Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Bernard Teissier

Crible de Brun

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 7, nº 2 (1965-1966), exp. nº 11, p. 1-13
<http://www.numdam.org/item?id=SDPP_1965-1966__7_2_A1_0>

CRIBLE DE BRUN

par Bernard TEISSIER

1. Préliminaires.

Notre but est d'exposer la méthode suivie par V. BRUN, dans [1], pour obtenir quelques résultats concernant les doublets de nombres premiers et la conjecture de Goldbach.

2. Le crible d'Eratosthène.

Le crible d'Eratosthène est une méthode permettant de déterminer les nombres premiers $\sqrt{a} < p \leqslant a$, connaissant les nombres premiers $2 \leqslant p \leqslant \sqrt{a}$. Cette méthode est fondée sur le fait que, si un nombre $n \leqslant a$ est composé, il a au moins un diviseur premier $p \leqslant \sqrt{a}$. On peut présenter le crible d'Eratosthène sous la forme suivante :

Considérons les progressions arithmétiques :

$$
\begin{array}{ll}
(L_0) & 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad \ldots \quad x \\
(L_1) & 0 \ldots 2 \ldots 4 \ldots 6 \quad \ldots \quad \lambda_1\, 2 \\
(L_2) & 0 \quad \ldots \quad 3 \quad \ldots \quad 6 \quad \ldots \quad \lambda_2\, 3 \\
\vdots & \vdots \\
(L_n) & 0 \quad \ldots \quad p_n \quad \ldots \quad \lambda_n\, p_n \quad \text{ou} \quad p_n \leqslant \sqrt{x} < p_{n+1} \quad .
\end{array}
$$

Chaque progression est telle que son dernier terme soit $\leqslant x$, i. e. $\lambda_i = [\frac{x}{p_i}]$. On voit facilement que les termes de la première ligne, qui sont différents de tous les termes des lignes restantes, sont les nombres premiers $\sqrt{x} < p \leqslant x$ et le nombre 1 .

3. Nombres premiers $\sqrt{x} \leqslant p \leqslant x$.

(A) On se propose de dénombrer les nombres premiers $\sqrt{x} \leqslant p \leqslant x$ ainsi mis en évidence. Pour cela, BRUN commence par généraliser le crible d'Eratosthène sous la forme suivante :

Considérons les progressions arithmétiques :

$$
\begin{array}{llllll}
(L_0) & \Delta & \Delta + D & \cdots & \Delta + \lambda_0 D \\
(L_1) & a_1 & a_1 + p_1 & \cdots & a_1 + \lambda_1 p_1 \\
\vdots & \vdots & \vdots & & \vdots \\
(L_r) & a_r & a_r + p_r & \cdots & a_r + \lambda_r p_r
\end{array}
$$

s'étendant jusqu'à x , i. e. $\lambda_0 = [\frac{x - \Delta}{D}]$; $\lambda_i = [\frac{x - a_i}{p_i}]$, $p_1 , \ldots , p_r$ sont les r premiers nombres premiers, et D , Δ , a_1 , ... , a_r sont des entiers vérifiant :

(i) $\quad 0 < \Delta \leqslant D < x$,

(ii) $\quad 0 < a_i \leqslant p_i < x$,

(iii) $\quad (D , p_i) = 1$ pour tout $1 \leqslant i \leqslant r$.

DÉFINITION 1. – $N(D , x , 2 , \ldots , p_r)$ <u>est le nombre de termes de la première ligne différents de tous les termes des lignes restantes. Ce nombre dépend également de</u> Δ, a_1 , ... , a_r .

DÉFINITION 2. – <u>Un élément de la première ligne est dit barré par l'ensemble de lignes</u> $(L_1 , \ldots , L_n)$, <u>s'il est égal à un élément d'une de ces lignes</u>.

