Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Jean-Marc Deshouillers

Sur la fonction de répartition de certaines fonctions arithmétiques définies sur l'ensemble des nombres premiers moins un

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 11, n° 2 (1969-1970), exp. n° 17, p. 1-13

<http://www.numdam.org/item?id=SDPP_1969-1970__11_2_A2_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
11e année, 1969/70, n° 17, 13 p.

27 avril 1970

SUR LA FONCTION DE RÉPARTITION DE CERTAINES FONCTIONS ARITHMÉTIQUES DÉFINIES SUR L'ENSEMBLE DES NOMBRES PREMIERS MOINS UN

par Jean-Marc DESHOUILLERS

1. Introduction.

I. KÁTAI montre dans ses articles [2] et [3] le résultat suivant :

Soit g une fonction multiplicative à valeurs réelles positives ; posons

$$g^*(n) = \begin{cases} g(n) , & \text{quand } |\log g(n)| \leqslant 1 , \\ 1 , & \text{quand } |\log g(n)| > 1 , \end{cases}$$

et soit $G_N(x) = \frac{1}{\mathrm{li}\ N} \sum_{g(p-1)<x} 1$.

Alors, si les conditions (1), (2), (3), (4) énoncées ci-dessous sont satisfaites, quand N tend vers l'infini, $G_N(x)$ tend vers une limite $G(x)$, G étant une fonction continue (on appellera G la fonction de répartition de la suite $g(p-1)$).

(1) $\sum_p \frac{1 - g^*(p)}{p}$ est convergente ;

(2) $\sum_p \frac{(1 - g^*(p))^2}{p}$ est convergente ;

(3) $\sum_{|\log g(p)|>1} \frac{1}{p}$ est convergente ;

(4) $\sum_{g(p)\neq 1} \frac{1}{p}$ est divergente.

Ce résultat est essentiellement qualitatif, en ce sens qu'il ne nous indique pas pour quels intervalles I on a des "chances non nulles" de trouver des nombres premiers p pour lesquels $g(p-1)$ est dans I , c'est-à-dire sur quels intervalles la fonction G est strictement croissante.

Le but du présent papier est de montrer que, pour une certaine classe de fonctions arithmétiques (plus restreinte que celle considérée par KÁTAI), on peut déterminer exactement les intervalles sur lesquels G croît strictement ; plus précisément, nous nous proposons de montrer (§ 3) le résultat suivant.

THÉORÈME (Théorème 2). - Soit g une fonction multiplicative à valeurs dans l'intervalle $[0 , 1]$, satisfaisant les conditions (A) à (D) suivantes :

(A) $\exists\, p_1$, $\exists\, \alpha > 0$: $1 - \frac{1}{p^\alpha} \leqslant g(p) \leqslant 1$ <u>si</u> $p \geqslant p_1$;

(B) $\exists\, p_2$: $g(p) \geqslant g(p')$ <u>si</u> $p \geqslant p' \geqslant p_2$;

(C) $\sum_p (1 - g(p))$ <u>est divergente</u> ;

(D) $g(2^k) \leqslant g(2)$ <u>si</u> $k \geqslant 1$.

<u>Alors</u>

$$G(x) = \lim_{N\to\infty} \frac{1}{\operatorname{li} N} \sum_{\substack{g(p-1)<x \\ p\leqslant N}} 1$$

<u>existe, est une fonction continue de</u> x , <u>strictement croissante sur l'intervalle</u> $(0 , g(2))$, <u>et en outre</u> $G(g(2)) = 1$.

La démonstration s'effectue de la manière suivante : Pour tout intervalle $I = (\xi - \varepsilon , \xi + \varepsilon) \subset (0 , g(2))$, nous construirons deux nombres a et b tels que

(1.1) $\qquad g(p - 1) \leqslant \xi + \varepsilon$, $\qquad$ si $p \equiv a + 1 \ [a^2 b]$,

(1.2) $\qquad \sum_{\substack{p\leqslant x \\ p\equiv a+1\ [a^2b]}} g(p - 1) > (\xi - \varepsilon) \sum_{\substack{p\leqslant x \\ p\equiv a+1\ [a^2b]}} 1$, dès que x est assez grand .

Par ailleurs, il est aisé de constater que les conditions (A) à (C) impliquent les conditions (1) à (4), ce qui assure l'existence et la continuité de G . Enfin, l'égalité $G(g(2)) = 1$ est triviale, d'après l'hypothèse (D). En effet, si $p \neq 2$, il existe un entier positif k tel que $2^k \| p - 1$. Posons $p - 1 = 2^k . n$. On a $g(p - 1) = g(2^k)\, g(n) \leqslant g(2).1 = g(2)$.

