Université Lyon 1 Claude Bernard

Mémoire en vue de l'obtention du diplôme du
Master de l'université de Lyon 1
en mathématiques

Directeur de mémoire : Élie Mosaki

Le théorème de Shnirel'man-Goldbach

Simon Boyer
<boyer@math.univ-lyon1.fr>

Lyon, 2012

À la mémoire de Christian Goldbach (1690-1764) qui en 18 mots passionna des générations de mathématiciens, pendant toute une vie pour certains d'entre eux, et depuis quelques mois pour moi-même.
Je lui dédie ce mémoire, à lui qui a initié mon entrée dans le monde de la théorie des nombres.

Remerciements

Je remercie toutes celles et ceux qui m'ont accompagné au cours de ce mémoire, en particulier ceux que je vais oublier :

- *Élie Mosaki*, mon directeur de mémoire et professeur d'arithmétique, pour sa présence, son attention, son écoute, ses précieux conseils. Si cela était possible, j'aimerais faire à nouveau un mémoire sous sa direction.
- *Emmanuel Fricain*, mon professeur d'arithmétique, pour m'avoir éclairé sur les nombres et avoir répondu à mes multiples questions (ainsi que pour faire partie de ma bibliographie).
- *Abdel Yakoub*, délégué et précieux camarade de promotion, collègue arithméticien, ami et conseiller, pour son humour, son soutien et son thé bio.
- *Julie Rouchier*, pour avoir lu et relu mon mémoire, et surtout pour avoir supporté mes interminables monologues d'explications arithmétiques.
- *Serge Parmentier*, mon professeur de géométrie, pour m'avoir orienté vers un potentiel directeur de mémoire, à savoir Boris Adamczewski.
- *Boris Adamczewski*, chargé de recherche à l'Institut Camille Jordan, pour m'avoir permis de trouver mon directeur de mémoire Élie Mosaki.
- *Jiang Zeng*, mon professeur de théorie des nombres, pour m'avoir grandement initié à la combinatoire.
- *Tous les enseignants du Master* pour leur investissement.
- *Toute l'équipe de la bibliothèque du bâtiment Braconnier*, pour sa disponibilité et sa gentillesse.
- *La Police Nationale*, pour m'avoir redonné le goût des mathématiques, et sans qui je n'aurais jamais fait ce mémoire.
- *Leonhard Euler* pour avoir répondu à la lettre de Christian Goldbach.

Avant-propos

Les nombres premiers sont l'une des plus grandes sources de passion et de mystère dans la communauté mathématiques. On ne sait trop estimer depuis combien de temps l'humanité en a connaissance. Certaines sources - très remises en cause - diraient depuis 20 000 ans. D'autres - incontestables - diraient il y a au moins 2 300 ans. En tout cas, voilà plus de 2000 ans que l'Homme les étudie, et pourtant leur essence lui échappe toujours. Preuves en sont les grandes conjectures modernes de la théorie des nombres, aussi nombreuses que difficiles (voir Annexe 1). Même les génies de notre temps sont très loin d'avoir compris le fonctionnement exact des nombres premiers. Ces nombres naturels à la définition si simple et intuitive, du moins une fois posé le principe de la multiplication, ont l'air d'aller et venir à leur guise. Évidemment, les mathématiciens ont beaucoup appris sur eux, notamment qu'ils se raréfient, mais des questions fondamentales restent en suspens.

Le but de ce mémoire ne sera clairement pas de faire un état des lieux de toutes les connaissances modernes sur les nombres premiers. Ce travail dépasserait sans aucun doute la taille de plusieurs thèses. Ce mémoire sera centré sur une question encore ouverte concernant les nombres premiers, une question fondamentale et d'une difficulté extrême [1] : la conjecture de Goldbach. Énoncée en 1742 par Christian Goldbach dans une lettre (voir Annexe 2) envoyée à Leonhard Euler, elle a fait couler l'encre et la sueur de centaines de mathématiciens depuis 270 ans. Des avancées en apparence [2] colossales ont été faites, mais personne n'a atteint le but ultime.

1. Olivier Ramaré a même confié, très récemment, à propos de cette conjecture : "Peut-être qu'on ne verra pas la démonstration avant mille ans !"

2. En apparence, car comme le fait remarquer David Larousserie : "Pour un mathématicien, avancer à petits pas ne signifie pas forcément se rapprocher du but".

Originellement, cette conjecture a été énoncée ainsi par Goldbach : *Tout nombre strictement supérieur à 2 peut être écrit comme une somme de trois nombres premiers*[3]. Il est à noter que Goldbach considère 1 comme un nombre premier, la norme à ce propos ayant changé aujourd'hui. Euler a répondu à son collègue Goldbach par une lettre (voir Annexe 2) où il reformule la conjecture, par : *Tout nombre pair peut être écrit comme somme de deux nombres premiers*[4]. Fait surprenant, la conjecture énoncée par Euler est plus forte mais il ne paraît pas s'en rendre compte. Elle prendra quand même le nom de conjecture de Goldbach. Avec la norme moderne considérant que 1 n'est pas un nombre premier, voici la formulation actuelle de la célèbre conjecture de Goldbach : *Tout nombre pair supérieur ou égal à 4 peut être écrit comme somme de deux nombres premiers.* Ce problème à l'énoncé si simple s'est avéré être d'une difficulté insurmontable. Même la version faible de la conjecture, appelée "faible" car conséquence directe de la conjecture (forte) de Goldbach, n'a pas été démontrée : *Tout nombre impair supérieur ou égal à 7 peut être écrit comme somme de trois nombres premiers.* Elle a tout de même été démontrée par Ivan Matveyevich Vinogradov en 1937 *à partir d'un certain rang*[5], ce qui est une très grande avancée. Ce résultat est maintenant connu sous le nom de théorème de Vinogradov.

Il est à noter que beaucoup d'éléments laissent présager que la conjecture de Goldbach est vraie, même il faut être très prudent, car les nombres premiers peuvent réserver bien des surprises[6]. Tout d'abord, les ordinateurs nous ont permis de vérifier (voir Annexe 3) cette conjecture au cas par cas jusqu'à $4 \cdot 10^{18}$. Évidemment, ce n'est rien face à l'infini, mais tout de même, c'est rassurant. Ensuite, de nombreux résultats peuvent donner l'espoir que la conjecture de Goldbach est vraie. C'est le cas du théorème de Vinogradov, cité ci-avant, mais aussi du théorème de Shnirel'man-Goldbach (objet de ce mémoire), des travaux de Chudakov, van der Corput et Estermann, qui, inspirés des travaux de Vinogradov, ont montré que *presque tout entier pair*

3. En version originale : *Es scheinet wenigstens, daß eine jede Zahl, die größer ist als 2, ein aggregatum trium numerorum primorum sey.*

4. En version originale : *ein jeder numerus par eine summa duorum numerorum primorum sey.*

5. Vinogradov a montré l'existence d'un M tel que tout nombre impair au-delà de M est somme de trois nombre premiers. Depuis, ce M a pu être calculé explicitement et amélioré, mais il reste bien trop gros pour qu'un ordinateur puisse vérifier la conjecture faible pour les cas (finis) en dessous de M.

6. En effet, on peut noter qu'avant 1957, on avait vérifié au cas par cas que pour tout $x < 26861$, il y avait toujours autant ou plus de nombres premiers inférieurs ou égaux à x de la forme $4n + 3$ que de nombres premiers inférieurs ou égaux à x de la forme $4n + 1$. Mais en 1957, J.Leech a prouvé que pour x=26861, ceci est faux.

est somme de deux nombres premiers, du théorème de Chen Jing-run, qui dit que *tout entier pair suffisamment grand est la somme d'un nombre premier et d'un nombre qui est soit premier, soit qui a deux facteurs premiers distincts*, et, très récemment, des travaux de Terence Tao, qui a montré que *tout entier impair est la somme d'au plus 5 nombres premiers, impliquant que tout entier est la somme d'au plus 6 nombres premiers*. Pourtant, rien ni personne ne peut aujourd'hui prouver ou infirmer la conjecture de Goldbach.

Ces différents théorèmes qui viennent d'être cités montrent quatre approches possibles de la conjecture de Goldbach. Une première consiste à la démontrer à partir d'un certain rang, puis de réduire ce rang jusqu'à être capable de montrer informatiquement (ou à la main...) les cas finis manquant, c'est-à-dire ceux en dessous de ce rang. C'est l'approche théorique originelle de Vinogradov pour la conjecture de Goldbach faible. Une seconde consiste à écrire les entiers pairs comme somme de deux entiers dont on contrôle les facteurs premiers. C'est l'approche de Chen Jing-run, dans les traces d'Alfréd Rényi [7], combinée avec la première approche. La troisième consiste à écrire les entiers comme somme d'un nombre contrôlé de nombres premiers. C'est la base du théorème de Shnirel'man-Goldbach, suivi des progrès spectaculaires de, entre autres, Terence Tao. Enfin, la quatrième consiste à prouver la conjecture de Goldbach pour presque tous les nombres pairs. C'est en quelque sorte l'approche de Chudakov, van der Corput et Estermann.

Il est fort intéressant de relater les premiers progrès qui ont été faits sur la conjecture de Goldbach pendant ces 270 années, même si aucun n'a abouti à sa preuve. En effet, ce n'est qu'en observant l'histoire des travaux sur un sujet ouvert que l'on peut espérer entrevoir à quel point on s'est approché du résultat tant attendu, et surtout, comment [8]. Il est à noter, de manière pas si surprenante pour qui connaît l'histoire de la théorie des nombres, qu'aucun véritable progrès n'a été fait en direction de la conjecture de Goldbach avant 1920. Viggo Brun a été le premier à trouver un résultat s'en approchant de loin : *Tout entier pair suffisamment grand est somme de deux entiers ayant chacun au plus 9 facteurs premiers*. Son résultat a été amélioré maintes fois jusqu'à celui de Chen cité ci-avant. Après Brun, Godfrey Harold Hardy et

7. Qui avait montré en 1948 qu'il existe un M tel que tout entier pair suffisamment grand peut s'écrire comme la somme d'un nombre premier et d'un nombre ayant au plus M facteurs premiers. Chen Jing-run a montré que $M \leq 2$.

8. Comme le dit Olivier Ramaré à propos des travaux autour de la conjecture de Goldbach : "Ces travaux sont cependant intéressants, car pour aborder la démonstration finale, nous avons besoin de comprendre les entiers et les nombres premiers. Les outils et méthodes développés dans des cas plus 'simples' pourront donc être utiles. On ne sait jamais".

John Edensor Littlewood ont démontré en 1922 la conjecture de Goldbach faible *pour tout entier impair suffisamment grand*, mais en admettant hélas l'hypothèse de Riemann généralisée. Il faudra attendre les travaux de Vinogradov en 1937 pour que cette conjecture de Goldbach faible *pour tout entier impair suffisamment grand* soit démontrée indépendamment de l'hypothèse de Riemann généralisée. Mais la première avancée vraiment significative à été faite par Lev Genrikhovich Schnirel'man en 1930. Ce mathématicien biélorusse a démontré l'existence d'un entier M tel que tout entier supérieur ou égal à 2 peut s'écrire comme somme d'au plus M nombres premiers. Ce résultat porte le nom de *théorème de Shnirel'man-Goldbach*.

Le cœur de ce mémoire sera le théorème de Shnirel'man-Goldbach.

Pourquoi ce choix ? Justement parce que c'est le premier résultat fondamental en direction de la conjecture de Goldbach, qui permet enfin aux mathématiciens d'avoir un vrai angle d'attaque pour ce problème : réduire l'entier M dans le théorème jusqu'à 2. On aurait pu imaginer traiter de travaux plus récents, comme ceux de Tao ayant réduit M jusqu'à 6. Mais ces travaux utilisent des méthodes dépassant par leur complexité l'objectif de ce mémoire. Seule exception à noter : on utilisera une méthode plus récente que le théorème de Shnirel'man-Goldbach pour démontrer ce dernier : le crible de Selberg, créé par Atle Selberg en 1947. C'est en fait le choix qui a été fait par Nathanson [7]. À nouveau, pourquoi ce choix ? Parce que d'une part le crible de Selberg est beaucoup plus pratique, efficace et élégant que le crible de Brun utilisé originellement par Shnirel'man, et d'autre part le crible de Selberg est une méthode très utile et très centrale en théorie des nombres, encore utilisée aujourd'hui, et qui mérite grandement que l'on s'y attarde.

Ainsi, l'objectif de ce mémoire est clairement d'exposer le théorème de Shnirel'man-Goldbach et sa preuve, tout en présentant la méthode du crible de Selberg que l'on utilisera pour celle-ci. En espérant que cette lecture vous éclaire, vous pouvez tourner la page pour la débuter.

Table des matières

Conventions et notations

Même s'il sera souvent rappelé le sens des notations au cours de ce mémoire, il est essentiel de dresser ici une liste des conventions et notations qui seront utilisées. La plupart sont classiques en théorie des nombres.

• $\ll$ et $\mathcal{O}$, notations respectives de E.G.H.Landau et I.M.Vinogradov ayant le même sens, signifient *borné asymptotiquement*, c'est-à-dire que, pour deux fonctions f et g, $f \ll g$ ou $f = \mathcal{O}(g)$ signifient qu'il existe $\lambda > 0$ tel que pour tout x où cela a un sens, $|f(x)| \leq \lambda |g(x)|$.

• $\pi(x)$ désigne le nombre de nombres premiers inférieurs ou égaux à x réel.

• C_n^m, prononcée m *parmi* n, désigne $\frac{n!}{m!(n-m)!}$ et n'aura ici pour nous un sens que lorsque m et n sont deux entiers naturels vérifiant $m \leq n$. Cet entier représente le nombre de manières de choisir m éléments dans un ensemble à n éléments.

• $v_p(n)$, avec p un nombre premier et n un entier naturel, désigne la *valuation p-adique de n*, c'est-à-dire la puissance associée à p (éventuellement nulle) dans la décomposition de n en facteurs premiers.

• $\lfloor x \rfloor$ désigne la *partie entière* du réel x, c'est-à-dire le plus grand entier inférieur ou égal à x.

• $a|b$ (respectivement, $a \nmid b$) signifie a *divise* b (respectivement, a *ne divise pas* b) avec a et b entiers, c'est-à-dire qu'il existe (respectivement, n'existe pas) k entier tel que $b = ak$.

• De manière générale, sauf mention contraire et comme il est de coutume en théorie des nombres, la lettre p désigne un nombre premier.

Introduction

Comme annoncé dans l'avant-propos, ce mémoire sera articulé autour du théorème de Shnirel'man-Goldbach. Ce théorème s'énonce ainsi :

Théorème A. *Il existe un entier $M \geq 1$ tel que tout entier supérieur ou égal à 2 est la somme d'au plus M nombres premiers.*

Cependant, le choix a été fait d'introduire en premier les outils qui permettront sa démonstration. Ce choix vient d'un souci de clarté, car il n'est pas aisé de comprendre les fondements d'une preuve si l'on y admet des résultats délicats.

Ainsi, le premier chapitre, très court, sera consacré à une inégalité de Chebychev, utilisant des outils arithmétiques plutôt simples en comparaison du reste du mémoire. Cette inégalité permettra de démontrer un théorème essentiel à la preuve du Théorème A :

Théorème B.

$$\sum_{N \leq x} r(N) \gg \frac{x^2}{(\log x)^2},$$

où r(N) représente le nombre de représentations de N comme somme de deux nombres premiers (avec par exemple 5+7 et 7+5 comptant comme deux représentations différentes).

Le second chapitre, le plus gros, sera entièrement consacré au célèbre crible de Selberg. Il permettra d'aboutir à un théorème essentiel dans la preuve du théorème de Shnirel'man-Goldbach, qui s'énoncera ainsi :

Théorème C.

$$\sum_{N \leq x} r(N)^2 \ll \frac{x^3}{(\log x)^4},$$

où r(N) représente le nombre de représentations de N comme somme de deux nombres premiers (avec par exemple 5+7 et 7+5 comptant comme deux représentations différentes).

Pour ce second chapitre, on peut se poser la question de ce qu'est un crible, et citer Cécile Dartyge et Gérald Tenenbaum [4] qui en donne une définition : *Soient A et B deux suites d'entiers. Un* crible *de A relativement à B est une méthode, basée sur un procédé d'élimination, qui vise à détecter les éléments de A appartenant à B.* Le but du chapitre sera de présenter cette puissante méthode de la théorie des nombres qu'est le crible de Selberg, de démontrer les théorèmes sur lesquels elle s'axe et de l'appliquer dans un cas bien précis qui permettra d'aboutir au Théorème C. En fait, on pourrait même avancer que le crible de Selberg est le cœur de la preuve du Théorème A. Ceci est vrai pour ce mémoire, mais rappelons que le crible de Selberg est plus récent que le théorème de Shnirel'man-Goldbach, et que Shnirel'man avait utilisé un autre crible : celui de Brun.

Enfin, le troisième chapitre présentera le théorème de Shnirel'man-Goldbach, c'est-à-dire le Théorème A, objectif de ce mémoire, et sa preuve, qui en plus d'utiliser des outils combinatoires utilisera les Théorèmes B et C.

À la fin de ce mémoire, il nous sera permis d'espérer que le lecteur sera devenu plus familier avec la méthode du crible de Selberg et aura pu se convaincre de la véracité du théorème de Shnirel'man-Goldbach.

Précisons aussi que certains ouvrages ont beaucoup inspiré ce mémoire, sans y être cités explicitement, tels ceux d'Andrews [1], de Wang [9], de Hardy et Wright [3], et de Vinogradov [8].

Chapitre 1

Une inégalité de Chebychev

Dans la démonstration du théorème de Shnirel'man-Goldbach, le Théorème A, nous aurons besoin du Théorème B que l'on rappelle ici :

$$\sum_{N \leq x} r(N) \gg \frac{x^2}{(\log x)^2},$$

où $r(N)$ représente le nombre de façons d'écrire N comme somme de deux nombres premiers (où par exemple 5+7 et 7+5 comptent comme deux représentations différentes). Pour le montrer, nous allons d'abord prouver l'inégalité suivante, dite inégalité de Chebychev, où $\pi(x)$ représente le nombre de nombres premiers inférieurs ou égaux à x :

Théorème 1.

$$\forall x \in [2, +\infty[,\ \pi(x) \geq \frac{\log 2}{6} \frac{x}{\log x}.$$

Pour démontrer ce théorème, nous allons utiliser deux lemmes en nous inspirant largement d'un cours d'Emmanuel Fricain [6].

