

SÉMINAIRE DELANGE-PISOT-POITOU. THÉORIE DES NOMBRES

JEAN-LOUIS NICOLAS

**Sur l'ordre maximum d'un élément dans le groupe
 S_n des permutations, II**

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 8, n° 2 (1966-1967),
exp. n° 11, p. 1-18

http://www.numdam.org/item?id=SDPP_1966-1967__8_2_A2_0

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1966-1967, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

SUR L'ORDRE MAXIMUM D'UN ÉLÉMENT DANS LE GROUPE S_n DES PERMUTATIONS, II.

par Jean-Louis NICOLAS

Soit $g(n) = \sup_{\sigma \in S_n} [\text{ordre de } \sigma]$.

1. Rappel de propriétés élémentaires de $g(n)$ ([1], § 61, et [2]).

$g(n)$ est croissante, mais non strictement croissante ;

$$g(n) = \sup_{n_1 + n_2 + \dots + n_k = n} [p. p. c. m. (n_1, n_2, \dots, n_k)] ;$$

$$g(n) = \sup_{\sum p^r \leq n} [p^r \text{ (} p \text{ premier, } r \in \mathbb{N}^*)].$$

Définition. - Soit $\ell : \mathbb{N}^* \rightarrow \mathbb{N}$.

$$\ell(1) = 0 ,$$

$$\ell\left(\prod_{i=1}^k p_i^{\alpha_i}\right) = \sum_{i=1}^k \ell(p_i^{\alpha_i}) \quad \text{avec } p_i \text{ premier et } \alpha_i \in \mathbb{N}^* .$$

ℓ est une fonction arithmétique additive :

$$(m, n) = 1 \implies \ell(mn) = \ell(m) + \ell(n) ,$$

et sa restriction aux nombres p^α (p premier, $\alpha \in \mathbb{N}^*$) est l'application identique. On a $\ell(k) \leq k$ pour tout k , et $\ell(k) = k$ entraîne $k = p^\alpha$.

Remarque. - Si $\alpha = 0$, $\ell(p^\alpha) = 0 \neq p^\alpha = 1$.

On a donc :

$$(1) \quad g(n) = \sup_{\ell(k) \leq n} k .$$

Ce qui équivaut à

$$(2) \quad \begin{cases} \ell(g(n)) \leq n \\ M > g(n) \implies \ell(M) > n . \end{cases}$$

Remarquons que (3) est équivalent à (3') :

$$(3') \quad M > g(n-1) \implies \ell(M) \geq n .$$

Propriété caractéristique. - Les deux propriétés suivantes sont équivalentes :

$$(a) \quad m \in g(\underline{\mathbb{N}}) \quad ,$$

$$(b) \quad M > m \implies \ell(M) > \ell(m) \quad .$$

Démonstration.

(a) $\implies$ (b) . Soit $m \in g(\underline{\mathbb{N}})$, et soit $M > m$, (3) et (2) donnent :

$$\ell(M) > n \geq \ell(g(n)) = \ell(m) \quad .$$

(b) $\implies$ (a) . Soit m vérifiant (b). Si $m \notin g(\underline{\mathbb{N}})$, comme g est croissante et non bornée, il existe n tel que

$$g(n-1) < m < g(n) \quad .$$

(3') et (2) donnent :

$$\ell(m) \geq n \geq \ell(g(n)) \quad .$$

On a construit $M = g(n)$, $M > m$ et $\ell(M) \leq \ell(m)$, ce qui contredit l'hypothèse.

COROLLAIRE. - Si $M \neq g(n)$ et si $\ell(M) \leq \ell(g(n))$, alors $M < g(n)$.

C'est une autre façon d'écrire : (a) $\implies$ (b) .

Remarque. - Soit $f : \underline{\mathbb{N}}^* \rightarrow \underline{\mathbb{R}}$ une fonction arithmétique.