NOTATIONS. - Les lettres p , q (indexées ou accentuées) désignent exclusivement des nombres premiers.

$p^k \| n$ signifie que p^k divise n , et que p^{k+1} ne divise pas n ($p^k | n$ et $p^{k+1} \nmid n$).

(m , n) désigne le p. g. c. d. des deux nombres entiers, et $[m , n]$ désigne leur p. p. c. m.

$\operatorname{li} x = \int_2^x \frac{dt}{\log t}$.

$\omega(n)$ est le nombre de facteurs premiers distincts de n .

$\circledast$ désigne un nombre réel compris entre -1 et $+1$. Sa valeur peut changer d'une ligne à l'autre.

$$E^*(x , d) = \sup_{y \leqslant x} \sup_{(k,d)=1} \left|\pi(y , d , k) - \frac{\mathrm{li}\, y}{\varphi(d)}\right| .$$
$$\pi(x , d) = \sup_{k} \pi(x , d , k) .$$

2. Etude de la somme $\sum g(p - 1)$, lorsque $p \leqslant x$ et $p \equiv a + b \ [a^2 b]$.

Dans tout ce paragraphe, les lettres a et b désigneront deux nombres entiers positifs, tels que :

(i) $2 \| a$,
(ii) $(a , b) = 1$,
(iii) $(a + 1 , b) = 1$,
(iv) a et b sont quadratfrei.

Soit d un nombre entier ; nous conviendrons de noter $d' = \frac{d}{(a , d)}$.

THÉORÈME 1. - Soit g une fonction multiplicative à valeurs dans l'intervalle $[0 , 1]$, satisfaisant la condition (A) du théorème 2 cité dans l'introduction ; alors :

$$\lim_{x \to \infty} \frac{\varphi(a^2 b)}{\mathrm{li}\, x} \sum_{\substack{p \leqslant x \\ p \equiv a+1 \ [a^2 b]}} g(p - 1) = g(a) \prod_{\substack{p \nmid a \\ p \nmid b}} \left(1 + \sum_{k=1}^{\infty} \frac{g(p^k) - g(p^{k-1})}{p^{k-1}(p - 1)}\right) .$$

2.1. - Pour la démonstration du théorème 1, nous aurons à utiliser quelques lemmes que nous groupons ici.

LEMME 1. - Considérons le système de congruences

$$(*) \qquad \begin{cases} p \equiv a + 1 \ [a^2 b] , \\ p \equiv 1 \ [d] . \end{cases}$$

Si $(d' , ab) > 1$, le système est impossible.
Si $(d' , ab) = 1$, il existe un entier u_d premier à abd' , tel que le système $(*)$ soit équivalent à la congruence $(**)$:

$$(**) \qquad p \equiv u_d \ [a^2 bd'] .$$

Supposons qu'il existe un nombre premier q tel que $q | (d' , ab)$, et soit p une solution du système $(*)$; posons $p = \lambda a^2 b + a + 1$.

Soit $q | a$; alors $q^2 | d$, donc $q^2 | p - 1$, et alors $q^2 | a(1 + \lambda ab)$, donc $q^2 | a$, ce qui est contraire à l'hypothèse (iv).

- Soit $q|b$; puisque $q|d'$, $q|d$, donc $q|p-1$, d'où $q|a(1+\lambda ab)$, et donc $q|a$, ce qui est contraire à l'hypothèse (ii).

Supposons maintenant que $(d' , ab) = 1$. On peut alors trouver deux entiers μ et ν , tels que $\nu ab + 1 = \mu d'$. Posons $u_d = \nu a^2 b + a + 1 = \mu a d' + 1$; d'après la condition (iii) et les deux expressions de u_d , on a

$$(u_d , a) = (u_d , b) = (u_d , d') = 1 ,$$

d'où $(u_d , abd') = 1$. Il est maintenant aisé de remarquer que les différents systèmes de congruences suivants sont équivalents :

$$(**) \qquad p \equiv u_d \ [a^2 bd'] ,$$

$$\begin{cases} p \equiv \nu a^2 b + a + 1 \ [a^2 b] , \\ p = \nu a^2 b + a + 1 \ [d'] , \end{cases}$$

car $(d' , a^2 b) = 1$,

$$\begin{cases} p \equiv a + 1 \ [a^2 b] , \\ p \equiv 1 \ [d'] , \end{cases}$$

$$(*) \qquad \begin{cases} p \equiv a + 1 \ [a^2 b] , \\ p \equiv 1 \ [d] , \end{cases}$$

car la première congruence de $(*)$ implique $p \equiv 1 \ [q]$, pour tout q divisant a .

