Conjecture de Goldbach : approches algébrique et géométrique basées sur les restes modulaires

Denise Vella

1er Novembre 2008

1 Introduction

La conjecture de Goldbach (1742) énonce que tout nombre pair $2a$ supérieur ou égal à 4 est la somme de deux nombres premiers p et q. Le nombre p et le nombre q sont appelés des décomposants de Goldbach de $2a$. Cette note présente deux visions de la conjecture de Goldbach, une vision algébrique et une vision géométrique, toutes deux basées sur l'étude des restes modulaires des entiers selon des modules premiers. Les décomposants de Goldbach d'un entier pair $2a$ sont les nombres premiers inférieurs ou égaux à a solutions de systèmes de congruence généralisés découlant de cette représentation. Enfin, sera présentée une conjecture portant sur le partage des décomposants de Goldbach et qui donne à penser que la possibilité d'une démonstration de la conjecture de Goldbach par récurrence pourrait être envisagée.

2 Traitement algébrique d'un exemple

Dans une note précédente, on a présenté le choix que nous réitérons ici de représenter chaque entier par ses restes selon les modules premiers successifs.

Intéressons nous au nombre entier 40, dont on cherche les décomposants de Goldbach. On ne va s'intéresser qu'aux restes des entiers inférieurs à 20 selon les modules premiers inférieurs à la racine de 40, i.e. selon les modules 2, 3 et 5. 40 est représenté par le triplet $(0(2), 1(3), 0(5))$. Puisque seuls les nombres premiers non congrus à 40 selon tous ces modules peuvent être décomposants de Goldbach de 40, on cherche s'il existe des nombres premiers dont la représentation serait :

- soit $(1(2), 2(3), 1(5))$,
- soit $(1(2), 2(3), 2(5))$,
- soit $(1(2), 2(3), 3(5))$,
- soit $(1(2), 2(3), 4(5))$.

Considérons le premier triplet $(1(2), 2(3), 1(5))$. Les solutions satisfaisant la première coordonnée d'un tel triplet sont les nombres x strictement positifs tels qu'il existe y entier positif ou nul tel que l'équation $x - 2y - 1 = 0$ admet une solution (i.e. on cherche une solution qui soit forcément un nombre impair). Les solutions satisfaisant à la deuxième coordonnée du triplet sont les nombres x strictement positifs tels qu'il existe z entier positif ou nul tel que $x - 3z - 2 = 0$

admet une solution (on cherche un nombre qui soit non congru à 1 mod 3, en étant en l'occurrence congru à 2 mod 3).
Enfin, les solutions satisfaisant à la troisième coordonnée du triplet sont les nombres x strictement positifs tels qu'il existe t entier positif ou nul tel que $x - 5t - 1 = 0$ admet une solution (on cherche un nombre qui soit non congru à 0 mod 5 en étant en l'occurrence congru à 1 mod 5).

Pour le premier triplet, on aboutit donc au système d'équations diophantiennes :

$$\begin{cases} x - 2y - 1 = 0 \\ x - 3z - 2 = 0 \\ x - 5t - 1 = 0 \end{cases}$$

Pour les deuxième, troisième et quatrième triplets, on aboutit aux systèmes d'équations diophantiennes :

$$\begin{cases} x - 2y - 1 = 0 \\ x - 3z - 2 = 0 \\ x - 5t - 2 = 0 \end{cases}$$

$$\begin{cases} x - 2y - 1 = 0 \\ x - 3z - 2 = 0 \\ x - 5t - 3 = 0 \end{cases}$$

$$\begin{cases} x - 2y - 1 = 0 \\ x - 3z - 2 = 0 \\ x - 5t - 4 = 0 \end{cases}$$

Le premier système d'équations admet $(x = 11, y = 5, z = 3, t = 2)$ comme solution, 11 est décomposant de Goldbach de 40.
Le deuxième système d'équations admet $(x = 17, y = 8, z = 5, t = 3)$ comme solution, 17 est décomposant de Goldbach de 40.

