COMPOSITIO MATHEMATICA

JEAN-MARC DESHOUILLERS

Sur la croissance de certaines fonctions de répartition

Compositio Mathematica, tome 31, n° 3 (1975), p. 259-284

<http://www.numdam.org/item?id=CM_1975__31_3_259_0>

COMPOSITIO MATHEMATICA, Vol. 31, Fasc. 3, 1975, pag. 259–284
Noordhoff International Publishing
Printed in the Netherlands

SUR LA CROISSANCE DE CERTAINES FONCTIONS DE REPARTITION

Jean-Marc Deshouillers

Abstract

I. Kátai gave conditions under which the distribution function G of numbers $g(F(p))$ exists and is continuous, when g is a multiplicative arithmetical function, F an integer-valued polynomial and p runs through the set of prime numbers; in this paper we give conditions under which the distribution function is strictly increasing, showing in a more precise form that $G(x)$ is strictly less than $G(y)$ as soon as there exists a large prime p_0 such that $x < g(F(p_0)) < y$.

1. Introduction

1.1. Nous désignerons par g une fonction arithmétique multiplicative à valeurs dans $]0, 1]$, et nous poserons

$$G_N(x) = (\text{li } N)^{-1} \text{ Card } \{p \leqq N : g(p+1) < x\}.$$

On doit à I. Kátai (cf. [6]) et P. D. T. A. Elliott (cf. [3]) le théorème suivant:

THÉORÈME A: *Si g est fortement multiplicative (c'est-à-dire si $g(p^\alpha) = g(p)$ pour tout nombre premier p et tout entier positif α), la limite, lorsque N tend vers ∞, de $G_N(x)$ existe et définit une fonction continue G de x si et seulement si la série de terme général $(1-g(p))\cdot p^{-1}$ converge, et la série des inverses des nombres premiers p pour lesquels $g(p)$ est différent de 1, diverge.*

Nous nous proposons d'étudier ici la *croissance* de la fonction limite G, appelée *fonction de répartition* des nombres $g(p+1)$. Dans la note [2],

nous avons déjà abordé cette question (à quelques modifications mineures près); nous allons donner quelques résultats (théorèmes (0), (1) et (2)) qui étendent notablement ceux de la note. Avant de citer les résultats les plus généraux, énonçons le théorème (0), qui est essentiellement un corollaire des théorèmes A, (1) et (2) et dont la formulation est particulièrement aisée:

THÉORÈME (0): *Soit g une fonction fortement multiplicative à valeurs dans $]0,1]$ et telle que la fonction de répartition G des nombres $g(p+1)$ existe et soit continue; on a l'équivalence des deux propriétés:*

(1) $$G(x) < G(y)$$

(2) *Il existe un nombre premier p_0 impair tel que l'on ait:*

$$x < g(p_0+1) < y$$

En outre si la série $\sum(1-g(p))$ diverge tandis que son terme général tend vers zéro, la fonction G croît strictement sur $[0, g(2)[$ et $G(g(2))$ vaut 1.

1.2. I. Kátai (cf. [5]) et P. D. T. A. Elliott (loc. cit.) se sont également interessé à la répartition des nombres $g(F(p))$, lorsque F est un polynôme et g n'est plus supposée fortement multiplicative. La situation est un peu moins agréable dans ce cas, dans la mesure où l'on ne connaît pas de condition (maniable) qui soit nécessaire et suffisante pour l'existence et la continuité de la fonction de répartition G des nombres $g(F(p))$, qui est définie (lorsqu'elle existe) par la relation:

$$G(x) = \lim_{N\to\infty} G_N(x) = \lim_{N\to\infty} (\mathrm{li}\, N)^{-1}\, \mathrm{Card}\,\{p \leqq N : g(F(p)) < x\}.$$

A partir de maintenant, on suppose que g et F vérifient les conditions (C) suivantes:

(C) g est une fonction multiplicative à valeurs dans $]0,1]$; F est un polynôme sans facteur carré tel que pour tout entier n positif ou nul $F(n)$ soit un entier strictement positif et tel que le degré de F (noté $\partial^0 F$) soit supérieur ou égal à 1.

Pour tout entier d positif, on notera $\lambda_F(d)$ (ou $\lambda(d)$) le nombre d'entiers n tels que l'on ait:

$$F(n) \equiv 0 \,(\text{mod. } d), \qquad 0 \leqq n < d, \qquad (n, d) = 1.$$

On a les résultats suivants

THÉORÈME (1): *On suppose que g et F satisfont, outre les conditions* (C), *les conditions* (3), (4) *et* (5) *suivantes*:

(3) *la série* $\sum \lambda_F(p) \cdot (1 - g(p)) \cdot p^{-1}$ *converge,*

(4) *la série de terme général* p^{-1}, *étendue aux nombres premiers p pour lesquels* $\lambda_F(p) \cdot (1 - g(p)) \neq 0$, *diverge,*

(5) *pour tout entier* α *appartenant à l'intervalle* $[1, \partial^0 F - 1]$, *on a*:

$$\lim_{p \to \infty} (\lambda_F(p^\alpha) \cdot (1 - g(p^\alpha))) = 0.$$

Alors la fonction de répartition G des nombres $g(F(p))$ *existe et est continue*; *en outre on a l'équivalence des deux propriétés*:

(6) $$G(x) < G(y).$$

(7) *Il existe un nombre premier* p_0 *supérieur à* $\text{Max}\,(F(0), \partial^0 F + 1)$ *tel que* $x < g(F(p_0)) < y$.

Comme nous le verrons dans le quatrième paragraphe, l'existence et la continuité de G ont été démontrées par I. Kátai. Nous démontrerons la partie importante du théorème (1) (c'est-à-dire l'implication (7) $\Rightarrow$ (6)) dans le cinquième paragraphe, en utilisant quelques résultats techniques démontrés dans les deuxième et troisième sections. Dans le sixième paragraphe, en combinant le théorème (1) et des techniques de crible, nous nous attacherons à caractériser les intervalles sur lesquels G est croissante et nous obtiendrons le théorème (2):

THÉORÈME (2): *Soient g et F une fonction multiplicative et un polynôme satisfaisant les conditions* (C), (3), (4) *et* (5), *et les deux suivantes*:

(8) $$\sum \lambda_F(p) \cdot (1 - g(p)) \text{ diverge}$$

(9) $$\forall \alpha \in \mathbb{N}_\cap [1, 10(\partial^0 F)^2] : \lim_{p \to \infty} \lambda_F(p^\alpha) \cdot (1 - g(p^\alpha)) = 0.$$

Il existe un nombre réel θ tel que G croisse strictement sur $[0, \theta[$, et $G(\theta) = 1$.

Enfin, dans le dernier paragraphe, on complètera la démonstration du théorème (0).

Avant d'aborder la démonstration de ces résultats, nous allons faire quelques remarques et préciser les notations.

REMARQUE (1): L'idée de la démonstration du Théorème (1) est la suivante:

A partir du moment où il existe un nombre premier p_0 'général' tel que $x < g(F(p_0)) < y$, on peut construire une progression arithmétique $an+b$ satisfaisant les conditions:

(i) $p \equiv b \,(\text{mod. } a) \Rightarrow F(p_0) \| F(p)$ (et alors $g(F(p)) < y$),
(ii) $\lim_{n\to\infty} \varphi(a)/\text{li}\, n \sum_{p\leqq n,\, p\geqq b(a)} g(F(p))$ est proche de $g(F(p_0))$; il résulte alors de i et de ii qu'il y a 'beaucoup' de p tels que $g(F(p))$ soit supérieur à x (cf. lemme (6)).

REMARQUE (2): La condition $p_0 > \text{Max}\,(F(0), \partial^0 F + 1)$ est indispensable: Définissons en effet g par $g(p^\alpha) = \varphi(p^\alpha)/p^\alpha$ sauf si $p = 3$, auquel cas $g(3^\alpha) = 1$, et $F(n) = n+1$; d'après le Théorème (0), G croît strictement sur $[0, \frac{1}{2}[$ et $G(\frac{1}{2}) = 1$; cependant: $g(F(2)) = g(2+1) = g(3) = 1$.

