A $\bigcup B) = P(A) + P(B) - P(A \bigcap B)$

# Conjecture de Goldbach : approches algébrique et géométrique basées sur les restes modulaires

Denise Vella

1er Novembre 2008

## 1 Introduction

La conjecture de Goldbach (1742) énonce que tout nombre pair $2a$ supérieur ou égal à 4 est la somme de deux nombres premiers $p$ et $q$. Le nombre $p$ et le nombre $q$ sont appelés des décomposants de Goldbach de $2a$. Cette note présente deux visions de la conjecture de Goldbach, une vision algébrique et une vision géométrique, toutes deux basées sur l'étude des restes modulaires des entiers selon des modules premiers. Les décomposants de Goldbach d'un entier pair $2a$ sont les nombres premiers inférieurs ou égaux à $a$ solutions de systèmes de congruence généralisés découlant de cette représentation. Enfin, sera présentée une conjecture portant sur le partage des décomposants de Goldbach et qui donne à penser que la possibilité d'une démonstration de la conjecture de Goldbach par récurrence pourrait être envisagée.

## 2 Traitement algébrique d'un exemple

Dans une note précédente, on a présenté le choix que nous réitérons ici de représenter chaque entier par ses restes selon les modules premiers successifs.

Intéressons nous au nombre entier 40, dont on cherche les décomposants de Goldbach. On ne va s'intéresser qu'aux restes des entiers inférieurs à 20 selon les modules premiers inférieurs à la racine de 40, i.e. selon les modules 2, 3 et 5. 40 est représenté par le triplet $(0(2), 1(3), 0(5))$. Puisque seuls les nombres premiers non congrus à 40 selon tous ces modules peuvent être décomposants de Goldbach de 40, on cherche s'il existe des nombres premiers dont la représentation serait :

- soit $(1(2), 2(3), 1(5))$,
- soit $(1(2), 2(3), 2(5))$,
- soit $(1(2), 2(3), 3(5))$,
- soit $(1(2), 2(3), 4(5))$.

Considérons le premier triplet $(1(2), 2(3), 1(5))$. Les solutions satisfaisant la première coordonnée d'un tel triplet sont les nombres $x$ strictement positifs tels qu'il existe $y$ entier positif ou nul tel que l'équation $x - 2y - 1 = 0$ admet une solution (i.e. on cherche une solution qui soit forcément un nombre impair). Les solutions satisfaisant à la deuxième coordonnée du triplet sont les nombres $x$ strictement positifs tels qu'il existe $z$ entier positif ou nul tel que $x - 3z - 2 = 0$

admet une solution (on cherche un nombre qui soit non congru à 1 mod 3, en étant en l'occurrence congru à 2 mod 3).
Enfin, les solutions satisfaisant à la troisième coordonnée du triplet sont les nombres $x$ strictement positifs tels qu'il existe $t$ entier positif ou nul tel que $x - 5t - 1 = 0$ admet une solution (on cherche un nombre qui soit non congru à 0 mod 5 en étant en l'occurrence congru à 1 mod 5).

Pour le premier triplet, on aboutit donc au système d'équations diophantiennes :

$$\begin{cases} x - 2y - 1 = 0 \\ x - 3z - 2 = 0 \\ x - 5t - 1 = 0 \end{cases}$$

Pour les deuxième, troisième et quatrième triplets, on aboutit aux systèmes d'équations diophantiennes :

$$\begin{cases} x - 2y - 1 = 0 \\ x - 3z - 2 = 0 \\ x - 5t - 2 = 0 \end{cases}$$

$$\begin{cases} x - 2y - 1 = 0 \\ x - 3z - 2 = 0 \\ x - 5t - 3 = 0 \end{cases}$$

$$\begin{cases} x - 2y - 1 = 0 \\ x - 3z - 2 = 0 \\ x - 5t - 4 = 0 \end{cases}$$

Le premier système d'équations admet $(x = 11, y = 5, z = 3, t = 2)$ comme solution, 11 est décomposant de Goldbach de 40.
Le deuxième système d'équations admet $(x = 17, y = 8, z = 5, t = 3)$ comme solution, 17 est décomposant de Goldbach de 40.

