SÉMINAIRE DE THÉORIE DES NOMBRES DE BORDEAUX

JEAN-MARC DESHOUILLERS

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

Séminaire de théorie des nombres de Bordeaux (1969-1970), exp. nº 12, p. 1-16
<http://www.numdam.org/item?id=STNB_1969-1970____A12_0>

SUR LA FONCTION DE REPARTITION DE CERTAINES FONCTIONS ARITHMETIQUES DEFINIES SUR L'ENSEMBLE DES NOMBRES PREMIERS MOINS UN

par

Jean-Marc DESHOUILLERS

-:-:-:-

§ 1. - INTRODUCTION

I. Katai montre en [2] le résultat suivant :

Soit g une fonction multiplicative à valeurs réelles positives ; posons

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

et soit

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

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. $\sum_{|\text{Log } g(p)|>1} \frac{1}{p}$ 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 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 I. Katai), on peut déterminer exactement les intervalles sur lesquels G croît strictement ; plus précisément nous nous proposons de montrer le

THEOREME 2. <u>Soit</u> g <u>une fonction multiplicative à valeurs dans l'intervalle</u> $[0,1]$, <u>satisfaisant les conditions</u> A <u>à</u> D <u>suivantes</u> :

A. $\exists p_1,\ \exists \alpha > 0 : 1 - \frac{1}{p^\alpha} \leq g(p) < 1$ si $p \geq p_1$

B. $\exists\, p_2 : g(p) \geq g(p')$ si $p \geq p' \geq p_2$

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

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

<u>Alors</u>

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

<u>existe</u>, <u>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 :

(*) voir également les résultats analogues énoncés aux paragraphes 4.2 et 4.5.

(1.1) $\quad g(p-1) \leq \xi+\varepsilon \quad$ si $\; p \equiv a+1\ [a^2b]$

(1.2) $\quad \sum\limits_{\substack{p\leq x \\ p\equiv a+1[a^2b]}} g(p-1) > (\xi-\varepsilon) \sum\limits_{\substack{p\leq x \\ p\equiv a+1[a^2b]}} 1$, 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 .

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 $k^{k+1} \nmid n$) .

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

. $\mathrm{li}\, x = \int_2^x \frac{dt}{\mathrm{Log}\, t}$.

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

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

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

. $\pi(x, d) = \sup\limits_{k} \pi(x, d, k)$.

. $\pi(x, d, k)$ désigne le nombre de nombres premiers inférieurs ou égaux à x et congrus à k modulo d .

§.2. - ETUDE DE LA SOMME $g(p-1)$, LORSQUE $p \leq x$ ET $p \equiv a+1\ [a^2b]$

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

<u>i/</u> $2 \| a$

<u>ii/</u> $(a, b) = 1$

<u>iii/</u> $(a+1, b) = 1$

<u>iv/</u> a et b sont quadratfrei.

Soit d un nombre entier ; nous conviendrons de noter :

$$d' = \frac{d}{(a, d)} .$$

THEOREME 1. <u>Soit</u> g <u>une fonction multiplicative à valeurs dans l'intervalle</u> $[0, 1]$ <u>satisfaisant la condition</u> A (cf. p. 2) ; <u>alors</u> :

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

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

LEMME 1. <u>Considérons le système de congruences</u>

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

. <u>Si</u> $(d', ab) > 1$, <u>le système est impossible.</u>

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

$$(**) \qquad p \equiv u_d \, [abd'] .$$

. 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 <u>iv/</u>.

- 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 <u>ii/</u>.

. 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 <u>iii/</u> et les deux expressions de u_d, il est facile de voir que

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

d'où $\quad (u_d, abd') = 1$.

Il est maintenant aisé de remarquer que les différents systèmes de congruences suivants sont équivalents :

$$(**) \quad \left\{ p \equiv u_d \quad [a^2 b d'] \right.$$

$$\begin{cases} p \equiv \nu a^2 b + a + 1 & [a^2 b] \\ p = \nu a^2 b + a + 1 & [d'] \end{cases} \qquad \text{car } (d', a^2 b) = 1$$

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

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

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

LEMME 2. <u>Considérons les fonctions multiplicatives</u> ρ <u>et</u> ψ <u>définies par</u> :

$\psi(p^k) = 1$ <u>si</u> $p \mid ab$ <u>et</u> $k \geq 1$; $\psi(p^k) = p^{k-1}(p-1)$ <u>si</u> $p \nmid ab$ <u>et</u> $k \geq 1$;

$\rho(2) = 1$; $\rho(2^k) = 0$ <u>si</u> $k \geq 2$; $\rho(p^k) = 0$ <u>si</u> $p \mid b$ <u>et</u> $k > 1$;

$\rho(p) = 1$ <u>si</u> $p \mid a$; $\rho(p^k) = 0$ <u>si</u> $p \mid a$ <u>et</u> $k \geq 2$

$\rho(p^k) = 1$ <u>si</u> $p \nmid a$, $p \nmid b$, <u>et</u> $k \geq 1$.