LEMME 2. - Considérons les fonctions multiplicatives ρ et ψ , définies par :

$\psi(p^k) = 1$, si $p|ab$ et $k \geqslant 1$;
$\psi(p^k) = p^{k-1}(p-1)$, si $p \nmid ab$ et $k \geqslant 1$;
$\rho(p^k) = 0$, si $p|b$ et $k > 1$;
$\rho(p) = 1$, si $p|a$;
$\rho(p^k) = 0$, si $p|a$ et $k \geqslant 2$;
$\rho(p^k) = 1$, si $p \nmid a$, $p \nmid b$, et $k \geqslant 1$.

Soit d un nombre entier ; il existe un nombre entier u_d premier à abd' , tel que

$$\sum_{\substack{p \equiv 1 \ [d] \\ p \equiv a+1 \ [a^2 b] \\ p \leqslant x}} 1 = \rho(d) \, \pi(x , a^2 bd' , u_d) = \frac{\rho(d) \, \mathrm{li} \, x}{\psi(d) \, \varphi(a^2 b)} + \theta \rho(d) \, E^*(x , abd') .$$

Si $(d' , ab) = 1$, nous prendrons pour u_d la valeur trouvée dans le lemme 1 ; si $(d' , ab) > 1$, nous choisirons $u_d = 1$. La première égalité provient du fait que $\rho(d) = 0$ si, et seulement si, $(d' , ab) > 1$, et la seconde du fait que $\rho(d)\, \varphi(a^2 bd') = \rho(d)\, \varphi(a^2 b)\, \psi(d)$.

LEMME 3. - Soit d un nombre entier tel que $\rho(d) = 1$.

1° Il existe au plus $M = 2^{\omega(a)}$ nombres entiers positifs δ , tels que $\rho(\delta) = 1$ et $\delta' = d'$.

2° $d \geqslant d' \geqslant d/a$.

3° $$\sum_{y \leqslant d \leqslant z} \rho(d)\, E^*(x , a^2 bd') \leqslant M \sum_{aby \leqslant \delta \leqslant a^2 bz} E^*(x , \delta) .$$

Il suffit de remarquer que, lorsque $\rho(d) = 1$, on peut écrire

$$d = p_1 p_2 \cdots p_m q_1^{v_1} q_2^{v_2} \cdots q_n^{v_n}$$

(expression dans laquelle $p_i \mid a$, $q_j \nmid ab$), et qu'alors

$$d' = q_1^{v_1} \cdots q_n^{v_n} .$$

LEMME 4 (BRUN-TITCHMARSH). - Soit ζ un nombre réel positif ; il existe une constante $c(\zeta)$ telle que, pour tout nombre entier $k \leqslant x^{1-\zeta}$,

$$\pi(x , k) < c(\zeta) \frac{x}{\varphi(k) \log x} .$$

Ce résultat se déduit du théorème 4.1 de K. PRACHAR ([4], p. 44).

LEMME 5 (d'après BOMBIERI). - Soit c un nombre réel positif,

$$\sum_{d \leqslant cx^{1/3}} E^*(x , d) = o(\mathrm{li}\, x) .$$

C'est une conséquence du théorème 4 de E. BOMBIERI ([1], p. 203).

LEMME 6. - Soit λ une fonction multiplicative à valeurs réelles positives, telle que :

1° $\lambda(p) = 1$, pour tout nombre premier p ;

2° $\exists\, \eta$, tel que $0 < \eta < 1/2$, et tel que $\lambda(d) \leqslant d^{\eta}$ pour tout nombre entier d.

Alors on a

$$(6.1) \qquad \sum_{1\leqslant d\leqslant x} \lambda(d) = O(x) \quad ,$$

$$(6.2) \qquad \sum_{1\leqslant d\leqslant x} \frac{\lambda(d)}{d^{\eta}} = O(x^{1-(\eta/2)}) \quad .$$

Commençons par montrer que (6.1) entraîne (6.2).

$$\sum_{1\leqslant d\leqslant x} \lambda(d)/d^{\eta} = \sum_{1\leqslant d\leqslant x^{1/2}} (d)/d^{\eta} + \sum_{x^{1/2}<d\leqslant x} (d)/d^{\eta} \quad ,$$

d'où

$$\sum_{1\leqslant d\leqslant x} \lambda(d)/d^{\eta} \leqslant x^{1/2} + x^{-\eta/2}\, O(x) = O(x^{1-(\eta/2)}) \quad ,$$

car $1 - (\eta/2) > 1/2$.

