SÉMINAIRE N. BOURBAKI

PHILIPPE MICHEL

Progrès récents du crible et applications

Séminaire N. Bourbaki, 1997-1998, exp. n° 842, p. 185-209.

<http://www.numdam.org/item?id=SB_1997-1998__40__185_0>

Séminaire BOURBAKI Mars 1998
50ème année, 1997-98, n° 842

PROGRÈS RÉCENTS DU CRIBLE ET APPLICATIONS
[d'après Duke, Fouvry, Friedlander, Iwaniec]

par **Philippe MICHEL**

1. INTRODUCTION

On sait au moins depuis Euclide qu'il existe une infinité de nombres premiers. Depuis lors, un des problèmes les plus motivants de la théorie des nombres est de déterminer si certaines propriétés arithmétiques sont satisfaites par une infinité de nombres premiers. Le raisonnement par l'absurde original d'Euclide peut être adapté dans certains cas, le plus bel exemple à ce jour étant la preuve par Elkies de l'infinitude de l'ensemble des nombres premiers supersinguliers associés à une courbe elliptique sur $\mathbb{Q}$ [E]. Dans d'autres cas, des techniques plus indirectes sont nécessaires : l'invention par Dirichlet de la théorie analytique des fonctions L et des caractères permirent à celui-ci de résoudre le problème de l'infinité de nombres premiers dans les progressions arithmétiques. Mais il existe toute une classe de problèmes qui résistent aux méthodes précédentes (sans doute à cause de leur nature "non-multiplicative") ; ainsi les questions suivantes ne sont toujours pas résolues :

– existe-t-il une infinité de nombres premiers de la forme $p+2$ (resp. n^2+1) avec p premier (resp. n entier) ?

C'est pour tenter de résoudre ces questions (en l'occurence la première) que la théorie moderne du crible fut inventée par Brun au début du siècle. Son point d'orgue se situe dans les années 70-80, quand on a pu montrer l'existence d'une infinité d'entiers ayant au plus deux facteurs premiers de l'une des deux formes prescrites ci-dessus [C], [I2] (on pourra aussi consulter l'exposé de Deshouillers à ce séminaire [D]). Cependant, pour des raisons propres au crible, on ne pouvait espérer atteindre les nombres premiers eux-mêmes. Dans leurs travaux fondamentaux, Duke, Friedlander et Iwaniec [DFI] puis Friedlander et Iwaniec [FrI3] jettent les bases d'une approche nouvelle du crible, qui autorise enfin la détection des nombres premiers. La fin de cette introduction est consacrée à la description des problèmes qui ont été résolus grâce à cette approche.

Équidistribution des racines d'une congruence quadratique. Étant donné $f \in \mathbb{Z}[X]$ un polynôme irréductible de degré ≥ 2, notons $\rho_f(n)$ le nombre de solutions dans $\mathbb{Z}/n\mathbb{Z}$ de

la congruence

$$f(\nu) \equiv 0 (\mathrm{mod}\ n). \tag{1}$$

On associe à chaque solution $0 \leq \nu < n$ de la congruence (1), la fraction $\{\frac{\nu}{n}\} \in [0,1[$, et on veut étudier la répartition de cet ensemble dans l'intervalle $[0,1[$. Quand la variable n décrit l'ensemble des entiers, Hooley a montré l'équidistribution de ces fractions [Ho1]. Il est alors naturel de conjecturer que l'équidistribution persiste quand n est restreint à l'ensemble des nombres premiers. La première application spectaculaire de ces nouvelles méthodes est la démonstration de cette conjecture pour les polynômes de degré 2, d'abord pour ceux de discriminant négatif par Duke, Friedlander et Iwaniec [DFI] puis pour ceux de discriminant positif par Toth [To] :

THÉORÈME 1.1. — *Soit $f(X) = aX^2 + bX + c$ un polynôme à coefficients entiers, irréductible, de degré 2. Alors l'ensemble*

$$\{\{\frac{\nu}{p}\} \in [0,1[,\ f(\nu) \equiv 0 (\mathrm{mod}\ p), p \text{ premier}\}$$

est uniformément distribué sur $[0,1]$; plus précisément, on a pour tout $0 \leq a < b \leq 1$

$$\frac{1}{\pi(x)} \sum_{p \leq x} \sum_{\substack{f(\nu) \equiv 0 (\mathrm{mod}\ p), \\ a < \frac{\nu}{p} < b}} 1 = b - a + o(1),\ x \to +\infty.$$

REMARQUE 1.2. — Le théorème 1.1 appliqué au polynôme $f(X) = X^2 + 1$ a pour corollaire l'équidistribution des "angles" θ_p associés aux sommes de Salié : ces angles sont définis par

$$S(1,1;p) := \sum_{x \in \mathbb{F}_p^\times} \left(\frac{x}{p}\right) \mathrm{e}(\frac{x + x^{-1}}{p}) := 2\cos\theta_p,\ \theta_p \in [0,\pi].$$

Si $p \equiv 3 (\mathrm{mod}\, 4)$, on a $\theta_p = \pi/2$; le théorème 1.1 implique que les angles $\{\theta_p,\ p \equiv 1(4)\}$ sont équidistribués sur $[0,\pi]$ pour la mesure de Lebesgue. C'est l'un des rares exemples —avec les sommes de Gauss cubiques [HB-P]— de sommes d'exponentielles de module premier pour lesquelles on sache établir des résultats d'équidistribution (voir [K] pour une très belle exposition de ces sujets).

Représentations des nombres premiers par des polynômes. Un autre problème, qui n'est pas sans lien avec le précédent, est la conjecture suivante (qui remonte à Bouniakovski et qui a été généralisée par Schinzel) :

CONJECTURE 1.3. — *Étant donné un polynôme f à coefficients entiers, irréductible dans $\mathbb{Z}[X]$ dont le coefficient du terme dominant est positif et tel que le p.g.c.d des $\{f(n),\ n \in \mathbb{Z}\}$ vaut 1, alors f représente une infinité de nombres premiers.*

Jusqu'à présent, seul le cas des polynômes de degré 1 a été résolu (c'est le théorème de Dirichlet pour les nombres premiers dans les progressions arithmétiques) ; de plus, d'après Iwaniec [I2], une infinité d'entiers ayant au plus deux facteurs premiers sont représentables par un polynôme de degré 2 satisfaisant les hypothèses de la conjecture précédente. On peut aussi étudier le problème moins difficile de la représentabilité des nombres premiers par un polynôme en 2 variables ; le cas des polynômes irréductibles de degré 2 est alors complètement connu (et dû à Iwaniec [I1]). Le travail fondamental de Friedlander-Iwaniec [FrI2] traite le cas d'un polynôme de degré 4, à savoir $f(X,Y) = X^2 + Y^4$:

THÉORÈME 1.4. — *Il existe une infinité de nombres premiers de la forme $p = a^2 + b^4$ où a et b sont des entiers ; plus précisément on a pour $x \to +\infty$*

$$\sum_{p \leq x} \log p \sum_{a^2+b^4=p} 1 = \frac{4}{\pi}\kappa x + o(x),$$

a et b décrivant les entiers positifs et κ désignant la constante

$$\kappa = \int_0^1 (1-t^4)^{1/2} dt = \Gamma(1/4)^2/6\sqrt{2\pi}.$$

Cet énoncé fort élémentaire est en fait l'aboutissement d'un travail de longue haleine qui a débuté avec le théorème suivant de Fouvry et Iwaniec [FoI] :

THÉORÈME 1.5. — *Il existe une infinité de nombres premiers de la forme $p = a^2 + b^2$ où a est un entier et b est un nombre premier ; plus précisément, on a l'égalité suivante quand $x \to +\infty$,*

$$\sum_{p \leq x} \log p \sum_{a^2+b^2=p} \Lambda(b) = 2 \prod_p (1 - \frac{\chi_4(p)}{(p-1)(p-\chi_4(p))})x + o(x),$$

où χ_4 est le caractère non-trivial modulo 4.

Il faut aussi remarquer que ces énoncés fournissent des *équivalents* alors que le crible classique nous avait plutôt habitués à des *minorations* comme dans [C, I2] !

Le plan de cet exposé est le suivant : dans la première partie, on décrit la méthode générale du crible ainsi que ses limites (le phénomène de parité) puis les innovations qui ont permis de les dépasser. Les sections suivantes donnent les preuves des théorèmes 1.1 et 1.4 en se concentrant particulièrement sur ce dernier.

Remerciements : je tiens à remercier R. de la Bretèche et L. Lafforgue de leur assistance dans la rédaction de cet exposé, ainsi que H. Iwaniec pour des discussions éclairantes et les notes qu'il m'a communiquées au sujet du crible et de ses développements.

Dans la suite, $\mu(n), \Lambda(n), \omega(n), \tau(n), \left(\frac{m}{n}\right)$ désigneront la fonction de Moebius, la fonction de von Mangolt, la fonction nombre de diviseurs premiers, la fonction nombre de diviseurs de l'entier n et le symbole de Jacobi. On note $\mathrm{e}(z) := \exp(2i\pi z)$, et $n \sim N$ signifie $N \leq n < 2N$. Les variables p et q représenteront exclusivement des nombres premiers.

