

MÉTHODES PROBABILISTES ET COMBINATOIRES EN THÉORIE DES NOMBRES

par

PAUL ERDŐS et JEAN-LOUIS NICOLAS

[Budapest; Limoges]

RÉSUMÉ. — Soit $F(n) = \max_t (\sum_{d|n, t/2 < d \leq t} 1)$. Les grandes valeurs de la fonction F sont obtenues pour les nombres n F -hautement abondants (i. e. $m < n \Rightarrow F(m) < F(n)$).

Soit $d(n) = \sum_{d|n} 1$. On démontre que, pour un nombre n F -hautement abondant, on a

$$c_1 \frac{d(n)}{\sqrt{\log n \log \log n}} \leq F(n) \leq c_2 \frac{d(n)}{\sqrt{\log n \log \log n}}.$$

La minoration est obtenue à l'aide du théorème central limite des probabilités, la majoration par des techniques combinatoires basées sur le théorème de Sperner. On utilise également la méthode des « bénéfiques » précédemment introduite dans l'étude des nombres hautement composés de RAMANUJAN, et certains problèmes d'optimisation en nombres entiers.

Introduction

Soit n un entier positif. On désigne par $d(n)$ le nombre de diviseurs de n , et par $\sigma(n)$ la somme des diviseurs de n . On a ainsi (cf. [11], chap. 16), pour $n = \prod_{i=1}^k p_i^{\alpha_i}$,

$$d(n) = \sum_{d|n} 1 = \prod_{i=1}^k (\alpha_i + 1)$$

et

$$\sigma(n) = \sum_{d|n} d = \prod_{i=1}^k \left(\frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \right).$$

Nous allons étudier plus précisément les deux fonctions suivantes :

$$g(n) = \max_{1 \leq m \leq n} \frac{1}{m} \sum_{d|n, d \leq m} d$$

et

$$F(n) = \max_t q_t(n) \quad \text{avec} \quad q_t(n) = \sum_{d|n, t/2 < d \leq t} 1.$$

Ces deux fonctions sont liées par les inégalités

$$(1) \quad \frac{1}{2} F(n) \leq g(n) \leq 2F(n).$$

On a en effet, pour tout m :

$$g(n) \geq \frac{1}{m} \sum_{d|n, m/2 < d \leq m} d \geq \frac{1}{m} \sum_{d|n, m/2 < d \leq m} \frac{m}{2} = \frac{1}{2} q_m(n),$$

ce qui entraîne $g(n) \geq 1/2 F(n)$; et d'autre part, on a

$$g(n) \geq \frac{2}{m} \sum_{d|n, d \leq m/2} d.$$

Soit m_0 une valeur pour laquelle le maximum est atteint, on a

$$\begin{aligned} g(n) &= \frac{1}{m_0} \sum_{d|n, d \leq m_0} d = \frac{1}{m_0} \sum_{d|n, d \leq m_0/2} d + \frac{1}{m_0} \sum_{d|n, m_0/2 < d \leq m_0} d \\ &\leq \frac{g(n)}{2} + F(n), \end{aligned}$$

d'où l'on tire $g(n) \leq 2F(n)$.

Remarquons encore que l'on a, pour tout n , $g(n) \geq \sigma(n)/n$, avec égalité lorsque n est une puissance d'un nombre premier. La détermination des entiers n tels que $g(n) = \sigma(n)/n$ n'est pas facile.

Enfin $g(n)$ est une fonction surmultiplicative : si n_1 et n_2 sont premiers entre eux, on a $g(n_1 n_2) \geq g(n_1) g(n_2)$.

En effet, soit

$$\begin{aligned} g(n_1) &= \frac{1}{m_1} \sum_{d|n_1, d \leq m_1} d_1, \\ g(n_2) &= \frac{1}{m_2} \sum_{d_2|n_2, d_2 \leq m_2} d_2. \end{aligned}$$

Il vient $g(n_1) g(n_2) = (1/m_1 m_2) \sum_{d \in D} d$

Les éléments $d \in D$, divisent $n_1 n_2$ et sont $\leq m_1 m_2$. On a donc

$$g(n_1) g(n_2) \leq \frac{1}{m_1 m_2} \sum_{d|n_1 n_2, d \leq m_1 m_2} d \leq g(n_1 n_2).$$

Pour la fonction F , nous avons la proposition suivante :

PROPOSITION 1. — On a, pour tout n , $(\log 2 / \log 2n) d(n) \leq F(n) \leq d(n)$.

Démonstration. — Soit k l'entier tel que $2^{k-1} \leq n < 2^k$. On a

$$k = \left[\frac{\log n}{\log 2} \right] + 1 \leq \frac{\log 2n}{\log 2}.$$

Si l'on répartit les $d(n)$ diviseurs de n dans les intervalles $(2^{i-1}, 2^i]$ pour $i = 1$ à k , un des intervalles contiendra plus de $d(n)/k$ diviseurs.

Nous allons étudier les grandes valeurs que peuvent atteindre les fonctions g et F .

Pour étudier les grandes valeurs que prend une fonction arithmétique f , on définit les nombres f -hautement abondants :

Définition. — Dire que n est f -hautement abondant équivaut à dire

$$m < n \Rightarrow f(m) < f(n).$$

Lorsque $f = d$, on trouve les nombres hautement composés de RAMANUJAN (cf. [12] et [16]). Les nombres σ -hautement abondants ont aussi été étudiés (cf. [1]), mais la plupart des techniques ne se généralisent pas aux fonctions non multiplicatives.

On obtient les résultats suivants :

THÉORÈME 1. — On a $\lim_{x \rightarrow \infty} (1/x) \sum_{n \leq x} F(n) = +\infty$.

THÉORÈME 2. — Si n est un nombre F -hautement abondant, on a

$$c_1 \frac{d(n)}{\sqrt{\log n \log \log n}} \leq F(n) \leq c_2 \frac{d(n)}{\sqrt{\log n \log \log n}}.$$

THÉORÈME 3. — Soit q un nombre premier et a un entier; il existe n_0 tel que, si n est F -hautement abondant et $n \geq n_0$, alors q^a divise n .

Compte tenu de l'inégalité (1) ces résultats s'appliquent aussi à la fonction g . Sous cette forme, ils avaient été esquissés dans [5].

