# *Un parcours explicite en théorie multiplicative*

mémoire d'habilitation

Olivier Ramaré

Mémoire présenté pour l'obtention

de l'Habilitation à Diriger des Recherches

Université de Lille 1

Olivier Ramaré

présenté et soutenu publiquement le 6 Juin 2003

devant le jury composé de

| | |
|---|---|
| Jean-Marc Deshouillers | Président |
| Michel Balazard | Rapporteur |
| Hédi Daboussi | Rapporteur |
| Andrew Granville | Rapporteur |
| Henryk Iwaniec | Examinateur |
| Hervé Queffelec | Examinateur |

# Préface

Voici une version éditée du mémoire que j'ai présenté pour obtenir mon habilitation à diriger des recherches. Le mémoire à proprement parler contenait aussi des reproductions d'articles déjà publiés ailleurs, et que j'ai omises ici. Par ailleurs, le paysage mathématique ayant évolué entretemps, j'ai ajouté des notes en bas de pages pour indiquer des développements récents.

Cette monographie se trouve à présent constituée de textes originaux qui m'ont servis de base pour des expositions orales, ainsi que d'un article non publié. J'ai aussi ajouté un article d'exposition sur des propriétés de pseudo-périodicité de la fonction $\psi$ de Chebyschev, lequel n'apparaissait pas dans le mémoire initial. J'espère que ce livre sera utile !

Olivier Ramaré
7 avril 2010

# Un parcours explicite en théorie multiplicative

Depuis douze ans, mon travail porte essentiellement sur les nombres premiers, avec un accent sur la nature effective des résultats. Pour en saisir l'unité, le mieux me semble de revenir à mon premier résultat où je montre que tout entier (sauf 1) est somme d'au plus sept nombres premiers. Tout d'abord, il ne s'agit pas d'un résultat asymptotique ; ensuite la preuve compte trois ingrédients essentiels : un crible enveloppant, des renseignements explicites sur la distribution des nombres premiers en progressions arithmétiques de petits modules (i.e. à peu de choses près des modules inférieurs à 60) et des renseignements sur de petits intervalles comprenant des nombres premiers.

On trouve des traces du crible enveloppant dans [*Hooley,* 1957], entre les équations $(50)$ et $(51)$, dans [*Linnik,* 1961, section 1.5] $^*$qui utilise la terminologie "quasi-prime" puis dans [*Hooley,* 1976] dont j'ai repris la terme de crible enveloppant. C'est peut être maladroit, mais ce que ces auteurs utilisaient est depuis devenu la notion de crible préliminaire et se distingue de ce qui est ici fait en ce qu'il s'agit d'introduire un sous-ensemble bien défini, alors que nous utilisons une suite que nous ne contrôlons que très peu. La méthode développée dans [*Ramaré,* 1995] et plus complétement dans [*Ramaré & Ruzsa,* 2001] permet d'obtenir de bons résultats dans la majoration du nombre de représentations dans un problème ternaire. Disons $N = r + s + t$ où $r$ parcourt une suite dont le crible de Selberg donne une majoration $\beta$ de la fonction caractéristique, et où $s$ et $t$ parcourent chacun des suites pour lesquelles il existe une "bonne" inégalité de type grand crible, le terme "bonne" dépendant des renseignements accessibles. Nous obtenons une

$*$. Ramachandra a aussi participé à ce cercle d'idées.

majoration de ce nombre de représentations par une expression du type

$$\sum_{d\leq D}\sum_{a \bmod^* d} w(a/d)S(a/d)T(a/d) \tag{1}$$

où $S$ et $T$ sont les polynômes trigonométriques associés respectivement à $S$ et à $T$, et $w(a/d)$ est une quantité similaire mais plus simple associée à $\beta$ :

$$w(a/d) = \lim_{M\to\infty} \frac{1}{M} \sum_{m\leq M} \beta(m)e(am/d). \tag{2}$$

Il faut remarquer que dans les applications, chaque sommant a le bonne ordre de grandeur (c'est à dire qu'il n'est plus nécessaire d'utiliser l'inégalité de Parseval comme dans la méthode du cercle ; cela se voit aussi au $1/M$ de la formule (2)). La suite $\beta$ est toujours relativement bien distribuée dans les progressions arithmétiques, ce qui fait que l'on peut penser $w(a/d)$ comme $\kappa^{\omega(d)}/d$ où $\kappa$ est la dimension du crible intervenant. Une inégalité de grand crible nous permet alors de raccourcir considérablement la somme sur $d$ en (1) et de ne garder que les petits modules, "petits" dépendant directement de ce que l'inégalité de grand crible perd pour chacune des deux suites que parcourent $s$ et $t$.

Cette technique permet d'incorporer directement des inégalités de grand crible, mais elle a le défaut de ne s'appliquer qu'aux fonctions du type de $\beta$, i.e. si l'on raisonne en termes de formes linéaires et bilinéaires, qu'à la partie linéaire. Dans ce cas, elle permet d'éviter la méthode du cercle (pour les nombres premiers, la difficulté de la méthode du cercle provient bien évidemment de la partie bilinéaire ...).

Dans les problèmes explicites sur les nombres premiers, il faut réduire la sommation sur $d$ à $d \leq D_0$ où $D_0$ est une constante (par exemple 60), et pour se faire raffiner l'inégalité du grand crible. Un tel raffinement est possible pour toutes les suites criblées, ce qui est montré en général dans [*Ramaré & Ruzsa,* 2001] (au moins en ce qui concerne les cribles de dimension finie. Mais nous donnons au chapitre 1 un exemple avec un crible de dimension "infinie"). Ce même article montre que (1) donne accès a des résultats optimaux dans un cadre assez large. Notons finalement qu'en suivant une idée de Davenport, il est possible de réduire avec succès le nombre moyen de représentations d'un problème additif binaire à un problème additif ternaire.

Dans [*Granville & Ramaré,* 1996], la partie bilinéaire de la fonction caractéristique des nombres premiers est abordée d'un point de vue explicite, avec un succès relatif, puisque avec A.Granville nous mettons en place le procédé $A$ des sommes d'exponentielles mais

omettons le procédé $B$ (la formule de Poisson).

En reprenant l'optique proposée par (1), il nous faut encore nous occuper de la distribution des nombres premiers dans les petites progressions arithmétiques. La voie a ici été tracée par [*McCurley,* 1984a] dont nous reprenons et simplifions les résultats dans [*Ramaré & Rumely,* 1996]. Nous sommes même en mesure d'élargir quelque peu la région explicite sans zéros, mais l'effort fourni n'a malheureusement que peu d'influence numérique. *

Pour ce qui est des modules moyennement grands, les estimations explicites butent notamment sur le problème du zéro de Siegel, ou, ce qui revient au même à minorer $L(1,\chi)$ lorsque $\chi$ est un caractère primitif réel. Ma seule contribution au domaine est [*Ramaré,* 2009] une minoration purement analytique de $L(1,\chi)$ qui tienne compte du nombres de facteurs premiers du conducteur du caractère. Dans [*Ramaré,* 2002], j'obtiens par ailleurs une méthode qui donne la même précision sur la distribution des nombres premiers en progressions arithmétiques en n'utilisant qu'une minoration en moyenne de $L(1,\chi)$, la moyenne portant sur tous les caractères modulo $q$. La méthode est numériquement satisfaisante et en guise d'application, nous obtenons des théorèmes de type Chebyshev pour $\sum \Lambda(n)/n$ où la somme porte sur les nombres premiers inférieurs à une bonne donée et dans une progression arithmétique de petit module (disons de module $\leq 60$).

Finalement, le programme proposé pour majorer la constante de Šnirel'man demande de montrer que les petits entiers sont sommes d'au plus 7 nombres premiers en utilisant un algorithme glouton. Il faut alors déterminer de petits intervalles contenant des nombres premiers. † Ce travail a connu bien des stades et la version finale [*Ramaré & Saouter,* 2003] donne des intervalles notoirement plus petits que ceux donnés par L.Schoenfeld. L'un des ingrédients (ma moitié du travail) est en fait une technique de lissage où l'on supprime de surcroît la contribution des bords de l'intervalle (là où la fonction de lissage est proche de 0) à l'aide du théorème de Brun-Titchmarsh. Ceci donne d'excellents résultats théoriquement et numériquement moyennant une optimisation numérique délicate. En supposant que l'on sait vérifier l'hypothèse de Riemann jusqu'à la hauteur $T_0$, notre

∗. Depuis, [*Kadiri,* 2002] améliore réellement la région explicite sans zéros. Ce travail a pris forme d'articles dans [*Kadiri,* 2005] et [*Kadiri,* 2009].

†. Voir aussi [*Dusart,* 1998, section 1.5] et [*Dusart,* 2007, proposition 6.8]

méthode garantit que les intervalles

$$[X(1-\Delta^{-1}),X] \qquad \text{avec} \qquad \Delta \gg T_0(\operatorname{Log} T_0)^{-1/2}$$

et $X \geq (T_0 \operatorname{Log} T_0)^2$ contiennent au moins un nombre premier, alors que le même genre de techniques sans crible ne donnent que la borne $\Delta \gg T_0(\operatorname{Log} T_0)^{-1}$. Compléter la preuve pour que le résultat soit valable pour tout $X$ relève alors de l'algorithmique (il s'agit d'engendrer des familles de nombres premiers ayant beaucoup d'individus et dont le test de primalité soit rapide, mais il s'agit là du domaine de mon co-auteur en la matière, i.e. Y.Saouter).

C'est aussi à l'aide de lissages efficaces que j'ai abordé des majorations du type $|L(1,\chi)| \leq \frac{1}{2}\operatorname{Log} q + C$. En effet, ne sachant établir que $L(1,\chi)$ n'était pas petit, je voulais au moins montrer qu'il ne pouvait pas être très grand (d'un point de vue explicite). Dans [*Ramaré,* 2001] et [*Ramaré,* 2004], je montre que l'on peut prendre $C = 0$ dans le cas des caractères pairs, améliorant en cela légèrement un travail de S.Louboutin. La méthode reste toutefois plus flexible et permet d'aborder des majorations de type $(\frac{1}{4}+\varepsilon)\operatorname{Log} q + C$.

Un autre problème classique est utilisé par la communauté pour mesurer les avancées dans notre connaissance explicite des nombres premiers, à savoir le problème des 7 cubes : montrer que tout entier $\geq 8\,043$ est somme de 7 cubes. Si j'ai bon nombre de résultats en la matière, un seul [*Bertault* et al. *,* 1999] est publié $^*$ et présent dans ce mémoire : il établit que tous les entiers de certaines progressions arithmétiques vérifient la propriété demandée. S'il s'agit en l'apparence d'un résultat sporadique, je tiens à faire remarquer que les conditions de congruence ne sont pas des conditions de divisibilité (qui simplifient notoirement le problème) mais que la preuve s'appuie sur la relative équi-distribution des racines cubiques d'un même nombre modulo un nombre premier $\equiv 1[3]$, ainsi que sur l'existence d'un nombre premier dans un intervalle explicite assez petit modulo $3 \times 37$, le premier argument étant nouveau dans le domaine.

Dans la catégorie des problèmes polynômiaux, [*Branton & Ramaré,* 1998] étudie la structure de l'ensemble des racines d'un polynôme modulo une puissance d'un nombre premier, l'originalité de l'approche venant de ce que nous ne faisons aucune hypothèse sur le discriminant de ce polynôme et que nous n'utilisons pas le lemme de Hensel mais une étude combinatoire.

$*$. Depuis, j'ai publié [*Ramaré,* 2005] et [*Ramaré,* 2007]. Voir aussi [*Kadiri,* 2006].

Un dernier volet, plus récent, de mes travaux concerne le caractère presque périodique de certains termes d'erreur apparaissant à propos des nombres premiers. Cet intérêt provient surtout des techniques novatrices introduites dans [*Kaczorowski,* 1991]. * Dans [*Kaczorowski & Ramaré,* 2003], nous avons grandement simplifié son formalisme (l'essentiel des preuves s'appliquent maintenant à des fonctions presque périodiques ordinaires sur la droite réelle au lieu de séries de Dirichlet particulières) et obtenu l'existence de plusieurs densité liées à ces termes d'erreur, densités nettement plus fortes que celles utilisées dans [*Rubinstein & Sarnak,* 1994]. Nous ne sommes toutefois pas encore en mesure d'aborder la densité naturelle (dont on sait qu'elle peut ne pas exister) mais disposons d'une conjecture qui permettrait d'éclairer ce domaine, ainsi que de plusieurs résultats partiels. †

Le lecteur pourrait se demander pourquoi j'ai écarté certains travaux de ce mémoire parce qu'ils ne cadraient pas avec l'optique "explicite" du titre et pourquoi je maintiens celui-ci et la réponse tient en ceci : la technique que nous déployons n'est pas asymptotique, mais dès que nous savons calculer une discrépance de distribution à un temps fini, alors nous pouvons affirmer qu'elle se répète de façon infinie à intervalle borné multiplicativement. Le caractère explicite serait complet si nous avions une borne pour la longueur des intervalles. Il est possible d'obtenir une telle borne mais nous n'avons pas mis le programme en place (ou plutôt nous l'avons mis en place mais jamais implémenté). Finalement [*Kaczorowski & Ramaré,* 2003] contient aussi une extension du champs d'application à la classe de Selberg.

La présente thèse est constituée d'articles publiés, de rédactions d'exposés et de notes non publiées et qui trouveront ici une expression. L'indépendance des divers chapitres a pour effet direct une certaine redondance : l'exposé à propos de la constante de Šnirel'man reprend bien des choses de l'article sur le même sujet (dont l'introduction s'inspire à son tour de cet exposé...), mais les points de vue y sont très largement différents.

Il est toujours un peu difficile d'établir une classification qui permette de ranger convenablement les diverses contributions d'un auteur, et bien plus lorsque l'on est l'auteur. L'ordonnancement adopté ici permet une lecture structurée, mais il existe d'autres liens entre différentes parties (les parties 2, 3 et 4 sont par exemple largement emmélées : la seconde est nécessaire à la première et à la cinquième, un résultat de laquelle est

∗. Lire aussi notamment [*Kaczorowski,* 1993] et [*Kaczorowski,* 1994].

†. [*Schlage-Puchta,* 2009] donne une preuve de cette conjecture.

nécessaire à la troisième). D'ailleurs le lecteur attentif aura remarqué que ce découpage n'est pas celui que nous avons pourtant adopté dans cette introduction...

Signalons ici **une notation** peu usuelle : nous utiliserons $f = \mathcal{O}^*(g)$ pour dire que $|f| \leq g$, soit un $\mathcal{O}$ avec une constante implicite égale à 1.

*Des remerciements sont dûs à la communauté du logiciel libre. Ce mémoire est écrit à l'aide de LaTeX 2ε et de ses multiples extensions, dont fancyhdr, authordate, amsmath et footmisc. Les dessins ont eux été réalisés à l'aide de xfig et de gnuplot, les calculs à l'aide de GP/PARI.*

# Crible et problème de Goldbach

Nous avons regroupé dans cette partie les expositions qui reposent essentiellement sur le crible, et à une exception près, sur le crible supérieur de Selberg. Elle contient

Une approche nouvelle du crible de Selberg.

*Il ne s'agit pas d'un article mais d'une exposition qui contient du matériel publié dans d'autres articles ainsi que des résultats indépendants.*

Un crible local pour les nombres premiers.

*Un divertissement quelque peu surprenant où l'on obtient une borne inférieure de type Tchebyshev pour les nombres premiers en utilisant un crible.*

Sur le problème de Goldbach effectif.

*Il s'agit de la version écrite d'un exposé sur le problème de Schnirel'man. Il reprend l'historique du problème et explique l'évolution des approches.*

Les deux articles suivants appartenaient à cette partie :

On Šnirel'man's constant. [*Ramaré,* 1995]

*L'article principal sur la constante de Šnirel'man. Il s'agit d'une version améliorée de ma thèse [Ramaré, 1991].*

Additive properties of dense subsets of sifted sequences. [*Ramaré & Ruzsa,* 2001]

*Cet article avec I. Ruzsa présente la forme aboutie de la technique du crible enveloppant pour des suites "suffisamment criblées".*

# Chapitre 1

# Une approche nouvelle du crible de Selberg

Cette partie a fait l'objet de nombreux exposés entre 1993 et 2000 et une bonne partie constitue la troisième section de [*Ramaré & Ruzsa,* 2001]. Ce matériel se retrouve encore en partie dans [*Ramaré,* 2007] et, exposé de façon différente, par endroit plus complète mais parfois moins, dans [*Ramaré,* 2009]. Bien que l'exposé reste assez élémentaire, il est préférable que le lecteur supposé connaisse les bases du crible supérieur de Selberg.

## 1.1 Le problème initial

Nous nous donnons deux objets :

(1) Une suite hôte finie $\mathcal{A}$, par exemple la suite des entiers entre $N_0+1$ et $N_0+N$.

(2) Pour tout $d \leq D$, un sous-ensemble $\mathcal{K}_d \subset \mathbb{Z}/d\mathbb{Z}$.

Nous supposons bien sûr que la suite des $\mathcal{K}_d$ est consistante, ce par quoi nous entendons que $\sigma_d^q(\mathcal{K}_q) = \mathcal{K}_d$ dès que $d|q$ et où $\sigma_d^q$ est la projection canonique de $\mathbb{Z}/q\mathbb{Z}$ sur $\mathbb{Z}/d\mathbb{Z}$. Plus important, nous supposons que la suite des $\mathcal{K}_d$ est multiplicativement scindée, i.e. que $\mathcal{K}_{d_1d_2} \simeq \mathcal{K}_{d_1} \times \mathcal{K}_{d_2}$ si $(d_1,d_2)=1$ via l'isomorphisme chinois. Il est évidemment équivalent de se donner pour chaque nombre premier $p$ une suite consistante $(\mathcal{K}_{p^\nu})_\nu$ où $\mathcal{K}_{p^\nu} \subset \mathbb{Z}/p^\nu\mathbb{Z}$. De façon générale, si $\mathcal{A}$ désigne un ensemble de classes modulo $d$, nous utiliserons aussi $\mathcal{A}$ pour l'ensemble des entiers qui appartiennent à ces classes ou pour celui des entiers $x$ modulo $q$ tels que $\sigma_d^q(x)$ tombe dans $\mathcal{A}$, lorsque $d|q$

bien entendu. Cette suite $(\mathcal{K}_d)_d$ définit un compact $\mathcal{K}$ dans $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$.

Nous nous intéressons alors à la suite

$$\mathcal{S} = \{n \in \mathcal{A} \quad / \quad \forall d \leq D, \quad n \in \mathcal{K}_d\} \tag{1.1}$$

et notamment à construire une fonction majorant sa fonction caractéristique.

Il s'agit là du problème classique du crible. Nous n'avons pas l'impression d'avoir fait grand chose et pourtant la moitié de l'exposé se situe ici. En effet

(1) L'approche usuelle consiste à regarder les classes que l'on ôte et non celles que l'on garde. Ceci induit un manque de régularité des expressions que l'on manipule. On trouve toutefois la trace de notre façon de faire dans [*Bombieri & Davenport,* 1968] où ils démontrent le théorème de Brun-Titchmarsh de façon étonnante. Cet article est d'ailleurs l'ancêtre de ce travail.

(2) Nous regardons ce qui se passe modulo $p$, mais aussi modulo $p^2, p^3, \ldots$ ce qui induit des complications notoires. [*Gallagher,* 1974] donne une solution partielle à cette question dans le cas où la suite hôte est un intervalle et [*Selberg,* 1976] une solution plus complète, mais la complexité des expressions l'oblige là encore à contrôler le terme d'erreur par le grand crible ce qui limite l'utilisation à la suite hôte des entiers dans un intervalle. Par ailleurs, l'exposition de cette solution demande une dizaine de pages sans que la longueur contribue à la clarté.

(3) On se ramène usuellement à la condition $P(n) \equiv 0[d]$ pour un certain polynôme $P$ par différentes astuces, ce qui est inutile ici.

L'exposition ci-dessous présente plusieurs avantages comparées à la présentation classique :

(a) Elle donne une expression claire des $\lambda_d$ qui rend triviale l'inégalité $|\lambda_d| \leq 1$. (extension de [*van Lint & Richert,* 1965])

(b) Elle est utilisable sur les suites.

(c) Il est possible d'introduire des pondérations.

(d) Elle permet de faire le lien entre le crible de Selberg et la dérivation de Bombieri-Davenport du théorème de Brun-Titchmarsh.

Cette technique est bien sûr utile pour obtenir une information sur le cardinal de $\mathcal{S}$ ! ! Elle est liée à la technique que j'appellerai ici d'affaiblissement (Mollification). C'est

d'ailleurs à partir de cette technique que Selberg a inventé le procédé de crible qui nous intéresse ici. Motohashi l'a beaucoup étudiée et utilisée. On s'en sert pour les théorèmes de densité par exemple, ou pour minorer le nombre de zéros de $\zeta$ sur la droite critique. Récemment, Michel l'a utilisée pour évaluer le nombre de fonctions $L$ modulaires s'annulant au point critique. Elle se confond souvent avec un crible préliminaire (par exemple dans la méthode de dispersion ou au niveau des cribles pondérés).

## 1.2 Théorie générale

Il nous faut tout d'abord quelques résultats préliminaires.

### ○○ Le système frontière $(\mathcal{L}_d)_d$.

Nous avons besoin d'une autre suite d'ensembles $(\mathcal{L}_d)_{d\geq 1}$ complémentaire des $(\mathcal{K}_d)$ : nous posons $\mathcal{L}_1 = \{1\}$ et $\mathcal{L}_{p^\nu} = \mathcal{K}_{p^{\nu-1}} - \mathcal{K}_{p^\nu}$, i.e. l'ensemble des éléments $x \in \mathbb{Z}/p^\nu\mathbb{Z}$ tels que $\sigma_{p^{\nu-1}}^{p^\nu}(x) \in \mathcal{K}_{p^{\nu-1}}$ mais qui n'appartiennent pas à $\mathcal{K}_{p^\nu}$. Nous définissons $\mathcal{L}_d$ par "multiplicativité". Il est important de remarquer que contrairement à ce qui se passe pour $\mathcal{K}$, *nous n'avons pas* $\mathcal{L}_\ell = \mathcal{L}_d/\ell\mathbb{Z}$ si $\ell|d$. La notation $\mathbb{1}_{\mathcal{A}}$ désignant la fonction caractéristique de $\mathcal{A}$, nous avons par définition

$$\begin{cases} \mathbb{1}_{\mathcal{L}_d} = \displaystyle\prod_{p^\nu \| d} \left(\mathbb{1}_{\mathcal{K}_{p^{\nu-1}}} - \mathbb{1}_{\mathcal{K}_{p^\nu}}\right) = (-1)^{\omega(d)} \sum_{\delta|d} \mu(d/\delta)\mathbb{1}_{\mathcal{K}_\delta} \\ \mathbb{1}_{\mathcal{K}_d} = \displaystyle\prod_{p^\nu \| d} \left(\mathbb{1} - \mathbb{1}_{\mathcal{L}_p} - \mathbb{1}_{\mathcal{L}_{p^2}} - \cdots - \mathbb{1}_{\mathcal{L}_{p^\nu}}\right) = \sum_{\delta|d} (-1)^{\omega(d)} \mathbb{1}_{\mathcal{L}_\delta}. \end{cases} \tag{1.2}$$

### ○○ Les fonctions $G$.

Soit $\rho$ une fonction arithmétique qui ne s'annule pas. Considérons

$$\begin{aligned} G_d(z) &= \sum_{d|q\leq z} \Big( \sum_{d|f|q} \mu(q/f)/\rho(f)\Big) \\ &= \frac{1}{\rho(d)} \sum_{q\leq z/d} \prod_{p^\nu \| q} \left( \frac{\rho\left(p^{v_p(d)}\right)}{\rho\left(p^{v_p(d)+\nu}\right)} - \frac{\rho\left(p^{v_p(d)}\right)}{\rho\left(p^{v_p(d)+\nu-1}\right)} \right) \end{aligned} \tag{1.3}$$

où $v_p(d)$ désigne la valuation $p$-adique de $d$ et $a\|b$ signifie que $a|b$ et que $a$ et $b/a$ sont premiers entre eux. Si cette dernière écriture est pratique dans lorsque l'on veut calculer

$G_d$, nous recherchons une autre écriture qui soit plus simple à manier. Introduisons la solution $h$ de $1/\rho = \mathbb{1} \star h$. Si $\rho$ est multiplicative, $h$ est donnée explicitement par

$$h(\delta) = \prod_{p^\nu \| \delta} \left( \frac{1}{\rho(p^\nu)} - \frac{1}{\rho(p^{\nu-1})} \right). \tag{1.4}$$

Notons que si, de plus, $\rho$ est positive et décroît sur les puissances de nombres premiers, la fonction $h$ est alors positive ou nulle. En utilisant $h$, nous obtenons

$$G_d(z) = \sum_{d|q\leq z} \sum_{d|f|q} \mu(q/f) \sum_{\delta|f} h(\delta) = \sum_{\delta \leq z} h(\delta) \sum_{d|q\leq z} \sum_{[d,\delta]|f|q} \mu(q/f)$$

soit encore

$$G_d(z) = \sum_{\delta/\,[d,\delta]\leq z} h(\delta). \tag{1.5}$$

De cette expression découle la généralisation suivante d'un lemme de [*van Lint & Richert,* 1965] :

**Lemme 1.2.1** *Supposons $h \geq 0$. Alors $G_\ell(z\ell/d) \leq G_d(z) \leq G_\ell(z)$ pour $\ell|d$.*

Ces fonctions ont été étudiées de façon extensive dans le cadre du crible de Selberg, études que le lecteur trouvera dans [*Halberstam & Richert,* 1974] (attention tout de même au léger changement de notations).

### ○○ Extension du crible supérieur de Selberg pour un intervalle.

Nous recherchons les solutions des problèmes extrêmaux suivants :

$$\begin{cases} \sum_d \lambda_d^* = 1 \qquad , \quad \lambda_d^* = 0 \quad \text{if } d \geq D \\ \text{Terme principal de } \displaystyle\sum_{N_0 < n \leq N_0+N} \left( \sum_{d/n \in \mathcal{K}_d} \lambda_d^* \right)^2 \quad \text{minimal} \end{cases} \tag{1.6}$$

et

$$\begin{cases} \lambda_1 = 1 \qquad , \quad \lambda_d = 0 \quad \text{if } d \geq D \\ \text{Terme principal de } \displaystyle\sum_{N_0 < n \leq N_0+N} \left( \sum_{d/n \in \mathcal{L}_d} \lambda_d \right)^2 \quad \text{minimal.} \end{cases} \tag{1.7}$$

Nous passons d'un problème à l'autre en utilisant (1.2) :

$$\text{(1.8)} \qquad \begin{cases} (-1)^{\omega(d)}\lambda_d = \sum_{d|\ell} \lambda_\ell^* \quad , \quad \lambda_\ell^* = \sum_{\ell|d} \mu(d/\ell)(-1)^{\omega(d)}\lambda_d, \\ \beta(n) = \Big( \sum_{d/n\in\mathcal{K}_d} \lambda_d^* \Big)^2 \quad , \quad \sum_{d/n\in\mathcal{L}_d} \lambda_d = \sum_{d/n\in\mathcal{K}_d} \lambda_d^*. \end{cases}$$

La résolution du premier problème est très simple grâce au caractère multiplicativement scindé des $(\mathcal{K}_d)_d$ et se fait selon la méthode de diagonalisation de Selberg. En effet, nous avons

$$\begin{aligned} \sum_{N_0<n\le N_0+N} \Big( \sum_{d/n\in\mathcal{K}_d} \lambda_d^* \Big)^2 &= \sum_{d_1,d_2\le D} \lambda_{d_1}^*\lambda_{d_2}^* \sum_{\substack{N_0<n\le N_0+N \\ n\in\mathcal{K}_{[d_1,d_2]}}} 1 \\ &= \sum_{d_1,d_2\le D} \lambda_{d_1}^*\lambda_{d_2}^* \frac{|\mathcal{K}_{[d_1,d_2]}|}{[d_1,d_2]} N + \text{ terme d'erreur} \end{aligned}$$

Posons $\rho(d) = \frac{|\mathcal{K}_d|}{d}$ et soit $h$ la solution de $1/\rho = \mathbb{1} \star h$. Il vient

$$\begin{aligned} \sum_{d_1,d_2\le D} \lambda_{d_1}^*\lambda_{d_2}^* \frac{|\mathcal{K}_{[d_1,d_2]}|}{[d_1,d_2]} &= \sum_{d_1,d_2\le D} \lambda_{d_1}^*\rho(d_1)\lambda_{d_2}^*\rho(d_2)(\mathbb{1}\star h)((d_1,d_2)) \\ &= \sum_{d\le D} h(d) \Big( \sum_{d|q\le D} \lambda^* d\rho(d) \Big)^2. \end{aligned}$$

Nous définissons à ce niveau les variables auxiliaires $y_d$ définies par

$$y_d = \sum_{q/d|q\le D} \lambda_d^*\rho(d).$$

Il s'agit là d'un système linéaire triangulaire qui a des 1 sur la diagonale. Il s'inverse par conséquent et nous passons des $(y_d)$ aux $(\lambda_q^*)$ par

$$\rho(q)\lambda_q^* = \sum_{d/q|d\le D} \mu(d/q) y_d.$$

En effet, la solution est unique et le lecteur vérifiera facilement que le membre de droite convient.

