



HAL
open science

Sur les conjectures de Goldbach forte et faible (quelques remarques historico-épistémologiques)

Daniel Parrochia

► To cite this version:

Daniel Parrochia. Sur les conjectures de Goldbach forte et faible (quelques remarques historico-épistémologiques). 2023. <hal-04346907>

HAL Id: hal-04346907

<https://hal.science/hal-04346907v1>

Preprint submitted on 15 Dec 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons CC BY 4.0 - Attribution - International License

Sur les conjectures de Goldbach forte et faible (quelques remarques historico-épistémologiques)

Daniel Parrochia

Université de Lyon (France)

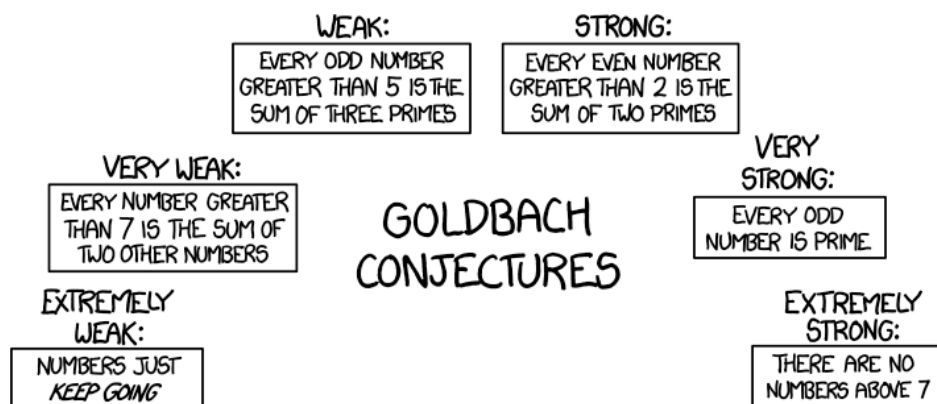


FIGURE 1 – xkcd - The Goldbach's conjectures

Résumé.

La manie anglo-saxonne de décomposer toute argumentation en versions fortes et faibles peut donner lieu à des plaisanteries comme celles qu'illustre le dessin de la Fig. 1 emprunté à la bande dessinée en ligne xkcd créée par Randall Munroe. Mais cet article est très sérieux. Nous rappelons d'abord quelques éléments d'histoire liés à la conjecture de Goldbach, notamment sa formulation exacte par Goldbach lui-même, puis par Euler. Nous développons ensuite les premières approches : en premier lieu l'approche combinatoire, partant du crible d'Eratosthène et allant jusqu'aux méthodes plus raffinées de Legendre et surtout de Brun, généralisée ensuite par Schnirelmann puis Ramaré, poursuivie enfin, depuis Vinogradov, par Mint-Chit Liu et

Wang Tianze ; en second lieu l'approche analytique, lancée par Euler, qui connut son heure de gloire à la fin du XIX^e siècle avec Hadamard et de La Vallée-Poussin, permettant notamment de démontrer le fameux "théorème des nombres premiers". Comme on le sait, la méthode passe par une formule qui égale un produit sur les nombres premiers à la fonction zêta de Riemann, somme définie à partir de simples entiers. La fonction zêta apparaissant au dénominateur, il faut alors, pour que la méthode fonctionne, éviter les points où celle-ci s'annule. D'où la chasse aux régions du plan complexe dépourvues de zéros, chasse lancée en 1849 par Riemann lui-même, dont les résultats restèrent au départ très partiels, mais dont l'irruption des ordinateurs a amplifié la portée à cause des vérifications possibles (voir les travaux de Pierre Dussart en 1998). Un affaiblissement de la question – la quête de régions du plan complexe où la fonction zêta a *peu* de zéros, inaugurée par Bohr et Landau – aboutit aux travaux de Gallagher et Vaughan, qui convertissent les renseignements sur les zéros en informations directes sur les nombres premiers, ce qui améliore la perspective. Finalement, dans les années 2010, les approches combinatoire et eulérienne vont converger dans les travaux de Christian Mauduit, Joël Rivat, et bientôt Terence Tao, ce dernier ayant réussi à montrer que tout entier pair est somme de 5 nombres premiers. Depuis, Harald Helfgott a été en mesure de descendre de 5 à 3 et de prouver la conjecture ternaire. Il reste que la conjecture initiale de Goldbach (la conjecture dite "binaire" ou conjecture "forte") résiste encore pour l'instant à toute démonstration.

Mots clés. Conjecture de Goldbach, conjecture de Legendre, théorème des nombres premiers, fonction zêta, Olivier Ramaré, Terence Tao, Harald Helfgott.

1 Introduction

Le 7 juin 1742, le mathématicien allemand Christian Goldbach (1690-1764), alors en Russie¹, écrit de Moscou une lettre à son éminent collègue Leonhard Euler (1707-1783), en Allemagne, où il propose la conjecture suivante :

Conjecture 1.1 (Goldbach). *Tout nombre strictement supérieur à 2 peut être écrit comme une somme de trois nombres premiers.*

1. Goldbach, fils d'un pasteur de Brandebourg (Prusse), avait fait des études de droit et de mathématiques à Königsberg, sa ville natale. Grand voyageur, polyglotte, il était capable d'écrire en allemand, latin, français, italien et russe. Installé en Russie depuis 1725, tuteur du futur empereur Pierre II dès 1728, il entre au Ministère des Affaires Etrangères de Russie précisément en 1742 (voir [Rosen 04]), l'année où il énonce sa fameuse conjecture.

La phrase exacte, écrite en allemand, énonce très exactement cette conjecture. Ce sont les derniers mots de la lettre, écrits verticalement dans la marge (voir Fig. 2), sachant que Goldbach admettait 1 comme nombre premier : « die unitatem mit dazu gerechnet ».

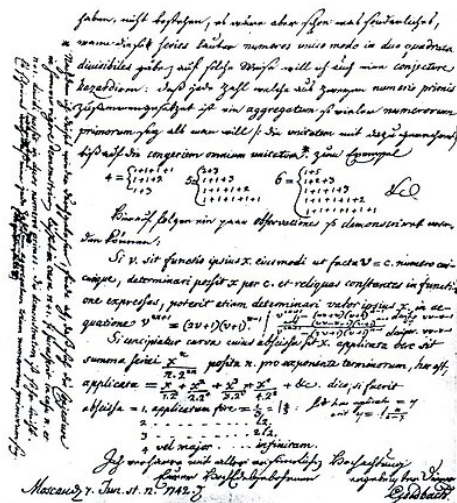


FIGURE 2 – La lettre de Goldbach à Euler, 7 juin 1742

Cet énoncé – aujourd’hui connu (si l’on remplace 2 par 7) comme la conjecture de Goldbach "faible" (ou ternaire, ou impaire) – ne surprend pas son correspondant. La lettre d’Euler, en provenance de Berlin et datée du 30 juin 1742 (voir [Euler Archive 42], 135), rappelle en effet à Goldbach que cet énoncé découle d’un énoncé antérieur que Goldbach lui a déjà communiqué et qui s’énonce ainsi :

Conjecture 1.2 (Euler (d’après Goldbach)). *Tout nombre pair peut être écrit comme somme de deux nombres premiers (jeder numerus par eine summa duorum numerorum primorum sey)*

Les deux conjectures, bien entendu, sont équivalentes : si tout nombre pair supérieur à 2 peut s’écrire comme somme de trois premiers, l’un d’entre eux est nécessairement 2, et ainsi, tout nombre pair supérieur à 0 peut s’écrire comme somme de deux premiers.

2 Un peu d'histoire

2.1 L'énoncé fondamental

La conjecture de Goldbach, dans sa formulation moderne (où le nombre 1 n'est plus désormais considéré comme premier), s'énonce ainsi :

Conjecture 2.1 (Formulation contemporaine : conjecture de Goldbach "forte" (ou "binaire")). *Tout nombre pair supérieur ou égal à 4 est la somme de deux nombres premiers.*

Cette formulation, différente de celle de Goldbach (voir [Euler 65]), mérite un commentaire. Rappelons qu'un nombre premier est un entier naturel qui admet exactement deux diviseurs distincts entiers et positifs. Ces deux diviseurs sont 1 et le nombre considéré, puisque tout nombre, composé ou non, a toujours pour diviseurs 1 et lui-même. Selon cette définition, les nombres 0 et 1 ne sont donc ni premiers ni composés : 1 n'est pas premier car il n'a qu'un seul diviseur entier positif et 0 non plus car il est divisible par tous les entiers positifs. Au cours de l'histoire, les mathématiciens ont cependant beaucoup varié dans leur conception de "1". Dans l'Antiquité, à de rares exceptions près – dont Speusippe (voir [Tarán 81], 70) –, "1" n'était même pas considéré comme un nombre² (et donc, a fortiori, il ne pouvait être un nombre premier). Il faut attendre Simon Stevin (1585) pour qu'il le devienne. Ensuite, pendant plusieurs siècles, les avis seront partagés quant à savoir s'il faut considérer "1" comme premier ou non. La raison en est que la factorisation, en ce temps-là, n'est pas un objet d'intérêt en tant que tel, le calcul d'un plus grand diviseur, celui des nombres parfaits³ ou amicaux⁴ étant le centre des préoccupations. D'où, selon Caldwell et Xiong (voir [Caldwell-Xiong], 3-5) la répartition à peu près égale des mathématiciens de l'époque : certains, dont L. Euler (1770) (voir [Euler Archive 42], 14-16) sont partisans d'exclure l'unité des nombres premiers. En revanche, comme il était aussi raisonnable de définir l'ensemble des nombres premiers (ou non composés) comme le complémentaire de l'ensemble des composés, d'autres mathématiciens,

2. Il ne l'est, en particulier, ni par Aristote, ni par Euclide, ni par Théon de Smyrne (voir [Smith 68], 20).

3. Rappelons qu'un nombre parfait est un nombre égal à la somme de ses diviseurs propres (un diviseur propre étant un diviseur autre que le nombre lui-même). Ainsi le premier nombre parfait est 6. En effet 1, 2 et 3 sont les diviseurs propres de 6 et $1+2+3=6$. Cette terminologie remonte au IX^e livre des *Eléments* d'Euclide et elle est reprise par Nicomaque de Gérase.

