Le grand crible dans la théorie analytique des nombres

Enrico Bombieri

1974

Astérisque, tome 18 (1974)

Introduction

Les notes qui suivent développent un cours donné en Mai 1973 au Collège de France sur "le grand crible".

La méthode du grand crible est, à l'heure actuelle, l'un des outils les plus puissants en théorie multiplicative des nombres. Grosso modo, on peut la définir comme l'analyse harmonique des progressions arithmétiques, aussi bien du point de vue additif que multiplicatif. Un rôle fondamental y est joué par deux inégalités (cf. th. 4, cor. 2 et th. 7, 8, 7A) que l'on peut interpréter comme des variantes de l'inégalité de Bessel pour des systèmes "presque" orthogonal de fonctions.

Les applications à la théorie des nombres prennent deux formes :

La première, et la plus élémentaire, est la forme additive, étudiée aux §§ 2, 3, qui conduit directement aux résultats arithmétiques typiques du crible de Selberg. On trouvera au §§ 0, 1 la définition d'un crible, et le théorème de Linnik sur le plus petit non-reste quadratique mod. p ; nous avons donné aussi la formulation de Rényi du grand crible.

La seconde forme du grand crible est multiplicative ; elle concerne l'analyse harmonique relativement aux caractères $\chi(n)$ de Dirichlet ; c'est l'objet des §§ 4, 5.

La suite de ces notes est consacrée aux applications de la forme multiplicative du grand crible. Au § 6, nous démontrons un théorème de densité pour les zéros des fonctions L, et nous en déduisons le théorème de Linnik sur le plus petit nombre premier appartenant à une progression arithmétique. Une variante du théorème de densité, utilisable dans l'étude des nombres premiers appartenant à de petits intervalles, est discutée au § 10.

Le § 7 contient une démonstration simplifiée du théorème de Bombieri-Vinogradov sur la distribution des nombres premiers dans les progressions arithmétiques. Les §§ 8, 9 appliquent ce résultat au théorème de Rényi sur l'équation $p+2 = p_1 \cdots p_r$, avec $p, p_1, \ldots, p_r$ premiers ; nous donnons une démonstration simple du fait que cette équation est résoluble avec $r \leq 4$.

Le § 11 contient des remarques bibliographiques relatives aux différentes sections.

En résumé, ces notes contiennent quelques-unes des applications les plus importantes de la méthode du grand crible : théorèmes de densité, distribution des nombres premiers dans les progressions arithmétiques, lien avec le petit crible de Brun-Selberg, etc. Toutefois, l'exposé n'a rien de

systématique ; je me suis borné à donner des échantillons des diverses façons dont on peut appliquer la méthode ; bien souvent aussi, pour simplifier les démonstrations, je n'ai pas donné les énoncés les plus forts possibles.

§ 0. Préliminaires

Soient :

(a) un ensemble $\mathcal{N}$ d'entiers,

(b) un ensemble $\mathcal{P}$ de nombres premiers,

(c) pour tout $p \in \mathcal{P}$, un ensemble Ω_p de classes mod p.

Un crible est par définition la donnée de $(\mathcal{N}, \mathcal{P}, \Omega_p)$ et l'on s'intéresse à l'ensemble criblé

$$\mathcal{N}_0 = \{n \in \mathcal{N} \mid n \pmod p \notin \Omega_p \text{ pour tout } p \in \mathcal{P}\}.$$

On remarque que, dans la pratique, on prend

$\mathcal{N} = \{M < n \leq M + N\}$ un intervalle de longueur N, ou

$\mathcal{N} = \{p \leq N\}$ l'ensemble des nombres premiers $\leq N$, ou

$\mathcal{N} = \{f(n) \leq N\}$ où f est un polynôme.

Plaçons-nous dans le premier cas, et posons $\omega(p) = |\Omega_p|$, nombre d'éléments de Ω_p. Le problème fondamental est d'obtenir des majorations et des minorations pour $|\mathcal{N}_0|$ en fonction de N, $\mathcal{P}$ et des $\omega(p)$. L'ensemble criblé $\mathcal{N}_0$ est très sensible au choix des éléments de Ω_p, comme on le voit dans les exemples suivants :

$$\text{(I)} \quad \begin{cases} \mathcal{N} = (1, N) \\ \mathcal{P} = (p \leq N) \\ \Omega_p = \{0\} \end{cases} \qquad \text{(II)} \quad \begin{cases} \mathcal{N} = (1, N) \\ \mathcal{P} = (p \leq N) \\ \Omega_p = \begin{cases} \{0\} & \text{si } p \leq N/2 \\ \{1\} & \text{si } N/2 < p \leq N \end{cases} \end{cases}$$

Dans (I), $\mathcal{N}_0$ est l'ensemble des entiers $\leq N$ qui ne sont divisibles par aucun nombre premier $\leq N$, et l'on a donc $|\mathcal{N}_0| = 1$.