Démontrons maintenant la relation (6.1). Posons $\lambda(d) = \sum_{\delta|d} \nu(\delta)$; ν est une fonction multiplicative, telle que

$$\nu(p) = \lambda(p) - 1 = 0 \quad , \qquad \text{pour tout nombre premier } p \quad ,$$

$$|\nu(d)| = \prod_{p^k \| d} |\lambda(p^k) - \lambda(p^{k-1})| \leqslant \prod_{p^k \| d} (p^k)^{\eta} = d^{\eta} \quad , \qquad \text{pour tout entier } d \quad .$$

$$\Lambda(x) = \sum_{1\leqslant d\leqslant x} \lambda(d) = \sum_{1\leqslant d\leqslant x} \sum_{\delta|d} \nu(\delta) \quad ,$$

$$|\Lambda(x)| = \Big| \sum_{\delta\leqslant x} \nu(\delta) \sum_{\substack{d\leqslant x \\ \delta|d}} 1 \Big| \leqslant \sum_{\delta\leqslant x} |\nu(\delta)| \frac{2x}{\delta} = 2x \sum_{\delta\leqslant x} \frac{|\nu(\delta)|}{\delta} \quad .$$

La série $\sum_p \frac{|\nu(p^2)|}{p^2}$ est convergente, car la série $\sum_p p^{2\eta}/p^2$ converge, et donc le produit $\prod_p \Big(1 + \sum_{k=2}^{\infty} \frac{|\nu(p^k)|}{p^k}\Big)$ converge vers $\sum_d \frac{|\nu(d)|}{d}$, ce qui entraîne (6.1).

2.2. - Démontrons maintenant le théorème 1.

Il est clair que si la relation (A) est vérifiée pour une certaine valeur α_0 de α, elle est également vérifiée pour toutes les valeurs de α inférieures à α_0. Sans perte de généralité, on peut donc choisir α inférieur à $1/2$; c'est ce que nous ferons dans tout ce paragraphe. Choisissons alors $\zeta = \alpha/4$.

Posons $g(d) = \sum_{n|d} h(n)$; h est une fonction multiplicative, telle que

$$h(p^k) = g(p^k) - g(p^{k-1}) \quad ,$$

$$|h(d)| \leqslant 1 \quad .$$

$$S(x) = \sum_{\substack{p \leqslant x \\ p \equiv a+1 \ [a^2 b]}} g(p-1) = \sum_{\substack{p \leqslant x \\ p \equiv a+1 \ [a^2 b]}} \sum_{d \mid p-1} h(d) = \sum_{d \leqslant x} h(d) \sum_{\substack{p \equiv 1 \ [d] \\ p \equiv a+1 \ [a^2 b] \\ p \leqslant x}} 1 \ ,$$

$$S(x) = \sum_{d \leqslant x} h(d)\ \rho(d)\ \pi(x\ ,\ a^2\ bd'\ ,\ u_d) \ ,$$

d'après le lemme 2. Décomposons $S(x)$ en trois sommes partielles $S_1(x)$, $S_2(x)$, $S_3(x)$, selon que d appartient aux intervalles $[1\ ,\ x^{1/3}[$, $]x^{1/3}\ ,\ x^{1-\zeta}[$, $]x^{1-\zeta}\ ,\ x]$.

$$S_1(x) = \frac{\operatorname{li} x}{\varphi(a^2 b)} \sum_{d \leqslant x^{1/3}} \frac{h(d)\ \rho(d)}{\psi(d)} + \theta \sum_{d \leqslant x^{1/3}} |h(d)|\ \rho(d)\ E^*(x\ ,\ a^2\ bd') \ ,$$

toujours d'après le lemme 2.

$$\sum_{d \leqslant x^{1/3}} \frac{h(d)\ \rho(d)}{\psi(d)} = (1 + o(1)) \prod_p \left(1 + \sum_{k=1}^{\infty} \frac{h(p^k)\ \rho(p^k)}{\psi(p^k)}\right)$$

$$= (1 + o(1))\ g(a) \prod_{p \nmid ab} \left(1 + \sum_{k=1}^{\infty} \frac{g(p^k) - g(p^{k-1})}{p^{k-1}(p-1)}\right) \ .$$

Cette écriture a un sens du fait que les produits infinis convergent, car la série $\sum_p \frac{|g(p) - 1|}{p}$ converge (hypothèse (A)).

$$\left| \sum_{d \leqslant x^{1/3}} |h(d)|\ \rho(d)\ E^*(x\ ,\ a^2\ bd') \right| \leqslant \sum_{d \leqslant x^{1/3}} \rho(d)\ E^*(x\ ,\ a^2\ bd') = o(\operatorname{li} x) \ ,$$

d'après les lemmes 3 et 5.

