Conjecture de Goldbach et nullité du déterminant d'une matrice de Sylvester, janvier 2012.

février et mars 2012.

retour au maillage, mars 2012.

incongruences, mars 2012.

Lier décomposants de Goldbach et non-résidus quadratiques.

Ritz-Rydberg, avril 2012.

incongruences, avril 2012.

extraits littéraires.

Infinitude de l'ensemble des nombres premiers jumeaux, mai 2012.

Etude élémentaire de la Conjecture de Goldbach, mai 2012.

nuage rose.

Infinitude de l'ensemble des nombres premiers de la forme $6n + 1$, puis de l'ensemble des nombres premiers jumeaux qui en découle presque, juin 2012.

Conjecture des nombres premiers jumeaux, juin 2012.

Étude de deux conjectures concernant les nombres premiers, juin 2012.

Générer des couples de nombres premiers jumeaux, juin 2012.

Infinité de l'ensemble des nombres premiers jumeaux.

Une tentative de minoration probabiliste.

Découverte d'une loi tout extraordinaire par rapport à certaines sommes de restes des nombres premiers, juillet 2012.

Méthode constructive pour trouver les décomposants de Goldbach d'un nombre pair ou les couples de nombres premiers jumeaux, septembre 2012.

Conjecture de Goldbach et nullité du déterminant d'une matrice de Sylvester

Denise Vella-Chemla

1/1/2012

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers. Trouver les décomposants de Goldbach d'un nombre pair n équivaut à trouver les racines communes de deux polynômes : le premier polynôme a pour seules racines les nombres premiers impairs inférieurs ou égaux à n ; le second polynôme a pour seules racines leur complémentaire à n. Par exemple, trouver les décomposants de Goldbach de 6 consiste à trouver les racines communes des polynômes $x^2 - 8x + 15 = (x-3)(x-5)$, et $x^2 - 4x + 3 = (x-1)(x-3)$.

Les coefficients et les racines des deux polynômes vérifient les équations de Viète : dans le cas général d'un polynôme unitaire $x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_2x^2 + a_1x + a_o$:

$x_1 + x_2 + ... + x_n = -a_{n-1}$
$x_1x_2 + x_1x_3 + ... + x_{n-1}x_n = a_{n-2}$ (*somme de tous les produits* 2 à 2)
$x_1x_2x_3 + x_1x_2x_4 + ... + x_{n-2}x_{n-1}x_n = -a_{n-3}$ (*somme de tous les produits* 3 à 3)
...
$x_1x_2...x_k + x_1x_2...x_{k+1} + ... + x_{n-k}x_{n-k+1}...x_n = (-1)^k a_{n-k}$ (*somme de tous les produits k à k*)
...
$x_1x_2...x_n = (-1)^n a_o$.

Les coefficients du deuxième polynôme sont les coefficients du développement de Taylor du premier polynôme. Dans le cas du nombre pair $n = 6$, les coefficients du premier polynôme sont :

$$\begin{aligned} a_1 &= 1 \\ a_2 &= -8 \\ a_3 &= 15 \end{aligned}$$

Les coefficients du deuxième polynôme sont :

$$\begin{array}{lllll} b_1 = & & & & +a_1, \\ b_2 = & & -2a_1n & & -a_2, \\ b_3 = & a_1n^2 & +a_2n & & +a_3. \end{array}$$

Deux polynômes ont des racines communes si leur résultant (le déterminant de leur matrice de Sylvester) est nul.

On rappelle que la matrice de Sylvester de $P(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n$ et $Q(x) = b_0x^n + b_1x^{n-1} + b_2x^{n-2} + \ldots + b_{n-1}x + b_n$ est :

$$\begin{pmatrix} a_0 & 0 & \ldots & 0 & b_0 & 0 & \ldots & 0 \\ a_1 & a_0 & \ddots & 0 & b_1 & b_0 & \ddots & 0 \\ \vdots & a_1 & \ddots & \vdots & \vdots & b_1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & b_0 \\ a_n & \vdots & \ddots & a_1 & b_n & \vdots & \ddots & b_1 \\ 0 & a_n & \vdots & \vdots & 0 & b_n & \vdots & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & a_n & 0 & \ldots & 0 & b_n \end{pmatrix}$$

Dans le cas où $n = 6$, exprimons le résultant uniquement en fonction des coefficients du premier polynôme. C'est le déterminant de la matrice suivante :

$$\begin{pmatrix} a_1 & 0 & b_1 & 0 \\ a_2 & a_1 & b_2 & b_1 \\ a_3 & a_2 & b_3 & b_2 \\ 0 & a_3 & 0 & b_3 \end{pmatrix} = \begin{pmatrix} a_1 & 0 & a_1 & 0 \\ a_2 & a_1 & -2a_1n - a_2 & a_1 \\ a_3 & a_2 & a_1n^2 + a_2n + a_3 & -2a_1n - a_2 \\ 0 & a_3 & 0 & a_1n^2 + a_2n + a_3 \end{pmatrix}$$

Le résultant des deux polynômes dans le cas où $n = 6$ est égal à :

$$a_1^4n^4 + 4a_1^3a_2n^3 + 4a_1^3a_3n^2 + 5a_1^2a_2^2n^2 + 8a_1^2a_2a_3n + 2a_1a_2^3n + 4a_1a_2^2a_3$$

Il se factorise en $(n-6)(n-8)^2(n-10)$ et s'annule donc bien pour 6.

Passons au cas des nombres pairs 8 et 10, compris entre les nombres premiers 7 et 11. Les 3 nombres premiers impairs que sont $3, 5$ *et* 7 fournissent les valeurs suivantes des coefficients des deux polynômes :

$$\begin{array}{lllll} a_1 = & & & & 1 \\ a_2 = & & & & -15 \\ a_3 = & & & & 71 \\ a_4 = & & & & -105 \\ b_4 = & -a_1n^3 & -a_2n^2 & -a_3n & -a_4 \\ b_3 = & & 3a_1n^2 & +2a_2n & +a_3 \\ b_2 = & & & -3a_1n & -a_2 \\ b_1 = & & & & +a_1 \end{array}$$

Dans les cas où $n = 8$ *ou* 10, exprimons le résultant uniquement en fonction des coefficients du premier polynôme. C'est le déterminant de la matrice $\begin{pmatrix} a_1 & 0 & 0 & b_1 & 0 & 0 \\ a_2 & a_1 & 0 & b_2 & b_1 & 0 \\ a_3 & a_2 & a_1 & b_3 & b_2 & b_1 \\ a_4 & a_3 & a_2 & b_4 & b_3 & b_2 \\ 0 & a_4 & a_3 & 0 & b_4 & b_3 \\ 0 & 0 & a_4 & 0 & 0 & b_4 \end{pmatrix}$ qui vaut :

$$\begin{pmatrix} a_1 & 0 & 0 & a_1 & 0 & 0 \\ a_2 & a_1 & 0 & -3a_1n - a_2 & a_1 & 0 \\ a_3 & a_2 & a_1 & 3a_1n^2 + 2a_2n + a_3 & -3a_1n - a_2 & a_1 \\ a_4 & a_3 & a_2 & -a_1n^3 - a_2n^2 - a_3n - a_4 & 3a_1n^2 + 2a_2n + a_3 & -3a_1n - a_2 \\ 0 & a_4 & a_3 & 0 & -a_1n^3 - a_2n^2 - a_3n - a_4 & 3a_1n^2 + 2a_2n + a_3 \\ 0 & 0 & a_4 & 0 & 0 & -a_1n^3 - a_2n^2 - a_3n - a_4 \end{pmatrix}$$

Le résultant des deux polynômes en fonction de n vaut :

$$-n^9+90n^8-3576n^7+82320n^6-1209744n^5+11767200n^4-75743744n^3+311032320n^2-739123200n+774144000$$

et se factorise en :

$$-(n-6)(n-8)^2(n-10)^3(n-12)^2(n-14)$$

Le résultant s'annule bien en 8 et 10.
Les racines multiples sont dûes au fait qu'en combinant de toutes les manières possibles les nombres premiers $3, 5$ *et* 7, on obtient les sommes suivantes : $3+3 = 6, 3+5 = 8, 3+7 = 10, 5+3 = 8, 5+5 = 10, 5+7 = 12, 7+3 = 10, 7+5 = 12, 7+7 = 14$. On a bien deux manières différentes d'obtenir 8, trois d'obtenir 10, 2 d'obtenir 12 et une manière d'obtenir les deux extrema 6 et 14. Le résultant contient donc en substance toute l'information concernant des décompositions de Goldbach de nombres pairs (pas tous, cela sera vu dans le cas suivant) compris entre deux nombres premiers successifs.

Passons au nombre pair 12. Les nombres premiers impairs sont $3, 5, 7$ *et* 11 fournissent les valeurs suivantes des coefficients des deux polynômes :

$$\begin{array}{rrrrrr}
a_1 = & & & & & 1 \\
a_2 = & & & & & -26 \\
a_3 = & & & & & 236 \\
a_4 = & & & & & -886 \\
a_5 = & & & & & 1155 \\
b_5 = & a_1 n^4 & +a_2 n^3 & +a_3 n^2 & +a_4 n & +a_5 \\
b_4 = & & -4a_1 n^3 & -3a_2 n^2 & -2a_3 n & -a_4 \\
b_3 = & & & 6a_1 n^2 & +3a_2 n & +a_3 \\
b_2 = & & & & -4a_1 n & -a_2 \\
b_1 = & & & & & a_1
\end{array}$$

Le résultant des deux polynômes vaut :

$$\begin{aligned}
&n^{16} - 208 * n^{15} + 20140 * n^{14} - 1204960 * n^{13} + 49855072 * n^{12} - 1512487936 * n^{11} + 34800798080 * n^{10} \\
&-619431879680 * n^9 + 8618909904128 * n^8 - 94050771759104 * n^7 + 802095988997120 * n^6 \\
&-5289268303093760 * n^5 + 26434722173927424 * n^4 - 96780810002890752 * n^3 \\
&+244741340434268160 * n^2 - 381863291623833600 * n + 276876106924032000
\end{aligned}$$

Il se factorise en $(n-6)(n-8)^2(n-10)^3(n-12)^2(n-14)^3(n-16)^2(n-18)^2(n-22)$ et s'annule bien en 12.
Par contre, ce résultant ne s'annule pas en 20 : en combinant les seuls nombres premiers $3, 5, 7$ et 11, on ne peut obtenir 20 dont les décompositions de Goldbach sont $3+17$ et $7+13$.

Pour $n = 14$, écrivons seulement les coefficients de la deuxième équation en fonction de ceux de la première.

$$\begin{array}{rrrrrrr}
b_6 = & -a_1 n^5 & -a_2 n^4 & -a_3 n^3 & -a_4 n^2 & -a_5 n & -a_6 \\
b_5 = & & 5a_1 n^4 & +4a_2 n^3 & +3a_3 n^2 & +2a_4 n & +a_5 \\
b_4 = & & & -10a_1 n^3 & -6a_2 n^2 & -3a_3 n & -a_4 \\
b_3 = & & & & +10a_1 n^2 & +4a_2 n & +a_3 \\
b_2 = & & & & & -5a_1 n & -a_2 \\
b_1 = & & & & & & +a_1
\end{array}$$

Cela nous permet de voir apparaître en diagonale les coefficients du binôme de Newton.

En résumé, un même résultant fonction de n dont on doit démontrer la nullité intervient pour tous les nombres pairs compris entre deux nombres premiers successifs.

On constate que dans les factorisations des polynômes trouvées,

$$\begin{aligned}
&(n-6)(n-8)^2(n-10) \\
&-(n-6)(n-8)^2(n-10)^3(n-12)^2(n-14) \\
&(n-6)(n-8)^2(n-10)^3(n-12)^2(n-14)^3(n-16)^2(n-18)^2(n-22)
\end{aligned}$$

du fait de la commutativité de l'addition, les facteurs de la forme $(n-2p)$ avec p premier apparaissent à une puissance impaire tandis que les facteurs de la forme $(n-2c)$ avec c composé apparaissent à une puissance paire. On passe d'un résultant au résultant "suivant" en multipliant la factorisation par $2n+1$ facteurs supplémentaires, le $+1$ correspondant à l'ajout du facteur $(n-2p)$, p étant le dernier nombre premier ajouté à la liste. Si l'on cherche une sorte d"'invariant de boucle"* lors du passage d'un nombre pair au suivant, il faudrait montrer que le nombre de racines du polynôme résultant inférieures à un certain nombre k est toujours supérieur au nombre de nombres pairs plus petits que k "à couvrir", ou dit autrement que lorsqu'on ajoute un nouveau nombre premier, on ne peut pas engendrer de "trou" dans la liste ordonnée des nombres pairs (un nombre pair sans décomposition de Goldbach)†.

*notion intervenant dans les preuves de programmes de Hoare.

†On pourrait même envisager de simplement démontrer que le passage d'un résultant au résultant suivant permet d'obtenir seulement la décomposition de Goldbach d'un nombre pair de plus et alors la conjecture serait démontrée.

La recherche de décomposants de Goldbach par résolution d'équations algébriques est surprenante car elle nous fait réaliser qu'une éventuelle démonstration par récurrence pourrait "aller très lentement" : il "suffirait" de démontrer qu'avec k nombres premiers différents, on arrive à fabriquer *le* nombre $2k+2$.

Avec k nombres différents, je peux fabriquer au minimum $2k-1$ sommes de deux nombres différentes.
Quand j'ajoute un nombre premier (p_{k+1}) à mon ensemble de nombres premiers, je suis sûre d'ajouter au minimum 2 nouvelles sommes à mon ensemble de sommes de deux nombres (qui sont p_k+p_{k+1} et $2p_{k+1}$ si on appelle p_k le plus grand des nombres premiers de l'ensemble initial, avant qu'on y ait ajouté le nombre premier p_{k+1}).

Avec 3 et 5, j'arrive à fabriquer 6 par addition.
($a=2$, $2a-1=3$, $3+3, 3+5, 5+5$)
Avec 3, 5 et 7, j'arrive à fabriquer 8 par addition.
($a=3$, $2a-1=5$, $3+3, 3+5, 5+5, 5+7, 7+7$)
Avec 3, 5, 7 et 11, j'arrive à fabriquer 10 par addition.
($a=4$, $2a-1=7$, $3+3, 3+5, 5+5, 5+7, 7+7, 7+11, 11+11$)
Avec 3, 5, 7, 11 et 13, j'arrive à fabriquer 12 par addition.
($a=5$, $2a-1=9$, $3+3, 3+5, 5+5, 5+7, 7+7, 7+11, 11+11, 11+13, 13+13$)
Avec 3, 5, 7, 11, 13 et 17, j'arrive à fabriquer 14 par addition.
($a=6$, $2a-1=11$, $3+3, 3+5, 5+5, 5+7, 7+7, 7+11, 11+11, 11+13, 13+13, 13+17, 17+17$)

Il faut démontrer par récurrence qu'avec k nombres premiers, j'arrive toujours à fabriquer les nombres pairs de 6 jusqu'à $2k+2$.

1) *initialisation de la récurrence* : avec les 2 premiers nombres premiers impairs que sont 3 et 5, j'arrive à fabriquer le nombre pair 6.

2) *récurrence proprement dite* : si j'arrive à fabriquer tous les nombres pairs jusqu'à $2k+2$ avec k nombres premiers et que j'ajoute un $k+1^{ème}$ nombre premier à ma liste, j'arriverai avec mon nouvel ensemble de nombres premiers à fabriquer en plus le nombre pair $2k+4$.

Trois cas sont alors à distinguer :
a) j'arrivais déjà à fabriquer $2k+4$ avant même d'ajouter le nouveau nombre premier ; ok.
b) je n'arrivais pas à fabriquer $2k+4$ avant l'ajout du nouveau nombre premier ; je rajoute deux nouvelles décompositions à mon ensemble : $2p_{k+1}$ et p_k+p_{k+1}.
Alors deux sous-cas :
b1) Si $2k+4$ est un double de nombre premier, il vérifie trivialement la conjecture ; ok.
b2) Il faut que je montre que $2k+4$ est bien décomposable en la somme p_k+p_{k+1}.
Mais si $2k+4$ est le plus petit nombre pair qui ne soit pas un double de premier alors il est le nombre pair qui suit $2p_k$, il est donc égal à $2p_k+2$ et est donc égal à $p_k+(p_k+2)$ qui est bien une décomposition de Goldbach puisque p_k+2 est alors forcément égal à p_{k+1} qui est un nombre premier.
Dans les trois cas, la récurrence a avancé d'un pas mais je me trompe parce que je considère que l'on n'ajoute que deux nouvelles décompositions à chaque étape, alors qu'on peut en ajouter bien plus, et qu'il y a donc plein d'autres cas à traiter.

($D.\ Vella-Chemla,\ 24/2/2012$)

La recherche de décomposants de Goldbach par résolution d'équations algébriques est surprenante car elle nous fait réaliser qu'une éventuelle démonstration par récurrence pourrait "aller très lentement" : il "suffirait" de démontrer qu'avec a nombres premiers différents, on arrive à fabriquer *le* nombre $2a+2$.

Avec a nombres premiers différents ordonnés strictement, je peux fabriquer $2a-1$ nombres pairs différents par addition. Quand j'ajoute un nombre premier (p_{der}) à mon ensemble de nombres premiers, je suis sûre d'ajouter 2 nouvelles sommes à mon ensemble de sommes (qui sont $p_{avantder}+p_{der}$ et $2p_{der}$ si on appelle $p_{avantder}$ le plus grand des nombres premiers de l'ensemble initial, avant qu'on y ait ajouté le nombre premier p_{der}).

Avec 3 et 5, j'arrive à fabriquer 6 par addition.
$(a=2,\ 2a-1=3,\ 3+3, 3+5, 5+5)$
Avec 3, 5 et 7, j'arrive à fabriquer 8 par addition.
$(a=3,\ 2a-1=5,\ 3+3, 3+5, 5+5, 5+7, 7+7)$
Avec 3, 5, 7 et 11, j'arrive à fabriquer 10 par addition.
$(a=4,\ 2a-1=7,\ 3+3, 3+5, 5+5, 5+7, 7+7, 7+11, 11+11)$
Avec 3, 5, 7, 11 et 13, j'arrive à fabriquer 12 par addition.
$(a=5,\ 2a-1=9,\ 3+3, 3+5, 5+5, 5+7, 7+7, 7+11, 11+11, 11+13, 13+13)$
Avec 3, 5, 7, 11, 13 et 17, j'arrive à fabriquer 14 par addition.
$(a=6,\ 2a-1=11,\ 3+3, 3+5, 5+5, 5+7, 7+7, 7+11, 11+11, 11+13, 13+13, 13+17, 17+17)$

Il faut démontrer par récurrence qu'avec a nombres premiers, j'arrive toujours à fabriquer les nombres pairs de 6 jusqu'à $2a+2$.

1) *initialisation de la récurrence* : avec les 2 premiers nombres premiers impairs que sont 3 et 5, j'arrive à fabriquer le nombre pair 6.

2) *récurrence proprement dite* : si j'arrive à fabriquer tous les nombres pairs jusqu'à $2a+2$ avec a nombres premiers et que j'ajoute un $a+1^{ème}$ nombre premier à ma liste, j'arriverai avec mon nouvel ensemble de nombres premiers à fabriquer en plus le nombre pair $2a+4$.

Trois cas sont alors à distinguer :
a) j'arrivais déjà à fabriquer $2a+4$ avant même d'ajouter le nouveau nombre premier ; ok.
b) je n'arrivais pas à fabriquer $2a+4$ avant l'ajout du nouveau nombre premier ; je rajoute deux nouvelles décompositions à mon ensemble : $2p_{der}$ et $p_{avantder}+p_{der}$.
Alors deux sous-cas :
b1) Si le nombre pair ajouté est un double de nombre premier (en l'occurrence le double de p_{der}), il vérifie trivialement la conjecture ; ok.
b2) Il faut que je montre que $2a+4$ est bien décomposable en la somme $p_{avantder}+p_{der}$.
Mais si $2a+4$ est le plus petit nombre pair qui ne soit pas un double de premier alors il est le nombre pair qui suit $2p_{avantder}$, il est donc égal à $2p_{avantder}+2$ et est donc égal à $p_{avantder}+(p_{avantder}+2)$ qui est bien une décomposition de Goldbach puisque $p_{avantder}+2$ est alors forcément égal à p_{der} qui est un nombre premier.
Dans les trois cas, la récurrence a avancé d'un pas.

$(D.\ Vella-Chemla,\ 24/2/2012)$

On note $\mathbb{P}_{i\in\mathbb{N}}$, la suite croissante des nombres premiers impairs.
On cherche à démontrer par récurrence la propriété $g(k)\ :\ \exists\, p_i,\ p_j \in \mathbb{P}_k,\ 2k+2 = p_i + p_j$.

Illustration :
Avec les deux plus petits nombres premiers impairs que sont 3 *et* 5*, j'arrive à obtenir* 6 *par addition de deux nombres (*$6 = 3 + 3$*).*
Avec 3, 5 *et* 7*, j'arrive à obtenir* 8 *par addition de deux nombres.*
Avec 3, 5, 7 *et* 11*, j'arrive à obtenir* 10 *par addition de deux nombres.*
Avec 3, 5, 7, 11 *et* 13*, j'arrive à obtenir* 12 *par addition de deux nombres.*
Avec 3, 5, 7, 11, 13 *et* 17*, j'arrive à obtenir* 14 *par addition de deux nombres.*

1) : $g(2)$.

2) : $g(k) \implies g(k+1)$.

a) : si $\exists\, p_i,\ p_j \in \mathbb{P}_k,\ 2k+4 = p_i + p_j$ alors $g(k+1)$.
b) sinon :
b1) si $2k+4 = 2p_{k+1},\ g(k+1)$.
b2) sinon on doit montrer qu'$\exists\, p_i,\ i \leq k,\ 2k+4 = p_i + p_{k+1}$.
L'hypothèse de récurrence est que tous les nombres de 6 à $2k+2$ sont chacun décomposables en une somme de deux nombres premiers pris parmi les k premiers nombres premiers impairs, ce que l'on peut écrire par les $k-1$ égalités suivantes :

$$\begin{aligned} g(k):\quad & 6 = p_{6,1} + p_{6,2} \\ & 8 = p_{8,1} + p_{8,2} \\ & 10 = p_{10,1} + p_{10,2} \\ & \vdots \\ & 2k+2 = p_{2k+2,1} + p_{2k+2,2} \end{aligned}$$

On peut réécrire chacune de ces égalités pour obtenir des égalités portant sur le nombre pair $2k+4$ que l'on cherche à décomposer (égalités sur $2k+4$ avec en partie droite deux nombres premiers et un nombre pair) :

$$\begin{aligned} & 2k+4 = p_{6,1} + p_{6,2} + 2k - 2 \\ & 2k+4 = p_{8,1} + p_{8,2} + 2k - 4 \\ & 2k+4 = p_{10,1} + p_{10,2} + 2k - 6 \\ & \vdots \\ & 2k+4 = p_{2k+2,1} + p_{2k+2,2} + 2 \end{aligned}$$

On dispose d'autre part de k égalités liant p_{k+1} et chacun des p_i pour tout $i \leq k$ (égalités sur p_{k+1} avec en partie droite un nombre premier et un nombre pair) :

$$p_{k+1} = p_i + 2a_i$$

Alors deux cas :
- soit j'arrive à apparier une égalité sur p_{k+1} et une égalité sur $2k+4$ et cela me permet de trouver une décomposition de Goldbach de $2k+4$;
- soit il faut trouver pourquoi le système constitué des égalités portant sur $2k+4$ et des inégalités de la forme suivante $2k+4 \neq p_{k+1} + p_i, \forall i \leq k$ aboutit à une contradiction (en ajoutant p_{k+1} à l'ensemble des nombres premiers, les seules sommes de deux nombres premiers ajoutées à l'ensemble des sommes sont de la forme $p_{k+1} + p_i$).

$(D.\ Vella - Chemla,\ 4/3/2012)$

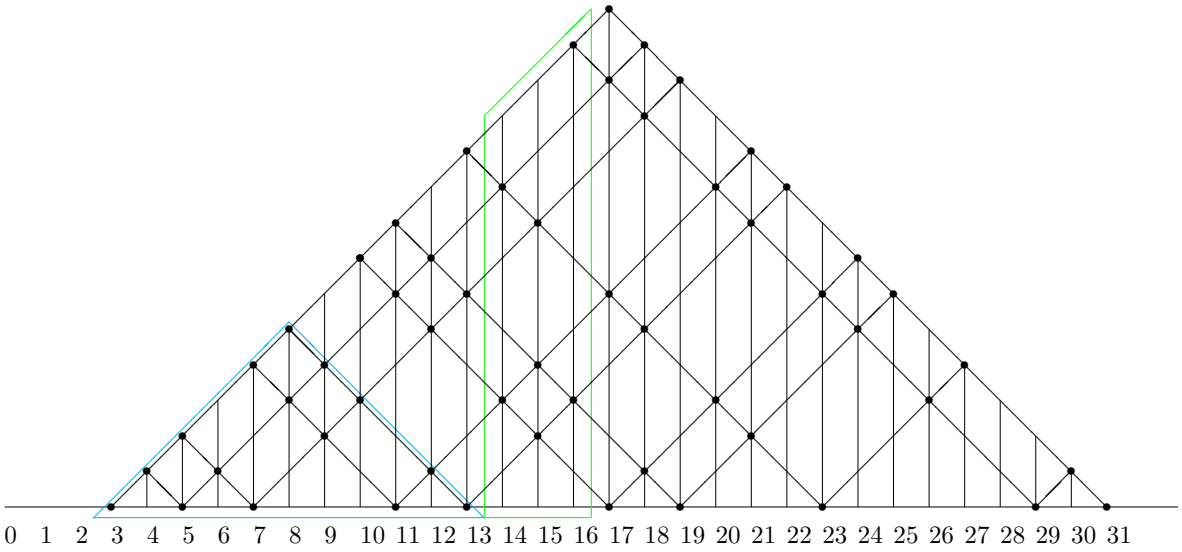
On note $\mathbb{P}_{i\in\mathbb{N}}$, la suite croissante des nombres premiers impairs. $p_1 = 3,\ p_2 = 5,\ p_3 = 7\ldots$
On cherche à démontrer par récurrence la propriété $g(k)\ :\ \forall\, x\ \leq\ p_k + 3,\ \exists\, p_i,\ p_j \in \mathbb{P}_k,\ x = p_i + p_j$.

1) $g(1)$ puisque $6 = 3 + 3$.

2) $g(k)\ \Longrightarrow\ g(k+1)$.

$$
\begin{aligned}
g(k):\quad & 6 = p_{6,1} + p_{6,2}\\
& 8 = p_{8,1} + p_{8,2}\\
& 10 = p_{10,1} + p_{10,2}\\
& \vdots\\
& p_k + 3 = p_{p_k+3,1} + p_{p_k+3,2}
\end{aligned}
$$

Il faut montrer que l'existence de décompositions de Goldbach pour les nombres pairs de 6 à p_k+3 entraîne l'existence de décompositions de Goldbach pour les nombres pairs de $p_k + 5$ à $p_{k+1} + 3$.
Dans le maillage de représentation des décompositions, on a entouré la partie du maillage représentant les décompositions de Goldbach des nombres de $p_k + 5$ à $p_{k+1} + 3$ pour $p_k = 23$.



$(D.\,Vella - Chemla,\ 7/3/2012)$


0 1 2 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 29 30

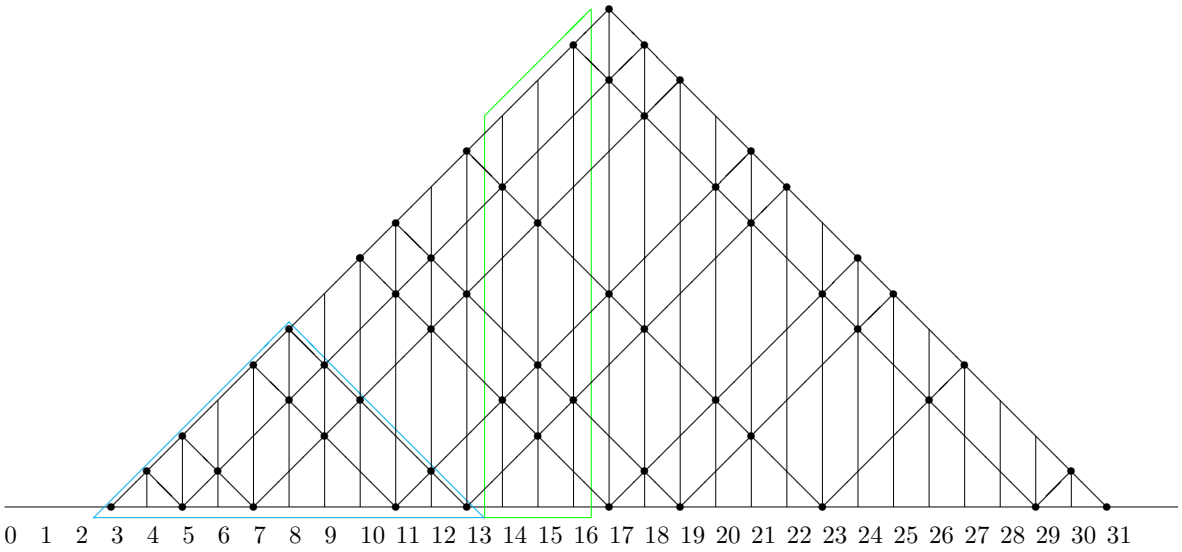
On note $\mathbb{P}_{i\in\mathbb{N}}$, la suite croissante des nombres premiers impairs. $p_1 = 3,\ p_2 = 5,\ p_3 = 7\ldots$
On cherche à démontrer par récurrence la propriété $g(k)\ :\ \forall\, x\ \leq\ p_k + 3,\ \exists\, p_i,\ p_j \in \mathbb{P}_k,\ x = p_i + p_j$.

1) $g(1)$ puisque $6 = 3 + 3$.

2) $g(k)\ \Longrightarrow\ g(k+1)$.

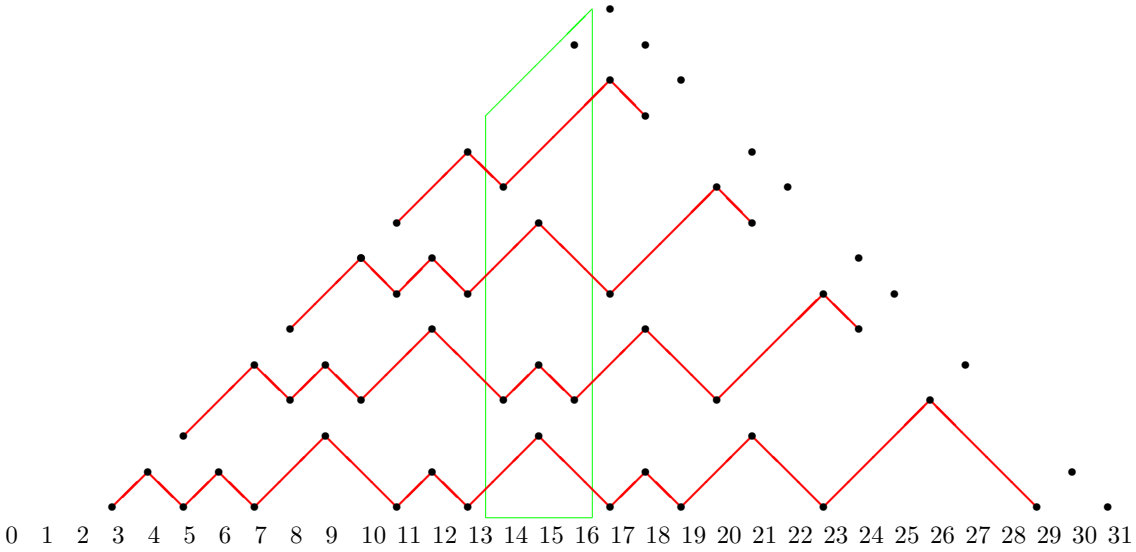
$$
\begin{aligned}
g(k):\quad & 6 = p_{6,1} + p_{6,2}\\
& 8 = p_{8,1} + p_{8,2}\\
& 10 = p_{10,1} + p_{10,2}\\
& \vdots\\
& p_k + 3 = p_{p_k+3,1} + p_{p_k+3,2}
\end{aligned}
$$

Il faut montrer que l'existence de décompositions de Goldbach pour les nombres pairs de 6 à p_k+3 entraîne l'existence de décompositions de Goldbach pour les nombres pairs de $p_k + 5$ à $p_{k+1} + 3$.
Dans le maillage de représentation des décompositions, on a entouré la partie du maillage représentant les décompositions de Goldbach des nombres de $p_k + 5$ à $p_{k+1} + 3$ pour $p_k = 23$.



$(D.\,Vella - Chemla,\ 7/3/2012)$

Peut-être que la notion de "mots de Dyck", illustrée en rouge dans le maillage ci-dessous, peut aider à compter le nombre de décompositions de Goldbach contenues par la zone délimitée en vert.



$(D.\,Vella - Chemla,\ 9/3/2012)$

La conjecture de Goldbach stipule que tout nombre pair supérieur ou égal à 6 est la somme de deux nombres premiers impairs.
On cherche à démontrer : $\forall\, n \geq 6,\ \exists\, p \leq n/2,\ \exists\, q \geq n/2,\ p\ et\ q\ premiers\ impairs,\ n = p+q,$

Cela équivaut à: $\forall\, n \geq 6,\ \exists\, p \leq n/2,\ p\ premier\ impair,\ \forall\, q \leq \sqrt{n},\ q\ premier\ impair,\ p \not\equiv n\ (mod\ q)$

Par exemple, 98 a pour plus petit décomposant de Goldbach 19 parce que 3, 5, 7, 11, 13 et 17, les plus petits nombres premiers impairs, sont tous congrus à 98 selon un module premier impair inférieur à $\sqrt{98}$ tandis que 19 n'est congru à 98 selon aucun d'entre eux.

$$98 \equiv 3\ (mod\ 5).$$
$$98 \equiv 5\ (mod\ 3).$$
$$98 \equiv 7\ (mod\ 7).$$
$$98 \equiv 11\ (mod\ 3).$$
$$98 \equiv 13\ (mod\ 5).$$
$$98 \equiv 17\ (mod\ 3).$$

$$98 \not\equiv 19\ (mod\ 3).$$
$$98 \not\equiv 19\ (mod\ 5).$$
$$98 \not\equiv 19\ (mod\ 7).$$

On choisit de démontrer plutôt :

$$(\exists\, n \geq 6,\ \forall\, p \leq n/2,\ \forall\, q \leq \sqrt{n},\ p\ et\ q\ premiers\ impairs,\ n \equiv p\ (mod\ q)) \implies false$$

Notons $p_1, p_2, \ldots, p_k$ les nombres premiers impairs inférieurs ou égaux à $n/2$ et $q_1, q_2, \ldots, q_k$, les nombres premiers impairs inférieurs ou égaux à $\sqrt{n}$. Les q_i sont les modules selon lesquels n est congru aux différents p_i.
Cherchons à établir d'où provient la contradiction. On a :

$$n \equiv p_1\ (mod\ q_1)$$
$$n \equiv p_2\ (mod\ q_2)$$
$$\ldots$$
$$n \equiv p_k\ (mod\ q_k)$$

Le problème consiste à "agréger" les différentes congruences concernant n : on ne peut pas par exemple déduire des différentes congruences sur n la congruence suivante :

$$n^k \equiv \prod_{p_1}^{p_k} p_i\ (mod\ \prod_{q_1}^{q_k} q_i)$$

Illustrons cette impossibilité sur un exemple :
$n \equiv 2\ (mod\ 3)$ a pour solutions entières $2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38, ...$
$n \equiv 3\ (mod\ 5)$ a pour solutions entières $3, 8, 13, 18, 23, 28, 33, 38, ...$
Mais les solutions du système constitué des 2 congruences sont $8, 23, 38, ...$, i.e. les solutions de la congruence $n \equiv 8\ (mod\ 15)$ qui ne s'obtient pas par une simple "multiplication terme à terme" des deux congruences initiales, mais par l'application complexe du théorème des restes chinois.

D'après le théorème des restes chinois, les q_i étant soit égaux soit premiers entre eux 2 à 2, le système de congruences

$$n \equiv p_1\ (mod\ q_1)$$
$$n \equiv p_2\ (mod\ q_2)$$
$$\ldots$$
$$n \equiv p_k\ (mod\ q_k)$$

admet une solution unique $n\ (mod\ M = \prod_{i=1}^{\lfloor\sqrt{n}\rfloor} q_i)$ qui est égale à

$$\Sigma_1^{n/2} p_i y_i M_i\ avec\ M_i = M/q_i\ (où\ M = PPCM(q_i))\ et\ y_i M_i \equiv 1\ (mod\ q_i).$$

On n'arrive toujours pas à établir pourquoi le système de congruences sur n implique une contradiction.

(Denise Chemla, 28/3/2012)

Lier décomposants de Goldbach et non-résidus quadratiques

Denise Vella-Chemla

16/4/2012

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.
Dans ses Recherches Arithmétiques, Gauss définit la notion de résidu quadratique modulo un entier de la façon suivante : a est résidu quadratique de b s'il existe c tel que $a \equiv c^2 \ (mod\ b)$.
Nous allons, pour les nombres pairs n inférieurs à 100, étudier le caractère de résiduosité quadratique à n de leurs décomposants de Goldbach, ainsi que celui de leur produit. Nous utiliserons la lettre R entre parenthèses pour signifier qu'un nombre est résidu quadratique du module n considéré et la lettre N pour signifier qu'il est non-résidu quadratique du module en question.

