

GRANDES VALEURS D'UNE FONCTION LIEE AU PRODUIT D'ENTRIERS CONSECUTIFS

Paul Erdős ⁽¹⁾ et Jean-Louis Nicolas ⁽²⁾

*(1)(2) Département de Mathématiques, U.E.R. des Sciences de Limoges, 123 rue Albert Thomas
 87060 Limoges - France.*

Résumé : Désignons par $f(n)$ le plus grand entier k pour lequel il existe un m tel que $n \mid \prod_{1 \leq i \leq k} (m+i)$ et que n ne divise aucun produit de $k-1$ nombres choisis parmi $m+1, \dots, m+k$. Nous remarquons d'abord que la valeur moyenne de $f(n)$, pour $1 \leq n \leq x$ est environ $\log \log x$.

Nous démontrons :

$$\max_{n \leq x} f(n) = \frac{e^{\gamma/2}}{2} \frac{\log x}{\sqrt{\log \log x}} + \frac{\gamma e^{\gamma}}{4} \frac{\log x}{\log \log x} (1+o(1))$$

(γ = Constante d'Euler).

On dit que n est f -hautement abondant, si $n' < n \Rightarrow f(n') < f(n)$. Nous faisons une étude détaillée des facteurs premiers des nombres f -hautement abondants. Les résultats montrent quelques ressemblances, mais aussi de nettes différences avec les nombres hautement composés de Ramanujan, par exemple les facteurs premiers des nombres f -hautement abondants sont loin d'être des nombres premiers consécutifs.

Nous énonçons quelques problèmes irrésolus.

Summary : Denote by $f(n)$ the largest integer k for which there is an m so that $n \mid \prod_{i=1}^k (m+i)$, but n does not divide the product of any $(k-1)$ of the integers $m+1, \dots, m+k$. We first of all observe that the mean value of $f(n)$, for $n \in [1, x]$ is about $\log \log x$.

We prove

$$\max_{n \leq x} f(n) = \frac{1}{2} e^{\gamma/2} \frac{\log x}{\sqrt{\log \log x}} + \frac{\gamma e^{\gamma}}{4} \frac{\log x}{\log \log x} (1+o(1))$$

(γ = Euler constant).

Define n to be f -highly abundant if, for every $n' < n$, we have $f(n') < f(n)$. We make a detailed study of the prime factors of the f -highly abundant numbers. The results show some similarity but also striking contrast with the highly composite numbers of Ramanujan e. g. there are very large gaps in the prime factorisation of the f -highly abundant numbers.

We state several unsolved problems.

I. - INTRODUCTION

Soit $m \geq 1$, $k \geq 1$. On pose $\pi = \pi(m, k) = (m+1)\dots(m+k)$ et pour $1 \leq i \leq k$, $\pi_i^* = \pi_i^*(m, k) = \frac{\pi(m, k)}{m+i}$.

On appelle $P(m, k)$ l'ensemble des n tels que $n \mid \pi$ et $\forall i, 1 \leq i \leq k, n \nmid \pi_i^*$. Si $n \in P(m, k)$, on a $\forall i, 1 \leq i \leq k, (m+i, n) > 1$. Si $n \in P(m, k)$, $\forall i, 1 \leq i \leq k, \exists q$ premier, $q \mid n$ tel que $v_q(n) > v_q(\pi_i^*)$, en désignant par v_q la valuation q -adique.

Pour n fixé, on appelle $f(n)$ le plus grand k pour lequel il existe m tel que $n \in P(m, k)$. On a $f(n) \leq n$ et comme $m \equiv m' \pmod{n}$ entraîne $P(m, k) = P(m', k)$, on a :

$$f(n) = \max \{ k ; n \in P(m, k) ; 1 \leq m \leq n ; 1 \leq k \leq n \}.$$

Exemple : Soit $n = t!$. On a de façon évidente $t! \in P(1, t-1)$, ce qui entraîne $f(t!) \geq t-1$. D'autre part, pour tout $m \geq 1$, $t! \mid \pi(m, t)$, ce qui entraîne que $\forall m \geq 1$, $t! \notin P(m, t+1)$ et donc $f(t!) \leq t$. P. ERDÖS avait conjecturé que pour $n \geq 2k$, $\binom{n}{k}$ avait un diviseur de la forme $n-i$, $0 \leq i \leq k-1$. Dans l'article [Sch], A. SCHINZEL donnait le contre exemple $n = 99215$, $k = 15$, et A. SCHINZEL et P. ERDÖS démontraient que la conjecture était fautive pour une infinité de n . Peut être existe-t-il une constante $c > 0$ telle que $\binom{n}{k}$ a un diviseur d vérifiant $cn \leq d \leq n$. Il en résulte pour la fonction f : pour $1 \leq t \leq 14$, $f(t!) = t-1$, $f(15!) = 15$, car $15! \in P(99200, 15)$ et pour une infinité de t , on a $f(t!) = t$.

L'étude de la fonction f est une généralisation du problème de JACOBSTAHL (cf. [Erd]), qui propose d'étudier $C(n)$ la longueur de la plus longue suite d'entiers tous non premiers avec n . On a : $f(n) \leq C(n)$, et on peut montrer qu'il existe a tel que $f(n^a) = C(n)$. Le théorème 2 nous donnera une estimation asymptotique pour l'ordre maximum de $f(n)$. On connaît beaucoup moins sur $C(n)$. (cf. [Iwa]). On trouvera d'autres résultats sur des sujets voisins dans [Sel] et [Gri].

Nous démontrerons les théorèmes suivants :

THEOREME 1. Soit $\omega(n) = \sum_{p|n} 1$; $\Omega(n) = \sum_{p|n} v_p(n)$; $\omega^*(n) = \sum_{p|n, p > \omega(n)} 1$. Alors on a :
 $\omega^*(n) \leq f(n) \leq \Omega(n)$ pour tout n , et

$$\sum_{n \leq x} f(n) = (x \log \log x)(1+o(1)).$$

Il est faux que $\omega(n) \leq f(n)$: $f(210) = 3$.

THEOREME 2. L'ordre maximum de la fonction $f(n)$ est :

$$e^{\gamma/2} \frac{\log n}{\sqrt{\log \log n}} + \frac{\gamma e^{\gamma}}{4} \frac{\log n}{\log \log n} (1+o(1))$$

où γ est la constante d'Euler, ce qui veut dire que $f(n)$ est toujours inférieur ou égal à cette quantité, et qu'il y a égalité pour une infinité de n .

THEOREME 3. On dit que n est f-hautement abondant si $n' < n \Rightarrow f(n') < f(n)$. Il existe des constantes c_1 et $c_2 > 0$ telles que, pour un nombre n f-h.a. assez grand, on ait, en posant $k = f(n)$:

i) Si p premier vérifie

$$\log p \leq e^{-\gamma/2} \sqrt{\log k} \left(1 - \frac{c_1}{\sqrt[4]{\log k}}\right)$$

alors p divise n .

ii) Si p premier vérifie

$$e^{-\gamma/2} \sqrt{\log k} \left(1 + \frac{c_2}{\sqrt[4]{\log k}}\right) \leq \log p \text{ et } p \leq k/2$$

alors p ne divise pas n .

iii) Si $p | n$ et si $p > k$, alors tous les nombres premiers q tels que $k < q < p$ divisent n et le plus grand facteur premier P de n vérifie : $P \sim 1/2 \log n$.

Pour étudier les grandes valeurs de la fonction f , nous avons défini, après RAMANUJAN (cf [Ram]), les nombres f-h.a. Les premières valeurs sont 2, 6, 24, 120, 560. On a $560 = 2^4 \cdot 5 \cdot 7 \in P(73,5)$, et c'est la forme de ce nombre, non multiple de 3 qui a fait deviner la forme générale des nombres f-h.a. donnée par le théorème 3.

La précision des résultats des théorèmes 2 et 3 est surprenante, si l'on compare avec ceux obtenus sur le problème de JACOBSTAHN par exemple. De même si l'on considère la restriction f_Q de f à l'ensemble $Q = \{n ; p < q \Rightarrow v_p(n) \geq v_q(n)\}$ il est impossible de donner un équivalent pour l'ordre maximum de F_Q . On a : $f_Q(n) \leq \frac{2 \log n}{\log \log n} (1+o(1))$ pour tout n , en utilisant la proposition 3 et les résultats du crible linéaire (cf. [Iwa]). Mais on ne peut pas affirmer

pour le moment l'existence de k entiers consécutifs tous multiples d'un nombre premier $p \leq k^{1-\epsilon}$.

La meilleure minoration est donc $f_Q(n) \geq \frac{\log n}{\log \log n} (1+o(1))$ pour une infinité de n (comprenant les valeurs $n = t!$).

Au paragraphe 2, nous démontrons le théorème 1 et au paragraphe 3, la minoration dans le théorème 2. Au paragraphe 4 nous prouvons deux lemmes qui ont un intérêt intrinsèque :

Le lemme 3 est un lemme de crible linéaire et nous remercions H. IWANIEC pour ses remarques sur ce sujet. Ce lemme sera l'outil fondamental de toutes les démonstrations qui suivront. Malheureusement nous ne donnons pas de valeurs numériques aux constantes qui y figurent, car elles sont difficilement calculables ; cela nous empêche d'explicitier c_1 et c_2 dans le théorème 3. On ne peut donc pas utiliser i et ii de ce théorème pour construire un algorithme de calcul des nombres f-h.a.

