

SÉMINAIRE DELANGE-PISOT-POITOU. THÉORIE DES NOMBRES

EDWARD BRISSE

**Estimation supérieure du nombre des nombres premiers contenus dans
des progressions arithmétiques par la méthode du crible de Selberg**

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 2 (1960-1961), exp. n° 5,
p. 1-20

http://www.numdam.org/item?id=SDPP_1960-1961__2__A5_0

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1960-1961, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

ESTIMATION SUPÉRIEURE DU NOMBRE DES NOMBRES PREMIERS
CONTENUS DANS DES PROGRESSIONS ARITHMÉTIQUES
PAR LA MÉTHODE DU CRIBLE DE SELBERG

par Edward BRISSE

Soient $k_1, \dots, k_N$ des entiers donnés, non nécessairement tous distincts.
Soit $f(k)$ une fonction arbitraire, réelle ou complexe, définie aux points k_i .
Pour tout entier d positif, on définit

$$S_d = \sum_{\substack{1 \leq i \leq N \\ d | k_i}} f(k_i) \quad ,$$

$$S = \sum_{\substack{1 \leq i \leq N \\ k_i = 1}} f(k_i) \quad .$$

LEMME. -

$$S = \sum_d \mu(d) S_d$$

où d est étendu à tous les diviseurs des k_i (autrement $S_d = 0$).

Démonstration. -
$$S = \sum_{\substack{1 \leq i \leq N \\ k_i = 1}} f(k_i) = \sum_{1 \leq i \leq N} f(k_i) \sum_{d | k_i} \mu(d) \quad ,$$

car

$$\sum_{d | k_i} \mu(d) = \begin{cases} 1 & \text{pour } k_i = 1 \\ 0 & \text{autrement} \end{cases} \quad ,$$

D'où

$$S = \sum_d \mu(d) \sum_{\substack{d | k_i \\ 1 \leq i \leq N}} f(k_i) = \sum_d \mu(d) S_d \quad .$$

Soient $n_1, \dots, n_N$ des entiers naturels, distincts ou non, $N > 1$.

Posons

$$(1) \quad \left[\begin{array}{l} S = N(n; p \nmid n, p \leq z) \\ D = \prod_{p \leq z} p \quad (z \geq 2 \text{ sera précisé ultérieurement}) \end{array} \right. .$$

LEMME. -

$$S = \sum_{d|D} \mu(d) S_d$$

Démonstration.

$$(2) \quad S = \sum_{n, (n,D)=1} 1 = \sum_n \sum_{d|(n,D)} \mu(d) = \sum_{d|D} \mu(d) S_d ,$$

cù

$$S_d = \sum_{n, d|n} 1 ,$$

Supposons maintenant que S_d vérifie une relation d'approximation du type

$$(3) \quad S_d = \frac{\omega(d)}{d} N + R_d , \quad |R_d| \leq \omega(d) ,$$

cù $\omega(1) = 1$ et $\omega(m)$ est une fonction multiplicative positive

LEMME.

$$(4) \quad S = N \sum_{d|D} \mu(d) \frac{\omega(d)}{d} + O\left(\sum_{d|D} |R_d|\right) ,$$

$$(5) \quad S = N \prod_{p \leq z} \left(1 - \frac{\omega(p)}{p}\right) + O\left(\sum_{d|D} |R_d|\right) .$$

Démonstration.

(4) résulte immédiatement de (2) et (3) ;

(5) résulte de ce que, $\omega(m)$ étant une fonction multiplicative,

$$\sum_{d|D} \mu(d) \frac{\omega(d)}{d} = \prod_{p \leq z} \left(1 + \mu(p) \frac{\omega(p)}{p}\right) = \prod_{p \leq z} \left(1 - \frac{\omega(p)}{p}\right) .$$

Il convient maintenant de remplacer la fonction de Möbius $\mu(d)$ par une autre fonction ρ_d plus aisément maniable.

ρ_d est telle que :

$$(6) \quad \left[\begin{array}{l} \rho_1 = 1 \\ \sum_{\substack{d|m \\ m>1}} \rho_d \geq 0 \end{array} \right. \quad \text{a lieu pour tous les entiers } m .$$

Alors

$$(7) \quad \sum_{d|m} \rho_d \geq \sum_{d|m} \mu(d) ,$$

et

$$(8) \quad S \leq \sum_n \sum_{d|(n,D)} \rho_d = \sum_{d|D} \rho_d S_d ,$$

d'après (2), (6) et (7), semblablement,

$$S = N \sum_{d|D} \rho_d \frac{\omega(d)}{d} + o\left(\sum_{d|D} |\rho_d R_d|\right) ,$$

d'après (3) et (8).