4. Deux nombres entiers strictement positifs sont dits amicaux (ou amiables ou aimables) s'ils sont distincts et si chacun des deux est égal à la somme des diviseurs stricts de l'autre. La notion de "nombre amical" est ainsi une généralisation de la notion de "nombre parfait", qui est, en quelque sorte, un nombre amical avec lui-même.

dont Ch. Goldbach (1742) (voir [Euler Archive 42]) (comme on peut le voir dans sa lettre à Euler) ou encore E. Waring (1782) (voir [Waring 82], 379) penchent en faveur de l'inclusion. Quoi qu'il en soit les mathématiciens ont fini par trancher. Pour les raisons qu'on a dites, "1" n'est plus aujourd'hui un nombre premier et la conjecture de Goldbach a dû être reformulée.

2.2 Variantes de la conjecture de Goldbach

Nous n'avons énoncé jusqu'ici que ce qu'on appelle désormais la conjecture "forte" de Goldbach, simple réécriture moderne de la conjecture initiale. Mais de nombreuses variantes ont été produites depuis.

Ainsi, la conjecture selon laquelle tous les nombres impairs supérieurs ou égaux à 9 sont la somme de trois nombres premiers (impairs) est appelée la conjecture "faible" de Goldbach.

Le mathématicien russe Ivan Vinogradov (1891-1983) (voir [Vinogradov 37¹]; ou encore [Vinogradov 37²]; [Vinogradov 54]) a prouvé que tout nombre impair suffisamment grand est la somme de trois nombres premiers, et Estermann (voir [Estermann 38]) a prouvé que presque tous les nombres pairs sont la somme de deux nombres premiers. La signification de l'expression "suffisamment grand", utilisée par Vinogradov, visait originellement un nombre N tel que :

$$N \geq 3^{3^{15}} \approx e^{e^{16,573}} \approx 3,25 \times 10^{6846168}.$$

Ce nombre a ensuite été réduit à $e^{e^{11,503}}$, soit environ $3,3310^{4300}$ par les mathématiciens chinois Chen Jingrun et Wang Yuan (voir [Chen-Wang 89]). Chen (voir [Chen 73], [Chen 78]) a également montré que tous les nombres pairs suffisamment grands sont la somme d'un nombre premier et du produit d'au plus deux nombres premiers. Enfin – nous y reviendrons plus loin –, on notera comme une avancée majeure que, plus de deux siècles et demi après l'énoncé de la conjecture originale, la conjecture "faible" de Goldbach ait été prouvée par le mathématicien péruvien Harald Andrés Helfgott (voir [Helfgott 13], [Helfgott 14¹]).

Une version plus forte de la conjecture "faible", à savoir que tout nombre impair supérieur ou égal à 7 peut être exprimé comme la somme d'un nombre premier et de deux fois un nombre premier, est connue sous le nom de "conjecture de Lemoine" ou, dans les pays anglosaxons, "conjecture de Levy". Elle s'exprime comme suit.

$$\forall n \in \mathbb{N} + 3, \exists p, q \in \mathcal{P} \mid 2n + 1 = p + 2q,$$

où \mathcal{P} désigne l'ensemble des nombres premiers,

Une autre affirmation, cette fois-ci directement équivalente à la conjecture de Goldbach, est que, pour tout entier positif n , il existe des nombres premiers p et q tels que :

$$\phi(p) + \phi(q) = 2n,$$

où $\phi(x)$ est la fonction totient d'Euler ⁵ (voir Fig.3), avec $\phi(p) = p-1$ pour p premier.) Erdős et Moser ont envisagé d'abandonner la restriction selon laquelle p et q soient premiers dans cette équation comme un moyen peut-être plus simple de déterminer si de tels nombres existent toujours (voir [Guy 94],105).

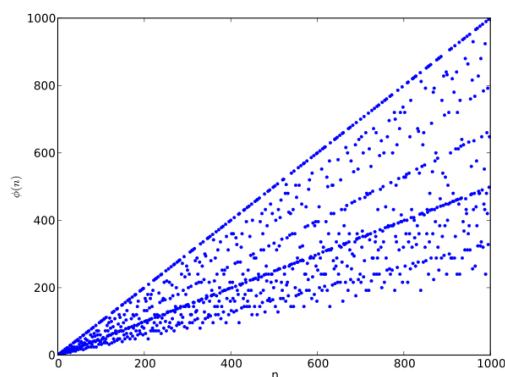


FIGURE 3 – La fonction "totient" (ou indicatrice d'Euler)

On connaît encore d'autres variantes de la conjecture de Goldbach ⁶, incluant notamment les affirmations selon lesquelles tout nombre pair supérieur ou égal à 6 est la somme de deux nombres premiers impairs, et tout nombre entier supérieur à 17 la somme d'exactly trois nombres premiers distincts.

Soit maintenant $R(n)$ le nombre de représentations d'un nombre pair n comme somme de deux nombres premiers. Alors la conjecture "étendue" de Goldbach déclare

5. La fonction totient d'Euler (autrement nommée "l'indicatrice d'Euler") est une fonction arithmétique de la théorie des nombres qui, à tout entier naturel n non nul, associe le nombre d'entiers compris entre 1 et n (inclus) et premiers avec n .

6. Il y a même une version due à Descartes, dans un manuscrit posthume, mais elle est anecdotique et peu claire. Cf. là-dessus le commentaire de Helfgott (voir [Helfgott 14³], 5), qui cite lui-même [Dickson 66]).

que

$$R(n) \sim 2\Pi_2 \prod_{\substack{k=2 \\ p_k | n}} \frac{p_{k-1}}{p_{k-2}} \int_2^n \frac{dx}{(\ln x)^2},$$

où Π_2 est la constante des nombres premiers jumeaux (voir [Halberstam-Richert])⁷.

2.3 Les vérifications expérimentales

Les différents essais de vérifications de la conjecture de Goldbach (forte) n'ont cessé de progresser depuis le XIX^e siècle, l'ordinateur, à partir des années 1960, permettant d'atteindre des limites inégalées. Nous récapitulons les différents résultats dans la table suivante :

Limite	Référence
1×10^4	Desboves 1885
1×10^5	Pipping 1938
1×10^8	Stein and Stein 1965
2×10^{10}	Granville et al. 1989
4×10^{11}	Sinisalo 1993
1×10^{14}	Deshouillers et al. 1998
4×10^{14}	Richstein 1999, 2001
2×10^{16}	Oliveira e Silva (Mar. 24, 2003)
6×10^{16}	Oliveira e Silva (Oct. 3, 2003)
2×10^{17}	Oliveira e Silva (Feb. 5, 2005)
3×10^{17}	Oliveira e Silva (Dec. 30, 2005)
12×10^{17}	Oliveira e Silva (Juil. 14, 2008)
4×10^{18}	Oliveira e Silva (Avr. 2012)

TABLE 1 – Vérifications de la validité de la conjecture de Goldbach

7. Deux nombres premiers sont dits "jumeaux" lorsqu'ils sont séparés de deux unités. Ainsi les paires 3 et 5, 17 et 19 ou encore 41 et 43, 71 et 73, pour s'en tenir aux jumeaux inférieurs à 100. Mais certains peuvent être très grands : par exemple, $2003663613 \cdot 2^{195000} - 1$ et $2003663613 \cdot 2^{195000+1}$ sont encore des nombres premiers jumeaux. Brun attribue l'origine de cette idée de gémellité numérique au mathématicien allemand Paul Gustav Stäckel (1862-1919), qui l'aurait introduite dans un article de 1816 (voir [Stäckel 16]). Toutefois, nous n'avons pas trouvé l'expression "Zwillingsprimzahlen" dans cet article, et l'équivalent anglais "twin primes" n'apparaît qu'en 1930, dans la 1ère édition de *Number, the language of science*, le célèbre livre de Tobias Dantzig. L'origine des expressions "nombres premiers cousins" et "nombres premiers sexy" qui désignent respectivement les couples $(p, p + 4)$ et $(p, p + 6)$ n'est pas connue.

Aucun contre-exemple n'ayant été trouvé jusqu'à 4×10^{18} , la conjecture forte de Goldbach a toutes les chances d'être vraie, mais encore faut-il le prouver, ce qui est une autre affaire.

3 Les premières approches

3.1 La voie combinatoire

La méthode combinatoire, qui prend sa source dans l'Antiquité, utilise la notion de "crible"⁸. Un crible est une sorte de tamis qui laisse passer certains éléments et en retient d'autres. Eratosthène⁹ a été le premier à utiliser cet instrument en mathématiques pour déterminer la suite des nombres premiers. Son tableau supprime d'une table d'entiers de 2 à N tous les multiples d'un entier (autres que lui-même). Il ne reste plus alors que les entiers qui ne sont multiples d'aucun entier à part 1 et eux-mêmes, et qui sont donc les nombres premiers. On élimine successivement les multiples de 2, puis les multiples de 3 restants, puis les multiples de 5 restants, et ainsi de suite en rayant à chaque fois tous les multiples du plus petit entier restant. On s'arrête lorsque le carré du plus petit entier restant est supérieur au plus grand entier restant, car dans ce cas, tous les nombres non-premiers ont déjà été rayés précédemment. À la fin du processus, tous les entiers qui n'ont pas été rayés sont les nombres premiers inférieurs à N (voir Fig. 4).

