Sur les grands cribles de Linnik et Rényi

K. F. Roth

Soit N un entier naturel, et soit $\mathcal{N}$ un sous-ensemble non vide de l'ensemble des entiers

$$1, 2, \ldots, N. \tag{1}$$

Soit Z le nombre d'éléments de $\mathcal{N}$. On note $Z(p,h)$ le nombre d'éléments de $\mathcal{N}$ tombant dans la classe de congruence h modulo p, de sorte que

$$Z(p,h) = \sum_{\substack{n \in \mathcal{N} \\ n \equiv h \pmod{p}}} 1. \tag{2}$$

Pour chaque nombre premier p, la variance

$$D(p) = \sum_{h=0}^{p-1} \left\{ Z(p,h) - \frac{Z}{p} \right\}^2 \tag{3}$$

fournit une mesure de la régularité de la distribution des éléments de $\mathcal{N}$ parmi les classes de congruence modulo p.

Soit $X \geq 2$, et soit $\mathcal{P}^* = \mathcal{P}^*(X)$ l'ensemble de tous les nombres premiers p satisfaisant

$$p \leq X. \tag{4}$$

On désigne par $\mathcal{P}$ un sous-ensemble arbitraire de $\mathcal{P}^*$, et on note $|\mathcal{P}|$ le nombre d'éléments de $\mathcal{P}$.

Les grands cribles de Linnik et Rényi fournissent des estimations supérieures du type

$$\sum_{p \in \mathcal{P}} pD(p) < K(N, Z, \mathcal{P}),$$

où K est entièrement déterminé par l'"ensemble de criblage" $\mathcal{P}$ ainsi que par les valeurs de N et Z. Ces estimations impliquent, dans des circonstances étonnamment générales, qu'à l'exception d'un nombre comparativement petit de nombres premiers, pour chaque nombre premier p de $\mathcal{P}^*$ les éléments de $\mathcal{N}$ sont (en un sens convenable) bien répartis parmi les classes de congruence modulo p. Le trait remarquable de ces résultats est qu'ils sont entièrement indépendants du choix particulier $\mathcal{N}$ de Z entiers distincts parmi les entiers (1).

La méthode de Linnik, telle qu'affinée par Rényi, donne

$$\sum_{p \leq X} pD(p) \ll Z^{2/3} N^{4/3} X^{1/3} \tag{5}$$

pourvu que $X \leq N^{3/5}$, ou plus généralement

$$\sum_{p \in \mathcal{P}} pD(p) \ll Z^{2/3} N^{4/3} |\mathcal{P}|^{1/3}, \tag{6}$$

Référence : revue Mathematika, une revue de mathématiques pures et appliquées, Vol. 12. Partie 1., Juin 1965, n° 23.

toujours sous réserve que $X \leq N^{1/2}|\mathcal{P}|^{1/6}$. (Ces résultats sont implicites dans la démonstration du lemme 1 de [2]. Ils sont aussi démontrés dans [6], où ils correspondent à des cas particuliers du théorème 5.) Ici, comme dans tout l'article, les constantes implicites dans l'usage de la notation $\ll$ sont absolues.

La méthode de Rényi, d'autre part, donne

$$\sum_{p \leq X^2} pD(p) \ll Z(N + X^3). \tag{7}$$

(Une exposition claire de la démonstration de (7) par Rényi dans le cas important $X = N^{1/3}$ est donnée par lui dans [3] ; et l'extension à X non restreint se trouve dans [5]. Les deux cas sont aussi établis dans [6], où ils apparaissent respectivement comme les théorèmes 6 et 6'. En fait, Rényi a aussi démontré des théorèmes bien plus généraux en théorie des probabilités, donnant (7) comme cas particulier. Voir [4], ainsi que les travaux antérieurs cités dans cet article.)

L'inégalité

$$\sum_{p \leq N^{1/3}} pD(p) \ll ZN, \tag{8}$$

qui est le cas particulier $X = N^{1/3}$ de (7), est extraordinairement puissante. Par exemple, si l'on prend $\mathcal{N}$ pour l'ensemble de tous les nombres premiers ne dépassant pas un grand entier N, le membre de gauche de (8) est certainement

$$\gg N^2(\log\log N)/(\log N)^2$$

[puisque $Z(p, 0) = 1$ pour chaque $p \leq N^{1/3}$], tandis que le membre de droite est

$$\ll N^2/(\log N).$$

L'inégalité (7) est moins efficace lorsque l'ordre de grandeur de X est substantiellement supérieur à $N^{1/3}$, cependant, et lorsque $X = N^{1/3}$ l'inégalité devient complètement inefficace. L'inégalité de Linnik-Rényi (5) [et aussi (6)] fournit une information non triviale lorsque $X = N^{1/2}$, par exemple, mais dans aucun cas cette inégalité n'atteint un degré de précision comparable à celui de (8).

