№ 3/2014

Le problème ternaire de Goldbach

Harald Helfgott

Leonhard Euler (1707–1783), l'un des plus grands mathématiciens du XVIII$^{\text{e}}$ siècle et de tous les temps, entretenait une correspondance régulière avec l'un de ses amis : Christian Goldbach (1690–1764), un amateur polymathe qui vivait et travaillait en Russie, tout comme Euler. Dans une lettre datée de juin 1742, Goldbach établit une conjecture (c'est-à-dire une hypothèse éclairée) sur les nombres premiers :

> *Es scheinet wenigstens, dass eine jede Zahl, die größer ist als 2, ein aggregatum trium numerorum primorum sey.*
>
> Il semble [. . .] que tout nombre entier naturel supérieur à 2 puisse être écrit comme la somme de trois nombres premiers.

Dans cet instantané, nous décrirons dans quelle mesure la communauté mathématique a résolu la conjecture de Goldbach, en soulignant les progrès récents.

1 Conjectures faible et forte de Goldbach

Depuis l'énoncé original de la conjecture de Goldbach, sa formulation est passée de « plus grand que 2 » à « plus grand que 5 », puisque 1 n'est plus considéré comme un nombre premier. La conjecture a longtemps été divisée en deux catégories :

- La conjecture faible (ou ternaire) de Goldbach, qui stipule que tout nombre entier impair n supérieur à 5 peut s'écrire comme la somme de trois nombres premiers ;
  par exemple : $11 = 3 + 3 + 5,\ 21 = 2 + 2 + 17$
- La conjecture forte (ou binaire) de Goldbach, qui stipule que tout nombre entier pair n supérieur à 2 peut s'écrire comme la somme de deux nombres premiers ;
  par exemple : $10 = 5 + 5,\ 36 = 13 + 23$

Comme leur nom l'indique, la conjecture forte implique la conjecture faible. (Pour exprimer un nombre impair $n \geq 5$ comme la somme de trois nombres premiers, il suffit de soustraire 3 pour obtenir un nombre pair $n - 3 \geq 2$. Si la conjecture forte est vraie, nous pouvons exprimer $n - 3$ comme une somme de deux nombres premiers p_1, p_2 ; donc $n = (n - 3) + 3$ est la somme des nombres premiers p_1, p_2 et 3. Comme Euler l'a fait remarquer lui-même à Goldbach, la conjecture forte implique également (et est impliquée par) l'affirmation originale de Goldbach.

L'historique du problème peut être consulté sur [1, Ch. XVIII].

Voici un bref résumé : Dans la première moitié du XVII^e^ siècle, René Descartes (1596-1650) a obtenu une propriété similaire à celle de Goldbach dans un manuscrit qui ne sera publié qu'à titre posthume (en 1901 !). Au cours du XIX^e^ siècle, des calculs ont été effectués mais n'ont malheureusement pas abouti à des résultats concluants (vérification de la conjecture pour les petits nombres entiers à la main). La conjecture forte est encore hors de portée. En 2013, j'ai terminé la preuve de la conjecture faible de Goldbach alors que j'y travaillais depuis plusieurs années.

2 Preuve de la conjecture faible de Goldbach

La démonstration s'appuie sur des fondements établis au début du XX^e^ siècle par Hardy, Littlewood et Vinogradov. En 1937, Vinogradov a prouvé [10] que la conjecture est valable pour tous les nombres impairs plus grands qu'une certaine constante C.[1] Depuis, la constante C a été spécifiée et améliorée pro-

[1] Hardy et Littlewood avaient déjà démontré la même propriété, en admettant que l'hypothèse de Riemann généralisée est vraie (consultez l'instantané « Série Dirichlet » (n°6/2014)