Le lemme 4 étudie la relation entre les quantités : $W = \prod_{p \in \mathcal{P}} (1-1/p)$ et $S = \sum_{p \in \mathcal{P}} (\log p/p)$ définies sur un ensemble \mathcal{P} de nombres premiers.

Le paragraphe 5 donne une première majoration de f basée sur les lemmes 3 et 4 et sur la notion de facteur premier «essentiel» de $n \in P(m,k)$. Le paragraphe 6 étudie les nombres f-h.a. Les propositions 5 à 9 fournissent des propriétés de ces nombres et forment un cheminement qui mène à la démonstration du théorème 3. On peut noter ici que la structure des nombres f-h.a. est très différente de celle des nombres hautement composés de RAMANUJAN avec essentiellement deux blocs de facteurs premiers : les petits nombres premiers d'une part, et ceux plus grands que $k/2$ d'autre part.

Enfin, le paragraphe 7 utilise les résultats du théorème 3 pour appliquer la méthode de crible dans de meilleures conditions que dans le paragraphe 5, ce qui nous donne les deux premiers termes du développement asymptotique de l'ordre maximum de f (qui constituent le théorème 2). Au prix de calculs plus longs, il est d'ailleurs possible d'améliorer ce développement.

II. - DEMONSTRATION DU THEOREME 2

Soit $n = p_1^{\alpha_1} \dots p_r^{\alpha_r} p_{r+1}^{\alpha_{r+1}} \dots p_{r+s}^{\alpha_{r+s}}$ la décomposition de n en facteurs premiers, r étant choisi tel que $p_r \leq \omega(n) < p_{r+1}$. On a donc $\omega^*(n) = s$ et on pose $n' = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. Soit m une solution des congruences :

$$\begin{cases} m \equiv -1 \pmod{n'} \\ m \equiv r-i \pmod{p_i^{\alpha_i}}, r+1 \leq i \leq r+s. \end{cases}$$

On a alors $n \in P(m,s)$ et donc $f(n) \geq s = \omega^*(n)$.

Pour démontrer $f(n) \leq \Omega(n)$, on raisonne par récurrence sur la valeur de $\Omega(n) = A$. Si n est premier, on a $f(n) = 1 = \Omega(n)$. Supposons que pour $\Omega(n) \leq A-1$ on ait $f(n) \leq \Omega(n)$ et soit n tel que $\Omega(n) = A$. Soit $k = f(n)$, et soit m tel que $n \in P(m, k)$. On a $(n, m+k) = d > 1$. Montrons que $n/d \in P(m, k-1)$. En effet $n \mid \pi(m, k) \Rightarrow n/d \mid \pi(m, k-1)$, et si n/d divisait $\pi_i^*(m, k-1)$ avec $1 \leq i \leq k-1$, cela entraînerait que n divise $\pi_i^*(m, k)$, ce qui est faux. On a donc :

$$f(n/d) \geq k-1 = f(n)-1$$

et l'hypothèse de récurrence dit que $f(n/d) \leq \Omega(n/d) \leq \Omega(n)-1$; cela donne $f(n) \leq \Omega(n)$.

On a ensuite

$$\begin{aligned} \sum_{n=1}^x \omega^*(n) &\geq \sum_{\substack{n=1 \\ \omega(n) \leq 3 \log \log x}}^x \sum_{\substack{p \mid n \\ p > 3 \log \log x}} 1 = \\ &= \sum_{n=1}^x \sum_{\substack{p \mid n \\ p > 3 \log \log x}} 1 - \sum_{\substack{n=1 \\ \omega(n) > 3 \log \log x}}^x \sum_{\substack{p \mid n \\ p > 3 \log \log x}} 1 = S_1 - S_2 \end{aligned}$$

On a

$$S_2 \leq \sum_{\substack{n=1 \\ \omega(n) > 3 \log \log x}}^x \sum_{\substack{\omega(n) \leq \frac{\log x}{\log 2} \\ \omega(n) > 3 \log \log x}} 1$$

et par la proposition 3 de [Nic], $S_2 = o(x)$.

Evaluons S_1 :

$$S_1 = \sum_{3 \log \log x < p \leq x} \left[\frac{x}{p} \right] = x \log \log x + O(x \log \log \log x)$$

On a donc $\sum_{n \leq x} \omega^*(n) \geq x \log \log x (1+o(1))$ et comme on a $\sum_{n \leq x} \Omega(n) = x \log \log x (1+o(1))$,

(cf. [Har], ch. 22) cela achève la démonstration du théorème 1.

III. - LA MINORATION DANS LE THEOREME 2

Nous allons démontrer la proposition suivante :

PROPOSITION 1. Soit k assez grand, il existe n tel que $f(n) \geq k$ et tel que

$$\log n \leq 2k e^{-\gamma/2} \sqrt{\log k} - k \gamma + O\left(\frac{k \log \log k}{\sqrt{\log k}}\right)$$

La démonstration repose sur deux lemmes :

LEMME 1. Soit $k \in \mathbb{N}$, $k \geq 4$. Soit p un nombre premier, $p \leq k/2$. Si $p^\alpha \parallel k!$, alors $p^\alpha > k$.

Démonstration. On s'assure d'abord directement que le lemme est vrai pour $k \leq 8$. Supposons maintenant $k \geq 9$. On sait que l'on a :

$$\alpha = v_p(k!) = [k/p] + [k/p^2] + \dots > (k/p) - 1$$

Pour $p = 2$, on a $\alpha = v_2(k!) > (k/2) - 1$, et l'on a pour tout $x \geq 8$, $2^{x/2-1} \geq x$, d'où l'on déduit $2^\alpha > k$.

Pour $3 \leq p \leq k/3$, l'étude de la fonction $x \rightarrow ((k/x) - 1) \log x$ décroissante pour $x \geq e$ montre que :

$$p^\alpha > p^{k/p-1} \geq (k/3)^2 \geq k$$

Pour $k/3 < p \leq k/2$, c'est-à-dire $2 \leq k/p < 3$, on a $\alpha = v_p(k!) = 2$ et $p^\alpha > k^2/9 \geq k$.

LEMME 2. Soit $v_p(m)$ la valuation p -adique de m . Si l'on a $v_p(m) = \alpha \geq 1$ et si $v_p(j) < \alpha$ (en particulier si $1 \leq j < p^\alpha$) alors on a $v_p(m+j) = v_p(j)$.

Démonstration. C'est une propriété classique de la valuation p -adique.

Démonstration de la Proposition 1. Soit k assez grand, et $z \leq k/2$. Soit $p_1 = 2, p_2 = 3, \dots, p_r$ les nombres premiers $\leq z$, et soit $1 = u_1 < u_2 < \dots < u_s < k$ les nombres dont tous les facteurs premiers sont $> z$. On a donc $s = \Phi(k, z)$, où Φ est la fonction de De BRUIJN (cf. [Bru]). Soit maintenant $k < q_1 < q_2 < \dots < q_s < 2k \log k$, s nombres premiers. On pose, pour $1 \leq i \leq r$:

$$\alpha_i = v_{p_i}(k!) = [k/p_i] + [k/p_i^2] + \dots$$

On a :

$$(k/p_i) - 1 \leq \alpha_i \leq k/(p_i - 1)$$

On résout les congruences :

$$\begin{cases} m + u_i \equiv 0 \pmod{q_i}, & 1 \leq i \leq s \\ m \equiv 0 \pmod{p_i^{\alpha_i}}, & 1 \leq i \leq r \end{cases}$$

On pose $n = \prod_{1 \leq i \leq s} q_i \prod_{1 \leq i \leq r} p_i^{\alpha_i}$. Soit m une solution des congruences précédentes. Montrons que l'on a $n \in P(m, k)$.

On a d'abord $n \mid \pi$ puisque $q_i \mid (m+u_i)$, que $p_i^{\alpha_i} \mid k!$ et que $\pi = k! \binom{m+k}{k}$.

Ensuite, montrons que n ne divise pas π_j^* pour tout j , $1 \leq j \leq k$. Si $j = u_i$, comme $q_i > k$, $m + u_i$ est le seul facteur de π divisible par q_i , donc $q_i \nmid \pi_j^*$ et donc $n \nmid \pi_j^*$.

Si $j \neq u_i$ pour tout i , alors j a un facteur premier $p \leq z$. On a : $v_p(n) = v_p(\pi)$. En effet, $v_p(n) = v_p(k!)$ et par les lemmes 1 et 2, $v_p(k!) = v_p(\pi)$.

On a donc $v_p(\pi_j^*) < v_p(\pi) = v_p(n)$ et $n \nmid \pi_j^*$. Comme $n \in P(m, k)$, on a donc $f(n) \geq k$. On a ensuite :

$$\begin{aligned} \log n &= \sum_{p \leq z} v_p(k!) \log p + \sum_{i=1}^s \log q_i \\ &\leq \sum_{p \leq z} \frac{k \log p}{p-1} + s \log(2k \log k) \end{aligned}$$

On choisit $\log z = e^{-\gamma/2} \sqrt{\log k}$. D'après les formules 1.6 et 1.16 de De BRUIJN [Bru], on a :

$$s = \Phi(k, z) = k \left(\prod_{p \leq z} (1-1/p) \right) \left(1 + O\left(e^{-\frac{\log k}{\log z}} \right) \right)$$

et avec la formule de MERTENS, (cf. [Pra]), p. 81)

$$s = \Phi(k, z) = \frac{k e^{-\gamma/2}}{\sqrt{\log k}} \left(1 + O\left(\frac{1}{\log k} \right) \right)$$

On a d'autre part, (cf. [Lan], p. 200) :

$$\sum_{p \leq z} \frac{\log p}{p-1} = \log z - \gamma + O\left(\frac{1}{\log z} \right)$$

ce qui achève la démonstration de la proposition 1.