Dans le présent article, nous démontrons un résultat qui conserve la puissance de l'inégalité de Rényi (8) lorsque l'on augmente la portée des "nombres premiers de criblage". Par exemple, en écrivant $X = N^{1/2}/(\log N)^{1/2}$ dans le corollaire 1 ci-dessous, on obtient

$$\sum_{p \leq N^{1/2}/(\log N)^{1/2}} pD(p) \ll ZN. \tag{9}$$

Grosso modo, notre théorème est équivalent au résultat de Rényi lorsque $X = N^{1/3}$, et est supérieur aux résultats de Linnik-Rényi et de Rényi pour X plus grand. Notre corollaire 2 représente un raffinement des résultats correspondants dus à Linnik-Rényi et à Rényi (voir [3] ; théorèmes 2 et 3).

Nous énonçons maintenant notre résultat principal.

Théorème. *Soit N un entier naturel, et soit $\mathcal{N}$ un ensemble de Z entiers naturels distincts ne dépassant pas N. Soit $X \geq 2$, et soit $\mathcal{P}$ un ensemble de nombres premiers distincts p, chacun satisfaisant $p \leq X$. Alors il existe une constante absolue positive c, telle que pour tout nombre $R \geq 2$,*

$$\sum_{p \in \mathcal{P}} pD(p) \leq c(ZN + ZX^2 \log R + Z^2|\mathcal{P}|R^{-2}); \tag{10}$$

où $D(p)$ est défini par (2), (3), et $|\mathcal{P}|$ désigne le nombre d'éléments de $\mathcal{P}$.

En prenant $\mathcal{P} = \mathcal{P}^*$ et $R = X$, on obtient le résultat suivant.

Corollaire 1. *Si $N \geq 2$ et $X \geq N^{1/2}(\log N)^{-1/2}$, alors*

$$\sum_{p \leq X} pD(p) \leq ZX^2 \log X. \tag{11}$$

Pour voir que le théorème implique aussi le corollaire 2 ci-dessous, il suffit de prendre $\mathcal{P}$ constitué des nombres premiers "exceptionnels", de sorte que

$$D(p) \geq f(p) \left(\frac{Z}{pQ(p)} \right)^2$$

pour chaque p de $\mathcal{P}$; puis en écrivant

$$R = c^{1/2}\sigma^{-1/2},$$

où c est la constante apparaissant dans (10) (que l'on peut choisir de sorte que $c \geq 1$, de sorte que $R \geq \sigma^{-1/2} \geq 2$). Car avec ce choix de $\mathcal{P}$, le membre de gauche de (10) est $\geq 4Z^2\sigma|\mathcal{P}|$.

Corollaire 2. *Pour chaque nombre premier $p \leq X$, soit $Q(p)$ un nombre réel satisfaisant $Q(p) \geq 1$, et soit $f(p)$ un entier satisfaisant $1 \leq f(p) \leq p$. On pose*

$$\sigma = \frac{1}{4} \min_{p \leq X} \frac{f(p)}{p\{Q(p)\}^2}. \tag{12}$$

Alors, pour chaque $p \leq X$, à l'exception de

$$\leq \frac{N + X^2 \log(1/\sigma)}{Z\sigma}$$

nombres premiers "exceptionnels", on a

$$|Z(p,h) - \frac{Z}{p}| < \frac{Z}{pQ(p)}$$

pour tout résidu h modulo p en dehors d'au plus $f(p) - 1$ classes de résidus "irrégulières".

Linnik et Rényi ont en fait énoncé leurs résultats en termes de constantes explicites. Les constantes implicites dans nos résultats sont aussi faciles à calculer ; mais il serait trompeur de le faire car nous n'avons fait aucun effort d'économie en ce qui concerne les constantes. De plus, si nos résultats

devaient être rendus explicites, il serait plus approprié de les énoncer sous une forme légèrement différente.

Bien que la démonstration de notre théorème diffère à divers égards des deux méthodes de Linnik et de Rényi, elle utilise aussi les idées de base de chacune de ces méthodes.

Nous aurons besoin du lemme suivant. Dans la démonstration du lemme, et dans la démonstration du théorème, $e(\alpha)$ désignera $e^{2\pi i\alpha}$.