3 Généralisation

On peut généraliser l'exemple présenté ci-dessus. Les systèmes d'équations diophantiennes que les nombres premiers décomposants de Goldbach d'un nombre pair $2a$ doivent satisfaire contiennent des équations de la forme :

$$x - p_i x_i - C_i = 0,$$

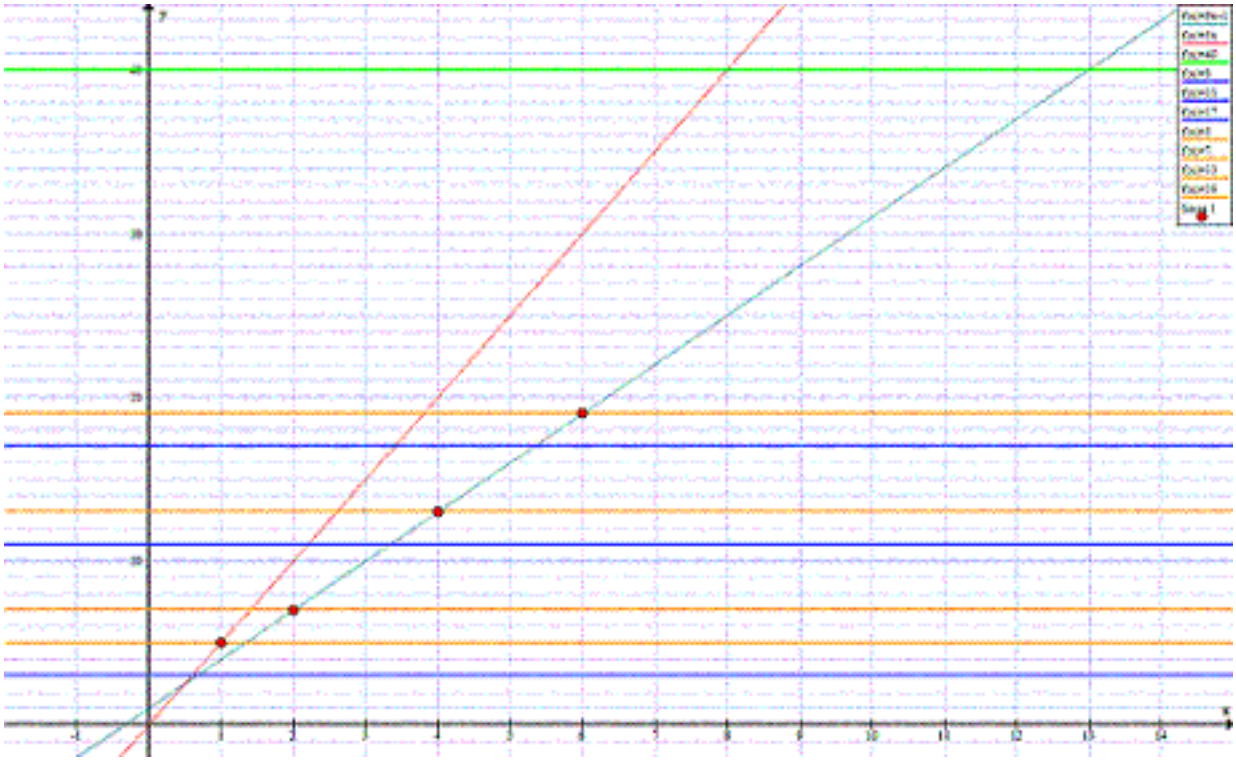
les p_i étant les nombres premiers inférieurs à $\sqrt{2a}$ et les constantes C_i prenant toutes les valeurs possibles qui soient à la fois différentes de 0 et différentes du reste de $2a$ modulo p_i.

Reste à prouver (sic !) pourquoi il existe toujours un nombre premier solution x de l'un de ces systèmes d'équations diophantiennes.