2. LE CRIBLE

La méthode du crible est très ancienne et remonte à Erathosthène. Elle permet de dresser très facilement la liste des nombres premiers plus petits qu'un certain x : on écrit la liste de tous les entiers $\leq x$, on raye 1 et tous les multiples de 2, puis tous les multiples de 3, et ainsi de suite. On considère le plus petit nombre non rayé (il est alors premier) et on raye tous ses multiples... L'algorithme s'arrête quand le nombre non rayé est $> x^{1/2}$, on obtient alors la liste de tous les nombres premiers compris entre $x^{1/2}$ et x :

$$\not{1}, \not{2}, \not{3}, \not{4}, 5, \not{6}, 7, \not{8}, \not{9}, \not{10}, 11.$$

Cette procédure se généralise dans le cadre suivant : on se donne une suite de complexes $\mathcal{A} = \{\rho_n\}_{n\geq 1}$ et on désire des informations sur la somme restreinte aux nombres premiers

$$A_{\mathcal{P}}(x) := \sum_{p\leq x} \rho_p,$$

ou sur sa variante pondérée

$$A_\Lambda(x) := \sum_{n\leq x} \Lambda(n)\rho_n,\ x \to +\infty.$$

Le crible d'Erathosthène se formalise comme suit : notons pour $z \geq 1$, $P(z)$ le produit des nombres premiers $p \leq z$ et

$$A(x,z) := \sum_{\substack{n\leq x \\ (n,P(z))=1}} \rho_n.$$

On désire donc estimer la somme $A(x,z)$ avec $z = x^{1/2}$ (dans la pratique, on peut même prendre z légèrement plus petit que $x^{1/2}$, puisque les termes de la somme $A(x,z)$ qui correspondent à des entiers non premiers ont exactement deux facteurs premiers $\geq z$ et sont de ce fait peu nombreux). Dans cette somme, la condition $(n,P(z)) = 1$ est détectée par l'identité de convolution suivante qui synthétise le principe d'inclusion-exclusion

$$\sum_{d|(n,P(z))} \mu(d) = \begin{cases} 1 \text{ si } (n,P(z)) = 1, \\ 0 \text{ sinon,} \end{cases}$$

l'analogue pour $A_\Lambda(x)$ étant l'identité de convolution

$$\Lambda(n) = -\sum_{d|n} \mu(d)\log(n/d). \tag{2}$$

On obtient d'une part l'identité dite de Lagrange

$$A(x,z) = \sum_{d|P(z)} \mu(d)A_d(x), \text{ avec } A_d(x) := \sum_{n\equiv 0 (\mathrm{mod}\ d)} \rho_n, \tag{3}$$

et d'autre part

$$A_\Lambda(x) = -\sum_{d\le x}\mu(d)\log d\ A_d(x), \tag{4}$$

ce qui lie le problème de détecter les nombres premiers à l'étude de la suite $\mathcal{A}$ dans les progressions arithmétiques. Il est alors naturel d'écrire la somme $A_d(x)$ sous la forme

$$A_d(x) := g(d)A(x) + r_d(x), \tag{5}$$

où $g(d)$ est une certaine fonction multiplicative (qui doit être vue comme la "probabilité d'être divisible par d") vérifiant (noter que seuls les modules d sans facteurs carrés nous intéressent)

$$g(1) = 1,\ 0 \le g(p) < 1,\ |g(p)| \ll 1/p \tag{6}$$

et où la quantité $r_d(x)$ est considérée comme un terme d'erreur.

REMARQUE 2.1. — Il n'est pas exclu que $g(d)$ soit nul pour tout $d \neq 1$.

À partir de (5), on obtient

$$A(x,z) = A(x)\prod_{p\le z}(1-g(p)) + \sum_{d|P(z)}\mu(d)r_d(x), \tag{7}$$

$$A_\Lambda(x) = \Big(-\sum_{d\le x}\mu(d)g(d)\log d\Big)A(x) + \sum_{d\le x}\mu(d)\log d\ r_d(x). \tag{8}$$

On remarque l'égalité formelle

$$-\sum_{d\ge 1}\mu(d)g(d)\log d = \prod_p(1-g(p))\big(1-\frac{1}{p}\big)^{-1},$$

qui est une égalité rigoureuse sous la condition

$$\forall y > 2,\ \sum_{d\le y}\mu(d)g(d) \ll (\log y)^{-8}. \tag{9}$$

Cette hypothèse permet alors d'extraire un terme principal heuristique pour $A_\Lambda(x)$:

$$A_\Lambda(x) = \prod_p(1-g(p))\big(1-\frac{1}{p}\big)^{-1} \times A(x) + O\Big(\frac{A(x)}{\log x}\Big) + \sum_{d\le x}\mu(d)\log d\ r_d(x).$$

REMARQUE 2.2. — Dans la pratique, la majoration (9) est conséquence de la détermination d'une région sans zéros convenable pour la série de Dirichlet

$$L_g(s) = \sum_{d\ge 1}\mu^2(d)g(d)d^{-s} = \prod_p(1+g(p)p^{-s}),$$

ce qui correspond à un analogue pour la fonction L_g de la méthode de Hadamard-de la Vallée-Poussin dans le Théorème des Nombres Premiers.

Il est donc raisonnable de chercher des hypothèses qui suffisent à assurer l'égalité

$$\sum_{n\leq x}\Lambda(n)\rho_n = \prod_p(1-g(p))(1-\frac{1}{p})^{-1}\times A(x)+o(A(x)),\ \text{quand } x\to+\infty. \tag{10}$$

Aparté. En pratique, les expressions (7) et (8) ne sont pas satisfaisantes. En effet la deuxième somme du membre de droite comporte beaucoup trop de termes pour être traitée efficacement, même dans les cas les plus favorables (par exemple quand $\mathcal{A}$ est la suite constante égale à 1 : on a $g(d)=1/d$ et $|r_d(x)|=|[\frac{x}{d}]-\frac{[x]}{d}|\leq 2$). Pour remédier à ce problème, et dans le cas original où les ρ_n sont positifs, Brun [Br] eut l'idée de remplacer la fonction μ par deux fonctions auxiliaires $\mu_D^{\pm}$, à supports dans l'ensemble des entiers sans facteurs carrés plus petits qu'un certain paramètre $D<x$ et qui vérifient

$$\mu_D^{\pm}(1)=1,\ |\mu_D^{\pm}(n)|\leq 1,\ \text{et}\ \sum_{d|n}\mu_D^{-}(d)\leq\sum_{d|n}\mu(d)\leq\sum_{d|n}\mu_D^{+}(d),$$

l'égalité (7) devenant alors l'encadrement

$$A(x)\sum_{\substack{d|P(z),\\ d\leq D}}\mu_D^{-}(d)g(d)+R_D^{-}(x)\leq A(x,z)\leq A(x)\sum_{\substack{d|P(z),\\ d\leq D}}\mu_D^{+}(d)g(d)+R_D^{+}(x), \tag{11}$$

avec

$$R_D^{\pm}(x):=\sum_{\substack{d|P(z),\\ d\leq D}}\mu_D^{\pm}(d)r_d(x).$$

La théorie classique du crible s'est alors developpée dans cette direction, les efforts étant principalement concentrés sur l'optimisation du choix des fonctions d'encadrement $\mu_D^{\pm}(n)$, sur l'encadrement du terme principal [HR] et éventuellement sur l'étude précise des termes d'erreurs $R^{\pm}(D)$ [I3]. Pour ce faire, on a besoin de l'hypothèse fondamentale :

HYPOTHÈSE **Cr.** 1. — Il existe $0<\delta\leq 1$ tel que pour tout $A>0$, et tout $x\geq x(\delta,A)$ on a en posant $D=x^{\delta}$,

$$\sum_{d\leq D}\mu^2(d)|r_d(x)|\ll_A\Big(\sum_{n\leq x}|\rho_n|\Big)(\log x)^{-A}. \tag{12}$$

Le paramètre δ est appelé un *exposant de répartition* de la suite $\{\rho_n\}$, il mesure la qualité de la distribution de $\{\rho_n\}$ dans les progressions arithmétiques de grand module d. Cependant, il est apparu assez vite que l'hypothèse **Cr.**1 seule est insuffisante pour détecter des nombres premiers (c'est-à-dire montrer que la minoration de (11) est non triviale) même si l'exposant de répartition est arbitrairement proche de 1. On a en effet l'exemple instructif de Selberg suivant : la suite $\mathcal{A}$ définie par $\rho_n=(1+\lambda(n))/2$ où $\lambda(n)=(-1)^{\omega(n)}$ est la fonction de Liouville (ρ_n est donc la fonction caractéristique des entiers ayant un nombre pair de facteurs premiers) ; elle a des exposants de répartition arbitrairement proches de 1, pourtant le support de (ρ_n) ne contient aucun nombre premier (c'est le phénomène de parité) ! Dans certains cas, la détection des nombres premiers est pourtant possible, mais elle requiert des arguments *ad hoc*, propres à chaque situation

qui permettent de modifier le traitement trop général du crible classique et d'éviter le phénomène de parité (le premier exemple remonte à Iwaniec et Jutila [IJ] et concernait les nombres premiers dans les petits intervalles ; voir aussi les articles de Harman et Fouvry pour deux autres exemples importants [F1, Ha]).

Le phénomène de parité a été analysé en grand détail par Bombieri [B] puis Friedlander-Iwaniec [FrI1] et on imagine qu'il doit constituer la seule obstruction à la détection des nombres premiers par les méthodes du crible. Les travaux de Duke-Friedlander-Iwaniec et de Friedlander-Iwaniec ont profondément modifié les règles du jeu en montrant qu'il suffit d'introduire dans la mécanique du crible une seconde hypothèse "raisonnable" et très générale (notée **Cr.**2) qui interdit tout phénomène de parité et qui permet — potentiellement — de produire des nombres premiers.

2.1. **Le crible dans les suites oscillantes**

Nous décrivons ici la première approche suivie par Duke-Friedlander-Iwaniec [DFI] et qui concerne le cas où la suite $\{\rho_n\}$ est oscillante. Ils obtiennent le résultat très général suivant :

THÉORÈME 2.3. — *Soit $\{\rho_n\}$ une suite de complexes vérifiant les propriétés suivantes*

- *pour tout $n \geq 1$, on a $|\rho_n| \leq \tau(n)^{1998}$ et pour tout $d \geq 1$ sans facteur carré on a*

$$\sum_{\substack{n\leq x\\ n\equiv 0(\mathrm{mod}\ d)}} |\rho_n| \ll \frac{\tau(d)^{1998}}{d} x.$$

- *Pour tout $0 < \delta < 1/2$ et tout $A > 0$ on a la majoration*

$$\sum_{d\leq x^\delta} |\sum_{dn\leq x} \rho_{dn}| \ll_{\delta,A} x \log^{-A} x \text{ quand } x \to +\infty. \tag{13}$$

- *Pour tout $0 < \delta' < 1/3$, tout $A > 0$ et pour toutes suites de complexes $\{\alpha_m\}, \{\beta_n\}$, telles que α_m est nul hors des nombres premiers et que $|\alpha_p| \leq 1$, $|\beta_n| \leq \omega(n)$, on a la majoration*

$$\sum_{w\leq m\leq x^{\delta'}} \alpha_m \sum_{\substack{mn\leq x,\\ (m,n)=1}} \beta_n \rho_{mn} \ll_{\delta',A} x \log^{-A} x, \text{ quand } x \to +\infty, \tag{14}$$

où on a posé $w := x^{\log\log^{-3} x}$.