REMARQUE (3): Les conditions (3) et (4) du Théorème (1) sont très vraisemblablement suffisantes; la condition (5) est introduite pour des raisons techniques et n'est sans doute pas nécessaire.

REMARQUE (4): La valeur $10(\partial^0 F)^2$ dans le Théorème (2) n'a pas une grande signification; on peut la remplacer par $\partial^0 F(\text{Log}\, \partial^0 F + 7)$ en faisant appel à une version plus élaborée du crible (cf. [4] chap. 10), et par $2\partial^0 F + 1$ si on suppose en outre F irréductible (cf. [8]); l'hypothèse H de A. Schinzel implique que l'on peut remplacer cette valeur par 1.

REMARQUE (5): Les théorèmes (0), (1) et (2) se transposent bien évidemment aux cas où g est une fonction *additive* à valeurs non-négatives, ou non-positives.

REMARQUE (6): Si le Lecteur ne se perd pas dans la partie technique des démonstrations, il le devra au Referee qui m'a fait préciser bien des points qui étaient à peine ébauchés dans la première version de cet article.

Notations:

- les lettres p, q et r désignent exclusivement des nombres premiers,
- (a, b) désigne le p.g.c.d. des entiers a et b et $[a, b]$ leur p.p.c.m.
- $\operatorname{li} x = \lim_{\varepsilon \to 0^+} \int_0^{1-\varepsilon} (\operatorname{Log} t)^{-1} dt + \int_{1-\varepsilon}^{x} (\operatorname{Log} t)^{-1} dt \sim x/\operatorname{Log} x$
- $\rho(d) = \operatorname{Card} \{m : F(m) \equiv 0 \,(\text{mod. } d), 0 \leqq m < d\}$
- $\lambda(d) = \operatorname{Card} \{m : F(m) \equiv 0 \,(\text{mod. } d), 0 \leqq m < d, (m, d) = 1\}$
- $\partial^0 F$ (ou simplement ∂) est le degré du polynôme F,
- κ est le nombre de facteurs irréductibles (sur $\mathbb{Q}$) de F.
- $a|b$ signifie que a divise b et $a||b$ signifie que si $p^\alpha|a$ et $p^{\alpha+1} \nmid a$ alors $p^\alpha|b$ et $p^{\alpha+1} \nmid b$.
- $\nu(d)$ est le nombre de facteurs premices distincts de d
- μ désigne la fonction de Möbius et φ l'indicatrice d'Euler.
- si L est un nombre réel positif et g une fonction arithmétique multiplicative, on note:

$$g_L(n) = \prod_{\substack{p^\alpha || n \\ p^\alpha \leqq L}} g(p^\alpha)$$

2. Quelques résultats auxiliaires

Dans ce paragraphe, ainsi que dans tous les suivants à l'exception du dernier, g, F, p_0 satisfont les relations (C), (3), (4), (5) et (7).

D'après les conditions imposées à F et p_0, p_0 ne divise pas $F(p_0)$: on peut écrire $F(p_0) = q_1^{\alpha_1} \dots q_n^{\alpha_n}$, où les q_i sont des nombres premiers distincts deux à deux, et distincts de p_0, et où les α_i sont des entiers strictement positifs. On note $Q = \{q_1, \dots, q_n\}$. Soit z un nombre réel supérieur à $\operatorname{Max} \{p_0, q_1, \dots, q_n\}$; on pose:

$$a = F(p_0) \prod_{p \leqq z} p \tag{10}$$

LEMME (1): *Il existe un entier b premier à a tel que pour tout entier positif k on ait*:

$$(F(ak+b), a) = F(p_0). \tag{11}$$

Remarquons d'abord que la congruence $F(n) \equiv 0 \,(\text{mod. } p_0)$ a au plus $\partial^0 F$ solutions modulo p_0 (car $F(0) \not\equiv 0 \,(\text{mod. } p_0)$). Puisque p_0 est supérieur

à $\partial^0 F+1$, il existe un entier b' non divisible par p_0 tel que $F(b') \not\equiv 0 \pmod{p_0}$.

Définissons alors b comme étant la plus petite solution positive du système:

$$\begin{cases} b \equiv p_0 & (\text{mod. } a/p_0) \\ b \equiv b' & (\text{mod. } p_0). \end{cases} \tag{12}$$

On vérifie alors que b satisfait aux conditions du lemme (1).

LEMME (2): *On définit a et b par les relations* (10) *et* (12). *Pour tout entier positif d, le système (en u)*

$$\begin{cases} 1 \leqq u \leqq [a, d] \\ u \equiv b \,(\text{mod. } a) \\ F(u) \equiv 0 \,(\text{mod. } d) \\ (u, [a, d]) = 1 \end{cases} \tag{13}$$

est impossible si (a, d) ne divise pas $F(p_0)$. Si (a, d) divise $F(p_0)$, il admet $\lambda(d/(a, d))$ solutions.

(i) On suppose que (a, d) ne divise pas $F(p_0)$; on est alors dans au moins un des trois cas suivants:

– $p_0 | d$; on a alors:

$$u \equiv b' \,(\text{mod. } p_0) \text{ et } F(u) \equiv 0 \,(\text{mod. } p_0)$$

ces deux congruences sont incompatibles car $F(b') \not\equiv 0 \,(\text{mod. } p_0)$ par définition de b'.

– $\exists i \in [1, n] : q_i^{\alpha_i + 1}$ divise d; on a alors:

$$u \equiv p_0 \,(\text{mod } q_i^{\alpha_i + 1}) \quad \text{et} \quad F(u) \equiv 0 \,(\text{mod. } q_i^{\alpha_i + 1})$$

et ces deux congruences sont incompatibles car $F(p_0) \not\equiv 0 \,(\text{mod. } q_i^{\alpha_i + 1})$, par définition de α_i.

– Il existe un nombre premier p inférieur ou égal à z et distinct de $p_0, q_1, \ldots, q_n$, tel que p divise d; alors on a:

$u \equiv p_0 \,(\text{mod. } p)$ et $F(u) \equiv 0 \,(\text{mod. } p)$, ce qui est impossible car $F(p_0) \not\equiv 0 \,(\text{mod. } p)$.

(ii) On suppose maintenant que (a, d) divise $q_1^{\alpha_1} \cdot \ldots \cdot q_n^{\alpha_n}$; tous les facteurs premiers de $d/(a, d)$ sont supérieurs à z, et le système (13) est équivalent au système (14)

$$(14) \qquad \begin{cases} 1 \leqq u \leqq [a, d] \\ u \equiv b \,(\text{mod. } a) \\ F(u) \equiv 0 \,(\text{mod. } d/(a, d)) \\ (u, [a, d]) = 1. \end{cases}$$

D'après le 'théorème chinois', chaque solution du système (15) (ci-dessous) induit une solution unique du système (14) (et ce de manière surjective), et par définition de la fonction λ, le système (15) admet $\lambda(d/(a, d))$ solutions.

$$(15) \qquad \begin{cases} 1 \leqq u \leqq d/(a, d) \\ F(u) \equiv 0 \,(\text{mod. } d/(a, d)) \\ (u, d/(a, d)) = 1. \end{cases}$$

LEMME (3): *Soit $\rho(d)$ le nombre de solutions de la congruence $F(u) \equiv 0$ (mod. d), où $0 \leqq u < d$.*

(i) *Les fonctions λ et ρ sont multiplicatives*

(ii) *Il existe un nombre réel positif C tel que pour tout nombre premier p et tout entier naturel α, on ait*

$$\lambda(p^\alpha) \leqq \rho(p^\alpha) \leqq C$$

(iii) *On définit les fonctions λ' et ψ' par les relations*

$$\lambda'(d) = \begin{cases} \lambda(d/(a, d)) & \text{si } (a, d) \mid F(p_0) \\ 0 & \text{sinon} \end{cases}$$

$$\psi'(d) = \begin{cases} \varphi^{-1}(d/(a, d)) & \text{si } (a, d) \mid F(p_0) \\ 0 & \text{sinon} \end{cases}$$

Les fonctions λ' et ψ' sont multiplicatives.

La démonstration des assertions (i) et (iii) ne pose aucune difficulté; l'assertion (ii) est dûe à T. Nagel (cf. [7]).