La condition $\sum_q \lambda_q^* = 1$ se traduit en termes des $(y_d)$ par

$$1 = \sum_q \lambda_q^* = \sum_d h(d) y_d.$$

Nous devons alors de minimiser la forme quadratique $\sum_d h(d) y_d^2$ sous la contrainte linéaire $1 = \sum_d h(d) y_d$. En utilisant des multiplicateurs de Lagrange par exemple, nous constatons qu'à l'optimum, les $y_d$ sont tous égaux et que leur valeur commune est $1/\sum_d h(d)$ soit $1/G_1(D)$, la fonction $G$ étant bien sûr celle associée à $\rho$.*

Nous obtenons

$$\lambda_d^* = \frac{d}{|\mathcal{K}_d|} \frac{\sum_{q \le Q/d} \mu(q)}{G_1(D)} \quad \text{et} \quad \lambda_d = (-1)^{\omega(d)} \frac{G_d(D)}{G_1(D)}. \tag{1.9}$$

D'un point de vue information, le passage des $(\lambda_d^*)$ aux $(\lambda_d)$ s'explique par la remarque suivante : lorsque nous écrivons $n \in \mathcal{K}_{p^\nu}$, nous oublions que nous savons déjà que $n \in \mathcal{K}_{p^{\nu-1}}$ ; éliminer cette redondance conduit aux $(\mathcal{L}_d)$ et aux $(\lambda_d)$.

Pour ce qui est d'obtenir une majoration de $|\mathcal{S}|$ (donné par (1.1)), nous obtenons directement

$$|\mathcal{S}| \le \sum_{n \le N} \Big( \sum_{d/n \in \mathcal{K}_d} \lambda_d^* \Big)^2 = \sum_{n \le N} \Big( \sum_{d/n \in \mathcal{L}_d} \lambda_d \Big)^2 \le \frac{N}{G_1(D)} + D^2.$$

Le passage des $(\lambda_d^*)$ aux $(\lambda_d)$ est donc extrêment intéressant en ce qui concerne le terme d'erreur, grâce au lemme 1.2.1.

Dans [*Selberg,* 1976] et [*Motohashi,* 1983], le lecteur trouvera une autre exposition et dans [*Gallagher,* 1974] du matériel sur un sujet très voisin. †

### ○○ Extension du crible supérieur de Selberg pour des suites.

Nous sommes maintenant en mesure de traiter le problème de cribler des suites et non seulement des intervalles. Soit $(\varphi_n)_{n \in \mathbb{Z}}$ une suite pondérée avec des poids positifs ou nuls et telle que $\sum_n \varphi_n < +\infty$. Soit $\mathcal{K}$ un compact multiplicativement scindé. Supposons qu'il existe une fonction multiplicative $\sigma^*$, un paramètre $X$ et une fonction $R_d^*$ tels

∗. Si jamais $h(d)$ s'annulle, la valeur correspondante de $y_d$ n'a aucune espèce d'influence et de même, le $\lambda_d$ correspondant apparaîtra toujours avec le coefficient $h(d)$. La solution $y_d$ que nous choisissons est celle qui donne des formules uniformes. Nous verrons au niveau du théorème 1.3.1 une justification de cette définition des $\lambda_d$.

†. Ainsi à présent que dans [*Ramaré,* 2009].

que

$$\sum_{n\in\mathcal{K}_d}\varphi_n = \sigma^*(d)X + R_d^*. \tag{1.10}$$

De façon équivalente, nous nous donnons $\sigma$ et $(R_d)$ tels que

$$\sum_{n\in\mathcal{L}_d}\varphi_n = \sigma(d)X + R_d. \tag{1.11}$$

Nous passons de (1.10) à (1.11) en utilisant (1.2). Récapitulons les formules de passage :

$$\begin{cases} (-1)^{\omega(d)}\sigma(d) = \displaystyle\sum_{\delta|d}\mu(d/\delta)\sigma^*(\delta), \\ \sigma^*(d) = \displaystyle\sum_{\delta|d}(-1)^{\omega(\delta)}\sigma(\delta). \end{cases} \tag{1.12}$$

Toute l'analyse précédente passe alors sans autre forme de procès avec $\rho = \sigma^*$, et nous donne au final

$$\sum_{n\in\mathcal{K}}\varphi_n \leq \frac{X}{G_1(z)} + \sum_{d_1,d_2}\lambda_{d_1}\lambda_{d_2}R_{[d_1,d_2]}. \tag{1.13}$$

Notons que si $\sigma^*$ est positive et décroît sur les puissances de nombres premiers (hypothèses plausibles si l'on pense à $\sigma^*(d)$ comme à une densité), alors nous avons encore $|\lambda_d| \leq 1$. De plus l'ensemble $\mathcal{L}_d$ est souvent beaucoup plus petit que $\mathcal{K}_d$ ce qui fait que $R_d$ est de même beaucoup plus petit que $R_d^*$ ; Ceci résulte en un terme d'erreur, au niveau de (1.13), beaucoup plus facile a contrôler et explique a posteriori pourquoi nous avons introduit les $\lambda_d$.

### ○○ Dimension du crible

L'objet de cet exposition n'est pas d'évaluer les fonctions $G$ et nous dirons simplement que nous avons un crible de dimension $\kappa \geq 0$ dès que

$$G_1(z) = C(\mathcal{K})\operatorname{Log}^{\kappa} z + \mathcal{O}(\operatorname{Log}^{\kappa-1} z) \tag{1.14}$$

où $C(\mathcal{K})$ est une constante strictement positive. Le lecteur peut consulter [*Halberstam & Richert,* 1974] et [*Gallagher,* 1974] pour de plus amples détails. Bien que ce que nous ayons fait soit particulièrement adapté aux cribles possédant une dimension, cela reste

valable sous des conditions bien plus générales et s'applique notamment aux cribles de "dimension infinie".

○○ **Cribles sans facteurs carrés**

Lorsque $(\sigma_{p^{\nu-1}}^{p^\nu})^{-1}(\mathcal{K}_{p^{\nu-1}}) = \mathcal{K}_{p^\nu}$ dès que $\nu \geq 2$, nous disons que $\mathcal{K}$ est sans facteurs carrés. Il s'agit là d'une des conditions usuelles du crible de Selberg classique. Il faut remarquer qu'alors, la condition de Johnsen-Gallagher détaillée ci-après en (1.15) est automatiquement vérifiée et que $\mathcal{L}_{p^\nu} = \emptyset$ pour $\nu \geq 2$. De plus, bien que $\lambda_d$ soit défini et en général non nul pour tout $d \leq z$, seuls les $d$ sans facteurs carrés interviennent dans (1.13) si $\mathcal{K}$ est sans facteurs carrés. En particulier, et en anticipant sur la partie 1.4, $w(a/q) = 0$ si $q$ est divisible par un carré ce que l'on peut montrer de deux façons : en remplaçant les $\lambda_d^*$ par les $\lambda_d$ dans $(4.1)$ ou en remarquant que le théorème chinois nous donne $\sum_{b \in \mathcal{K}_q} e(ab/q) = 0$.

Nous renvoyons le lecteur aux parties VI et VII de ce chapitre ainsi qu'à [*Gallagher,* 1974] pour des exemples de cribles qui ne soient pas sans facteurs carrés.

## 1.3 Extension grand crible.

Dans toute cette section, nous supposons en outre que $\mathcal{K}$ vérifie une hypothèse introduite par Johnsen (cf [*Gallagher,* 1974] et [*Selberg,* 1976]) et qui s'écrit :

(1.15) $\quad \forall p \geq 2, \forall \nu \geq 1, \forall a \in \mathcal{K}_{p^\nu}$ la quantité $\displaystyle\sum_{\substack{n \equiv a[p^\nu] \\ n \in \mathcal{K}_{p^{\nu+1}}}} 1$ est indépendante de $a$.

Comme l'introduction de cette condition dans notre contexte précis est due à [*Gallagher,* 1974], nous parlerons de la condition de Johnsen-Gallagher, qui ne sous-entend pas que $\mathcal{K}$ est multiplicativement scindé. Mais tous nos exemples vérifieront aussi cette dernière hypothèse.

Par ailleurs, nous dirons que la suite $(\varphi_n)_{n \geq 1}$ est portée par $\mathcal{K}$ jusqu'au niveau $D$ si

(1.16) $$\varphi_n \neq 0 \implies \forall d \leq D, n \in \mathcal{K}_d.$$

Nous avons alors la généralisation suivante d'une identité connue ( [*Bombieri & Davenport,* 1968], [*Montgomery,* 1971] et [*Bombieri,* 1987/1974]) :

**Théorème 1.3.1** *Supposons que $\mathcal{K}$ vérifie la condition de Johnsen-Gallagher* (1.15)*. Soit $(\varphi_n)$ une suite portée par $\mathcal{K}$ jusqu'au niveau $Q$. Alors*

$$\sum_{q\le Q} G_q(Q)|\mathcal{K}_q| \sum_{b\in\mathcal{K}_q} \Big|\sum_{\ell|q} \mu(\frac{q}{\ell})\frac{|\mathcal{K}_\ell|}{|\mathcal{K}_q|} \sum_{m\equiv b[\ell]} \varphi_n\Big|^2 = \sum_{q\le Q}\sum_{a \bmod {}^* q} \Big|\sum_n \varphi_n e(\frac{na}{q})\Big|^2.$$

Il est facile de suivre la preuve qui suit et de montrer que la condition (1.15) est effectivement nécessaire. Il faut remarquer que pour manipuler les modules $q$ sans facteurs carrés, nous avons besoin d'une définition convenable des $G_q$, définition qui vient naturellement dans notre approche.

**Preuve.** Soit $\Delta(Q)$ le membre de droite de l'égalité ci-dessus. Nous avons

$$\Delta(Q) = \sum_{m,n} \varphi_m\overline{\varphi_n} \sum_{d|m-n} d \sum_{q\le Q/d} \mu(q)$$

et identifions la sommation interne comme étant $G_1(Q)|\mathcal{K}_d|\lambda_d^*$. En échangeant les $\lambda^*$ pour les $\lambda$, nous obtenons

$$\Delta(Q) = \sum_q G_q(Q)\Big\{\sum_{d|q}\mu(q/d)|\mathcal{K}_d| \sum_{m\equiv n[d]} \varphi_m\overline{\varphi_n}\Big\}.$$

Définissons maintenant

$$\Theta(q) = |\mathcal{K}_q| \sum_{b\in\mathcal{K}_q} \Big|\sum_{\ell|q}\mu(q/\ell)\frac{|\mathcal{K}_\ell|}{|\mathcal{K}_q|}\sum_{m\equiv b[\ell]}\varphi_n\Big|^2.$$

Grâce à la condition de Johnsen-Gallagher, nous vérifions que

$$\Theta(q) = \sum_{d|q}\sum_{m\equiv n[d]} \varphi_m\overline{\varphi_n}|\mathcal{K}_d| \sum_{\substack{\ell_1|q,\ell_2|q\\(\ell_1,\ell_2)=d}} \mu(q/\ell_1)\mu(q/\ell_2).$$

Il suffit alors de calculer la somme intérieure. Or

$$\sum_{\substack{\ell_1|q,\ell_2|q\\(\ell_1,\ell_2)=d}} \mu(q/\ell_1)\mu(q/\ell_2) = \sum_{r_1|q/d, r_2|q/d} \mu((q/d)/r_1)\mu((q/d)/r_2)\sum_{\substack{\delta|r_1\\\delta|r_2}}\mu(\delta) = \mu(q/d)$$

comme demandé. $\diamond\diamond\diamond$

Remarquons qu'en utilisant le théorème 1.3.1 avec l'inégalité du grand crible, nous retrouvons la borne donnée dans [*Gallagher,* 1974].

Nous allons utiliser le théorème 1.3.1 pour améliorer l'inégalité du grand crible. L'auteur remercie H.Iwaniec pour de nombreuses discussions qui ont, entre autres, mené au résultat suivant :

**Théorème 1.3.2** *Supposons que $\mathcal{K}$ vérifie la condition de Johnsen-Gallagher* (1.15)*. Soit $(\varphi_n)$ une suite portée par $\mathcal{K}$ jusqu'au niveau $Q$. Alors pour $Q_0 \leq Q$, nous avons*

$$\sum_{q\leq Q_0}\sum_{a \mod {}^*q}\left|\sum_n \varphi_n e(na/q)\right|^2 \leq \frac{G_1(Q_0)}{G_1(Q/Q_0)}\sum_n |\varphi_n|^2(N+Q^2)$$

**Preuve.** Désignons par $\Sigma(Q_0)$ le membre de gauche de l'inégalité à établir. Grâce au théorème 1.3.1 et en utilisant la notation $\Theta(q)$ qui apparaît dans sa preuve, nous avons

$$\begin{aligned}\Sigma(Q_0) &= \sum_{q\leq Q_0} G_q(Q)\frac{G_q(Q_0)}{G_q(Q)}\Theta(q) \leq \max_{q\leq Q_0}\left(\frac{G_q(Q_0)}{G_q(Q)}\right)\sum_{q\leq Q_0} G_q(Q)\Theta(q)\\ &\leq \max_{q\leq Q_0}\left(\frac{G_q(Q_0)}{G_q(Q)}\right)\sum_{q\leq Q} G_q(Q)\Theta(q) = \max_{q\leq Q_0}\left(\frac{G_q(Q_0)}{G_q(Q)}\right)\Sigma(Q)\end{aligned}$$

et nous concluons en utilisant le lemme 1.2.1. $\diamond\diamond\diamond$

Si $\mathcal{K}$ ne vérifie pas la condition de Johnsen-Gallagher, un résultat plus faible est toutefois accessible :

**Théorème 1.3.3** *Supposons que $\mathcal{K}$ soit multiplicativement scindé. Soit $(\varphi_n)$ une suite portée par $\mathcal{K}$ jusqu'au niveau $Q$. Alors pour $Q_0 \leq Q$, nous avons*

$$\sum_{q\leq Q_0}\sum_{a \mod {}^*q}\left|\sum_n \varphi_n e(na/q)\right|^2 \leq \frac{1}{\tilde{G}(Q,Q_0)}\sum_n |\varphi_n|^2(N+(Q_0Q)^2)$$

*où*

$$\tilde{G}(Q,Q_0) = \sum_{\substack{d\leq Q,\\ (d,P(Q_0))=1}} h(d).$$

**Preuve.** Par dualité, le problème se réduit à majorer

$$\sum_n\Big(\sum_{n\in\tilde{\mathcal{K}}_d}\lambda_d^*\Big)^2 f(n)\left|\sum_{q\leq Q_0}\sum_{a \mod {}^*q} b(q,a)e(na/q)\right|^2$$

où $f$ est la fonction de Beurling-Selberg dont la transformée de Fourier est nulle hors de $[-1/(Q_0Q)^2, 1/(Q_0Q)^2]$ et telle que $\hat{f}(0) = N + (QQ_0)^2$. Quant à $\tilde{\mathcal{K}}_d$, nous le définissons par multiplicativité : $\tilde{\mathcal{K}}_{p^\alpha} = \mathcal{K}_{p^\alpha}$ si $p > Q_0$ et $\tilde{\mathcal{K}}_{p^\alpha} = \mathbb{Z}/p^\alpha\mathbb{Z}$ sinon. Le résultat s'ensuit. ◇◇◇

## 1.4 Étude approfondie dans le cas des intervalles.

○○ **Coefficients de Fourier des poids de Selberg.**

Supposons que $\mathcal{K}$ soit multiplicativement scindé et vérifie la condition de Johnsen-Gallagher (1.15). Nous définissons, pour $a$ premier à $q$,

$$w(a/q) = \lim_{Y\to\infty} \frac{1}{Y} \sum_{n\le Y} \Big( \sum_{n\in\mathcal{K}_d} \lambda_d^* \Big)^2 e(na/q) = \sum_{q|[d_1,d_2]} \frac{\lambda_{d_1}^* \lambda_{d_2}^*}{[d_1,d_2]} \sum_{b\in\mathcal{K}_{[d_1,d_2]}} e(ab/q)$$
$$= \sum_{q|[d_1,d_2]} \frac{\lambda_{d_1}^* \lambda_{d_2}^*}{[d_1,d_2]} |\mathcal{K}_{[d_1,d_2]}| \frac{\sum_{b\in\mathcal{K}_q} e(ab/q)}{|\mathcal{K}_q|} = w_q^\sharp \frac{\sum_{b\in\mathcal{K}_q} e(ab/q)}{|\mathcal{K}_q|} \qquad (1.17)$$

disons. En remplaçant $\lambda^*$ par sa valeur, nous obtenons

$$G_1(z)^2 w_q^\sharp = \sum_{q|[d_1,d_2]} \frac{(d_1,d_2)}{|\mathcal{K}_{(d_1,d_2)}|} \sum_{d_1|\ell_1\le z} \sum_{d_2|\ell_2\le z} \mu(\ell_1/d_1)\mu(\ell_2/d_2)$$
$$= \sum_{\ell_1,\ell_2\le z} \sum_{\substack{d_1|\ell_1,d_2|\ell_2 \\ q|[d_1,d_2]}} \frac{(d_1,d_2)}{|\mathcal{K}_{(d_1,d_2)}|} \mu(\ell_1/d_1)\mu(\ell_2/d_2)$$

i.e.

$$G_1(z)^2 w_q^\sharp = \sum_{\delta\le z} h(\delta) \sum_{\ell_1,\ell_2\le z} \sum_{\substack{\delta|d_1|\ell_1 \\ \delta|d_2|\ell_2 \\ q|[d_1,d_2]}} \mu(\ell_1/d_1)\mu(\ell_2/d_2) = \sum_{\delta\le z} h(\delta)\rho_z(q,\delta) \qquad (1.18)$$

avec

$$\rho_z(q,\delta) = \sum_{\ell_1',\ell_2'\le z/\delta} \sum_{\substack{d_1|\ell_1',d_2|\ell_2' \\ q/(\delta,q)|[d_1,d_2]}} \mu(\ell_1'/d_1)\mu(\ell_2'/d_2)$$

et nous évaluons maintenant la somme interne par multiplicativité. Elle vaut 0 dès qu'il existe un nombre premier $p$ divisant $\ell_1'$ ou $\ell_2'$ mais pas $q/(\delta/q)$. Soit à présent un nombre

premier $p$ tel que $p^a \| \ell_1'$, $p^b \| \ell_2'$ et $p^c \| q/(\delta, q)$ avec $c \geq 1$. Nous vérifions successivement que la valeur de notre somme est 0 si $c \leq \max(a,b) - 1$, ou si $c = \max(a,b) > \min(a,b) \geq 1$. Sa valeur est 1 si $c = \max(a,b) > \min(a,b) = 0$ et $-1$ si $c = a = b$. Nous pouvons donc écrire $\ell_1' = q_1 q_3$, $\ell_2' = q_2 q_3$ avec $q = q_1 q_2 q_3$ et $(q_1, q_2) = (q_1, q_3) = (q_2, q_3) = 1$, et la valeur de la somme interne est alors $(-1)^{\omega(q_3)}$. Par conséquent

$$\rho_z(q,\delta) = \sum_{\substack{q/(\delta,q) = q_1 q_2 q_3 \\ (q_1,q_2)=(q_1,q_3)=(q_2,q_3)=1 \\ \max(q_1 q_3 \delta, q_2 q_3 \delta) \leq z}} (-1)^{\omega(q_3)}. \tag{1.19}$$

Remarquons que $\rho_z(q,\delta) = 1$ si $q\delta \leq z$ et vaut 0 si $\sqrt{q\delta} > z$ (puisque $\max(q_1 q_3, q_2 q_3) \geq \sqrt{q/\delta}$). De plus nous vérifions que $|\rho_z(q,\delta)| \leq 3^{\omega(q/(\delta,q))}$.

Dans le cas d'un crible de dimension $\kappa$, d'après (1.14) et le lemme 1.2.1

$$\begin{cases} w_q^\sharp = \dfrac{1}{G_1(z)}\big(1 + \mathcal{O}((3^{\omega(q)} + \operatorname{Log} q)/\operatorname{Log} z)\big), \\ |G_1(z) w_q^\sharp| \ll 3^{\omega(q)}. \end{cases} \tag{1.20}$$

Considérons pour finir $\sum_{b \in \mathcal{K}_q} e(ab/q)$. Tout d'abord, le théorème chinois nous donne

$$\Big|\sum_{b \in \mathcal{K}_q} e(ab/q)\Big| \leq \prod_{p^\nu \| q} \big(p^\nu - |\mathcal{K}_{p^\nu}|\big). \tag{1.21}$$

Ensuite, si $c/M = a/q$ avec $(a,q) = 1$, nous avons

$$\frac{1}{|\mathcal{K}_M|} \sum_{b \in \mathcal{K}_M} e(cb/M) = \frac{1}{|\mathcal{K}_q|} \sum_{b \in \mathcal{K}_q} e(ab/q).$$

### ○○ Distribution des poids de Selberg dans les progressions arithmétiques.

Supposons que $\mathcal{K}$ soit multiplicativement scindé et vérifie la condition de Johnsen-Gallagher (1.15) et soit de dimension $\kappa$ (cf (1.14)). Supposons en outre que

$$p^\nu - |\mathcal{K}_{p^\nu}| \leq c p^{\nu\xi} \tag{1.22}$$

pour un certain $c > 0$ et $\xi \in [0, \frac{1}{2}[$, ce qui implique

$$|G_1(z)w(a/q)| \ll q^{-1/2}. \tag{1.23}$$

Alors, en utilisant des caractères additifs :

$$\sum_{n\le X}\Big(\sum_{n\in\mathcal{K}_d}\lambda_d\Big)^2 e(na/q) = X w_q^{\#}\frac{\sum_{b\in\mathcal{K}_q} e(ab/q)}{|\mathcal{K}_q|} + \mathcal{O}(z^2)$$
$$= \frac{X}{G_1(z)}\frac{\sum_{b\in\mathcal{K}_q} e(ab/q)}{|\mathcal{K}_q|} + \mathcal{O}\Big(z^2 + \frac{X\sqrt{q}}{|\mathcal{K}_q|G_1(z)\operatorname{Log} z}\Big)$$

la dernière égalité venant de (1.20), (1.21) and (1.22). Nous en déduisons aisément

$$\sum_{\substack{n\le X\\ n\equiv b[q]}}\Big(\sum_{n\in\mathcal{K}_d}\lambda_d\Big)^2 = \begin{cases} \frac{X}{G_1(z)|\mathcal{K}_q|} & \text{if } b\in\mathcal{K}_q \\ 0 & \text{else}\end{cases} + \mathcal{O}\Big(z^2 + \frac{X\sqrt{q}}{|\mathcal{K}_q|G_1(z)\operatorname{Log} z}\Big). \tag{1.24}$$

### ○○ Développement de Fourier de $\beta$.

Afin de disposer d'un environnement confortable pour évaluer des sommes du type $\sum_n \beta(n)F(n)$ où $\beta$ est définie en (1.8), nous recherchons une autre expression de $\beta$ comme dans [*Ramaré,* 1995]. Nous opérons sous la condition de Johnsen-Gallagher (1.15) ajouté à la supposition que $\mathcal{K}$ est multiplicativement scindé.. Nous avons

$$\beta(n) = \Big(\sum_{d/n\in\mathcal{K}_d}\lambda_d^*\Big)^2 = \sum_{d_1,d_2}\lambda_{d_1}\lambda_{d_2}\mathbb{1}_{\mathcal{K}_{[d_1,d_2]}}(n).$$

Exprimons à présent la fonction caractéristique intérieure à cette somme en utilisant des caractères additifs. Nous arrivons à

$$\beta(n) = \sum_{d_1,d_2}\frac{\lambda_{d_1}\lambda_{d_2}}{|\mathcal{K}_{[d_1,d_2]}|}\sum_{a\ mod\ [d_1,d_2]}\Big\{\sum_{b\in\mathcal{K}_{[d_1,d_2]}} e(-ab/[d_1,d_2])\Big\}e(an/[d_1,d_2])$$
$$= \sum_{d_1,d_2}\frac{\lambda_{d_1}\lambda_{d_2}}{|\mathcal{K}_{[d_1,d_2]}|}\sum_{q|[d_1,d_2]}\sum_{a\ mod^* q}\Big\{\sum_{b\in\mathcal{K}_{[d_1,d_2]}} e(-ab/q)\Big\}e(an/q)$$

ce qui nous donne l'écriture fondamentale

$$\beta(n) = \sum_{q \leq z^2} \sum_{b \ mod^* q} w(a/q)e(an/q). \tag{1.25}$$

## 1.5 La méthode de Bombieri-Davenport.

L'une des premières utilisations de l'inégalité du grand crible à des fins de crible justement est un théorème de [*Bombieri & Davenport,* 1968]. Ils utilisent notamment la valeur du module des sommes de Gauss. Nous présentons ici une approche qui généralise la leur et obtenons un équivalent du théorème 1.3.1 par cette voie, généralisation qui nous permet de pointer clairement les arguments. La condition de Johnsen-Gallagher y apparaîtra encore mais de façon différente. Enfin, en spécialisant la preuve ci-dessous au cas des nombres premiers, le lecteur trouvera une simplification de la preuve de [*Bombieri & Davenport,* 1968].

Commençons par une définition :

**Définition 1.5.1 (Définition 5.1)** *Une suite $(\mathfrak{K}_q)_{q \leq Q}$ est dite un système orthonornal sur $\mathcal{K}$ dès que l'on a*

1. *Chaque élément de $\mathfrak{K}_q$ est une fonction de $\mathbb{Z}/q\mathbb{Z}$ dans $\mathbb{C}$.*
2. $\forall \chi \in \mathfrak{K}_q, \forall x \notin \mathcal{K}_q, \chi(x) = 0$.
3. *Si $d|q \leq Q$ et $\chi \in \mathfrak{K}_d$, alors $\tilde{\chi}$ défini par $\tilde{\chi}(x) = \chi(x + d\mathbb{Z})$ si $x \in \mathcal{K}_q$ et $\tilde{\chi}(x) = 0$ sinon est dans $\mathfrak{K}_q$.*
4. $\forall (\chi_1, \chi_2) \in \mathfrak{K}_q^2$, *nous avons*

$$\sum_{a \ mod \ q} \chi_1(a)\overline{\chi_2(a)} = \begin{cases} 0 \ \textit{si} \ \chi_1 \neq \chi_2, \\ |\mathcal{K}_q| \ \textit{si} \ \chi_1 = \chi_2 \end{cases}$$

5. $|\mathfrak{K}_q| = |\mathcal{K}_q|$.
6. *Si $\chi$ provient (selon $(3)$) de $\mathfrak{K}_{d_1}$ et de $\mathfrak{K}_{d_2}$, alors $\chi$ provient de $\mathfrak{K}_{(d_1,d_2)}$.*

Nous appellerons caractères les éléments de $\mathfrak{K}_q$, bien qu'*ils ne soient généralement pas multiplicatifs*. La notion de caractère induit est naturelle à partir de la propriété $(3)$. La notion de conducteur s'établit directement à l'aide de $(6)$. Soit alors $\mathfrak{K}_q^*$ l'ensemble des caractères de conducteur $q$.

La condition $(6)$ est assez contraignante et donnons un exemple où cette condition n'est pas réalisée. Prenons $\mathcal{K}_2 = \{1, 2\}$, $\mathcal{K}_3 = \{1, 2\}$, et $\mathcal{K}_6 = \{1, 2\}$ ; Dans $\mathfrak{K}_2$, $\mathfrak{K}_3$ et $\mathfrak{K}_6$, nous mettons la fonction constante 1 (de conducteur 1) et la fonction qui vaut 1 sur 1 et $-1$ sur 2. Cette dernière fonction est induite par une fonction modulo 2 et par une fonction modulo 3 mais pas par une fonction modulo 1. Remarquons que les conditions $(1)$—$(5)$ sont réalisées.