Lemme 2.

$$\forall n \in \mathbb{N}^*,\ \frac{4^n}{2n} \leq C_n^{2n}.$$

Preuve. Soit $n \in \mathbb{N}^*$. Remarquons tout d'abord que :

$$2^{2n-1} = (1+1)^{2n-1} = \sum_{k=0}^{2n-1} C_k^{2n-1}.$$

On sait de plus que C_k^{2n-1} est maximal pour $k = n$, c'est à dire que $\forall k \in [\![0, 2n-1]\!]$, on a $C_k^{2n-1} \leq C_n^{2n-1}$. Donc

$$2^{2n-1} \leq \sum_{k=0}^{2n-1} C_n^{2n-1} = 2nC_n^{2n-1}.$$

Ainsi

$$\frac{4^n}{2n} \leq 2C_n^{2n-1} = C_n^{2n-1} + C_{n-1}^{2n-1} = C_n^{2n}.$$

□

Lemme 3.

$$\forall (p,n) \in \mathbb{P} \times \mathbb{N}^*,\ p^{v_p(C_n^{2n})} \leq 2n.$$

Preuve. Soit $(p,n) \in \mathbb{P} \times \mathbb{N}^*$. On a $v_p(C_n^{2n}) = v_p((2n)!) - 2v_p(n!)$. On rappelle la formule de Legendre (voir [2] page 67) sur la valuation p-adique :

$$v_p(n!) = \sum_{k=0}^{\infty} \lfloor \frac{n}{p^k} \rfloor.$$

Donc

$$v_p(C_n^{2n}) = \sum_{k=0}^{\infty} \left(\lfloor \frac{2n}{p^k} \rfloor - 2\lfloor \frac{n}{p^k} \rfloor \right).$$

Mais le terme $\lfloor \frac{2n}{p^k} \rfloor - 2\lfloor \frac{n}{p^k} \rfloor$ est nul dès que $\frac{2n}{p^k} < 1$, donc dès que $\frac{\log 2n}{\log p} < k$, et aussi quand $k = 0$. On a ainsi

$$v_p(C_n^{2n}) = \sum_{k=1}^{\lfloor \frac{\log 2n}{\log p} \rfloor} \left(\lfloor \frac{2n}{p^k} \rfloor - 2\lfloor \frac{n}{p^k} \rfloor \right).$$

Et la fonction $t \mapsto \lfloor 2t \rfloor - 2\lfloor t \rfloor$ est 1-périodique, valant 0 pour $t \in [0, \frac{1}{2}[$ et 1 pour $t \in [\frac{1}{2}, 1[$. Donc pour tout t réel, $\lfloor 2t \rfloor - 2\lfloor t \rfloor \leq 1$. Ainsi

$$v_p(C_n^{2n}) \leq \sum_{k=1}^{\lfloor \frac{\log 2n}{\log p} \rfloor} 1 = \left\lfloor \frac{\log 2n}{\log p} \right\rfloor \leq \frac{\log 2n}{\log p}.$$

D'où

$$p^{v_p(C_n^{2n})} \leq 2n.$$

□

On peut maintenant démontrer le Théorème 1.

Démonstration du Théorème 1. Remarquons que l'on a, pour $n \in \mathbb{N}^*$,

$$C_n^{2n} = \prod_{p \leq 2n} p^{v_p(C_n^{2n})}.$$

Donc, par les Lemmes 2 et 3, on a

$$\frac{4^n}{2n} \leq C_n^{2n} = \prod_{p \leq 2n} p^{v_p(C_n^{2n})} \leq \prod_{p \leq 2n} (2n) = (2n)^{\pi(2n)}.$$

On applique log aux membres de gauche et de droite, pour obtenir

$$n \log 4 - \log(2n) \leq \pi(2n) \log(2n),$$

c'est-à-dire

$$\frac{(2n)\log 2}{\log(2n)} - 1 \leq \pi(2n).$$

Il est aisé de voir que :

$$\frac{n \log 2}{\log n} \leq \frac{(2n)\log 2}{\log(2n)} - 1.$$

Ainsi

$$\frac{n \log 2}{\log n} \leq \pi(2n).$$

Prenons x réel tel que $x \geq 2$. On pose $n = \lfloor \frac{x}{2} \rfloor \in \mathbb{N}^*$. Alors

$$n \leq 2n \leq x < 2(n+1).$$

Ainsi, par croissance de π, on a

$$\frac{\log 2}{\log x}\left(\frac{x}{2} - 1\right) \leq \frac{n \log 2}{\log n} \leq \pi(2n) \leq \pi(x).$$

Supposons maintenant $x \geq 3$. Alors on a

$$\frac{\log 2}{\log x}\left(\frac{x}{2} - 1\right) = \frac{x}{\log x} \log 2 \left(\frac{1}{2} - \frac{1}{x}\right) \geq \frac{x}{\log x} \log 2 \left(\frac{1}{2} - \frac{1}{3}\right) = \frac{x}{\log x} \frac{\log 2}{6}.$$

Ainsi

$$\frac{x}{\log x} \frac{\log 2}{6} \leq \pi(x).$$

Supposons maintenant $2 \leq x < 3$. Alors $\pi(x) = 1$ et :

$$\frac{x}{\log x}\frac{\log 2}{6} \leq \frac{3}{\log 2}\frac{\log 2}{6} = \frac{1}{2}.$$

Donc

$$\frac{x}{\log x}\frac{\log 2}{6} \leq \pi(x).$$

Dans tous les cas, le théorème est vérifié.

□

Nous pouvons maintenant démontrer le résultat nécessaire au théorème de Shnirel'man-Goldbach, à savoir le Théorème B :

Théorème B.

$$\sum_{N \leq x} r(N) \gg \frac{x^2}{(\log x)^2}.$$

Démonstration du Théorème B. Si on a p et q premiers tels que $p, q \leq \frac{x}{2}$, alors $p + q \leq x$. Ainsi, par le Théorème 1 :

$$\sum_{N \leq x} r(N) \geq \sum_{p,q \leq \frac{x}{2}} 1 = \pi(x/2)^2 \geq \frac{(\log 2)^2}{36}\frac{(\frac{x}{2})^2}{(\log \frac{x}{2})^2}.$$

Donc

$$\sum_{N \leq x} r(N) \gg \frac{x^2}{(\log x)^2}.$$

□

Chapitre 2

Le crible de Selberg

Le mathématicien Atle Selberg a développé en 1947 un crible en théorie des nombres, désormais appelé le crible de Selberg. S'inscrivant dans la continuité des cribles d'Eratosthène, de Legendre et de Brun, cette méthode permet d'évaluer le cardinal d'ensembles d'entiers de manière très efficace. Elle a abouti à de nombreuses avancées importantes en théorie des nombres, en particulier le théorème de Chen évoqué dans l'avant-propos.

2.1 Présentation

Nous allons ici présenter ce crible, en particulier dans le but de démontrer le Théorème C, qui sera nécessaire à la démonstration du théorème A. Rappelons ce Théorème C :

$$\sum_{N\leq x} r(N)^2 \ll \frac{x^3}{(\log x)^4}.$$

où $r(N)$ représente le nombre de façons d'écrire N comme somme de deux nombres premiers (où par exemple 5+7 et 7+5 comptent comme deux représentations différentes).

Ce qui suit est très largement inspiré d'un cours de Cécile Dartyge et Gérald Tenenbaum [4], pour les Théorèmes 4 et 8 ainsi que pour la démonstration du Théorème 4. Comme à l'habitude en théorie des nombres, p et q désigneront toujours des nombres premiers.

On se donne $\mathcal{A}$ un ensemble fini d'entiers naturels non nuls. On se donne $\mathcal{P}$ un ensemble de nombres premiers. Dès lors, on cherche à évaluer la quantité $S(\mathcal{A}, \mathcal{P}, z)$ définie pour tout réel $z \geq 2$ par

$$S(\mathcal{A}, \mathcal{P}, z) = |\{a \in \mathcal{A} : (p|a \text{ et } p \in \mathcal{P}) \Rightarrow p \geq z\}|,$$

c'est-à-dire le nombre d'éléments de $\mathcal{A}$ dont les facteurs premiers qui sont dans $\mathcal{P}$ sont plus grands que z. On notera maintenant aussi, pour tout entier $d \geq 1$,

$$\mathcal{A}_d = \{a \in \mathcal{A} : d|a\},$$

c'est-à-dire le sous-ensemble de $\mathcal{A}$ des éléments divisibles par d.

En pratique, pour tout d sans facteur carré ayant tous ses facteurs premiers dans $\mathcal{P}$, on essayera de mettre $|\mathcal{A}_d|$ sous la forme

$$|\mathcal{A}_d| = X\frac{\omega(d)}{d} + \mathcal{R}(\mathcal{A}, d), \tag{2.1}$$

où X est indépendant de d et où ω est une fonction arithmétique multiplicative vérifiant $\omega(n) = 0$ si n a des facteurs carrés ou si n a des facteurs premiers en dehors de $\mathcal{P}$, et où $\mathcal{R}(\mathcal{A}, d)$ est un « reste » que l'on peut aisément majorer.

2.2 Démonstration du premier théorème

En supposant que l'on ait mis $|\mathcal{A}_d|$ sous la forme (2.1), on a alors le théorème suivant :

Théorème 4. *On suppose qu'il existe $A_1 > 1$ tel que pour tout nombre premier p on ait*

$$0 \leq \frac{\omega(p)}{p} \leq 1 - \frac{1}{A_1}. \tag{2.2}$$

Alors on a, pour tout réel $z \geq 2$, la majoration

$$S(\mathcal{A}, \mathcal{P}, z) \leq \frac{X}{G(z)} + \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\nu(d)}|\mathcal{R}(\mathcal{A}, d)|,$$

où $\nu(d)$ désigne le nombre de facteurs premiers distincts de d et où on a posé

$$G(z) = \sum_{\substack{d<z \\ d|P(z)}} g(d), \tag{2.3}$$

avec $P(z)$ défini par

$$P(z) = \prod_{\substack{p \in \mathcal{P} \\ p<z}} p,$$

et avec g fonction arithmétique multiplicative définie pour p premier par

$$g(p) = \frac{\omega(p)}{p - \omega(p)}. \tag{2.4}$$

En pratique, il est très difficile d'estimer la fonction G, sauf sous une condition bien précise qui sera présentée dans la partie 2.3 intitulée « Démonstration du second théorème ».

Nous allons maintenant démontrer ce Théorème 4. Avant tout, notons (b, c) le pgcd de deux entiers b et c, et $[b, c]$ leur ppcm. Soit $z \geq 2$. L'idée de départ de Selberg est de considérer une suite $\{\lambda_d\}$ de réels vérifiant seulement $\lambda_1 = 1$ et définie uniquement sur les d diviseurs de $P(z)$, c'est-à-dire sur les d sans facteurs carrés dont les facteurs premiers sont strictement inférieurs à z. Pour le côté pratique des calculs, nous étendons cette suite en posant $\lambda_d = 0$ si $d \geq z$ ou si $d \not| P(z)$. Tout l'objectif du crible sera de choisir judicieusement cette suite.

On pose, pour tout entier $n \geq 1$,

$$s^+(n) = \left(\sum_{d|(n,P(z))} \lambda_d \right)^2.$$

Il est évident que pour tout entier $n \geq 1$, on a $s^+(n) \geq 0$, et $s^+(n) = \lambda_1 = 1$ dès que $(n, P(z)) = 1$. Or il est clair que

$$\{n \in \mathcal{A} : (p|n \text{ et } p \in \mathcal{P}) \Rightarrow p \geq z\} = \{n \in \mathcal{A} : (n, P(z)) = 1\},$$

car $P(z)$ est le produit des nombres premiers dans $\mathcal{P}$ inférieurs à z. On a ainsi, en notant $[d_1, d_2]$ le ppcm de d_1 et d_2,

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}, z) &= \sum_{\substack{n \in \mathcal{A} \\ (n,P(z))=1}} 1 \\ &= \sum_{\substack{n \in \mathcal{A} \\ (n,P(z))=1}} s^+(n) \\ &\leq \sum_{n \in \mathcal{A}} s^+(n) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{n\in\mathcal{A}} \left(\sum_{d|(n,P(z))} \lambda_d \right)^2 \\
&= \sum_{n\in\mathcal{A}} \sum_{\substack{d_1|(n,P(z))\\ d_2|(n,P(z))}} \lambda_{d_1}\lambda_{d_2} \\
&= \sum_{\substack{d_1|P(z)\\ d_2|P(z)}} \sum_{\substack{n\in\mathcal{A}\\ [d_1,d_2]|n}} \lambda_{d_1}\lambda_{d_2} \\
&= \sum_{\substack{d_1|P(z)\\ d_2|P(z)}} \lambda_{d_1}\lambda_{d_2} \Big(\sum_{\substack{n\in\mathcal{A}\\ [d_1,d_2]|n}} 1 \Big) \\
&= \sum_{\substack{d_1|P(z)\\ d_2|P(z)}} \lambda_{d_1}\lambda_{d_2} |\mathcal{A}_{[d_1,d_2]}|.
\end{aligned}
$$

car $\mathcal{A}_{[d_1,d_2]} = \{a \in \mathcal{A} : [d_1,d_2]|a\}$. On utilise maintenant la forme (2.1) de $|\mathcal{A}_m|$ avec $m = [d_1,d_2]$:

$$
S(\mathcal{A},\mathcal{P},z) \leq \sum_{\substack{d_1|P(z)\\ d_2|P(z)}} \lambda_{d_1}\lambda_{d_2} \left(X\frac{\omega([d_1,d_2])}{[d_1,d_2]} + \mathcal{R}(\mathcal{A},[d_1,d_2]) \right).
$$

Ainsi

$$
S(\mathcal{A},\mathcal{P},z) \leq X\Sigma_1 + \Sigma_2, \tag{2.5}
$$

où

$$
\Sigma_1 = \sum_{\substack{d_1|P(z)\\ d_2|P(z)}} \lambda_{d_1}\lambda_{d_2} \frac{\omega([d_1,d_2])}{[d_1,d_2]}, \tag{2.6}
$$

et

$$
\Sigma_2 = \sum_{\substack{d_1|P(z)\\ d_2|P(z)}} \lambda_{d_1}\lambda_{d_2} \mathcal{R}(\mathcal{A},[d_1,d_2]). \tag{2.7}
$$

Tout le problème maintenant est de majorer Σ_1 et Σ_2 en choisissant judicieusement la suite $\{\lambda_d\}$. Pour cela, nous allons démontrer deux lemmes. Le premier, avec les mêmes définitions que le Théorème 4, dit que :

Lemme 5.

$$
\Sigma_1 \geq \frac{1}{G(z)}, \tag{2.8}
$$

et même

$$\Sigma_1 = \frac{1}{G(z)} \text{ si } \lambda_d = \frac{d\mu(d)g(d)}{\omega(d)G(z)} \sum_{l|\frac{P(z)}{d}} g(l), \tag{2.9}$$

où μ est la fonction de Möbius, c'est-à-dire la fonction multiplicative définie par $\mu(1) = 1$, $\mu(p) = -1$ et $\mu(p^\alpha) = 0$ si $\alpha \geq 2$.

Preuve. Par 2.6, on a

$$\Sigma_1 = \sum_{d_1|P(z),d_2|P(z)} \lambda_{d_1}\lambda_{d_2} \frac{\omega([d_1,d_2])}{[d_1,d_2]}.$$

Pour se débarrasser du ppcm, on note $r = (d_1, d_2)$. On a alors s_1 et s_2 tels que $d_1 = s_1 r$ et $d_2 = s_2 r$. Et ainsi $[d_1, d_2] = s_1 s_2 r$, donc $\omega([d_1, d_2]) = \omega(s_1 s_2 r)$. Mais on sait que $(s_1, r) = 1$ car d_1 n'a pas de facteur carré. Donc, ω étant multiplicative :

$$\omega(d_1) = \omega(s_1 r) = \omega(s_1)\omega(r),$$

et ainsi

$$\omega(s_1 s_2 r) = \omega(s_1)\omega(s_2 r) = \frac{\omega(d_1)}{\omega(r)}\omega(d_2),$$

car $\omega(r) \neq 0$ puisque $\omega(d_1) \neq 0$ (il n'a évidemment aucun facteur carré non plus). On vient de montrer que

$$\frac{\omega([d_1,d_2])}{[d_1,d_2]} = \frac{\omega(d_1)\omega(d_2)r}{d_1 d_2 \omega(r)}.$$

On reporte dans Σ_1 :

$$\Sigma_1 = \sum_{d_1|P(z),d_2|P(z)} \lambda_{d_1}\lambda_{d_2} \frac{\omega(d_1)\omega(d_2)}{d_1 d_2} \frac{(d_1,d_2)}{\omega((d_1,d_2))}.$$

On note maintenant $h(r) = \frac{r}{\omega(r)}$ pour r tel que $\omega(r) \neq 0$. Ainsi

$$\Sigma_1 = \sum_{d_1|P(z),d_2|P(z)} \lambda_{d_1}\lambda_{d_2} \frac{\omega(d_1)\omega(d_2)}{d_1 d_2} h(d_1,d_2). \tag{2.10}$$

On cherche à réécrire h sous la forme $h = \frac{1}{g} * \mathbf{1}$, où $*$ est le produit de convolution et $\mathbf{1}$ est la fonction arithmétique constante de valeur 1. Et comme $\mathbf{1}^{-1} = \mu$ (pour la convolution bien sûr, où μ est la fonction de Möbius), on a $\frac{1}{g} = h * \mu$. De plus, h est clairement multiplicative sur son domaine de

définition (car ω est multiplicative). μ est aussi multiplicative. Donc $\frac{1}{g}$ est multiplicative. On la détermine entièrement en la calculant pour tout nombre premier p (car on ne considère que les entiers sans facteurs carrés, et donc pas les p^α avec $\alpha \geq 2$) :

$$\frac{1}{g}(p) = h * \mu(p) = h(p)\mu(1) + h(1)\mu(p) = \frac{p}{\omega(p)} - 1 = \frac{p - \omega(p)}{\omega(p)}.$$

D'autre part, d'après l'hypothèse (2.2), on a $p - \omega(p) = p(1 - \frac{\omega(p)}{p}) \geq \frac{p}{A_1} > 0$. La fonction g est donc bien définie, par :

$$g(p) = \frac{\omega(p)}{p - \omega(p)}.$$

Comme $h = \frac{1}{g} * \mathbf{1}$, on reporte dans 2.10 :

$$\begin{aligned}
\Sigma_1 &= \sum_{d_1|P(z),d_2|P(z)} \lambda_{d_1}\lambda_{d_2} \frac{\omega(d_1)\omega(d_2)}{d_1 d_2} (\frac{1}{g} * \mathbf{1})((d_1, d_2)) \\
&= \sum_{d_1|P(z),d_2|P(z)} \lambda_{d_1}\lambda_{d_2} \frac{\omega(d_1)\omega(d_2)}{d_1 d_2} \sum_{k|(d_1,d_2)} \frac{1}{g(k)} \\
&= \sum_{d_1|P(z),d_2|P(z)} \lambda_{d_1}\lambda_{d_2} \frac{\omega(d_1)\omega(d_2)}{d_1 d_2} \sum_{\substack{k|d_1 \\ k|d_2}} \frac{1}{g(k)} \\
&= \sum_{k|P(z)} \frac{1}{g(k)} \sum_{\substack{d_1|P(z),d_2|P(z) \\ k|d_1,k|d_2}} \lambda_{d_1}\lambda_{d_2} \frac{\omega(d_1)\omega(d_2)}{d_1 d_2} \\
&= \sum_{k|P(z)} \frac{1}{g(k)} \left(\sum_{\substack{d|P(z) \\ k|d}} \frac{\lambda_d \omega(d)}{d} \right)^2 .
\end{aligned}$$

Si on écrit $y_k = \sum_{\substack{d|P(z) \\ k|d}} \frac{\lambda_d \omega(d)}{d}$, on a Σ_1 sous forme quadratique $\sum_{k|P(z)} \frac{1}{g(k)} y_k^2$. On cherche à minimiser cette forme quadratique en fonction de ses paramètres λ_d sous la contrainte $\lambda_1 = 1$. Exprimons les λ_k en fonction des y_k. Pour cela, pour tout entier $d \geq 1$, on note $f(d) = \frac{\lambda_d \omega(d)}{d}$. On a ainsi $y_k = \sum_{\substack{d|P(z) \\ k|d}} f(d)$.