Ainsi donc, si les λ_d sont des réels quelconques et $\lambda_1 = 1$, on peut poser

$$(9) \quad \sum_{d|m} \rho_d = \left(\sum_{d|m} \lambda_d\right)^2 .$$

La formule (9) admet pour réciproque

$$\rho_d = \sum_{d=[d_1, d_2]} \lambda_{d_1} \lambda_{d_2} .$$

On est donc parvenu à établir la formule ci-dessous,

$$S = N(n ; d \nmid n, 1 \leq d \leq z) \leq \sum_n \left(\sum_{\substack{d|n \\ d \leq z}} \lambda_d \right)^2 ,$$

où les λ_d sont réels, arbitraires, avec $\lambda_1 = 1$.

Dans tout ce qui suit, nous poserons

$$f(d) = \frac{d}{\omega(d)}$$

qui est une fonction multiplicative avec les conditions :

- $1 < f(d) \leq \infty$ pour $d > 1$;
- $f(d) = \infty$ entraîne $\omega(d) = 0$ donc $S_d = 0$;
- $f(1) = 1$.

Alors,

$$(10) \quad S_d = \frac{N}{f(d)} + R_d .$$

THÉOREME. - Pour tout entier r positif, on pose

$$(11) \quad \begin{cases} f_1(r) = \sum_{d|r} \mu(d) f\left(\frac{r}{d}\right) \\ Z = \sum_{r \leq z} \frac{\mu^2(r)}{f_1(r)} \end{cases} .$$

Alors, si S , $f(n)$, R_d , n_1 , ..., n_N sont définis comme précédemment,

$$(12) \quad S \leq \frac{N}{Z} + O\left(\sum_{d_1, d_2 \leq z} |\lambda_{d_1} \lambda_{d_2} R_{[d_1, d_2]}|\right)$$

$$\lambda_d = \frac{\mu(d)}{Z} \prod_{p|d} \left(1 - \frac{1}{f(p)}\right)^{-1} \left(\sum_{\substack{r \leq z \\ (r, d)=1}} \frac{\mu^2(r)}{f_1(r)} \right) .$$

Remarques. - On suppose implicitement $f_1(r) \neq 0$, ce qui est vrai car

$$f_1(r) = f(r) \prod_{p|r} \left(1 - \frac{1}{f(p)}\right) \text{ et } f(d) > 1 .$$

En outre, la valeur de f est parfaitement définie à partir de celle de f_1

$$\begin{aligned}
\sum_{\delta|r} f_1(\delta) &= \sum_{\delta|r} \sum_{d|\delta} \mu(d) f\left(\frac{\delta}{d}\right) \\
&= \sum_{s|r} f(s) \sum_{d|\frac{r}{s}} \mu(d) \\
&= f(r) \quad .
\end{aligned}$$

Enfin, le nombre de termes de O dans (12) est z^2 . Dans (4), il est $2^{\pi(z)} > 2^{cz/\log z}$.

Démonstration. - De (8) et (10), on tire

$$S \leq \sum_{d|D} \rho_d S_d = \sum_{d|D} \left(\sum_{d=[d_1, d_2]} \lambda_{d_1} \lambda_{d_2} \right) \left(\frac{N}{f(d)} + R_d \right) ,$$

soit

$$(13) \quad S \leq \sum_{d \leq z^2} \left(\sum_{\substack{d=[d_1, d_2] \\ d_1, d_2 \leq z}} \lambda_{d_1} \lambda_{d_2} \right) \frac{N}{f(d)} + O\left(\sum_{d_1, d_2 \leq z} |\lambda_{d_1} \lambda_{d_2} R_{[d_1, d_2]}| \right) .$$

De plus, si

$$\begin{aligned}
a &= p_1^{\alpha_1} \dots p_r^{\alpha_r} , \\
b &= p_1^{\beta_1} \dots p_r^{\beta_r} ,
\end{aligned}$$

alors,

$$\begin{aligned}
[a, b] &= p_1^{\min(\alpha_1, \beta_1)} \dots p_r^{\min(\alpha_r, \beta_r)} , \\
(a, b) &= p_1^{\max(\alpha_1, \beta_1)} \dots p_r^{\max(\alpha_r, \beta_r)} ,
\end{aligned}$$

et comme

$$\alpha_i + \beta_i = \min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) ,$$

$$ab = (a, b)[a, b] ;$$

et, pour toute fonction multiplicative,

$$f(a) f(b) = f((a, b)) f([a, b]) \quad .$$

D'après (13) et cette propriété,

$$(14) \quad S \leq N \sum_{d_1, d_2 \leq z} \frac{\lambda_{d_1}}{f(d_1)} \frac{\lambda_{d_2}}{f(d_2)} f((d_1, d_2)) + O\left(\sum_{d_1, d_2 \leq z} |\lambda_{d_1} \lambda_{d_2} R[d_1, d_2]| \right) \\ = NQ + O(R) \quad .$$