# 3 Généralisation

On peut généraliser l'exemple présenté ci-dessus. Les systèmes d'équations diophantiennes que les nombres premiers décomposants de Goldbach d'un nombre pair $2a$ doivent satisfaire contiennent des équations de la forme :

$$x - p_i x_i - C_i = 0,$$

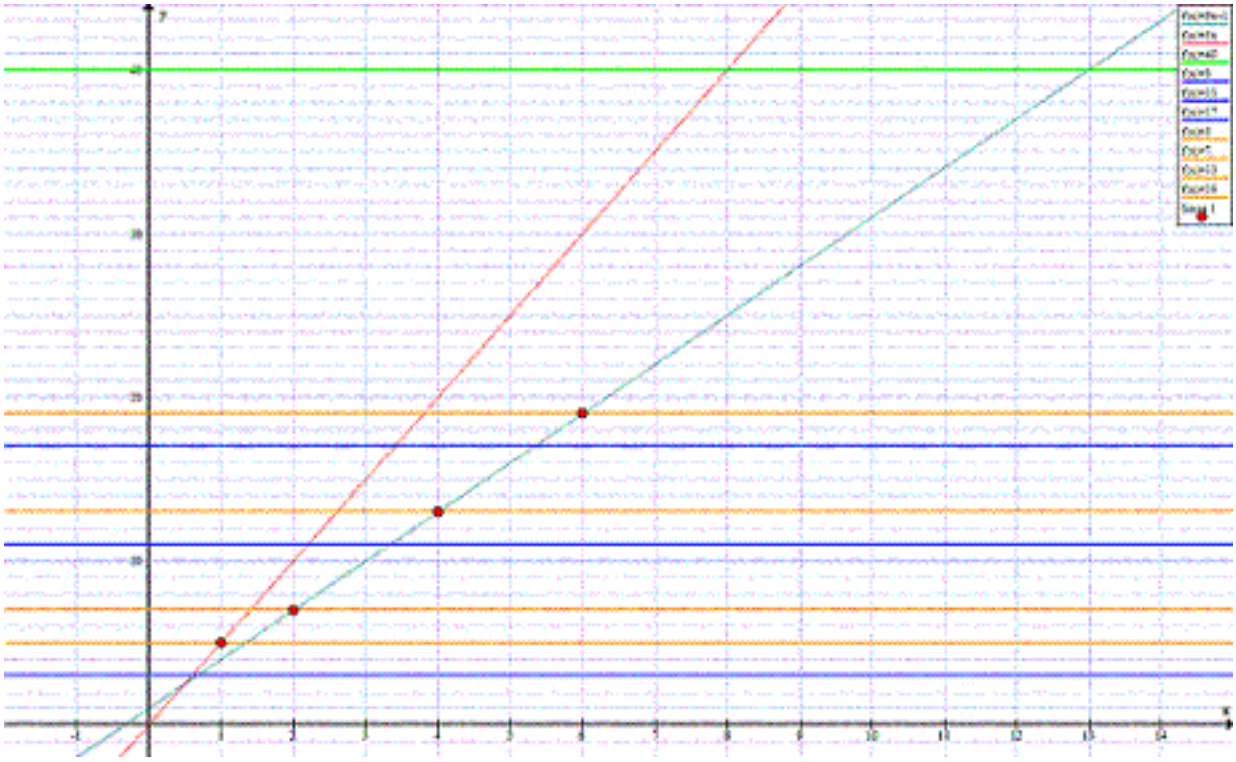
les $p_i$ étant les nombres premiers inférieurs à $\sqrt{2a}$ et les constantes $C_i$ prenant toutes les valeurs possibles qui soient à la fois différentes de 0 et différentes du reste de $2a$ modulo $p_i$.

Reste à prouver (sic !) pourquoi il existe toujours un nombre premier solution $x$ de l'un de ces systèmes d'équations diophantiennes.

Matiiassevitch a trouvé en 1970 la réponse au dixième problème de Hilbert : il n'existe aucun algorithme général permettant d'affirmer l'existence de solutions pour les équations diophantiennes.

Je me demande cependant si dans le cas qui nous intéresse ici de systèmes d'équations diophantiennes d'un type particulier, on ne pourrait pas prouver l'existence d'un nombre premier solution en utilisant le théorème de Minkowski. Ce théorème peut être utilisé d'une façon très élégante pour montrer par exemple qu'un nombre premier congru à 1 modulo 4 est toujours somme de deux carrés, ou qu'un nombre entier est toujours somme de 4 carrés. Ces deux preuves sont fournies dans le livre Arithmétique de Marc Hindry [9]. On définit un "réseau" de points à coordonnées entières. On délimite un convexe symétrique autour de l'origine et qui soit d'une taille supérieure à une taille fixée. Le théorème permet d'établir qu'un tel convexe contient toujours un point à coordonnées entières (en l'occurrence, il faudrait se débrouiller pour que le point en question soit le nombre premier inférieur à $a$ recherché).