Module	*Produit*
8	$3\ (N) \times 5\ (N) = 15 = -1\ (N)$
12	$5\ (N) \times 7\ (N) = 35 = -1\ (N)$
16	$3\ (N) \times 13\ (N) = 7\ (N)$ $5\ (N) \times 11\ (N) = 7\ (N)$ *On réapplique aux produits* $7 \times 7 = 49 = 1\ (R)$
18	$5\ (N) \times 13\ (R) = 65 = 11\ (N)$ $7\ (R) \times 11\ (N) = 77 = 5\ (N)$ *On réapplique aux produits* $11 \times 5 = 55 = 1\ (R)$
20	$3\ (N) \times 17\ (N) = 51 = 11\ (N)$ $7\ (N) \times 13\ (N) = 91 = 11\ (N)$ *On réapplique aux produits* $11 \times 11 = 121 = 1\ (R)$
24	$5\ (N) \times 19\ (N) = 95 = -1\ (N)$ $7\ (N) \times 17\ (N) = 119 = -1\ (N)$ $11\ (N) \times 13\ (N) = 143 = -1\ (N)$
28	$5\ (N) \times 23\ (N) = 115 = 3\ (N)$ $11\ (N) \times 17\ (N) = 187 = 19\ (N)$ *On réapplique aux produits* $3 \times 19 = 57 = 1\ (R)$
30	$7\ (N) \times 23\ (N) = 151 = 1\ (R)$ $11\ (N) \times 19\ (R) = 209 = 29 = -1\ (N)$ $13\ (N) \times 17\ (N) = 221 = 11\ (N)$ *On réapplique aux produits* $29 \times 11 = 19\ (R)$ $19 \times 19 = 361 = 1\ (R)$
32	$3\ (N) \times 29\ (N) = 87 = 23\ (N)$ $13\ (N) \times 19\ (N) = 247 = 23\ (N)$ *On réapplique aux produits* $23 \times 23 = 529 = 17\ (R)$ $17 \times 17 = 289 = 1\ (R)$

Module	*Produit*
36	$5\ (N) \times 31\ (N) = 155 = 11\ (N)$ $7\ (N) \times 29\ (N) = 203 = 23\ (N)$ $13\ (O) \times 23\ (N) = 299 = 11\ (N)$ $17\ (N) \times 19\ (N) = 323 = 35 = -1\ (N)$ *On réapplique aux produits* $11 \times 23 = 1$
40	$3\ (N) \times 37\ (N) = 111 = 31\ (N)$ $11\ (N) \times 29\ (N) = 319 = -1\ (N)$ $17\ (N) \times 23\ (N) = 391 = 31\ (N)$ *On réapplique aux produits* $31 \times 31 = 961 = 1\ (R)$
42	$5\ (N) \times 37\ (R) = 185 = 17\ (N)$ $11\ (N) \times 31\ (N) = 341 = 5\ (N)$ $13\ (N) \times 29\ (N) = 377 = 41 = -1\ (N)$ $19\ (N) \times 23\ (N) = 437 = 17\ (N)$ *On réapplique aux produits* $17 \times 5 = 85 = 1\ (R)$
44	$3\ (N) \times 41\ (N) = 123 = 35\ (N)$ $7\ (N) \times 37\ (R) = 259 = 39\ (N)$ $13\ (N) \times 31\ (N) = 403 = 7\ (N)$ *On réapplique aux produits* $35 \times 39 = 1365 = 1\ (R)$
48	$5\ (N) \times 43\ (N) = 215 = 23\ (N)$ $7\ (N) \times 41\ (N) = 287 = 47 = -1\ (N)$ $11\ (N) \times 37\ (N) = 407 = 23\ (N)$ $17\ (N) \times 31\ (N) = 527 = 47 = -1\ (N)$ $19\ (N) \times 29\ (N) = 551 = 23\ (N)$ *On réapplique aux produits* $23^2 = 529 = 1\ (R)$
50	$3\ (N) \times 47\ (N) = 141 = 41\ (R)$ $7\ (N) \times 43\ (N) = 301 = 1\ (R)$ $13\ (N) \times 37\ (N) = 481 = 31\ (R)$ $19\ (R) \times 31\ (R) = 589 = 39\ (R)$ *On réapplique aux produits* $41 \times 39 = 1599 = -1\ (R)$
52	$5\ (N) \times 47\ (N) = 235 = 27\ (N)$ $11\ (N) \times 41\ (N) = 451 = 35\ (N)$ $23\ (N) \times 29\ (R) = 667 = 43\ (N)$ *On réapplique aux produits* $27 \times 43 \times 43 \times 35 = 1747305 = 1\ (R)$ $27 \times 27 = 1\ (R)$
54	$7\ (R) \times 47\ (N) = 329 = 5\ (N)$ $11\ (N) \times 43\ (R) = 473 = 41\ (N)$ $13\ (R) \times 41\ (N) = 533 = 47\ (N)$ $17\ (N) \times 37\ (R) = 629 = 35\ (N)$ $23\ (N) \times 31\ (R) = 713 = 11\ (N)$ *On réapplique aux produits* $5 \times 11 = 1\ (R)$ $41 \times 47 \times 35 = -1\ (R)$
56	$3\ (N) \times 53\ (N) = 159 = 47\ (N)$ $13\ (N) \times 43\ (N) = 559 = -1\ (N)$ $19\ (N) \times 37\ (N) = 703 = 31\ (N)$ *On réapplique aux produits* $47 \times 31 = 1\ (R)$

Module	*Produit*
60	$7\ (N) \times 53\ (N) = 371 = 11\ (N)$ $13\ (N) \times 47\ (N) = 611 = 11\ (N)$ $17\ (N) \times 43\ (N) = 731 = 11\ (N)$ $19\ (N) \times 41\ (N) = 779 = -1\ (N)$ $23\ (N) \times 37\ (N) = 851 = 11\ (N)$ $29\ (N) \times 31\ (N) = 899 = -1\ (N)$ *On réapplique aux produits* $11^2 = 1\ (R)$
64	$3\ (N) \times 61\ (N) = 183 = 55\ (N)$ $5\ (N) \times 59\ (N) = 295 = 39\ (N)$ $11\ (N) \times 53\ (N) = 583 = 7\ (N)$ $17\ (R) \times 47\ (N) = 799 = 31\ (N)$ $23\ (N) \times 41\ (R) = 943 = 47\ (N)$ *On réapplique aux produits* $31^2 = 1\ (R)$ $47^4 = 1\ (R)$ $55 \times 7 = 385 = 1\ (R)$ $39 \times 39 \times 47 = 71487 = -1\ (N)$
66	$5\ (N) \times 61\ (N) = 305 = 41\ (N)$ $7\ (N) \times 59\ (N) = 413 = 17\ (N)$ $13\ (N) \times 53\ (N) = 689 = 29\ (N)$ $19\ (N) \times 47\ (N) = 893 = 35\ (N)$ $23\ (N) \times 43\ (N) = 989 = 65\ (N)$ $29\ (N) \times 37\ (R) = 1073 = 17\ (N)$ *On réapplique aux produits* $41 \times 29 = 1189 = 1\ (R)$ $17 \times 35 = 595 = 1\ (R)$
68	$7\ (N) \times 61\ (N) = 427 = 19\ (N)$ $31\ (N) \times 37\ (N) = 1147 = 59\ (N)$ *On réapplique aux produits* $19^2 \times 59^2 = 1256641 = 1\ (R)$
70	$3\ (N) \times 67\ (N) = 201 = 61\ (N)$ $11\ (R) \times 59\ (N) = 649 = 19\ (N)$ $17\ (N) \times 53\ (N) = 901 = 61\ (N)$ $23\ (N) \times 47\ (N) = 1081 = 31\ (N)$ $29\ (R) \times 41\ (N) = 1189 = -1\ (N)$ *On réapplique aux produits* $61 \times 31 = 1891 = 1\ (R)$
72	$5\ (N) \times 67\ (N) = 335 = 47\ (N)$ $11\ (N) \times 61\ (N) = 671 = 23\ (N)$ $13\ (N) \times 59\ (N) = 767 = 47\ (N)$ $19\ (N) \times 53\ (N) = 1007 = -1\ (N)$ $29\ (N) \times 43\ (N) = 1247 = 23\ (N)$ $31\ (N) \times 41\ (N) = 1271 = 47\ (N)$ *On réapplique aux produits* $47^2 \times 23^2 = 1168561 = 1\ (R)$
76	$3\ (N) \times 73\ (R) = 219 = 67\ (N)$ $5\ (N) \times 71\ (N) = 355 = 51\ (N)$ $17\ (N) \times 59\ (N) = 1003 = 15\ (N)$ $23\ (N) \times 53\ (N) = 1219 = 3\ (N)$ $29\ (N) \times 47\ (N) = 1363 = 71\ (N)$ *On réapplique aux produits* $51 \times 3 = 153 = 1\ (R)$ $15 \times 71 = 1065 = 1\ (R)$

Module	*Produit*
78	$5\ (N) \times 73\ (N) = 365 = 53\ (N)$ $7\ (N) \times 71\ (N) = 497 = 29\ (N)$ $11\ (N) \times 67\ (N) = 737 = 35\ (N)$ $17\ (N) \times 61\ (R) = 1037 = 23\ (N)$ $19\ (N) \times 59\ (N) = 1121 = 29\ (N)$ $31\ (N) \times 47\ (N) = 1457 = 53\ (N)$ $37\ (N) \times 41\ (N) = 1517 = 35\ (N)$ *On réapplique aux produits* $53^2 = 2809 = 1\ (R)$ $29 \times 35 = 1015 = 1\ (R)$ $23^3 = 12167 = -1\ (N)$
80	$7\ (N) \times 73\ (N) = 511 = 31\ (N)$ $13\ (N) \times 67\ (N) = 871 = 71\ (N)$ $19\ (N) \times 61\ (N) = 1159 = 39\ (N)$ $37\ (N) \times 43\ (N) = 1591 = 71\ (N)$ *On réapplique aux produits* $31^2 = 961 = 1\ (R)$ $39^2 = 1521 = 1\ (R)$ $71^2 = 5041 = 1\ (R)$
84	$5\ (N) \times 79\ (N) = 395 = 59\ (N)$ $11\ (N) \times 73\ (N) = 803 = 47\ (N)$ $13\ (N) \times 71\ (N) = 923 = -1\ (N)$ $17\ (N) \times 67\ (N) = 1139 = 47\ (N)$ $23\ (N) \times 61\ (N) = 1403 = 59\ (N)$ $31\ (N) \times 53\ (R) = 1643 = 47\ (N)$ $37\ (R) \times 47\ (N) = 1739 = 59\ (N)$ $41\ (N) \times 43\ (R) = 1763 = -1\ (N)$ *On réapplique aux produits* $47 \times 59 = 2773 = 1\ (R)$
88	$5\ (N) \times 83\ (N) = 415 = 63\ (N)$ $17\ (N) \times 71\ (N) = 1207 = 63\ (N)$ $29\ (N) \times 59\ (N) = 1711 = 39\ (N)$ $41\ (N) \times 47\ (N) = 1927 = 79\ (N)$ *On réapplique aux produits* $39 \times 79 = 3081 = 1\ (R)$
90	$7\ (N) \times 83\ (N) = 581 = 41\ (N)$ $11\ (N) \times 79\ (R) = 869 = 59\ (N)$ $17\ (N) \times 73\ (N) = 1241 = 71\ (N)$ $19\ (R) \times 71\ (N) = 1349 = -1\ (N)$ $23\ (N) \times 67\ (N) = 1541 = 11\ (N)$ $29\ (N) \times 61\ (R) = 1769 = 59\ (N)$ $31\ (R) \times 59\ (N) = 1829 = 29\ (N)$ $37\ (N) \times 53\ (N) = 1961 = 71\ (N)$ $43\ (N) \times 47\ (N) = 2021 = 41\ (N)$ *On réapplique aux produits* $41 \times 11 = 451 = 1\ (R)$ $59 \times 29 = 1711 = 1\ (R)$ $71^2 = 5041 = 1\ (R)$
92	$3\ (N) \times 89\ (N) = 267 = 83\ (N)$ $13\ (R) \times 79\ (N) = 1027 = 15\ (N)$ $19\ (N) \times 73\ (R) = 1387 = 7\ (N)$ $31\ (N) \times 61\ (N) = 1891 = 51\ (N)$ *On réapplique aux produits* $83 \times 51 = 4233 = 1\ (R)$

Module	*Produit*
96	$7\ (N) \times 89\ (N) = 623 = 47\ (N)$
	$13\ (N) \times 83\ (N) = 1079 = 23\ (N)$
	$17\ (N) \times 79\ (N) = 1343 = 95 = -1\ (N)$
	$23\ (N) \times 73\ (R) = 1679 = 47\ (N)$
	$29\ (N) \times 67\ (N) = 1943 = 23\ (N)$
	$37\ (N) \times 59\ (N) = 2183 = 71\ (N)$
	$43\ (N) \times 53\ (N) = 2279 = 71\ (N)$
	On réapplique aux produits
	$47^2 = 1\ (R)$
	$23 \times 71 = 1\ (R)$
98	$19\ (N) \times 79\ (R) = 1501 = 31\ (N)$
	$31\ (N) \times 67\ (R) = 2077 = 19\ (N)$
	$37\ (R) \times 61\ (N) = 2257 = 3\ (N)$
	On réapplique aux produits
	$31 \times 19 = 1\ (R)$
100	$3\ (N) \times 97\ (N) = 291 = 91\ (N)$
	$11\ (N) \times 89\ (R) = 979 = 79\ (N)$
	$17\ (N) \times 83\ (N) = 1411 = 11\ (N)$
	$29\ (R) \times 71\ (N) = 2059 = 59\ (N)$
	$41\ (R) \times 59\ (N) = 2419 = 19\ (N)$
	$47\ (N) \times 53\ (N) = 2491 = 91\ (N)$
	On réapplique aux produits
	$91 \times 11 = 1\ (R)$
	$79 \times 19 = 1\ (R)$
	$59^5 = -1\ (N)$

Le problème auquel on est confronté, c'est que si on étudie maintenant les produits pour les nombres premiers impairs qui ne sont pas des décomposants de Goldbach de n, rien ne semble les distinguer des décomposants. Par exemple, pour le nombre pair 100, on obtient pour les produits des non-décomposants de Goldbach :

Module	*Produit*
100	$7\ (N) \times 93\ (N) = 651 = 51\ (N)$
	$13\ (N) \times 87\ (N) = 1131 = 31\ (N)$
	$19\ (N) \times 81\ (R) = 1539 = 39\ (N)$
	$23\ (N) \times 77\ (N) = 1771 = 71\ (N)$
	$31\ (N) \times 69\ (R) = 2179 = 79\ (N)$
	$37\ (N) \times 63\ (N) = 2331 = 31\ (N)$
	On réapplique aux produits
	$31 \times 71 = 1\ (R)$
	$51^2 = 1\ (R)$
	$39^5 = -1\ (N)$
	$79^5 = -1\ (N)$

Annexe 1 : Groupe des unités

Un décomposant de Goldbach de n, s'il existe, est un élément du groupe des unités $(\mathbb{Z}/n\mathbb{Z})^*$. Son complémentaire à n appartient lui aussi au groupe des unités. Le groupe des unités forme un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, \times)$. Son ordre divise l'ordre du groupe en question.

Annexe 2 : Journal mathématique de Gauss

On lit dans le journal mathématique de Gauss qu'il s'est intéressé à la conjecture de Goldbach en date du 14 mai 1796. Les traducteurs du journal en français, P. Eymard et J.P. Lafon, écrivent en préface à leur traduction : *"à plusieurs reprises, nous voyons Gauss découvrir d'importants théorèmes par des essais numériques et provoquer l'heureuse rencontre des chiffres, forçant ensuite la démonstration rigoureuse par une recherche de plusieurs mois"*.
Gauss écrit également en date du 9 juillet 1814 : *"Dedekind a de cette manière vérifié la proposition pour tous les nombres premiers inférieurs à 100"*.
Cependant, Henri Poincaré écrit dans la Science et l'Hypothèse : *"une accumulation de faits n'est pas plus une science qu'un tas de pierres n'est une maison"*.

Annexe 3 : articles 101 et 106 des Recherches Arithmétiques

Article 101 : Tout nombre non-divisible par p, qui est résidu de p sera aussi résidu de p^n ; celui qui ne sera pas résidu de p ne le sera pas non plus de p^n.

Article 106 : On voit de ce qui précède, qu'il suffit de reconnaître si un nombre donné est résidu ou non-résidu d'un nombre premier donné, et que tous les cas reviennent à celui-là.
Un nombre quelconque A, non-divisible par un nombre premier $2m + 1$, est résidu ou non-résidu de ce nombre premier suivant que $A^m \equiv +1$ *ou* $\equiv -1$ $(mod\ 2m + 1)$.

Annexe 4 : Nombre de résidus quadratiques d'un module quelconque

Les formules suivantes, fournies par M. Banderier, permettent de calculer le nombre de résidus quadratiques (noté $\rho_2(n)$) du module n :

- $\rho_2(2) = 2$
- $\rho_2(p) = \dfrac{p+1}{2}$
- $\rho_2(2^n) = \dfrac{3}{2} + \dfrac{2^n}{6} + \dfrac{(-1)^{n+1}}{6}$
- $\rho_2(p^n) = \dfrac{3}{4} + \dfrac{(p-1)(-1)^{n+1}}{4(p+1)} + \dfrac{p^{n+1}}{2(p+1)}$
- $\rho_2(mn) = \rho_2(m)\rho_2(n)$.

Alain Connes avait donné en novembre 2010 à l'Institut Henri Poincaré une conférence intitulée *Espace-Temps et Nombres premiers : deux défis pour la géométrie*. Cette conférence est visionnable à l'adresse : `http://www.poincare.fr/evenements/item/29-espace-temps.html`

Cette conférence n'est pas compréhensible par le néophyte mais le conférencier insiste sur le fait que cela n'a pas d'importance, on pourra la comprendre parfois 10 ans plus tard.

Il cite en début de conférence le principe de Ritz-Rydberg qui s'écrit :

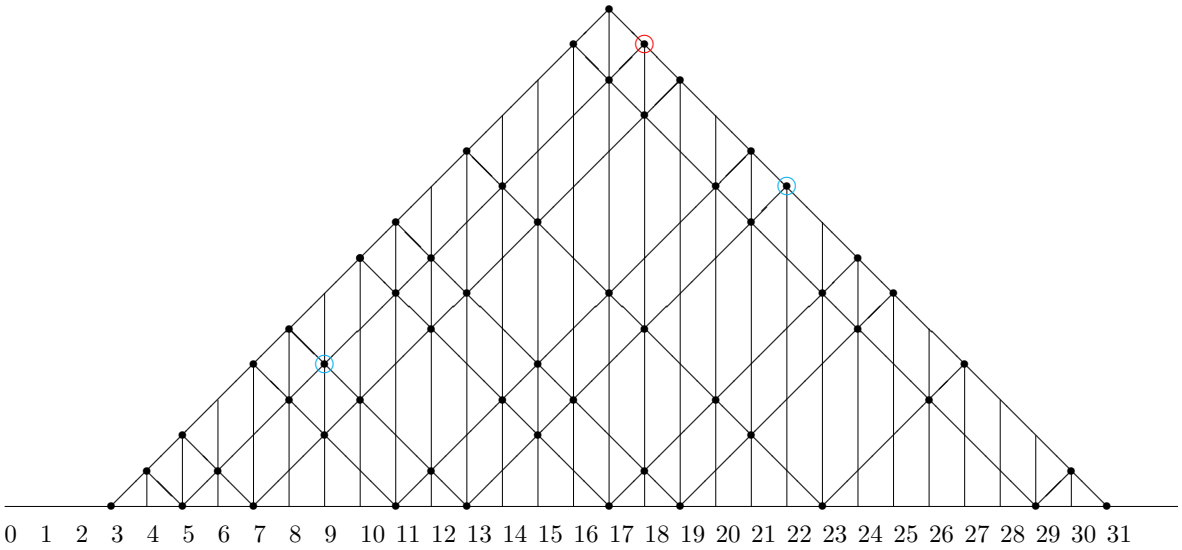
$$\nu_{\alpha\beta} + \nu_{\beta\gamma} \to \nu_{\alpha\gamma}$$

On peut "lier" ce principe à la Conjecture de Goldbach de la façon suivante :

$$\begin{array}{ll} 18 & = 5 + 13 \\ 44 & = 13 + 31 \\ \hline 36 & = 5 + 31 \end{array}$$

α correspond à l'entier 5, β à l'entier 13 et γ à l'entier 31. $\nu_{\alpha\beta}$ correspond à l'entier 18, $\nu_{\beta\gamma}$ correspond à l'entier 44 et $\nu_{\alpha\gamma}$ correspond à l'entier 36. On voit que $\nu_{\alpha\gamma} = \nu_{\alpha\beta} + \nu_{\beta\gamma} - 2\beta$.

La "déduction" de la décomposition de Goldbach du nombre pair 36 des décompositions de Goldbach des nombres pairs 18 et 44 se représente ainsi sur le maillage des décompositions de Goldbach ($\nu_{\alpha\beta}$ et $\nu_{\beta\gamma}$ représentés de couleur cyan, $\nu_{\alpha\gamma}$ représenté de couleur rouge) :



On pourrait exprimer une sorte de non-commutativité de la relation "=" (que l'on doit lire ici "a pour décomposition de Goldbach") comme ceci :

$$\begin{array}{lll} 18 & = 5 + 13 & = 13 + 5 \\ 44 & = 13 + 31 & \neq 5 + 39 \\ \hline 36 & = 5 + 31 & \end{array}$$

Essayons d'étudier plus avant la façon dont une décomposition de Goldbach est *engendrée* par deux autres décompositions de Goldbach.

La décomposition $16 = 3 + 13$ peut être considérée comme engendrée par les couples de décompositions parentes suivantes :

$$\begin{array}{ll} (14 = 3 + 11, & 24 = 11 + 13) \\ (10 = 3 + 7, & 20 = 7 + 13) \\ (8 = 3 + 5, & 18 = 5 + 13) \end{array}$$

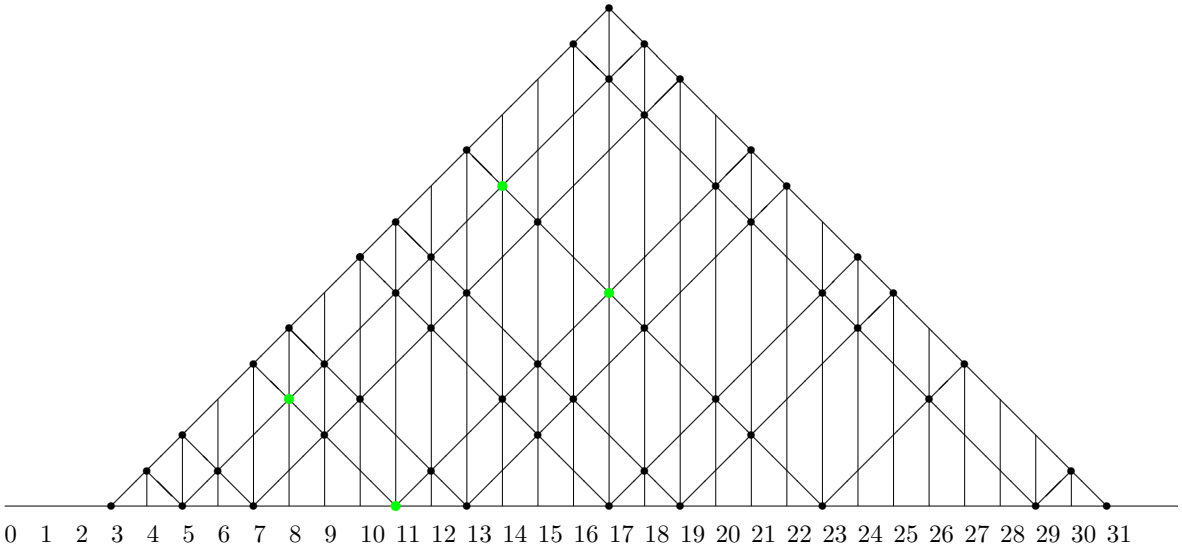
Tandis que $16 = 3 + 13$ peut être considérée comme engendrée par les seules décompositions parentes $(12 = 5 + 7, 18 = 7 + 11)$.

Similairement, la décomposition $28 = 5 + 23$ peut être considérée comme engendrée par les couples de décompositions parentes suivantes :

$$\begin{array}{ll} (12 = 5 + 7, & 30 = 7 + 23) \\ (16 = 5 + 11, & 34 = 11 + 23)(*) \\ (18 = 5 + 13, & 36 = 13 + 23) \\ (22 = 5 + 17, & 40 = 17 + 23) \\ (24 = 5 + 19, & 42 = 19 + 23) \end{array}$$

Tandis que $28 = 11 + 17$ peut être considérée comme engendrée par les seules décompositions parentes $(24 = 11 + 13, 30 = 13 + 17)$.

Graphiquement, le principe de Ritz-Rydberg se lit sur le maillage des décompositions en voyant une décomposition comme engendrée par les sommets de la diagonale opposée d'un rectangle dont elle est l'un des sommets et dont un double de premier est le sommet opposé. On fournit en vert le rectangle des décompositions marquées d'une étoile ci-dessus $28 = 5 + 23, 16 = 5 + 11, 22 = 11 + 11, 34 = 11 + 23$.



(*Denise Vella − Chemla*, 20/4/2012)

La conjecture de Goldbach* stipule que tout nombre pair supérieur ou égal à 6 est la somme de deux nombres premiers impairs.
Cela équivaut à: $\forall\, n \geq 6,\ \exists\, p \leq n/2,\ p\ premier\ impair,\ \forall\, q \leq \sqrt{n},\ q\ premier\ impair,\ p \not\equiv n\ (mod\ q)$

Par exemple, 98 a pour plus petit décomposant de Goldbach 19 parce que 3, 5, 7, 11, 13 et 17, les plus petits nombres premiers impairs, sont tous congrus à 98 selon un module premier impair inférieur à $\sqrt{98}$ tandis que 19 n'est congru à 98 selon aucun d'entre eux.

$98 \equiv 3\ (mod\ 5)$.
$98 \equiv 5\ (mod\ 3)$.
$98 \equiv 7\ (mod\ 7)$.
$98 \equiv 11\ (mod\ 3)$.
$98 \equiv 13\ (mod\ 5)$.
$98 \equiv 17\ (mod\ 3)$.

$98 \not\equiv 19\ (mod\ 3)$.
$98 \not\equiv 19\ (mod\ 5)$.
$98 \not\equiv 19\ (mod\ 7)$.

On choisit de démontrer plutôt :

$$(\exists\, n \geq 6,\ \forall\, p \leq n/2,\ \exists\, q \leq \sqrt{n},\ p\ et\ q\ premiers\ impairs,\ n \equiv p\ (mod\ q)) \implies false.$$

Notons $p_1, p_2, \ldots, p_k$ les nombres premiers impairs inférieurs ou égaux à $n/2$ et $q_1, q_2, \ldots, q_k$, les nombres premiers impairs inférieurs ou égaux à $\sqrt{n}$. Les q_i sont les modules selon lesquels n est congru aux différents p_i. Cherchons à établir d'où provient la contradiction. On a† :

$$\begin{aligned} &n \equiv p_1\ (mod\ q_1)\\ &n \equiv p_2\ (mod\ q_2)\\ &\ldots\\ &n \equiv p_k\ (mod\ q_k) \end{aligned}$$

D'après le théorème des restes chinois, les q_i étant soit égaux soit premiers entre eux 2 à 2, le système de congruences

$$\begin{aligned} &n \equiv p_1\ (mod\ q_1)\\ &n \equiv p_2\ (mod\ q_2)\\ &\ldots\\ &n \equiv p_k\ (mod\ q_k) \end{aligned}$$

aboutit à une contradiction de deux façons possibles.

Premier cas : Soit la contradiction provient du fait que le système contient des congruences contradictoires, telles que $n \equiv p_i\ (mod\ q), n \equiv p_j\ (mod\ q)$ avec $p_i \not\equiv p_j\ (mod\ q)$.

Second cas : Soit la contradiction provient du principe de *"descente infinie"* de Fermat : on ne conserve du système de congruences qu'un sous-ensemble de celui-ci, contenant des congruences selon des modules tous différents (les congruences omises étant non-contradictoires avec les congruences conservées sinon on se situerait dans le premier cas). Ce nouveau système S admet une solution unique n modulo M, le plus petit commun multiple des q_i. Le plus petit nombre vérifiant cette congruence unique ne satisfait pas la conjecture de Goldbach. Mais si l'on prend maintenant un sous-ensemble S' de congruences du nouveau système S, il admettra une solution unique également et le plus petit nombre n' vérifiant cette congruence

* $\forall\, n \geq 6,\ \exists\, p \leq n/2,\ \exists\, q \geq n/2,\ p\ et\ q\ premiers\ impairs,\ \ n = p + q,$

†Le problème consiste à "agréger" les différentes congruences concernant n : on ne peut pas par exemple déduire des différentes congruences sur n la congruence suivante :

$$n^k \equiv \prod_{p_1}^{p_k} p_i\ (mod\ \prod_{q_1}^{q_k} q_i)$$

Illustrons cette impossibilité sur un exemple :

$n \equiv 2\ (mod\ 3)$ *a pour solutions entières* $2,\ 5,\ 8,\ 11,\ 14,\ 17,\ 20,\ 23,\ 26,\ 29,\ 32,\ 35,\ 38, \ldots$
$n \equiv 3\ (mod\ 5)$ *a pour solutions entières* $3,\ 8,\ 13,\ 18,\ 23,\ 28,\ 33,\ 38, \ldots$

Mais les solutions du système constitué des 2 congruences sont $8, 23, 38, \ldots$, i.e. les solutions de la congruence $n \equiv 8\ (mod\ 15)$ qui ne s'obtient pas par une simple "multiplication terme à terme" des deux congruences initiales, mais par l'application complexe du théorème des restes chinois.

unique sera plus petit que n et ne vérifiera pas la conjecture de Goldbach non plus. On aboutit donc à une contradiction dans tous les cas[‡].

(Denise Chemla, 26/4/2012)

[‡]Illustrons l'inclusion d'ensembles de nombres en terme d'inclusion inverse des systèmes de congruences : le système de congruences

$$n \equiv 3 \ (mod\ 5)$$
$$n \equiv 5 \ (mod\ 7)$$

est inclu dans le système de congruence

$$n \equiv 1 \ (mod\ 3)$$
$$n \equiv 3 \ (mod\ 5)$$
$$n \equiv 5 \ (mod\ 7)$$

$5 \times 7 = 35,\ 3 \times 7 = 21,\ 3 \times 5 = 15, 3 \times 5 \times 7 = 105.$
$2 \times 35 \equiv 1 \ (mod\ 3),\ 21 \equiv 1 \ (mod\ 5),\ 15 \equiv 1 \ (mod\ 7).$
Le deuxième système a pour solution unique les nombres congrus à $1 \times 70 + 3 \times 21 + 5 \times 15 = 70 + 63 + 75 = 208 = 103 \ (mod\ 105)$ qui sont les nombres de la suite $103, 208, 313, \ldots$
Le premier système a quant à lui pour solution unique les nombres congrus à $3 \times 21 + 5 \times 15 = 63 + 75 = 138 = 33 \ (mod\ 35)$ qui sont les nombres de la suite $33, 68, 103, 138, 173, 208, 243, 278, 313, \ldots$
Comme prévu, les nombres vérifiant le deuxième système de congruences (plus contraint, une congruence supplémentaire) vérifient également le premier système (moins contraint).

Annexe : articles 33 à 36 (théorème des restes chinois) des Recherches Arithmétiques de Gauss

33. 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 $z \equiv a \pmod{A}$, $z \equiv b \pmod{B}$, etc. se ramèneront à une seule $z \equiv r \pmod{R}$ qui leur équivaudra, R étant le produit des nombres A, B, C, etc.: il suit de là réciproquement qu'une seule condition $z \equiv r \pmod{R}$ peut être décomposée en plusieurs $z \equiv r \pmod{A}$, $z \equiv r \pmod{B}$; $z \equiv r \pmod{C}$, etc. si A, B, C, etc. sont les différens facteurs premiers entr'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.

345. Soient comme ci-dessus les conditions $z \equiv a \pmod{A}$, $z \equiv b \pmod{B}$, $z \equiv c \pmod{C}$, etc. On résoudra tous les modules en facteurs premiers entr'eux; A en $A'A''A'''$ etc.; B en $B'B''B'''$ etc.; de manière que les nombres A', A'', etc., B', B'', etc. soient premiers ou puissances de nombres premiers; si l'un des nombres A, B, C, etc. était premier lui-même ou puissance d'un nombre premier, il n'y aurait, pour lui, aucune décomposition à faire. Alors ce qui précède fait voir que l'on peut, aux conditions données, substituer les suivantes $z \equiv a \pmod{A'}$, $z \equiv a \pmod{A''}$, $z \equiv a \pmod{A'''}$, etc.; $z \equiv b \pmod{B'}$, $z \equiv b \pmod{B''}$, etc., etc.; Or, à moins que tous les nombres A, B, C, etc. ne fussent premiers entr'eux; par exemple, si A n'est pas premier avec B, il est évident que tous les diviseurs premiers ne peuvent être différens dans A et dans B, mais qu'il doit y avoir quelqu'un des diviseurs A', A'', etc., qui trouve son égal, son multiple, ou son sousmultiple parmi les diviseurs B', B'', etc. Soit d'abord $A' = B'$, les conditions $z \equiv a \pmod{A'}$, $z \equiv b \pmod{B'}$, doivent être identiques, et l'on doit avoir $a \equiv b \pmod{A'}$ ou $\pmod{B'}$; ainsi l'une ou l'autre de ces deux conditions peut être rejetée; mais si l'on n'a pas $a \equiv b \pmod{A'}$, le problème est impossible. Soit ensuite B' un multiple de A', la condition $z \equiv a \pmod{A'}$ doit être contenue dans celle-ci, $z \equiv b \pmod{B'}$, ou bien celle-ci, $z \equiv b \pmod{A'}$, qui se déduit de la dernière, doit être équivalente à la première; d'où il suit que la condition $z \equiv a \pmod{A'}$, peut être rejetée, si elle ne contrarie pas l'autre, auquel cas le problème serait im-

C

possible. Quand toutes les conditions superflues sont ainsi rejetées, il est évident que tous les modules qui restent sont premiers entr'eux ; on est sûr alors de la possibilité du problème, et on peut procéder d'après la manière enseignée plus haut.

55. Si nous supposons comme au n° 32 $z \equiv 17 \pmod{504}$, $\equiv -4 \pmod{35}$, $\equiv 33 \pmod{16}$; ces conditions peuvent se décomposer en celles qui suivent : $z \equiv 17 \pmod{8}$, $\equiv 17 \pmod{9}$, $\equiv 17 \pmod{7}$; $z \equiv -4 \pmod{5}$, $\equiv -4 \pmod{7}$; $z \equiv 33 \pmod{16}$. De ces conditions on peut rejeter $z \equiv 17 \pmod{8}$ et $z \equiv 17 \pmod{7}$, car la première est renfermée dans la condition $z \equiv 33 \pmod{16}$, et la seconde est équivalente à $z \equiv -4 \pmod{7}$: il reste ainsi

$$z \equiv \left\{\begin{array}{r} 17 \pmod{9} \\ -4 \pmod{5} \\ -4 \pmod{7} \\ 33 \pmod{16} \end{array}\right\} \text{ d'où l'on tire } z \equiv 3041 \pmod{5040}.$$

Au reste il est clair qu'il sera souvent plus commode de ramener à une seule les conditions qui restent et qui proviennent de la même, ce qui se fera sans peine. Par exemple, quand on a rejeté quelques-unes des conditions $z \equiv a \pmod{A}$, $z \equiv a \pmod{A'}$, etc. celle qui se composera des conditions restantes sera $z \equiv a$, suivant le module formé par le produit de tous les modules qui restent. Ainsi dans notre exemple des conditions $z \equiv -4 \pmod{5}$, $z \equiv -4 \pmod{7}$; on tire sur-le-champ la condition $z \equiv -4 \pmod{35}$, d'où elles dérivent ; il s'ensuit qu'il n'est pas indifférent, quant à la briéveté du calcul, de rejeter l'une ou l'autre des conditions équivalentes ; mais il n'entre pas dans notre plan de parler de ces détails ni d'autres artifices pratiques que l'usage apprend mieux que les préceptes.

56. Quand tous les modules A, B, C, etc. sont premiers entr'eux, il est préférable le plus souvent d'employer la méthode suivante. On déterminera un nombre α congru à l'unité suivant A, et à 0 suivant le produit des autres modules ; c'est-à-dire, que α sera une valeur quelconque de l'expression $\frac{1}{BCD \text{ etc.}} \pmod{A}$, multipliée par BCD etc. (n° 32) ; mais il vaut mieux prendre la plus petite de ces valeurs. Soit de même $\beta \equiv 1 \pmod{B}$, et $\equiv 0 \pmod{ACD \text{ etc.}}$;

$\gamma \equiv 1$ (mod. C), et $\equiv 0$ (mod. ABD etc.). Alors si l'on cherche un nombre z qui soit congru aux nombres a, b, c, etc. suivant les modules A, B, C, etc. respectivement, on pourra poser..... $z \equiv \alpha a + \beta b + \gamma c +$ etc. (mod. $ABCD$ etc.); en effet on a évidemment $\alpha a \equiv a$ (mod. A), et les autres termes sont $\equiv 0$ (mod. A); donc $z \equiv a$ (mod. A). La démonstration est la même pour les autres modules. Cette solution est préférable à la première; quand on a à résoudre plusieurs problèmes du même genre, pour lesquels les valeurs de A, B, C, etc. sont les mêmes; car alors on trouve pour α, β, etc. des valeurs constantes. Ceci s'applique au problème de chronologie dans lequel on cherche le quantième de l'année pour laquelle l'indiction, le nombre d'or et le cycle solaire sont donnés. Ici $A = 15$, $B = 19$, $C = 28$; ainsi comme la valeur de l'expression $\frac{1}{19.28}$ (mod. 15), ou $\frac{1}{532}$ (mod. 15) est 13, on aura $\alpha = 6916$; on trouvera de même $\beta = 4200$, $\gamma = 4845$. Donc le nombre cherché sera le résidu *minimum* du nombre $6916a + 4200b + 4845c$, a représentant l'indiction, b le nombre d'or, et c le cycle solaire.

37. Nous n'en dirons pas davantage sur les congruences du premier degré, qui ne renferment qu'une seule inconnue; il nous reste à parler des congruences qui renferment plusieurs inconnues; mais, comme il faudrait donner trop d'extension à ce chapitre, si nous voulions exposer chaque chose en toute rigueur, et notre projet n'étant pas d'épuiser ici la matière, mais seulement de présenter ce qui est le plus digne d'attention; nous bornerons notre recherche à un petit nombre d'observations, réservant l'exposition complète pour une autre occasion.

1°. De même que dans les équations, on voit qu'il faut avoir autant de congruences qu'il y a d'inconnues à déterminer.

2°. Soient donc proposées les congruences

$$ax + by + cz \ldots \equiv f \text{ (mod. } m) \ldots (A)$$
$$a'x + b'y + c'z \ldots \equiv f' \ldots\ldots\ldots (A')$$
$$a''x + b''y + c''z \ldots \equiv f'' \ldots\ldots\ldots (A'')$$
etc.

en même nombre que les inconnues x, y, z, etc.

1 Extraits de *Comprendre les mathématiques* de Claude-Paul Bruter

p. 9
Ces ouvrages, formellement bons par ailleurs, mais où tout est mécaniquement et froidement démontré et enchaîné pour satisfaire à une vocation de rigueur qui, certes, répond à une nécessité, mais a perdu ses racines.

[Les savants] se sont toujours efforcés de faire connaître autour d'eux la manière dont ils comprenaient les événements, d'autant plus que cette manière, à tort ou à raison, leur semblait être en progrès par rapport aux savoirs antérieurs.

p. 10
L'un des rôles majeurs de l'éducation est de former l'esprit des jeunes gens pour qu'ils soient mieux à même, notamment par leur équilibre intérieur, de supporter les souffrances, de venir à bout des épreuves quelle qu'en soit la nature, d'apporter leur contribution pour réduire autant que faire se peut, à l'échéance la plus brève possible, les désagréments que notre humanité peut connaître.
Une telle formation suppose qu'on développe et élargisse la sensibilité de l'être, et non point qu'on la restreigne, qu'on développe et élargisse à travers cette sensibilité aiguisée le souci de comprendre, et non point qu'on fige l'intelligence dans les limites d'un domaine de pensée borné. L'intuition de Poincaré lui a fait pressentir des évolutions dont il s'est alarmé. Il a craint que l'enseignement, en particulier celui des mathématiques, ne se dirige vers des formes qui émousse la sensibilité plutôt qu'elles ne l'exercent, comme cela lui paraît nécessaire.

p. 29
Pourtant, l'homme a besoin du rêve pour concevoir de meilleures organisations, il a besoin de s'évader, par moments, de la réalité et de reposer son psychisme afin de reprendre assez de forces intérieures pour pouvoir affronter à nouveau les difficultés quotidiennes. L'homme est ici un enfant.
Les constructions ou modèles mathématiques apparaissent alors parfois comme des jouets, inoffensifs, initiatiques et curatifs, avec lesquels les hommes peuvent faire travailler leur imagination, se donner de l'importance et une raison d'être, construire des mondes parfois baroques, dévoiler des fantasmes qui peuplent leur esprit et dont ils se délivrent par le jeu. Sans doute ces jouets n'ont-ils pas exactement les mêmes fonctions chez les adultes et chez les enfants. Mais les uns et les autres partagent à leur égard des réactions communes dans la mesure où ils pratiquent les mêmes opérations mentales et de la même manière.
Ces réactions, parce qu'elles sont d'ordre affectif, marquent les individus : découragement et parfois rejet de la part de ceux qui éprouvent quelque difficulté, quelles qu'en soient les raisons, à comprendre et interpréter le discours mathématique, enthousiasme au contraire de la part d'autres, tenaces, stimulés par la difficulté à vaincre, joyeux de l'avoir surmontée, excités par le merveilleux d'une démonstration où la perfection du raisonnement n'a pas voilé l'éclat de l'étincelle divinatoire, épanouis enfin par la beauté de la perspective des théorèmes réunis en une théorie harmonieuse.

Un autre aspect sémantique de la notion d'application se rencontre également dans la littérature : les termes “projection”, “injection”, “immersion”, “surjection” et “submersion” le révèlent en partie. On s'amusera un instant, bien sûr, de l'aspect facétieux du mathématicien que pourrait révéler le choix d'une terminologie “aquatique”. A vrai dire, ce choix est particulièrement heureux car l'image marine est l'une des meilleures qui soit pour évoquer un milieu topologique, souple et indifférencié, au sein duquel un objet peut être “plongé” - autre terme mathématique. Cette terminologie souffre pourtant d'une insuffisance : elle se rapporte en effet au caractère local de l'application ; elle en évoque plus difficilement l'effet global. Globalement, la projection, la submersion, aplatit, plaque l'objet de départ sur l'espace d'arrivée, de sorte que l'objet plaqué a au plus la même dimension que celle de l'espace d'arrivée (il ne s'agit pas ici d'une dimension au sens métrique du terme, mais du nombre de directions suffisantes pour établir un repère à partir duquel on peut situer tout point de l'espace). Au contraire, la dimension de l'objet source est conservée si l'on procède à une immersion de cet objet. Reste le cas où la dimension de l'objet source est égale à celle de l'espace d'arrivée : parmi les applications de ce type figurent notamment les changements de repères qui permettront d'examiner l'objet sous des angles et à partir de points de vue différents. Ces changements de repères sont très utilisés pour obtenir des présentations simples et éclairantes des objets,

permettant de les classer facilement, de mettre en évidence certaines propriétés. Les submersions plus générales permettent de procéder à des découpes en tranches : leur dimension est égale à la différence entre les dimensions des espaces source et image.
On voit ici apparaître les notions essentielles de singularité et d'extrémalité, profondément liées l'une à l'autre. Pour des raisons d'ordre physique et même métaphysique, ces notions sont d'une extrême fécondité et d'une grande importance. Elles apparaissent dans l'œuvre de Fermat, et joueront un rôle de plus en plus manifeste dans le développement des mathématiques.
Sur le plan psychologique, la singularité possède une double propriété : elle est attirante par son originalité, dérangeante par son étrangeté. Sur le plan physique, elle possède aussi une double propriété : elle est à la fois un obstacle et, par cela même, un élément autour duquel se structure et s'organise son voisinage. La singularité renferme ainsi toute l'ambiguïté du monde. La prise de conscience des propriétés de la singularité nous permet de mieux accepter le caractère ambigu de ce monde, caractère contre lequel il devient absurde de s'insurger, qu'il est finalement vain de vouloir combattre.
C'est la géométrie qui permet d'établir un lien entre singularité et extrémalité, via la notion de bord d'un objet. Le bord est en effet la partie de l'objet où la dimension s'affaiblit : si le couteau est globalement un objet de dimension 3, la surface du manche est de dimension 2, la partie coupante de la lame est une ligne de dimension 1, et même, si l'on a affaire à un couteau-scie, les extrémités des dents de la scie sont des points de dimension 0. Le bord du couteau est composé de toutes ces parties de dimensions inférieures à 3. Cette définition topologique du bord coïncide ici avec la définition métrique : si l'on parvient à définir une notion de distance entre points du couteau, ce bord se confond avec le lieu des points du couteau les plus écartés, situés sur des droites traversant le couteau. Ces points extrêmes qui définissent le bord sont également singuliers, particuliers, rares parmi l'infinité des points qui forment le domaine du couteau.
La reconnaissance de la prégnance, en mathématiques, des concepts d'extrémalité et de singularité, la prise de conscience de l'importance de leur rôle dans l'activité des mathématiciens sont récentes. Pourtant, il s'agit encore ici de notions naturelles, inscrites dans notre physiologie, son organisation, son mode de fonctionnement, dont l'emploi, primitivement inconscient, est sous l'empire de la nécessité intérieure. On voit ici la présence de la rationalité cachée, implicite, dans le processus qui conduit à l'emploi intuitif de ces concepts fondamentaux, puis à leur mise en lumière.
Ces niveaux profonds, où s'exerce de manière non simpliste la rationalité physique, parce qu'ils sont difficilement atteints par l'analyse consciente et complète, sont parfois hâtivement dénommés "irrationnels", dans le meilleur des cas du ressort de l'intuition. L'intuition, "forme de connaissance immédiate qui ne recourt pas au raisonnement", est malgré tout l'expression d'un processus rationnel qui, dans un premier temps, dépasse nos capacités de perception et d'analyse. Tels des panneaux qui jalonnent une piste, des étapes de ce processus peuvent émerger au niveau conscient, pouvant guider l'activité de l'esprit dans sa recherche de la rationalité sous-jacente, à l'origine même de ces indicateurs de rationalité.
Ce point de vue de Sirius, sous-tendu en premier lieu par un souci d'universalité, présente l'avantage de promouvoir la réponse à la question : dans quelle mesure une vérité locale a-t-elle une valeur plus générale ? Cette question en appelle d'autres : il faut en effet s'entendre au préalable sur l'étendue de cette généralité, et pour cela définir avec précision le cadre le plus large à l'intérieur duquel on pourra, de manière pertinente, travailler. Une fois cette mise en forme accomplie, qui permet d'élaguer les propriétés secondaires et de mettre en évidence les propriétés fondatrices et principales, reprend le travail proprement constructif du mathématicien. Toute l'histoire du progrès des mathématiques est profondément marquée par l'influence déterminante de la construction de ces théories chaque fois plus englobantes. C'est en définitive par leur intermédiaire que des propriétés d'apparence particulières révèlent leur signification générale, et finalement parviennent à être démontrées.