IV. - DEUX LEMMES IMPORTANTS

LEMME 3 (Lemme de crible). Soit \mathcal{A} un ensemble de X nombres entiers consécutifs. Soit \mathcal{P} un ensemble de nombres premiers tels que :

$$(1) \quad \sum_{\substack{p \leq X \\ p \in \mathcal{P}}} \frac{\log p}{p} \leq \lambda \sqrt{\log X}$$

où λ est un nombre positif fixé. On pose $W(z) = \prod_{\substack{p \leq z \\ p \in \mathcal{P}}} (1 - \frac{1}{p})$. Soit $\mathcal{S}(\mathcal{A}, \mathcal{P}, z)$ l'ensemble des éléments de \mathcal{A} divisibles par aucun nombre premier $p \in \mathcal{P}$, $p < z$, et $S(\mathcal{A}, \mathcal{P}, z) = \text{card } \mathcal{S}(\mathcal{A}, \mathcal{P}, z)$; alors on a :

pour $1 \leq z \leq X \exp(-\sqrt{\log X})$:

$$(2) \quad S(\mathcal{A}, \mathcal{P}, z) = X W(z) \left(1 + O\left(\frac{1}{\sqrt{\log X}}\right)\right)$$

et pour $1 \leq z \leq X$:

$$(3) \quad S(\mathcal{A}, \mathcal{P}, z) = X W(z) \left(1 + O\left(\frac{\log \log X}{\sqrt{\log X}}\right)\right)$$

où les 0 dépendent de λ , mais sont uniformes par rapport à \mathcal{A} , \mathcal{P} , z .

Démonstration. La condition (1) entraîne :

$$(4) \quad \sum_{\substack{p \in \mathcal{P} \\ z \leq p \leq X}} \frac{1}{p} \leq \frac{1}{\log z} \sum_{\substack{p \in \mathcal{P} \\ z \leq p \leq X}} \frac{\log p}{p} \leq \lambda \frac{\sqrt{\log X}}{\log z}$$

On pose $z_1 = \exp\left(\frac{\log X}{\log \log 3 X}\right)$. Alors le lemme fondamental de la théorie du crible linéaire dit que pour $z \leq z_1$ on a : (cf. [Hal], p. 82 ou p. 209)

$$(5) \quad S(\mathcal{A}, \mathcal{P}, z) = X W(z) \left(1 + O\left(\frac{1}{\log X}\right)\right)$$

On a ensuite, compte tenu de (4), pour $z_1 < z \leq X$:

$$\begin{aligned} \frac{W(z)}{W(z_1)} &= \sum_{\substack{z_1 \leq p < z \\ p \in \mathcal{P}}} \left(1 - \frac{1}{p}\right) = \exp\left(\sum_{\substack{z_1 \leq p < z \\ p \in \mathcal{P}}} \log\left(1 - \frac{1}{p}\right)\right) = \exp\left(-\sum_{\substack{z_1 \leq p < z \\ p \in \mathcal{P}}} \frac{1}{p} + O\left(\frac{1}{z_1}\right)\right) \\ &= \exp\left(O\left(\frac{1}{z_1}\right)\right) \left(1 - \sum_{\substack{z_1 \leq p < z \\ p \in \mathcal{P}}} \frac{1}{p} + O\left(\frac{\log X}{\log^2 z_1}\right)\right) \end{aligned}$$

$$(6) \quad \frac{W(z)}{W(z_1)} = \left(1 - \sum_{\substack{z_1 \leq p < z \\ p \in \mathcal{P}}} \frac{1}{p}\right) \left(1 + O\left(\frac{(\log \log 3 X)^2}{\log X}\right)\right)$$

Lorsque $z_1 \leq z \leq X^{1/3}$, on applique deux fois l'inégalité de BUCHSTAB (cf. [Hal], p. 39), où \mathcal{A}_d désigne l'ensemble des éléments de \mathcal{A} multiples de d :

$$S(\mathcal{A}, \mathcal{P}, z) = S(\mathcal{A}, \mathcal{P}, z_1) - \sum_{\substack{z_1 \leq p < z \\ p \in \mathcal{P}}} S(\mathcal{A}_p, \mathcal{P}, p)$$

$$S(\mathcal{A}_p, \mathcal{P}, p) = S(\mathcal{A}_p, \mathcal{P}, z_1) - \sum_{\substack{z_1 \leq q < p \\ q \in \mathcal{P}}} S(\mathcal{A}_{pq}, \mathcal{P}, q)$$

On a donc :

$$S(\mathcal{A}, \mathcal{P}, z) \geq S(\mathcal{A}, \mathcal{P}, z_1) - \sum_{\substack{z_1 \leq p < z \\ p \in \mathcal{P}}} S(\mathcal{A}_p, \mathcal{P}, z_1)$$

et

$$S(\mathcal{A}, \mathcal{P}, z) \leq S(\mathcal{A}, \mathcal{P}, z_1) - \sum_{\substack{z_1 \leq p < z \\ p \in \mathcal{P}}} S(\mathcal{A}_p, \mathcal{P}, z_1) + \sum_{\substack{z_1 \leq q < p < z \\ p, q \in \mathcal{P}}} S(\mathcal{A}_{pq}, \mathcal{P}, z_1)$$

Comme $z \leq X^{1/3}$, on peut appliquer le lemme fondamental de la théorie du crible linéaire :

$$S(\mathcal{A}_p, \mathcal{P}, z_1) = \frac{X}{p} W(z_1) \left(1 + O\left(\frac{1}{\log X}\right)\right)$$

$$S(\mathcal{A}_{pq}, \mathcal{P}, z_1) = O\left(\frac{X}{pq}\right) W(z_1)$$

et l'on a, avec (4) :

$$\sum_{\substack{z_1 \leq q < p < z \\ q, p \in \mathcal{P}}} \frac{1}{pq} \leq \left(\sum_{\substack{z_1 \leq p < z \\ p \in \mathcal{P}}} \frac{1}{p}\right)^2 = O\left(\frac{(\log \log 3X)^2}{\log X}\right)$$

Il s'ensuit que, en utilisant (5) avec $z = z_1$:

$$S(\mathcal{A}, \mathcal{P}, z) = X W(z_1) \left(1 - \sum_{\substack{z_1 \leq p < z \\ p \in \mathcal{P}}} \frac{1}{p} + O\left(\frac{1}{\log X} \sum_{\substack{z_1 \leq p < z \\ p \in \mathcal{P}}} \frac{1}{p}\right) + O\left(\frac{(\log \log 3X)^2}{\log X}\right)\right)$$

et par (4) et (6), on a pour $z_1 \leq z \leq X^{1/3}$:

$$(7) \quad S(\mathcal{A}, \mathcal{P}, z) = X W(z) \left(1 + O\left(\frac{(\log \log 3X)^2}{\log X}\right)\right)$$

On pose $z_0 = \exp(\sqrt{\log X})$ et $z_3 = X/z_0$. Lorsque $X^{1/3} \leq z \leq X$, on remarque que l'on a (comme pour (6)) :

$$(8) \quad \frac{W(z)}{W(X^{1/3})} = 1 + O\left(\frac{1}{\sqrt{\log X}}\right), \text{ puisque } \sum_{\substack{X^{1/3} \leq p \\ p \in \mathcal{P}}} \frac{1}{p} \leq \frac{3\lambda}{\sqrt{\log X}}$$

et que, pour $z_0 \leq z \leq X$, on a :

$$(9) \quad W(z) \asymp W(z_0) \text{ puisque } \sum_{\substack{z_0 \leq p \\ p \in \mathcal{P}}} \frac{1}{p} \leq \lambda$$

Il vient alors ; pour $X^{1/3} \leq z \leq z_3$:

$$(10) \quad S(\mathcal{A}, \mathcal{P}, z) = S(\mathcal{A}, \mathcal{P}, X^{1/3}) - \sum_{\substack{X^{1/3} \leq p < z \\ p \in \mathcal{P}}} S(\mathcal{A}_p, \mathcal{P}, p)$$

Mais, par le lemme fondamental :

$$S(\mathcal{A}_p, \mathcal{P}, p) \leq S(\mathcal{A}_p, \mathcal{P}, z_0) \ll \frac{X}{p} W(z_0)$$

et :

$$(11) \quad \sum_{\substack{X^{1/3} \leq p < z \\ p \in \mathcal{P}}} S(\mathcal{A}_p, \mathcal{P}, p) \ll X W(z_0) \sum_{\substack{X^{1/3} \leq p \\ p \in \mathcal{P}}} 1/p \ll \frac{X W(z_0)}{\sqrt{\log X}} \ll \frac{X W(z)}{\sqrt{\log X}}$$

compte tenu de (4) et (9).

On a, par (7) et (8) :

$$S(\mathcal{A}, \mathcal{P}, X^{1/3}) = X W(z) \left(1 + O\left(\frac{(\log \log 3 X)^2}{\log X}\right) \right)$$

et par (10) et (11), pour $X^{1/3} \leq z \leq z_3$:

$$(12) \quad S(\mathcal{A}, \mathcal{P}, z) = X W(z) \left(1 + O\left(\frac{1}{\sqrt{\log X}}\right) \right)$$

ce qui avec (5) et (7) démontre (2).