# 4 Présentation géométrique du même exemple



Sur le repère cartésien de la figure ci-dessus, la droite horizontale verte d'équation $y = 40$ correspond au nombre 40.

Les restes de 40 selon les modules 3 et 5 se lisent sur l'axe des ordonnées (on a omis d'illustrer que 40 est pair pour augmenter la lisibilité de la figure).

Les droites horizontales bleues d'équations $y = 3$, $y = 11$ et $y = 17$ correspondent aux nombres premiers 3, 11 et 17 qui sont tous les trois décomposants de Goldbach de 40 tandis que les droites horizontales oranges d'équations $y = 5$, $y = 7$, $y = 13$ et $y = 19$ correspondent aux nombres premiers qui ne sont pas décomposants de Goldbach de 40.

Les points rouges montrent l'élimination de ces nombres premiers qui ne peuvent être décomposants de Goldbach de 40 sous prétexte qu'ils sont congrus à 40 selon un certain module. Les trois points rouges de la droite $y = 3x + 1$ éliminent les nombres premiers 7, 13 et 19 tandis que le point rouge sur la droite d'équation $y = 5x$ élimine le nombre premier 5.

Les droites horizontales bleues n'ayant pas de points d'intersection à coordonnées entières avec les droites $y = 3x + 1$ ou $y = 5x$ fournissent une visualisation des décomposants de Goldbach de 40.

On ne s'est pas intéressé à la droite d'équation $y = 9$, pourtant le nombre 9 est intéressant lorsqu'on recherche les décomposants de Goldbach de 40 parce qu'il n'est jamais congru à 40 selon les modules 2, 3 et 5 (la représentation de 9 est en effet $(1(2), 0(3), 4(5))$). On voit que 9 est composé car la droite $y = 3x$ a comme point commun avec la droite $y = 9$ le point $(3, 9)$ de coordonnées entières.

Pour aboutir à une démonstration géométrique de la conjecture de Goldbach, il faudrait être capable d'une part de compter le nombre de points à coordonnées entières qui se trouvent à l'intérieur d'un certain espace à définir précisément, et d'autre part d'utiliser un principe de raisonnement (tel que le principe des tiroirs, ou un principe combinatoire plus complexe) qui nous permettrait de déduire qu'on peut toujours trouver une droite qui n'a aucune intersection à coordonnées entières avec les droites affines visualisant l'appartenance de $2a$ à ses classes d'équivalence selon les modules premiers inférieurs à $\sqrt{2a}$.

Alain Connes a parlé dans plusieurs conférences du "démon de l'algèbre" et de "l'ange de la géométrie" selon une idée d'Hermann Weyl. Ces notions visaient peut-être à faire appréhender "l'évidence qui saute aux yeux" devant certaines démonstrations purement géométriques (on peut penser pour illustrer cela à certaines animations sur la toile faisant se déplacer les pièces d'un puzzle et rendant immédiate à notre perception visuelle la démonstration du théorème de Pythagore[1]). La représentation géométrique, sous prétexte qu'elle permet cette perception visuelle globale et immédiate d'un problème, nous évitant ainsi d'avoir à suivre le déroulement séquentiel du langage algébrique, permettrait-elle d'aboutir à une démonstration géométrique de la conjecture de Goldbach ? Le tout petit exemple fourni montre que la quantité d'éléments visuels à intégrer simultanément peut être importante.

[1] On trouve même un film de transvasement de liquides de deux parallélépipèdes plats et carrés ($a^2$ et $b^2$) vers un troisième ($c^2$).

# 5 Différentes causes, produisant les mêmes effets, peuvent provoquer une illusion de périodicité

En écumant les bibliothèques municipales, j'ai trouvé un jour un très beau livre de Davis et Hersh [2] en annexe duquel étaient fournies les décompositions de Goldbach suivantes (entre autres).