LEMME (4) (Bombieri): *Soient k et ℓ deux entiers premiers entre eux; on pose*:

$$\pi(x; k, \ell) = \text{Card}\,\{p \leqq x : p \equiv \ell \,(\text{mod. } k)\},$$

$$E^*(x; k) = 1 + \operatorname*{Max}_{y \leqq x} \operatorname*{Max}_{(\ell, k)=1} |\pi(y; k, \ell) - \text{li } y/\varphi(k)|.$$

Pour tout couple de nombres réels positifs C, ε (*où* $0 < \varepsilon < \frac{1}{2}$) *et tout nombre réel positif* A, *on a*:

$$\sum_{k \leqq x^{\frac{1}{2}-\varepsilon}} C^{\nu(k)} \cdot E^*(x; k) = O_{C,\varepsilon,A}(x(\text{Log } x)^{-A}).$$

La démonstration de ce lemme est essentiellement celle utilisée par H. E. Richert (cf. [8], p. 20); remarquons dès maintenant que l'on ne restreint pas la généralité du lemme en supposant que C est un nombre entier. D'après l'inégalité de Cauchy-Schwarz, on a:

$$S \overset{\text{def}}{=} \sum_{k \leqq x^{\frac{1}{2}-\varepsilon}} C^{\nu(k)} E^*(x; k) \leqq \Big(\sum_{k \leqq x^{\frac{1}{2}-\varepsilon}} C^{2\nu(k)}/k\Big)^{\frac{1}{2}} \Big(\sum_{k \leqq x^{\frac{1}{2}-\varepsilon}} k(E^*(x; k))^2\Big)^{\frac{1}{2}}$$

En utilisant la majoration triviale: $E^*(x; k) \leqq x/k$, valable pour $k \leqq x^{\frac{1}{2}}$ et x assez grand, et la majoration (qui s'obtient de manière analogue au lemme 3 de [8]):

$$\sum_{k \leqq u} h^{\nu(k)}/k = (1 + \log u)^h,$$

valable pour tout entier positif h, on trouve:

$$S = O((\text{Log } x)^{C^2} \cdot x^{\frac{1}{2}} \cdot \Big(\sum_{k \leqq x^{\frac{1}{2}-\varepsilon}} E^*(x; k)\Big)^{\frac{1}{2}}).$$

On utilise alors le puissant théorème de E. Bombieri (cf. [1], th. 4):

$$\sum_{k \leqq x^{\frac{1}{2}-\varepsilon}} E^*(x; k) = O(x \cdot (\text{Log } x)^{-B}),$$

pour tout réel positif B. En choisissant $B = 2C^2 + 2A$, on obtient la majoration souhaitée.

LEMME (5): *On pose*: $L = (\text{Log } x)/5$; *on a*:

$$|\sum_{p \leqq x} g_L(F(p)) - g(F(p))| = o(\text{li } x),$$

lorsque g et F satisfont les relations (C), (3), (4), (5).

Si F est un polynôme de degré 1, c'est le lemme 12, p. 82 de [5]; si F n'est pas supposé de degré 1, on déduit du lemme cité la relation:

$$(16) \qquad |\sum_{p \leqq x} g_L(F(p)) - g_M(F(p))| = o(\mathrm{li}\, x), \quad \text{où} \quad M = x^{\frac{1}{2}}.$$

Posons:

$$V_0(x) = \sum_{p \leqq x} g(F(p)), \qquad V_1(x) = \sum_{p \leqq x} g_M(F(p)).$$

Puisque la fonction g est à valeurs dans $]0, 1]$, $g_M(n)$ est toujours supérieur ou égal à $g(n)$; il nous suffit donc de majorer $V_1(x) - V_0(x)$; on a:

$$V_1(x) - V_0(x) = \sum_{p \leqq x} \prod_{\substack{q^\alpha \| F(p) \\ q^\alpha \leqq M}} g(q^\alpha) \cdot (1 - \prod\nolimits_p^{(M)} g(q^\alpha)),$$

où l'exposant (M) du produit signifie qu'il est étendu aux puissances q^α telles que $q^\alpha \| F(p)$ et $q^\alpha > M$; on a:

$$V_1(x) - V_0(x) \leqq \sum_{p \leqq x} (1 - \prod\nolimits_p^{(M)} g(q^\alpha))$$

On peut alors écrire:

$$V_1(x) - V_0(x) < \sum_{\alpha=1}^{\partial - 1} \sum\nolimits^{(\alpha)} (1 - \prod\nolimits_p^{(M)} g(q^\alpha) + \sum\nolimits^{*} (1 - \prod\nolimits_p^{(M)} g(q^\alpha))$$

où ∂ désigne le degré de F, où l'exposant (α) signifie que la somme est étendue aux nombres premiers p inférieurs ou égaux à x pour lesquels il existe un nombre premier q tel que q^α divise exactement $F(p)$, et où l'étoile signifie que la somme est étendue aux nombres premiers p inférieurs ou égaux à x pour lesquels il existe un nombre premier q et un entier α supérieur ou égal au degré ∂ de F tels que q^α soit supérieur à M et q^α divise exactement $F(p)$.

Nous commencerons par les sommes $\sum^{(\alpha)}$. D'après la condition (5), pour tout $\alpha < \partial$, il existe une fonction $\varepsilon_\alpha(x)$ de limite nulle (lorsque x tend vers l'infini) telle que $g(q^\alpha)$ soit supérieur à $1 - \varepsilon_\alpha(x)$ dès que q^α

est une puissance d'un nombre premier qui soit supérieure à M et qui divise exactement un nombre $F(p)$. Mais $F(p)$, avec p inférieur ou égal à x a au plus 2∂ tels diviseurs; on a donc:

$$\sum^{(\alpha)}(1-\prod^{(M)} g(q^\alpha)) \leqq \sum_{p\leqq x}(1-(1-\varepsilon_\alpha(x))^{2\partial})$$
$$= O(1-(1-\varepsilon_\alpha(x))^{2\partial})\cdot \operatorname{li} x = o(\operatorname{li} x).$$

Etudions maintenant la somme $\sum^*$. Chaque terme de la somme est inférieur ou égal à 1; on a donc:

$$\sum^* (1-\prod^{(M)} g(q^\alpha)) \leqq \operatorname{Card}\{p\leqq x : q^\alpha > M, \alpha \geqq \partial, q^\alpha \| F(p)\}$$
$$\leqq \operatorname{Card}\{p\leqq x : \exists\{q,\alpha\}, q > x^{\frac{1}{3}}, q^\alpha > M, \alpha\geqq\partial, q^\alpha\|F(p)\}$$
$$+\operatorname{Card}\{p\leqq x : \exists\{q,\alpha\}, q\leqq x^{\frac{1}{3}}, q^\alpha > M, \alpha\geqq\partial, q^\alpha\|F(p)\}.$$

Le premier terme du second membre est majoré par:

$$\operatorname{Card}\{p\leqq x : \exists q, q > x^{\frac{1}{3}}, q^\partial | F(p)\}.$$

Avec les notations de [5], cette expression est $N_2(F, x, x^{\frac{1}{3}}, \infty, \partial)$, et d'après le lemme 6 de [5], cette expression est $o(\operatorname{li} x)$.

Le second terme du second membre est majoré par:

$$\operatorname{Card}\{n\leqq x : \exists(q,\alpha), q < x^{\frac{1}{3}}, q^\alpha > M, q^\alpha | F(n)\}.$$

En notant β le plus petit entier tel que q^β soit supérieur à M, on peut majorer la dernière expression par:

$$\sum_{q\leqq x} \operatorname{Card}\{n\leqq x : F(n)\equiv 0 \,(\text{mod. } q^\beta)\}$$
$$\leqq \sum_{q\leqq x} p(q^\beta)(1+x/q^\beta) = O(x^{\frac{1}{3}}\cdot x^{\frac{1}{2}}) = o(\operatorname{li} x).$$

La quantité $V_1(x)-V_0(x)$ qui est une somme finie de termes qui sont $o(\operatorname{li} x)$ est elle-même $o(\operatorname{li} x)$; ce résultat et la relation (16) impliquent le lemme (5).