La démonstration du théorème 1 se trouve dans [7] et [13]. Elle utilise le résultat suivant (cf. [9], p. 256, th. 10);

LEMME 1. — Soit d_a la densité supérieure des entiers n ayant un diviseur d vérifiant $a < d \leq 2a$. On a $\lim_{a \rightarrow \infty} d_a = 0$.

A partir d'un résultat de P. ERDÖS [6], on peut montrer que, pour tout ε et a assez grand, on a

$$\frac{1}{(\log a)^{\alpha + \varepsilon}} \leq d_a \leq \frac{c}{(\log a)^\alpha \sqrt{\log \log a}},$$

avec $\alpha = 1 - (\log(e \log 2)/\log 2) = 0,086$ (cf. G. TENENBAUM [18]).

Le problème d'une bonne estimation de $\sum_{n \leq x} F(n)$ ne semble pas facile.

L'intérêt du théorème 2 dépend surtout des méthodes utilisées : La minoration est obtenue à l'aide du théorème central limite des probabilités, et la majoration par des techniques combinatoires basées sur le théorème de Sperner.

Dans les théorèmes 2 et 3, on a pu utiliser, pour étudier les nombres F -hautement abondants, la méthode des nombres hautement composés supérieurs de RAMANUJAN et l'étude des « bénéfiques » (cf. [16] et [12]) bien que la fonction F ne soit pas multiplicative. Cela a été possible à cause de la proposition 1 : les fonctions F et d ne s'écartent pas trop l'une de l'autre.

Dans la démonstration du théorème 2, on considérera d'abord les nombres $n=2.3 \dots p_k$ produits des k -premiers nombres premiers (prop. 3 et 5), puis à l'aide de la méthode des bénéfiques (prop. 4), on verra que pour les nombres F -hautement abondants, tout se passe essentiellement de la même façon.

1. Théorème central limité des probabilités

Soit $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ un entier et sa décomposition en facteurs premiers. Soit d un diviseur de n . On peut considérer $\log d$ comme une variable aléatoire somme des k variables aléatoires X_i prenant comme valeur : $0, \log p_i, 2 \log p_i, \dots, \alpha_i \log p_i$ avec égale probabilité. On peut appliquer le théorème central limite des probabilités, pour montrer que, lorsque k tend vers l'infini, la distribution de $\log d$ tend vers la distribution de Gauss. Plus précisément, nous allons appliquer le théorème de Berry-Esseen ([8], t. 2, p. 544) qui donne une évaluation du reste.

Soit $P(\lambda)$ la probabilité qu'un diviseur d de n vérifie :

$$-\lambda \leq \frac{\log d - (1/2) \log n}{S(n)} \leq \lambda.$$

Soit

$$(2) \quad A(\lambda) = \frac{1}{\sqrt{2\pi}} \int_{-\lambda}^{\lambda} \exp(-t^2/2) dt$$

On a

$$(3) \quad |P(\lambda) - A(\lambda)| \leq 12 \frac{\rho(n)}{S^3(n)}.$$

Soit μ_i la moyenne de la variable X_i , $S^2(n)$ est la variance de la somme

$$(4) \quad S^2(n) = \sum_{i=1}^k E(X_i - \mu_i)^2 = \sum_{i=1}^k \frac{\alpha_i(\alpha_i + 2)}{12} \log^2 p_i.$$

D'autre part, $\rho(n)$ est le moment du troisième ordre

$$(5) \quad \rho(n) = \sum_{i=1}^k E(|X_i - \mu_i|^3) = \sum_{i=1}^k \frac{J(\alpha_i) \log^3 p_i}{8},$$

avec

$$J(\alpha) = \frac{\alpha^2(\alpha + 2)^2}{4(\alpha + 1)} \quad \text{si } \alpha \text{ est pair,}$$

$$J(\alpha) = \frac{(\alpha + 1)((\alpha + 1)^2 - 2)}{4} \quad \text{si } \alpha \text{ est impair.}$$

On rappelle que, pour une variable aléatoire discrète X qui prend des valeurs $(x_i)_{1 \leq i \leq T}$ avec égale probabilité, l'espérance mathématique de la variable X^m est

$$E(X^m) = \frac{1}{T} \sum_{i=1}^T x_i^m.$$

PROPOSITION 2. — Pour tout n entier, et λ réel > 0 , on a

$$F(n) \geq \frac{d(n) \log 2}{2\lambda S(n) + \log 2} \left(A(\lambda) - 12 \frac{\rho(n)}{S^3(n)} \right),$$

$\rho(n)$ et $S(n)$ étant définis par (5) et (4), et $A(\lambda)$ par (2).

Démonstration. — La formule (3) nous dit que le nombre de diviseurs d vérifiant :

$$\frac{1}{2} \log n - \lambda S(n) \leq \log d \leq \frac{1}{2} \log n + \lambda S(n)$$

est égal à $P(\lambda) d(n)$, et vérifié :

$$(6) \quad P(\lambda) d(n) \geq d(n) \left(A(\lambda) - \frac{12 \rho(n)}{S^3(n)} \right).$$

Si l'on coupe l'intervalle $((1/2) \log n - \lambda S(n), (1/2) \log n + \lambda S(n))$ en sous-intervalles de longueur $\log 2$, il y aura au plus $((2\lambda S(n)/\log 2) + 1)$ sous-intervalles, et l'un de ces sous-intervalles contiendra plus que $P(\lambda) d(n)/((2\lambda S(n)/\log 2) + 1)$ valeurs de $\log d$, avec d divisant n .

La proposition résulte alors de l'inégalité (6).

PROPOSITION 3. — Soit $n = 2.3 \dots p_k$ le produit des k premiers nombres premiers. Soit $\eta > 0$ fixé, on a, pour k assez grand

$$F(n) \geq \frac{2 \log 2}{\sqrt{2\pi}} (1 - \eta) \frac{d(n)}{\sqrt{\log n \log \log n}}$$

Démonstration. — On applique la proposition précédente. Il faut calculer $S(n)$ et $\rho(n)$.

Soit $\theta(x) = \sum_{p \leq x} \log p$ la fonction de Chebichev [Čebyšev] (cf. [11], chap. 22). On a $n = \exp(\theta(p_k))$.