On a, lorsque $n|P(z)$:

$$f(n) = \sum_{d|\frac{P(z)}{n}} \mu(d) y_{nd}.$$

En effet,

$$\begin{aligned}
\sum_{d|\frac{P(z)}{n}} \mu(d) y_{nk} &= \sum_{d|\frac{P(z)}{n}} \mu(d) \sum_{l|\frac{P(z)}{nd}} f(nld) \\
&= \sum_{m|\frac{P(z)}{n}} f(nm) \sum_{d,l \,:\, dl=m} \mu(d) \\
&= \sum_{m|\frac{P(z)}{n}} f(nm) \sum_{d|m} \mu(d) \\
&= \sum_{m|\frac{P(z)}{n}} f(nm)\delta(m) \\
&= f(n).
\end{aligned}$$

Ainsi, pour $n|P(z)$, on a

$$\frac{\lambda_n \omega(n)}{n} = \sum_{d|\frac{P(z)}{n}} \mu(d) y_{nd}. \tag{2.11}$$

Et la contrainte $\lambda_1 = 1$ nous donne

$$1 = \sum_{d|P(z)} \mu(d) y_d. \tag{2.12}$$

Mais on a choisi les y_d nuls dès que $d \geq z$. On peut donc réécrire :

$$1 = \sum_{\substack{d<z \\ d|P(z)}} \mu(d) y_d.$$

On va modifier cette somme en utilisant le fait que $\omega(d) \neq 0 \Rightarrow g(d) \neq 0$.

$$1 = \sum_{\substack{d<z \\ d|P(z)}} \frac{\mu(d) y_d}{\sqrt{g(d)}} \sqrt{g(d)}.$$

On remarque que $d|P(z) \Rightarrow \mu(d) \in \{-1, +1\} \Rightarrow \mu(d)^2 = 1$. On applique alors l'inégalité de Cauchy-Schwarz et (2.6), pour trouver

$$
\begin{aligned}
1 &\leq \left(\sum_{\substack{d<z\\ d|P(z)}} \frac{\mu(d)^2 y_d^2}{\sqrt{g(d)}^2}\right)^{\frac{1}{2}} \left(\sum_{\substack{d<z\\ d|P(z)}} \sqrt{g(d)}^2\right)^{\frac{1}{2}} \qquad (2.13)\\
&= \left(\sum_{\substack{d<z\\ d|P(z)}} \frac{y_d^2}{g(d)}\right)^{\frac{1}{2}} \left(\sum_{\substack{d<z\\ d|P(z)}} g(d)\right)^{\frac{1}{2}}\\
&= (\Sigma_1)^{\frac{1}{2}} \left(\sum_{\substack{d<z\\ d|P(z)}} g(d)\right)^{\frac{1}{2}}.
\end{aligned}
$$

Donc

$$\Sigma_1 \geq \frac{1}{G(z)},$$

où, on le rappelle, $G(z) = \sum_{\substack{d<z\\ d|P(z)}} g(d)$. Ceci démontre 2.8.

On ne peut ainsi pas espérer mieux qu'une égalité entre Σ_1 et $\frac{1}{G(z)}$. Celle-ci, dans l'inégalité 2.13 de Cauchy-Schwarz, pour d fixé vérifiant $d|P(z)$ et $d < z$, ne se produit que s'il existe un réel t tel que

$$\frac{\mu(d) y_d}{\sqrt{g(d)}} = t\sqrt{g(d)},$$

c'est-à-dire tel que

$$\mu(d) y_d = t g(d). \qquad (2.14)$$

Et avec 2.12, on trouve alors que

$$1 = \sum_{d<z, d|P(z)} t g(d),$$

et donc $t = \frac{1}{G(z)}$ par 2.3. En remplaçant dans 2.14, on se rend compte qu'il faut choisir les y_d ainsi :

$$y_d = \frac{\mu(d) g(d)}{G(z)}. \qquad (2.15)$$

On en déduit alors, pour tout $d|P(z)$ et $d < z$, en combinant 2.11 et 2.15, les λ_d par :

$$\lambda_d = \frac{d}{\omega(d)} \sum_{l|\frac{P(z)}{d}} \mu(l) y_{dl},$$

donc, par 2.14 :

$$\lambda_d = \frac{d\mu(d)g(d)}{\omega(d)G(z)} \sum_{l|\frac{P(z)}{d}} g(l), \tag{2.16}$$

On choisit les λ_d de cette manière. On a donc $\Sigma_1 = \frac{1}{G(z)}$. Ceci démontre 2.9, et achève de démontrer le Lemme 5.

□

Le deuxième lemme porte une propriété des λ_l :

Lemme 6. *Pour tout $l < z$ tel que $l|P(z)$, on a $|\lambda_l| \leq 1$.*

Preuve. Pour tous $l \geq 1$ et $d \geq 1$, si $(l, d) > 1$, alors ld a des facteurs carrés, donc $y_{ld} = 0$. Ainsi, pour $l < z$ tel que $l|P(z)$ fixé, on peut réécrire 2.16 :

$$\begin{aligned} \lambda_l &= \frac{l}{\omega(l)} \sum_{\substack{l|\frac{P(z)}{d} \\ (l,d)=1}} \mu(d) y_{ld} \\ &= \frac{l}{\omega(l)} \sum_{\substack{l|\frac{P(z)}{d} \\ (l,d)=1}} \mu(l)\mu(ld) y_{ld}, \end{aligned}$$

car μ multiplicative et $\mu(l)^2 = 1$, donc $(l, d) = 1 \Rightarrow \mu(d) = \mu(l)\mu(ld)$. Maintenant, on utilise 2.15 et la multiplicité de g :

$$\begin{aligned} \lambda_l &= \frac{l\mu(l)}{\omega(l)} \sum_{\substack{l|\frac{P(z)}{d}, ld<z \\ (l,d)=1}} \frac{g(ld)}{G(z)} \\ &= \frac{l\mu(l)}{\omega(l)G(z)} \sum_{\substack{l|\frac{P(z)}{d}, ld<z \\ (l,d)=1}} g(l)g(d) \end{aligned}$$

$$= \frac{l\mu(l)g(l)}{\omega(l)G(z)} \sum_{\substack{l|\frac{P(z)}{d}, ld<z \\ (l,d)=1}} g(d). \tag{2.17}$$

Mais on a d'une part, par multiplicité de g et ω, et par 2.4 :

$$\frac{lg(l)}{\omega(l)} = \prod_{p|l} \frac{p}{\omega(p)} \frac{\omega(p)}{p-\omega(p)} = \prod_{p|l} \frac{1}{1-\frac{1}{\omega(p)}}, \tag{2.18}$$

et d'autre part, toujours pour $l < z$ tel que $l|P(z)$ fixé, avec 2.3 :

$$\begin{aligned} G(z) &= \sum_{\substack{d<z \\ d|P(z)}} g(d) \\ &= \sum_{r|l} \sum_{\substack{d<z, d|P(z) \\ (d,l)=r}} g(d), \end{aligned}$$

en séparant la somme sur d selon les valeurs que prend le pgcd de l et d. Dans cette somme sur d, on a $(d,l) = r$ donc $d|r$. Notons-y $m = \frac{d}{r}$ pour effectuer le changement de variable $d = mr$. On somme ainsi maintenant sur m au lieu de d. On obtient :

$$G(z) = \sum_{r|l} \sum_{\substack{m<\frac{z}{r} : mr|P(z) \\ (mr,l)=r}} g(mr).$$

On remarque maintenant que dans la somme sur m, on a $(mr,l) = r \Leftrightarrow (m,l) = 1$. En effet, on a $mr|P(z)$ donc $(m,r) = 1$ car $P(z)$ sans facteur carré. Ainsi

$$\begin{aligned} G(z) &= \sum_{r|l} \sum_{\substack{m<\frac{z}{r} : mr|P(z) \\ (m,l)=1}} g(mr) \\ &= \sum_{r|l} g(r) \sum_{\substack{m<\frac{z}{r}, m|\frac{P(z)}{r} \\ (m,l)=1}} g(m), \end{aligned}$$

car g est multiplicative. De plus, quand $r|l$, on a $\frac{z}{l} < \frac{z}{r}$ et $\frac{P(z)}{l}|\frac{P(z)}{r}$. Donc on peut minorer $G(z)$:

$$G(z) \geq \left(\sum_{r|l} g(r) \right) \left(\sum_{\substack{m<\frac{z}{l}, m|\frac{P(z)}{l} \\ (m,l)=1}} g(m) \right). \tag{2.19}$$

Et on a, encore par multiplicité de g, et par 2.4 :

$$\begin{aligned} \sum_{r|l} g(r) &= \prod_{p|l} (1 + g(p)) \\ &= \prod_{p|l} (1 + \frac{\omega(p)}{p - \omega(p)}) \\ &= \prod_{p|l} \frac{p}{p - \omega(p)} \\ &= \prod_{p|l} \frac{1}{1 - \frac{1}{\omega(p)}}. \end{aligned} \tag{2.20}$$

On reconnaît à la dernière ligne l'égalité 2.18. On a donc, en remplaçant dans 2.19 :

$$G(z) \geq \frac{lg(l)}{\omega(l)} \sum_{\substack{m<\frac{z}{l}, m|\frac{P(z)}{l} \\ (m,l)=1}} g(m). \tag{2.21}$$

Et on connaît $|\lambda_l|$ par 2.17 :

$$|\lambda_l| = \frac{lg(l)}{\omega(l)G(z)} \sum_{\substack{l<\frac{z}{d}, l|\frac{P(z)}{d} \\ (l,d)=1}} g(d).$$

Ainsi, en remplaçant dans 2.21, on a $|\lambda_l| \leq 1$. Ceci démontre le Lemme 6. □

Les Lemmes 5 et 6 vont nous permettre de démontrer le Théorème 4. Souvenons-nous par 2.7 que :

$$\Sigma_2 = \sum_{\substack{d_1|P(z) \\ d_2|P(z)}} \lambda_{d_1} \lambda_{d_2} \mathcal{R}(\mathcal{A}, [d_1, d_2]).$$

On utilise le Lemme 6 :

$$|\lambda_l| \leq 1,$$

et

$$\lambda_l = 0 \Leftrightarrow d \not| P(z).$$

Ainsi,

$$\begin{aligned}
\Sigma_2 &\leq \sum_{\substack{d_1<z, d_2<z \\ d_1|P(z), d_2|P(z)}} |\mathcal{R}(\mathcal{A}, [d_1, d_2])| \\
&= \sum_{\substack{d<z^2 \\ d|P(z)}} |\mathcal{R}(\mathcal{A}, d)| \sum_{\substack{d_1<z, d_2<z \\ d_1|P(z), d_2|P(z) \\ [d_1,d_2]=d}} 1 \\
&= \sum_{\substack{d<z^2 \\ d|P(z)}} |\mathcal{R}(\mathcal{A}, d)| \cdot |\{(d_1, d_2) : d_1 < z, d_2 < z, d_1|P(z), d_2|P(z), [d_1, d_2] = d\}|.
\end{aligned}$$

Notons $\mathcal{F}_d = \{(d_1, d_2) : d_1 < z, d_2 < z, d_1|P(z), d_2|P(z), [d_1, d_2] = d\}$ pour simplifier :

$$\Sigma_2 \leq \sum_{\substack{d<z^2 \\ d|P(z)}} |\mathcal{R}(\mathcal{A}, d)| \cdot |\mathcal{F}_d|. \tag{2.22}$$

Montrons alors le lemme suivant :

Lemme 7. *Pour tout d sans facteur carré :*

$$|\mathcal{F}_d| = 3^{\nu(d)} \tag{2.23}$$

où, rappelons-le, $\nu(d)$ compte le nombre de facteurs premiers de d.

Preuve. Soit d sans facteur carré. On peut écrire $d = p_1 \dots p_{\nu(d)}$ où les p_i sont des facteurs premiers deux à deux distincts. On veut calculer le nombre d'éléments de $\mathcal{F}_d$. Pour cela, prenons (d_1, d_2) dans $\mathcal{F}_d$. Comme $[d_1, d_2] = d$, on a $d_1|d$ et $d_2|d$. Ainsi, d_1 et d_2 sont sans facteur carré avec tous leurs facteurs premiers dans $\{p_1, \dots, p_{\nu(d)}\}$. Plus encore, il faut que les facteurs premiers de d_1 et d_2 réunis fassent $\{p_1, \dots, p_{\nu(d)}\}$, pour que $[d_1, d_2] = d$. Pour chaque $i \in [\![1, \nu(d)]\!]$, on a donc 3 possibilités seulement :

$$(1) \quad p_i|d_1 \text{ et } p_i \not| d_2$$

(2) $p_i \not| d_1$ et $p_i | d_2$

(3) $p_i | d_1$ et $p_i | d_2$.

Les facteurs premiers de d_1 et d_2 les déterminant entièrement, il y a autant de manières de choisir d_1 et d_2 que de choisir si les p_i vérifient chacun le cas 1, le cas 2 ou le cas 3, c'est-à-dire $3^{\nu(d)}$ possibilités. Donc $|\mathcal{F}_d| = 3^{\nu(d)}$. □

Ainsi, par 2.22 et 2.23 :

$$\Sigma_2 \leq \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\nu(d)} |\mathcal{R}(\mathcal{A}, d)|.$$

On a en plus $\Sigma_1 = \frac{1}{G(z)}$ d'après le point 2.9 du Lemme 5, et $S(\mathcal{A}, \mathcal{P}, z) \leq X\Sigma_1 + \Sigma_2$ d'après 2.5. On en déduit le Théorème 4 :

$$S(\mathcal{A}, \mathcal{P}, z) \leq \frac{X}{G(z)} + \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\nu(d)} |\mathcal{R}(\mathcal{A}, d)|.$$

□

2.3 Démonstration du second théorème

Dans le Théorème 4, il est plus aisé d'estimer G sous une condition supplémentaire sur ω, qui est la suivante : on suppose qu'il existe $A_2 \geq 1$ et κ réel deux constantes telles que pour tout réel $z \geq 2$, pour tout $v \in [2, z]$, on ait

$$-A_2 \leq \sum_{v \leq p < z} \frac{\omega(p) \log p}{p} - \kappa \log \frac{z}{v} \leq A_2. \tag{2.24}$$

Le réel κ est appelé la dimension du crible. L'hypothèse ci-dessus signifie en fait que ω vaut κ en valeur moyenne. Et sous cette hypothèse, on peut énoncer le théorème suivant :

Théorème 8. *Sous les hypothèses* (2.2) *et* (2.24)*, on a*

$$S(\mathcal{A}, \mathcal{P}, z) \leq XV(z)e^{\gamma\kappa}\Gamma(\kappa+1)\left(1 + \mathcal{O}\left(\frac{1}{\log z}\right)\right) + \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\nu(d)} |\mathcal{R}(\mathcal{A}, d)|,$$

où $V(z) = \prod_{p<z}(1 - \frac{\omega(p)}{p})$*,* γ *est la constante d'Euler et* Γ *est la fonction d'Euler.*

Ce théorème est celui qui nous intéresse réellement pour les applications, car il nous donne une majoration de $S(\mathcal{A}, \mathcal{P}, z)$ facile à évaluer.

Commençons la démonstration du Théorème 8, en se plaçant donc sous l'hypothèse (2.24). Cette démonstration est très largement inspirée de Halberstam et Richert [5]. Nous allons démontrer 4 lemmes préliminaires :

Lemme 9. *On note* $W(z) = \prod_{p<z}(1 - \frac{1}{p})$. *On a*

$$\frac{W(v)}{W(z)} = \frac{\log z}{\log v}\left\{1 + \mathcal{O}\left(\frac{1}{\log z}\right)\right\} \quad si \;\; 2 \leq v \leq z, \tag{2.25}$$

Preuve. Un classique de l'arithmétique (voir [7] page 165) nous dit que :

$$\prod_{p<z}(1 - \frac{1}{p}) = \frac{e^{-\gamma}}{\log z}\left\{1 + \mathcal{O}\left(\frac{1}{\log z}\right)\right\}; \tag{2.26}$$

Ce résultat, combiné à la définiton de W, implique immédiatement que, pour tout $z \geq 2$:

$$\frac{W(v)}{W(z)} = \frac{\log z}{\log v}\left\{1 + \mathcal{O}\left(\frac{1}{\log z}\right)\right\} \quad \text{si} \;\; 2 \leq v \leq z.$$

□

Maintenant, on analyse plus en détails les conséquences de l'hypothèse (2.24) à travers le lemme suivant :

Lemme 10. *Avec* $2 \leq v \leq z$, *on a*

$$-\frac{A_2}{\log v} \leq \sum_{v \leq p < z} \frac{\omega(p)}{p} - \kappa \log \frac{\log z}{\log v} \leq \frac{A_2}{\log v} \tag{2.27}$$

et il existe $C_1 > 0$ *et* $C_2 > 0$ *tels que pour tout* $s \geq 0$,

$$-C_1 \frac{A_2}{\log v} \leq \sum_{v \leq p < z} \frac{g(p)}{p^s} - \kappa \sum_{v \leq p < z} \frac{1}{p^{s+1}} \leq C_2 \frac{1}{\log v}, \tag{2.28}$$

où g *est définie comme dans le Théorème 4.*

Preuve. On utilise la formule sommatoire d'Abel (on a $1 < v \leq z$) :

$$\sum_{v \leq n < z} a(n) f(n) = A(z) f(z) - A(v) f(v) - \int_v^z A(t) f'(t) \mathrm{d}t,$$

avec $a(n) := \mathbf{1}_{\mathbb{P}}(n)\frac{\omega(n)\log n}{n}$ ($\mathbf{1}_{\mathbb{P}}$ est l'indicatrice des nombres premiers), $f(x) := \frac{1}{\log x}$ ($\mathcal{C}^1$ sur $[v,z]$), et $A(x) := \sum_{n<x} a(n) = \sum_{p<x} \frac{\omega(p)\log p}{p}$. On obtient ainsi :

$$\sum_{v\le p<z} \frac{\omega(p)}{p} = \frac{1}{\log z}\sum_{p<z}\frac{\omega(p)\log p}{p} - \frac{1}{\log v}\sum_{p<v}\frac{\omega(p)\log p}{p} + \int_v^z \frac{1}{t(\log t)^2}\sum_{p<t}\frac{\omega(p)\log p}{p}\mathrm{d}t.$$

Or

$$\begin{aligned} -\frac{1}{\log v}\sum_{p<v}\frac{\omega(p)\log p}{p} &= -\frac{1}{\log z}\sum_{p<v}\frac{\omega(p)\log p}{p} + (\frac{1}{\log z} - \frac{1}{\log v})\sum_{p<v}\frac{\omega(p)\log p}{p} \\ &= -\frac{1}{\log z}\sum_{p<v}\frac{\omega(p)\log p}{p} - \left(\int_v^z \frac{1}{t(\log t)^2}\right)\sum_{p<v}\frac{\omega(p)\log p}{p}. \end{aligned}$$

Donc

$$\sum_{v\le p<z} \frac{\omega(p)}{p} = \frac{1}{\log z}\sum_{v\le p<z}\frac{\omega(p)\log p}{p} + \int_v^z \frac{1}{t(\log t)^2}\sum_{v\le p<t}\frac{\omega(p)\log p}{p}\mathrm{d}t.$$

Et l'hypothèse (2.24) nous dit que :

$$\sum_{v\le p<z}\frac{\omega(p)\log p}{p} \le \kappa\log\frac{z}{v} + A_2.$$

Donc

$$\sum_{v\le p<z} \frac{\omega(p)}{p} \le \frac{\kappa\log\frac{z}{v} + A_2}{\log z} + \int_v^z \frac{\kappa\log\frac{t}{v} + A_2}{t(\log t)^2}\mathrm{d}t. \tag{2.29}$$

Calculons l'intégrale :

$$\begin{aligned} \int_v^z \frac{\kappa\log\frac{t}{v} + A_2}{t(\log t)^2}\mathrm{d}t &= \int_v^z \frac{\kappa}{t\log t}\mathrm{d}t + \int_v^z \frac{-\kappa\log v + A_2}{t(\log t)^2}\mathrm{d}t \\ &= \kappa\Big[\log\log t\Big]_v^z + (\kappa\log v - A_2)\Big[\frac{1}{\log t}\Big]_v^z \\ &= \kappa\log\frac{\log z}{\log v} + \frac{\kappa\log v - A_2}{\log z} + \frac{-\kappa\log v + A_2}{\log v} \\ &= \kappa\log\frac{\log z}{\log v} - \frac{\kappa\frac{\log z}{\log v} + A_2}{\log z} + \frac{A_2}{\log v}. \end{aligned}$$

Ainsi :

$$\frac{\kappa \log \frac{z}{v} + A_2}{\log z} + \int_v^z \frac{\kappa \log \frac{t}{v} + A_2}{t(\log t)^2} \mathrm{d}t = \kappa \log \frac{\log z}{\log v} + \frac{A_2}{\log v}.$$

Donc, en remplaçant dans 2.29 :

$$\sum_{v \leq p < z} \frac{\omega(p)}{p} \leq \kappa \log \frac{\log z}{\log v} + \frac{A_2}{\log v},$$

c'est-à-dire

$$\sum_{v \leq p < z} \frac{\omega(p)}{p} - \kappa \log \frac{\log z}{\log v} \leq \frac{A_2}{\log v}. \tag{2.30}$$

Ceci prouve la partie droite de 2.27 dans le Lemme 10.