Avant d'énoncer le lemme suivant, précisons les notations: soit $\mathscr{A}$ une suite strictement croissante d'entiers positifs et f une application de $\mathscr{A}$ dans $\mathbb{R}$; on notera $\mathscr{S}(\mathscr{A}, n)$ (resp. $\mathscr{S}(\mathscr{A}, n; P)$) l'ensemble des éléments de $\mathscr{A}$ inférieurs ou égaux à n (resp. et possédant la propriété P); on pose en outre

$$S(\mathscr{A}, n) = \text{Card } \mathscr{S}(\mathscr{A}, n) \qquad S(\mathscr{A}, n; P) = \text{Card } \mathscr{S}(\mathscr{A}, n; P)$$
$$S^f(\mathscr{A}, n) = \sum_{a \in \mathscr{S}(\mathscr{A}, n)} f(a) \qquad S^f(\mathscr{A}, n; P) = \sum_{a \in \mathscr{S}(\mathscr{A}, n; P)} f(a).$$

Avec ces notations on a le lemme suivant:

LEMME 6: *Soit $\mathscr{A}$ une suite strictement croissante d'entiers positifs, $\mathscr{B}$ une sous-suite de $\mathscr{A}$, et f une application de $\mathscr{A}$ dans $\mathbb{R}$ telle que*

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

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

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

Alors, pour tout nombre réel η de l'intervalle $[0, \gamma[$ on a

$$\liminf_{n \to \infty} \frac{S(\mathscr{A}, n; \eta < f(a) < \beta)}{S(\mathscr{A}, n)} \geqq \delta \frac{\gamma - \eta}{\beta - \eta}$$

On a en effet

$$\begin{aligned}
\liminf_{n \to \infty} \frac{S(\mathscr{A}, n; \eta < f(a) < \beta)}{S(\mathscr{A}, n)} &\geqq \liminf_{n \to \infty} \frac{S(\mathscr{B}, n; f(b) > \eta)}{S(\mathscr{A}, n)} \\
&\geqq \liminf_{n \to \infty} \frac{S(\mathscr{B}, n; f(b) > \eta)}{S(\mathscr{B}, n)} \cdot \frac{S(\mathscr{B}, n)}{S(\mathscr{A}, n)} \\
&\geqq \delta \cdot \liminf_{n \to \infty} \frac{S(\mathscr{B}, n; f(b) > \eta)}{S(\mathscr{B}, n)}.
\end{aligned}$$

Supposons que la dernière limite écrite soit inférieure à $(\gamma - \eta)/(\beta - \eta)$; dans ce cas, il existe un nombre réel positif ε et une suite d'entiers n_i tendant vers l'infini telle que l'on ait:

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

Mais on a

$$\begin{aligned} S^f(\mathscr{B}, n_i) &= S^f(\mathscr{B}, n_i; f(b) \leqq \eta) + S^f(\mathscr{B}, n_i; f(b) > \eta) \\ &\leqq \eta \cdot S(\mathscr{B}, n_i; f(b) \leqq \eta) + \beta \cdot S(\mathscr{B}, n_i; f(b) > \eta) \\ &\leqq \eta \cdot S(\mathscr{B}, n_i) + (\beta - \eta) S(\mathscr{B}, n_i; f(b) > \eta) \\ &\leqq S(\mathscr{B}, n_i) \cdot \left[\eta + (\beta - \eta) \left(\frac{\gamma - \eta}{\beta - \eta} - \varepsilon \right) \right] \\ S^f(\mathscr{B}, n_i) &\leqq (\gamma - (\beta - \eta)\varepsilon) \cdot S(\mathscr{B}, n_i) \end{aligned}$$

et cette dernière inégalité contredit l'inégalité (ii), ce qui achève la démonstration du lemme (6).

3. Calcul de la valeur moyenne de $g(F(p))$

PROPOSITION (1): *On suppose que g et F satisfont les conditions* (C), (3), (4), (5) *et* (7), *que a est défini par* (10) *et que b satisfait les conditions du lemme* (1); *on pose*:

$$V(x) = \sum_{\substack{p \leqq x \\ p \equiv b \pmod a}} g(F(p))$$

On a:

$$V(x) = (1 + o(1)) \frac{\operatorname{li} x}{\varphi(a)} g(F(p_0)) \prod_{p > z} \left(1 + \sum_{\alpha = 1}^{\infty} \frac{\lambda(p^\alpha)(g(p^\alpha) - g(p^{\alpha-1}))}{p^{\alpha-1}(p-1)} \right)$$

D'après le lemme (5), il suffit d'estimer la quantité

$$V_L(x) = \sum_{\substack{p \leqq x \\ p \equiv b \pmod{a}}} g_L(F(p)), \qquad \text{où } L = (\operatorname{Log} x)/5$$

En effet, g est à valeurs dans $]0, 1]$ et satisfait: $0 \leqq g(F(p)) \leqq g_L(F(p))$ et on a donc:

$$0 \leqq V_L(x) - V(x) \leqq \sum_{p \leqq x} (g_L(F(p)) - g(F(p))) = o(\operatorname{li} x). \tag{17}$$

Posons

$$h(n) = \sum_{d \mid n} \mu(d) g(n/d) \quad \text{et} \quad h_L(n) = \sum_{d \mid n} \mu(d) g_L(n/d)$$

en utilisant la formule d'inversion de Möbius, on a:

$$V_L(x) = \sum_{\substack{p \leqq x \\ p \equiv b (\mathrm{mod.}\ a)}} \sum_{d | F(p)} h_L(d)$$
$$= \sum_d h_L(d) \cdot \mathrm{Card}\,\{p \leqq x : p \equiv b\,(\mathrm{mod.}\ a),\ F(p) \equiv 0\,(\mathrm{mod.}\ d)\}.$$

D'après les lemmes (2) et (3), on peut écrire:

$$V_L(x) = \sum_d h_L(d) \frac{\lambda'(d)}{\varphi([a,d])} \mathrm{li} x + \theta \sum_d h_L(d)\lambda'(d) E^*(x, [a,d]) \tag{18}$$

où $|\theta| \leqq 1$, et où E^* a la même signification que dans le lemme (4).

D'après la définition de h_L, on voit qu'elle est une fonction multiplicative caractérisée par la relation: $h_L(p^\alpha) = g_L(p^\alpha) - g_L(p^{\alpha-1})$, où p est un nombre premier, et α un entier supérieur ou égal à 1. Puisque $g_L(n)$ est toujours compris entre 0 et 1, et que h_L est multiplicative, on a:

$$|h_L(d)| \leqq 1, \quad \text{pour tout entier } d. \tag{19}$$

De manière élémentaire, on a:

$$\sum_{p^\alpha \leqq L} \log p < \mathrm{Log}\, 4 \cdot L,$$

on en déduit que:

$$\prod_{p^\alpha \leqq L} p < x^{(\mathrm{Log}\, 4)/5} < x^{\frac{1}{3}}$$

Tout nombre supérieur à $x^{\frac{1}{3}}$ a donc au moins un facteur p^α supérieur à L; on a donc:

$$h_L(d) = 0 \quad \text{si } d \text{ est supérieur à } x^{\frac{1}{3}}. \tag{20}$$

Remarquons également que la relation (20) justifie l'écriture (18), où les sommations sur d sont en fait des sommes finies.

3.1. On va commencer par étudier le terme principal (noté T.P.) du second membre de (18), c'est-à-dire la première somme de (18), sans le facteur li x.