La démonstration de (3) est du même type : Soit $z_3 \leq z \leq X$, on a :

$$(13) \quad S(\mathcal{A}, \mathcal{P}, z) = S(\mathcal{A}, \mathcal{P}, z_3) - \sum_{\substack{z_3 \leq p < z \\ p \in \mathcal{P}}} S(\mathcal{A}_p, \mathcal{P}, p)$$

et par le lemme fondamental :

$$S(\mathcal{A}_p, \mathcal{P}, p) \leq S(\mathcal{A}_p, \mathcal{P}, X/p) \ll \frac{X}{p} W\left(\frac{X}{p}\right)$$

On remarque d'abord que, pour $1 \leq u \leq z_0$, on a :

$$\begin{aligned} W(u) &= W(z_0) \prod_{\substack{u \leq p < z_0 \\ p \in \mathcal{P}}} (1 - 1/p) \leq W(z_0) \prod_{u \leq p < z_0} (1 - 1/p) \\ &\ll W(z_0) \log z_0 \prod_{p < u} (1 - 1/p) \ll \frac{W(z_0) \log z_0}{1 + \log u} \end{aligned}$$

par la formule de MERTENS. (On a ajouté 1 au dénominateur pour donner un sens à la formule pour $u = 1$).

On a ensuite :

$$\sum_{z_3 \leq p < z} \frac{1}{p} W\left(\frac{X}{p}\right) \leq \sum_{z_3 \leq p < X} \frac{1}{p} W\left(\frac{X}{p}\right) \leq \sum_{j=0}^{[\log z_0]} W(e^j) \sum_{\frac{X}{e^{j+1}} \leq p < \frac{X}{e^j}} \frac{1}{p}$$

De la formule classique : $\sum_{p \leq y} 1/p = \log \log y + B + O(1/\log y)$, on déduit que

$$\sum_{y/e < p \leq y} \frac{1}{p} = O\left(\frac{1}{\log y}\right)$$

et l'on a :

$$\begin{aligned} \sum_{z_3 \leq p < z} \frac{1}{p} W\left(\frac{X}{p}\right) &<< \frac{1}{\log X} \sum_{j=0}^{[\log z_0]} W(e^j) << \frac{W(z_0)}{\sqrt{\log X}} \sum_{j=0}^{[\log z_0]} \frac{1}{1+j} \\ &<< W(z_0) \frac{\log \log X}{\sqrt{\log X}} \end{aligned}$$

La formule (13) donne alors :

$$S(\mathcal{A}, \mathcal{P}, z) = S(\mathcal{A}, \mathcal{P}, z_3) + O\left(X W(z_0) \frac{\log \log X}{\sqrt{\log X}}\right)$$

et par (12), (8) et (9), on achève la démonstration de (3).

LEMME 4. Soit \mathcal{P} une famille finie de nombres premiers. On pose :

$$W(\mathcal{P}) = \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p}\right); S(\mathcal{P}) = \sum_{p \in \mathcal{P}} \frac{\log p}{p}; F(\mathcal{P}) = W(\mathcal{P}) S(\mathcal{P})$$

Il existe une constante $C_1 > 0$ telle que l'on ait :

$$F(\mathcal{P}) \geq e^{-\gamma} - \frac{C_1}{S(\mathcal{P})}$$

où γ est la constante d'Euler.

Avec les résultats de ROSSER et SCHOENFELD, la fonction F est croissante sur les ensembles $Q_\xi = \{p; p \text{ premier} \leq \xi\}$.

Démonstration. Soit $y \in \mathcal{P}$. On a :

$$W(\mathcal{P} \setminus \{y\}) = \frac{y}{y-1} W(\mathcal{P}); S(\mathcal{P} \setminus \{y\}) = S(\mathcal{P}) - \frac{\log y}{y}$$

$$(14) \quad F(\mathcal{P}) - F(\mathcal{P} \setminus \{y\}) = \frac{W(\mathcal{P})}{y-1} (\log y - S(\mathcal{P}))$$

On a de même, pour $z \notin \mathcal{P}$:

$$(15) \quad F(\mathcal{P} \cup \{z\}) - F(\mathcal{P}) = \frac{W(\mathcal{P})}{z} \left(\left(1 - \frac{1}{z}\right) \log z - S(\mathcal{P}) \right)$$

1ère Etape. - On ajoute à \mathcal{P} les nombres premiers n'appartenant pas à \mathcal{P} et $\leq \xi = e^{S(\mathcal{P})}$, ce qui d'après (15) fait diminuer F . On peut supposer que $S(\mathcal{P}) \geq \log 2$ (sinon le lemme est trivial). On a donc :

$$\mathcal{P}_0 = \mathcal{P} \cup Q_\xi, \quad \xi \geq 2$$

$$F(\mathcal{P}_0) \leq F(\mathcal{P}) \quad \text{et} \quad S(\mathcal{P}_0) \geq \xi = S(\mathcal{P}).$$

2ème Etape. - Soit maintenant $y_1 > y_2 > \dots > y_s > \xi$ les nombres premiers $\in \mathcal{P}_0$ et $> \xi$. On enlève de \mathcal{P}_0 les nombres premiers y_1, y_2, \dots tant que cela fait diminuer F . Concrètement, on définit $\mathcal{P}_1 = \mathcal{P}_0 \setminus \{y_1\}$ et pour $2 \leq i \leq s$, $\mathcal{P}_i = \mathcal{P}_{i-1} \setminus \{y_i\}$. On pose :

$$a_i = \log y_i - S(\mathcal{P}_{i-1}) \quad i = 1, 2, \dots, s$$

On notera que a_i ne peut être nul, car les logarithmes des nombres premiers sont \mathbb{Q} -linéairement indépendants.

Si tous les a_i sont > 0 , on pose $\mathcal{P}' = \mathcal{P}_s = Q_\xi$. D'après la formule (14), on a $F(\mathcal{P}') \leq F(\mathcal{P}_0)$ ce qui entraîne $F(Q_\xi) \leq F(\mathcal{P})$.

Si les a_i ne sont pas tous > 0 , soit i_0 le plus petit indice tel que $a_i < 0$. On pose $\mathcal{P}' = \mathcal{P}_{i_0-1}$ et $\xi' = y_{i_0}$. On a alors d'après la formule (14), $F(\mathcal{P}') \leq F(\mathcal{P}_0)$ et on remarque que $Q_\xi \subset \mathcal{P}' \subset Q_{\xi'}$, et que $\log \xi' < S(\mathcal{P}')$. Comme dans la 1ère étape, on rajoute à \mathcal{P}' tous les nombres premiers $\leq \xi'$ ce qui diminue F , et l'on a alors

$$F(Q_{\xi'}) \leq F(\mathcal{P}') \leq F(\mathcal{P}_0) \leq F(\mathcal{P})$$

avec $\xi' > \xi$. Il reste à évaluer $F(Q_{\xi'})$. On a :

$$W(Q_{\xi'}) = \prod_{p \leq \xi'} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log \xi'} \left(1 + O\left(\frac{1}{\log \xi'}\right)\right)$$

$$S(Q_{\xi'}) = \sum_{p \leq \xi'} \frac{\log p}{p} = \log \xi' + O(1)$$

ce qui donne

$$F(Q_\xi) = e^{-\gamma} + O\left(\frac{1}{\log \xi}\right)$$

c'est-à-dire, il existe $C_1 > 0$ tel que,

$$F(Q_\xi) \geq e^{-\gamma} - \frac{C_1}{\log \xi}$$

le lemme 4 découle alors de : $S(\mathcal{P}) = \log \xi \leq \log \xi'$.

La formule 3.24 de [Ros] dit que $S(Q_\xi) \leq \log \xi$. La formule (14) dit alors que : $F(Q_\xi)$ est fonction croissante de ξ , pour $\xi \geq 2$. La démonstration précédente donne aussi, pour $S(\mathcal{P}) \geq \log 2$:

$$(16) \quad F(\mathcal{P}) \geq F(Q_\xi) \quad \text{avec} \quad \xi = e^{S(\mathcal{P})}$$

COROLLAIRE. Avec les notations du lemme précédent, il existe deux constantes $C_2 > 0$ et $C_3 > 0$ telles que, pour tout \mathcal{P} , on ait

$$W(\mathcal{P}) \geq \min\left(C_2, \frac{C_3}{S(\mathcal{P})}\right)$$

Démonstration. On a :

$$-\log W(\mathcal{P}) = \sum_{p \in \mathcal{P}} -\log\left(1 - \frac{1}{p}\right) \leq \sum_{p \in \mathcal{P}} \frac{1}{p} + C_4 \leq \frac{1}{\log 2} S(\mathcal{P}) + C_4$$

$$\text{avec } C_4 = \sum_p (-\log(1 - 1/p) - 1/p).$$

Ce qui donne :

$$(17) \quad W(\mathcal{P}) \geq \exp\left(-\frac{S(\mathcal{P})}{\log 2} - C_4\right)$$

Maintenant, le lemme 4 nous dit que

$$W(\mathcal{P}) \geq \frac{e^{-\gamma}}{S(\mathcal{P})} \left(1 - \frac{C_1}{S(\mathcal{P})}\right)$$

On voit, que pour $S(\mathcal{P}) \geq 2 C_1$, on a $W(\mathcal{P}) \geq \frac{C_3}{S(\mathcal{P})}$ avec $C_3 = \frac{1}{2} e^{-\gamma}$. Et pour $S(\mathcal{P}) \leq 2 C_1$, (17) nous donne :

$$W(\mathcal{P}) \geq \exp\left(-\frac{2C_1}{\log 2} - C_4\right) = C_2$$

V. - UNE PREMIERE MAJORATION DANS LA DEMONSTRATION DU THEOREME 2

Soit $n \in P(m, k)$. On dit que p est un facteur premier essentiel de n , si $p^\alpha \parallel n$ et s'il existe i , $1 \leq i \leq k$, tel que $p^\alpha \nmid \pi_i^*$.