On dit que f est grande en n , si $m < n \implies f(m) < f(n)$;

On dit que f est petite en n , si $m > n \implies f(m) > f(n)$.

La propriété caractéristique s'écrit alors :

L'ensemble des nombres $n \in \underline{\mathbb{N}}^*$, où ℓ est petite, est exactement $g(\underline{\mathbb{N}})$.

Soit $d(n)$ le nombre de diviseurs de n ([1], § 60). RAMANUJAN [3] appelle "Highly composite number" un nombre en lequel la fonction d est grande, et utilise pour étudier ces nombres des méthodes qui peuvent s'appliquer à d'autres fonctions, et en particulier à ℓ .

Relation entre ℓ et g .

1° Calcul de $\ell(g(n))$. On définit sur $\underline{\mathbb{N}}$ la relation d'équivalence

$$n \sim n' \iff g(n) = g(n') \quad .$$

Soit $\hat{n}$ le plus petit élément de la classe de n . On a

$$g(\hat{n}) = g(n) ; \quad \hat{n} \leq n ; \quad g(\hat{n}-1) < g(\hat{n}) \quad .$$

(3') donne $\ell(g(\hat{n})) \geq \hat{n}$, et (2) donne $\ell(g(\hat{n})) \leq \hat{n}$, donc

$$\ell(g(n)) = \ell(g(\hat{n})) = \hat{n}.$$

On a en fait démontré les équivalences :

$$n = \hat{n} \iff \ell(g(n)) = n \iff g(n) > g(n-1) \iff n \in \ell \circ g(\underline{\mathbb{N}}).$$

2° ℓ est strictement croissante sur $g(\underline{\mathbb{N}})$. Soit $g(m) < g(n)$, alors $g(m) < g(\hat{n})$, donc $m < \hat{n}$ (g est croissante) et, avec (2),

$$\ell(g(m)) \leq m < \hat{n} = \ell(g(n)).$$

3° $g(\ell(N)) \geq N$ pour tout $N \in \underline{\mathbb{N}}^*$. L'égalité a lieu si, et seulement si, $N \in g(\underline{\mathbb{N}})$. Puisque $g(\ell(N)) = \sup_{\ell(k) \leq \ell(N)} k$, N est une valeur possible de k , et $g(\ell(N)) \geq N$.

Si $N \notin g(\underline{\mathbb{N}})$, il ne peut y avoir égalité, car $g(\ell(N)) \in g(\underline{\mathbb{N}})$.

Si $N = g(n)$, $g(\ell(g(n))) = g(\hat{n}) = g(n)$.

4° Soient $A \in g(\underline{\mathbb{N}})$, et A^* le suivant de A dans $g(\underline{\mathbb{N}})$; alors

$$(4) \quad \ell(A) \leq n < \ell(A^*) \quad \text{entraîne} \quad g(n) = A.$$

On a $g(n) \leq g[\ell(A^*) - 1] < g(\ell(A^*)) = A^*$, car $\ell(A^*) \in \ell(g(\underline{\mathbb{N}}))$. D'autre part, $g(n) \geq g(\ell(A)) = A$, donc $g(n) = A$.

5° On a

$$(5) \quad A < N \leq A^* \implies \ell(N) \geq \ell(A^*),$$

$g(\ell(N)) \geq N$, donc $g(\ell(N)) \geq A^*$.

Or si $\ell(N) < \ell(A^*)$, on aurait $g(\ell(N)) \leq A$ d'après (4), d'où contradiction.

Finalement, la restriction de ℓ à $g(\underline{\mathbb{N}})$ est une bijection croissante sur $\ell(g(\underline{\mathbb{N}}))$, et l'application réciproque est g . (4) nous permet de calculer $g(n)$ si $n \notin \ell(g(\underline{\mathbb{N}}))$, et (5) nous donne une minoration pour $\ell(N)$ si $N \notin g(\underline{\mathbb{N}})$.