Remarquons d'abord (cf. la définition de λ' dans le lemme (3)) que lorsque $\lambda'(d)$ est différent de 0, (a, d) divise $F(p_0)$; d'après la définition de a,

tous les facteurs premiers de $d/(a,d)$ sont supérieurs à z, et a et $d/(a,d)$ sont donc premiers entre eux et on a:

$$\varphi(a)\cdot\varphi(d/(a,d)) = \varphi(ad/(a,d)) = \varphi([a,d]).$$

On en déduit:

$$T.P. = \sum_d h_L(d)\cdot\lambda'(d)\cdot\varphi^{-1}([a,d]) = \varphi^{-1}(a)\sum_d h_L(d)\lambda'(d)\varphi(d/(a,d)).$$

D'après la définition de ψ' (cf. lemme (3)), cette expression vaut également

$$(\varphi(a))^{-1}\sum_d h_L(d)\cdot\lambda'(d)\cdot\psi'(d).$$

Puisque la fonction $h_L\cdot\lambda'\cdot\psi'$ est un produit de fonctions multiplicatives, elle est multiplicative, et la dernière somme écrite admet une factorisation en produit (fini) eulérien:

$$\prod_p (1+\sum_{\alpha=1}^{\infty} h_L(p^\alpha)\cdot\lambda'(p^\alpha)\cdot\psi'(p^\alpha)).$$

Remarquons que $\varphi(p^\alpha/(a,p^\alpha))$ est supérieur ou égal à $K\cdot p^\alpha$, avec $K = z^{-\gamma}/2$, où γ est le plus grand exposant apparaissant dans la décomposition canonique de a en produit de facteurs premiers; (en effet, si p est supérieur à z, on a: $\varphi(p^\alpha/(a,p^\alpha)) = \varphi(p^\alpha) \geqq p^\alpha/2$, et si p est inférieur ou égal à z, on a:

$$\varphi(p^\alpha/(a,p^\alpha)) \geqq (p^{\mathrm{Max}(0,\alpha-\gamma)}) \geqq p^{\alpha-\gamma}/2 \geqq (z^{-\gamma}/2)\cdot p^\alpha).$$

On a alors les relations:

$$|h(p^\alpha)\cdot\lambda'(p^\alpha)\cdot\psi'(p^\alpha)| \leqq |h(p^\alpha)|C\cdot\lambda(p)\varphi^{-1}(p^\alpha/(a,p^\alpha))$$

$$\leqq \begin{cases} (C/K)\cdot(1-g(p))\cdot p^{-1}\lambda(p) & \text{si } \alpha = 1, \\ (C/K)\cdot p^{-\alpha} & \text{si } \alpha > 1. \end{cases}$$

Compte tenu de la relation (3), ces majorations impliquent la convergence (absolue) du produit:

$$\prod_p (1+\sum_{\alpha=1}^{\infty} h(p^\alpha)\cdot\lambda'(p^\alpha)\cdot\psi'(p^\alpha)).$$

On a de même les majorations:

$$|h_L(p^\alpha)-h(p^\alpha)|\cdot\lambda'(p^\alpha)\cdot\psi'(p^\alpha)=0 \qquad \text{si } p^\alpha \leqq L,$$

$$|h_L(p^\alpha)-h(p^\alpha)|\cdot\lambda'(p^\alpha)\cdot\psi'(p^\alpha)=|h(p^\alpha)|\cdot\lambda'(p^\alpha)\cdot\psi'(p^\alpha)$$
$$\text{si } p^{\alpha-1} \text{ est supérieur à } L,$$

et dans ce cas on utilise les majorations précédemment obtenues,

$$|h_L(p^\alpha)-h(p^\alpha)|\cdot\lambda'(p^\alpha)\cdot\psi'(p^\alpha)=(1-g(p^\alpha))\cdot\lambda'(p^\alpha)\cdot\psi'(p^\alpha)$$
$$\text{si } p^{\alpha-1}\leqq L<p^\alpha,$$

et cette expression se majore de manière analogue par

$$\begin{cases}(1-g(p))\cdot\lambda(p)\cdot(C/K)\cdot p^{-1} & \text{si } \alpha=1,\\ (C/K)\cdot p^{-\alpha} & \text{si } \alpha\geqq 2.\end{cases}$$

On en déduit:

$$\lim_{x\to\infty}\prod_p(1+\sum_{\alpha=1}^{\infty}h_L(p^\alpha)\cdot\lambda'(p^\alpha)\cdot\psi'(p^\alpha))=\prod_p(1+\sum_{\alpha=1}^{\infty}h(p^\alpha)\cdot\lambda'(p^\alpha)\cdot\psi'(p^\alpha)).$$

Etudions maintenant chaque 'facteur local' du dernier produit infini:
· Si p est inférieur ou égal à z et ne divise pas $F(p_0)$, on a: $(a,p)=p$ et le facteur local vaut 1.
· Si p est l'un des q_i, on a:

$$(a,q_i^\alpha)=q_i^{\inf(\alpha_i+1,\alpha)}, \qquad \text{donc } (a,q_i^\alpha) \text{ divise } F(p_0)$$

si et seulement si α est inférieur ou égal à α_i, auquel cas on a

$$(a,q_i^\alpha)=q_i^\alpha, \qquad \text{et donc } \lambda'(q_i^\alpha)\psi'(q_i^\alpha)=1.$$

Si α est supérieur à α_i, on a en revanche $\lambda'(q_i^\alpha)\psi'(q_i^\alpha)=0$. Le 'facteur local' vaut donc:

$$1+\sum_{\alpha=1}^{\alpha_i}h(q_i^\alpha)=g(q_i^{\alpha_i}).$$

· Si p est supérieur à z on a: $\lambda'(p^\alpha)\psi'(p^\alpha)=\lambda(p^\alpha)\varphi^{-1}(p^\alpha)$, et en exprimant h en fonction de g, on obtient pour le facteur local

$$1+\sum_{\alpha=1}^{\infty}\frac{\lambda(p^\alpha)(g(p^\alpha)-g(p^{\alpha-1}))}{p^{\alpha-1}(p-1)}.$$

On déduit de ce qui précède que le 'terme principal' du second membre de (18) vaut

$$(21)\quad (1+o(1))\varphi^{-1}(a)\cdot g(F(p_0))\cdot \prod_{p>z}\left(1+\sum_{\alpha=1}^{\infty}\frac{\lambda(p^\alpha)(g(p^\alpha)-g(p^{\alpha-1}))}{p^{\alpha-1}(p-1)}\right).$$

3.2. Etudions maintenant le 'terme complémentaire' du second membre de (18); en appelant $\nu(d)$ le nombre de facteurs premiers distincts de l'entier d, on a, d'après le lemme (3):

$$(22)\qquad \lambda'(d) \leqq C^{\nu(d)}.$$

D'après les relations (19), (20) et (22), on a

$$\begin{aligned}\sum_d h_L(d)\lambda'(d)E^*(x,[a,d]) &\leqq \sum_{d\leqq x^{\frac{1}{3}}} C^{\nu(d)}E^*(x,[a,d])\\ &\leqq \sum_{d\leqq x^{\frac{1}{3}}} C^{\nu([a,d])}E^*(x,[a,d])\\ &\leqq C^{\nu(a)}\sum_{d\leqq x^{\frac{1}{3}}} C^{\nu(d)}E^*(x,[a,d])\\ &\leqq C^{\nu(a)}\cdot d(a)\sum_{t\leqq ax^{\frac{1}{3}}} C^{\nu(t)}E^*(x,t)\end{aligned}$$

car $d(a)$ (le nombre de diviseurs de l'entier a) majore le nombre de manières d'écrire un entier comme p.p.c.m. de a et d'un autre entier. Du lemme (4), on déduit alors la majoration:

$$(23)\qquad \sum_d h_L(d)\cdot\lambda'(d)\cdot E^*(x,[a,d]) = o(\mathrm{li}\, x).$$

3.3. La proposition (1) découle des relations (17), (18), (21) et (23).

4. Existence et continuité de G

Le théorème 8 de l'article [5], de Kátai, se lit ainsi (dans le cas $s = 1$):

THÉORÈME B: *Soit F un polynôme sans facteur carré, de degré $\partial^0 F$ strictement positif, à valeurs entières positives, différent du polynôme x, et f une fonction additive à valeurs réelles satisfaisant les relations*:

(i) $\sum_p \bar{f}(p)\cdot\rho(p)\cdot p^{-1}$ *converge*

(ii) $\sum_p \bar{f}^2(p) \cdot \rho(p) \cdot p^{-1}$ *converge*

(iii) *la série des inverses des nombres premiers tels que* $f(p) \cdot \rho(p)$ *soit différent de O est divergente,*

(iv) $\lim_{p \to \infty} f(p^\alpha) \cdot \rho(p^\alpha) = 0$, *pour* $\alpha = 1, 2, \ldots \partial^0 F - 1$ *avec*

$$\bar{f}(p) = \begin{cases} f(p) & \text{si } f(p) \leqq 1, \\ 1 & \text{si } f(p) \geqq 1, \end{cases}$$

et $\rho(d)$ *désignant le nombre de solutions du système*: $F(n) \equiv 0 \pmod{d}$, $0 \leqq n < d$.