(B) On se propose d'évaluer $N(D , x , 2 , \ldots , p_r)$. Or, on sait évaluer les termes de la forme :

$$N(D , x) = \lambda_0 + 1 \qquad \text{d'où} \qquad N(D , x) = \frac{x}{D} + \theta , \quad -1 \leqslant \theta \leqslant 1 .$$

On peut, pour se ramener au calcul de tels termes, utiliser la formule :

$$(1) \quad N(D, x, 2, \ldots, p_r) = N(D, x, 2, \ldots, p_{r-1}) - N(Dp_r, x, 2, \ldots, p_{r-1}) .$$

<u>Démonstration</u>. – On barre tous les termes communs à la ligne (L_0) et aux r lignes suivantes, et eux seulement ; on barre d'abord les termes communs à (L_0) et aux $r - 1$ lignes suivantes, puis les termes communs à (L_0) et (L_r), différents de tous les termes de $(L_1 , \ldots , L_{r-1})$. Or, d'après un théorème classique, puisque $(D , p_r) = 1$, les termes communs à (L_0) et (L_r) forment une progression arithmétique de même nature que (L_0) ; i. e. :

$$\Delta' \ , \quad \Delta' + Dp_r \ , \quad \ldots \ , \quad \Delta' + \lambda Dp_r \qquad \text{où} \quad \lambda = \left[\frac{x - \Delta'}{Dp_r}\right] \ ,$$

avec $0 < \Delta' \leqslant Dp_r$, et $(Dp_r \ , \ p_i) = 1$ pour tout $1 \leqslant i \leqslant r - 1$.

On a donc :

$$N - N(D, x, 2, \ldots, p_r) = N - N(D, x, 2, \ldots, p_{r-1}) + N(Dp_r, x, 2, \ldots, p_{r-1}) \ ,$$

où N est le nombre d'éléments de la première ligne, d'où (1).

Remarque. - $N(Dp_r \ , \ x \ , \ 2 \ , \ \ldots \ , \ p_{r-1})$ ne se rapporte pas au même crible, puisque, en général, $\Delta' \neq \Delta$. Cependant l'approximation faite à la fin du calcul prend en compte toutes les différences de cette nature, et justifie que nous cessions dès maintenant de faire la distinction.

(C) En écrivant (1) pour les lignes (L_1), $(L_1 \ , \ L_2)$, ..., $(L_1 \ , \ \ldots, \ L_r)$, et en sommant, il vient :

$$(2) \quad N(D \ , \ x \ , \ 2 \ , \ \ldots \ , \ p_r) = N(D \ , \ x) - \sum_{1 \leqslant i_1 \leqslant r} N(Dp_{i_1} \ , \ x \ , \ 2 \ , \ \ldots \ , \ p_{i_1 - 1}) \ .$$

Ces résultats obtenus, BRUN revient au cas qui l'intéresse, i. e. $D = 1$:

$$(2') \quad N(1 \ , \ x \ , \ 2 \ , \ \ldots \ , \ p_r) = N(1 \ , \ x) - \sum_{1 \leqslant i_1 \leqslant r} N(p_{i_1} \ , \ x \ , \ 2 \ , \ \ldots \ , \ p_{i_1 - 1}) \ .$$

Pour faire apparaître des termes de la forme $N(A \ , \ x)$, on peut appliquer (2) à chacun des termes de la somme, puis recommencer sur les termes obtenus, etc. Supposons que la formule obtenue au bout de m telles opérations soit :

$$(3) \quad N(1,x,2,\ldots,p_r) = N(1,x) - \sum_{1 \leqslant i_1 \leqslant r} N(p_i,x) + \sum_{\substack{1 \leqslant i_1 \leqslant r \\ 1 \leqslant i_2 < i_1}} N(p_{i_1},p_{i_2},x) - \sum_{\substack{1 \leqslant i_1 \leqslant r \\ 1 \leqslant i_2 < i_1 \\ 1 \leqslant i_3 < i_2}} N(p_{i_1},p_{i_2},p_{i_3},x) +$$

$$\ldots + (-1)^m \sum_{\substack{1 \leqslant i_1 \leqslant r \\ 1 \leqslant i_2 < i_1 \\ \vdots \\ 1 \leqslant i_m < i_{m-1}}} N(p_{i_1},p_{i_2},\ldots,p_{i_m},x) - (-1)^m \sum_{\substack{1 \leqslant i_1 < r \\ 1 \leqslant i_2 < i_1 \\ \vdots \\ 1 \leqslant i_{m+1} < i_m}} N(p_{i_1},p_{i_2},\ldots,p_{i_{m+1}},x,2,\ldots,p_{i_{m+1}-1})$$

En appliquant (2) à chacun des termes de la dernière somme, on trouve (3) à l'ordre $m + 1$. La formule, étant vraie pour $m = 1$, est vraie pour tout $1 \leqslant m \leqslant r$.