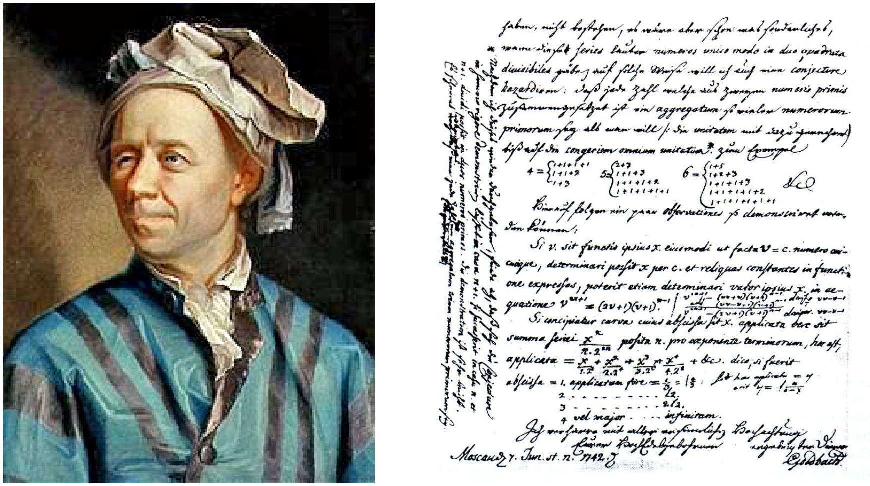

FIGURE 1 – Euler et la lettre de Goldbach. Il n'est pas facile de trouver un portrait authentique de Goldbach.

gressivement, mais la meilleure (c'est-à-dire la plus petite) valeur disponible de C,

$$C = e^{3100} \approx 2 \cdot 10^{1346}$$

(Liu-Wang [8]), était beaucoup trop grande. Nous n'avons malheureusement pas l'espoir de pouvoir vérifier les premiers 10^{1346} cas par ordinateur – et il est même très improbable qu'une civilisation terrestre ou extraterrestre puisse un jour vérifier 10^{120} cas de n'importe quel énoncé imaginable, un par un : le nombre de picosecondes depuis le début de l'univers est inférieur à 10^{30}, alors que le nombre de protons dans l'univers observable est actuellement estimé à 10^{80}, ce qui signifie que même des calculs parallèles et la dictature galactique ne seraient pas suffisants.

J'ai obtenu une valeur de C inférieure à 10^{27}. La conjecture binaire de Goldbach avait déjà été vérifiée par ordinateur jusqu'à $4 \cdot 10^{18}$ [9]. En utilisant ces calculs, on peut vérifier la conjecture de Goldbach ternaire jusqu'à 10^{27} en quelques heures sur un ordinateur de bureau moderne.[2] Cela signifie que la conjecture ternaire (faible) de Goldbach est maintenant prouvée pour tous les entiers (impairs).

pour plus d'information sur l'hypothèse de Riemann généralisée). L'hypothèse de Riemann généralisée est une conjecture standard de longue date qui n'est toujours pas prouvée.

[2] En fait, D. Platt et moi-même [6] l'avions déjà vérifiée jusqu'à $8{,}8 \cdot 10^{30}$ sur des ordinateurs parallèles.

Il est facile de comprendre pourquoi un calcul « brute-force » permet de vérifier une conjecture comme celle de Goldbach pour des valeurs de n plus petites qu'une constante C : un calcul doit être fini. Mais pourquoi une preuve mathématique donnerait-elle une limite valable uniquement pour une valeur de *n plus grande* qu'une constante C ?

3 Méthodes utilisées pour prouver le théorème

Elles sont caractéristiques des preuves « semi-analytiques », c'est-à-dire des preuves qui utilisent des outils tels que le calcul infinitésimal, l'analyse de Fourier, etc. De telles preuves démontrent généralement bien plus que le simple fait qu'un nombre entier peut être écrit d'une certaine manière (dans notre cas comme une somme de trois nombres premiers). Elles donnent également une estimation du nombre de façons dont cela est possible. L'estimation se présente sous la forme suivante : Le nombre de manières d'écrire un entier n d'une certaine façon est égal à un « terme principal » (une fonction $f(n)$) et à un « terme d'erreur » qui peut être positif ou négatif, dont la valeur absolue est $g(n)$. Si $f(n) > g(n)$, ceci démontre qu'il y a au moins une façon d'écrire n comme la somme de trois nombres premiers.