On a d'autre part : $\theta(x) \sim x$ et $p_k \sim k \log k$ (cf. [11], chap. 22), d'où il vient

$$\log n = \theta(p_k) \sim p_k \sim k \log k$$

et

$$(7) \quad k \sim \frac{\log n}{\log \log n}$$

On a, d'après (4) :

$$\begin{aligned} S^2(n) &= \frac{1}{4} \sum_{i=1}^k \log^2 p_i = \frac{1}{4} \int_1^{p_k} \log t d[\theta(t)] \\ &= \frac{1}{4} \theta(x) \log x \Big|_1^{p_k} - \int_1^{p_k} \frac{\theta(x)}{x} dx \\ &= \frac{1}{4} \theta(p_k) \log p_k + O(p_k) \sim \frac{1}{4} k \log^2 k, \end{aligned}$$

d'où l'on tire

$$S(n) \sim \frac{1}{2} \sqrt{k \log k} \sim \frac{1}{2} \sqrt{\log n \log \log n}.$$

On calcule de même

$$\rho(n) = \frac{1}{8} \sum_{i=1}^k \log^3 p_i \sim \frac{k}{8} \log^3 k$$

et

$$\rho(n) \sim \frac{\log n}{8} (\log \log n)^2.$$

La proposition 2 montre alors que, pour tout λ fixé, on a

$$F(n) \geq \frac{d(n) \log 2}{\sqrt{\log n \log \log n}} (1 - \varepsilon) \frac{A(\lambda)}{\lambda}.$$

Quand $\lambda \rightarrow 0$, $A(\lambda) \sim 2\lambda/\sqrt{2\pi}$, ce qui achève la démonstration.

2. Étude des nombres F -hautement abondants

Grâce à la proposition 1, un nombre F -hautement abondant a beaucoup de diviseurs. On va pouvoir utiliser, pour étudier ces nombres, les techniques utilisées pour étudier les nombres hautement composés de RAMANUJAN. Rappelons rapidement certains résultats (cf. [12] et [16]) :

Soit $\varepsilon > 0$, la fonction $d(n)/n^\varepsilon$ a un maximum qu'elle atteint en $N_\varepsilon = \prod p^{\alpha_p}$ avec $\alpha_p = [1/(p^\varepsilon - 1)]$, où $[u]$ désigne la partie entière de u .

Un tel nombre N_ε est dit hautement composé supérieur. On pose $x = 2^{1/\varepsilon}$, soit $\varepsilon = (\log 2)/(\log x)$, et pour k entier :

$$x_k = x^{\log(1 + (1/k))/\log 2}.$$

L'exposant α_p de p dans la décomposition en facteurs premiers de N_ε se calcule alors :

$$(x_{k+1} < p \leq x_k) \Leftrightarrow (\alpha_p = k),$$

et si l'on pose $\theta(x) = \sum_{p \leq x} \log p$ la fonction de Chebychev, on a

$$\log N_\varepsilon = \theta(x) + \theta(x_2) + \dots + \theta(x_k) + \dots,$$

cette sommation étant finie puisque, pour $k > (\log x)/(\log 2)^2$, on a $x_k < 2$.

Pour un entier n quelconque, on appelle bénéfice de n par rapport à N_ε la quantité

$$\text{bén } n = \log \frac{d(N_\varepsilon)}{N_\varepsilon^\varepsilon} - \log \frac{d(n)}{n^\varepsilon} = \varepsilon \log \frac{n}{N_\varepsilon} - \log \frac{d(n)}{d(N_\varepsilon)}.$$

Le bénéfice est toujours positif ou nul. De plus, il est additif sur les nombres premiers p :

$$(8) \quad \text{bén} \left(\prod p^{\beta_p} \right) = \sum_p \left(\varepsilon \log(p^{\beta_p - \alpha_p}) - \log \frac{\beta_p + 1}{\alpha_p + 1} \right)$$

et, par le choix des α_p , chaque terme de la sommation est positif. Enfin le bénéfice de $N_\varepsilon p^\beta$ est croissant pour $\beta \geq 0$ et décroissant pour $\beta \leq 0$

PROPOSITION 4. — Soit n un nombre F -hautement abondant et N_ε le nombre hautement composé supérieur précédant n .

On pose $x = 2^{1/\varepsilon}$ et $x_2 = x^{(\log 3/2)/(\log 2)}$. On sait que l'on a

$$x \sim \log N_\varepsilon \sim \log n \quad \text{et} \quad n < 2xN_\varepsilon.$$

Alors, si $n = \prod p^{\beta_p}$, on a les résultats suivants :

- (i) pour tout p , $p^{\beta_p} = O(x^{2 \log x})$;
- (ii) pour $x_2 < p < x$, on a $\beta_p = 1$ sauf pour $O(\sqrt{x \log x})$ nombres premiers;
- (iii) pour $p > x$, on a $\beta_p = 0$ sauf pour $O(\sqrt{x \log x})$ nombres premiers;
- (iv) pour $p < x_2$, on a $\beta_p > 0$ sauf pour au plus $O(\log x)$ nombres premiers.

Démonstration. — Majorons d'abord le bénéfice. Comme n est F -hautement abondant, on a $F(N_\varepsilon) < F(n)$, et, par la proposition 1 :

$$\frac{d(N_\varepsilon) \log 2}{\log(2N_\varepsilon)} \leq F(N_\varepsilon) < F(n) < d(n),$$

d'où

$$\begin{aligned} \text{bén } n &= \varepsilon \log \frac{n}{N_\varepsilon} - \log \frac{d(n)}{d(N_\varepsilon)} \leq \log \frac{d(N_\varepsilon)}{d(n)} + \varepsilon \log 2x \\ &\leq \log \frac{\log(2N_\varepsilon)}{\log 2} + O(1), \end{aligned}$$

$$(9) \quad \text{bén } n \leq (1 + \eta) \log x.$$

Les points (ii) et (iii) se démontrent alors comme la proposition 4 de [12].