2. Etude de la décomposition en facteurs premiers de $g(n)$.

Pour cela, on va utiliser systématiquement la propriété caractéristique. On rappelle que $v_p(N)$ désigne le plus grand exposant α tel que p^α divise N .

PROPRIETE 1. - Soient p, q deux nombres premiers, $p < q$. Si

$$\alpha = v_p(g(n)) \quad \text{et} \quad \beta = v_q(g(n)),$$

alors $\beta \leq \alpha + 1$.

Démonstration. - On peut supposer $\beta \geq 2$ (si $\beta = 0$ ou 1 , c'est évident).

Soit $M = \frac{p^k}{q} g(n)$, avec k défini par $pq > p^k > q$.

On a $M > g(n)$, donc $\ell(M) > \ell(g(n))$, donc si $\alpha \neq 0$,

$$p^{\alpha+k} + q^{\beta-1} > p^\alpha + p^\beta,$$

ce qui entraîne

$$p^{\alpha+1} q + q^{\beta-1} > p^\alpha + q^\beta,$$

$$p^\alpha(pq - 1) > q^{\beta-1}(q - 1) \geq pq^{\beta-1},$$

$$(6) \quad p^\alpha q > p^{\alpha-1}(pq - 1) > q^{\beta-1},$$

$$q^\alpha > p^\alpha \geq q^{\beta-2},$$

$\alpha > \beta - 2$, donc $\beta \leq \alpha + 1$.

Si $\alpha = 0$, $\ell(M) > \ell(g(n))$ s'écrit :

$$p^k + q^{\beta-1} > q^\beta,$$

les calculs sont les mêmes, la majoration (6) $pq - 1 < pq$ n'ayant pas à être faite.

PROPRIÉTÉ 2. - Soit p le plus grand nombre premier divisant $g(n)$. On a $v_p(g(n)) = 1$, sauf pour $n = 4$.

On désigne par q le nombre premier suivant p .

Si $\alpha = v_p(g(n)) \geq 2$, on pose $M = \frac{q}{p} g(n) > g(n)$;

$$\ell(M) - \ell(g(n)) = q + p^{\alpha-1} - p^\alpha.$$

D'après le postulat de Bertrand ([1], § 22), $q < 2p$, donc

$$q + p^{\alpha-1} - p^\alpha < 2p + p^{\alpha-1} - p^\alpha \leq 2p + p - p^2 = p(3 - p),$$

car la fonction $\alpha \mapsto p^{\alpha-1} - p^\alpha$ est décroissante.

Si $p \geq 3$, $\ell(M) - \ell(g(n)) \leq 0$, il y a contradiction.

Si $p = 2$, il reste à résoudre $g(n) = 2^\alpha$.

Si $\alpha \geq 3$, $M = 2^{\alpha-1} 3 > g(n)$ et $\ell(M) - \ell(g(n)) = 3 - 2^{\alpha-1} < 0$; les seules solutions sont $g(2) = 2$ et $g(4) = 4$. Seule cette dernière est exception.

PROPRIÉTÉ 3. - $g(n)$ est pair pour $n \neq 3, 8, 15$.

LEMME. - Si deux nombres premiers distincts p et p' ne divisent pas $g(n)$, tout nombre premier $q \geq p + p'$ ne divise pas $g(n)$.

Démonstration du lemme. - Soit $p < p'$, et supposons que $q \geq p + p'$ ne divise pas $g(n)$. Soit $k \geq 1$, défini par

$$p^k + p' \leq q \leq p^{k+1} + p' - 1,$$

et posons $M = \frac{p^k p'}{q} g(n)$, on a

$$\ell(M) - \ell(g(n)) = p^k + p' - q \leq 0.$$

D'autre part,

$p^k p' - q \geq p^k p' - p^{k+1} - p' + 1 = p^k(p' - p) - p' + 1 \geq p(p' - p) - p' + 1$,
et

$$p(p' - p) - p' + 1 = (p - 1)(p' - p - 1) \geq 0,$$

donc $M \geq g(n)$, il y a contradiction.

