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
(Théorie des nombres)
2e année, 1960/61, n° 5

6 et 11 janvier 1961

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

par Edward BRISSE

Soient $k_1 , \ldots , k_N$ 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

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

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

LEMME. - $$S = \sum_d \mu(d)\, S_d$$

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

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

car

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

D'où

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

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

Posons

(1)
$$\begin{cases} S = N(n ; p \nmid n , p \leq z) \\ D = \prod_{p \leq z} p \qquad (z \geqslant 2 \text{ sera précisé ultérieurement}) \end{cases} .$$

LEMME. -
$$S = \sum_{d \mid D} \mu(d)\, S_d .$$

Démonstration.

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

où
$$S_d = \sum_{n, d \mid n} 1 .$$

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

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

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

LEMME.

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

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

Démonstration.

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

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

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

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)
$$\begin{cases} \rho_1 = 1 \\ \sum_{\substack{d|m \\ m>1}} \rho_d \geqslant 0 \quad \text{a lieu pour tous les entiers } m \quad . \end{cases}$$

Alors

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

et

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

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

$$S = N \sum_{d|D} \rho_d\,\frac{\omega(d)}{d} + O\Big(\sum_{d|D} |\rho_d\, R_d|\Big) \quad ,$$

d'après (3) et (8).

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

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

La formule (9) admet pour réciproque

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

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

$$S = N(n\ ;\ d \nmid n\ ,\ 1 \leq d \leq z) \leq \sum_{n} \Big(\sum_{\substack{d \mid n \\ d \leq z}} \lambda_d \Big)^2 \quad ,$$

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,

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

THÉORÈME. - Pour tout entier r positif, on pose

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

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

$$S \leq \frac{N}{Z} + \alpha \Big(\sum_{d_1, d_2 \leq z} |\lambda_{d_1}\ \lambda_{d_2}\ R_{[d_1, d_2]} \Big) \tag{12}$$

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

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

$$f_1(r) = f(r) \prod_{p \mid r} \Big(1 - \frac{1}{f(p)}\Big) \quad \text{et} \quad f(d) > 1 \quad .$$

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

$$\sum_{\delta|r} f_1(\delta) = \sum_{\delta|r} \sum_{d|\delta} \mu(d)\, f\left(\frac{\delta}{d}\right)$$

$$= \sum_{s|r} f(s) \sum_{d|\frac{r}{s}} \mu(d)$$

$$= f(r) \quad .$$

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

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

soit

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

De plus, si

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad ,$$

$$b = p_1^{\beta_1} \cdots p_r^{\beta_r} \quad ,$$

alors,

$$[a\ ,\ b) = p_1^{\min(\alpha_1, \beta_1)} \cdots p_r^{\min(\alpha_r, \beta_r)} \quad ,$$

$$(a\ ,\ b] = p_1^{\max(\alpha_1, \beta_1)} \cdots p_r^{\max(\alpha_r, \beta_r)} \quad ,$$

et comme

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

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

et, pour toute fonction multiplicative,

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

D'après (13) et cette propriété,

$$(14)\quad S \leq N \sum_{d_1, d_2 \leq z} \frac{\lambda_{d_1}}{f(d_1)} \frac{\lambda_{d_2}}{f(d_2)} f((d_1, d_2)) + O\Big(\sum_{d_1, d_2 \leq z} |\lambda_{d_1}\, \lambda_{d_2}\, R_{[d_1, d_2]}| \Big)$$

$$= NQ + O(R) \quad .$$

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

$$(15)\qquad Q = \sum_{d_1, d_2 \leq z} \frac{\lambda_{d_1}}{f(d_1)} \frac{\lambda_{d_2}}{f(d_2)} \sum_{\substack{r \mid d_1 \\ d_1 \mid d_2}} f_1(r)$$

$$= \sum_{r \leq z} f_1(r) \Big(\sum_{\substack{r \mid d \\ d \leq z}} \frac{\lambda(d)}{f(d)} \Big)^2$$

$$= \sum_{r \leq z} f_1(r)\, y_r^2 \quad ,$$

où

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

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

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

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 :

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

Nous devons donc rendre extremum la forme

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

Pour un multiplicateur indéterminé η ,

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

L'équation à résoudre admet les solutions :

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

d'où

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

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

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

et d'après (17),

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

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

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

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

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

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

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

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

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

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 $d > 1$,

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

et cherchons une évaluation générale de Z et R .