Q est une forme quadratique par rapport aux variables λ_d . D'après la formule donnant $f(r)$ en fonction de f_1 ,

$$(15) \quad Q = \sum_{d_1, d_2 \leq z} \frac{\lambda_{d_1}}{f(d_1)} \frac{\lambda_{d_2}}{f(d_2)} \sum_{\substack{r|d_1 \\ d_1|d_2}} f_1(r) \\ = \sum_{r \leq z} f_1(r) \left(\sum_{\substack{r|d \\ d \leq z}} \frac{\lambda(d)}{f(d)} \right)^2 \\ = \sum_{r \leq z} f_1(r) y_r^2 \quad ,$$

où

$$y_r = \sum_{\substack{d \leq z \\ r|d}} \frac{\lambda_d}{f(d)} = \sum_{m \leq z/r} \frac{\lambda_{rm}}{f(rm)} \quad .$$

On cherche maintenant à minimiser Q par la méthode du multiplicateur indéterminé de Lagrange en choisissant convenablement les λ_d , avec $\lambda_1 = 1$.

Il est facile de minimiser Q en faisant intervenir les y_r .

Définissons donc la transformation inverse

$$(16) \quad \frac{\lambda_d}{f(d)} = \sum_{r \leq z/d} \mu(r) y_{rd} \quad .$$

En effet,

$$\sum_{m \leq z/r} \frac{\lambda_{rm}}{f(rm)} = \sum_{m \leq z/r} \sum_{k \leq z/rm} \mu(k) y_{krm} = \sum_{v \leq z/r} y_{rv} \sum_{k|v} \mu(k) = y_r$$

la condition $\lambda_1 = 1$ se traduit par :

$$(17) \quad 1 = \frac{\lambda_1}{f(1)} = \sum_{r \leq z} \mu(r) y_r = F \quad .$$

Nous devons donc rendre extremum la forme

$$Q = \sum_{r \leq z} f_1(r) y_r^2 \quad \text{avec la condition } F = 1 \quad .$$

Pour un multiplicateur indéterminé η ,

$$\frac{\partial Q}{\partial y_r} + \eta \frac{\partial F}{\partial y_r} = 0 \quad (r = 1, \dots, [z]) \quad .$$

L'équation à résoudre admet les solutions :

$$y_1(\eta) , \dots , y_{[z]}(\eta) \quad ,$$

d'où

$$2f_1(r) y_r + \eta \mu(r) = 0 \quad .$$

Comme on a toujours $f_1(r) \neq 0$,

$$(18) \quad y_r(\eta) = -\frac{\eta}{2} \frac{\mu(r)}{f_1(r)} \quad ,$$

et d'après (17),

$$-\frac{\eta}{2} \sum_{r \leq z} \frac{\mu^2(r)}{f_1(r)} = 1 \quad ,$$

On arrive à la valeur de η , qui reportée dans (18) conduit à

$$(19) \quad y_r = \frac{\mu(r)}{f_1(r)} \left(\sum_{s \leq z} \frac{\mu^2(s)}{f_1(s)} \right)^{-1} = \frac{\mu(r)}{Z f_1(r)} \quad .$$

Reportons dans (14) et (15), on trouve la première formule (12).

Il reste à évaluer les λ_d . D'après (16) et (19), on déduit

$$(20) \quad \frac{\lambda_d}{f(d)} = \sum_{r \leq z/d} \frac{\mu(r) \mu(rd)}{zf_1(rd)} = \frac{\mu(d)}{f_1(d)} \frac{1}{z} \sum_{\substack{r \leq z/d \\ (r,d)=1}} \frac{\mu^2(r)}{f_1(r)}.$$

On peut se contenter de limiter la somme aux r et d semi-premiers (quadratifrei) et premiers entre eux. De plus, d'après (11) et la propriété de multiplication des f (r est semi-premier),

$$(21) \quad \begin{aligned} f_1(r) &= \sum_{\delta|r} \mu(\delta) f\left(\frac{r}{\delta}\right) \\ &= f(r) \sum_{\delta|r} \frac{\mu(\delta)}{f(\delta)} \\ &= f(r) \prod_{p|r} \left(1 - \frac{1}{f(p)}\right); \end{aligned}$$

et, pour r et d semi-premiers et premiers entre eux,

$$\begin{aligned} f_1(rd) &= f(rd) \prod_{p|rd} \left(1 - \frac{1}{f(p)}\right) = f(r) f(d) \prod_{p|r} \left(1 - \frac{1}{f(p)}\right) \prod_{p|d} \left(1 - \frac{1}{f(p)}\right) \\ &= f_1(r) f_1(d) \end{aligned}$$

ce qui, reporté dans (20), détermine complètement les valeurs des λ_d . De (21) résulte, pour r semi-premier, $f_1(r) > 0$, et ainsi $f(p) > 1$.

