Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Jean-Marc Deshouillers

Crible de Selberg. Méthodes de la borne inférieure

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 10, n° 2 (1968-1969), exp. n° 14, p. 1-7

<http://www.numdam.org/item?id=SDPP_1968-1969__10_2_A1_0>

Séminaire DELANGE-PISOT
(Théorie des nombres)
10e année, 1968/69, n° 14

24 mars 1969

CRIBLE DE SELBERG
MÉTHODES DE LA BORNE INFÉRIEURE

par Jean-Marc DESHOUILLERS

0. Généralités sur le crible de Selberg.

On se propose de résoudre le problème suivant : Soient $\mathcal{A} = \{a_\nu\}$, $\nu \in (1 , n)$, une famille de n nombres entiers, $\mathcal{P}$ une famille de r nombres premiers $p_1 , \dots , p_r$, et $\mathcal{Q}$ une famille de nombres $^1q_i , \dots , {}^{k_i}q_i$, i variant de 1 à r . Soit $\mathcal{B}$ l'ensemble des éléments a_ν de $\mathcal{A}$, pour lesquels il existe au moins une congruence du type $a_\nu \equiv {}^{\ell}q_i \ [p_i]$; on se propose de calculer le cardinal S de l'ensemble $\mathcal{A} - \mathcal{B}$, ou du moins de l'approcher.

Remarque. - Le problème ainsi posé est une généralisation de l'hypothèse de Goldbach, de l'hypothèse sur les nombres premiers jumeaux, de l'hypothèse de Bouniakowsky, etc.

La méthode introduite par V. BRUN [2] a pour base la propriété suivante de la fonction μ de Möbius :

$$\sum_{d|n} \mu(d) = \begin{cases} 0 , & \text{si } n > 1 , \\ 1 , & \text{si } n = 1 . \end{cases}$$

On définit $\sigma(a_\nu)$ de la manière suivante :

$$\sigma(a_\nu) = \begin{cases} 1 , & \text{si } a_\nu \in \mathcal{A} - \mathcal{B} , \\ \pi p_i , & \text{pour lesquels } \exists\, \ell : a_\nu \equiv {}^{\ell}q_i \ [p_i] , \text{ si } a_\nu \in \mathcal{B} . \end{cases}$$

Soit $s^0(a_\nu) = \sum_{d|\sigma(a_\nu)} \mu(d)$, alors :

$$S = \sum_\nu s^0(a_\nu) = \sum_{d|\pi} \mu(d) \sum_{d|\sigma(a_\nu)} 1_\nu ,$$

où π désigne le produit des éléments de $\mathcal{P}$. BRUN considère les cas où

$$\sum_{d|\sigma(a_\nu)} 1_\nu = \frac{n}{f(d)} + Rd ,$$

avec f multiplicative $(1 < f(p) \leqslant p)$ et $|Rd| \leqslant d/f(d)$, ce qui est assez restrictif, mais vérifié dans les cas énoncés dans la remarque. On arrive alors à la formule fondamentale :

$$(1) \qquad S = n \sum_{d|\pi} \frac{\mu(d)}{f(d)} + \sum_{d|\pi} \mu(d)\, Rd \quad .$$

(Pour plus de détails, on peut se référer à l'exposé de E. BRISSE [1].)

Malheureusement, la formule (1) est de peu d'intérêt car le champ de sommation est trop vaste. Or, si l'on restreint le champ de sommation, il faut pouvoir affirmer que le nouvel S' obtenu est supérieur (ou inférieur) à S, ce qui implique une grande difficulté dans le choix du nouveau domaine.

SELBERG [6] remarque que le choix de la fonction μ n'est pas impératif. Soit, en effet, une fonction λ, définie sur les diviseurs de π, pour laquelle on peut affirmer que

$$(2) \qquad s(a_\nu) = \sum_{d|\sigma(a_\nu)} \lambda(d) \leqslant s^0(a_\nu) \qquad (\text{resp. } \geqslant) \quad .$$

On en déduit $S_\lambda \leqslant S$ (resp. $\geqslant$), où S_λ est l'expression (1) dans laquelle on remplace μ par λ. Pour limiter le champ de sommation, il suffit donc de limiter le support de λ. On prend donc un support $\mathcal{Q}$ aussi simple que possible (par exemple $\mathcal{Q} = \{d \ ; \ (d|\pi) \ , \ (d \leqslant z)\}$), et le problème est alors la détermination de la suite λ.

Or ce problème est dissymétrique : pour la borne supérieure, la méthode de SELBERG donne pratiquement la meilleure expression de λ que l'on puisse espérer, alors que pour la borne inférieure, SELBERG donne différentes méthodes, parmi lesquelles aucune n'est pleinement satisfaisante (cf. SELBERG [7]).