En d'autres termes, Ératosthène remarque qu'un nombre est premier s'il n'est divisible par aucun entier inférieur ou égal à sa racine carrée. Il aboutit ainsi à l'algorithme efficace qu'on a décrit, qui déduit la liste des nombres premiers inférieurs ou égaux à x de ceux qui sont inférieurs ou égaux à la racine carrée de x .

Cette propriété peut s'exprimer sous une forme un peu plus mathématique :

Théorème 3.1. *Lors du tamisage de la séquence d'entiers consécutifs allant de 1 à x par les nombres premiers p_1, p_2, \dots, p_r , où $p_r \leq \sqrt{x}$, il suffit de considérer les multiples des nombres premiers inférieurs ou égaux à \sqrt{x} .*

Démonstration. Raisonnons par l'absurde. Supposons que, pour retenir dans le crible tous les nombres composés de 1 à x , nous devions considérer un nombre premier

8. Du latin *cribrum* devenu, par dissimilation, en bas-latin, *criblum*, ou de l'arabe *gharbala*, dont dérivent grabeler et le moyen français *grabel* ("crible").

9. Eratosthène de Cyrène (276-194 avant J.-C.), géographe, philosophe et mathématicien grec, est à l'origine du crible qui porte son nom.

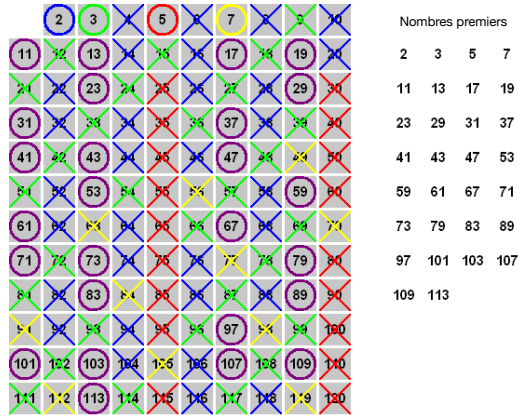


FIGURE 4 – Le crible d’Eratosthène

supérieur à \sqrt{x} . Cela signifierait qu’il existe un nombre composé $c \leq x$ qui n’a pas été retenu dans le tamis lors du criblage par les nombres premiers p_1, p_2, \dots, p_r . Cela voudrait donc dire que c n’est un multiple d’aucun des nombres premiers p_1, p_2, \dots, p_r , car si c’était le cas, il serait retenu dans le tamis. Ainsi, chacun des facteurs premiers de c doit être supérieur à p_r et donc supérieur à \sqrt{x} . Mais cela voudrait dire que c lui-même serait supérieur à x , contredisant l’hypothèse selon laquelle $c \leq x$. Par conséquent, la supposition est fausse et le théorème 3.1 établi. \square

3.1.1 Adrien-Marie Legendre et Viggo Brun

Les recherches de Legendre Un autre mathématicien, le Français Adrien-Marie Legendre a, lui aussi, fait usage de cribles en théorie des nombres, dans le cas d’une recherche sur les nombres premiers.

Sous le nom de "conjecture de Legendre", on lui attribue en effet l’énoncé selon lequel on peut toujours trouver un nombre premier entre deux carrés. En réalité, on ne trouve pas cette affirmation, en tout cas sous cette forme, dans les écrits de Legendre. En revanche, dans la quatrième partie de son *Essai sur la théorie des nombres* (voir [Legendre 08], 399-401), au paragraphe 9, qui propose la "démonstration de divers théorèmes sur les progressions arithmétiques", le mathématicien croit démontrer un théorème dont l’une des conséquences est bien cette affirmation. Dans ce passage, en effet, Legendre se propose de montrer que toute progression arithmétique dont le premier terme et la raison sont premiers entre eux contient une infinité de nombres premiers et, subsidiairement, de trouver des limites qui comprennent nécessairement

des nombres premiers. La solution de ces deux problèmes, et notamment du deuxième, s'appuie sur une proposition dont Legendre croyait avoir fourni la preuve, mais à laquelle il n'était parvenu, comme l'ont bien vu certains mathématiciens contemporains (Lejeune-Dirichlet par exemple, que par une "heureuse induction". En tout cas, l'une des conséquences les plus générales de son théorème était que, une limite L étant fixée, on devait toujours pouvoir trouver un nombre premier entre L et $L + 2\sqrt{L}$. Il est alors facile de voir qu'en posant $L = a^2$, $L + 2\sqrt{L}$ devient le début d'un carré qu'on peut majorer par $(a + 1)^2$. L'ensemble donne alors effectivement la "conjecture de Legendre".

Le lien entre cette conjecture et la conjecture de Goldbach n'est cependant pas direct. Il faut avant tout se souvenir que les nombres premiers peuvent prendre différentes formes. On a d'abord le théorème suivant, énoncé par Legendre dès l'introduction de son *Essai sur la théorie des Nombres* (voir [Legendre 08], §19, 11)

Théorème 3.2. *Tout nombre premier p supérieur à 3 est tel que $p = 6k \pm 1$.*

Démonstration. Soit $q = 2n + 1$ un nombre impair, avec $n \geq 3$. La division de q par 6 donne un reste qui ne peut être que l'un des nombres 1, 3, 5. Donc, tout nombre impair q est tel que $q = 6k + 1$ ou $q = 6k + 3$ ou encore $q = 6k + 5$. Mais la deuxième formule, divisible par 3, ne peut convenir à un nombre premier p . Quant à la troisième, elle contient les mêmes nombres que $6k - 1$. Donc, tout nombre premier p supérieur à 3 est de la forme :

$$p = 6k \pm 1.$$

□

Mais Legendre a montré également à la suite (voir [Legendre 08], §22) que, tout nombre impair se présentant sous la forme $2n + 1$, laquelle se subdivise, selon que n est lui-même pair ou impair, en les formes $4n + 1$ et $4n - 1$ ou $4n + 3$, deux grandes divisions des nombres premiers se font jour :

- L'une comprenant les nombres premiers de type $4n + 1$, à savoir : 1, 5, 13, 17, 29, 37, 41, 53, 61, 73, etc.
- L'autre comprenant les nombres premiers de type $4n - 1$ ou $4n + 3$, à savoir : 3, 7, 11, 19, 23, 31, 43, 47, 59, etc.

La conjecture de Goldbach peut donc se préciser de la façon suivante : tout nombre pair supérieur à 4 est la somme de deux nombres premiers au moins de deux manières.

En particulier, lorsque le nombre pair est double d'un nombre impair, il est toujours simultanément la somme de deux nombres premiers de la forme $4n + 1$ et la somme de deux nombres premiers de la forme $4n - 1$.

Il est alors facile de voir que la première partie de la conjecture suppose qu'entre un nombre plus grand que 6 et son double, il y a toujours au moins deux nombres premiers, énoncé qui est vrai à partir du nombre 14, même en ne comptant pas la décomposition en deux nombres premiers égaux.

Par ailleurs, sachant, comme l'a rapporté Legendre, que tout nombre premier de la forme $4n + 1$ est la somme de deux carrés (résultat de Fermat redémontré par Euler), on peut en conclure qu'un nombre quelconque est toujours la somme de quatre carrés ou d'un nombre moindre de carrés.

Le bénéfice de la méthode de Legendre est ainsi de faire apparaître que la conjecture de Goldbach est liée à divers autres théorèmes de théorie des nombres.

La percée de Viggo Brun Aucune avancée majeure sur la conjecture de Goldbach n'intervint avant le début du XX^e siècle. En raison de difficultés de nature probabiliste, nul n'arriva à poursuivre les travaux de Legendre. Il fallut attendre 1915 pour que le mathématicien norvégien Viggo Brun (1885-1978) comprenne comment faire. L'apport principal de Brun se mesure à trois avancées majeures.

1) En premier lieu, utilisant des travaux de Jean Merlin¹⁰, Brun modifie le crible d'Eratosthène-Legendre en le transformant en un double crible. Cette démarche permet d'apporter des résultats sur les paires de nombres dont la somme est un nombre pair, et aussi de réduire la taille du plus grand nombre premier utilisé pour le criblage, avec pour résultat que certains nombres (ceux ayant au plus neuf facteurs premiers) tombent dans son champ d'application.

Des essais numériques font qu'on estime généralement que le nombre de représentations d'un nombre croît avec le nombre lui-même. D'où des images bien connues comme celle des partitions d'entiers de 4 à 50 ou celle de la fameuse "comète de Goldbach" quand on poursuit les décompositions par ordinateur jusqu'à des valeurs numériques élevées¹¹.

10. Jean Merlin (1876-1914), mathématicien français normalien, spécialisé en théorie des nombres, mais envoyé au front et mort au début de la grande guerre, n'a pas eu le temps d'écrire. Mais Jacques Hadamard a pu présenter devant la société de mathématique la méthode qu'il envisageait d'utiliser en vue de démontrer le théorème de Goldbach (voir [Hadamard 15]).

11. Dans la Fig. 5, On lit par exemple qu'un nombre pair de l'ordre de 1 million (la notation $1e+06$ signifie 1×10^6) a un nombre de représentations au moins supérieur à 2000.