Ces propriétés générales s'imposent au mathématicien : la familiarité avec les cas particuliers lui permet de voir aussitôt la structure sous-jacente aux exemples qu'il manipule, ses articulations principales qu'il traduit sous forme d'axiomes. Il n'y a en l'occurrence rien d'irrationnel dans cette démarche ; tout au contraire, elle est l'expression d'une rationalité très claire et en quelque sorte naturelle. La nécessité et le bon sens imposent de montrer aux collègues l'organisation discrète de l'univers à l'intérieur duquel ils travaillent. La meilleure intelligence de cet univers, observé de plus loin mais avec un regard pénétrant, permet de mieux déceler et mettre au jour les chemins qui courent entre les propositions.
Proposons cette comparaison : cet univers des idées est semblable dans sa genèse à celui d'un univers géographique, à une planète dont nous essayons de préciser le relief. Par temps clair, ou parce que nous sommes proches et dotés de très bons instruments, pics, cols et vallées se font voir d'emblée sous un jour cohérent, une sorte de nécessité interne implique leur présence en tel lieu, leur étendue. Il arrive fréquemment que les conditions d'observation ne soient pas aussi favorables. Mais l'observateur averti, doté d'une expérience professionnelle, d'une grande patience et d'une grande concentration, repère des

indices, de plus en plus nombreux au fil du temps, de sorte que le paysage géographique dont il veut percer les secrets finit, petit à petit, par prendre forme. Des pans de cet univers se mettent en place, la position de tel indice étant induite, s'expliquant par celle de tel autre. Un seuil de reconstitution atteint, le voile se déchire et le paysage apparaît en toute clarté.
Par intuition, nous désignons un ensemble d'activités mentales qui comprend l'observation et la réminiscence de faits analogues et d'indices. Ceux-ci suggèrent l'existence de telle propriété, dont on finit par conjecturer la présence. Ce sont les premiers éléments d'un puzzle que des raisons morphologiques locales vont permettre de reconstituer. En l'occurrence, la culture mathématique du chercheur, ses compétences dans d'autres domaines, la maîtrise et la souplesse qu'il a acquises dans l'exercice du raisonnement, faisant appel à des raisons plus ou moins diverses et lointaines, à des comparaisons entre situations a priori étrangères les unes aux autres, lui permettent de deviner, de remarquer ou simplement de souligner la présence de telle ou telle propriété, et finalement d'exposer les raisons de son existence.
On peut alors soutenir que l'intuition est une manifestation très fine et très élaborée de la rationnalité profonde de l'être. Les qualités intrinsèques, la formation, et en particulier l'exercice sont à la source du déploiement de cette intuition.
L'image géographique que nous avons prise n'est pas innocente. Elle témoigne du caractère spatial de notre activité mentale. Elle prend en compte des considérations de nature géométrique dans le déroulement même de cette activité : le raisonnement n'est autre, souvent, que la description de l'enchaînement de morphologies s'emboîtant à la manière des pièces d'un puzzle. Cette vision décrit le raisonnement achevé. Le raisonnement actif, opératoire, créateur, est un processus constructif qui déplace les pièces, les retourne parfois de manière inattendue, les déforme, les relie, vérifie et justifie la possibilité de leur accouplement. Ce qui amène à distinguer deux types de démonstration : celle qui ne fait que s'appuyer sur des résultats connus, de la déduction desquels on justifie l'assertion proposée ; celle qui non seulement utilise le procédé précédent, mais s'appuie aussi sur un mode original de construction, auquel la démonstration doit son caractère excitant, fascinant, sa beauté propre. Le développement de la topologie est caractéristique de ce point de vue, comme le montrent par exemple les travaux de Thurston et Poenaru qui fourmillent de constructions originales. C'est à ce niveau sans doute que l'on se rapproche le plus de l'irrationalité. L'irruption de cette nouvelle manière de faire détruit une routine mentale, une tendance à l'ankylose de l'esprit. C'est à ce moment-là que l'on savoure le fin plaisir apporté par l'astuce, sorte d'aiguillon habile qui excite et fait rire l'esprit.
La construction permet d'insuffler la vie aux mathématiques ; quant au raisonnement, il est le ciment qui donne à l'édifice intellectuel sa solidité.
Nous avons maintenant en main assez d'éléments pour pouvoir aborder ici de manière brève, et pour conclure, ce thème pédagogique : comment développer, chez l'enfant, la rationalité dans ses formes directes ou subtiles ? A l'évidence, l'étude des mathématiques favorisera la formation des procédures de raisonnement. Cette étude suppose que l'on ne se contente pas, comme on le fait malheureusement depuis quelques années, d'enseigner des recettes aux élèves. Une telle cuisine scolaire est insipide, et sans grand intérêt pour la formation de l'esprit. Il est indispensable que ces élèves rencontrent des démonstrations vraies, parviennent à les maîtriser, d'abord pour s'exercer au raisonnement brut, mais également pour développer l'intuition. Comme Poincaré l'a souligné, l'exercice de la géométrie est plus apte à favoriser l'expression de l'intuition : c'est en effet en géométrie élémentaire que l'on rencontre le plus aisément ces constructions originales et pourtant faciles qui entraînent l'esprit à l'élaboration de petits puzzles mentaux attrayants. Une société ne saurait, sans risque grave pour sa pérennité, renoncer à ces jouets éducatifs millénaires, et dont les qualités ont été éprouvées au fil des siècles.

p. 79
Cette procédure qui consiste, étant donné une difficulté, à prendre de la hauteur, à adopter en quelque sorte un point de vue de Sirius pour mieux dominer la situation, doit-elle être considérée comme une démarche rationnelle ou non ? Donnons d'abord quelques exemples élémentaires où, cachée sous des habits bien différents, cette procédure est employée. Nous la rencontrons en premier lieu dans l'algèbre : celle de l'arithmétique, où l'on a commencé par remplacer les nombres par des lettres et raisonner sur des expressions littérales ; celle des espaces fonctionnels où les fonctions polynomiales, à travers la géométrie algébrique et l'arithmétique, ont joué un rôle central. Nous rencontrons à nouveau cette procédure en théorie des nombres, au moment où la création des nombres complexes, plus généralement lors de la création des nombres par la méthode des extensions. Les prémisses de cette procédure apparaissent également dans la conception, entrevue par N. Oresme ou Kant, d'espaces multidimensionnels.
Il est clair que, dans ces situations, l'observation répétée de cas possédant la même formulation est une invite naturelle à établir des formulations générales, des énoncés qui transcendent les cas particuliers. La démarche de l'esprit, autant fondée sur l'analogie que sur la synthèse, est une démarche de bon sens.

2 Extraits de *La construction des nombres* de Claude-Paul Bruter

p. 25
Provenant de Sur la nature des mathématiques, Paris, Gauthier-Villars, 1973
Etant donné un objet O' défini sur un ensemble E', et vérifiant les propriétés $P'_1, P'_2, \ldots, P'_n$, trouver un objet défini sur un ensemble E contenant E', vérifiant non seulement les propriétés précédentes $P'_1, P'_2, \ldots, P'_n$ mais de plus des propriétés $P'_{n+1}, P'_{n+2}, \ldots, P'_{n+m}$ et tel que la restriction de O à E' soit O'.

p. 34
Or le mode de construction de cet ensemble conduit à définir une notion d'ordre, et l'on montre facilement que : $\mathbb{N}$ est un ensemble muni d'un ordre total, d'une loi de composition additive, associative et commutative, possédant un élément neutre, et grâce à laquelle des opérations telles que $32 + 24 = 56$ ont un sens. On dit que $\mathbb{N}$ a la structure de demi-groupe commutatif, et non pas de groupe puisqu'en dehors de l'élément neutre, aucun élément ne possède de symétrique.

p. 216
Et quelles leçons de modestie et d'humilité, mais aussi d'optimisme, ne peut-on tirer de cette lenteur à accepter et à comprendre quelques-unes des plus simples de nos constructions ! Que les physiciens, perplexes, voire inquiets, tourmentés, qui s'interrogent sur l'intelligibilité du monde subatomique, veuillent bien se pénétrer de ces leçons, se rassurer, prendre patience : une longue adaptation de la pensée à nos constructions mentales, aux observations nouvelles, est parfois nécessaire jusqu'au moment où, la familiarité aidant, l'assimilation parvient à son terme, l'adéquation entre la construction et le fait sensible atteint un degré tel que la construction, aussi rudimentaire et imparfaite soit-elle, apparaît comme naturelle, comme imposée par la nécessité ; alors la construction fait sens, l'obscurité s'estompe, le paysage devient lumineux, et l'intelligibilité s'affirme.
"Le monde est un animal" disait Platon. Comme il est fascinant d'observer le développement de l'univers symbolique et grouillant construit par les physiciens et les mathématiciens ! A partir de quelques germes discrets de monades, à l'infini il s'auto-reproduit, envahissant l'espace, le meublant sans arrêt dans des directions de plus en plus nombreuses, de plus en plus denses, dessinant des figures de plus en plus enchevêtrées et tordues. Une longue préparation est nécessaire avant que ne soient libérées ces croissances fulgurantes. Pas à pas travaille d'abord la pensée. Puisque, lorsque les temps sont mûrs, apparaît la notion, le concept, la construction, et, sous le nom de théorème, le fait et son explication, qu'on appelle aussi démonstration.

p. 217
Avec Gauss sur les entiers, puis avec Cauchy sur les polynômes, par l'intermédiaire de relations d'équivalence, définies de manière algébrique de manière à être compatibles avec la structure des ensembles originels de nombres, on a pris l'habitude de couper ceux-ci en tranches égales ; chaque tranche est projetée sur un seul "point", qu'on peut désigner par un seul symbole, et qu'on peut appeler aussi "nombre nouveau". Un ensemble O_1 de tels nouveaux nombres possède une structure héritée de celle de l'ensemble originel O_0 considéré. Mais il faut souligner que chaque nouveau nombre, chaque tranche, hérite également en quelque sorte de cette structure interne. Evidemment, les structures filles ne sont pas forcément identiques en tout point aux structures mères, ni même entre elles, le fisc, en somme, étant passé par là.
En introduisant, sur O_1 maintenant, une relation d'équivalence convenable, on fabrique un nouvel ensemble de nombres O_2. Pour peu que O_0 soit un ensemble infini, on peut prolonger parfois jusqu'à l'infini ce processus de descente, de création de nombres structurés. Le procédé connaît un début d'emploi en physique où chaque nombre nouveau caractérise un état particulaire plus fin, structuré par un groupe de symétries, souvent un groupe de rotations.
Le progrès dans cette voie réside dans l'établissement de relations d'équivalence engendrant des tranches inégales. On peut commencer par supposer, par exemple, comme dans les pavages irréguliers de Penrose, la présence de deux types de tranches, et même, pour aller au plus simple, supposer que ces tranches forment un découpage périodique de l'ensemble de nombres considéré. On peut alors imaginer que la fabrication des tranches, leur localisation, dépendent de conditions extérieures qui fixent le découpage, d'une section particulière donc du fibré des contraintes. L'histoire de la construction des nombres n'a

certainement pas atteint son terme.

p. 219
Mais on peut s'interroger : pourquoi s'arrêter en si bon chemin, et ne pas appeler tout simplement nombre tout élément d'un ensemble muni d'une ou de plusieurs lois d'opérations, présentant entre elles des liens de compatibilité nécessaire, dont la nature et le mode opératoire sont, bien sûr, parfaitement définis, ou encore, plus généralement, pourquoi ne pas considérer que tout ensemble sur lequel opère un algorithme est un ensemble de nombres ?

p. 222
Le dernier point sera consacré, à travers la question de la validité du modèle numérique, à l'examen du bien-fondé du platonisme. Celui-ci postule l'existence d'un schéma préétabli selon lequel le monde est organisé, et qui s'exprime en termes mathématiques.
Il est clair que le platonisme vient en droite ligne du pythagorisme. Cette forme d'idéologie a joué et continue de jouer un rôle moteur et positif très important dans le développement des sciences, des mathématiques et de la physique en particulier. Aussi ne serait-il guère politique d'essayer de montrer que les hommes de science qui se réclament du platonisme sont encore imprégnés de ce mode de pensée qui fut celui de l'enfance de l'humanité, émerveillée par un monde peuplé de personnages héroïques, représentatifs, symboliques, mais aussi refuges auprès desquels s'ébauchent les premiers apprentissages de la vie sociale.

La célèbre formule "tout est nombre" fait partie du corpus des conceptions pythagoriciennes. Les capacités croissantes des ordinateurs, la richesse potentielle des représentations numériques que nous avons rencontrées, confortent sur le plan pratique les adeptes néopythagoriciens. La réalité est sans doute plus nuancée. Un nombre est un absolu instantané, statique. Le monde est beaucoup plus flou, il est constamment changeant. Aussi les nombres, qui sont des représentations, ne peuvent-ils fournir, en général, sur le plan pratique cela s'entend, que des approximations. Le "tout est nombre", qui a certes sa vérité sur les plans théorique et abstrait, devrait pour le moins être nuancé ; il serait plus exact d'énoncer, d'ailleurs de manière peut-être trop optimiste, "presque tout peut être approché par le nombre".

A quoi j'ajoute pour ma part, "je ne sais plus du tout ce qu'est un nombre, mais je sais m'en servir...".

3 Dans *Comment l'esprit vient aux savants* de Claude Brezinski

p. 9
Albert Einstein : Je cherche quand je veux, je trouve quand je peux.

Jérôme K. Jérôme : Après avoir cherché sans trouver, il arrive qu'on trouve sans chercher.

p. 20
Jack Lang : "Il faut être provoqué par les pensées des autres". Cette phrase s'applique à toute activité créatrice et, bien sûr, à la recherche scientifique.

p. 33
Mark Kac (Enigmas of chance, University of California Press, Berkeley, 1987, p. 39).
Il y a grossièrement deux sortes de créativité mathématique. La première, semblable à la conquête d'un pic montagneux, consiste à résoudre un problème demeuré ouvert et qui a attiré l'attention de nombreux mathématiciens. L'autre est l'exploration d'un nouveau territoire.

p. 53
Claude Bernard (Introduction à l'étude de la médecine expérimentale, J.B.Baillière et fils, Paris, 1865, p. 66-67).

Il n'y a pas de règles à donner pour faire naître dans le cerveau, à propos d'une observation donnée, une idée juste et féconde... Son apparition a été toute spontanée, et sa nature est toute individuelle. C'est un sentiment particulier, un quid proprium qui constitue l'originalité, l'invention ou le génie de chacun. Une idée neuve apparaît comme une relation nouvelle ou inattendue que l'esprit aperçoit entre les choses... Mais comme les sens, les intelligences n'ont pas toutes la même puissance ni la même acuité, et il est des rapports subtils et délicats qui ne peuvent être sentis, saisis et dévoilés que par des esprits plus perspicaces, mieux doués ou placés dans un milieu intellectuel qui les prédispose d'une manière favorable... Mais il est aussi des faits qui ne disent rien à l'esprit du plus grand nombre, tandis qu'ils sont lumineux pour d'autres. Il arrive même qu'un fait ou une observation reste très longtemps devant les yeux d'un savant sans rien lui inspirer ; puis tout à coup vient un trait de lumière, et l'esprit interprète le même fait tout autrement qu'auparavant et lui trouve des rapports tout nouveaux. L'idée neuve apparaît alors avec la rapidité de l'éclair comme une sorte de révélation subite ; ce qui prouve bien que dans ce cas, la découverte réside dans un sentiment des choses qui est non seulement personnel mais qui est même relatif à l'état actuel dans lequel se trouve l'esprit.

p. 61
Ivan Pavlov (cité dans E. Saparina, éd. Mir Moscou, 1987, p. 220-221).
Que voudrais-je souhaiter à la jeunesse de ma Patrie consacrée à la science ?
Avant tout, de l'esprit de suite. Je ne pourrai jamais parler sans émotion de cette condition primordiale d'une féconde activité scientifique. De l'esprit de suite, encore de l'esprit de suite, toujours de l'esprit de suite. Dès le début de votre travail, habituez-vous à un rigoureux esprit de suite dans l'accumulation des connaissances. Etudiez l'abc de la science avant d'essayer d'en atteindre les sommets. N'entreprenez jamais ce qui suit avant d'avoir assimilé ce qui précède. Ne tentez jamais de cacher les lacunes de vos connaissances, même par les hypothèses les plus hardies. Pour attrayants que soient les reflets chatoyants de cette bulle de savon, elle ne peut manquer de crever, et il ne vous restera rien d'autre qu'un pénible sentiment de confusion.
Cultivez en vous la retenue et la patience. Apprenez à faire les corvées dans la science. Etudiez, comparez, accumulez les faits. Quelle que soit la perfection de l'aile de l'oiseau, elle ne pourrait jamais s'élever sans s'appuyer sur l'air. Les faits sont l'air du savant. Sans eux, vous ne pourrez jamais prendre votre essor. Sans eux, vos "théories" resteront de vains efforts.
Mais, en étudiant, en expérimentant, en observant, tâchez de ne pas rester à la surface des faits. Ne vous transformez pas en archivistes des faits. Essayez de pénétrer le mystère de leur apparition. Cherchez opiniâtrement les lois qui les régissent.
Deuxièmement, je vous souhaite de la modestie. Ne croyez jamais que vous savez déjà tout. Et quelle que soit l'estime que l'on ait pour vous, ayez toujours le courage de vous dire : je suis un ignorant.
Ne laissez pas l'orgueil s'emparer de vous. Sinon vous vous obstinerez là où il faut tomber d'accord, vous refuserez un conseil utile et une aide amicale, vous perdrez le sens de l'objectivité...
Troisièmement, je vous souhaite la passion. Rappelez-vous que la science exige d'un homme sa vie entière... La science demande de gros efforts et une passion ardente. Soyez passionné dans votre travail et dans vos recherches.

p. 74
Louis Leprince-Ringuet (Les rayons cosmiques, Albin Michel, paris, 1945, p. 367).
Pour être à même de découvrir, il faut choisir une direction, s'y tenir longtemps avec ténacité, et ne la quitter que pour de très sérieuses raisons : tout choix est limitatif, cette limitation fait que l'on connaît parfois assez mal les autres branches de la science.

p. 114, 115
Pour que se produise l'illumination, il faut penser sans arrêt à son problème, il ne faut jamais le perdre de vue. Les opinions concordent sur ce point. Ainsi celle de Buffon (Histoire naturelle, générale et particulière, avec la description du cabinet du Roy. Matières générales, tome 1, premier discours, édition de l'imprimerie nationale, Paris 1749).
L'invention dépend de la patience ; il faut voir, regarder longtemps son sujet ; alors il se déroule et se développe peu à peu ; vous sentez un petit coup d'électricité qui vous frappe la tête et en même temps vous saisit le cœur : voilà le moment du génie.

Isaac Newton :
Si j'ai fait quelque découverte, c'est en pensant sans cesse au sujet qui m'occupait, en l'envisageant sous

toutes ses faces ; la recherche d'une vérité cachée m'en a souvent découvert d'autres auxquelles je n'eusse jamais songé. Une découverte en amène une autre, et l'on est étonné soi-même des aperçus qui naissent d'un examen sérieux et attentif... Je tiens le sujet de ma recherche constamment devant moi, et j'attends que les premières lueurs commencent à s'ouvrir devant moi, lentement, peu à peu, jusqu'à ce qu'elles se changent en une clarté pleine et entière.

Ivan Pavlov :
Le matin, levez-vous avec votre problème devant vos yeux. Déjeunez avec lui. Allez au laboratoire avec lui. Prenez votre déjeuner de midi avec lui. Rentrez chez vous le soir avec lui. Dînez avec lui. Gardez-le avec vous après dîner. Allez au lit avec lui. Rêvez-en.

Ainsi donc, quel que soit leur domaine, les scientifiques ont toujours en tête le problème qui les préoccupe. C'est ainsi que la solution peut leur apparaître tout d'un coup dans des situations bizarres où l'esprit peut vagabonder à loisir. Ainsi Jacques Monod disant un lundi matin à une collaboratrice : "j'ai pensé à ça hier, en escaladant un rocher à Fontainebleau".

p. 118
Jean Guitton (Le travail intellectuel, Aubier-Montaigne, Paris, 1986)
La règle d'or du travail intellectuel peut se traduire ainsi ; "Ne tolère ni de demi-travail, ni de demi-repos. Donne-toi tout entier ou détends-toi absolument. Qu'il n'y ait jamais en toi de mélange des genres !"

p.122
William Shockley (prix Nobel de Physique 1956)
Une conclusion vitale atteinte en pensant à la pensée est que la créativité est associée à l'échec. L'esprit qui crée une association d'idées relativement nouvelle et ordonnée a habituellement erré par des chemins détournés apparemment infructueux et a enduré des désappointements. Cependant les travaux entrepris qui mènent à ces frustrations sont une part essentielle de la créativité. Entreprendre de tels travaux permet à l'esprit compétent de se rendre compte des concepts qui sont les attributs clés de la situation chaotique à laquelle on est confronté. La méthodologie de l'échec créatif utilise un ensemble d'outils de pensée scrutatrice qui, même si ses premiers efforts échouent, rendent le chercheur conscient des attributs clés du problème. Ainsi, penser à la pensée encourage à la tolérance de ses limitations humaines inévitables et permet à l'individu d'être plus créatif en reconnaissant que ses échecs sont souvent des cubes utilisables pour acquérir de la puissance intellectuelle dans une nouvelle situation.

Yukawa (prix Nobel de Physique 1949 pour sa découverte théorique de l'existence du méson)
Les erreurs, bien sûr, ne sont en aucune façon gaspillées... selon le vieux dicton "l'erreur est la mère du succès". J'ai moi-même souvent travaillé dur du matin jusqu'au crépuscule seulement pour jeter à la corbeille, en désespoir de cause, ce que j'avais fait. Quantitativement, ce que je garde parce que quelque chose peut en sortir est incomparablement plus petit que ce que j'ai jeté et cependant c'est cela, je crois, qui sert de base à la création.

p. 123
Jules Tannery : Chaque découverte vient à son heure ; elle est rendue possible par celles qui l'ont précédée. C'est, à chaque instant, ce que l'on sait qui suggère les questions et les moyens d'y répondre.
Bien des propositions nouvelles ont été acquises par l'observation, surtout dans la Théorie des nombres... Bien entendu ces calculs ne se font pas au hasard ; ils sont dirigés par une pensée, une analogie, un pressentiment que leurs résultats vérifient ou modifient. Le mathématicien attend parfois le résultat du calcul où il est plongé avec la même impatience que le physicien, le résultat d'une expérience cruciale... Une partie du génie d'invention consiste pour le mathématicien, à imaginer de nouveaux problèmes où il puisse pénétrer avec les méthodes dont il dispose... Dans les diverses sciences, la matière et les instruments diffèrent, la marche de l'invention est la même. Mêmes essais, mêmes tâtonnements, même patience active et tendue, pour ainsi dire, vers un objet qui s'éclaire parfois, mêmes espoirs trompés, même finesse et même imagination pour saisir les analogies, les liens cachés, les rapports inattendus.

Henri Poincaré : On ne parvient au général que par le particulier ; cela est vrai même dans les sciences exactes ; car, si elles procèdent dans la démonstration du général au particulier, elles doivent dans l'invention

suivre la marche inverse, comme les sciences d'observation elles-mêmes.

Emile Borel : L'invention proprement dite, l'invention vraiment féconde consiste, en mathématiques comme dans les autres sciences, dans la découverte d'un point de vue nouveau pour classer et interpréter les faits.

Michel de Rozière : Sans doute les faits sont indispensables ; mais il ne faut pas oublier cependant que des faits isolés, en quelque nombre qu'ils soient, ne sont pas de la science, pas plus que des fragments ou des molécules de marbre ne sont des statues ; ce qui la constitue, ce sont les rapports des faits entre eux, c'est leur dépendance d'un principe commun.

p. 127
Lewis Carroll (cité par J.Gattégno dans sa biographie *Lewis Carroll, une vie*, Seuil, Paris, 1974, p. 150)
Je doute fort qu'il existe dans tout l'univers de la science un domaine aussi fascinant pour l'explorateur, aussi riche en trésors cachés, aussi fertile en surprises délicieuses, que celui des mathématiques pures. Leur charme réside principalement, selon moi, dans la certitude absolue de leurs résultats ; car c'est bien ce à quoi aspire l'intellect humain, par dessus tous les trésors de l'esprit !... La plupart des autres sciences sont en perpétuel changement, les vérités sans prix d'une génération se voient traitées de paradoxes par la suivante et balayées par celle d'après, qui n'y voit que sottises et puérilités.

p. 129
Autres domaines créatifs : Somerset Maugham
Les histoires viennent à moi directement. Je suis convaincu que le subconscient effectue le travail réellement difficile. Vous créez de façon originale à partir du subconscient et ensuite, les réécritures et les révisions suivent avec le polissage et les extensions jusqu'à ce que vous soyez convaincu que vous ayez, par le travail conscient de l'esprit, fait du mieux que vous pouviez.

Concorcet : La marche de la science est lente, et s'effectue par paliers
Il est des obstacles qui ne peuvent être vaincus que par le temps, des travaux dont rien ne peut accélérer le succès et pour lesquels il faut une volonté longtemps soutenue, longtemps dirigée vers le même but, autant que des moyens vastes et les efforts combinés d'un grand nombre de savants.

p. 131
Albert Szent-Györgyi (découvreur de la vitamine C)
La condition préalable à la découverte scientifique est une société qui n'exige pas du savant d'être "utile", mais qui lui accorde la liberté nécessaire à la méditation et au travail minutieux et consciencieux sans lequel la création est impossible... Le vrai savant est prêt à supporter les privations, et si besoin est, la faim, plutôt que de se laisser dicter la direction que son travail doit prendre.

p. 132
Albert Einstein
Je sais, de par ma propre et douloureuse recherche, qu'il est difficile, dans la quête de la vérité, d'avancer avec certitude, si peu que ce soit ; il y a tant d'impasses avant d'arriver à comprendre ce qui est vraiment significatif !
Le chemin direct s'est révélé comme étant le seul praticable. La seule chose qui soit incompréhensible est d'avoir été obligé de tâtonner si longtemps avant de trouver ce qui était tout proche.

Henri Lebesgue
...Tout homme qui trouve quelque chose de vraiment important est dépassé par sa propre découverte ; il ne la comprend pas lui-même, et seulement partiellement, qu'en y réfléchissant ensuite longuement.

P. Lecomte du Noüy
Car il ne suffit pas au savant de voir. Il doit convaincre. Et pour cela, il doit s'astreindre à employer, a posteriori, les méthodes classiques ; il doit, après avoir d'un coup d'aile survolé la forêt vierge, construire la route qui permettra au touriste de se rendre au même point.

4 Avant-propos du livre *Symétrie et mathématique moderne* d'Hermann Weyl

René Descartes : Discours de la Méthode
Regulae ad directionem ingenii
Règle 10 (regula decima) :
"Ut ingenium fiat sagax, exerceri debet
Pour être intelligent, il faut travailler.
Non statim in difficilioribus
Il ne faut pas s'occuper tout de go des choses difficiles
Artes levissimas et simplicissimas
Etudier d'abord les arts les plus communs et les plus simples
Ceux surtout qui sont régis par l'ordre..."
Et quelles sont donc ces arts gymniques de l'intellect :
"ceux des ouvriers qui tissent la toile et font les tapis, ceux des femmes qui font de la broderie ou de la dentelle ainsi que toutes les combinaisons de nombres, et toutes les opérations de l'arithmétique ; tous ces arts exercent l'esprit de façon admirable".

5 Dans *Deux et deux font-ils quatre ?* De Didier Nordon

une citation d'Alain Connes p. 45
Quand on effectue un long calcul algébrique, la durée nécessaire est souvent très propice à l'élaboration dans le cerveau de la représentation mentale des concepts utilisés. C'est pourquoi l'ordinateur, qui donne le résultat d'un tel calcul en supprimant la durée, n'est pas nécessairement un progrès. On croit gagner du temps, mais le résultat brut d'un calcul sans la représentation mentale de sa signification n'est pas un progrès.

6 Dans *Pour l'honneur de l'esprit humain* de Jean Dieudonné

p. 19
Comme chez beaucoup de savants, la vie du mathématicien est dominée par une insatiable curiosité, un désir de résoudre les problèmes étudiés qui confine à la passion, et arrive à le faire presque totalement s'abstraire de la réalité ambiante ; les distractions ou bizarreries des mathématiciens célèbres n'ont pas d'autre origine. C'est que la découverte d'une démonstration ne s'obtient en général qu'après des périodes de concentration intense et soutenue qui se renouvellent parfois pendant des mois ou des années avant que le résultat cherché ne soit atteint. Gauss lui-même a reconnu avoir cherché le signe d'une expression algébrique pendant plusieurs années, et Poincaré, à qui on demandait comment il était arrivé à ses découvertes, répondait "en y pensant souvent" ; il a d'ailleurs décrit dans le détail le déroulement de ses réflexions et tentatives qui l'ont conduit à l'un de ses plus beaux résultats, la découverte des fonctions fuchsiennes.
La possibilité de disposer d'assez de temps pour se livrer à ses travaux est donc ce que recherche avant tout un mathématicien, et c'est pourquoi, depuis le XIX^e siècle, ce sont les carrières d'enseignement dans les universités ou les écoles techniques, où le nombre d'heures de cours est relativement faible et les vacances longues, qui ont leur préférence. L'importance de la rémunération n'arrive qu'en seconde ligne, et l'on a vu récemment, aux Etats-Unis entre autres, des mathématiciens abandonner des situations lucratives dans l'industrie pour revenir dans l'Université, au prix d'un sérieux abattement de salaire.

7 Alain Connes : Conférence *Le grand soir* à la Fondation Cartier

Le spectre provient de l'interaction entre l'atome et la radiation.

8 Dans *Essai sur la psychologie de l'invention dans le domaine mathématique* d'Henri Poincaré

p. 10
Une citation de Hermite : "En mathématiques, nous sommes davantage des serviteurs que des maîtres". Bien que la vérité ne nous soit pas encore connue, elle préexiste et nous impose inéluctablement le chemin que nous devons suivre sous peine de nous égarer.

p. 37
Inventer, c'est choisir.
Cette conclusion très remarquable apparaît d'autant plus frappante si nous la comparons avec ce que Paul Valéry écrit : "Il faut être deux pour inventer. L'un forme les combinaisons, l'autre choisit, reconnaît ce qu'il désire, et ce qui lui importe dans l'ensemble des produits du premier". Ce qu'on appelle "génie" est bien moins l'acte de celui-ci - l'acte qui combine - que la promptitude du second à comprendre la valeur de ce qui vient de se produire et à saisir ce produit".
On voit combien le mathématicien et le poète sont d'accord sur ce point de vue fondamental : l'invention consiste en un choix.

p. 48
Le critique littéraire Emile Faguet écrivait : "Un problème se révèle soudain quand on ne l'étudie plus et probablement parce qu'il n'est plus étudié ; quand on ne s'attend plus qu'à se reposer, à se détendre pour une courte période ; fait qui prouverait - et il est à craindre que les paresseux puissent en faire mauvais usage - que le repos est la condition de l'œuvre.

p. 49
Devons-nous alors accepter la thèse de Buffon selon laquelle le génie pourrait n'être qu'une longue patience ?

p. 51
Ceci une fois reconnu, nous ne pouvons plus penser au conscient comme étant subordonné à l'inconscient. Au contraire, il déclenche son action et définit plus ou moins la direction générale dans laquelle cet inconscient doit travailler.

p. 57
Pascal, dans *L'art de persuader*, remarque le fait évident que, de même qu'il n'est pas possible de tout démontrer, il est également impossible de tout définir, et cela pour la même raison. Il existe des idées primitives qu'il est impossible de définir.

p. 59
1) préparation
2) incubation
3) illumination (après une période de repos)
4) vérification et finition
Vérification : Le sentiment d'absolue certitude qui accompagne l'inspiration correspond en général à la réalité ; mais il peut arriver qu'il nous ait trompés. Il faut vérifier s'il en est ainsi par l'intervention de notre raison proprement dite, tâche qui appartient à notre conscient.
Finition : pour exposer les résultats avec précision.

Selon moi, importance du “bain d’idées”.

p. 60
Nous en arrivons donc à la conclusion qui semble paradoxale à laquelle, du reste, il nous faudra apporter une correction comme nous l’avons fait dans le cas de Newton que cette intervention de notre volonté, c’est-à-dire d’une des plus hautes facultés de notre âme, se produit dans une partie assez mécanique du travail, où elle est en quelque sorte subordonnée à l’inconscient, bien que le surveillant.

9 Dans *L’étrange beauté des mathématiques* de David Ruelle

p. 35
Utiliser la force brute
ou bien
Trouver une idée astucieuse qui rend le problème facile. Pour la plupart des mathématiciens, c’est la bonne méthode. Dans le cas présent, l’idée astucieuse est de comprendre que le théorème du papillon appartient à la géométrie projective plutôt qu’à la géométrie euclidienne.

p. 67
Chapitre intitulé Structures
De ce que nous avons vu, il ressort que les mathématiques possèdent une nature double. D’une part, elles peuvent être développées en utilisant un langage formel, des lois de déduction strictes et un système d’axiomes. Tous les théorèmes peuvent être obtenus et vérifiés mécaniquement. C’est ce que nous appellerons l’aspect *formel* des mathématiques. D’autre part, la pratique des mathématiques repose sur des idées, comme l’idée de Klein sur les différentes géométries. C’est ce que nous pouvons appeler l’aspect *conceptuel* ou *structurel*.
Un exemple de considération structurelle nous est apparu lors de l’étude du “théorème du papillon” au chapitre 4. Nous avons alors vu combien il est important de savoir à quel type de géométrie appartient un théorème, lorsqu’il s’agit de le démontrer. Mais le concept de géométrie projective n’est pas explicite dans les axiomes qui sont généralement utilisés pour les fondements des mathématiques. Dans quel sens la géométrie projective est-elle présente dans les axiomes de la théorie des ensembles ? Quelles sont les structures qui donnent un sens aux mathématiques ? Dans quel sens la statue est-elle présente dans le bloc de pierre avant que le ciseau du sculpteur ne l’en dégage ?
Avant de discuter les structures, il convient de regarder d’un peu plus près les *ensembles* qui jouent un rôle si fondamental dans les mathématiques modernes. Passons d’abord en revue quelques notions intuitives, quelques notations et la terminologie de base. L’ensemble $S = \{a, b, c\}$ est une collection d’objets appelés “éléments de l’ensemble S”. L’ordre dans lequel les éléments sont présentés n’a pas d’importance. Pour exprimer que a est un élément de S, on écrit $a \in S$. Les ensembles $\{a\}$ et $\{b, c\}$ sont des *sous-ensembles* de $\{a, b, c\}$. L’ensemble $\{a, b, c\}$ est fini (il contient 3 éléments), mais il existe aussi des ensembles infinis. Par exemple, l’ensemble $\{0, 1, 2, 3, ...\}$ des entiers naturels, ou l’ensemble des points sur un cercle sont des ensembles infinis. Etant donné des ensembles S et T, supposons que pour chaque élément x de S, un (unique) élément $f(x)$ de T soit donné. Nous disons alors que f est une *application* de S dans T. On peut également dire que f est une *fonction* définie sur S et avec des valeurs dans T. On peut, par exemple, définir une application de l’ensemble $\{0, 1, 2, ...\}$ des entiers naturels dans lui-même, telle que $f(x) = 2x$. D’autres applications ou fonctions des entiers naturels avec des valeurs dans les entiers naturels sont données par $f(x) = xx = x^2$ ou $f(x) = x...x = x^n$.
Le concept général de fonction (ou d’application) a émergé lentement dans l’histoire des mathématiques, mais il est au centre de notre compréhension actuelle des structures mathématiques.
Les mathématiciens ont essayé de manière répétée de définir avec précision et généralité les structures qu’ils emploient. Le programme d’Erlangen de Klein est un pas dans cette direction. Les structures considérées par Klein étaient géométriques, associées chacune à une famille d’applications : congruences (pour la géométrie euclidienne), transformations affines (pour la géométrie affine), transformations projectives, et ainsi de suite. Le très idéologique Bourbaki donne une définition des structures fondée sur les ensembles. Je vais essayer de donner une description informelle de l’idée de Bourbaki. Supposons que nous voulions comparer des objets de taille différente. Nous écrivons $a \leq b$ pour indiquer que a est inférieur ou égal à b. (Certaines conditions doivent être satisfaites, par exemple si $a \leq b$ et $b \leq c$, alors $a \leq c$). Nous voulons donc définir une structure d’ordre ($\leq$ est appelé un ordre). Pour ce faire, nous avons besoin d’un

ensemble S d'objets $a, b, \ldots$ que nous allons comparer. Ensuite, nous pouvons également introduire un autre ensemble T formé de paires d'éléments (a, b) de S : les paires pour lesquelles $a \leq b$. (Nous serons peut-être amenés à considérer également d'autres ensembles, pour imposer la condition que si $a \leq b$ et $b \leq c$, alors $a \leq c \ldots$). En bref, nous considérons un certain nombre d'ensembles S, T, dans une certaine relation (T est constitué de paires d'éléments de S) et cela définit une relation d'ordre sur l'ensemble S. D'autres structures sont définies de manière semblable sur l'ensemble S en introduisant à chaque fois divers ensembles qui se trouvent dans une relation particulière vis-à-vis de S. Supposons, par exemple, que l'ensemble S a une structure qui permet d'additionner ses éléments, c'est-à-dire que pour chaque couple d'éléments a, b, il existe un troisième élément c pour lequel nous pouvons écrire $a + b = c$. La structure à définir sur S devra prendre en considération un nouvel ensemble T constitué de triplets d'éléments de S : les triplets (a, b, c) pour lesquels $a + b = c$. Les traités de mathématiques donnent la définition de nombreuses structures comme *structure de groupe*, *topologie de Hausdorff*, etc. Ces structures sont à la base de l'algèbre, de la topologie, et des mathématiques modernes en général.

Dotons l'ensemble S d'une relation d'ordre, de même pour l'ensemble S'. Supposons que nous avons un moyen d'associer à chaque élément $a, b, \ldots$ de S un élément $a', b', \ldots$ de S'. En langage mathématique, nous dirons que nous avons une application de S dans S' envoyant les éléments $a, b, c, \ldots$ de S sur les éléments $a', b', c', \ldots$ de S'. Supposons que si $a \leq b$ alors $a' \leq b'$, c'est-à-dire que l'application conserve l'ordre. Utilisons une flèche pour indiquer cette application de S dans S' :

$$S \to S'$$

.
De manière plus générale, on écrit souvent $S \to S'$ pour indiquer le passage d'un ensemble avec une certaine structure à un ensemble qui possède une structure similaire, tout en respectant cette structure (dans l'exemple ci-dessus, c'est la structure d'ordre qui est respectée). En langage technique, la flèche est dite représenter un *morphisme* (Par exemple, si S et S' ont une structure où des éléments peuvent être additionnés, et le morphisme envoie les éléments $a, b, c, \ldots$ de S vers les éléments $a', b', c', \ldots$ de S', alors $a + b = c$ doit entraîner $a' + b' = c'$). Si nous considérons des ensembles sans structure additionnelle, les morphismes $S \to S'$ ne sont autres que les applications de S dans S'.
Une idée naturelle est de considérer maintenant tous les ensembles avec un certain type de structure et tous les morphismes correspondant : on parle alors de *catégorie*. Il y a donc une catégorie des ensembles dont les morphismes sont les applications, une catégorie des ensembles ordonnés, où les morphismes sont les applications que préservent l'ordre, une catégorie des groupes, etc. Dans cette manière de voir les choses, il est utile de pouvoir appliquer les objets d'une catégorie dans les objets d'une autre catégorie, tout en préservant les morphismes. Lorsque c'est le cas, on dit qu'on a un *foncteur* d'une catégorie vers une autre. Les catégories et les foncteurs ont été introduits vers 1950 par Eilenberg et MacLane et sont rapidement devenus des objets conceptuels importants en topologie et en algèbre. On peut considérer les catégories et les foncteurs comme la base idéologique d'une partie importante des mathématiques de la fin du XX^e siècle, utilisés de manière systématique par des mathématiciens comme Grothendieck.

En résumé, nous pouvons dire que les structures et leurs relations apparaissent comme une préoccupation constante, en arrière-plan idéologique dans d'importants domaines des mathématiques de la fin du XX^e siècle. Certaines questions seront systématiquement posées, certaines constructions seront systématiquement tentées. Dans une certaine mesure, nous avons donc répondu à la question de découvrir les éléments conceptuels de base des mathématiques. La réponse est donnée en terme de structures, de morphismes et peut-être de catégories, de foncteurs et de concepts apparentés. Et la qualité de cette réponse peut être jugée par la richesse des résultats obtenus.
A ce point de notre parcours, il me faut corriger une impression fausse que je viens peut-être de donner, selon laquelle la pensée mathématique d'aujourd'hui serait dominée par les catégories, les foncteurs et ainsi de suite. Nous pouvons seulement dire qu'il existe une tendance générale à vouloir clarifier les aspects conceptuels et à ne pas se contenter de calculer sans comprendre. Cependant, les considérations structurelles peuvent être minimales. Pour donner un exemple de mathématiques d'un style différent, je voudrais mentionner le travail de Paul Erdös (le nom est hongrois et se prononce "Erdeuche"). Erdös était un mathématicien très atypique, qui voyageait sans cesse et ne dépendait pas d'une institution fixe. Sa contribution aux mathématiques est variée et importante. Il avait la très belle idée qu'il existe un Livre "dans lequel Dieu conserve les démonstrations parfaites des théorèmes mathématiques" (accessoirement, Erdös ne croyait pas en Dieu qu'il appelait *Le Fasciste suprême)*. Sous l'influence d'Erdös, une approximation fascinante du Livre a été écrite, intitulée *Proofs from the Book* ("Démonstrations ex-

traites du Livre"). Cet ouvrage est d'une lecture relativement facile et donne une vue résolument non bourbakiste des mathématiques. Les considérations structurales n'en sont pas absentes mais elles restent à l'arrière-plan. Paul Erdös était un de ces mathématiciens qui s'acharnent à trouver la solution d'un problème, mathématiciens très différents des constructeurs de théories comme André Weyl ou Alexandre Grothendieck. Pour bien résoudre des problèmes, il faut aussi être un mathématicien conceptuel, et avoir une bonne compréhension des structures. Mais les structures restent des outils pour celui qui résoud des problèmes, et non l'objet principal de son étude.