Démonstration de (i). — Supposons que l'on ait $p^\beta = c x^{2 \log x}$. On aurait alors en utilisant la formule (8) :

$$\text{bén } n \geq \varepsilon \log(p^{\beta-\alpha}) - \log \frac{\beta+1}{\alpha+1},$$

$$\text{bén } n > 2\varepsilon(\log x)^2 + \varepsilon \log c - \varepsilon \alpha \log p - \log \frac{\beta+1}{\alpha+1}.$$

Mais

$$(10) \quad \alpha = \left[\frac{1}{p^\varepsilon - 1} \right] < \frac{1}{\varepsilon \log p - 1} \leq \frac{1}{\varepsilon \log p},$$

entraîne $\varepsilon \alpha \log p \leq 1$.

D'autre part

$$\beta = \frac{2 \log^2 x + \log c}{\log p} \leq \frac{2 \log^2 x + \log c}{\log 2} \quad \text{et} \quad \varepsilon = \frac{\log 2}{\log x},$$

on aurait alors

$$\text{bén } n \geq (2 \log 2) \log x - 2 \log \log x + O(1).$$

Pour $p^\beta > c x^{2 \log x}$, comme le bénéfice croît avec β , on aurait *a fortiori* la relation précédente, qui est en contradiction avec (9).

Démonstration de (iv). — Si $p < x_2$ ne divise pas n , cela entraîne, par la formule (8) :

$$\text{bén } n \geq \varepsilon \log \frac{1}{p^\alpha} - \log \frac{1}{\alpha+1} = \log(\alpha+1) - \alpha \varepsilon \log p,$$

avec $\alpha = \alpha_p = [1/(p^\varepsilon - 1)]$. Comme $p < x_2$, on a $\alpha \geq 2$, et la formule (10) donne $\alpha \varepsilon \log p \leq 1$. On a donc

$$\text{bén } n \geq \log 3 - 1 > 0.$$

Si une famille de nombres premiers p_1, \dots, p_h ne divisait pas n , cela donnerait, par la formule (8) :

$$\text{bén } n \geq h(\log 3 - 1).$$

Maïs, par (9), on a $\text{bén } n = O(\log x)$, on en déduit que l'on doit avoir $h = O(\log x)$.

Minoration dans le théorème 2. — La minoration, dans le théorème 2, se démontre comme la proposition 3, en utilisant les propriétés énoncées dans la proposition 4 : Si n est F -hautement abondant, on a

$$\begin{aligned} S^2(n) &= \sum_{p^\alpha \parallel n} \frac{\alpha(\alpha+2)}{12} \log^2 p \\ &= \sum_{p < x_2 \text{ ou } p > x, p^\alpha \parallel n} \frac{\alpha(\alpha+2)}{12} \log^2 p + \frac{1}{4} \sum_{x_2 < p < x} \log^2 p \\ &\quad - \sum_{x_2 < p < x, p^\alpha \neq p} \frac{\alpha(\alpha+2)}{12} \log^2 p = \mathcal{S}_1 + \mathcal{S}_2 + \mathcal{S}_3. \end{aligned}$$

Par un calcul déjà vu, on a

$$\mathcal{S}_2 \sim \frac{1}{4} x \log x \sim \frac{1}{4} \log n \log \log n.$$

Dans les sommes \mathcal{S}_1 et \mathcal{S}_3 , le nombre de termes est

$$O(x_2) = O(x^{(\log 3/2)/(\log 2)})$$

et chaque terme est inférieur ou égal à

$$\frac{\alpha(\alpha+2)}{12} \log^2 p \leq \frac{1}{4} (\log p^2)^2 = O(\log^4 x),$$

d'où

$$S(n) \sim \sqrt{\mathcal{S}_2} \sim \frac{1}{2} \sqrt{\log n \log \log n}.$$

On évalue de même $\rho(n) \sim ((\log n)/8) (\log \log n)^2$, et la proposition 2 donne pour toute constante $c_1 < (2 \log 2)/\sqrt{2\pi}$ et n F -hautement abondant assez grand

$$F(n) \geq c_1 \frac{d(n)}{\sqrt{\log n \log \log n}}.$$

3. Le théorème de Sperner

LEMME 3 (Théorème de Sperner) (cf. [3], t. 2, p. 114 et [9] p. 248). — Dans un ensemble à k éléments, si des parties A_1, A_2, \dots, A_h sont telles qu'aucune d'entre elles n'en contient une autre, leur nombre h vérifie :

$$h \leq \binom{k}{[k/2]}, \quad \text{ou} \quad \binom{k}{j} = \frac{k!}{j!(k-j)!} \text{ est le coefficient du binôme.}$$

Soit $n = 2.3 \dots p_k$ le produit des k premiers nombres premiers. Il y a une bijection simple entre les parties de l'ensemble $\{1, 2, \dots, k\}$ et les diviseurs d de n :

A $A \subset \{1, 2, \dots, k\}$, on fait correspondre $d_A = \prod_{i \in A} p_i$, et la relation $A \subset B$ se traduit par $d_A | d_B$.

A l'ensemble des diviseurs d de n vérifiant $t < d \leq 2t$, correspond une famille de Sperner :

$$A \subset B \quad \text{et} \quad A \neq B \Rightarrow d_A | d_B \quad \text{et} \quad d_A \neq d_B \rightarrow d_A \leq 2d_B,$$

et d'après le lemme précédent, on a donc

$$F_n \leq \binom{k}{[k/2]}.$$

Lorsque $k \rightarrow \infty$, la formule de Stirling ($n! \sim n^n e^{-n} \sqrt{2\pi n}$) donne

$$\binom{k}{[k/2]} \sim \sqrt{\frac{2}{\pi}} \frac{2^k}{\sqrt{k}}$$

et d'après la formule (7), on a $k \sim (\log n)/(\log \log n)$, ce qui donne pour $n = 2.3 \dots p_k$ assez grand

$$F(n) \leq (1+\varepsilon) \sqrt{\frac{2}{\pi}} d(n) \sqrt{\frac{\log \log n}{\log n}}.$$

On peut même démontrer, en utilisant le développement d'Euler-Mac-Laurin (cf. [15], p. 27) :

$$n! = n^n e^{-n} \sqrt{2\pi n} \exp\left(\frac{1}{12n} - \frac{\theta}{360n^3}\right) \quad \text{avec } 0 < \theta < 1,$$

que l'on a pour tout k ;

$$\binom{k}{[k/2]} \leq \sqrt{\frac{2}{\pi}} \frac{2^k}{\sqrt{k}}.$$

Le théorème de Sperner se généralise de la façon suivante :