Dans (II), $\mathcal{N}_0$ contient tous les nombres premiers p tels que $N/2 < p \leq N$, donc

$$|\mathcal{N}_0| \sim \frac{N}{2 \log N}.$$

On a $\omega(p) = 1$ dans les deux cas ; ceci montre que l'on ne doit pas s'attendre à des résultats asymptotiques sur $|\mathcal{N}_0|$ dans le cas le plus général.

Toutefois, pour des choix particuliers des Ω_p conduisant à des ensembles criblés de signification arithmétique simple, on conjecture qu'il existe une formule asymptotique pour $|\mathcal{N}_0|$.

Un exemple est le crible

$$\begin{cases} \mathcal{N} = (1, N) \\ \mathcal{P} = (p \leq \sqrt{N}) \\ \Omega_p = \mathcal{E} \pmod p \end{cases}$$

où $\mathcal{E}$ est un ensemble d'entiers fini fixé. La suite criblée $\mathcal{N}_0$ correspondante est essentiellement l'ensemble des entiers n tels que $\sqrt{N} < n \leq N$ et que $n - e$ soit premier pour tout $e \in \mathcal{E}$.

Démontrer une formule asymptotique pour $|\mathcal{N}_0|$ est d'habitude un problème très difficile, souvent même inabordable. L'importance de la méthode du crible est que, même si elle n'arrive presque jamais à résoudre complètement le problème en question, elle fournit le plus souvent des inégalités non triviales pour $|\mathcal{N}_0|$.

§ 1. Quelques exemples. Le crible de Linnik et Rényi

On va considérer trois exemples.

Exemples 1

- ***Exemple 1.*** *Le crible d'Eratosthène :*

$$\begin{cases} \mathcal{N} = (1, N) \\ \mathcal{P} = (p \leq \sqrt{N}) \\ \Omega_p = \{0\} \end{cases}$$

Il est évident que $\mathcal{N}_0 = \{1\} \cup \{$*nombres premiers* p *tels que* $\sqrt{N} < p \leq N\}$.

- ***Exemple 2.***

$$\begin{cases} \mathcal{N} = (1, N) \\ \mathcal{P} = (p \leq \sqrt{N}) \\ \Omega_p = \{0, 2\} \end{cases}$$

On voit aisément que $\mathcal{N}_0$ *décrit l'ensemble des nombres premiers jumeaux dans* $(\sqrt{N}, N)$.

- ***Exemple 3.***

$$\begin{cases} \mathcal{N} = (1, N) \\ \mathcal{P} = (p \leq \sqrt{N}) \\ \Omega_p = \{a \mid a \text{ } n'est \text{ } pas \text{ } résidu \text{ } quadratique \text{ } mod \text{ } p\} \end{cases}$$

Il est clair que $\mathcal{N}_0 \supseteq \{$*carrés* $\leq N\}$ *(est-il vrai qu'on a égalité si* N *est assez grand ?).*

Les estimations du crible donnent, dans les trois cas :

$$|\mathcal{N}_0| \ll \frac{N}{\log N}, \qquad |\mathcal{N}_0| \ll \frac{N}{(\log N)^2}, \qquad |\mathcal{N}_0| \ll \sqrt{N}.$$

On fait usage de la notation de Vinogradov $\ll_{a,b,\ldots}$ pour indiquer une inégalité avec un facteur constant non spécifié, qui dépend seulement des paramètres $a, b, \ldots$.

Les exemples 1 et 2 sont typiques du *petit crible* : $\omega(p)$ est borné, et l'exemple 3 est typique du *grand crible* : $\omega(p)$ croît comme p (on a $\omega(p) = \frac{p-1}{2}$ si $p > 2$).

La méthode de Viggo Brun ou de Selberg s'applique bien au petit crible. Le premier résultat sur le grand crible est dû à Linnik (1941) :

Théorème 1 (Linnik) *Soit $\mathcal{N} = (1, N)$, $\mathcal{P} = (p \leq \sqrt{N})$. Alors pour tout τ, $0 < \tau < 1$, on a*

$$|\mathcal{N}_0| \leq \frac{c_0 N}{\tau^2 \, \#\{p \in \mathcal{P} \mid \omega(p) > \tau p\}}.$$

On ne démontrera pas ici ce théorème, car on obtiendra plus loin des résultats beaucoup plus forts.

On conjecture que le plus petit non-résidu quadratique mod p est $\ll_\epsilon p^\epsilon$ pour tout p, et il est même $\ll (\log p)^2$ si l'hypothèse de Riemann pour les fonctions $L(s, \chi)$, $\chi \pmod p$, est vraie. On sait aussi qu'il est $\ll_\epsilon p^{\frac{1}{4\sqrt{e}}+\epsilon}$ pour tout p ; la démonstration (due à Burgess) utilise l'hypothèse de Riemann pour les courbes hyperelliptiques sur $\mathbb{F}_p$.

On a l'application suivante (due aussi à Linnik) du Théorème 1 :

Théorème 2 *Le nombre des nombres premiers $p \leq N$ tels que le plus petit non-résidu quadratique mod p soit $> N^\epsilon$ est borné par une constante $c(\epsilon)$.*

Corollaire 1 *Pour tout $\epsilon > 0$, le nombre des $p \leq x$ tels que le plus petit non-résidu quadratique mod p soit $> p^\epsilon$ est majoré par $\ll \log \log x$.*

Le corollaire montre que les exceptions à la conjecture sont très rares.