Infinitude de l'ensemble des nombres premiers jumeaux

Denise Chemla

23 mai 2012

On appelle nombres premiers jumeaux deux nombres premiers qui diffèrent de 2.

3 et 5 sont des nombres premiers jumeaux. 17 et 19 en sont également.

Dans la suite, on dénommera nombres premiers jumeaux *cadets* les nombres premiers qui ont un jumeau qui leur est strictement supérieur (pour les exemples cités, ce sont 3 et 17 qui sont des nombres premiers jumeaux *cadets*).

Pour prouver que l'ensemble des nombres premiers jumeaux cadets est infini, on va utiliser un argument similaire à celui appelé "diagonale de Cantor".

Supposons que l'ensemble des nombres premiers jumeaux cadets est fini. Notons le $\mathcal{C}adets = \{c_1, \ldots, c_n\}$. A chacun des éléments de cet ensemble $\mathcal{C}adets = \{c_1, \ldots, c_n\}$, on associe par une bijection l'ensemble de ses restes modulo les nombres premiers compris entre 2 et $c_n + 2$. Puis on invente un ensemble de restes selon les modules premiers compris entre 2 et $c_n + 2$ différent de tous les ensembles de restes déjà recensés. Cet ensemble de restes correspond à un nombre qui n'a pas été recensé alors qu'il aurait dû l'être dans l'ensemble fini des jumeaux cadets $\mathcal{C}adets$ initial. On a ainsi prouvé que l'ensemble des nombres premiers jumeaux cadets n'est pas fini et a fortiori, qu'il en est de même de l'ensemble des nombres premiers jumeaux.

Le nombre premier jumeau cadet 101 est codé par l'ensemble de restes suivant selon les modules compris entre 2 et 103 :

$\{1, 2, 1, 3, 2, 10, 16, 6, 9, 14, 8, 27, 19, 15, 7, 48, 42, 40, 34, 30, 28, 22, 18, 12, 4, 0, 101\}$

On notera que tous les nombres premiers jumeaux cadets sauf 3 sont congrus à 1 (mod 2) et à 2 (mod 3) (3 quant à lui est congru à 0 (mod 3)) ; d'une part, ils sont impairs ; d'autre part, ils doivent être congrus à 2 (mod 3) (sauf 3) car dans le cas contraire, soit, étant congrus à 0 (mod 3), ils ne seraient pas premiers, soit, étant congru à 1 (mod 3), leur *aîné* ne serait pas premier étant quant à lui congru à 0 (mod 3) puisque $1 + 2 \equiv 0$ (mod 3) et dans ces deux cas, ils ne pourraient pas être éléments de l'ensemble des nombres premiers jumeaux cadets.

Pour inventer un nouveau nombre premier jumeau cadet dont l'ensemble des restes n'appartient pas à l'ensemble fini des ensembles de restes déjà recensés,

on procède en "perturbant" une diagonale qui assure la "nouveauté" du nombre premier jumeau cadet fabriqué.

Le tableau suivant contient les restes associés aux nombres premiers jumeaux cadets, en nombre fini, qui appartiennent à $\mathcal{C}adets$.

Nous devons maintenant inventer un nouvel ensemble de restes, non encore recensé, par la méthode de la diagonale de Cantor, en modifiant les restes modulaires qui se trouvent sur une diagonale du tableau.

	2	3	5	7	11	...	$c_n + 2$
$c_1 = 3$	1	0	$\boxed{\mathrm{r}_{c_1,5}}$				
$c_2 = 5$	1	2		$\boxed{\mathrm{r}_{c_2,7}}$			
$c_3 = 11$	1	2			$\boxed{\mathrm{r}_{c_3,11}}$		
						...	
c_n	1	2					$\boxed{\mathrm{r}_{c_n,c_n+2}}$

Le plus petit nombre premier jumeau cadet 3 est congru à 0 (mod 3), les autres restes nuls se trouvent sur la deuxième diagonale descendante du tableau qui contient des restes modulaires de la forme $r_{i,i}$. La diagonale utilisée pour appliquer l'argument de Cantor est la troisième diagonale descendante, dont on a encadré les éléments dans le tableau.

Pour "perturber la diagonale", on change chacun des restes modulaires qui lui appartient par un autre reste modulaire selon le module considéré, le nouveau reste choisi devant respecter deux contraintes seulement : ne pas être nul et ne pas être égal à $p - 2$ quand on traite le module premier p (pour assurer que l'aîné de ce nombre premier est bien un nombre premier également).

On a inventé un ensemble de restes qui n'était pas déjà une ligne du tableau. Si notre ensemble d'ensembles de restes avait été complet, il aurait dû contenir cette nouvelle ligne or il ne la contient pas. Cela est contradictoire avec notre hypothèse de finitude de l'ensemble des nombres premiers jumeaux. L'idée du codage entraîne la contradiction [1]. On s'est appuyé pour pouvoir construire le "nouvel ensemble de restes" sur l'*Axiome du choix* qui a pour conséquence qu'on peut toujours choisir dans des ensembles d'entiers naturels contenant chacun 5 nombres ou plus un nombre dans chaque ensemble, en respectant la contrainte que, dans chacun des ensembles, l'élément choisi soit non nul et différent d'une valeur donnée.

[1] Cet ensemble de restes est le codage d'un nombre premier jumeau cadet qui n'appartient pas à l'ensemble des jumeaux cadets que l'on a supposé fini. La constitution même de ce nouvel ensemble de restes nous garantit que c'est un nombre premier jumeau cadet qui est inférieur à $(c_n + 2)^2$ que le théorème des restes chinois nous permet de calculer : aucun de ses restes selon les modules premiers compris entre 2 et $c_n + 2$ n'est nul et dans la mesure où aucun de ses restes selon un module premier p n'est égal à $p - 2$ (on s'est assuré de cela en construisant le nouvel ensemble de restes par perturbation de la bonne diagonale du tableau), ce nombre augmenté de 2 est premier également puisqu'il n'a aucun reste nul selon les nombres premiers considérés.

Etude élémentaire de la Conjecture de Goldbach

Denise Chemla

26/5/2012

La Conjecture de Goldbach (7 juin 1742) stipule que tout nombre pair supérieur ou égal à 6 est la somme de deux nombres premiers impairs. Si on note $\mathbb{P}^*$ l'ensemble des nombres premiers impairs*, on peut écrire la Conjecture de Goldbach ainsi :

$$\forall\, n \in 2\mathbb{N}\backslash\{0,2,4\},\ \exists\, p \in \mathbb{P}^*,\ p \leq n/2,\ \exists\, q \in \mathbb{P}^*,\ q \geq n/2,\ \ n = p+q$$

On appelle *décomposition de Goldbach* de n une telle somme $p+q$. p et q sont dits *décomposants de Goldbach* de n.
La Conjecture de Goldbach a été vérifiée par ordinateur jusqu'à 4.10^{18}†.

Dans la suite, n étant donné, on note :

- $\mathrm{P}_1^*(n) = \{x \in \mathbb{P}^* / x \leq \frac{n}{2}\}$,

- $\mathrm{P}_2^*(n) = \{x \in \mathbb{P}^* / x \leq \sqrt{n}\}$.

On peut reformuler la Conjecture de Goldbach par l'énoncé suivant :

$$\forall\, n \in 2\mathbb{N}\backslash\{0,2,4\},\ \exists\, p \in \mathbb{P}_1^*(n),\ \forall\, m \in \mathbb{P}_2^*(n),\ p \not\equiv n\ (mod\ m).$$

En effet,

$\forall\, n \in 2\mathbb{N}\backslash\{0,2,4\},\ \exists\, p \in \mathbb{P}_1^*(n),\ \forall\, m \in \mathbb{P}_2^*(n),$

$$\begin{aligned} & p \not\equiv n\ (mod\ m) \\ \Leftrightarrow\ & n - p \not\equiv 0\ (mod\ m) \\ \Leftrightarrow\ & n - p\ premier. \end{aligned}$$

1 Etude d'exemples

1.1 Exemple 1 : Pourquoi 19 est-il le plus petit décomposant de Goldbach de 98 ?

$$\begin{array}{ll} 98 \equiv 3\ (mod\ 5) & (98-3 = 95\ et\ 5|95) \\ 98 \equiv 5\ (mod\ 3) & (98-5 = 93\ et\ 3|93) \\ 98 \equiv 7\ (mod\ 7) & (98-7 = 91\ et\ 7|91) \\ 98 \equiv 11\ (mod\ 3) & (98-11 = 87\ et\ 3|87) \\ 98 \equiv 13\ (mod\ 5) & (98-13 = 85\ et\ 5|85) \\ 98 \equiv 17\ (mod\ 3) & (98-17 = 81\ et\ 3|81) \end{array}$$

$$\begin{array}{ll} 98 \not\equiv 19\ (mod\ 3) & (98-19 = 79\ et\ 3 \not| 79) \\ 98 \not\equiv 19\ (mod\ 5) & (98-19 = 79\ et\ 5 \not| 79) \\ 98 \not\equiv 19\ (mod\ 7) & (98-19 = 79\ et\ 7 \not| 79) \end{array}$$

Chacun des nombres premiers impairs compris entre 3 et 17 est congru à 98 selon un module premier impair appartenant à $\mathbb{P}_2^*(98)$ donc aucun de ces nombres ne peut être un décomposant de Goldbach de 98.

Par contre, comme requis : $\forall\, m \in \mathbb{P}_2^*(98),\ 19 \not\equiv 98\ (mod\ m)$.
Donc 19 est un décomposant de Goldbach de 98. Effectivement, $98 = 19 + 79$ avec 19 et 79 premiers.

*$\mathbb{P}^* = \{p_1 = 3, p_2 = 5, p_3 = 7, p_4 = 11, \ldots\}$
†par Oliveira e Silva le 4.4.2012

1.2 Exemple 2 : Pourquoi 3 est-il un décomposant de Goldbach de 40 ?

Dans le tableau suivant sont présentées les différentes classes d'équivalence des corps finis $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$ et $\mathbb{Z}/11\mathbb{Z}$.

$\mathbb{Z}/3\mathbb{Z}$	$\overline{0}$	$\overline{1}$	$\overline{2}$								
$\mathbb{Z}/5\mathbb{Z}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$						
$\mathbb{Z}/7\mathbb{Z}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$				
$\mathbb{Z}/11\mathbb{Z}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$

Dans chaque corps fini, on a coloré en rose la classe d'appartenance de 3, et on a coloré en bleu ciel la classe d'appartenance de 40, le nombre pair à décomposer.

Dans la mesure où $\forall\, m \in \mathbb{P}_2^*(40),\ 3 \not\equiv 40\ (mod\ m)$, 3 est un décomposant de Goldbach de 40. En effet, 40=3+37 avec 3 et 37 premiers.

1.3 Exemple 3 : cherchons les décomposants de Goldbach d'entiers naturels pairs qui sont $\equiv 2\ (mod\ 3)$ et $\equiv 3\ (mod\ 5)$ et $\equiv 3\ (mod\ 7)$.

Ces nombres dont on cherche des décomposants de Goldbach sont des entiers naturels de la forme *210k+38* (conséquemment au Théorème des restes chinois que l'on présentera plus loin).

On a vu que des nombres premiers impairs p qui sont $\not\equiv 2\ (mod\ 3)$ et $\not\equiv 3\ (mod\ 5)$ et $\not\equiv 3\ (mod\ 7)$ peuvent être des décomposants de Goldbach de ces nombres.
Si on omet le cas des "petits nombres premiers" (i.e. les cas de congruence à 0 selon un module et un seul),

- p *doit être* $\equiv 1\ (mod\ 3)$,
- p *doit être* $\equiv 1$ *ou* 2 *ou* $4\ (mod\ 5)$,
- p *doit être* $\equiv 1$ *ou* 2 *ou* 4 *ou* 5 *ou* $6\ (mod\ 7)$.

En combinant les différentes possibilités, on obtient :

$$
\begin{array}{llll}
1\ (mod\ 3)\ 1\ (mod\ 5)\ 1\ (mod\ 7) & \rightarrow & 210\mathrm{k}+1 \\
1\ (mod\ 3)\ 1\ (mod\ 5)\ 2\ (mod\ 7) & \rightarrow & 210\mathrm{k}+121 \\
1\ (mod\ 3)\ 1\ (mod\ 5)\ 4\ (mod\ 7) & \rightarrow & 210\mathrm{k}+151 \\
1\ (mod\ 3)\ 1\ (mod\ 5)\ 5\ (mod\ 7) & \rightarrow & 210\mathrm{k}+61 \\
1\ (mod\ 3)\ 1\ (mod\ 5)\ 6\ (mod\ 7) & \rightarrow & 210\mathrm{k}+181 \\
1\ (mod\ 3)\ 2\ (mod\ 5)\ 1\ (mod\ 7) & \rightarrow & 210\mathrm{k}+127 \\
1\ (mod\ 3)\ 2\ (mod\ 5)\ 2\ (mod\ 7) & \rightarrow & 210\mathrm{k}+37 \\
1\ (mod\ 3)\ 2\ (mod\ 5)\ 4\ (mod\ 7) & \rightarrow & 210\mathrm{k}+67 \\
1\ (mod\ 3)\ 2\ (mod\ 5)\ 5\ (mod\ 7) & \rightarrow & 210\mathrm{k}+187 \\
1\ (mod\ 3)\ 2\ (mod\ 5)\ 6\ (mod\ 7) & \rightarrow & 210\mathrm{k}+97 \\
1\ (mod\ 3)\ 4\ (mod\ 5)\ 1\ (mod\ 7) & \rightarrow & 210\mathrm{k}+169 \\
1\ (mod\ 3)\ 4\ (mod\ 5)\ 2\ (mod\ 7) & \rightarrow & 210\mathrm{k}+79 \\
1\ (mod\ 3)\ 4\ (mod\ 5)\ 4\ (mod\ 7) & \rightarrow & 210\mathrm{k}+109 \\
1\ (mod\ 3)\ 4\ (mod\ 5)\ 5\ (mod\ 7) & \rightarrow & 210\mathrm{k}+19 \\
1\ (mod\ 3)\ 4\ (mod\ 5)\ 6\ (mod\ 7) & \rightarrow & 210\mathrm{k}+139
\end{array}
$$

Voici quelques exemples de décomposants de Goldbach appartenant aux progressions arithmétiques trouvées pour quelques nombres de la progression arithmétique *210k+38*.

248 : 7 19 37 67 97 109
458 : 19 37 61 79 109 127 151 181 229 (*double de premier*)
668 : 7 37 61 67 97 127 181 211 229 271 331
878 : 19 67 109 127 139 151 271 277 307 331 337 379 421 439 (*double de premier*)
1088 : 19 37 67 79 97 151 181 211 229 277 331 337 349 379 397 457
487 541
1298 : 7 19 61 67 97 127 181 211 229 277 307 331 379 421 439
487 541 547 571 607

2 Objectif : aboutir à une contradiction à partir de l'hypothèse qu'un entier naturel pair ne vérifie pas la Conjecture de Goldbach

On cherche à démontrer l'impossibilité de l'existence d'un entier pair qui ne vérifie pas la Conjecture de Goldbach. Cela correspond au fait que l'hypothèse :

$$\exists\, x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},\ x \text{ ne vérifie pas la Conjecture de Goldbach}$$

permet d'aboutir à une contradiction.

Mais :

$$\begin{aligned}
&\exists\, x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},\ x \text{ ne vérifie pas la Conjecture de Goldbach}\\
\Leftrightarrow\ &\exists\, x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},\ \forall\, p \in \mathbb{P}_1^*(x),\ x-p \text{ composé}\\
\Leftrightarrow\ &\exists\, x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},\ \forall\, p \in \mathbb{P}_1^*(x),\ \exists\, m \in \mathbb{P}_2^*(x),\ x-p \equiv 0\ (mod\ m)\\
\Leftrightarrow\ &\exists\, x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},\ \forall\, p \in \mathbb{P}_1^*(x),\ \exists\, m \in \mathbb{P}_2^*(x),\ x \equiv p\ (mod\ m)
\end{aligned}$$

Par expansion des quantificateurs, on obtient :

$$\begin{aligned}
&p_1,\ldots,p_k \in \mathbb{P}_1^*(x),\ m_1,\ldots,m_l \in \mathbb{P}_2^*(x).\\
&\exists\, x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},\ \forall\, i \in [1,k],\ \exists\, j \in [1,l],\ x, \equiv p_i\ (mod\ m_j).
\end{aligned}$$

Ecrivons toutes les congruences :

$$\begin{aligned}
&p_1,\ldots,p_k \in \mathbb{P}_1^*(x),\ m_{j_1},\ldots,m_{j_k} \in \mathbb{P}_2^*(x).\\
&\exists\, x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},
\end{aligned}$$

$$\mathcal{S}_0 \begin{cases} x \equiv p_1\ (mod\ m_{j_1}) \\ x \equiv p_2\ (mod\ m_{j_2}) \\ \ldots \\ x \equiv p_k\ (mod\ m_{j_k}) \end{cases}$$

Il est important de noter que les modules sont des entiers naturels premiers impairs qui ne sont pas forcément tous différents.

3 Le Théorème des restes chinois

3.1 Rappels

On appelle progression arithmétique un ensemble d'entiers naturels de la forme $ax+b$ avec $a \in \mathbb{N}^*,\ b \in \mathbb{N}$ et $x \in \mathbb{N}$.
Un système de congruences ne contenant pas de contradiction se résoud par le Théorème des restes chinois. Le Théorème des restes chinois établit un isomorphisme entre $\mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_k\mathbb{Z}$ et $\mathbb{Z}/\prod_{i=1}^{k} m_i\mathbb{Z}$ si et seulement si les m_i sont deux à deux premiers entre eux ($\forall\, m_i \in \mathbb{N}^*,\ \forall\, m_j \in \mathbb{N}^*,\ (m_i, m_j) = 1$).
Le Théorème des restes chinois établit une bijection entre l'ensemble des systèmes de congruences non-contradictoires et l'ensemble des progressions arithmétiques.

On cherche l'ensemble des solutions du systèmes de congruences S suivant, de modules premiers tous différents :

$$\begin{cases} x \equiv r_1 \ (mod\ m_1) \\ x \equiv r_2 \ (mod\ m_2) \\ \dots \\ x \equiv r_k \ (mod\ m_k) \end{cases}$$

Posons $M = \prod_{i=1}^{k} m_i$.

Calculons : • $M_1 = M/m_1, M_2 = M/m_2, \dots, M_k = M/m_k$.

• $d_1, d_2, \dots, d_k$ tels que $\begin{cases} d_1.M_1 \equiv 1 \ (mod\ m_1) \\ d_2.M_2 \equiv 1 \ (mod\ m_2) \\ \dots \\ d_k.M_k \equiv 1 \ (mod\ m_k) \end{cases}$

La solution de S est $\boxed{\text{x} \equiv \Sigma_{i=1}^{k} r_i.d_i.M_i \ (mod\ M)}$.

3.2 Exemple 1

Cherchons à résoudre le système de congruences :

$$\begin{cases} x \equiv 1 \ (mod\ 3) \\ x \equiv 3 \ (mod\ 5) \\ x \equiv 5 \ (mod\ 7) \end{cases}$$

On pose $M = 3.5.7 = 105$.
$M_1 = M/3 = 105/3 = 35, \quad 35.y_1 \equiv 1 \ (mod\ 3), \quad y_1 = 2.$
$M_2 = M/5 = 105/5 = 21, \quad 21.y_2 \equiv 1 \ (mod\ 5), \quad y_2 = 1.$
$M_3 = M/7 = 105/7 = 15, \quad 15.y_3 \equiv 1 \ (mod\ 7), \quad y_3 = 1.$

$x \equiv r_1.M_1.y_1 + r_2.M_2.y_2 + r_3.M_3.y_3$
$\equiv 1.35.2 + 3.21.1 + 5.15.1 = 70 + 63 + 75 = 208 = 103 \ (mod\ 105)$
qui sont les nombres de la suite : $103, 208, 313, \dots,$
i.e. de la progression arithmétique : *105k+103*.

3.3 Exemple 2

Si on avait eu à résoudre presque le même système, mais avec une congruence en moins :

$$\begin{cases} x \equiv 3 \ (mod\ 5) \\ x \equiv 5 \ (mod\ 7) \end{cases}$$

On pose $M' = 5.7 = 35$.
$M'_1 = M'/5 = 7, \quad 7.y'_1 \equiv 1 \ (mod\ 5), \quad y'_1 = 3.$
$M'_2 = M'/7 = 5, \quad 5.y'_2 \equiv 1 \ (mod\ 7), \quad y'_2 = 3.$

$x \equiv r_1.M_1.y_1 + r_2.M_2.y_2$
$\equiv 3.3.7 + 5.3.5 = 63 + 75 = 138 = 33 \ (mod\ 35)$
qui sont les nombres de la suite : $33, 68, \underline{103}, 138, 173, \underline{208}, 243, \dots,$
i.e. de la progression arithmétique : *35k+33*

3.4 Puissance de la relation de congruence $\equiv$

La relation de congruence, inventée par Gauss, est une relation d'équivalence.

$$\frac{\begin{array}{c} a \equiv b \\ c \equiv d \end{array}}{\begin{array}{c} a + c \equiv b + d \\ ac \equiv bd \end{array}}$$

Comparons la résolution des deux systèmes :

$$\text{A} : \begin{cases} x \equiv 3 \ (mod\ 5) \\ x \equiv 5 \ (mod\ 7) \end{cases} \qquad \text{B} : \begin{cases} x \equiv 13 \ (mod\ 5) \\ x \equiv 5 \ (mod\ 7) \end{cases}$$

$$A : x \equiv 3.3.7 + 5.3.5 = 63 + 75 = 138 = 33 \ (mod\ 35)$$
$$B : x \equiv 13.3.7 + 5.3.5 = 273 + 75 = 348 = 33 \ (mod\ 35)$$

Comme 3 et 13 sont congrus (mod 5), on aboutit par congruence (mod 35) à la même progression arithmétique qui est solution des deux systèmes.

3.5 Que fait la bijection fournie par le Théorème des Restes Chinois ?

Le Théorème des restes chinois associe à tout système de congruences non-contradictoire de modules premiers une progression arithmétique.

Appelons E l'ensemble des systèmes de congruences de modules premiers. Appelons E' l'ensemble des progressions arithmétiques.

$$\begin{array}{ll} E & \to E' \\ sc_1 & \mapsto pa_1 \\ sc_2 & \mapsto pa_2 \\ sc_1 \wedge sc_2 & \mapsto pa_1 \cap pa_2. \end{array}$$

De plus,

$$(sc_1 \Rightarrow sc_2) \quad \Leftrightarrow (pa_1 \subset pa_2).$$

Une progression arithmétique étant une partie de $\mathbb{N}$ admet un plus petit élément. On choisira dans la suite de représenter une progression arithmétique par le plus petit entier naturel lui appartenant.

Si E et E' sont deux progressions arithmétiques, $E \subset E' \Rightarrow n' \leq n$

On appelle *"treillis"* un ensemble E muni d'une relation d'ordre partiel et tel que :

$$\forall\ a \in E,\ \forall\ b \in E,\ \{a, b\} \text{ admet une borne inférieure et une borne supérieure.}$$

L'ensemble des systèmes de congruences de modules tous premiers est un treillis muni d'un ordre partiel (basé sur la relation d'*implication logique* ($\Rightarrow$)).

L'ensemble des progressions arithmétiques est un treillis muni d'un ordre partiel (basé sur la relation d'*inclusion ensembliste* ($\subset$)).

3.6 Observons plus finement la bijection intervenant dans le *Théorème des Restes Chinois*

Voyons le résultat de l'application de la bijection (qu'on appellera trc) du Théorème des Restes Chinois au produit cartésien $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Les images sont des classes d'équivalence de $\mathbb{Z}/15\mathbb{Z}$.

$(0,0) \mapsto 0$
$(0,1) \mapsto 6$
$(0,2) \mapsto 12$
$(0,3) \mapsto 3$
$(0,4) \mapsto 9$
$(1,0) \mapsto 10$
$(1,1) \mapsto 1$
$(1,2) \mapsto 7$
$(1,3) \mapsto 13$
$(1,4) \mapsto 4$
$(2,0) \mapsto 5$
$(2,1) \mapsto 11$
$(2,2) \mapsto 2$
$(2,3) \mapsto 8$
$(2,4) \mapsto 14$

Dans ce tableau, la ligne $(1,3) \mapsto 13$ doit se lire "l'ensemble des nombres congrus à 1 (*mod* 3) et à 3 (*mod* 5) est égal à l'ensemble des nombres congrus à 13 (*mod* 15)". Il est à noter que la même ligne pourrait également se lire "13 est congru à 1 (*mod* 3) et à 3 (*mod* 5)"[‡].

Etudions maintenant la bijection qui envoie $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ sur $\mathbb{Z}/105\mathbb{Z}$

$(0,0,0) \mapsto 0$	$(0,1,0) \mapsto 21$	$(0,2,0) \mapsto 42$	$(0,3,0) \mapsto 63$	$(0,4,0) \mapsto 84$
$(0,0,1) \mapsto 15$	$(0,1,1) \mapsto 36$	$(0,2,1) \mapsto 57$	$(0,3,1) \mapsto 78$	$(0,4,1) \mapsto 99$
$(0,0,2) \mapsto 30$	$(0,1,2) \mapsto 51$	$(0,2,2) \mapsto 72$	$(0,3,2) \mapsto 93$	$(0,4,2) \mapsto 9$
$(0,0,3) \mapsto 45$	$(0,1,3) \mapsto 66$	$(0,2,3) \mapsto 87$	$(0,3,3) \mapsto 3$	$(0,4,3) \mapsto 24$
$(0,0,4) \mapsto 60$	$(0,1,4) \mapsto 81$	$(0,2,4) \mapsto 102$	$(0,3,4) \mapsto 18$	$(0,4,4) \mapsto 39$
$(0,0,5) \mapsto 75$	$(0,1,5) \mapsto 96$	$(0,2,5) \mapsto 12$	$(0,3,5) \mapsto 33$	$(0,4,5) \mapsto 54$
$(0,0,6) \mapsto 90$	$(0,1,6) \mapsto 6$	$(0,2,6) \mapsto 27$	$(0,3,6) \mapsto 48$	$(0,4,6) \mapsto 69$
$(1,0,0) \mapsto 70$	$(1,1,0) \mapsto 91$	$(1,2,0) \mapsto 7$	$(1,3,0) \mapsto 28$	$(1,4,0) \mapsto 49$
$(1,0,1) \mapsto 85$	$(1,1,1) \mapsto 1$	$(1,2,1) \mapsto 22$	$(1,3,1) \mapsto 43$	$(1,4,1) \mapsto 64$
$(1,0,2) \mapsto 100$	$(1,1,2) \mapsto 16$	$(1,2,2) \mapsto 37$	$(1,3,2) \mapsto 58$	$(1,4,2) \mapsto 79$
$(1,0,3) \mapsto 10$	$(1,1,3) \mapsto 31$	$(1,2,3) \mapsto 52$	$(1,3,3) \mapsto 73$	$(1,4,3) \mapsto 94$
$(1,0,4) \mapsto 25$	$(1,1,4) \mapsto 46$	$(1,2,4) \mapsto 67$	$(1,3,4) \mapsto 88$	$(1,4,4) \mapsto 4$
$(1,0,5) \mapsto 40$	$(1,1,5) \mapsto 61$	$(1,2,5) \mapsto 82$	$(1,3,5) \mapsto 103$	$(1,4,5) \mapsto 19$
$(1,0,6) \mapsto 55$	$(1,1,6) \mapsto 76$	$(1,2,6) \mapsto 97$	$(1,3,6) \mapsto 13$	$(1,4,6) \mapsto 34$
$(2,0,0) \mapsto 35$	$(2,1,0) \mapsto 56$	$(2,2,0) \mapsto 77$	$(2,3,0) \mapsto 98$	$(2,4,0) \mapsto 14$
$(2,0,1) \mapsto 50$	$(2,1,1) \mapsto 71$	$(2,2,1) \mapsto 92$	$(2,3,1) \mapsto 8$	$(2,4,1) \mapsto 29$
$(2,0,2) \mapsto 65$	$(2,1,2) \mapsto 86$	$(2,2,2) \mapsto 2$	$(2,3,2) \mapsto 23$	$(2,4,2) \mapsto 44$
$(2,0,3) \mapsto 80$	$(2,1,3) \mapsto 101$	$(2,2,3) \mapsto 17$	$(2,3,3) \mapsto 38$	$(2,4,3) \mapsto 59$
$(2,0,4) \mapsto 95$	$(2,1,4) \mapsto 11$	$(2,2,4) \mapsto 32$	$(2,3,4) \mapsto 53$	$(2,4,4) \mapsto 74$
$(2,0,5) \mapsto 5$	$(2,1,5) \mapsto 26$	$(2,2,5) \mapsto 47$	$(2,3,5) \mapsto 68$	$(2,4,5) \mapsto 89$
$(2,0,6) \mapsto 20$	$(2,1,6) \mapsto 41$	$(2,2,6) \mapsto 62$	$(2,3,6) \mapsto 83$	$(2,4,6) \mapsto 104$

Dans chaque case, on a coloré l'élément minimum de la case, sur lequel on peut imaginer que "se projettent" les nombres plus grands de cette case lorsqu'on supprime des congruences du système leur correspondant. On remarque qu'en appliquant la fonction *Succ* de l'Arithmétique de Peano (en ajoutant (1,1) récursivement à partir de (0,0)), on balaye toutes les cases du tableau une par une en parcourant des diagonales descendantes (et en allant dans la case en haut de la colonne ou dans la case à l'extrême gauche de la ligne lorsque la case d'arrivée se trouve être à l'extérieur du tableau).

On comprend aisément que les résultats observés sur le produit des 3 corps finis $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$ se généralisent si l'on considère des produits cartésiens d'autant de corps finis de module premier qu'on voudra.

3.7 La bijection *trc_restreint* (ou image minimum par *trc*)

On définit la bijection *trc_restreint* comme la bijection qui à un système de congruences associe **le plus petit entier naturel** de la progression arithmétique que lui associe le Théorème des restes chinois.

Il y a une conséquence importante au fait que *trc* (et *trc_restreint*) soient des bijections : la bijection *trc_restreint* associant à chaque système de congruence de modules premiers impairs qui sont des m_i tous différents, un nombre de la partie finie de $\mathbb{N}$ compris entre 0 et $\prod_{i=1}^{k} m_i$, si $sc_1 \Rightarrow sc_2$ et $sc_1 \neq sc_2$ alors la solution du système de congruences sc_1 (l'image de sc_1 par la bijection *trc_restreint*) est strictement supérieure à la solution du système de congruences sc_2.

3.8 Un exemple de l'image par la bijection *trc_restreint* d'un n-uplet et des n-uplets qui sont ses "projetés" selon certaines coordonnées

L'entier naturel 94 est compris entre $3.5 = 15$ et $3.5.7 = 105$. Etudions les "projetés" du triplet $(1,4,3)$ appartenant au produit cartésien $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ sur chacune de ses coordonnées.

[‡]On peut considérer que cette propriété correspond à une sorte de "fractalité" de l'ensemble des entiers, ou "auto-similarité" qui fait qu'une même propriété se retrouve au niveau des éléments et au niveau des ensembles d'éléments de $\mathbb{N}$.

$$\begin{aligned} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} &\to \mathbb{N} \\ (1,4,3) &\mapsto 94 \end{aligned}$$

$$\begin{aligned} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} &\to \mathbb{N} \\ (1,4) &\mapsto 4 \end{aligned}$$

$$\begin{aligned} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} &\to \mathbb{N} \\ (1,3) &\mapsto 10 \end{aligned}$$

$$\begin{aligned} \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} &\to \mathbb{N} \\ (4,3) &\mapsto 24 \end{aligned}$$

94 a trois images qui lui sont strictement inférieures par la bijection *trc_restreint*. 94 se projette dans des nombres strictement plus petits que lui parce que $3.5 < 3.7 < 5.7 < 94 < 3.5.7$.

4 Descente infinie de Fermat

4.1 Rappels

Utiliser la méthode de la Descente infinie de Fermat pour prouver la Conjecture de Goldbach consiste à démontrer que si un nombre ne vérifiait pas la Conjecture de Goldbach, il y en aurait un plus petit qui ne la vérifierait pas non plus et ainsi de proche en proche, jusqu'à atteindre des nombres si petits qu'on sait qu'ils vérifient la Conjecture.

La méthode de la Descente infinie de Fermat découle du fait qu'il n'existe pas de suite infinie strictement décroissante d'entiers naturels. Le mode de raisonnement sur lequel se base la Descente Infinie de Fermat est le raisonnement par l'absurde :

- on suppose que x est le plus petit entier tel que P(x) ;
- on montre qu′alors P(x') avec x' <x ;
- on a abouti à une contradiction.

Si $P(n)$ pour un entier naturel n donné, il existe une partie non vide de $\mathbb{N}$ contenant un élément qui vérifie la propriété P. Cette partie admet un plus petit élément. En l'occurrence, la propriété P consiste à ne pas vérifier le Conjecture de Goldbach.

On rappelle qu'on cherche à aboutir à une contradiction à partir de l'hypothèse :

$p_1, \ldots, p_k \in \mathbb{P}_1^*(x),\ m_{j_1}, \ldots, m_{j_k} \in \mathbb{P}_2^*(x).$
$\exists\, x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},$

$$\mathcal{S}_0 \begin{cases} x \equiv p_1 \ (mod\ m_{j_1}) \\ x \equiv p_2 \ (mod\ m_{j_2}) \\ \ldots \\ x \equiv p_k \ (mod\ m_{j_k}) \end{cases}$$

Il est important de se rappeler que certains modules peuvent être égaux.

4.2 Première étape

Transformons le système de façon à ordonner les modules selon un ordre croissant et à éliminer les redondances.

$p'_1, \ldots, p'_k \in \mathbb{P}_1^*(x),\ n_{j_1}, \ldots, n_{j_k} \in \mathbb{P}_2^*(x).$
$\exists \quad x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18},$

$$\mathcal{S} \begin{cases} x \equiv p'_1 \ (mod\ n_{j_1}) \\ x \equiv p'_2 \ (mod\ n_{j_2}) \\ \ldots \\ x \equiv p'_k \ (mod\ n_{j_k}) \end{cases}$$

$\mathcal{S}$ a pour image d par la bijection *trc_restreint*.

4.3 D'où peut provenir la contradiction ?

Elle peut provenir du principe de Descente infinie de Fermat.

On sait que la bijection *trc_restreint* fournit comme solution de $\mathcal{S}$ l'entier naturel d qui est le plus petit entier de la progression arithmétique associée à $\mathcal{S}$ par le Théorème des Restes Chinois.

Le système $\mathcal{S}$ est tel que d ne vérifie pas la Conjecture de Goldbach.

On cherche un système de congruences $\mathcal{S}'$, impliqué par $\mathcal{S}$ et $\neq$ de $\mathcal{S}$, à qui soit associé par la bijection *trc_restreint* un entier naturel $d' < d$, avec d' ne vérifie pas la Conjecture de Goldbach non plus.

Considérons un système de congruences $\mathcal{S}'$ constitué d'un certain nombre de congruences de $\mathcal{S}$ selon des modules m_i premiers impairs tous différents, i compris entre 1 et k, tels que $d > \prod_{i=1}^{k} m_i$.

Pour pouvoir descendre une marche de Fermat, il faut que $d' < d$. Or on a vu que $d' < d$ découle du fait que *trc_restreint* est une bijection.

Comment être sûr que d' ne vérifie pas la Conjecture de Goldbach non-plus ?

Il faut pour cela que les congruences conservées du système $\mathcal{S}$ initial soient telles que d' soit congru à tous les nombres premiers impairs de $\mathbb{P}_1^*(d')$ selon un module premier impair de $\mathbb{P}_2^*(d')$.

Dit autrement, il faut être sûr qu'en enlevant des congruences pour faire diminuer strictement la solution du système, on ne va pas "perdre" des congruences qui assuraient la non-vérification par d' de la Conjecture de Goldbach.

4.4 Deuxième étape

On conserve du système résultant un maximum de congruences dans un système $\mathcal{S}'$ de telle manière que d, la solution du système initial $\mathcal{S}$, soit strictement supérieur au produit des modules conservés dans le nouveau système et que chaque module intervenant dans une congruence conservée du système soit inférieur à $\sqrt{d'}$.

$p'_1, \ldots, p'_{k'} \in \mathbb{P}_1^*(x),\ n_{j_1}, \ldots, n_{j_{k'}} \in \mathbb{P}_2^*(d')$.
$\exists \quad x \in 2\mathbb{N}\backslash\{0,2,4\},\ x \geq 4.10^{18}$,

$$\mathcal{S}' \begin{cases} x \equiv p'_1 \ (mod\ n_{j_1}) \\ x \equiv p'_2 \ (mod\ n_{j_2}) \\ \ldots \\ x \equiv p'_{k'} \ (mod\ n_{j_{k'}}) \end{cases}$$

On a $d > \prod_{u=1}^{k'} n_{j_u}$. Les p'_x sont des nombres premiers impairs tous différents et les n_y sont des nombres premiers impairs tous différents et ordonnés selon un ordre croissant.

$\mathcal{S}'$ a pour image d' par la bijection *trc_restreint*.

4.5 Pourquoi d' ne vérifie-t-il pas la Conjecture de Goldbach non plus ?

On a $\quad d' < \prod_{u=1}^{k'} n_{j_u} < d.$

Donc $\quad \dfrac{d'}{2} < \dfrac{d}{2} \Leftrightarrow \mathbb{P}_1^*(d') \subset \mathbb{P}_1^*(d).$

Mais $\forall\, m_i \in \mathbb{P}_2^*(d), \qquad d' \equiv d\ (mod\ m_i).$

Donc $\forall p_i \in \mathbb{P}_1^*(d),\ \exists m_i \in \mathbb{P}_2^*(d), \qquad d \equiv p_i\ (mod\ m_i).$

$\Leftrightarrow$ $\forall p_i \in \mathbb{P}_1^*(d),\ \exists m_i \in \mathbb{P}_2^*(d), \qquad d' \equiv p_i\ (mod\ m_i)$

$\Rightarrow$ $\forall p_i \in \mathbb{P}_1^*(d'),\ \exists m_i \in \mathbb{P}_2^*(d'), \qquad d' \equiv p_i\ (mod\ m_i)$

L'implication est vraie parce que les modules conservés appartiennent à $\mathbb{P}_2^*(d')$.

Cette dernière ligne exprime que d' ne vérifie pas non plus la Conjecture de Goldbach.

5 Conclusion

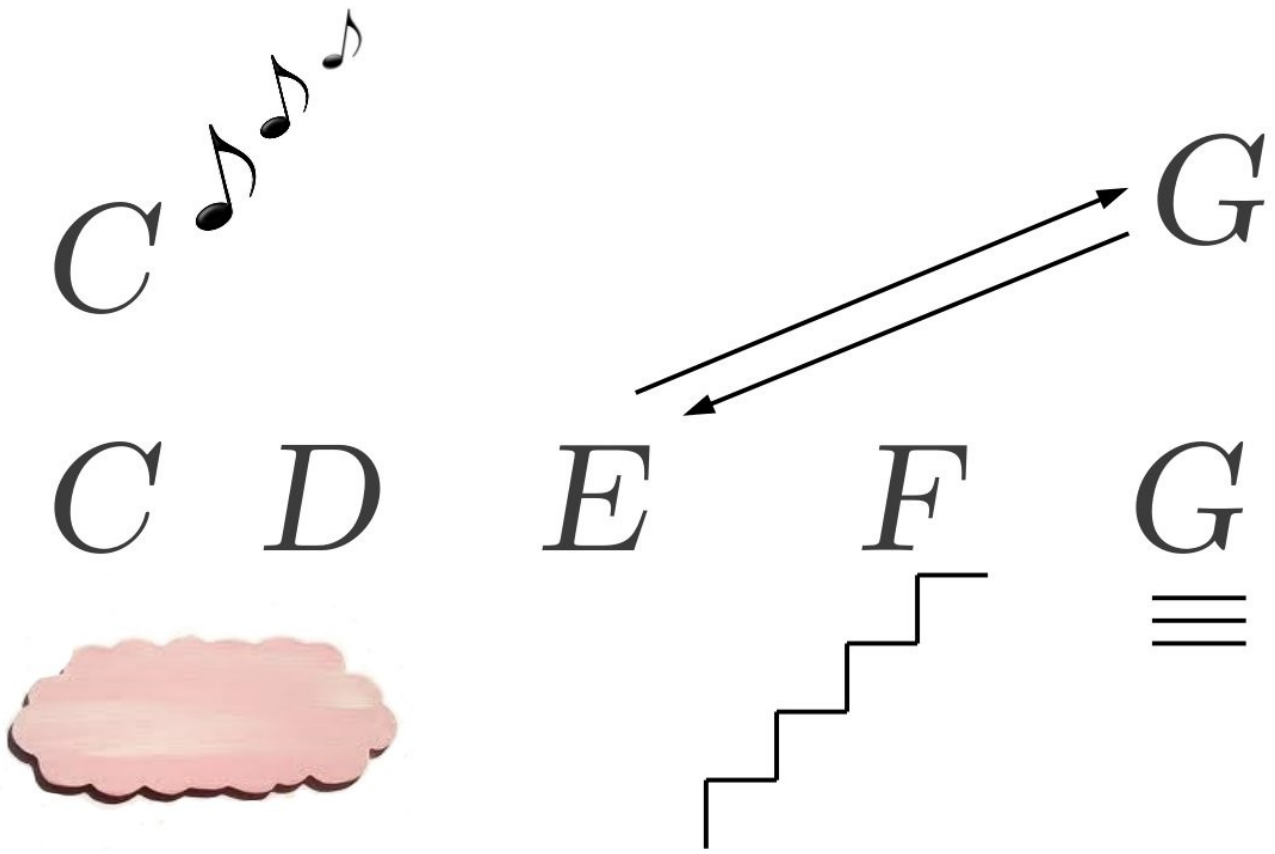
Si un nombre d ne vérifie pas la Conjecture de Goldbach, on est assuré de toujours pouvoir obtenir un $d' < d$ ne vérifiant pas non-plus la Conjecture de Goldbach, on a établi une contradiction à partir de l'hypothèse que d était le plus petit entier ne vérifiant pas la Conjecture de Goldbach.

On a ainsi établi qu'on aboutit toujours à une contradiction si on part de l'hypothèse qu'un entier ne vérifie pas la Conjecture de Goldbach.

Pour cela, on a utilisé ce que l'on pourrait appeler un *"Système de NUmération par les Restes dans les Parties Finies de* $\mathbb{N}$*"*[§].