Alors, quand $x \to +\infty$, on a

$$\sum_{p\leq x} \rho_p = o(\pi(x)).$$

REMARQUE 2.4. — Des trois propriétés ci-dessus, les deux dernières sont essentielles : dans (13), on reconnaît l'hypothèse **Cr.**1, où la fonction $g(d)$ introduite dans la décomposition (5) est la fonction nulle et où on demande que l'exposant de répartition soit

arbitrairement proche de $1/2$. La majoration (14) est nécessaire pour éviter le phénomène de parité, elle introduit un deuxième paramètre $\delta' < 1/3$ qu'on peut appeler "second exposant de répartition" ; celui-ci doit être arbitrairement proche de $1/3$.

Preuve. — On cherche à estimer $A(x,z)$ pour z "proche" de $x^{1/2}$. On commence par réduire la difficulté du problème en diminuant artificiellement z : étant donné $w \leq z$, (w est défini dans l'énoncé du théorème précédent, il est beaucoup plus petit que z), on a l'identité de Buchstab

$$A(x,z) = A(x,w) - \sum_{w \leq p < z} A_p(x,p).$$

Après avoir appliqué à nouveau cette égalité aux termes $A_p(x,p)$, on obtient l'égalité

$$A(x,z) = A(x,w) - \sum_{w \leq p < z} A_p(x,w) + \sum_{w \leq p < q < z} A_{pq}(x,p).$$

Enfin, on applique l'identité de Lagrange (3) aux deux premiers termes du membre de gauche pour obtenir, après l'introduction du paramètre de troncature $z < D < x^{1/2}$

$$A(x,z) = \sum_{\substack{d|P(z) \\ d<D}}^{w} \mu(d) A_d(x) + \sum_{\substack{d|P(z) \\ d \geq D}}^{w} \mu(d) A_d(x) + \sum_{w \leq p < q < z} A_{pq}(x,p), \tag{15}$$

la notation $\sum^w$ signifiant que l'on somme sur les entiers d ayant au plus un facteur premier $\geq w$. La deuxième somme de (15) comporte très peu de termes et peut être majorée trivialement. La première est une somme dans des progressions arithmétiques de module $\leq D$ et on peut appliquer (13) si $D = x^{1/2-\epsilon}$, $\epsilon > 0$ arbitrairement petit. Toute la difficulté est transférée dans la troisième somme

$$\sum_{w \leq p < q < z} A_{pq}(x,p) = \sum_{w \leq p < z} \sum_{p < q < z} \sum_{\substack{nq \leq x/p \\ p'|n \Longrightarrow p' \geq p}} \rho_{pqn}$$

qui porte sur des entiers ayant au moins deux facteurs premiers. Par des majorations triviales, on montre que la contribution des $p > y = x^{1/3-\epsilon}$ est négligeable (en effet elle porte sur des entiers ayant au plus trois facteurs premiers tous compris entre y et $z = x^{1/2-\epsilon}$, le nombre de ceux qui ont deux facteurs premiers est majoré par $x^{1-2\epsilon}$ et, pour ceux qui en ont trois, le plus petit facteur premier est compris entre $y = x^{1/3-\epsilon}$ et $x^{1/3}$ ce qui fournit à nouveau une contribution négligeable pour $\epsilon \to 0^+$). Puis par un procédé technique, on transforme la somme restante de façon à supprimer les contraintes $p < q$ et $p'|n \Longrightarrow p' > p$ et à rendre les variables p et nq indépendantes. On se ramène alors à estimer des formes bilinéaires du type (14) avec des coefficients α_p, β_m vérifiant $|\alpha_p| \leq 1$, et $|\beta_m| \leq \omega(m)$.

□

REMARQUE 2.5. — Notons que si ρ_n est multiplicative ($\rho_{mn} = \rho_m \rho_n$ pour $(m,n) = 1$), le théorème précédent ne donne rien. En effet, essentiellement, la forme bilinéaire de (14)

se factorise en un produit de deux formes linéaires $(\sum_m \alpha_m \rho_m)(\sum_n \beta_n \rho_n)$ dont on ne sait rien dire. Mais dans ce cas le problème peut souvent être traité par d'autres techniques (en particulier par la théorie analytique des fonctions L, par exemple quand $\rho_n = \chi(n)$ est un caractère de Dirichlet non trivial).

2.2. **Le crible dans les ensembles d'entiers peu denses**

On peut noter que le théorème 2.3 ne donne un résultat non trivial que si la suite $\{|\rho_p|\}$ est assez "dense" : $\sum_{p\leq x} |\rho_p| \gg \pi(x)$. Pour pouvoir cribler des ensembles peu denses (par exemple les entiers de la forme $a^2 + b^4$) Friedlander et Iwaniec [FrI3] ont développé une autre approche beaucoup plus subtile dont le point de départ est une variante de l'identité de Vaughan : pour $z < n \leq x$, et tout $y > 0$ on a

$$\Lambda(n) = \sum_{\substack{d|n \\ d\leq y}} \mu(d)\log(n/d) - \sum_{\substack{cd|n \\ d\leq y, c\leq z}} \mu(d)\Lambda(c) + \sum_{\substack{cd|n \\ d>y, c>z}} \mu(d)\Lambda(c). \tag{16}$$

On veut estimer la somme

$$\begin{aligned}\sum_{z<n\leq x} \Lambda(n)\rho_n \;=\; & -\sum_{d\leq y} \mu(d)\log d\; A_d(x) + \sum_{d\leq y} \mu(d) \sum_{\substack{n\leq x \\ n\equiv 0 (\mathrm{mod}\, d)}} \log n\; \rho_n \\ & - \sum_{\substack{d\leq y \\ c\leq z}} \mu(d)\Lambda(c) A_{cd}(x) + \sum_{\substack{d>y \\ c>z}} \mu(d)\Lambda(c) A_{dc}(x)\end{aligned}$$

où, dans la pratique, y et z sont très proches. La première des quatre sommes est traitée *via* la décomposition (5). Elle fournit, par (9), le terme principal

$$\prod_p (1 - g(p))\big(1 - \frac{1}{p}\big)^{-1} A(x)\,;$$

le terme d'erreur est majoré grâce à **Cr.1**, le module d allant jusqu'à $D' = y \leq D$.

La deuxième et la troisième sont elles aussi traitées par la décomposition (5) (après une intégration par partie dans la deuxième somme afin de tenir compte du facteur $\log n$). On obtient d'une part un "terme principal" qui est (pour la deuxième somme) de la forme

$$A(x) \sum_{d\leq y} \mu(d) g(d) \ll A(x)/\log y,$$

la majoration provenant de l'hypothèse (9) : on a donc tenu compte des oscillations de la fonction de Moebius. Les termes d'erreurs sont majorés à nouveau par (12) mais cette fois-ci (dans le troisième terme) le module $d' = cd$ varie jusqu'à yz, ce qui impose les contraintes $y, z \leq D^{1/2}$.

Dans la dernière somme (notons-la $\sum_{d>y,c>z}$), la décomposition (5) et l'hypothèse **Cr.1** ne sont d'aucun secours et c'est à ce point qu'il est nécessaire d'introduire une nouvelle hypothèse. On commence par une réduction : on considère deux nouveaux paramètres

$y < y' < x^{1/2}$, $z < z' < x^{1/2}$ tels que y' et z' soient très proches de $x^{1/2}$ (en un sens que nous ne précisons pas). Alors $\sum_{d>y,c>z}$ se décompose en trois paquets

$$\sum_{d>y,c>z} = \sum_{d>y',c>z'} + \sum_{\substack{c>z \\ y<d\leq y'}} + \sum_{\substack{z<c\leq z' \\ y'<d}} \text{ (rappelons qu'on a aussi } cd \leq x).$$

Dans le premier paquet, les variables c et d sont localisées près de $x^{1/2}$ et la somme correspondante comporte très peu de termes, on les majore "trivialement" en oubliant les compensations que peuvent apporter les variations de signe de la fonction de Moebius. Cependant il est essentiel pour mettre cette idée en œuvre de perturber[1] au début la fonction ρ_n en la multipliant par une fonction de crible majorante. On utilise, par exemple, la fonction du crible de Brun $\lambda^+_{D'}(n) := \sum_{d|n} \mu^+_{D'}(d)$ où $\mu^+_{D'}$ est supportée dans l'intervalle $[1, D']$, avec D' très petit (en particulier on prend $D' < z$, de sorte que pour $n > z$ premier $\lambda^+_{D'}(n)\rho_n = \rho_n$). Cette perturbation complique considérablement le traitement décrit précédemment, en revanche elle permet de donner une majoration non triviale pour $\sum_{d>y',c>z'}$.