[Preuve du Théorème 2] Considérons le crible

$$\begin{cases} \mathcal{N} = (1, N) \\ \mathcal{P} = \{p \leq \sqrt{N} \mid \text{tout } b \leq N^\epsilon \text{ est résidu quadratique mod } p\} \\ \Omega_p = \{\text{non-résidus quadratiques mod } p\} \end{cases}$$

On a $\omega(p) = \frac{p-1}{2}$ $(p > 2)$. Soit maintenant $n \leq N$, tel que tout facteur premier q de n satisfasse à $q \leq N^\epsilon$. Il est clair que, si $p \in \mathcal{P}$, alors n est résidu quadratique mod p, car tout diviseur premier q de n l'est. On a donc $n \in \mathcal{N}_0$, autrement dit $\mathcal{N}_0 \supseteq \mathcal{N}1$ où

$$\mathcal{N}_1 = \{n \leq N \mid \text{tout diviseur premier } q \text{ de } n \text{ satisfait à } q \leq N^\epsilon\}.$$

Lemme 1 *Il existe une fonction $\delta(\epsilon) > 0$ telle que*

$$|\mathcal{N}_1| \sim \delta(\epsilon) N.$$

Le Théorème 2 est une conséquence immédiate du lemme, car le Théorème 1 (avec $\tau = 1/3$) donne

$$\delta(\epsilon) N \sim |\mathcal{N}_1| \leq |\mathcal{N}_0| \ll \frac{N}{|\mathcal{P}|},$$

c'est-à-dire $|\mathcal{P}| \ll \delta(\epsilon)^{-1}$. Q.E.D.

[Preuve du Lemme] Soit $R(N, z)$ le nombre des entiers $n \leq N$ dont tous les facteurs premiers soient $\leq z$. Si $p' < p$ sont deux nombres premiers consécutifs, on a

$$R(N, p) = \sum_{r=0}^{\infty} R\left(\frac{N}{p^r}, p'\right)$$

car tout nombre $n \leq N$ n'ayant que des facteurs premiers $\leq p$ s'écrit de façon unique comme $n = p^r n'$ où $n' \leq \frac{N}{p^r}$ n'a que des facteurs premiers $\leq p'$. Par récurrence, on voit que, si $y \leq z$, on a

$$R(N,y) = R(N,z) - \sum_{y<p\leq z} R\left(\frac{N}{p}, p'\right) - \sum_{y<p\leq z} \sum_{r=2}^{\infty} R\left(\frac{N}{p^r}, p'\right)$$

où p' est le nombre premier qui précède p.

Il est clair que la somme double est $o(N)$ car $R(N,z) \leq N$ et $\sum_p \sum_{r=2}^{\infty} \frac{1}{p^r} < +\infty$, donc

$$R(N,y) \sim R(N,z) - \sum_{y<p\leq z} R\left(\frac{N}{p}, p'\right).$$

Supposons trouvés un entier $k \geq 1$ et une fonction $\delta(u)$ définie pour $u > 1/k$ et de classe C^1 telle que la formule asymptotique

$$R(N,z) \sim \delta\left(\frac{\log z}{\log N}\right) N, \quad N \to \infty$$

soit valable pour $\frac{\log z}{\log N} > 1/k$. Nous démontrerons que la même formule asymptotique vaut encore pour $\frac{\log z}{\log N} > 1/(k+1)$ à condition de définir $\delta(u)$ dans l'intervalle $\frac{1}{k+1} < u \leq \frac{1}{k}$ par l'équation

$$\delta(u) = 1 - \int_u^1 \delta\left(\frac{v}{1-v}\right) \frac{dv}{v}.$$

Comme pour $k = 1$ on peut prendre $\delta(u) = 1$ pour $u > 1$, une simple récurrence sur k montrera alors que $R(N,z) \sim \delta\left(\frac{\log z}{\log N}\right) N$ où la fonction $\delta(u)$ est définie par

$$\begin{cases} \delta(u) = 1 & \text{si } u \geq 1 \\ \delta(u) = 1 - \int_u^1 \delta\left(\frac{v}{1-v}\right) \frac{dv}{v} & \text{si } 0 < u < 1. \end{cases}$$

Comme $\delta(u) \geq 0$ et $\delta'(u) = \frac{1}{u}\delta\left(\frac{u}{1-u}\right)$, il est clair que $\delta(u) > 0$ pour $u > 0$ et cela complètera la démonstration du lemme.