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

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

et soit

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

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

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

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

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

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

ou

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

soit

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

D'autre part,

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

D'où

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

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 :

$$R \leq \{ \sum_{d \leq z} \mu^2(d)\, \omega(d) \prod_{p \mid d} (1 - \frac{1}{f(p)})^{-1} \}^2$$

$$= \{ \sum_{d \leq z} \mu^2(d)\, \omega(d) \prod_{p \mid d} (1 - \frac{\omega(p)}{p})^{-1} \}^2 \quad .$$

Alors,

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

$$\leq z \sum_{d \leq z} \mu^2(d) \prod_{p \mid d} \frac{\omega(p)}{p} (1 - \frac{\omega(p)}{p})^{-1}$$

$$= z \sum_{d \leq z} \mu^2(d) \prod_{p \mid d} (\frac{\omega(p)}{p} + \frac{\omega^2(p)}{p^2} + \ldots)$$

$$= z \sum_{m \in (z)} \prod_{p \mid m} (\frac{\omega(p)}{p})^{m_p}$$

$$\leq z \prod_{p \leq z} (1 - \frac{\omega(p)}{p})^{-1} \quad .$$

D'où

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

THÉORÈME FONDAMENTAL. - Soient $a_1 , \ldots , a_s , b_1 , \ldots , b_s$ des entiers, et, pour $i = 1 , \ldots , s$, 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

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

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

Soit finalement

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

Alors, pour $N \geq 2$,

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

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

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

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 $\omega(d) \geq d$,

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

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

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

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

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

Il est clair que

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

Les conditions étant remplies, il s'ensuit que

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

où

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

et

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

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

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

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

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

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

On doit encore poser

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

et

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

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

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

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

De plus,

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

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

Alors,

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

ce qui démontre la relation pour tout s.

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

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

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

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

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

et réciproquement.

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

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

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 $a_k \, b_i = a_i \, b_k$ entrainerait $a_i = \pm a_k$, $b_i = \pm b_k$ à cause de $a_i \neq 0$ et $(a_i \, , \, b_i) = 1$, et ce cas a été exclu.

Pour tout u, on pose

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

et $\overset{k}{u}$ 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 $\overset{k}{u} = 1$.

Soit encore

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

Les P_k sont évidemment des diviseurs de E et

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

$$\sum_{m \leqslant z} \frac{1}{m} \prod_{p | m} \omega(p)^{m_p} = \sum_{m \leqslant z} \frac{1}{m} \prod_{k=0}^{s} \prod_{\substack{\omega(p)=k \\ p | m}} \omega(p)^{m_p}$$

$$= \sum_{m \leqslant z} \frac{1}{m} \prod_{k=0}^{s} \prod_{\substack{\omega(p)=k \\ p | m}} k^{m_p} \geqslant \sum_{m \leqslant z} \frac{1}{m} \prod_{k=0}^{s} \prod_{\substack{\omega(p)=k \\ p | m}} d_k(p^{\alpha})$$

$$= \sum_{m \leqslant z} \frac{1}{m} \prod_{k=0}^{s} d_k(\overset{k}{m}) = \sum_{m \leqslant z} \frac{1}{m} d_0(\overset{0}{m}) \dots d_s(\overset{s}{m}) \quad .$$