Q est donc définie positive, dans (15).

Comme application, posons

$$f(d) = \frac{d}{\omega(d)}, \quad \omega(1) = 1$$

et pour $d > 1$,

$$1 \leq \omega(d) < d,$$

et cherchons une évaluation générale de Z et R .

Soit (z) l'ensemble des nombres naturels m pour lesquels

$$\prod_{p|m} p \leq z,$$

et soit

$$m = \prod_{p|m} p^m .$$

En particulier, tous les $m \leq z$ appartiennent à (z) .

THÉOREME. -
$$Z = \sum_{m \in (z)} \frac{1}{m} \prod_{p|m} \omega(p)^m ;$$

$$R = \sum_{d_1, d_2 \leq z} |\lambda_{d_1} \lambda_{d_2} R_{[d_1, d_2]}| \leq z^2 \prod_{p \leq z} (1 - \frac{\omega(p)}{p})^{-2} .$$

Démonstration. - D'après (11) et (21),

$$Z = \sum_{r \leq z} \mu^2(r) \frac{\omega(r)}{r} \prod_{p|r} (1 - \frac{\omega(p)}{p})^{-1} ,$$

ou

$$Z = \sum_{r \leq z} \mu^2(r) \prod_{p|m} (\frac{\omega(p)}{p} + \frac{\omega^2(p)}{p^2} + \dots) ,$$

soit

$$Z = \sum_{m \in (z)} \frac{1}{m} \prod_{p|m} \omega(p)^m .$$

D'autre part,

$$|R_{[d_1, d_2]}| \leq \omega([d_1, d_2]) = \frac{\omega(d_1) \omega(d_2)}{\omega((d_1, d_2))} \leq \omega(d_1) \omega(d_2) .$$

D'où

$$R \leq \sum_{d_1, d_2 \leq z} |\lambda_{d_1} \lambda_{d_2} \omega(d_1) \omega(d_2)| = \{ \sum_{d \leq z} |\lambda_d \omega(d)| \}^2 .$$

En remplaçant λ_d par sa valeur tirée de (12), et en observant l'inégalité évidente :

$$0 < \sum_{\substack{r \leq z/d \\ (r,d)=1}} \frac{\mu^2(r)}{f_1(r)} \leq \sum_{r \leq z} \frac{\mu^2(r)}{f_1(r)} = z, \quad ,$$

il vient :

$$\begin{aligned} R &\leq \left\{ \sum_{d \leq z} \mu^2(d) \omega(d) \prod_{p|d} \left(1 - \frac{1}{f(p)}\right)^{-1} \right\}^2 \\ &= \left\{ \sum_{d \leq z} \mu^2(d) \omega(d) \prod_{p|d} \left(1 - \frac{\omega(p)}{p}\right)^{-1} \right\}^2. \end{aligned}$$

Alors,

$$\begin{aligned} \sum_{d \leq z} \mu^2(d) \omega(d) \prod_{p|d} \left(1 - \frac{\omega(p)}{p}\right)^{-1} &= \sum_{d \leq z} d \mu^2(d) \prod_{p|d} \frac{\omega(p)}{p} \left(1 - \frac{\omega(p)}{p}\right)^{-1} \\ &\leq z \sum_{d \leq z} \mu^2(d) \prod_{p|d} \frac{\omega(p)}{p} \left(1 - \frac{\omega(p)}{p}\right)^{-1} \\ &= z \sum_{d \leq z} \mu^2(d) \prod_{p|d} \left(\frac{\omega(p)}{p} + \frac{\omega^2(p)}{p^2} + \dots \right) \\ &= z \sum_{m \in (z)} \prod_{p|m} \left(\frac{\omega(p)}{p} \right)^m p \\ &\leq z \prod_{p \leq z} \left(1 - \frac{\omega(p)}{p}\right)^{-1}. \end{aligned}$$

D'où

$$R \leq z^2 \prod_{p \leq z} \left(1 - \frac{\omega(p)}{p}\right)^{-2}.$$

THÉOREME FONDAMENTAL. — Soient $a_1, \dots, a_s, b_1, \dots, b_s$ des entiers, et, pour $i = 1, \dots, s$, soit $a_i \neq 0$, $(a_i, b_i) = 1$ et non identiquement à la fois, $a_i = \pm a_k$, $b_i = \pm b_k$ pour $i \neq k$.

Soit $\omega(p)$ le nombre de solutions distinctes mod p de

$$(a_1 m + b_1) \dots (a_s m + b_s) \equiv 0 \pmod{p},$$

et l'on suppose $\omega(p) < p$ pour tout p .