L'existence d'un tel système est un problème auquel nous apportons une réponse partielle avec le lemme 1.5.2. Si $\mathcal{K} = \mathbb{Z}/M\mathbb{Z}$, alors les fonctions $n \mapsto e(na/q)$ forment un tel système et si $\mathcal{K}$ est l'ensemble des inversibles, nous pouvons prendre pour $\mathfrak{K}_q$ l'ensemble des caractères multiplicatifs modulo $q$.

D'après (5) toute fonction sur $\mathbb{Z}/q\mathbb{Z}$ dont le support est dans $\mathcal{K}_q$ peut s'écrire comme une combinaison linéaire d'éléments de $\mathfrak{K}_q$. Plus précisément, étant donné un entier $q \leq Q$ et un entier $a$, la fonction $e_{\mathcal{K}_q}(.a/q)$ définie par $x \mapsto e(xa/q)$ si $x \in \mathcal{K}_q$ et par $x \mapsto 0$ sinon s'exprime par

$$e_{\mathcal{K}_q}(xa/q) = \sum_{\chi \in \mathfrak{K}_q} \left( \frac{1}{|\mathcal{K}_q|} \sum_{k \ mod \ q} e(ka/q)\overline{\chi(k)} \right) \chi(x). \tag{1.26}$$

Soit alors $(\varphi_n)_{n \leq N}$ une suite de nombres complexes portée par $\mathcal{K}$ jusqu'au niveau $Q$. Posons

$$S(\alpha) = \sum_{n \leq N} \varphi_n e(n\alpha) \ , \ (\alpha \in \mathbb{R}/\mathbb{Z}) \tag{1.27}$$

et

$$S(\chi) = \sum_{n \leq N} \varphi_n \chi(n) \ , \ (\chi \in \mathfrak{K}_q, q \leq Q), \tag{1.28}$$

la distinction entre (1.27) et (1.28) étant claire de par le contexte. Remarquons que $S(\chi) = S(\chi')$ si $\chi$ et $\chi'$ sont induits par un même caractère.

Par (1.26), nous avons

$$\sum_{a \ mod \ d} |S(a/d)|^2 = \frac{d}{|\mathcal{K}_d|} \sum_{\chi \in \mathfrak{K}_d} |S(\chi)|^2. \tag{1.29}$$

Nous avons alors

$$\sum_{q|d} \sum_{a \bmod^* q} |S(a/q)|^2 = \frac{d}{|\mathcal{K}_d|} \sum_{f|d} \sum_{\chi \in \mathfrak{K}_f^*} |S(\chi)|^2, \tag{1.30}$$

et la formule d'inversion de Möbius nous donne

$$\sum_{a \bmod^* q} |S(a/q)|^2 = \sum_{f|q} \Big( \sum_{d|q/f} \mu(\frac{q}{df}) \frac{df}{|\mathcal{K}_{df}|} \Big) \sum_{\chi \in \mathfrak{K}_f^*} |S(\chi)|^2. \tag{1.31}$$

Il nous suffit alors d'insérer $(5.6)$ dans l'inégalité du grand crible

$$\sum_{q \leq Q} \sum_{a \ mod^* q} |S(a/q)|^2 \leq \sum_{n \leq N} |\varphi_n|^2 (N + Q^2) \tag{1.32}$$

pour obtenir

**Théorème 1.5.1** *Soit $Q$ et $N$ des réels positifs. Soit $\mathcal{K}$ comme ci-dessus et soit $(\mathfrak{K}_q)_{q \leq Q}$ un système orthonormal pour $\mathcal{K}$. Donnons-nous aussi une suite de complexes $(\varphi_n)_{n \leq N}$ portée par $\mathcal{K}$ jusqu'au niveau $Q$. Nous avons alors*

$$\sum_{f \leq Q} G_f(Q) \sum_{\chi \in \mathfrak{K}_f^*} |S(\chi)|^2 \leq \sum_{n \leq N} |\varphi_n|^2 (N + Q^2) \tag{1.33}$$

*où*

$$G_f(Q) = \sum_{q \leq Q/f} \Big( \sum_{d|q} \mu(q/d) \frac{df}{|\mathcal{K}_{df}|} \Big). \tag{1.34}$$

Il s'agit bien sûr des mêmes fonctions $G$ que celles qui interviennent dans la définition des $\lambda_d$ associés à $\mathcal{K}$ i.e. $G_f(Q) = \lambda_f \, (-1)^{\omega(f)} G_1(Q)$. De même, une petite manipulation montre bien évidemment que

$$\sum_{\chi \in \mathfrak{K}_f^*} |S(\chi)|^2 = |\mathcal{K}_q| \sum_{b \in \mathcal{K}_q} \Big| \sum_{\ell | q} \mu(q/\ell) \frac{|\mathcal{K}_\ell|}{|\mathcal{K}_q|} \sum_{m \equiv b[\ell]} \varphi_n \Big|^2.$$

Ce théorème est vide si il n'existe pas de système orthonormal pour $\mathcal{K}$. Nous montrons maintenant que :

**Théorème 1.5.2** *Si le compact $\mathcal{K}$ est multiplicativement scindé et vérifie la condition de Johnsen-Gallagher* (1.15) *alors il existe un système orthonormal pour $\mathcal{K}$. De façon (partiellement) converse si il existe un système orthonormal alors la condition de Johnsen-Gallagher* (1.15) *est vérifiée.*

**Preuve.** Commençons par la condition nécessaire. Par multiplicativité, il nous suffit de construire un tel système pour $\mathcal{K}_{p^\nu}$. Remarquons que

$$|\mathcal{K}_{p^\nu}| = \frac{|\mathcal{K}_p|}{|\mathcal{K}_1|}\frac{|\mathcal{K}_{p^2}|}{|\mathcal{K}_p|}\cdots\frac{|\mathcal{K}_{p^\nu}|}{|\mathcal{K}_{p^{\nu-1}}|} \tag{1.35}$$

Procédons par induction sur $\nu$. Pour $\nu = 0$, nous prenons pour $\mathfrak{K}_1$ l'ensemble constitué de la fonction constante 1. Supposons alors $\mathfrak{K}_{p^{\nu-1}}$ construit. Nous considérons tout d'abord $\mathfrak{K}'$ l'ensemble des relevés des éléments de $\mathfrak{K}_{p^{\nu-1}}$ dans $\mathbb{Z}/p^\nu\mathbb{Z}$. Il vient

$$\forall(\chi_1,\chi_2)\in\mathfrak{K}',\ \sum_{a\ mod p^\nu}\chi_1(a)\overline{\chi_2(a)} = \sum_{b\in\mathcal{K}_{p^{\nu-1}}}\chi_1(b)\overline{\chi_2(b)}\sum_{\substack{a\in\mathcal{K}_{p^\nu}\\ a\equiv b[p^{\nu-1}]}}1$$

et (1.15) et $(5.10)$ nous assurent que la propriété $(4)$ est vérifiée sur $\mathfrak{K}'$. Il nous suffit alors de compléter $\mathfrak{K}'$ en une base orthogonale de l'ensemble des fonctions sur $\mathbb{Z}/p^\nu\mathbb{Z}\to\mathbb{C}$ qui valent 0 en dehors de $\mathcal{K}_{p^\nu}$, et de normaliser cette base en accord avec $(3)$ pour conclure la preuve.

Pour montrer que les hypothèses faites sur $\mathcal{K}$ sont effectivement nécessaires, nous procédons comme suit. Soit $W_d^q(x)$ le nombre de points de $\mathcal{K}_q$ qui sont congrus à $x$ modulo $d$ si $d|q$. Soit $\chi_1$ et $\chi_2$ deux caractères modulo $d$. En les écrivant leur produit scalaire modulo $q$, nous obtenons

$$\sum_{x\in\mathcal{K}_d} W_d^q(x)\chi_1(x)\overline{\chi_2(x)} = \delta_{\chi_1=\chi_2}|\mathcal{K}_q|.$$

En notant $\chi_0$ le caractère constant (de conducteur 1), nous obtenons

$$\sum_{x\in\mathcal{K}_d} W_d^q(x)\chi(x) = 0 \quad (\chi\neq\chi_0).$$

Comme par ailleurs l'orthogonalité à $\chi_0$ nous donne aussi

$$\sum_{x\in\mathcal{K}_d}\chi(x) = 0 \quad (\chi\neq\chi_0),$$

nous en déduisons que $W_d^q(x)$ est constant, et vaut donc $|\mathcal{K}_q|/|\mathcal{K}_d|$. $\diamond\diamond\diamond$

## 1.6 Application. Sur un problème de Gallagher.

Soit $k \geq 1$ un entier fixé. Considérons

$$\mathcal{R}_k(p) = \big\{n \,/\, n = a_0 + a_1 p + \ldots, \text{ avec } a_\nu \in [0, p-1] \text{ et } a_\nu \neq 0 \text{ si } \nu < k\big\}.$$

Alors

$$\#\big\{n \leq N \,/\, \forall p \neq n,\ n \in \mathcal{R}_k(p)\big\} \leq (1+o(1))\frac{2^k (k!)^2}{\mathbf{2k}} \frac{N}{\mathrm{Log}^k N}$$

ce qui améliore le résultat de [*Gallagher,* 1974] du facteur $2k$. Pour obtenir ce résultat il suffit d'utiliser 1.13 sur la suite des nombres premiers.

## 1.7 Application. Un théorème de type Bombieri-Vinogradov.

Nous nous penchons à présent sur un très grand crible. En cours de route, nous montrerons que la condition de Johnsen-Gallagher ne peut pas être ôtée sans autre forme de procès de l'énoncé du théorème 1.3.2.

### ○○ Une inégalité de grand crible.

**Théorème 1.7.1** *Il existe une constante $C$ telle que, pour tous nombres réels $Q_0 \geq C$ et $N$, nous avons*

$$\sum_{q \leq Q_0} \sum_{a \mod {}^* q} \left| \sum_{n \leq N} \varphi_n e(n^2 a/q) \right|^2 \leq 6000 Q_0 \,\mathrm{Log}_2^2\, 3Q_0 \cdot (N + Q_0 g(Q_0)) \cdot \sum_{n \leq N} |\varphi_n|^2,$$

*avec $g(x) = \exp(20 \,\mathrm{Log}_2(3x)\,\mathrm{Log}_3(9x))$ et ceci pour toute suite de complexes $(\varphi_n)$*

Nous utilisons ici les notations $\mathrm{Log}_2 = \mathrm{Log}\,\mathrm{Log}$ et $\mathrm{Log}_3 = \mathrm{Log}\,\mathrm{Log}\,\mathrm{Log}$.

**Preuve.** Ce que nous prouvons en modifiant légèrement la preuve du théorème 1.3.2 : il nous faut majorer

$$\max_{d \leq Q_0} \{\, G_d(Q_0)/G_d(Q) \,\}.$$

Pour cela, il nous faut avant tout définir notre crible et évaluer les fonctions $G$ qui apparaissent. Nous criblons jusqu'au niveau $Q = \max(N, Q_0 g(Q_0))$.

Lorsque $d$ est sans facteurs carrés, nous prenons pour $\mathcal{K}_d$ l'ensemble des carrés et lorsque $d$ n'est pas sans facteurs carrés, nous relevons trivialement $\mathcal{K}_\ell$ dans $\mathbb{Z}/d\mathbb{Z}$, où $\ell$ est le noyau sans facteurs carrés de $d$. Cet ensemble vérifie la condition de Johnsen-Gallagher et

$$\text{(1.36)} \qquad \begin{cases} |\mathcal{K}_{p^\nu}|p^{-\nu} = \dfrac{p+1}{2p} & \text{si} \quad p \neq 2 \quad \text{et} \quad \nu \geq 1, \\ |\mathcal{K}_{2^\nu}|2^{-\nu} = 1 & \text{si} \quad \nu \geq 1. \end{cases}$$

La fonction $h$ associée est alors nulle sur les entiers sans facteurs carrés et

$$h(2) = 0, \quad h(p) = \frac{p-1}{p+1} \quad \text{si} \quad p \neq 2.$$

Dans cette situation, nous avons

$$\begin{aligned} G_d(Q) &= \sum_{\delta /\, [d,\delta] \leq Q} h(\delta) = \sum_{\substack{q,r \\ (q,d)=1, r|d, \\ q \leq Q/d}} h(r)h(q) \\ &= (\mathbb{1} \star h)(d) \sum_{\substack{q \leq Q/d \\ (q,d)=1}} h(q) \end{aligned}$$

(en écrivant $\delta = qr$) à partir du moment où $d \leq Q$. Pour $f$ entier impair, nous obtenons alors

$$G_{2^u f}(Q) = \prod_{p|f} \frac{2p}{p+1} \sum_{\substack{q \leq Q/(2^u f) \\ (q,2f)=1}} \mu^2(q) \prod_{p|q} \left( \frac{p-1}{p+1} \right).$$

Nous définissons alors les fonctions multiplicatives $a$ et $b$ par

$$\begin{cases} a(p^\nu) = 0 \quad \text{si } p|2f \text{ et } \nu \geq 1 \\ a(p^\nu) = 0 \quad \text{si } \nu \geq 2 \\ a(p) = \dfrac{p-1}{p+1} \quad \text{si } p \nmid 2f \end{cases} \qquad \begin{cases} b(p^\nu) = 0 \quad \text{si } \nu \geq 3, \text{ ou } \nu = 2 \text{ et } p|2f \\ b(p) = -1 \quad \text{si } p|2f \\ b(p) = \dfrac{-2}{p+1} \quad \text{si } p \nmid 2f \\ b(p^2) = -\dfrac{p-1}{p+1} \quad \text{si } p \nmid 2f \end{cases}$$

de telle sorte que $a = \mathbb{1} \star b$ et

$$G_{2^u f}(Q) = \prod_{p|f} \frac{2p}{p+1} \sum_{q \le Q/(2^u f)} a(q).$$

Nous utilisons alors

$$\sum_{n \le X} 1 = X + \mathcal{O}^*(X^\alpha) \qquad (\alpha > 0, X \ge 0) \tag{1.37}$$

pour obtenir, lorsque $\alpha \ge 3/4$,

$$\sum_{q \le D} a(q) = \sum_{d \ge 1} b(d) \Big\{ \frac{D}{d} + \mathcal{O}^*((D/d)^\alpha) \Big\} = B(f) D + \mathcal{O}^* \Big( D^\alpha B^* \prod_{p|2f} \Big( 1 + \frac{1}{p^\alpha} \Big) \Big)$$

où $B(f) = \sum_{d \ge 1} b(d)/d$ et

$$B^* = \prod_{p \ge 3} \Big( 1 + \frac{2}{(p+1)p^{3/4}} + \frac{p-1}{(p+1)p^{3/2}} \Big) \le 2.3.$$

Nous remarquons que

$$\begin{aligned} B(f) &= \prod_{p \ge 2} \Big( 1 - \frac{3p-1}{p^2(p+1)} \Big) \prod_{p|2f} \Big( 1 - \frac{1}{p} \Big) \Big( 1 - \frac{3p-1}{p^2(p+1)} \Big)^{-1} \\ &\ge 0.35 \prod_{p|2f} \Big( 1 - \frac{1}{p} \Big) \Big( 1 - \frac{3p-1}{p^2(p+1)} \Big)^{-1} \Big( 1 + \frac{1}{p} \Big) \prod_{p|2f} \Big( 1 + \frac{1}{p} \Big)^{-1} \\ &\ge 0.35 \prod_{p|2f} \Big( 1 + \frac{1}{p} \Big)^{-1}. \end{aligned}$$

Par conséquent, en nous affranchissant du facteur 2, nous obtenons

$$\sum_{q \le D} a(q) = B(f) D \Big( 1 + \mathcal{O}^* \Big( 17 D^{\alpha - 1} \prod_{p|f} \Big( 1 + \frac{1}{p^\alpha} \Big)^2 \Big) \Big)$$

où nous choisissons alors $\alpha = \max(3/4, 1 - 1/\operatorname{Log}\operatorname{Log}(3f))$. Il vient avec $L = \operatorname{Log} 3f$ :

$$\prod_{\substack{p|f\\ p\geq L}}\Big(1+\frac{1}{p^\alpha}\Big)^2 \leq \exp\Big(\frac{2\operatorname{Log} f}{L^\alpha \operatorname{Log} L}\Big) \leq 4.7.$$

Par ailleurs

$$\prod_{p\leq L}\Big(1+\frac{1}{p^\alpha}\Big)^2\Big(1+\frac{1}{p}\Big)^{-2} \leq \exp\Big(\sum_{p\leq L}\frac{1}{p^\alpha}-\frac{1}{p}\Big) \leq \exp\Big(\sum_{p\leq L}\frac{1}{p}(e^{(1-\alpha)\operatorname{Log} p}-1)\Big)$$

et nous utilisons alors $e^x - 1 \leq ex$ si $0 \leq x \leq 1$ d'où

$$\prod_{p\leq L}\Big(1+\frac{1}{p^\alpha}\Big)^2\Big(1+\frac{1}{p}\Big)^{-2} \leq \exp\Big(2.4(1-\alpha)\sum_{p\leq L}\frac{\operatorname{Log} p}{p}\Big) \leq e^{2.4} \leq 12$$

en utilisant $\sum_{p\leq L}(\operatorname{Log} p)/p \leq \operatorname{Log} L$ dès que $L \geq 1$ d'après [*Rosser & Schoenfeld,* 1962, (3.24)]. Ceci nous donne

$$\begin{aligned}\prod_{p|f}\Big(1+\frac{1}{p^\alpha}\Big)^2 &\leq (4.7\times 12)\prod_{p\leq L}\Big(1+\frac{1}{p}\Big)^2 \leq 57\exp\sum_{p\leq L}\frac{2}{p}\\ &\leq 57\exp(2\operatorname{Log}\operatorname{Log} L+2) \leq 422\operatorname{Log}\operatorname{Log}(3f)^2\end{aligned}$$

à l'aide de $\sum_{p\leq L} 1/p \leq \operatorname{Log}\operatorname{Log} L + 1$ dès que $L \geq 3$, que nous prenons encore dans [*Rosser & Schoenfeld,* 1962, (3.20)], et par conséquent

$$1 - 2830\operatorname{Log}\operatorname{Log}(3f)^2\exp\Big(-\frac{\operatorname{Log} D}{\operatorname{Log}\operatorname{Log}(3f)}\Big) \leq \frac{1}{DB(f)}\sum_{q\leq D}a(q) \leq 2830\operatorname{Log}\operatorname{Log}(3f)^2.$$

Pour la majoration, nous prenons $D = Q_0/(2^u f)$ et pour la minoration, $D = Q/(2^u f)$. Comme

$$\operatorname{Log} D \geq \operatorname{Log}(Q/Q_0) \geq 20\operatorname{Log}\operatorname{Log}(3Q_0)\operatorname{Log}\operatorname{Log}\operatorname{Log}(9Q_0), \tag{1.38}$$

nous avons, pour $Q_0$ suffisamment grand,

$$1 - 2830\operatorname{Log}\operatorname{Log}(3f)^2\exp\Big(-\frac{\operatorname{Log} D}{\operatorname{Log}\operatorname{Log}(3f)}\Big) \geq 1 - 2830\operatorname{Log}\operatorname{Log}(9Q_0)^{-18} \geq 1/2.$$

Il vient finalement

$$\max_{d\leq Q_0}\{\, G_d(Q_0)/G_d(Q)\,\} \leq 6000(\operatorname{Log}\operatorname{Log}(3Q_0))^2 Q_0/Q$$

ce qui conclut la preuve. $\diamond\diamond\diamond$

$\circ\circ$ **Optimalité du théorème 1.7.1.**

En ce qui concerne la borne donnée par le théorème 1.7.1, nous montrons ici qu'elle est optimale. En effet, prenons pour $(\varphi_n)$ la fonction caractéristique des nombres premiers de l'intervalle $]N/2, N]$, puis remplaçons le membre de droite du théorème 1.7.1 par l'expression donnée au théorème 1.3.1. Il nous suffit de restreindre la sommation au module $q = 1$ pour conclure que le membre de gauche est effectivement au moins de la taille du membre de droite.

$\circ\circ$ **Un théorème de type Bombieri-Vinogradov.**

**Théorème 1.7.2** *Pour tout $A \geq 1$, il existe $B$ tel que pour tout $D \leq P(\operatorname{Log} P)^{-B}$ et $D \geq N/g(N)$, nous avons*

$$\sum_{d\leq D}\max_{a \bmod^* d}\Big|\sum_{\substack{n\sim N, p\sim P\\ n^2p\equiv a[d]}}\alpha(n) - \frac{\pi(P)}{\phi(d)}\sum_{(n,d)=1}\alpha(n)\Big| \ll_A P\sqrt{N}\|\alpha\|/(\operatorname{Log} P)^A$$

*pour toute suite de complexes $(\alpha(n))_n$.*

Et par exemple le niveau de distribution de la suite $p_1^2p_2$ avec $N \leq p_1, p_2 \leq 2N$ des nombres premiers est supérieur à $N$. En utilisant les résultats généraux du crible pondéré, on en déduit par exemple que la suite $2 + p_1^2p_2$ avec $\frac{1}{2} \leq p_1/p_2 \leq 2$ contient une infinité de nombres ayant au plus 4 facteurs premiers.

**Preuve.** Nous suivons le schéma de preuve proposée par [*Bombieri* et al. , 1986]. Posons $D = P/(\operatorname{Log} P)^{2A+4}$ et étudions

$$\Sigma = \sum_{d\leq D}\max_{a \bmod^* d}\Big|\sum_{\substack{n\sim N, p\sim P\\ n^2p\equiv a[d]}}\alpha(n) - \frac{\pi(P)}{\phi(d)}\sum_{(n,d)=1}\alpha(n)\Big|.$$

Nous avons

$$\Sigma = \sum_{d\le D} \max_{a \bmod^* d} \Big| \frac{1}{\phi(d)} \sum_{\chi \bmod^* d \atop \chi\neq\chi_0} S(\chi)T(\chi)\bar\chi(a)\Big|$$
$$\le \sum_{d\le D} \frac{1}{\phi(d)} \sum_{\chi \bmod^* d \atop \chi\neq\chi_0} |S(\chi)|\,|T(\chi)|$$

avec

$$S(\chi) = \sum_{n\sim N} \alpha(n)\,\chi(n^2) \quad \text{et} \quad T(\chi) = \sum_{p\sim P} \chi(p). \tag{1.39}$$

De façon standard, nous avons

$$\Sigma \ll \operatorname{Log} D \sum_{1<q\le D} \frac{1}{\phi(q)} \sum_{\chi \bmod^* q} |S(\chi)|\,|T(\chi)|$$
$$\ll (\operatorname{Log} D)^2 \Big( \sum_{1<q\le D_0} \sum_{\chi \bmod^* q} |S(\chi)|^2\Big)^{1/2} \max_{\chi \bmod^* q \atop 1<q\le D_0} |T(\chi)| + (\operatorname{Log} D)\Sigma'.$$

Rappelons l'inégalité classique de Gallagher :

$$\sum_{\chi \bmod^* q} |S(\chi)|^2 \le \frac{\phi(q)}{q} \sum_{a \bmod^* q} |S(a/q)|^2. \tag{1.40}$$

Nous utilisons alors le théorème de Siegel-Walfish pour les $T(\chi)$ et le théorème 1.7.1 pour les $S(\chi)$ via l'inégalité ci-dessus, ce qui nous donne

$$\Sigma \ll_{C_1} (\operatorname{Log} P)^{-C_1} P D_0^{1/2} (\operatorname{Log} D_0)(N + D_0 g(D_0))^{1/2} \|\alpha\|_2 + (\operatorname{Log} D)\Sigma'$$

pour $D_0 = (\operatorname{Log} P)^{2A+6}$ et $C_1 = 2A+6$. Pour ce qui est de $\Sigma'$, nous découpons la sommation en $q$ selon la taille de $q$. Il nous reste à majorer

$$\Sigma''(Q) = \frac{\operatorname{Log} Q}{Q} \sum_{Q<q\le 2Q} \sum_{\chi \bmod^* q} |S(\chi)|\,|T(\chi)|$$

que nous traitons par Cauchy-Schwartz et l'inégalité du grand crible :

$$\Sigma''(Q) \ll \frac{\operatorname{Log} Q}{Q}(P + P^{1/2}Q)\Big( \sum_{Q<q\le 2Q} \sum_{\chi \bmod^* q} |S(\chi)|^2\Big)^{1/2}.$$

Nous appliquons alors le théorème 1.7.1 et atteignons, pour $N \geq Dg(D)$,

$$\begin{aligned}\Sigma''(Q) &\ll \frac{\mathrm{Log}^2 Q}{Q}(P + P^{1/2}Q)Q^{1/2}\|\alpha\|_2 N^{1/2} \\ &\ll \|\alpha\|_2 P^{1/2}N^{1/2}\Big(\frac{P^{1/2}}{Q^{1/2}} + Q^{1/2}\Big)\,\mathrm{Log}^2 Q\end{aligned}$$

En collectant nos estimées, il s'ensuit que

$$\Sigma \ll_A \|\alpha\|_2 (\mathrm{Log}\, D)^3 P N^{1/2}\left((\mathrm{Log}\, P)^{-C_1} D_0^{1/2} + \frac{1}{D_0^{1/2}} + \frac{D^{1/2}}{P^{1/2}}\right)$$

ce qui nous permet de conclure facilement. $\diamond\diamond\diamond$

Nous avons convolé les $n^2$ avec des nombres premiers, mais n'importe quelle suite vérifiant un théorème de Siegel-Walfish bien entendu conviendrait. Et en utilisant simplement la suite des entiers, nous pouvons même gagner une puissance au niveau du terme d'erreur comme nous le montrons ci-après :

**Théorème 1.7.3** *Si $D \leq N/g(N)$ et $D \leq M^{2/3}$, nous avons*

$$\sum_{d\leq D}\max_{a \bmod^* d}\Big|\sum_{\substack{n\sim N, m\sim M\\ n^2 m\equiv a[d]}}\alpha(n) - \frac{M}{\phi(d)}\sum_{(n,d)=1}\alpha(n)\Big| \ll_A \|\alpha\|_2\sqrt{N}M\left(M^{-1/6}+N^{-1/2}\right)g(D)$$

*pour toute suite de complexes $(\alpha(n))_n$.*

**Preuve.** Nous suivons le schéma de preuve précédente et étudions

$$\Sigma = \sum_{d\leq D}\max_{a \bmod^* d}\Big|\sum_{\substack{n\sim N, m\sim M\\ n^2 m\equiv a[d]}}\alpha(n) - \frac{M}{d}\sum_{(n,d)=1}\alpha(n)\Big|.$$

Nous avons

$$\begin{aligned}\Sigma &= \sum_{d\leq D}\max_{a \bmod^* d}\Big|\frac{1}{\phi(d)}\sum_{\substack{\chi \bmod d\\ \chi\neq\chi_0}} S(\chi)T(\chi)\bar{\chi}(a)\Big| \\ &\leq \sum_{d\leq D}\frac{1}{\phi(d)}\sum_{\substack{\chi \bmod d\\ \chi\neq\chi_0}}|S(\chi)|\,|T(\chi)|\end{aligned}$$

avec (1.39). De façon habituelle, nous écrivons

$$\begin{aligned}\Sigma &\ll \operatorname{Log} D \sum_{1<q\le D} \frac{1}{\phi(q)} \sum_{\chi \bmod {}^* q} |S(\chi)|\,|T(\chi)| \\ &\ll (\operatorname{Log} D)^2 \Big( \sum_{1<q\le D_0} \sum_{\chi \bmod {}^* q} |S(\chi)|^2 \Big)^{1/2} \max_{\substack{\chi \bmod {}^* q \\ 1<q\le D_0}} |T(\chi)| + (\operatorname{Log} D)\Sigma'.\end{aligned}$$

Rappelons l'inégalité classique de Gallagher (1.40). Nous utilisons alors le théorème de Siegel-Walfish pour les $T(\chi)$ et le théorème 1.7.1 pour les $S(\chi)$ via l'inégalité ci-dessus, ce qui nous donne pour $N \ge D_0 g(D_0)$

$$\Sigma \ll_{C_1} (\operatorname{Log} D_0) D_0^{1/2} D_0^{1/2} N^{1/2} \|\alpha\|_2 + (\operatorname{Log} D)\Sigma'.$$

Pour ce qui est de $\Sigma'$, nous découpons la sommation en $q$ selon la taille de $q$. Il nous reste à majorer

$$\Sigma''(Q) = \frac{\operatorname{Log} Q}{Q} \sum_{Q<q\le 2Q} \sum_{\chi \bmod {}^* q} |S(\chi)|\,|T(\chi)|$$

que nous traitons en employant les inégalités de Cauchy-Schwartz et du grand crible, ce qui nous amène à :

$$\Sigma'(Q) \ll \frac{\operatorname{Log} Q}{Q} (M + M^{1/2}Q) \Big( \sum_{Q<q\le 2Q} \sum_{\chi \bmod {}^* q} |S(\chi)|^2 \Big)^{1/2}.$$

À l'aide du théorème 1.7.1, nous obtenons alors pour $N \ge Q g(Q)$

$$\begin{aligned}\Sigma''(Q) &\ll \frac{\operatorname{Log} Q}{Q} (M + M^{1/2}Q)\, \|\alpha\|^2 (Q^{1/2}N^{1/2} + Q g(Q)^{1/2}) \\ &\ll \|\alpha\|_2 M N^{1/2} \Big( \frac{1}{Q^{1/2}} + \frac{Q^{1/2}}{M^{1/2}} + \frac{g(Q)^{1/2}}{N^{1/2}} + \frac{Q}{M^{1/2}N^{1/2}} g(Q)^{1/2} \Big) \operatorname{Log} Q\end{aligned}$$

Par conséquent

$$\Sigma \ll \|\alpha\|_2 M N^{1/2} \left( \frac{D_0}{M} + \frac{D_0^{3/2}}{MN^{1/2}} + \frac{1}{D_0^{1/2}} + \frac{D^{1/2}}{M^{1/2}} + \frac{1}{N^{1/2}} + \frac{D}{M^{1/2}N^{1/2}} \right) g(D)$$

Nous prenons $D_0 = M^{2/3}$ ce qui donne

$$\Sigma \ll \|\alpha\|_2 \, MN^{1/2} \left( M^{-1/3} + N^{-1/2} + M^{-1/6} + \frac{D}{M^{1/2}N^{1/2}} \right) g(D)$$

et nous utilisons enfin $D \leq \sqrt{M^{2/3}N}$ ce qui nous permet de conclure facilement. $\diamond\diamond\diamond$

# Chapitre 2

# Un crible local pour les nombres premiers

Vioci une note de 1989 qui n'a pas été publiée. Le théorème 2.2.1 présente toutefois un intêret indépendant.