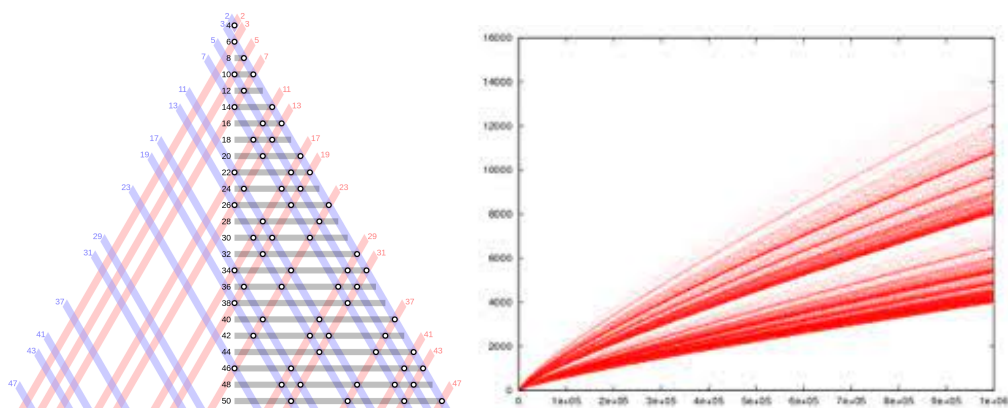


FIGURE 5 – Décomposition des pairs et comète de Goldbach

2) Brun a ensuite fait et exploité un certain nombre d'observations concernant les calculs de composants utilisés dans le crible d'Eratosthène-Legendre, cela afin de développer diverses estimations de la limite inférieure de la quantité de nombres susceptibles de survivre à ce processus de tri.

3) Enfin, il a utilisé certaines approximations asymptotiques (comme, par exemple, celles données par les formules de Mertens et Stirling) pour montrer qu'une des estimations améliorées de la limite inférieure permettait d'établir un résultat concernant la conjecture de Goldbach.

La démarche de Brun, exposée notamment dans [Brun 15] et [Brun 20] a été plusieurs fois commentée (voir notamment [Teissier 65-66] et surtout [Farrugia 18]), sans être pour autant très éclairée, les quarante pages assez denses de son article principal étant relativement indigestes. On considère aujourd'hui la question comme un cas particulier d'une fonction importante en théorie des nombres, la fonction "nombre

de facteurs premiers distincts", notée ω ¹².

Brun part du crible d'Eratosthène qui stipule, comme on l'a vu, qu'on peut déterminer des nombres premiers p tels que $\sqrt{a} < p \leq a$, connaissant les nombres premiers $2 \leq p \leq \sqrt{a}$.

En écriture mathématique moderne (voir [Goudout 16]), pour calculer le nombre de nombres premiers inférieurs à x , on pose, pour $z = 0$:

$$P_z = \prod_{\substack{p \leq z \\ p \text{ premier}}} p,$$

et on a alors, pour $x \geq 1$:

$$\pi(x) - \pi(\sqrt{x}) + 1 = \#\{1 \leq n \leq x \mid \text{pgcd}(n, P_{\sqrt{x}}) = 1\}.$$

Pour calculer le cardinal de cet ensemble, il suffit alors d'estimer la taille du complémentaire en utilisant la formule du crible pour une union d'ensembles. Par exemple, pour savoir combien d'entiers inférieurs à x sont divisibles par 2 ou 3, il faut compter les entiers pairs (il y en a $\lfloor \frac{x}{2} \rfloor$) et les entiers divisibles par 3 ($\lfloor \frac{x}{3} \rfloor$), mais en enlevant les entiers divisibles par 2 et par 3, comptés 2 fois ($\lfloor \frac{x}{6} \rfloor$). On aboutit alors à la formule suivante :

$$\pi(x) - \pi(\sqrt{x}) + 1 = \sum_{d \mid P_{\sqrt{x}}} \mu(d) \lfloor \frac{x}{d} \rfloor. \quad (1)$$

où μ est la fonction de Möbius, à support sur les entiers sans facteur carré et valant -1 puissance le nombre de facteurs premiers.

On obtient alors une majoration grâce à la formule :

$$\delta \leq 1 * \mu_{2\ell}$$

où $*$ désigne la convolution classique entre fonctions multiplicatives¹³, δ la fonction

12. Comme le montre Elie Goudout dans sa thèse (voir [Goudout 19]), on sait depuis Euclide qu'il existe une infinité de nombres premiers, et donc que $\{\omega(n) : n \geq 1\} = \mathbb{N}$. Il devient alors naturel d'étudier la structure des ensembles \mathcal{E}_k , définis pour $k > 0$ par :

$$\mathcal{E}_k := \{n \geq 1 : \omega(n) = k\}.$$

Se posent alors différentes questions, dont celle à laquelle Brun répond, à savoir, dans quelle mesure une structure multiplicative de n donne des informations sur celle de $n + 1$, et qui est aujourd'hui considérée comme un cas particulier de l'étude des systèmes translés en théorie des nombres.

13. Pour f et g deux fonctions définies sur \mathbb{N}^* et $n \geq 1$, on pose $(f * g)(n) = \sum_{d \mid n} f(d)g(n/d)$.

indicatrice de $\{1\}$ et $\mu_{2\ell}$ la fonction μ tronquée aux entiers avec au moins 2ℓ facteurs premiers.

Avec cette méthode, en optimisant le paramètre z introduit précédemment et l'étape 2ℓ à laquelle on s'arrête de cribler, on obtient assez facilement :

$$\pi(x) \ll \frac{x \log \log x}{\log x}.$$

La méthode de Brun peut alors s'attaquer à une vaste catégorie de problèmes. On peut, en particulier, s'intéresser aux ensembles du type :

$$\{n \in \mathcal{A} \mid \text{pgcd}(n, P_z) = 1\},$$

où \mathcal{A} peut être un ensemble plus général, et non pas forcément $[1, x]$, puisqu'on sait désormais estimer $\mathcal{A}_d := \{n \in \mathcal{A} \mid d \mid n\}$. Et par exemple, en prenant $\mathcal{A} = \{n(n+2) \mid n \leq x\}$, Brun démontre en 2019 le théorème suivant :

Théorème 3.3. $\#\{p \leq x \mid p \text{ et } p+2 \text{ sont premiers}\} \ll \frac{x(\log \log x)^2}{(\log x)^2}$.

On ne peut malheureusement déduire de ce théorème qu'il existe une infinité de nombres premiers jumeaux. En revanche, Brun parvient à montrer qu'il existe une infinité d'entiers n tels que $n(n+2)$ ait moins de 9 facteurs premiers. En d'autres termes, la conjecture de Goldbach est majorée par le théorème : "tout nombre pair est la somme de 9 nombres premiers". Les approches successives qui suivront se borneront à abaisser l'estimation de cette somme.

3.1.2 La suite de l'approche combinatoire

Olivier Ramaré (voir [Ramaré 13]) a pu résumer l'apport essentiel de Brun à la démonstration plus spécifique de la conjecture de Goldbach de la façon suivante. Si on note $R_2(N)$, le nombre de façons d'écrire l'entier N comme somme de deux nombres premiers, Brun est en fait parvenu à montrer, à l'aide de son crible, que, à un terme correctif près, $R_2(N)$ était inférieur à $8r\#_2(N)$, où $r\#_2$ est la fonction asymptotique conjecturée pour $R_2(N)$ si N est grand (on note l'inégalité $R_2(N) < 8 R\#_2(N)$). Et $R\#_2(N)$ a une expression simple et connue. En d'autres termes, on majore le nombre de manières d'écrire la somme de 2 nombres premiers avec seulement un facteur multiplicatif constant. D'un autre point de vue, cette majoration signifie que, si on prend entre 1 et N toutes les sommes de deux nombres premiers, certains entiers ne sont pas plus représentés que d'autres : la distribution de ces sommes est bien répartie.

De Šchnirel'man à Linnik Une telle révolution dans la façon de voir les choses a eu rapidement des applications : ainsi le Russe Lev Genrikhovich Šchnirel'man a démontré en 1933 l'existence d'une constante C_s telle que tout entier supérieur ou égal à 2 est la somme d'au plus C_s nombres premiers. Toutefois, il n'a pas calculé cette fameuse constante C_s ¹⁴.

Le mathématicien russe Youri Vladimirovitch Linnik (1915-1972), né en Ukraine, comme beaucoup d'autres¹⁵, devait poursuivre à sa manière la voie de Šchnirel'man. Dans un article de 1941, il introduisit la méthode dite "du grand crible" en théorie des nombres. Par "grand crible", terme utilisé par Linnik lui-même, il entendait l'opération d'élimination de certaines classes de résidus modulo p à partir d'un ensemble donné d'entiers où p a augmenté, tout comme peut-être le nombre de classes. Sa motivation pour introduire cette méthode était d'attaquer l'hypothèse de Vinogradov concernant la taille du plus petit non-résidu quadratique. L'hypothèse du mathématicien russe Yvan Vinogradov (1891-1983) concernait la taille du plus petit non-résidu quadratique n_p modulo p . Vinogradov avait conjecturé que n_p était $O(p^e)$ pour tout $e > 0$. Linnik, en utilisant sa méthode du grand crible, a pu montrer que le nombre de nombres premiers $p < x$ pour lequel $n_p > p^e$ est $O(\ln \ln x)$. La méthode du grand crible de Linnik s'est avérée très importante et a été développée ensuite par beaucoup d'autres mathématiciens..

Le résultat de Ramaré C'est cette méthode inaugurée par Brun et poursuivie par Šchnirel'man que Ramaré a suivie pour établir, en 1995, que tout entier pair est somme d'au plus 6 nombres premiers (voir [Ramaré 95]).