Démonstration de la propriété 3. - Si 2 ne divise pas $g(n)$, $g(n)$ est "quadrattfrei" (propriété 1), et 11 ne divise pas $g(n)$. Sinon, en effet, soit $M = \frac{12}{11} g(n)$, $M > g(n)$, et $\ell(M) - \ell(g(n)) \leq 4 + 6 - 11 < 0$. D'après le lemme, tout nombre premier supérieur ou égal à 13 ne divise pas $g(n)$. Donc $g(n)$ divise $3 \cdot 5 \cdot 7 = 105$. En examinant les valeurs de $g(n)$, on trouve comme seule exception $n = 3, 8, 15$, où $g(n)$ vaut 3, 15, 105.

COROLLAIRE. - Pour tout $n \in \mathbb{N}^*$, $\frac{g(n+1)}{g(n)} \leq 2$ ou, ce qui est équivalent, pour tout $A \in g(\mathbb{N})$, $\frac{A^*}{A} \leq 2$.

Effectivement, si $g(n+1) \neq g(n)$, en posant $g(n) = A$, on a $g(n+1) = A^*$.

Supposons que A^* soit pair et que $\frac{A^*}{A} > 2$, on aurait $A < \frac{A^*}{2} < A^*$, donc, d'après (5), $\ell(\frac{A^*}{2}) \geq \ell(A^*)$, ce qui est faux. Si $A^* = 3, 15, 105$, on trouve $A = 2, 12, 84$, la relation est encore vérifiée.

PROPRIÉTÉ 4. - Soient λ, μ deux nombres premiers, $\alpha = v_\lambda(g(n))$ et $\beta = v_\mu(g(n))$, on a :

$$\frac{1}{\lambda\mu} \leq \frac{\lambda^\alpha}{\mu^\beta} \leq \lambda\mu.$$

Il suffit de vérifier l'une des inégalités, par exemple $\frac{1}{\lambda\mu} \leq \frac{\lambda^\alpha}{\mu^\beta}$. Soit k défini par $\mu - 1 < \lambda^k \leq \lambda(\mu - 1)$. On a donc $k \geq 2$ si $\lambda < \mu$, et $k = 1$ si $\lambda > \mu$. Posons $M = \frac{\lambda^k}{\mu} g(n)$, on a

$$M > g(n) \quad \text{et} \quad \ell(M) - \ell(g(n)) > 0 ,$$

donc

$$(7) \quad \lambda^{\alpha+k} - \lambda^\alpha + \mu^{\beta-1} - \mu^\beta > 0 .$$

Posons $x = \frac{\lambda^\alpha}{\mu^\beta}$, on obtient

$$x > \frac{1 - \frac{1}{\mu}}{\lambda^k - 1} > \frac{1 - \frac{1}{\mu}}{\lambda(\mu - 1)} = \frac{1}{\lambda\mu} .$$

Ce raisonnement ne vaut que pour $\alpha \geq 1$ et $\beta \geq 2$.

Pour $\beta = 1$, l'inégalité (7) est encore vérifiée.

Si $\beta = 0$, on a toujours $\lambda^\alpha \geq \frac{1}{\lambda\mu}$.

Si $\alpha = 0$:

- si $\lambda < \mu$, d'après la propriété 1, $\beta \leq 1$ et $\frac{1}{\lambda\mu} \leq \frac{1}{\mu}$;
 - si $\lambda > \mu$: si $\beta = 1$, on a bien $\frac{1}{\lambda\mu} \leq \frac{1}{\mu}$; si $\beta \geq 2$, l'inégalité (7) devient $\lambda + \mu^{\beta-1} - \mu^\beta > 0$. Posons $x = \frac{1}{\mu^\beta}$,

$$x > \frac{1 - \frac{1}{\mu}}{\lambda} = \frac{\mu - 1}{\lambda\mu} \geq \frac{1}{\lambda\mu} .$$

Dans ce cas, on obtient d'ailleurs un meilleur résultat.