Dans le deuxième paquet, la somme vaut essentiellement (modulo la perturbation)

$$\sum_{c>z} \Lambda(c) \sum_{n} \sum_{\substack{y<d\leq y' \\ cdn\leq x}} \mu(d)\rho_{cdn},$$

C'est alors qu'on fait l'hypothèse suivante, analogue de (14). Notant

$$\gamma(n, C) := \sum_{\substack{d|n \\ d\leq C}} \mu(d).$$

On suppose :

HYPOTHÈSE **Cr. 2.** — Pour tout $A > 0$, il existe $\eta > 0$ et $\alpha > 0$ tels qu'on ait la majoration

$$\sum_{m} |\sum_{\substack{n\sim N \\ mn\leq x}} \gamma(n, C)\mu(mn)\rho_{mn}| \ll_A A(x)\log^{-A} x, \tag{17}$$

uniformément pour x, C et N vérifiant

$$1 \leq C \leq x/D,\ D^{1/2-\eta} < N < x^{1/2}\log^{-\alpha} x.$$

REMARQUE 2.6. — Cette hypothèse est l'analogue de l'hypothèse (14) ; c'est une manière subtile de traduire les oscillations de la fonction $\mu(n)$ relativement à la suite ρ_n. Notons que **Cr.2** n'est vraisemblable que si l'on a $C < N$, c'est-à-dire $x/D \leq D^{1/2-\eta}$, et donc $D \geq x^{2/3+\eta}$, ceci pour assurer que les changements de signe de $\mu(n)$ ne seront pas compensés par ceux de $\gamma(n, C)$. On remarque enfin (en prenant $C = 1$) que l'exemple de

[1] suivant une idée de Bombieri [B].

Selberg $\rho_n = \frac{1+\lambda(n)}{2}$ ne vérifie pas l'hypothèse **Cr.**2 : la fonction de Moebius restreinte aux entiers ayant un nombre pair de facteurs premiers est égale à 1 ; on a ainsi évacué le phénomène de parité.

Utilisant l'hypothèse **Cr.**2 (avec $C = 1$), on montre que $\sum_{\substack{c>z \\ y<d\leq y'}} = o(A(x))$.

Le dernier paquet est traité de manière similaire, en échangeant les rôles des variables c et d : pour faire apparaître la fonction de Moebius à partir de $\Lambda(c)$ on utilise la relation (2). La décomposition (5) et les hypothèses **Cr.**1 et **Cr.**2 permettent en définitive de majorer convenablement cette dernière somme. On obtient ainsi le théorème suivant [FrI3] :

THÉORÈME 2.7. — *Soit $\{\rho_n\}$ une suite de réels positifs supportée par les entiers sans facteur carré. On suppose qu'on a une décomposition de la forme* (5), *la fonction g vérifiant* (6), *et les majorations*

$$A(x^{1/2}) \ll A(x)\log^{-2} x, \text{ et } A_d(x) \ll g(d)A(x) \text{ uniformément pour } d \leq x^{1/3}.$$

On suppose aussi que $g(d)$ vérifie (9) *et que pour $y \to +\infty$*

$$\sum_{d\leq y} \mu^2(d)g(d) = c_1 \log y + c_0 + O(\log^{-8} y),$$

pour certaines constantes c_0, c_1 avec $c_1 > 0$. On suppose enfin que pour tout x assez grand les hypothèses **Cr.**1 *et* **Cr.**2 *sont vérifiées pour un exposant de répartition $\delta > 2/3$ et $D = x^\delta$.*

Alors pour $x \to +\infty$ on a l'égalité

$$\sum_{n\leq x} \Lambda(n)\rho_n = \prod_p \big(1 - g(p)\big)\big(1 - \frac{1}{p}\big)^{-1} \times A(x) + o(A(x)). \tag{18}$$

Si ρ_n n'est pas supportée par les entiers sans facteurs carrés le théorème précédent admet une variante nécessitant des hypothèses supplémentaires techniques mais dont les principales restent **Cr.**1 et **Cr.**2.

3. ÉQUIDISTRIBUTION DES RACINES D'UNE CONGRUENCE QUADRATIQUE

Soit $f(x) = aX^2 + bX + c$ un polynôme à coefficients entiers, irréductible et de degré 2, soit $\Delta := b^2 - 4ac$ son discriminant. Notons, pour h et n des entiers ≥ 1

$$\rho_f(h;n) := \sum_{\substack{\nu(\mathrm{mod}\, n), \\ f(\nu)\equiv 0(\mathrm{mod}\, n)}} \mathrm{e}(\frac{h\nu}{n}).$$

D'après le critère d'équidistribution de Weyl, montrer le théorème 1.1 revient à montrer que pour tout $h \in \mathbb{Z} - \{0\}$ on a

$$\sum_{p \leq x} \rho_f(h;p) = o_{f,h}(\frac{x}{\log x}), \text{ pour } x \to +\infty. \tag{19}$$

On applique le théorème 2.3 à la fonction $\rho_n := \rho_f(h,n)$ et un petit miracle se produit : la vérification des hypothèses (13), (14) se ramène à un seul type de majoration sur la suite (ρ_n) qui s'énonce comme suit [To, DFI] :

PROPOSITION 3.1. — *Soit $0 < |h| \leq d \leq M$. Alors pour tout $\eta > 0$, on a la majoration*

$$\mathcal{L}_{h,d}(M) := \sum_{\substack{m \sim dM \\ m \equiv 0(d)}} \rho_f(h;m) = O_{f,\eta}\Big((\frac{d}{M})^{\frac{1}{4(\eta+1)}} M^{1+1/\eta^2}\Big).$$

Preuve. — Cette majoration est difficile et nous n'en donnons qu'un vague aperçu dans le cas où $\Delta < 0$. On rappelle d'une part que le groupe $SL_2(\mathbb{Z})$ agit par changement linéaire des variables sur l'ensemble des formes quadratiques binaires $\alpha X^2 + \beta XY + \gamma Y^2$ de discriminant Δ, et que pour $\Delta < 0$, il existe une bijection $SL_2(\mathbb{Z})$-équivariante qui va des formes positives vers le demi-plan de Poincaré $\mathcal{H}$ et qui est donnée par

$$(\alpha X^2 + \beta XY + \gamma Y^2) \to \frac{-\beta + i\sqrt{-\Delta}}{2\gamma}.$$

D'autre part, on a une correspondance (qui remonte à Gauss [GA]) entre les solutions de la congruence $f(\nu) \equiv 0 (\mathrm{mod}\, n)$ et les représentations de n par les différentes classes d'équivalence de formes quadratiques positives à coefficients entiers de discriminant Δ sous l'action de SL_2 (voir le lemme 4.4 dans la section suivante). Ces faits permettent d'exprimer la somme $\mathcal{L}_{h,d}(M)$ en termes d'une série de Poincaré $P_h(z)$ non-holomorphe, relative au sous-groupe de congruence $\Gamma_0(ad)$ et à la pointe ∞. Elle est évaluée en des points du demi-plan correspondant à certaines classes de formes quadratiques entières de discriminant Δ modulo l'action de $\Gamma_0(a)$. Il faut recourir aux méthodes profondes de la "Kloostermanie" [DI] (développement spectral, développement de Fourier de la série de Poincaré aux pointes et ultimement, majorations de sommes de sommes de Kloosterman) pour borner uniformément, suivant l'entier d, cette série. Pour plus de détails et pour le cas des discriminants positifs, nous renvoyons à [DFI, To].

□

Il est clair que cette proposition suffit pour vérifier (13). Pour vérifier la condition (14), on se ramène essentiellement à estimer des formes bilinéaires $\mathcal{B}(M,N)$ de la forme

$$\sum_{m \sim M} \alpha_m \sum_{\substack{n \sim N \\ (m,n)=1}} \beta_n \rho_f(h;mn) = \sum_{\substack{n,\ \alpha (\mathrm{mod}\, n) \\ f(\alpha) \equiv 0 (\mathrm{mod}\, n)}} \sum \beta_n \sum_{\substack{m, \\ (m,n)=1}} \alpha_m \sum_{\substack{\nu (\mathrm{mod}\, mn), \\ \nu \equiv \alpha(n), f(\nu) \equiv 0 (mn)}} e(\frac{h\nu}{mn}),$$

avec $4MN \leq x$, $w \leq M \leq x^{1/3-\epsilon}$. Par Cauchy-Schwarz on a

$$\mathcal{B}(M,N)^2 \ll N\log^4 N \times \sum_{m_1,m_2} \alpha_{m_1}\overline{\alpha}_{m_2}\mathcal{B}_{m_1,m_2}(N)$$

avec

$$\mathcal{B}_{m_1,m_2}(N) = \sum_{\substack{(n,m_1m_2)=1\\ n\sim N}} \sum\sum_{\substack{f(\nu_j)\equiv 0(nm_j)\\ \nu_1\equiv\nu_2(n)}} \mathrm{e}(h(\frac{\nu_1}{m_1n} - \frac{\nu_2}{m_2n})).$$

Les termes diagonaux $\mathcal{B}_{m_1,m_1}(N)$ sont estimés trivialement et contribuent à $\mathcal{B}(M,N)^2$ par $O(MN^2\log^8 MN)$. Pour $m_1 \neq m_2$, m_1, m_2 et n sont premiers entre eux deux à deux (m_1 et m_2 sont premiers) et on obtient

$$\mathcal{B}_{m_1,m_2}(N) = \sum_{\substack{(n,m_1m_2)=1\\ n\sim N}} \sum_{f(\nu)\equiv 0(nm_1m_2)} \mathrm{e}(\frac{h(m_2-m_1)\nu}{m_1m_2n})$$

qui est (à un terme d'erreur admissible près) la somme $\mathcal{L}_{h(m_2-m_1),m_1m_2}(N)$. On utilise alors la proposition 3.1 car $h(m_2-m_1) \leq m_1m_2 \leq x^{2/3-2\epsilon} \leq N$ et ceci permet de vérifier (14).