## 2.1 Introduction

La théorie générale du crible telle qu'elle a été développée par Selberg démontre qu'il n'existe pas de crible établissant l'existence d'une infinité de nombres premiers, et ce en vertu du célèbre principe de parité. De façon équivalente, le crible ne saurait donner mieux que $\pi(X) \leq (2 + o(1))X/\operatorname{Log} X$ où la constante 2 est capitale.

S'il s'agit de l'état des choses en toute généralité, il est possible de passer outre la barrière théorique si l'on utilise des propriétés supplémentaires des termes d'erreur. La terminologie appelle ces cribles des cribles locaux. Nous en présentons ici un qui brise le principe de parité en s'appuyant sur le fait que les parties fractionnaires $\{X/d\}$ pour $d \leq X$ sont en moyennes $< 1$. Plusieurs versions de ce fait sont développées en deuxième section, qui présente d'ailleurs un intérêt indépendant.

Le terme d'erreur est une chose, mais il faut rappeler que dans le cas précis des nombres premiers, le terme principal est délicat à évaluer puisque l'on n'a guère d'information sur la distribution de la fonction de Möbius ; Nous utilisons ici des identités combinatoires

pour évaluer le terme principal de façon suffisamment précise. Nous allons donc établir

$$(\dagger) \qquad 0.19X + \mathcal{O}(X^{2/3}\operatorname{Log} X) \leq \psi(X) \leq (2-0.19)X + \mathcal{O}(X^{2/3}\operatorname{Log} X),$$

à l'aide des poids

$$\sum_{d|n} \rho_d \quad \text{avec} \quad \rho_d = \mu(d)\left(1 - \frac{\gamma + \operatorname{Log} d}{\operatorname{Log} X}\right)$$

où $\gamma = 0.577\,215\,664\,\ldots$ est la constante d'Euler.

Rappelons qu'à la fin de l'exposé "On elementary methods in prime number-theory and their limitations", de 1952 à Oslo, Selberg mentionne la possibilité de construire un telle crible à partir des poids

$$\sum_{d|n} \rho_d \quad \text{avec} \quad \rho_d = \mu(d)\left(1 - \frac{\operatorname{Log} d}{\operatorname{Log} X}\right).$$

Dans notre traitement du terme principal, le $\gamma$ additionnel est essentiel.

Nous notons la partie entière du réel $y$ par $[y]$ et sa partie fractionnaire par $\{y\}$, de telle sorte que $y = [y] + \{y\}$. Rappelons que nous écrivons $y = \mathcal{O}^*(z)$ pour $|y| \leq z$.

## 2.2 Valeur moyenne des $\{X/d\}$

Soit $X \geq 1$ un nombre réel. Dans cette section, nous étudions les parties fractionnaires $\{X/d\}$, pour $d$ entier $\leq X$.

Soit $f$ une fonction (qui peut dépendre de $X$) à valeurs complexes. Supposons que

$$(H_1) \qquad \sum_{d\leq y} f(d) = M(f)y + \mathcal{O}(y^{1-\delta}) \qquad (X^{\frac{1}{1+\delta}} \leq y \leq X)$$

et

$$(H_2) \qquad \sum_{d\leq X^{\frac{1}{1+\delta}}} |f(d)| = \mathcal{O}((|M(f)| + \delta^{-1})\, X^{\frac{1}{1+\delta}})$$

avec $\delta > 0$, $M(f)$ et $C(f)$ des constantes dépendant de $f$ et $X$. Alors nous avons

$$(2.1) \qquad \sum_{d\leq y} \frac{f(d)}{d} = M(f)\operatorname{Log} y + C(f) + \mathcal{O}(\delta^{-1}y^{-\delta}) \qquad (X^{\frac{1}{1+\delta}} \leq y \leq X)$$

avec

$$C(f) = M(f) + \int_1^X \Big(\sum_{d\le t} f(d) - M(f)t\Big)\frac{dt}{t^2}.$$

La fonction $f(d) = \Lambda(d)$ avec $\delta^{-1} = c\sqrt{\operatorname{Log} X}$ vérifie donc ces hypothèses pour un certain $c > 0$. Les $\mathcal{O}$ de cette section dépendent au plus des constantes impliquées dans les $\mathcal{O}$ de $(H_1)$ et $(H_2)$ mais non de $\delta$, $X$, $M(f)$ ou $f$. Notre "constante" $C(f)$ dépend de $X$ mais l'intérêt principal de $(2.1)$ est que $C(f)$ ne dépende pas de $y$. Pour $\lambda > 0$, nous définissons

$$c_1(\lambda) = \lambda\int_\lambda^\infty \{t\}\frac{dt}{t^2}$$

ainsi que

$$c_2(\lambda) = \lambda\int_\lambda^\infty \{t\}\operatorname{Log} t\frac{dt}{t^2}.$$

Nous décrivons ces deux fonctions à la fin de cette section.

**Théorème 2.2.1** *Pour $\lambda \ge 1$ et $f$ vérifiant les conditions ci-dessus, nous avons*

$$\begin{cases} \displaystyle\sum_{d\le X/\lambda} f(d)\{X/d\} = c_1(\lambda)M(f)\frac{X}{\lambda} + \mathcal{O}\Big((|M(f)| + \delta^{-1})X^{\frac{1}{1+\delta}}\Big), \\ \displaystyle\sum_{d\le X/\lambda} f(d)\{X/d\}\operatorname{Log}\frac{X}{d} = c_2(\lambda)M(f)\frac{X}{\lambda} + \mathcal{O}\Big((|M(f)| + \delta^{-1})X^{\frac{1}{1+\delta}}\operatorname{Log} X\Big), \end{cases}$$

*Ces formules sont valables pour tout $\lambda > 0$ pour lequel $(H_1)$ est valide pour tout $y \le X/\lambda$.*

**Preuve.** Pour $\lambda \le X^{\frac{\delta}{1+\delta}}$, le lemme découle directement de $(H_2)$. Sinon posons $D = X^{\frac{1}{1+\delta}} \le X/\lambda$ et $L = X/D$. En nous inspirant du principe de l'hyperbole de Dirichlet, nous écrivons

$$\sum_{d\le X/\lambda} f(d)[X/d] = \sum_{d\le D} f(d)\sum_{\ell\le X/d} 1 + \sum_{\ell\le L}\sum_{d\le \min(X/\lambda, X/\ell)} f(d) - \sum_{\ell\le L} 1\sum_{d\le D} f(d).$$

En discutant selon que $\ell \le \lambda$ ou non et en utilisant $(H_1)$ et $(H_2)$, nous obtenons

$$\sum_{d\le X/\lambda} f(d)[X/d] = X(M(f)\operatorname{Log} X + C(f)) + M(f)X\left(\gamma - \frac{\{\lambda\}}{\lambda} - \sum_{\ell\le\lambda}\frac{1}{\ell}\right) + \mathcal{O}(R)$$

où

$$R = M(f)XL^{-1} + \delta^{-1}XD^{-\delta} + \lambda(X/\lambda)^{1-\delta} + \delta^{-1}X^{1-\delta}L^{\delta} + M(f)D + D^{1-\delta}$$
$$\ll \delta^{-1}XD^{-\delta} + \lambda^{\delta}X^{1-\delta} + M(f)D \ll \delta^{-1}XD^{-\delta} + M(f)D.$$

En comparant $\sum_{d\le X/\lambda} f(d)\{X/d\}$ à $\sum_{d\le X/\lambda} f(d)[X/d]$, nous obtenons

$$\sum_{d\le X/\lambda} f(d)\{X/d\} = M(f)X\Big(-\gamma + \frac{\{\lambda\}}{\lambda} - \operatorname{Log}\lambda + \sum_{\ell\le\lambda}\frac{1}{\ell}\Big) + \mathcal{O}(R).$$

Nous écrivons alors

$$\frac{\{\lambda\}}{\lambda} + \sum_{\ell\le\lambda}\frac{1}{\ell} = 1 + \sum_{\ell\le\lambda}\big(\frac{1}{\ell} - \frac{1}{\lambda}\big) = 1 + \operatorname{Log}\lambda - \int_1^{\lambda}\frac{\{t\}}{t^2}dt$$

et rappelons que

$$\gamma - 1 = -\int_1^{\infty}\frac{\{t\}}{t^2}dt$$

ce qui nous permet de conclure facilement en ce qui concerne la première égalité du lemme tout au moins. La seconde s'en déduit essentiellement par sommations par parties. $\diamond\diamond\diamond$

À partir du Théorème 2.2.1 et de l'estimation élémentaire classique

$$\sum_{d\le X}\mu^2(d) = \frac{6}{\pi^2}X + \mathcal{O}(\sqrt{X}), \qquad (X\ge 1)$$

nous obtenons

**Lemme 2.2.1** *Pour $\lambda \ge 1$, nous avons d'une part*

$$\sum_{d\le X/\lambda}\mu^2(d)\,\{X/d\} = \frac{6}{\pi^2}c_1(\lambda)\frac{X}{\lambda} + \mathcal{O}(X^{2/3}),$$

*et d'autre part*

$$\sum_{d\le X}\mu^2(d)\left\{\frac{X}{d}\right\}\operatorname{Log}\frac{X}{d} = \frac{6}{\pi^2}C_3X + \mathcal{O}(X^{2/3}\operatorname{Log}X)$$

*avec* $C_3 = c_2(1) = \int_1^{\infty}\{t\}\operatorname{Log}t\,dt/t^2 = 0.49\ldots$

**Une étude rapide de $c_1$ et de $c_2$ :**

Les fonctions $c_1$ et $c_2$ sont continues, dérivables en tout point $\lambda$ non entier et dérivables à droite et à gauche aux entiers. Nous avons

$$\lambda c_1'^{\pm}(\lambda) = c_1(\lambda) - \{\lambda \pm\}$$

où $c_1'^{+}$ désigne la dérivée à droite et $c_1'^{-}$ celle à gauche. Comme $c_1(\lambda) \in ]0,1[$, il vient $c_1'^{+}(n) > 0$ et $c_1'^{-}(n) > 0$ pour tout entier $n$. L'équation différentielle ci-dessus nous donne alors les variations : en effet dans $]n, n+1[$, il existe $\lambda_n$ pour lequel $c_1'(\lambda_n) = 0$, la dérivée étant positive à gauche de $\lambda_n$ et négative à sa droite. Passé ce point, $c_1(\lambda)$ commence à décroître, mais $\{\lambda\}$ croît, ce qui laisse la dérivée de plus en plus négative. En conséquence, $c_1$ est unimodale sur chaque intervalle $]n, n+1[$, et le même raisonnement s'applique à $c_2$.

Par ailleurs, nous avons

$$c_1(\lambda) = \frac{1}{2} - \frac{B_1(\lambda)}{\lambda} + 2\lambda \int_{\lambda}^{\infty} B_1(t) \frac{dt}{t^3}$$

avec $B_1(t) = \int_0^u (\{u\} - \frac{1}{2}) du \leq 0$, ce qui nous donne

$$\frac{1}{2} - \frac{B_1(\lambda)}{\lambda} - \frac{1}{4\lambda} \leq c_1(\lambda) \leq \frac{1}{2} - \frac{B_1(\lambda)}{\lambda}.$$

En particulier $c(\lambda) = \frac{1}{2} + \mathcal{O}^*(1/(4\lambda))$. Comme $c(\lambda_n) = \{\lambda_n\} = \lambda_n - n$, il vient

$$\lambda_n = n + \frac{1}{2} + \mathcal{O}^*(1/(4n)).$$

Remarquons aussi la valeur spéciale $c_1(1) = 1 - \gamma$, qui constitue quasiment la définition de la constante d'Euler $\gamma$.

## 2.3 Le crible

**Lemme 2.3.1 (Terme Principal)** *Pour $X \geq 1$, nous avons*

$$\sum_{d \leq X} \frac{\mu(d)}{d} \left( \operatorname{Log} \frac{X}{d} + \gamma \right) = 1 + \mathcal{O}^* \left( \frac{7}{12} \frac{6}{\pi^2} \right) + \mathcal{O}\big(X^{-\frac{1}{2}}\big).$$

**Preuve.** Nous commençons par remarquer que

$$\sum_{d\le X}\frac{\mu(d)}{d}\sum_{m\le X/d}\frac{1}{m}=1,$$

et il nous suffit alors d'utiliser

$$\sum_{m\le y}\frac{1}{m}=\operatorname{Log} y+\gamma+\mathcal{O}^*(7/(12y))\qquad(y\ge 1).$$

Le lemme s'ensuit directement. $\diamond\diamond\diamond$

Pour établir $(\dagger)$, nous procédons comme suit :

$$\begin{aligned}\sum_{n\le X}\Lambda(n)&=\sum_{n\le X}\left(\sum_{d|n}\mu(d)\left(\operatorname{Log}\frac{X}{d}+\gamma\right)\right)-\operatorname{Log}X-\gamma\\&=\sum_{d\le X}\mu(d)\left(\operatorname{Log}\frac{X}{d}+\gamma\right)\left[\frac{X}{d}\right]-\operatorname{Log}X-\gamma\\&=\left(1+\mathcal{O}^*\left(\frac{7}{12}\frac{6}{\pi^2}+\frac{6}{\pi^2}C_3+\frac{6}{\pi^2}\gamma(1-\gamma)\right)\right)X+\mathcal{O}(X^{2/3}\operatorname{Log}X),\end{aligned}$$

et le miracle tient en ce que

$$\frac{6}{\pi^2}\big(\tfrac{7}{12}+C_3+\gamma(1-\gamma)\big)=0.80\ldots$$

Une dernière remarque : avec $\sum_{d|n}\mu(d)\operatorname{Log}\frac{X}{d}$ au lieu de $\sum_{d|n}\mu(d)(\operatorname{Log}\frac{X}{d}+\gamma)$, notre constante devient $1+\mathcal{O}^*(\frac{6}{\pi^2}(\frac{7}{12}+\gamma+C_3))$ qui peut être $<0$ !

# Chapitre 3

# Sur le problème de Goldbach effectif

Voici un article d'exposition constitué de trois parties. Dans la première, nous retraçons l'histoire des majorations de la constante de Šnivel'man à travers ses principales étapes et arrivons ainsi à un résultat de l'auteur : tout entier pair est somme d'au plus 6 nombres premiers. La seconde partie ébauche les grandes lignes de la preuve de ce dernier théorème. Enfin, dans une troisième partie, nous commentons des résultats récents sur la connaissance numérique de la répartition des nombres premiers dans les progressions arithmétiques. Il s'agit là d'un outil important pour la seconde partie.

## 3.1 Introduction.

Nous nous intéressons ici au problème de Goldbach (1742) qui se forme des deux assertions suivantes :

"Tout entier pair est somme d'au plus deux nombres premiers",

"Tout entier impair $\neq 1$ est somme d'au plus trois nombres premiers".

La seconde découle aisément de la première et il s'agit en fait ici de la formulation d'Euler.

Le résultat le plus important dans cette direction est bien sûr celui de Vinogradov qui obtenait en 1937 que tout entier impair assez grand peut être écrit comme somme de trois nombres premiers. Vinogradov utilisait alors la méthode du cercle et des renseignements

profonds sur la distribution des nombres premiers dans les progressions arithmétiques. L'on peut se demander ce que "assez grand" signifie dans ce théorème ; [*Chen & Wang,* 1989] montre que l'on peut remplacer "assez grand" par "supérieur à $\exp(100\ 000)$" (ce qui laisse l'infini à un distance respectable : ce théorème n'est connu pour aucun des entiers de l'univers). $^*$

D'un point de vue effectif, le problème principal vient d'une mauvaise connaissance de la distribution des nombres premiers dans les progressions arithmétiques de modules de l'ordre d'une puissance de logarithme du nombre que l'on cherche à représenter. La borne de J. Chen & T. Wang est très large non pas à cause de l'éventuel zéro de Siegel mais à cause d'une mauvaise connaissance des zéros des fonctions $L$.

## 3.2 L'approche de Šnirel'man.

En 1933 et de façon remarquablement élémentaire, Šnirel'man établissait le théorème suivant :

**Théorème 3.2.1 ( [*Šnirel'man,* 1933])** *Il existe un plus petit entier $w$ tel que tout entier $\neq 1$ soit somme d'au plus $w$ nombres premiers.*

C'est cet entier $w$ qui porte le nom de constante de Šnirel'man. Détaillons la preuve de Šnirel'man :

Posons

$$\rho(N) = \sum_{p_1+p_2=N} 1. \tag{3.1}$$

Alors nous savons minorer $\rho(N)$ en moyenne :

$$\sum_{N\leq X} \rho(N) \geq \pi(X/2)^2 \gg \Big(\frac{X}{\operatorname{Log} X}\Big)^2 \quad \text{pour } X \geq 2\ . \tag{3.2}$$

Par ailleurs, nous savons majorer chaque $\rho(N)$ en utilisant un argument de crible :

$$\rho(N) \ll \mathfrak{S}_2(N)\frac{N}{\operatorname{Log}^2 N} \tag{3.3}$$

$*$. Depuis [*Liu & Wang,* 2002] ont amélioré cette borne mais elle reste gigantesque. [*Deshouillers* et al. , 1997] ont aussi montré que tout entier impair $\geq 3$ est somme d'au plus trois nombres premiers sous l'hypothèse de Riemann généralisée. Sous seulement l'hypothèse de Riemann, voir [*Kaniecki,* 1995].

pour $N$ entier pair $\geq 2$.

Le facteur arithmétique $\mathfrak{S}_2(N)$ tient compte des obstructions locales à représenter $N$ comme somme de deux nombres premiers et s'écrit :

$$\mathfrak{S}_2(N) = \mathfrak{S}_2 \prod_{\substack{p|N \\ p\neq 2}} \Big(\frac{p-1}{p-2}\Big) \quad \text{avec} \quad \mathfrak{S}_2 = 2\prod_{p\geq 3}\Big(1-\frac{1}{(p-1)^2}\Big)\,.$$

On conjecture que $\rho(N)$ est équivalent à $\mathfrak{S}_2(N)\frac{N}{\mathrm{Log}^2\, N}$ , ce qui montre que notre argument ne perd qu'une constante. Il convient aussi de noter que, si le facteur arithmétique n'est pas borné, il est toutefois constant en moyenne ainsi que toutes ses puissances.

A partir de la connaissance de $\rho(N)$ en moyenne (3.2) et de la majoration (3.3), qui nous assure que $\rho(N)$ n'est pas distribuée de façon trop irrégulière, nous pouvons conclure que $\rho(N)$ est souvent non nul. En effet, l'inégalité de Cauchy-Schwarz nous donne

$$\begin{aligned}\Big(\sum_{N\leq X}\rho(N)\Big)^2 &\leq \sum_{N\leq X}\rho(N)^2 \sum_{\substack{N\leq X\\ \rho(N)\neq 0}} 1\\ &\ll \frac{X^2}{\mathrm{Log}^4\, X}\sum_{N\leq X}\mathfrak{S}_2^2(N)\sum_{\substack{N\leq X\\ \rho(N)\neq 0}} 1 \ll \frac{X^3}{\mathrm{Log}^4\, X}\sum_{\substack{N\leq X\\ \rho(N)\neq 0}} 1.\end{aligned}$$

En composant avec (3.2), nous obtenons

$$X \ll \mathrm{Card}\{N\leq X,\ \exists p_1,p_2\ /\ N=p_1+p_2\} \tag{3.4}$$

L'ensemble $\mathcal{A}$ des entiers qui sont somme de deux nombres premiers admet donc une densité positive. La théorie de Šnirel'man sur l'addition des suites (théorie qui fut forgée pour ce problème) permet alors de conclure que tout entier pair est somme d'un nombre borné d'éléments de $\mathcal{A}$ et l'on finit en remarquant que, si $N$ est un entier impair $\geq 3$, $N-3$ est pair.

Certains détails technique de cette preuve s'allègent si l'on opère avec $N$ dans un intervalle $]X,2X]$ et avec

$$r_2(N) = \sum_{\substack{p_1+p_2=N\\ p_1\leq X}} \mathrm{Log}\, p_1 \tag{3.5}$$

où l'on a ajouté un poids lisse $\mathrm{Log}\, p_1$ et une condition de taille sur $p_1$, ce qui ne change pas la nature arithmétique de $r_2(N)$ car $X$ et $N$ sont de tailles comparables. On conjecture que $r_2(N) \sim \mathfrak{S}_2(N)\frac{X}{\mathrm{Log}\, X}$ .

## 3.3 Un peu d'histoire

Depuis 1933, de nombreux mathématiciens se sont penchés sur le problème d'obtenir une majoration numérique de la constante $w$ de Šnirel'man. La chasse a été ouverte par [*Klimov,* 1969] qui obtenait $w \leq 6.10^9$, début peu encourageant mais vite amélioré dans [*Klimov* et al. *,* 1972] en $w \leq 115$, où l'on aborde des zones raisonnables.

De 1972 à 1982, d'autres majorations ont été obtenues mais nous n'en présentons que trois qui nous intéressent particulièrement.

[*Deshouillers,* 1972/73] ajoutait une idée en remarquant que l'inégalité de Cauchy-Schwarz n'avait pas de raisons d'être meilleure que celle de Hölder et en utilisant celle-ci, il obtenant $w \leq 67$. Un troisième pas était franchi entre 1976 et 1977 avec l'apparition de la démonstration, optimale tant sur les plans théorique que numérique, donnée par [*Montgomery & Vaughan,* 1973] de l'inégalité de Brun-Titchmarsh. [*Vaughan,* 1977] et [*Deshouillers,* 1976?] obtenaient alors successivement $w \leq 27$ et $w \leq 26$, et il apparaît à ce moment une disparité remarquable dans leurs peuves ; elles sont très semblables et partent toutes deux d'une application de l'inégalité de Hölder avec un exposant $\lambda$ attaché à $\rho(N)$. Mais, il semble à Vaughan que la valeur optimale de $\lambda$ est 3,75 et à Deshouillers que cette valeur optimale est 9 ! À comparer de plus près les deux preuves, on constate de légères différences dans le traitement du facteur arithmétique. C'est en fait là que réside le problème principal et il n'est pas difficile de se convaincre que, de ce point de vue, l'exposant $\lambda = \infty$ est optimal. Mais cela nécessite une modification de la preuve.

## 3.4 Une idée de Shapiro & Warga...

Une telle modification a été théoriquement mise au point dans [*Shapiro & Warga,* 1950].

Leur idée repose sur une inégalité du type suivant :

$$\sum_{X<N\leq 2X} \mathfrak{S}_2^{-1}(N) r_2(N) \leq \max_{X<N\leq 2X} \mathfrak{S}_2^{-1}(N) r_2(N) \sum_{\substack{X<N\leq 2X \\ r_2(N)\neq 0}} 1 \,, \tag{3.6}$$

qui a l'immense avantage de ne rien perdre, au moins de façon conjecturale, puisque l'on pense que $\mathfrak{S}_2^{-1}(N)r_2(N)$ est constant (et vaut $X/\operatorname{Log} X$ cf. (3.5)).

Le crible de Selberg nous donne

$$r_2(N) \leq (8+o(1))\mathfrak{S}_2(N)\frac{X}{\operatorname{Log} X} \tag{3.7}$$

où l'on ne perd donc que le facteur $8+o(1)$. Toutefois, il est plus difficile d'obenir un minoration du membre de gauche de (3.6). La technique standard consiste à écrire

$$\mathfrak{S}_2^{-1}(N) = \mathfrak{S}_2^{-1} \sum_{\substack{d|N \\ d \text{ impair}}} \frac{\mu(d)}{\phi(d)} \, . \tag{3.8}$$

On obtient alors

$$\sum_{X<N\leq 2X} \mathfrak{S}_2^{-1}(N)r_2(N) = \mathfrak{S}_2^{-1} \sum_{d \text{ impair}} \frac{\mu(d)}{\phi(d)} \left\{ \sum_{\substack{X<N\leq 2X \\ N\equiv 0[2d]}} r_2(N) \right\}$$

et la somme intérieure dans le membre de droite fait clairement appel à la répartition des nombres premiers dans les progressions arithmétiques. Grâce au facteur $\phi(d)^{-1}$, nous montrons à l'aide de l'inégalité de Brun-Titchmarsh que la série en $d$ est convergente ; la connaissance des premiers termes nous permet alors d'approcher l'équivalent. Toutefois, rien de numérique n'était connu jusqu'à très récemment sur la répartition des nombres premiers en progressions arithmétiques (nous y reviendrons) ce qui laissait la démonstration "théorique".

Arrêtons-nous un instant pour regarder la meilleure majoration de la constante de Šnirel'man que pourrait donner cette preuve ; au mieux, nous obtiendrions que le cardinal des entiers sommes de deux nombres premiers entre $X$ et $2X$ est minoré par $\frac{X}{2} \times \frac{1}{8}$, c'est-à-dire qu'en gros un entier pair sur 8 est somme de deux nombres premiers. Le théorème de Mann nous dit alors que tout entier pair est somme d'au plus 8 entiers, chacun étant somme d'au plus deux nombres premiers. La limite de la méthode est par conséquent $w \leq 2 \times 8 + 1 = 17$.

Remarquons encore qu'il faudrait ajouter une idée pour atteindre cette limite puisqu'il apparaît des termes d'erreur. Le mieux que l'on puisse raisonnablement espérer en suivant cette preuve est donc $w \leq 19$. Ce qui fut achevé par Riesel & Vaughan en 1983.

## 3.5 ... Et la réalisation de Riesel & Vaughan.

Ils obtiennent précisément

**Théorème 3.5.1 (Théorème [*Riesel & Vaughan,* 1983])** *Tout entier pair est somme d'au plus 18 nombres premiers.*

Leur preuve suit celle de Shapiro & Warga. Mais tout d'abord, ils montrent en utilisant le grand crible pondéré de Montgomery & Vaughan que, pour tout réel $X > 1$ et tout entier pair $N$ dans $]X, 2X]$, on a

$$r_2(N) \leq 8\mathfrak{S}_2(N)\frac{X}{\operatorname{Log} X}\ . \tag{3.9}$$

(Ils prouvent en fait un résultat un peu plus précis que celui-là). Le point remarquable ici est d'avoir obtenu la constante 8 sans terme d'erreur additionnel. La seconde idée majeure trouve son origine dans le lemme suivant :

**Lemme 3.5.1** *Soit $d$ un entier $\geq 1$, $I$ un intervalle borné ne contenant aucun des facteurs premiers de $d$, on a*

$$\sum_{N\equiv 0[d]}\left(\sum_{\substack{p_1+p_2=N\\ p_1,p_2\in I}}\operatorname{Log} p_1\ \operatorname{Log} p_2\right) = \frac{1}{\phi(d)}\sum_{\chi\ \mathrm{mod}\ d}\chi(-1)|S(\chi)|^2$$

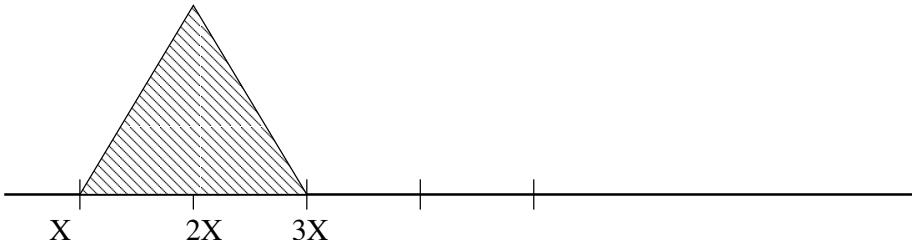
*avec $S(\chi)=\sum_{p\in I}\operatorname{Log} p\,\chi(p)$ et où la somme est prise sur tous les caractères de Dirichlet modulo $d$.*

Cette identité est remarquable en ce qu'elle remplace les variables $\left(\sum_{N\equiv 0[d]}\cdots\right)_d$ par les variables $\big(S(\chi)\big)_\chi$ (historiquement introduites dans [*Bombieri & Davenport,* 1968]), et que ces dernières ont un unique pic sur le caractère principal et sont petites partout ailleurs.