1. Méthode de la borne supérieure.

Soit $\mathcal{Q}$ un ensemble de diviseurs de π [1], et soit

$$\mathcal{Q}^* = \{(d_1 \ , \ d_2) \ ; \ d_1 \ \text{ et } \ d_2 \in \mathcal{Q}\} \quad .$$

On appelle :

$\mathcal{C}(\mathcal{Q}) = \{s$, définies en (2), pour lesquelles support $(\lambda) \subset \mathcal{Q}\}$,
$\mathcal{C}^{(+)}(\mathcal{Q}) = \{s \in \mathcal{C}(\mathcal{Q}) \ ; \ \forall \ \nu : \ s(a_\nu) \geqslant s^0(a_\nu)\}$.

---

[1] Possédant la propriété d'être "clos pour les diviseurs" (i. e. si $d \in \mathcal{Q}$ et si $\delta|d$, alors $\delta \in \mathcal{Q}$).

On a alors les propriétés suivantes :

(i) Si s_1 et s_2 appartiennent à $\mathcal{C}(\mathbb{Q})$, $s_1 . s_2 \in \mathcal{C}(\mathbb{Q}^*)$, car

$$\Big(\sum_{\substack{d_1 \mid \sigma(a_\nu) \\ d_1 \in \mathbb{Q}}} \lambda_1(d_1)\Big)\Big(\sum_{\substack{d_2 \mid \sigma(a_\nu) \\ d_2 \in \mathbb{Q}}} \lambda_2(d_2)\Big) = \sum_{d \in \mathbb{Q}^*} \Big(\sum_{[d_1,d_2]=d} \lambda_1(d_1)\,\lambda_2(d_2)\Big) \quad ;$$

(ii) Si s_1 et s_2 appartiennent à $\mathcal{C}^{(+)}(\mathbb{Q})$, $s_1 . s_2 \in \mathcal{C}^{(+)}(\mathbb{Q}^*)$;

(iii) Si $\lambda(1) = 1$ et si $s \in \mathcal{C}(\mathbb{Q})$, $s^2 \in \mathcal{C}^{(+)}(\mathbb{Q}^*)$.

L'ensemble de telles fonctions sera noté $\mathcal{C}^{(2)}(\mathbb{Q})$.

SELBERG procède alors de la manière suivante : On choisit

$$\mathbb{Q} = \{d \; ; \; (d \mid \pi) \; , \; (d \leqslant z^{1/2})\} \quad ,$$

et on cherche une fonction λ (définie sur $\mathbb{Q}$, et $\lambda_1 = 1$), telle que la quantité $H(\lambda) = \sum_{d \in \mathbb{Q}^*} \frac{\Lambda(d)}{f(d)}$ soit minimale :

$$\Big(\Lambda(d) = \sum_{\substack{[d_1,d_2]=d \\ d_1,d_2 \in \mathbb{Q}}} \lambda(d_1)\,\lambda(d_2)\Big) \quad .$$

Ce choix de la fonction s dans $\mathcal{C}^{(2)}(\mathbb{Q})$, alors que l'on cherchait la borne inférieure pour s dans $\mathcal{C}^{(+)}(\mathbb{Q}^*)$, n'est pas restrictif, ce qui peut se justifier pour des raisons heuristiques, ou, a posteriori par la qualité des résultats obtenus.

Pour déterminer le "inf" de $H(\lambda)$, on considère les valeurs $\lambda(d)$ comme étant indépendantes, et on applique le calcul des variations. On trouve alors (SELBERG [7]), les valeurs des $\lambda(d)$ pour lesquelles le "inf" est atteint, ainsi que la valeur du "inf" : $\Big(\sum_{d \in \mathbb{Q}} \frac{1}{g(d)}\Big)^{-1}$ où g est l'inverse de Möbius de f ,

$$\Big(f(d) = \sum_{\delta \mid d} g(\delta)\Big) \quad .$$

2. Première méthode de la borne inférieure.

Les difficultés, pour la borne inférieure, proviennent du fait que l'on n'a pas réussi à trouver de domaine $\mathbb{Q}$ tel que $\sup_{s \in \mathcal{C}^{(-)}(\mathbb{Q})} H(\lambda)$ soit facilement approximable : les $\mathcal{C}^{(-)}(\mathbb{Q})$, en effet, ne possèdent pas de sous-classes suffisamment riches et maniables pour être comparées à $\mathcal{C}^{(2)}(\mathbb{Q})$ dans le cas de borne supérieure.

La première méthode (cf. SELBERG [7] ou HALBERSTAM et ROTH [3]), consiste à "localiser" le problème pour pouvoir appliquer la méthode de la borne supérieure.