Pour passer de k à $k+1$, nous procèderons de la manière suivante : soit $N^{\frac{1}{k+1}+\epsilon} < z \leq N^{\frac{1}{k}}$ où $\epsilon > 0$ est fixé. On a :

$$R(N,z) \sim N - \sum_{z<p\leq N} R\left(\frac{N}{p}, p'\right).$$

Comme $\log p' \sim \log p$ et $p > N^{\frac{1}{k+1}+\epsilon}$, on a

$$\frac{\log p'}{\log(N/p)} > \frac{1}{k} + \frac{\epsilon}{k},$$

et l'hypothèse de récurrence montre que

$$R\left(\frac{N}{p}, p'\right) = \delta\left(\frac{\log p'}{\log(N/p)}\right) \frac{N}{p} + o\left(\frac{N}{p}\right)$$

pour $z < p \leq N$. On a également $\sum_{z<p\leq N} \frac{1}{p} \ll \log\left(\frac{\log N}{\log z}\right) + 1 \ll 1$, d'où

$$R(N,z) \sim N - \sum_{z<p\leq N} \delta\left(\frac{\log p'}{\log(N/p)}\right)\frac{N}{p}.$$

Comme $\delta(u)$ est de classe C^1 pour $u > \frac{1}{k}$, on peut remplacer $\frac{\log p'}{\log(N/p)}$ par $\frac{\log p}{\log(N/p)}$ dans la formule ci-dessus. Soit maintenant $A(t) = \sum_{t<p\leq N} \frac{1}{p}$. On a

$$-\sum_{z<p\leq N} \delta\left(\frac{\log p}{\log(N/p)}\right)\frac{1}{p} = \int_z^N \delta\left(\frac{\log t}{\log(N/t)}\right) dA(t);$$

utilisant l'estimation élémentaire $A(t) = \log\left(\frac{\log N}{\log t}\right) + O\left(\frac{1}{\log t}\right)$, on trouve, après changement de variables et intégration par parties :

$$\int_z^N \delta\left(\frac{\log t}{\log(N/t)}\right) dA(t) \sim -\int_{\log z/\log N}^1 \delta\left(\frac{v}{1-v}\right)\frac{dv}{v}.$$

§ 2. La forme analytique additive du grand crible

Soit $x_1, x_2, \ldots, x_R$ des points réels distincts mod 1, et posons

$$\|\delta\| = \min_{r\neq s} \|x_r - x_s\|$$

où $\|x\|$ désigne la distance de x à l'entier le plus proche. Le but de cette section est d'obtenir des inégalités pour des sommes trigonométriques de la forme

$$S(x) = \sum_{n=M+1}^{M+N} a_n e(nx)$$

où $e(x) = e^{2\pi i x}$. On cherche à majorer la forme quadratique $\sum_{r=1}^R |S(x_r)|^2$.

Théorème 3 *Soit $S(x) = \sum_{n=M+1}^{M+N} a_n e(nx)$. Alors on a*

$$\sum_{r=1}^R |S(x_r)|^2 \leq (N + 2\delta^{-1}) \sum_{n=M+1}^{M+N} |a_n|^2.$$

Ce théorème constitue la forme additive du grand crible sous son aspect analytique. Pour le démontrer, nous utiliserons une méthode de dualité combinée à une fonction auxiliaire bien choisie.

Lemme 2 *Soit c_n des coefficients complexes. L'inégalité*

$$\sum_{r=1}^R \left|\sum_{n=M+1}^{M+N} a_n c_n(r)\right|^2 \leq A \sum_{n=M+1}^{M+N} |a_n|^2$$

est équivalente à l'inégalité duale

$$\sum_{n=M+1}^{M+N} \left|\sum_{r=1}^R z_r c_n(r)\right|^2 \leq A \sum_{r=1}^R |z_r|^2$$

pour toutes les suites complexes z_r.

Appliquons ce lemme avec $c_n(r) = e(nx_r)$. La forme duale à démontrer devient :

$$\sum_{n=M+1}^{M+N} \left| \sum_{r=1}^{R} z_r e(nx_r) \right|^2 \leq (N + 2\delta^{-1}) \sum_{r=1}^{R} |z_r|^2.$$

Soit b_n une suite de nombres réels positifs ou nuls telle que $b_n \geq 1$ pour $M+1 \leq n \leq M+N$. Il est clair que le membre de gauche de l'inégalité duale est majoré par

$$\sum_{n=-\infty}^{+\infty} b_n \left| \sum_{r=1}^{R} z_r e(nx_r) \right|^2 = \sum_{r=1}^{R} \sum_{s=1}^{R} z_r \overline{z_s} B(x_r - x_s)$$

où $B(x) = \sum_{n=-\infty}^{+\infty} b_n e(nx)$.

Nous choisissons b_n de telle sorte que son support soit fini ou que sa transformée de Fourier $B(x)$ décroisse très rapidement en dehors de l'origine. Un choix particulièrement efficace est lié aux fonctions d'approximation de Selberg, qui permettent d'obtenir la constante optimale $N + \delta^{-1} - 1$ sous certaines conditions, mais la borne $N + 2\delta^{-1}$ s'obtient plus simplement en prenant une fonction en chapeau ou un noyau de Fejér modifié.