LEMME 4 (cf. [4]). — Soit $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. La plus grande famille de diviseurs de n , tels qu'aucun d'entre eux n'en divise un autre, est obtenue en considérant la famille

$$\prod_{i=1}^k p_i^{\beta_i}, \quad 0 \leq \beta_i \leq \alpha_i \quad \text{et} \quad \sum_{i=1}^k \beta_i = \left\lfloor \frac{1}{2} \sum_{i=1}^k \alpha_i \right\rfloor.$$

Désignons par $D(n)$ le cardinal de cette famille. I. ANDERSON [2] a démontré que

$$(11) \quad D(n) \leq \frac{d(n)}{2^{\Omega(n)}} \left(\frac{\Omega(n)}{[\Omega(n)/2]} \right) \leq \sqrt{\frac{2}{\pi}} \frac{d(n)}{\sqrt{\Omega(n)}},$$

où $\Omega(n) = \alpha_1 + \alpha_2 + \dots + \alpha_k$.

Appliquons cela à un nombre n F -hautement abondant. Il résulte de la proposition 4 que

$$(12) \quad \Omega(n) = \sum_{p \leq x} 1 + O(\sqrt{x}) \log x \sim \frac{\log n}{\log \log n}.$$

On obtient ainsi la majoration

$$F(n) \leq D(n) \leq c_2 \frac{d(n) \sqrt{\log \log n}}{\sqrt{\log n}}.$$

Pour faire passer $\sqrt{\log \log n}$ du numérateur au dénominateur nous aurons besoin d'améliorer le théorème de Sperner, en suivant pour cela SARKÖZY et SZEMEREDI (cf. [17] et [14]).

4. Majoration de $F(n)$. Cas des nombres sans facteurs carrés

LEMME 5. — Soit λ réel, $0 < \lambda < 1/2$. On a

$$1 + \binom{n}{1} + \dots + \binom{n}{[\lambda n]} = O\left(\frac{1}{\lambda^\lambda (1-\lambda)^{1-\lambda}}\right)^n.$$

Démonstration. — On majore la somme de gauche par une progression géométrique de premier terme $\binom{n}{[\lambda n]}$ puis on applique la formule de Stirling.

LEMME 6 (de Sperner amélioré). — Soit un nombre sans facteur carré, $n = p_1 p_2 \dots p_k$. Soit $1 \leq b \leq k$. Soit d_1, \dots, d_s une famille de s diviseurs de n vérifiant

$$s > 2^b \binom{k-b}{[(k-b)/2]}.$$

Alors il existe i et j tels que $d_j/d_i \geq p_{b+1}$.

Démonstration. — Tout diviseur d de n s'écrit $d = d' d''$, où la première composante d' divise $p_1 p_2 \dots p_b$, et la deuxième d'' divise $p_{b+1} \dots p_k$. Le nombre de valeurs possibles de d' est 2^b . Par le principe des tiroirs, pour une certaine valeur d' , il y a plus de $s/2^b$ éléments de $\{d_1, \dots, d_s\}$ dont la première composante soit d' . Quitte à réindexer, on peut supposer que ce sont d_1, \dots, d_m avec

$$m \geq s/2^b > \binom{k-b}{[(k-b)/2]}.$$

On applique le lemme 3 (théorème de Sperner) à d_1'', \dots, d_m'' . Il existe alors i et j tels que d_i'' divise d_j'' , ce qui entraîne $d_j/d_i = d_j''/d_i'' \geq p_{b+1}$.

PROPOSITION 5. — Soit $n = p_1 p_2 \dots p_k$, avec $p_1 < p_2 < \dots < p_k$, un entier sans facteur carré. Soit $1 \leq b \leq k$. Soit \mathcal{H} un ensemble de h diviseurs premiers de n pris parmi p_1, \dots, p_b et ayant la propriété que $p_i \in \mathcal{H}$ et $p_j \in \mathcal{H}$ et $p_i > p_j \Rightarrow p_i/p_j > 2$. Soit $\lambda \in \mathbf{R}$, $0 < \lambda < 1/2$. Alors on a

$$[\lambda h] \left[F(n) - 2^{k-h} \left(1 + \binom{h}{1} + \dots + \binom{h}{[\lambda h]} \right) \right] \leq 2^b \binom{k-b}{[(k-b)/2]}.$$

Démonstration. — Soit $d_1 < d_2 < \dots < d_{F(n)}$ une famille de diviseurs de n , concrétisant la définition de $F(n)$. On a donc $d_{F(n)} < 2d_1$.

Pour chaque valeur de i , $1 \leq i \leq F(n)$, soit $r(i)$ le nombre de diviseurs premiers de d_i appartenant à \mathcal{H} . On construit alors la famille $\delta_{i,j} = d_i/p_{m_j}$ pour $1 \leq j \leq r(i)$ et $p_{m_j} \in \mathcal{H}$.

Ces nombres $\delta_{i,j}$ ont les trois propriétés suivantes :

— ils sont distincts : Si l'on avait $d_i/p = d_{i'}/p'$ avec $p > p'$, cela entraînerait $d_i/d_{i'} > p/p' > 2$, ce qui n'est pas possible;

— le quotient $\delta_{i,j}/\delta_{i',j'}$ est majoré par p_b . On a

$$\frac{\delta_{i,j}}{\delta_{i',j'}} \leq \frac{d_i}{p} \frac{p'}{d_{i'}} \leq \frac{d_i}{d_{i'}} \frac{p'}{p} \leq 2 \frac{p_b}{2} = p_b;$$

— combien y a-t-il de $\delta_{i,j}$? Parmi les diviseurs de n , il y en a $2^{k-h} \binom{h}{s}$ qui sont divisibles par exactement s éléments de \mathcal{H} . Le nombre de $\delta_{i,j}$ est donc supérieur à

$$[\lambda h] \left[F(n) - 2^{k-h} \sum_{1 \leq i \leq \lambda h} \binom{n}{i} \right]$$

pour n'importe quelle valeur de λ .

Il ne reste plus qu'à appliquer le lemme 6 à la famille $\delta_{i,j}$ pour achever la démonstration.