Voici un exemple très simplifié : Prenons l'hypothèse qu'une estimation avec $f(n) = n^2$, $g(n) = 1000n^{3/2}$ a été démontrée. On y arrive alors avec $f(n) > g(n)$, et cela se produit pour tous les $n > C$, où $C = 10^6$.

Voici ce qui se produit généralement : On parvient à démontrer que $f(n)$ **est** plus grand que $g(n)$, mais seulement lorsque que n est suffisamment grand. Le cas des n plus petits doit être vérifié à la main (c'est-à-dire par ordinateur). Le but est donc de faire en sorte que le terme d'erreur $g(n)$ soit aussi petit que possible, et par conséquent C plus petit.[3]

Quels sont les principaux outils d'analyse utilisés ? Certains lecteurs connaissent bien l'analyse de Fourier, c'est-à-dire la pratique consistant à décomposer une fonction f du temps en ondes sinusoïdales de différentes fréquences. En fait, nous le faisons tous les jours, lorsque nous réglons une radio analogique, ou quand notre cerveau capte une note de musique parmi plusieurs notes jouées en même temps.

En fait, l'analyse de Fourier est plus générale que cela, f n'a pas besoin d'être une fonction d'une variable continue telle que le temps. En particulier, même si f est définie uniquement sur les entiers, nous pouvons toujours la décomposer en fréquences. Il est très simple de dessiner ces fréquences sur un cercle et de les

[3] On peut aussi « truquer le jeu » (en donnant par exemple plus de poids à certains nombres premiers) de sorte que le terme principal devienne plus grand par rapport au terme d'erreur. Ce « truquage » présente aussi d'autres avantages, surtout si les poids sont continus.

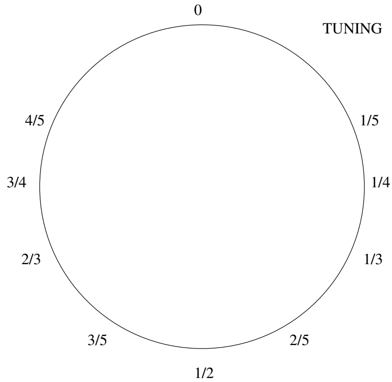

FIGURE 2 – Molette de radio d'un vrai théoricien des nombres.

étiqueter avec des nombres réels de 0 à 1 comme nous le faisons habituellement, en placant les fréquences sur une ligne et on leur attribuant des étiquettes telles que « 88 MHz » ou « A = 440 Hz ». C'est la raison pour laquelle la méthode générale que nous décrivons s'appelle la *méthode du cercle*.

Dans notre cas, nous pouvons définir f comme étant une fonction telle que $f(n) = 1$ lorsque n est un nombre premier, et $f(n) = 0$ lorsque n n'est pas un nombre premier.[4] Pourquoi est-il utile de décomposer une telle fonction en fonctions de la forme $n \mapsto \sin(2\pi\alpha n)$ ou $n \mapsto \cos(2\pi\alpha n)$?

Un problème additif, tel que celui de Goldbach, peut être reformulé en termes de *convolutions*. La convolution (additive) $g * h$ de deux fonctions g, h est une nouvelle fonction construite à partir de g et h. Pour un nombre n donné, elle est définie comme étant la somme de $g(m_1)h(m_2)$ sur tous les couples d'entiers m_1, m_2, telles que $m_1 + m_2 = n$. Voici la formule résultante :

$$(g * h)(n) = \sum_{m_1+m_2=n} g(m_1)h(m_2).$$

Ainsi, pour la fonction f que nous venons de définir, si nous démontrons que $(f * f)(n) > 0$, alors cela implique que n peut s'écrire comme la somme de deux nombres premiers d'au moins une façon, alors que si nous démontrons que $(f * f * f)(n) > 0$, cela implique que n peut s'écrire comme la somme de trois nombres premiers d'au moins une façon[5].

Une des propriétés de base d'une décomposition en fréquences est qu'une

[4] En pratique, nous utilisons une version légèrement plus compliquée où $f(n)$ décroit continuellement lorsque n croît, entre autre.