PROPOSITION 2. Soit $e(n) = \prod_{\substack{p \mid n \\ p \text{ essentiel}}} p^\alpha$. On a $e(n) \in P(m, k)$.

Démonstration. On a $e(n) \mid n \mid \pi$. Montrons que, $\forall i$, $1 \leq i \leq k$, $e(n) \nmid \pi_i^*$. Comme $n \nmid \pi^*$, il existe q premier, $q^\beta \parallel n$, tel que $q^\beta \nmid \pi_i^*$. Ce nombre q est essentiel donc $q^\beta \parallel e(n)$ et donc $e(n) \nmid \pi_i^*$.

PROPOSITION 3. Soit $n \in P(m, k)$. On suppose que p est un facteur premier essentiel de n ; alors on a :

$$\alpha = v_p(n) \geq r = \text{Card} \{ i ; 1 \leq i \leq k ; p \mid m + i \} \geq [k/p]$$

et si tous les facteurs premiers de n sont essentiels, on a :

$$\sum_{p \mid n ; p \leq k} (\log p)/p \leq (2 \log n)/k$$

Démonstration. Si p est essentiel, $\exists i$, $1 \leq i \leq k$ tel que $p^\alpha \nmid \pi_i^*$. On a donc :

$$v_p(n) \geq v_p(\pi_i^*) + 1 \geq r - 1 + 1 = r \geq [k/p]$$

Cela entraîne

$$n = \prod_{p \mid n} p^{v_p(n)} \geq \prod_{\substack{p \mid n \\ p \leq k}} p^{(k/p)-1}$$

et encore :

$$\prod_{\substack{p \mid n \\ p \leq k}} p^{k/p} \leq n^2$$

ce qui achève la démonstration.

PROPOSITION 4. Soit k assez grand, et soit $n \in P(m, k)$ alors on a :

$$2 e^{-\gamma/2} k \sqrt{\log k} + o(k) \leq \log n.$$

Démonstration. D'après la proposition 2, on peut supposer que tous les facteurs premiers de n sont essentiels. On peut supposer de plus que $\log n \leq 2 k \sqrt{\log k}$. On pose :

$$S(z) = \sum_{p|n; p < z} (\log p)/p; W(\mathcal{P}) = \prod_{p|n; p < z} (1 - 1/p)$$

On a, d'après la proposition 3, pour $z \leq k$

$$S(z) \leq 4\sqrt{\log k}$$

ce qui entraîne, d'après le corollaire du lemme 4, pour $z \leq k$

$$(18) \quad W(z) \gg 1/\sqrt{\log k}$$

On applique le lemme de crible avec $\mathcal{P} = \{p; p|n\}$ et $\mathcal{A} = \{m+i; 1 \leq i \leq k\}$. On choisit $z_0 = \exp(\sqrt{\log k})$, $z = k/z_0$. Le nombre de $(m+i)$ non rayés par des $p \in \mathcal{P}$, $p < z$ est :

$$S(\mathcal{A}, \mathcal{P}, z) = k W(z) \left(1 + O\left(\frac{1}{\sqrt{\log k}}\right)\right)$$

Les nombres $(m+i) \in \mathcal{S}(\mathcal{A}, \mathcal{P}, z)$ doivent être multiples de $p|n$, $p > z$.

Les p tels que $z \leq p \leq k$ peuvent en rayer au plus $[k/p] + 1$ et les $p > k$ au plus 1.

On pose

$$U = \sum_{\substack{p|n \\ z \leq p \leq k}} \left[\frac{k}{p}\right] \text{ et } T = \sum_{\substack{p|n \\ p > k}} 1$$

On doit avoir :

$$\sum_{z \leq p \leq k} \left(\left[\frac{k}{p}\right] + 1\right) + T \geq S(\mathcal{A}, \mathcal{P}, z)$$

soit

$$U + T + O\left(\frac{k}{\log k}\right) \geq k W(z) \left(1 + O\left(\frac{1}{\sqrt{\log k}}\right)\right)$$

compte tenu de (18),

$$\frac{k}{\log k} = O\left(\frac{k W(z)}{\sqrt{\log k}}\right)$$

et l'on doit avoir

$$(19) \quad U + T \geq k W(z) \left(1 + O\left(\frac{1}{\sqrt{\log k}}\right)\right)$$

D'autre part, la proposition 3 donne :

$$\begin{aligned}
\log n &= \sum_{\substack{p|n \\ p \leq k}} v_p(n) \log p + \sum_{\substack{p|n \\ p > k}} v_p(n) \log p \\
&\geq T \log k + \sum_{\substack{p|n \\ p < z}} \left[\frac{k}{p} \right] \log p + U \log z \\
&= T \log k + k S(z) + O(z) + U \log k - U \sqrt{\log k}.
\end{aligned}$$

Or,

$$U = \sum_{\substack{p|n \\ z \leq p \leq k}} \left[\frac{k}{p} \right] \leq \frac{k}{\log z} \sum_{\substack{p|n \\ p \leq k}} \frac{\log p}{p} << \frac{k}{\sqrt{\log k}}$$

et l'on obtient :

$$\log n \geq (U + T) \log k + k S(z) + O(k).$$

En comparant avec (19) on obtient :

$$k W(z) \left(1 + O\left(\frac{1}{\sqrt{\log k}}\right) \right) \leq \frac{\log n}{\log k} - \frac{k S(z)}{\log k} + O\left(\frac{k}{\log k}\right).$$

Compte tenu de (18) le dernier terme d'erreur est négligeable, et l'on a :

$$(20) \quad k W(z) \left(1 + O\left(\frac{1}{\sqrt{\log k}}\right) \right) + \frac{k}{\log k} S(z) \leq \frac{\log n}{\log k}$$

Comme on a supposé $\log n \leq 2k\sqrt{\log k}$, cela entraîne

$$W(z) << \frac{1}{\sqrt{\log k}}$$

et d'après le corollaire du lemme 4, on a aussi :

$$S(z) \gg \sqrt{\log k}$$

On a donc d'après le lemme 4 :

$$W(z) \geq \frac{e^{-\gamma}}{S(z)} \left(1 + O\left(\frac{1}{\sqrt{\log k}}\right) \right)$$

La relation (20) devient :

$$(21) \quad k W(z) + \frac{k e^{-\gamma}}{\log k W(z)} \leq \frac{\log n}{\log k} + O\left(\frac{k}{\log k}\right)$$

et comme, pour tout $x > 0$, on a : $x + \frac{a}{x} \geq 2\sqrt{a}$, on a :

$$\frac{2e^{-\gamma/2}}{\sqrt{\log k}} \leq \frac{\log n}{k \log k} + O\left(\frac{1}{\log k}\right)$$

ce qui démontre la proposition 4.

VI. - NOMBRES f-HAUTEMENT ABONDANTS

Soit n un nombre f-h.a. assez grand, $k = f(n)$ et m tel que $n \in P(m, k)$. On a :

$$(22) \quad \log n \leq 2k e^{-\gamma/2} \sqrt{\log k}$$

car n est certainement plus petit que le nombre construit dans la proposition 1. De plus la proposition 2 dit que tous les facteurs premiers de n sont essentiels, et la proposition 3 donne :

$$\sum_{p \mid n; p \leq k} (\log p)/p \leq (2 \log n)/k \leq 4e^{-\gamma/2} \sqrt{\log k}$$

ce qui nous permettra d'appliquer le lemme de crible avec $\mathcal{P} = \{p; p \mid n\}$ et $\lambda = 4e^{-\gamma/2}$.

PROPOSITION 5. Soit n un nombre f-h.a. assez grand, $k = f(n)$ et $T = \sum_{\substack{p \mid n \\ p > k}} 1$. Alors on a :

$$T = k \frac{e^{-\gamma/2}}{\sqrt{\log k}} \left(1 + O\left(\frac{1}{\sqrt{\log k}}\right)\right)$$

Démonstration. Soit m tel que $n \in P(m, k)$. On applique le lemme de crible à $\mathcal{A} = \{m + i; 1 \leq i \leq k\}$. Chaque élément de \mathcal{A} doit être non premier avec n . Si, de plus, $m + i \in \mathcal{P}(\mathcal{A}, \mathcal{P}, k)$ il doit être divisible par $p \mid n$, $p > k$. Chaque $p > k$ peut diviser au plus un élément de \mathcal{A} donc on doit avoir :

$$S(\mathcal{A}, \mathcal{P}, k) \leq T$$

En fait, on a $S(\mathcal{A}, \mathcal{P}, k) = T$, car si deux nombres premiers $p_1 \neq p_2$, $p_1 > k$, $p_2 > k$ divisaient le même élément de \mathcal{A} , on aurait encore $n/p_1 \in P(m, k)$ et n ne serait pas f-h.a.