4. REPRÉSENTATION D'UN NOMBRE PREMIER PAR LE POLYNÔME X^2+Y^4.

Selon le théorème de Fermat, un nombre premier impair p est représenté par le polynôme X^2+Y^2 si et seulement si $p \equiv 1 (\mathrm{mod}\, 4)$, p est alors la norme d'un entier de Gauss $z = a+ib \in \mathbb{Z}[i]$ qui engendre un idéal premier de $\mathbb{Z}[i]$ et qu'on appellera nombre premier de Gauss. On peut chercher les premiers de Gauss d'une forme particulière. Dans [FoI] Fouvry et Iwaniec ont étudié les premiers de Gauss dont la partie imaginaire b fait partie d'un ensemble d'entiers $\mathcal{N}$ fixé et ils démontrent le théorème général suivant

THÉORÈME 4.1. — *Soit $\mathcal{N} \subset \mathbb{N}$ un ensemble d'entiers assez dense (au sens qu'il existe une constante $A > 0$ telle que, pour $x \to +\infty$, on ait $|\mathcal{N} \cap [1,x]| \gg x/\log^A x$). Alors, on a, pour $x \to +\infty$, l'équivalence asymptotique*

$$\sum_{p\leq x} \log p \sum_{\substack{a^2+b^2=p,\\ b\in\mathcal{N}}} 1 \simeq \prod_p (1-\frac{\chi_4(p)}{p-1}) \times \sum_{\substack{a^2+b^2\leq x\\ b\in\mathcal{N}}} \prod_{p|b} (1-\frac{\chi_4(p)}{p-1})^{-1},$$

où χ_4 est le caractère non-trivial modulo 4.

Cela signifie que les parties imaginaires des nombres premiers de Gauss sont harmonieusement réparties dans tout ensemble assez dense, en particulier prenant $\mathcal{N}$ l'ensemble des nombres premiers, on obtient le théorème 1.5. Friedlander et Iwaniec ont ensuite étendu ce résultat à l'ensemble des carrés : cet ensemble est certes très particulier mais aussi *beaucoup moins dense* ce qui rend la preuve du théorème 1.4 très difficile.

Considérant un ensemble d'entiers $\mathcal{N}$ a priori quelconque, on cherche à cribler la suite

$$\mathcal{A} := \{\rho_n := \sum_{a^2+b^2=n} \mathfrak{z}(b)\},$$

où $\mathfrak{z}$ est la fonction caractéristique de $\mathcal{N}$. Pour détecter des nombres premiers on cherche à appliquer le théorème 2.7 dont les hypothèses essentielles sont **Cr.**1 et **Cr.**2.

4.1. **Répartition des entiers de Gauss dans les progressions arithmétiques**

Dans cette section, nous expliquons comment on peut vérifier la majoration (12). Une découverte très surprenante, faite par Fouvry et Iwaniec, est que la suite (ρ_n) considérée a un exposant de répartition extrêmement élevé. On a

$$A_d(x) = \sum_{\substack{a^2+b^2\leq x \\ a^2+b^2\equiv 0 (\mathrm{mod}\, d)}} \mathfrak{z}(b),$$

et il est raisonnable d'espérer que $A_d(x)$ est bien approchée par

$$M_d(x) = \frac{1}{d} \sum_{a^2+b^2\leq x} \rho(b;d)\mathfrak{z}(b),$$

où $\rho(b;d)$ est le nombre de solutions de la congruence $\alpha^2 + b^2 \equiv 0 (\mathrm{mod}\, d)$.

THÉORÈME 4.2. — *Soit $\mathcal{N}$ un ensemble d'entiers et posons $N(x^{1/2}) = |\mathcal{N} \cap [1, x^{1/2}]|$. Alors pour tout $\epsilon > 0$ et tout $D < x$ on a la majoration*

$$\sum_{d\leq D} |A_d(x) - M_d(x)| \ll_\epsilon N(x^{1/2})^{1/2} x^{1/2+\epsilon} D^{1/4}.$$

Si $\mathcal{N}$ est l'ensemble des carrés, on a la majoration plus précise suivante : soit $g(n)$ la fonction multiplicative, supportée par les entiers sans facteur carré, définie par

$$g(p) = \frac{1}{p}\big(1 + \chi_4(p)(1 - \frac{1}{p})\big).$$

Posant alors $r_d(x) := A_d(x) - g(d)A(x)$, on a pour tout $\epsilon > 0$ et pour tout $D < x$,

$$\sum_{d\leq D} \mu^2(d)|r_d(x)| \ll_\epsilon x^{9/16+\epsilon} D^{1/4}.$$

REMARQUE 4.3. — Ce résultat signifie que si l'ensemble $\mathcal{N}$ est assez dense, pour tout $\epsilon > 0$, $1 - \epsilon$ est un exposant de répartition pour la suite (ρ_n), et si $\mathcal{N}$ est l'ensemble des carrés, l'exposant devient $3/4 - \epsilon$; ces deux valeurs sont optimales (dans le dernier cas on a $A(x) \simeq \kappa x^{3/4}$). Remarquons aussi que, pour $\mathcal{N}$ l'ensemble des carrés, la vérification de (9) pour la fonction $g(d)$ résulte facilement de l'existence de la région sans zéro "standard" de la fonction $L(\chi_4, s)$ associée au caractère de Dirichlet non-trivial d'ordre 4.

Preuve. — La preuve de cette proposition repose principalement sur une propriété d'espacement exceptionnel des fractions $\frac{\nu}{d} (\mathrm{mod}\, 1)$ où ν est racine de l'équation

$$\nu^2 + 1 \equiv 0 (\mathrm{mod}\, d). \tag{20}$$

On utilise à nouveau la correspondance entre les racines de l'équation précédente et les représentations de d par la forme quadratique $r^2 + s^2$:

LEMME 4.4. — (Gauss) *Il existe une bijection entre les racines* $\nu (\mathrm{mod}\, d)$ *de la congruence* (20) *et les représentations de* d *de la forme*

$$d = r^2 + s^2,\ (r, s) = 1,\ -s < r \leq s.$$

Elle est donnée par la congruence $\nu s \equiv r (\mathrm{mod}\, d)$. *On a*

$$\frac{\nu}{d} \equiv \frac{r}{sd} - \frac{\overline{r}}{s} (\mathrm{mod}\, 1)$$

où $\overline{r}$ *est l'inverse de* r *modulo* s.

Notons que $|r|/sd \leq 1/2s^2$, si bien que $\frac{\nu}{d}$ est proche d'un rationnel dont le dénominateur est petit ($\leq d^{1/2}$). On en déduit que les fractions $\{\frac{\nu}{d} (\mathrm{mod}\, 1),\ \nu^2 + 1 \equiv 0 (\mathrm{mod}\, d),\ 8D \leq d \leq 9D\}$, dont les r correspondants ont même signe, sont bien espacées de $1/36D$ modulo 1 : plus précisément, notant $||\ ||$ la distance à l'entier le plus proche, on a la minoration [2]

$$||\frac{\nu_1}{d_1} - \frac{\nu_2}{d_2}|| \geq 1/36D \text{ pour } \frac{\nu_1}{d_1} \not\equiv \frac{\nu_2}{d_2} (\mathrm{mod}\, 1).$$

On en déduit, par l'inégalité du grand crible :

PROPOSITION 4.5. — *Pour toute suite* (α_n) *de complexes, on a la majoration*

$$\sum_{d \leq D} \sum_{\nu^2 + 1 \equiv 0 (\mathrm{mod}\, d)} |\sum_{n \leq N} \alpha_n \mathrm{e}(\frac{\nu n}{d})|^2 \ll (D + N) \sum_{n \leq N} |\alpha_n|^2, \tag{21}$$

où la constante impliquée dans le symbole de Vinogradov est absolue.

Nous passons à la preuve du théorème 4.2. On commence par remplacer (à un terme d'erreur admissible près) la fonction caractéristique de l'intervalle $[1, x]$ par une fonction $f \in C_c^\infty(\mathbb{R})$ et on considère

$$A_d(f) := \sum_{b \leq x} \mathfrak{z}(b) \sum_{\substack{a \\ a^2 + b^2 \equiv 0 (\mathrm{mod}\, d)}} f(a^2 + b^2) = \sum_b \mathfrak{z}(b) \sum_{\substack{\alpha (\mathrm{mod}\, d) \\ \alpha^2 + b^2 \equiv 0 (\mathrm{mod}\, d)}} \sum_{a \equiv \alpha (\mathrm{mod}\, d)} f(a^2 + b^2).$$

On applique la formule de Poisson à cette expression

$$A_d(f) = \frac{1}{d} \sum_b \mathfrak{z}(b) \rho(b; d) \int_{\mathbb{R}} f(t^2 + b^2) dt + \sum_{k \in \mathbb{Z} - \{0\}} \frac{1}{d} \sum_b \mathfrak{z}(b) \rho(k, b; d) I(k, b; d),$$

[2] En général, deux rationnels distincts (mod 1) de dénominateur $\leq D$ sont au mieux espacés de $1/D^2$ modulo 1.

avec

$$\rho(k,b;d) := \sum_{\substack{\alpha(\mathrm{mod}\, d)\\ \alpha^2+b^2\equiv 0(\mathrm{mod}\, d)}} \mathrm{e}(\frac{k\alpha}{d}), \rho(b;d) := \rho(0,b;d)$$

et

$$I(k,b;d) = \int_{\mathbb{R}} f(t^2+b^2)\,\mathrm{e}(\frac{tk}{d})dt.$$

Le premier terme correspondant à la fréquence $k = 0$ fournit le terme principal et n'est autre que $M_d(f)$ alors que les fréquences $k \neq 0$ donnent des termes d'erreur. Par homogénéité $\rho(k,b;d)$ vaut essentiellement

$$\rho(kb,1;d) = \sum_{\nu^2+1\equiv 0(\mathrm{mod}\, d)} \mathrm{e}(\frac{kb\nu}{d}),$$

et ces termes peuvent être traités *via* l'inégalité de grand crible (21).

□

4.2. **Vérification de la condition Cr.2**

On suppose à présent que $\mathfrak{z}$ est la fonction caractéristique des carrés. Dans cette section, nous vérifions l'hypothèse **Cr.2** pour la suite (ρ_n) correspondante, via la proposition ci-dessous et dont la preuve occupe 80 des 100 pages que compte [FrI2] !