La relation de congruence fait de l'ensemble $\mathbb{N}$ des entiers naturels un ensemble fractal.

[§] un $SNURPF$.


C
G
C D E F G

Infinitude de l'ensemble des nombres premiers de la forme $6n+1$, puis de l'ensemble des nombres premiers jumeaux qui en découle presque (Denise Chemla, 5 juin 2012)

1 Rappels

Rappelons le contenu du Triangle de Pascal qui contient les coefficients binomiaux.

								1										$\rightarrow$	1
							1		1									$\rightarrow$	2
						1		2		1								$\rightarrow$	4
					1		3		3		1							$\rightarrow$	8
				1		4		6		4		1						$\rightarrow$	16
			1		5		10		10		5		1					$\rightarrow$	32
		1		6		15		20		15		6		1				$\rightarrow$	64
	1		7		21		35		35		21		7		1			$\rightarrow$	128
1		8		28		56		70		56		28		8		1		$\rightarrow$	256

La somme de tous les coefficients de la $n^{ième}$ ligne vaut : 2^n.

$$\sum_{p=1}^{n} C_n^p = 2^n$$

Rappelons que le nombre de façons d'avoir au moins un zéro parmi 4 nombres est égal à $\sum_{p=1}^{n} C_n^p - 1$:

0	$-$	$-$	$-$	1
$-$	0	$-$	$-$	2
$-$	$-$	0	$-$	3
$-$	$-$	$-$	0	4
0	0	$-$	$-$	1
0	$-$	0	$-$	2
0	$-$	$-$	0	3
$-$	0	0	$-$	4
$-$	0	$-$	0	5
$-$	$-$	0	0	6
0	0	0	$-$	1
0	0	$-$	0	2
0	$-$	0	0	3
$-$	0	0	0	4
0	0	0	0	1

Rappelons enfin quelles sont les écritures par les restes modulo les nombres premiers successifs des premiers entiers. On ajoute à chaque "mot" de restes le mot n-uplet $(1, 1, 1, 1, \ldots)$.

mod	2	3	5	7	11	13	...
1	1	1	1	1	1	1	...
2	0	2	2	2	2	2	...
3	1	0	3	3	3	3	...
4	0	1	4	4	4	4	...
5	1	2	0	5	5	5	...
6	0	0	1	6	6	6	...
7	1	1	2	0	7	7	...
8	0	2	3	1	8	8	...
9	1	0	4	2	9	9	...
10	0	1	0	3	10	10	...
11	1	2	1	4	0	11	...
12	0	0	2	5	1	12	...
13	1	1	3	6	2	0	...

2 Infinitude de l'ensemble des nombres premiers de la forme $6n + 1$

On démontre par récurrence la propriété $P(p_i)$ qui est qu'il y a toujours un nombre premier de la forme $6n+1$ supérieur à $\#p_{i-1}$ et inférieur à $\#p_i$. On rappelle que la primorielle $\#p_i$ est le produit des nombres premiers compris entre 2 et p_i.

1) initialisation de la récurrence : la propriété est vraie pour $p_3 = 5$. Il y a un nombre premier 7 de la forme $6n + 1$ compris entre $\#3 = 2.3 = 6$ et $\#5 = 2.3.5 = 30$.

2) Passage de $P(p_i)$ à $P(p_{i+1})$: la propriété est vraie pour p_i signifie qu'il y a un nombre premier compris entre $\#p_{i-1}$ et $\#p_i$. Montrons qu'il y a un nombre premier de plus de la forme $6n + 1$ compris entre $\#p_i$ et $\#p_{i+1}$. De $\#p_i$ à $\#p_{i+1}$, il y a $\#p_i(p_{i+1} - 1)$ nombres différents. Mais parmi ces nombres, seuls $2^{i+1} - 1$ contiennent au moins un zéro dans leur écriture par les restes. Puisque $\#p_i(p_{i+1} - 1)$ est très supérieur à $2^{i+1} - 1$ (voir l'inégalité ci-après pour $p_i = 7$), les nombres restant ayant une écriture par les restes qui ne contient aucun zéro sont premiers. Seuls $\frac{1}{6}$ des nombres en question sont de la forme $6n - 1$. Ils ne peuvent tous être de la forme $6n - 1$. L'un des nombres qui n'est pas de la forme $6n - 1$ est de la forme $6n + 1$. Il n'avait pas été trouvé jusque-là car les nombres compris entre $\#p_i$ et $\#p_{i+1}$ sont tous différents de ceux déjà rencontrés jusqu'à $\#p_i$.

Pour $p_i = 7$, on a l'inégalité suivante :

$$\#p_i(p_{i+1} - 1) \gg 2^{i+1} - 1$$
$$2.3.5.7.(11 - 1) \gg 2.2.2.2.2 - 1$$

3 Infinitude de l'ensemble des nombres premiers jumeaux

Comme on peut le voir puis le comprendre dans le tableau qui fournit les écritures par les restes des premiers entiers, il y a autant de couples de nombres premiers jumeaux que de nombres pairs "coincés" entre deux nombres premiers jumeaux. Observons l'écriture par les restes de tels nombres. Un nombre pair $p_i + 1$ qui est entre les nombres premiers jumeaux p_i et $p_i + 2$ doit être :

- congru à 1 (mod p_i) ;
- non congru à $p_k - 1$ et non congru à 1 pour tout $k < i$.

Pour démontrer par récurrence qu'il existe toujours un tel nombre pair différent de ceux précédemment rencontrés entre $\#p_{i-1}$ et $\#p_i$, il faut démontrer que le nombre de nombres pairs "coincés" entre deux nombres premiers jumeaux (que l'on appellera $NbPairsMilieuxJumeaux$ est toujours supérieur strictement à 1. La "nouveauté" des nombres compris entre $\#p_i$ et $\#p_{i+1}$ garantit qu'on a trouvé un nouveau nombre pair entre deux nouveaux nombres premiers jumeaux et ainsi que l'ensemble des nombres premiers jumeaux est infini.

$$NbPairsMilieuxJumeaux = \frac{1}{p_i}\left[\#p_i(p_{i+1}-1) - \left(\sum_{k=1}^{i-1} 2^k.C_{i-1}^k - 1\right)\right]$$

La multiplication par $\frac{1}{p_i}$ est nécessitée pour calculer le nombre de mots qui contiennent un 1 en dernière lettre (i.e. $(mod\ p_i)$).

L'expression $\#p_i(p_{i+1}-1)$ compte le nombre de mots entre $\#p_i$ et $\#p_{i+1}$.

On soustrait de ce nombre de mots total la valeur de $\sum_{k=1}^{i-1} 2^k.C_{i-1}^k - 1$ qui correspond au nombre de mots contenant au moins un $p_k - 1$ ou un 1 comme lettre parmi les $i-1$ premières lettres de leur écriture par les restes (i.e. $(mod\ p_k)$, pour tout p_k inférieur strictement à i). Le reste 1 correspond au fait que le nombre p_i précédant le nombre pair p_i+1 n'est pas premier tandis que le reste $p_k - 1$ correspond au fait que le nombre p_i+2 suivant le nombre pair p_i+1 n'est pas premier). Le nombre de mots à éliminer étant égal à 3^{i-1} est comme dans la section précédente bien inférieur au nombre de mots total et on est ainsi assuré de toujours trouver entre deux primorielles sucessives un nombre pair "coincé" entre deux nombres premiers.

4 Existence d'un décomposant de Goldbach pour tout nombre pair supérieur ou égal à 6

La Conjecture de Goldbach (7 juin 1742) stipule que tout nombre pair supérieur ou égal à 6 est la somme de deux nombres premiers impairs. Si on note $\mathbb{P}^*$ l'ensemble des nombres premiers impairs :

$$\mathbb{P}^* = \{p_1 = 3, p_2 = 5, p_3 = 7, p_4 = 11, \ldots\},$$

on peut écrire la Conjecture de Goldbach ainsi :

$$\forall\, n \in 2\mathbb{N}\backslash\{0,2,4\},\ \exists\, p \in \mathbb{P}^*,\ p \leq n/2,\ \exists\, q \in \mathbb{P}^*,\ q \geq n/2,\ \ n = p+q.$$

Dans la suite, n étant donné, on note : $\mathbb{P}^*(n) = \{x \in \mathbb{P}^* / x \leq n\}$,

Un nombre premier qui n'est jamais congru à n, un nombre pair supérieur ou égal à 6 donné, selon aucun module de $\mathbb{P}^*(n)$, est un décomposant de Goldbach de n.
En effet,

$$\begin{aligned} \forall\, n \in 2\mathbb{N}\backslash\{0,2,4\},\ \exists\, p \in \mathbb{P}^*(n),\ \forall\, m \in \mathbb{P}^*(n), \quad & p \not\equiv n\ (mod\ m) \\ & \Leftrightarrow n - p \not\equiv 0\ (mod\ m) \\ & \Leftrightarrow n - p\ premier. \end{aligned}$$

On va chercher pour n un nombre pair compris entre deux primorielles successives $\#p_i$ et $\#p_{i+1}$ un nombre premier inférieur à $\#p_i$ non congru à n selon tout module premier inférieur à p_i. On va montrer que parmi les nombres inférieurs à $\#p_i$, il y en a au moins un qui n'est congru ni à 0 (donc il est premier) ni à n (donc il ne partage aucun de ses restes avec n). On a vu dans la section précédente que 3^i nombres inférieurs à $\#p_i$ ont au moins l'un de leurs restes qui est nul ou bien égal à une valeur donnée (en l'occurrence le reste de n selon le module considéré). Mais 3^i est toujours très inférieur à $\#p_i$ donc il existe toujours un nombre inférieur à $\#p_i$ qui n'est congru à 0 selon aucun module et qui n'est jamais congru à n selon aucun module inférieur à p_i. Ce nombre est un décomposant de Goldbach de n.

$$Si \quad \#p_i < n < \#p_{i+1} \quad alors \quad NbDecompGoldbach(n) > \#p_i - 3^i > 1.$$

Conjecture des nombres premiers jumeaux

Denise Vella-Chemla

7/6/2012

1 Introduction

Dans cette note, on étudie la conjecture des nombres premiers jumeaux selon une approche combinatoire. Cette approche, que l'on pourrait qualifier de lexicale, utilise des mots de représentation des entiers par leurs restes modulaires selon les nombres premiers successifs.

2 Énoncé

On appelle *nombres premiers jumeaux* deux nombres premiers dont la différence est 2.
Exemples :

3 et 5 sont des nombres premiers jumeaux.
29 et 31 sont des nombres premiers jumeaux.

La conjecture des nombres premiers jumeaux stipule que l'ensemble des nombres premiers jumeaux est infini.
Note : dans la suite, on utilisera à plusieurs reprises la notion de primorielle. On appelle *primorielle* d'un nombre premier p_i le produit de tous les nombres premiers inférieurs ou égaux à p_i.

$$\#p_i = \prod_{p_1=2,\ p_k\ premier}^{p_i} p_k$$

3 Représentation par les restes

Représentons les premiers entiers naturels par leurs restes modulo les nombres premiers successifs.
On ajoute à chaque *"mot"* de restes le mot n-uplet infini $(1, 1, 1, 1, \ldots)$ qui représente l'entier naturel 1.

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

Observons quelques représentations par les restes qui sont pertinentes par rapport à la conjecture des nombres premiers jumeaux.

6, un nombre pair entre les deux premiers jumeaux 5 et 7 a pour représentation 0 0 1 6 6 6 .... Il a un 1 en troisième position parce que 5 a un 0 à cette position (un nombre premier a toujours un 0 dans sa propre colonne, aucun 0 avant celle-ci et lui-même comme reste modulo tout nombre premier qui lui est strictement supérieur). 6 a un 6 en quatrième position parce que 7 a un 0 à cette position-là (la sienne propre). Les deux premières lettres du mot de représentation du nombre 6 ne sont ni des 1 ni des $p_k - 1$ (ni 1 ni 1 dans la colonne correspondant au nombre premier 2, ni 1 ni 2 dans la colonne correspondant au nombre premier 3).

18, entre 17 et 19, a pour représentation 0 0 3 4 7 5 1 18 ... : il n'a ni 1 ni $p_k - 1$ parmi ses six premières lettres, correspondant à ses restes modulo $2, 3, 5, 7, 11$ et 13. Le mot de 18 a un 1 en septième position (correspondant à son reste modulo 17 : $18 = 17 + 1$) et 18 a un reste de 18 en huitième position (correspondant à son reste modulo $19 = 18 + 1$).

4 Tentative de démonstration

Entre $\#p_i$ et $\#p_{i+1}$, il y a $(p_{i+1} - 1)\#p_i$ nombres. Considérons les mots formés des $\pi(\sqrt{n}) + 2$ premières lettres de leur représentation par les restes.

On doit prouver qu'on peut toujours trouver parmi ces nombres un entier naturel pair n juste entre deux premiers* car l'écriture de "son mot" est caractérisée ainsi :

- elle ne contient aucun 1 (le nombre précédant le nombre pair est donc premier) pour toutes ses lettres jusqu'à la $\pi(\sqrt{n})$ème ;
- elle ne contient aucun $p_k - 1$ (le nombre suivant le nombre pair est donc premier) pour toutes ses lettres jusqu'à la $\pi(\sqrt{n})$ème ;
- sa lettre suivante (de rang $\pi(\sqrt{n}) + 1$) vaut 1 ;
- la lettre suivant cette dernière (de rang $\pi(\sqrt{n}) + 2$) vaut $p_i + 1$.

*L'expression *juste entre deux premiers* signifie que le premier nombre premier est le prédécesseur du nombre pair et que le second est son successeur, dans l'arithmétique de Peano.

5 Conclusion

On a essayé d'utiliser pour démontrer la conjecture des nombres premiers jumeaux un *"Système de NUmération par les Restes dans les Parties Finies de* $\mathbb{N}$*"*.

On se situe dans le cadre d'une *théorie lexicale des nombres*, selon laquelle les nombres sont des mots.

Annexe : rappels de combinatoire

Rappelons le contenu du Triangle de Pascal qui contient les coefficients binomiaux.

$$\begin{array}{ccccccccccccccccc|cc}
&&&&&&&&1&&&&&&&& & \rightarrow & 1\\
&&&&&&&1&&1&&&&&&& & \rightarrow & 2\\
&&&&&&1&&2&&1&&&&&& & \rightarrow & 4\\
&&&&&1&&3&&3&&1&&&&& & \rightarrow & 8\\
&&&&1&&4&&6&&4&&1&&&& & \rightarrow & 16\\
&&&1&&5&&10&&10&&5&&1&&& & \rightarrow & 32\\
&&1&&6&&15&&20&&15&&6&&1&& & \rightarrow & 64\\
&1&&7&&21&&35&&35&&21&&7&&1& & \rightarrow & 128\\
1&&8&&28&&56&&70&&56&&28&&8&&1 & \rightarrow & 256
\end{array}$$

La somme de tous les coefficients de la $n^{ième}$ ligne vaut : 2^n.

$$\sum_{p=1}^{n} C_n^p = 2^n$$

Rappelons que le nombre de façons d'avoir au moins un zéro parmi 4 nombres est égal à

$$\sum_{p=1}^{n} C_n^p - 1 = 2^4 - 1$$

:

$$\begin{array}{cccccc}
0 & - & - & - & & 1\\
- & 0 & - & - & & 2\\
- & - & 0 & - & & 3\\
- & - & - & 0 & & 4\\
\\
0 & 0 & - & - & & 1\\
0 & - & 0 & - & & 2\\
0 & - & - & 0 & & 3\\
- & 0 & 0 & - & & 4\\
- & 0 & - & 0 & & 5\\
- & - & 0 & 0 & & 6\\
\\
0 & 0 & 0 & - & & 1\\
0 & 0 & - & 0 & & 2\\
0 & - & 0 & 0 & & 3\\
- & 0 & 0 & 0 & & 4\\
\\
0 & 0 & 0 & 0 & & 1
\end{array}$$

Si l'on souhaite compter le nombre de façons d'avoir au moins un zéro ou un $p'_k = p_k - 1$ dans chaque ligne de la façon suivante :

0	–	–	–	1	p'_1	–	–	–	$1'$											
–	0	–	–	2	–	p'_2	–	–	$2'$											
–	–	0	–	3	–	–	p'_3	–	$3'$											
–	–	–	0	4	–	–	–	p'_4	$4'$											
0	0	–	–	1	0	p'_2	–	–	$1'$	p'_1	0	–	–	$1''$	p'_1	p'_2	–	–	$1'''$	
0	–	0	–	2	0	–	p'_3	–	$2'$	p'_1	–	0	–	$2''$	p'_1	–	p'_3	–	$2'''$	
0	–	–	0	3	0	–	–	p'_4	$3'$	p'_1	–	–	0	$3''$	p'_1	–	–	p'_4	$3'''$	
–	0	0	–	4	–	p'_2	0	–	$4'$	–	0	p'_3	–	$4''$	–	p'_2	p'_3	–	$4'''$	
–	0	–	0	5	–	p'_2	–	0	$5'$	–	0	–	p'_4	$5''$	–	p'_2	–	p'_4	$5'''$	
–	–	0	0	6	–	–	p'_3	0	$6'$	–	–	0	p'_4	$6''$	–	–	p'_3	$'p_4$	$6'''$	
0	0	0	–	1	p'_1	0	0	–	1	...										8 *variantes par ligne*
0	0	–	0	2	p'_1	0	–	0	2	...										8 *variantes par ligne*
0	–	0	0	3	0	–	p'_2	0	3	...										8 *variantes par ligne*
–	0	0	0	4	–	p'_2	0	0	4	...										8 *variantes par ligne*
0	0	0	0	1	p'_1	0	0	0	1	...										16 *variantes*

on voit qu'à chaque ligne correspondent 2^k possibilités qui correspondent aux différentes façons de changer les 0 en $p'_k = p_k - 1$ dans cette ligne.

On obtient donc $\sum 2^k.C_n^k$ possibilités en tout. On calcule que $\sum 2^k.C_n^k = 3^k$.

Exemples :
(1.1)=1=3^0
$(1.1) + (1.2) = 3 = 3^1$
$(1.1) + (2.2) + (1.4) = 9 = 3^2$
$(1.1) + (3.2) + (3.4) + (1.8) = 27 = 3^3$
$(1.1) + (4.2) + (6.4) + (4.8) + (1.16) = 81 = 3^4$
$(1.1) + (5.2) + (10.4) + (10.8) + (5.16) + (1.32) = 243 = 3^5$.

Effectivement, chaque position peut prendre trois valeurs différentes : 0, $p_k - 1$ ou bien ni l'un ni l'autre, ce qui permet de bien comprendre le sens de cette formule 3^k.

Étude de deux conjectures concernant les nombres premiers

Denise Vella-Chemla

7/6/2012

1 Introduction

Dans cette note, on étudie selon une même approche deux conjectures concernant les nombres premiers, la conjecture des nombres premiers jumeaux et la conjecture de Goldbach. Cette approche, que l'on pourrait qualifier de lexicale, utilise des mots de représentation des entiers par leurs restes modulaires selon les nombres premiers successifs.

2 Conjecture des nombres premiers jumeaux

On appelle *nombres premiers jumeaux* deux nombres premiers dont la différence est 2.
Exemples :

3 et 5 sont des nombres premiers jumeaux.
29 et 31 sont des nombres premiers jumeaux.

La conjecture des nombres premiers jumeaux stipule que l'ensemble des nombres premiers jumeaux est infini.
Note : dans la suite, on utilisera à plusieurs reprises la notion de primorielle. On appelle *primorielle* d'un nombre premier p_i le produit de tous les nombres premiers inférieurs ou égaux à p_i.

$$\#p_i = \prod_{p_1=2,\ p_k\ premier}^{p_i} p_k$$

3 Conjecture de Goldbach

Notons $\mathbb{P}^*$ l'ensemble des nombres premiers impairs. $\mathbb{P}^* = \{p_1 = 3, p_2 = 5, p_3 = 7, p_4 = 11, \ldots\}$

La conjecture de Goldbach, énoncée dans une lettre de Goldbach à Euler du 7 juin 1742 puis reformulée par Euler, stipule que tout nombre pair supérieur ou égal à 6 est la somme de deux nombres premiers impairs.
On peut l'écrire :

$$\begin{array}{c} \forall\, n \ \in\ 2\mathbb{N}\backslash\{0,2,4\}, \\ \exists\, p \ \in\ \mathbb{P}^*,\ p \ \leq\ n/2, \\ \exists\, q \ \in\ \mathbb{P}^*,\ q \ \geq\ n/2, \\ n = p + q \end{array}$$

p et q sont appelés *décomposants de Goldbach* de n.

La conjecture de Goldbach* est équivalente à l'énoncé suivant :

$$\forall\, n \in 2\mathbb{N}\backslash\{0,2,4\},\ \exists\, p \in \mathbb{P}^*,\ \forall\, m \in \mathbb{P}^*,\\ p \not\equiv n\ (mod\ m)$$

En effet,

$$\forall\, n \in 2\mathbb{N}\backslash\{0,2,4\},\ \exists\, p \in \mathbb{P}^*,\ \forall\, m \in \mathbb{P}^*,\\ p \not\equiv n\ (mod\ m) \Leftrightarrow n-p \not\equiv 0\ (mod\ m) \Leftrightarrow n-p\ premier$$

4 Représentation par les restes

Représentons les premiers entiers naturels par leurs restes modulo les nombres premiers successifs.
On ajoute à chaque *"mot"* de restes le mot n-uplet infini $(1,1,1,1,\ldots)$ qui représente l'entier naturel 1.

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

Observons quelques représentations par les restes qui sont pertinentes par rapport aux deux conjectures qui nous intéressent.

4.1 Conjecture des jumeaux

6, un nombre pair entre les deux premiers jumeaux 5 et 7 a pour représentation 0 0 1 6 6 6 ....
18, entre 17 et 19, a pour représentation 0 0 3 4 7 5 1 18 ...

4.2 Conjecture de Goldbach

37, de représentation 1 1 2 2 4 11 3 18 14 8 6 0 37 37 37 ..., est un décomposant de Goldbach de 98, de décomposition 0 2 3 0 10 7 13 3 6 1 5 24 16 12 4 ....

*La conjecture de Goldbach a été vérifiée par ordinateur jusqu'à 4.10^{18} (par l'équipe portugaise d'Oliveira e Silva, le 4 avril 2012).

5 Démonstration de la conjecture des nombres premiers jumeaux

Entre $\#p_i$ et $\#p_{i+1}$, il y a $(p_{i+1}-1)\#p_i$ nombres. Considérons les mots formés des $i+1$ premières lettres de leur représentation par les restes.

On peut toujours trouver parmi ces nombres un entier naturel pair juste entre deux premiers[†] car l'écriture de "son mot" est caractérisée ainsi :

- elle ne contient aucun 1 (le nombre précédant le nombre pair est donc premier) pour toutes ses lettres jusqu'à la i-1ème ;
- elle ne contient aucun $p_k - 1$ (le nombre suivant le nombre pair est donc premier) pour toutes ses lettres jusqu'à la i-1ème ;
- sa ième lettre vaut 1 ;
- sa i+1ème lettre vaut $p_i + 1$.

En effet, les nombres ne contenant ni 1 ni $p_k - 1$ sur leurs $i-1$ premières lettres sont en quantité $3^{i-1}-1$ (explication fournie en annexe). D'autre part,

$$\begin{array}{lllllll} \frac{1}{p_{i+1}}.(p_{i+1}-1). & \#p_i. & & & & \frac{1}{p_i} & \gg 3^{i-1}-1 \\ \underbrace{\frac{1}{p_{i+1}}.(p_{i+1}-1)}_{\approx 1}. & 2.5. & 3. & \ldots & p_{i-1}. & p_i.\frac{1}{p_i} & \gg 3^{i-1}-1 \\ & 3^2 & 3 & \ldots & p_{i-1} & 1 & \gg 3^{i-1}-1 \end{array}$$

Il y a donc toujours au moins un nombre satisfaisant les contraintes souhaitées. Il y a autant de couples de nombres premiers jumeaux que de nombres premiers, un par primorielle au moins, donc une infinité.

6 Tentative de démonstration de la conjecture de Goldbach

Soit un nombre pair n compris entre $\#p_i$ et $\#p_{i+1}$. On rappelle que la notation $\pi(x)$ désigne le nombre de nombres premiers inférieurs ou égaux à x.

Voyons si l'on peut toujours trouver, parmi les nombres inférieurs à $n/2$, un entier naturel dont l'écriture par les restes est caractérisée ainsi :

- elle est différente en chaque lettre sur ses $\pi(n/2)$ premières lettres de celle de n (pour garantir que le complémentaire à n de ce nombre est premier) ;
- elle est non-nulle en chaque lettre sur les $\pi(n/2)$ lettres en question (pour garantir que ce nombre est premier).

En effet, les nombres qui ont une de leur $\pi(n/2)$ premières lettres qui est soit nulle soit égale à $p-1$ selon le nombre premier p sont en nombre $3^{\pi(n/2)}-1$ (explication fournie en annexe).

Une petite astuce nous permettra lorsque nécessaire d'obtenir "un trois de plus" que le nombre de facteurs d'une primorielle :

$$\begin{array}{llllll} \underbrace{2.3.5}_{>3^3}. & \underbrace{7.11}_{>3^3}. & \ldots & p_{i-1} & \gg & 3^i \\ & & \ldots & >3 & \gg & 3^i \end{array}$$

[†]L'expression *juste entre deux premiers* signifie que le premier nombre premier est le prédécesseur du nombre pair et que le second est son successeur, dans l'arithmétique de Peano.

Rappelons le théorème de Bertrand qui énonce que quelque soit i un entier naturel, p_i étant le ième nombre premier, $p_{i+1} < 2p_i$.

De
$$\#p_i \quad \leq \quad n \quad \leq \quad \#p_{i+1},$$
on tire
$$\#p_{i-1} \quad \leq \quad 3.\ldots.p_i \quad \leq \quad n/2 \quad \leq \quad 3.\ldots.p_{i+1} \quad \leq \quad p_i\#p_i \quad \leq \quad p_{i+1}\#p_i \quad \leq \quad \#p_{i+1}.$$

L'inégalité à l'extrême-gauche de la ligne ci-dessus découle du fait que tout nombre premier est strictement supérieur au nombre premier qui le précède tandis que la quatrième inégalité découle du théorème de Bertrand.

On a
$$n/2 \quad \geq \quad \#p_{i-1} \quad \geq \quad 3^i - 1.$$

La deuxième inégalité de la ligne ci-dessus provenant de l'application de ce que l'on a désigné comme la petite astuce.

On est assuré de trouver un nombre qui est différent de n sur ses i premières lettres alors qu'il faut qu'on soit assuré de trouver un nombre différent de n sur ses $n/2$ premières lettres. Comment être assuré de la différence des écritures sur les lettres de la $i+1^{ième}$ à la $n/2^{ième}$?

7 Conclusion

On a utilisé pour essayer de démontrer les deux conjectures un *"Système de NUmération par les Restes dans les Parties Finies de* $\mathbb{N}$*"*.

On se situe dans le cadre d'une *théorie lexicale des nombres*, selon laquelle les nombres sont des mots.

Annexe : rappels de combinatoire

Rappelons le contenu du Triangle de Pascal qui contient les coefficients binomiaux.

$$\begin{array}{ccccccccccccccccc|cc}
 & & & & & & & & 1 & & & & & & & & & \rightarrow & 1 \\
 & & & & & & & 1 & & 1 & & & & & & & & \rightarrow & 2 \\
 & & & & & & 1 & & 2 & & 1 & & & & & & & \rightarrow & 4 \\
 & & & & & 1 & & 3 & & 3 & & 1 & & & & & & \rightarrow & 8 \\
 & & & & 1 & & 4 & & 6 & & 4 & & 1 & & & & & \rightarrow & 16 \\
 & & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & & & \rightarrow & 32 \\
 & & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & & & \rightarrow & 64 \\
 & 1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1 & & \rightarrow & 128 \\
1 & & 8 & & 28 & & 56 & & 70 & & 56 & & 28 & & 8 & & 1 & \rightarrow & 256
\end{array}$$

La somme de tous les coefficients de la $n^{ième}$ ligne vaut : 2^n.

$$\sum_{p=1}^{n} C_n^p = 2^n$$

Rappelons que le nombre de façons d'avoir au moins un zéro parmi 4 nombres est égal à

$$\sum_{p=1}^{n} C_n^p - 1 = 2^4 - 1$$

:

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

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

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

0	0	0	0	1

Si l'on souhaite compter le nombre de façons d'avoir au moins un zéro ou un $p'_k = p_k - 1$ dans chaque ligne de la façon suivante :

0	–	–	–	1	p'_1	–	–	–	$1'$
–	0	–	–	2	–	p'_2	–	–	$2'$
–	–	0	–	3	–	–	p'_3	–	$3'$
–	–	–	0	4	–	–	–	p'_4	$4'$

0	0	–	–	1	0	p'_2	–	–	$1'$	p'_1	0	–	–	$1''$	p'_1	p'_2	–	–	$1'''$
0	–	0	–	2	0	–	p'_3	–	$2'$	p'_1	–	0	–	$2''$	p'_1	–	p'_3	–	$2'''$
0	–	–	0	3	0	–	–	p'_4	$3'$	p'_1	–	–	0	$3''$	p'_1	–	–	p'_4	$3'''$
–	0	0	–	4	–	p'_2	0	–	$4'$	–	0	p'_3	–	$4''$	–	p'_2	p'_3	–	$4'''$
–	0	–	0	5	–	p'_2	–	0	$5'$	–	0	–	p'_4	$5''$	–	p'_2	–	p'_4	$5'''$
–	–	0	0	6	–	–	p'_3	0	$6'$	–	–	0	p'_4	$6''$	–	–	p'_3	$'p_4$	$6'''$

0	0	0	–	1	p'_1	0	0	–	1	...	8 *variantes par ligne*
0	0	–	0	2	p'_1	0	–	0	2	...	8 *variantes par ligne*
0	–	0	0	3	0	–	p'_2	0	3	...	8 *variantes par ligne*
–	0	0	0	4	–	p'_2	0	0	4	...	8 *variantes par ligne*

0	0	0	0	1	p'_1	0	0	0	1	...	16 *variantes*

on voit qu'à chaque ligne correspondent 2^k possibilités qui correspondent aux différentes façons de changer les 0 en $p'_k = p_k - 1$ dans cette ligne.

On obtient donc $\sum 2^k.C_n^k$ possibilités en tout. On calcule que $\sum 2^k.C_n^k = 3^k$.
Effectivement, chaque position peut prendre trois valeurs différentes : 0, $p_k - 1$ ou bien ni l'un ni l'autre, ce qui permet de bien comprendre le sens de cette formule 3^k.

Générer des couples de nombres premiers jumeaux

Denise Vella-Chemla

7/6/2012

1 Introduction

Dans cette note, on étudie la conjecture des nombres premiers jumeaux selon une approche combinatoire. Cette approche, que l'on pourrait qualifier de lexicale, utilise des mots de représentation des entiers par leurs restes modulaires selon les nombres premiers successifs.

2 Énoncé

On appelle *nombres premiers jumeaux* deux nombres premiers dont la différence est 2.
Exemples :

3 et 5 sont des nombres premiers jumeaux.
29 et 31 sont des nombres premiers jumeaux.

La conjecture des nombres premiers jumeaux stipule que l'ensemble des nombres premiers jumeaux est infini.

3 Représentation par les restes

Représentons les premiers entiers naturels par leurs restes modulo les nombres premiers successifs.
On ajoute à chaque *"mot"* de restes le mot n-uplet infini $(1, 1, 1, 1, \ldots)$ qui représente l'entier naturel 1.

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

Observons quelques représentations par les restes qui sont pertinentes par rapport à la conjecture des nombres premiers jumeaux.

6, un nombre pair entre les deux premiers jumeaux 5 et 7 a pour représentation 0 0 1 6 6 6 .... Il a un 1 en troisième position parce que 5 a un 0 à cette position (un nombre premier est congru à 0 modulo lui-même, jamais congru à 0 modulo un nombre premier qui lui est strictement inférieur et congru à lui-même modulo tout nombre premier qui lui est strictement supérieur). 6 a un 6 en quatrième position parce que 7 a un 0 à cette position-là (le reste de 7 modulo lui-même). Les deux premières lettres du mot de représentation du nombre 6 ne sont ni des 1 ni des $p_k - 1$ (ni 1 ni 1 dans la colonne correspondant au nombre premier 2, ni 1 ni 2 dans la colonne correspondant au nombre premier 3) car si tel était le cas, l'un ou l'autre de 5 ou 7 serait composé.

18, entre 17 et 19, a pour représentation 0 0 3 4 7 5 1 18 ... : il n'a ni 1 ni $p_k - 1$ parmi ses six premières lettres, correspondant à ses restes modulo $2, 3, 5, 7, 11$ et 13. Le mot de 18 a un 1 en septième position (correspondant à son reste modulo 17 : $18 = 17 + 1$) et 18 a un reste de 18 en huitième position (correspondant à son reste modulo $19 = 18 + 1$).

4 Générer les couples de nombres premiers jumeaux

On va générer des couples de nombres premiers jumeaux en appliquant le théorème des restes chinois à des systèmes de congruences. On a vu qu'on "refuse" les restes 1 et $p_k - 1$ modulo p_k.

On représentera la résolution du système de congruences suivant :

$$\begin{cases} x \equiv 0 \ (mod\ 2) \\ x \equiv 0 \ (mod\ 3) \\ x \equiv 2 \ (mod\ 5) \end{cases}$$

par l'application 0 0 2 $\rightarrow$ 12 dans la mesure où 12 est le plus petit entier solution du système de congruences en question.

Au troisième niveau, on trouve les solutions suivantes :

0 0 0 $\rightarrow$ 0
0 0 2 $\rightarrow$ 12
0 0 3 $\rightarrow$ 18

toutes deux inférieures à $25 = 5^2$, qui fournissent donc deux pairs entre deux premiers jumeaux :
$11 < 12 < 13$ et $17 < 18 < 19$.

Au niveau suivant, on trouve combinatoirement les solutions ci-après :

0 0 0 0 $\rightarrow$ ~~0~~	0 0 2 0 $\rightarrow$ 42	0 0 3 0 $\rightarrow$ ~~168~~
0 0 0 2 $\rightarrow$ 30	0 0 2 2 $\rightarrow$ 72	0 0 3 2 $\rightarrow$ 198
0 0 0 3 $\rightarrow$ 150	0 0 2 3 $\rightarrow$ 192	0 0 3 3 $\rightarrow$ 108
0 0 0 4 $\rightarrow$ 60	0 0 2 4 $\rightarrow$ 102	0 0 3 4 $\rightarrow$ 18
0 0 0 5 $\rightarrow$ 180	0 0 2 5 $\rightarrow$ 12	0 0 3 5 $\rightarrow$ 138

dont seules les quatre solutions colorées sont inférieures à $49 = 7^2$. Parmi toutes les autres solutions, seule une, le nombre pair 168 n'est pas juste entre deux nombres premiers jumeaux ($169 = 13^2$), tous les autres pairs étant entre deux nombres premiers jumeaux.

Enfin, détaillons un niveau supplémentaire :

0 0 0 0 0 → ~~0~~	0 0 2 0 0 → 462	0 0 3 0 0 → 1848
0 0 0 0 2 → 420	0 0 2 0 2 → 882	0 0 3 0 2 → 2268
0 0 0 0 3 → 630	0 0 2 0 3 → 1092	0 0 3 0 3 → 168
0 0 0 0 4 → 840	0 0 2 0 4 → 1302	0 0 3 0 4 → 378
0 0 0 0 5 → 1050	0 0 2 0 5 → 1512	0 0 3 0 5 → 588
0 0 0 0 6 → 1260	0 0 2 0 6 → 1722	0 0 3 0 6 → 798
0 0 0 0 7 → 1470	0 0 2 0 7 → 1932	0 0 3 0 7 → 1008
0 0 0 0 8 → 1680	0 0 2 0 8 → 2142	0 0 3 0 8 → 1218
0 0 0 0 9 → 1890	0 0 2 0 9 → 42	0 0 3 0 9 → 1428
0 0 0 2 0 → 660	0 0 2 2 0 → 1122	0 0 3 2 0 → 198 *J*
0 0 0 2 2 → 1080	0 0 2 2 2 → 1542	0 0 3 2 2 → 618 *J*
0 0 0 2 3 → 1290	0 0 2 2 3 → 1752	0 0 3 2 3 → 828 *J*
0 0 0 2 4 → 1500	0 0 2 2 4 → 1962	0 0 3 2 4 → 1038
0 0 0 2 5 → 1710	0 0 2 2 5 → 2172	0 0 3 2 5 → 1248
0 0 0 2 6 → 1920	0 0 2 2 6 → 72 *J*	0 0 3 2 6 → 1458
0 0 0 2 7 → 2130	0 0 2 2 7 → 282 *J*	0 0 3 2 7 → 1668 *J*
0 0 0 2 8 → 30	0 0 2 2 8 → 492	0 0 3 2 8 → 1878 *J*
0 0 0 2 9 → 240	0 0 2 2 9 → 702	0 0 3 2 9 → 2088 *J*
0 0 0 3 0 → 990	0 0 2 3 0 → 1452 *J*	0 0 3 3 0 → 528
0 0 0 3 2 → 1410	0 0 2 3 2 → 1872 *J*	0 0 3 3 2 → 948
0 0 0 3 3 → 1620 *J*	0 0 2 3 3 → 2082 *J*	0 0 3 3 3 → 1158
0 0 0 3 4 → 1830	0 0 2 3 4 → 2292	0 0 3 3 4 → 1368
0 0 0 3 5 → 2040	0 0 2 3 5 → 192 *J*	0 0 3 3 5 → 1578
0 0 0 3 6 → 2250	0 0 2 3 6 → 402	0 0 3 3 6 → 1788 *J*
0 0 0 3 7 → 150 *J*	0 0 2 3 7 → 612	0 0 3 3 7 → 1998 *J*
0 0 0 3 8 → 360	0 0 2 3 8 → 822 *J*	0 0 3 3 8 → 2208
0 0 0 3 9 → 570 *J*	0 0 2 3 9 → 1032 *J*	0 0 3 3 9 → 108 *J*
0 0 0 4 0 → 1320 *J*	0 0 2 4 0 → 1782	0 0 3 4 0 → 858 *J*
0 0 0 4 2 → 1740	0 0 2 4 2 → 2202	0 0 3 4 2 → 1278 *J*
0 0 0 4 3 → 1950 *J*	0 0 2 4 3 → 102 *J*	0 0 3 4 3 → 1488 *J*
0 0 0 4 4 → 2160	0 0 2 4 4 → 312 *J*	0 0 3 4 4 → 1698 *J*
0 0 0 4 5 → 60 *J*	0 0 2 4 5 → 522 *J*	0 0 3 4 5 → 1908
0 0 0 4 6 → 270 *J*	0 0 2 4 6 → 732	0 0 3 4 6 → 2118
0 0 0 4 7 → 480	0 0 2 4 7 → 942	0 0 3 4 7 → 18 *J*
0 0 0 4 8 → 690	0 0 2 4 8 → 1152 *J*	0 0 3 4 8 → 228 *J*
0 0 0 4 9 → 900	0 0 2 4 9 → 1362	0 0 3 4 9 → 438
0 0 0 5 0 → 1650	0 0 2 5 0 → 2112 *J*	0 0 3 5 0 → 1188
0 0 0 5 2 → 2070	0 0 2 5 2 → 222	0 0 3 5 2 → 1608 *J*
0 0 0 5 3 → 2280	0 0 2 5 3 → 432 *J*	0 0 3 5 3 → 1818
0 0 0 5 4 → 180 *J*	0 0 2 5 4 → 642 *J*	0 0 3 5 4 → 2028 *J*
0 0 0 5 5 → 390	0 0 2 5 5 → 852	0 0 3 5 5 → 2238 *J*
0 0 0 5 6 → 600 *J*	0 0 2 5 6 → 1062 *J*	0 0 3 5 6 → 138 *J*
0 0 0 5 7 → 810 *J*	0 0 2 5 7 → 1272	0 0 3 5 7 → 348 *J*
0 0 0 5 8 → 1020 *J*	0 0 2 5 8 → 1482 *J*	0 0 3 5 8 → 558
0 0 0 5 9 → 1230 *J*	0 0 2 5 9 → 1692	0 0 3 5 9 → 768

qui est obtenu en admettant combinatoirement des congruences possibles à $0, 2, 3, 4, 5, 6, 7, 8$ ou 9 modulo 11. On a coloré les nombres inférieurs à $121 = 11^2$. On a indiqué par un J les nombres qui sont des pairs juste entre deux nombres premiers.

On voit qu'aux niveaux successifs, on obtiendra $((((((3.5).9).11).15).17).21)\ldots$ nombres pour les modules premiers jusqu'à 23 par exemple.

Mais on voit également que les pairs "juste entre deux premiers" peuvent s'hériter d'un niveau à l'autre ou pas (12 a disparu entre les deux derniers niveaux alors que $18, 30$ et 42 ont été conservés). S'il n'y avait aucun pair à un niveau, il n'y aurait aucun pair au niveau inférieur. Et cela pourrait aboutir à une contradiction par descente puisque les pairs d'un niveau s'obtiennent par expansion des mots des pairs

des niveaux inférieurs.

Il faudrait aussi être assuré qu'il n'est pas possible qu'il y ait une "stabilisation de la population" qui ferait qu'à partir d'un certain niveau, on n'obtiendrait pas de "nouveau" pair juste entre deux premiers, ce qui pourrait avoir pour conséquence la finitude de l'ensemble des nombres premiers jumeaux.

Infinité de l'ensemble des nombres premiers jumeaux

Denise Vella-Chemla

11/6/2012

1 Introduction

Dans cette note, on essaie de démontrer la conjecture des nombres premiers jumeaux en utilisant un argument similaire à celui d'Euclide pour démontrer l'infinité de l'ensemble des nombres premiers. Cette approche, que l'on pourrait qualifier de lexicale, utilise des mots de représentation des entiers par leurs restes modulaires selon les nombres premiers successifs.

2 Énoncé

On appelle *nombres premiers jumeaux* deux nombres premiers dont la différence est 2.
Exemples :

3 et 5 sont des nombres premiers jumeaux.
29 et 31 sont des nombres premiers jumeaux.

La conjecture des nombres premiers jumeaux stipule que l'ensemble des nombres premiers jumeaux est infini.

3 Représentation par les restes

Représentons les premiers entiers naturels par leurs restes modulo les nombres premiers successifs.
Pour passer du *"mot"* d'un nombre au mot de son successeur*, on ajoute à ce mot le mot n-uplet infini $(1, 1, 1, 1, \ldots)$ qui représente l'entier naturel 1.