[5] Pouvez-vous trouver pourquoi ?

convolution se comporte très bien sous une telle décomposition : La *transformée de Fourier* de $g*h$ (c'est à dire sa décomposition en fréquences) est simplement le produit de la transformée de Fourier de g et de la transformée de Fourier de h.[6]

Il s'avère que $\widehat{f}(\alpha)$ est particulièrement grand lorsque α est proche d'un nombre rationnel à petit dénominateur (comme les nombres dessinés dans la figure 2). Ceci est comparable au signal radio qui s'intensifie lorsque vous vous rapprochez de la fréquence d'une station de radio donnée en tournant le bouton. Les morceaux du cercle proches de ces nombres rationnels sont appelés *arcs majeurs* ; Le reste est appelé *arcs mineurs*. Depuis Vinogradov, l'idée de base est d'estimer la valeur de $\widehat{f}(\alpha)$ aussi précisément que possible pour un α donné sur les arcs majeurs, et de montrer qu'elle est petite en dehors de ces arcs. Cela permet alors d'estimer une intégrale que l'on sait égale à $(f * f * f)(n)$.

Par ailleurs, c'est là que l'approche de base s'effondre pour le problème binaire. Les arcs majeurs sont appelés « majeurs » non pas parce qu'ils sont grands (ils ne le sont pas), mais parce qu'ils apportent une contribution majeure à l'intégrale de $\widehat{f}(\alpha)^3$ sur le cercle. Si, au contraire, vous intégrez $\widehat{f}(\alpha)^2$ (comme vous devez le faire lorsque vous additionnez 2 nombres premiers plutôt que 3), la contribution des nombres des arcs « majeurs » n'est plus majeure, elle est supplantée par l'intégrale de $|\widehat{f}(\alpha)|^2$ sur les arcs mineurs : la quadrature amplifie les pics, mais pas autant que l'élévation au cube. Pour aller encore plus loin, il faudrait être capable d'estimer $\widehat{f}(\alpha)$ assez précisément sur les arcs mineurs, mais à ce jour personne ne sait comment le faire.

4 Conclusion

C'est la structure de base. Qu'y a-t-il de nouveau dans mon travail ? Je suis reparti de zéro pour ma démonstration et j'ai trouvé des améliorations dans chaque section : Les estimations de $\widehat{f}(\alpha)$ sur les arcs majeurs, les limites supérieures sur les arcs mineurs (la partie la plus difficile, de mon point de vue), ainsi que la manière dont les deux sont constitués. Plusieurs techniques que j'ai dû améliorer ou développer sont également utiles dans d'autres secteurs de la théorie des nombres ou pour les mathématiques appliquées.

Vous trouverez une partie de ces informations dans un exposé plus long et plus détaillé que j'ai rédigé il y a quelques mois. Le texte actuel est en partie fondé sur cet exposé, à la différence près que le texte actuel se concentre sur les nouveautés. La première version de cet autre exposé a été publiée dans

[6] Une transformée de Fourier $\widehat{f}$ est une fonction de l'espace des fréquences (dans notre cas, le cercle) vers les nombres complexes. Cela permet de connaître la « quantité » de $n \mapsto \sin(2\pi\alpha n)$ ou $n \mapsto \cos(2\pi\alpha n)$ présente dans f, c'est-à-dire, l'équivalent de l'intensité du signal lorsque vous réglez le bouton de votre radio sur α.

mon blogue (http://valuevar.wordpress.com), et des versions ultérieures ont été publiées (en espagnol et en français) sur [7] et [2]. Le même exposé a servi de base pour un article plus détaillé qui paru dans les actes de la Conférence Internationale des Mathématiciens, en relation avec mon intervention en Corée en août 2014. Je vous invite donc à lire l'une ou l'autre de ces versions. Si vous souhaitez avoir une vue d'ensemble, consultez mes articles [4], [3], [5], je me suis efforcé de les rendre aussi clairs et lisibles que possible.