<u>Soit</u> d <u>un nombre entier</u> ; <u>il existe un nombre entier</u> u_d <u>premier à</u> abd' <u>tel que</u> :

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

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 $\rho(d)\,\varphi(a^2db') = \rho(d)\,\varphi(a^2b)\,\psi(d)$.

LEMME 3. <u>Soit</u> d <u>un nombre entier tel que</u> $\rho(d) = 1$.

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

2) $d \geq d' \geq d/a$.

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

Il suffit de remarquer que, lorsque $\rho(d) = 1$, on peut écrire $d = p_1 p_2 \ldots p_m q_1^{v_1} q_2^{v_2} \ldots q_n^{v_n}$, expression dans laquelle $p_i | a$, $q_j \nmid ab)$, et qu'alors $d' = q_1^{v_1} \ldots q_n^{v_n}$.

LEMME 4 (Brun-Titchmarsh). <u>Soit</u> ζ <u>un nombre réel positif</u> ; <u>il existe une constante</u> $c(\zeta)$ <u>telle que pour tout nombre entier</u> $k \leq x^{1-\zeta}$:

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

Ce résultat se déduit du théorème 4.1, p. 44 de K. Prachar [3].

LEMME 5 (d'après Bombieri). <u>Soit</u> c <u>un nombre réel positif</u>

$$\sum_{d \leq c x^{\frac{1}{3}}} E^*(x, d) = o(\mathrm{li}\ x) .$$

C'est une forme affaiblie du théorème 4, p. 203 de E. Bombieri [1].

LEMME 6. <u>Soit</u> λ <u>une fonction multiplicative à valeurs réelles positives telle que</u> :

1) $\lambda(p) = 1$ pour tout nombre premier p.

2) $\exists \eta : 0 < \eta < \frac{1}{2}$ tel que $\lambda(d) \leq d^r$ pour tout nombre entier d.

Alors :

$$(6.1) \qquad \sum_{1 \leq d \leq x} \lambda(d) = 0(x)$$

$$(6.2) \qquad \sum_{1 \leq d \leq x} \frac{\lambda(d)}{d^\eta} = 0(x^{1-\frac{\eta}{2}})$$

. Commençons par montrer que (6. 1) entraîne (6. 2).

$$\sum_{1 \leq d \leq x} \lambda(d)/d^\eta = \sum_{1 \leq d \leq x^{\frac{1}{2}}} \lambda(d)/d^\eta + \sum_{x^{\frac{1}{2}} < d \leq x} \lambda(d)/d^\eta$$

d'où

$$\sum_{1 \leq d \leq x} \lambda(d)/d^\eta \leq x^{\frac{1}{2}} + x^{-\eta/2} . 0(x) = 0(x^{1-\eta/2}) \quad \text{car} \quad 1-\eta/2 > 1/2 .$$

. Montrons maintenant la relation (6. 1). Posons

$$\lambda(d) = \sum_{\delta \mid d} \nu(\delta) ;$$

ν est une fonction multiplicative telle que :

. $\nu(p) = \lambda(p) - 1 = 0$ pour tout nombre premier p

. $|\nu(d)| = \prod_{p^k \| d} |\lambda(p^k) - \lambda(p^{k-1})| \leq \prod_{p^k \| d} (p^k)^\eta = d^\eta$ pour tout entier d.

$$\Lambda(x) = \sum_{1 \leq d \leq x} \lambda(d) = \sum_{1 \leq d \leq x} \sum_{\delta \mid d} \nu(\delta)$$

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

La série $\sum_p \frac{|\nu(p^2)|}{p^2}$ est convergente car la série $\sum p^{2\eta}/p^2$ converge et donc le produit $\prod_p (1 + \sum_{k=2}^{\infty} \frac{|\nu(p^k)|}{p^k})$ converge vers $\sum_d \frac{|\nu(d)|}{d}$, ce qui entraîne (6. 1).