On a donc :

$$(23) \quad T = S(\mathcal{A}, \mathcal{P}, k) = k W(k) \left(1 + O\left(\frac{\log \log k}{\sqrt{\log k}}\right)\right).$$

Si l'on pose $W(z) = \frac{e^{-\gamma/2}}{\sqrt{\log k}} (1 + u)$ dans l'inégalité (21), on obtient compte tenu de (22) :

$$2 + u^2(1 + o(1)) \leq 2 + O\left(\frac{1}{\sqrt{\log k}}\right)$$

soit :

$$u = O\left(\frac{1}{4\sqrt{\log k}}\right)$$

et par (8) :

$$(24) \quad W(k) = W(z) \left(1 + O\left(\frac{1}{\sqrt{\log k}}\right)\right) = \frac{e^{-\gamma/2}}{\sqrt{\log k}} \left(1 + O\left(\frac{1}{4\sqrt{\log k}}\right)\right)$$

ce qui, avec (23) achève la démonstration de la proposition 5.

LEMME 5. Soit $m \geq 1$, $k \geq 1$ et $n \in P(m, k)$. Soit p un nombre premier divisant au moins deux nombres $m + i$ pour $1 \leq i \leq k$. Alors il existe $\beta \in \mathbb{Z}$, et $m' \geq 1$ tels que $n' = p^\beta n \in P(m', k)$ et

$$v_p(n') = v_p(\pi(m', k)) \leq v_p((k + p - 1)!) \leq k/(p - 1) + 1.$$

Démonstration. Soit $n = p^\alpha p_2^{\alpha_2} \dots p_r^{\alpha_r}$. On définit a par : $m \equiv a \pmod{p}$ et $0 \leq a \leq p - 1$, et l'on pose $\alpha' = v_p(\pi(a, k)) \leq v_p((k + p - 1)!)$. Soit $n' = p^{\alpha'} p_2^{\alpha_2} \dots p_r^{\alpha_r} = p^\beta n$ avec $\beta = \alpha' - \alpha$. On prend pour m' une solution des congruences :

$$\begin{cases} m' \equiv a \pmod{p^{\alpha'}} \\ m' \equiv m \pmod{p_2^{\alpha_2} \dots p_r^{\alpha_r}} \end{cases}$$

On va montrer que $n' \in P(m', k)$. On remarque d'abord que, par le lemme 2, on a, pour $1 \leq i \leq k$:

$$(25) \quad v_p(m' + i) = v_p(m' - a + a + i) = v_p(a + i)$$

car $v_p(a + i) < \alpha' \leq v_p(m' - a)$, puisque nous avons supposé que p divise deux nombres $(m + i)$ ou, ce qui est équivalent, deux nombres $(a + i)$.

Montrons que n' divise $\pi(m', k)$; on a :

$$(26) \quad \alpha' = v_p(n') = \sum_{1 \leq i \leq k} v_p(a + i) = \sum_{1 \leq i \leq k} v_p(m' + i) = v_p(\pi(m', k))$$

et pour $2 \leq j \leq r$,

$$\pi(m',k) \equiv \pi(m,k) \equiv 0 \pmod{p_j^{\alpha_j}}$$

On doit ensuite montrer que pour tout i , il existe $q \mid n'$ tel que $v_q(n') > v_q(\pi_i^*(m'))$. Si $(m' + i)$ est multiple de p , on choisit $q = p$ et la relation (26) donne le résultat. Si $m' + i$ n'est pas multiple de p , comme $n \in P(m,k)$, il existe j , $2 \leq j \leq r$, tel que $\alpha_j = v_{p_j}(n) > v_{p_j}(\pi_i^*(m))$; et comme $\pi_i^*(m) \equiv \pi_i^*(m') \pmod{p_j^{\alpha_j}}$, on a, par le lemme 2 :

$$v_{p_j}(\pi_i^*(m')) = v_{p_j}(\pi_i^*(m)) < \alpha_j = v_{p_j}(n')$$

PROPOSITION 6. Soit n un nombre f-h.a. et $k = f(n)$. Soit $p \mid n$. Alors on a :

$$v_p(n) \leq v_p((k + p - 1)!) \leq k/(p - 1) + 1$$

Démonstration. Soit m tel que $n \in P(m,k)$, et supposons d'abord que p divise un seul nombre $(m + i)$ pour $1 \leq i \leq k$. Si $v_p(n) \geq 2$, il est clair que $n/p \in P(m,k)$ et n n'est pas f-h.a. On a donc $v_p(n) = 1$, qui est bien inférieur à $v_p((k + p - 1)!)$.

Si p divise deux nombres $(m + i)$ au moins, on construit n' et m' par le lemme 5. Comme $n' \in P(m',k)$, $f(n') \geq k = f(n)$ et comme n est f-h.a. on a $n' \geq n$, c'est-à-dire $\beta \geq 0$, c'est-à-dire

$$v_p(n) \leq v_p(n') \leq v_p((k + p - 1)!),$$

d'après le lemme 5.

PROPOSITION 7. Soit p_0 un nombre premier fixé ; soit n un nombre f-h.a. assez grand, $k = f(n)$ et m tel que $n \in P(m,k)$. Alors on a

$$v_{p_0}(n) = v_{p_0}((m + 1) \dots (m + k))$$

Démonstration. Il suffit de démontrer que $v_{p_0}(n) \geq v_{p_0}(\pi)$, puisque $n \mid \pi$. Soit $m + i_1, m + i_2, \dots, m + i_X$ la famille des $m + i$, $1 \leq i \leq k$, qui sont multiples de p_0 . On

applique à l'ensemble $\mathcal{A} = \left\{ \frac{m + i_1}{p_0}, \dots, \frac{m + i_X}{p_0} \right\}$ le lemme de crible avec $\mathcal{P} = \{p; p \mid n\}$. On a $|X - \frac{k}{p_0}| \leq 1$; la condition (1) est vérifiée, et l'on a :

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}, X) &= X W(X) \left(1 + O\left(\frac{\log \log X}{\sqrt{\log X}}\right) \right) \\ &= \frac{k}{p_0} W(k) \left(1 + O\left(\frac{\log \log k}{\sqrt{\log k}}\right) \right) \end{aligned}$$

compte tenu de (8). On a ensuite, avec (24) :

$$(27) \quad r = S(\mathcal{A}, \mathcal{P}, k) = S(\mathcal{A}, \mathcal{P}, X) + O\left(\frac{k}{\log k}\right) \gg \frac{k}{\sqrt{\log k}}$$

où la constante implicite dépend de p_0 .

Soit $(m + i)/p_0 \in \mathcal{A}_1$. Comme $n \in P(m, k)$ il existe $q \mid n$, tel que $v_q(n) > v_q(\pi_1^*)$. Si $(m + i)/p_0 \in \mathcal{S}(\mathcal{A}, \mathcal{P}, k)$, on a $q = p_0$ (et dans ce cas $p_0 \mid n$ et $v_{p_0}(m + i) = 1$) ou $q > k$.

Supposons $v_{p_0}(n) < v_{p_0}(\pi) = v_{p_0}(\pi_1^*) + 1$, alors on ne peut avoir $q = p_0$ et l'on a $q > k$. Soit q_1, q_2, \dots, q_r les nombres premiers $> k$ ainsi construits pour les différents $(m + i)/p_0 \in \mathcal{S}(\mathcal{A}, \mathcal{P}, k)$, et soit $\alpha = v_{p_0}(\pi)$. Il est facile de voir que

$$n_1 = \frac{p_0^{\alpha - v_{p_0}(n)} n}{q_1 q_2 \dots q_r} \in P(m, k).$$

A l'aide du lemme 5, on construit à partir de n_1 , $n' = p_0^\beta n_1$ et m' tel que $n' \in P(m', k)$. On a : $\alpha' + v_{p_0}(n') \leq k/(p_0 - 1) + 1$. On aurait alors $f(n') \geq k$ et $n' < n$ car, par (27) on a :

$$\frac{k/(p_0 - 1) + 1}{p_0} \leq k^r$$

pour k assez grand.

PROPOSITION 8. Soit $\epsilon > 0$ fixé. Soit n un nombre f-h.a. assez grand, $k = f(n)$ et m tel que $n \in P(m, k)$. Soit p tel que $p \mid n$ et $k^\epsilon \leq p \leq k$, alors p divise un seul $m + i$ ($1 \leq i \leq k$), et donc $p > k/2$.

Démonstration. Supposons que p divise r nombres $(m + i)$, $1 \leq i \leq k$, avec $r \geq 2$. Parmi ces r nombres, s sont pairs et l'on a $s \geq r/3$ (le plus mauvais cas étant $r = 3$). D'autre part p est essentiel et la proposition 3 donne $v_p(n) \geq r$. On peut trouver $r - s$ nombres premiers q_1, \dots, q_{r-s} tous plus grands que k , ne divisant pas n et inférieurs à $2k \log k$. On considère $n' = \frac{n q_1 q_2 \dots q_{r-s}}{p^{v_p(n)}}$ et l'on détermine m' par

$$\begin{cases} m' \equiv m \pmod{n} \\ m' + i_j \equiv 0 \pmod{q_j}, 1 \leq j \leq r-s \end{cases}$$

où $m' + i_j$ est le $j^{\text{ème}}$ nombre impair de l'ensemble des $(m + i)$ multiples de p . On a alors $n' \in P(m', k)$, les $(m + i)$ pairs multiples de p étant rayés par 2 à cause de la proposition 7. On a de plus

$$\frac{n'}{n} \leq \frac{(2k \log k)^{2r/3}}{p^r}$$

et si $p > (2k \log k)^{2/3}$, on a $n' < n$ et $f(n') \geq f(n)$ ce qui contredit le fait que n est f.h.a.