Avec $m = r$, (3) fournit une expression de $N(1 \ , \ x \ , \ 2 \ , \ \ldots \ , \ p_r)$ en fonction de termes de la forme $N(A \ , \ x)$.

Cherchons une approximation de $N(1, x, 2, \dots, p_n)$ à l'aide de (3) : d'après :

(i) $$N(1, x, 2, 3, \dots, p_n) \leqslant N(1, x, 2, 3, \dots, p_r) ,$$

(ii) $$N(A, x, 2, \dots, p_k) \leqslant N(A, x) ,$$

(iii) $$N(A, x) = \frac{x}{A} + \theta , \quad -1 \leqslant \theta \leqslant 1 ,$$

nous obtenons, par exemple pour m pair :

$$(4)\quad N(1,x,2,3,\dots,p_r,\dots,p_n) < x\Big[1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} - \dots - \frac{1}{p_r} + \frac{1}{2.3} + \frac{1}{2.5} + \dots + \frac{1}{p_r\, p_{r-1}} - \frac{1}{5.3.2} - \frac{1}{7.3.2} - \dots - \frac{1}{p_r\, p_{r-1}\, p_{r-2}} + \dots + \frac{1}{p_m\, p_{m-1} \dots 3.2} + \dots + \frac{1}{p_r\, p_{r-1} \dots p_{r-m+1}}\Big] + R$$

où R désigne le nombre de termes à l'intérieur de la parenthèse :

$$R = 1 + r + \binom{r}{2} + \dots + \binom{r}{m} ,$$

m et r vérifiant $m \leqslant r \leqslant n$, n tel que $p_n \leqslant \sqrt{x} < p_{n+1}$.

La forme des approximations faites ne permet pas d'utiliser un procédé analogue pour obtenir une minoration de $N(1, x, 2, \dots, p_r)$.

4. Etude du crible de Brun.

Considérons maintenant le crible :

(L_0)	Δ	$\Delta + D$	$\dots$	$\Delta + \lambda_0\, D$
(L_1)	a_1	$a_1 + 2$	$\dots$	$a_1 + \lambda_1\, 2$
(L_2)	a_2	$a_2 + p_2$	$\dots$	$a_2 + \lambda_2\, p_2$
(L'_2)	a'_2	$a'_2 + p_2$	$\dots$	$a'_2 + \lambda'_2\, p_2$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
(L_r)	a_r	$a_r + p_r$	$\dots$	$a_r + \lambda_r\, p_r$
(L'_r)	a'_r	$a'_r + p'_r$	$\dots$	$a'_r + \lambda'_r\, p_r$,

où $p_1, \dots, p_r$ sont les r premiers nombres premiers, Δ , D , a_i , a'_i sont des entiers vérifiant :

(i) $$0 < \Delta \leqslant D < x ,$$

(ii) $$0 < a_i \leqslant p_i < x ; \quad 0 < a'_i \leqslant p_i < x ,$$

(iii) $$(D , p_i) = 1 \quad \text{pour tout} \quad 1 \leqslant i \leqslant r ,$$

les progressions s'étendant jusqu'à x .

Remarque. - (L'_1) doit se confondre avec (L_1) si l'on ne veut pas barrer tous les termes de (L_0). Il y a donc une ligne exceptionnelle.

(A) Usages de ce crible. - Prenons $r = n$ tel que $p_n \leqslant \sqrt{x} < p_{n+1}$, puis :

(i) Prenons $\Delta = D = 1$, $a_i = p_i$ pour $i = 1 , 2 , \dots , r$, $a'_i = 2$ pour $i = 2 , \dots , r$. On voit facilement que les éléments de la première ligne, différents de tous les termes des autres lignes, sont les nombres premiers $\sqrt{x} + 2 < p \leqslant x$ tels que $p - 2$ soit premier, et le nombre 1 .

(ii) Soit x un nombre pair. Choisissons $\Delta = D = 1$; $a_i = p_i$ et $a'_i \equiv x \pmod{p_i}$. On voit facilement que, si un nombre k de la première ligne est non barré, et n'est pas le nombre 1 :

(a) $$\sqrt{x} < k \leqslant x - \sqrt{x} ,$$

(b) k est premier ,

(c) $$\sqrt{x} < x - k \leqslant x - \sqrt{x} ,$$

(d) $x - k$ est premier .