Soit finalement

$$E = \prod_{i=1}^s a_i \prod_{1 \leq i < k \leq s} (a_i b_k - a_k b_i).$$

Alors, pour $N \geq 2$,

$$N(m \leq N; a_i m + b_i \text{ premier pour } i = 1, \dots, s) < \frac{C(s)}{\log^s N} N \prod_{p|E} \left(1 - \frac{1}{p}\right)^{\omega(p)-s}$$

où $C(s)$ ne dépend que de s et non de $a_1, \dots, a_s, b_1, \dots, b_s$ et N .

Démonstration. - Soit

$$n = \prod_{1 \leq i \leq s} (a_i m + b_i) \text{ pour } 1 \leq m \leq N,$$

on a toujours $n \neq 0$, sauf pour au plus un nombre fini de valeurs de m . $\omega(d)$ est le nombre de solutions distinctes mod d de

$$\prod_{i=1}^s (a_i m + b_i) \equiv 0 \pmod{d}$$

si $\omega(d) \geq d$,

$$\prod_{i=1}^s (a_i m + b_i) \equiv 0 \pmod{d}, \quad \forall m \text{ entier}.$$

Donc il y a un nombre fini de facteurs premiers dans la suite.

Il est nécessaire de supposer $\omega(d) < d$ pour tout d .

$$\omega(d' d'') = \omega(d') \omega(d'') \text{ si } (d', d'') = 1.$$

Donc, $\omega(d)$ est une fonction multiplicative, $\omega(1) = 1$.

Il est clair que

$$S_d = \sum_{\substack{n \\ d|n \\ n \leq N}} 1 = \frac{\omega(d)}{d} N + R_d, \text{ avec } |R_d| \leq \omega(d).$$

Les conditions étant remplies, il s'ensuit que

$$S = N(m \leq N; p \nmid \prod_{i=1}^s (a_i m + b_i) \text{ pour } p \leq z) < \frac{N}{z} + O(R)$$

où

$$z \geq \sum_{m \leq z} \frac{1}{m} \prod_{p|m} \omega(p)^m ,$$

et

$$|R| \leq z^2 \prod_{p \leq z} \left(1 - \frac{\omega(p)}{p}\right)^{-2} , \quad z \geq 2 .$$

Estimation de Z . Soit s entier naturel positif. Désignons par $d_s(m)$ le nombre de décompositions de m de la forme

$$m = k_1 \dots k_s , \quad 1 \leq k_i \leq m , \quad i = 1 , \dots , s ,$$

où deux décompositions

$$m = k_1' \dots k_s' \quad \text{et} \quad m = k_1'' \dots k_s''$$

sont identiques si et seulement si $k_1' = k_1'' , \dots , k_s' = k_s''$.

En particulier

$$d_1(m) = 1 , \quad \forall \quad m \geq 1$$

$$d_2(m) = d(m) .$$

On doit encore poser

$$d_0(m) = 0 \quad \text{pour} \quad m > 1$$

et

$$d_s(1) = 1 \quad \text{pour} \quad s \geq 0 .$$

Nous allons montrer que $d_s(m)$ est une fonction multiplicative de m et que,
 $\forall \quad s \geq 0 ,$

$$s^\alpha \geq d_s(p^\alpha) , \quad \alpha \text{ entier} \geq 0 .$$

Pour $\alpha = s = 0$, on convient que $s^\alpha = 1$, pour $s \leq 1$, ceci est trivial.

De plus,

$$d_2(p^\alpha) = d(p^\alpha) = 1 + \alpha \leq 2^\alpha .$$

Supposons la relation $d_s(p^\alpha) \leq s^\alpha$ vraie pour $s = 2, \dots, r$.

Alors,

$$d_{r+1}(p^\alpha) = \sum_{0 \leq a \leq \alpha} d_r(p^a) \leq \sum_{a=0}^{\alpha} r^a \leq (r+1)^\alpha ,$$

ce qui démontre la relation pour tout s .

La multiplicativité de $d_s(m)$ résulte de ce fait que si

$$m = m' m'' , \quad (m' , m'') = 1 ,$$

toute décomposition $m = k_1 \dots k_s$ a lieu d'une façon, et d'une seule, sous la forme $m = m' m''$ avec

$$k_i = k_i' k_i'' , \quad i = 1 , \dots , s ,$$

$$(k_i' , k_i'') = 1 , \quad (k_i' , m_i'') = 1 , \quad (k_i'' , m_i') = 1$$

et réciproquement.

On a $\omega(p) = s$ pour tout $p \nmid E$, car toute congruence

$$a_i m + b_i \equiv 0 \pmod{p} , \quad i = 1 , \dots , s$$

a pour $p \nmid E$ juste une solution à cause de $(p , a_i) = 1$.