À partir d'une inégalité de type $R_2(N) < 8 R_{\#_2}(N)$, Ramaré trouve une interprétation géométrique du terme de droite et introduit le concept de "suite enveloppante", suite 8 fois plus grande que la première et qui "enveloppe" donc celle-ci. Les écritures de l'entier N se présentent alors sous la forme $N = a + p$, avec a dans la nouvelle suite (et p premier). Améliorant la construction, Ramaré obtient la formule de l'in-

14. Selon Dunham (voir [Dunham 90], 83), Šchnirel'man aurait montré par la suite (voir [Šchnirel'man 39]) que tout nombre pair peut être écrit comme la somme d'au plus 300.000 nombres premiers. Nous n'avons malheureusement pas retrouvé ce nombre, ni aucun autre, dans l'article de Šchnirel'man (en russe) ci-dessus mentionné. Cette indication (comme d'autres que l'on trouve ailleurs) semble une pure invention.

15. Le site internet <https://mathshistory.st-andrews.ac.uk/Countries/Ukraine/> donne la liste des mathématiciens nés en Ukraine, parmi lesquels, on trouvera, outre Linnik, Arnold, Besicovitch, Drinfeld, Gelfand, Kac, Lifshitz, Lukasiewicz, Mazur, Ostrogradski, Pfeiffer, Sheffer, Ulam, Voronoï... qui ont contribué au progrès de la mathématique mondiale, et d'abord russe, ce qui mériterait d'être rappelé aux plus oubliés des hommes politiques.

égalité pour "presque tous" les entiers N , ce qui lui a permis, après quelques étapes techniques, de démontrer son résultat.

L'intérêt des suites enveloppantes étant qu'on peut les manipuler et travailler avec, on sait comment leurs termes sont distribués. Si le crible permet une majoration de la suite des nombres premiers, la question se pose alors de savoir si l'on peut comprendre ce qui se passe entre la majoration et la vraie suite. En 1937, Vinogradov avait tenté de répondre à cette question en substituant à la suite des nombres premiers une fonction caractéristique $1|P$ qui associe 1 à chaque nombre premier et 0 aux autres entiers. En simplifiant un peu, on peut dire également qu'il s'agit de considérer de façon similaire la fonction $1|A$, fonction caractéristique de la suite A enveloppante définie plus haut. La question posée devient alors de comprendre une certaine fonction g définie par $1|P = 1|A + g$. C'est cette fonction g qui permet de dire ce qui se passe entre la majoration et la vraie suite. Le mieux est de laisser la parole à Olivier Ramaré :

"La fonction $1|A$ peut s'écrire comme une somme sur les diviseurs d de n d'une suite de coefficients I_d qui dépendent de d . Et I_d devient nul dès que d est grand. Du coup, on peut facilement majorer $1|A$, car le nombre de coefficients non nuls reste petit. Peut-on faire de même pour g ? La réponse est non, mais Vinogradov remarque que l'on peut tout de même écrire g sous une forme dite bilinéaire qui simplifie les choses. Il écrit $g(n)$ comme la somme d'un produit de coefficients al et bm tels que n est le produit de m et de l , qui ne peuvent être ni trop petits ni trop grands... Cette observation débloque la situation, et Vinogradov montre en 1937 que tout entier impair assez grand est somme de 3 nombres premiers. L'énoncé est précisé en 2002 par Mint-Chit Liu, de l'université de Hong Kong, et Wang Tianze, de l'université du Henan : tout impair supérieur ou égal à 10^{1350} est bien somme de trois nombres premiers. Pour démontrer la conjecture de Goldbach ternaire, il ne reste alors plus qu'un nombre fini de cas à vérifier ! Mais la vérification est impossible, car même avec tous les ordinateurs de la Terre, il faudrait des milliards de fois l'âge de l'Univers pour tester tous les nombres impairs plus petits que 10^{1350} " (voir [Ramaré 13]).

3.2 La voie analytique

La méthode analytique a débuté avec l'approche eulérienne du problème, liée à l'histoire de la fonction ζ .

3.2.1 Vers la fonction ζ

Rappelons qu'en 1644, Pietro Mengoli (1626-7?-1686), mathématicien italien élève de Cavalieri, pose une question qui va mener tout droit à la découverte de la fonction ζ : combien vaut la somme de la série numérique :

$$\sum_{n=1}^{\infty} \frac{1}{n^2}.$$

À l'époque, ni Leibniz, ni les Bernoulli, ni James Stirling ne réussissent à sommer cette série. Mais Leonhard Euler, en 1731, en calcule la somme à 10^{-6} près, conjecture, à partir de là, en 1735, qu'elle vaut $\pi^2/6$, et obtient finalement la première justification rigoureuse de la formule en 1743, énonçant explicitement :

Les travaux d'Euler

Théorème 3.4. $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$.

Ne s'arrêtant pas à ce résultat, il poursuit sa recherche et, utilisant les nombres B_{2k} , appelés depuis nombres de Bernoulli, il trouve finalement la formule générale

$$\sum_{n=1}^{\infty} \frac{1}{n^{2k}} = \frac{|B_{2k}| 2^{2k-1} \pi^{2k}}{(2k)!}, \quad (2)$$

les B_j étant définis par l'identité formelle :

$$\frac{t}{e^t - 1} = \sum_{j \geq 0} B_j \frac{t^j}{j!}.$$

Euler introduit du même coup la fonction zêta, notée ζ , sur les réels supérieurs à 1 par :

$$\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}, \quad (3)$$

le théorème 3.4 correspondant simplement à $\zeta(2)$.

À l'aide de manipulations de séries divergentes, il réussit également à définir et à calculer la valeur de $\zeta(k)$ pour les entiers k négatifs et trouve ainsi une forme particulière de ce qui sera la relation fonctionnelle de la fonction zêta :

$$\zeta(1 - k) = 2(2\pi)^{-k} \cos(\pi k/2) \Gamma(s) \zeta(k).$$

Il ne réussira cependant pas à calculer $\zeta(2k + 1)$ mais trouvera la curieuse formule suivante, qui fait le lien avec la théorie des nombres premiers, et qu'on appelle depuis un produit eulérien :

$$\zeta(k) = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{1}{p^k}}, \quad (4)$$

où le produit infini est effectué sur l'ensemble \mathcal{P} des entiers premiers p .

Par conséquent, était ainsi révélé un lien, inconnu jusque-là, entre les nombres premiers et la fonction ζ .

L'inégalité de Tchebychev Parmi les mathématiciens ayant anticipé le théorème des nombres premiers, on peut mentionner, dans l'école eulérienne, Panoufti Tchebychev (1821-1894) qui, à côté de travaux en probabilités et statistiques, a travaillé aussi en théorie des nombres et obtenu des résultats sur la conjecture de Gauss-Legendre (1792-1797). $\pi(n)$ étant le nombre de nombres premiers inférieurs à n , Gauss et Legendre avaient conjecturé que la fonction $\pi(n)$ était asymptotiquement équivalente à $\frac{n}{\ln n}$ quand n tend vers l'infini. Tchebychev renforça la plausibilité de cette conjecture en prouvant, d'une part que la fonction $\pi(n)$ était asymptotiquement de l'ordre de $\frac{n}{\ln n}$, d'autre part que si la suite de terme général $\frac{\pi(n) \ln n}{n}$ était convergente, alors sa limite devait être 1. Concernant le premier résultat il démontrait, plus précisément que, pour tout x suffisamment grand, on a

$$a < \frac{\pi(x) \ln x}{x} < \frac{6}{5}a,$$

où la constante a vaut 0,92129... Comme $7/8 < a$ et $9/8 > 6,5a$, on rend cette inégalité plus parlante en augmentant légèrement l'intervalle et en posant (voir [Rubinstein-Sarnak 94]) :

$$\frac{7}{8} < \frac{\pi(x) \ln x}{x} < \frac{9}{8}.$$

Les travaux de Riemann On doit ensuite à Bernhard Riemann (1826-1866) une avancée capitale. Le passage de $\zeta(k)$ à $\zeta(s)$; autrement dit l'étude de la fonction zêta comme fonction d'une variable complexe. Une fois remplacé k par s , la série (3) définit d'abord une fonction analytique de la variable s dans le demi-plan $\sigma > 1$ (en posant, ici $\sigma = \Re s$ et $\tau = \Im s$). Une fois changé k en s dans l'identité eulérienne, cette fonction

vérifie (4), ce qui prouve notamment que $\zeta(s)$ ne s'annule pas dans ce demi-plan. En utilisant des techniques très récentes d'analyse complexe (notamment le théorème des résidus) et harmonique (l'inversion de Fourier), Riemann obtient alors à partir de là un ensemble impressionnant de résultats, dont la formule suivante :

$$\frac{T}{2\pi} \ln \frac{T}{2\pi} - \frac{T}{2\pi} + O(\ln T)$$

donnant le nombre de zéros de la fonction $\zeta(s)$ dans le rectangle $[0, 1] \times [0, iT]$. Il explicite ensuite le lien entre la fonction $\pi(x)$ et la fonction $\zeta(s)$, qui s'exprime par la formule suivante :

$$\ln \zeta(s) = s \int_2^\infty \frac{\pi(x)}{x(x^s - 1)} dx,$$

(avec $\sigma > 1$) qu'il s'agira d'inverser pour obtenir le théorème des nombres premiers.