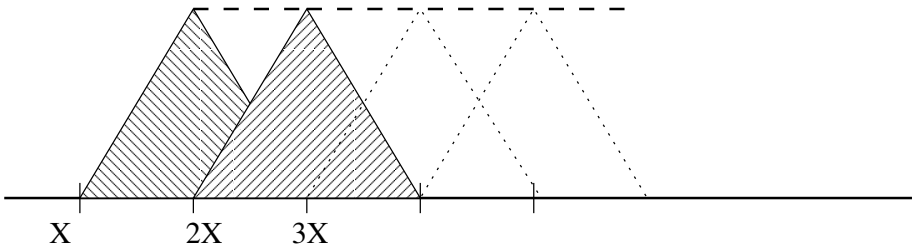
Toutefois, pour pouvoir utiliser cette identité, il nous faut opérer avec le nombre de représentations

$$r_I(N) = \sum_{\substack{p_1+p_2=N\\ p_1,p_2\in I}}\operatorname{Log} p_1\ \operatorname{Log} p_2 \tag{3.10}$$

et ce dernier n'est plus "plat à l'infini". Précisons cela : l'équivalent conjecturé pour $r_I(N)$ est $\mathfrak{S}_2(N)s_I(N)$ où, si l'on prend $I=]\frac{X}{2},\frac{3X}{2}]$, le graphe de $s_I$ est le suivant :




Il n'est donc pas constant. Pourtant, si l'on considère $r_{I_1} + r_{I_2}$ avec $I_1 = ]\frac{X}{2}, \frac{3X}{2}]$ et $I_2 = ]X, 2X]$, on obtient




où l'on voit apparaître une région plate entre $2X$ et $3X$ ... Riesel & Vaughan réitèrent ce procédé 201 fois pour obtenir un nombre de représentations à peu près constant.

Réunissant ces deux arguments, ils concluent.

Il est remarquable que cette preuve n'utilise pas de renseignements sur la répartition des nombres premiers dans les progressions arithmétiques autres que ceux qui sont issus du crible (seules les tables de Rosser & Schoenfeld sont utilisées).

## 3.6 Faire mieux.

Dans la preuve précédente, le seul endroit où nous perdons quelque chose est l'inégalité qui provient de crible. Tout repose sur

$$r_2(N) \leq 8 \times \text{valeur conjecturée} .$$

Mais en fait, nous n'avons besoin de cette majoration que "presque partout", i.e. en dehors d'un ensemble de petit cardinal. En utilisant la méthode du cercle et le théorème de Siegel-Walfish, on peut alors obtenir pour tout $\varepsilon > 0$

$$r_2(N) \leq (1+\varepsilon) \times \text{valeur conjecturée} \quad pp .$$

Nous allons montrer comment éviter ce théorème pour obtenir

$$r_2(N) \leq (2+\varepsilon) \times \text{valeur conjecturée} \quad pp\ .$$

pour tout $\varepsilon > 0$, ce qui nous amènera au résultat suivant :

**Théorème 3.6.1** *Tout entier pair est somme d'au plus 6 membres premiers.*

Signalons qu'en utilisant une méthode analogue, j'ai obtenu dans ma thèse $w \leq 13$.

Nous allons à présent donner les grandes lignes de cette méthode.

Il nous faut tout d'abord signaler que les règles du jeu ont changé depuis Riesel & Vaughan. En effet, nous sommes à présent en mesure de démontrer de façon numérique le théorème des nombres pemiers dans des progressions de module $\leq 60$. Nous renvoyons le lecteur au paragraphe X pour plus de détails. Dans la méthode de Shapiro & Warga, la minoration ne présente donc plus de difficultés.

## 3.7 Un problème plus général.

Ici, nous recherchons une majoration du nombre de représentations d'un entier $N$ en somme de deux nombres premiers, problème qui est contenu dans le suivant :

**Problème :** Soit $\alpha$ une suite pondérée positive à support dans $[0, X]$ et $N$ un entier $\geq X$ ; Construire une majoration de

$$r(N) = \sum_{\sqrt{X}<p} \alpha(N-p)\ .$$

Nous considérons $R(N) = \sum_y \beta(y)\alpha(N-y)$ où $\beta$ est une suite pondérée qui majore la fonction caractéristique des nombres premiers $> \sqrt{X}$. Nous avons bien sûr

$$r(N) \leq R(N)$$

et il nous reste à choisir $\beta$ de façon à ne pas perdre trop.

Nous prenons

$$\beta(y) = \left( \sum_{\substack{d|y \\ d \leq X^{\frac{1}{2}+\varepsilon}}} \lambda_d \right)^2 \tag{3.11}$$

pour un $\varepsilon > 0$ où les $\lambda_d$ sont ceux de Selberg. Notre fonction $\beta$ a bien la propriété attendue et l'on a

$$\sum_{y\leq X}\beta(y) = \big(2+\varepsilon+o(1)\big)\frac{X}{\operatorname{Log} X} \qquad\qquad (X\to+\infty)$$

ce qui signifie que notre suite est $(2+\varepsilon)$ fois plus large que la suite des nombres premiers. Une manipulation standard nous donne alors

$$R(N) = \sum_{d\leq X^{\frac{2}{2+\varepsilon}}} w_d \sum_{a \mod d}^{*} S_\alpha(a/d)e(-Na/d) \tag{3.12}$$

où

$$\begin{cases} e(u) = \exp(2i\pi u)\ , \\ S_\alpha(u) = \displaystyle\sum_m \alpha(m)e(mu)\ , \\ w_d \simeq \dfrac{\mu(d)}{\phi(d)}\dfrac{2+\varepsilon}{\operatorname{Log} X} \end{cases}$$

Le coefficient $w_d$ appelle quelques explications. Tout d'abord le signe "$\simeq$" est à lire comme "se comporte comme" ; plus précisément, il peut être remplacé par une équivalence si $d$ est borné par une puissance fixée de $\operatorname{Log} X$. Pour $d$ plus grand, nous disposons de majorations du type

$$|\operatorname{Log} X\,\phi(d)w_d| \ll 3^{w(d)}\ .$$

Notons ici que $w_d$ correspond pour la suite $\beta$ à la quantité $\frac{1}{X}\sum_{p\leq X} e(pa/d)$ pour la fonction caractéristique des nombres premiers.

Remarquons dès à présent que cette expression de $R(N)$ est bien adaptée pour employer l'inégalité du grand crible.

## 3.8 Schéma de la preuve du théorème.

Nous posons $S_\alpha = T$ où $T(u) = \sum_{p\leq X} \operatorname{Log}\ p\, e(pu)$ et avons

$$r_2(N) \leq R_2(N)$$

(modulo le changement de notations $r_2(N)$ au lieu de $R(N)$). La méthode de Shapiro & Warga nous mène à considérer

$$\sum_{\substack{X<N\leq 2X\\ r_2(N)\neq 0}} \mathfrak{S}_2^{-1}(N) R_2(N)$$

qui se réécrit en

$$\sum_{d\leq X^{\frac{2}{2+\varepsilon}}} w_d \sum_{a \mod d}^{*} T(a/d)\bar{U}(a/d) \tag{3.13}$$

où $U(x) = \sum_{\substack{X<N\leq 2X\\ r_2(N)\neq 0}} \mathfrak{S}_2^{-1}(N) e(Nu)$.

Sur cette expression, nous voyons clairement que nous nous occupons d'un problème ternaire (et non binaire ; la sommation en $N$ fournit la troisième variable).

Pour étudier cette quantité, écartons tout d'abord les grands "$d$" à l'aide de l'inégalité du grand crible (et de celle de Cauchy-Schwarz pour séparer $T$ et $\bar{U}$)

$$\left| \sum_{B<d\leq X^{\frac{2}{2+\varepsilon}}} w_d \sum_{a \mod d}^{*} T(a/d)\bar{U}(a/d) \right| \ll \frac{1}{\operatorname{Log} X} \sqrt{X \operatorname{Log} X}\sqrt{X}\Big(X^{\frac{2}{2+\epsilon}} + \frac{X}{B}\Big)\,. \tag{3.14}$$

ceci est à comparer à $X^2/\operatorname{Log} X$. Nous prendrons $B = X^{0.3}$ ($B/\sqrt{\operatorname{Log} X} \to +\infty$ suffirait).

Ensuite, remplaçons $T(a/d)$ par sa valeur conjecturée $\frac{\mu(d)}{\phi(d)}T(0)$. Nous obtenons :

$$\sum_{d\leq B} w_d \sum_{a \mod {}^{*}d}^{*} \frac{\mu(d)}{\phi(d)} T(0)\bar{U}(a/d) \simeq \frac{2+\varepsilon}{\operatorname{Log} X} T(0) \sum_{\substack{X<N\leq 2X\\ r_2(N)\neq 0}} \mathfrak{S}_2^{-1}(N) \sum_{d\leq B} \frac{\mu^2(d)}{\phi^2(d)} c_d(N) \tag{3.15}$$

c'est-à-dire que ce terme vaut, à des termes d'erreur près,

$$\frac{2+\epsilon}{\operatorname{Log} X} X\Big(1+\mathcal{O}\Big(\frac{1}{\sqrt{B}}\Big)\Big) \sum_{\substack{X<N\leq 2X\\ r_2(N)\neq 0}} 1 \tag{3.16}$$

moyennant de remarquer que $\mathfrak{S}_2(N) = \sum_d \frac{\mu^2(d)}{\phi^2(d)} c_d(N)$.

Nous avons enfin à contrôler l'erreur commise en remplaçant $T(a/d)$ par $\frac{\mu(d)}{\phi(d)}T(0)$.

Or

$$\left|\sum_{d\leq B} w_d \sum_{a \bmod d}^{*} \Big(T(a/d) - \frac{\mu(d)}{\phi(d)} T(0)\Big)\bar{U}(a/d)\right|^2$$

$$\ll X(X+B^2) \sum_{d\leq B} |w_d|^2 \sum_{a \bmod d}^{*} \left|T(a/d) - \frac{\mu(d)}{\phi(d)} T(0)\right|^2 \qquad (3.17)$$

et, suivant la démonstration du théorème de Barban-Davenport-Halberstam, nous introduisons les caractères de Dirichlet. Notre majoration se réécrit, à une constante $> 0$ multiplicative près,

$$X(X+B^2) \sum_{1\neq q\leq B} t(q) \sum_{\chi \bmod q}^{*} |T(\chi)|^2 \qquad (3.18)$$

avec

$$t(q) = q \sum_{\substack{d\leq B \\ d\equiv 0[q]}} \frac{|w_d|^2}{\phi(d)} \, . \qquad (3.19)$$

Maintenant, si $q$ est grand, $t(q)$ est petit $\Big(\mathcal{O}\big(\frac{1}{q^{2-\epsilon}} \frac{1}{\mathrm{Log}^2\, X}\big)\Big)$ et

$$\sum_{q\leq B} \sum_{\chi \bmod q}^{*} |T(\chi)|^2 \leq \frac{X \ \mathrm{Log} \ X(X+\sqrt{X}^2)}{\mathrm{Log} \ \frac{\sqrt{X}}{B}} \, , \qquad (3.20)$$

d'où

$$\sum_{A\leq q\leq B} t(q) \sum_{\chi \bmod q}^{*} |T(\chi)|^2 \ll \frac{1}{A^{2-\varepsilon}} \frac{X^2}{\mathrm{Log}^2\, X} \, . \qquad (3.21)$$

Lorsque $q$ est petit, $T(\chi)$ l'est aussi grâce au théorème des nombres premiers dans les progessions arithmétiques.

Nous obtenons par ce procédé

$$\text{Si} \quad X \geq \exp(67) \quad \text{alors} \quad \text{Card}\big\{X < N \leq 2X/N = p_1 + p_2\big\} \geq \frac{X}{2\times 2,5}$$

et il nous faut à présent conclure que tout entier pair est somme d'au plus $3\times 2$ nombres premiers. Remarquons que nous ne savons pas montrer le résultat précédent pour $X < \exp(67)$ ce qui nous empêche d'utiliser le théorème de Mann. Pourtant, nous pouvons montrer par un simple argument de descente que tout entier pair $\leq \exp(72)$ est somme

d'au plus 6 nombres premiers. En effet, soit $N$ un tel entier. Les tables de [*Rosser & Schoenfeld,* 1975] nous donnent un $\varepsilon > 0$ tel que l'intervalle $[(1-\varepsilon)N, N]$ contienne un nombre premier au moins, disons $p$. Alors $N - p \leq \varepsilon \exp(72)$ et l'on itère le procédé $^*$. Il y avait donc un problème pour les entiers $\geq \exp(67)$, qui est résolu au paragraphe suivant.

## 3.9 Un résultat de théorie additive.

Nous devons ce résultat à Deshouillers, qui fut entre autre mon directeur de thèse, et je suis ici heureux de le remercier pour ce résutat fort utile. Il s'agit d'une version effective d'un théorème d'Ostmam.

Nous adoptons la notation usuelle : si $\mathcal{A}$ est une suite d'entiers et si $X$ est un réel, alors $A(x)$ est le nombre d'éléments de $\mathcal{A}$ qui sont dans $[1, X]$.

**Théorème 3.9.1 (Deshouillers, 1991)** *Soit $\mathcal{A}$ une suite d'entiers contenant $0$. Nous supposons qu'il existe un réel $\sigma$ et des entiers $H, U$ et $n_0$ tels que*

1. *Pour $n \geq n_0$, on a $A(n) \geq \sigma n + (H-1)\frac{K(K+1)}{2}$,*
2. *$\{0, 1, \cdots, K\} \subset \mathcal{A}$ et $\{n_0, n_0+1 \cdots, n_0+U\} \subset \mathcal{A}$ ,*
3. *$(K+1)H\sigma \geq K + H$ .*

*Alors tout entier $\geq Hn_0$ est somme d'au plus $H$ éléments de $\mathcal{A}$.*

Remarquons que hypothèses et conclusions sont similaires à celles du théorème de Mann usuel, mais qu'ici, seuls des renseignements asymptotiques sur $\mathcal{A}$ sont accessibles. L'hypothèse (1) seule n'est pas suffisante pour assurer la conclusion car nous avons à éviter le cas des progressions arithmétiques. Il est marquant que l'hypothèse (2) soit suffisante pour écarter ce cas.

Nous prendrons $H = 3$, $K = 39$, $\sigma = \frac{7}{20}$ et $n_0 = 1.002.10^{30}$ pour conclure. L'hypothèse (2) est vérifiée par un calcul sur ordinateur.

$*$. En fait, les dites tables ne suffisent pas tout à fait, mais en utilisant le fait que l'hypothèse de Riemann a été vérifiée jusqu'à une plus grande hauteur qu'en 1976, il est possible de les améliorer. De plus l'article [*Ramaré & Saouter,* 2003] contient maintenant de bien meilleures valeurs.

## 3.10 Résultats effectifs sur la répartition des nombres premiers en progressions arithmétiques.

Donnons-nous un entier $d \geq 1$ et un entier $a$ premier à $d$. Nous nous intéressons à

$$\theta(X; d, a) = \sum_{\substack{p \leq X \\ p \equiv a[d]}} \text{Log } p$$

Avant d'exposer notre problème, introduisons une notation pratique : si $f$ et $g$ sont deux fonctions, $f$ à valeurs complexes et $g$ à valeurs réelles, l'écriture $f(x) = \mathcal{O}^*\big(g(x)\big)$ signifie $|f(x)| \leq g(x)$.

Notre problème s'énonce alors ainsi :

Déterminer des couples $(\varepsilon_d, X_0)$ tels que

$$\theta(X, d, a) = \frac{X}{\phi(d)}\big(1 + \mathcal{O}^*(\varepsilon_d)\big) \quad \text{pour} \quad X \geq X_0 \ .$$

Rappelons que le théorème des nombres premiers dans les progressions arithmétiques nous assure que, pour $d$ fixé,

$$\theta(X; d, a) \sim \frac{X}{\phi(d)} \quad (X \to +\infty) \ .$$

Pour $d = a = 1$, des solutions très satisfaisantes ont été obtenues par Rosser et Schoenfeld dans un travail qui s'étend de 1941 à 1976 : [*Rosser,* 1941], [*Rosser & Schoenfeld,* 1975], [*Schoenfeld,* 1976]

Ces résultats s'appuyent sur un procédé de régularisation de $\theta(X; 1, 1)$ qui s'est avéré très efficace. [*McCurley,* 1984a] et [*McCurley,* 1984b] a adapté ce procédé aux fonctions $\theta(X; d, a)$. Donnons-en le principe. Soit $h$ un réel $> 0$ et considérons

$$\theta_1(X; d, a) = \frac{1}{h}\int_0^h \theta(X + t; d, a)dt \ .$$

Alors $\theta_1(X; d, a) \geq \theta(X; d, a)$ et pour $h = 1$ et $X$ entier, nous avons égalité. Maintenant, nous remarquons que, vu le type de résultats recherchés, nous ne serons pas capables de distinguer $\theta(X; d, a)$ de $\theta\Big(X(1 + \varepsilon_d); d, a\Big)$, ce qui fait que nous pouvons prendre $h$ de la forme $\delta X$ !

Nous pouvons aussi étendre le procédé en considérant

$$\theta_m(X;d,a) = \frac{1}{(\delta X)^m}\int_0^{\delta X}\cdots\int_0^{\delta X}\theta(X+t_1+\cdots+t_m;d,a)dt_1\cdots dt_m$$

où $m$ est un entier $\geq 1$. A présent, nous exprimons $\theta(X+y;d,a)$ à l'aide des fonctions $L$ de Dirichlet et obtenons un résultat du type suivant (nous ne donnons pas l'énoncé précis qui est long mais simplement la forme du résultat).

**Théorème 3.10.1 ( [*McCurley,* 1984b])** *Soit $d$, $a$ et $m$ des entiers $\geq 1$, $a$ étant premier à $d$. Soit $X$, $H$ et $\delta$ des réels $> 0$ avec $m\delta \geq \frac{1-X}{X}$. Alors*

$$\begin{aligned}\frac{\phi(d)}{X}\left|\theta(X;d,a)-\frac{X}{\phi(d)}\right| &\leq (1+\frac{m\delta}{2})\sum_{\chi \bmod d}\sum_{\substack{\rho\in Z(\chi)\\ |\gamma|\leq H}}\frac{X^{\beta-1}}{|\rho|}\\ &+\frac{\left(1+(1+\delta)^{m+1}\right)^m}{\delta^m}\sum_{\chi \bmod d}\sum_{\substack{\rho\in Z(\chi)\\ |\gamma|> H}}\frac{X^{\beta-1}}{|\rho|^{m+1}}+\frac{m\delta}{2}\\ &+ \quad \textit{termes d'erreurs}\end{aligned}$$

*où $Z(\chi)$ désigne l'ensemble de zéros $\rho = \beta + i\gamma$ de la fonction $L(s,\chi)$ qui vérifient $0 < \beta < 1$.*

Ce théorème donne de mauvais résultats pour un module $d$ arbitraire. Par contre, pour un $d$ donné (disons $d = 3$ pour fixer les esprits), nous disposons d'une information supplémentaire qui accroît énormément la puissance du théorème précédent. En effet, nous pouvons montrer par des calculs numériques que, pour tout caractère $\chi$ modulo $d$, les zéros $\rho = \beta + i\gamma$ de $L(s,\chi)$ qui vérifient $0 < \beta < 1$ et $|\gamma| \leq H$ pour un $H$ fixé numériquement sont en fait tels que $\beta = \frac{1}{2}$. Dans cette direction, nous disposons du théorème suivant de Rumely :

**Théorème 3.10.2 ( [*Rumely,* 1993])** *Soit $d$ un entier $\leq 60$ et $a$ un entier premier à $d$. Soit $\chi$ un caractère modulo $d$. Alors les zéros $\rho = \beta + i\gamma$ de $L(s,\chi)$ qui vérifient $0 < \beta < 1$ et $|\gamma| \leq 2500$ sont tels que $\beta = \frac{1}{2}$.*

Les résultats de Rumely sont en fait plus étendus, tant en modules qu'en hauteur pour certains modules. À l'aide de ces calculs, le théorème cité de McCurley donne facilement des résultats du type suivant * :

∗. Depuis, l'article [*Ramaré & Rumely,* 1996] donne de meilleurs résultats.

**Théorème 3.10.3** *Soit $d$ un entier $\leq 60$ et $a$ un entier premier à $d$. Pour tout $X \geq 10^{20}$, nous avons*

$$\theta(X, d, a) = \frac{X}{\phi(d)}\big(1 + \mathcal{O}^*(0.011)\big) \ .$$

Il est à noter que, primo, [*McCurley,* 1984b] donne déjà de tels résultats dans le cas $d = 3$. (Il disposait d'analogues des calculs de Rumely dans ce cas) et, secundo, que, pour des valeurs aussi faibles de $X$, la zone infinie sans zéro est presque sans effet.

Enfin, la formulation même de ce résultat appelle un commentaire. Les calculs de Rumely ont été effectués jusqu'à une hauteur fixée indépendamment du module $d$ mais nos résultats sont presque uniformes en $d$. Par exemple, pour $d = 5$, nous ne pourrions remplacer $0.011$ que par $0.008$, ce qui est très surprenant puisque, $\phi(d)$ sommes intervenant, on s'attendrait à une perte d'un facteur multiplicatif $\phi(60)/\phi(5)$ ! C'est là l'un des effets inattendus mais très agréable du paramètre $m$ de Rosser. De façon heuristique, on constate que notre $\varepsilon_d$ ne dépend de $d$ que d'un facteur $\operatorname{Log}\phi(d)$ (et non pas $\phi(d)$).

# Distribution explicite des nombres premiers

Cette partie regroupait deux articles qui ont chacun une histoire assez longue et dont les versions finales sont écrites avec des co-auteurs. Ces deux articles complétaient (et étaient nécessaires à) l'article sur la constante de Šnirel'man. Ils avaient alors été écrits assez vite. Ils ont été remaniés par la suite, mais ont surtout été étoffés grâce à l'apport de deux co-auteurs. On y trouvait :

Primes in arithmetic progressions. [*Ramaré & Rumely,* 1996].

*Un article écrit avec R. Rumely. Il faut noter qu'en plus d'informations d'ordre numériques sur $\psi(X;q,a)$, nous montrons en outre comment n'utiliser que des caractères primitifs pour évaluer $\psi(X;q,a)$ et ce avec une perte bien moindre qu'usuellement (introduction de la partie 4.3). Cet article étend aussi quelque peu la zone sans zéros de fonctions $L$ de petits conducteurs, mais cette partie a été rendue obsolète par les travaux de [Kadiri, 2005] et [Kadiri, 2009].*

Short effective intervals containing primes. [*Ramaré & Saouter,* 2003].

*Un article écrit avec Y. Saouter. Son originalité vient du fait que nous introduisons un argument de crible.*

# Majorations/Minorations de $L(1, \chi)$

Nous reproduisons ici un seul exposé :

Minoration de $L(1, \chi)$.

*Un exposé qui retrace l'histoire des minorations de $L(1, \chi)$.*

Cette partie contenait :

Sur un théorème de Mertens. [*Ramaré,* 2002].

*Nous étudions la preuve Mertens permettant de montrer que toute progression arithmétique contient la proportion correcte de nombres premiers. Nous la modifions pour en améliorer la dépendance en $q$, ce que nous réalisons essentiellement à l'aide d'une inégalité de crible pour contrôler (en $X$) le terme d'erreur et d'une technique "bilinéaire" pour ce concerne la dépendance en $q$. Bien que nous n'utilisions qu'une majoration en moyenne quadratique des $1/L(1, \chi)$, une amélioration effective de la $q$-dépendance de notre terme d'erreur améliorerait la borne effective pour le zéro de Siegel (pourvu que cette amélioration gagne plus qu'un $\mathrm{Log}^3\, q$). Notre méthode permet par ailleurs d'obtenir de bonnes bornes pour $\sum_{n\equiv a[q], n\leq X} \Lambda(n)/n$ pour de petits $q$.*

A purely analytical lower bound for $L(1, \chi)$. [*Ramaré,* 2009].

*Un article qui n'existait à l'époque que sous forme de préprint mais a été publié depuis.*

Approximate Formulae for $L(1, \chi)$. I et II. [*Ramaré,* 2001] et [*Ramaré,* 2004].

*Deux articles où nous donnons des majorations de $L(1, \chi)$ de la forme $\frac{1}{2}\,\mathrm{Log}\, q + C$ avec $C$ assez petit. Dans le second, certains facteurs eulériens sont traités*

*de façon spéciale. Ce dernier travail améliore et étend au cas des caratères impairs des résultats de [Louboutin, 1993] et [Louboutin, 1996].*

# Chapitre 4

# Minoration de $L(1, \chi)$

Voici un exposé de 1996 sur le sujet du titre. L'avant dernière partie est nouvelle et a donné lieu à la note [*Ramaré,* 2009].

## 4.1 Introduction.

Voici le problème général qui nous intéresse : quel est le lien entre le groupe additif $\mathbb{Z}/q\mathbb{Z}$ et le groupe multiplicatif $(\mathbb{Z}/q\mathbb{Z})^*$ ? Par exemple, si $q$ est un nombre premier, disons égal à $p$, on sait qu'il y a $(p-1)/2$ éléments de $(\mathbb{Z}/q\mathbb{Z})^*$ qui ne sont pas des carrés. Quelle est la taille du plus petit d'entre eux ?

Pour appréhender la structure multiplicative de $(\mathbb{Z}/q\mathbb{Z})^*$, nous introduisons les caractères de Dirichlet $\chi\ :\ \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ tels que $\chi(n) = 0$ si $(n, q) \neq 1$ et $\chi(mn) = \chi(m)\chi(n)$. Si $f|q$, un caractère modulo $f$ se remonte en un caractère modulo $q$ et si un caractère modulo $q$ provient d'un caractère modulo $f_1$ et $f_2$, alors il provient d'un caractère modulo leur pgcd, ce qui permet de définir la notion de conducteur d'un caractère (le plus petit $f$ tel que $\chi$ provienne de $\mathbb{Z}/f\mathbb{Z}$) et celle de caractère primitif (dont le conducteur est égal à $q$). Notons que ces notions tiennent compte des deux structures additives et multiplicatives. Une façon d'étudier le rapport entre les deux structures consiste à étudier $\sum_n \chi(n)f(n)$ où $f$ dépend de la structure additive.