Les premières[2] décompositions des nombres de 20902 à 20924 sont :

$$\begin{array}{lll} 20902 & = 3 & +20899 \\ 20904 & = 5 & +20890 \\ 20906 & = 3 & +20903 \\ 20908 & = 5 & +20903 \\ 20910 & = 7 & +20903 \\ 20912 & = 13 & +20899 \\ 20914 & = 11 & +20903 \\ 20916 & = 13 & +20903 \\ 20918 & = 19 & +20899 \\ 20920 & = 17 & +20903 \\ 20922 & = 19 & +20903 \\ 20924 & = 3 & +20921 \end{array}$$

Et les premières décompositions des nombres de 20962 à 20984 sont ;

$$\begin{array}{lll} 20962 & = 3 & +20959 \\ 20964 & = 5 & +20959 \\ 20966 & = 3 & +20963 \\ 20968 & = 5 & +20963 \\ 20970 & = 7 & +20963 \\ 20972 & = 13 & +20959 \\ 20974 & = 11 & +20963 \\ 20976 & = 13 & +20963 \\ 20978 & = 19 & +20959 \\ 20980 & = 17 & +20963 \\ 20982 & = 19 & +20963 \\ 20984 & = 3 & +20981 \end{array}$$

En étudiant les restes modulaires, j'ai analysé pourquoi on aboutissait à la même suite de nombres premiers dans les deux cas (en espérant profondément que les mêmes causes produiraient les mêmes effets, selon l'adage). En fait, cela n'est pas du tout le cas : prenons le cas des nombres 20912 et 20972 qui ont tous les deux pour plus petit décomposant 13, c'est à dire ne peuvent avoir ni l'un ni l'autre 3, 5, 7 et 11 comme décomposants sous prétexte qu'ils partagent avec ceux-ci des classes de congruence. 20912 partage sa classe de congruence avec le nombre premier 3, cela modulo 7 alors que 20972 partage sa classe de congruence avec le même nombre premier 3 modulo 13. Les classes de congruence modulo 5, 7 et 11 sont partagées selon le même module. Quant aux deux nombres suivants, 20914 et 20974, qui ont tous deux pour plus petit décomposant 11, on voit sur leur écriture par les restes que c'est bien leur congruence commune à 1 modulo 3

[2]Celles faisant intervenir le nombre premier le plus petit possible étant donné un nombre pair.

qui fait éliminer 7 comme décomposant pour chacun d'entre eux. Par contre, la congruence à 3 se fait modulo 11 pour le premier et modulo 67 pour le second. La congruence à 5 se fait modulo 7 pour le premier et modulo 13 pour le second.

La base des nombres premiers jusqu'à 149 (le plus grand premier inférieur à la racine de 20984) qui a été utilisée est :
(2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97,101,103,107, 109,113,127,131,137,139,149).

Les écritures par les restes modulaires des nombres auxquels on s'intéresse sont :

20912 : plus petit décomposant 13
0-2(5,11)-2(7)-3(3)-1-8-2-12-5-3-18-7-2-14-44-30-26-50-8-38-34-56-79-86-57-5-3-47-93-7-84-83-88-62

20914 : plus petit décomposant 11
0-1(7)-4-5(5)-3(3)-10-4-14-7-5-20-9-4-16-46-32-28-52-10-40-36-58-81-88-59-7-5-49-95-9-86-85-90-64

20972 : plus petit décomposant 13
0-2(5,11)-2(7)-0-6-3(3)-11-15-19-5-16-30-21-31-10-37-27-49-1-27-21-37-56-57-20-65-63-0-44-67-17-12-11-122

20974 : plus petit décomposant 11
0-1(7)-4-2-8-5(5)-13-17-21-7-18-32-23-33-12-39-29-51-3(3)-29-23-39-58-59-22-67-65-2-46-69-19-14-13-124

# 6 Une nouvelle conjecture liée à la conjecture de Goldbach

Dans la mesure où un nombre premier $p$ décomposant de Goldbach d'un nombre pair $2a$ est non congru à $2a$ selon tout module, j'ai pensé qu'un tel nombre premier devait assez souvent être également un décomposant d'un pair à distance $6k$ de $2a$, puisque $2a$ et $2a + 6k$ partagent leur coordonnée selon les modules 2 et 3 simultanément.

On peut tester informatiquement cette conjecture selon laquelle tout nombre pair $2a$ supérieur à 14 et inférieur à $3.10^6$ partage au moins l'un de ses décomposants de Goldbach avec $2a - 6$. Dominique Ceugniet [3] confirme cette nouvelle conjecture jusqu'à $16.10^8$. Il a également fait quelques statistiques : pour les nombres pairs compris entre $15.10^8$ (inclus) et $16.10^8$ (exclu), le nombre maximum d'essais à effectuer avant de trouver deux décompositions qui partagent un nombre premier est 8979, tandis que la moyenne du nombre d'essais à effectuer dans cette zone de nombres est 290.