§ 3. Applications arithmétiques. Le crible de Selberg (I)

Revenons au problème du crible arithmétique formulé au § 0. Nous allons appliquer le Théorème 3 au cas où les points x_r sont les fractions rationnelles épurées a/q avec $(a, q) = 1$ et $q \leq Q$.

Si $r \neq s$, soient $x_r = a/q$ et $x_s = a'/q'$. On a

$$\left| \frac{a}{q} - \frac{a'}{q'} \right| = \frac{|aq' - a'q|}{qq'} \geq \frac{1}{qq'} \geq \frac{1}{Q^2}.$$

Par conséquent, on peut choisir $\delta = Q^{-2}$. Le Théorème 3 donne immédiatement l'inégalité suivante :

Théorème 4 *Soit $S(x) = \sum_{n=M+1}^{M+N} a_n e(nx)$. Alors on a*

$$\sum_{q \leq Q} \sum_{a \pmod q}^{*} |S(a/q)|^2 \leq (N + 2Q^2) \sum_{n=M+1}^{M+N} |a_n|^2$$

où $\sum^*$ indique que la somme porte sur les classes d'un système premier de résidus mod q.

Soit maintenant $\mathcal{N}_0$ l'ensemble criblé défini par un ensemble d'entiers $\mathcal{N} = \{M+1, \ldots, M+N\}$, un ensemble de premiers $\mathcal{P}$ et des ensembles de mauvais résidus Ω_p de cardinal $\omega(p)$.

Introduisons la fonction caractéristique de l'ensemble criblé : $a_n = 1$ si $n \in \mathcal{N}_0$ et $a_n = 0$ sinon. On a alors $S(a/q) = \sum_{n \in \mathcal{N}_0} e(na/q)$.

Pour un nombre premier $p \in \mathcal{P}$ et $a \pmod p$, on examine la répartition des éléments de $\mathcal{N}_0$ dans les classes de restes. Par définition, si $n \in \mathcal{N}_0$, $n \pmod p$ ne peut pas appartenir à Ω_p. En utilisant les propriétés d'orthogonalité des caractères additifs, on établit la relation fondamentale suivante entre la variance de la distribution et le grand crible :

Théorème 5 *On a l'estimation*

$$|\mathcal{N}_0| \leq \frac{N + 2Q^2}{L(Q)}$$

où

$$L(Q) = \sum_{q \leq Q} \mu^2(q) \prod_{p|q} \frac{\omega(p)}{p - \omega(p)}.$$

Ce résultat est d'une importance capitale : il montre que le grand crible est capable de fournir des majorations d'une qualité au moins égale à celle du crible de Selberg, tout en s'appliquant à des situations où $\omega(p)$ est grand (de l'ordre de $p/2$), comme dans le cas des non-résidus quadratiques.

§ 4. La forme multiplicative du grand crible

Dans cette section, nous passons de l'analyse harmonique additive (liée aux points a/q) à l'analyse harmonique multiplicative, qui utilise les caractères de Dirichlet $\chi \pmod q$.

Soit χ un caractère primitif mod q. Les sommes de Gauss associées

$$\tau(\chi) = \sum_{b \pmod q} \chi(b) e(b/q)$$

jouent le rôle d'opérateur de transition entre les deux formes du crible. On sait que pour un caractère primitif, $|\tau(\chi)| = \sqrt{q}$. De plus, on a la relation d'inversion classique :

$$\chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{b \pmod q} \overline{\chi}(b) e(nb/q).$$

Soit $S(x) = \sum_{n=M+1}^{M+N} a_n e(nx)$ la somme trigonométrique additive étudiée précédemment. Définissons son analogue multiplicatif pour un caractère χ :

$$\psi(\chi) = \sum_{n=M+1}^{M+N} a_n \chi(n).$$

En substituant la relation d'inversion dans l'expression de $\psi(\chi)$, on obtient :

$$\psi(\chi) = \frac{1}{\tau(\overline{\chi})} \sum_{b \pmod q} \overline{\chi}(b) S(b/q).$$

En prenant le module au carré et en sommant sur tous les caractères primitifs χ mod q, l'orthogonalité des caractères permet de basculer vers les sommes additives :

$$\sum_{\chi \pmod q}^{*} |\psi(\chi)|^2 \leq \frac{1}{q} \sum_{\chi \pmod q} \left| \sum_{b \pmod q} \overline{\chi}(b) S(b/q) \right|^2$$

$$\sum_{\chi \pmod q}^{*} |\psi(\chi)|^2 \leq \frac{\phi(q)}{q} \sum_{b \pmod q}^{*} |S(b/q)|^2 \leq \sum_{b \pmod q}^{*} |S(b/q)|^2.$$

En sommant cette inégalité sur tous les modules $q \leq Q$ et en injectant le résultat du Théorème 4, nous obtenons le théorème fondamental de la forme multiplicative du grand crible :

Théorème 6 *Soit a_n des nombres complexes quelconques. On a*

$$\sum_{q\leq Q}\frac{q}{\phi(q)}\sum_{\chi}^{*}\sum_{(\mathrm{mod}\ q)}\left|\sum_{n=M+1}^{M+N}a_n\chi(n)\right|^2\leq(N+2Q^2)\sum_{n=M+1}^{M+N}|a_n|^2.$$

Remarque 1 *Cette formulation montre que les fonctions $\chi(n)/\sqrt{\phi(q)}$ pour $q\leq Q$ et χ primitif se comportent comme un système presque orthogonal face à des suites de longueur N, la perturbation étant contrôlée par le terme $2Q^2$.*

§ 5. La forme analytique multiplicative du grand crible

Dans cette section, nous approfondissons la structure analytique des sommes de caractères. L'objectif principal est d'obtenir des majorations plus fines pour les moyennes de grands systèmes de sommes de Dirichlet.