Alors la fonction de répartition des nombres $f(F(p))$ *existe et est continue.*

Pour démontrer l'existence et la continuité de la fonction de répartition des nombres $g(F(p))$, il suffit bien entendu de démontrer que la fonction de répartition des nombres $f(F(p))$ existe et est continue, en posant $f = -\operatorname{Log} g$. Puisque g est multiplicative à valeurs dans $]0, 1]$, il est clair que f est bien définie et représente une fonction additive à valeurs réelles (positives). Il nous reste à vérifier que F et f satisfont les conditions du théorème B si F et g satisfont les conditions (C), (3), (4) et (5).

Commençons par remarquer que la convergence de la série de terme général $f(p) \cdot \rho(p) \cdot p^{-1}$ implique (i) et (ii) si f est à valeurs *positives* (ce qui est le cas). D'après la relation (5), avec $\alpha = 1$, on a

$$\lim \lambda(p) \cdot (1 - g(p)) = 0;$$

on en déduit l'équivalence de $\lambda(p) \cdot (1 - g(p))$ et $-\lambda(p) \cdot \operatorname{Log}(1 - (1 - g(p)))$ lorsque p tend vers l'infini. Les séries à termes *positifs ou nuls*

$$\sum \lambda(p) \cdot (1 - g(p)) \cdot p^{-1} \quad \text{et} \quad \sum -\lambda(p) \cdot \operatorname{Log}(1 - (1 - g(p))) \cdot p^{-1}$$

sont de même nature; mais $-\operatorname{Log}(1 - (1 - g(p)))$ est égal à f; on déduit donc de (3) et (5) que la série de terme général $\lambda(p) \cdot f(p) \cdot p^{-1}$ est convergente, ce qui est presque ce que nous voulons. En effet, $\lambda(p)$ n'est différent de $\rho(p)$ que si 0 est une solution de la congruence $F(n) \equiv 0 \pmod{p}$, c'est-à-dire que $\lambda(p)$ est égal à $\rho(p)$ si p ne divise pas $F(0)$, ce qui est le cas si p est supérieur à $F(0)$ (puisque nous avons supposé dans les conditions (C) que $F(0)$ est strictement positif); la convergence de la série de terme

général $\lambda(p) \cdot f(p) \cdot p^{-1}$ implique donc la convergence de la série de terme général $\rho(p) \cdot f(p) \cdot p^{-1}$, et, comme nous l'avons remarqué, ceci implique que f satisfait (i) et (ii).

La propriété (iv) est la traduction de la propriété (5), puisque $\lambda(p)$ et $\rho(p)$ sont égaux dès que p est assez grand; de manière analogue, la propriété (iii) est la traduction de la propriété (4).

5. Fin de la demonstration du théorème (1)

D'après la définition de p_0 (et la convergence du produit infini que nous avons rencontré), on peut trouver un nombre réel z assez grand pour satisfaire:

- $z \geqq \max(p_0, q_1, \ldots, q_n)$
- $g(F(p_0)) \prod_{p>z} \left(1 + \sum_{\alpha=1}^{\infty} \frac{\lambda(p^\alpha)(g(p^\alpha) - g(p^{\alpha-1}))}{p^{\alpha-1}(p-1)}\right) > \frac{g(F(p_0)) + x}{2}$.

Un tel z étant choisi, on lui fait correspondre a et b, comme il a été indiqué au second paragraphe.

Appliquons maintenant le lemme (6) dans le cadre suivant: $\mathscr{A}$ est la suite des nombres premiers, et $\mathscr{B}$ la sous-suite de $\mathscr{A}$ constituée par les nombres premiers congrus à b modulo a, $f = g_0 F$.

D'après le théorème des nombres premiers, et sa généralisation aux progressions arithmétiques (d'après le lemme (1), a et b sont premiers entre eux), on a:

$$S(\mathscr{A}, n) \sim \operatorname{li} n$$

$$S(\mathscr{B}, n) \sim \varphi^{-1}(a) \operatorname{li} n.$$

On peut donc prendre $\delta = \varphi^{-1}(a)$.

On peut également choisir $\beta = g(F(p_0))$; en effet, si p appartient à $\mathscr{B}$, on a: $g(F(p)) \leqq g(F(p_0))$.

D'après la proposition (1), et le choix de z, on peut prendre:

$$\gamma = \frac{g(F(p_0)) + x}{2}.$$

Choisissons $\eta = x$; on trouve:

$$G(g(F(p_0)))-G(x) \geqq \frac{1}{\varphi(a)} \frac{g(F(p_0))-x}{2} \frac{1}{g(F(p_0))-x} = \frac{1}{2\varphi(a)}.$$

A fortiori, on a: $G(y)-G(x) > 0$.

6. Demonstration du théorème (2)

6.1. Pour démontrer le théorème (2), on démontrera la proposition suivante:

PROPOSITION (2): *Sous les hypothèses du théorème* (2), *pour tout couple de nombres réels* x *et* y *satisfaisant les relations*:

$$0 < G(x) < 1 \quad et \quad 0 < y < x, \tag{24}$$

on a:

$$0 < G(y) < G(x).$$

D'après (24), il existe un nombre premier p_0 supérieur à

$$\text{Max}\,(F(0), \partial^0 F+1)$$

tel que l'on ait:

$$g(F(p_0)) > x.$$

Ecrivons alors $F(p_0) = q_1^{\alpha_1} \cdot \ldots \cdot q_n^{\alpha_n}$; on remarquera que p_0 n'appartient pas à l'ensemble $\mathcal{Q} = \{q_1, \ldots, q_n\}$.

Puisque F n'a pas de facteur carré, son discriminant Δ est un entier non nul; si p ne divise pas $\Delta \cdot F(0)$, on a l'égalité de $\rho(p^\alpha)$ et de $\lambda(p^\alpha)$ (déjà vu dans le quatrième paragraphe) et $\rho(p^\alpha) = \rho(p)$ (cf. par exemple le théorème 123 p. 97 de Hardy et Wright, an introduction to number theory). On a donc $\lambda(p^2) = \lambda(p)$ dès que p est assez grand, disons dès que p est supérieur à q.

D'après (8) et (9), on voit que le produit infini de terme général $g(p)$, étendu aux nombres premiers p tels que $\lambda(p)$ soit different de zéro, diverge, tandis que le terme général tend vers zéro. On en déduit qu'il existe un ensemble fini $\mathcal{R} = \{r_1, r_2, \ldots, r_s\}$ de nombres premiers distincts satisfaisant les relations:

(25a) $$r_j \geqq q, \qquad j = 1, \ldots, s$$

(25b) $$\mathscr{R} \cap (\mathscr{Q} \cup \{p_0\}) = \emptyset$$

(25c) $$\lambda(r_j) \neq 0 \qquad j = 1, \ldots, s$$

(25d) $$y < g(F(p_0)) \prod_{j=1}^{s} g(r_j) < x.$$

6.2. Nous allons démontrer maintenant par une technique de crible, qu'il existe un nombre premier q tel $F(q)$ ne diffère de $F(p_0) \cdot r_1 \cdot \ldots r_s$ que par la présence de *peu* de *grands* facteurs premiers et il en résultera que $g(F(q))$ est compris entre y et x; pour mener à bien cette tâche, nous nous appuierons sur le lemme suivant, essentiellement dû à Halberstam et Richert:

LEMME (7): *Soit $\mathscr{A}$ un ensemble fini d'entiers positifs, $\mathscr{P}$ un ensemble de nombres premiers (on suppose que $\bar{\mathscr{P}}$, le complémentaire de $\mathscr{P}$ par rapport à l'ensemble des nombres premiers, est fini et on note $\bar{\Pi}$ le produit des éléments de $\bar{\mathscr{P}}$), ω une fonction multiplicative, X un nombre réel supérieur à 2, κ un entier positif satisfaisant les conditions*:

$$(\Omega_1) \quad 0 \leqq \omega(p)/p \leqq 1 - 1/A_1$$

$$(\Omega_2) \quad \Big| \sum_{w \leqq p < u} \omega(p) \cdot \operatorname{Log} p \cdot p^{-1} - \kappa \operatorname{Log}(u/w) \Big| \leqq A_2 \quad si \quad 2 \leqq w \leqq u$$

$$(R) \quad \sum_{d < x^{5/12}, (d, \bar{\Pi}) = 1} \mu^2(d) \cdot 3^{\nu(d)} |R_d(X)| \leqq A_3 X/(\operatorname{Log} X)^{\kappa+1}$$

où les constantes A_1, A_2, A_3 sont des constantes supérieures à 1, et où

$$R_d(X) = \operatorname{Card}\{a \in \mathscr{A} : a \equiv 0 \,(\text{mod. } d)\} - (\omega(d)/d) \cdot X.$$

Alors, il existe un nombre réel X_0 tel que l'on ait:

$$S(\mathscr{A}, \mathscr{P}, t) \stackrel{\text{def}}{=} \operatorname{Card}\{a \in \mathscr{A} : (p | a \text{ et } p \in \mathscr{P}) \Rightarrow (p > t)\} > 0$$

dès que X est supérieur à X_0 et t inférieur à $X^{1/9\kappa}$.

C'est essentiellement le théorème 7.4 de Halberstam et Richert (cf. [4]); l'énoncé que nous en donnons correspond au cas où L est une constante

absolue et où α vaut $\frac{1}{3}$. D'après la table 1 p. 212 et les estimations de Hagedorn p. 221, on a

$$\alpha(\operatorname{Log} X)/\operatorname{Log} t \geqq (\operatorname{Log} X)/(3(\operatorname{Log} X)/9\kappa) \geqq 3\kappa \geqq \nu_\kappa,$$

et l'expression $W(t)$ est positive d'après sa définition.

Pour appliquer ce lemme, il nous reste un petit travail de préparation à effectuer: d'après la définition de la fonction λ, la congruence

$$F(n) \equiv 0 \,(\text{mod. } r_j), \qquad 0 < n < r_j$$

a $\lambda(r_j)$ solutions (pour $j = 1, \ldots, s$), et d'après la condition (25a), la congruence $F(n) \equiv 0 \,(\text{mod. } r_j^2)$, $0 < n < r_j^2$, $(n, r_j) = 1$ a également $\lambda(r_j)$ solutions. La congruence

$$F(n) \equiv 0 \,(\text{mod. } r_j), \qquad 0 < n < r_j^2, \qquad (n, r_j) = 1$$

a trivialement $r_j \cdot \lambda(r_j)$ solutions; il résulte de cela et de (25c) que le système $F(n) \equiv 0 \,(\text{mod. } r_j)$, $F(n) \not\equiv 0 \,(\text{mod. } r_j^2)$, $(n, r_j) = 1$ a au moins une solution; soit u_j une telle solution. Considérons alors le système:

$$\begin{cases} m \equiv u_j \,(\text{mod. } r_j^2) & j = 1; \ldots, s \\ m \equiv p_0 \,(\text{mod. } q_i^{\alpha_i + 1}) & i = 1, \ldots, n \end{cases}$$

d'après le théorème chinois, ce système est équivalent à une congruence de la forme:

$$m \equiv U \,(\text{mod. } K), \qquad \text{avec } K = \prod_{i=1}^{n} q_i^{\alpha_i + 1} \cdot \prod_{j=1}^{s} r_j^2, \tag{26}$$

et en outre U et K sont premiers entre eux (puisqu'il en est de même pour u_j et r_j, p_0 et q_i).

Notons N un entier qui sera destiné à tendre vers l'infini, et appliquons le lemme (7) dans le cadre suivant:

$$\mathscr{A} = \{F(p) : p \leqq N \text{ et } p \equiv U \,(\text{mod. } K)\}$$

$$\mathscr{P} = \{p : p \nmid K\} \text{ (et alors } \bar{\mathscr{P}} = \mathscr{R} \cup \mathscr{Q} = \{p : p | K\})$$

ω la fonction multiplicative définie sur les nombres sans facteur carré et telle que: $\omega(p) = 0$ si $p|K$, $\omega(p) = p \cdot \lambda(p)/(p-1)$ si $p \nmid K$,
$X = (\operatorname{li} N)/\varphi(K)$.
κ le nombre de polynômes irréductibles intervenant dans la décomposi-

tion de F: $F = F_1 \dots F_\kappa$, où les F_k sont irréductibles et donc premiers entre eux deux à deux, d'après la condition (C); notons que l'on a: $1 \leqq \kappa \leqq \partial^0 F$.

Vérifions que les conditions (Ω_1), (Ω_2) et (R) du lemme (7) sont satisfaites:

(Ω_1) Notons tout d'abord que la minoration $\omega(p)/p \geqq 0$ est triviale; nous allons montrer que l'on a $\omega(p)/p \leqq 1 - 1/2C$, où C est un majorant des termes $\rho(p^\alpha)$ (cf. lemme (3) pour l'existence de C); distinguons deux cas:

(i) si p est supérieur ou égal à $2C+1$, on a:
$\omega(p)/p \leqq \lambda(p)/(p-1) \leqq C/2C \leqq \frac{1}{2} \leqq 1 - 1/2C$.

(ii) si p est inférieur ou égal à $2C$, il suffit de démontrer que $\omega(p)/p$ est inférieur ou égal à $(p-2)/(p-1)$, et il suffit donc de démontrer que $\omega(p)$ est nul dès que $\lambda(p)$ est égal à $p-1$; distinguons encore deux cas:

(α) si $p = p_0$, on a $\lambda(p_0) < p_0 - 1$ par le lemme (1)

(β) si $p \neq p_0$, et si $\lambda(p) = p-1$, on a $F(p_0) \equiv 0 \,(\text{mod. } p)$ donc p divise K et il résulte de la définition de ω que $\omega(p) = 0$.

(Ω_2) Soit λ_k $(k = 1, \dots, \kappa)$ la fonction λ relative au polynôme F_k, i.e.

$$\lambda_k(p) = \text{Card}\,\{m : 0 < m < p, F_k(m) \equiv 0 \,(\text{mod. } p)\},$$

et définissons de manière similaire la fonction ρ_k; il existe un entier D tel que pour tout nombre premier p supérieur à D, on ait:

$$\lambda_k(p) = \rho_k(p) \qquad (k = 1, \dots, \kappa),\ \lambda(p) = \rho(p)$$

$$\rho(p) = \sum_{k=1}^{\kappa} \rho_k(p)$$

en effet les deux premières relations sont satisfaites dès que D est supérieur à $F(0)$; par ailleurs le p.g.c.d. des polynômes F_i et F_j (avec $i \neq j$) est un entier strictement positif $D_{i,j}$, et dès que p est supérieur à tous les $D_{i,j}$, tout système de la forme $F_i(m) \equiv F_j(m) \equiv 0 \,(\text{mod. } p)$ est impossible, et cela implique la troisième relation.

Pour vérifier (Ω_2), il suffit alors de vérifier chacune des relations:

$$\Big| \sum_{w \leqq p < u} \rho_k(p) \cdot \text{Log}\, p \cdot p^{-1} - \text{Log}\,(u/w) \Big| = O(1)$$

et cela est un résultat classique dû à T. Nagel (cf. [7]).