L'exemple d'un décomposant partagé trouvé après 8979 essais est :
1 508 792 552 = 17 959 + 1 508 774 593

[3] Un internaute compatissant, polytechnicien, et féru d'optimisation informatique.

1 508 792 546 = 17 959 + 1 508 774 587

Cette conjecture nous fait nous demander si une démonstration par récurrence (la "démonstration par excellence" selon Poincaré) ne pourrait pas être envisagée pour prouver la conjecture de Goldbach (chaque nombre pair, selon qu'il serait congru à 0, 2 ou 4 (modulo 6) "hériterait" d'un décomposant de Goldbach d'un nombre pair plus petit que lui, de proche en proche).

## Bibliographie

(1) C.F. Gauss, *Recherches arithmétiques*, Ed. Jacques Gabay, 1801.
(2) P.J. Davis, R.Hersh, *l'Univers mathématique*, Ed. Gauthier-Villars, 1985
(3) D. Nordon, M.Mendès-France (illustrations), *Les mathématiques pures n'existent pas !*, Ed. Actes Sud, 1985.
(4) D. Nordon, *Les obstinations d'un mathématicien*, Ed. Belin Pour La Science, 2003.
(5) A. Doxiadis, *Oncle Pétros et la conjecture de Goldbach*, Ed. Points, 2002.
(6) L. Euler, *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs*, Commentatio 175 indicis Enestroemiani, Bibliothèque impartiale 3, 1751, p.10-31.
(7) J. Hadamard, *Essai sur la psychologie de l'invention dans le domaine mathématique*, suivi de H. Poincaré, *L'invention mathématique*, Ed. Jacques Gabay, 2000.
(8) C. Laisant, *Sur un procédé expérimental de vérification de la conjecture de Goldbach*, Bulletin de la SMF n°25 de 1897.
(9) M. Hindry, *Arithmétique*, Ed. Calvage et Mounet, 2008.

Je voudrais expliquer ici ce que j'entends par chercher le $b$ minimum des $ax+b$ et montrer qu'il est toujours inférieur à la moitié du pair dont on cherche une décomposition de Goldbach.

Je suis désolée d'être contrainte de toujours passer par l'étude d'un exemple pour m'expliquer mais je crois que tout ça est généralisable (enfin, si ce n'est qu'on a pas grand chose comme formule, en matière de nombres premiers).
J'utilise intensivement le théorème des restes chinois pour la recherche des solutions.

On cherche les décomposants de Goldbach de nombres qui sont congrus à 0 (mod 2), 2 (3), 3 (5) et 3 (7) (*je n'ai pas réécrit mod à chaque fois dans les parenthèses*).
Voilà comment on applique le chinois : on calcule les différentes fractions de 210 (=2x3x5x7) par 2, puis par 3, puis par 5, puis par 7.
On obtient les nombres 105, 70, 42 et 30. On cherche quels sont les multiples de ces nombres qui soient congrus à 1, d'abord mod 2, puis mod 3, puis mod 5, puis mod 7.
105 est directement congru à 1 mod 2.
70 est directement congru à 1 mod 3.
42 n'est pas directement congru à 1 mod 5, c'est son multiple 126 qui l'est.
30 n'est pas directement congru à 1 mod 7, c'est son multiple 120 qui l'est.

On fait le produit scalaire de ce vecteur de quatre entiers (105 70 42 30) par le vecteur des 4 restes modulaires sur lesquels on s'est fixé (0 2 3 3). On obtient 878, qui est en fait un représentant de tous les entiers de la forme 210k+38 (*à la fin de cette note, je fournirai les décomposants de Goldbach des plus petits nombres de cette forme, soit des nombres 248, 458, 668, 878, 1088, 1298, 1508, 1718, 1928 et 2138*).

On cherche donc des décomposants de Goldbach de nombres de la forme 210k+38.

Les décomposants de Goldbach possibles sont congrus à 1 (mod 2), à 1 (mod 3), à 1, 2 ou 4 (mod 5) et à 1,2,4,5 ou 6 (mod 7).