$$S_2(x) = \sum_{x^{1/3} \leqslant d \leqslant x^{1-\zeta}} \rho(d)\ h(d)\ \pi(x\ ,\ a^2\ bd'\ ,\ u_d) = O\left(\sum_{x^{1/3} \leqslant d \leqslant x^{1-\zeta}} \frac{\rho(d)\,|h(d)|}{\varphi(a^2 b)\ \psi(d)} \operatorname{li} x \right),$$

d'après le lemme 4 et le lemme 2. La série figurant dans le terme O étant convergente (nous venons de le voir), $S_2(x) = o(\operatorname{li} x)$.

Remarquons ensuite que $\pi(x\ ,\ a^2\ bd') \leqslant \frac{x}{a^2\ bd'} + 1$; mais, grâce au lemme 3, $\frac{x}{a^2\ bd'} \leqslant \frac{x}{abd}$; d'où, lorsque $d \leqslant x$, $\pi(x\ ,\ a^2\ bd') \leqslant c\ \frac{x}{d}$, la constante c ne dépendant que de a et b .

$$S_3(x) = \sum_{x^{1-\zeta} \leqslant d \leqslant x} h(d)\ \rho(d)\ \pi(x\ ,\ a^2\ bd'\ ,\ u_d) \ ,$$

$$|S_3(x)| \leqslant cx \sum_{x^{1-\zeta} \leqslant d \leqslant x} \frac{|h(d)|}{d} \leqslant cx^{\zeta} \sum_{1 \leqslant d \leqslant x} |h(d)| \ .$$

Posons $\bar{h}(p) = 1$, $\bar{h}(p^k) = p^{\alpha k} h(p^k)$ si $k > 1$, $\bar{h}(d) = \prod_{p^k \| d} \bar{h}(p^k)$, $\bar{h}$ satisfait les conditions du lemme 6, et donc

$$|S_3(x)| \leqslant cx^{\zeta}\, O(x^{1-(\alpha/2)}) = O(x^{1-(\alpha/4)}) = o(\mathrm{li}\ x) , \qquad \text{car } \zeta = \alpha/4 .$$

Le théorème 1 est ainsi démontré.

3. Démonstration du théorème 2.

Dans tout ce paragraphe, g désigne une fonction multiplicative satisfaisant les conditions (A) à (D) du théorème 2, cité dans l'introduction.

Nous commencerons par montrer, grâce aux lemmes 7 et 8, que l'on peut choisir deux nombres entiers a et b tels que les relations (1.1) et (1.2) soient satisfaites. Nous en déduirons le théorème 2 par le lemme 9.

LEMME 7. - *Soit $\chi(p)$ une suite de nombres réels positifs, décroissante et de limite nulle, telle que la série de terme général $\chi(p)$ soit divergente. Soient u et v deux nombres entiers premiers entre eux.*

La série de terme général $\chi(p)$, où $p \equiv u[v]$, diverge.

Il suffit de constater que l'ensemble des nombres premiers contenus dans une progression arithmétique, possède une densité relative positive par rapport à l'ensemble des nombres premiers (à condition bien sûr qu'il possède au moins deux éléments). On applique alors le lemme plus général suivant.

LEMME 7'. - *Soit $u(n)$ une suite de nombres réels positifs décroissante, de limite nulle, et telle que la série associée diverge ; soit n_1 , ... , n_k , ... une suite de nombres entiers croissante, et telle qu'il existe un entier A pour lequel $n_k \leqslant k.A$, pour tout k ; alors la série de terme général $u(n_k)$ diverge.*

Puisque la suite $u(n)$ est non-croissante,

$$u(n_k) \geqslant u(k.A) ,$$

$$A.u(n_k) \geqslant A.u(k.A) \geqslant u(k.A) + u(k.A + 1) + \ldots + u((k + 1).A - 1) ,$$

$$\sum_{k=1}^{m} u(n_k) \geqslant \frac{1}{A} \sum_{n=A}^{(m+1)A-1} u(n) ;$$

faisons tendre alors m vers l'infini.

LEMME 8. - Soit a_n une suite de nombres réels positifs, de limite nulle, telle que la série associée soit divergente, et soit J un intervalle d'intérieur non vide inclus dans R^+. On peut trouver un nombre impair d'éléments a_i distincts, dont la somme appartient à J.

Il suffit de remarquer que l'ensemble des sommes finies d'éléments de la suite a_n est dense dans R^+.

