Vers une preuve de la conjecture de Goldbach

Denise Vella

Décembre 2005

1 Rappels

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

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

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

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

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

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

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

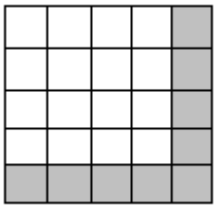
Sont colorés en rouge les nombres premiers de la forme $4n+1$. Sont colorés en vert les nombres premiers de la forme $4n+3$. Dans la troisième ligne du tableau sont fournis les restes modulo 19 des carrés des deux nombres au-dessus de lui (ils ont en effet même reste, comme on l'a vu). Enfin, sont surmontés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

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

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

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

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



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

2 Etude d'exemples

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

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

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

2.1 Les $4x+2$

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

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

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

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

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

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

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

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

2.2 Les $4x$

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

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

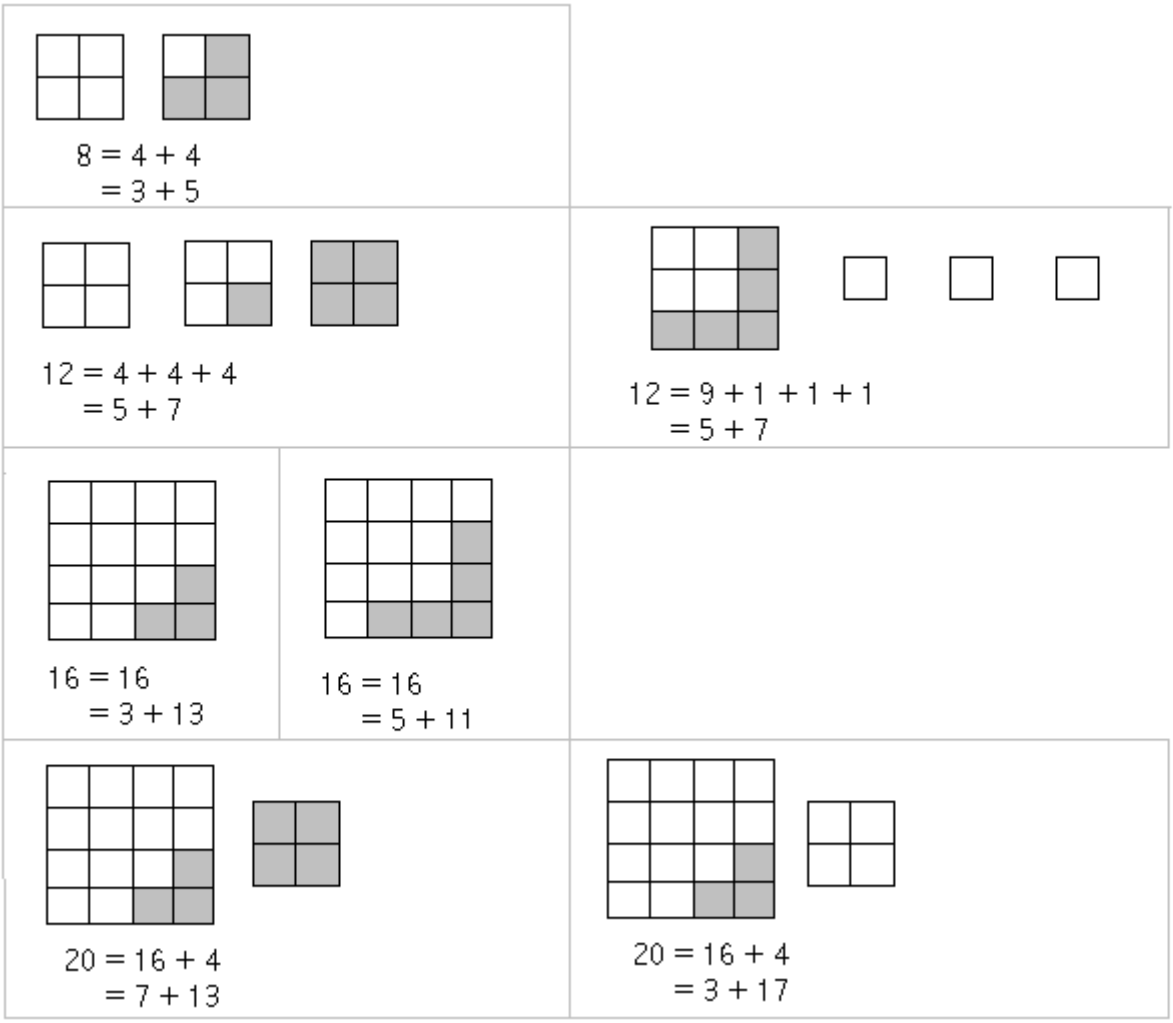
Résoudre la conjecture de Goldbach est équivalent à démontrer que quelque soit x, il existe a et b tels que $a+b = x-1$ et $4a+3$ est premier et $4b+1$ est premier.