En procédant exactement de même à partir de

$$\kappa \log \frac{z}{v} - A_2 \leq \sum_{v \leq p < z} \frac{\omega(p) \log p}{p},$$

on démontre la partie gauche de 2.27, à savoir :

$$-\frac{A_2}{\log v} \leq \sum_{v \leq p < z} \frac{\omega(p)}{p} - \kappa \log \frac{\log z}{\log v}.$$

Passons à 2.28 dans le Lemme 10, encadrement uniforme en $s \geq 0$. On remarque d'abord que :

$$\sum_{v \leq p < z} \frac{\omega(p)}{p \log p} = \frac{1}{(\log z)^2} \sum_{p < z} \frac{\omega(p) \log p}{p} - \frac{1}{(\log v)^2} \sum_{p < v} \frac{\omega(p) \log p}{p} + 2 \int_v^z \frac{1}{t(\log t)^3} \sum_{p < t} \frac{\omega(p) \log p}{p} \mathrm{d}t,$$

en faisant la sommation d'Abel avec $a(n) := \mathbf{1}_{\mathbb{P}}(n) \frac{\omega(n) \log n}{n}$ et $f(x) := \frac{1}{(\log x)^2}$.
Mais

$$\begin{aligned} -\frac{1}{(\log v)^2} \sum_{p < v} \frac{\omega(p) \log p}{p} &= -\frac{1}{(\log z)^2} \sum_{p < v} \frac{\omega(p) \log p}{p} + \left(\frac{1}{(\log z)^2} - \frac{1}{(\log v)^2} \right) \sum_{p < v} \frac{\omega(p) \log p}{p} \\ &= -\frac{1}{(\log z)^2} \sum_{p < v} \frac{\omega(p) \log p}{p} - 2 \left(\int_v^z \frac{1}{t(\log t)^3} \right) \sum_{p < v} \frac{\omega(p) \log p}{p}. \end{aligned}$$

Donc

$$\sum_{v\le p<z}\frac{\omega(p)}{p\log p}=\frac{1}{(\log z)^2}\sum_{v\le p<z}\frac{\omega(p)\log p}{p}+2\int_v^z\frac{1}{t(\log t)^3}\sum_{v\le p<t}\frac{\omega(p)\log p}{p}\mathrm{d}t.$$

Avec l'hypothèse (2.24), on trouve :

$$\sum_{v\le p<z}\frac{\omega(p)}{p\log p}\le\frac{\kappa\log\frac{z}{v}+A_2}{(\log z)^2}+2\int_v^z\frac{\kappa\log\frac{t}{v}+A_2}{t(\log t)^3}\mathrm{d}t. \tag{2.31}$$

Calculons l'intégrale comme avant :

$$\begin{aligned}2\int_v^z\frac{\kappa\log\frac{t}{v}+A_2}{t(\log t)^3}\mathrm{d}t &= 2\int_v^z\frac{\kappa}{t(\log t)^2}\mathrm{d}t+2\int_v^z\frac{-\kappa\log v+A_2}{t(\log t)^3}\mathrm{d}t\\ &= \frac{\kappa\log v+A_2}{(\log v)^2}-\frac{\kappa\log\frac{z}{v}+A_2}{(\log z)^2}-\frac{\kappa}{\log z}.\end{aligned}$$

Donc, en remplaçant dans 2.31 :

$$\begin{aligned}\sum_{v\le p<z}\frac{\omega(p)}{p\log p} &\le \frac{\kappa\log v+A_2}{(\log v)^2}-\frac{\kappa}{\log z}\\ &\le \frac{1}{\log v}\left(\kappa+\frac{A_2}{\log v}\right).\end{aligned} \tag{2.32}$$

D'autre part, avec $v=p$ et $z=p+\varepsilon$, $0<\varepsilon<1$, dans l'hypothèse (2.24), on trouve que :

$$\frac{\omega(p)}{p}\log p\le\kappa\log\frac{p+\varepsilon}{p}+A_2,$$

et donc, en faisant $\varepsilon\to 0$, on trouve :

$$\frac{\omega(p)}{p}\log p\le A_2. \tag{2.33}$$

D'autre part, avec l'hypothèse (2.2) qui dit que $\frac{\omega(p)}{p}\le 1-\frac{1}{A_1}$, et 2.4, on a

$$\begin{aligned}g(p) &= \frac{\omega(p)}{p-\omega(p)}\\ &= \frac{\omega(p)}{p}\frac{1}{1-\frac{\omega(p)}{p}}\end{aligned}$$

$$\leq \frac{\omega(p)}{p} A_1.$$

Et donc, en combinant avec 2.33, on trouve :

$$g(p) \log p \leq A_1 A_2. \tag{2.34}$$

En combinant les inégalités 2.32 et 2.34, on trouve :

$$\begin{aligned} \sum_{v \leq p < z} \frac{\omega(p)}{p} g(p) &= \sum_{v \leq p < z} \frac{\omega(p)}{p \log p} g(p) \log p \\ &\leq A_1 A_2 \sum_{v \leq p < z} \frac{\omega(p)}{p \log p} \\ &\leq \frac{A_1 A_2}{\log v} \left(\kappa + \frac{A_2}{\log v} \right). \end{aligned} \tag{2.35}$$

Par définition de g en 2.4, il est immédiat que $g(p) = \frac{\omega(p)}{p} + \frac{\omega(p)}{p} g(p)$. Donc, avec les inégalités 2.30, 2.35 et le fait que $\sum_{v \leq p < z} \frac{1}{p} = \log \frac{\log z}{\log v} + \mathcal{O}\left(\frac{1}{\log v}\right)$, on a

$$\begin{aligned} \sum_{v \leq p < z} g(p) &= \sum_{v \leq p < z} \frac{\omega(p)}{p} + \sum_{v \leq p < z} \frac{\omega(p)}{p} g(p) \\ &\leq \kappa \log \frac{\log z}{\log v} + \frac{A_2}{\log v} + \frac{A_1 A_2}{\log v} \left(\kappa + \frac{A_2}{\log v} \right) \\ &= \kappa \sum_{v \leq p < z} \frac{1}{p} + \mathcal{O}\left(\frac{1}{\log v} \right). \end{aligned} \tag{2.36}$$

Ainsi il existe $C_2 > 0$ tel que

$$\sum_{v \leq p < z} g(p) - \kappa \sum_{v \leq p < z} \frac{1}{p} \leq C_2 \frac{1}{\log v}.$$

D'autre part, par définition de g en 2.4, $g(p) \geq \frac{\omega(p)}{p}$, donc, comme $-\frac{A_2}{\log v} \leq \sum_{v \leq p < z} \frac{\omega(p)}{p} - \kappa \log \frac{\log z}{\log v}$ par l'hypothèse (2.2), on trouve qu'il existe $C_1 > 0$ tel que :

$$\sum_{v \leq p < z} g(p) - \kappa \sum_{v \leq p < z} \frac{1}{p} \geq -C_1 \frac{A_2}{\log v}.$$

Ainsi

$$-C_1\frac{A_2}{\log v} \leq \sum_{v\leq p<z} g(p) - \kappa \sum_{v\leq p<z} \frac{1}{p} \leq C_2\frac{1}{\log v}. \tag{2.37}$$

Pour arriver au résultat du Lemme 10, à $s \geq 0$ fixé, on utilise la formule sommatoire d'Abel pour obtenir

$$\sum_{v\leq p<z} \frac{g(p)-\frac{\kappa}{p}}{p^s} = \frac{A(z)}{z^s} - \frac{A(v)}{v^s} + s\int_v^z \frac{A(t)}{t^{s+1}}\mathrm{d}t,$$

en ayant pris $a(n) := \mathbf{1}_{\mathbb{P}}(n)(g(n)-\frac{\kappa}{n})$ et $f(x) := \frac{1}{t^s}$. On a ainsi $A(x) = \sum_{p<x} g(p) - \kappa\sum_{p<x}\frac{1}{p}$. Mais

$$\begin{aligned} -\frac{A(v)}{v^s} &= -\frac{A(v)}{z^s} + (\frac{1}{z^s}-\frac{1}{v^s})A(v) \\ &= -\frac{A(v)}{z^s} - s\left(\int_v^z \frac{1}{t^{s+1}}\mathrm{d}t\right)A(v). \end{aligned}$$

Donc

$$\sum_{v\leq p<z} \frac{g(p)-\frac{\kappa}{p}}{p^s} = \frac{1}{z^s}\sum_{v\leq p<z}(g(p)-\frac{\kappa}{p}) + s\int_v^z \frac{1}{t^{s+1}}\sum_{v\leq p<t}(g(p)-\frac{\kappa}{p})\mathrm{d}t. \tag{2.38}$$

Or on vient de voir que en 2.37 que :

$$-C_1\frac{A_2}{\log v} \leq \sum_{v\leq p<z} g(p) - \kappa \sum_{v\leq p<z} \frac{1}{p} \leq C_2\frac{1}{\log v}.$$

Donc, combiné à 2.38, on trouve :

$$\frac{-C_1}{z^s}\frac{A_2}{\log v} - C_1 s\left(\int_v^z \frac{1}{t^{s+1}}\mathrm{d}t\right)\frac{A_2}{\log v} \leq \sum_{v\leq p<z} \frac{g(p)-\frac{\kappa}{p}}{p^s} \leq \frac{C_2}{z^s}\frac{1}{\log v} + C_2 s\left(\int_v^z \frac{1}{t^{s+1}}\mathrm{d}t\right)\frac{1}{\log v},$$

c'est-à-dire

$$\frac{-C_1}{z^s}\frac{A_2}{\log v} - C_1\left(\frac{1}{v^s}-\frac{1}{z^s}\right)\frac{A_2}{\log v} \leq \sum_{v\leq p<z} \frac{g(p)-\frac{\kappa}{p}}{p^s} \leq \frac{C_2}{z^s}\frac{1}{\log v} + C_1\left(\frac{1}{v^s}-\frac{1}{z^s}\right)\frac{1}{\log v},$$

soit

$$\frac{-C_1}{v^s}\frac{A_2}{\log v} \leq \sum_{v\leq p<z} \frac{g(p)-\frac{\kappa}{p}}{p^s} \leq \frac{C_2}{v^s}\frac{1}{\log v}.$$

Donc, pour tout $s \geq 0$ on a $\frac{1}{v^s} \leq 1$, on trouve que

$$-C_1\frac{A_2}{\log v} \leq \sum_{v\leq p<z} \frac{g(p)}{p^s} - \kappa \sum_{v\leq p<z} \frac{1}{p^{s+1}} \leq C_2\frac{1}{\log v}.$$

Ceci conclut la démonstration du Lemme 10.

□

Nous nous intéressons maintenant à $V(z) = \prod_{p<z}(1-\frac{\omega(p)}{p})$ défini dans le Théorème 8 :

Lemme 11. *Avec $2 \leq v \leq z$, on a, uniformément en $s \geq 0$,*

$$\prod_{v\leq p<z} \left(1+\frac{g(p)}{p^s}\right)\left(1-\frac{1}{p^{s+1}}\right)^{\kappa} = 1 + \mathcal{O}\left(\frac{1}{\log v}\right), \tag{2.39}$$

et on a aussi

$$\frac{V(v)}{V(z)} = \left(\frac{\log z}{\log v}\right)^{\kappa}\left\{1+\mathcal{O}\left(\frac{1}{\log v}\right)\right\}. \tag{2.40}$$

Enfin, on a

$$V(z) = \left(\prod_p \left(1-\frac{\omega(p)}{p}\right)\left(1-\frac{1}{p}\right)^{-\kappa}\right)\frac{e^{-\gamma\kappa}}{(\log z)^{\kappa}}\left\{1+\mathcal{O}\left(\frac{1}{\log v}\right)\right\}, \tag{2.41}$$

où le produit infini considéré est convergeant, vérifiant :

$$\prod_p \left(1-\frac{\omega(p)}{p}\right)\left(1-\frac{1}{p}\right)^{-\kappa} \geq \exp(-A_1A_2(1+\kappa+A_2)) > 0. \tag{2.42}$$

Preuve. Montrons 2.39. On a, par définition de g en 2.4 :

$$g(p) = \frac{\omega(p)}{p} + \frac{\omega(p)}{p}g(p),$$

c'est-à-dire

$$(1-\frac{\omega(p)}{p})g(p)^2=\frac{\omega(p)}{p}g(p).$$

Par l'hypothèse (2.2), on en déduit que

$$\frac{1}{A_1}g(p)^2\leq\frac{\omega(p)}{p}g(p). \tag{2.43}$$

Mais dans la preuve du Lemme 10, on avait trouvé l'inégalité 2.35 :

$$\sum_{v\leq p<z}\frac{\omega(p)}{p}g(p)\leq\frac{A_1A_2}{\log v}\left(\kappa+\frac{A_2}{\log v}\right).$$

D'où, combiné à 2.43, on trouve :

$$\sum_{v\leq p<z}g(p)^2\leq\frac{A_1^2A_2}{\log v}\left(\kappa+\frac{A_2}{\log v}\right),$$

c'est-à-dire

$$\sum_{v\leq p<z}g(p)^2=\mathcal{O}\left(\frac{1}{\log v}\right).$$

Maintenant, on écrit :

$$\prod_{v\leq p<z}\left(1+\frac{g(p)}{p^s}\right)\left(1-\frac{1}{p^{s+1}}\right)^{\kappa}=\exp\sum_{v\leq p<z}\left(\log\left(1+\frac{g(p)}{p^s}\right)+\kappa\log\left(1-\frac{1}{p^{s+1}}\right)\right).$$

Utilisons le fait que $\log(1+x)=x+\mathcal{O}(x^2)$ dès que $x\geq-\frac{1}{2}$:

$$\prod_{v\leq p<z}\left(1+\frac{g(p)}{p^s}\right)\left(1-\frac{1}{p^{s+1}}\right)^{\kappa}=\exp\sum_{v\leq p<z}\left(\frac{g(p)}{p^s}+\mathcal{O}(g(p)^2)-\kappa\frac{1}{p^{s+1}}+\mathcal{O}\left(\frac{1}{p^2}\right)\right). \tag{2.44}$$

Par le point 2.28 du Lemme 10, on a

$$\sum_{v\leq p<z}\frac{g(p)}{p^s}-\kappa\sum_{v\leq p<z}\frac{1}{p^{s+1}}=\mathcal{O}\left(\frac{1}{\log v}\right). \tag{2.45}$$

Et au début de cette preuve, on a vu que :

$$\sum_{v\leq p<z}g(p)^2=\mathcal{O}\left(\frac{1}{\log v}\right). \tag{2.46}$$

Enfin, il est connu que :

$$\sum_{v\leq p<z}\frac{1}{p^2}=\mathcal{O}\left(\frac{1}{\log v}\right). \tag{2.47}$$

Donc, en combinant 2.45, 2.46 et 2.47 dans 2.44, on a

$$\prod_{v\leq p<z}\left(1+\frac{g(p)}{p^s}\right)\left(1-\frac{1}{p^{s+1}}\right)^{\kappa}=\exp\left(\mathcal{O}\left(\frac{1}{\log v}\right)\right)=1+\mathcal{O}\left(\frac{1}{\log v}\right).$$

Ceci démontre 2.39.

Passons à 2.40. Le résultat 2.39 que l'on vient de démontrer nous dit que, dans le cas $s=0$,

$$\prod_{v\leq p<z}(1+g(p))(1-\frac{1}{p})^{\kappa}=1+\mathcal{O}\left(\frac{1}{\log v}\right).$$

D'autre part, on réutilise $W(z)=\prod_{p<z}(1-\frac{1}{p})$ introduit dans le Lemme 9. Un calcul très rapide nous montre que :

$$\prod_{v\leq p<z}(1+g(p))(1-\frac{1}{p})^{\kappa}=\frac{V(v)}{V(z)}\frac{W(z)^{\kappa}}{W(v)^{\kappa}}.$$

Donc

$$\frac{V(v)}{V(z)}=\frac{W(z)^{\kappa}}{W(v)^{\kappa}}\left(1+\mathcal{O}\left(\frac{1}{\log v}\right)\right).$$

Ainsi, par le Lemme 9, on trouve

$$\frac{V(v)}{V(z)}=\left(\frac{\log z}{\log v}\right)^{\kappa}\left(1+\mathcal{O}\left(\frac{1}{\log v}\right)\right).$$

Ceci démontre 2.40.