Lemme. *Soit N un entier naturel, et soient R, η des nombres réels satisfaisant $R \geq 2$, $0 < \eta \leq \frac{1}{2}$ respectivement. Alors il existe une suite*

$$d_0, d_1, d_2, \ldots \tag{13}$$

de nombres réels satisfaisant

$$|d_m - 1| < R^{-1} \quad \text{pour } m = 0, 1, \ldots, N \tag{14}$$

et

$$\sum_{m=1}^{\infty} |d_m| < \infty, \tag{15}$$

telle qu'en écrivant

$$\Psi(\alpha) = d_0 + 2\sum_{m=1}^{\infty} d_m \cos 2\pi m\alpha, \tag{16}$$

on ait

$$\Psi(\alpha) = 0 \quad \text{pour} \quad \eta \leq \alpha \leq 1 - \eta \tag{17}$$

et

$$\int_0^1 \Psi^2(\alpha) d\alpha \leq N + \eta^{-1} \log R. \tag{18}$$

Démonstration. Posons

$$k = [\log R] + 1, \tag{19}$$

$$\delta = \eta/(2k). \tag{20}$$

Soit $\psi_0(\alpha)$ la fonction qui est périodique modulo 1 et satisfait

$$\psi_0(\alpha) = \begin{cases} 1 & \text{pour } -k\delta < \alpha < k\delta \\ 0 & \text{pour } k\delta < \alpha < 1 - k\delta \\ \frac{1}{2} & \text{pour } \alpha = \pm k\delta. \end{cases}$$

Nous définissons les fonctions $\psi_1, \psi_2, \ldots, \psi_k$ inductivement au moyen des relations

$$\psi_j(\alpha) = \frac{1}{2\delta}\int_{-\delta}^{\delta} \psi_{j-1}(\alpha + \beta) d\beta \quad (j = 1, 2, \ldots, k). \tag{21}$$

Il est facile de voir que la fonction ψ_k satisfait

$$\psi_k(0) = 1, \tag{22}$$

$$\psi_k(\alpha) = 0 \quad \text{pour} \quad 2k\delta \leq \alpha \leq 1 - 2k\delta \tag{23}$$

et

$$0 \leq \psi_k(\alpha) \leq 1 \quad \text{pour tout réel } \alpha. \tag{24}$$

De plus, des intégrations répétées du développement de Fourier de ψ_0 donnent

$$\psi_k(\alpha) \equiv \sum_{v=-\infty}^{\infty} a_v e(v\alpha), \tag{25}$$

où

$$a_v = \frac{\sin 2\pi vk\delta}{v\pi} \left(\frac{\sin 2\pi v\delta}{2\pi v\delta} \right)^k \quad \text{pour } v \neq 0. \tag{26}$$

Nous écrivons

$$M = [k\eta^{-1}] + N, \tag{27}$$

et pour tout entier m, nous définissons

$$d_m = \sum_{u=-2M}^{2M} \sum_{v=-\infty}^{\infty} a_v = \sum_{|m-v| \leq 2M}^{\infty} a_v; \tag{28}$$

de sorte que

$$\Psi(\alpha) = d_0 + 2 \sum_{m=1}^{\infty} d_m \cos 2\pi m\alpha = \psi_k(\alpha) \sum_{u=-2M}^{2M} e(u\alpha). \tag{29}$$

Nous remarquons que, par (22) et (25),

$$\sum_{v=-\infty}^{\infty} a_v = 1.$$

Ainsi, si $|m| \leq M$ (comme c'est certainement le cas lorsque $|m| \leq N$), il résulte de (28) et (26) que

$$\begin{aligned} |d_m - 1| \leq 2 \sum_{v>M} |a_v| &\leq \frac{2}{\pi} \left(\frac{1}{2\pi\delta} \right)^k \sum_{v=M+1}^{\infty} \frac{1}{v^{k+1}} \\ &\leq \frac{2}{\pi k} \left(\frac{1}{2\pi\delta M} \right)^k. \end{aligned}$$