Soit χ un caractère primitif de module q. Nous considérons des sommes de la forme

$$S(t,\chi)=\sum_{n=M+1}^{M+N}a_n\chi(n)n^{-it}$$

où t est un paramètre réel. La présence du facteur n^{-it} nécessite une formulation plus souple que celle obtenue au § 4, afin de traiter simultanément les variations en χ et en t.

Pour ce faire, on introduit un ensemble de paires (χ_r,t_r) pour $r=1,\dots,R$, où chaque χ_r est un caractère primitif de module $q_r\leq Q$, et les t_r sont des nombres réels. On impose une condition de séparation sur les t_r pour les caractères identiques : si $\chi_r=\chi_s$ avec $r\neq s$, alors $|t_r-t_s|\geq\delta$.

L'application directe des méthodes de dualité et des propriétés d'orthogonalité semi-analytique conduit au résultat fondamental suivant :

Théorème 7 *Avec les notations précédentes, on a*

$$\sum_{r=1}^{R}\left|\sum_{n=M+1}^{M+N}a_n\chi_r(n)n^{-it_r}\right|^2\leq C(N,Q,\delta)\sum_{n=M+1}^{M+N}|a_n|^2$$

où la constante $C(N,Q,\delta)$ dépend de la géométrie de la distribution des points t_r et de la taille maximale des modules Q.

L'intérêt majeur de cette forme réside dans son application immédiate à l'étude de la fonction zéta de Riemann et des fonctions L de Dirichlet dans la bande critique. Elle constitue le pont analytique permettant de transformer des informations combinatoires sur les progressions arithmétiques en estimations précises sur la densité des zéros.

§ 6. Applications. Le théorème de Linnik

Nous abordons ici l'une des applications les plus célèbres de la forme multiplicative du grand crible : la distribution des zéros des fonctions L de Dirichlet et son lien avec le plus petit nombre premier dans une progression arithmétique.

Soit $\phi(q)$ la fonction d'Euler et χ un caractère mod q. On s'intéresse au nombre de zéros $\rho = \beta + i\gamma$ de la fonction $L(s,\chi)$ situés dans un rectangle critique $\alpha \leq \beta \leq 1$, $|\gamma| \leq T$. Notons $N(\alpha, T, \chi)$ ce nombre.

En utilisant le Théorème 7 de la section précédente, on peut majorer la somme de ces zéros sur l'ensemble des caractères primitifs de module inférieur à Q.

Théorème 8 *Pour tout $\alpha \geq 1/2$, on a*

$$\sum_{q \leq Q} \sideset{}{^*}\sum_{\chi \pmod q} N(\alpha, T, \chi) \ll (Q^2 T)^{c(1-\alpha)}$$

où c est une constante positive absolue.

Ce théorème de densité de zéros est l'outil crucial pour prouver le théorème de Linnik sans supposer l'hypothèse de Riemann généralisée.

Théorème 9 (Linnik) *Soient $q \geq 1$ et a un entier tel que $(a,q) = 1$. Il existe deux constantes absolues c_1 et L telles que le plus petit nombre premier $p \equiv a \pmod q$ satisfait à*

$$p \ll q^L.$$

La constante L est appelée la *constante de Linnik*. La preuve consiste à utiliser la formule explicite pour la fonction $\psi(x,\chi)$ exprimée en somme sur les zéros de $L(s,\chi)$, puis à exploiter le fait que le théorème de densité garantit qu'il y a très peu de zéros proches de la ligne $\beta = 1$, ce qui empêche une annulation totale des termes principaux.

§ 7. Le théorème de Bombieri

Cette section est consacrée à la démonstration du théorème de distribution moyenne des nombres premiers, souvent appelé le théorème de Bombieri-Vinogradov. Ce résultat montre que, *en moyenne*, les nombres premiers sont distribués dans les progressions arithmétiques de manière aussi régulière que ce que prédit l'hypothèse de Riemann généralisée.

Posons comme d'habitude

$$\psi(x; q, a) = \sum_{\substack{n \leq x \\ n \equiv a \pmod q}} \Lambda(n)$$

et

$$E(x; q) = \max_{(a,q)=1} \left| \psi(x; q, a) - \frac{x}{\phi(q)} \right|.$$

Le théorème affirme que l'erreur maximale $E(x;q)$ est petite en moyenne pour des modules q allant presque jusqu'à $\sqrt{x}$.