*Nous supposerons dans la suite que $\chi$ est un caractère primitif de conducteur $q$ et que $\chi$ est quadratique, i.e. $\bar{\chi} = \chi$, i.e. $\chi(n) \in \{1, -1, 0\}$. Un petit calcul montre que $q$ est alors de la forme $m$, $4m$ ou $8m$ où $m$ est un entier impair sans facteurs carrés.*

Premier essai : essayons de calculer la transformée de Fourier modulo $q$ de $\chi$. Pour cela posons $\tau(\chi) = \sum_{n \mod q} \bar{\chi}(n)e(n/q)$. Alors

$$\begin{cases} \chi(n) = \dfrac{1}{\tau(\chi)} \sum\limits_{a \mod q} \bar{\chi}(a)e(an/q) \qquad (n \mod q) \\ |\tau(\chi)| = \sqrt{q} \qquad \text{(Parseval)}. \end{cases} \tag{4.1}$$

Remarquons que l'on n'a pas vraiment calculé la transformée de Fourier de $\chi$ mais obtenu une relation entre cette transformée et $\chi$. Vers 1801, Gauss a établi

$$\tau(\chi) = \begin{cases} \sqrt{q} & \text{si } \chi(-1) = +1, \\ i\sqrt{q} & \text{si } \chi(-1) = -1. \end{cases} \tag{4.2}$$

Dans le cas d'un caractère qui n'est pas spécialement quadratique, nous ne connaissons pas précisément la transformée de Fourier, mais l'expression obtenue a cependant de nombreuses applications. Signalons ici l'inégalité de Polya-Vinogradov, valable pour tout $X \geq 1$ :

$$\Big|\sum_{n \leq X} \chi(n)\Big| \ll \sqrt{q}\,\operatorname{Log} q. \tag{4.3}$$

Second essai : examinons

$$L(s,\chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s} = \prod_{p \geq 2} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}. \tag{4.4}$$

Pour $\Re s > 1$ cette série converge absolument ce qui rend les renseignements difficiles à extraire. Il commence à se passer des choses intéressantes si $\Re s = 1$ et particulièrement si $s = 1$. On montre facilement que $L(1,\chi) \geq 0$. Le problème est alors double

$$\begin{cases} \text{1. Majorer } L(1,\chi), \text{ i.e. montrer que } \chi(n) \text{ est souvent} \neq +1, \\ \text{2. Minorer } L(1,\chi), \text{ i.e. montrer que } \chi(n) \text{ est souvent} \neq -1. \end{cases}$$

Nous nous intéressons ici au second problème. (Et on passe sous silence le résultat de Burgess qui appartient au premier problème). Remarquons que le premier problème correspond à montrer que $L(s,\chi) \neq \zeta(s)$. Le second problème est un peu plus difficile à interpréter dû au fait que $\chi$ est une fonction multiplicative. Si l'on note $\lambda$ la fonction de

Liouville (de série de Dirichlet $\zeta(2s)/\zeta(s)$), il faut montrer que $L(s,\chi)\neq\zeta(2s)/\zeta(s)$. Ce principe sera utilisé et avalidé dans la quatrième section.

## 4.2 Minoration de $L(1,\chi)$ sous $\chi(-1)=-1$.

Dirichlet s'est occupé de minorer $L(1,\chi)$ en 1837 pour montrer que les nombres premiers étaient équidistribués dans les classes de congruences. Il montrait

$$L(1,\chi)=-\pi q^{-3/2}\sum_{n=1}^{q} n\chi(n) \qquad (\chi(-1)=-1), \tag{4.5}$$

et donnait aussi une formule dans le cas où $\chi(-1)=1$. On obtient ces formules à l'aide de la transformée de Fourier rappelée dans la première section. Il n'est pas très difficile de déduire de la formule précédente que

$$L(1,\chi)=\frac{\pi}{q^{1/2}(2-\chi(2))}\sum_{1\leq n<q/2}\chi(n) \qquad (\chi(-1)=-1), \tag{4.6}$$

et donc si $q$ est un nombre premier ($\equiv 3[4]$), la somme sur $n$ est un entier impair d'où l'on déduit $\sqrt{q}L(1,\chi)\geq\pi/(2-\chi(2))$. Pour résoudre le cas général, Dirichlet en 1839 s'est appuyé sur la théorie des formes quadratiques et des extensions quadratiques imaginaires de $\mathbb{Q}$, théorie qui était en plein essor à ce moment.

### 4.2.1 Lien avec les corps quadratiques imaginaires.

Le caractère $\chi$ est très lié à l'extension $K=\mathbb{Q}(\sqrt{-q})$. Par exemple

$$\zeta_K(s)=\sum_{\mathfrak{A}\text{ idéal entier}} N\mathfrak{A}^{-s}=\zeta(s)L(s,\chi). \tag{4.7}$$

Jacobi a anticipé le résidu en 1 de cette fonction et Dirichlet montrait en 1839 que

$$L(1,\chi)=\pi h(-q)/\sqrt{q} \qquad (\chi(-1)=-1,\quad q\geq 5) \tag{4.8}$$

où $h(-q)$ est le nombre de classes d'idéaux de $K$. Par ailleurs $h(-q)$ est aussi le nombre de classes de formes quadratiques

$$Q(x,y) = ax^2 + bxy + cy^2$$

avec $a, b, c \in \mathbb{Z}$ et $4ac - b^2 = q$ sous l'action de $GL_2(\mathbb{Z})$, deux formes étant équivalentes si l'on peut passer de l'une à l'autre par un changement de variables à coefficients dans $\mathbb{Z}$. Les $h(-q)$ classes ont un unique représentant (que l'on dit réduit) qui vérifie

$$\text{(4.9)} \qquad \begin{cases} 4ac - b^2 = q, \\ (a,b,c) = 1, \\ -a \leq b < a \end{cases} \qquad \begin{cases} c \geq a \text{ si } b \leq 0, \\ c > a \text{ si } b > 0. \end{cases}$$

Un tel triplet $(a,b,c)$ vérifie $a \leq \sqrt{q/3}$ et $\sqrt{q}/2 \leq c \leq q/(3a)$. A chaque forme quadratique, on associe l'idéal de $K$ engendré par $a$ et $a\tau(Q) = (-b + i\sqrt{q})/2$ et cela induit une bijection entre les classes de formes et les classes d'idéaux. Par ailleurs, à chaque forme quadratique, on associe le point $\tau(Q)$ et deux points sont équivalents sous $GL_2(\mathbb{Z})$ si et seulement si les formes correspondantes sont équivalentes.

On peut considérer l'équivalence sur $\mathbb{Q}$ et non sur $\mathbb{Z}$, ce que fit Gauss. On ne parle plus alors de *classe* mais de *genre*. Il montre qu'il y a $2^{\omega(q)-1}$ genres de formes. Deux formes sont dans le même genre si et seulement si elles représentent les mêmes entiers modulo tout $m \geq 1$. En convertissant ce résultat en termes du groupe de classes $\mathcal{C}\ell(q)$, on montre en fait que

$$\text{(4.10)} \qquad \mathcal{C}\ell(q)/\mathcal{C}\ell(q)^2 \cong \left(\mathbb{Z}/2\mathbb{Z}\right)^{\omega(q)-1}$$

ce qui implique que $2^{\omega(q)-1} | h(-q)$. Remarquons que pour obtenir le nombre de genres, le théorème de Dirichlet sur l'existence de nombres premiers dans des progressions arithmétiques n'est pas nécessaire bien que beaucoup de preuves l'utilisent. Nous avons donc

$$\text{(4.11)} \qquad L(1,\chi) \geq \pi 2^{\omega(q)-1}/\sqrt{q} \qquad (\chi(-1) = -1, \quad q \geq 5).$$

Telle était donc la situation en 1839. Vient ensuite l'époque de Riemann, Hadamard et de la Vallée-Poussin et l'accent est mis sur les zéros des fonctions $\zeta$ et $L$.

### 4.2.2 Lien avec les zéros des fonctions $L$.

Il convient de rappeler trois résultats pour illustrer la situation.

**Théorème 4.2.1 (Hecke ≍1915)** *Il existe une constante $c>0$ telle que $L(s,\chi)\neq 0$ pour $\Re s \geq 1-c/\operatorname{Log} q$ et $s$ réel si et seulement si il existe une constante $c'>0$ telle que $L(1,\chi)\geq c'/\operatorname{Log} q$.*

**Théorème 4.2.2 (Littlewood, 1927)** *Si $L(s,\chi)\neq 0$ pour $\Re s > \frac{1}{2}$ alors on a $2e^{\gamma}(1+o(1))\operatorname{Log}\operatorname{Log} q \geq L(1,\chi)\geq (1+o(1))\frac{\pi^2 e^{-\gamma}}{12}/\operatorname{Log}\operatorname{Log} q$.*

**Théorème 4.2.3 ( [*Pintz,* 1976])** *Si il existe $\beta$ réel tel que $1-\beta=o(1/\operatorname{Log} q)$ et $L(\beta,\chi)=0$ alors $L(1,\chi)\sim(1-\beta)\sum_{n\leq q^2}\mathbb{1}\star\chi(n)/n$.*

[*Rosser,* 1949] et [*Rosser,* 1950] a montré que $L(s,\chi)>0$ si $0\leq s\leq 1$ et $q\leq 1000$ et [*Low,* 1968] ont montré que ce même résultat est valable pour $q\leq 593\ 000$ et $q\neq 115\ 147$. Par ailleurs [*Shanks,* 1973] a vérifié numériquement la conclusion du théorème 4.2.2 et n'a pas observé de violations. Linnik, Walfisz et Chowla ont montré que les ordres de grandeurs des bornes de ce même sont optimaux à constante multiplicative près, et plus précisément qu'il existe une infinité de $\chi$ pour lesquels $L(1,\chi)\leq(1+o(1))\frac{\pi^2}{6e^{\gamma}}/\operatorname{Log}\operatorname{Log} q$ et une infinité de $\chi$ pour lesquels $L(1,\chi)\geq(1+o(1))e^{\gamma}\operatorname{Log}\operatorname{Log} q$.

Seul un caractère $\chi$ modulo $q$ peut avoir un zéro $\rho=\beta+i\gamma$ qui ne vérifie pas (cf [*Kadiri,* 2009])

$$\beta\leq 1-1/(6.71\operatorname{Log}\max(q,q|\gamma|)). \tag{4.12}$$

On appelle un tel zéro un zéro de Siegel, ou un zéro exceptionnel. Un tel phénomène se produit parce que les procédés qui permettent d'obtenir des régions sans zéros pour les fonctions $L$ comparent deux fonctions $L$. La conclusion est en essence que l'une des deux fonctions n'a pas de zéro proche de l'axe $\Re s=1$. Ce principe a été poussé à son maximum par Deuring en 1933, Mordell en 1934, Heilbronn en 1934 et finalement Siegel en 1935. [*Tatuzawa,* 1951] apportait la dernière touche en montrant que pour tout $\varepsilon>0$

$$L(1,\chi)\geq\frac{\varepsilon}{10q^{\varepsilon}}\qquad\text{sauf pour au plus une valeur de } q.$$

L'exception restante est une maladie de la méthode. Un autre interprétation de cette méthode donne lieu au phénomène de prolifération des zéros de [*Montgomery,* 1971]. *

∗. Voire aussi [*Balasubramanian & Ramachandra,* 1982].

### 4.2.3 Lien avec l'existence de nombres premiers en progressions arithmétiques.

Pour $a$ premier à $q$, nous posons

$$\psi(X;q,a)=\sum_{n\leq X,\ n\equiv a[q]}\Lambda(n). \tag{4.13}$$

Nous avons le résultat suivant (essentiellement dû à Gallagher) qui s'appuye sur le phénomène de Deuring-Heilbronn : si il y a un zéro exceptionnel, alors les autres fonctions $L$ ne s'annulent pas dans un domaine d'autant plus grand que ce zéro est proche de 1. Si $L(\beta,\chi)=0$ pour un $\beta$ qui vérifie $1-\beta=o(1/\operatorname{Log} q)$, nous posons $\delta=1-\beta$. Dans ce cas nous avons

$$\psi(X;q,a)=\frac{X}{\phi(q)}\big(1-\chi(a)\frac{X^{-\delta}}{\beta}\big)+\mathcal{O}\bigg(\frac{X\delta\operatorname{Log}T}{\phi(q)}\big(\frac{e^{-c_1\frac{\operatorname{Log}X}{\operatorname{Log}T}}}{\operatorname{Log}X}+\frac{q\operatorname{Log}X}{\sqrt{T}}+\frac{T^{5.5}}{\sqrt{x}}\big)\bigg)$$

si $x\geq T^{c_2}\geq T\geq q$ où $c_1,c_2>0$ sont deux constantes effectives et la constante impliquée dans le $\mathcal{O}$ est aussi explicite. Si un tel zéro exceptionnel n'existe pas, la formule précédente est valable en posant $\beta=\frac{1}{2}$ dans le terme principal et $\delta\operatorname{Log}T=1$ dans le terme d'erreur.

Comme $1-X^{-\delta}/\beta=1-\exp(-\delta\operatorname{Log}X)-\delta X^{-\delta}/\beta\gg\delta\operatorname{Log}X$, nous obtenons

$$\psi(X;q,a)\sim\frac{X}{\phi(q)}\big(1-\chi(a)\frac{X^{-\delta}}{\beta}\big)\qquad\text{si}\quad\frac{\operatorname{Log}X}{\operatorname{Log}q}\to\infty. \tag{4.14}$$

Notons que ce résultat contient le théorème de Linnik (cf [*Bombieri,* 1987/1974]). Par conséquent l'une quelconque des inégalités $\psi(X;q,a)\geq\varepsilon X/\phi(q)$ et $\psi(X;q,a)\leq(2-\varepsilon)X/\phi(q)$ pour un $\varepsilon>0$ implique $\delta\operatorname{Log}X\geq\operatorname{Log}1/(1-\varepsilon')$ pour un $\varepsilon'\in]0,\varepsilon[$. [*Motohashi,* 1979] a montré des résultats similaires de façon beaucoup plus élémentaire. Par conséquent pour $c\geq1$, les trois problèmes suivants sont équivalents $^*$ :

$$\begin{cases}\text{1. Rendre effectif } \psi(X;q,a)\sim X/\phi(q) \text{ pour } q\leq(\operatorname{Log}X)^{c'}\ (\forall c'<c),\\ \text{2. Rendre effectif } L(1,\chi)\gg q^{-1/c'}\ (\forall c'<c),\\ \text{3. Rendre effectif } \psi(X;q,a)\leq\frac{(2-\varepsilon)X}{\phi(q)}\ (\varepsilon>0) \text{ pour } q\leq(\operatorname{Log}X)^{c'}\ (\forall c'<c).\end{cases}$$

$*$. Une preuve détaillée se trouve dans [*Basquin,* 2006], qui est repris dans [*Ramaré,* 2009].

La constante 2 du théorème de Brun-Titchmarsh est donc liée au zéro de Siegel. Malheureusement cette constante est une maladie du crible à cause du phénomène de parité de Bombieri-Selberg.

## 4.3 Valeur de $L(1,\chi)$ et forme modulaire.

Le principe de comparaison précédent serait parfait si l'on disposait de fonctions $L$ ayant des zéros très proches de 1, mais l'existence de telles fonctions est contraire à l'hypothèse de Riemann généralisée ...

[*Birch & Swinnerton-Dyer,* 1965] énonçait une conjecture indiquant que certaines fonctions $L$ liée à des courbes elliptiques devaient s'annuler en $\frac{1}{2}$ et ce même avec un zéro triple et [*Armitage,* 15] exhibait des exemples de fonctions $L$ (non abéliennes) telles que $L(\frac{1}{2}) = 0$.

[*Montgomery & Weinberger,* 1973] utilisent des fonctions $L$ (classiques) qui ont un zéro proche de $\frac{1}{2}$ pour montrer que $\sqrt{q}L(1,\chi) \geq 4\pi$ si $10^{12} \leq q \leq 10^{2500}$.

Finalement ( ?) [*Goldfeld,* 1985] poussait le principe de comparaison un cran plus loin et montre comment utiliser l'influence d'un zéro triple d'une fonction $L$ de courbe elliptique en $\frac{1}{2}$ pour obtenir

$$\sqrt{q}L(1,\chi) \gg_\varepsilon \mathrm{Log}^{1-\varepsilon} q. \tag{4.15}$$

Si ce résultat est infiniment meilleur que les précédents, il reste assez faible parce que $\frac{1}{2}$ est loin de 1. Toutefois pour appliquer ce résultat, il faut montrer que la valeur d'une fonction $L$ est nulle, ce qui ne peut pas se faire par calcul approché ... [*Gross & Zagier,* 1983] résolvait ce dernier problème et obtenait donc (4.15). D'un point de vue méthodologique, il convient de noter que la preuve de Goldfeld s'appuye sur la théorie des formes quadratiques.

## 4.4 Remarques sur les minorations de $L(1,\chi)$.

Probablement le point le plus fascinant en ce qui concerne la minoration de $L(1,\chi)$ est que toute méthode semble donner $\sqrt{q}L(1,\chi) \gg 1$ et pas mieux. Par exemple, j'ai montré de façon effective et plutôt élémentaire (cf "Sur un théorème de Mertens") que

$$\sum_{p\leq X,\ p\equiv a[q]} \frac{\mathrm{Log}\, p}{p} = \frac{\mathrm{Log}\, X}{\phi(q)} + C(q,a) + \mathcal{O}(\mathrm{Log}^3 q/\sqrt{q}) \tag{4.16}$$

ce qui donne $\frac{\mathrm{Log}^3 q}{\sqrt{q}} L(1,\chi) \gg 1/q$ ... Ici le $\sqrt{q}$ provient de $\sum_{\chi \mod {}^* q} |L(1,\chi)|^{-2} \ll q$ qui est essentiellement optimale. Avec H.Iwaniec, nous avons mis au point une forme bilinéaire qui permet d'obtenir

$$\left| \sum_{p \le X} \mathrm{Log}\, p\; e(pa/q) \right| \ll \frac{\sqrt{q}}{\phi(q)} X, \qquad \big(q \le \exp(\mathrm{Log}^{1/30} X)\big) \tag{4.17}$$

de façon effective. Cela donne encore $\sqrt{q} L(1,\chi) \gg 1$ ...

## 4.5 Une preuve simple de $\sqrt{q} L(1,\chi) \gg 2^{\omega(q)}$.

Jusqu'à présent, sans la formule des classes de Dirichlet, on ne peut obtenir que $\sqrt{q} L(1,\chi) \gg 1$ et cette borne est difficile à atteindre.

En continuant mes recherches, je me suis penché sur la preuve suivante (dont je n'ai pas réussie à tracer l'origine). Posons

$$S(\alpha) = \sum_{n \ge 1} \Big( \sum_{d|n} \chi(d) \Big) e^{-\alpha n} \qquad (\alpha > 0).$$

En remarquant que $\mathbb{1} \star \chi(n) \ge 0$ et même $\ge 1$ si $n$ est un carré, on obtient

$$S(\alpha) \ge \sum_{m \ge 1} e^{-\alpha m^2} \gg 1/\sqrt{\alpha}. \tag{4.18}$$

Par ailleurs, en intervertissant les sommations, nous obtenons

$$S(\alpha) = \frac{1}{\alpha} L(1,\chi) - \sum_{d \ge 1} \chi(d) \rho(\alpha d) \qquad \big(\rho(t) = \frac{1}{t} - \frac{1}{e^t - 1}\big). \tag{4.19}$$

Une intégration par parties et l'inégalité de Polya-Vinogradov mentionnée plus haut donnent alors $|\sum_{d \ge 1} \chi(d) \rho(\alpha d)| \ll \sqrt{q}\, \mathrm{Log}\, q$. En choisissant $\alpha^{-1} = \mathrm{Cte}\, q\, \mathrm{Log}^2 q$, nous obtenons $L(1,\chi) \gg 1/(\sqrt{q}\, \mathrm{Log}\, q)$. Pour enlever le $\mathrm{Log}\, q$, il suffit de remarquer qu'il provient d'un défaut de lissage dans l'inégalité de Polya-Vinogradov. En fait l'écriture

$$\sum_{d \ge 1} \chi(d) \rho(\alpha d) = \frac{-i}{\sqrt{q}} \sum_{a \mod q} \chi(a) \sum_{n \ge 1} \rho(\alpha n) e(an/q) \tag{4.20}$$

avec $\chi(-1) = -1$ fait apparaître essentiellement $\int_0^\infty \rho(\alpha t) \sin(2\pi t a/q) dt$. Comme $\rho$ est

assez lisse, cette transformée se concentre autour de 0. Cela nous donne

$$\Big|\sum_{d\geq 1}\chi(d)\rho(\alpha d)\Big| \ll (1+\alpha q)\sqrt{q} \tag{4.21}$$

et le choix $\alpha^{-1} = \text{Cte}\, q$ donne $\sqrt{q}L(1,\chi) \geq c$.

Que vaut $c$ ? En calculant $\sum_{n\geq 1}\rho(\alpha n)e(an/q)$ pour $a = 1, 2, \ldots, 10$, on arrive à s'approcher de la meilleure valeur possible et l'on obtient $c = 3.1415$ ... En fait, en poursuivant cette démonstration, on peut obtenir $c = \pi - o(1)$ ! Nous allons adopter une façon un peu plus sophistiquée et beaucoup plus rapide qui donne

$$\sqrt{q}L(1,\chi) \geq \pi(1-o(1)) \quad , \quad \sqrt{q}L(1,\chi) \geq \pi 2^{\omega(q)-1}/10, \tag{4.22}$$

et ce sans employer la formule des classes de Dirichlet. Le lecteur trouvera une version détaillée de cette preuve (et notamment son adaptation aux caractères pairs) dans [*Ramaré,* 2009]. Posons

$$f(\tau) = \frac{\sqrt{q}L(1,\chi)}{2\pi} + \sum_{n\geq 1}\mathbb{1}\star\chi(n)e^{\frac{2i\pi n\tau}{\sqrt{q}}} \qquad (\Im\tau > 0). \tag{4.23}$$

On montre (c'est la théorie développée vers 1927 par Hecke entre forme modulaire et équation fonctionnelle) que $f(-1/\tau) = (\tau/i)f(\tau)$ en considérant

$$\Phi(s) = \left(2\pi/\sqrt{q}\right)^{-s}\Gamma(s)L(s,\chi)\zeta(s) \tag{4.24}$$

qui vérifie $\Phi(s) = \Phi(1-s)$. Il suffit pour cela d'écrire

$$S(\alpha) = \frac{1}{2i\pi}\int_{2-i\infty}^{2+i\infty}\Gamma(s)L(s,\chi)\zeta(s)\alpha^{-s}ds, \tag{4.25}$$

de déplacer la droite d'intégration en $\Re s = \frac{1}{2}$, d'utiliser l'équation fonctionnelle et de revenir en $\Re s = 2$. Prenant $\tau = ix$ avec $x > 0$, nous obtenons

$$\frac{1-x}{2}\frac{\sqrt{q}L(1,\chi)}{\pi} = x\sum_{n\geq 1}\mathbb{1}\star\chi(n)e^{-\frac{2\pi nx}{\sqrt{q}}} - \sum_{n\geq 1}\mathbb{1}\star\chi(n)e^{-\frac{2\pi n}{x\sqrt{q}}}. \tag{4.26}$$

Il convient à présent d'améliorer l'argument $\mathbb{1}\star\chi(m^2) \geq 1$. Soit $\lambda$ la fonction de Liouville. $\mathbb{1}\star\lambda$ est la fonction caractéristique des carrés et $\mu^2\star\lambda = \delta$ l'unité de la convolution. Par

conséquent $\mathbb{1} \star \chi = (\mu^2 \star \chi) \star (\mathbb{1} \star \lambda)$. Posons $\nu = \mu^2 \star \chi \geq 0$. Notre formule s'écrit

$$\frac{1-x}{2}\frac{\sqrt{q}L(1,\chi)}{\pi} = \sum_{m\geq 1} \nu(m) g(x,m) \tag{4.27}$$

où

$$g(x,m) = x\sum_{n\geq 1} e^{-\frac{2\pi m x}{\sqrt{q}}n^2} - \sum_{n\geq 1} e^{-\frac{2\pi m}{x\sqrt{q}}n^2}. \tag{4.28}$$

La clé (miraculeuse) vient de ce que si $x$ n'est ni trop proche de 0, ni trop proche de 1, on a $g(x,m) \geq 0$ pour tout $m \geq 1$. Il faut souligner ici que je ne dispose d'aucune bonne raison permettant de deviner ce fait a priori et que la preuve en est très calculatoire. Nous prenons alors $x = 0.43542$ et vérifions que

$$g(x,m) = \frac{1-x}{2} + \mathcal{O}(m/\sqrt{q}), \quad g(x,m) \geq 0, \quad \min_{m\leq\sqrt{q}} g(x,m) \geq \frac{1-x}{20} \tag{4.29}$$

ce qui nous donne $\sqrt{q}L(1,\chi) \geq \pi(1+\mathcal{O}(1/\sqrt{q}))$ si l'on ne garde que le terme $m=1$. En ne gardant que les $m \leq \sqrt{q}$, nous obtenons

$$\sqrt{q}L(1,\chi) \geq \frac{\pi}{10}\sum_{m\leq\sqrt{q}} \nu(m). \tag{4.30}$$

Or $\nu(p) = 1 + \chi(p) = 1$ si $p|q$. Comme il y a un diviseur sur deux de $q$ sous $\sqrt{q}$, nous obtenons le résultat annoncé. Remarquons que cette preuve montre clairement que le problème est de montrer que $\nu(p) \neq 0$ assez souvent, i.e. que $\chi \neq \lambda$.

Pour revenir à la formulation initiale, nous utilisons ici le fait que si $q$ admet des diviseurs, nous avons un renseignement sur $(\mathbb{Z}/q\mathbb{Z})^*$, i.e. que certains points n'y appartiennent pas. Cette propriété a déjà été utilisée par [*Graham & Ringrose,* 1990] pour agrandir la région sans zéro de $L(s,\chi)$ sous les mêmes hypothèses. Ils obtiennent que $L(s,\chi)$ ne s'annule pas (sauf en ce qui concerne un éventuel zéro de Siegel) dans la région

$$\sigma \geq 1 - C\min\left(\frac{\operatorname{Log}\operatorname{Log} q}{\operatorname{Log} q}, \frac{1}{\sqrt{\operatorname{Log} q \operatorname{Log}\max(p, d(q))}}\right) \qquad |t| \leq 1, \tag{4.31}$$

où $p$ est le plus grand diviseur premier de $q$.

## 4.6 Quelques compléments.

○○ Pour ce qui est du II-b, il convient de signaler le résultat de [*Haneke,* 1973] et [*Haneke,* 1976] qui dit que $L(s,\chi)$ ne s'annule pas dans la région $\Re s \geq 1 - c/\sqrt{q}$ et $|s| \leq 1$. Ce résultat ne découle pas directement du résultat de Pintz cité, ni de celui de [*Goldfeld & Schinzel,* 1975] cité ci-après.

○○ [*Goldfeld & Schinzel,* 1975] ont montré que si il y a un zéro exceptionnel alors

$$L(1,\chi) \sim (1-\beta)\frac{\pi^2}{6} \sum_{\substack{Q \in \mathcal{Q}_q^{\text{réduit}} \\ a \leq \sqrt{q}/4}} \frac{1}{a}. \tag{4.32}$$

○○ L'argument du paragraphe II-c est probablement plus clair si l'on indique qu'il existe deux constantes explicites $c_1 > 0$ et $c_2 > 0$ telles que si $L(\beta,\chi) = 0$ pour un $\beta$ tel que $(1-\beta)\operatorname{Log} T \leq c_1$ alors aucune des fonctions $L$ associée à des caractères de module $\leq T$ n'admet de zéros dans la région

$$\sigma \geq 1 + c_2 \operatorname{Log}((1-\beta)\operatorname{Log} T)/\operatorname{Log} T, \quad |t| \leq T \tag{4.33}$$

sauf peut-être $\beta$. cf [*Bombieri,* 1987/1974].

○○ En utilisant la théorie des formes quadratiques, on obtient (cf [*Oesterlé,* 1985])

$$\sum_{m \geq 1} \frac{\nu(m)}{m^s} = \sum_{Q \in \mathcal{Q}_q^{\text{réduit}}} \frac{1}{a^s} + \sum_{Q \in \mathcal{Q}_q^{\text{réduit}}} \sum_{\substack{(x,y) \in \mathbb{Z} \times \mathbb{N}^o \\ (x,y)=1}} \frac{1}{Q(x,y)^s} \tag{4.34}$$

où $\mathcal{Q}_q^{\text{réduit}}$ est l'ensemble des formes quadratiques réduites de discriminant $-q$ et est donc de cardinal $h(-q)$. Remarquons qu'une telle forme quadratique vérifie $Q(x,y) \geq c$ si $y \geq 1$. En utilisant cette expression, on peut remplacer le 10 dans (4.30) par un 3.

○○ Posons $F(\tau) = f(\tau/\sqrt{q})$. En utilisant le théorème converse de Weyl (1967), on montre que $F$ vérifie

$$F(\gamma\tau) = \chi(d)(c\tau + d)F(\tau), \qquad (\Im\tau > 0, \quad \gamma \in \Gamma_0(q), \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}). \tag{4.35}$$

L'espace de ces formes est invariant sous l'involution de Fricke qui transforme $F(\tau)$ en

$F(-1/(q\tau))/(\sqrt{q}\tau)$. En ces termes, la relation que nous avons utilisée se traduit par le fait que la fonction $f$ est un point fixe de cette involution.

○○ En utilisant des formes quadratiques, on obtient facilement $h(-q) \geq \frac{1}{2}d((q+1)/4)$ si $q \equiv -1[4]$ en comptant les formes quadratiques réduites ayant $b = -1$.