PROPRIÉTÉ 5. - Soit p le plus grand nombre premier divisant $g(n)$; soit q le nombre premier suivant p ; soit λ un nombre premier tel que $\alpha = v_\lambda(g(n)) \geq 2$, alors,

$$\lambda^\alpha - \lambda^{\alpha-1} < q \quad \text{et} \quad \lambda < q^{1/\alpha} + 1 .$$

On pose $M = \frac{q}{\lambda} g(n)$, $M > g(n)$, donc

$$\ell(M) - \ell(g(n)) = q + \lambda^{\alpha-1} - \lambda^\alpha > 0 ,$$

donc $\lambda^\alpha - \lambda^{\alpha-1} < q$. D'autre part, les solutions de cette inéquation en λ vérifient $\lambda < q^{1/\alpha} + 1$.

PROPRIÉTÉ 6. - Soient A et A^* deux éléments consécutifs de $g(\mathbb{N})$, p le plus grand nombre premier divisant A , q son suivant. On a

$$\ell(A^*) - \ell(A) \leq q - p .$$

Soit A_1 le plus petit nombre de $g(\mathbb{N})$ vérifiant $\frac{Aq}{p} \leq A_1$. On a, d'après (5),

$$\ell\left(\frac{Aq}{p}\right) = \ell(A) + q - p \geq \ell(A_1) ,$$

et

$$\ell(A^*) - \ell(A) \leq \ell(A_1) - \ell(A) \leq q - p .$$

COROLLAIRE. - Quand n tend vers l'infini, le plus grand nombre premier p divisant $g(n)$ tend vers l'infini.

D'après la propriété 5, pour chaque $\lambda \leq p$, on a $\lambda^\alpha < \frac{q\lambda}{\lambda - 1}$, donc

$$\ell(g(n)) \leq \sum_{\lambda \leq p} \frac{q\lambda}{\lambda - 1} .$$

D'après (4) et la propriété 6, $n - \ell(g(n)) < q - p$. Donc,

$$n \leq \sum_{\lambda \leq p} \frac{q\lambda}{\lambda - 1} + q - p .$$

On voit que, si p est fixé, n est majoré, ce qui établit le corollaire.

PROPRIÉTÉ 7. - Soit $k \in \mathbb{N}$; soient $2, 3, \dots, p_k$ les k premiers nombres premiers. On suppose que $p_k < p$, p étant toujours le plus grand nombre premier divisant $g(n)$. On pose :

$$\alpha_i = v_{p_i}(g(n)) \quad \text{pour} \quad i = 1, 2, \dots, k ,$$

et

$$m = \sum_{i=1}^k \ell(p_i^{\alpha_i}) .$$

Alors il existe une constante c_k indépendante de p telle que

$$m > \frac{1}{c_k} p^{1-(1/k)} .$$

D'autre part, soit μ un nombre premier ne divisant pas $g(n)$ et tel que $\mu > e^{\frac{1}{\theta(p_k)}}$, alors

$$m < \mu \frac{1/k}{\mu^{1/k} - c_k} .$$

Démonstration. - Soit $\gamma : \mathbb{N}^* \rightarrow \mathbb{N}$, la fonction définie par

$$\gamma(j) = \sup_{\sum_{i=1}^k \ell(p_i^{a_i}) \leq j} \left(\prod_{i=1}^k p_i^{a_i} \right) .$$