Pour $i \neq k$, et pour le même m , on n'a pas

$$a_i m + b_i \equiv a_k m + b_k \equiv 0 \pmod{p}$$

car, alors, $p \mid (a_i b_k - a_k b_i)$, et on aurait $p \mid E$, et partout où $i \neq k$, $a_i b_k - a_k b_i \neq 0$, car sinon $a_k b_i = a_i b_k$ entraînerait $a_i = \frac{+}{-} a_k$, $b_i = \frac{+}{-} b_k$ à cause de $a_i \neq 0$ et $(a_i , b_i) = 1$, et ce cas a été exclu.

Pour tout u , on pose

$$u = u^0 \dots u^s \quad \text{où} \quad u = \prod_{p_i | u} p_i^{\alpha_i}$$

et $\frac{k}{u}$ désigne

$$\prod_{\substack{p_i | u \\ \omega(p_i)=k}} p_i^{\alpha_i} \quad .$$

Si pour un k il n'y a aucune valeur de $p_i | u$ telle que $\omega(p) = k$, on pose $\frac{k}{u} = 1$.

Soit encore

$$P_k = \prod_{\substack{p | u \\ \omega(p)=k}} p \quad k = 0, \dots, s-1 \quad .$$

Les P_k sont évidemment des diviseurs de E et

$$(P_k, P_j) = 1 \quad \text{pour} \quad k \neq j \quad .$$

$$\begin{aligned} \sum_{m \leq z} \frac{1}{m} \prod_{p | m} \omega(p)^m &= \sum_{m \leq z} \frac{1}{m} \prod_{k=0}^s \prod_{\substack{p | m \\ \omega(p)=k}} \omega(p)^m \\ &= \sum_{m \leq z} \frac{1}{m} \prod_{k=0}^s \prod_{\substack{p | m \\ \omega(p)=k}} k^m \geq \sum_{m \leq z} \frac{1}{m} \prod_{k=0}^s \prod_{\substack{p | m \\ \omega(p)=k}} d_k(p^\alpha) \\ &= \sum_{m \leq z} \frac{1}{m} \prod_{k=0}^s d_k\left(\frac{k}{m}\right) = \sum_{m \leq z} \frac{1}{m} d_0\left(\frac{0}{m}\right) \dots d_s\left(\frac{s}{m}\right) \quad . \end{aligned}$$

Parce que $d_s(m)$ est multiplicative et $s^\alpha \geq d_s(p^\alpha)$.

Maintenant, on a

$$\sum_{m \leq z} \frac{1}{m} d_0\left(\frac{0}{m}\right) \dots d_s\left(\frac{s}{m}\right) \geq \sum \frac{1}{k_1} \sum \frac{1}{k_2} \dots \sum \frac{1}{k_s} \quad ,$$

où, à droite, la sommation est étendue aux

$$1 \leq k_1, \dots, k_s \leq z^{1/s} \quad ,$$

avec

$$(k_1, P_0) = 1, (k_2, P_0 P_1) = 1, \dots, (k_s, P_0 \dots P_{s-1}) = 1.$$

Car dans le produit $\sum \frac{1}{k_1} \dots \sum \frac{1}{k_s}$, on considère tous les termes en $\frac{1}{m}$ avec $m = k_1 \dots k_s \leq z$.

On écrit

$$\begin{aligned} k_1 &= k_1^1 k_1^2 \dots k_1^s \\ k_2 &= k_2^1 k_2^2 \dots k_2^s \\ &\vdots \\ k_s &= k_s^1 k_s^2 \dots k_s^s. \end{aligned}$$

Alors

$$m = k_1 \dots k_s = k_1^1 (k_1^2 k_2^2) \dots (k_1^s \dots k_s^s) = m^1 \dots m^s,$$

et

$$m^i = k_1^i \dots k_i^i.$$

est une décomposition de m^i . Il y en a

$$d_i(\bar{m}) \quad i = 1, \dots, s.$$

Alors $\sum \frac{1}{k_1} \dots \sum \frac{1}{k_s}$ comprend $\frac{1}{m}$ au plus $d_0(\bar{m}) \dots d_s(\bar{m})$ fois car, si $m = k_1^1 \dots k_s^1 = k_1 \dots k_s$, et si les décompositions sont distinctes, il y a au moins un i pour lequel la décomposition est différente.

$$Z = \sum_{\substack{m \leq z \\ (m, k) = 1}} \frac{1}{m} > C \frac{\varphi(k)}{k} \log z, \quad z \geq 2.$$

En effet, soient $N \geq 2$ et P un ensemble quelconque de premiers $\leq N$. Soit N_P l'ensemble de tous les $n \leq N$ qui ont leurs facteurs premiers hors de P (P comprend toujours 1).

Alors,

$$\prod_{p \in P} \left(1 - \frac{1}{p}\right)^{-1} \leq B \sum_{m \in N_P} \frac{1}{m},$$

où B est une constante positive indépendante de P et N .