Passons à 2.41. On utilise encore une fois 2.39 :

$$\prod_{v\leq p<z}(1+g(p))(1-\frac{1}{p})^{\kappa}=1+\mathcal{O}\left(\frac{1}{\log v}\right),$$

sauf que maintenant, on fait $z\to+\infty$:

$$\prod_{p\geq v}(1+g(p))(1-\frac{1}{p})^{\kappa}=1+\mathcal{O}\left(\frac{1}{\log v}\right),$$

et on écrit z à la place de v :

$$\prod_{p\geq z}(1+g(p))(1-\frac{1}{p})^{\kappa}=1+\mathcal{O}\left(\frac{1}{\log z}\right),$$

puis on utilise, par 2.4, $1+g(p)=\left(1-\frac{\omega(p)}{p}\right)^{-1}$:

$$\prod_{p\geq z}\left(1-\frac{\omega(p)}{p}\right)^{-1}(1-\frac{1}{p})^{\kappa}=1+\mathcal{O}\left(\frac{1}{\log z}\right).$$

Ainsi, par définitions de V et W :

$$\begin{aligned}
V(z) &= \prod_{p<z}\left(1-\frac{\omega(p)}{p}\right)\\
&= \prod_{p<z}\left(1-\frac{\omega(p)}{p}\right)\prod_{p\geq z}\left(1-\frac{\omega(p)}{p}\right)(1-\frac{1}{p})^{-\kappa}\prod_{p\geq z}\left(1-\frac{\omega(p)}{p}\right)^{-1}(1-\frac{1}{p})^{\kappa}\\
&= \prod_{p<z}\left(1-\frac{\omega(p)}{p}\right)\prod_{p\geq z}\left(1-\frac{\omega(p)}{p}\right)(1-\frac{1}{p})^{-\kappa}\left\{1+\mathcal{O}\left(\frac{1}{\log z}\right)\right\}\\
&= \prod_{p}\left(1-\frac{\omega(p)}{p}\right)(1-\frac{1}{p})^{-\kappa}\prod_{p<z}(1-\frac{1}{p})^{\kappa}\left\{1+\mathcal{O}\left(\frac{1}{\log z}\right)\right\}\\
&= \left(\prod_{p}\left(1-\frac{\omega(p)}{p}\right)(1-\frac{1}{p})^{-\kappa}\right)W(z)^{\kappa}\left\{1+\mathcal{O}\left(\frac{1}{\log z}\right)\right\}. \qquad (2.48)
\end{aligned}$$

Au tout début de la démonstration du Lemme 9, on a utilisé le résultat 2.26 suivant :

$$\prod_{p<z}(1-\frac{1}{p})=\frac{e^{-\gamma}}{\log z}\left\{1+\mathcal{O}\left(\frac{1}{\log z}\right)\right\}.$$

On le réutilise ici, en remarquant qu'il implique :

$$W(z)^{\kappa}=\frac{e^{-\kappa\gamma}}{(\log z)^{\kappa}}\left\{1+\mathcal{O}\left(\frac{1}{\log z}\right)\right\}.$$

Ainsi, par 2.48 :

$$V(z) = \left(\prod_p \left(1 - \frac{\omega(p)}{p}\right) (1 - \frac{1}{p})^{-\kappa} \right) \frac{e^{-\kappa\gamma}}{(\log z)^\kappa} \left\{ 1 + \mathcal{O}\left(\frac{1}{\log z}\right) \right\}.$$

Ceci démontre 2.41.

Reste finalement à montrer la remarque qui porte sur le produit $\prod_p \left(1 - \frac{\omega(p)}{p}\right) (1 - \frac{1}{p})^{-\kappa}$. Pour cela, on débute avec l'inégalité évidente suivante :

$$\prod_{p<z} (1 + g(p))(1 - \frac{1}{p})^\kappa \leq \exp\left\{ \sum_{p<z} g(p) - \kappa \sum_{p<z} \frac{1}{p} \right\}.$$

D'autre part, dans la démonstration du Lemme 10, on avait prouvé que :

$$\sum_{v \leq p < z} g(p) \leq \kappa \log \frac{\log z}{\log v} + \frac{A_2}{\log v} + \frac{A_1 A_2}{\log v} \left\{ \kappa + \frac{A_2}{\log v} \right\}.$$

On prend $v = e$ dans cette inégalité, pour obtenir

$$\sum_{e \leq p < z} g(p) \leq \kappa \log\log z + A_2 + A_1 A_2 (\kappa + A_2),$$

donc

$$\sum_{p<z} g(p) \leq g(2) + \kappa \log\log z + A_2 + A_1 A_2 (\kappa + A_2).$$

Or, par l'hypothèse (2.2), et comme $1 + g(p) = \frac{1}{1 - \frac{\omega(p)}{p}}$, on a $g(2) \leq A_1 - 1$.
D'autre part, on sait que :

$$\sum_{p<z} \frac{1}{p} > \log\log z.$$

Ainsi

$$\sum_{p<z} g(p) - \kappa \sum_{p<z} \frac{1}{p} \leq A_1 - 1 + A_2 + A_1 A_2 (\kappa + A_2) \leq A_1 A_2 (1 + \kappa + A_2).$$

Donc

$$\prod_{p<z} (1 + g(p))(1 - \frac{1}{p})^\kappa \leq \exp\{A_1 A_2 (1 + \kappa + A_2)\},$$

c'est-à-dire

$$\prod_{p<z}\left(1-\frac{\omega(p)}{p}\right)^{-1}(1-\frac{1}{p})^{\kappa}\leq\exp\{A_1A_2(1+\kappa+A_2)\}.$$

On fait $z\to+\infty$, pour trouver

$$\prod_{p}\left(1-\frac{\omega(p)}{p}\right)^{-1}(1-\frac{1}{p})^{\kappa}\leq\exp\{A_1A_2(1+\kappa+A_2)\}.$$

Ceci achève la démonstration du lemme.

□

Et enfin, pour terminer cette série de lemmes, nous nous attaquons à la délicate fonction $G(z)=\sum_{\substack{d<z\\ d|P(z)}}g(d)$:

Lemme 12. *Pour tout $z\geq 2$, on a*

$$\frac{1}{G(z)}=\mathcal{O}(V(z)). \tag{2.49}$$

et aussi

$$G(z)\log z=(\kappa+1)\sum_{\substack{d<z\\ d|P(z)}}g(d)\log d+\mathcal{O}(G(z)). \tag{2.50}$$

De 2.49 et 2.50, il découle

$$\frac{1}{G(z)}=V(z)e^{\gamma\kappa}\Gamma(\kappa+1)\left\{1+\mathcal{O}\left(\frac{1}{\log z}\right)\right\}. \tag{2.51}$$

Preuve. Commençons par montrer 2.49. L'hypothèse (2.24) dit que, pour tout $v\in[2,z]$:

$$\sum_{v\leq p<z}\frac{\omega(p)\log p}{p}\leq\kappa\log\frac{z}{v}+A_2.$$

Donc

$$\begin{aligned}\sum_{p<z}\frac{\omega(p)}{p}\log^n p &= \int_2^z\sum_{t\leq p<z}\frac{\omega(p)\log p}{p}\mathrm{d}(\log^{n-1}t)\\ &\leq \int_1^z\left(\kappa\log\frac{z}{t}+A_2\right)\mathrm{d}(\log^{n-1}t)\end{aligned}$$

$$
\begin{aligned}
&= (\kappa \log z + A_2)\log^{n-1} z - \kappa \frac{n-1}{n}\log^n z \\
&= \frac{\kappa}{n}\log^n z + A_2 \log^{n-1} z, \qquad (2.52)
\end{aligned}
$$

ceci étant vrai pour $n \geq 1$. Maintenant, on va introduire une astuce de calcul, et utiliser à la fois 2.20 et 2.3 :

$$
\begin{aligned}
\frac{1}{V(z)} - G(z) &= \sum_{d|P(z)} g(d) - \sum_{\substack{d<z \\ d|P(z)}} g(d) \\
&= \sum_{\substack{d\geq z \\ d|P(z)}} g(d) \\
&\leq \sum_{\substack{d\geq z \\ d|P(z)}} g(d)\left(\frac{d}{z}\right)^{\frac{1}{\log z}} \\
&\leq z^{-\frac{1}{\log z}} \sum_{d|P(z)} g(d) d^{\frac{1}{\log z}} \\
&= e^{-1}\prod_{p<z}\left(1 + g(p)p^{\frac{1}{\log z}}\right),
\end{aligned}
$$

la dernière ligne s'obtenant par multiplicité de $n \mapsto g(n)n^{\frac{1}{\log z}}$. Donc, en multipliant par $V(z) = \prod_{p<z}(1 - \frac{\omega(p)}{p})$:

$$
1 - V(z)G(z) \leq e^{-1}\prod_{p<z}\left(1 + g(p)p^{\frac{1}{\log z}}\right)\left(1 - \frac{\omega(p)}{p}\right). \qquad (2.53)
$$

Or, par définition de g en 2.4, on a :

$$
\begin{aligned}
\left(1 + g(p)p^{\frac{1}{\log z}}\right)\left(1 - \frac{\omega(p)}{p}\right) &= \left(1 + \frac{\omega(p)}{p-\omega(p)}p^{\frac{1}{\log z}}\right)\left(1 - \frac{\omega(p)}{p}\right) \\
&= 1 + \frac{\omega(p)}{p-\omega(p)}p^{\frac{1}{\log z}} - \frac{\omega(p)}{p} - \frac{\omega(p)^2}{p-\omega(p)}p^{\frac{1}{\log z}-1} \\
&= 1 - \frac{\omega(p)}{p} + \frac{\omega(p)p^{\frac{1}{\log z}-1}(p-\omega(p)}{p-\omega(p)} \\
&= 1 - \frac{\omega(p)}{p} + \frac{\omega(p)}{p^{1-\frac{1}{\log z}}}.
\end{aligned}
$$

D'où, en remplaçant dans 2.53 :

$$\begin{aligned} 1 - V(z)G(z) &\leq e^{-1} \prod_{p<z} \left(1 - \frac{\omega(p)}{p} + \frac{\omega(p)}{p^{1-\frac{1}{\log z}}}\right) \\ &\leq \exp\left\{-1 + \sum_{p<z} \omega(p) \left(\frac{1}{p^{1-\frac{1}{\log z}}} - \frac{1}{p}\right)\right\}. \end{aligned} \tag{2.54}$$

On utilise maintenant l'inégalité 2.52 pour trouver :

$$\begin{aligned} \sum_{p<z} \omega(p) \left(\frac{1}{p^{1-\frac{1}{\log z}}} - \frac{1}{p}\right) &= \sum_{n=1}^{\infty} \frac{\log^{-n} z}{n!} \sum_{p<z} \frac{\omega(p)}{p} \log^n p \\ &\leq \sum_{n=1}^{\infty} \frac{1}{n!} \left(\frac{\kappa}{n} + \frac{A_2}{\log z}\right) \\ &\leq \kappa \sum_{n=1}^{\infty} \frac{1}{n.n!} + \frac{A_2}{\log 2} e \\ &\leq 2\kappa \sum_{n=1}^{\infty} \frac{1}{n!} + \frac{A_2}{\log 2} e \\ &= 2\kappa e + \frac{A_2}{\log 2} e. \end{aligned}$$

Donc, en remplaçant dans 2.54 :

$$1 - V(z)G(z) \leq \exp\left\{-1 + 2\kappa e + \frac{A_2}{\log 2} e\right\} = \mathcal{O}(1).$$

Ainsi $\frac{1}{G(z)} = \mathcal{O}(V(z))$. Ceci prouve clairement 2.49.

Nous allons maintenant passer à la preuve de 2.50. Introduisons les fonctions :

$$G(x, z) = \sum_{\substack{d<x \\ d|P(z)}} g(d)$$

et

$$G_p(x, z) = \sum_{\substack{d<x \\ d|P(z) \\ (d,p)=1}} g(d), \tag{2.55}$$

où p est diviseur premier de $P(z)$. Avec ce même p, on a :

$$\begin{aligned} G(x,z) &= \sum_{\substack{d<x\\ d|P(z)\\ (d,p)=1}} g(d) + \sum_{\substack{d'<x\\ d'|P(z)\\ (d',p)=p}} g(d') \\ &= \sum_{\substack{d<x\\ d|P(z)\\ (d,p)=1}} g(d) + \sum_{\substack{m<x/p\\ m|P(z)\\ (m,p)=1}} g(pm) \\ &= \sum_{\substack{d<x\\ d|P(z)\\ (d,p)=1}} g(d) + g(p) \sum_{\substack{m<x/p\\ m|P(z)\\ (m,p)=1}} g(m) \\ &= G_p(x,z) + g(p) G_p(x/p,z), \end{aligned}$$

en ayant fait le changement de variable $d' = pm$, possible car $(d',p) = p \Rightarrow p|d'$. On multiplie par $1-\frac{\omega(p)}{p}$ en utilisant, par 2.4, le fait que $g(p)\left(1-\frac{\omega(p)}{p}\right) = \frac{\omega(p)}{p}$:

$$\begin{aligned} \left(1-\frac{\omega(p)}{p}\right) G(x,z) &= G_p(x,z) - \frac{\omega(p)}{p} G_p(x,z) + \frac{\omega(p)}{p} G_p(x/p,z) \\ &= G_p(x,z) - \frac{\omega(p)}{p}\left(G_p(x,z) - G_p(x/p,z)\right). \end{aligned}$$

Donc

$$G_p(x,z) = \left(1-\frac{\omega(p)}{p}\right) G(x,z) + \frac{\omega(p)}{p}\left(G_p(x,z) - G_p(x/p,z)\right).$$

On remplace x par x/p :

$$G_p(x/p,z) = \left(1-\frac{\omega(p)}{p}\right) G(x/p,z) + \frac{\omega(p)}{p}\left(G_p(x/p,z) - G_p(x/p^2,z)\right). \tag{2.56}$$

Remarquons, en y faisant le changement de variable $d = pm$, que :

$$\sum_{\substack{d<x\\ d|P(z)}} g(d)\log d = \sum_{\substack{d<x\\ d|P(z)}} g(d) \sum_{p|d} \log p$$

$$= \sum_{p<z} g(p)\log p \sum_{\substack{m<x/p \\ m|P(z) \\ (m,p)=1}} g(m).$$

Maintenant, on combine cette égalité avec 2.55 et 2.56 pour avoir :

$$\begin{aligned}
\sum_{\substack{d<x \\ d|P(z)}} g(d)\log d &= \sum_{p<z} g(p)\log(p) G_p(x/p,z) \\
&= \sum_{p<z} g(p)\left(1-\frac{\omega(p)}{p}\right)\log(p) G(x/p,z) \\
&\quad + \sum_{p<z} g(p)\log(p)\frac{\omega(p)}{p}\left(G_p(x/p,z) - G_p(x/p^2,z)\right) \\
&= \sum_{p<z}\frac{\omega(p)}{p}\log p \sum_{\substack{d<x/p \\ d|P(z)}} g(d) + \sum_{p<z}\frac{g(p)\omega(p)}{p}\log p \sum_{\substack{x/p^2\le d<x/p \\ d|P(z) \\ (d,p)=1}} g(d) \\
&= \sum_{\substack{d<x \\ d|P(z)}} g(d) \sum_{p<min(x/d,z)} \frac{\omega(p)}{p}\log p \\
&\quad + \sum_{\substack{x/z^2\le d<x \\ d|P(z)}} g(d) \sum_{\substack{\sqrt{x/d}\le p<min(x/d,z) \\ (p,d)=1}} \frac{g(p)\omega(p)}{p}\log p \\
&= \sum_{\substack{d<x/z \\ d|P(z)}} g(d)\sum_{p<z}\frac{\omega(p)}{p}\log p + \sum_{\substack{x/d\le d<x \\ d|P(z)}} g(d)\sum_{p<x/d}\frac{\omega(p)}{p}\log p \\
&\quad + \sum_{\substack{x/z^2\le d<x \\ d|P(z)}} g(d) \sum_{\substack{\sqrt{x/d}\le p<min(x/d,z) \\ (p,d)=1}} \frac{g(p)\omega(p)}{p}\log p.
\end{aligned}$$

On pose $x = z$, ce qui fait disparaître la première somme à droite :

$$\sum_{\substack{d<z \\ d|P(z)}} g(d)\log d = \sum_{\substack{z/d\le d<z \\ d|P(z)}} g(d)\sum_{p<z/d}\frac{\omega(p)}{p}\log p + \sum_{\substack{d<z \\ d|P(z)}} g(d) \sum_{\substack{\sqrt{z/d}\le p<z/d \\ (p,d)=1}} \frac{g(p)\omega(p)}{p}\log p. \tag{2.57}$$

D'une part, l'hypothèse (2.24) nous dit que :

$$\sum_{p<y} \frac{\omega(p)}{p} \log p = \kappa \log y + \mathcal{O}(1).$$

donc ici, avec $y = z/d$, on a

$$\sum_{p<z/d} \frac{\omega(p)}{p} \log p = \kappa \log \frac{z}{d} + \mathcal{O}(1). \tag{2.58}$$

D'autre part, par le 2.36 de la preuve du Lemme 10, on a :

$$\sum_{v\leq p<y} g(p) \leq \kappa \log \frac{\log y}{\log v} + \mathcal{O}\left(\frac{1}{\log v}\right),$$

donc ici, avec $v = \sqrt{z/d}$ et $y = z/d$, on a

$$\sum_{\sqrt{z/d}\leq p<z/d} g(p) \leq \kappa \log \frac{\log\left(z/d\right)}{\log \sqrt{z/d}} + \mathcal{O}\left(\frac{1}{\log \sqrt{z/d}}\right) = \mathcal{O}(1),$$

et le 2.33 de la preuve du Lemme 10 dit que :

$$\frac{\omega(p)}{p} \log p \leq A_2,$$

donc

$$\sum_{\substack{\sqrt{z/d}\leq p<z/d \\ (p,d)=1}} \frac{g(p)\omega(p)}{p} \log p = \mathcal{O}\left(\sum_{\sqrt{z/d}\leq p<z/d} g(p)\right) = \mathcal{O}(1). \tag{2.59}$$

On en conclut, en injectant 2.58 et 2.59 à 2.57, que :

$$\sum_{\substack{d<z \\ d|P(z)}} g(d) \log d = \sum_{\substack{z/d\leq d<z \\ d|P(z)}} g(d) \left(\kappa \log \frac{z}{d} + \mathcal{O}(1)\right) + \left(\sum_{\substack{d<z \\ d|P(z)}} g(d)\right) \mathcal{O}(1),$$

donc, par définition de G en 2.3, on a :

$$\sum_{\substack{d<z \\ d|P(z)}} g(d) \log d \;\; = \sum_{\substack{z/d\leq d<z \\ d|P(z)}} g(d) \left(\kappa \log \frac{z}{d} + \mathcal{O}(1)\right) + \mathcal{O}(G(z))$$

$$
\begin{aligned}
&= \kappa \sum_{\substack{d<z \\ d|P(z)}} g(d) \log \frac{z}{d} + \mathcal{O}(G(z)) \\
&= \kappa \sum_{\substack{d<z \\ d|P(z)}} g(d) \log z - \kappa \sum_{\substack{d<z \\ d|P(z)}} g(d) \log d + \mathcal{O}(G(z)).
\end{aligned}
$$

Donc

$$
G(z) \log z = (\kappa + 1) \sum_{\substack{d<z \\ d|P(z)}} g(d) \log d + \mathcal{O}(G(z)).
$$

Ceci prouve 2.50.