Lorsque $k^\epsilon \leq p \leq (2k \log k)^{2/3}$, on considère un entier A fixé tel que $\phi(A) < \frac{\epsilon}{2}A$ où ϕ est la fonction d'Euler, et parmi les r nombres $(m+i)$ multiples de p on distingue les s d'entre eux non premiers avec A . On a

$$r - s \leq ([r/A] + 1) \phi(A) \leq \frac{\epsilon}{2}(r + A).$$

On construit n' et m' comme précédemment, on a $n' \in P(m', k)$ et

$$\frac{n'}{n} \leq \frac{(2k \log k)^{r-s}}{p^r} \leq \frac{(2k \log k)^{(\epsilon/2)(r+A)}}{k^{\epsilon r}}$$

On a $n' < n$ pour k assez grand, car $r \geq k/p - 1$ tend vers l'infini.

PROPOSITION 9. Soit n un nombre f.h.a. assez grand, $k = f(n)$ et m tel que $n \in P(m, k)$. Alors pour $p \mid n$, $p < k/2$ on a :

$$v_p(n) = v_p((m+1) \dots (m+k))$$

Démonstration. D'après la proposition précédente on peut supposer $p < k^\epsilon$. On applique alors le lemme de crible à $\mathcal{A} = \left\{ \frac{m+i}{p}; 1 \leq i \leq k; p \mid m+i \right\}$ et à $\mathcal{P} = \left\{ p; p \mid n \right\}$. On a $k/p > k^{1-\epsilon}$ et :

$$S(\mathcal{A}, \mathcal{P}, k/p) = k/p W(k/p) \left(1 + O\left(\frac{\log \log k}{\sqrt{\log k}} \right) \right)$$

et l'on a par la proposition 8, $S(\mathcal{A}, \mathcal{P}, k/p) = S(\mathcal{A}, \mathcal{P}, k/2)$. En tenant compte de (8) et de (24), on a :

$$(28) \quad r = S(\mathcal{A}, \mathcal{P}, k/2) = \frac{k}{p} \frac{e^{-\gamma/2}}{\sqrt{\log k}} \left(1 + O\left(\frac{1}{\sqrt[4]{\log k}} \right) \right)$$

La fin de la démonstration ressemble à celle de la proposition 7. Si $(m+i)/p \in \mathcal{F}(\mathcal{A}, \mathcal{P}, k/2)$, il existe $q \mid n$ tel que $v_q(n) > v_q(\pi_i^*(m))$ et l'on a $q = p$ ou $q > k/2$. Si l'on suppose $v_p(n) < v_p(\pi(m, k))$, on ne peut avoir $q = p$, et l'on a $q > k/2$. Soit q_1, \dots, q_r les nombres premiers $> k/2$ ainsi construits pour les différents $(m+i)/p \in \mathcal{F}(\mathcal{A}, \mathcal{P}, k/2)$. Chaque q_j divise au plus un nombre $m+i$ ($1 \leq i \leq k$) d'après la proposition 8. Comme p est essentiel, on a : $v_p(n) \geq (k/p) - 1$.

Si l'on avait $v_p(n) < v_p(\pi)$, on définirait alors n' et m' par le lemme 5, on aurait

$$v_p(n') - v_p(n) \leq \frac{k}{p-1} + 1 - \frac{k}{p} + 1 = \frac{k}{p(p-1)} + 2$$

$n' \in P(m', k)$, et on verrait aussi que $n'' = n'/q_1 q_2 \dots q_r \in P(m', k)$. Il reste à vérifier que $n'' < n$: cela résulte de :

$$\left(\frac{k}{p(p-1)} + 2\right) \log p = o\left(\frac{k}{p\sqrt{\log k}} (\log k/2)\right)$$

Démonstration du théorème i. Soit p ne divisant pas n , $p < k^\epsilon$. On applique le lemme de crible à l'ensemble $\mathcal{A} = \{(m+i)/p ; 1 \leq i \leq k ; p \mid m+i\}$ comme dans la proposition 9, et $r = S(\mathcal{A}, \mathcal{P}, k/2)$ est donné par (28).

Pour chaque $(m+i)/p \in \mathcal{S}(\mathcal{A}, \mathcal{P}, k/2)$, on peut définir un nombre premier $q \mid n$, $q > k/2$ et tel que $q \mid m+i$. Soit q_1, q_2, \dots, q_r les nombres premiers ainsi construits.

On construit alors par le lemme 5 $n' = p^\alpha n$ et m' avec $v_p(n') = \alpha \leq \frac{k}{p-1} + 1$ et $n' \in P(m', k)$. On vérifie que

$$n'' = p^\alpha \frac{n}{q_1 q_2 \dots q_r} \in P(m', k).$$

On a ensuite :

$$\begin{aligned} \log \frac{n''}{n} &\leq \left(\frac{k}{p-1} + 1\right) \log p - \frac{k}{p\sqrt{\log k}} \frac{e^{-\gamma/2}}{\sqrt{\log k}} \left(1 + O\left(\frac{1}{\sqrt[4]{\log k}}\right)\right) \log k/2 \\ &\leq \frac{k}{p} \left[\left(\frac{p}{p-1} + \frac{p}{k}\right) \log p - e^{-\gamma/2} \sqrt{\log k} \left(1 + O\left(\frac{1}{\sqrt[4]{\log k}}\right)\right) \right] \end{aligned}$$

Pour $p \leq \sqrt{\log k}$, on a $\frac{p}{p-1} + \frac{p}{k} \leq 3$, et le crochet est négatif. Pour $\sqrt{\log k} \leq p \leq \exp(e^{-\gamma/2} \sqrt{\log k} (1 - c_1/\sqrt[4]{\log k}))$ on a $\frac{p}{p-1} + \frac{p}{k} = 1 + O\left(\frac{1}{\sqrt{\log k}}\right)$ et le crochet est négatif pour c_1 assez grand. On a alors $n'' < n$, $f(n'') \geq f(n)$ ce qui contredit l'hypothèse et donc p doit diviser n .

Démonstration du théorème ii. Soit $p \mid n$, $p < k^\epsilon$. On sait que p est essentiel et donc $\alpha = v_p(n) \geq k/p - 1$. On applique le lemme de crible à

$$\mathcal{A} = \{(m+i)/p ; 1 \leq i \leq k ; p \mid m+i\},$$

et $r = S(\mathcal{A}, \mathcal{P}, k/2)$ est toujours donné par (28). On considère ensuite :

$$\mathcal{B} = \{m+i ; 1 \leq i \leq k ; (m+i)/p \in \mathcal{S}(\mathcal{A}, \mathcal{P}, k/2) \text{ ou } p^2 \mid m+i\}$$

Soit $m+i_1, \dots, m+i_s$ les éléments de \mathcal{B} et q_1, \dots, q_s des nombres premiers ne divisant pas n ,

dans l'intervalle $[k, 2k \log k]$. On pose $n' = \frac{n}{p^\alpha} q_1 q_2 \dots q_s$ et on définit m' par les congruences :

$$\begin{cases} m' \equiv m \pmod{n} \\ m' \equiv -i_j \pmod{q_j} \quad 1 \leq j \leq s \end{cases}$$

Pour montrer $n' \in P(m', k)$ la seule difficulté nouvelle est de montrer $n' \notin \pi_i^*(m')$ lorsque p divise $m + i$. Dans ce cas, ou bien $m + i$ avait un autre diviseur premier q , $q \mid n$, $q < k/2$, et alors la proposition 9 permet de conclure, ou bien $m + i \in \mathcal{B}$ et il existe j tel que $q_j \notin \pi_i^*(m')$.

On a enfin :

$$\log \frac{n'}{n} \leq [S(\mathcal{A}, \mathcal{P}, k/2) + \frac{k}{p^2} + 1] \log(2k \log k) - (\frac{k}{p} - 1) \log p$$

et comme précédemment, cette quantité est négative dès que

$$\log p > e^{-\gamma/2} \sqrt{\log k} (1 + c_2 / \sqrt[4]{\log k}).$$

Démonstration du théorème iii. Soit $p \mid n$, $p > k = f(n)$ et supposons que q , $k \leq q < p$ ne divise pas n . Nous allons montrer que $f(n \cdot q/p) \geq f(n)$. D'abord, il résulte de la proposition 6 que $v_p(n) = 1$. Ensuite, p est essentiel, il existe i_0 tel que $p \mid m + i_0$, et comme $p > k$, cet i_0 est unique. On définit m' par les congruences :

$$\begin{cases} m' \equiv m \pmod{n/p} \\ m' \equiv -i_0 \pmod{q} \end{cases}$$

On constate alors que $n' = n \cdot q/p \in P(m', k)$, ce qui entraîne $f(n') \geq k$.

Soit q_1, \dots, q_T les diviseurs premiers de n qui sont $> k$, et soit $\pi(x) = \sum_{p \leq x} 1$. On a :

$$\pi(q_T) = T + \pi(k) = \frac{e^{-\gamma/2}}{\sqrt{\log k}} k (1 + O(\frac{1}{\sqrt[4]{\log k}}));$$

et par le théorème des nombres premiers, le plus grand facteur premier $P = q_T$ de n s'écrit :

$$P = e^{-\gamma/2} k \sqrt{\log k} (1 + O(\frac{1}{\sqrt[4]{\log k}})) = \frac{1}{2} \log n (1 + O(\frac{1}{\sqrt[4]{\log \log n}}))$$

en anticipant sur la démonstration du théorème 2.