PROPOSITION 4.6. — *Pour tout $\epsilon > 0$, et pour tout $A > 0$ la majoration* (17) *est satisfaite uniformément pour*

$$1 \leq C \leq N^{1-\epsilon} \text{ et pour } x^{1/4+\epsilon} < N < x^{1/2}\log^{-B(A)} x,$$

où $B(A) > 0$ ne dépend que de A.

Pour simplifier, nous ne considérons que le cas $C = 1$. Il s'agit d'estimer des sommes de la forme

$$\mathcal{B}(M,N) := \sum_m f(m^{1/2})|\sum_{n\sim N,(m,n)=1} \mu(n)\rho_{mn}|, \text{ où } MN \leq 4x$$

et $f(z)$ est une certaine fonction sur $\mathbb{C}$, C^∞, radiale, à support compact contenu dans la couronne $\{z \in \mathbb{C}, |z| \in]\sqrt{M}/2, 3\sqrt{M}[\}$ et qui majore la fonction caractéristique de l'intervalle $[\sqrt{M}, \sqrt{2M}]$; en outre on peut supposer que l'on a $(n,2) = 1$ dans la somme précédente.

Ici, il est nécessaire de faire une incursion dans le domaine des entiers de Gauss $\mathbb{Z}[i]$. Notons que, d'après la condition $(m,n) = 1$, une écriture de mn comme somme de deux carrés détermine de manière presque unique (aux unités de $\mathbb{Z}[i]$ près) des écritures de m et n comme sommes de deux carrés et inversement. En d'autres termes, on a

$$\rho_{mn} = \frac{1}{16}\sum_{|w|^2=m}\sum_{\substack{|z|^2=n\\ (z\bar{z},2w\bar{w})=1}} \mathfrak{z}(\Re e\,\overline{w}z),$$

où les z, w sont dans $\mathbb{Z}[i]$ et le facteur $16 = 4^2$ provient des 4 unités de $\mathbb{Z}[i]$. Comme z est premier à 2, on peut supposer, quitte à le multiplier par une unité, qu'il désigne un entier de Gauss *primaire*, c'est-à-dire qu'il vérifie

$$z := r + is \equiv 1 (\mathrm{mod}\, 2(1+i)), \text{ et donc } r \equiv 1 (\mathrm{mod}\, 2), s \equiv r - 1 (\mathrm{mod}\, 4).$$

Avec cette normalisation, z est déterminé complètement par son idéal. On a alors

$$\mathcal{B}(M,N) = \frac{1}{4} \sum_{w} f(w) | \sideset{}{^\wedge}\sum_{\substack{|z|^2 \sim N, \\ (|z|^2, |w|^2)=1}} \mu(|z|^2) \mathfrak{z}(\Re e \overline{w} z)|,$$

avec $\beta_z := \mu(|z|^2)$ et $\sum^\wedge$ signifiant que l'on somme sur des entiers de Gauss primaires. Par découpage, on peut encore supposer que z est confiné dans un petit secteur angulaire. Quand $\beta_z := \mu(|z|^2)$ n'est pas nul, z est *primitif* au sens que $(r,s) = 1$. Par Cauchy-Schwarz, on a

$$|\mathcal{B}(M,N)|^2 \ll M \sideset{}{^\wedge}\sum_{z_1,z_2} \beta_{z_1}\beta_{z_2} \sum_{\substack{w \\ (|w|^2, |z_1 z_2|^2)=1}} f(w) \mathfrak{z}(\overline{w} z_1) \mathfrak{z}(\overline{w} z_2) := M \sideset{}{^\wedge}\sum_{z_1,z_2} \beta_{z_1}\beta_{z_2} C(z_1,z_2).$$

Par un argument technique, on peut oublier la condition $(|w|^2, |z_1 z_2|^2) = 1$ et imposer la condition $(z_1, z_2) = 1$.

On utilise maintenant le fait que $\mathfrak{z}(b)$ est la fonction caractéristique des carrés. Notant $c_1^2 = \overline{w} z_1$ et $c_2^2 = \overline{w} z_2$, on peut paramétrer l'entier de Gauss w par le couple de carrés d'entiers (c_1^2, c_2^2). On a

$$i\Delta w = c_1^2 z_2 - c_2^2 z_1, \text{ avec } \Delta := \Delta(z_1,z_2) = \Im m \overline{z}_1 z_2 = r_1 s_2 - r_2 s_1,$$

et comme w décrit tous les entiers de Gauss, l'égalité précédente s'interprète sous la forme de la congruence

$$c_1^2 z_2 - c_2^2 z_1 \equiv 0 (\mathrm{mod}\, \Delta).$$

On a donc

$$C(z_1,z_2) = \sideset{}{^\wedge}\sum\sum_{\substack{(c_1,c_2) \in \mathbb{Z}^2 \\ c_1^2 z_2 \equiv c_2^2 z_1 (\mathrm{mod}\, \Delta)}} f\left(\frac{c_1^2 z_2 - c_2^2 z_1}{|\Delta|}\right).$$

On peut alors appliquer la formule de Poisson qui transforme l'expression précédente en

$$\frac{1}{|z_1 z_2|^{1/2}} \sum_{h_1,h_2} G(h_1,h_2) F(h_1,h_2)$$

où $G(h_1,h_2)$ est une sorte de somme de Gauss bidimensionnelle

$$G(h_1,h_2) = \frac{1}{|\Delta|} \sum_{\substack{\alpha_1,\alpha_2 \in \mathbb{Z}/|\Delta|\mathbb{Z} \\ \alpha_1^2 z_2 \equiv \alpha_2^2 z_1 (\mathrm{mod}\, |\Delta|)}} \mathrm{e}\left(\frac{h_1\alpha_1 + h_2\alpha_2}{|\Delta|}\right)$$

et $F(h_1,h_2)$ est la transformée de Fourier

$$F(h_1,h_2) := \iint f(\frac{z_2}{|z_2|}t_1^2 - \frac{z_1}{|z_1|}t_2^2)\,\mathrm{e}(h_1t_1+h_2t_2)dt_1dt_2.$$

Au prix d'arguments délicats, on montre[3] que le terme principal provient des fréquences nulles $h_1 = h_2 = 0$. Alors $G(0,0)$ compte le nombre de solutions de la congruence $\alpha_1^2 z_2 \equiv \alpha_2^2 z_1 (\mathrm{mod}\,|\Delta|)$ donc, par homogénéité, se ramène à la congruence $\alpha^2 \equiv z_1/z_2 (\mathrm{mod}\,|\Delta|)$ dans $\mathbb{Z}/\Delta\mathbb{Z}$ (cette congruence a un sens, car z_1/z_2 est congru modulo Δ à un rationnel dont le dénominateur est premier à Δ). On montre alors que $C(z_1,z_2)$ peut être remplacé par

$$C_{0,0}(z_1,z_2) = 2\hat{f}(0)N^{-1/2} \sum_{\substack{d|\Delta \\ d \text{ impair}}} \frac{\phi(d)}{d}\left(\frac{z_1/z_2}{d}\right)\log 2|\frac{z_1z_2}{\Delta}|,$$

où $\left(\frac{z_1/z_2}{d}\right)$ est le symbole de Jacobi qui a donc un sens. Pour simplifier la suite de l'exposé, on oubliera le facteur $\log 2|\frac{z_1z_2}{\Delta}|$ et on est alors essentiellement ramené à savoir majorer des sommes de la forme

$$B(D,N) := \sum_{\substack{d \text{ impair} \\ d\sim D}} \sum\sum\nolimits^{\wedge}_{\substack{(z_1,z_2)=1 \\ \Delta(z_1,z_2)\equiv 0(\mathrm{mod}\,d)}} \beta_{z_1}\beta_{z_2}\left(\frac{z_1/z_2}{d}\right), \tag{22}$$

où les entiers $z_i = r_i + is_i$ sont primitifs, primaires, confinés dans un secteur angulaire et vérifient $|z_i|^2 \sim N$. Notons que D peut prendre de très grandes valeurs ($D \ll N$) si bien qu'on doit analyser une somme dans des progressions arithmétiques de très grand module (D n'a rien à voir avec la variable D de la condition **Cr.**1). On découpe la somme précédente en trois parties suivant que

$$D \le X, \tag{23}$$

$$X < D \le |\Delta|/X, \tag{24}$$

$$D > |\Delta|/X, \tag{25}$$

avec $X = \log^{1998} N$: ce découpage est réminiscent de la preuve "moderne" du théorème de Bombieri-Vinogradov [BFI] et aussi de la méthode inventée par Dirichlet pour le problème des diviseurs. Chacune de ces trois parties nécessite une méthode très spécifique.