Grâce à 2.49 et 2.50, on peut démontrer 2.51. Écrivons $\mathcal{O}(G(z)) = G(z) \log(z) r(z)$ où $r(z) = \mathcal{O}\left(\frac{1}{\log z}\right)$. Posons également $T(z) = \sum_{\substack{d<z \\ d|P(z)}} g(d) \log d$. Ainsi, par 2.50, on a :

$$
G(z) = \frac{\kappa + 1}{\log z} T(z) + G(z) r(z),
$$

donc

$$
G(z)(1 - r(z)) = \frac{\kappa + 1}{\log z} T(z),
$$

et donc

$$
G(z) = \frac{1}{1 - r(z)} \frac{\kappa + 1}{\log z} T(z). \tag{2.60}
$$

Par définition de r, on peut supposer $|r(y)| \leq \frac{1}{2}$ dès que $y \geq z$ car $z \geq 2$, en particulier $|r(z)| \leq \frac{1}{2}$ donc $1 - r(z) > 0$. On pose maintenant :

$$
E(y) := \log \left\{ \frac{\kappa + 1}{\log^{\kappa+1} y} T(y) \right\}. \tag{2.61}
$$

Ainsi

$$
E(y) = \log(\kappa + 1) - (\kappa + 1) \log \log y + \log(T(y)).
$$

On a, dès que $y \geq z$, par définition de T et par 2.60, et comme $r(y) = \mathcal{O}\left(\frac{1}{\log y}\right)$:

$$
E'(y) = -\frac{\kappa + 1}{y \log y} + \frac{T'(y)}{T(y)}
$$

$$
\begin{aligned}
&= -\frac{\kappa+1}{y\log y} + \frac{G(y)}{yT(y)} \\
&= -\frac{\kappa+1}{y\log y} + \frac{1}{1-r(y)}\frac{\kappa+1}{y\log y} \\
&= \frac{\kappa+1}{y\log y}\frac{r(y)}{1-r(y)} \\
&= \mathcal{O}\left(\frac{1}{y\log^2 y}\right).
\end{aligned}
$$

Et donc

$$\int_z^\infty E'(y)\mathrm{d}y < \infty.$$

D'où, par 2.61, l'existence d'une constante λ (indépendante de z) telle que :

$$\frac{\kappa+1}{\log^{\kappa+1} z}T(z) = \exp E(z) = \lambda \exp\left\{-\int_z^\infty E'(y)\mathrm{d}y\right\} = \lambda\left\{1+\mathcal{O}\left(\frac{1}{\log z}\right)\right\}.$$

Ainsi

$$T(z) = \frac{\lambda}{\kappa+1}\log^{\kappa+1} z\left\{1+\mathcal{O}\left(\frac{1}{\log z}\right)\right\}. \tag{2.62}$$

Et de plus, comme $r(z) = \mathcal{O}\left(\frac{1}{\log z}\right)$:

$$\frac{1}{1-r(z)} = 1 + \frac{r(z)}{1-r(z)} = 1+\mathcal{O}\left(\frac{1}{\log z}\right). \tag{2.63}$$

Donc, en combinant 2.60, 2.62 et 2.63 :

$$G(z) = \frac{1}{1-r(z)}\frac{\kappa+1}{\log z}T(z) = \lambda\log^\kappa z\left\{1+\mathcal{O}\left(\frac{1}{\log z}\right)\right\}. \tag{2.64}$$

Il ne reste plus que le problème de l'évaluation de λ. Pour cela, on utilise les deux formules suivantes qu'il est aisé de démontrer (où $l>0$ et $s>0$, et où Γ est la fonction Gamma d'Euler) en rappelant 2.3 et 2.4 :

$$\int_1^\infty \frac{\log^{l-1} y}{y^{s+1}}\mathrm{d}y = \frac{1}{s^l}\int_0^\infty e^{-t}t^{l-1}\mathrm{d}t = \frac{\Gamma(l)}{s^l}, \tag{2.65}$$

et

$$\prod_p \left(1+\frac{g(p)}{p^s}\right) = \sum_{d=1}^{\infty} \frac{\mu^2(d)g(d)}{d^s} = s\int_0^{\infty} \frac{G(y)}{y^{s+1}}\mathrm{d}y. \tag{2.66}$$

Soit $y \geq 2$. On combine 2.64, 2.65 et 2.66 :

$$\begin{aligned}\prod_p \left(1+\frac{g(p)}{p^s}\right) &= s\int_1^{\infty} \frac{\lambda \log^{\kappa} y + \mathcal{O}(\log^{\kappa-1} y)}{y^{s+1}}\mathrm{d}y \\ &= \lambda\frac{\Gamma(\kappa+1)}{s^{\kappa}} + \mathcal{O}\left(\frac{1}{s^{\kappa-1}}\right),\end{aligned}$$

et ainsi

$$\lambda = \frac{1}{\Gamma(\kappa+1)} \lim_{s\to 0^+} s^{\kappa} \prod_p \left(1+\frac{g(p)}{p^s}\right). \tag{2.67}$$

Maintenant, utilisons la fonction ζ de Riemann (pour $u > 1$) :

$$\zeta(u) = \prod_p \left(1-\frac{1}{p^u}\right)^{-1}.$$

On sait que :

$$\lim_{s\to 0^+} s\zeta(s+1) = 1,$$

et donc

$$s^{\kappa} \sim \zeta^{-\kappa}(s+1) \text{ quand } s \to 0^+.$$

Ainsi, en remplaçant dans 2.67, et en utilisant la définition 2.4 de g :

$$\begin{aligned}\lambda &= \frac{1}{\Gamma(\kappa+1)} \lim_{s\to 0^+} \zeta^{-\kappa}(s+1) \prod_p \left(1+\frac{g(p)}{p^s}\right) \\ &= \frac{1}{\Gamma(\kappa+1)} \lim_{s\to 0^+} \prod_p \left(1-\frac{1}{p^{s+1}}\right)^{\kappa} \left(1+\frac{g(p)}{p^s}\right) \\ &= \frac{1}{\Gamma(\kappa+1)} \prod_p \left(1-\frac{1}{p}\right)^{\kappa} (1+g(p)) \\ &= \frac{1}{\Gamma(\kappa+1)} \prod_p \left(1-\frac{1}{p}\right)^{\kappa} \left(1+\frac{\omega(p)}{p}\right)^{-1}.\end{aligned}$$

D'où, par 2.64 :

$$G(z) = \frac{1}{\Gamma(\kappa+1)} \prod_p \left(1-\frac{1}{p}\right)^{\kappa} \left(1+\frac{\omega(p)}{p}\right)^{-1} \log^{\kappa} z \left\{1+\mathcal{O}\left(\frac{1}{\log z}\right)\right\}.$$

Donc, en utilisant le point 2.42 du Lemme 11, on a :

$$\frac{1}{G(z)} = V(z)e^{\gamma\kappa}\Gamma(\kappa+1)\left\{1+\mathcal{O}\left(\frac{1}{\log z}\right)\right\}.$$

Ceci conclut la preuve du Lemme 12.

□

Nous pouvons maintenant démontrer très rapidement le Théorème 8. En effet, grâce au Théorème 4 et au premier résultat du Lemme 12, on obtient immédiatement que :

$$S(\mathcal{A},\mathcal{P},z) \leq XV(z)e^{\gamma\kappa}\Gamma(\kappa+1)\left(1+\mathcal{O}\left(\frac{1}{\log z}\right)\right) + \sum_{\substack{d<z^2\\ d|P(z)}} 3^{\nu(d)}|\mathcal{R}(\mathcal{A},d)|.$$

Nous allons à ce stade passer à une application du crible de Selberg.

2.4 Application

L'application qui suit, utilisant le Théorème 8 ci-avant du crible de Selberg, est intégralement un travail personnel, inspiré d'aucun ouvrage ni d'aucun cours. Il est à préciser qu'une version différente de cette application existe, par Nathanson [7], qui n'utilise que le Théorème 4, plus faible que le 8. Le choix a été fait ici d'utiliser le Théorème 8 pour mieux appréhender d'un point de vue personnel le crible de Selberg, mais aussi parce que cette méthode paraissait fortement intéressante.

Nous allons utiliser le crible de Selberg, à savoir le Théorème 8, pour démontrer le Théorème C, que l'on rappelle encore une fois ici :

$$\sum_{N\leq x} r(N)^2 \ll \frac{x^3}{(\log x)^4},$$

où $r(N)$ désigne le nombre de représentations de N comme somme de deux nombres premiers (où par exemple 5+7 et 7+5 comptent comme deux représentations différentes).

En fait, nous nous intéressons à $r(N)$ seul, qui s'écrit

$$r(N) = \sum_{\substack{p,q \leq N \\ p+q=N}} 1,$$

ou bien, en notant $\mathbb{P}$ l'ensemble des nombres premiers,

$$r(N) = \sum_{\substack{p \leq N \\ N-p \in \mathbb{P}}} 1.$$

On cherche ainsi à majorer $|\{p \leq N : N - p \in \mathbb{P}\}|$. Pour cela, on fixe x que l'on peut choisir assez grand, et on pose $z = \frac{\sqrt{x}}{(\log x)^4}$. En choisissant justement x assez grand, on suppose $2z < x$. On écrit alors :

$$\sum_{N \leq x} r(N)^2 = \sum_{\substack{N \leq x \\ N \equiv 1[2]}} r(N)^2 + \sum_{\substack{2z \leq N \leq x \\ N \equiv 0[2]}} r(N)^2 + \sum_{\substack{N < 2z \\ N \equiv 0[2]}} r(N)^2. \tag{2.68}$$

On va ainsi naturellement étudier 3 cas selon les valeurs que prend N entier naturel dans la sommation.

Cas 1 : N est impair et $N \leq x$.

Le seul moyen de décomposer N en deux nombres premiers serait d'écrire $N = 2 + (N-2)$ quand $N - 2$ est premier, et donc $r(N) \leq 2$. Ainsi

$$\begin{aligned} \sum_{\substack{N \leq x \\ N \equiv 1[2]}} r(N)^2 &\leq \sum_{\substack{N \leq x \\ N \equiv 1[2]}} 4 \\ &\leq 4x \\ &\ll \frac{x^3}{(\log x)^4}. \end{aligned}$$

Cas 2 : N est pair et $N < 2z$.

Comme $r(N)^2 \leq N^2$, on a $r(N)^2 < 4z^2 = \frac{4x}{(\log x)^8}$, donc

$$\begin{aligned}
\sum_{\substack{N<2z\\N\equiv 0[2]}} r(N)^2 &< \sum_{\substack{N<2z\\N\equiv 0[2]}} \frac{4x}{(\log x)^8} \\
&= \frac{4x}{(\log x)^8} \sum_{\substack{N<2z\\N\equiv 0[2]}} 1 \\
&\leq \frac{4x}{(\log x)^8} 2z \\
&= \frac{8x^{\frac{3}{2}}}{(\log x)^{12}} \\
&\ll \frac{x^3}{(\log x)^4}.
\end{aligned}$$

Cas 3 : N est pair et $2z \leq N \leq x$.

C'est ici que l'on utilise le crible de Selberg. On note $\mathcal{A} = \{n(N-n) : 0 \leq n \leq N\}$. Ce sera le $\mathcal{A}$ utilisé dans le crible. On considérera que $\mathcal{P} = \mathbb{P}$. Vérifions l'hypothèse (2.1) sur $|\mathcal{A}_d|$ pour d sans facteur carré :

$$\begin{aligned}
|\mathcal{A}_d| &= \sum_{\substack{a\in\mathcal{A}\\a\equiv 0[d]}} 1 \\
&= \sum_{\substack{0\leq n\leq N\\n(N-n)\equiv 0[d]}} 1 \\
&= \sum_{\substack{0\leq u<d\\u(N-u)\equiv 0[d]}} \sum_{\substack{0\leq n\leq N\\n\equiv u[d]}} 1 \\
&= \sum_{\substack{0\leq u<d\\u(N-u)\equiv 0[d]}} \lfloor \frac{N}{d} \rfloor \\
&= \sum_{\substack{0\leq u<d\\u(N-u)\equiv 0[d]}} (\frac{N}{d} + \{\frac{N}{d}\}).
\end{aligned}$$

On note maintenant $\omega(d) = |\{0 \leq u < d : u(N-u) \equiv 0[d]\}|$. On a ainsi

$$|\mathcal{A}_d| = \omega(d)(\frac{N}{d} + \{\frac{N}{d}\})$$

$$= \quad N\frac{\omega(d)}{d} + \{\frac{N}{d}\}\omega(d).$$

Il reste à noter $\mathcal{R}(\mathcal{A}, d) = \{\frac{N}{d}\}\omega(d)$ pour avoir

$$|\mathcal{A}_d| = N\frac{\omega(d)}{d} + \mathcal{R}(\mathcal{A}, d).$$

On étend ω aux entiers n avec facteurs carrés en posant $\omega(n) = 0$. Le théorème des restes chinois nous indique de manière évidente que ω est multiplicative. D'autre part, on a $|\mathcal{R}(\mathcal{A}, d)| \leq \omega(d)$. Ce « reste » est donc facilement majorable. On a bien toutes les conditions de l'hypothèse (2.1).

Vérifions maintenant l'hypothèse (2.2). Soit p premier. On veut compter le nombre d'éléments dans $\{0 \leq u < p : u(N-u) \equiv 0[p]\}$ pour estimer $\omega(p)$. Il est clair que si $N \equiv 0[p]$, alors seul 0 est dans cet ensemble. Et sinon, on a deux éléments dans l'ensemble, à savoir 0 et le représentant de N modulo p dans $[\![0, p-1]\!]$. Ceci nous pose problème en $p = 2$ avec N impair. Comme on a supposé N pair, on a

$$\omega(p) = \begin{cases} 1 & \text{si } p = 2 \\ 2 & \text{sinon} \end{cases}$$

Donc

$$0 \leq \frac{\omega(p)}{p} \leq \max\left(\frac{1}{2}, \frac{2}{3}\right) = \frac{2}{3} = 1 - \frac{1}{3}.$$

L'hypothèse (2.2) est bien vérifiée avec $A_1 = 3 > 1$.

Il nous reste enfin l'hypothèse (2.24) à vérifier. Pour cela, on utilise la formule de Mertens (déjà utilisée page 21) :

$$\sum_{p<y} \frac{\log p}{p} = \log y + \mathcal{O}(1).$$

Dans notre cas, on prend $v \in [2, z]$, et on estime :

$$\begin{aligned} \sum_{v \leq p < z} \frac{\omega(p)\log p}{p} &= \sum_{p<z} \frac{\omega(p)\log p}{p} - \sum_{p<v} \frac{\omega(p)\log p}{p} \\ &= \frac{\log 2}{2} + 2\sum_{2<p<z} \frac{\log p}{p} - \frac{\log 2}{2} - 2\sum_{2<p<v} \frac{\log p}{p} \end{aligned}$$

$$
\begin{aligned}
&= 2\left(\sum_{p<z}\frac{\log p}{p}-\sum_{p<v}\frac{\log p}{p}\right)\\
&= 2(\log z+\mathcal{O}(1))-2(\log v+\mathcal{O}(1))\\
&= 2\log\frac{z}{v}+\mathcal{O}(1).
\end{aligned}
$$

Ainsi, en prenant $\kappa = 2$ la dimension du crible, on a l'existence de $A_2 \geq 1$ indépendant de v et z tel que :

$$-A_2 \leq \sum_{v\leq p<z}\frac{\omega(p)\log p}{p}-\kappa\log\frac{z}{v}\leq A_2.$$

L'hypothèse (2.24) est bien vérifiée. On peut donc appliquer le Théorème 8 du crible de Selberg. On obtient que :

$$
\begin{aligned}
S(\mathcal{A},\mathcal{P},z) &\leq NV(z)e^{2\gamma}\Gamma(3)\left(1+\mathcal{O}\left(\frac{1}{\log z}\right)\right)+\sum_{\substack{d<z^2\\ d|P(z)}}3^{\nu(d)}|\mathcal{R}(\mathcal{A},d)|\\
&\leq xV(z)e^{2\gamma}\Gamma(3)\left(1+\mathcal{O}\left(\frac{1}{\log z}\right)\right)+\sum_{\substack{d<z^2\\ d|P(z)}}3^{\nu(d)}|\mathcal{R}(\mathcal{A},d)|,
\end{aligned}
$$

où, rappelons-le, $V(z)=\prod_{p<z}(1-\frac{\omega(p)}{p})$. Le point très important ici est que la constante implicite dans $\mathcal{O}\left(\frac{1}{\log z}\right)$ ne dépend pas de N pair, car on obtient ce $\mathcal{O}$ à partir de $G(z)$ (voir en plus la preuve du Lemme 12 pour les détails), et $G(z)$ est lui-même défini (voir 2.3) à partir de ω qui ne dépend pas de N pair comme on l'a vu ci-haut. De plus, $\Gamma(3) = 2$ et $e^{2\gamma} \simeq 3,17 \leq 4$, donc on a

$$S(\mathcal{A},\mathcal{P},z)\leq 8xV(z)\left(1+\mathcal{O}\left(\frac{1}{\log z}\right)\right)+\sum_{\substack{d<z^2\\ d|P(z)}}3^{\nu(d)}|\mathcal{R}(\mathcal{A},d)|.$$

Majorons tout d'abord $V(z)$. On a

$$
\begin{aligned}
V(z) &= \frac{1}{2}\prod_{2<p<z}(1-\frac{2}{p})\\
&\leq \frac{1}{2}\prod_{p<z}(1-\frac{1}{p})^2
\end{aligned}
$$

$$\ll \frac{1}{(\log z)^2}.$$

La constante implicite dans la dernière domination est clairement indépendante de N. D'autre part, $|\mathcal{R}(\mathcal{A}, d)| \leq \omega(d)$. Et comme ω est multiplicative et que $\omega(p) \leq 2$ pour tout p premier, on a $\omega(d) \leq 2^{\nu(d)}$ où $\nu(d)$ compte le nombre de facteurs premiers de d (on rappelle que d est sans facteur premier dans notre cas). Donc

$$\begin{aligned}
\sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\nu(d)}|\mathcal{R}(\mathcal{A}, d)| &\leq \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\nu(d)}\omega(d) \\
&\leq \sum_{\substack{d<z^2 \\ d|P(z)}} 6^{\nu(d)} \\
&\leq z^2 \sum_{d|P(z)} \frac{6^{\nu(d)}}{d} \\
&= z^2 \prod_{p<z}(1+\frac{6}{p}) \\
&\leq z^2 \prod_{p<z}(1+\frac{1}{p})^6 \\
&\ll z^2(\log z)^6.
\end{aligned}$$

La constante implicite dans la dernière domination est clairement indépendante de N. Ainsi, on obtient que

$$S(\mathcal{A}, \mathcal{P}, z) \ll 8\frac{x}{(\log z)^2} + z^2(\log z)^6.$$

Avec toutes les remarques faites auparavant, il est clair que la constante implicite dans cette domination est indépendante de N. On a choisi z en fonction de x, à savoir $z = \frac{\sqrt{x}}{(\log x)^4}$, de façon à avoir le plus petit majorant possible. On a $\log z = \frac{1}{2}\log x - 4\log\log x$, donc $\log z \sim \frac{1}{2}\log x$ et $z^2(\log z)^6 \sim \frac{1}{64}\frac{x}{(\log x)^2}$. Donc

$$S(\mathcal{A}, \mathcal{P}, z) \ll 8\frac{x}{\frac{1}{4}(\log x)^2} + \frac{1}{64}\frac{x}{(\log x)^2},$$

ce qui signifie

$$S(\mathcal{A}, \mathcal{P}, z) \ll \frac{x}{(\log x)^2}.$$

On s'intéresse au comportement de x en $+\infty$, donc on peut supposer $z < x$ comme on a posé $z = \frac{\sqrt{x}}{(\log x)^4}$. On a de plus imposé un contrôle sur N par le bas : on a fait l'hypothèse $N \geq 2z$. Ainsi $N - z \geq z$, et donc

$$\begin{aligned}
|\{p \leq N : N-p \in \mathbb{P}\}| &= \sum_{\substack{p \leq N \\ N-p \in \mathbb{P}}} 1 \\
&= \sum_{\substack{p \leq z \\ N-p \in \mathbb{P}}} 1 + \sum_{\substack{z < p \leq N-z \\ N-p \in \mathbb{P}}} 1 + \sum_{\substack{N-z < p \leq N \\ N-p \in \mathbb{P}}} 1 \\
&\leq z + (\sum_{\substack{z < p \leq N-z \\ N-p \in \mathbb{P}}} 1) + z \\
&= 2z + \sum_{\substack{z < p \leq N-z \\ N-p \in \mathbb{P}}} 1 \\
&= \frac{2\sqrt{x}}{(\log x)^4} + \sum_{\substack{z < p \leq N-z \\ N-p \in \mathbb{P}}} 1.
\end{aligned}$$