Théorème 10 (Bombieri-Vinogradov) *Pour toute constante $A > 0$, il existe une constante $B = B(A) > 0$ telle que, si $Q = x^{1/2}(\log x)^{-B}$, on a*

$$\sum_{q \leq Q} E(x; q) \ll \frac{x}{(\log x)^A}.$$

Pour démontrer ce théorème, on commence par utiliser l'orthogonalité des caractères pour se ramener à des estimations sur les caractères :

$$E(x;q) \leq \frac{1}{\phi(q)} \sum_{\chi \pmod q} \max_{y \leq x} |\psi(y,\chi)| + O((\log x)^2)$$

où $\psi(y,\chi) = \sum_{n \leq y} \Lambda(n)\chi(n)$.

On sépare ensuite la contribution des caractères induits par des caractères primitifs. La contribution des petits modules (ceux pour lesquels $\leq (\log x)^B$) est contrôlée par le théorème de Siegel-Walfisz. Pour les grands modules, on utilise une identité combinatoire sur la fonction de von Mangoldt $\Lambda(n)$ (telle que l'identité de Vaughan ou une décomposition équivalente en moyennes de produits de convolution) qui permet de transformer $\psi(y,\chi)$ en combinaisons de sommes bilinéaires.

Ces sommes bilinéaires sont ensuite majorées en moyenne sur q grâce à la forme multiplicative du grand crible obtenue au § 4, ce qui fournit la borne attendue.

§ 8. Une application du petit crible

Dans cette section, nous faisons une transition vers le petit crible de Brun-Selberg afin de préparer les outils combinatoires nécessaires à la preuve du théorème de Rényi. Le grand crible fournit des majorations globales puissantes, mais l'analyse fine de la structure des diviseurs d'un entier nécessite parfois des techniques de crible local.

Soit $\mathcal{A}$ un ensemble fini d'entiers et $\mathcal{P}$ un ensemble de nombres premiers. Pour un nombre réel $z \geq 2$, on définit la fonction de crible

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

et l'on cherche à évaluer ou à majorer le cardinal de l'ensemble criblé

$$S(\mathcal{A}, \mathcal{P}, z) = \{n \in \mathcal{A} \mid (n, P(z)) = 1\}.$$

En combinant les estimations obtenues par le théorème de Bombieri-Vinogradov (Théorème 9) sur la distribution moyenne des restes et une identité de crible de type Selberg ou Rosser-Iwaniec, on établit des bornes supérieures et inférieures de la forme :

$$S(\mathcal{A}, \mathcal{P}, z) \leq XV(z)F(s) + R$$

$$S(\mathcal{A}, \mathcal{P}, z) \geq XV(z)f(s) - R$$

où X est une approximation du cardinal de $\mathcal{A}$, $V(z)$ est le produit de probabilités de crible $\prod(1 - \omega(p)/p)$, $s = \frac{\log x}{\log z}$, et R est un terme de reste.

Grâce au théorème du § 7, le terme de reste R, qui implique des sommes de fonctions d'erreur sur les progressions arithmétiques, est contrôlé de manière extrêmement efficace *en moyenne*, ce qui permet de choisir un paramètre de crible z beaucoup plus grand que dans les méthodes classiques de Brun.

§ 9. Le théorème de Rényi

Le théorème de Rényi concerne une approximation de la conjecture de Goldbach, affirmant que tout nombre entier pair assez grand peut s'écrire comme la somme d'un nombre premier et d'un nombre presque premier contenant un nombre borné de facteurs premiers.

Soit P_r un entier ayant au plus r facteurs premiers, comptés avec leur multiplicité. On s'intéresse à l'équation

$$2N = p + P_r$$

où p est un nombre premier.

Théorème 11 (Rényi) *Il existe un entier positif r tel que tout nombre pair assez grand $2N$ est représentable sous la forme $2N = p + P_r$.*

Nous donnons ici la preuve du fait que cette équation est résoluble avec $r \leq 4$. La méthode consiste à poser $\mathcal{A} = \{2N - p \mid p < 2N\}$ et à lui appliquer les bornes inférieures du crible développées au § 8.

On choisit le paramètre de crible $z = (2N)^\theta$ avec un θ convenable. Le théorème de Bombieri-Vinogradov permet de prendre θ proche de $1/2$. L'analyse pondérée des fonctions $f(s)$ et $F(s)$ du crible montre alors que le nombre d'éléments de $\mathcal{A}$ qui survivent au crible par les premiers inférieurs à z est strictement positif.

Comme ces éléments n'ont pas de petits facteurs premiers, le nombre total de leurs facteurs premiers ne peut pas dépasser un seuil fixe, que l'on calcule comme étant inférieur ou égal à 4. Cela démontre la résolubilité de l'équation.

§ 10. Une variante du théorème de densité

Dans cette dernière section technique, nous étudions une variante du théorème de densité des zéros des fonctions L de Dirichlet (Théorème 8), adaptée à l'étude des nombres premiers dans des intervalles courts de la forme $(x, x + x^\theta)$ avec $\theta < 1$.