Commentaire de l'auteur (2023) :

L'article mentionné a été publié sous le titre

H. A. Helfgott, *The ternary Goldbach problem*, Proceedings of the International Congress of Mathematicians (ICM 2014), Seoul, Korea, August 13–21, 2014. Vol. II : Invited lectures, 391–418, KM Kyung Moon Sa, 2014.

L'auteur prépare également un livre avec la version finale de la preuve. Une grande partie est déjà disponible sur

https://webusers.imj-prg.fr/~harald.helfgott/anglais/book.html.

Crédits images

Fig. 1, image de gauche : « Leonhard Euler, un portrait par Emanuel Handmann, 1753 ». Licence du domaine public via Wikimedia Commons, http://commons.wikimedia.org/wiki/File:Leonhard_Euler.jpg, [En ligne ; Consulté le 06-Août-2014].

Fig. 1, image de droite : « Christian Goldbach : Correspondance mathématique et physique de quelques célèbres géomètres du XVIII^{e} siècle (Vol. 1), St. Pétersbourg 1843, p. 125–129 ». Licence du domaine public via Wikimedia Commons, http://commons.wikimedia.org/wiki/File:Letter_Goldbach-Euler.jpg, [En ligne ; Consulté le 06-Août-2014].

Références

[1] L. E. Dickson, *History of the theory of numbers. Vol. I : Divisibility and primality.*, Chelsea Publishing Co., New York, 1966.

[2] H. A. Helfgott, *La conjecture de Goldbach ternaire*, Preprint. To appear in *Gaz. Math.*

[3] ———, *Major arcs for Goldbach's problem*, Preprint. Available as http://arxiv.org/abs/1305.2897.

[4] ———, *Minor arcs for Goldbach's problem*, Preprint. Available as http://arxiv.org/abs/1205.5252.

[5] ———, *The Ternary Goldbach Conjecture is true*, Preprint. Available as http://arxiv.org/abs/1312.7748.

[6] H. A. Helfgott et D. Platt, *Numerical verification of ternary Goldbach*, To appear in *Exp. Maths.* Available as `arXiv:1305.3062`.

[7] H.A. Helfgott, *La conjetura débil de Goldbach*, Gac. R. Soc. Mat. Esp. **16** (2013), n° 4.

[8] M. Ch. Liu et T. Wang, *On the Vinogradov bound in the three primes Goldbach conjecture*, Acta Arith. **105** (2002), n° 2, 133–175, http://dx.doi.org/10.4064/aa105-2-3.

[9] T. Oliveira e Silva, S. Herzog et S. Pardi, *Empirical verification of the even Goldbach conjecture, and computation of prime gaps, up to* $4 \cdot 10^{18}$, Accepted for publication in Math. Comp., 2013.

[10] I. M. Vinogradov, *Representation of an odd number as a sum of three primes*, Dokl. Akad. Nauk. SSR **15** (1937), 291–294.

Harald Helfgott *est chercheur à l'école Normale Supérieure de Paris, France.*

Traduit de l'anglais par
Judith Nataf

Sujets mathématiques
Algèbre et théorie des nombres

Liens avec d'autres domaines
Informatique

DOI
10.14760/SNAP-2014-003-FR

Les *Instantanés de recherche mathématique d'Oberwolfach* donnent un aperçu passionant de la recherche mathématique d'aujourd'hui. Ils ont été rédigés par des participants aux conférences de l'institut de recherche mathématique d'Oberwolfach (MFO). Ce projet d'instantanés est conçu pour promouvoir la compréhension et l'appréciation des mathématiques modernes et de la recherche en mathématique, et s'adresse au public intéressé du monde entier. Tous les instantanés sont publiés en collaboration avec la plateforme IMAGINARY et sont disponibles sur www.imaginary.org/fr/snapshots et sur www.mfo.de/snapshots.

ISSN 2626-1995

Mathematisches Forschungsinstitut
Oberwolfach gGmbH
Schwarzwaldstr. 9 – 11
77709 Oberwolfach
Allemagne

Mathematisches
Forschungsinstitut
Oberwolfach

Member of Leibniz
Leibniz Association

IMAGINARY
open mathematics