Si l'on appelle $\mathcal{D}$ l'ensemble des diviseurs de π, et $\mathcal{D}^{(i)}$ le sous-ensemble de $\mathcal{D}$ formé par les éléments admettant p_i comme plus grand facteur premier, la fonction criblante $s^{(0)}$ s'écrit :

$$s^{(0)}(a_\nu) = \sum_{d \mid \sigma(a_\nu)} \mu(d) = 1 + \sum_{i=1}^{r} \sum_{\delta}^{(i)} \mu(p_i\, \delta) \quad ,$$

où l'exposant (i) du sigma signifie que l'on somme sur les δ tels que $\delta p_i \in \mathcal{D}^{(i)}$ et $\delta p_i \mid \sigma(a_\nu)$.

En posant $s_i^{(0)}(a_\nu) = \sum_{\delta}^{(i)} [-\mu(p_i\, \delta)]$, on remarque que :

(i) $s_i^{(0)}(a_\nu) = \begin{cases} 1 \text{ , si } p_i \text{ est le plus petit premier diviseur } \sigma(a_\nu) \text{ ,} \\ 0 \text{ , sinon ,} \end{cases}$

(ii) $s^{(0)}(a_\nu) = 1 - \sum_{i=1}^{r} s_i^{(0)}(a_\nu)$.

Soient $\mathcal{C}_i$ l'ensemble des fonctions $s_i(a_\nu) = \sum_{d}^{(i)} \lambda(p_i\, d)$, et $\mathcal{C}_i^{(+)}$ l'ensemble de celles qui satisfont $s_i^{(+)}(a_\nu) \geqslant s_i^{(0)}(a_\nu)$. A toute famille de $(s_i^{(+)})_{i \in (1,r)}$, on fait correspondre la fonction $s^{(-)}$ de $\mathcal{C}^{(-)}$:

$$(3) \qquad s^{(-)}(a_\nu) = 1 - \sum_{i=1}^{r} s_i^{(+)}(a_\nu) \quad .$$

A partir du moment où l'on se restreint à chercher $s^{(-)}$ de cette forme, on peut trouver pratiquement le meilleur s possible, mais la forme (3) est très limitative. On procède alors de la manière suivante : Soit

$$\Omega_i = \{d \; ; \; d \mid \prod_{j=1}^{i-1} p_j \; ; \; d \leqslant (z/p_i)^{1/2}\} \quad ,$$

on cherche la fonction $s_i^{(+)}$ de la forme

$$s_i^{(+)}(a_\nu) = \Big(\sum_{\substack{d \in \Omega_i \\ dp_i \mid \sigma(a_\nu)}} \lambda_d^{(i)} \Big)^2 \quad ,$$

et on applique le calcul des variations comme dans le cas de la borne supérieure. En posant $\mathcal{Q}_i = \sum_{d \in \Omega_i} \frac{1}{g(d)}$, on trouve

$$(4) \qquad S \geqslant n\Big(1 - \sum_{i=1}^{r} \frac{1}{f(p_i)\ \wp_i}\Big) - zK \ ,$$

où K est aisément calculable.

3. Seconde méthode de la borne inférieure.

Elle est fondée sur la remarque suivante, due à SELBERG [7] : Soient $s^{(-)} \in \mathcal{C}^{(-)}$, et λ une application quelconque de $\underset{\sim}{\mathbb{N}}$ dans $\underset{\sim}{\mathbb{R}}$ avec $\lambda(1) = 1$, alors soit

$$s_1(a_\nu) = s^{(-)}(a_\nu)\Big\{\sum_{d \mid \sigma(a_\nu)} \lambda(d)\Big\}^2 , \qquad s_1 \in \mathcal{C}^{(-)} \ .$$

Mais il est difficile d'appliquer ce résultat, car, $s^{(-)}$ étant donnée, on ne sait pas trouver la meilleure suite λ.

On prend en fait la suite λ, trouvée pour la borne supérieure, en justifiant heuristiquement ce choix comme suit :

La suite λ en question donne de bons résultats, car la fonction s associée vaut 1 si $\sigma(a_\nu) = 1$, et est assez proche de 0 si $\sigma(a_\nu) > 1$. On peut donc espérer que la fonction s_1 soit plus intéressante que la fonction $s^{(-)}$, puisque l'on peut réduire $|s^{(-)}(a_\nu)|$ quand $\sigma(a_\nu) > 1$.

