# L'INÉGALITÉ DU GRAND CRIBLE PAR LA FONCTION DE SELBERG

Olivier Ramaré

Abstract. Exposé introductif sur l'inégalité du grand crible que nous démontrons à l'aide d'un lissage. Nous établissons aussi la forme arithmétique du grand crible, due à Montgomery. Version du 10 Février 2000.

Le lecteur trouvera deux autres approches classiques dans les monographes respectivement de Bombieri et de Montgomery cités ci-après.

## I. Une formule de Poisson.

Bien que la formule de Poisson soit d'un usage courant en théorie analytique des nombres, il n'est pas facile de trouver dans cette littérature une telle formule avec des hypothèses assez larges. Nous donnons ici une telle formule.

La transformée de Fourier d'une fonction $f : \mathbb{R} \to \mathbb{R}$ est définie au point $x$ par

$$\hat{f}(x) = \int_{-\infty}^{\infty} f(t)\, e(xt) dt = \lim_{T\to\infty} \int_{-T}^{T} f(t)\, e(xt) dt$$

avec $e(\alpha) = \exp(2i\pi\alpha)$. Nous avons, sous l'hypothèse supplémentaire que $f$ et $\hat{f}$ appartiennent à $\mathcal{L}^1(\mathbb{R})$,

$$f(t) = \int_{-\infty}^{\infty} \hat{f}(x)\, e(-xt) dx.$$

Dans cette partie uniquement, nous posons

$$\sum_{n\in\mathbb{Z}}^{\text{sym}} \varphi_n = \lim_{N\to\infty} \sum_{-N\le n\le N} \varphi_n$$

si cette limite existe.

Nous avons alors le théorème suivant dû à Bochner :

**Théorème.** *Soit $f : \mathbb{R} \to \mathbb{R}$ et $\alpha$ réel. Supposons que*

(1) *la fonction $f$ est continue est $\mathbb{R}$,*
(2) *la série $\sum_{n\in\mathbb{Z}}^{\text{sym}} f(t+n)e(\alpha(t+n))$ converge uniformément pour $t \in [-\frac{1}{2}, \frac{1}{2}]$,*
(3) *la série $\sum_{k\in\mathbb{Z}}^{\text{sym}} \hat{f}(k-\alpha)$ converge.*

*Alors*

$$\sum_{n\in\mathbb{Z}}^{\text{sym}} f(n)e(\alpha(n)) = \sum_{k\in\mathbb{Z}}^{\text{sym}} \hat{f}(k-\alpha).$$

Remarquons que sous les deux premières hypothèses, la preuve montre que $\hat{f}$ existe.

*Preuve.* Voir le livre de Chandrasekharan, cité ci-dessous, chapître II, théorème 1. $\diamond\diamond\diamond$

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

**II. Une bonne fonction de lissage.**

Voici notre fonction favorite :

**Théorème.** *Soit $N \geq 1$ et $\delta > 0$ deux réels. Il existe une fonction $b(t) = b_{N,\delta}(t)$ de $\mathbb{R}$ dans $\mathbb{R}$ telle que*

(1) *$b$ est $C^\infty$.*
(2) *$b(t) = \mathcal{O}_{N,\delta}(|t|^{-2})$ quand $|t| \to \infty$.*
(3) *$b(t) \geq 0$ pour tout $t$.*
(4) *$b(t) \geq 1$ pour tout $t \in [1, N]$.*
(5) *$\hat{b}(x) = 0$ si $|x| \geq \delta$.*
(6) *$\hat{b}(0) = N - 1 + \delta^{-1}$.*

La fonction $b$ ressemble à :

Nous avons aussi $b(t) \leq 2$. Pour la construction, le lecteur consultera l'article de Vaaler cité ci-après.

**III. L'inégalité du grand crible.**

Soit $(\varphi_n)$ une suite de complexes. Posons

$$S(\alpha) = \sum_{1 \leq n \leq N} \varphi_n e(n\alpha).$$

Un ensemble fini $\mathcal{X} \subset \mathbb{R}/\mathbb{Z}$ est dit $\delta$-bien espacé si l'on a

$$\min\left\{\|x - x'\|, \quad x, x' \in \mathcal{X},\ x \neq x'\right\} \geq \delta,$$

où $\|y\|$ est pris sur le cercle de circonférence unité ($\|y\| = \min_{k\in\mathbb{Z}} |y - k|$), et donc $\delta < 1/2$. Dans le cas (fortement inintéressant) où $\mathcal{X}$ est réduit à un point, on prend $\delta = 1/2$. Nous avons alors

$$\sum_{x\in\mathcal{X}} |S(x)|^2 \leq \sum_{n\leq N} |\varphi_n|^2\ (N - 1 + \delta^{-1}) \qquad (\mathcal{X}\ \delta\text{-bien espacé}) \tag{3.1}$$

*Preuve.* Écrivons

$$\sum_{x\in\mathcal{X}} |S(x)|^2 = \sum_{1\leq n\leq N} \sum_{x\in\mathcal{X}} \varphi_n \overline{S(x)}\, e(nx).$$