Si en effet P est l'ensemble de tous les facteurs premiers $\leq N$

$$\sum_{m \leq N} \frac{1}{m} = \log N + O(1), \quad N \geq 1.$$

Supposons P non vide et l'inégalité démontrée pour $m \in N_P$. Soit q un facteur premier hors de P . Soient P' l'ensemble des facteurs premiers de P privé de q , et $N_{P'}$ l'ensemble correspondant à N_P , éventuellement réduit à 1. On obtient la suite d'inégalités:

$$\prod_{p \in P'} \left(1 - \frac{1}{p}\right)^{-1} = \left(1 - \frac{1}{q}\right) \prod_{p \in P} \left(1 - \frac{1}{p}\right)^{-1}$$

$$\sum_{m \in N_{P'}} \frac{1}{m} = \sum_{m \in N_P} \frac{1}{m} - \sum_{\substack{m \in N_P \\ q|m}} \frac{1}{m}$$

$$\sum_{\substack{m \in N_P \\ q|m}} \frac{1}{m} \leq \sum_{m' \in N_P} \frac{1}{qm'} = \frac{1}{q} \sum_{m' \in N_P} \frac{1}{m'}$$

$$\sum_{m \in N_{P'}} \frac{1}{m} \geq \left(1 - \frac{1}{q}\right) \sum_{m \in N_P} \frac{1}{m},$$

et si,

$$\prod_{p \in P} \left(1 - \frac{1}{p}\right)^{-1} \leq B \sum_{m \in N_P} \frac{1}{m},$$

alors

$$\begin{aligned} \prod_{p \in P'} \left(1 - \frac{1}{p}\right)^{-1} &= \left(1 - \frac{1}{q}\right) \prod_{p \in P} \left(1 - \frac{1}{p}\right)^{-1} \\ &\leq \left(1 - \frac{1}{q}\right) B \sum_{m \in N_P} \frac{1}{m} \leq \sum_{m \in N_{P'}} \frac{1}{m}. \end{aligned}$$

Si P est l'ensemble des entiers non divisibles par k ,

$$\begin{aligned}
 z &\geq \sum_{\substack{m \leq z \\ (m,k)=1}} \frac{1}{m} \geq \frac{1}{B} \prod_{\substack{p \leq z \\ p \nmid k}} \left(1 - \frac{1}{p}\right)^{-1} \geq \frac{\varphi(k)}{Bk} \prod_{p \leq z} \left(1 - \frac{1}{p}\right)^{-1} \\
 &> c \frac{\varphi(k)}{k} \log z, \quad z \geq 2.
 \end{aligned}$$

Pour $z \geq 2^s$,

$$z > c \left(\prod_{i=1}^s \frac{\varphi(p_0 \cdots p_{i-1})}{p_0 \cdots p_{i-1}} \log z^{1/s} \right)$$

où c ne dépend que de s , soit

$$z > c \frac{\varphi^s(p_0) \varphi^{s-1}(p_1) \cdots \varphi(p_{s-1})}{p_0^s p_1^{s-1} \cdots p_{s-1}} \log^s z = c \frac{\log^s z}{k}$$

Estimation de R . - L'inégalité

$$|R| \leq z^2 \prod_{p \leq z} \left(1 - \frac{\omega(p)}{p}\right)^{-2}, \quad z \geq 2,$$

trouvée plus haut, peut se transformer ainsi :

$$|R| \leq cz^2 \prod_{s < p \leq z} \left(1 - \frac{s}{p}\right)^{-2} = O(z^2 \log^{2s} z)$$

où c dépend des nombres premiers $\leq s$ ce qui, reporté dans l'inégalité précédente pour $z \geq 2^s$ donne

$$S < ck \frac{N}{\log^s z} + O(z^2 \log^{2s} z),$$

avec

$$k = \prod_{p|E} \left(1 - \frac{1}{p}\right)^{\omega(p)-s} \geq 1.$$

En effet,

$$\prod_{p \in M} \left(1 - \frac{s}{p}\right)^{-1} < c \prod_{p \in M} \left(1 - \frac{1}{p}\right)^{-s}$$

où s est un entier fixé et M un ensemble infini quelconque de facteurs premiers $> |s|$, où c dépend uniquement de s et non de M .

$$(1 - \frac{1}{p})^s = 1 - \frac{s}{p} + \frac{\delta(s, p)}{p^2}$$

$$\begin{aligned} |\delta(s, p)| &= |(\frac{s}{2}) - \frac{1}{p} (\frac{s}{3}) + \dots| \leq |s|^2 (1 + \frac{|s|}{p} + \frac{|s|^2}{p^2} + \dots) \\ &\leq \frac{|s|^2}{1 - \frac{|s|}{p}} \leq |s|^2 (1 + |s|) = c(s) \end{aligned}$$