Matiiassevitch a trouvé en 1970 la réponse au dixième problème de Hilbert : il n'existe aucun algorithme général permettant d'affirmer l'existence de solutions pour les équations diophantiennes.

Je me demande cependant si dans le cas qui nous intéresse ici de systèmes d'équations diophantiennes d'un type particulier, on ne pourrait pas prouver l'existence d'un nombre premier solution en utilisant le théorème de Minkowski. Ce théorème peut être utilisé d'une façon très élégante pour montrer par exemple qu'un nombre premier congru à 1 modulo 4 est toujours somme de deux carrés, ou qu'un nombre entier est toujours somme de 4 carrés. Ces deux preuves sont fournies dans le livre Arithmétique de Marc Hindry [9]. On définit un "réseau" de points à coordonnées entières. On délimite un convexe symétrique autour de l'origine et qui soit d'une taille supérieure à une taille fixée. Le théorème permet d'établir qu'un tel convexe contient toujours un point à coordonnées entières (en l'occurrence, il faudrait se débrouiller pour que le point en question soit le nombre premier inférieur à a recherché).

4 Présentation géométrique du même exemple



Sur le repère cartésien de la figure ci-dessus, la droite horizontale verte d'équation $y = 40$ correspond au nombre 40.

Les restes de 40 selon les modules 3 et 5 se lisent sur l'axe des ordonnées (on a omis d'illustrer que 40 est pair pour augmenter la lisibilité de la figure).

Les droites horizontales bleues d'équations $y = 3$, $y = 11$ et $y = 17$ correspondent aux nombres premiers 3, 11 et 17 qui sont tous les trois décomposants de Goldbach de 40 tandis que les droites horizontales oranges d'équations $y = 5$, $y = 7$, $y = 13$ et $y = 19$ correspondent aux nombres premiers qui ne sont pas décomposants de Goldbach de 40.

Les points rouges montrent l'élimination de ces nombres premiers qui ne peuvent être décomposants de Goldbach de 40 sous prétexte qu'ils sont congrus à 40 selon un certain module. Les trois points rouges de la droite $y = 3x + 1$ éliminent les nombres premiers 7, 13 et 19 tandis que le point rouge sur la droite d'équation $y = 5x$ élimine le nombre premier 5.

Les droites horizontales bleues n'ayant pas de points d'intersection à coordonnées entières avec les droites $y = 3x + 1$ ou $y = 5x$ fournissent une visualisation des décomposants de Goldbach de 40.

On ne s'est pas intéressé à la droite d'équation $y = 9$, pourtant le nombre 9 est intéressant lorsqu'on recherche les décomposants de Goldbach de 40 parce qu'il n'est jamais congru à 40 selon les modules 2, 3 et 5 (la représentation de 9 est en effet $(1(2), 0(3), 4(5))$). On voit que 9 est composé car la droite $y = 3x$ a comme point commun avec la droite $y = 9$ le point $(3, 9)$ de coordonnées entières.

Pour aboutir à une démonstration géométrique de la conjecture de Goldbach, il faudrait être capable d'une part de compter le nombre de points à coordonnées entières qui se trouvent à l'intérieur d'un certain espace à définir précisément, et d'autre part d'utiliser un principe de raisonnement (tel que le principe des tiroirs, ou un principe combinatoire plus complexe) qui nous permettrait de déduire qu'on peut toujours trouver une droite qui n'a aucune intersection à coordonnées entières avec les droites affines visualisant l'appartenance de $2a$ à ses classes d'équivalence selon les modules premiers inférieurs à $\sqrt{2a}$.

