Astérisque

ENRICO BOMBIERI

Le grand crible dans la théorie analytique des nombres

Astérisque, tome 18 (1974)

<http://www.numdam.org/item?id=AST_1987__18__1_0>

TABLE DES MATIÈRES

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" orthogonaux 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 théoreme 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

$$\mathcal{N} = \{M < n \leqq M+N\}$$

un intervalle de longueur N, ou

$$\mathcal{N} = \{p \leqq N\}$$

l'ensemble des nombres premiers $\leqq N$, ou

$$\mathcal{N} = \{f(n),\ n \leqq N\}$$

où f est un polynôme.

Plaçons-nous dans le premier cas, et posons

$$\omega(p) = |\Omega_p|, \quad \text{nombre d'éléments de } \Omega_p.$$

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 :

$$\text{I} \quad \begin{cases} \mathcal{N} = (1,N) \\ \mathcal{P} = (p \leqq N) \\ \Omega_p = \{0\} \end{cases}$$

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

Dans (I), $\mathcal{N}_0$ est l'ensemble des entiers $\leqq N$ qui ne sont divisibles par aucun