Le nombre de termes non effacés de la première ligne est donc le nombre de décompositions de x en la somme de deux nombres premiers compris entre $\sqrt{x}$ et $x - \sqrt{x}$ (si l'on distingue les décompositions $x = p_1 + p_2$ et $x = p_2 + p_1$).

Remarque. - Si $p_i | x$, les lignes L_i et L'_i se confondent.

(B) Evaluation du nombre $P(1 , x , 2 , 3 , \dots , p_r)$ de termes non barrés de la première ligne dans le cas où toutes les lignes sont distinctes. - Un raisonnement analogue à celui du § 3 (B) fournit :

(5) $$P(D , x , 2 , 3 , \dots , p_r)$$
$$= P(D, x, 2, \dots, p_{r-1}) - P_{\Delta_1}(Dp_r, x, r, \dots, p_{r-1}) - P_{\Delta_2}(Dp_r, x, 2, \dots, p_{r-1})$$

pour $r > 1$, et pour $r = 1$:

$$P(D , x , 2) = P(D , x) - P(2D , x) .$$

Remarquons que $P(A , x) = N(A , x)$.

De plus, en vertu de la linéarité des équations, pour la même raison qu'en 3 (B) (remarque), nous utiliserons la formule plus simple :

$$(6) \quad P(D , x , 2 , 3 , \dots , p_r) = P(D , x , 2 , 3 , \dots , p_{r-1}) - 2P(Dp_r , x , 2 , \dots , p_{r-1}) \; .$$

Enfin, la recherche d'une minorante étant toujours difficile, on remarque que, si l'on cherche une majorante, et puisque

$$P(D , x , 2 , 3 , \dots , p_r) < P(D , x , 3 , \dots , p_r) \; ,$$

on peut ne pas tenir compte de la première ligne. On obtient, par un calcul analogue à celui du § 3 (C), pour m pair : $m < r < n$,

$$(7) \quad P(1 , x , 2 , \dots , p_2 , \dots , p_n) < P(1 , x , 3 , \dots , p_r)$$

$$< x[1 - \frac{2}{3} - \frac{2}{5} - \dots - \frac{2}{p_r} + \frac{2^2}{5.3} + \frac{2^2}{7.3} + \dots + \frac{2^2}{p_r\, p_{r-1}} - \dots$$

$$+ \frac{2^m}{p_{m+1}\, p_m \dots 5.3} + \dots + \frac{2^m}{p_r\, p_{r-1} \dots p_{r-m+1}}] + R \; ,$$

où $R = 1 + 2r + \binom{r}{2} 2^2 + \dots + 2^m\binom{r}{m}$.

Appelons Σ_i la i-ième fonction symétrique élémentaire de $(\frac{2}{3} , \frac{2}{5} , \dots , \frac{2}{p_r})$; alors :

$$(7') \qquad P(1 , x , \dots , p_r) < x[1 - \Sigma_1 + \Sigma_2 - \dots + \Sigma_m] + R \; ,$$

et une majoration du 2e membre fournira une majoration de

$$P(1 , x , 2 , \dots , p_n) < P(1 , x , 3 , \dots , p_r) \; .$$

Nous pouvons écrire :

$$(8) \qquad 1 - \Sigma_1 + \Sigma_2 - \dots + \Sigma_m - \Sigma_{m+1} + \dots \pm \Sigma_r = \prod_{2\leq i\leq r} (1 - \frac{2}{p_i}) \; ;$$

or :

$$x[1 - \Sigma_1 + \Sigma_2 - \dots + \Sigma_m]$$

$$= x[1 - \Sigma_1 + \Sigma_2 - \dots + \Sigma_m - \dots \pm \Sigma_r] + x[\Sigma_{m+1} - \dots \mp \Sigma_r] \; ,$$

et l'on sait que :

$$\Sigma_1\, \Sigma_{k-1} > k\, \Sigma_k \qquad \text{d'où} \qquad \Sigma_k < \frac{\Sigma_1^k}{k!} \; ,$$

et le second crochet est une suite de termes alternés qui décroissent en valeur absolue si $\Sigma_1 < m$. Donc si $\Sigma_1 < m < r < n$, nous pouvons écrire :

$$P(1 , x , 2 , \ldots , p_n) < x \prod_{2\leq i\leq r} (1 - \frac{2}{p_i}) + x\,\Sigma_{m+1} + R \quad .$$

De plus :

(i) $\prod_{2\leq i\leq r} (1 - \frac{2}{p_i}) < \exp(-\Sigma_1)$, d'après une inégalité classique.