2. 2. Montrons maintenant le théorème 1.

Il est clair que si la relation A est vérifiée pour une certaine valeur α_o de α, elle est également vérifiée pour toutes les valeurs de α inférieures à α_o. 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

$$. \quad h(p^k) = g(p^k) - g(p^{k-1}) \qquad . \quad |h(d)| \le 1 \, .$$

$$S(x) = \sum_{\substack{p \le x \\ p \equiv a+1[a^2b]}} g(p-1) = \sum_{\substack{p\le x \\ p\equiv a+1[a^2b]}} \sum_{d|p-1} = \sum_{d\le x} h(d) \sum_{\substack{p\equiv 1[a]_2 \\ p\equiv a+1[a^2b] \\ p\le x}} 1 \, .$$

$$S(x) = \sum_{d\le x} h(d)\, \rho(d)\, \pi(x, a^2bd', u_d) \quad \text{d'après le lemme 2 .}$$

Décomposons $S(x)$ en trois sommes partielles $S_1(x)$, $S_2(x)$, $S_3(x)$ selon que d appartient aux intervalles $[1, x^{\frac13}]$, $]x^{\frac13}, x^{1-\zeta}]$, $]x^{1-\zeta}, x]$.

$$. \quad S_1(x) = \frac{\mathrm{li}\, x}{\varphi(a^2b)} \sum_{d\le x^{\frac13}} \frac{h(d)\,\rho(d)}{\psi(d)} + \theta \sum_{d\le x^{\frac13}} |h(d)|\, \rho(d)\, E^*(x, a^2bd') \, ,$$

toujours d'après le lemme 2.

$$\sum_{d\le x^{\frac13}} \frac{h(d)\,\rho(d)}{\psi(d)} = (1+o(1)) \prod_p \Big(1 + \sum_{k=1}^{\infty} \frac{h(p^k)\,\rho(p^k)}{\psi(p^k)}\Big)$$

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

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).

$$\Big| \sum_{d\le x^{\frac13}} |h(d)|\, \rho(d)\, E^*(x, a^2bd') \Big| \le \sum_{d\le x^{\frac13}} \rho(d)\, E^*(x, a^2bd') = o(\mathrm{li}\, x)$$

d'après les lemmes 3 et 5 .

$$. \quad S_2(x) = \sum_{x^{\frac13} \le d \le x^{1-\zeta}} \rho(d)\, h(d)\, \pi(x, a^2bd', u_d)$$

$$= O\Big(\sum_{x^{\frac13} \le d \le x^{1-\zeta}} \frac{\rho(d)\, |h(d)|}{\varphi(a^2b)\, \psi(d)} \, \mathrm{li}\, x \Big)$$

d'après le lemme 4 et le lemme 2. La série figurant dans le terme 0 étant convergente (nous venons de le voir), $S_2(x) = o(\mathrm{li}\, x)$.

. Remarquons ensuite que

$$\pi(x, a^2 b d') \leq \frac{x}{a^2 b d'} + 1 \quad ;$$

mais, grâce au lemme 3,

$$\frac{x}{a^2 b d'} \leq \frac{x}{a b d} \quad ;$$

d'où, lorsque $d \leq x$: $\pi(x, a^2 b d') \leq c \frac{x}{d}$, la constante c ne dépendant que de a et b ,

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

$$|S_3(x)| \leq c\, x \sum_{x^{1-\zeta} \leq d \leq x} \frac{|h(d)|}{d} \leq c\, x^{\zeta} \sum_{1 \leq d \leq x} |h(d)| \,.$$

Posons $\bar{h}(p) = 1$, $\bar{h}(p^k) = p^k\, h(p^k)$ si $k > 1$.

$\bar{h}$ satisfait les conditions du lemme 6, et donc

$$|S_3(x)| \leq c\, x^{\zeta}\; 0(x^{1-\frac{\alpha}{2}}) = 0\,(x^{1-\frac{\alpha}{4}}) = o(\mathrm{li}\, x) \quad , \quad \text{car} \quad \zeta = \alpha/4 \,.$$

Le théorème 1 est ainsi démontré.

§ 3. - DEMONSTRATION DU THEOREME 2

Dans tout ce paragraphe, g désigne une fonction multiplicative à valeurs dans l'intervalle $[0, 1]$ satisfaisant les conditions A à D citées page 20-02.