Premier cas : 1 (2) 1 (3) 1 (5) 1 (7)
combinaison linéaire correspondante :
1x105+1x70+1x126+1x120 = 421 (210) = 1 (210)
Les nombres solutions sont 1, 211, 421,...

Deuxième cas : 1 (2) 1 (3) 1 (5) 2 (7)
combinaison linéaire correspondante :
1x105+1x70+1x126+2x120 = 541 (210) = 121 (210)
Plus petite solution : 121

Troisième cas : 1 (2) 1 (3) 1 (5) 4 (7)
combinaison linéaire correspondante :
1x105+1x70+1x126+4x120 = 781 (210) = 151 (210)

Quatrième cas : 1 (2) 1 (3) 1 (5) 5 (7)
combinaison linéaire correspondante :
1x105+1x70+1x126+5x120 = 901 (210) = 61 (210)

Cinquième cas : 1 (2) 1 (3) 1 (5) 6 (7)
combinaison linéaire correspondante :
1x105+1x70+1x126+6x120 = 1021 (210) = 181 (210)

Sixième cas : 1 (2) 1 (3) 2 (5) 1 (7)
combinaison linéaire correspondante :
1x105+1x70+2x126+1x120 = 547 (210) = 127 (210)

Septième cas : 1 (2) 1 (3) 2 (5) 2 (7)
combinaison linéaire correspondante :
1x105+1x70+2x126+2x120 = 667 (210) = 37 (210)

Huitième cas : 1 (2) 1 (3) 2 (5) 4 (7)
combinaison linéaire correspondante :
1x105+1x70+2x126+4x120 = 907 (210) = 67 (210)

Neuvième cas : 1 (2) 1 (3) 2 (5) 5 (7)
combinaison linéaire correspondante :
1x105+1x70+2x126+5x120 = 1027 (210) = 187 (210)

Dixième cas : 1 (2) 1 (3) 2 (5) 6 (7)
combinaison linéaire correspondante :
1x105+1x70+2x126+6x120 = 1147 (210) = 97 (210)

Onzième cas : 1 (2) 1 (3) 4 (5) 1 (7)
combinaison linéaire correspondante :
1x105+1x70+1x126+1x120 = 799 (210) = 169 (210)

Douzième cas : 1 (2) 1 (3) 4 (5) 2 (7)
combinaison linéaire correspondante :
1x105+1x70+1x126+1x120 = 919 (210) = 79 (210)

Treizième cas : 1 (2) 1 (3) 4 (5) 4 (7)
combinaison linéaire correspondante :
1x105+1x70+1x126+1x120 = 1159 (210) = 109 (210)

Quatorzième cas : 1 (2) 1 (3) 4 (5) 5 (7)
combinaison linéaire correspondante :
1x105+1x70+1x126+1x120 = 1279 (210) = 19 (210)

Quinzième cas : 1 (2) 1 (3) 4 (5) 6 (7)
combinaison linéaire correspondante :
1x105+1x70+1x126+1x120 = 1399 (210) = 139 (210)

Si on remet les solutions minimales dans l'ordre croissant (ce que j'avais appelé les $b$ du $ax + b$ avec ici $a$ qui vaut tout le temps 210), on obtient la suite

de nombres suivante (on laisse de côté 1) :
19, 37, 61, 67, 79, 97, 109, 121, 127, 139, 161, 169, 181, 187, puis (en recommençant à partir de 210), 229, 247, 271, etc.
Si on calcule les écarts entre ces nombres successifs, on obtient 18, 18, 24, 6, 12, 18, 12, 12, 6, 12, 12, 18, 12, 6. On constate (et on conjecture du même coup, mais c'est peut-être trivialement démontrable parce que tous les nombres qu'on a choisi était tous congru à 1 (mod 2) et à 1 (mod 3)), on constate donc que tous ces écarts sont divisibles par 6.
Dans cette suite de nombres, les seuls dont on soit sûr qu'ils sont premiers sont les nombres inférieurs à 120 ($= 11^2 - 1$), en l'occurrence les nombres 19, 37, 61, 67, 79, 97 et 109 (remarque : d'ailleurs, le premier nombre ensuite 121 est composé, 121 est le carré de 11).

A cause du "rouleau" autour de 210, et des combinaisons linéaires qui font intervenir des multiples de produits de nombres premiers qui soient congrus à 1 modulo les nombres premiers considérés, je n'arrive pas à raisonner comme il faut, et donc à prouver que le plus petit des nombres premiers trouvés est forcément ( !) inférieur à la moitié du nombre pair que l'on cherche à décomposer.