Considérons le produit infini

$$\prod_p \left(1 + \sum_{k=1}^{\infty} \frac{g(p^k) - g(p^{k-1})}{p^{k-1}(p-1)}\right) .$$

Il converge (nous l'avons vu dans le paragraphe (2.2)).

Chacun de ses facteurs (G_p) est inférieur à l'unité.

En effet,

$$G_p = 1 + \sum_{k=1}^{\infty} \frac{g(p^k) - g(p^{k-1})}{p^{k-1}(p-1)} = 1 - \frac{1}{p-1} + \left(1 - \frac{1}{p}\right) \sum_{k=1}^{\infty} \frac{g(p^k)}{p^k} ,$$

$$G_p \leqslant 1 - \frac{1}{p-1} + \frac{1}{p-1}\left(1 - \frac{1}{p}\right) \sum_{k=1}^{\infty} \frac{1}{p^{k-1}} \leqslant 1 - \frac{1}{p-1} + \frac{1}{p-1} = 1 .$$

On peut donc trouver un nombre p_ε (que nous supposerons supérieur à 3), tel que

$$1 - \frac{\varepsilon}{3} \leqslant \prod_{p>p_\varepsilon} \left(1 + \sum_{k=1}^{\infty} \frac{g(p^k) - g(p^{k-1})}{p^{k-1}(p-1)}\right) \leqslant 1 .$$

Posons alors $b = \prod_{3\leqslant p\leqslant p_\varepsilon} p$. Considérons l'ensemble $\underset{\sim}{Q}$ des nombres premiers congrus à -1 modulo b. D'après les hypothèses (B) et (C) et d'après le lemme 7, le produit $\prod_{q\in Q} g(q)$ diverge vers zéro.

On peut donc trouver, grâce au lemme 8, un nombre impair d'éléments de $\underset{\sim}{Q}$ $(q_1 , q_2 , \cdots , q_{2k+1})$, tels que

$$\xi - \frac{\varepsilon}{3} < g(2) \prod_{i=1}^{2k+1} g(q_i) < \xi + \frac{\varepsilon}{2} .$$

Posons alors $a = 2q_1 q_2 \cdots q_{2k+1}$.

On vérifie alors que a et b satisfont les conditions (i) à (iv) du début du paragraphe 2 ; seule, la condition (iii) n'est pas tout-à-fait évidente : puisque $q_i \equiv -1 \ [b]$, $a = -2 \ [b]$, soit $a + 1 = -1 \ [b]$, d'où $(a + 1 , b) = 1$.

On peut donc appliquer le théorème 1 avec les valeurs a et b ainsi déterminées, et l'on obtient

$$(***) \qquad \xi - \frac{2\varepsilon}{3} < \lim_{x\to\infty} \frac{\varphi(a^2 b)}{\mathrm{li}\, x} \sum_{\substack{p\leqslant x \\ p\equiv a+1\ [a^2 b]}} g(p-1) < \xi + \varepsilon \ ,$$

car

$$1 \geqslant \prod_{p\nmid ab} \left(1 + \sum_{k=1}^{\infty} \frac{g(p^k) - g(p^{k-1})}{p^{k-1}(p-1)}\right) \geqslant \prod_{p>p_\varepsilon} G_p \ .$$

Il ne nous reste plus qu'à montrer un dernier lemme concernant les valeurs moyennes et les densités relatives de suites pour achever la démonstration du théorème 2.

Soient $\mathcal{A}$ une suite d'entiers croissante, $\mathcal{B}$ une sous-suite de $\mathcal{A}$, et f une application de $\mathcal{A}$ dans $[0 , +\infty[$. Notons $\mathcal{S}(\mathcal{A} , n)$ (resp. $\mathcal{S}(\mathcal{A} , n/P)$) l'ensemble des éléments de $\mathcal{A}$ inférieurs ou égaux à n (resp. et possédant la propriété (P)). Posons, en outre,

$$S(\mathcal{A} , n/P) = |\mathcal{S}(\mathcal{A} , n/P)| \ ; \qquad S(\mathcal{A} , n) = |\mathcal{S}(\mathcal{A} , n)| \ ,$$

$$S^f(\mathcal{A} , n/P) = \sum_{a\in\mathcal{S}(\mathcal{A},n/P)} f(a) \qquad \text{et} \qquad S^f(\mathcal{A} , n) = \sum_{a\in\mathcal{S}(\mathcal{A},n)} f(a) \ .$$

LEMME 9. - <u>Supposons que</u> $\mathcal{A}$, $\mathcal{B}$ <u>et</u> f <u>satisfassent les trois conditions suivantes</u> :

(i) $f(\mathcal{B}) \subset [0 , \beta[$;

(ii) $\liminf_{n\to\infty} \dfrac{S^f(\mathcal{B} , n)}{S(\mathcal{B} , n)} \geqslant \gamma > 0$;

(iii) $\liminf_{n\to\infty} \dfrac{S(\mathcal{B} , n)}{S(\mathcal{A} , n)} \geqslant \delta > 0$.