VII. - DEMONSTRATION DU THEOREME 2

Le théorème 2 se déduira de la proposition suivante :

PROPOSITION 10. Soit n un nombre f-h.a., $k = f(n)$. On a :

$$\log n = 2 e^{-\gamma/2} k \sqrt{\log k} - \gamma k + O\left(\frac{k}{\sqrt[4]{\log k}}\right)$$

La majoration est donnée par la proposition 1. Montrons la minoration :

LEMME 6. Soit p premier et $n \geq 1$. On a :

$$\frac{n}{p-1} - \left(\frac{\log n}{\log p} + 2\right) \leq v_p(n!) < \frac{n}{p-1}$$

Démonstration. Immédiate à partir de la formule $v_p(n!) = \sum_{r \geq 1} [n/p^r]$.

On pose ensuite $z = \exp(e^{-\gamma/2} \sqrt{\log k} (1 + \frac{c_2}{\sqrt[4]{\log k}}))$ et $z' = \exp(e^{-\gamma/2} \sqrt{\log k} (1 - \frac{c_1}{\sqrt[4]{\log k}}))$ de telle sorte que, d'après le théorème 3, $p \leq z' \Rightarrow p \mid n$ et $z \leq p \leq k/2 \Rightarrow p \nmid n$. A l'aide de la formule (cf. [Lan], p. 200) :

$$(29) \quad \sum_{p \leq x} \frac{\log p}{p} = \log x - \gamma - b + O\left(\frac{1}{\log x}\right)$$

avec

$$b = \sum_p \frac{\log p}{p(p-1)} = 0,75537,$$

on a :

$$(30) \quad S(z) = \sum_{\substack{p \mid n \\ p \leq z}} \frac{\log p}{p} = e^{-\gamma/2} \sqrt{\log k} \left(1 + O\left(\frac{1}{\sqrt[4]{\log k}}\right)\right)$$

On applique la formule (5) à l'ensemble

$$\mathcal{A}' = \{m + i; 1 \leq i \leq k\}$$

et l'on a, en posant $V = \sum_{\substack{p \mid n \\ p > k/2}} 1$:

$$(31) \quad V = S(\mathcal{A}', \mathcal{A}, z) = k W(z) \left(1 + O\left(\frac{1}{\log k}\right)\right)$$

comme pour la formule (23), puisqu'on sait, d'après la proposition 8 que $p > k/2$ ne divise au

plus qu'un élément de \mathcal{A} . On a ensuite, pour $p \mid n$, $p < z$, $v_p(n) \geq v_p(k!)$ par la proposition 9 et :

$$\begin{aligned} \log n &= \sum_{\substack{p \mid n \\ p < z}} v_p(n) \log p + \sum_{\substack{p \mid n \\ p > k/2}} \log p \\ (32) \quad \log n &\geq \sum_{\substack{p \mid n \\ p < z}} k \frac{\log p}{p-1} + V \log(k/2) + O(z \log k) \end{aligned}$$

en utilisant le lemme 6. Il vient ensuite :

$$\sum_{\substack{p \mid n \\ p < z}} \frac{\log p}{p-1} = S(z) + \sum_{\substack{p \mid n \\ p < z}} \frac{\log p}{p(p-1)} = S(z) + b + O\left(\sum_{p > z} \frac{\log p}{p(p-1)}\right) = S(z) + b + O(1/z')$$

La formule (32) devient alors, compte tenu de (31)

$$(33) \quad \log n \geq k S(z) + k b + k W(z) \log k + O\left(\frac{k}{\sqrt{\log k}}\right)$$

car $W(z) \sim \frac{e^{-\gamma/2}}{\sqrt{\log k}}$. Il reste à appliquer le lemme 4 sous la formule de l'inégalité (16) : on pose

$\log \xi = S(z)$, on a par (29) :

$$\begin{aligned} F(Q_\xi) &= \prod_{p \leq \xi} \left(1 - \frac{1}{p}\right) \sum_{p \leq \xi} \frac{\log p}{p} = e^{-\gamma} \left(1 - \frac{b+\gamma}{\log \xi} + O\left(\frac{1}{(\log \xi)^2}\right)\right) \\ &= e^{-\gamma} \left(1 - \frac{b+\gamma}{S(z)}\right) + O(\log k)^{-1} \end{aligned}$$

en utilisant (30). Il s'ensuit que, en utilisant à nouveau (30) :

$$\begin{aligned} W(z) &\geq \frac{e^{-\gamma}}{S(z)} - \frac{b+\gamma}{S^2(z)} e^{-\gamma} + O(\log k)^{-3/2} \\ &\geq \frac{e^{-\gamma}}{S(z)} - \frac{b+\gamma}{\log k} + O(\log k)^{-5/4} \end{aligned}$$

En reportant dans (33), et sachant que $x + \frac{a}{x} \geq 2\sqrt{a}$, on achève la démonstration de la proposition 10.

Démonstration du théorème 2. On calcule d'abord le développement asymptotique de la fonction réciproque de la fonction $k \mapsto 2 e^{-\gamma/2} k \sqrt{\log k} - \gamma k$, et on en déduit qu'il existe une constante c_3 telle que pour n f-h.a. on ait $f(n) \leq \psi(n)$, avec :

$$\psi(n) = \frac{e^{\gamma/2}}{2} \frac{\log n}{\sqrt{\log \log n}} + \frac{\gamma}{4} e^{\gamma} \frac{\log n}{\log \log n} + c_3 \frac{\log n}{(\log \log n)^{5/4}}$$

Soit maintenant N quelconque et $n' \leq N < n''$ les deux nombres f-h.a. qui l'entourent. On a $f(N) \leq f(n')$ et $f(n') \leq \psi(n') \leq \psi(N)$, puisque pour $n \geq n_0$, $\psi(n)$ est croissante en n ; cela achève la démonstration.

QUELQUES PROBLEMES NON RESOLUS

Désignant par $n_1, n_2, \dots, n_j, \dots$ la suite des nombres f-h.a. il ne nous a pas été possible de répondre aux questions suivantes : A-t-on toujours $f(n_{j+1}) - f(n_j) = 1$? ou même seulement $f(n_{j+1}) - f(n_j)$ est-elle bornée ? Existe-t-il $c > 0$ tel que $n_{j+1} / n_j = O(\log n_j)^c$? Il serait aussi intéressant de savoir si la proposition 9 est valable pour tous les nombres f-h.a.

ADDITIF. Dans le lemme 4, nous donnons une minoration de la fonction F . Une majoration avait été obtenue par H. DAVENPORT (J. London Math. Soc, 7, 1932, p. 290-296) qui a démontré lorsque $\mathcal{P} = \{p \mid n\}$:

$$\overline{\lim} \frac{F(\mathcal{P})}{\log \log n} = \frac{1}{4}.$$

REFERENCES

- [Bru] N.G. de BRUIJN. «*On the number of uncanceled elements in the sieve of Eratosthenes*». Nederl. Akad. Wetensch. Proc. t. 53, p. 803-812 : Indag. Math., t. 12, (1950), p. 247-256.
- [Erd] P. ERDÖS. «*On the integers relatively prime to n and on a number theoretic function considered by Jacobstahl*». Math. Scand. t. 10, (1962), p. 163-170.
- [Gri] C.A. GRIMM. «*A conjecture on consecutive composite numbers*». Amer. Math. Monthly, t. 76, (1969), p. 1126-1128.
- [Hal] H. HALBERSTAM and H.E. RICHERT. «*Sieve methods*». Academic Press, London (1974).
- [Har] G.H. HARDY and E.M. WRIGHT. «*An introduction to the theory of numbers*». 4th edition. - Oxford, the Clarendon Press, (1960).
- [Iwa] H. IWANIEC. «*On the error term in the linear sieve*». Acta Arithmetica, t. 19, (1971), p. 1-30.
- [Lan] E. LANDAU. «*Handbuch der Lehre von der Verteilung der Primzahlen*». Leipzig und Berlin, B.G. Teubner, (1909), 2^e edition, Chelsea (1953).
- [Nic] P. ERDÖS et J.L. NICOLAS. «*Sur la fonction nombre de diviseurs premiers de n* ». L'enseignement Mathématique, II^e série, t. XXVII, fasc. 1-2, 1981, p. 3-27.
- [Pra] K. PRACHAR. «*Primzahlverteilung*». Berlin, Springer-Verlag, (1957) (Die Grundlehren der mathematischen Wissenschaft, 91).
- [Ram] S. RAMANUJAN. «*Highly composite numbers*». Proc. London math. Soc. Series 2, t. 14 (1915), p. 347-400 ; and Collected papers. - Cambridge, at the University Press, (1927), p. 78-128.
- [Ros] J.B. ROSSER and L. SCHOENFELD. «*Approximate formulas for some functions of prime numbers*». Illinois J. of math., t. 6, (1962), p. 64-94.
- [Sch] A. SCHINZEL. «*Sur un problème de P. Erdős*». Colloq. Math. t. 5, (1958), p. 198-204.
- [Sel] P. ERDÖS and J.L. SELFRIDGE. «*Some problems on the prime factors of consecutive integers II*». Proc. Washington State Univ. Conf. on number theory. - (1971), p. 13-21. Math. Rev. t. 47, n^o 5 (1974) # 6625.