3.2.2 Le théorème des nombres premiers

Justement, l'approche eulérienne-riemannienne a certainement connu son heure de gloire en 1896, lorsque le Français Jacques Hadamard et le Belge Charles-Jean de La Vallée-Poussin ont démontré indépendamment, mais grâce à cette approche, ce fameux théorème des nombres premiers, qui s'énonce ainsi :

Théorème 3.5. *La fonction π qui à un réel x associe $\pi(x)$, le nombre de nombres premiers inférieurs ou égaux à x , est équivalente, lorsque x tend vers $+\infty$, au quotient de x par son logarithme népérien. On a :*

$$\pi(x) \underset{x \rightarrow \infty}{\sim} \frac{x}{\ln(x)},$$

c'est-à-dire :

$$\lim_{x \rightarrow +\infty} \pi(x) \frac{\ln(x)}{x} = 1.$$

Ce théorème des nombres premiers, version analytique du théorème fondamental de l'arithmétique, est donc équivalent, en un certain sens, à l'assertion selon laquelle la fonction zêta de Riemann ne s'annule pas sur l'abscisse de partie réelle 1. Dans ses grandes lignes, la démonstration, qui passe par cette formule égalant la fonction zêta de Riemann, somme définie à partir de simples entiers, à un produit sur les nombres premiers, relie ainsi un calcul sur des entiers à un calcul sur des nombres premiers. On dispose alors d'une voie potentielle pour déduire des propriétés des nombres premiers de celles des entiers.

Comme la formule utilisée comprend la fonction zêta au dénominateur, il faut cependant, pour que la méthode fonctionne, éviter les points où celle-ci s'annule : ses "zéros".

La chasse aux zéros La chasse aux régions du plan complexe, où est définie la fonction zêta et où elle ne s'annule pas, avait été lancée dès 1849 par Bernhard Riemann lui-même. Les résultats restaient malheureusement très partiels, tant et si bien que cette méthode ne permettait d'étudier, en l'état des connaissances, que des sommes de fonctions sur des nombres premiers qui ne dépendaient pas vraiment de ceux-ci, mais uniquement de la classe modulo n d'un petit entier¹⁶. L'irruption des ordinateurs a transfiguré cette méthode et en a amplifié la portée, puisqu'on peut vérifier maintenant numériquement que de larges régions du plan complexe ne contiennent aucun zéro.

Les calculs de Dusart Par exemple, en 1998, en utilisant de tels calculs informatiques, Pierre Dusart, de l'université de Limoges, a montré que le nombre $\pi(x)$ de nombre premiers inférieurs ou égaux à x est supérieur ou égal à $\frac{x}{\ln x - 1}$ dès que x est supérieur ou égal à 5293 (voir [Dusart 98], 36). C'est une sorte d'amélioration du théorème des nombres premiers. De plus, c'est un résultat exact, vrai dès que x a atteint cette valeur alors que le théorème des nombres premiers était un résultat asymptotique, valide seulement lorsque x tendait vers l'infini.

4 Convergence des méthodes

La chasse aux régions du plan complexe ne comportant aucun zéros de la fonction zêta, inaugurée par Riemann et poursuivie avec l'aide de l'informatique, avait connu une inflexion – disons même un affaiblissement – au début du XX^e siècle, plus précisément dès le milieu des années 1910.

En effet, plutôt que de déterminer des régions où la fonction zêta ne s'annulait pas, en 1914, le Danois Harald Bohr (1887-1951)¹⁷ et l'Allemand Edmund Landau (1877-1938)¹⁸ relaxèrent la demande et essayèrent plutôt de chercher des régions où la

16. Rappelons que la classe modulo n d'un entier est le reste de la division de celui-ci par n .

17. Harald Bohr, mathématicien danois, spécialiste de théorie des nombres, était le frère de Niels Bohr. Anecdotiquement, c'était un grand footballeur qui avait obtenu, avec l'équipe nationale danoise, la médaille d'argent aux Jeux Olympiques de 1908.

18. Mathématicien allemand spécialisé en théorie des nombres, titulaire d'une chaire à l'université de Göttingen dont il fut exclu par le régime nazi en 1933 du fait qu'il était juif. Lui, n'était pas le

fonction zêta avait *peu* de zéros. Ce changement d'approche allait se révéler essentiel et permettre de démontrer plusieurs théorèmes.

4.1 Les travaux de Gallagher et Vaughan

Il fallut cependant attendre 1968 pour que Patrick Gallagher (1935-2019) de l'université Columbia, aux États-Unis, remarque que le procédé utilisé pour démontrer les conjectures du type de celle de Goldbach était anormalement complexe. On partait habituellement de la fonction zêta, on en tirait des renseignements sur les zéros de cette fonction et on convertissait celle-ci en information sur les nombres premiers. Pourquoi ne pas sauter l'étape qui s'occupait des zéros ? Gallagher y parvint en écrivant un développement du rapport entre la dérivée de la fonction zêta et la fonction zêta elle-même qu'il arriva à traiter. Il redémontra ainsi les théorèmes les plus difficile du domaine de façon directe (voir [Gallagher 71];[Gallagher 73]).

Robert Vaughan (né en 1945), enseignant à l'université d'État de Pennsylvanie, parachèvera, quant à lui, en 1977 (voir [Vaughan 77]), ce changement de perspective, en transposant cette façon de faire au niveau de la fonction caractéristique des nombres premiers $1|P$.

4.2 L'approche de Vinogradov

C'est à ce moment précis que les approches combinatoire et eulérienne se sont mises à converger. Voici la nouvelle méthodologie qui s'en dégage : il s'agit désormais d'écrire la fonction $1|P$ comme la somme de plusieurs termes. Dans cette décomposition, certains termes sont susceptibles d'être étudiés directement (et ressemblent à ceux qui viennent du crible) et d'autres sont du type "bilinéaire", mis en avant par Vinogradov. Dans les "bons" cas, on parvient à majorer ces derniers par des quantités assez petites. C'est par exemple l'approche suivie par Christian Mauduit (1959-2019) et Joël Rivat (né en 1966), de l'institut de mathématiques de Luminy, qui créèrent la surprise en 2010 en démontrant qu'il existe, à un terme d'erreur près, autant de nombres premiers dont la somme des chiffres en binaire est paire ou impaire (voir [Mauduit-Rivat 10]).

Mais une célèbre méthode, déjà utilisée par Vinogradov, va permettre de résoudre la question de l'écriture des entiers en sommes de nombres premiers : c'est la méthode dite "du cercle", inventée par les mathématiciens anglais Godfrey Harold Hardy (1877-1947) et John Edensor Littlewood (1885-1977), qui l'ont développée dans une

frère du physicien juif russe Lev Landau, avec lequel il n'avait, à notre connaissance, nulle parenté.

série d'articles de 1920 à 1928. Grosso modo, il s'agit de faire une analyse de Fourier sur les entiers.

4.3 La méthode du cercle de Hardy-Littlewood

Rappelons qu'étant donné une fonction $f : \mathbb{R} \rightarrow \mathbb{C}$, on définit la transformée de Fourier $\widehat{f} : \mathbb{R} \rightarrow \mathbb{C}$ de la fonction f par :

$$\widehat{f}(r) = \int_{\mathbb{R}} f(x)e(-xr)dx$$

avec la notation $e(t) = e^{2\pi it}$. Alors, sous certaines conditions (f doit être notamment suffisamment bornée et à décroissance rapide), la formule d'inversion de Fourier permet d'écrire que :

$$f(x) = \int_{\mathbb{R}} \widehat{f}(r)e(xr)dx,$$

ce qui signifie que la fonction initiale $x \rightarrow f(x)$ a pu être décomposée en une somme de fonctions exponentielles complexes $x \rightarrow e(xr)$, chacune étant en quelque sorte présente avec une "force" $\widehat{f}(r)$ ¹⁹.

On peut faire la même chose si f est une fonction $f : \mathbb{Z} \rightarrow \mathbb{C}$. Dans ce cas, c'est même plus simple, \widehat{f} étant définie par une somme du type $\widehat{f}(\alpha) = \sum_n f(n)e(-\alpha n)$, et non par une intégrale. La transformée est alors une fonction $\widehat{f} : \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{C}$. Mais on est ici dans le cas inverse : on a au départ une fonction $f : \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{C}$ et la transformée est une suite $\{a_n\}$, c'est-à-dire une fonction $\widehat{f} : \mathbb{Z} \rightarrow \mathbb{C}$. Topologiquement parlant, \mathbb{R}/\mathbb{Z} est un cercle et les valeurs de \widehat{f} sont donc réparties sur la circonférence, tout comme les fréquences de chaînes radio. D'où le schéma de la Fig. 6, que nous empruntons à Harald Helfsgott.

L'intérêt d'utiliser la transformée de Fourier est que la transformée du produit de convolution de deux fonctions est égal au produit des transformées. Rappelons que le produit de convolution (additif) de $f, g : \mathbb{Z} \rightarrow \mathbb{C}$ est défini par :

$$(f * g)(n) = \sum_m \in \mathbb{Z} f(m)g(n - m).$$

19. Dans le cas d'une réception radio, par exemple, il y a un signal global capté qui est décomposé en des contributions de différentes fréquences. $\widehat{f}(r)$ va être grand lorsque r sera proche de la fréquence d'une chaîne de radio, et petit sinon. Le travail du récepteur radio est de retrouver la contribution des fréquences autour d'un r_0 donné.

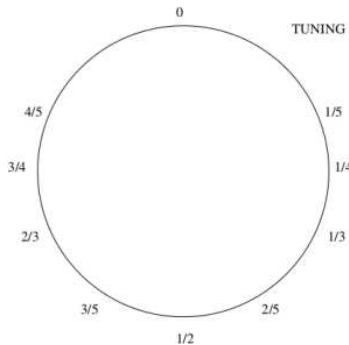


FIGURE 6 – La radio du théoricien des nombres (d’après [Helfgott 14³])

Il apparaît alors clairement que $(f * g)(n)$ ne peut être non-nul que si n peut être écrit sous la forme $n = m_1 + m_2$ pour m_1 et m_2 tels que $f(m_1)$ et $g(m_2)$ soient non nuls. Si on rajoute une troisième fonction – par exemple h et un troisième terme m_3 , il en sera de même.