*selon l'arithmétique de Peano

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

Observons quelques représentations par les restes qui sont pertinentes par rapport à la conjecture des nombres premiers jumeaux.

6, le nombre pair juste entre les deux nombres premiers jumeaux 5 et 7 a pour représentation 0 0 1 6 6 6 ... . Il a un 1 en troisième position parce que 5 a un 0 à cette position (un nombre premier est congru à 0 modulo lui-même, jamais congru à 0 modulo un nombre premier qui lui est strictement inférieur et congru à lui-même modulo tout nombre premier qui lui est strictement supérieur). 6 a un 6 en quatrième position parce que 7 a un 0 à cette position-là (le reste de 7 modulo lui-même). Les deux premières lettres du mot de représentation du nombre 6 ne sont ni des 1 ni des $p_k - 1$ (ni 1 ni 1 dans la colonne correspondant au nombre premier 2, ni 1 ni 2 dans la colonne correspondant au nombre premier 3) car si tel était le cas, l'un ou l'autre de 5 ou 7 serait composé.

18, entre 17 et 19, a pour représentation 0 0 3 4 7 5 1 18 ... : il n'a ni 1 ni $p_k - 1$ parmi ses six premières lettres, correspondant à ses restes modulo $2, 3, 5, 7, 11$ et 13. Le mot de 18 a un 1 en septième position (correspondant à son reste modulo 17 : $18 = 17 + 1$) et 18 a un reste de 18 en huitième position (correspondant à son reste modulo $19 = 18 + 1$).

Un nombre pair $p_i + 1$ juste entre deux nombres premiers jumeaux p_i et $p_i + 2$ a son écriture qui se caractérise ainsi :

- elle ne contient ni 1 ni $p_k - 1$ pour tout module p_k strictement inférieur à p_i ;
- elle contient un 1 représentant le reste de $p_i + 1$ $(mod\ p_i)$;
- elle contient un $p_i + 1$ représentant le reste de $p_i + 1$ $(mod\ p_i + 2)$.

4 Euclide et l'infinité de l'ensemble des nombres premiers jumeaux

Supposons que l'ensemble des nombres naturels pairs juste entre deux nombres premiers jumeaux soit fini. On note dans un tableau les restes des nombres pairs en question modulo les nombres premiers successifs allant de 2 à $p_{supermax}$ où $p_{supermax}$ est le plus grand des nombres premiers inférieur à $\prod_{p_k=2}^{p_i} p_k$, p_i étant quant à lui le plus grand nombre premier inférieur à $(p_{max} + 2)^2$, si p_{max} est le plus grand des nombres premiers jumeaux cadets en nombre fini.

	2	3	5	7	11	...		...	$p_{dernier\_1}$	...	$p_{supermax}$
$pair_1 = 4$	0	1	4	4	4	...		...		...	
$pair_2 = 6$	0	0	1	6	6	...		...		...	
$pair_3 = 12$	0	0	2	5	1	...		...		...	
	...	...	...	...	...	...	1	...	...	...	
$pair_n$	0	0			...		...		1	...	

Remarquons dans le tableau l'existence d'une "sorte de diagonale" de restes 1, correspondant aux restes de nos nombres pairs en nombre fini modulo le nombre premier jumeau cadet qui est leur prédécesseur. Dans la mesure où tous les nombres premiers ne sont pas des jumeaux, un 1 d'une ligne est toujours dans une colonne à droite de celle dans laquelle se trouve le 1 de la ligne précédente, d'où l'expression "sorte de diagonale".

Inventons un nouveau nombre pair qui n'appartient pas au tableau alors qu'il aurait dû le faire. Ce nombre est $\#p_{dernier\_1}$, où $p_{dernier\_1}$ est le nombre premier précédant le dernier nombre pair recensé dans le tableau initial et où la notation $\#p_k$ désigne la "primorielle" de p_k, i.e. le produit de tous les nombres premiers inférieurs ou égaux à p_k. Il n'a que des restes nuls pour tous les nombres premiers compris entre 2 et $p_{dernier\_1}$. Il est plus grand que le dernier pair recensé, il est plus petit que le produit des modules compris entre 2 et $p_{supermax}$ et pourtant, il n'est pas dans le tableau recensant tous les nombres pairs juste entre deux jumeaux, supposé fini, initial.

On a inventé un ensemble de restes qui n'était pas déjà une ligne du tableau. Si notre ensemble d'ensembles de restes avait été complet, il aurait dû contenir cette nouvelle ligne or il ne la contient pas. Cela est contradictoire avec notre hypothèse de finitude de l'ensemble des nombres premiers jumeaux. L'idée du codage entraîne la contradiction. Cet ensemble de restes n'est peut-être pas le codage d'un nombre pair juste entre deux nombres premiers jumeaux : de la même manière, la construction par Euclide d'un "nouveau" nombre premier de la forme $\#p_k + 1$ ne permet pas toujours d'obtenir un nombre effectivement premier. Par exemple, 2.3.5.7.11.13 = 30031 = 59.509. On sait cependant qu'il est inférieur au produit des modules considérés et que le théorème des restes chinois nous permettrait2*3*5+1 de le calculer.

Infinité de l'ensemble des nombres premiers jumeaux

Denise Vella-Chemla

11/6/2012

1 Introduction

Dans cette note, on essaie de démontrer la conjecture des nombres premiers jumeaux en utilisant l'argument de la diagonale de Cantor. Cette approche, que l'on pourrait qualifier de lexicale, utilise des mots de représentation des entiers par leurs restes modulaires selon les nombres premiers successifs.

2 Énoncé

On appelle *nombres premiers jumeaux* deux nombres premiers dont la différence est 2.
Exemples :

3 et 5 sont des nombres premiers jumeaux.
29 et 31 sont des nombres premiers jumeaux.

La conjecture des nombres premiers jumeaux stipule que l'ensemble des nombres premiers jumeaux est infini.

3 Représentation par les restes

Représentons les premiers entiers naturels par leurs restes modulo les nombres premiers successifs.
Pour passer du *"mot"* d'un nombre au mot de son successeur*, on ajoute à ce mot le mot n-uplet infini $(1, 1, 1, 1, \ldots)$ qui représente l'entier naturel 1.

*selon l'arithmétique de Peano

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

Observons quelques représentations par les restes qui sont pertinentes par rapport à la conjecture des nombres premiers jumeaux.

6, le nombre pair juste entre les deux nombres premiers jumeaux 5 et 7 a pour représentation 0 0 1 6 6 6 ... . Il a un 1 en troisième position parce que 5 a un 0 à cette position (un nombre premier est congru à 0 modulo lui-même, jamais congru à 0 modulo un nombre premier qui lui est strictement inférieur et congru à lui-même modulo tout nombre premier qui lui est strictement supérieur). 6 a un 6 en quatrième position parce que 7 a un 0 à cette position-là (le reste de 7 modulo lui-même). Les deux premières lettres du mot de représentation du nombre 6 ne sont ni des 1 ni des $p_k - 1$ (ni 1 ni 1 dans la colonne correspondant au nombre premier 2, ni 1 ni 2 dans la colonne correspondant au nombre premier 3) car si tel était le cas, l'un ou l'autre de 5 ou 7 serait composé.

18, entre 17 et 19, a pour représentation 0 0 3 4 7 5 1 18 ... : il n'a ni 1 ni $p_k - 1$ parmi ses six premières lettres, correspondant à ses restes modulo $2, 3, 5, 7, 11$ et 13. Le mot de 18 a un 1 en septième position (correspondant à son reste modulo 17 : $18 = 17 + 1$) et 18 a un reste de 18 en huitième position (correspondant à son reste modulo $19 = 18 + 1$).

Un nombre pair $p_i + 1$ juste entre deux nombres premiers jumeaux p_i et $p_i + 2$ a son écriture qui se caractérise ainsi :

- elle ne contient ni 1 ni $p_k - 1$ pour tout module p_k strictement inférieur à p_i ;
- elle contient un 1 représentant le reste de $p_i + 1$ $(mod\ p_i)$;
- elle contient un $p_i + 1$ représentant le reste de $p_i + 1$ $(mod\ p_i + 2)$.

4 Diagonale de Cantor

Supposons que l'ensemble des nombres naturels pairs juste entre deux nombres premiers jumeaux soit fini. On note dans un tableau les restes des nombres pairs en question modulo les nombres premiers successifs allant de 2 à $p_{supermax}$ où $p_{supermax}$ est le plus grand des nombres premiers inférieur à $\prod_{p_k=2}^{p_i} p_k$, p_i étant quant à lui le plus grand nombre premier inférieur à $(p_{max} + 2)^2$, si p_{max} est le plus grand des nombres premiers jumeaux cadets en nombre fini.

	2	3	5	7	11	...		...		...	$p_{dernier\_1}$	...	$p_{supermax}$
$pair_1 = 4$	0	1	$\boxed{\mathrm{r}_{1,1}}$					...		...		...	
$pair_2 = 6$	0	0	1	$\boxed{\mathrm{r}_{2,1}}$				...		...		...	
$pair_3 = 12$	0	0			$\boxed{\mathrm{r}_{3,1}} = 1$			...		...		...	
						...		...	1	...		...	
$pair_n$	0	0					$\boxed{\mathrm{r}_{n,c_n}}$	...		...	1	...	

La diagonale utilisée pour appliquer l'argument de Cantor est la troisième diagonale descendante, dont on a encadré les éléments dans le tableau. Remarquons également dans ce tableau l'existence d'une "sorte de diagonale" de restes 1, correspondant aux restes de nos nombres pairs en nombre fini modulo le nombre premier jumeau cadet qui est leur prédécesseur. Dans la mesure où tous les nombres premiers ne sont pas des jumeaux, un 1 d'une ligne est toujours dans une colonne à droite de celle dans laquelle se trouve le 1 de la ligne précédente, d'où l'expression "sorte de diagonale".

Pour "perturber la diagonale", on change chacun des restes modulaires qui lui appartiennent par un autre reste modulaire selon le module considéré, le nouveau reste choisi devant respecter deux contraintes seulement : ne pas être égal à 1 (pour assurer que le prédécesseur de ce nombre pair est bien un nombre premier) et ne pas être égal à $p_k - 1$ quand on traite le module premier p_k (pour assurer que le successeur de ce nombre pair est bien un nombre premier également). On complète le préfixe ainsi formé par des nombres respectant la même contrainte (ni 1 ni $p_k - 1$) jusqu'à la position du 1 dans le mot du dernier pair de l'ensemble fini des pairs que l'on a recensés initialement. Les conditions imposées garantissent que son prédécesseur et son successeur n'ont tous deux aucun diviseur inférieur ou égal à $p_{dernier\_1}$,le nombre premier précédant le dernier nombre pair recensé dans le tableau initial. Mais on n'arrive pas à trouver comment démontrer que le prédécesseur et le successeur de ce nombre doivent par conséquent être premiers. Le nouveau nombre ajouté au tableau se calcule par le théorème des restes chinois. Il est inférieur au produit des modules et aurait donc dû apparaître dans le tableau initial.

On a inventé un ensemble de restes qui n'était pas déjà une ligne du tableau. Si notre ensemble d'ensembles de restes avait été complet, il aurait dû contenir cette nouvelle ligne or il ne la contient pas. Cela est contradictoire avec notre hypothèse de finitude de l'ensemble des nombres premiers jumeaux. L'idée du codage entraîne la contradiction[†]. On s'est appuyé pour pouvoir construire le "nouvel ensemble de restes" sur l'*Axiome du choix* qui a pour conséquence qu'on peut toujours choisir dans des ensembles d'entiers naturels contenant chacun 5 nombres ou plus, un nombre dans chaque ensemble, en respectant la contrainte que, dans chacun des ensembles, l'élément choisi est différent de deux valeurs données (en l'occurrence 1 et $p_k - 1$).

[†]Il faudrait trouver un moyen de faire en sorte que cet ensemble de restes soit le codage d'un nombre pair juste entre deux nombres premiers jumeaux, car notre manière de construire le préfixe de son mot nous garantit qu'il n'appartenait pas à l'ensemble des nombres pairs juste entre deux nombres premiers jumeaux que l'on a supposé fini initial. La constitution même de ce nouvel ensemble de restes ne nous garantit cependant pour l'instant pas que c'est un nombre pair juste entre deux nombres premiers jumeaux. On sait cependant qu'il est inférieur au produit des modules considérés et que le théorème des restes chinois nous permet de le calculer. Il reste à démontrer qu'il a un peu plus loin dans son écriture, mais c'est forcément après $p_{supermax}$ car sinon notre nouveau nombre aurait fait partie de l'ensemble fini initial, un reste de 1 et un reste égal à lui-même selon deux nombres premiers successifs.

Infinité de l'ensemble des nombres premiers jumeaux

Denise Vella-Chemla

14/6/2012

1 Énoncé

On appelle *nombres premiers jumeaux* deux nombres premiers dont la différence est 2.

Exemples :

3 et 5 sont des nombres premiers jumeaux.
29 et 31 sont des nombres premiers jumeaux.

La conjecture des nombres premiers jumeaux stipule que l'ensemble des nombres premiers jumeaux est infini. On essaie ci-après de démontrer la conjecture des nombres premiers jumeaux en utilisant un argument similaire à celui d'Euclide pour démontrer l'infinité de l'ensemble des nombres premiers.

2 Euclide et l'infinité de l'ensemble des nombres premiers jumeaux

Supposons que l'ensemble des nombres premiers jumeaux

$$\mathcal{J} = \{3, 5, 7, 11, 13, 17, 19, 29, 31, 41, 43, \ldots, j_{max}\}$$

soit fini.

Appelons j_{max} le plus grand des nombres premiers jumeaux, $j_{max} - 2$ appartient lui-aussi à $\mathcal{J}$.
On note $\#p_k$ la *primorielle* de p_k qui est le produit de tous les nombres premiers inférieurs ou égaux à p_k.

Intéressons-nous aux deux nombres entiers naturels $n_{moins} = \#j_{max} - 1$ et $n_{plus} = \#j_{max} + 1$.

Le second de ces deux nombres, n_{plus}, a un diviseur premier p. Cependant, p n'est pas l'un des nombres premiers inférieurs ou égaux à j_{max} car sinon p serait un diviseur de n_{plus}, du produit $\#j_{max}$, et donc aussi de leur différence $n_{plus} - \#j_{max} = 1$, ce qui est impossible (ceci est l'argument utilisé par Euclide pour prouver l'infinitude de l'ensemble des nombres premiers ; il est à noter que la construction par Euclide d'un "nouveau" nombre premier de la forme $\#p_k + 1$ ne permet pas toujours d'obtenir un nombre effectivement premier. Par exemple, $2.3.5.7.11.13 = 30031 = 59.509$).

Le premier de ces deux nombres, n_{moins}, a un diviseur premier p'. Cependant, p' n'est pas l'un des nombres premiers inférieurs ou égaux à j_{max} car sinon p' serait un diviseur de n_{moins}, du produit $\#j_{max}$, et donc aussi de leur différence $n_{moins} - \#j_{max} = -1$, ce qui est impossible. En fait, dit de cette manière, cela est faux car $\#j_{max} - 1$ a clairement plusieurs diviseurs. Ne peut-on dire cependant $\#j_{max} - 1$, étant congru à -1 selon tout p_k inférieur ou égal à j_{max} ne peut être premier selon le même argument qu'Euclide utilise et qui semble être équivalent à $\#j_{max}+1$ étant congru à 1 selon tout p_k inférieur ou égal à j_{max}, est premier.

On a trouvé deux nombres, nécessairement premiers, dont la différence est 2, et qui n'appartenaient pas à l'ensemble $\mathcal{J}$ initial.

Ainsi, un ensemble fini $\mathcal{J} = \{3, 5, 7, 11, 13, 17, 19, 29, 31, 41, 43, \ldots, j_{max}\}$ ne peut constituer la collection de *tous* les nombres premiers jumeaux.

1 Une tentative de minoration probabiliste

Si on utilise les inégalités de Bonferroni, qui généralisent l'inégalité de Boole, et qui fournissent des majorants et des minorants de la probabilité d'unions finies d'événements, on voit que l'on peut minorer le nombre de décompositions de Goldbach pour les doubles de nombres premiers (de la forme $2p$) par :

$$\frac{\not{2}\, p}{\not{2}}\frac{1}{2}\prod_{\substack{p_k=3,\\ p_k\ premier}}^{p_k=\lfloor\sqrt{2p}\rfloor}\left(1-\frac{2}{p_k}\right)$$

Cependant, par programme, la minoration n'a pas lieu avant même le double de nombre premier 200 006 comme attesté dans le tableau suivant :

n	$NbDG(n)$	*minoration proposée*
202	9	$4,99451$
2 018	28	$26,8755$
20 014	174	$164,054$
200 006	1 071	$1\,101,84$
2 000 006	7 336	$7\,885,59$
20 000 038	53 269	$58\,711,6$

Si l'on poursuit le raisonnement, la minoration du nombre de décompositions de Goldbach pour les doubles de nombres composés (de la forme $2c$) devrait être quant à elle :

$$\frac{\not{2}\, c}{\not{2}}\frac{1}{2}\prod_{\substack{p_k=3,\\ p_k\ premier,\\ p_k\nmid c}}^{p_k=\lfloor\sqrt{2p}\rfloor}\left(1-\frac{2}{p_k}\right)\prod_{\substack{p_k=3,\\ p_k\ premier,\\ p_k\mid c}}^{p_k=\lfloor\sqrt{2p}\rfloor}\left(1-\frac{1}{p_k}\right)$$

Dans la mesure où $1-\frac{2}{p_k}<1-\frac{1}{p_k}$, un double de nombre composé devrait toujours avoir davantage de décompositions de Goldbach qu'un double de nombre premier le divisant. Le nombre de décompositions de Goldbach d'un nombre pair de la forme $6p$ devrait être approximativement le double de celle du nombre pair double de nombre premier de la forme $2p$ correspondant. Le nombre de décompositions de Goldbach d'un nombre pair de la forme $10p$ devrait être approximativement plus grande dans un rapport de $\frac{4}{3}$ que celle du nombre pair double de nombre premier de la forme $2p$ correspondant. Le nombre de décompositions de Goldbach d'un nombre pair de la forme $14p$ devrait être approximativement plus grande dans un rapport de $\frac{6}{5}$ que celle du nombre pair double de nombre premier de la forme $2p$ correspondant. Le nombre de décompositions de Goldbach d'un nombre pair de la forme $30p$ devrait être approximativement plus grande dans un rapport de $\frac{8}{3}$ que celle du nombre pair double de nombre premier de la forme $2p$ correspondant. Cependant, le tableau suivant montre qu'il y a beaucoup plus de décompositions de Goldbach que les minorations proposées :

$2p$	$6p$	$10p$	$14p$	$30p$
202	606	1 010	1 414	3 030
2 018	6 054	10 090	14 126	30 270
20 014	60 042	100 070	140 098	300 210
200 006	600 018	1 000 030	1 400 042	3 000 090
2 000 006	6 000 018	10 000 030	14 000 042	30 000 090
20 000 038	60 000 114	100 000 190	140 000 266	300 000 570

$NbDg(2p)$	$NbDg(6p)$	$NbDg(10p)$	$NbDg(14p)$	$NbDg(30p)$
9	27	25	30	110
28	140	136	157	629
174	809	806	957	3 951
1 071	5 306	5 421	6 405	27 311
7 336	37 319	38 805	46 681	201 989
53 269	278 690			

Découverte d'une loi tout extraordinaire par rapport à certaines sommes de restes des nombres premiers

Denise Vella-Chemla

7/7/2012

1 Introduction

Dans cette note, on présente une découverte surprenante que l'on vient d'effectuer sur certaines sommes de restes des nombres premiers.

Représentons les premiers entiers naturels par leurs restes modulo les nombres premiers successifs.
Pour passer du *"mot"* d'un nombre au mot de son successeur selon l'arithmétique de Peano, on ajoute à ce mot le mot n-uplet infini $(1, 1, 1, 1, \ldots)$ qui représente l'entier naturel 1.

mod	2	3	5	7	11	13	17	19	...
1	1	1	1	1	1	1	1	1	...
2	⓪	2	2	2	2	2	2	2	...
3	①	⓪	3	3	3	3	3	3	...
4	⓪	①	4	4	4	4	4	4	...
5	①	②	⓪	5	5	5	5	5	...
6	⓪	⓪	①	6	6	6	6	6	...
7	①	①	②	⓪	7	7	7	7	...
8	⓪	②	③	①	8	8	8	8	...
9	①	⓪	④	②	9	9	9	9	...
10	⓪	①	⓪	③	10	10	10	10	...
11	①	②	①	④	⓪	11	11	11	...
12	⓪	⓪	②	⑤	①	12	12	12	...
13	①	①	③	⑥	②	⓪	13	13	...
14	⓪	②	④	⓪	③	①	14	14	...
15	①	⓪	⓪	①	④	②	15	15	...

On a entouré dans la table les restes que l'on va sommer au paragraphe suivant.

2 Calcul des sommes de restes de chaque nombre entier

Pour copier la forme d'un paragraphe de l'article d'Euler *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs**, introduisons la fonction f qui associe à tout x entier la somme des restes de x dans ses divisions par tous les nombres premiers inférieurs ou égaux à x.

On peut modifier une phrase qu'Euler utilise pour présenter les images par sa fonction sommes des diviseurs des nombres de 1 à 100 ainsi : *pour mettre devant les yeux la progression des sommes des restes des nombres selon les modules premiers qui leur sont inférieurs, j'ajouterai la table suivante qui contient ces sommes pour les nombres naturels depuis l'unité jusqu'à 100.*

*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.

$f(1) = 0$	$f(21) = 26$	$f(41) = 74$	$f(61) = 171$	$f(81) = 308$
$f(2) = 0$	$f(22) = 21$	$f(42) = 75$	$f(62) = 156$	$f(82) = 287$
$f(3) = 1$	$f(23) = 29$	$f(43) = 88$	$f(63) = 164$	$f(83) = 309$
$f(4) = 1$	$f(24) = 33$	$f(44) = 89$	$f(64) = 180$	$f(84) = 320$
$f(5) = 3$	$f(25) = 37$	$f(45) = 95$	$f(65) = 180$	$f(85) = 321$
$f(6) = 1$	$f(26) = 31$	$f(46) = 84$	$f(66) = 182$	$f(86) = 299$
$f(7) = 4$	$f(27) = 37$	$f(47) = 98$	$f(67) = 200$	$f(87) = 290$
$f(8) = 6$	$f(28) = 37$	$f(48) = 108$	$f(68) = 200$	$f(88) = 300$
$f(9) = 7$	$f(29) = 46$	$f(49) = 116$	$f(69) = 193$	$f(89) = 323$
$f(10) = 4$	$f(30) = 46$	$f(50) = 124$	$f(70) = 198$	$f(90) = 337$
$f(11) = 8$	$f(31) = 56$	$f(51) = 119$	$f(71) = 217$	$f(91) = 341$
$f(12) = 8$	$f(32) = 65$	$f(52) = 119$	$f(72) = 232$	$f(92) = 340$
$f(13) = 13$	$f(33) = 62$	$f(53) = 134$	$f(73) = 252$	$f(93) = 330$
$f(14) = 10$	$f(34) = 54$	$f(54) = 145$	$f(74) = 234$	$f(94) = 305$
$f(15) = 8$	$f(35) = 53$	$f(55) = 145$	$f(75) = 247$	$f(95) = 305$
$f(16) = 12$	$f(36) = 59$	$f(56) = 152$	$f(76) = 247$	$f(96) = 324$
$f(17) = 18$	$f(37) = 70$	$f(57) = 146$	$f(77) = 250$	$f(97) = 348$
$f(18) = 20$	$f(38) = 61$	$f(58) = 131$	$f(78) = 253$	$f(98) = 364$
$f(19) = 27$	$f(39) = 57$	$f(59) = 147$	$f(79) = 274$	$f(99) = 375$
$f(20) = 28$	$f(40) = 62$	$f(60) = 154$	$f(80) = 289$	$f(100) = 393$

Et là, chose extraordinaire, lorsqu'on calcule les différences entre les images par f de deux nombres entiers successifs, on réalise que ces différences nous permettent de voir apparaître trivialement les nombres premiers car les différences en question pour ces nombres sont les nombres entiers naturels successifs depuis 1.

$f(1) = 0$		$f(21) = 26$		$f(41) = 74$	12	$f(61) = 171$	17	$f(81) = 308$			
$f(2) = 0$		$f(22) = 21$		$f(42) = 75$		$f(62) = 156$		$f(82) = 287$			
$f(3) = 1$	1	$f(23) = 29$	8	$f(43) = 88$	13	$f(63) = 164$		$f(83) = 309$	22		
$f(4) = 1$		$f(24) = 33$		$f(44) = 89$		$f(64) = 180$		$f(84) = 320$			
$f(5) = 3$	2	$f(25) = 37$		$f(45) = 95$		$f(65) = 180$		$f(85) = 321$			
$f(6) = 1$		$f(26) = 31$		$f(46) = 84$		$f(66) = 182$		$f(86) = 299$			
$f(7) = 4$	3	$f(27) = 37$		$f(47) = 98$	14	$f(67) = 200$	18	$f(87) = 290$			
$f(8) = 6$		$f(28) = 37$		$f(48) = 108$		$f(68) = 200$		$f(88) = 300$			
$f(9) = 7$		$f(29) = 46$	9	$f(49) = 116$		$f(69) = 193$		$f(89) = 323$	23		
$f(10) = 4$		$f(30) = 46$		$f(50) = 124$		$f(70) = 198$		$f(90) = 337$			
$f(11) = 8$	4	$f(31) = 56$	10	$f(51) = 119$		$f(71) = 217$	19	$f(91) = 341$			
$f(12) = 8$		$f(32) = 65$		$f(52) = 119$		$f(72) = 232$		$f(92) = 340$			
$f(13) = 13$	5	$f(33) = 62$		$f(53) = 134$	15	$f(73) = 252$	20	$f(93) = 330$			
$f(14) = 10$		$f(34) = 54$		$f(54) = 145$		$f(74) = 234$		$f(94) = 305$			
$f(15) = 8$		$f(35) = 53$		$f(55) = 145$		$f(75) = 247$		$f(95) = 305$			
$f(16) = 12$		$f(36) = 59$		$f(56) = 152$		$f(76) = 247$		$f(96) = 324$			
$f(17) = 18$	6	$f(37) = 70$	11	$f(57) = 146$		$f(77) = 250$		$f(97) = 348$	24		
$f(18) = 20$		$f(38) = 61$		$f(58) = 131$		$f(78) = 253$		$f(98) = 364$			
$f(19) = 27$	7	$f(39) = 57$		$f(59) = 147$	16	$f(79) = 274$	21	$f(99) = 375$			
$f(20) = 28$		$f(40) = 62$		$f(60) = 154$		$f(80) = 289$		$f(100) = 393$			

On se contentera de citer Euler dans le texte, en utilisant l'orthographe de son époque : *Ces choses remarquées, il ne sera pas difficile de faire l'application de cette formule à chaque nombre premier proposé et de se convaincre de sa vérité, par autant d'exemples qu'on voudra développer. Et comme je dois avouër 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. [...] Je crois ces exemples suffisants pour ne pas s'imaginer que c'est par un pur hazard que ma règle se trouve d'accord avec la vérité.*

Méthode constructive pour trouver les décomposants de Goldbach d'un nombre pair ou les couples de nombres premiers jumeaux

Denise Vella-Chemla

1/9/2012

1 Introduction

Dans cette note, on présente une méthode constructive qui permet de trouver les décomposants de Goldbach d'un nombre pair ou bien les nombres pairs entre deux nombres premiers jumeaux en utilisant le théorème des restes chinois.

Pour trouver certains décomposants de Goldbach de x, on s'intéresse aux nombres de l'intervalle de nombres $[1, A]$ où A est le produit des nombres premiers compris entre 2 et $\lfloor\sqrt{x}\rfloor$: on élimine de l'intervalle $[1, A]$ tout nombre y qui aurait un reste nul selon un module premier inférieur à $\lfloor\sqrt{x}\rfloor$ (quitte à éliminer ce faisant de petits nombres premiers inférieurs à $\sqrt{x}$ qui pourraient cependant être des décomposants de Goldbach de x). On élimine également tout nombre qui partagerait un reste modulaire avec x selon un module premier inférieur à $\lfloor\sqrt{x}\rfloor$, ce qui aurait pour conséquence que son complémentaire à x serait composé. Il faut enfin s'assurer de l'appartenance du nombre à un certain intervalle pour qu'il soit solution.

Tous les nombres "atteints" par cette méthode n'ont aucun diviseur premier inférieur à $\sqrt{x}$. Si l'on pouvait être assuré que cette méthode permet à tout coup d'atteindre un nombre inférieur à $x/2$, ce nombre n'ayant pas de diviseur inférieur à $\sqrt{x}$ serait premier. De plus, comme il ne partagerait aucun reste avec x, son complémentaire à x serait premier également, ce qui ferait de lui un décomposant de Goldbach de x. Malheureusement, on verra qu'on n'arrive pas pour l'instant à assurer l'appartenance des nombres trouvés à certains intervalles d'entiers.

Pour trouver certains nombres pairs éventuellement compris entre deux nombres premiers jumeaux, on procède de la même manière en se plaçant sur un intervalle $[1, A]$. On élimine cette fois tout nombre qui aurait un reste égal à 1 de façon à ce que le nombre qui le précède n'ait aucun reste nul selon un module qui lui serait inférieur, ce qui l'empêcherait d'être premier. On élimine également tout nombre qui aurait un reste valant $p_k - 1$ selon un module quelconque p_k de façon à ce que le nombre qui le suit n'ait pas de reste nul selon le module p_k en question, ce qui pourrait l'empêcherait d'être premier. Il faut enfin s'assurer de l'appartenance du nombre à un certain intervalle pour qu'il soit solution.

2 Bases modulaires et familles génératrices utilisées dans l' application du théorème des restes chinois

Pour les nombres pairs compris entre 10 et 24 (i.e. compris entre le carré de 3 et le carré de 5), on prendra le couple $(2, 3)$ comme base modulaire. On devra alors utiliser comme famille génératrice le couple $(3, 4)$ car $3 = 1 \times 3$ est congru à 1 (mod 2) et $4 = 2 \times 2$ est congru à 1 (mod 3) pour trouver les combinaisons linéaires fournies par le théorème des restes chinois. On peut en quelque sorte considérer que le nombre 3 est le "vecteur" $(1, 0)$ tandis que le nombre 4 est le "vecteur" $(0, 1)$.

Pour les nombres pairs compris entre 26 et 48 (i.e. compris entre le carré de 5 et le carré de 7), on prendra comme base modulaire de nombres premiers le triplet $(2, 3, 5)$. On devra utiliser comme famille génératrice le triplet $(15, 10, 6)$ car $15 = 1 \times 3 \times 5$ est congru à 1 $(mod\ 2)$, $10 = 1 \times 2 \times 5$ est congru à 1 $(mod\ 3)$ et $6 = 1 \times 2 \times 3$ est congru à 1 $(mod\ 5)$. Comme au paragraphe précédent, on peut considérer que $15 = (1, 0, 0)$, $10 = (0, 1, 0)$ et $6 = (0, 0, 1)$.

Pour les nombres pairs compris entre 50 et 120 (i.e. compris entre le carré de 7 et le carré de 11), on prendra comme base modulaire de nombres premiers le quadruplet $(2, 3, 5, 7)$, on utilise comme famille génératrice le quadruplet $(105, 70, 126, 120)$ car $105 = 1 \times 3 \times 5 \times 7$ est congru à 1 $(mod\ 2)$, $70 = 1 \times 2 \times 5 \times 7$ est congru à 1 $(mod\ 3)$, $126 = 3 \times 2 \times 3 \times 7$ est congru à 1 $(mod\ 5)$ et $120 = 4 \times 2 \times 3 \times 5$ est congru à 1 $(mod\ 7)$.

Pour trouver les décomposants de Goldbach de x, seront générés par la méthode

$$\prod_{\substack{p_k\ premier \\ p_k \nmid x \\ 3 \leq p_k \leq \lfloor \sqrt{x} \rfloor}} (p_k - 2) \prod_{\substack{p_k\ premier \\ p_k | x \\ 3 \leq p_k \leq \lfloor \sqrt{x} \rfloor}} (p_k - 1)$$

nombres entiers dont seule l'appartenance à certains intervalles d'entiers assurera qu'ils sont effectivement des décomposants de Goldbach du nombre pair x considéré.

Pour la conjecture des nombres premiers jumeaux, p étant un nombre premier impair donné, seront générés par la méthode d'élimination systématique des restes 1 ou $p_k - 1$ (on travaille de manière "absolue" plutôt que "relativement à" x)

$$\prod_{5 \leq p_k \leq p} (p_k - 2)$$

nombres pairs dont seule l'appartenance à certains intervalles d'entiers assurera qu'ils sont effectivement des nombres pairs entre deux nombres premiers jumeaux. On cherchera à trouver un nouveau couple de nombres premiers jumeaux entre une primorielle* et la suivante, de façon à mettre en bijection l'infinité de l'ensemble des nombres premiers prouvée par Euclide et l'infinité de l'ensemble des nombres premiers jumeaux.

3 Calcul de décomposants de Goldbach

Dans les tableaux ci-après, on fournit l'écriture par les restes, la combinaison linéaire, la classe d'équivalence fournie par le théorème des restes chinois modulo le produit de nombres premiers de la base modulaire utilisée et le fait que ce nombre soit décomposant de Goldbach du nombre pair considéré.

3.1 Décomposants de Goldbach de nombres pairs compris entre 10 et 24

Pour trouver certains décomposants de Goldbach des nombres pairs compris entre $10 = 3^2 + 1$ et $24 = 5^2 - 1$, on utilise la base modulaire $(2, 3)$, la famille génératrice $(3, 4)$ et on travaille modulo $6 = 2 \times 3$.

On note dans un tableau les vecteurs éventuellement solutions car jamais congrus à 0 ou à x selon aucun module de la base, la combinaison linéaire correspondante, le nombre inférieur à 6 de mêmes classes d'équivalence sur les corps finis et d'une croix dans la dernière colonne si le nombre de la troisième colonne est décomposant de Goldbach du nombre pair considéré.

- $x = 10 = (0, 1)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 6)$	*décomp. de Goldbach de* x
$(1, 2)$	$1 \times 3 + 2 \times 4 = 11$	5	$*$

*On appelle primorielle d'un nombre premier p le produit de tous les nombres premiers inférieurs ou égaux à p.

- $x = 12 = (0, 0)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 6)$	*décomp. de Goldbach de* x
$(1, 1)$	$1 \times 3 + 1 \times 4 = 7$	1	
$(1, 2)$	$1 \times 3 + 2 \times 4 = 11$	5	$*$

- $x = 14 = (0, 2)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 6)$	*décomp. de Goldbach de* x
$(1, 1)$	$1 \times 3 + 1 \times 4 = 7\ (*)$	1	

- $x = 16 = (0, 1)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 6)$	*décomp. de Goldbach de* x
$(1, 2)$	$1 \times 3 + 2 \times 4 = 11$	5	$*$

- $x = 18 = (0, 0)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 6)$	*décomp. de Goldbach de* x
$(1, 1)$	$1 \times 3 + 1 \times 4 = 7$	1	
$(1, 2)$	$1 \times 3 + 2 \times 4 = 11$	5	$*$

- $x = 20 = (0, 2)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 6)$	*décomp. de Goldbach de* x
$(1, 1)$	$1 \times 3 + 2 \times 4 = 7\ (*)$	1	

- $x = 22 = (0, 1)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 6)$	*décomp. de Goldbach de* x
$(1, 2)$	$1 \times 3 + 2 \times 4 = 11$	5	$*$

- $x = 24 = (0, 0)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 6)$	*décomp. de Goldbach de* x
$(1, 1)$	$1 \times 3 + 1 \times 4 = 7$	1	
$(1, 2)$	$1 \times 3 + 2 \times 4 = 11$	5	$*$

3.2 Décomposants de Goldbach de nombres pairs compris entre 26 et 48

Pour trouver certains décomposants de Goldbach des nombres pairs compris entre $26 = 5^2+1$ et $48 = 7^2-1$, on utilise la base modulaire $(2, 3, 5)$, la famille génératrice $(15, 10, 6)$ et on travaille modulo $30 = 2 \times 3 \times 5$.

On note dans un tableau les vecteurs éventuellement solutions car jamais congrus à 0 ou à x selon aucun module de la base, la combinaison linéaire correspondante, le nombre inférieur à 30 de mêmes classes d'équivalence sur les corps finis et d'une croix dans la dernière colonne si le nombre de la troisième colonne est décomposant de Goldbach du nombre pair considéré.

- $x = 26 = (0, 2, 1)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 30)$	*décomp. de Goldbach de* x
$(1, 1, 2)$	$1 \times 15 + 1 \times 10 + 2 \times 6 = 37$	7	$*$
$(1, 1, 3)$	$1 \times 15 + 1 \times 10 + 3 \times 6 = 43$	13	$*$
$(1, 1, 4)$	$1 \times 15 + 1 \times 10 + 4 \times 6 = 49$	19	$*$

- $x = 28 = (0, 1, 3)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 30)$	*décomp. de Goldbach de* x
$(1, 2, 1)$	$1 \times 15 + 2 \times 10 + 1 \times 6 = 41$	11	$*$
$(1, 2, 2)$	$1 \times 15 + 2 \times 10 + 2 \times 6 = 47$	17	$*$
$(1, 2, 4)$	$1 \times 15 + 2 \times 10 + 4 \times 6 = 59$	29	

- $x = 30 = (0, 0, 0)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 30)$	*décomp. de Goldbach de* x
$(1, 1, 1)$	$1 \times 15 + 1 \times 10 + 1 \times 6 = 31$	1	
$(1, 1, 2)$	$1 \times 15 + 1 \times 10 + 2 \times 6 = 37$	7	$*$
$(1, 1, 3)$	$1 \times 15 + 1 \times 10 + 3 \times 6 = 43$	13	$*$
$(1, 1, 4)$	$1 \times 15 + 1 \times 10 + 4 \times 6 = 49$	19	$*$
$(1, 2, 1)$	$1 \times 15 + 2 \times 10 + 1 \times 6 = 41$	11	$*$
$(1, 2, 2)$	$1 \times 15 + 2 \times 10 + 2 \times 6 = 47$	17	$*$
$(1, 2, 3)$	$1 \times 15 + 2 \times 10 + 3 \times 6 = 53$	23	$*$
$(1, 2, 4)$	$1 \times 15 + 2 \times 10 + 4 \times 6 = 59$	29	

- $x = 32 = (0, 2, 2)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 30)$	*décomp. de Goldbach de* x
$(1, 1, 1)$	$1 \times 15 + 1 \times 10 + 1 \times 6 = 31$	1	
$(1, 1, 3)$	$1 \times 15 + 1 \times 10 + 3 \times 6 = 43$	13	$*$
$(1, 1, 4)$	$1 \times 15 + 1 \times 10 + 4 \times 6 = 49$	19	$*$

- $x = 34 = (0, 1, 4)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 30)$	*décomp. de Goldbach de* x
$(1, 2, 1)$	$1 \times 15 + 2 \times 10 + 1 \times 6 = 41$	11	$*$
$(1, 2, 2)$	$1 \times 15 + 2 \times 10 + 2 \times 6 = 47$	17	$*$
$(1, 2, 3)$	$1 \times 15 + 2 \times 10 + 3 \times 6 = 53$	23	$*$

- $x = 36 = (0, 0, 1)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 30)$	*décomp. de Goldbach de* x
$(1, 1, 2)$	$1 \times 15 + 1 \times 10 + 2 \times 6 = 37$	7	$*$
$(1, 1, 3)$	$1 \times 15 + 1 \times 10 + 3 \times 6 = 43$	13	$*$
$(1, 1, 4)$	$1 \times 15 + 1 \times 10 + 4 \times 6 = 49$	19	$*$
$(1, 2, 2)$	$1 \times 15 + 2 \times 10 + 2 \times 6 = 47$	17	$*$
$(1, 2, 3)$	$1 \times 15 + 2 \times 10 + 3 \times 6 = 53$	23	$*$
$(1, 2, 4)$	$1 \times 15 + 2 \times 10 + 4 \times 6 = 59$	29	$*$

- $x = 38 = (0, 2, 3)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 30)$	*décomp. de Goldbach de* x
$(1, 1, 1)$	$1 \times 15 + 1 \times 10 + 1 \times 6 = 31$	1	
$(1, 1, 2)$	$1 \times 15 + 1 \times 10 + 2 \times 6 = 37$	7	$*$
$(1, 1, 4)$	$1 \times 15 + 1 \times 10 + 4 \times 6 = 49$	19	$*$

- $x = 40 = (0, 1, 0)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 30)$	*décomp. de Goldbach de* x
$(1, 2, 1)$	$1 \times 15 + 2 \times 10 + 1 \times 6 = 41$	11	$*$
$(1, 2, 2)$	$1 \times 15 + 2 \times 10 + 2 \times 6 = 47$	17	$*$
$(1, 2, 3)$	$1 \times 15 + 2 \times 10 + 3 \times 6 = 53$	23	$*$
$(1, 2, 4)$	$1 \times 15 + 2 \times 10 + 4 \times 6 = 59$	29	$*$

- $x = 42 = (0, 0, 2)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 30)$	*décomp. de Goldbach de* x
$(1, 1, 1)$	$1 \times 15 + 1 \times 10 + 1 \times 6 = 31$	1	
$(1, 1, 3)$	$1 \times 15 + 1 \times 10 + 3 \times 6 = 43$	13	$*$
$(1, 1, 4)$	$1 \times 15 + 1 \times 10 + 4 \times 6 = 49$	19	$*$
$(1, 2, 1)$	$1 \times 15 + 2 \times 10 + 1 \times 6 = 41$	11	$*$
$(1, 2, 3)$	$1 \times 15 + 2 \times 10 + 3 \times 6 = 53$	23	$*$
$(1, 2, 4)$	$1 \times 15 + 2 \times 10 + 4 \times 6 = 59$	29	$*$

- $x = 44 = (0, 2, 4)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 30)$	*décomp. de Goldbach de* x
$(1, 1, 1)$	$1 \times 15 + 1 \times 10 + 1 \times 6 = 31$	1	
$(1, 1, 2)$	$1 \times 15 + 1 \times 10 + 2 \times 6 = 37$	7	$*$
$(1, 1, 3)$	$1 \times 15 + 1 \times 10 + 3 \times 6 = 43$	13	$*$

- $x = 46 = (0, 1, 1)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ (*mod* 30)	*décomp. de Goldbach de* x
$(1, 2, 2)$	$1 \times 15 + 2 \times 10 + 2 \times 6 = 47$	17	$*$
$(1, 2, 3)$	$1 \times 15 + 2 \times 10 + 3 \times 6 = 53$	23	$*$
$(1, 2, 4)$	$1 \times 15 + 2 \times 10 + 4 \times 6 = 59$	29	$*$

- $x = 48 = (0, 0, 3)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ (*mod* 30)	*décomp. de Goldbach de* x
$(1, 1, 1)$	$1 \times 15 + 1 \times 10 + 1 \times 6 = 31$	1	
$(1, 1, 2)$	$1 \times 15 + 1 \times 10 + 2 \times 6 = 37$	7	$*$
$(1, 1, 4)$	$1 \times 15 + 1 \times 10 + 4 \times 6 = 49$	19	$*$
$(1, 2, 1)$	$1 \times 15 + 2 \times 10 + 1 \times 6 = 41$	11	$*$
$(1, 2, 2)$	$1 \times 15 + 2 \times 10 + 2 \times 6 = 47$	17	$*$
$(1, 2, 4)$	$1 \times 15 + 2 \times 10 + 4 \times 6 = 59$	19	$*$

3.3 Décomposants de Goldbach de nombres pairs compris entre 50 et 100, ainsi que du nombre 120 qui a de nombreux petits diviseurs

Pour trouver certains décomposants de Goldbach des nombres pairs compris entre $50 = 7^2 + 1$ et $120 = 11^2 - 1$, on utilise la base modulaire $(2, 3, 5, 7)$, la famille génératrice $(105, 70, 126, 120)$ et on travaille modulo $210 = 2 \times 3 \times 5 \times 7$.