L'intérêt essentiel de cette méthode réside dans le fait qu'elle admet une généralisation facile (cf. MIECH [5]). Revenons à la formule (4), et regardons dans un cas particulier (celui de la démonstration du théorème des nombres premiers) la signification du z. Supposons que l'on ait trouvé un résultat non trivial ($S = \varphi(n)$, où $\lim_{n\to\infty} \varphi(n) = +\infty$) en prenant $z = n^{1/3}$. Le résultat prend alors la forme suivante :

- Il existe $\varphi(n)$ nombres compris entre 0 et n n'admettant aucun facteur premier inférieur à $n^{1/3}$.

Il est alors clair que l'on en déduit :

- Il existe $\varphi(n)$ nombres compris entre 0 et n et admettant au plus deux facteurs premiers.

On voit donc que le résultat s'exprime en terme de nombres presque-premiers, et non en terme de nombres premiers.

On peut donc se proposer de déterminer directement le nombre de nombres presque-premiers. Mais alors la fonction $s^{(0)}$ n'a pas une expression maniable ; en revanche on peut déterminer assez facilement une fonction $s^{(-)}$ maniable, mais qui

n'est visiblement pas une "bonne fonction" $s^{(-)}$, et il est donc intéressant d'avoir un procédé pour améliorer la fonction $s^{(-)}$. (Exemple : Si l'on cherche le nombre de nombres presque-premiers d'ordre 2, on peut poser

$$s^{(-)}(n) = 1 - \sum_{\substack{p \mid n \\ p \in \mathcal{P}}} \frac{1}{2} \ .)$$

4. Combinaison de la borne supérieure et de la borne inférieure.

Nous supposerons ici (notations du paragraphe 0) que $k_i = 1$ et ${}^1q_i = 0$. On se donne deux entiers $x < y$. On suppose que $\mathcal{P}$ est l'ensemble des nombres premiers inférieurs à x, et $\mathcal{Q}$ l'ensemble des nombres premiers inférieurs à y. Soit $\psi^{(b)}(x , y)$ le nombre d'éléments a_ν de $\mathcal{A}$ tels que :

(i) a_ν n'a pas de facteur premier $p < y$,

(ii) a_ν possède au plus b facteurs premiers $y \leqslant p < x$;

et soit $\mathcal{S}(\mathcal{A} , \mathcal{P})$ le nombre d'éléments de $\mathcal{A}$ premiers à tous les éléments p de $\mathcal{P}$:

$$\psi^{(b)}(x , y) \geqslant \mathcal{S}(\mathcal{A} , \mathcal{Q}) - \frac{1}{b+1} \sum_{y \leqslant p < x} \mathcal{S}(\mathcal{A}_p , \mathcal{Q}) \ ,$$

où $\mathcal{A}_p = \{a' \ ; \ pa' \in \mathcal{A}\}$.

Il est alors clair que l'on peut déterminer une minoration de $\psi^{(b)}(x , y)$ en combinant les méthodes de bornes inférieures et de bornes supérieures.

Cette méthode, due à P. KÜHN (citée en [4]), a l'avantage de ne faire calculer que la borne inférieure pour $\mathcal{S}(\mathcal{A} , \mathcal{Q})$ où les nombres premiers sont "petits" (comparés à $\mathcal{A}$).

BIBLIOGRAPHIE

[1] BRISSE (Edward). - Estimation supérieure du nombre des nombres premiers contenus dans des progressions arithmétiques par la méthode du crible de Selberg, Séminaire Delange-Pisot : Théorie des nombres, 2e année, 1960/61, n° 5, 20 p.

[2] BRUN (Viggo). - Le crible d'Eratosthène et le théorème de Goldbach, Norske Vidensk. Selsk., Skr., Kristiania, 1920, n° 3, 36 p.

[3] HALBERSTAM (H.) et ROTH (K. F.). - Sequences. Volume I. - Oxford, at The Clarendon Press, 1966.

[4] KÜHN (P.). - Neue Abschätzungen auf Grund der Viggo Brunschen Siebmethode, Tolfte Skandinaviska Matematikerkongressen [12. 1953. Lund], p. 160-168. - Lund, Håkan Ohessons Boktryckeri, 1954.

[5] MIECH (R. J.). - Almost primes generated by a polynomial, Acta Arithm., Warszawa, t. 10, 1964, p. 9-30.

[6] SELBERG (Atle). - On an elementary method in the theory of primes, Norske Vidensk. Selsk., Forhandl., Trondhjem, t. 19, 1947, n° 18, p. 64-67.

[7] SELBERG (Atle). - On elementary methods in primenumber-theory and their limitations, 11te Skandinaviske Matematikerkongress [11. 1949. Trondheim], p. 13-22. - Oslo, A. W. Brøggers Boktrykkeri, 1952.

(Texte remis le 24 mars 1969)

Jean-Marc DESHOUILLERS
24 rue Arnoux
92 - BOURG-la-Reine