<u>Alors,</u>

$$\forall\ \eta \in [0 , \gamma[\ , \qquad \liminf_{n\to\infty} \frac{S(\mathcal{A} , n/\eta < f(a) < \beta)}{S(\mathcal{A} , n)} \geqslant \delta\, \frac{\gamma - \eta}{\beta - \eta} \ .$$

En effet,

$$\liminf_{n\to\infty} \frac{S(\mathcal{A} , n/\eta < f(a) < \beta)}{S(\mathcal{A} , n)} \geqslant \liminf_{n\to\infty} \frac{S(\mathcal{B} , n/f(b) > \eta)}{S(\mathcal{A} , n)}$$

$$\geqslant \liminf \frac{S(\mathcal{B} , n/f(b) > \eta)}{S(\mathcal{B} , n)} \frac{S(\mathcal{B} , n)}{S(\mathcal{A} , n)}$$

$$\geqslant \delta \liminf \frac{S(\mathcal{B} , n/f(b) > \eta)}{S(\mathcal{B} , n)} \ .$$

Montrons, en raisonnant par l'absurde, que

$$\liminf_{n\to\infty} \frac{S(\mathcal{B}\ ,\ n/f(b) > \eta)}{S(\mathcal{B}\ ,\ n)} \geqslant \frac{\gamma - \eta}{\beta - \eta} \quad .$$

S'il n'en est pas ainsi, il existe un nombre réel ε' positif, et une suite d'entiers n_i , pour lesquels

$$\frac{S(\mathcal{B}\ ,\ n_i/f(b) > \eta)}{S(\mathcal{B}\ ,\ n_i)} < \frac{\gamma - \eta}{\beta - \eta} - \varepsilon' \quad .$$

Mais

$$S^f(\mathcal{B}\ ,\ n_i) = S^f(\mathcal{B}\ ,\ n_i/f(b) \leqslant \eta) + S^f(\mathcal{B}\ ,\ n_i/f(b) > \eta)$$

$$\leqslant \eta . S(\mathcal{B}\ ,\ n_i/f(b) \leqslant \eta) + \beta . S(\mathcal{B}\ ,\ n_i/f(b) > \eta) \quad ,$$

et du fait que $S(\mathcal{B}\ ,\ n_i) = S(\mathcal{B}\ ,\ n_i/f(b) \leqslant \eta) + S(\mathcal{B}\ ,\ n_i/f(b) > \eta)$,

$$\frac{S^f(\mathcal{B}\ ,\ n_i)}{S(\mathcal{B}\ ,\ n_i)} \leqslant (\beta - \eta) \frac{S(\mathcal{B}\ ,\ n_i/f(b) > \eta)}{S(\mathcal{B}\ ,\ n_i)} + \eta < \gamma - \varepsilon' \quad ,$$

ce qui contredit l'hypothèse (ii).

Appliquons le lemme 9, lorsque :

$\mathcal{A} = \{p \mid p \text{ premier}\}$,

$\mathcal{B} = \{p \mid p \equiv a + 1 \ [a^2 b]\}$,

$f(p) = g(p - 1)$,

$\beta = \xi + \varepsilon$,

car $g(p - 1) \leqslant g(a)$, puisque $q \mid a$ entraîne $q \| p - 1$,

$\gamma = \xi - \frac{2\varepsilon}{3}$, par la formule (***),

$\delta = \frac{1}{\varphi(a^2 b)}$, par le théorème des nombres premiers dans les progressions arithmétiques.

Prenons alors $\eta = \xi - \varepsilon$; on obtient

$$\liminf_{x\to\infty} \frac{1}{\operatorname{li} x} \sum_{\substack{p\leqslant x \\ \xi-\varepsilon\leqslant g(p-1)\leqslant\xi+\varepsilon}} 1 > 0 \quad .$$

4. Quelques compléments.

4.1. - Les fonctions $\frac{\varphi(n)}{n}$, $\frac{n}{\sigma(n)}$ satisfont les conditions (A) à (D) du théorème 2.