(ii) $\Sigma_{m+1} < \frac{\Sigma_1^{m+1}}{(m+1)!} < (\frac{3\,\Sigma_1}{m+1})^{m+1}$, d'après la formule de Stirling.

(iii) $R < 1 + 2r + (2r)^2 + \ldots + (2r)^m < (2r)^{m+1}$.

D'où :

(9) $P(1 , x , 2 , \ldots , p_n) < x \exp(-\Sigma_1) + x(\frac{3\,\Sigma_1}{m+1})^{m+1} + (2r)^{m+1}$ si $\Sigma_1 \leq m \leq r \leq n$,

et Σ_1 ne dépend que du choix de r .

BRUN choisit r tel que :

$$x^{1/(30 \log\log x)} < 2r < x^{1/(24 \log\log x)} \quad ,$$

et m tel que :

$$12 \log\log x < m < 18 \log\log x \quad ,$$

et l'on a bien alors :

$$\Sigma_1 \leq m \leq r \leq n \qquad \text{pour} \quad x > x_0 \quad .$$

En effet, d'après un résultat classique :

$$\frac{\Sigma_1}{2} + \frac{1}{2} = \log\log p_r + C + o(1) \quad \text{(voir [2])} \qquad \text{où} \quad |C| < \frac{1}{2} \quad ,$$

d'où :

$$\log\log p_r - 1 < \frac{\Sigma_1}{2} < \log\log p_r \qquad \text{pour} \quad x > x_0 \quad .$$

De plus :

$$n = \pi(\sqrt{x}) > A\,\frac{\sqrt{x}}{\log x} \qquad \text{et} \qquad x^{1/(24 \log\log x)} = o(\frac{\sqrt{x}}{\log x}) \quad ,$$

d'où, pour x suffisamment grand :

$$2 \log\log p_r - 2 < \Sigma_1 < 2 \log\log p_r < 12 \log\log x < m < 18 \log\log x$$
$$< \frac{1}{2}\, x^{1/(30 \log\log x)} < r \,, \quad r < \frac{1}{2}\, x^{1/(24 \log\log x)} < n \quad ,$$

et l'on peut majorer

$$x \exp(-\Sigma_1) + x\left(\frac{3\,\Sigma_1}{m+1}\right)^{m+1} + (2r)^{m+1}$$

à l'aide de ces encadrements de m, r, et Σ_1. Il vient :

$$P(1, x, 2, \dots, p_n) < \frac{\exp 2}{(\log p_r)^2}\, x + x\left(\frac{6 \log\log p_r}{12 \log\log x}\right)^{12 \log\log x} + x^{\frac{18 \log\log x}{24 \log\log x}}$$

$$< \frac{8}{(\log 2r)^2}\, x + x\, \frac{1}{1{,}6 \log\log x} + x^{3/4}$$

$$< x\, \frac{7.200}{(\log x)^2}\, (\log\log x)^2 + \frac{x}{(\log x)^6} + x^{3/4} \quad ,$$

d'où finalement, pour une certaine constante K assez grande, $x > x_0$:

$$P(1, x, 2, \dots, p_n) < K\, x\, \frac{(\log\log x)^2}{(\log x)^2} \quad .$$

Pour $x > 3$, soit $Z(x)$ le nombre de nombres premiers jumeaux compris entre 0 et x :

$$Z(x) < \sqrt{x} + P(1, x, 2, \dots, p_n) \quad ,$$

et, puisque $\sqrt{x} = o\left(x\, \frac{(\log\log x)^2}{(\log x)^2}\right)$:

(10) $$Z(x) < A\, x\, \frac{(\log\log x)^2}{(\log x)^2} \quad .$$

Remarque. - E. LANDAU a montré dans [3] que, si l'on fait $m = r = n$ dans (6), le reste R est tellement grand que l'on n'obtient même pas une majoration de la forme $Z(x) < K\, \frac{x}{\log x}$.