Rajoutons dans la dernière somme la propriété $\forall q, (q|p(N-p) \Rightarrow q \geq z)$, car avec $z < p \leq N - z$ tel que $N-p$ premier, si on a q premier tel que $q|p(N-p)$, alors soit $q = p$ et donc $q \geq z$, soit $q = N - p$ et donc $q \geq N - (N - z) = z$ (c'est tout l'intérêt du contrôle de N par le bas). Ainsi :

$$\begin{aligned}
|\{p \leq N : N-p \in \mathbb{P}\}| &\leq \frac{2\sqrt{x}}{(\log x)^4} + \sum_{\substack{z < p \leq N-z \\ N-p \in \mathbb{P} \\ \forall q, (q|p(N-p) \Rightarrow q \geq z)}} 1 \\
&\leq \frac{2\sqrt{x}}{(\log x)^4} + \sum_{\substack{z < p \leq N-z \\ \forall q, (q|p(N-p) \Rightarrow q \geq z)}} 1 \\
&\leq \frac{2\sqrt{x}}{(\log x)^4} + \sum_{\substack{z < n \leq N-z \\ \forall q, (q|n(N-n) \Rightarrow q \geq z)}} 1 \\
&\leq \frac{2\sqrt{x}}{(\log x)^4} + \sum_{\substack{n \leq N \\ \forall q, (q|n(N-n) \Rightarrow q \geq z)}} 1 \\
&= \frac{2\sqrt{x}}{(\log x)^4} + \sum_{\substack{a \in \mathcal{A} \\ \forall q, (q|a \Rightarrow q \geq z)}} 1
\end{aligned}$$

$$= \frac{2\sqrt{x}}{(\log x)^4} + S(\mathcal{A}, \mathcal{P}, z).$$

De plus, $\frac{2\sqrt{x}}{(\log x)^4} \ll \frac{x}{(\log x)^2}$ et $S(\mathcal{A}, \mathcal{P}, z) \ll \frac{x}{(\log x)^2}$, donc

$$|\{p \leq N : N - p \in \mathbb{P}\}| \ll \frac{x}{(\log x)^2}.$$

Le membre de gauche n'étant autre que $r(N)$, on a

$$r(N) \ll \frac{x}{(\log x)^2}.$$

On se rapproche fortement du résultat recherché, car alors

$$r(N)^2 \ll \frac{x^2}{(\log x)^4}.$$

Et on a vu que cette domination était indépendante de N. Donc il existe $c > 0$ une constante indépendante de N telle que :

$$r(N)^2 \leq c\frac{x^2}{(\log x)^4}.$$

On fait la somme sur les entiers pairs $2z \leq N \leq x$, pour obtenir

$$\begin{aligned}
\sum_{\substack{2z \leq N \leq x \\ N \equiv 0[2]}} r(N)^2 &\leq \sum_{\substack{2z \leq N \leq x \\ N \equiv 0[2]}} c\frac{x^2}{(\log x)^4} \\
&= c\frac{x^2}{(\log x)^4} \sum_{\substack{2z \leq N \leq x \\ N \equiv 0[2]}} 1 \\
&\leq c\frac{x^3}{(\log x)^4}.
\end{aligned}$$

Ainsi, on a

$$\sum_{\substack{2z \leq N \leq x \\ N \equiv 0[2]}} r(N)^2 \ll \frac{x^3}{(\log x)^4}.$$

Conclusion.

Donc on termine la preuve grâce aux 3 cas étudiés et à 2.68 :

$$\sum_{N \leq x} r(N)^2 \ll \frac{x^3}{(\log x)^4}.$$

Chapitre 3

Le théorème de Shnirel'man-Goldbach

En 1930, le mathématicien biélorusse Lev Shnirel'man démontre un puissant théorème, première véritable avancée sur la conjecture de Goldbach, après presque 200 ans. Ce théorème, à l'énoncé simple et court, est le Théorème A. Rappelons-le ici :

Théorème de Shnirel'man-Goldbach. *Tout entier supérieur ou égal à 2 est la somme d'un nombre borné de nombres premiers.*

Par la suite, nous reformulerons le théorème en :
Il existe un entier $M \geq 1$ tel que tout entier supérieur ou égal à 2 est la somme d'au plus M nombres premiers.

Le lien avec la conjecture de Goldbach est immédiat, car cette dernière dit que tout nombre pair supérieur ou égal à 4 est somme de deux nombres premiers. Il y a aussi un lien direct avec la conjecture de Goldbach faible, qui dit que tout nombre impair supérieur ou égal à 7 est somme de trois nombres premiers. De plus, la conjecture de Goldbach implique la conjecture de Goldbach faible [1]. Donc, comme 2 et 3 sont premiers, la conjecture de Goldbach implique $M = 3$ dans le théorème de Shnirel'man-Goldbach.

Réciproquement, ce théorème nous rapprocherait fortement des deux conjectures si l'on parvenait à réduire M jusqu'à 3 [2]. En tout cas, M ne peut

1. Car un nombre impair (≥ 7) peut s'écrire $N + 3$ avec N pair (≥ 4), et donc s'écrire $p + q + 3$ si N peut s'écrire $p + q$ avec p et q premiers.

2. Attention, avec $M = 3$, le théorème ne montre même pas la conjecture de Goldbach faible. En effet, les nombres premiers s'écrivent comme la somme d'un nombre premier (et $1 \leq 3$) mais pas forcément de trois. De même les nombres de la forme $p + 2$, p premier, s'écrivent comme la somme de deux nombres premiers (et $2 \leq 3$) mais pas forcément de trois.

descendre en dessous de 3 (le nombre 27, par exemple, n'est pas premier et ne peut pas s'écrire comme somme de deux nombres premiers, donc pour lui, $M \geq 3$).

Nous allons ici donner les étapes qui mènent à la démonstration du théorème de Shnirel'man-Goldbach, étapes largement inspirées des travaux de Nathanson [7]. Ces dernières font appel à plusieurs notions, dont la densité de Shnirel'man et les Théorèmes B et C démontrés aux chapitres précédents.

Soit $n \geq 2$. Notre but sera de trouver $M \geq 1$ indépendant de n tel que :

$$\exists k \leq M, \exists (p_1, \ldots, p_k) \in \mathcal{P}^k : n = p_1 + \cdots + p_k$$

Mais plus n est grand, plus il paraît difficile de trouver ces k nombres premiers, avec k borné par une constante, car les nombres premiers se raréfient. Ceci n'est pas grave, car si on n'arrive pas à écrire directement n comme somme de k nombres premiers, on peut essayer de l'écrire comme somme de k nombres qui s'écrivent eux-mêmes comme somme de deux nombres premiers, c'est-à-dire :

$$\exists k \leq M, \exists (p_{1,1}, p_{1,2}, \ldots, p_{k,1}, p_{k,2}) \in \mathcal{P}^{2k} : n = (p_{1,1} + p_{1,2}) + \cdots + (p_{k,1} + p_{k,2})$$

Pourquoi plutôt essayer de démontrer ce résultat ? Parce que l'ensemble des nombres qui s'écrivent comme somme de deux nombres premiers a l'air bien plus gros que l'ensemble des nombres premiers. Et même, la conjecture de Goldbach nous dit que tous les nombres pairs supérieurs ou égaux à 4 sont dans cet ensemble. De plus, pour se débarrasser du problème de vocabulaire entre « au plus M nombres » et « exactement M nombres », rajoutons 0 à l'ensemble. Notons donc :

$$\mathcal{A} = \{0\} \cup \{p + q : p, q \in \mathcal{P}\}$$

On aimerait montrer qu'il existe $M \geq 1$ indépendant de n tel que :

$$\exists (a_1, \ldots, a_M) \in \mathcal{A}^M : n = a_1 + \cdots + a_M$$

Pour cela, on aimerait montrer que $\mathcal{A}$ contient suffisamment d'entiers pour décomposer n. Pour traduire « suffisamment d'entiers », on va introduire la notion de densité de Shnirel'man.

Définition. Soit $\mathcal{B}$ un ensemble d'entiers. Pour tout réel x, soit $\mathcal{B}(x)$ le nombre d'éléments non nuls de $\mathcal{B}$ inférieurs ou égaux à x, c'est-à-dire,

$$\mathcal{B}(x) = \sum_{\substack{b\in\mathcal{B}\\ 1\leq b\leq x}} 1$$

La fonction $x \mapsto \mathcal{B}(x)$ est appelée *fonction de comptage* de l'ensemble $\mathcal{B}$.

Remarquons que pour $x > 0$, on a

$$0 \leq \mathcal{B}(x) \leq [x] \leq x$$

et donc

$$0 \leq \frac{\mathcal{B}(x)}{x} \leq 1$$

On définit alors la *densité de Shnirel'man* de $\mathcal{B}$, notée $\sigma(\mathcal{B})$, par

$$\sigma(\mathcal{B}) = \inf_{N\in\mathbb{N}^*} \frac{\mathcal{B}(N)}{N}$$

Si $1 \notin \mathcal{B}$, alors $\sigma(\mathcal{B}) = 0$ car $\mathcal{B}(1) = 0$.

Et pour tout $N \geq 1$, on a $\mathcal{B}(N) \geq \sigma(\mathcal{B})N$.

Enfin, il est clair que

$$0 \leq \sigma(\mathcal{B}) \leq 1$$

On peut voir σ comme une probabilité, en cela que c'est la plus faible probabilité d'obtenir un élément de $\mathcal{B}$ dans $[\![1, N]\!]$ parmi tous les $N \in \mathbb{N}^*$.

En fait, si la densité de Shnirel'man de $\mathcal{B}$ est strictement positive, cela signifie intuitivement que les éléments de $\mathcal{B}$ sont suffisamment présents partout. Ce fait est illustré à travers le théorème suivant :

Théorème 13. (Shnirel'man) *Soit $\mathcal{B}$ un ensemble d'entiers contenant 0 et vérifiant $\sigma(\mathcal{B}) > 0$. Alors il existe $K \geq 1$ tel que tout entier naturel s'écrit comme la somme de K éléments de $\mathcal{B}$.*

Pour démontrer ce théorème, on utilise le lemme suivant :

Lemme 14. *Soit $\mathcal{B}$ un ensemble d'entiers contenant 0 et vérifiant $\sigma(\mathcal{B}) \geq \frac{1}{2}$. Alors tout entier naturel s'écrit comme somme de deux éléments de $\mathcal{B}$.*

Preuve. Soit $\beta = \sigma(\mathcal{B})$. Soit $N \geq 0$. Si $N \in \mathcal{B}$, il est évidemment somme de 2 éléments de $\mathcal{B}$, car on a $N = 0 + N$ et $0 \in \mathcal{B}$. Supposons donc $N \notin \mathcal{B}$. On définit alors $\mathcal{B}_1$ et $\mathcal{B}_2$ par

$$\mathcal{B}_1 = \{N - b : b \in \mathcal{B}, 1 \leq b \leq N - 1\}$$

et

$$\mathcal{B}_2 = \{b : b \in \mathcal{B}, 1 \leq b \leq N-1\}$$

Comme $N \notin \mathcal{B}$, il est immédiat que $\mid \mathcal{B}_1 \mid = \mid \mathcal{B}_2 \mid = \mathcal{B}(N)$. Et donc

$$\mid \mathcal{B}_1 \mid + \mid \mathcal{B}_2 \mid = 2\mathcal{B}(N)$$

Or on sait que $\mathcal{B}(N) \geq \beta N$, donc $2\mathcal{B}(N) \geq 2\beta N \geq N$ car $\beta \geq \frac{1}{2}$. D'où

$$\mid \mathcal{B}_1 \mid + \mid \mathcal{B}_2 \mid \geq N$$

Et $\mathcal{B}_1$ et $\mathcal{B}_2$ sont tous deux dans $[\![1, N-1]\!]$, donc, par la principe des tiroirs, $\mathcal{B}_1 \cap \mathcal{B}_2 \neq \emptyset$. En effet, supposons par l'absurde que $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$. Alors :

$$\mid \mathcal{B}_1 \cup \mathcal{B}_2 \mid = \mid \mathcal{B}_1 \mid + \mid \mathcal{B}_2 \mid \geq N$$

Mais $\mathcal{B}_1 \cup \mathcal{B}_2 \in [\![1, N-1]\!]$, donc $\mid \mathcal{B}_1 \cup \mathcal{B}_2 \mid \leq N-1$. C'est absurde.

On a ainsi $N - b_1 = b_2$ pour un certain $(b_1, b_2) \in \mathcal{B}^2$, c'est-à-dire que N est la somme de 2 éléments de $\mathcal{B}$.

Ceci conclut la démonstration.

□

Pour démontrer le théorème de Shnirel'man, on utilise aussi le théorème suivant, appelé Théorème de Shnirel'man :

Théorème 15. *Soient $\mathcal{B}_1$ et $\mathcal{B}_2$ des ensembles d'entiers contenant 0. Alors*

$$\sigma(\mathcal{B}_1 + \mathcal{B}_2) \geq \sigma(\mathcal{B}_1) + \sigma(\mathcal{B}_2) - \sigma(\mathcal{B}_1)\sigma(\mathcal{B}_2)$$

Preuve. On cherche à minorer $\sigma(\mathcal{B}_1 + \mathcal{B}_2)$, donc à minorer $\frac{(\mathcal{B}_1+\mathcal{B}_2)(N)}{N}$ pour tout $N \geq 1$.

On fixe $N \geq 1$. On va essayer d'évaluer $(\mathcal{B}_1 + \mathcal{B}_2)(N)$, c'est-à-dire de compter les éléments non nuls de $\mathcal{B}_1 + \mathcal{B}_2$ qui ne dépassent pas N.

1^{er} *cas :* $\mathcal{B}_1(N)\mathcal{B}_2(N) = 0$.

On peut supposer $\mathcal{B}_1(N) = 0$ sans perte de généralité. Alors évidemment $\sigma(\mathcal{B}_1) = 0$. D'autre part, $\mathcal{B}_2 \subset \mathcal{B}_1 + \mathcal{B}_2$, donc on a $\sigma(\mathcal{B}_2) \leq \sigma(\mathcal{B}_1 + \mathcal{B}_2)$. Ainsi :

$$\sigma(\mathcal{B}_1 + \mathcal{B}_2) \geq \sigma(\mathcal{B}_1) + \sigma(\mathcal{B}_2) - \sigma(\mathcal{B}_1)\sigma(\mathcal{B}_2).$$

2^{nd} cas : $\mathcal{B}_1(N)\mathcal{B}_2(N) \neq 0$.

On a $\mathcal{B}_1(N) \neq 0$. On pose $k = \mathcal{B}_1(N) \geq 1$. On peut ainsi définir

$$1 \leq a_1 < \cdots < a_k \leq N$$

les éléments non nuls de $\mathcal{B}_1$ ne dépassant pas N. On a aussi $\mathcal{B}_2(N) \neq 0$. Comme pour $\mathcal{B}_1$, on définit

$$1 \leq b_1 < \cdots < b_{k'} \leq N$$

où $k' = \mathcal{B}_2(N) \geq 1$. On pose de plus $b_0 = 0$, qui est élément de $\mathcal{B}_2$.

Dès lors, on note r_0 le plus grand indice tel que $b_{r_0} < a_1$. Il est clair que cet indice existe car il peut être nul ($b_0 = 0$). Pour $1 \leq j \leq k-1$, on construit de même r_j le plus grand indice tel que $a_j + b_{r_j} < a_{j+1}$. Et enfin, on note r_k le plus grand indice tel que $a_k + b_{r_k} \leq N$. On a ainsi :

$$\begin{aligned} 0 = b_0 \ &< \ \cdots < b_{r_0} < a_1 + b_0 < \cdots < a_1 + b_{r_1} < a_2 + b_0 < \cdots \\ \cdots \ &< \ a_{k-1} + b_{r_{k-1}} < a_k + b_0 < \cdots < a_k + b_{r_k} \leq N \end{aligned}$$

Comme $0 \in \mathcal{B}_1 \cup \mathcal{B}_2$, tous les éléments ordonnés ci-dessus (N non forcément compris) sont dans $\mathcal{B}_1 + \mathcal{B}_2$. En plus, ils sont disjoints et ne dépassent pas N. En excluant b_0 qui est nul, il y a $\sum_{j=0}^{k}(r_j + 1) - 1$ tels éléments, donc on a :

$$(\mathcal{B}_1 + \mathcal{B}_2)(N) \geq \sum_{j=0}^{k}(r_j + 1) - 1 = \sum_{j=0}^{k} r_j + k$$

Maintenant, pour $1 \leq j \leq k-1$, par définition des r_j, il est clair que ces derniers représentent le nombre d'éléments non nuls de $\mathcal{B}_2$ ne dépassant pas $a_{j+1} - a_j - 1$, car

$$\max_{0 \leq i \leq k'}(a_j + b_{r_j}) < a_{j+1} \Longleftrightarrow \max_{0 \leq i \leq k'}(b_{r_j}) \leq a_{j+1} - a_j - 1$$

Donc pour $1 \leq j \leq k-1$, $r_j = \mathcal{B}_2(a_{j+1} - a_j - 1)$. De même, $r_0 = \mathcal{B}_2(a_1 - 1)$ et $r_k = \mathcal{B}_2(N - a_k)$. Ainsi :

$$\sum_{j=0}^{k} r_j = \mathcal{B}_2(a_1 - 1) + \sum_{j=1}^{k-1} \mathcal{B}_2(a_{j+1} - a_j - 1) + \mathcal{B}_2(N - a_k)$$

Or, pour tout $L \geq 1$, $\mathcal{B}_2(L) \geq \sigma(\mathcal{B}_2)L$, donc

$$\begin{aligned}
\sum_{j=0}^{k} r_j &\geq \sigma(\mathcal{B}_2)(a_1 - 1) + \sum_{j=1}^{k-1} \sigma(\mathcal{B}_2)(a_{j+1} - a_j - 1) + \sigma(\mathcal{B}_2)(N - a_k) \\
&= \sigma(\mathcal{B}_2)(a_1 - 1 + \sum_{j=1}^{k-1}(a_{j+1} - a_j - 1) + N - a_k) \\
&= \sigma(\mathcal{B}_2)(a_1 - 1 + a_k - a_1 - (k-1) + N - a_k) \\
&= \sigma(\mathcal{B}_2)(N - k)
\end{aligned}$$

Comme

$$(\mathcal{B}_1 + \mathcal{B}_2)(N) \geq \sum_{j=0}^{k}(r_j + 1) - 1 = \sum_{j=0}^{k} r_j + k$$

on a

$$(\mathcal{B}_1 + \mathcal{B}_2)(N) \geq \sigma(\mathcal{B}_2)(N - k) + k$$

Or $k = \mathcal{B}_1(N)$, donc $k \geq \sigma(\mathcal{B}_1)N$. Ainsi

$$\begin{aligned}
(\mathcal{B}_1 + \mathcal{B}_2)(N) &\geq \sigma(\mathcal{B}_2)(N - k) + k \\
&= \sigma(\mathcal{B}_2)N + (1 - \sigma(\mathcal{B}_2))k \\
&\geq \sigma(\mathcal{B}_2)N + (1 - \sigma(\mathcal{B}_2))\sigma(\mathcal{B}_1)N \\
&= (\sigma(\mathcal{B}_1) + \sigma(\mathcal{B}_2) - \sigma(\mathcal{B}_1)\sigma(\mathcal{B}_2))N
\end{aligned}$$

Ainsi

$$\frac{(\mathcal{B}_1 + \mathcal{B}_2)(N)}{N} \geq \sigma(\mathcal{B}_1) + \sigma(\mathcal{B}_2) - \sigma(\mathcal{B}_1)\sigma(\mathcal{B}_2)$$

Et donc

$$\sigma(\mathcal{B}_1 + \mathcal{B}_2) = \inf_{N \in \mathbb{N}^*} \frac{(\mathcal{B}_1 + \mathcal{B}_2)(N)}{N} \geq \sigma(\mathcal{B}_1) + \sigma(\mathcal{B}_2) - \sigma(\mathcal{B}_1)\sigma(\mathcal{B}_2)$$

Ceci conclut la démonstration du théorème.