En outre, par (27), (20) et (19),

$$\left(\frac{1}{2\pi M\delta} \right)^k < \left(\frac{1}{\pi} \right)^k < e^{-k} < \frac{1}{R},$$

de sorte que (14) est satisfaite. La relation (17) est une conséquence immédiate de (23), puisque $2k\delta = \eta$. Enfin, compte tenu de (29) et (24),

$$\int_0^1 \Psi^2(\alpha) d\alpha \leq \int_0^1 \left| \sum_{u=-2M}^{2M} e(u\alpha) \right|^2 d\alpha = 4M + 1,$$

de sorte que (18) est vraie. Ceci achève la démonstration du lemme.
Démonstration du théorème. Nous appliquons le lemme avec

$$\eta = \frac{1}{2}X^{-2}, \tag{30}$$

et choisissons une suite (13) ayant les propriétés affirmées dans le lemme ; cette suite dépendra, bien entendu, de N, R et X. Nous écrivons

$$d_{-m} = d_m \quad (m = 1, 2, 3, \dots). \tag{31}$$

Soit Ψ la fonction définie, en termes de la suite $\{d_m\}$, par (16) ; de sorte que

$$\Psi(x) = \sum_{m=-\infty}^{\infty} d_m e(mx). \tag{32}$$

Nous écrivons

$$U = c_1(N + X^2 \log R), \tag{33}$$

où la constante absolue positive c_1 est choisie de sorte que (18) assure que

$$\int_0^1 \Psi^2(x)dx < U. \tag{34}$$

Dans toute la démonstration, p (et p') désigne un nombre premier satisfaisant (4). Nous définissons, pour chaque p,

$$\Phi_p(x) = \sum_{a=1}^{p-1} \Psi\left(x + \frac{a}{p}\right), \tag{35}$$

et remarquons que, par (32),

$$\Phi_p(x) = p \sum_{m=-\infty}^{\infty} d_m e(mx) - \sum_{m=-\infty}^{\infty} d_m e(mx). \tag{36}$$

En outre, pour chaque p, nous définissons

$$\phi_{p,h}(x) = \frac{1}{(2Up)^4}\Phi_p(x)e(hx) \tag{37}$$

pour $h = 0, 1, \dots, p-1$.

Or, par (17), $\Phi_p(x) = 0$ à moins que α ne soit à une distance $\frac{1}{2}X^{-2}$ d'un certain point a/p, avec $(a, p) = 1$. De plus, si p, p' sont des nombres premiers distincts [satisfaisant (4), comme toujours] et $(a, p) = 1$, alors

$$\left|\frac{a}{p} - \frac{a'}{p'}\right| \geq \frac{1}{pp'} \geq X^{-2}.$$

Il s'ensuit que (pour tout h, h')

$$\int_0^1 \phi_{p,h}(x)\phi_{p',h'}(-x)dx = 0 \quad \text{pourvu que } p \neq p'. \tag{38}$$

De plus, puisque, pour chaque α, au plus un des termes de la somme du membre de droite de (35) est non nul, on a (pour tout h, h')

$$\int_0^1 \phi_{p,h}(\alpha)\phi_{p,h'}(-\alpha)d\alpha = \frac{1}{2Up}\sum_{a=1}^{p-1} e\left(\frac{(h-h')a}{p}\right)\int_0^1 \Psi^2(\alpha)e\left((h-h')\alpha\right)d\alpha.$$

Par conséquent, compte tenu de (34),

$$\left|\int_0^1 \phi_{p,h}(\alpha)\phi_{p,h'}(-\alpha)d\alpha\right| < \frac{1}{2p} \quad \text{si} \quad (h-h', p) = 1, \tag{39}$$

et

$$\int_0^1 |\phi_{p,h}(\alpha)|^2 d\alpha < \frac{1}{2}. \tag{40}$$

Nous écrivons

$$S(\alpha) = \sum_{n\in\mathcal{N}} e(n\alpha) \tag{41}$$

(où $\mathcal{N}$ est la sélection, introduite au début de l'article, de Z entiers distincts parmi $1, 2, \ldots, N$). Nous allons montrer que (10) est une conséquence de l'inégalité (analogue à celle utilisée par Rényi)

$$\int_0^1 |S(\alpha) - \sum_{p\le X}\sum_{h=0}^{p-1} v(p,h)\phi_{p,h}(\alpha)|^2 d\alpha \ge 0, \tag{42}$$

où

$$v(p,h) = \int_0^1 S(\alpha)\phi_{p,h}(-\alpha)d\alpha. \tag{43}$$

Nous remarquons que $v(p,h)$ est réel, et est en fait donné par [cf. (36)]

$$(2Up)^t v(p,h) = p\sum_{n\in\mathcal{N}} d_{n-h} - \sum_{n\in\mathcal{N}} d_{n-h}. \tag{44}$$