Ceci nous suggère que, pour étudier le problème de Goldbach, on définisse des fonctions f, g, h de telle sorte qu’elles prennent des valeurs non-nulles seulement aux nombres premiers. Hardy et Littlewood avaient défini $f(n) = g(n) = h(n) = 0$ pour n non-premier (ou n nul, ou n négatif) et $f(n) = g(n) = h(n) = (\log n)e^{n/N}$ pour n premier (où N est un paramètre à fixer ultérieurement).

Le produit $(f * g * h)(n) = 0$ si et seulement si n peut être écrit comme une somme de trois nombres premiers. L’objectif est donc de montrer que $(f * gh)(n)$ (c’est-à-dire $(f * f * f)$) est non-nulle pour tout n supérieur à une constante. Puisque la transformée du produit de convolution est égale au produit des transformées, on a :

$$(f * g * h)(n) = \int_0^1 \widehat{f}gh(\alpha)e(\alpha n)d\alpha = \int_0^1 \widehat{f}.\widehat{g}.\widehat{h}(\alpha)e(\alpha n)d\alpha$$

et il faut montrer que $I = \int_0^1 \widehat{f}.\widehat{g}.\widehat{h}(\alpha)e(\alpha n)d\alpha = \int_0^1 (\widehat{f}(\alpha))^3 e(\alpha n)d\alpha \neq 0$.

Il se trouve que $\widehat{f}(\alpha)$ est particulièrement grand quand α est proche d’un rationnel à petit dénominateur (tout comme – si l’on reprend la métaphore radiophonique – une chaîne radio est particulièrement claire à la fréquence où elle est supposée transmettre).

Cela suggère la stratégie suivante : on estime $f(\alpha)$ pour tous les α compris dans des petits arcs de cercle autour des rationnels à petit dénominateur (ce qu’on appelle les

"arcs majeurs", ainsi nommés parce que leur contribution est majeure, malgré leur petitesse; on borne $f(\alpha)$ pour α en dehors des arcs majeurs (ce qu'on appelle les "arcs mineurs"); puis on montre que la contribution des arcs mineurs à l'intégrale est plus petite en valeur absolue que la contribution des arcs majeurs, forçant ainsi l'intégrale I à être non-nulle.

4.4 L'approche de Terence Tao

Cette méthode extraordinaire ne permet malheureusement pas de traiter la conjecture de Goldbach binaire, ou forte : le "bruit" qui vient des arcs mineurs dépasse largement la contribution des arcs majeurs comme l'a bien expliqué Terence Tao.

On notera d'ailleurs que, début 2012, c'est lui, Terence Tao (né en 1975), titulaire de nombreuses distinctions dont la médaille Fields 2006, qui, via cette méthode du cercle, a amené l'un des plus grands progrès de ces dernières décennies. Utilisant une décomposition améliorée de la fonction caractéristique, il réussit à montrer que, pour tout entier impair N inférieur ou égal à 10^{1300} , il existe 3 nombres premiers p_1, p_2, p_3 tels que $N - (p_1 + p_2 + p_3)$ soit compris entre 0 et 10^{14} . Comme des calculs directs montrent que tout entier pair inférieur ou égal à 10^{14} est somme d'au plus 2 nombres premiers, cela implique que tout entier pair est somme de 5 nombres premiers (voir [Tao 12]).

Tao a présenté l'histoire récente de la conjecture de Goldbach en ces termes :

"Il avait été établi par Vinogradov (voir [Vinogradov 37¹]), en utilisant la méthode du cercle de Hardy-Littlewood, que la conjecture impaire de Goldbach était valable pour tout x impair suffisamment grand. L'argument de Vinogradov peut être rendu effectif, et divers seuils explicites pour "suffisamment grand" ont d'ailleurs été proposés dans la littérature ; en particulier, Chen et Wang (voir [Chen-Wang 89]) ont établi la conjecture impaire de Goldbach pour tout $x \geq \exp(\exp(11.503)) \approx \exp(99012)$, et Liu & Wang [24] ont ensuite étendu ce résultat à la plage $x \geq \exp(3100)$. À l'autre extrémité, en combinant la vérification numérique de Richstein (voir [Richstein 00]) de la conjecture paire de Goldbach pour tout $x \leq 4 \times 10^{14}$ avec des intervalles courts effectifs contenant des nombres premiers (basés sur une vérification de l'hypothèse de Riemann par van de Lune et Wedeniwski (voir [Wedeniwski 03])), Ramaré et Saouter (voir [Ramaré-Saouter 03]) ont vérifié l'étrange conjecture de Goldbach pour $n \geq 1,13 \times 10^{22} \approx \exp(28)$. En utilisant des vérifications numériques ultérieures de la conjecture paire de Goldbach et l'hypothèse de Riemann, il est possible d'augmenter quelque peu ce seuil inférieur, mais l'étrange conjecture de Goldbach est aussi souvent formulée de manière presque équivalente (et légèrement plus forte)

comme l'affirmation selon laquelle tout nombre impair supérieur à sept est la somme de trois nombres premiers impairs. Notons que cette conjecture est vraie si nous supposons vraie l'hypothèse de Riemann (voir [Deshouillers et al. 97])" (voir [Tao 12], 1-2).

On peut encore résumer son article de la façon suivante :

La preuve que tout nombre impair N supérieur à 1 peut être exprimé comme la somme d'au plus cinq nombres premiers, améliore en fait le résultat de Ramaré selon lequel ce nombre peut être exprimé comme la somme d'au plus six nombres premiers. Pour ce faire, Tao utilise la susdite méthode du cercle de Hardy-Littlewood et Vinogradov, ainsi qu'une célèbre identité de Vaughan. Les techniques, qui peuvent être intéressantes pour d'autres problèmes de type Goldbach, incluent l'utilisation de sommes exponentielles lissées et l'optimisation des paramètres d'identité de Vaughan pour économiser ou réduire certaines pertes logarithmiques. Sont également employées plusieurs échelles suivant certaines idées de Bourgain, et l'utilisation du principe d'incertitude de Montgomery et du grand crible pour améliorer les estimations L2 sur les arcs majeurs. L'argument de Tao s'appuie également sur certains précédents travaux numériques, à savoir la vérification de Richstein de la conjecture paire de Goldbach jusqu'à 4×10^{14} , et la vérification de van de Lune et (indépendamment) de Wedeniwski de l'hypothèse de Riemann jusqu'à la hauteur de $3,29 \times 10^9$.

4.5 Le résultat de Harald Helfgott

Une dernière amélioration de ces résultats est venue enfin avec les travaux du mathématicien péruvien Harald Helfgott (né en 1977). Pour traiter la somme de 3 nombres premiers, Helfgott suit la même voie que Tao, mais avec, entre autres éléments nouveaux, des majorations plus précises des termes de la décomposition (voir [Helfgott 14²], [Helfgott 14³]). Au départ, sa preuve faisait appel à des estimations sur le nombre de nombres premiers inférieurs à une borne fixée obtenues grâce à de gros calculs rendus réalisables depuis 2011 par un algorithme de David Platt, de l'université de Bristol, au Royaume-Uni. Ces calculs vraiment énormes - l'équivalent de 1 million d'années de temps de calcul sur un processeur ordinaire - avaient permis en 2013 d'abaisser la constante C de Vinogradov réduite par Liu et Wang à $e^{3100} > 10^{1346}$ à une valeur de 10^{29} . Helfgott et Platt ont alors vérifié la conjecture pour tous les nombres impairs jusqu'à $8,8 \times 10^{30}$ par ordinateur, ce qui était déjà - comme Helfgott l'écrit lui-même - "la fin de l'histoire". Mais, en décembre 2013, Helfgott a encore réduit C à 10^{27} , ce qui fait que la vérification de la conjecture

ternaire de Goldbach pour tout $n \leq 10^{27}$ impair peut maintenant être refaite à la maison durant un week-end. Ainsi, toutes les pièces du puzzle ont été désormais assemblées et, après deux cent cinquante ans d'effort, la conjecture de Goldbach ternaire est donc considérée comme résolue (voir [Helfgott 14¹])

Toutefois, nous sommes bien loin de la conjecture de Goldbach binaire. Pour cette dernière, les méthodes que nous venons d'évoquer ne fonctionnent pas, car il reste des termes dans la décomposition dont on ne peut rien dire. La bonne méthode reste à trouver.

5 Bilan

Il a fallu près de trois siècles pour démontrer la conjecture de Goldbach ternaire (ou impaire). Si nous récapitulons les différentes étapes, nous obtenons la liste suivante :

1742 : Tout nombre pair plus grand que 2 est la somme de deux nombres premiers (Christian Goldbach).

1920 : Tout entier pair assez grand est somme de deux entiers composés chacun de 9 facteurs premiers au plus (Viggo Brun).

1933 : Il existe une constante C_s telle que tout entier supérieur à 1 est somme de C_s nombres premiers au plus (Lev Šchnirel'man).

1951 : Il existe une constante K telle que tout entier pair assez grand est somme de deux nombres premiers et d'au plus K puissances de 2 (Yuri Linnik).

1966 : Tout entier pair assez grand est somme d'un nombre premier et d'un nombre ayant au plus deux facteurs premiers (Chen Jingrun).

1995 : Tout entier pair est somme de six nombres premiers au plus (Olivier Ramaré).

2012 : Tout entier impair supérieur à 1 est somme de cinq nombres premiers au plus (Terence Tao).