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) (p. 20-03) 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 airthmétique 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 non-croissante de limite nulle et telle que la série associée diverge ; soit $n_1, \dots, n_k, \dots$ une suite de nombres entiers croissante et telle qu'il existe un entier A pour lequel $n_k \leq k.A$, pour tout k ; alors la série de terme général $u(n_k)$ diverge.

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

$$u(n_k) \geq u(k.A)$$

$$A.u(n_k) \geq A.u(k.A) \geq u(k.A) + u(k.A+1) + \dots + u((k+1).A-1)$$

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

faisons tendre alors m vers l'infini. Le résultat en découle.

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 page 20-08).

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

En effet

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

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

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

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

Posons alors

$$b = \prod_{3 \leq p \leq p_\varepsilon} p .$$

Considérons l'ensemble 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 Q , $(q_1, q_2, \ldots, q_{2k+1})$ tels que :

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

Posons alors

$$a = 2 q_1 q_2 \ldots q_{2k+1} .$$

On vérifie alors que a et b satisfont les conditions i/ et iv/ de la page 20-04 ; seule, la condition iii/ n'est pas tout à fait évidente : puisque $q_i \equiv -1\ [b]$, $a \equiv -2\ [b]$ soit $a+1 \equiv -1\ [b]$, 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 :

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

$$\text{car} \qquad 1 \ge \prod_{p \nmid ab} \Big(1 + \sum_{k=1} \frac{g(p^k) - g(p^{k-1})}{p^{k-1}(p-1)}\Big) \ge \prod_{p > p_\varepsilon} G_p \; .$$

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 :

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

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

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

<u>i/</u> $\quad f(\mathcal{B}) \subset [0, \beta[$

<u>ii/</u> $\quad \liminf\limits_{n\to\infty} \dfrac{S^f(\mathcal{B}, n)}{S(\mathcal{B}, n)} \ge \gamma > 0$

<u>iii/</u> $\quad \liminf\limits_{n\to\infty} \dfrac{S(\mathcal{B}, n)}{S(\mathcal{A}, n)} \ge \delta > 0$.

<u>Alors</u>, $\forall \eta \in [0, \gamma[$

$$\liminf_{n\to\infty} \frac{S(\mathcal{A}, n/\eta < f(a) < \beta)}{S(\mathcal{A}, n)} \ge \delta \frac{\gamma - \eta}{\beta - \eta} \; .$$

En effet :

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

$$\geq \liminf_{n\to\infty} \frac{S(\mathcal{B}, n/f(b) > \eta)}{S(\mathcal{B}, n)} \cdot \frac{S(\mathcal{B}, n)}{S(\mathcal{A}, n)}$$

$$\geq \delta . \liminf_{n\to\infty} \frac{S(\mathcal{B}, n/f(b) > \eta)}{S(\mathcal{B}, n)} .$$

Montrons, en raisonnant par l'absurde :

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

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

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

Mais

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

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

et du fait que

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

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

ce qui contredit l'hypothèse ii/ .

Appliquons le lemme 9, lorsque $\mathcal{A} = \{p \;/\; p \text{ premier}\}$,

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

$$\beta = \xi + \varepsilon \qquad \text{car} \qquad g(p-1) \leq g(a)$$

puisque $q \mid a$ entraîne $q \parallel p-1$.

$\gamma = \xi - \frac{2\varepsilon}{3}$ par la formule (***) de la page 20-12.

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

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

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

§ 4. - QUELQUES COMPLEMENTS

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 tout nombre premier assez grand que possède cette dernière propriété.

4.2. - On peut supprimer l'hypothèse D et montrer le

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

Pour montrer ce résultat, on reprend le second paragraphe en remplaçant la condition i/ , page 20-04, par la condition i'/ : $2^k \| a$, et la condition iv/ par $\frac{a}{2^k}$ 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 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 :

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

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

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

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 croît strictement sur $I \Leftrightarrow I \subset \overline{\{g(p-1)\}}$, $\overline{\{g(p-1)\}}$ désignant l'adhérence de l'ensemble des nombres $g(p-1)$.

-:-:-:-

BIBLIOGRAPHIE

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

[2] I. KATAI. - On the distribution of arithmetical functions on the set prime plus one. Compositio mathematica (1967).

[3] K. PRACHAR. - Primzahlverteilung. Springer Verlag (1957).

-:-:-:-

Jean-Marc DESHOUILLERS
Centre de Mathématiques
Ecole Polytechnique
75 - PARIS V.