L'inégalité (42) donne

$$I_1 - 2I_2 + I_3 \ge 0, \tag{45}$$

où

$$I_1 = \int_0^1 |S(\alpha)|^2 d\alpha = \sum_{n\in\mathcal{N}} 1 = Z,$$

$$I_2 = \int_0^1 S(\alpha)\sum_{p\le X}\sum_{h=0}^{p-1'} v(p,h)\phi_{p,h}(-\alpha)d\alpha$$

$$= \sum_{p\le X}\sum_{h=0}^{p-1''} v^2(p,h)$$

et

$$I_3 = \int_0^1 \left|\sum_{p\le X}\sum_{h=0}^{p-1''} v(p,h)\phi_{p,h}(\alpha)\right|^2 d\alpha.$$

Nous remarquons que, puisque

$$\left(\sum_{h=0}^{p-1''} |v(p,h)|\right)^2 \le p\sum_{h=0}^{p-1''} v^2(p,h),$$

nous avons, par (38), (39) et (40),

$$I_3 < \frac{1}{2}\sum_{p\le X}\sum_{h=0}^{p-1} v^2(p,h) + \frac{1}{2}\sum_{p\le X}\frac{1}{p}\sum_{h=0}^{p-1}\sum_{h'\neq h}|v(p,h)v(p,h')|$$
$$\le \sum_{p\le X}\sum_{h=0}^{p-1'} v^2(p,h).$$

Ces relations, conjointement avec (45), donnent

$$\sum_{p\le X}\sum_{h=0}^{p-1}\nu^2(p,h) \le Z. \tag{46}$$

Nous désignons maintenant par $\lambda(p,h)$ la valeur commune des deux membres de la relation (44). Compte tenu de la forme du membre de droite de cette relation, nous avons [cf. (2)]

$$\lambda(p,h) = p(1+\Delta)\left\{Z(p,h) - \frac{Z}{p}\right\} + (\Delta - \Delta')Z,$$

où

$$\Delta = \frac{1}{Z(p,h)}\sum_{n\in\mathcal{N},(d_{n-h}-1)}$$

et

$$\Delta' = \frac{1}{Z}\sum_{n\in\mathcal{N},(d_{n-h}-1)}.$$

ici Δ est interprété comme valant 0 si $Z(p,h) = 0$. (Le fait que Δ, Δ' dépendent de divers paramètres ne sera pas pertinent pour l'argument qui suit.) Nous remarquons que, par (14) et (31), nous avons $|\Delta| < R^{-1}$ et $|\Delta'| < R^{-1}$, de sorte qu'en particulier,

$$1 + \Delta > \frac{1}{2}, \quad |\Delta - \Delta'| < 2R^{-1}.$$

Il s'ensuit que [en utilisant l'inégalité $(x+y)^2 \le 2(x^2+y^2)$]

$$\begin{aligned} p\left\{Z(p,h) - \frac{Z}{p}\right\}^2 &\le \frac{8}{p}\left\{\lambda^2(p,h) + (2R^{-1}Z)^2\right\} \\ &\le U\nu^2(p,h) + p^{-1}Z^2R^{-2}, \end{aligned} \tag{47}$$

compte tenu de la définition de $\lambda(p,h)$.

En sommant (47), d'abord sur les classes de résidus h modulo p, puis sur les nombres premiers p constituant $\mathcal{P}$, on obtient (10) en utilisant (46) et en rappelant la définition (33) de U. Ceci achève la démonstration du théorème.

Références

1. Ju. V. Linnik, "The large sieve", *Comptes Rendus (Doklady) de l'Académie des Sciences de l'URSS*, 30(1941), 292-294.
2. A. Rényi, "On the representation of even numbers as the sum of a prime and an almost prime number", *Bulletin (Izvestia) de l'URSS, Ser. Math.*, 12 (1948), 57-58. (En russe, mais une traduction de l'Amer. Math. Soc. est disponible : *Selected transl. ser. II vol. 19.*)
3. ————, "On the large sieve of Ju. V. Linnik", *Compositio Math.*, 8 (1950), 68-75.
4. ————, "New version of the probabilistic generalization of the large sieve", *Acta Math. Acad. Sci. Hungar.*, 10 (1959), 217-226. (Cet article contient une liste complète de références, et en particulier des références pour les versions antérieures de l'approche probabiliste de Rényi.)
5. ————, "Probabilistic methods in number theory", *Progress in Math.*, 4 (1958), 465-510. (En chinois.)
6. H. Halberstam et K. F. Roth, "Sequences", Clarendon Press Oxford (en cours de publication) Chapitre IV, § 10.

University College, London.

(Reçu le 3 novembre 1964.)