○○ [*Oesterlé,* 1985] montre que

$$\sqrt{q}L(1,\chi)/\pi \geq C \prod_{p\in P(q)} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right) \operatorname{Log} q \tag{4.36}$$

où $P(q)$ est l'ensemble des facteurs premiers de $q$ à l'exception du plus grand d'entre eux. Il montre en outre que l'on peut prendre $C = 1/7000$ et même $C = 1/55$ si $q$ est premier à 5077.

○○ Pour ce qui est du II-c, rappelons le résultat suivant de [*Turán,* 1959] : il existe une constante effective $q_0$ telle que si $P = \exp(\operatorname{Log}^2 q(\operatorname{Log}\operatorname{Log} q)^2)$ et $q \geq q_0$ alors

$$\beta \leq 2\frac{\operatorname{Log}\operatorname{Log}\operatorname{Log} q}{\operatorname{Log}\operatorname{Log} q} + \frac{1}{\operatorname{Log} P} \max_{1\leq x\leq P} \operatorname{Log}\Big|\sum_{n\leq x} \Lambda(n)\chi(n)\Big|. \tag{4.37}$$

# Nombres premiers et formes bilinéaires

Le lecteur trouvera ici :

Formes bilinéaires et nombres premiers. Une version simple de la méthode de Vinogradov.

*Forme écrite de plusieurs exposés, le plus ancien datant de Juillet 1994 à Lillafüred (Hongrie). Il est fait mention d'un article qui deviendra [Ramaré, 2010] quelques dix ans plus tard ! Par ailleurs, cette méthode est à la base de [Ramaré, 2006] qui est un livre de vulgarisation de haut niveau. Elle est aussi exposée dans [Iwaniec & Kowalski, 2004, section 13.2].*

Cette partie contenait aussi :

Explicit bounds on exponential sums and the scarcity of squarefree binomial coefficient.

*Un article écrit avec A. Granville où nous développons des outils pour donner des bornes explicites pour des sommes d'exponentielles sur les nombres premiers.*

# Chapitre 5

# Formes bilinéaires et nombres premiers – Une version simple de la méthode de Vinogradov

Le contenu de cette partie a été utilisé dans plusieurs exposés mais n'a jusqu'à présent fait l'objet d'aucune exposition écrite. Nous appliquons la méthode pour améliorer un résultat de Daboussi.

## 5.1 Les problèmes de base.

Le problème initial, si l'on souhaite travailler sur les nombres premiers, c'est bien sûr de les définir. Vous savez tous ce qu'est un nombre premier : c'est un entier $p$ qui n'a pas de diviseur inférieur à sa racine carrée et vous savez probablement tous que cette définition est relativement inutilisable. [*Euler,* 1737] puis Dirichlet vers 1810 introduirent une définition à l'aide de séries de Dirichlet. En écrivant

$$\zeta(s) = \sum_n \frac{1}{n^s} = \prod \left( \frac{1}{1 - \frac{1}{p^s}} \right)$$

et en prenant la dérivée logarithmique, on obtient

$$\sum_n \frac{\Lambda(n)}{n^s} = -\frac{\zeta'(s)}{\zeta(s)} \quad \text{où} \quad \Lambda(n) = \begin{cases} \operatorname{Log} p & \text{si } n = p^\nu \\ 0 & \text{sinon} \end{cases}.$$

Comme il y a relativement peu d'entiers de la forme $p^\nu$ avec $\nu \geq 2$, $\Lambda(n)$ porte essentiellement les nombres premiers. $^*$ De l'autre côté de l'égalité, on ne trouve que des fonctions portant sur des entiers et l'on peut donc travailler. Typiquement, cela permet d'obtenir des formules asymptotiques pour

$$\sum_{\substack{p \leq X \\ p \equiv a[q]}} 1$$

pourvu que $q$ reste assez petit par rapport a $X$, disons $q \leq (\operatorname{Log} X)^A$ pour un $A \geq 0$,

En 1916, Brun est revenu sur la première définition des nombres premiers que je vous ai présentée. Sa technique est connue maintenant sous le nom de crible et a un domaine d'applications plus étendu que la méthode précédente mais donne des résultats plus faibles. Par exemple le crible de Brun permet de majorer la somme précédente de façon non triviale pour $q$ de l'ordre de $X^{1/2}$. mais pas d'en avoir de formule asymptotique. Il permet aussi d'obtenir une excellente borne supérieure pour

$$\sum_{p_1+p_2=N} 1.$$

Si le crible de Brun ne donne que des bornes supérieures, c'est parce qu'il est incapable de travailler directement avec des nombres premiers mais seulement avec des suites qui contiennent strictement la suite des nombres premiers, comme par exemple la suite des entiers n'ayant pas de facteurs premiers inférieurs à $z = X^{\epsilon(X)}$, où $\epsilon(X)$ est une fonction de $X$ tendant lentement vers 0.

Parmis les sommes qui échappent à ces techniques et que l'on souhaiterait étudier, mentionnons

$$\sum_{\sqrt{X} < p \leq \sqrt{2X}} e(X/p) \quad \text{et} \quad S(a/q) = \sum_{p \leq X} e(ap/q).$$

Il faut remarquer que l'hypothèse de Riemann généralisée ne simplifie en rien l'étude des

$*$. Pour compléter les informations historiques, signalons que la fonction $\Lambda$ est provient des travaux de H. von Mangoldt en 1894, et porte d'ailleurs son nom.

sommes précédentes.

## 5.2 L'introduction des formes bilinéaires.

Vient ensuite le travail de Vinogradov (1937) qui obtient enfin une façon assez souple de travailler sur les nombres premiers. Il a fallu bien des années pour comprendre ce que Vinogradov avait fait, ce que Linnik avait continué, mais une version assez claire a émergé dans les années 60-70 et une version très claire dans les années 80-90 avec les travaux d'Iwaniec/ Fouvry/ Bombieri/ Friedlander. Il se trouve qu'à l'heure actuelle cette version ne semble pas être universellement connue des personnes qui travaillent sur des nombres premiers, ce qui provoque quelques quiproquos entre ceux qui déclarent que tel problème est faisable et ceux qui l'annoncent inattaquables.

Parallèlement à l'école continentale, il y a eu l'école anglaise avec des personnalités comme Hardy, Ramanujan, Littlewood, Ingham, Titchmarsh et bien d'autres, qui se sont concentrés sur la fonction $\zeta$ et l'étude des estimées de densité et donc en quelque sorte ont développé l'approche analytique. Les deux écoles sont à présent unifiées, et je vous dirai comment plus loin. Bien sûr le découpage entre école continentale et école anglaise est trop rigide pour être tout à fait correct, et l'on ne sait pas où mettre Weyl et Selberg par exemples (et non des moindres ! !). Il donne toutefois une bonne idée de la situation.

#### La méthode de Vinogradov. Une identité de crible.

Je me propose à présent de présenter la méthode de Vinogradov de façon moderne, et simple.

La méthode de Vinogradov pour évaluer les sommes oscillante portant sur les nombres premiers est réputée difficile et au mieux lourde à mettre en œuvre. Nous présentons ici l'essence de cette méthode de façon extrêmement simple.

La méthode repose sur l'identité suivante. Soit $f : \mathbb{N} \to \mathbb{C}$ une fonction bornée en module par 1 et soit $z$ et $X$ deux paramètres réels tels que $4 \leq z^2 \leq X$. Nous posons

$$r(n) = r_{z,\sqrt{X}}(n) = \sum_{\substack{p|n \\ z<p\leq\sqrt{X}}} 1, \quad \text{et} \quad P(z) = \prod_{p\leq z} p.$$

Alors

$$\boxed{\sum_{X/2<p\leq X} f(p) = \sum_{\substack{X/2<\ell\leq X\\(\ell,P(z))=1}} f(\ell) - \sum_{z<p\leq\sqrt{X}} \sum_{\substack{X/2p<d\leq X/p\\(d,P(z))=1}} \frac{f(dp)}{r(d)+1} + R(f;z,X)} \tag{5.1}$$

avec

$$R(f;z,X) = \sum_{z<p\leq\sqrt{X}} \sum_{\substack{X/(2p^2)<t\leq X/p^2\\(t,P(z))=1}} \frac{f(tp^2)}{r(pt)(r(pt)+1)}.$$

Le terme $R(f;z,X)$ doit être regardé comme un terme d'erreur et nous avons par exemple à notre disposition l'inégalité

$$|R(f;z,X)| \leq \frac{3X}{4} \sum_{z<p\leq\sqrt{X}} \frac{1}{p^2} \leq \frac{3X}{2z}.$$

Bien sûr, le crible permet d'évaluer le premier terme de notre identité.

**Preuve.** Pour établir l'identité en question, nous écrivons

$$\sum_{X/2<p\leq X} f(p) = \sum_{\substack{X/2<\ell\leq X\\(\ell,P(z))=1}} f(\ell) - \sum_{z<p\leq\sqrt{X}} \sum_{\substack{X/(2p)<d\leq X/p\\(d,P(z))=1}} \frac{f(dp)}{r(dp)}.$$

Comme $r(dp) = r(d)+1$ dès que $d$ n'est pas divisible par $p$, nous pouvons remplacer $r(dp)$ par $r(d)+1$ pourvu que nous corrigions la formule pour les $dp$ de la forme $tp^2$. $\diamond\diamond\diamond$

**La théorie en général.**

Il convient à présent de s'arrêter pour regarder ce que nous avons écrit et pour cela nous allons supposer que $f$ est de nature oscillante, par exemple $f(n) = e(\alpha n)$ si $n \in ]\sqrt{X}, X]$. Le problème est alors de montrer que $\sum_p f(p)$ est $o(\sum_p 1)$. La première somme porte sur des entiers que l'on dit "criblés". Le crible permet de traiter de telles sommes dès que $z$ est assez petit, essentiellement de l'ordre d'une petite puissance de $X$ pour que le terme d'erreur qui provient de l'évaluation de cette somme soit négligeable. On dit parfois que c'est la partie linéaire à cause de la façon dont on l'évalue, mais je parlerai de cela plus tard. Passons à la seconde somme et regardons ce que l'on peut

en faire. Et bien la grande idée consiste à l'écrire sous la forme

$$\sum_{z<m\leq\sqrt{X}} \sum_{n\leq X/m} a_n b_m f(mn) \tag{5.2}$$

où les coefficients $a_n$ et $b_m$ sont bornés et à oublier leur définitions ! ! On ne garde que les domaines de sommation. Les deux variables $m$ et $n$ sont essentiellement indépendantes (la condition $mn \leq X$ n'est pas très contraignante) ce qui rend cette somme suffisamment souple. On peut par exemple privilégier une variable et appliquer l'inégalité de Cauchy-Schwarz. Les sommes de type (5.2) sont dites bilinéaires et si il s'agit effectivement d'une grande idée que d'ignorer la définition des $a_n$, $b_m$, c'est que, sachant à présent la forme des formules que nous souhaitons, il est possible d'en trouver d'autres, ce qui a donné les identités de Linnik, Vaughan et Heath-Brown pour les plus célèbres, mais on sait à présent en construire beaucoup.

Pour aller plus loin, il faudrait analyser ce que l'on entend par la partie criblée. De telles sommes s'évaluent en termes de $\sum_{q|n\leq X} f(n)$ où la somme est en $n$. Il est parfois possible d'ajouter des sommes du type $\sum_{q|n\leq X} \tau_r(n) f(n)$ où $\tau_r$ est la fonction qui compte les $r$-uplets de diviseurs. C'est dans cette voix que s'était déjà engagé Linnik en 40-50. Le point culminant de cette approche est probablement le théorème de Fouvry qui dit que si les fonctions $\tau_2, \ldots, \tau_{12}$ ont un exposant de distribution strictement supérieur à $\frac{1}{2}$, alors il en est de même de la fonction caractéristique des nombres premiers. * La partie moderne se retrouve dans les identités de Gallagher, Vaughan, Heath-Brown, Iwaniec et Harman pour ne citer que quelques contributions majeures. Voir en particulier [*Gallagher,* 1968], [*Vaughan,* 1975], [*Iwaniec & Jutila,* 1979], [*Heath-Brown,* 1982], [*Harman,* 1982] et [*Friedlander & Iwaniec,* 1998].

Pour illustrer plus avant cette technique, il faut que je détaille la partie "criblée". On voit souvent apparaître des sommes du type

$$\sum_{mn\leq X} a_m b_n f(mn)$$

où $a_m$ est une fonction mystérieuse (du genre $\mu(m)$) et $b_n$ est une fonction bien connue en moyenne (du genre 1 ou $\mathrm{Log}\, n$). Cela ne suffit pas pour évaluer la somme précédente car si on l'écrit

$$\sum_{m\leq X} a_m \sum_{n\leq X/m} b_n f(mn)$$

∗. Résultat amélioré dans [*Fouvry,* 1984] : il suffit à présent des six premières fonctions de diviseurs.

et bien, dès que $m$ est grand, $\sum_{n\leq X/m} b_n f(mn)$ n'est *pas* une valeur moyenne (Pensez à $X/2 < m \leq X$, et $\sum_{n\leq X/m} 1 = X/m + \mathcal{O}(1)$). Cela ne fonctionne que si l'on peut interdire à $m$ d'être grand. La partie criblée se ramène précisément à des sommes du type

$$\sum_{\substack{mn\leq X\\ m\leq M}} a_m b_n f(mn).$$

Avec les années, la technique a pris le pas sur le géométrique et toute somme du type précédent à tendance à s'appeler "partie criblée" ... On dit aussi partie linéaire, ce qui est plus clair.

Je peux maintenant vous donner d'autres écritures de la fonction caractéristique des nombres premiers. Par exemple, on peut écrire

$$\Lambda(n) = \sum_{\substack{\ell m=n\\ \ell\leq X^{1/5}}} \mu(\ell)\operatorname{Log} m + \sum_{\substack{\ell m=n\\ \ell\leq X^{2/5}}} c_\ell + \sum_{\substack{\ell m=n\\ X^{1/5}<\ell,m\leq X^{4/5}}} a_\ell \Lambda(m)$$

pour $X^{1/5} < n \leq X$ avec

$$\begin{cases} c_\ell = - \displaystyle\sum_{\substack{hs=\ell\\ h\leq X^{1/5}, s\leq X^{1/5}}} \mu(h)\Lambda(s) & |c_\ell| \leq \operatorname{Log}\ell \\ a_\ell = - \displaystyle\sum_{\substack{hs=\ell\\ s\leq X^{1/5}}} \mu(s) & |a_\ell| \leq d(\ell). \end{cases}$$

Traduction en termes de séries de Dirichlet

$$\frac{-\zeta'}{\zeta} = F_K - \zeta F_K M_L - \zeta' M_L + \big(\frac{-\zeta'}{\zeta} - F_K\big)(1-\zeta M_L)$$

avec $F_K(s) = \sum_{n\leq K} \Lambda(n) n^{-s}$ et $M_L(s) = \sum_{n\leq L} \mu(n) n^{-s}$, où le lecteur avisé reconnaîtra l'influence des estimations de densité au dernier facteur. Dans notre exemple nous avons pris $K = L = X^{1/5}$.

En fait l'idée d'introduire des formes bilinéaires est due à Vinogradov et c'est aussi l'une des clefs du théorème de valeur moyenne. Toutefois la formulation de Vinogradov que l'on trouvera dans son monographe (écrit pourtant dans les années 50 et réécrit en 80) est extrêmement plus compliquée, ce qui fait que la folk-lore dit que la méthode de Vinogradov est difficilement utilisable, contrairement à ce que je viens de vous montrer. Ceci est dû à ce que le crible était beaucoup moins bien maîtrisé du temps de Vinogradov

(notamment à cause de l'absence de la méthode de Rankin). On pourra consulter le livre de Ellison sur les nombres premiers, qui date cette fois-ci de 1975. Ici, il faut que j'indique que la méthode proposée plus haut a été motivée par la présentation de ce livre.

Alors que l'obtention de formes bilinéaires était l'objectif déclaré de Vinogradov, il fallut attendre 1968 et le travail de [*Gallagher,* 1968] pour que l'on s'aperçoive que les techniques développées dans le cadre des estimées de densité permettaient d'écrire des identités similaires à $(Bin)$. Ces technique ont été initiées par [*Bohr & Landau,* 1914] et [*Carlson,* 1920].

La grande philosophie à retenir de ceci, c'est que la fonction caractéristique des nombres premiers s'exprime comme celle d'une suite criblée et d'une forme bilinéaire.

## 5.3 Une application.

Nous présentons ici une application de la formule (5.1) où nous allons étudier la forme bilinéaire de façon assez fine. Nous avons dit que dans $(Bin)$, il était usuel d'ignorer la définition des coefficients, cette définition étant souvent au-delà de notre capacité d'étude. Toutefois, dans (5.1), l'un des coefficients est la fonction caractéristique des nombres premiers, et nous pouvons dès lors remplacer, au cours d'une majoration, ces coefficients par des entiers sans petits facteurs premiers, ce que nous illustrons ici.

Nous nous intéressons à

$$S(\alpha) = \sum_{X<p\leq X'} e(p\alpha). \tag{5.3}$$

où $2 \leq X \leq X' \leq 2X$, et plus précisément lorsque $\alpha$ est de la forme $\beta + a/q$ avec $a$ premier à $q$, $q$ relativement petit et $|\beta|$ petit. Notre but est de démontrer que $S(\alpha) = o(X/\operatorname{Log} X)$ dès que $q \to \infty$, ce que ne donne pas les techniques usuelles.

[*Daboussi,* 1996] a obtenu

$$|S(a/q)| \ll \frac{\operatorname{Log}^{1-\delta} X}{\sqrt{q}} \frac{X}{\operatorname{Log} X} \qquad (q \leq X^{1/4}) \tag{5.4}$$

pour un certain $\delta > 0$ et je me suis aperçu que Vinogradov avait déjà considéré ce problème en 76, dans la seconde édition de son livre ! Il est toutefois difficile de reconnaître ce résultat à cause de ses notations (cf Selected Works, chapitre 4 de Special Variants

of the Method of Trigonometrical Sums, Théorème 2, page 344. Prendre $r = \operatorname{Log} N$, on vérifie que $\epsilon_1 = 5\epsilon$ convient). Il obtient

$$|S(a/q)| \ll_A \frac{\operatorname{Log}^5 q}{\sqrt{q}} \frac{X}{\operatorname{Log} X} \qquad (q \leq \operatorname{Log}^A X,\ A \geq 0). \tag{5.5}$$

Tout en simplifiant la preuve, la version de la section précédente permet d'améliorer ce résultat.

**Théorème 5.3.1** *Pour $X \geq 1$, tout $q \leq \exp(\frac{1}{4}\operatorname{Log}^{1/2} X)$ et tout $\alpha = a/q + \beta$ avec $|\beta| \leq \exp(2\operatorname{Log}^{1/2} X)X^{-1}$ et $a$ premier à $q$, nous avons*

$$|S(\alpha)| \ll \frac{\operatorname{Log}^2 q \operatorname{Log}\operatorname{Log} q}{\sqrt{q}} \frac{X}{\operatorname{Log} X}.$$

Nous obtenons en fait $\sqrt{q}/\phi(q)$ comme dépendance en $q$, mais nous ne donnons ci-dessous qu'une preuve simplifiée. Laquelle contient néanmoins l'essentiel de l'architecture. *

Toutes les constantes sont explicites bien que malheureusement assez grandes.

Sous l'hypothèse de Riemann pour les fonctions $L$, nous avons

$$|S(a/q)| \ll \left(\frac{\mu^2(q)}{\phi(q)} + \sqrt{q^2/X}\operatorname{Log} X\right) \frac{X}{\operatorname{Log} X} \tag{5.6}$$

alors qu'en utilisant le théorème des nombres premiers pour le module $q$ et en supposant qu'il y ait effectivement un zéro de Siegel, nous obtenons

$$|S(a/q)| \sim \frac{\sqrt{q}}{\phi(q)} \frac{X^{1-\delta}}{\operatorname{Log} X}.$$

**Preuve.** *Si l'exposé précédent est destiné à un public général, les lignes qui suivent s'adressent elles à des spécialistes.* Nous utilisons l'identité précédente avec $\operatorname{Log} z = (\operatorname{Log} X/\operatorname{Log} q) - 1$. Remarquons que cela nous garantit $q \leq z^{1/9}$. Le lemme fondamental

∗. Voir [*Ramaré,* 2010] pour plus de détails.

du crible de Brun nous donne

$$\sum_{\substack{X<d\le X'\\(d,P(z))=1}}(1\pm\Re e(d\alpha))=\prod_{\substack{p\le z\\(p,q)=1}}\big(1-1/p\big)(X'-X)(1+\mathcal{O}(e^{-\operatorname{Log}M/\operatorname{Log}z}))$$
$$+\mathcal{O}\Big(\sum_{\substack{m\le M\\(m,q)=1}}1/\|m\alpha\|\Big)$$
$$=\prod_{\substack{p\le z\\(p,q)=1}}\big(1-1/p\big)(X'-X)(1+\mathcal{O}(q^{-2/3}))+\mathcal{O}\Big(\frac{X\operatorname{Log}q}{q\operatorname{Log}X}\Big)$$

en prenant $M=X/(q\operatorname{Log}X)$ et $q\le X^{1/4}$. En faisant de même avec la partie imaginaire et en comparant avec $|\sum_{\substack{X<d\le X'\\(d,P(z))=1}}1|$, nous obtenons

$$\Big|\sum_{\substack{X<d\le X'\\(d,P(z))=1}}e(d\alpha)\Big|\ll\frac{X}{q^{2/3}\operatorname{Log}X}.$$

Pour majorer la partie bilinéaire, nous découpons tout d'abord sommation en $p$ en parties diadiques $]P,P']$ avec $P<P'\le 2P$ et utilisons l'inégalité de Cauchy-Schwartz. Il vient

$$\Sigma(P)=\Big|\sum_{P<p\le P'}\sum_{\substack{X/p<d\le X'/p\\(d,P(z))=1}}\frac{e(dp\alpha)}{r(d)+1}\Big|^2$$
$$\ll\frac{P}{\operatorname{Log}P}\sum_{-X/P\le d\le X/P}\sum_{\substack{X/P'<d_1,d_2\le X/P\\(d_1d_2,P(z))=1\\d_1-d_2=d}}\sum_{n\sim P}\Big(\sum_{m|n}\lambda_m\Big)^2e(nd\alpha)$$

où la sommation en $n$ est venue remplacer la sommation en $p$ et où les $\lambda_d$ sont ceux du crible de Selberg pour cribler tous les facteurs premiers $\le y=P^{1/4}$ et ne divisant pas $q$. La notation "$n\sim P$" est mise pour remplacer "$\max(X/d_1,X/d_2)\le n\le\min(X'/d_1,X'/d_2)$". Le crible de Brun nous donne encore

$$\sum_{\substack{X/P'<d_1,d_2\le X/P\\(d_1d_2,P(z))=1\\d_1-d_2=d}}1\ll\frac{X}{P(\operatorname{Log}z)^2}\prod_{\substack{p|d\\p|P(z)}}\big(1+1/p\big)=\frac{X}{P(\operatorname{Log}z)^2}g(d)\qquad\text{si}\quad d\ne0.$$

Nous distinguons selon que $d = 0$, ou $q|d \neq 0$ ou non et obtenons

$$\Sigma(P) \ll \frac{P}{\operatorname{Log} P}\Bigg( \quad \frac{P}{\operatorname{Log} y}\left(\frac{X}{P\operatorname{Log} z} + \frac{X}{Pq}\frac{X}{P\operatorname{Log}^2 z}\right) + \frac{X}{P(\operatorname{Log} z)^2}\sum_{\substack{1\le d\le X/P\\ d\not\equiv 0[q]}} g(d)\sum_{m_1,m_2\le y}|\lambda_{m_1}\lambda_{m_2}|\sum_{[m_1,m_2]|n\sim P} e(nd\alpha)\Bigg)$$

Maintenant les $\lambda_d$ sont bornés en module par 1 ce qui nous donne :

$$\begin{aligned}\Sigma(P) &\ll \frac{q}{\phi(q)}\frac{X^2}{q\operatorname{Log}^2 P\operatorname{Log}^2 z} + \frac{X}{\operatorname{Log} P(\operatorname{Log} z)^2}\sum_{\substack{m_1,m_2\le y\\ (m_1m_2,q)=1}}\sum_{1\le d\le X/P}\frac{g(d)}{\|[m_1,m_2]d\alpha\|}\\ &\ll \frac{1}{\phi(q)}\frac{X^2}{\operatorname{Log}^2 P\operatorname{Log}^2 z} + \frac{X^2qy^2}{P\operatorname{Log} P(\operatorname{Log} z)^2}\\ &\ll \frac{1}{\phi(q)}\frac{X^2}{\operatorname{Log}^2 P\operatorname{Log}^2 z}\left(1+\frac{q^2\operatorname{Log} P}{P^{1/4}}\right) \ll \frac{1}{\phi(q)}\frac{X^2}{\operatorname{Log}^2 P\operatorname{Log}^2 z}.\end{aligned}$$

Il nous faut ensuite sommer les $\Sigma(P)^{1/2}$, ce qui donne

$$\frac{1}{\sqrt{\phi(q)}}\frac{X\operatorname{Log}(X^{1/2}/z)}{\operatorname{Log}^2 z} \ll \frac{\operatorname{Log}\operatorname{Log} q\,(\operatorname{Log}^2 q)}{q^{1/2}}\frac{X}{\operatorname{Log} X}.$$

La preuve de notre théorème est alors complète. $\diamond\diamond\diamond$

# Problèmes polynomiaux

Cette partie contenait les articles suivants :

Nombres de racines d'un polynôme entier modulo $q$. [*Branton & Ramaré,* 1998]

*Un article en commun avec M. Branton.*

On sums of seven cubes. [*Bertault* et al. *,* 1999].

*Un article en commun avec F. Bertault et P. Zimmermann. Bien plus de matériel (en partie en collaboration avec E. Bombieri) concernant les sommes de 7 cubes a été l'objet de nombreux exposés, mais seule cette petite partie est à ce jour sortie des tiroirs.*[*]

∗. Depuis, j'ai écrit [*Ramaré,* 2005] et [*Ramaré,* 2007].

# Oscillations des termes d'erreur

Le lecteur trouvera ici l'article d'exposition :

Propriétés de densité de l'ensemble des entiers tels que $\psi(r) - r > 0$.

Cette partie contenait l'article suivant :

Almost periodicity of some error terms in prime number theory [*Kaczorowski & Ramaré,* 2003].

*Un article en commun avec J. Kaczorowski, où nous montrons que les termes d'erreurs usuels apparaissant au niveau des nombres premiers sont presque périodiques au sens de Stepanov, que les densités afférantes sont semi-continues supérieurement, toujours au sens de Stepanov, et presque périodiques au sens de Weyl. Ceci a plusieurs conséquences, dont le fait qu'une irrégularité de distribution se répète à l'infini et à intervalle multiplicativement borné.*

# Chapitre 6

# Propriétés de densité de l'ensemble des entiers tels que $\psi(r) - r > 0$

Nous motivons ici et introduisons les notions nécessaires à la compréhension d'un travail en commun avec Jerzy Kaczorowski.

## 6.1 Introduction.

Les problèmes qui nous intéressent concernent l'ensemble des valeurs prises par des fonctions "arithmétiques" liées aux nombres premiers. Pour illustrer mon propos et le rendre plus concret, je vais rappeler deux problèmes et résultats attenants.

**Premier problème :**

Nous regardons tout d'abord l'ensemble

$$\mathcal{A}_y = \{ r \in \mathbb{N} \quad / \quad \psi(r) - r > y\sqrt{r} \} \qquad (y \in \mathbb{R})$$

et nous nous demandons ce que nous pouvons dire sur sa "densité" (logarithmique, naturelle, ...). La fonction $\psi$ qui intervient ici est bien sûr celle de Tchebychef.

En 1914, Littlewood montrait $A_y(R) = \Omega(R^{1/2} \operatorname{Log}\operatorname{Log}\operatorname{Log} R)$ ce qui est resté inchangé jusqu'en 1994 où Kaczorowski obtenait $A_y(R) = \Omega_\varepsilon(R^{1-\varepsilon})$ pour tout $\varepsilon > 0$.

La preuve de Littlewood (ou celle postérieure d'Ingham) se décompose en deux : soit l'hypothèse de Riemann est fausse et le résultat découle d'un théorème $\Omega$ du type de Landau, soit l'hypothèse de Riemann est vraie et la preuve devient difficile.

**Nous nous restreignons ici au cas où l'hypothèse de Riemann est vérifiée** et proposons une description de la situation.