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

Maintenant, on a

$$\sum_{m \leqslant z} \frac{1}{m} d_0(\overset{0}{m}) \dots d_s(\overset{s}{m}) \geqslant \sum \frac{1}{k_1} \sum \frac{1}{k_2} \dots \sum \frac{1}{k_s} \quad ,$$

où, à droite, la sommation est étendue aux

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

avec

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

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

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

Alors

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

et

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

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

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

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

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

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,

$$\prod_{p \subset P} (1 - \frac{1}{p})^{-1} \leq B \sum_{m \subset N_P} \frac{1}{m} \quad ,$$

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

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

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

Supposons P non vide et l'inégalité démontrée pour $m \subset N_P$. 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:

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

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

$$\sum_{\substack{m \subset N_P \\ q \mid m}} \leq \sum_{m' \subset N_P} \frac{1}{qm'} = \frac{1}{q} \sum_{m \subset N_P} \frac{1}{m}$$

$$\sum_{m \subset N_{P'}} \frac{1}{m} \geq (1 - \frac{1}{q}) \sum_{m \subset N_P} \frac{1}{m} \quad ,$$

et si,

$$\prod_{p \subset P} (1 - \frac{1}{p})^{-1} \leq B \sum_{m \subset N_P} \frac{1}{m} \quad ,$$

alors

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

$$\leq (1 - \frac{1}{q}) \, B \sum_{m \subset N_P} \frac{1}{m} \leq \sum_{m \subset N_{P'}} \frac{1}{m} \quad .$$

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

$$Z \geqslant \sum_{\substack{m \leqslant z \\ (m,k)=1}} \frac{1}{m} \geqslant \frac{1}{B} \prod_{\substack{p \leqslant z \\ p \nmid k}} (1 - \frac{1}{p})^{-1} \geqslant \frac{\varphi(k)}{Bk} \prod_{p \leqslant z} (1 - \frac{1}{p})^{-1}$$

$$> C \frac{\varphi(k)}{k} \log z \ , \qquad z \geqslant 2 \ .$$

Pour $z \geqslant 2^s$,

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

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

$$|R| \leqslant z^2 \prod_{p \leqslant z} (1 - \frac{\omega(p)}{p})^{-2} \ , \qquad z \geqslant 2 \ ,$$

trouvée plus haut, peut se transformer ainsi :

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

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

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

avec

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

En effet,

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

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 .

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

$$|\delta(s\ ,\ p)| = |\binom{s}{2} - \frac{1}{p}\binom{s}{3} + \ldots| \leqslant |s|^2 \left(1 + \frac{|s|}{p} + \frac{|s|^2}{p^2} + \ldots\right|$$

$$\leqslant \frac{|s|^2}{1 - \frac{|s|}{p}} \leqslant |s|^2 (1 + |s|) = c(s)$$

à cause de

$$\binom{s}{n} \leqslant |s|^n \quad \text{et} \quad p \geqslant |s| + 1 \quad .$$

D'où

$$\prod_{p \subset M} (1 - \frac{1}{p})^s (1 - \frac{s}{p})^{-1} \leqslant \prod_{p \subset M} (1 - \frac{s}{p} + \frac{c(s)}{p^2})(1 - \frac{s}{p})^{-1}$$

$$\leqslant \prod_{p \subset M} (1 + \frac{c(s)(1 + |s|)}{p^2})$$

$$\leqslant \prod_{n=1}^{\infty} (1 + \frac{c(s)(1 + |s|)}{n^2}) < \infty \quad .$$

Posons

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

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

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

et

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

d'où, pour $s \geqslant 1$,

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

Evidemment

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

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

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 ,

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

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

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

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.

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

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

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

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

est

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

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

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

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

Soit g entier pair positif

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

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

où $c = c(k)$ pour $k \geqslant 3$.

BIBLIOGRAPHIE

[1] PRACHAR (Karl). – Primzahlverteilung. – Berlin, Göttingen, Heidelberg, Springer-Verlag, 1957 (Die Grundlehren der mathematischen Wissenchaften, 42).

[2] SELBERG (Atle). – An elémentary 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. Forth., 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.