J'espère que mon explication aura été suffisamment claire...

Voici les décomposants de Goldbach des 210k+38 ; en font systématiquement partie des nombres de la suite bizarre qu'on a identifiée par le chinois.

$248 = 7 + 241 = 19 + 229 = 37 + 211 = 67 + 181 = 97 + 151 = 109 + 139$

$458 = 19 + 439 = 37 + 421 = 61 + 397 = 79 + 379 = 109 + 349 = 127 + 331 = 151 + 307 = 181 + 277 = 229 + 229$

$668 = 7 + 661 = 37 + 631 = 61 + 607 = 67 + 601 = 97 + 571 = 127 + 541 = 181 + 487 = 211 + 457 = 229 + 439 = 271 + 397 = 331 + 337$

$878 = 19 + 859 = 67 + 811 = 109 + 769 = 127 + 751 = 139 + 739 = 151 + 727 = 271 + 607 = 277 + 601 = 307 + 571 = 331 + 547 = 337 + 541 = 379 + 499 = 421 + 457 = 439 + 439$

$1088 = 19 + 1069 = 37 + 1051 = 67 + 1021 = 79 + 1009 = 97 + 991 = 151 + 937 = 181 + 907 = 211 + 877 = 229 + 859 = 277 + 811 = 331 + 757 = 337 + 751 = 349 + 739 = 379 + 709 = 397 + 691 = 457 + 631 = 487 + 601 = 541 + 547$

$1298 = 7 + 1291 = 19 + 1279 = 61 + 1237 = 67 + 1231 = 97 + 1201 = 127 + 1171 = 181 + 1117 = 211 + 1087 = 229 + 1069 = 277 + 1021 = 307 + 991 = 331 + 967 = 379 + 919 = 421 + 877 = 439 + 859 = 487 + 811 = 541 + 757 = 547 + 751 = 571 + 727 = 607 + 691$

$1508 = 19 + 1489 = 37 + 1471 = 61 + 1447 = 79 + 1429 = 109 + 1399 = 127 + 1381 = 181 + 1327 = 211 + 1297 = 229 + 1279 = 271 + 1237 = 277 + 1231 = 307 + 1201 = 337 + 1171 = 379 + 1129 = 421 + 1087 = 439 + 1069 = 457 + 1051 = 487 + 1021 = 499 + 1009 = 541 + 967 = 571 + 937 = 601 + 907 = 631 + 877 = 739 + 769 = 751 + 757$

$1718 = 19 + 1699 = 61 + 1657 = 97 + 1621 = 109 + 1609 = 139 + 1579 = 151 + 1567 = 229 + 1489 = 271 + 1447 = 337 + 1381 = 397 + 1321 = 421 + 1297 = 439 + 1279 = 487 + 1231 = 547 + 1171 = 601 + 1117 = 631 + 1087 = 709 + 1009 = 727 + 991 = 751 + 967 = 811 + 907 = 859 + 859$

$1928 = 61 + 1867 = 67 + 1861 = 97 + 1831 = 127 + 1801 = 139 + 1789 = 151 + 1777 = 181 + 1747 = 229 + 1699 = 271 + 1657 = 307 + 1621 = 331 + 1597 = 349 + 1579 = 379 + 1549 = 397 + 1531 = 439 + 1489 = 457 + 1471 = 499 + 1429 = 547 + 1381 = 601 + 1327 = 607 + 1321 = 631 + 1297 = 691 + 1237 = 727 + 1201 = 757 + 1171 = 811 + 1117 = 859 + 1069 = 877 + 1051 = 907 + 1021 = 919 + 1009 = 937 + 991$

$2138 = 7 + 2131 = 109 + 2029 = 127 + 2011 = 139 + 1999 = 151 + 1987 = 271 + 1867 = 277 + 1861 = 307 + 1831 = 337 + 1801 = 349 + 1789 = 379 + 1759 = 397 + 1741 = 439 + 1699 = 541 + 1597 = 571 + 1567 = 607 + 1531 = 691 + 1447 = 709 + 1429 = 739 + 1399 = 757 + 1381 = 811 + 1327 = 859 + 1279 = 907 + 1231 = 937 + 1201 = 967 + 1171 = 1009+ 1129 = 1021+ 1117 = 1051+ 1087 = 1069+ 1069$