On note dans un tableau les vecteurs éventuellement solutions car jamais congrus à 0 ou à x selon aucun module de la base, la combinaison linéaire correspondante, le nombre inférieur à 210 de mêmes classes d'équivalence sur les corps finis et d'une croix dans la dernière colonne si le nombre de la troisième colonne est décomposant de Goldbach du nombre pair considéré.

- $x = 50 = (0, 2, 0, 1)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ (*mod* 210)	*décomp. de Goldbach de* x
$(1, 1, 1, 2)$	$1 \times 105 + 1 \times 70 + 1 \times 126 + 2 \times 120$	121	
$(1, 1, 1, 3)$	$... + 120$	31	$*$
$(1, 1, 1, 4)$	$... + 120$	151	
$(1, 1, 1, 5)$	$... + 120$	61	
$(1, 1, 1, 6)$	$... + 120$	181	
$(1, 1, 2, 2)$	$1 \times 105 + 1 \times 70 + 2 \times 126 + 2 \times 120$	37	$*$
$(1, 1, 2, 3)$	$... + 120$	157	
$(1, 1, 2, 4)$	$... + 120$	67	
$(1, 1, 2, 5)$	$... + 120$	187	
$(1, 1, 2, 6)$	$... + 120$	97	
$(1, 1, 3, 2)$	$1 \times 105 + 1 \times 70 + 3 \times 126 + 2 \times 120$	163	
$(1, 1, 3, 3)$	$... + 120$	73	
$(1, 1, 3, 4)$	$... + 120$	193	
$(1, 1, 3, 5)$	$... + 120$	103	
$(1, 1, 3, 6)$	$... + 120$	13	$*$
$(1, 1, 4, 2)$	$1 \times 105 + 1 \times 70 + 4 \times 126 + 2 \times 120$	79	
$(1, 1, 4, 3)$	$... + 120$	199	
$(1, 1, 4, 4)$	$... + 120$	109	
$(1, 1, 4, 5)$	$... + 120$	19	$*$
$(1, 1, 4, 6)$	$... + 120$	139	

- $x = 52 = (0, 1, 2, 3)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 210)$	*décomp. de Goldbach de* x
$(1, 2, 1, 1)$	$1 \times 105 + 2 \times 70 + 1 \times 126 + 1 \times 120$	71	
$(1, 2, 1, 2)$	$... + 120$	191	
$(1, 2, 1, 4)$	$... + 240$	11	$*$
$(1, 2, 1, 5)$	$... + 120$	131	
$(1, 2, 1, 6)$	$... + 120$	41	$*$
$(1, 2, 3, 1)$	$1 \times 105 + 2 \times 70 + 3 \times 126 + 1 \times 120$	113	
$(1, 2, 3, 2)$	$... + 120$	23	$*$
$(1, 2, 3, 4)$	$... + 240$	53	
$(1, 2, 3, 5)$	$... + 120$	173	
$(1, 2, 3, 6)$	$... + 120$	83	
$(1, 2, 4, 1)$	$1 \times 105 + 2 \times 70 + 4 \times 126 + 1 \times 120$	29	$*$
$(1, 2, 4, 2)$	$... + 120$	149	
$(1, 2, 4, 4)$	$... + 240$	59	
$(1, 2, 4, 5)$	$... + 120$	179	
$(1, 2, 4, 6)$	$... + 120$	89	

- $x = 54 = (0, 0, 4, 5)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 210)$	*décomp. de Goldbach de* x
$(1, 1, 1, 1)$	$1 \times 105 + 1 \times 70 + 1 \times 126 + 1 \times 120$	1	
$(1, 1, 1, 2)$	$... + 120$	121	
$(1, 1, 1, 3)$	$... + 120$	31	$*$
$(1, 1, 1, 4)$	$... + 120$	151	
$(1, 1, 1, 6)$	$... + 240$	181	
$(1, 1, 2, 1)$	$1 \times 105 + 1 \times 70 + 2 \times 126 + 1 \times 120$	127	
$(1, 1, 2, 2)$	$... + 120$	37	$*$
$(1, 1, 2, 3)$	$... + 120$	157	
$(1, 1, 2, 4)$	$... + 120$	67	
$(1, 1, 2, 6)$	$... + 240$	97	
$(1, 1, 3, 1)$	$1 \times 105 + 1 \times 70 + 3 \times 126 + 1 \times 120$	43	$*$
$(1, 1, 3, 2)$	$... + 120$	163	
$(1, 1, 3, 3)$	$... + 120$	73	
$(1, 1, 3, 4)$	$... + 120$	193	
$(1, 1, 3, 6)$	$... + 240$	13	$*$
$(1, 2, 1, 1)$	$1 \times 105 + 2 \times 70 + 1 \times 126 + 1 \times 120$	71	
$(1, 2, 1, 2)$	$... + 120$	191	
$(1, 2, 1, 3)$	$... + 120$	101	
$(1, 2, 1, 4)$	$... + 120$	11	$*$
$(1, 2, 1, 6)$	$... + 240$	41	$*$
$(1, 2, 2, 1)$	$1 \times 105 + 2 \times 70 + 2 \times 126 + 1 \times 120$	197	
$(1, 2, 2, 2)$	$... + 120$	107	
$(1, 2, 2, 3)$	$... + 120$	17	$*$
$(1, 2, 2, 4)$	$... + 120$	137	
$(1, 2, 2, 6)$	$... + 240$	167	
$(1, 2, 3, 1)$	$1 \times 105 + 2 \times 70 + 3 \times 126 + 1 \times 120$	113	
$(1, 2, 3, 2)$	$... + 120$	23	$*$
$(1, 2, 3, 3)$	$... + 120$	143	
$(1, 2, 3, 4)$	$... + 120$	53	
$(1, 2, 3, 6)$	$... + 240$	83	

- $x = 56 = (0, 2, 1, 0)$

coordonnées	*combinaison linéaire*	*sol.min.*($\neq 0$) (*mod* 210)	*décomp. de Goldbach de* x
$(1,1,1,1)$	$1\times 105 + 1\times 70 + 1\times 126 + 1\times 120$	127	
$(1,1,1,2)$	$... + 120$	37	$*$
$(1,1,1,3)$	$... + 120$	157	
$(1,1,1,4)$	$... + 120$	67	
$(1,1,1,5)$	$... + 120$	187	
$(1,1,1,6)$	$... + 120$	97	
$(1,1,3,1)$	$1\times 105 + 1\times 70 + 3\times 126 + 1\times 120$	43	$*$
$(1,1,3,2)$	$... + 120$	163	
$(1,1,3,3)$	$... + 120$	73	
$(1,1,3,4)$	$... + 120$	193	
$(1,1,3,5)$	$... + 120$	103	
$(1,1,3,6)$	$... + 120$	13	$*$
$(1,1,4,1)$	$1\times 105 + 1\times 70 + 4\times 126 + 1\times 120$	169	
$(1,1,4,2)$	$... + 120$	79	
$(1,1,4,3)$	$... + 120$	199	
$(1,1,4,4)$	$... + 120$	109	
$(1,1,4,5)$	$... + 120$	19	$*$
$(1,1,4,6)$	$... + 120$	139	

- $x = 58 = (0, 1, 3, 2)$

coordonnées	*combinaison linéaire*	*sol.min.*($\neq 0$) (*mod* 210)	*décomp. de Goldbach de* x
$(1,2,1,1)$	$1\times 105 + 2\times 70 + 1\times 126 + 1\times 120$	71	
$(1,2,1,3)$	$... + 240$	101	
$(1,2,1,4)$	$... + 120$	11	$*$
$(1,2,1,5)$	$... + 120$	131	
$(1,2,1,6)$	$... + 120$	41	$*$
$(1,2,2,1)$	$1\times 105 + 2\times 70 + 2\times 126 + 1\times 120$	197	
$(1,2,2,3)$	$... + 240$	17	$*$
$(1,2,2,4)$	$... + 120$	137	
$(1,2,2,5)$	$... + 120$	47	$*$
$(1,2,2,6)$	$... + 120$	167	
$(1,2,4,1)$	$1\times 105 + 2\times 70 + 4\times 126 + 1\times 120$	29	$*$
$(1,2,4,3)$	$... + 240$	59	
$(1,2,4,4)$	$... + 120$	179	
$(1,2,4,5)$	$... + 120$	89	
$(1,2,4,6)$	$... + 120$	209	

Note : on voit apparaître sans surprise symétriquement par rapport à une ligne médiane dans le tableau certaines décompositions de Goldbach de $266 = 56 + 210$; en effet, $210 = 2\times 3\times 5\times 7$ permet de conserver les mêmes restes modulaires et cela permet de conserver la non-congruence à 0 et x des solutions.

$$\begin{aligned} 266 &= 127 + 139 \\ &= 157 + 109 \\ &= 67 + 199 \end{aligned}$$

Le tableau fournit également une décomposition de $476 = 56 + 2\times 210$ qui se décompose en $157 + 319$.

- $x = 60 = (0, 0, 0, 4)$

coordonnées	*combinaison linéaire*	*sol.min.*($\neq 0$) (*mod* 210)	*décomp. de Goldbach de* x
$(1,1,1,1)$	$1\times 105+1\times 70+1\times 126+1\times 120$	1	
$(1,1,1,2)$	$\ldots+120$	121	
$(1,1,1,3)$	$\ldots+120$	31	$*$
$(1,1,1,5)$	$\ldots+240$	61	
$(1,1,1,6)$	$\ldots+120$	181	
$(1,1,2,1)$	$1\times 105+1\times 70+2\times 126+1\times 120$	127	
$(1,1,2,2)$	$\ldots+120$	37	$*$
$(1,1,2,3)$	$\ldots+120$	157	
$(1,1,2,5)$	$\ldots+240$	187	
$(1,1,2,6)$	$\ldots+120$	97	
$(1,1,3,1)$	$1\times 105+1\times 70+3\times 126+1\times 120$	43	$*$
$(1,1,3,2)$	$\ldots+120$	163	
$(1,1,3,3)$	$\ldots+120$	73	
$(1,1,3,5)$	$\ldots+240$	103	
$(1,1,3,6)$	$\ldots+120$	13	$*$
$(1,1,4,1)$	$1\times 105+1\times 70+4\times 126+1\times 120$	169	
$(1,1,4,2)$	$\ldots+120$	79	
$(1,1,4,3)$	$\ldots+120$	199	
$(1,1,4,5)$	$\ldots+240$	19	$*$
$(1,1,4,6)$	$\ldots+120$	139	
$(1,2,1,1)$	$1\times 105+2\times 70+1\times 126+1\times 120$	71	
$(1,2,1,2)$	$\ldots+120$	191	
$(1,2,1,3)$	$\ldots+120$	101	
$(1,2,1,5)$	$\ldots+240$	131	
$(1,2,1,6)$	$\ldots+120$	41	$*$
$(1,2,2,1)$	$1\times 105+2\times 70+2\times 126+1\times 120$	197	
$(1,2,2,2)$	$\ldots+120$	107	
$(1,2,2,3)$	$\ldots+120$	17	$*$
$(1,2,2,5)$	$\ldots+240$	47	$*$
$(1,2,2,6)$	$\ldots+120$	167	
$(1,2,3,1)$	$1\times 105+2\times 70+3\times 126+1\times 120$	113	
$(1,2,3,2)$	$\ldots+120$	23	$*$
$(1,2,3,3)$	$\ldots+120$	143	
$(1,2,3,5)$	$\ldots+240$	173	
$(1,2,3,6)$	$\ldots+120$	83	
$(1,2,4,1)$	$1\times 105+2\times 70+4\times 126+1\times 120$	29	$*$
$(1,2,4,2)$	$\ldots+120$	149	
$(1,2,4,3)$	$\ldots+120$	59	
$(1,2,4,5)$	$\ldots+240$	89	
$(1,2,4,6)$	$\ldots+120$	209	

- $x = 62 = (0, 2, 2, 6)$

coordonnées	*combinaison linéaire*	*sol.min.*($\neq 0$) (*mod* 210)	*décomp. de Goldbach de* x
$(1,1,1,1)$	$1\times 105 + 1\times 70 + 1\times 126 + 1\times 120$	1	
$(1,1,1,2)$	$... + 120$	121	
$(1,1,1,3)$	$... + 120$	31	$*$
$(1,1,1,4)$	$... + 120$	151	
$(1,1,1,5)$	$... + 120$	61	
$(1,1,3,1)$	$1\times 105 + 1\times 70 + 3\times 126 + 1\times 120$	43	$*$
$(1,1,3,2)$	$... + 120$	163	
$(1,1,3,3)$	$... + 120$	73	
$(1,1,3,4)$	$... + 120$	193	
$(1,1,3,5)$	$... + 120$	103	
$(1,1,4,1)$	$1\times 105 + 1\times 70 + 4\times 126 + 1\times 120$	169	
$(1,1,4,2)$	$... + 120$	79	
$(1,1,4,3)$	$... + 120$	199	
$(1,1,4,4)$	$... + 120$	109	
$(1,1,4,5)$	$... + 120$	19	$*$

- $x = 64 = (0, 1, 4, 1)$

coordonnées	*combinaison linéaire*	*sol.min.*($\neq 0$) (*mod* 210)	*décomp. de Goldbach de* x
$(1,2,1,2)$	$1\times 105 + 2\times 70 + 1\times 126 + 2\times 120$	191	
$(1,2,1,3)$	$... + 120$	101	
$(1,2,1,4)$	$... + 120$	11	$*$
$(1,2,1,5)$	$... + 120$	131	
$(1,2,1,6)$	$... + 120$	41	$*$
$(1,2,2,2)$	$1\times 105 + 2\times 70 + 2\times 126 + 2\times 120$	107	
$(1,2,2,3)$	$... + 120$	17	$*$
$(1,2,2,4)$	$... + 120$	137	
$(1,2,2,5)$	$... + 120$	47	$*$
$(1,2,2,6)$	$... + 120$	167	
$(1,2,3,2)$	$1\times 105 + 2\times 70 + 3\times 126 + 2\times 120$	23	$*$
$(1,2,3,3)$	$... + 120$	143	
$(1,2,3,4)$	$... + 120$	53	$*$
$(1,2,3,5)$	$... + 120$	173	
$(1,2,3,6)$	$... + 120$	83	

- $x = 66 = (0, 0, 1, 3)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 210)$	*décomp. de Goldbach de* x
$(1,1,2,1)$	$1\times 105 + 1\times 70 + 2\times 126 + 1\times 120$	127	
$(1,1,2,2)$	$... + 120$	37	$*$
$(1,1,2,4)$	$... + 240$	67	
$(1,1,2,5)$	$... + 120$	187	
$(1,1,2,6)$	$... + 120$	97	
$(1,1,3,1)$	$1\times 105 + 1\times 70 + 3\times 126 + 1\times 120$	43	$*$
$(1,1,3,2)$	$... + 120$	163	
$(1,1,3,4)$	$... + 240$	193	
$(1,1,3,5)$	$... + 120$	103	
$(1,1,3,6)$	$... + 120$	13	$*$
$(1,1,4,1)$	$1\times 105 + 1\times 70 + 4\times 126 + 1\times 120$	169	
$(1,1,4,2)$	$... + 120$	79	
$(1,1,4,4)$	$... + 240$	109	
$(1,1,4,5)$	$... + 120$	19	$*$
$(1,1,4,6)$	$... + 120$	139	
$(1,2,2,1)$	$1\times 105 + 2\times 70 + 2\times 126 + 1\times 120$	197	
$(1,2,2,2)$	$... + 120$	107	
$(1,2,2,4)$	$... + 240$	137	
$(1,2,2,5)$	$... + 120$	47	$*$
$(1,2,2,6)$	$... + 120$	167	
$(1,2,3,1)$	$1\times 105 + 2\times 70 + 3\times 126 + 1\times 120$	113	
$(1,2,3,2)$	$... + 120$	23	$*$
$(1,2,3,4)$	$... + 240$	53	$*$
$(1,2,3,5)$	$... + 120$	173	
$(1,2,3,6)$	$... + 120$	83	
$(1,2,4,1)$	$1\times 105 + 2\times 70 + 4\times 126 + 1\times 120$	29	$*$
$(1,2,4,2)$	$... + 120$	149	
$(1,2,4,4)$	$... + 240$	179	
$(1,2,4,5)$	$... + 120$	89	
$(1,2,4,6)$	$... + 120$	209	

Note : on voit apparaître sans surprise symétriquement par rapport à une ligne médiane dans le tableau certaines décompositions de Goldbach de $274 = 64 + 210$; en effet, $210 = 2\times 3\times 5\times 7$ permet de conserver les mêmes restes modulaires et cela permet de conserver la non-congruence à 0 et x des solutions.

$$\begin{aligned} 274 &= 191 + 83 \\ &= 107 + 167 \\ &= 101 + 173 \\ &= 137 + 137 \end{aligned}$$

Parmi les nombres trouvés par la méthode proposée, seul 143 est divisible par 11.

- $x = 68 = (0, 2, 3, 5)$

coordonnées	*combinaison linéaire*	*sol.min.*($\neq 0$) (*mod* 210)	*décomp. de Goldbach de* x
$(1,1,1,1)$	$1\times 105+1\times 70+1\times 126+1\times 120$	1	
$(1,1,1,2)$	$\ldots+120$	121	
$(1,1,1,3)$	$\ldots+120$	31	$*$
$(1,1,1,4)$	$\ldots+120$	151	
$(1,1,1,6)$	$\ldots+240$	181	
$(1,1,2,1)$	$1\times 105+1\times 70+2\times 126+1\times 120$	127	
$(1,1,2,2)$	$\ldots+120$	37	$*$
$(1,1,2,3)$	$\ldots+120$	157	
$(1,1,2,4)$	$\ldots+120$	67	
$(1,1,2,6)$	$\ldots+240$	97	
$(1,1,4,1)$	$1\times 105+1\times 70+4\times 126+1\times 120$	169	
$(1,1,4,2)$	$\ldots+120$	79	
$(1,1,4,3)$	$\ldots+120$	199	
$(1,1,4,4)$	$\ldots+120$	109	
$(1,1,4,6)$	$\ldots+240$	139	

- $x = 70 = (0, 1, 0, 0)$

coordonnées	*combinaison linéaire*	*sol.min.*($\neq 0$) (*mod* 210)	*décomp. de Goldbach de* x
$(1,2,1,1)$	$1\times 105+2\times 70+1\times 126+1\times 120$	71	
$(1,2,1,2)$	$\ldots+120$	191	
$(1,2,1,3)$	$\ldots+120$	101	
$(1,2,1,4)$	$\ldots+120$	11	$*$
$(1,2,1,5)$	$\ldots+120$	131	
$(1,2,1,6)$	$\ldots+120$	41	$*$
$(1,2,2,1)$	$1\times 105+2\times 70+2\times 126+1\times 120$	197	
$(1,2,2,2)$	$\ldots+120$	107	
$(1,2,2,3)$	$\ldots+120$	17	$*$
$(1,2,2,4)$	$\ldots+120$	137	
$(1,2,2,5)$	$\ldots+120$	47	$*$
$(1,2,2,6)$	$\ldots+120$	167	
$(1,2,3,1)$	$1\times 105+2\times 70+3\times 126+1\times 120$	113	
$(1,2,3,2)$	$\ldots+120$	23	$*$
$(1,2,3,3)$	$\ldots+120$	143	
$(1,2,3,4)$	$\ldots+120$	53	$*$
$(1,2,3,5)$	$\ldots+120$	173	
$(1,2,3,6)$	$\ldots+120$	83	
$(1,2,4,1)$	$1\times 105+2\times 70+4\times 126+1\times 120$	29	$*$
$(1,2,4,2)$	$\ldots+120$	149	
$(1,2,4,3)$	$\ldots+120$	59	$*$
$(1,2,4,4)$	$\ldots+120$	179	
$(1,2,4,5)$	$\ldots+120$	89	
$(1,2,4,6)$	$\ldots+120$	209	

- $x = 72 = (0, 0, 2, 2)$

coordonnées	*combinaison linéaire*	*sol.min.*($\neq 0$) (*mod* 210)	*décomp. de Goldbach de* x
$(1,1,1,1)$	$1\times 105+1\times 70+1\times 126+1\times 120$	1	
$(1,1,1,3)$	$...+240$	31	$*$
$(1,1,1,4)$	$...+120$	151	
$(1,1,1,5)$	$...+120$	61	$*$
$(1,1,1,6)$	$...+120$	181	
$(1,1,3,1)$	$1\times 105+1\times 70+3\times 126+1\times 120$	43	$*$
$(1,1,3,3)$	$...+240$	73	
$(1,1,3,4)$	$...+120$	193	
$(1,1,3,5)$	$...+120$	103	
$(1,1,3,6)$	$...+120$	13	$*$
$(1,1,4,1)$	$1\times 105+1\times 70+4\times 126+1\times 120$	169	
$(1,1,4,3)$	$...+240$	199	
$(1,1,4,4)$	$...+120$	109	
$(1,1,4,5)$	$...+120$	19	$*$
$(1,1,4,6)$	$...+120$	139	
$(1,2,1,1)$	$1\times 105+2\times 70+1\times 126+1\times 120$	71	
$(1,2,1,3)$	$...+240$	101	
$(1,2,1,4)$	$...+120$	11	$*$
$(1,2,1,5)$	$...+120$	131	
$(1,2,1,6)$	$...+120$	41	$*$
$(1,2,3,1)$	$1\times 105+2\times 70+3\times 126+1\times 120$	83	
$(1,2,3,3)$	$...+240$	113	
$(1,2,3,4)$	$...+120$	23	
$(1,2,3,5)$	$...+120$	143	
$(1,2,3,6)$	$...+120$	53	$*$
$(1,2,4,1)$	$1\times 105+2\times 70+4\times 126+1\times 120$	209	
$(1,2,4,3)$	$...+240$	29	$*$
$(1,2,4,4)$	$...+120$	149	
$(1,2,4,5)$	$...+120$	59	$*$
$(1,2,4,6)$	$...+120$	179	

- $x = 74 = (0, 2, 4, 4)$

coordonnées	*combinaison linéaire*	*sol.min.*($\neq 0$) (*mod* 210)	*décomp. de Goldbach de* x
$(1,1,1,1)$	$1\times 105+1\times 70+1\times 126+1\times 120$	1	
$(1,1,1,2)$	$...+120$	121	
$(1,1,1,3)$	$...+120$	31	$*$
$(1,1,1,5)$	$...+240$	61	$*$
$(1,1,1,6)$	$...+120$	181	
$(1,1,2,1)$	$1\times 105+1\times 70+2\times 126+1\times 120$	127	
$(1,1,2,2)$	$...+120$	37	$*$
$(1,1,2,3)$	$...+120$	157	
$(1,1,2,5)$	$...+240$	187	
$(1,1,2,6)$	$...+120$	97	
$(1,1,3,1)$	$1\times 105+1\times 70+3\times 126+1\times 120$	43	$*$
$(1,1,3,2)$	$...+120$	163	
$(1,1,3,3)$	$...+120$	73	
$(1,1,3,5)$	$...+240$	103	
$(1,1,3,6)$	$...+120$	13	$*$

- $x = 76 = (0, 1, 1, 6)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 210)$	*décomp. de Goldbach de* x
$(1, 2, 2, 1)$	$1 \times 105 + 2 \times 70 + 2 \times 126 + 1 \times 120$	197	
$(1, 2, 2, 2)$	$... + 120$	107	
$(1, 2, 2, 3)$	$... + 120$	17	$*$
$(1, 2, 2, 4)$	$... + 120$	137	
$(1, 2, 2, 5)$	$... + 120$	47	$*$
$(1, 2, 3, 1)$	$1 \times 105 + 2 \times 70 + 3 \times 126 + 1 \times 120$	113	
$(1, 2, 3, 2)$	$... + 120$	23	$*$
$(1, 2, 3, 3)$	$... + 120$	143	
$(1, 2, 3, 4)$	$... + 120$	53	$*$
$(1, 2, 3, 5)$	$... + 120$	173	
$(1, 2, 4, 1)$	$1 \times 105 + 2 \times 70 + 4 \times 126 + 1 \times 120$	29	$*$
$(1, 2, 4, 2)$	$... + 120$	149	
$(1, 2, 4, 3)$	$... + 120$	59	$*$
$(1, 2, 4, 4)$	$... + 120$	179	
$(1, 2, 4, 5)$	$... + 120$	89	

- $x = 78 = (0, 0, 3, 1)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 210)$	*décomp. de Goldbach de* x
$(1, 1, 1, 2)$	$1 \times 105 + 1 \times 70 + 1 \times 126 + 2 \times 120$	121	
$(1, 1, 1, 3)$	$... + 120$	31	$*$
$(1, 1, 1, 4)$	$... + 120$	151	
$(1, 1, 1, 5)$	$... + 120$	41	$*$
$(1, 1, 1, 6)$	$... + 120$	161	
$(1, 1, 2, 2)$	$1 \times 105 + 1 \times 70 + 2 \times 126 + 2 \times 120$	37	$*$
$(1, 1, 2, 3)$	$... + 120$	157	
$(1, 1, 2, 4)$	$... + 120$	67	$*$
$(1, 1, 2, 5)$	$... + 120$	187	
$(1, 1, 2, 6)$	$... + 120$	97	
$(1, 1, 4, 2)$	$1 \times 105 + 1 \times 70 + 4 \times 126 + 2 \times 120$	79	
$(1, 1, 4, 3)$	$... + 120$	199	
$(1, 1, 4, 4)$	$... + 120$	109	
$(1, 1, 4, 5)$	$... + 120$	19	$*$
$(1, 1, 4, 6)$	$... + 120$	139	
$(1, 2, 1, 2)$	$1 \times 105 + 2 \times 70 + 1 \times 126 + 2 \times 120$	191	
$(1, 2, 1, 3)$	$... + 120$	101	
$(1, 2, 1, 4)$	$... + 120$	11	$*$
$(1, 2, 1, 5)$	$... + 120$	131	
$(1, 2, 1, 6)$	$... + 120$	41	$*$
$(1, 2, 2, 2)$	$1 \times 105 + 2 \times 70 + 2 \times 126 + 2 \times 120$	107	
$(1, 2, 2, 3)$	$... + 120$	17	$*$
$(1, 2, 2, 4)$	$... + 120$	137	
$(1, 2, 2, 5)$	$... + 120$	47	$*$
$(1, 2, 2, 6)$	$... + 120$	167	
$(1, 2, 4, 2)$	$1 \times 105 + 2 \times 70 + 4 \times 126 + 2 \times 120$	149	
$(1, 2, 4, 3)$	$... + 120$	59	$*$
$(1, 2, 4, 4)$	$... + 120$	179	
$(1, 2, 4, 5)$	$... + 120$	89	
$(1, 2, 4, 6)$	$... + 120$	209	

- $x = 80 = (0, 2, 0, 3)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 210)$	*décomp. de Goldbach de* x
$(1,1,1,1)$	$1 \times 105 + 1 \times 70 + 1 \times 126 + 1 \times 120$	1	
$(1,1,1,2)$	$... + 120$	121	
$(1,1,1,4)$	$... + 240$	51	$*$
$(1,1,1,5)$	$... + 120$	171	
$(1,1,1,6)$	$... + 120$	81	
$(1,1,2,1)$	$1 \times 105 + 1 \times 70 + 2 \times 126 + 1 \times 120$	127	
$(1,1,2,2)$	$... + 120$	37	$*$
$(1,1,2,4)$	$... + 240$	67	$*$
$(1,1,2,5)$	$... + 120$	187	
$(1,1,2,6)$	$... + 120$	97	
$(1,1,3,1)$	$1 \times 105 + 1 \times 70 + 3 \times 126 + 1 \times 120$	43	$*$
$(1,1,3,2)$	$... + 120$	163	
$(1,1,3,4)$	$... + 240$	193	
$(1,1,3,5)$	$... + 120$	103	
$(1,1,3,6)$	$... + 120$	13	$*$
$(1,1,4,1)$	$1 \times 105 + 1 \times 70 + 4 \times 126 + 1 \times 120$	169	
$(1,1,4,2)$	$... + 120$	79	
$(1,1,4,4)$	$... + 240$	109	
$(1,1,4,5)$	$... + 120$	19	$*$
$(1,1,4,6)$	$... + 120$	139	

- $x = 82 = (0, 1, 2, 5)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 210)$	*décomp. de Goldbach de* x
$(1,2,1,1)$	$1 \times 105 + 2 \times 70 + 1 \times 126 + 1 \times 120$	71	$*$
$(1,2,1,2)$	$... + 120$	191	
$(1,2,1,3)$	$... + 120$	101	
$(1,2,1,4)$	$... + 120$	11	$*$
$(1,2,1,6)$	$... + 240$	41	$*$
$(1,2,3,1)$	$1 \times 105 + 2 \times 70 + 3 \times 126 + 1 \times 120$	113	
$(1,2,3,2)$	$... + 120$	23	$*$
$(1,2,3,3)$	$... + 120$	143	
$(1,2,3,4)$	$... + 120$	53	$*$
$(1,2,3,6)$	$... + 240$	83	
$(1,2,4,1)$	$1 \times 105 + 2 \times 70 + 4 \times 126 + 1 \times 120$	29	$*$
$(1,2,4,2)$	$... + 120$	149	
$(1,2,4,3)$	$... + 120$	59	$*$
$(1,2,4,4)$	$... + 120$	179	
$(1,2,4,6)$	$... + 240$	89	

- $x = 84 = (0, 0, 4, 0)$

coordonnées	*combinaison linéaire*	*sol.min.*($\neq 0$) (*mod* 210)	*décomp. de Goldbach de* x
$(1,1,1,1)$	$1\times 105+1\times 70+1\times 126+1\times 120$	1	
$(1,1,1,2)$	$\ldots+120$	121	
$(1,1,1,3)$	$\ldots+120$	31	$*$
$(1,1,1,4)$	$\ldots+120$	151	
$(1,1,1,5)$	$\ldots+120$	61	$*$
$(1,1,1,6)$	$\ldots+120$	181	
$(1,1,2,1)$	$1\times 105+1\times 70+2\times 126+1\times 120$	127	
$(1,1,2,2)$	$\ldots+120$	37	$*$
$(1,1,2,3)$	$\ldots+120$	157	
$(1,1,2,4)$	$\ldots+120$	67	$*$
$(1,1,2,5)$	$\ldots+120$	187	
$(1,1,2,6)$	$\ldots+120$	97	
$(1,1,3,1)$	$1\times 105+1\times 70+3\times 126+1\times 120$	43	$*$
$(1,1,3,2)$	$\ldots+120$	163	
$(1,1,3,3)$	$\ldots+120$	73	$*$
$(1,1,3,4)$	$\ldots+120$	193	
$(1,1,3,5)$	$\ldots+120$	103	
$(1,1,3,6)$	$\ldots+120$	13	
$(1,2,1,1)$	$1\times 105+2\times 70+1\times 126+1\times 120$	71	$*$
$(1,2,1,2)$	$\ldots+120$	191	
$(1,2,1,3)$	$\ldots+120$	101	
$(1,2,1,4)$	$\ldots+120$	11	$*$
$(1,2,1,5)$	$\ldots+120$	131	
$(1,2,1,6)$	$\ldots+120$	41	$*$
$(1,2,2,1)$	$1\times 105+2\times 70+2\times 126+1\times 120$	197	
$(1,2,2,2)$	$\ldots+120$	107	
$(1,2,2,3)$	$\ldots+120$	17	$*$
$(1,2,2,4)$	$\ldots+120$	137	
$(1,2,2,5)$	$\ldots+120$	47	$*$
$(1,2,2,6)$	$\ldots+120$	167	
$(1,2,3,1)$	$1\times 105+2\times 70+3\times 126+1\times 120$	113	
$(1,2,3,2)$	$\ldots+120$	23	$*$
$(1,2,3,3)$	$\ldots+120$	143	
$(1,2,3,4)$	$\ldots+120$	53	$*$
$(1,2,3,5)$	$\ldots+120$	173	
$(1,2,3,6)$	$\ldots+120$	83	

- $x = 86 = (0, 2, 1, 2)$

coordonnées	*combinaison linéaire*	*sol.min.*($\neq 0$) (*mod* 210)	*décomp. de Goldbach de* x
$(1,1,2,1)$	$1\times 105+1\times 70+2\times 126+1\times 120$	127	
$(1,1,2,3)$	$\ldots+240$	157	
$(1,1,2,4)$	$\ldots+120$	67	$*$
$(1,1,2,5)$	$\ldots+120$	187	
$(1,1,2,6)$	$\ldots+120$	97	
$(1,1,3,1)$	$1\times 105+1\times 70+3\times 126+1\times 120$	43	$*$
$(1,1,3,3)$	$\ldots+240$	73	$*$
$(1,1,3,4)$	$\ldots+120$	193	
$(1,1,3,5)$	$\ldots+120$	103	
$(1,1,3,6)$	$\ldots+120$	13	$*$
$(1,1,4,1)$	$1\times 105+1\times 70+4\times 126+1\times 120$	169	
$(1,1,4,3)$	$\ldots+240$	79	$*$
$(1,1,4,4)$	$\ldots+120$	199	
$(1,1,4,5)$	$\ldots+120$	109	
$(1,1,4,6)$	$\ldots+120$	19	$*$

- $x = 88 = (0, 1, 3, 4)$

coordonnées	*combinaison linéaire*	*sol.min.*($\neq 0$) (*mod* 210)	*décomp. de Goldbach de* x
$(1, 2, 1, 1)$	$1 \times 105 + 2 \times 70 + 1 \times 126 + 1 \times 120$	71	$*$
$(1, 2, 1, 2)$	$... + 120$	191	
$(1, 2, 1, 3)$	$... + 120$	101	
$(1, 2, 1, 5)$	$... + 240$	131	
$(1, 2, 1, 6)$	$... + 120$	41	$*$
$(1, 2, 2, 1)$	$1 \times 105 + 2 \times 70 + 2 \times 126 + 1 \times 120$	197	
$(1, 2, 2, 2)$	$... + 120$	107	
$(1, 2, 2, 3)$	$... + 120$	17	$*$
$(1, 2, 2, 5)$	$... + 240$	137	
$(1, 2, 2, 6)$	$... + 120$	47	$*$
$(1, 2, 4, 1)$	$1 \times 105 + 2 \times 70 + 4 \times 126 + 1 \times 120$	29	$*$
$(1, 2, 4, 2)$	$... + 120$	149	
$(1, 2, 4, 3)$	$... + 120$	59	$*$
$(1, 2, 4, 5)$	$... + 240$	179	
$(1, 2, 4, 6)$	$... + 120$	89	

- $x = 92 = (0, 2, 2, 1)$

coordonnées	*combinaison linéaire*	*sol.min.*($\neq 0$) (*mod* 210)	*décomp. de Goldbach de* x
$(1, 1, 1, 2)$	$1 \times 105 + 1 \times 70 + 1 \times 126 + 2 \times 120$	121	
$(1, 1, 1, 3)$	$... + 120$	31	$*$
$(1, 1, 1, 4)$	$... + 120$	151	
$(1, 1, 1, 5)$	$... + 120$	61	$*$
$(1, 1, 1, 6)$	$... + 120$	181	
$(1, 1, 3, 2)$	$1 \times 105 + 1 \times 70 + 3 \times 126 + 2 \times 120$	163	
$(1, 1, 3, 3)$	$... + 120$	73	$*$
$(1, 1, 3, 4)$	$... + 120$	193	
$(1, 1, 3, 5)$	$... + 120$	103	
$(1, 1, 3, 6)$	$... + 120$	13	$*$
$(1, 1, 4, 2)$	$1 \times 105 + 1 \times 70 + 4 \times 126 + 2 \times 120$	79	$*$
$(1, 1, 4, 3)$	$... + 120$	199	
$(1, 1, 4, 4)$	$... + 120$	109	
$(1, 1, 4, 5)$	$... + 120$	19	$*$
$(1, 1, 4, 6)$	$... + 120$	139	

- $x = 94 = (0, 1, 4, 3)$

coordonnées	*combinaison linéaire*	*sol.min.*($\neq 0$) (*mod* 210)	*décomp. de Goldbach de* x
$(1, 2, 1, 1)$	$1 \times 105 + 1 \times 70 + 1 \times 126 + 1 \times 120$	71	$*$
$(1, 2, 1, 2)$	$... + 120$	191	
$(1, 2, 1, 4)$	$... + 240$	11	$*$
$(1, 2, 1, 5)$	$... + 120$	131	
$(1, 2, 1, 6)$	$... + 120$	41	$*$
$(1, 2, 2, 1)$	$1 \times 105 + 1 \times 70 + 3 \times 126 + 1 \times 120$	197	
$(1, 2, 2, 2)$	$... + 120$	107	
$(1, 2, 2, 4)$	$... + 240$	137	
$(1, 2, 2, 5)$	$... + 120$	47	$*$
$(1, 2, 2, 6)$	$... + 120$	167	
$(1, 2, 3, 1)$	$1 \times 105 + 1 \times 70 + 4 \times 126 + 1 \times 120$	113	
$(1, 2, 3, 2)$	$... + 120$	23	$*$
$(1, 2, 3, 4)$	$... + 240$	53	$*$
$(1, 2, 3, 5)$	$... + 120$	173	
$(1, 2, 3, 6)$	$... + 120$	83	$*$

- $x = 90 = (0, 0, 0, 6)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 210)$	*décomp. de Goldbach de* x
$(1,1,1,1)$	$1\times 105+1\times 70+1\times 126+1\times 120$	1	
$(1,1,1,2)$	$...+120$	121	
$(1,1,1,3)$	$...+120$	31	$*$
$(1,1,1,4)$	$...+120$	151	
$(1,1,1,5)$	$...+120$	61	$*$
$(1,1,2,1)$	$1\times 105+1\times 70+2\times 126+1\times 120$	127	
$(1,1,2,2)$	$...+120$	37	$*$
$(1,1,2,3)$	$...+120$	157	
$(1,1,2,4)$	$...+120$	67	$*$
$(1,1,2,5)$	$...+120$	187	
$(1,1,3,1)$	$1\times 105+1\times 70+3\times 126+1\times 120$	43	$*$
$(1,1,3,2)$	$...+120$	163	
$(1,1,3,3)$	$...+120$	73	$*$
$(1,1,3,4)$	$...+120$	193	
$(1,1,3,5)$	$...+120$	103	
$(1,1,4,1)$	$1\times 105+1\times 70+4\times 126+1\times 120$	169	
$(1,1,4,2)$	$...+120$	79	$*$
$(1,1,4,3)$	$...+120$	199	
$(1,1,4,4)$	$...+120$	109	
$(1,1,4,5)$	$...+120$	19	$*$
$(1,2,1,1)$	$1\times 105+2\times 70+1\times 126+1\times 120$	71	$*$
$(1,2,1,2)$	$...+120$	191	
$(1,2,1,3)$	$...+120$	101	
$(1,2,1,4)$	$...+120$	11	$*$
$(1,2,1,5)$	$...+120$	131	
$(1,2,2,1)$	$1\times 105+2\times 70+2\times 126+1\times 120$	197	
$(1,2,2,2)$	$...+120$	107	
$(1,2,2,3)$	$...+120$	17	$*$
$(1,2,2,4)$	$...+120$	137	
$(1,2,2,5)$	$...+120$	47	$*$
$(1,2,3,1)$	$1\times 105+2\times 70+3\times 126+1\times 120$	113	
$(1,2,3,2)$	$...+120$	23	$*$
$(1,2,3,3)$	$...+120$	143	
$(1,2,3,4)$	$...+120$	53	$*$
$(1,2,3,5)$	$...+120$	173	
$(1,2,4,1)$	$1\times 105+2\times 70+4\times 126+1\times 120$	29	$*$
$(1,2,4,2)$	$...+120$	149	
$(1,2,4,3)$	$...+120$	59	$*$
$(1,2,4,4)$	$...+120$	179	
$(1,2,4,5)$	$...+120$	89	