Alain Connes a parlé dans plusieurs conférences du "démon de l'algèbre" et de "l'ange de la géométrie" selon une idée d'Hermann Weyl. Ces notions visaient peut-être à faire appréhender "l'évidence qui saute aux yeux" devant certaines démonstrations purement géométriques (on peut penser pour illustrer cela à certaines animations sur la toile faisant se déplacer les pièces d'un puzzle et rendant immédiate à notre perception visuelle la démonstration du théorème de Pythagore[1]). La représentation géométrique, sous prétexte qu'elle permet cette perception visuelle globale et immédiate d'un problème, nous évitant ainsi d'avoir à suivre le déroulement séquentiel du langage algébrique, permettrait-elle d'aboutir à une démonstration géométrique de la conjecture de Goldbach ? Le tout petit exemple fourni montre que la quantité d'éléments visuels à intégrer simultanément peut être importante.

[1] On trouve même un film de transvasement de liquides de deux parallélépipèdes plats et carrés (a^2 et b^2) vers un troisième (c^2).

5 Différentes causes, produisant les mêmes effets, peuvent provoquer une illusion de périodicité

En écumant les bibliothèques municipales, j'ai trouvé un jour un très beau livre de Davis et Hersh [2] en annexe duquel étaient fournies les décompositions de Goldbach suivantes (entre autres).

Les premières[2] décompositions des nombres de 20902 à 20924 sont :

$$\begin{array}{lll} 20902 & = 3 & +20899 \\ 20904 & = 5 & +20890 \\ 20906 & = 3 & +20903 \\ 20908 & = 5 & +20903 \\ 20910 & = 7 & +20903 \\ 20912 & = 13 & +20899 \\ 20914 & = 11 & +20903 \\ 20916 & = 13 & +20903 \\ 20918 & = 19 & +20899 \\ 20920 & = 17 & +20903 \\ 20922 & = 19 & +20903 \\ 20924 & = 3 & +20921 \end{array}$$

Et les premières décompositions des nombres de 20962 à 20984 sont ;

$$\begin{array}{lll} 20962 & = 3 & +20959 \\ 20964 & = 5 & +20959 \\ 20966 & = 3 & +20963 \\ 20968 & = 5 & +20963 \\ 20970 & = 7 & +20963 \\ 20972 & = 13 & +20959 \\ 20974 & = 11 & +20963 \\ 20976 & = 13 & +20963 \\ 20978 & = 19 & +20959 \\ 20980 & = 17 & +20963 \\ 20982 & = 19 & +20963 \\ 20984 & = 3 & +20981 \end{array}$$

En étudiant les restes modulaires, j'ai analysé pourquoi on aboutissait à la même suite de nombres premiers dans les deux cas (en espérant profondément que les mêmes causes produiraient les mêmes effets, selon l'adage). En fait, cela n'est pas du tout le cas : prenons le cas des nombres 20912 et 20972 qui ont tous les deux pour plus petit décomposant 13, c'est à dire ne peuvent avoir ni l'un ni l'autre 3, 5, 7 et 11 comme décomposants sous prétexte qu'ils partagent avec ceux-ci des classes de congruence. 20912 partage sa classe de congruence avec le nombre premier 3, cela modulo 7 alors que 20972 partage sa classe de congruence avec le même nombre premier 3 modulo 13. Les classes de congruence modulo 5, 7 et 11 sont partagées selon le même module. Quant aux deux nombres suivants, 20914 et 20974, qui ont tous deux pour plus petit décomposant 11, on voit sur leur écriture par les restes que c'est bien leur congruence commune à 1 modulo 3

[2]Celles faisant intervenir le nombre premier le plus petit possible étant donné un nombre pair.

qui fait éliminer 7 comme décomposant pour chacun d'entre eux. Par contre, la congruence à 3 se fait modulo 11 pour le premier et modulo 67 pour le second. La congruence à 5 se fait modulo 7 pour le premier et modulo 13 pour le second.

La base des nombres premiers jusqu'à 149 (le plus grand premier inférieur à la racine de 20984) qui a été utilisée est :
(2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97,101,103,107, 109,113,127,131,137,139,149).