4.3. **Le cas des plus petits modules**

On considère la zone (23). Par une astuce technique, on peut à nouveau oublier la condition $(z_1,z_2) = 1$ dans la définition de $B(D,N)$. On a alors

$$B(D,N) \simeq \sum_d \sum_{\omega(\mathrm{mod}\,4d)} \left(\frac{\omega}{d}\right) \sum\sum\nolimits^{\wedge}_{z_1\equiv\omega z_2(4d)} \beta_{z_1}\overline{\beta}_{z_2}$$

[3] au moins en moyenne sur z_1, z_2.

$$= \frac{1}{\Phi(d)} \sum_{\chi} \mathcal{I}(\chi) | \sum_{z} \mu(|z|^2)\chi(z)|^2$$

où χ parcourt les caractères de $(\mathbb{Z}[i]/4d\mathbb{Z}[i])^\times$, $\Phi(d) := |(\mathbb{Z}[i]/4d\mathbb{Z}[i])^\times|$ et

$$\mathcal{I}(\chi) = \sum_{\omega \in \mathbb{Z}/4d\mathbb{Z}} \left(\frac{\omega}{d}\right) \chi(\omega)$$

est une somme incomplète. Dans la somme $\sum_z^\wedge \mu(|z|^2)\chi(z)$ on détecte la condition que z est confiné dans un secteur angulaire par un développement en série de Fourier, ce qui produit des sommes de la forme

$$\mathcal{S}_{\chi,k} := \sum_{|z|^2 \sim N}^\wedge \mu(|z|^2)\chi(z)(\frac{z}{|z|})^k,$$

avec $k \in \mathbb{Z}$, $|k| \leq \exp(\sqrt{\log N})$. Rappelons que la somme porte sur des entiers de Gauss primaires et que $\chi(z)(\frac{z}{|z|})^k$ définit donc un caractère de Hecke ψ sur les idéaux de $\mathbb{Z}[i]$ par $\psi(z\mathbb{Z}[i]) = \chi(z)(\frac{z}{|z|})^k$. La somme $\mathcal{S}_{\chi,k}$ est une somme partielle sur les coefficients de l'inverse de la série L du caractère de Hecke

$$L(\psi, s) = \sum_{\mathfrak{a}} \psi(\mathfrak{a})N(\mathfrak{a})^{-s} = \prod_{\mathfrak{p}} (1 - \psi(\mathfrak{p})N(\mathfrak{p})^{-s})^{-1}.$$

La majoration cherchée pour $\mathcal{S}_{\chi,k}$ résulte de l'existence de régions sans zéros pour les fonctions $L(\psi, s)$. Elle est obtenue en adaptant la théorie analytique classique des fonctions L des caractères de Dirichlet ; en particulier, quand ψ est réel, on a recours à un analogue du théorème de Siegel. On obtient la majoration[4] : pour tout $A, B > 0$,

$$\mathcal{S}_{\chi,k} \ll_{A,B} N \log^{-A} N,$$

uniformément pour $d \leq \log^B N$ et $k \leq \exp(\sqrt{\log N})$. Ainsi on a exploité une première fois les oscillations de la fonction de Moebius.

4.4. **Le cas des modules intermédiaires**

Dans la zone (24), la théorie des fonctions L des caractères de Hecke est incapable de contrôler les oscillations de $\mu(|z|^2)\chi(z)$ et même l'hypothèse de Riemann généralisée ne permettrait de les contrôler correctement que pour $d \leq N^{1/2}/\log^{-B} N$. Pour éviter toute hypothèse et suivant une technique réminiscente du grand crible, on exploite la moyenne sur les modules d ; on repasse en "coordonnés cartésiennes" en écrivant $z_i = r_i + is_i$ et la somme $B(D, N)$ se ramène essentiellement à des sommes de la forme

$$B(D, R, S) = \sum_{d \sim D} \sum_{r_i \sim R} \sum_{\substack{s_i \sim S \\ r_1 s_2 \equiv r_2 s_1 (d)}} \beta_{r_1+is_1} \overline{\beta}_{r_2+is_2} \left(\frac{r_1 r_2}{d}\right) \tag{26}$$

[4]non effective si ψ est réel

$$= \sum_{d\sim D} \sum_{a(\mathrm{mod}\, d)} |\sum_{\substack{r\sim R, s\sim S \\ r\equiv as(d)}} \sum \beta_{r,s}\left(\frac{r}{d}\right)|^2,$$

avec $R, S \leq N^{1/2}$.

À ce niveau, la définition des coefficients $\beta_{r+is} := \beta_{r,s}$ n'a pas d'importance car les compensations proviendront des oscillations du symbole de Jacobi $\left(\frac{r}{d}\right)$. On va obtenir[5] des majorations, valables pour toute famille de complexes $\{\beta_{r,s}\}$, de la forme

$$\sum_{d\sim D} \sum_{a(\mathrm{mod}\, d)} |\sum_{\substack{r\sim R, s\sim S \\ r\equiv as(d)}} \sum \beta_{r,s}\left(\frac{r}{d}\right)|^2 \leq \Delta(R,S,D) \sum_{r,s} |\beta_{r,s}|^2,$$

où $\Delta(D,R,S)$ ne dépend que de D, R, S. Remarquons d'abord que la somme $B(D,R,S)$ est essentiellement symétrique en R et S (quitte à modifier les coefficients $\beta_{r,s}$). En effet par la congruence $r \equiv as(d)$ on a $\beta_{r,s}\left(\frac{r}{d}\right) = \beta_{r,s}\left(\frac{a}{d}\right)\left(\frac{s}{d}\right) := \beta'_{s,r}\left(\frac{s}{d}\right)$. On obtient la majoration recherchée en interprétant $\Delta(D,R,S)$ comme un majorant du carré de la norme de l'opérateur hilbertien qui aux familles de complexes $(\beta_{r,s})_{\substack{r\sim R \\ s\sim S}}$ associe la famille $(\alpha_{d,a})_{\substack{d\sim D \\ a(\mathrm{mod}\, d)}}$ définie par

$$\alpha_{d,a} := \sum_{\substack{r\sim R, s\sim S \\ r\equiv as(d)}} \sum \beta_{r,s}\left(\frac{r}{d}\right).$$

Par dualité, il suffit de montrer pour toute famille $(\alpha_{d,a})_{\substack{d\sim D \\ a(\mathrm{mod}\, d)}}$ la majoration

$$\sum_{r\sim R, s\sim S} \sum |\sum_{\substack{d, a(d) \\ r\equiv as(d)}} \sum \alpha_{d,a}\left(\frac{r}{d}\right)|^2 \leq \Delta(R,S,D) \sum_{d,a} |\alpha_{d,a}|^2.$$

Elle s'obtient en ouvrant le carré, en intervertissant les sommations et en majorant (par Polya-Vinogradov) la somme incomplète de caractères $\sum_r \left(\frac{r}{d_1 d_2}\right)$, et enfin en exploitant la symétrie entre les variables r et s. On obtient une borne $\Delta(D,R,S)$ qui est admissible pour notre problème dès que $X < D \leq (RS)^{1/2-\epsilon}$.

L'interversion du module. Pour traiter le cas des grands modules $D \geq (RS)^{1/2+\epsilon}$, on interprète la condition de congruence de (22), $r_1 s_2 \equiv r_2 s_1(d)$, en termes du diviseur complémentaire (cette astuce a été utilisée dans d'autres contextes par Hooley et Fouvry [Ho2, F2] par exemple). On a

$$|\Delta| = |r_1 s_2 - r_2 s_1| = dd' \Longrightarrow r_1 s_2 \equiv r_2 s_1(d'), \tag{27}$$

[5]suivant la philosophie du grand crible.

si bien que pour d' on a $X \leq d' \leq (RS)^{1/2-\epsilon}$, et le symbole de Jacobi devient essentiellement

$$\left(\frac{r_1 r_2}{d}\right) = \left(\frac{r_1 r_2}{|\Delta| d'}\right) = \left(\frac{r_1 r_2}{d'}\right)\left(\frac{r_1 r_2}{|\Delta|}\right).$$

On utilise alors le lemme suivant dont la démonstration repose principalement sur la loi de réciprocité quadratique :

LEMME 4.7. — *Soient z_1, z_2 primaires, primitifs, premiers entre eux et vérifiant $r_1 r_2 > 0$. Alors on a l'égalité*

$$\left(\frac{z_1/z_2}{\Delta}\right) = [z_1][z_2], \text{ avec } [z_1] := i^{\frac{r-1}{2}}\left(\frac{s_1}{|r_1|}\right).$$

Ce lemme transforme les sommes $B(D, R, S)$ en sommes de la forme $B'(D', R, S)$ avec $X < D' \leq N^{1/2}/X$ et

$$B'(D', R, S) := \sum_{d \sim D} \sum_{a (\mathrm{mod}\, d)} \Big|\sum_{\substack{r \sim R, s \sim S \\ r \equiv as(d)}} \beta_{r,s}[r + is]\Big(\frac{r}{d}\Big)\Big|^2.$$

Posant $\beta'_{r,s} = [r + is]\beta_{r,s}$, on est ramené au cas précédent. On dispose donc d'une majoration convenable des sommes $B(D, R, S)$ pour $D \in [X, (RS)^{1/2-\epsilon}] \cup [(RS)^{1/2+\epsilon}, RS/X]$. Reste à traiter la zone intermédiaire $D \in [(RS)^{1/2-\epsilon}, (RS)^{1/2+\epsilon}]$.

Agrandissement du module. Dans cette zone, on agrandit artificiellement le module d grâce à la remarque triviale que si p est premier $p \nmid r$, on a $\left(\frac{r}{d}\right) = \left(\frac{r}{dp^2}\right)$. Cela permet de majorer la somme $B(D, R, S)$ en termes de sommes $B(DP^2, R, S)$, si bien qu'en choisissant P assez grand pour que $DP^2 \geq (RS)^{1/2+\epsilon}$, on peut appliquer la méthode précédemment décrite.

4.5. **Les très grands modules**

La zone restante correspond aux grands modules (25) : on change le diviseur d en son complémentaire $\Delta/d := d' \leq X$ de la manière expliquée en 4.4 (27) et par les arguments décrits dans la partie 4.3, on se ramène à majorer des sommes de la forme (*cf.* 4.3 pour les notations)

$$\tilde{\mathcal{S}}_{\chi,k} := \sum_{|z|^2 \sim N}^{\wedge} \mu(|z|^2)\chi(z)\Big(\frac{z}{|z|}\Big)^k[z] := \sum_{n \sim N} \mu(n)\tilde{\lambda}_{\chi,k}(n)$$

où χ est un caractère de $(\mathbb{Z}[i]/4d'\mathbb{Z}[i])^\times$ et où

$$\tilde{\lambda}_{\chi,k}(n) = \sum_{z, |z|^2 = n}^{\wedge} \chi(z)\Big(\frac{z}{|z|}\Big)^k[z].$$

Cette fois, la torsion supplémentaire par le symbole (dit de Jacobi-Kubota) $[z]$ interdit l'emploi des méthodes de fonctions L de 4.3 : en effet la fonction $\tilde{\lambda}_{\chi,k}(n)$ n'est plus multiplicative et sa fonction L associée n'a pas de produit eulérien. En fait le symbole $[z]$ est

"presque" multiplicatif. On a le lemme suivant dont la preuve repose à nouveau sur la loi de réciprocité quadratique :

LEMME 4.8. — *Soient z, w primaires et primitifs. Alors*

$$[zw] = \epsilon(z,w)[w][z]\left(\frac{z}{w}\right), \text{ avec } \epsilon(z,w) = \pm 1 \text{ et } \left(\frac{z}{w}\right) = \left(\frac{\Re ezw}{|w|^2}\right).$$

En outre, le signe de $\epsilon(z,w)$ dépend des positions relatives de z, w, zw dans l'un des quatre quadrants du plan complexe. Le symbole $\left(\frac{z}{w}\right) = \left(\frac{\Re ezw}{|w|^2}\right)$ est appelé symbole de Dirichlet et est bien défini pour w primaire et primitif.