à cause de

$$\binom{s}{n} \leq |s|^n \quad \text{et} \quad p \geq |s| + 1$$

D'où

$$\begin{aligned} \prod_{p \in M} (1 - \frac{1}{p})^s (1 - \frac{s}{p})^{-1} &\leq \prod_{p \in M} (1 - \frac{s}{p} + \frac{c(s)}{p^2}) (1 - \frac{s}{p})^{-1} \\ &\leq \prod_{p \in M} (1 + \frac{c(s)(1 + |s|)}{p^2}) \\ &\leq \prod_{n=1}^{\infty} (1 + \frac{c(s)(1 + |s|)}{n^2}) < \infty \end{aligned}$$

Posons

$$z = N^{1/2} \log^{-2s} N$$

Pour $N \geq N_0(s)$, $z \geq 2^s$,

$$c \log N < \log z < \log N,$$

et

$$z^2 \log^{2s} z = O(N \log^{-2s} N)$$

d'où, pour $s \geq 1$,

$$S < ck \frac{N}{\log^s N}, \quad k \geq 1$$

Evidemment

$$S = N(m \leq N, p \nmid \prod_{i=1}^s (a_i m + b_i), p \leq z)$$

$$N(m \leq N, a_i m + b_i \text{ premier pour } i = 1, \dots, s) \\ \leq S + N(m \leq N, \min_{1 \leq i \leq s} |a_i m + b_i| \leq z) \quad .$$

On a

$$N(m \leq N, \min_{1 \leq i \leq s} |a_i m + b_i| \leq z) \\ \leq \sum_{i=1}^s N(m \leq N, |a_i m + b_i| \leq z) \quad ,$$

et pour tout i ,

$$N(m \leq N, |a_i m + b_i| \leq z) \leq \frac{2z}{|a_i|} + 1 = O(z)$$

où la constante devant z dans O est indépendante de a_i et b_i à cause de $|a_i| \geq 1$. D'où suit

$$N(m \leq N; \min_{1 \leq i \leq s} |a_i m + b_i| \leq z) = sO(z) = O(N^{1/2}) \quad .$$

D'où l'énoncé.

Cas particuliers. — Le nombre de facteurs premiers $p \leq N$, tels que $p + 2$ soit premier, est

$$< c \frac{N}{\log^2 N} \quad .$$

d'où $\sum \frac{1}{p} < \infty$ pour tous ces facteurs premiers.

$$N(p \leq x, |p + b| \text{ premier}) < c \frac{x}{\log^2 x} \prod_{p|b} \left(1 - \frac{1}{p}\right)^{-1} \quad .$$

$$N(p \leq N, kp + 1 \text{ premier}) < c \frac{N}{\log^2 N} \prod_{p|k} \left(1 - \frac{1}{p}\right)^{-1} \quad .$$

Le nombre de facteurs premiers p , $1 \leq p \leq N$, tels que $p + b_1, \dots, p + b_s$ soient premiers, avec

$$0 < b_1 < \dots < b_s$$

est

$$< c \frac{N}{\log^{s+1} N} \prod_{p|E} \left(1 - \frac{1}{p}\right)^{\omega(p) - (1+s)}.$$

$$E = \prod_{i=1}^s b_i \prod_{1 \leq i < k \leq s} (b_k - b_i),$$

et $\omega(p)$ est le nombre de solution distinctes mod p de

$$m(m + b_1) \dots (m + b_s) \equiv 0 \pmod{p}.$$

Soit g entier pair positif

$$N(p, g = p + q, q \text{ premier}) < c \frac{g}{\log^2 g} \prod_{p|g} \left(1 + \frac{1}{p}\right).$$

$$N(p_1, \dots, p_k \text{ premiers}, N = p_1 + \dots + p_k) < c \frac{N^{k-1}}{\log^k N}$$

où $c = c(k)$ pour $k \geq 3$.

BIBLIOGRAPHIE

- [1] PRACHAR (Karl). - Primzahlverteilung. - Berlin, Göttingen, Heidelberg, Springer-Verlag, 1957 (Die Grundlehren der mathematischen Wissenschaften, 42).
- [2] SELBERG (Atle). - An elementary proof of the Dirichlet's theorem about primes in an arithmetic progression, Annals of Math., Series 2, t. 50, 1949, p. 297-304.
- [3] SELBERG (Atle). - An elementary proof of the prime number theorem, Annals of Math., Series 2, t. 50, 1949, p. 305-313.
- [4] SELBERG (Atle). - On the normal density of primes in small intervals and the difference between consecutive primes, Arch. Math. Naturvid., t. 47, 1943, p. 87-105.
- [5] SELBERG (Atle). - On an elementary method in the theory of primes, Norske Vid. Selsk. Forh., Trondheim, t. 19, 1947, p. 64-67.
- [6] SELBERG (Atle). - An elementary proof of the prime-number theorem for arithmetic progression, Canadian J. Math., t. 2, 1950, p. 66-78.