**Second problème :**

Considérons à présent la fonction de comptage

$$N(R; 1, 3, 4) = \#\{r \leq R, \quad \psi(r; 4, 1) > \psi(r; 4, 3)\ \}$$

où $\psi(r; 4, a) = \sum_{n \leq r, n \equiv a[4]} \Lambda(n)$. Turan & Knapowski (1962) ont conjecturé que

$$\lim_{R \to \infty} \frac{N(R; 1, 3, 4)}{R} = 0$$

afin de confirmer une assertion de Tchebischev disant qu'il y avait plus de nombres premiers congrus à 3 modulo 4 qu'à 1 modulo 4. Un tel résultat restait largement hors d'atteinte puisque l'on n'avait aucune méthode donnant accès à la densité naturelle, jusqu'en 1992 où Kaczorowski obtenait (sous GRH) :

$$0 < \liminf \frac{N(R; 1, 3, 4)}{R} \leq 0.0000106$$
$$0.040540454 \leq \limsup \frac{N(R; 1, 3, 4)}{R} < 1.$$

les deux inégalités larges datant en fait de 1995.

La densité naturelle n'existe donc pas ! Que se passe-t'il ?

## 6.2 Fonctions presque-périodiques.

Il nous faut faire un détour par les fonctions presque périodiques pour pouvoir exposer nos résultats. Nous recommendons au lecteur la lecture de l'excellente monographie [*Bohr,* (1951) 1974], ainsi que celle du livre de référence [*Besicovitch,* 1955]. Si $f$ est

une fonction sur $\mathbb{R}$, la fonction $f_\tau$ se définit par $f_\tau(t) = f(t+\tau)$. Par ailleurs un sous-ensemble $E$ de la droite réelle est dit relativement dense (r.d.) si il existe un réel positif $\ell$ tel que tout intervalle de longueur $\geq \ell$ contienne au moins un point de $E$. Ce sont ces ensembles qui vont généraliser les progressions arithmétiques.

La distribution des valeurs de telles fonctions est très bien étudiée dans [*Bochner & Jessen,* 1934], et ce papier est essentiellement définitif en ce qui concerne la densité logarithmique.

Commençons par rappeler la première notion de presque-périodicité, avant de l'étendre. Une fonction $f$ de $C^0(\mathbb{R})$ est dite uniformément presque périodique (**Uap**) si l'une des trois propriétés équivalentes suivantes est vérifiée :

- $f$ est limite uniforme de combinaisons linéaires de $e^{i\lambda t}$ ($\lambda \in \mathbb{R}$).
- $\{f_\tau, \tau \in \mathbb{R}\}$ est relativement compact pour $\|\cdot\|_\infty$.
- $\forall \varepsilon > 0$, $UE(f,\varepsilon) = \{\tau \in \mathbb{R}, \|f - f_\tau\|_\infty \leq \varepsilon\}$ est r.d.

L'équivalence entre le premier et le troisième point constitue la théorie de Bohr, et la découverte de l'équivalence avec le second, la théorie de Bochner. Par *relativement compact*, nous entendons que son adhérence est compacte.

Nous introduisons aussi deux autres notions de fonctions presque périodiques.

Pour **S$^2$ap**, i.e. presque périodique au sens de [*Stepanoff,* 1926], il suffit de remplacer le Banach $(C^0(\mathbb{R}), \|\cdot\|_\infty)$ par $(L^2_{loc}(\mathbb{R}), \|\cdot\|_{S^2})$, où la (semi-)norme est définie par

$$\|f\|_{S^2} = \max_{x\in\mathbb{R}} \left( \int_x^{x+1} |f(t)|^2 dt \right)^{1/2}.$$

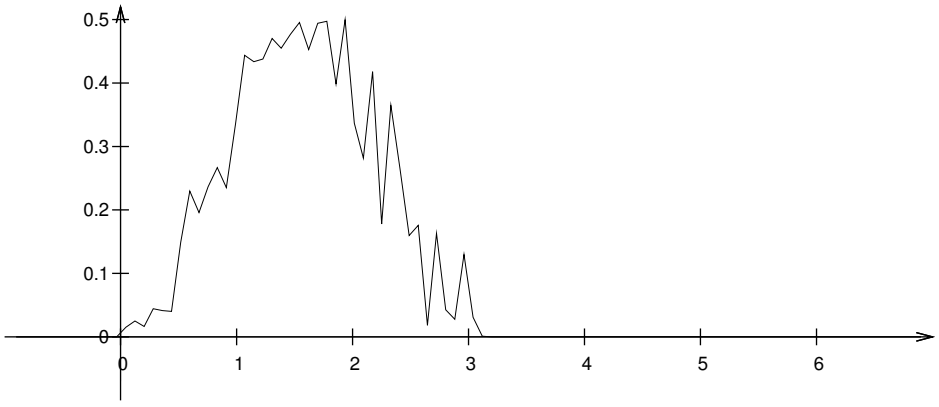
Pour **W$^2$ap**, i.e. presque périodique au sens de Weyl, il suffit de remplacer le Banach $(C^0(\mathbb{R}), \|\cdot\|_\infty)$ par $(L^2_{loc}(\mathbb{R}), \|\cdot\|_{W^2})$, où la (semi-)norme est définie par

$$\|f\|_{W^2} = \lim_{V\to\infty} \max_{x\in\mathbb{R}} \left( \frac{1}{V} \int_x^{x+V} |f(t)|^2 dt \right)^{1/2}.$$

Le fait que nous ayons encore l'équivalence des trois propriétés énoncées plus haut nous grarantit qu'il s'agit là de "bonnes" définitions, au sens où la théorie des fonctions **Uap** se transpose presque intégralement.

**Une propriété commune aux fonctions Uap et S$^2$ap :**

Supposons que l'on calcule $f$ entre 0 et 1 et que son graphe ressemble à




Nous pouvons peut alors retrouver cette forme de courbe à $\varepsilon$ près aussi loin que l'on veut, le long d'un ensemble r.d. Nous *exportons* donc un comportement qui a lieu à un temps fini jusqu'à l'infini. La notion de "comportement" demande une précision : il s'agit ici la forme de la courbe, et une déformation est mesurée par rapport à la norme utilisée. Le dernier théorème de cet exposé montre que nous pouvons utiliser la norme uniforme $\|\cdot\|_\infty$ dans le cas des fonctions qui nous intéresse.

Cette propriété n'est pas partagée par les fonctions W$^2$ap (parce que le $V$ dépend de $\varepsilon$) : nous pouvons d'ailleurs modifier le comportement de telles fonctions sur un intervalle fini sans changer leur norme afférente $\|f\|_{W^2}$.

## 6.3 Principe

Notre étude repose sur la fonction $\phi$ définie par :

$$e^{v/2}\phi(v) = \begin{cases} v + {\sum_{n\leq e^{-v}}}' \frac{\Lambda(n)}{n} + e^v + \frac{1}{2}\operatorname{Log}\Big(\frac{1-e^v}{1+e^v}\Big) + \gamma & \text{lorsque } v < 0 \\ e^v - {\sum_{n\leq e^{v}}}' \Lambda(n) - \frac{1}{2}\operatorname{Log}(1-e^{-2v}) - \operatorname{Log} 2\pi & \text{lorsque } v > 0, \end{cases} \tag{6.1}$$

où $\gamma$ est la constante d'Euler, et où le $'$ sur les sommations signifie qu'il faut affecter le dernier terme d'un coefficient $\frac{1}{2}$ lorsque $e^{-v}$ (resp. $e^{v}$) est un entier.

Nous pouvons alors déduire d'un lemme de Kaczowski de 1992 le théorème suivant :

**Théorème 6.3.1** *$\phi$ est S$^2$ap.*

Il montre en fait que

$$\phi(v) = S^2 \lim_{u \to 0^+} \sum_{\gamma > 0}{}' \frac{e^{(v+iu)\rho}}{\rho}.$$

Notons les points suivants :

- Kaczorowski utilisait cette propriété sans le dire et n'utilisait donc pas le théorème structural de Stepanoff.
- En écrivant ce théorème sous cette forme et en lui adjoignant la remarque sur l'exportation des comportements, nous voyons clairement comment obtenir des résultats sur les densités naturelles.
- Bien que presque seules les valeurs positives de $\phi$ nous intéressent, il faut noter que la théorie des fonctions presque-périodiques sur une demi-droite est beaucoup moins riche que celle des fonctions presque-périodiques sur $\mathbb{R}$ tout entier. Notre définition presque "anodine" de $\phi$ donne en fait bien plus de renseignements sur les propriétés de cette fonction.

Nous pouvons maintenant revenir aux problèmes de densité. Pour $f$ S$^2$ap à valeurs réelles, posons

$$\nabla_y(f, T) = e^{-T} \int_{-\infty}^{T} \mathbb{1}_{\{f(t)>y\}} e^t dt.$$

Alors $A_y(R)/R \simeq \nabla_y(\phi, \operatorname{Log} R)$. Nous émettons la conjecture suivante [*] :

**Conjecture 6.3.1** *$\nabla_y(\phi, \cdot)$ est Uap.*

Sauf peut-être pour $y$ appartenant à un ensemble dénombrable. Puisque cette fonction est uniformément continue (elle est même lipschitzienne), montrer qu'elle est S$^2$ap impliquerait qu'elle est Uap, à cause d'un théorème de Bochner.

[*]. [*Schlage-Puchta,* 2009] a depuis démontré cette conjecture pour une large classe de fonctions, classe qui inclut en particulier tous les exemples que nous avons considéré jusau'à présent.

## 6.4 Résultats

**Théorème 6.4.1** *Soit $f$ $S^2$ap à valeurs réelles. Il existe un ensemble au plus dénombrable $\mathcal{Y}$ tel que pour tout $y \in \mathbb{R} \setminus \mathcal{Y}$, la fonction $\nabla_y(\phi, \cdot)$ est W$^2$ap.*

Nous définissons alors une fonction admissible comme étant une fonction qui vérifie :
- $w : \mathbb{R} \to \mathbb{R}$, $w$ est croissante, $C^1$ par morceaux et appartient à $L^1(]-\infty, 0])$.
- $W(T) = \int_{-\infty}^{T} w(t)dt$ tend vers l'infini lorsque $T$ tend vers l'infini.

**Corollaire 6.4.1** *Soit $w$ une fonction admissible et telle que $w(t) = o(W(t))$ quand $t \to +\infty$. Soit de plus une fonction $f$ vérifiant les hypothèses du théorème précédent. Pour tout $y \in \mathbb{R} \setminus \mathcal{Y}$, nous avons*

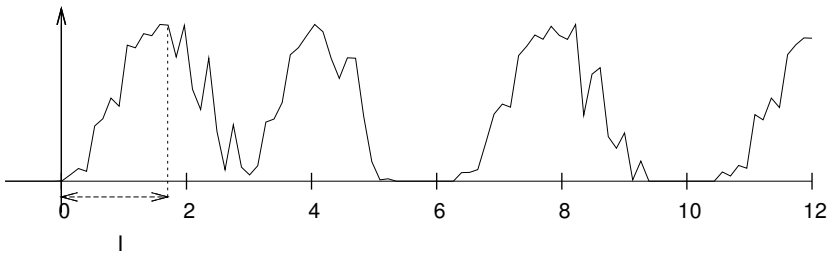
$$\frac{1}{W(T)} \int_{-\infty}^{T} \mathbb{1}_{\{f(t)>y\}} w(t)dt \to \delta_y \qquad (T \to +\infty).$$

Tant et si bien que nous ratons tout juste $w(t) = e^t$ ! ! Mais nous avons accès à des densité bien plus fortes mieux que la densité logarithmique ($w(t) = 1$, cf [*Rubinstein & Sarnak,* 1994]).

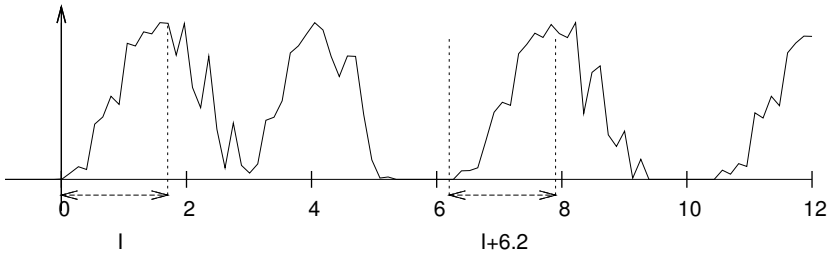
**Théorème 6.4.2** *Pour tout réel $v$, tout interval borné $I$ et tout reél $\varepsilon > 0$, il existe un réel $\alpha > 0$ tel que*

$$\forall v' \in \mathbb{R}, \quad \|\phi_v - \phi_{v'}\|_{S^2} \leq \alpha \implies \max_{t \in I} \left|\nabla_y(\phi, v+t) - \nabla_y(\phi, v'+t)\right| \leq \varepsilon.$$

Voici ce que que dit ce théorème. Supposons que $\nabla_y(\phi, \cdot)$ ressemble à




Alors on retrouve le comportement sur l'intervalle choisi $I$ jusqu'à l'infini, à $\varepsilon$ près, et ce, en norme sup :




Évidemment, ces fenêtres ne se recoupent pas nécessairement...

Concluons cette présentation par un problème ouvert : nous avons établi que les fonctions $\nabla_y(\phi,\cdot)$ étaient presque périodique en un sens ou en un autre, mais toujours au moins au sens asymptotique de Besicovitch. Elles ont par conséquent des périodes, qui ne dépendent d'ailleurs pas de la norme choisie, et dont il est aisé de montrer qu'elles appartiennent au $\mathbb{Q}$-espace vectoriel engendré par celles de $\phi$. Mais leur sont-elles égales ? Le cas de la fonction $\phi$ définie en (6.1) nous intéresse particulièrement ! Des calculs numériques ne produisent à l'heure actuelle pas de résultats concluants, mais il serait intéressant de voir le graphe de cette fonction sur un intervalle très long (au moins $10^9$ puisque les deux premiers zéros de la fonction zeta de Riemann sont de l'ordre de 14 et de 21).

# Table des matières

# Références


Armitage, J.V. 15. Zeta functions with a zero at s = $\frac{1}{2}$. *Inventiones Math.*, 199–205.

Balasubramanian, R., & Ramachandra, K. 1982. On the zeros of the Riemann zeta function and $L$-series. II. *Hardy-Ramanujan J.*, **5**, 1–30.

Basquin, J. 2006. Mémoire de DEA. 1–37.

Bertault, F., Ramaré, O., & Zimmermann, P. 1999. On Sums of Seven Cubes. *Math. Comp.*, **68**, 1303–1310.

Besicovitch, A.S. 1955. *Almost periodic functions*. New York : Dover Publications Inc.

Birch, B.J., & Swinnerton-Dyer, H.P.F. 1965. Notes on elliptic curves. II. *J. Reine Angew. Math.*, **218**, 79–108.

Bochner, S., & Jessen, B. 1934. Distribution functions and positive-definite functions. *Ann. of Math. (2)*, **35**(2), 252–257.

Bohr, H. (1951) 1974. *Fastperiodische Funktionen*. Berlin : Springer-Verlag. Reprint.

Bohr, H., & Landau, E. 1914. Sur les zéros de la fonction $\zeta(s)$ de *Riemann. C. R.*, **158**, 106–110.

Bombieri, E. 1987/1974. Le grand crible dans la théorie analytique des nombres. *Astérisque*, **18**, 103pp.

Bombieri, E., & Davenport, H. 1968. On the large sieve method. *Abh. aus Zahlentheorie und Analysis zur Erinnerung an Edmund Landau*, **Deut. Verlag Wiss., Berlin**, 11–22.

Bombieri, E., Friedlander, J.B., & Iwaniec, H. 1986. Primes in arithmetic progressions to large moduli. *Acta Math.*, **156**, 203–251.

Branton, M., & Ramaré, O. 1998. Nombres de racines d'un polynôme entier modulo $q$. *J. Théorie des Nombres de Bordeaux*, **10**, 125–134.

Carlson, F. 1920. Sur les zéros des séries de Dirichlet. *C. R.*, **171**, 339–341.

Chen, Jingrun, & Wang, Tianze. 1989. On the odd Goldbach problem. *Acta Math. Sin.*, **32**(5), 702–718.

Daboussi, H. 1996. Effective estimates of exponential sums over primes. *Analytic number theory. Vol. 1. Proceedings of a conference in honor of Heini Halberstam, May 16-20, 1995, Urbana, IL, USA. Boston, MA: Birkhaeuser. Prog. Math.*, **138**, 231–244.

Deshouillers, J.-M. 1972/73. Amélioration de la constante de Šnirelman dans le problème de Goldbach. *Séminaire Delange-Pisot-Poitou*, **14**(17), 4 pp.

Deshouillers, J.-M. 1976 ?. ? ?Amélioration de la constante de Šnirelman dans le problème de Goldbach. *Séminaire Delange-Pisot-Poitou*.

Deshouillers, J.-M., Effinger, G., te Riele, H., & Zinoviev, D. 1997. A complete Vinogradov $3$-primes theorem under the Riemann hypothesis. *Electron. Res. Announc. Amer. Math. Soc.*, **3**, 99–104 (electronic).

Dusart, P. 1998. *Autour de la fonction qui compte le nombre de nombres premiers*. Ph.D. thesis, Limoges, `http\string://www.unilim.fr/laco/theses/1998/T1998_01.pdf`. 173 pp.

Dusart, P. 2007. Estimates of some functions over primes without R. H. *Preprint.*

Euler, L. 1737. *Variae observationes circa series infinitas*. St Petersburg Academy.

Fouvry, E. 1984. Autour du théorème de Bombieri-Vinogradov. *Acta Math.*, **152**, 219–244.

Friedlander, J., & Iwaniec, H. 1998. Asymptotic sieve for primes. *Ann. of Math. (2)*, **148**(3), 1041–1065.

Gallagher, P.X. 1968. Bombieri's mean value theorem. *Mathematika*, **15**, 1–6.

Gallagher, P.X. 1974. Sieving by prime powers. *Acta Arith.*, **24**, 491–497.

Goldfeld, D. 1985. Gauss's class number problem for imaginary quadratic fields. *Bull. Amer. Math. Soc. (1)*, **13**, 23–37.

Goldfeld, D., & Schinzel, A. 1975. On Siegel's zero. *Ann. Scuola Norm. Sup. Pisa Cl. Sci.*, **4**, 571–575.

Graham, S.W., & Ringrose, C.J. 1990. Lower bounds for least quadratic non-residues. *progress in Math.*, **85**, 267–30 ?

Granville, A., & Ramaré, O. 1996. Explicit bounds on exponential sums and the scarcity of squarefree binomial coefficients. *Mathematika*, **43**(1), 73–107.

Gross, B., & Zagier, D. 1983. Points de Heegner et derivées de fonctions L. *C. R. Acad. Sci, Paris, Ser. I*, **297**, 85–87.

Halberstam, H., & Richert, H.E. 1974. Sieve methods. *Academic Press (London)*, 364pp.

Haneke, W. 1973. Über die reellen Nullstellen der Dirichletschen $L$-Reihen. *Acta Arith.*, **22**, 391–421.

Haneke, W. 1976. Corrigendum to Über die reellen Nullstellen der Dirichletschen $L$-Reihen. *Acta Arith.*, **31**, 99–100.

Harman, G. 1982. Primes in short intervals. *Math. Z.*, **180**(3), 335–348.

Heath-Brown, D.R. 1982. Prime numbers in short intervals and a generalized Vaughan identity. *Canad. J. Math.*, **34**(6), 1365–1377.

Hooley, C. 1957. On the representation of a number as a sum of two squares and a prime. *Acta Math.*, 189–210.

Hooley, C. 1976. *Applications of sieve methods to the theory of numbers*. Cambridge Tracts in Mathematics, vol. 70. Cambridge etc. : Cambridge University Press. XIV.

Iwaniec, H., & Jutila, M. 1979. Primes in short intervals. *Ark. Mat.*, **17**(1), 167–176.

Iwaniec, H., & Kowalski, E. 2004. *Analytic number theory*. American Mathematical Society Colloquium Publications. American Mathematical Society, Providence, RI. xii+615 pp.

Kaczorowski, J. 1991. The $k$-functions in multiplicative number theory. IV. On a method of A. E. Ingham. *Acta Arith.*, **57**(3), 231–244.

Kaczorowski, J. 1993. A contribution to the Shanks-Rényi race problem. *Quart. J. Math. Oxford Ser. (2)*, **44**(176), 451–458.

Kaczorowski, J. 1994. Results on the distribution of primes. *J. Reine Angew. Math.*, **446**, 89–113.

## Références


Kaczorowski, J., & Ramaré, O. 2003. Almost periodicity of some error terms in prime number theory. *Acta Arith.*, **106**(3), 277–297.

Kadiri, H. 2002. *Une région explicite sans zéros pour les fonctions $L$ de Dirichlet*. Ph.D. thesis, Université Lille 1. `http://tel.ccsd.cnrs.fr/documents/archives0/00/00/26/95/index_fr.html`.

Kadiri, H. 2005. Une région explicite sans zéros pour la fonction $\zeta$ de Riemann. *Acta Arith.*, **117**(4), 303–339.

Kadiri, H. 2006. Small intervals containing primes in arithmetic progressions and an application. *Submitted to Math. Comp.*, 1–18.

Kadiri, H. 2009. An explicit zero-free region for the Dirichlet $L$-functions. *To appear in J. Number Theory*.

Kaniecki, L. 1995. On Šnirelman's constant under the Riemann hypothesis. *Acta Arith.*, **72**(4), 361–374.

Klimov, N.I. 1969. A propos the computation of Šnirel'man's constant. *Volz. Mat. Sb. Vyp.*, **7**, 32–40.

Klimov, N.I., Pil'tjai, G.Z., & Septickaja, T.A. 1972. Eine Abschätzung der absoluten Konstante im Goldbach-Snirel'manschen Problem. *Issled. Teor. Cisel*, **Saratov 4**, 35–51.

Linnik, Yu.V. 1961. The dispersion method in binary additive problems. *Leningrad*, 208pp.

Liu, Ming-Chit, & Wang, Tianze. 2002. On the Vinogradov bound in the three primes Goldbach conjecture. *Acta Arith.*, **105**(2), 133–175.

Louboutin, S. 1993. Majorations explicites de $|L(1,\chi)|$. *C. R. Acad. Sci. Paris*, **316**, 11–14.

Louboutin, S. 1996. Majorations explicites de $|L(1,\chi)|$ (suite). *C. R. Acad. Sci. Paris*, **323**, 443–446.

Low, M. 1968. Real zeros of the Dedekind zeta function of an imaginary quadratic field. *Acta Arith.*, **14**, 117–140.

McCurley, K.S. 1984a. Explicit estimates for the error term in the prime number theorem for arithmetic progressions. *Math. Comp.*, **42**, 265–285.

McCurley, K.S. 1984b. Explicit estimates for $\theta(x;3,\ell)$ and $\psi(x;3,\ell)$. *Math. Comp.*, **42**, 287–296.

Montgomery, H., & Weinberger, P. 1973. Notes on small class numbers. *Acta Arith.*, **24**, 529–542.

Montgomery, H.L. 1971. Topics in Multiplicative Number Theory. *Lecture Notes in Mathematics (Berlin)*, **227**, 178pp.

Montgomery, H.L., & Vaughan, R.C. 1973. The large sieve. *Mathematika*, **20**(2), 119–133.

Motohashi, Y. 1979. A note on Siegel's zeros. *Proc. Jap. Acad., Ser. A*, **55**, 190–192.

Motohashi, Y. 1983. Sieve Methods and Prime Number Theory. *Tata Lectures Notes*, 205.

Oesterlé, J. 1985. Nombres de classes des corps quadratiques imaginaires. *Astérisque*, **121/122**, 309–323.

Pintz, J. 1976. Elementary methods in the theory of $L$-functions, II. On the greatest real zero of a real $L$-function. *Acta Arith.*, **31**, 273–289.

Ramaré, O. 1991. *Contribution au problème de Goldbach : tout entier $> 1$ est d'au plus 13 nombres premiers*. 1–70pp, Université Bordeaux I.

Ramaré, O. 1995. On Snirel'man's constant. *Ann. Scu. Norm. Pisa*, **21**, 645–706. `http://math.univ-lille1.fr/~ramare/Maths/Article.pdf`.

Ramaré, O. 2001. Approximate Formulae for $L(1,\chi)$. *Acta Arith.*, **100**, 245–266.

Ramaré, O. 2002. Sur un théorème de Mertens. *Manuscripta Math.*, **108**, 483–494.

Ramaré, O. 2004. Approximate Formulae for $L(1,\chi)$, II. *Acta Arith.*, **112**, 141–149.

Ramaré, O. 2005. An explicit seven cube theorem. *Acta Arith.*, **118**(4), 375–382.

Ramaré, O. 2006. *Variations modernes sur la suite des nombres premiers. De la densité des sin(p) lorsque p parcourt l'ensemble des nombres premiers.* Lulu.com. 105pp.

Ramaré, O. 2007. An explicit result of the sum of seven cubes. *Manuscripta Math.*, **124**(1), 59–75.

Ramaré, O. 2009. *Arithmetical aspects of the large sieve inequality*. Harish-Chandra Research Institute Lecture Notes, vol. 1. New Delhi : Hindustan Book Agency. With the collaboration of D. S. Ramana.

Ramaré, O. 2009. A purely analytical lower bound for $L(1,\chi)$. *Annales Mathématiques Blaise Pascal*, **16**(2), 259–265.

Ramaré, O. 2010. On Bombieri's asymptotic sieve. *J. Number Theory*, 40pp.

Ramaré, O., & Rumely, R. 1996. Primes in arithmetic progressions. *Math. Comp.*, **65**, 397–425.

Ramaré, O., & Ruzsa, I.M. 2001. Additive properties of dense subsets of sifted sequences. *J. Théorie N. Bordeaux*, **13**, 559–581.

Ramaré, O., & Saouter, Y. 2003. Short effective intervals containing primes. *J. Number Theory*, **98**, 10–33.

Riesel, H., & Vaughan, R.C. 1983. On sums of primes. *Arkiv för mathematik*, **21**, 45–74.

Rosser, J.B. 1941. Explicit bounds for some functions of prime numbers. *American Journal of Math.*, **63**, 211–232.

Rosser, J.B. 1949. Real roots of Dirichlet $L$-series. *Bull. Amer. Math. Soc.*, **55**, 906–913.

Rosser, J.B. 1950. Real roots of Dirichlet $L$-series. *J. Res. Nat. Bur. Standards*, 505–514.

Rosser, J.B., & Schoenfeld, L. 1962. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, **6**, 64–94.

Rosser, J.B., & Schoenfeld, L. 1975. Sharper bounds for the Chebyshev Functions $\vartheta(X)$ and $\psi(X)$. *Math. Comp.*, **29**(129), 243–269.

Rubinstein, M., & Sarnak, P. 1994. Chebyshev's bias. *Experiment. Math.*, **3**(3), 173–197.

Rumely, R. 1993. Numerical Computations Concerning the ERH. *Math. Comp.*, **61**, 415–440.

Schlage-Puchta, J.-C. 2009. Private communication.

Schoenfeld, L. 1976. Sharper bounds for the Chebyshev Functions $\vartheta(X)$ and $\psi(X)$ II. *Math. Comp.*, **30**(134), 337–360.

Selberg, A. 1976. Remarks on multiplicative functions. *Lectures Notes in Mathematics (Berlin)*, **626**, 232–241.

Shanks, D. 1973. Systematic examination of Littlewood's bounds on $L(1,\chi)$. *Proc. Sympos. Pure Math. (St Louis Univ. Mo.)*, **24**, 267–283.

Shapiro, H.N., & Warga, J. 1950. On the representation of large integers as sums of primes. *Comm. Pure Appl. Math.*, **3**, 153–176.

Šnirel'man, L.G. 1933. Über additive Eigenschaften von Zahlen. *Math. Ann.*, **107**, 649–690.

Stepanoff, W. 1926. Über einige Verallgemeinerungen der fast periodischen Funktionen. *Math. Ann.*, **95**(1), 473–498.

Tatuzawa, T. 1951. On a theorem of Siegel. *Jap. J. of Math.*, **21**, 163–178.

Turán, P. 1959. Real zeros of Dirichlet's $L$-functions. *Acta Arith.*, **5**, 309–314.

## Références

van Lint, J.E., & Richert, H.E. 1965. On primes in arithmetic progressions. *Acta Arith.*, **11**, 209–216.

Vaughan, R.C. 1975. Mean value theorems in prime number theory. *J. London Math Soc. (2)*, **10**, 153–162.

Vaughan, R.C. 1977. On the estimation of Schnirelman's constant. *J. Reine Angew. Math.*, **290**, 93–108.