Choix des paramètres. — Appliquons la proposition 5 au nombre $n = p_1, \dots, p_k$. Soit $\eta > 0$ donné. On choisit $b = [\eta k]$. Par le théorème des nombres premiers, pour $t > t_0(\eta)$, il existe un nombre premier entre t et $t(1+\eta)$. On peut donc choisir

$$h > \frac{\log b}{\log 2} (1-\eta) > \frac{\log k}{\log 2} (1-2\eta).$$

La proposition 5 donne alors :

$$F(n) \leq \frac{1}{(\lambda h)} \sqrt{\frac{2}{\pi}} \frac{2^k}{\sqrt{k-b}} + 2^{k-h} o\left(\frac{1}{\lambda^\lambda (1-\lambda)^{1-\lambda}}\right)^h.$$

Pour que le reste soit négligeable devant le premier terme, il faut choisir λ pour que $1/(\lambda^\lambda (1-\lambda)^{1-\lambda}) < \sqrt{2}$; ce qui donne $\lambda = 0,11$. On obtient

tableau qui a $j(n-k)$ éléments, chaque dame apparaît au plus $(k+1)$ fois. Le nombre de dames distinctes du tableau est donc $\geq j(n-k)/(k+1)$ et donc $\geq j$ (puisque $k < n/2$), ce qui vérifie la condition de Hall.

On peut alors marier un monsieur à une dame de sa connaissance, ce qui assure l'injection affirmée dans l'énoncé.

PROPOSITION 7. — Soit $\alpha_1, \alpha_2, \dots, \alpha_h$ des nombres réels ≥ 1 . On définit

$$\lambda_r = \lambda_r(\alpha_1, \dots, \alpha_h) = \sum_{1 \leq i_1 < i_2 < \dots < i_r \leq h} \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_r}$$

Les coefficients λ_r apparaissent dans le développement du produit

$$\prod_{i=1}^h (x + \alpha_i) = x^h + \lambda_1 x^{h-1} + \dots + \lambda_r x^{h-r} + \dots + \lambda_h.$$

Alors on a, pour $r \leq h/2$, $\lambda_r \leq 1/2^h \binom{h}{r} \prod_{i=1}^h (1 + \alpha_i)$.

Démonstration. — Le coefficient λ_r est une somme de $\binom{h}{r}$ termes indexés par les éléments $\{i_1, i_2, \dots, i_r\}$ de $\mathcal{P}_r(\{1, 2, \dots, h\})$. La proposition précédente montre, comme on a $\alpha_i \geq 1$, que $\lambda_r \leq \lambda_{r+1}$ pour $r < h/2$. On a ensuite

$$\frac{\lambda_r(\alpha_1, \alpha_2, \dots, \alpha_h)}{\prod_{1 \leq i \leq h} (\alpha_i + 1)} = \frac{\alpha_h \lambda_{r-1}(\alpha_1, \dots, \alpha_{h-1}) + \lambda_r(\alpha_1, \dots, \alpha_{h-1})}{(\prod_{1 \leq i \leq h-1} (\alpha_i + 1))(\alpha_h + 1)}.$$

Le membre de droite est une fonction homographique de α_h dont le déterminant est du signe de

$$\lambda_{r-1}(\alpha_1, \dots, \alpha_{h-1}) - \lambda_r(\alpha_1, \dots, \alpha_{h-1}).$$

Pour $r \leq h/2$, on a $r-1 < (h-1)/2$, et cette quantité est négative ou nulle. La fonction homographique de α_h est décroissante (ou constante) et donc maximale pour $\alpha_h = 1$. On peut faire le même raisonnement par rapport à $\alpha_1, \alpha_2, \dots, \alpha_{h-1}$, et on conclut que

$$\frac{\lambda_r(\alpha_1, \alpha_2, \dots, \alpha_h)}{\prod_{1 \leq i \leq h} (\alpha_i + 1)} \leq \frac{\lambda_r(1, 1, \dots, 1)}{\prod_{1 \leq i \leq h} (1 + 1)} = \frac{1}{2^h} \binom{h}{r}.$$

PROPOSITION 8. — Soit $n = p_1^{\alpha_1} \dots p_h^{\alpha_h}$. Soit \mathcal{H} un ensemble de h nombres premiers pris parmi p_1, p_2, \dots, p_h . Soit $r \leq h/2$. Le nombre de diviseurs de n ayant au plus r diviseurs premiers dans \mathcal{H} est inférieur ou égal à $(d(n)/2) \sum_{i \leq r} \binom{h}{i}$.

Démonstration. — L'ordre naturel des nombres n'intervenant pas, on peut réindexer les p_i de façon que $p_1, p_2, \dots, p_h \in \mathcal{H}$. Lorsque $r = 0$ il y a

$$A_0 = \prod_{b+1 \leq i \leq h} (\alpha_i + 1) = \frac{d(n)}{\prod_{1 \leq i \leq h} (\alpha_i + 1)}$$

diviseurs de n ayant r nombres premiers dans \mathcal{H} .

Lorsque $r = 1$, il y en a $A_1 = (\alpha_1 + \alpha_2 + \dots + \alpha_h) A_0$. De même

$$A_r = A_0 \sum_{1 \leq i_1 < i_2 < \dots < i_r \leq h} (\alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_r}) = \lambda_r(\alpha_1, \dots, \alpha_h) A_0.$$

La proposition 7 précédente permet de conclure.

6. Majoration de $F(n)$. Cas général

LEMME 7. — Soit $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Soit $1 \leq b \leq k$. Soit $n' = p_1^{\alpha'_1} \dots p_b^{\alpha'_b}$ et $n'' = p_{b+1}^{\alpha''_{b+1}} \dots p_k^{\alpha''_k}$. Soit d_1, \dots, d_s une famille de s diviseurs de n vérifiant $s > d(n') D(n'')$, où $D(n'')$ a été défini au lemme 4. Alors il existe i et j tels que $d_j/d_i \geq p_{b+1}$.

La démonstration est semblable à celle du lemme 6. On écrit un diviseur d de n sous la forme $d = d' d''$ avec $d' | n'$ et $d'' | n''$. On applique le principe des tiroirs à la famille d_1, \dots, d_s pour la composante d' , puis le lemme 4 à la composante d'' .