L'ensemble des nombres premiers satisfaisant $\frac{\varphi(p-1)}{p-1} > \frac{1}{3}$, admet donc une densité positive par rapport à l'ensemble des nombres premiers (on peut montrer qu'elle est comprise entre 1/3 et 1/2). Ce résultat est intéressant si on le compare à celui obtenu par E. VEGH :

Si un nombre premier p est tel que $\frac{\varphi(p-1)}{p-1} > \frac{1}{3}$, il admet au moins une paire de racines primitives consécutives.

Remarquons, pour clore cette partie, que A. BRAUER a conjecturé que tout nombre premier assez grand possède cette dernière propriété.

L'ensemble des nombres premiers p satisfaisant $\frac{p-1}{\sigma(p-1)} > \frac{1}{2}$ (resp. $< \frac{1}{2}$), c'est-à-dire tels que $p-1$ soit déficient (resp. abondant), admet une densité relative positive par rapport à l'ensemble des nombres premiers.

4.2. - On peut supprimer l'hypothèse (D), et montrer le théorème suivant.

THÉORÈME 2'. - Soit g une fonction multiplicative à valeurs dans l'intervalle $[0\ ,\ 1]$, satisfaisant les conditions (A) à (C). Alors $G(x)$ croît strictement sur l'intervalle $[0\ ,\ \sup_{k\geq 1} g(2^k))$, et en outre $G(\sup_{k\geq 1} g(2^k)) = 1$.

Pour montrer ce résultat, on reprend le second paragraphe en remplaçant la condition (i) par la condition (i') :

(i') $2^k \| a$,

et la condition (iv) par la condition (iv') :

(iv') $\frac{a}{2^k}$ et b sont quadratfrei,

ce qui ne présente pas de difficulté. Le point un peu plus délicat est le choix de a et b.

On choisit d'abord un intervalle $I = [\xi - \varepsilon\ ,\ \xi + \varepsilon) \subset [0\ ,\ \sup_{k\geq 1} g(2^k))$, et on suppose (quitte à le restreindre, ce qui est possible) qu'il vérifie la condition supplémentaire $I \subset [0\ ,\ g(2^k))$ pour un certain k.

On choisit alors b de la même manière que précédemment ; on considère l'ensemble $\mathcal{Q}$ des nombres premiers congrus à 2 modulo b, et l'on en choisit un nombre congru à $-k$ modulo $\varphi(b)$, de telle sorte que

$$\xi - \frac{\varepsilon}{3} < g(2^k)\ g(q_1 \cdots q_{\lambda\varphi(b)-k}) < \xi + \frac{\varepsilon}{3} ,$$

ce qui est possible en utilisant le lemme 7 et une version modifiée du lemme 8. La relation $(a+1\ ,\ b) = 1$ provient du fait que

$$2^k q_1 \cdots q_{\lambda\varphi(b)-k} + 1 \equiv 2^{\lambda\varphi(b)} + 1 \equiv 2 \ [b] \ ,$$

en utilisant le théorème de Fermat généralisé.

4.3. - Il est raisonnable de conjecturer que la conclusion du théorème 2 demeure, si on remplace la condition (A) par la condition (A') plus faible :

(A') La série $\sum_p \frac{1 - g(p)}{p}$ est convergente.

4.4. - Il semble sans espoir d'essayer de déterminer exactement la fonction G, même dans certains cas particuliers.

4.5. - On peut trouver des analogues aux théorèmes 2 et 2', quand g est une fonction multiplicative (resp. additive) à valeurs supérieures à l'unité (resp. positives ; ou négatives), en modifiant en conséquence les hypothèses (A) à (D).

4.6. - Soit g une fonction multiplicative à valeurs positives, telle que $G(x)$ existe et soit continue, et soit I un intervalle de R.

CONJECTURE.

$$G \text{ croît strictement sur } I \iff I \subset \overline{\{g(p-1)\}} \ ,$$

$\overline{\{g(p-1)\}}$ désignant l'adhérence de l'ensemble des nombres $g(p-1)$.

BIBLIOGRAPHIE

[1] BOMBIERI (E.). - On the large sieve, Mathematika, London, t. 12, 1965, p. 201-225.

[2] KATAI (I.). - On distribution of arithmetical functions on the set prime plus one, Compositio mathematica, Groningen, t. 19, 1968, p. 278-289.

[3] KATAI (I.). - On the distribution of arithmetical functions, Acta Math. Acad. scient. Hungaricae, t. 20, 1969, p. 69-87.

[4] PRACHAR (K.). - Primzahlverteilung. - Berlin, Springer-Verlag, 1957 (Grundlehren der mathematischen Wissenschaften, 91).

(Texte reçu le 25 mai 1970)

Jean-Marc DESHOUILLERS
Centre de Mathématiques
Ecole Polytechnique
17 rue Descartes
75 - PARIS 05