Ayant obtenu (10), BRUN peut démontrer le théorème suivant :

Si p_i, p'_i sont tels que $p'_i = p_i + 2$ soit premier, p_i étant premier, s'il y a une infinité de doublets, la série

$$\frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \dots + \frac{1}{p_i} + \frac{1}{p'_i} + \dots$$

est convergente.

Il utilise pour cela le résultat suivant :

Soit E un ensemble d'entiers positifs, et soient

$$\Phi(x) = \sum_{\substack{z\in E\\ z\leqslant x}} 1$$

et n un entier positif quelconque. On a :

$$\sum_{z\in E} [\frac{n}{z}] = \sum_{a=1}^{\infty} \Phi(\frac{n}{a}) \quad .$$

Les deux sommes sont en réalité finies.

Démonstration. - Le nombre de parties entières $[\frac{n}{z}]$, $z \in E$, valant a est $\Phi(\frac{n}{a}) - \Phi(\frac{n}{a+1})$, d'où :

$$\sum_{z\in E} [\frac{n}{z}] = \sum_{a=1}^{\infty} a(\Phi(\frac{n}{a}) - \Phi(\frac{n}{a+1})) = \sum_{a=1}^{\infty} \Phi(\frac{n}{a}) \quad ,$$

ce qui est le résultat annoncé.

On en déduit que, si $\lambda = [\frac{n}{5}]$, et p_μ le plus grand nombre premier $\leqslant n$ appartenant à un doublet :

$$Z(n) + Z(\frac{n}{2}) + \dots + Z(\frac{n}{\lambda}) = [\frac{n}{5}] + [\frac{n}{7}] + \dots + [\frac{n}{p_\mu}]$$

(on laisse 3 de côté pour ne pas faire figurer 5 dans deux doublets). Posant $\varphi(n) = A_n \frac{(\log\log n)^2}{(\log n)^2}$, il vient :

$$\frac{n}{2}[\frac{1}{5} + \frac{1}{7} + \dots + \frac{1}{p_\mu}] < \varphi(n) + \varphi(\frac{n}{2}) + \dots + \varphi(\frac{n}{\lambda}) \quad ;$$

$\varphi(\frac{n}{t})$ étant une fonction décroissante de t , le 2e membre est

$$< \int_1^\lambda \varphi(\frac{n}{t})\,dt < 2A \left[\frac{(\log\log\frac{n}{t})^2 + 2\log\log\frac{n}{t} + 2}{\log\frac{n}{t}} \right]_{t=1}^{t=[\frac{n}{5}]} ,$$

d'où :

$$\frac{1}{5} + \frac{1}{7} + \dots + \frac{1}{p_\mu} < 2A \left[\frac{(\log\log 5)^2 + 2\log\log 5 + 2}{\log 5} - \frac{(\log\log p_\mu)^2 + 2\log\log p_\mu + 2}{\log p_\mu} \right] ,$$

ce qui démontre la convergence.

Remarque. - E. LANDAU a donné une démonstration bien plus rapide dans [3], à partir de $Z(x) < K \frac{x(\log\log x)^2}{(\log x)^2}$.

(C) Le problème de Goldbach. - Il faut remplacer Σ_1 par

$$\Sigma_1' = \Sigma \frac{a(p_i)}{p_i} \qquad \text{où} \quad a(p_i) = \begin{cases} 1 & \text{si } p_i \mid x \\ 2 & \text{si } p_i \nmid x \end{cases} ,$$

d'où $\Sigma_1' < \Sigma_1$.

Soient p_{a_1} , ... , p_{a_ν} les nombres premiers $\leqslant \sqrt{x}$ divisant x ; alors :

$$\Sigma_1' = \Sigma_1 - \left(\frac{1}{p_{a_1}} + \dots + \frac{1}{p_{a_\nu}}\right) > \Sigma_1 - \left(\frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{p_\nu}\right) ,$$

d'où :

$$\Sigma_1' > 2 \log\log p_r - \log\log p_\nu - C .$$

Or $x = p_{a_1}^{\alpha_1} \cdots p_{a_\nu}^{\alpha_\nu} > p_\nu ! > \exp dp_\nu$ pour une certaine constante d (ČEBYŠEV), d'où $p_\nu < \frac{\log x}{d}$, puisque