REMARQUE 4.9. — Le symbole de Dirichlet $\left(\frac{z}{w}\right)$ peut être vu en termes du symbole de Jacobi (sur les entiers "naturels") de module $q = |w|^2$. Si $z = r + is$ et $\omega \in \mathbb{Z}$ est solution de $\omega^2 + 1 \equiv 0 (\mathrm{mod}\, q)$, alors on a

$$\left(\frac{z}{w}\right) = \left(\frac{r+\omega s}{q}\right).$$

Dans le traitement de $\tilde{\mathcal{S}}_{\chi,k}$, c'est précisément la non-multiplicativité de $[z]$ que l'on va exploiter. En effet, il existe pour la fonction $\mu(n)$ une identité combinatoire qui est l'analogue de l'identité (16) pour la fonction $\Lambda(n)$, elle ramène[6] l'estimation de $\tilde{\mathcal{S}}_{\chi,k}$ à celle de formes linéaires

$$\mathcal{L}_w(V) = \sum_{z,|z|^2\sim V}^{\wedge} \chi(z)(\frac{z}{|z|})^k [zw]$$

(avec w primaire et primitif), ou de formes bilinéaires

$$\mathcal{B}(U,V) = \sum_{w,|w|^2\sim U}^{\wedge} \sum_{z,|z|^2\sim V}^{\wedge} \alpha_w \beta_z \chi(wz) \left(\frac{wz}{|wz|}\right)^k [zw], \text{ avec } |\alpha_w|, |\beta_z| \leq 1.$$

Par le lemme précédent et la remarque qui le suit, la première somme vaut essentiellement

$$\sum_{z=r+is,|z|^2\sim V}^{\wedge} \chi(z)(\frac{z}{|z|})^k \left(\frac{s}{|r|}\right)\left(\frac{r+\omega s}{q}\right),$$

et la seconde prend la forme

$$\sum_{w,|w|^2\sim U}^{\wedge} \sum_{z,|z|^2\sim V}^{\wedge} \alpha'_w \beta'_z \left(\frac{z}{w}\right).$$

L'estimation de ces deux sommes est assez délicate et se ramène *via* la remarque 4.9 à des majorations de sommes incomplètes en des symboles de Jacobi (dans $\mathbb{Z}$). On obtient en définitive la majoration

$$\tilde{\mathcal{S}}_{\chi,k} \ll_{A,B} N^{1-\eta},$$

pour un certain $\eta > 0$ absolu, et ce uniformément pour $d, |k| \leq N^\eta$. Cette majoration est suffisante pour conclure la preuve de la proposition 4.6.

[6] comme dans la preuve du théorème 2.3.

REMARQUE 4.10. — Comme on le constate en comparant les hypothèses du théorème 2.7 avec les majorations obtenues dans les propositions 4.2 et 4.6, les conditions **Cr.1** et **Cr.2** sont satisfaites et de loin ! Par exemple, on obtient un exposant de répartition proche de 3/4 alors que 2/3 est suffisant. Il reste donc de la place pour d'autres applications. En allant dans le sens d'une difficulté croissante, l'étape suivante consisterait à étudier la représentabilité des nombres premiers par le polynôme $X^2 + Y^6 = X^2 + (Y^3)^2$, en prenant pour $\mathfrak{z}$ la fonction caractéristique des cubes. L'exposant de répartition de la suite (ρ_n) est alors arbitrairement proche mais inférieur à 2/3 (et c'est optimal !) ce qui est juste en dessous du seuil requis par le théorème 2.7 (l'hypothèse **Cr.**1) pour détecter des nombres premiers. Des arguments combinatoires encore plus élaborés permettront peut-être de diminuer ce seuil, quitte éventuellement à abandonner l'équivalent (18) pour une minoration. Pour ce qui est de l'hypothèse **Cr.**2, les arguments devraient pouvoir s'adapter, la détection des cubes se faisant cette fois-ci *via* le symbole cubique et en utilisant la loi de réciprocité correspondante. Ceci laisse un bon espoir de traiter le cas du polynôme $X^2 + Y^6$ qui n'est pas très éloigné[7] du polynôme $4(Y^2)^3 + 27X^2$ lequel est le discriminant d'une courbe elliptique. La représentabilité d'une infinité de nombres premiers par ce dernier montrerait alors l'existence d'une infinité de courbes elliptiques sur $\mathbb{Q}$ avec une seule place de mauvaise réduction (de type multiplicative).

BIBLIOGRAPHIE

[B] E. BOMBIERI – *The asymptotic sieve*, Mem. Acad. Naz. dei XL, 1/2, (1976), 243-269.

[BFI] E. BOMBIERI, J.B. FRIEDLANDER et H. IWANIEC – *Primes in arithmetic progressions to large moduli,* Acta Math. **156** (1986), 203-251.

[Br] V. BRUN – *La série* $1/5 + 1/7 + 1/11 + 1/13 + 1/17 + 1/19 + \ldots$ *où les dénominateurs sont des nombres premiers "jumeaux" est convergente ou finie*, Bull. Sci. Math **43**, 100-104, 124-128.

[C] J.R. CHEN – *On the representation of a large even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica **16** (1973), 157-176.

[D] J.-M. DESHOUILLERS – *Progrès récents des petits cribles arithmétiques (d'après Chen, Iwaniec,...)*, Séminaire Bourbaki, Vol. 1977/78, Exposé n° 520, Lect. Notes in Math. **710** (1979), 248-262.

[DI] J.-M. DESHOUILLERS et H. IWANIEC – *Kloosterman Sums and Fourier Coefficients of Cusp Forms*, Invent. Math. 70 (1982), 219-288.

[DFI] W. DUKE, J.B. FRIEDLANDER and H. IWANIEC – *Equidistribution of roots of quadratic congruences of prime moduli*, Annals of Math. **141** (1995), 423-441.

[7] il suffit de travailler dans $\mathbb{Z}[j]$, au lieu de $\mathbb{Z}[i]$.

[E] N. ELKIES – *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbb{Q}$, Invent. Math. **89** (1987), 561-567.

[FoI] E. FOUVRY and H. IWANIEC – *Gaussian Primes*, Acta. Arith., LXXIX.3 (1997), 249-287 (volume en l'honneur de J.W. Cassels).

[F1] E. FOUVRY – *Théorème de Brun-Titchmarsh ; application au théorème de Fermat,* Invent. Math. **79** (1985), 383-407.

[F2] E. FOUVRY – *Sur le problème des diviseurs de Titchmarsh,* J. Reine Angew. Math. **357** (1985), 51-76.

[FrI1] J.B. FRIEDLANDER and H. IWANIEC – *Bombieri's sieve*, in Analytic Number Theory, Proc. Halberstam conf., Allerton Park Illinois 1995, ed. Berndt et al., p. 411-430, Birkauser (Boston), 1996.

[FrI2] J.B. FRIEDLANDER and H. IWANIEC – *The polynomial* $X^2 + Y^4$ *captures its primes*, Annals of Math. (à paraître).

[FrI3] J.B. FRIEDLANDER and H. IWANIEC – *Asymptotic sieve for primes*, Annals of Math. (à paraître).

[GA] C. F. GAUSS – *Disquisitiones arithmeticae*, Traduction anglaise, Springer-Verlag (1986).

[HR] H. HALBERSTAM ans H.-E. RICHERT – Sieve methods, London Math. Soc. Monographs. 4. London-New York-San Francisco: Academic Press XIII (1974).

[HB-P] D.R. HEATH-BROWN and S.J. PATTERSON – *The distribution of Kummer Gauss sums at prime arguments*, J. Reine Angew. Math. **310** (1979), 111-130.

[Ha] G. HARMAN – *On the distribution of* αp *modulo one,* J. Lond. Math. Soc., II. Ser. 27 (1983), 9-18.

[Ho1] C. HOOLEY – *On the distribution of the roots of polynomial congruences,* Mathematika **11** (1964), 39-49.

[Ho2] C. HOOLEY – *On the Barban-Davenport-Halberstam Theorem I,* J. Reine Angew. Math. **274-275** (1975), 206-223.

[I1] H. IWANIEC – *Primes of the type* $\phi(x, y) + A$*, where* ϕ *is a quadratic form*, Acta Arith. XXI, **203-234** (1972).

[I2] H. IWANIEC – *Almost primes represented by a quadratic polynomial*, Inv. Math. **47** (1978), 171-188.

[I3] H. IWANIEC – *A new form of the error term in the linear sieve*, Acta Arith. XXXVII (1980), 307-320.

[IJ] H. IWANIEC and M. JUTILA – *Primes in short intervals*, Ark. Math. **17** (1980), 307-320.

[K] N.M. KATZ – *Exponential sums over finite fields and Differential equations over the complex numbers : some interactions,* Bull. Am. Math. Soc., Vol 23 nb. 2.

[S] A. SELBERG – On elementary methods in prime number theory and their limitations, Collected Works Vol I, p. 388-397, Springer (Berlin) 1989.

[To] A. TOTH – PhD. Thesis, Rutgers University (1996).

Philippe MICHEL

Université Paris-Sud
Département de Mathématiques
F-91405 ORSAY Cedex
E-mail : michel@math.u-psud.fr