Par conséquent,

$$\begin{aligned}\left(\sum_{x\in\mathcal{X}} |S(x)|^2\right)^2 &\leq \sum_{n\leq N} |\varphi_n|^2 \sum_{n\leq N} \left|\sum_{x\in\mathcal{X}} \overline{S(x)}\, e(nx)\right|^2 \\ &\leq \sum_{n\leq N} |\varphi_n|^2 \sum_{n\in\mathbb{Z}} b(n) \left|\sum_{x\in\mathcal{X}} \overline{S(x)}\, e(nx)\right|^2\end{aligned}$$

où $b = b_{N\delta}$ est la fonction donnée par le théorème de la seconde partie. Par ailleurs

$$\begin{aligned}\sum_{n\le N}|\varphi_n|^2\sum_{n\in\mathbb{Z}}b(n)\Big|\sum_{x\in\mathcal{X}}\overline{S(x)}\,e(nx)\Big|^2 &= \sum_{x,x'\in\mathcal{X}}\overline{S(x)}S(x')\sum_{n\in\mathbb{Z}}b(n)e(n(x-x'))\\ &= \sum_{x,x'\in\mathcal{X}}\overline{S(x)}S(x')\sum_{k\in\mathbb{Z}}\hat{b}(k-(x-x'))\\ &= \sum_{x\in\mathcal{X}}|S(x)|^2(N-1+\delta^{-1})\end{aligned}$$

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

Notons que

$$|S(x_0)| \le \sum_{n\le N}|\varphi_n|^2 N \tag{3.2}$$

ce qui fait que, lorsque $\delta^{-1} = o(N)$, l'inéquation (3.1) donne essentiellement la même majoration que (3.2), alors que l'on majore simultanément de nombreux termes.

Il existe à l'heure actuelle essentiellement quatre preuves de l'inégalité du grand crible. Celle que nous venons de donner dont l'idée se trouve dans un article de Davenport & Halberstam de 1966, une due à Gallagher et qui tente de comprendre le membre de gauche de (3.1) comme une somme de Riemann, une (due à Montgomery & Vaughan ?) qui passe par l'inégalité de Hilbert et une dernière, en fait plus ancienne, qui utilisait notamment des disques de Gegenbauer. La preuve que nous présentons est en quelque sorte la forme achevée de cette dernière approche. Le lecteur trouvera aussi des démonstration hybrides, comme celle que présente Vaaler dans l'article sus-cité et qui combine la technique de Selberg et l'idée de Gallagher.

## IV. L'inégalité du grand crible pour la suite de Farey.

Presque toutes les utilisations de (3.1) en théorie des nombres se font en prenant

$$\mathcal{X} = \{\tfrac{a}{q},\quad q\le Q, (a,q)=1, 1\le a\le q\}.$$

L'inégalité du grand crible ((3.1)) s'écrit alors :

$$\sum_{q\le Q}\sum_{a \bmod {}^*q}|S(a/q)|^2 \le \sum_{n\le N}|\varphi_n|^2\ (N-1+\delta^{-1}). \tag{3.3}$$

En effet, deux points distincts $a/q$ et $a'/q'$ de $\mathcal{X}$ vérifient

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

En fait, si $a/q$ et $a'/q'$ sont consécutifs, il est classique que $(q,q')=1$, et notamment $q\ne q'$ si $Q\ge 2$. La minoration précédente peut donc être remplacée par $\frac{1}{Q(Q-1)}$, qui est atteinte entre $1/Q$ et $1/(Q-1)$.

Notons que $|\mathcal{X}\| = \sum_{q\le Q}\phi(q) \asymp Q^2$, ce qui fait que les points de $\mathcal{X}$ sont quasiment équi-distribués sur le cercle.

La remarque vitale ensuite consiste à dire que $S(a/q)$ ne dépend que de la distribution de $(\varphi_n)_n$ modulo $q$ puisque nous avons

$$S(a/q) = \sum_{b \mod q}\biggl(\sum_{n\equiv b[q]}\varphi_n\biggr)e(ab/q).$$

En particulier, si $q = p$ est un nombre premier, nous avons

$$\sum_{a \mod {}^*p}|S(a/p)|^2 = p\sum_{b \mod p}\biggl|\sum_{n\equiv b[p]}\varphi_n - \frac{S(0)}{p}\biggr|^2.$$

**V. Le crible de Montgomery.**

Pour chaque nombre premier $p$, nous nous donnons un sous-ensemble $\mathcal{K}_p\subset\mathbb{Z}/p\mathbb{Z}$ (l'ensemble des classes que l'on garde).