$$\exp(-\Sigma_1') < \frac{\exp C}{(\log p_r)^2} \log p_\nu ,$$

on trouve facilement que

$$P'(1 , x , 2 , \dots , p_n) < K x \frac{(\log\log x)^3}{(\log x)^2} ,$$

ce qui permet de montrer que, si $G(2x)$ est le nombre de décompositions de $2x$ comme somme de deux nombres premiers,

$$G(2x) = o(\pi(2x)) .$$

Le crible de Brun fournit donc des résultats sur le problème des doublets et la conjecture de Goldbach, mais les résultats importants seraient obtenus par des minorations de $P(1 , x , 2 , \dots , p_n)$ et $P'(1 , x , 2 , \dots , p_n)$.

5. Le crible de Selberg (voir [4] et [5]).

La méthode de SELBERG est plus générale que celle de BRUN, et conduit à des résultats plus précis.

(a) Soit E un ensemble de N entiers positifs. Soit P un ensemble de nombres premiers. On note $\bar{P}$ l'ensemble des nombres entiers positifs dont tous les diviseurs premiers appartiennent à P $(1 \in \bar{P})$.

On se propose d'évaluer le nombre $N(E , P)$ d'éléments de E qui ne sont divisibles par aucun $p \in P$. On voit facilement que :

$$N(E , P) = \sum_{n \in N} \sum_{\substack{d|n \\ d \in \overline{P}}} \mu(d) \quad , \tag{11}$$

puis que :

$$\sum_{n \in N} \sum_{\substack{d|n \\ d \in \overline{P}}} \mu(d) = \sum_{d \in \overline{P}} \mu(d) \sum_{\substack{d|n \\ n \in E}} 1 \quad . \tag{12}$$

(b) On suppose connaître une approximation du nombre des éléments $n \in E$ divisibles par d , de la forme :

$$\sum_{d|n} 1 = \frac{N}{f(d)} + R_d \quad , \tag{13}$$

où $f(d) > 1$ est multiplicative, et où l'on sait majorer $|R_d|$.

Remarque. - D'après la définition de $\mu(a)$, il suffit de considérer les $d \in \overline{P}$ qui sont sans carré, et de supposer f faiblement multiplicative.

D'après (11), (12) et (13),

$$N(E , P) = N \sum_{d \in \overline{P}} \frac{\mu(d)}{f(d)} + \theta \sum_{d \in \overline{P}} |R_d| \qquad \text{où} \quad -1 \leqslant \theta \leqslant 1 \quad . \tag{14}$$

Or

$$\sum_{d \in \overline{P}} \frac{\mu(d)}{f(d)} = \prod_{p \in P} \left(1 - \frac{1}{f(p)}\right) \tag{15}$$

puisque f est multiplicative, d'où :

$$N(E , P) = N \prod_{p \in P} \left(1 - \frac{1}{f(p)}\right) + \theta \sum_{d \in \overline{P}} |R_d| \quad . \tag{16}$$

Mais le plus souvent, sauf si le nombre d'éléments de P est bien plus petit que N , le reste est plus grand que le terme principal.

L'idée de SELBERG est ici de majorer ou de minorer $\sum_{\substack{d|n \\ d \in \overline{P}}} \mu(d)$ par une expression qui permette de réduire le reste.

(c) (i) Soit $(\rho_d)_{d \in \overline{P}}$ un ensemble de nombres réels indexé sur $\overline{P}$, et tel que :

(α) $$\sum_{\substack{d|n \\ d\in\overline{P}}} p_d \geqslant \sum_{\substack{d|n \\ d\in\overline{P}}} \mu(d) \quad ,$$

(β) $$p_1 = 1 \quad ;$$

alors :

(17) $$N(E\ ,\ P) \leqslant N \sum_{d\in\overline{P}} \frac{p_d}{f(d)} + \sum_{d\in\overline{P}} |p_d||R_d| \quad .$$

(ii) Si l'on impose à $(p_d)_{d\in\overline{P}}$:

(α') $$\sum_{\substack{d|n \\ d\in\overline{P}}} p_d \leqslant \sum_{\substack{d|n \\ d\in\overline{P}}} \mu(d)$$

et (β), il vient :

(18) $$N(E\ ,\ P) \geqslant N \sum_{d\in\overline{P}} \frac{p_d}{f(d)} - \sum_{d\in\overline{P}} |p_d||R_d| \quad .$$

On a alors, dans les deux cas à résoudre, un problème d'extremum : Trouver le maximum ou le minimum de $\sum_{d\in\overline{P}} \frac{p_d}{f(d)}$, sous les conditions (α) ou (α') et (β), tout en obtenant un reste assez petit.