PROPOSITION 9. — Soit $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ et $1 \leq b \leq k$. Soit \mathcal{H} un ensemble de h diviseurs premiers de n pris parmi p_1, p_2, \dots, p_b et ayant la propriété que $p_i \in \mathcal{H}, p_j \in \mathcal{H}$ et $p_i > p_j \Rightarrow p_i > 2 p_j$. Soit λ réel, $0 < \lambda < 1/2$. On pose $\Omega = \sum_{b < i \leq k} \alpha_i$. On a alors :

$$(14) \quad [\lambda, h] \left[F(n) - \frac{d(n)}{2^h} \sum_{i \leq \lambda h} \binom{h}{i} \right] \leq \frac{d(n)}{2^\Omega} \binom{\Omega}{[\Omega/2]} \leq \sqrt{\frac{2}{\pi}} \frac{d(n)}{\sqrt{\Omega}}$$

La démonstration suit la démonstration de la proposition 5. On construit une famille $\delta_{i,j}$ de diviseurs distincts de n dont le quotient est majoré par p_b . On minore le cardinal de la famille $\delta_{i,j}$ par le nombre de gauche de l'inégalité (14) à l'aide de la proposition 8, puis on applique le lemme 7 et l'inégalité (11).

Majoration du théorème 2. — On va appliquer la proposition 9 en choisissant au mieux les paramètres : Montrons que l'on peut choisir $h/((\log k)/(\log 2))$ aussi voisin de 1 que l'on veut.

Soit η fixé; soit n un nombre F -hautement abondant assez grand, N_k le nombre hautement composé supérieur qui le précède et $x = 2^{1/\eta}$ comme dans

la proposition 4. Le théorème des nombres premiers dit que, pour δ fixé > 0 et $u \geq u_0(\delta)$, il existe au moins $(\delta/2)(u/\log u)$ nombres premiers entre $u(1-\delta)$ et u .

On choisit $y = \eta x$. Les nombres premiers p_1, \dots, p_b seront les diviseurs de n inférieurs à y . On distingue dans l'intervalle (y^η, y) les sous-intervalles

$$\left[\frac{(1-\delta)^j}{2^j} y, \frac{(1-\delta)^{j-1}}{2^j} y \right]; \dots; \left[\frac{(1-\delta)^2}{2} y, \frac{(1-\delta)}{2} y \right]; ((1-\delta)y, y)$$

dans chaque intervalle $(u(1-\delta), u)$ il y a au moins $(\delta/2)(u/\log u)$ nombres premiers : Si $u > x_2$, d'après la proposition 4 (ii), si $u < x_2$ d'après la proposition 4 (iv), on peut en choisir un qui divise n , et cela assure que $h \geq ((1-\eta) \log y)/(\log(2/(1-\delta)))$.

On choisit les autres paramètres comme dans le paragraphe 4 et, compte tenu de (12), on obtient pour n assez grand et F -hautement abondant

$$F(n) \leq \sqrt{\frac{2 \log 2}{\pi}} \frac{d(n)}{\sqrt{\log n \log \log n}}.$$

7. Démonstration du théorème 3

Le théorème 2 va nous permettre d'obtenir une meilleure majoration du bénéfice que la formule (9). Soit n un nombre F -hautement abondant et N_ε le nombre hautement composé supérieur précédant n . On a

$$c_1 \frac{d(N_\varepsilon)}{\sqrt{\log N_\varepsilon \log \log N_\varepsilon}} \leq F(N_\varepsilon) < F(n) < c_2 \frac{d(n)}{\sqrt{\log n \log \log n}},$$

l'inégalité de gauche se démontrant comme la proposition 3. On en déduit

$$\begin{aligned} \text{bén } n &= \varepsilon \log \frac{n}{N_\varepsilon} - \log \frac{d(n)}{d(N_\varepsilon)} \leq \log \frac{d(N_\varepsilon)}{d(n)} + O(1) \\ &\leq \log \frac{c_2}{c_1} \sqrt{\frac{\log N_\varepsilon \log \log N_\varepsilon}{\log n \log \log n}} + O(1) \end{aligned}$$

et comme $\log n \sim \log N_\varepsilon$, il vient

$$(15) \quad \text{bén } n = O(1).$$



Supposons maintenant que q^β , avec $\beta < a$ divise exactement n , cela entraînerait, d'après la formule (8) :

$$\begin{aligned} \text{bén } n &\geq \varepsilon \log q^{\beta-a} - \log \frac{\beta+1}{\alpha_q+1} \\ &\geq \log(\alpha_q+1) - \log(\beta+1) - 1 \\ &\geq \log(\alpha_q+1) - \log(\beta+1) - 1 \end{aligned}$$

en utilisant (10).

Quand n tend vers l'infini, q étant fixé, $\varepsilon \rightarrow 0$ et

$$\alpha = \left[\frac{1}{q^\varepsilon - 1} \right] = \frac{1}{e^{\varepsilon \log q} - 1} + O(1) \sim \frac{1}{\varepsilon \log q} \sim \frac{\log x}{\log 2 \log q},$$

d'où

$$\text{bén } n \geq \log \log x + O(1).$$

C'est en contradiction avec (15) et cela démontre le théorème 3. On peut préciser d'ailleurs le résultat suivant :

PROPOSITION 10. — Soit n un nombre F -hautement abondant assez grand; tout nombre premier $p < (\log n)^{10^{-3}}$ divise n .

Démonstration. — Il suffit d'expliciter la démonstration précédente, en utilisant les valeurs des constantes dans le théorème 2, $(c_2/c_1) \leq (1/0,11)$.

Remarque. — Bien que tous ces résultats soient effectifs, la proposition 10 ne permet pas de démontrer que tous les nombres F -hautement abondants sont pairs, ce que laisse supposer les tables. Pour la fonction g , on peut remarquer (cf. [13]) que si n est un nombre impair g -hautement abondant, n n'est divisible par aucun nombre premier $p \equiv 1 \pmod{4}$, ce qui permet de montrer que tous les nombres g -hautement abondants sont pairs.

Il est probable qu'il existe une astuce semblable pour la fonction F . En calculant les nombres F -hautement abondants jusqu'à $n = 370$ millions, on a pu constater qu'ils sont tous « sans trous » (Si p divise n , tout nombre premier inférieur à p divise n). En fait, tous ces nombres sont hautement composés sauf trois :

$$138\,600 (F = 18); \quad 360\,360 (F = 22); \quad 232\,792\,560 (F = 82).$$

Il semble difficile de dire s'il y a une infinité de telles exceptions, ou même s'il existe une infinité de nombres simultanément F -hautement abondants et hautement composés.