On peut reformuler ce théorème en

$$1 - \sigma(\mathcal{B}_1 + \mathcal{B}_2) \leq (1 - \sigma(\mathcal{B}_1))(1 - \sigma(\mathcal{B}_2)) \tag{3.1}$$

□

On peut maintenant faire la preuve du Théorème 13, le théorème de Shnirel'man :

Preuve du Théorème 13. Soit $\beta = \sigma(\mathcal{B})$. On a clairement $\beta \in]0, 1]$. Donc $0 \leq 1 - \beta < 1$, et ainsi

$$0 \leq (1 - \beta)^l \leq \frac{1}{2},$$

pour un certain entier $l \geq 1$. On va montrer que $\sigma(l\mathcal{B}) \geq \frac{1}{2}$ pour appliquer le lemme à $l\mathcal{B}$, où $l\mathcal{B} = \mathcal{B} + \cdots + \mathcal{B}$. Pour cela, on montre par récurrence que pour tout $s \geq 1$:

$$1 - \sigma(s\mathcal{B}) \leq (1 - \sigma(\mathcal{B}))^s \tag{3.2}$$

Pour $s = 1$, c'est vrai de manière triviale (on a même une égalité). Supposons (2) vraie pour un certain $s \geq 1$. On a

$$1 - \sigma((s + 1)\mathcal{B}) = 1 - \sigma(s\mathcal{B} + \mathcal{B})$$

On peut appliquer la reformulation (1) du Théorème 15 à $\mathcal{B}_1 = s\mathcal{B}$ et $\mathcal{B}_2 = \mathcal{B}$, car ces deux ensembles contiennent 0, et on trouve

$$1 - \sigma(s\mathcal{B} + \mathcal{B}) \leq (1 - \sigma(s\mathcal{B}))(1 - \sigma(\mathcal{B}))$$

Avec l'hypothèse de récurrence (2), on en déduit que

$$1 - \sigma(s\mathcal{B} + \mathcal{B}) \leq (1 - \sigma(\mathcal{B}))^s(1 - \sigma(\mathcal{B})) = (1 - \sigma(\mathcal{B}))^{s+1}$$

Ceci conclut la démonstration par récurrence. On prend $s = l$, et on trouve

$$1 - \sigma(l\mathcal{B}) \leq (1 - \sigma(\mathcal{B}))^l = (1 - \beta)^l \leq \frac{1}{2}$$

et donc

$$\sigma(l\mathcal{B}) \geq \frac{1}{2}$$

On applique le Lemme 14 à l'ensemble $l\mathcal{B}$ qui vérifie clairement les hypothèses. Et donc tout entier naturel s'écrit comme somme de 2 éléments de $l\mathcal{B}$. Ainsi, en posant $K = 2l$, on a que tout entier naturel s'écrit comme somme de K éléments de $\mathcal{B}$.

Ceci conclut la démonstration du théorème. □

Démonstration du Théorème A. On avait défini l'ensemble

$$\mathcal{A} = \{0, 1\} \cup \{p + q : p, q \in \mathcal{P}\}$$

Cet ensemble contient 0. Il resterait à prouver que sa densité de Shnirel'man est strictement positive pour que tout entier naturel soit somme de K éléments de $\mathcal{A}$ pour K fixé. Dans ce but, il nous faut évidemment minorer $\frac{\mathcal{A}(N)}{N}$ pour $N \geq 1$. On utilise pour cela $r(N)$ la fonction dénotant le nombre de représentations de N comme somme de deux nombres premiers (où par exemple 5+7 et 7+5 sont deux représentations différentes). Par l'inégalité de Cauchy-Schwarz, pour $x > 0$, on a

$$\left(\sum_{N \leq x} r(N)\right)^2 \leq \sum_{\substack{N \leq x \\ r(N) \geq 1}} 1 \sum_{N \leq x} r(N)^2$$

De plus

$$\mathcal{A}(x) = \sum_{N \in \{0,1\}} 1 + \sum_{\substack{2 \leq N \leq x \\ N = p+q}} 1$$

Donc

$$\mathcal{A}(x) = 2 + \sum_{\substack{2 \leq N \leq x \\ r(N) \geq 1}} 1$$

Et ainsi a fortiori on a

$$\sum_{\substack{N \leq x \\ r(N) \geq 1}} 1 \leq \mathcal{A}(x)$$

Donc, pour $x > 0$, on a

$$\frac{\mathcal{A}(x)}{x} \geq \frac{1}{x} \frac{\left(\sum_{N \leq x} r(N)\right)^2}{\sum_{N \leq x} r(N)^2}$$

Il nous reste à minorer $\left(\sum_{N \leq x} r(N)\right)^2$ et à majorer $\sum_{N \leq x} r(N)^2$. Pour cela, nous allons utiliser les deux résultats déjà démontrés dans les chapitres 1 et 2, à savoir les Théorèmes B et C. Le Théorème B nous dit que

$$\sum_{N \leq x} r(N) \gg \frac{x^2}{(\log x)^2}$$

Le Théorème C nous dit que

$$\sum_{N\leq x} r(N)^2 \ll \frac{x^3}{(\log x)^4}$$

Et ainsi

$$\frac{1}{x}\frac{\left(\sum_{N\leq x} r(N)\right)^2}{\sum_{N\leq x} r(N)^2} \gg \frac{1}{x}\frac{\frac{x^4}{(\log x)^4}}{\frac{x^3}{(\log x)^4}} = 1$$

Donc

$$\frac{\mathcal{A}(x)}{x} \gg 1$$

Ceci nous dit qu'il existe un rang $x_0 > 0$ et une constante $c_1 > 0$ tels que pour tout $x \geq x_0$, on ait $\mathcal{A}(x) \geq c_1 x$. Et comme $1 \in \mathcal{A}$, il existe une constante $c_0 > 0$ telle que pour tout $x \in]0, x_0[$, on ait $\mathcal{A}(x) \geq c_0 x$. Ainsi, pour tout $x > 0$, on a $\mathcal{A}(x) \geq \min(c_0, c_1)x > 0$. Donc $\sigma(\mathcal{A}) > 0$.

Ainsi $\mathcal{A}$ contient 0 et est de densité de Shnirel'man strictement positive. On peut lui appliquer le Théorème 13 : il existe $K \geq 1$ tel que tout entier naturel s'écrit comme la somme de K éléments de $\mathcal{A}$.

Prenons donc notre $n \geq 2$. On a $n - 2 \geq 0$. Ainsi, $n - 2$ s'écrit comme la somme de K éléments de $\mathcal{A}$.

Par définition de $\mathcal{A}$, $n - 2$ va s'écrire comme la somme de K_0 termes de $\{p + q : p, q \in \mathcal{P}\}$ plus un certain nombre de 1, noté K_1, avec $K_0 + K_1 \leq K$. D'où

$$n - 2 = \underbrace{1 + \cdots + 1}_{K_1} + (p_1 + q_1) + \cdots + (p_{K_0} + q_{K_0})$$

Ainsi, si K_1 est pair, c'est-à-dire $K_1 = 2H_1$, on a

$$n = \underbrace{2 + \cdots + 2}_{H_1+1} + (p_1 + q_1) + \cdots + (p_{K_0} + q_{K_0})$$

Et si K_1 est impair, c'est-à-dire $K_1 = 2H_1 + 1$, on a

$$n = \underbrace{2 + \cdots + 2}_{H_1} + 3 + (p_1 + q_1) + \cdots + (p_{K_0} + q_{K_0})$$

Et donc, dans tous les cas, n est la somme de $H_1 + 1 + 2K_0$ nombres premiers. Et $H_1 + 1 + 2K_0 \leq 3K$. Donc n est la somme d'au plus 3K nombres premiers. Ceci achève la démonstration. □

Annexes

Annexe 1 : Conjectures en théorie des nombres

La théorie des nombres regorge de conjectures. C'est à la fois frustrant et passionnant. Frustrant car on réalise à quel point on ne maîtrise pas des notions en apparence très simples, et passionnant car on réalise aussi qu'il reste un très grand travail de fond à effectuer pour comprendre cette branche des mathématiques. Sans doute en partie pour cela, Carl Friedrich Gauss disait : "La Mathématique est la reine des sciences et l'Arithmétique est la reine des mathématiques".

La particularité des problèmes en théorie des nombres réside dans leurs énoncés très simples. Ainsi peut-on encore citer Gauss qui disait à propos de problèmes arithmétiques : "Leur charme particulier vient de la simplicité des énoncés jointe à la difficulté des preuves". Il ne croyait pas si bien dire par *difficulté des preuves*, puisque nombre de ces problèmes sont encore ouverts aujourd'hui. En voici une liste non exhaustive (tous conjectures) inspirée en partie d'un ouvrage d'Apostol [2] :

Tout nombre pair supérieur ou égal à 4 est somme des deux nombres premiers (conjecture de Goldbach).

Tout nombre impair supérieur ou égal à 7 est somme des trois nombres premiers (conjecture de Goldbach faible).

Tout nombre pair supérieur ou égal à 2 est la différence de deux nombres premiers consécutifs d'une infinité de manières. (conjecture de Polignac).

Il existe une infinité de nombres premiers jumeaux[3].

3. *Jumeaux* signifie *dont la différence (absolue) vaut 2.* On remarque d'ailleurs que cette conjecture est conséquence évidente de la conjecture de Polignac.

Pour tout $k \geq 1$ entier, il existe une infinité de nombres premiers de la forme $n^2 + k$.

Pour tout $n \geq 2$ entier, il existe un nombre premier entre $n^2 - n$ et n^2, et un autre entre n^2 et $n^2 + n$ (conjecture d'Oppermann).

Il existe une infinité de nombres premiers qui ne s'écrivent qu'avec des 1 en base 10.

Il existe une infinité de nombres premiers de la forme $2^p - 1$ où p est premier.

Il existe une infinité de nombres composites de la forme $2^p - 1$ où p est premier.

Il existe une infinité de nombres premiers de la forme $2^{2^n} + 1$ où n est un entier naturel.

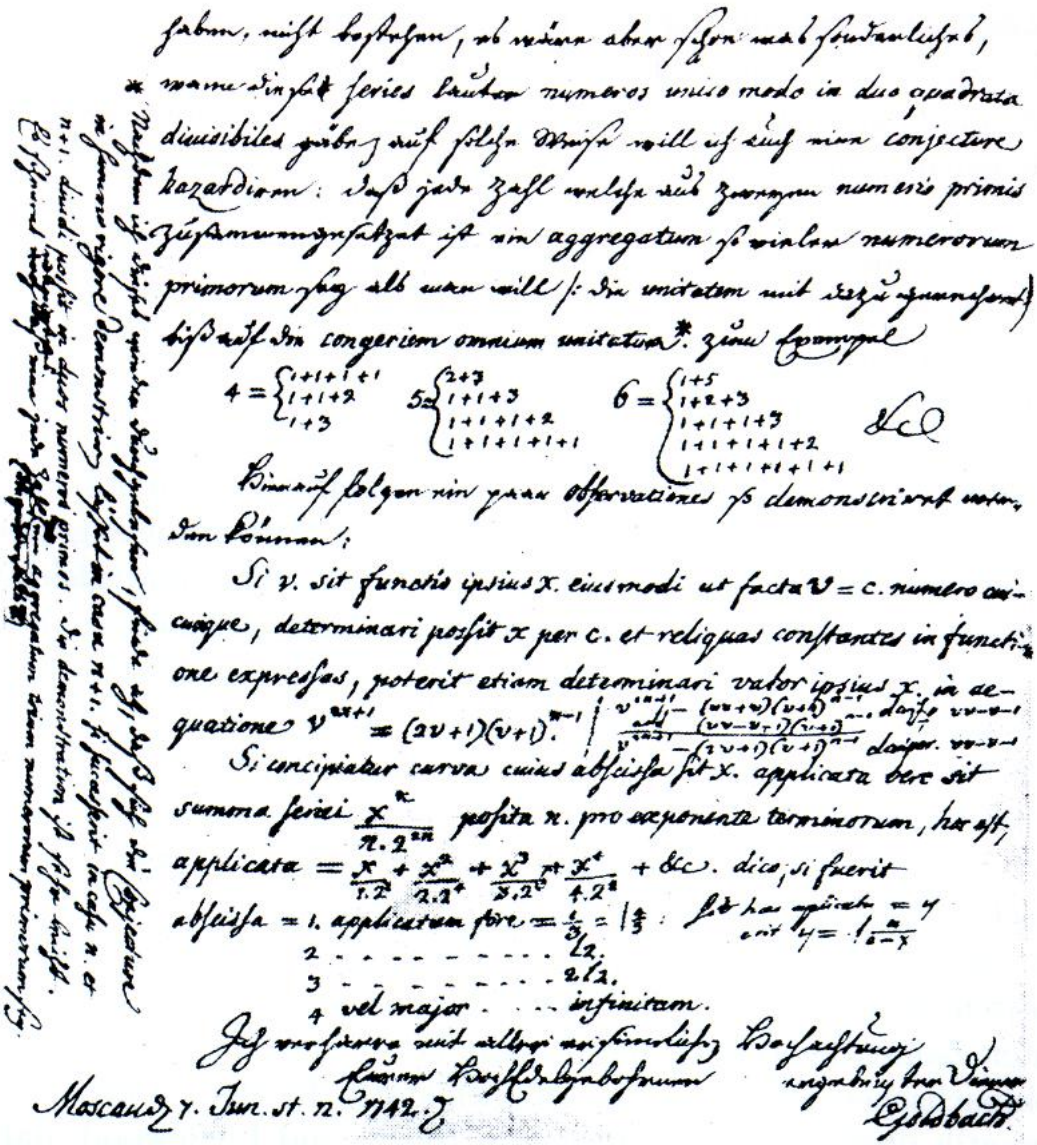
Il existe une infinité de nombres composites de la forme $2^{2^n} + 1$ où n est un entier naturel.

Aucun nombre impair n'est parfait[4].

4. *Parfait* signifie que *la somme de ses diviseurs est égale à deux fois lui-même.*

Annexe 2 : Correspondances entre Goldbach et Euler

Ci-dessous la lettre de Goldbach à Euler écrite à Moscou le 7 juin 1742. La conjecture de Goldbach est dans la dernière ligne (difficilement lisible) de la note verticale dans la marge : *Es scheinet wenigstens, daß eine jede Zahl, die größer ist als 2, ein aggregatum trium numerorum primorum sey.*



Ci-dessous un extrait de la réponse d'Euler à la lettre de Goldbach écrite à Berlin le 30 juin 1742. La conjecture de Goldbach réécrite (et rendue plus forte) par Euler est aux lignes 15 et 16 : *ein jeder numerus par eine summa duorum numerorum primorum sey.*

$2^{32}+1$, welche Zahl in duo quadrata est resolubilis, nempe 2^{32} et 1, divisibilis per $641 = 25^2 + 4^2$. Dahero der andere factor, den ich brevitatis gratia b nennen will, gewiss auch eine summa duorum quadratorum. Sit $b = pp + qq$, ita ut sit $2^{32}+1 = (25^2+4^2)(pp+qq)$, erit $2^{32}+1 = (25p+4q)^2 + (25q-4p)^2$ et simul $2^{32}+1 = (25p-4q)^2 + (25q+4p)^2$ und folglich zum wenigsten duobus modis eine summa duorum quadratorum. Hieraus kann man nun die resolutionem duplicem a priori finden. Denn es wird $p = 2556$ et $q = 409$ und folglich $2^{32}+1 = 65536^2 + 1^2 = 62264^2 + 20449^2$. Dass eine jegliche Zahl, welche in zwey numeros primos resolubilis ist, zugleich in quot, quis voluerit, numeros primos zertheilt werden könne, kann aus einer Observation, so Ew. vormals mit mir communicirt haben, dass nehmlich ein jeder numerus par eine summa duorum numerorum primorum sey, illustrirt und confirmirt werden. Denn, ist der numerus propositus n par, so ist er eine summa duorum numerorum primorum, und da $n-2$ auch eine summa duorum numerorum primorum ist, so ist n auch eine summa trium, und auch quatuor u. s. f. Ist aber n ein numerus impar, so ist derselbe gewiss eine summa trium numerorum primorum, weil $n-1$ eine summa duorum ist, und kann folglich auch in quotvis plures resolvirt werden. Dass aber ein jeder numerus par eine summa duorum primorum sey, halte ich für ein ganz gewisses theorema, ungeachtet ich dasselbe nicht demonstriren kann. — Dass $\frac{p+2\pm\sqrt{(4p-m+3)}}{m}$ nimmer ein numerus integer werden könne, erhellet daher, weilen wenn man diese Formul einem numero integro n gleich setzt, herauskommt $p = mn \pm \sqrt{(4mn-1)}$; es kann aber $4mn-1$ kein quadratum seyn.

Annexe 3 : Progression des tests de la conjecture de Goldbach

Tableau (non exhaustif) inspiré en partie du site WolframMathWorld [10] et relatant l'évolution depuis 1885 de la limite L jusqu'à laquelle a été vérifiée la conjecture de Goldbach (c'est-à-dire que tout nombre pair de 4 à L est somme de deux nombres premiers).

Année	Limite
1885	$1 \cdot 10^4$
1938	$1 \cdot 10^5$
1965	$1 \cdot 10^8$
1989	$2 \cdot 10^{10}$
1993	$4 \cdot 10^{11}$
1998	$1 \cdot 10^{14}$
1999	$4 \cdot 10^{14}$
2003	$6 \cdot 10^{16}$
2005	$3 \cdot 10^{17}$
2006	$4 \cdot 10^{17}$
2007	$1 \cdot 10^{18}$
2008	$1,2 \cdot 10^{18}$
2009	$1,6 \cdot 10^{18}$
2010	$2 \cdot 10^{18}$
2011	$2,6 \cdot 10^{18}$
2012	$4 \cdot 10^{18}$

Bibliographie

[1] E.G. Andrews. *The Theory of Partitions.* Cambridge Mathematical Press, Cambridge, 1984.

[2] T.M. Apostol. *Introduction to Analytic Number Theory.* Springer, New-York, 1976.

[3] G.H. Hardy et E.M. Wright. *Introduction à la Théorie des Nombres.* Vuibert, Paris, 2007.

[4] C. Dartyge et G. Tenenbaum. Méthodes de cribles. Master 2 de Mathématiques, 2008-2009. Université Nancy 1 Henry Poincaré.

[5] H. Halberstam et H.-E. Richert. *Sieve Methods.* Academic Press, London, 1974.

[6] E. Fricain. Cours d'arithmétique et combinatoire. Master 1 de Mathématiques, 2012. Université Lyon 1 Claude Bernard.

[7] M.B. Nathanson. *Additive Number Theory, The Classical Bases.* Springer, New-York, 1996.

[8] I.M. Vinogradov. *The Method of Trigonometrical Sums in the Theory of Numbers.* Interscience, London, s.d.

[9] Y. Wang. *The Goldbach Conjecture.* World Scientific, Singapore, 2002.

[10] WolframMathWorld. Goldbach conjecture. http ://mathworld.wolfram.com/GoldbachConjecture.html, 2012.

Index des notations

Index général