(R) Avec nos notations, nous avons:

$$R_d(X) = \text{Card}\,\{p \leqq N : p \equiv U \,(\text{mod. } K) \text{ et } F(p) \equiv 0 \,(\text{mod. } d)\} - X \cdot \omega(d)/d.$$

Lorsque d et K sont premiers entre eux (c'est le cas qui nous interesse), le système $p \equiv U \,(\text{mod. } K)$, $F(p) \equiv 0 \,(\text{mod. } d)$ équivaut à $\rho(d)$ systèmes:

$$\begin{cases} p \equiv U \,(\text{mod. } K) \\ F(p) \equiv v_\ell \,(\text{mod. } d) \end{cases} \qquad \ell = 1, \ldots, \rho(d)$$

qui lui-même équivaut à $\rho(d)$ congruences:

$$p \equiv V_\ell \,(\text{mod. } K \cdot d) \qquad \ell = 1, \ldots, \rho(d).$$

Parmi ces $\rho(d)$ congruences, $\lambda(d)$ sont de la forme:

$$p \equiv V_\ell \,(\text{mod. } K \cdot d), \qquad \text{avec } (V_\ell, K \cdot d) = 1,$$

et $\rho(d) - \lambda(d)$ sont de la forme:

$$p \equiv V_\ell \,(\text{mod. } K \cdot d), \qquad \text{avec } (V\ , K \cdot d) > 1.$$

On peut donc écrire:

$$|R_d(X)| = \Big|\sum_{l=1}^{\lambda(d)} \pi(N; K \cdot d, V_\ell) + \sum_{\ell=\lambda(d)+1}^{\rho(d)} \pi(N; K \cdot d, V_\ell) - X \cdot \omega(d)/d\Big|$$

d'après la définition de X et de ω, on a:

$$X \cdot \omega(d)/d = (\text{li } N)/\varphi(K \cdot d), \qquad (\text{car } (K, d) = 1);$$

en utilisant la notation introduite dans le lemme (4), on a:

$$|R_d(X)| \leqq \rho(d) E^*(N; K \cdot d) \leqq C^{\nu(d)} \cdot E^*(N; K \cdot d).$$

On en déduit:

$$\begin{aligned} \sum_{d < X^{5/12},\,(d,K)=1} \mu^2(d) 3^{\nu(d)} |R_d(X)| &\leqq \sum_{d < X^{5/12}} (3+C)^{\nu(d)} E^*(N; K \cdot d) \\ &\leqq \sum_{\delta < (KX)^{5/12}} (3+C)^{\nu(\delta)} \cdot E^*(N;\ \delta), \end{aligned}$$

et la vérification de la condition (R) est ramenée à une simple application du lemme (4).

Les conditions du lemme (7) étant satisfaites, il existe (lorsque N est suffisamment grand) un nombre premier p inférieur à N, congru à U

modulo K et tel que tout facteur premier de $F(p)$ ou bien divise K, ou bien est supérieur à $N^{1/10\partial^0 F}$ (on a en effet: $(li\, N/\varphi(K))^{1/9} \gg N^{1/10\partial^0 F}$); d'après la relation (26), la congruence $p \equiv U \pmod{K}$ implique:

$$r_j \| F(p) \quad (j = 1, \ldots, s) \quad \text{et} \quad q_i^{\alpha_i} \| F(p) \qquad (i = 1, \ldots, n).$$

On peut donc trouver une infinité de nombres premiers p tels que l'on ait:

$$(27) \quad F(p) = \prod_{j=1}^{s} r_j \prod_{i=1}^{n} q_i^{\alpha_i} \prod_{k=1}^{10(\partial^0 F)^2} p_k^{\beta_k} \quad \text{avec} \quad p_k > p^{1/10\partial^0 F} \quad \text{et} \quad \beta_k \leqq 10(\partial^0 F)^2.$$

6.3. D'après la multiplicativité de la fonction g, on a:

$$g(F(p)) = \prod_{j=1}^{s} g(r_j) \prod_{i=1}^{n} g(q_i^{\alpha_i}) \prod_{k=1}^{10(\partial^0 F)^2} g(p_k^{\beta_k})$$

d'après les relations (27) et (9), pour tout nombre réel positif ε, on peut trouver un nombre premier p satisfaisant:

$$(28) \quad \prod_{j=1}^{s} g(r_j) \prod_{i=1}^{n} g(q_i^{\alpha_i}) - \varepsilon < g(F(p)) < \prod_{j=1}^{s} g(r_j) \prod_{i=1}^{n} g(q_i^{\alpha_i});$$

en prenant ε assez petit, il résulte alors de (25d) et (28) que l'on peut trouver un nombre premier p (arbitrairement grand) tel que:

$$y < g(F(p)) < x$$

il résulte alors du Théorème (1) que l'on a l'inégalité:

$$G(y) < G(x).$$

6.4. La même démonstration implique que pour tout nombre réel positif z inférieur à y, on a $G(z) < G(y)$; il en résulte que $G(y)$ est strictement positif et la démonstration de la Proposition (2) est achevée. Le Théorème (2) s'en déduit immédiatement.

7. Demonstration du théorème (0)

La seule partie du théorème (0) qui ne résulte pas trivialement des

théorèmes A, (1) et (2) est le fait que la valeur du 'θ' du théorème (2) soit $g(2)$.

On a évidemment $G(g(2)) = 1$, car pour tout nombre premier impair p, on peut écrire:

$$p+1 = 2^k \cdot a, \qquad \text{avec } k \geqq 1 \quad \text{et} \quad 2 \nmid a;$$

on a alors:

$$g(p+1) = g(2^k) \cdot g(a) \leqq g(2^k) = g(2) \ (g \text{ est } \textit{fortement} \text{ multiplicative}).$$

Il résulte de la partie 6.2. que l'on peut trouver une suite $(p_m)_{m \in \mathbb{N}}$ de nombres premiers tels qúe l'on ait: $p_m + 1 \neq 2a_m$, où a_m a au plus 10 facteurs premiers (comptés avec leur multiplicité) tous supérieurs à $p^{1/10}$; puisque $g(p^\alpha)$ tend vers 1 (en effet g est *fortement* multiplicative et $1-g(p)$ tend vers 0), on a:

$$\lim_{m \to \infty} g(p_m+1) = \lim_{m \to \infty} g(2) \cdot g(a_m) = g(2);$$

soit alors x un nombre réel positif inférieur strictement à $g(2)$, on peut trouver un nombre premier impair tel que $g(p) > x$ et d'après la première partie du Théorème (0), on a $G(x) < 1$.

Added in Proof

Je tiens à remercier H. Delange qui m'a fait remarquer: 1^0 que le résultat obtenu par P. D. T. A. Elliott (cf. [3]) pour les fonctions fortement additives à valeurs positives a été récemment étendu par H. Daboussi au cas des fonctions additives à valeurs positives. 2^0 que si l'on suppose, dans le Théorème A, que la série $\sum (1-g(p)) \cdot p^{-1}$ diverge (pour g simplement multiplicative) alors la fonction G, si elle existe, possède un saut à l'origine et ne peut donc être continue.

Pour l'une ou l'autre de ces deux raisons, le Théorème 0 peut être étendu aux fonctions g multiplicztives à valeur dans $]0, 1]$, sous réserve de remplacer l'expression $g(2)$ de la fin de l'énoncé par $\mathrm{Sup}_{k \geqq 1} g(2^k)$.

BIBLIOGRAPHIE

[1] E. BOMBIERI: On the large sieve. *Mathematika 12* (1965) 201–225.
[2] J. M. DESHOUILLERS: Sur la répartition des valeurs des fonctions multiplicatives définies sur l'ensemble des nombres premiers moins un. *C. R. Acad. Sci. Paris Sér. A–B 271* (1970) A1141–A1143.
[3] P. D. T. A. ELLIOTT: On the limiting distribution of $f(p+1)$ for non-negative additive function. *Acta Arith. 25* (1974) 259–264.
[4] H. HALBERSTAM et H. E. RICHERT: *Sieve Methods*. Academic Press, London 1974.
[5] I. KATAI: On the distribution of arithmetical functions. *Acta Math. Acad. Sci. Hung. 20* (1969) 69–87.
[6] I. KATAI: On distribution of arithmetical functions on the set of prime plus one. *Compositio Math. 19* (1968) 278–289.
[7] T. NAGEL: *J. Math. Pures Appl. (8) 4* (1921) 343–356.
[8] H. E. RICHERT: Selberg's sieve with weights. *Mathematika 16* (1969) 1–22.

(Oblatum 6–XII–74 & 16–II–75)

U.E.R. de Mathématiques
Laboratoire associé au C.N.R.S.
Université de Bordeaux I
351, cours de la Libération
33405 TALENCE France