2014 : Conjecture de Goldbach ternaire (Harald Helfgott).

Nul ne sait si et quand tombera la conjecture de Goldbach binaire. Nous n'avons actuellement aucune idée de la méthode pour y parvenir. Tout ce que nous savons est qu'aucune des méthodes précédemment utiliser ne peut servir pour sa démonstration.

Il conviendra donc d'inventer une méthode nouvelle, dont personne, pour l'instant, n'a apparemment la moindre idée.

Références

- [Brun 15] Brun, V., "Über das goldbachsche gesetz und die anzahl der primzahlpaare", *Archiv for Mathematik og Naturvidenskab*, 34 (8), 3-19, 1915.
- [Brun 20] Brun, V., *Le crible d'Ératosthène et le théorème de Goldbach*, en commission chez Jacob Dybwab, Kristiana (Oslo), 1920.
- [Caldwell-Xiong] Caldwell, Ch. K., and Xiong, Y., "What is the smallest prime?", *Journal of Integer Sequences*, article 12.9.7, Vol. 15, 2012. Voir aussi : arXiv :1209.2007v2 [math.HO] 19 Sep 2012.
- [Chen 73] Chen, J. R., "On the Representation of a Large Even Integer as the Sum of a Prime and the Product of at Most Two Primes", *Sci. Sinica* 16, 157-176, 1973.
- [Chen 78] , Chen, J. R., "On the Representation of a Large Even Integer as the Sum of a Prime and the Product of at Most Two Primes, II", *Sci. Sinica* 21, 421-430, 1978.
- [Chen-Wang 89] Chen, J. R. and Wang, T.-Z., "On odd Goldbach Problem", *Acta Math. Sinica* 32, 702-718, 1989.
- [Dantzig 30] Dantzig, T., *Number : the language of science*, Mc Millan, New York, 1930, reprinted PI Press, 2005.
- [Desboves] Desboves, M., "Sur un théorème de Legendre et son application à la recherche de limites qui comprennent entre elles des nombres premiers", *Nouvelles annales de mathématiques*, 1re série, tome 14, 281-295, 1855.
- [Deshouillers et al. 97] Deshouillers, J.-M., Effinger, G., te Riele, H., Zinoviev, D., "A complete Vinogradov 3-primes theorem under the Riemann hypothesis", *Electron. Res. Announc. Amer. Math. Soc.*, 3, 99-104, 1997.
- [Dickson 66] Dickson, L. E., *History of the theory of numbers*, Vol. I : Divisibility and primality, Chelsea Publishing Co., New York, 1966.
- [Dunham 90] Dunham, W. *Journey through Genius : The Great Theorems of Mathematics*. New York : Wiley, 1990.‘
- [Dusart 98] Dusart, P., *Autour de la fonction qui compte le nombre des nombres premiers*, Thèse de doctorat, Université de Limoges, 1998.
- [Estermann 38] Estermann, T. "On Goldbach's Problem : Proof that Almost All Even Positive Integers are Sums of Two Primes", *Proc. London Math. Soc.*, Ser. 2 44, 307-314, 1938.

- [Euler 65] Euler, L. und Goldbach, Ch. *Briefwechsel 1729-1764*, Akademie-Verlag, Berlin, 1965.
- [Euler Archive 42] Euler, L., *Copy of Letter 00766* (Lettre XLIV), <http://eulerarchive.maa.org/correspondence/correspondents/Goldbach.html>, 1742.
- [Farrugia 18] Farrugia, J. A., Brun's 1920 Theorem on Goldbach's Conjecture, thesis submitted in partial fulfillment of the requirements for the degree of Master of Science, Utah State University, Logan, Utah, 2018.
- [Gallagher 71] Gallagher, P., "A larger sieve", *Acta Arithmetica* 18, 77-81, 1971.
- [Gallagher 73] Gallagher, P., "The large sieve and probabilistic Galois theory", in Diamond, Harold G. (ed.). *Analytic number theory*, Proceedings of Symposia in Pure Mathematics. Vol. 24. American Mathematical Society, 91-101, 1973.
- [Goudout 16] Goudout, E., *Écarts entre les nombres premiers consécutifs et fonctions multiplicatives sur de petites intervalles. Introduction au domaine de recherche*, ENS, Département de mathématiques et applications, <https://www.math.ens.psl.eu>, 2016.
- [Goudout 19] Goudout, E., Étude de la fonction ω : petits intervalles et systèmes translétés, thèse, Université Paris-Diderot, 2019.
- [Guy 94] Guy, R. K., "Goldbach's Conjecture", *Unsolved Problems in Number Theory*, 2nd ed. New York, Springer-Verlag, 105-107, 1994.
- [Hadamard 15] Hadamard, J., "Un travail de Jean Merlin sur les nombres premiers", *Bulletin de Sciences Mathématiques*, 39, 121-136, 1915.
- [Halberstam-Richert] Halberstam, H. and Richert, H.-E., *Sieve Methods*, Academic Press, New York, 1974.
- [Helfgott 13] Helfgott, H. A. "The Ternary Goldbach Conjecture", *Gac. R. Soc. Mat. Esp.*, 16, 709-726, 2013.
- [Helfgott 14¹] Helfgott, H. A. "The Ternary Goldbach Conjecture Is True", <https://arxiv.org/pdf/1312.7748.pdf>, Jan. 17, 2014.
- [Helfgott 14²] Helfgott, H. A., "Major arcs for Goldbach's problem", arXiv :1305.2897 [math.NT] (ou arXiv :1305.2897v4 [math.NT]), 14 avril 2014.
- [Helfgott 14³] Helfgott, H. A., "La conjecture de Goldbach ternaire", *La Gazette des mathématiciens*, tome 140, 5-18, avril 2014.
- [Legendre 08] Legendre, A.-M. , *Essai sur la théorie des nombres*, 2e édition, Paris, Courcier, 1808.

- [Mauduit-Rivat 10] Mauduit, Ch., Rivat, J., "Sur un problème de Gelfond : la somme des chiffres des nombres premiers", *Annals of Mathematics*, vol. 171, n° 3, 2010,
- [Oliveira da Silva 15] Oliveira e Silva, T., "Goldbach Conjecture Verification", <https://sweet.ua.pt/tos/goldbach.html>, 30 décembre 2015.
- [Ramaré 95] Ramaré, O., "On Šnirel'man's constant", *Ann. Scuola Norm. Sup. Pisa Cl. Sci.*, vol. 22, no 4, 645-706, 1995.
- [Ramaré-Saouter 03] "Short effective intervals containing primes", *J. Number Theory* 98, no. 1, 10-33, 2003.
- [Ramaré 13] Ramaré, O., "Goldbach et les sommes de nombres premiers", *La Recherche*, 476, 68-71, juin 2013.
- [Richstein 00] Richstein, J., "Verifying the Goldbach conjecture up to 4×10^{14} ", *Mathematics of Computation*, 70, 1745-1749, 2000.
- [Rosen 04] Rosen, K. H., *Elementary Number Theory*, Addison-Wesley, 5e ed., Reading (Mass.), 2004.
- [Rubinstein-Sarnak 94] Rubinstein, M. and Sarnak, P., "Chebyshev's Bias", *Experimental Math.*, 3, 173-197, 1994.
- [Šnirel'man 39] vŠnirel'man, L. G., "Ob additivnykh svoystavakh chisel" ("On the Additive Properties of Numbers"), in *Izvestiya Donskogo politekhnicheskogo instituta v Novocherkasske*, 14 nos, 2-3 (1930), 3-28, also in *Uspekhi matematicheskikh nauk*, 6 (1939), 9-25, 1939.
- [Smith 68] Smith, D. E. Smith, *History of Mathematics*, Vol. II, Dovers publications, Dover, 1958.
- [Stäckel 16] Stäckel, P. G., "Die Darstellung der geraden Zahlen als Summen von zwei Primzahlen", *Sitz. Heidelberger Akad. Wiss. (Mat.-Natur. Kl.)*, 7A (10), 1916.
- [Tao 12] Tao, T., "Every odd number greater than 1 is the sum of at most five primes", arXiv :1201.6656 [math.NT], janvier 2012, (ou arXiv :1201.6656v4, juillet 2012).
- [Tarán 81] Tarán, L., *Speusippus of Athens : A Critical Study with a Collection of the Related Texts and Commentary*, Philosophia Antiqua, Vol. 39, E. J. Brill, Leiden, 1981.
- [Teissier 65-66] Teissier, B., "Crible de Brun", *Séminaire Delange-Pisot-Poitou. Théorie des nombres*, tome 7, No 2 (1965-1966). "
- [Vaughan 77] Vaughan, R. C., "Sommes Trigonométriques sur les Nombres Premiers", *C.R. Acad. Sci. Paris; Sér. A* Vol. 285, 981-983, 1977.

- [Vinogradov 37¹] Vinogradov, I. M. "Representation of an Odd Number as a Sum of Three Primes", *Comptes rendus (Doklady) de l'Académie des Sciences de l'U.R.S.S.* 15, 169-172, 1937.
- [Vinogradov 37²] Vinogradov, I. "Some Theorems Concerning the Theory of Primes", *Recueil Math.* 2, 179-195, 1937.
- [Vinogradov 54] Vinogradov, I. M., *The Method of Trigonometrical Sums in the Theory of Numbers*, London : Interscience, 1954.
- [Waring 82] Waring, E., *Meditationes algebraic*, J. Archdeacon, Cambridge, 1782.
- [Wedeniowski 03] Wedeniowski, S., "ZetaGrid - Computational verification of the Riemann Hypothesis", *Conference in Number Theory in Honour of Professor H.C. Williams*, Banff, Alberta, Canada, May 2003.