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

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

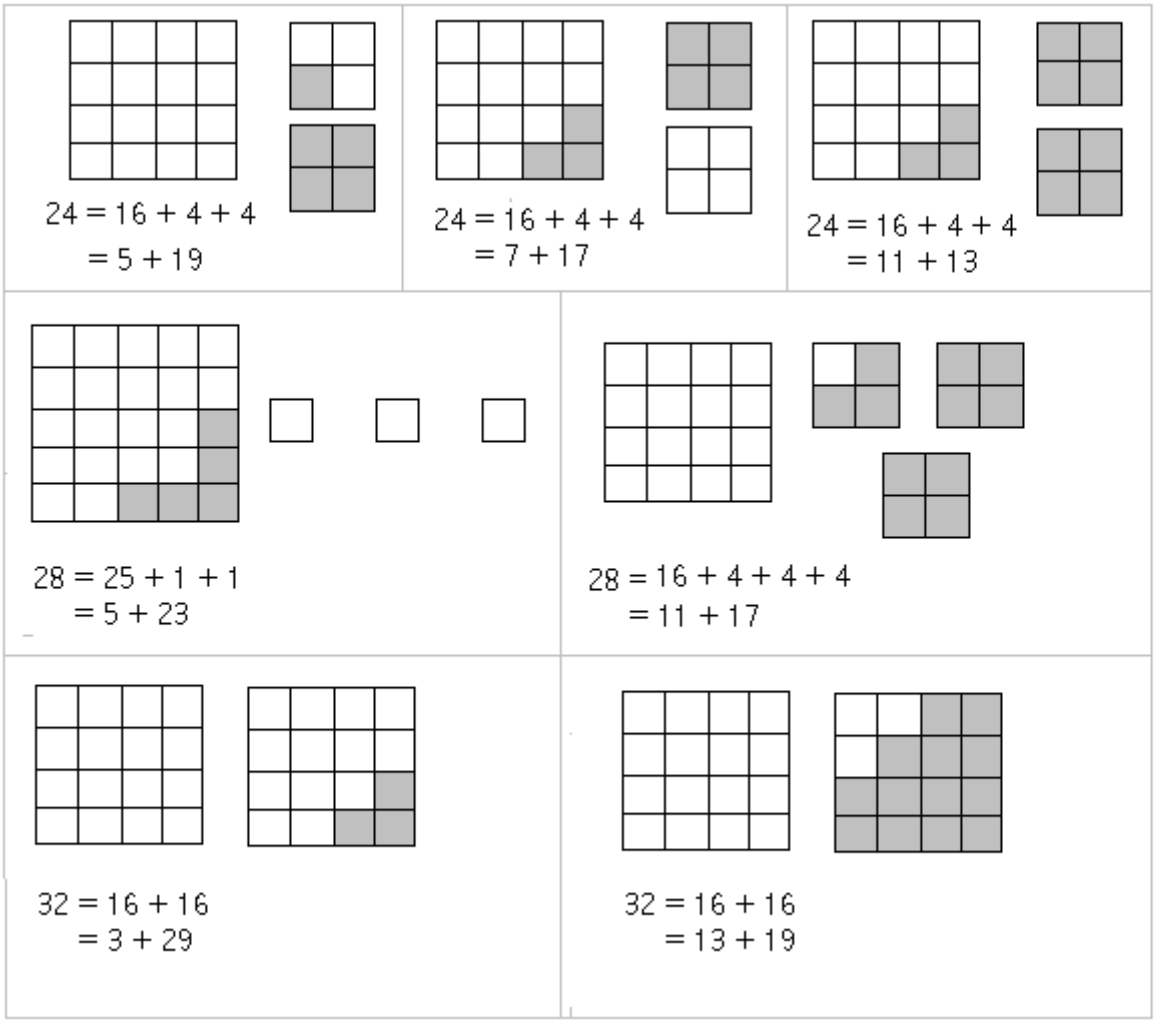
$$4x = a^2 + b^2 + c^2 + d^2 = (4n + 1) + (4n' + 3) = p_1 + p_2$$

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



3 Tentatives précédentes infructueuses

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



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

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

4 Conclusion

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