Nous dirons que la suite $(\varphi_n)_n$ est portée par $(\mathcal{K}_p)$ jusqu'au niveau $Q$ si nous avons

$$\forall n\le N \qquad \bigl[\varphi_n\neq 0 \implies \forall p\le Q,\quad n\in\mathcal{K}_p\bigr]. \tag{5.1}$$

Par exemple, pour cribler la suite des nombres premiers compris entre $\sqrt{N}$ et $N$, nous prendrons $\mathcal{K}_p = \mathbb{Z}/p\mathbb{Z}\setminus\{0\}$ et $Q=\sqrt{N}$. Notons que si (5.1) est vérifié pour un certain $Q$, elle est encore trivialement vraie pour tout $Q'$ inférieur à $Q$.

Posons

$$G(\mathcal{K},Q) = \sum_{q\le Q}\mu^2(q)\prod_{p|q}\bigl(\frac{p}{|\mathcal{K}_p|}-1\bigr). \tag{5.2}$$

Alors, si $(\varphi_n)_n$ est portée par $(\mathcal{K}_p)$ jusqu'au niveau $Q$, nous avons

$$\biggl|\sum_n\varphi_n\biggr|^2 \le \sum_n|\varphi_n|^2\frac{N-1+Q^2}{G(\mathcal{K},Q)}. \tag{5.3}$$

**Corollaire.** *Soit $Z$ le nombre d'entiers $n$ de $[1,N]$ qui vérifient $\forall p\le Q,\quad n\in\mathcal{K}_p$. Nous avons*

$$Z\le\frac{N-1+Q^2}{G(\mathcal{K},Q)}.$$

*Preuve du corollaire.* Nous prenons pour $(\varphi_n)$ la fonction caractéristique des $n\in[1,N]$ qui sont tels que $\forall p\le Q,\quad n\in\mathcal{K}_p$. L'inégalité (5.3) nous donne alors le résultat annoncé. $\diamond\diamond\diamond$

*Preuve de* (5.3). Nous procédons à reculons en trois étapes. Histoire se simplifier la typographie, nous posons :

$$g(q) = \mu^2(q)\prod_{p|q}\bigl(\frac{p}{|\mathcal{K}_p|}-1\bigr).$$

Tout d'abord, il suffit de démontrer l'inégalité suivante (pour $(\varphi_n)$ vérifiant (5.1)) :

$$g(q)\,|S(0)|^2 \leq \sum_{a \mod {}^*q} |S(a/q)|^2. \tag{5.4}$$

En effet, combiné à (3.3), cela nous donne bien l'inégalité attendue.

Secundo, pour prouver (5.4) pour $qq'$, il suffit de le prouver pour $q$ et pour $q'$ si $(q,q')=1$. En effet, dans ce cas, nous aurons :

$$\begin{aligned}\sum_{b \mod {}^*qq'} \left|S\Big(\frac{b}{qq'}\Big)\right|^2 &= \sum_{a' \mod {}^*q'}\ \sum_{a \mod {}^*q} \left|S\Big(\frac{a}{q}+\frac{a'}{q'}\Big)\right|^2 \\ &\geq \sum_{a' \mod {}^*q'} g(q')\left|S\Big(\frac{a'}{q'}\Big)\right|^2\end{aligned}$$

obtenue en appliquant (5.4) à $q$ et à la suite $(\varphi_n e(na'/q'))$ qui vérifie bien (5.1). Nous réappliquons (5.4), mais cette fois-ci à $q'$ et à la suite $(\varphi_n)$, ce qui nous donne

$$\sum_{b \mod {}^*qq'} \left|S\Big(\frac{b}{qq'}\Big)\right|^2 \geq g(q')g(q)|S(0)|^2 = g(qq')|S(0)|^2,$$

ce qui prouve notre assertion.

Finalement, il nous reste à prouver (5.4) pour $q=p$, un nombre premier. Dans ce cas, nous avons

(5.5)

$$\begin{aligned}\sum_{a \mod {}^*p} |S(a/p)|^2 &= \sum_{a \mod p} |S(a/p)|^2 - |S(0)|^2 = p\sum_{b \mod p}\Big|\sum_{n\equiv b[p]}\varphi_n\Big|^2 - |S(0)|^2 \\ &= p\sum_{b\in\mathcal{K}_p}\Big|\sum_{n\equiv b[p]}\varphi_n\Big|^2 - |S(0)|^2.\end{aligned}$$

Mais l'inégalité de Cauchy-Schwartz nous donne :

$$|S(0)|^2 = \Big|\sum_{b\in\mathcal{K}_p}\sum_{n\equiv b[p]}\varphi_n\Big|^2 \leq |\mathcal{K}_p|\sum_{b\in\mathcal{K}_p}\Big|\sum_{n\equiv b[p]}\varphi_n\Big|^2$$

ce qui combiné à (5.5) nous donne bien ce que nous souhaitions. ◇◇◇

## References

E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, Astérisque **18** (1974/1987), 103pp.

K. Chandrasekharan, *Arithmetical Functions*, Grundlehren der Mathematischen Wissenschaften (Springer-Verlag) **167**.

H. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Mathematics (Berlin) **227** (1971), 178pp.

J. Vaaler, *Somme Extremal Functions in Fourier Analysis*, Bull. AMS **12** (1985), 183–216..