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

Denise Vella

Décembre 2006

1 Introduction

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

2 Etude d'un exemple

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

Pour 98, ces restes sont :

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

On aboutit à la table suivante :

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

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

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

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

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

Mathématiquement, cela s'écrit[2] :

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

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

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

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

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

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

3 Les beautés cachées des tables de congruence

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5 Les Recherches arithmétiques de Gauss

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

6 Les preuves élémentaires d'Erdös

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

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

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

7 La découverte merveilleuse d'Euler

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

8 La géométrie des nombres de Minkowski

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

10 Conjecture des nombres premiers jumeaux

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

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

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

11 Raisonner probabilistiquement

11.1 Congruences

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

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

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

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

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

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

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

11.2 Incongruités (!)

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

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

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

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

Avec les nombres premiers 2, 3, et 5,

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

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

12 Résumé de la démonstration

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

13 Conclusion

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

Bibliographie

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

int fa(){
    int i;

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

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

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

int main (int argc, char* argv[]){
    int i, x;

    fa();
    fh();
    calcule();
    for (i = 1 ; i < taille ; i++)
        std::cout << " " << euler[i];}
```