Les écritures par les restes modulaires des nombres auxquels on s'intéresse sont :

20912 : plus petit décomposant 13
0-2(5,11)-2(7)-3(3)-1-8-2-12-5-3-18-7-2-14-44-30-26-50-8-38-34-56-79-86-57-5-3-47-93-7-84-83-88-62

20914 : plus petit décomposant 11
0-1(7)-4-5(5)-3(3)-10-4-14-7-5-20-9-4-16-46-32-28-52-10-40-36-58-81-88-59-7-5-49-95-9-86-85-90-64

20972 : plus petit décomposant 13
0-2(5,11)-2(7)-0-6-3(3)-11-15-19-5-16-30-21-31-10-37-27-49-1-27-21-37-56-57-20-65-63-0-44-67-17-12-11-122

20974 : plus petit décomposant 11
0-1(7)-4-2-8-5(5)-13-17-21-7-18-32-23-33-12-39-29-51-3(3)-29-23-39-58-59-22-67-65-2-46-69-19-14-13-124

6 Une nouvelle conjecture liée à la conjecture de Goldbach

Dans la mesure où un nombre premier p décomposant de Goldbach d'un nombre pair $2a$ est non congru à $2a$ selon tout module, j'ai pensé qu'un tel nombre premier devait assez souvent être également un décomposant d'un pair à distance $6k$ de $2a$, puisque $2a$ et $2a + 6k$ partagent leur coordonnée selon les modules 2 et 3 simultanément.

On peut tester informatiquement cette conjecture selon laquelle tout nombre pair $2a$ supérieur à 14 et inférieur à 3.10^6 partage au moins l'un de ses décomposants de Goldbach avec $2a - 6$. Dominique Ceugniet [3] confirme cette nouvelle conjecture jusqu'à 16.10^8. Il a également fait quelques statistiques : pour les nombres pairs compris entre 15.10^8 (inclus) et 16.10^8 (exclu), le nombre maximum d'essais à effectuer avant de trouver deux décompositions qui partagent un nombre premier est 8979, tandis que la moyenne du nombre d'essais à effectuer dans cette zone de nombres est 290.

L'exemple d'un décomposant partagé trouvé après 8979 essais est :
1 508 792 552 = 17 959 + 1 508 774 593

[3] Un internaute compatissant, polytechnicien, et féru d'optimisation informatique.

1 508 792 546 = 17 959 + 1 508 774 587

Cette conjecture nous fait nous demander si une démonstration par récurrence (la "démonstration par excellence" selon Poincaré) ne pourrait pas être envisagée pour prouver la conjecture de Goldbach (chaque nombre pair, selon qu'il serait congru à 0, 2 ou 4 (modulo 6) "hériterait" d'un décomposant de Goldbach d'un nombre pair plus petit que lui, de proche en proche).

Bibliographie

(1) C.F. Gauss, *Recherches arithmétiques*, Ed. Jacques Gabay, 1801.
(2) P.J. Davis, R.Hersh, *l'Univers mathématique*, Ed. Gauthier-Villars, 1985
(3) D. Nordon, M.Mendès-France (illustrations), *Les mathématiques pures n'existent pas !*, Ed. Actes Sud, 1985.
(4) D. Nordon, *Les obstinations d'un mathématicien*, Ed. Belin Pour La Science, 2003.
(5) A. Doxiadis, *Oncle Pétros et la conjecture de Goldbach*, Ed. Points, 2002.
(6) L. Euler, *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs*, Commentatio 175 indicis Enestroemiani, Bibliothèque impartiale 3, 1751, p.10-31.
(7) J. Hadamard, *Essai sur la psychologie de l'invention dans le domaine mathématique*, suivi de H. Poincaré, *L'invention mathématique*, Ed. Jacques Gabay, 2000.
(8) C. Laisant, *Sur un procédé expérimental de vérification de la conjecture de Goldbach*, Bulletin de la SMF n°25 de 1897.
(9) M. Hindry, *Arithmétique*, Ed. Calvage et Mounet, 2008.