Le problème est compliqué. On peut le simplifier en imposant aux p_d des conditions supplémentaires, mais on n'est plus certain alors d'obtenir le meilleur résultat possible.

SELBERG, pour diminuer $\sum |p_d||R_d|$, dans le cas de la recherche d'une majorante, pose $p_d = 0$ pour $d > z$, z étant un nombre à choisir :

$$p_d = \sum_{[d_1,d_2]=d} \lambda_{d_1} \lambda_{d_2} \qquad \text{où} \quad [d_1\ ,\ d_2] = \frac{d_1\ d_2}{(d_1\ ,\ d_2)} \quad ,$$

et $(\lambda_d)_{d\in\overline{P}}$ est une suite de nombres réels satisfaisant

$$\lambda_1 = 1 \quad ,$$

$$\lambda_d = 0 \qquad \text{pour} \quad d > z^{1/2} \quad .$$

On a bien alors :

$$\sum_{d|n} p_d = \{\sum_{d|n} \lambda_d\}^2 \geqslant \sum_{d|n} \mu(d) \quad .$$

Il s'agit alors de trouver le minimum de

$$N \sum_{d_1, d_2 < z^{1/2}} \frac{\lambda_{d_1} \lambda_{d_2}}{f(d_1)\, f(d_2)} f((d_1 , d_2)) \quad ,$$

sous la condition $\lambda_1 = 1$, SELBERG obtient

$$\frac{N}{\displaystyle\sum_{d \leqslant z^{1/2}} \frac{\mu^2(d)}{f'(d)}} \qquad \text{où} \quad f'(d) = f(d) \prod_{p|d} (1 - \frac{1}{f(p)}) \quad ,$$

puis il faut choisir z de façon à obtenir un reste assez petit.

Par cette méthode, SELBERG obtient une bien meilleure majoration que BRUN pour $Z(x)$, en prenant pour E l'ensemble des valeurs du polynôme $x(x + 2)$ pour x entier > 0 plus petit que N , pour P l'ensemble des nombres premiers $p \leqslant (N + 2)^{1/2}$, et $z = N^{1/2-\varepsilon}$, $\varepsilon > 0$ assez petit. SELBERG obtient en effet (voir [4]) :

$$Z(x) < \frac{10{,}6\, x}{(\log x)^2} \qquad \text{pour } x \text{ assez grand} .$$

Mais SELBERG a montré que, pour le problème des doublets et la conjecture de Goldbach, il ne pouvait obtenir que des minorantes négatives.

Cependant, d'autres méthodes, apparentées au crible, plus élaborées ont permis d'obtenir des résultats. En particulier, E. BOMBIERI a obtenu récemment des résultats bien proches de la conjecture de Goldbach.

BIBLIOGRAPHIE

[1] BRUN (Viggo). - La série $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\frac{1}{41}+\frac{1}{43}+\frac{1}{59}+\frac{1}{61}+\cdots$ où les dénominateurs sont "nombres premiers jumeaux" est convergente ou finie, Bull. Sc. math., 2e série, t. 43, 1919, 1re partie, p. 100-104 et 124-128.

[2] HARDY (G. H.) and WRIGHT (E. M.). - An introduction to the theory of numbers, 3rd edition. - Oxford, Clarendon Press, 1954.

[3] LANDAU (Edmund). - Elementary number theory. - New York, Chelsea publishing Company, 1958.

[4] SELBERG (Atle). - On an elementary method in the theory of primes, Norske Vid. Selks. Forh., Trondhjem, t. 19, 1947, n° 18, p. 64-67.

[5] SELBERG (Atle). - The general sieve-method and its place in prime number theory, Proceedings of the international congress of mathematician [1950. Cambridge], vol. 1, p. 282-292. - Providence, American mathematical Society, 1952.