- $x = 96 = (0, 0, 1, 5)$

coordonnées	*combinaison linéaire*	*sol.min.*($\neq 0$) (*mod* 210)	*décomp. de Goldbach de* x
$(1, 1, 2, 1)$	$1 \times 105 + 1 \times 70 + 2 \times 126 + 1 \times 120$	127	
$(1, 1, 2, 2)$	$... + 120$	37	$*$
$(1, 1, 2, 3)$	$... + 120$	157	
$(1, 1, 2, 4)$	$... + 120$	67	$*$
$(1, 1, 2, 6)$	$... + 240$	97	
$(1, 1, 3, 1)$	$1 \times 105 + 1 \times 70 + 3 \times 126 + 1 \times 120$	43	$*$
$(1, 1, 3, 2)$	$... + 120$	163	
$(1, 1, 3, 3)$	$... + 120$	73	$*$
$(1, 1, 3, 4)$	$... + 120$	193	
$(1, 1, 3, 6)$	$... + 240$	13	$*$
$(1, 1, 4, 1)$	$1 \times 105 + 1 \times 70 + 4 \times 126 + 1 \times 120$	169	
$(1, 1, 4, 2)$	$... + 120$	79	$*$
$(1, 1, 4, 3)$	$... + 120$	199	
$(1, 1, 4, 4)$	$... + 120$	109	
$(1, 1, 4, 6)$	$... + 240$	19	
$(1, 2, 2, 1)$	$1 \times 105 + 2 \times 70 + 2 \times 126 + 1 \times 120$	197	
$(1, 2, 2, 2)$	$... + 120$	107	
$(1, 2, 2, 3)$	$... + 120$	17	$*$
$(1, 2, 2, 4)$	$... + 120$	137	
$(1, 2, 2, 6)$	$... + 240$	167	
$(1, 2, 3, 1)$	$1 \times 105 + 2 \times 70 + 3 \times 126 + 1 \times 120$	113	
$(1, 2, 3, 2)$	$... + 120$	23	$*$
$(1, 2, 3, 3)$	$... + 120$	143	
$(1, 2, 3, 4)$	$... + 120$	53	$*$
$(1, 2, 3, 6)$	$... + 240$	83	$*$
$(1, 2, 4, 1)$	$1 \times 105 + 2 \times 70 + 4 \times 126 + 1 \times 120$	29	$*$
$(1, 2, 4, 2)$	$... + 120$	149	
$(1, 2, 4, 3)$	$... + 120$	59	$*$
$(1, 2, 4, 4)$	$... + 120$	179	
$(1, 2, 1, 6)$	$... + 240$	209	

- $x = 98 = (0, 2, 3, 0)$

coordonnées	*combinaison linéaire*	*sol.min.*($\neq 0$) (*mod* 210)	*décomp. de Goldbach de* x
$(1, 1, 1, 1)$	$1 \times 105 + 1 \times 70 + 1 \times 126 + 1 \times 120$	1	
$(1, 1, 1, 2)$	$... + 120$	121	
$(1, 1, 1, 3)$	$... + 120$	31	$*$
$(1, 1, 1, 4)$	$... + 120$	151	
$(1, 1, 1, 5)$	$... + 120$	61	$*$
$(1, 1, 1, 6)$	$... + 120$	181	
$(1, 1, 2, 1)$	$1 \times 105 + 1 \times 70 + 2 \times 126 + 1 \times 120$	127	
$(1, 1, 2, 2)$	$... + 120$	37	$*$
$(1, 1, 2, 3)$	$... + 120$	157	
$(1, 1, 2, 4)$	$... + 120$	67	$*$
$(1, 1, 2, 5)$	$... + 120$	187	
$(1, 1, 2, 6)$	$... + 120$	97	
$(1, 1, 4, 1)$	$1 \times 105 + 1 \times 70 + 4 \times 126 + 1 \times 120$	169	
$(1, 1, 4, 2)$	$... + 120$	79	$*$
$(1, 1, 4, 3)$	$... + 120$	199	
$(1, 1, 4, 4)$	$... + 120$	109	
$(1, 1, 4, 5)$	$... + 120$	19	$*$
$(1, 1, 4, 6)$	$... + 120$	139	

- $x = 100 = (0, 1, 0, 2)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 210)$	*décomp. de Goldbach de* x
$(1, 2, 1, 1)$	$1 \times 105 + 2 \times 70 + 1 \times 126 + 1 \times 120$	71	$*$
$(1, 2, 1, 3)$	$... + 240$	101	
$(1, 2, 1, 4)$	$... + 120$	11	$*$
$(1, 2, 1, 5)$	$... + 120$	131	
$(1, 2, 1, 6)$	$... + 120$	41	$*$
$(1, 2, 2, 1)$	$1 \times 105 + 2 \times 70 + 2 \times 126 + 1 \times 120$	197	
$(1, 2, 2, 3)$	$... + 240$	17	$*$
$(1, 2, 2, 4)$	$... + 120$	137	
$(1, 2, 2, 5)$	$... + 120$	47	$*$
$(1, 2, 2, 6)$	$... + 120$	167	
$(1, 2, 3, 1)$	$1 \times 105 + 2 \times 70 + 3 \times 126 + 1 \times 120$	113	
$(1, 2, 3, 3)$	$... + 240$	143	
$(1, 2, 3, 4)$	$... + 120$	53	$*$
$(1, 2, 3, 5)$	$... + 120$	173	
$(1, 2, 3, 6)$	$... + 120$	83	$*$
$(1, 2, 4, 1)$	$1 \times 105 + 2 \times 70 + 4 \times 126 + 1 \times 120$	29	$*$
$(1, 2, 4, 3)$	$... + 240$	59	$*$
$(1, 2, 4, 4)$	$... + 120$	179	
$(1, 2, 4, 5)$	$... + 120$	89	$*$
$(1, 2, 4, 6)$	$... + 120$	209	

- $x = 120 = (0, 0, 0, 1)$

coordonnées	*combinaison linéaire*	*sol.min.*($\neq 0$) (*mod* 210)	*décomp. de Goldbach de* x
$(1, 1, 1, 2)$	$1 \times 105 + 1 \times 70 + 1 \times 126 + 2 \times 120$	121	
$(1, 1, 1, 3)$	$... + 120$	31	$*$
$(1, 1, 1, 4)$	$... + 120$	151	
$(1, 1, 1, 5)$	$... + 120$	61	$*$
$(1, 1, 1, 6)$	$... + 120$	181	
$(1, 1, 2, 2)$	$1 \times 105 + 1 \times 70 + 2 \times 126 + 2 \times 120$	37	$*$
$(1, 1, 2, 3)$	$... + 120$	157	
$(1, 1, 2, 4)$	$... + 120$	67	$*$
$(1, 1, 2, 5)$	$... + 120$	187	
$(1, 1, 2, 6)$	$... + 120$	97	$*$
$(1, 1, 3, 2)$	$1 \times 105 + 1 \times 70 + 3 \times 126 + 2 \times 120$	163	
$(1, 1, 3, 3)$	$... + 120$	73	$*$
$(1, 1, 3, 4)$	$... + 120$	193	
$(1, 1, 3, 5)$	$... + 120$	103	$*$
$(1, 1, 3, 6)$	$... + 120$	13	$*$
$(1, 1, 4, 2)$	$1 \times 105 + 1 \times 70 + 4 \times 126 + 2 \times 120$	79	$*$
$(1, 1, 4, 3)$	$... + 120$	199	
$(1, 1, 4, 4)$	$... + 120$	109	$*$
$(1, 1, 4, 5)$	$... + 120$	19	$*$
$(1, 1, 4, 6)$	$... + 120$	139	
$(1, 2, 1, 2)$	$1 \times 105 + 2 \times 70 + 1 \times 126 + 2 \times 120$	191	
$(1, 2, 1, 3)$	$... + 120$	101	$*$
$(1, 2, 1, 4)$	$... + 120$	11	$*$
$(1, 2, 1, 5)$	$... + 120$	131	
$(1, 2, 1, 6)$	$... + 120$	41	$*$
$(1, 2, 2, 2)$	$1 \times 105 + 2 \times 70 + 2 \times 126 + 2 \times 120$	107	$*$
$(1, 2, 2, 3)$	$... + 120$	17	$*$
$(1, 2, 2, 4)$	$... + 120$	137	
$(1, 2, 2, 5)$	$... + 120$	47	$*$
$(1, 2, 2, 6)$	$... + 120$	167	
$(1, 2, 3, 2)$	$1 \times 105 + 2 \times 70 + 3 \times 126 + 2 \times 120$	23	$*$
$(1, 2, 3, 3)$	$... + 120$	143	
$(1, 2, 3, 4)$	$... + 120$	53	$*$
$(1, 2, 3, 5)$	$... + 120$	173	
$(1, 2, 3, 6)$	$... + 120$	83	$*$
$(1, 2, 4, 2)$	$1 \times 105 + 2 \times 70 + 4 \times 126 + 2 \times 120$	149	
$(1, 2, 4, 3)$	$... + 120$	59	$*$
$(1, 2, 4, 4)$	$... + 120$	179	
$(1, 2, 4, 5)$	$... + 120$	89	$*$
$(1, 2, 4, 6)$	$... + 120$	209	

Note 1 : le "rendement" est impressionnant ; 22 décomposants de Goldbach sur 40 cas envisagés (pour le nombre 60, on avait trouvé 10 décomposants de Goldbach sur 40 cas envisagés également).
Quant à $240 = (0, 0, 0, 2, 9, 6)$, en considérant les modules premiers jusqu'à 13, sur
$(3 - 3) \times (5 - 1) \times (7 - 2) \times (11 - 2) \times (13 - 2) = 2 \times 4 \times 5 \times 9 \times 11 = 3960$ nombres envisagés, 36 seront des décomposants de Goldbach de 240 (rappel : on prend combinatoirement $p_k - 1$ congruences dans le cas d'une congruence de x à 0 et $p_k - 2$ congruences dans le cas d'une congruence de x à un nombre non nul).

Note 2 : on voit apparaître sans surprise symétriquement par rapport à une ligne médiane dans le tableau certaines décompositions de Goldbach de $330 = 120 + 210$.

$$\begin{aligned} 330 &= 151 + 179 \\ &= 181 + 149 \\ &= 157 + 173 \\ &= 163 + 167 \\ &= 193 + 137 \\ &= 199 + 131 \\ &= 139 + 191 \end{aligned}$$

Parmi les nombres trouvés par la méthode proposée, $121, 143, 187$ sont composés.

4 Conséquence de ces expérimentations : nombres vérifiant obligatoirement la conjecture de Goldbach

Des expérimentations autour de la "comète" de Goldbach et de la représentation des décompositions par ce qu'on avait appelé "pliage de tissu" nous avait fait comprendre que les nombres qui ont de très nombreux diviseurs ont des nombres de décompositions de Goldbach très grands comparativement aux nombres qui les entourent. Par exemple, $2310 = 2 \times 3 \times 5 \times 7 \times 11$ a 114 décompositions alors que $2306 = 2 \times 1153$ qui est le double de premier immédiatement inférieur à 2310 n'en a que 34 ou bien $2326 = 2 \times 1163$ qui est le double de premier immédiatement supérieur à 2310 n'en a que 35. Si l'on considère les nombres inférieur et supérieur à 2310 de la forme $2p^2$, qui ont très peu de diviseurs également, que sont $2 \times 961 = 2 \times 31^2 = 1922$, celui-ci a 30 décomposants de Goldbach quand $2 \times 1369 = 2 \times 37^2 = 2738$ en a 17 à peine.

Reprenons l'exemple du nombre pair 60 congru à 0 (*mod* 2, 3 et 5). Dans la mesure où la méthode n'élimine que les nombres congrus à x selon un module ainsi que les petits premiers, s'il ne restait aucun nombre premier (si 60 n'avait aucun décomposant de Goldbach), cela signifierait que les nombres premiers compris entre $\sqrt{60}$ et $30 = 60/2$ seraient tous soit congrus à 0 (*mod* 2), ce qui est impossible, soit congrus à 0 (*mod* 3) ce qui ne l'est pas moins, soit congrus à 0 (*mod* 5), idem, soit tous congrus à 4 (*mod* 7), ce qui n'est trivialement pas le cas, les nombres premiers se distribuant quasiment équitablement selon toutes les classes de congruence pour un module donné. On déduit de ce raisonnement qu'un nombre divisible par tous les nombres premiers sauf un d'entre eux qui est inférieur à sa racine admet forcément un décomposant de Goldbach (cas des nombres 60, 70 ou 120 étudiés ci-dessus).

Dit autrement, considérons un nombre dont le vecteur dans la méthode ne contient qu'une seule coordonnée non nulle. Si on ne lui trouve aucun décomposant de Goldbach par la méthode, puisque les "grands" nombres premiers (supérieurs à $\lfloor\sqrt{x}\rfloor$) ne peuvent être congrus à 0 selon les modules premiers inférieurs à $\lfloor\sqrt{x}\rfloor$, cela signifierait que tous les nombres premiers compris entre $\lfloor\sqrt{x}\rfloor$ et $x - \lfloor\sqrt{x}\rfloor$ sont congrus à x selon le nombre premier pour lequel x a une coordonnée non nulle. Mais on sait que tous les nombres premiers d'un intervalle ne peuvent être tous congrus à une même valeur selon un module donné. Donc les nombres qui n'ont qu'une seule coordonnée non nulle (comme 60 par exemple, qui correspond au vecteur $(0, 0, 0, 4)$) sont assurés de se voir trouver un décomposant de Goldbach par la méthode fournie.

Le problème est qu'on ne voit pas comment étendre ce raisonnement dès que deux coordonnées sont non nulles.

5 Sempiternel problème de l'ordre sur les entiers naturels

Reprenons l'exemple de la recherche des décomposants de Goldbach de 96 mais en fournissant cette fois-ci les nombres trouvés par le calcul des combinaisons linéaires, avant qu'ils soient "diminués drastiquement" sous-prétexte qu'on les "ramène" dans l'intervalle $[1, 210]$. On va voir que l'ordre dans lequel les nombres sont rencontrés est totalement erratique et que les écarts qui les séparent sont très irréguliers (écarts fournis après remise en ordre après le tableau). De toute façon, il en est de même pour les nombres que l'on a "ramenés" sur l'intervalle $[1, 210]$. On a coloré les ordinaux en bleu pour faciliter la lecture du tableau.

- $x = 96 = (0, 0, 1, 5)$

coordonnées	*sol.avt modulo*	*ordre* 1	*sol.min.*$(\neq 0)$ (*mod* 210)	*ordre* 2
$(1, 1, 2, 1)$	547	1	127	18
$(1, 1, 2, 2)$	667	3	37	6
$(1, 1, 2, 3)$	787	7	157	22
$(1, 1, 2, 4)$	907	13	67	10
$(1, 1, 2, 6)$	1147	23	97	14
$(1, 1, 3, 1)$	673	4	43	7
$(1, 1, 3, 2)$	793	8	163	23
$(1, 1, 3, 3)$	913	14	73	11
$(1, 1, 3, 4)$	1033	19	193	27
$(1, 1, 3, 6)$	1273	27	13	1
$(1, 1, 4, 1)$	799	9	169	25
$(1, 1, 4, 2)$	919	15	79	12
$(1, 1, 4, 3)$	1039	20	199	29
$(1, 1, 4, 4)$	1159	24	109	16
$(1, 1, 4, 6)$	1399	29	19	3
$(1, 2, 2, 1)$	617	2	197	28
$(1, 2, 2, 2)$	737	5	107	15
$(1, 2, 2, 3)$	857	10	17	2
$(1, 2, 2, 4)$	977	16	137	19
$(1, 2, 2, 6)$	1217	25	167	24
$(1, 2, 3, 1)$	743	6	113	17
$(1, 2, 3, 2)$	863	11	23	4
$(1, 2, 3, 3)$	983	17	143	20
$(1, 2, 3, 4)$	1103	22	53	8
$(1, 2, 3, 6)$	1343	28	83	13
$(1, 2, 4, 1)$	869	12	29	5
$(1, 2, 4, 2)$	989	18	149	21
$(1, 2, 4, 3)$	1099	21	59	9
$(1, 2, 4, 4)$	1219	26	179	26
$(1, 2, 1, 6)$	1459	30	209	30

On constate que l'ordre d'énumération que l'on pourrait qualifier de "naturel" sur les vecteurs ne fournit pas les solutions selon l'ordre naturel sur les entiers. De plus, les écarts entre les solutions fournies par le théorème des restes chinois, une fois qu'on les a réordonnées selon l'ordre naturel sur les entiers, ne sont pas constants d'une solution à l'autre.

$$547 \xrightarrow{70} 617 \xrightarrow{50} 667 \xrightarrow{6} 673 \xrightarrow{64} 737 \xrightarrow{6} 743 \xrightarrow{44} 787 \xrightarrow{6} 793 \xrightarrow{6} 799 \xrightarrow{58} 857 \xrightarrow{6} 863 \xrightarrow{6} 869 \xrightarrow{38} 907$$

$$(907) \xrightarrow{6} 913 \xrightarrow{6} 919 \xrightarrow{58} 977 \xrightarrow{6} 983 \xrightarrow{6} 989 \xrightarrow{44} 1033 \xrightarrow{6} 1039 \xrightarrow{60} 1099 \xrightarrow{4} 1103 \xrightarrow{44} 1147 \xrightarrow{12} 1159$$

$$(1159) \xrightarrow{58} 1217 \xrightarrow{2} 1219 \xrightarrow{54} 1273 \xrightarrow{70} 1343 \xrightarrow{56} 1399 \xrightarrow{60} 1459$$

Quant à l'ordre et aux écarts une fois les solutions "ramenées" dans l'intervalle $[1, 210]$, il est le suivant :

$$13 \xrightarrow{4} 17 \xrightarrow{2} 19 \xrightarrow{4} 23 \xrightarrow{6} 29 \xrightarrow{8} 37 \xrightarrow{6} 43 \xrightarrow{10} 53 \xrightarrow{6} 59 \xrightarrow{8} 67 \xrightarrow{6} 73 \xrightarrow{6} 79 \xrightarrow{4} 83 \xrightarrow{14} 97 \xrightarrow{10} 107$$

$$(107) \xrightarrow{2} 109 \xrightarrow{4} 113 \xrightarrow{14} 127 \xrightarrow{10} 137 \xrightarrow{6} 143 \xrightarrow{6} 149 \xrightarrow{8} 157 \xrightarrow{6} 163 \xrightarrow{4} 167 \xrightarrow{2} 169 \xrightarrow{10} 179 \xrightarrow{14} 193$$

$$(193) \xrightarrow{4} 197 \xrightarrow{2} 199 \xrightarrow{10} 209$$

Dans le cas des nombres avant réduction modulo 210, si on arrivait à montrer que l'écart maximum entre deux solutions successives (au sens de l'ordre naturel sur les entiers) était systématiquement inférieur

à $x/2$ (ici 48, la moitié de 96), la méthode fournirait obligatoirement une solution. Mais on voit que $617 - 547 = 70$ étant supérieur à 48, cette approche ne convient pas.

Après réduction modulo 210, il faudrait être capable de montrer que le plus petit nombre trouvé est systématiquement inférieur à $x/2$.

Peut-être que la notion de réseau de points serait plus appropriée pour assurer l'existence d'une solution convenable.

5.1 Pistes

On serait tenté d'utiliser la notion mathématique de *Z-module* qui semble tout à fait correspondre à la méthode présentée ici mais le problème est que l'élimination de certains points, parce qu'ils ont certaines coordonnées (i.e. parce qu'ils appartiennent à certains hyperplans de nos réseaux finis de points), fait que l'on perd la propriété importante de groupe additif nécessaire pour mener un quelconque raisonnement.

De même, le théorème de Minkowski, qui pourrait peut-être nous permettre de dire que dans une certaine "boule" autour de l'origine, on est assuré de trouver un nombre premier (comme cela peut être fait par exemple pour prouver que les nombres premiers $4n + 1$ sont sommes de deux carrés), ne peut pas être utilisé non plus parce que notre élimination de points nous fait perdre la propriété de convexité essentielle pour pouvoir mener un tel raisonnement. Il faudrait de plus être capable de calculer le volume du simplexe unité, ce qui semble insurmontable.

6 Calcul de nombres pairs entre deux nombres premiers jumeaux

On rappelle qu'on élimine systématiquement les coordonnées 1 ou $p_k - 1$ selon tout p_k.

6.1 Calcul de nombres pairs entre deux nombres premiers jumeaux et qui sont compris entre 4 et 8

Rappel :
Base modulaire = $(2, 3)$
Famille génératrice = $(3, 4)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 6)$	*couple de jumeaux*
$(0, 0)$	$0 \times 3 + 0 \times 4 = 0$	6	$(5, 7)$

6.2 Calcul de nombres pairs entre deux nombres premiers jumeaux et qui sont compris entre 10 et 24

Rappel :
Base modulaire = $(2, 3, 5)$
Famille génératrice = $(15, 10, 6)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 30)$	*couple de jumeaux*
$(0, 0, 0)$	$0 \times 15 + 0 \times 10 + 0 \times 6 = 0$	30	$(29, 31)$
$(0, 0, 2)$	$0 \times 15 + 0 \times 10 + 2 \times 6 = 12$	12	$(11, 13)$
$(0, 0, 3)$	$0 \times 15 + 0 \times 10 + 3 \times 6 = 18$	18	$(17, 19)$

6.3 Calcul de nombres pairs entre deux nombres premiers jumeaux et qui sont compris entre 26 et 48

Rappel :
Base modulaire $= (2, 3, 5, 7)$
Famille génératrice $= (105, 70, 126, 120)$

Note 1 : on omet le $0 \times 105 + 0 \times 70$ dans le calcul de la combinaison linéaire.

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ (*mod* 210)	*couple de jumeaux*
$(0, 0, 0, 0)$	$0 \times 120 = 0$	0	
$(0, 0, 0, 2)$	$2 \times 120 = 240$	30	$(29, 31)$
$(0, 0, 0, 3)$	$3 \times 120 = 360$	150	$(149, 151)$
$(0, 0, 0, 4)$	$4 \times 120 = 480$	60	$(59, 61)$
$(0, 0, 0, 5)$	$5 \times 120 = 600$	180	$(179, 181)$
$(0, 0, 2, 0)$	$2 \times 126 = 252$	42	$(41, 43)$
$(0, 0, 2, 2)$	$2 \times 126 + 2 \times 120 = 492$	72	$(71, 73)$
$(0, 0, 2, 3)$	$2 \times 126 + 2 \times 120 = 612$	192	$(191, 193)$
$(0, 0, 2, 4)$	$2 \times 126 + 2 \times 120 = 732$	102	$(101, 103)$
$(0, 0, 2, 5)$	$2 \times 126 + 2 \times 120 = 852$	12	$(11, 13)$
$(0, 0, 3, 0)$	$3 \times 126 = 378$	168	$169 = 13^2$
$(0, 0, 3, 2)$	$3 \times 126 + 2 \times 120 = 618$	198	$(197, 199)$
$(0, 0, 3, 3)$	$3 \times 126 + 2 \times 120 = 738$	108	$(107, 109)$
$(0, 0, 3, 4)$	$3 \times 126 + 2 \times 120 = 858$	18	$(17, 19)$
$(0, 0, 3, 5)$	$3 \times 126 + 2 \times 120 = 978$	138	$(137, 139)$

Note 2 : même si dans le tableau ci-dessus, tous les nombres pairs sont solutions sauf un (168 a son successeur qui n'est pas premier), on est assuré d'avoir un nombre pair entre deux nombres premiers jumeaux seulement pour les nombres pairs inférieurs à $49 = 7^2$, en l'occurrence pour $12, 18, 30$ et 42.

On voit clairement apparaître des progressions arithmétiques de raison 120 qui est le dernier élément de la famille génératrice, selon lequel on a ordonné les résultats.

Le théorème de Dirichlet assure de trouver un nombre premier dans un progression arithmétique, mais la progression $ax + b$ en question doit être infinie, et les nombres a et b doivent être premiers entre eux, des conditions qui ne sont pas garanties ici, les nombres de la famille génératrice ayant systématiquement des plus grands communs diviseurs non égaux à 1 si on les considère deux à deux par exemple.

Terence Tao et Ben Green quant à eux s'intéressent à la fabrication de progressions arithmétiques de longueurs finies mais qui ne contiennent que des nombres premiers, ce qui n'est pas le cas des progressions rencontrées ici.

Pour atteindre notre but, il faudrait disposer d'un résultat intermédiaire en quelque sorte et qui affirmerait qu'un certain nombre de progressions arithmétiques, d'origines "décalées", de telles longueurs finies et raisons contraintes, seraient forcées de "taper" au moins une fois dans un intervalle de nombres de telle longueur, résultat dont on ne dispose absolument pas.

6.4 Calcul de nombres pairs entre deux nombres premiers jumeaux et qui sont compris entre 50 et 120

Rappel :
Base modulaire $= (2, 3, 5, 7, 11)$
Famille génératrice $= (1155, 1540, 1386, 330, 210)$

Note : on ne note plus les combinaisons linéaires, on fournit directement leur résultat obtenu en calculant le produit du vecteur ligne des coordonnées par le vecteur colonne de la famille génératrice. On note d'une

croix en dernière colonne les nombres inférieurs à $121 = 11^2$.

coordonnées	$sol = sol.min.(\neq 0)\ (mod\ 2310)$	$sol < 121$
$(0,0,0,0,0)$	0	
$(0,0,0,0,2)$	420	
$(0,0,0,0,3)$	630	
$(0,0,0,0,4)$	840	
$(0,0,0,0,5)$	1050	
$(0,0,0,0,6)$	1260	
$(0,0,0,0,7)$	1470	
$(0,0,0,0,8)$	1680	
$(0,0,0,0,9)$	1890	
$(0,0,0,2,0)$	660	
$(0,0,0,2,2)$	1080	
$(0,0,0,2,3)$	1290	
$(0,0,0,2,4)$	1500	
$(0,0,0,2,5)$	1710	
$(0,0,0,2,6)$	1920	
$(0,0,0,2,7)$	2130	
$(0,0,0,2,8)$	$2340 = 30$	$*$
$(0,0,0,2,9)$	240	
$(0,0,0,3,0)$	990	
$(0,0,0,3,2)$	1410	
$(0,0,0,3,3)$	1620	
$(0,0,0,3,4)$	1830	
$(0,0,0,3,5)$	2040	
$(0,0,0,3,6)$	2250	
$(0,0,0,3,7)$	$2460 = 150$	
$(0,0,0,3,8)$	360	
$(0,0,0,3,9)$	570	
$(0,0,0,4,0)$	1320	
$(0,0,0,4,2)$	1740	
$(0,0,0,4,3)$	1950	
$(0,0,0,4,4)$	2160	
$(0,0,0,4,5)$	$2370 = 60$	$*$
$(0,0,0,4,6)$	270	
$(0,0,0,4,7)$	480	
$(0,0,0,4,8)$	690	
$(0,0,0,4,9)$	900	
$(0,0,0,5,0)$	1650	
$(0,0,0,5,2)$	2070	
$(0,0,0,5,3)$	2280	
$(0,0,0,5,4)$	$2490 = 180$	
$(0,0,0,5,5)$	390	
$(0,0,0,5,6)$	600	
$(0,0,0,5,7)$	810	
$(0,0,0,5,8)$	1020	
$(0,0,0,5,9)$	1230	

$coordonnées$	$sol = sol.min.(\neq 0)\ (mod\ 2310)$	$sol < 121$
$(0,0,2,0,0)$	$2772 = 462$	
$(0,0,2,0,2)$	882	
$(0,0,2,0,3)$	1092	
$(0,0,2,0,4)$	1302	
$(0,0,2,0,5)$	1512	
$(0,0,2,0,6)$	1722	
$(0,0,2,0,7)$	2932	
$(0,0,2,0,8)$	2142	
$(0,0,2,0,9)$	$2352 = 42$	$*$
$(0,0,2,2,0)$	1122	
$(0,0,2,2,2)$	1542	
$(0,0,2,2,3)$	1752	
$(0,0,2,2,4)$	1962	
$(0,0,2,2,5)$	2172	
$(0,0,2,2,6)$	$2382 = 72$	$*$
$(0,0,2,2,7)$	282	
$(0,0,2,2,8)$	492	
$(0,0,2,2,9)$	702	
$(0,0,2,3,0)$	1452	
$(0,0,2,3,2)$	1872	
$(0,0,2,3,3)$	2082	
$(0,0,2,3,4)$	2292	
$(0,0,2,3,5)$	$2502 = 192$	
$(0,0,2,3,6)$	402	
$(0,0,2,3,7)$	612	
$(0,0,2,3,8)$	822	
$(0,0,2,3,9)$	1032	
$(0,0,2,4,0)$	1782	
$(0,0,2,4,2)$	2202	
$(0,0,2,4,3)$	$2412 = 102$	$*$
$(0,0,2,4,4)$	312	
$(0,0,2,4,5)$	522	
$(0,0,2,4,6)$	732	
$(0,0,2,4,7)$	942	
$(0,0,2,4,8)$	1152	
$(0,0,2,4,9)$	1362	
$(0,0,2,5,0)$	2112	
$(0,0,2,5,2)$	$2532 = 222$	
$(0,0,2,5,3)$	432	
$(0,0,2,5,4)$	642	
$(0,0,2,5,5)$	852	
$(0,0,2,5,6)$	1062	
$(0,0,2,5,7)$	1272	
$(0,0,2,5,8)$	1482	
$(0,0,2,5,9)$	1692	

$coordonnées$	$sol = sol.min.(\neq 0)\ (mod\ 2310)$	$sol < 121$
$(0,0,3,0,0)$	$4158 = 1848$	
$(0,0,3,0,2)$	2268	
$(0,0,3,0,3)$	$2478 = 168$	
$(0,0,3,0,4)$	378	
$(0,0,3,0,5)$	588	
$(0,0,3,0,6)$	798	
$(0,0,3,0,7)$	1008	
$(0,0,3,0,8)$	1218	
$(0,0,3,0,9)$	1428	
$(0,0,3,2,0)$	$2508 = 198$	
$(0,0,3,2,2)$	618	
$(0,0,3,2,3)$	828	
$(0,0,3,2,4)$	1038	
$(0,0,3,2,5)$	1248	
$(0,0,3,2,6)$	1458	
$(0,0,3,2,7)$	1668	
$(0,0,3,2,8)$	1878	
$(0,0,3,2,9)$	2088	
$(0,0,3,3,0)$	528	
$(0,0,3,3,2)$	948	
$(0,0,3,3,3)$	1158	
$(0,0,3,3,4)$	1368	
$(0,0,3,3,5)$	1578	
$(0,0,3,3,6)$	1788	
$(0,0,3,3,7)$	1998	
$(0,0,3,3,8)$	2208	
$(0,0,3,3,9)$	$2418 = 108$	$*$
$(0,0,3,4,0)$	858	
$(0,0,3,4,2)$	1278	
$(0,0,3,4,3)$	1488	
$(0,0,3,4,4)$	1698	
$(0,0,3,4,5)$	1908	
$(0,0,3,4,6)$	2118	
$(0,0,3,4,7)$	$2328 = 18$	$*$
$(0,0,3,4,8)$	228	
$(0,0,3,4,9)$	438	
$(0,0,3,5,0)$	1188	
$(0,0,3,5,2)$	1608	
$(0,0,3,5,3)$	1818	
$(0,0,3,5,4)$	2028	
$(0,0,3,5,5)$	2238	
$(0,0,3,5,6)$	$2448 = 138$	
$(0,0,3,5,7)$	348	
$(0,0,3,5,8)$	558	
$(0,0,3,5,9)$	768	

On constate qu'il y a très peu de solutions (7) dont on est assuré qu'il s'agit bien de nombres pairs entre deux nombres premiers jumeaux car ils sont inférieurs à $11^2 = 121$.

Annexe : Calcul de décomposants de Goldbach du nombre pair 128

128 étant une puissance de 2 a peu de diviseurs, cela diminue combinatoirement la quantité de nombres à étudier.

Pour trouver certains décomposants de Goldbach de 128 compris entre $122 = 11^2 + 1$ et $168 = 13^2 - 1$, on utilise la base modulaire $(2, 3, 5, 7, 11)$, la famille génératrice $(1155, 1540, 1386, 330, 210)$ et on travaille modulo $2310 = 2 \times 3 \times 5 \times 7 \times 11$.

En effet, $1155 = 1 \times 3 \times 5 \times 7 \times 11$ est congru à 1 (mod 2) (c'est le nombre correspondant au vecteur $(1, 0, 0, 0, 0)$) ; $1540 = 2 \times 2 \times 5 \times 7 \times 11$ est congru à 1 (mod 3) (et correspond au vecteur $(0, 1, 0, 0, 0)$) ; $1386 = 3 \times 2 \times 3 \times 7 \times 11$ est congru à 1 (mod 5) (et correspond au vecteur $(0, 0, 1, 0, 0)$) ; $330 = 1 \times 2 \times 3 \times 5 \times 11$ est congru à 1 (mod 7) (et correspond au vecteur $(0, 0, 0, 1, 0)$) ; $210 = 1 \times 2 \times 3 \times 5 \times 7$ est congru à 1 (mod 11) (et correspond au vecteur $(0, 0, 0, 0, 1)$).

- $x = 128 = (0, 2, 3, 2, 7)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 210)$	*D.G. de* 128
$(1,1,1,1,1)$	$1 \times 1155 + 1 \times 1540 + 1 \times 1386 + 1 \times 330 + 1 \times 210$	1	
$(1,1,1,1,2)$	$... + 210$	211	
$(1,1,1,1,3)$	$... + 210$	421	
$(1,1,1,1,4)$	$... + 210$	631	
$(1,1,1,1,5)$	$... + 210$	841	
$(1,1,1,1,6)$	$... + 210$	1051	
$(1,1,1,1,8)$	$... + 420$	1471	
$(1,1,1,1,9)$	$... + 210$	1681	
$(1,1,1,1,10)$	$... + 210$	1891	
$(1,1,1,3,1)$	$1 \times 1155 + 1 \times 1540 + 1 \times 1386 + 3 \times 330 + 1 \times 210$	661	
$(1,1,1,3,2)$	$... + 210$	871	
$(1,1,1,3,3)$	$... + 210$	1081	
$(1,1,1,3,4)$	$... + 210$	1291	
$(1,1,1,3,5)$	$... + 210$	1501	
$(1,1,1,3,6)$	$... + 210$	1711	
$(1,1,1,3,8)$	$... + 420$	2131	
$(1,1,1,3,9)$	$... + 210$	31	$*$
$(1,1,1,3,10)$	$... + 210$	241	
$(1,1,1,4,1)$	$1 \times 1155 + 1 \times 1540 + 1 \times 1386 + 4 \times 330 + 1 \times 210$	991	
$(1,1,1,4,2)$	$... + 210$	1201	
$(1,1,1,4,3)$	$... + 210$	1411	
$(1,1,1,4,4)$	$... + 210$	1621	
$(1,1,1,4,5)$	$... + 210$	1831	
$(1,1,1,4,6)$	$... + 210$	2041	
$(1,1,1,4,8)$	$... + 420$	151	
$(1,1,1,4,9)$	$... + 210$	361	
$(1,1,1,4,10)$	$... + 210$	471	
$(1,1,1,5,1)$	$1 \times 1155 + 1 \times 1540 + 1 \times 1386 + 5 \times 330 + 1 \times 210$	1321	
$(1,1,1,5,2)$	$... + 210$	1531	
$(1,1,1,5,3)$	$... + 210$	1741	
$(1,1,1,5,4)$	$... + 210$	1951	
$(1,1,1,5,5)$	$... + 210$	2161	
$(1,1,1,5,6)$	$... + 210$	61	$*$
$(1,1,1,5,8)$	$... + 420$	481	
$(1,1,1,5,9)$	$... + 210$	691	
$(1,1,1,5,10)$	$... + 210$	901	
$(1,1,1,6,1)$	$1 \times 1155 + 1 \times 1540 + 1 \times 1386 + 1 \times 330 + 1 \times 210$	1651	
$(1,1,1,6,2)$	$... + 210$	1861	
$(1,1,1,6,3)$	$... + 210$	2071	
$(1,1,1,6,4)$	$... + 210$	2281	
$(1,1,1,6,5)$	$... + 210$	181	
$(1,1,1,6,6)$	$... + 210$	391	
$(1,1,1,6,8)$	$... + 420$	811	
$(1,1,1,6,9)$	$... + 210$	1021	
$(1,1,1,6,10)$	$... + 210$	1231	

- *rappel* : $x = 128 = (0, 2, 3, 2, 7)$

coordonnées	*combinaison linéaire*	*sol.min.*$(\neq 0)$ $(mod\ 210)$	*D.G. de* 128
$(1,1,2,1,1)$	$1\times 1155 + 1\times 1540 + 2\times 1386 + 1\times 330 + 1\times 210$	1387	
$(1,1,2,1,2)$	$... + 210$	1597	
$(1,1,2,1,3)$	$... + 210$	1807	
$(1,1,2,1,4)$	$... + 210$	2017	
$(1,1,2,1,5)$	$... + 210$	2227	
$(1,1,2,1,6)$	$... + 210$	127	
$(1,1,2,1,8)$	$... + 420$	547	
$(1,1,2,1,9)$	$... + 210$	757	
$(1,1,2,1,10)$	$... + 210$	967	
$(1,1,2,3,1)$	$1\times 1155 + 1\times 1540 + 2\times 1386 + 3\times 330 + 1\times 210$	2047	
$(1,1,2,3,2)$	$... + 210$	2257	
$(1,1,2,3,3)$	$... + 210$	157	
$(1,1,2,3,4)$	$... + 210$	367	
$(1,1,2,3,5)$	$... + 210$	577	
$(1,1,2,3,6)$	$... + 210$	787	
$(1,1,2,3,8)$	$... + 420$	1207	
$(1,1,2,3,9)$	$... + 210$	1417	
$(1,1,2,3,10)$	$... + 210$	1627	
$(1,1,2,4,1)$	$1\times 1155 + 1\times 1540 + 2\times 1386 + 4\times 330 + 1\times 210$	67	$*$
$(1,1,2,4,2)$	$... + 210$	277	
$(1,1,2,4,3)$	$... + 210$	487	
$(1,1,2,4,4)$	$... + 210$	697	
$(1,1,2,4,5)$	$... + 210$	907	
$(1,1,2,4,6)$	$... + 210$	1117	
$(1,1,2,4,8)$	$... + 420$	1537	
$(1,1,2,4,9)$	$... + 210$	1747	
$(1,1,2,4,10)$	$... + 210$	1957	
$(1,1,2,5,1)$	$1\times 1155 + 1\times 1540 + 2\times 1386 + 5\times 330 + 1\times 210$	397	
$(1,1,2,5,2)$	$... + 210$	607	
$(1,1,2,5,3)$	$... + 210$	817	
$(1,1,2,5,4)$	$... + 210$	1027	
$(1,1,2,5,5)$	$... + 210$	1237	
$(1,1,2,5,6)$	$... + 210$	1447	
$(1,1,2,5,8)$	$... + 420$	1657	
$(1,1,2,5,9)$	$... + 210$	1867	
$(1,1,2,5,10)$	$... + 210$	2077	
$(1,1,2,6,1)$	$1\times 1155 + 1\times 1540 + 2\times 1386 + 6\times 330 + 1\times 210$	727	
$(1,1,2,6,2)$	$... + 210$	937	
$(1,1,2,6,3)$	$... + 210$	1147	
$(1,1,2,6,4)$	$... + 210$	1357	
$(1,1,2,6,5)$	$... + 210$	1567	
$(1,1,2,6,6)$	$... + 210$	1777	
$(1,1,2,6,8)$	$... + 420$	2197	
$(1,1,2,6,9)$	$... + 210$	97	$*$
$(1,1,2,6,10)$	$... + 210$	307	

- *rappel* : $x = 128 = (0, 2, 3, 2, 7)$

coordonnées	*combinaison linéaire*	*sol.min.*($\neq 0$) (*mod* 210)	*D.G. de* 128
$(1, 1, 4, 1, 1)$	$1 \times 1155 + 1 \times 1540 + 4 \times 1386 + 1 \times 330 + 1 \times 210$	1849	
$(1, 1, 4, 1, 2)$	$... + 210$	2059	
$(1, 1, 4, 1, 3)$	$... + 210$	2269	
$(1, 1, 4, 1, 4)$	$... + 210$	169	
$(1, 1, 4, 1, 5)$	$... + 210$	379	
$(1, 1, 4, 1, 6)$	$... + 210$	589	
$(1, 1, 4, 1, 8)$	$... + 420$	1009	
$(1, 1, 4, 1, 9)$	$... + 210$	1219	
$(1, 1, 4, 1, 10)$	$... + 210$	1429	
$(1, 1, 4, 3, 1)$	$1 \times 1155 + 1 \times 1540 + 4 \times 1386 + 3 \times 330 + 1 \times 210$	199	
$(1, 1, 4, 3, 2)$	$... + 210$	409	
$(1, 1, 4, 3, 3)$	$... + 210$	619	
$(1, 1, 4, 3, 4)$	$... + 210$	829	
$(1, 1, 4, 3, 5)$	$... + 210$	1039	
$(1, 1, 4, 3, 6)$	$... + 210$	1249	
$(1, 1, 4, 3, 8)$	$... + 420$	1669	
$(1, 1, 4, 3, 9)$	$... + 210$	1879	
$(1, 1, 4, 3, 10)$	$... + 210$	2089	
$(1, 1, 4, 4, 1)$	$1 \times 1155 + 1 \times 1540 + 4 \times 1386 + 4 \times 330 + 1 \times 210$	529	
$(1, 1, 4, 4, 2)$	$... + 210$	739	
$(1, 1, 4, 4, 3)$	$... + 210$	949	
$(1, 1, 4, 4, 4)$	$... + 210$	1159	
$(1, 1, 4, 4, 5)$	$... + 210$	1369	
$(1, 1, 4, 4, 6)$	$... + 210$	1579	
$(1, 1, 4, 4, 8)$	$... + 420$	1999	
$(1, 1, 4, 4, 9)$	$... + 210$	2209	
$(1, 1, 4, 4, 10)$	$... + 210$	109	$*$
$(1, 1, 4, 5, 1)$	$1 \times 1155 + 1 \times 1540 + 4 \times 1386 + 5 \times 330 + 1 \times 210$	859	
$(1, 1, 4, 5, 2)$	$... + 210$	1069	
$(1, 1, 4, 5, 3)$	$... + 210$	1279	
$(1, 1, 4, 5, 4)$	$... + 210$	1489	
$(1, 1, 4, 5, 5)$	$... + 210$	1699	
$(1, 1, 4, 5, 6)$	$... + 210$	1909	
$(1, 1, 4, 5, 8)$	$... + 420$	19	$*$
$(1, 1, 4, 5, 9)$	$... + 210$	229	
$(1, 1, 4, 5, 10)$	$... + 210$	439	
$(1, 1, 4, 6, 1)$	$1 \times 1155 + 1 \times 1540 + 4 \times 1386 + 6 \times 330 + 1 \times 210$	1189	
$(1, 1, 4, 6, 2)$	$... + 210$	1399	
$(1, 1, 4, 6, 3)$	$... + 210$	1609	
$(1, 1, 4, 6, 4)$	$... + 210$	1819	
$(1, 1, 4, 6, 5)$	$... + 210$	2029	
$(1, 1, 4, 6, 6)$	$... + 210$	2239	
$(1, 1, 4, 6, 8)$	$... + 420$	349	
$(1, 1, 4, 6, 9)$	$... + 210$	559	
$(1, 1, 4, 6, 10)$	$... + 210$	769	

On constate qu'il y a très peu de nombres qui sont inférieurs à $64 = 128/2$ (seulement 6) dont on est assuré qu'ils sont bien des décomposants de Goldbach de 128.