8. Algorithmes de calcul de $F(n)$

On pose $q_t(n) = \sum_{d|n, t/2 < d \leq t} 1$. On a donc $F(n) = \max_t q_t(n)$.
 Il est clair que, pour n fixé, $q_t(n)$ est constant lorsque t varie entre deux entiers consécutifs. D'autre part, en raison de la correspondance entre diviseurs $d \mapsto n/d$, on a, pour t non entier

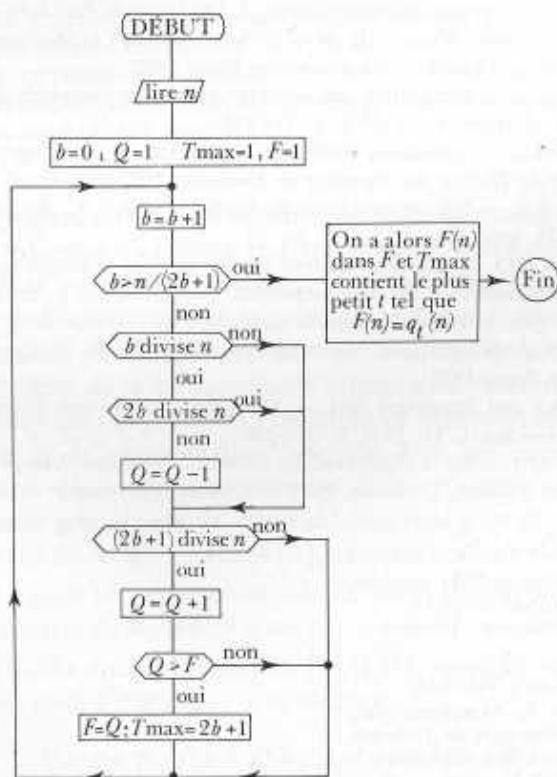
$$q_t(n) = q_{2n/t}(n).$$

On a donc

$$F(n) = \max_{t \leq \sqrt{2n}} q_t(n).$$

Le principe de l'algorithme est de calculer $q_t(n)$ de proche en proche en partant de $q_1(n) = 1$. En fait, on doit distinguer t pair et t impair; d'où on pose $t = 2b$ et $t = 2b+1$, en faisant varier b . On peut ainsi construire l'organigramme de calcul de F .

Si l'on veut calculer $F(n)$ pour des entiers consécutifs, l'algorithme ci-dessus peut aisément s'appliquer par une méthode de crible.



BIBLIOGRAPHIE

- [1] ALAOGU (L.) and ERDŐS (P.). — On highly composite and similar numbers, *Trans. Amer. math. Soc.*, t. 56, 1944, p. 448-469.
- [2] ANDERSON (I.). — On primitive sequences, *J. London math. Soc.*, t. 42, 1967, p. 137-148.
- [3] COMTET (L.). — *Analyse combinatoire*. — Paris, Presses Universitaires de France, 1970 (Collection « Sup », *Le Mathématicien*, 4 et 5).
- [4] de BRUIJN (N. G.), Van E. TENBERGEN (C.) and KRUYSWIJK (D.). — On the set of divisors of a number, *Nieuw Arch.*, Série 2, t. 23, 1949-1952, p. 191-193.
- [5] ERDŐS (P.) et NICOLAS (J.-L.). — Répartition des nombres superabondants, *Bull. Soc. math. France*, 1975, t. 103, p. 65-90.
- [6] ERDŐS (P.). — Sur une inégalité asymptotique en théorie des nombres [en russe], *Vestnik Leningrads. Univ.*, t. 13, 1960, p. 41-49.
- [7] ERDŐS (P.). — Problème 218 and solution, *Can. math. Bull.*, t. 17, 1974, p. 621-622.
- [8] FELLER (W.). — *An introduction to probability theory and its applications*. vol. 2. Second edition. — New York, Wiley, 1971.
- [9] HALBERSTAM (H.) and ROTH (K. F.). — *Sequences*. — Oxford, at the Clarendon Press, 1966.
- [10] HALL (P.). — On representatives of subsets, *J. London math. Soc.*, t. 10, 1935, p. 26-30.
- [11] HARDY (G. H.) and WRIGHT (E. M.). — *An introduction to the theory of numbers*. 4th edition. — Oxford, at the Clarendon Press, 1960.
- [12] NICOLAS (J.-L.). — Répartition des nombres hautement composés de Ramanujan, *Canad. J. of Math.*, t. 23, 1971, p. 116-130.
- [13] NICOLAS (J.-L.). — Quelques méthodes élémentaires en théorie des nombres, *Séminaire de Théorie des Nombres de Bordeaux*, 1975, exposé n° 13.
- [14] NICOLAS (J.-L.). — Sur un problème de Erdős et Moser, *C. R. Acad. Sc. Paris*, t. 282, 1976, série A, p. 9-12.
- [15] RADEMACHER (H.). — *Topics in analytic number theory*. — Berlin, Springer-Verlag, 1973 (*Die Grundlehren der mathematischen Wissenschaften*, p. 169).
- [16] RAMANUJAN (S.). — Highly composite numbers, *Proc. London math. Soc.*, Series 2, t. 14, 1915, p. 347-409; and "Collected papers", p. 78-128. — Cambridge, at the University Press, 1927.
- [17] SARKÖZY (A.) und SZEMEREDI (E.). — Über ein Problem von Erdős und Moser, *Acta Arithmetica*, t. 11, 1965, p. 205-208.
- [18] TENENBAUM (G.). — Sur la répartition des diviseurs, *Séminaire Delange-Pisot-Poitou : Théorie des nombres*, 17^e année, 1975/1976, Groupe d'étude n° G 14.

(Texte reçu le 31 mai 1976.)

Paul ERDŐS,
Akadémia Matematikai Intezete,
Reáltanoda u. 13-15,
H-1053 Budapest, Hongrie
et
Jean-Louis NICOLAS,
Département de Mathématiques,
U.E.R. des Sciences de Limoges,
123, rue Albert-Thomas,
87100 Limoges.