Pour obtenir des résultats fins sur de tels intervalles, il est nécessaire de disposer d'estimations locales sur les zéros, où la sommation sur les modules q est restreinte à un seul module ou à un ensemble très petit de modules, tandis que l'intégration en T est optimisée.

Théorème 12 *Soit χ un caractère mod q. On a, pour $\alpha \geq 1/2$, la majoration locale suivante :*

$$N(\alpha, T, \chi) \ll (qT)^{c'(1-\alpha)}$$

où la constante c' est optimisée grâce à des techniques de grands systèmes de polynômes de Dirichlet et au grand crible sous sa forme analytique multiplicative (§ 5).

Cette variante permet de s'affranchir de la moyenne sur les modules lorsque l'on s'intéresse à un problème arithmétique purement local (sans progression arithmétique variable). Elle intervient de manière cruciale dans la démonstration de l'existence de nombres premiers entre deux cubes consécutifs ou dans des intervalles de longueur $x^{\frac{7}{12}+\epsilon}$.

§ 11. Notes bibliographiques

Les présentes notes ne prétendent pas fournir un historique exhaustif de la méthode du grand crible, mais plutôt indiquer les sources principales des théorèmes présentés et guider le lecteur vers des développements ultérieurs.

La découverte originale du grand crible revient à Linnik (1941), qui l'a introduit pour étudier la répartition des grands d'un ensemble d'entiers dans les progressions arithmétiques, ce qui l'a conduit à son célèbre théorème sur le plus petit non-résidu quadratique (Théorème 1 et Théorème 2). La formulation probabiliste et statistique sous forme de variance a été développée ensuite de manière magistrale par Rényi (1947, 1948).

L'aspect analytique additif, basé sur les sommes trigonométriques et les inégalités du type Bessel (§ 2), a été profondément renouvelé par Roth (1965) et par Bombieri (1965). L'introduction de la méthode de dualité ("principe du grand crible") est principalement due à l'approche de Davenport et Halberstam (1966). La constante optimale $N + \delta^{-1} - 1$ mentionnée au § 2 découle des travaux fins de Montgomery et Vaughan (1973).

L'application au petit crible et la fonction $L(Q)$ introduite au § 3 proviennent directement des formulations de Selberg, qui a montré comment le grand crible pouvait avantageusement remplacer ou compléter le petit crible dans de nombreuses questions arithmétiques de structure multiplicative.

La transition vers la forme multiplicative (§ 4 et § 5) et l'utilisation systématique des sommes de Gauss pour l'étude des caractères primitifs de Dirichlet ont été initiées par Gallagher (1967) et perfectionnées par la suite par Montgomery dans sa monographie sur les sujets de théorie multiplicative des nombres (1971).

Les théorèmes de densité pour les zéros des fonctions L (§ 6) et la démonstration qui en découle pour le théorème de Linnik sur le plus petit nombre premier dans une progression arithmétique s'appuient sur les techniques de décompte de Montgomery.

Le théorème de distribution moyenne (§ 7), connu sous le nom de théorème de Bombieri-Vinogradov, a été établi indépendamment par A. I. Vinogradov (1965) et par Bombieri (1965) avec une forme plus précise pour le terme d'erreur. La simplification présentée ici, qui utilise l'identité combinatoire de Vaughan, permet d'éviter l'usage de machineries complexes sur les intégrales de contour.

Les applications combinées du petit crible et du grand crible pour l'équation de Goldbach-Rényi (§ 8 et § 9) trouvent leur origine dans les travaux de Rényi (1948). Les raffinements successifs permettant d'atteindre la résolubilité avec un nombre de facteurs $r \leq 4$ découlent d'améliorations structurelles apportées par Chen, Jing-run, ainsi que par Halberstam et Richert dans leur traité classique sur la théorie du crible.

Enfin, la variante locale du théorème de densité discutée au § 10 est intimement liée aux travaux de Huxley (1972) concernant les petits intervalles entre nombres premiers et les estimations de grands systèmes de polynômes de Dirichlet.

Références

[1] E. Bombieri, *On the large sieve*, Mathematika, vol. 12, 1965, p. 201–225.

[2] H. Davenport et H. Halberstam, *The values of a trigonometric polynomial at well spaced points*, Mathematika, vol. 13, 1966, p. 91–96.

[3] P. X. Gallagher, *The large sieve*, Mathematika, vol. 14, 1967, p. 14–20.

[4] U. V. Linnik, *The large sieve*, C. R. (Doklady) Acad. Sci. URSS, vol. 30, 1941, p. 292–294.

[5] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Mathematics, vol. 227, Springer-Verlag, 1971.

[6] A. Rényi, *On the representation of an even number as the sum of a prime and of an almost prime number*, Izv. Akad. Nauk SSSR Ser. Mat., vol. 12, 1948, p. 57–78.

[7] A. I. Vinogradov, *The density hypothesis for Dirichlet L-functions*, Izv. Akad. Nauk SSSR Ser. Mat., vol. 29, 1965, p. 903–934.