On a, pour tout j ,

$$\gamma(j) \leq \left(\frac{j}{k} \right)^k ,$$

$\gamma(j)$ étant un produit de k nombres de somme au plus j . D'autre part, si l'on fait

$$a_i = \left[\frac{\log \frac{j}{k}}{\log p_i} \right] ,$$

on voit que

$$\gamma(j) \geq \left(\frac{j}{k} \right)^k \frac{1}{e^{\theta(p_k)}} ,$$

où θ est la fonction de Čebyšev. D'autre part, on a

$$\ell(\gamma(j)) \leq j , \quad \gamma(m) = \prod_{i=1}^k p_i^{\alpha_i} \quad \text{et} \quad \ell(\gamma(m)) = m .$$

Considérons maintenant $M = \frac{\gamma(m+p)}{p\gamma(m)} g(n)$.

$$\ell(M) - \ell(g(n)) \leq m + p - p - m = 0 ,$$

donc $M < g(n)$,

$$\frac{(m+p)^k}{k^k} \frac{1}{e^{\theta(p_k)}} \leq \gamma(m+p) < p\gamma(m) \leq p \left(\frac{m}{k} \right)^k .$$

On en déduit

$$m > \frac{p}{p^{1/k} c_k - 1} > \frac{1}{c_k} p^{1-(1/k)} \quad \text{avec} \quad c_k = e^{\theta(p_k)/k} .$$

De même, on pose $M = \mu \frac{\gamma(m-\mu)}{\gamma(m)} g(n)$. Si $m < \mu$, le résultat est acquis, sinon on a $\ell(M) - \ell(g(n)) \leq 0$, donc $M < g(n)$,

$$\mu\gamma(m-\mu) < \gamma(m) ,$$

$$\mu(m-\mu)^k < m^k e^{\theta(p_k)} .$$

Comme $\mu^{1/k} > c_k$,

$$m < \mu \frac{\mu^{1/k}}{\mu^{1/k} - c_k}.$$

PROPRIÉTÉ 8. - Soit λ un nombre premier fixé ; soit $\alpha_\lambda = v_\lambda(g(n))$. Quand $n \rightarrow \infty$, on a

$$\alpha_\lambda \log \lambda = \log p + O(\log \log p),$$

p étant le plus grand nombre premier divisant $g(n)$.

Démonstration. - Etudions d'abord le cas $\lambda = 2$. Pour une autre valeur de λ , le résultat découlera de la propriété 4.

Utilisant les notations de la propriété 7, pour k donné,

$$\frac{m}{2^{\alpha_2}} = \sum_{i=1}^k \frac{\ell(p_i)^{\alpha_{p_i}}}{2^{\alpha_2}} \leq \sum_{i=1}^k \frac{p_i^{\alpha_{p_i}}}{2^{\alpha_2}} \leq 2 \sum_{i=1}^k p_i = 2P_k,$$

à l'aide de la propriété 4. P_k est défini comme étant la somme des k premiers nombres premiers. On a donc

$$2^{\alpha_2} \geq \frac{1}{2P_k c_k} p^{1-(1/k)}.$$

La propriété 4 nous donne ($\mu = p$, $\beta = 1$, $\lambda = 2$) : $2^{\alpha_2} \leq 2p$, donc

$$(1 - \frac{1}{k}) \log p + \log 2P_k c_k \leq \alpha_2 \log 2 \leq \log p + \log 2.$$

On en déduit $\alpha_2 \log 2 \sim \log p$.

On peut même préciser : si l'on fait $k = [\log p]$, on a

$$P_k \sim \frac{k^2}{2} \log k \quad ([2], \text{ page } 4),$$

$$\log P_k \sim 2 \log k \sim 2 \log \log p,$$

$$\log c_k = \frac{\theta(p_k)}{k} \sim \log k \sim \log \log p.$$

Donc,

$$\alpha_2 \log 2 = \log p + O(\log \log p).$$

PROPRIÉTÉ 9. - Avec les mêmes notations qu'à la proposition 8, on a

$$\frac{2^{\alpha_2}}{p} = o\left(\frac{1}{\log \log \log p}\right) .$$

Soit toujours k fixé et, pour $1 \leq i \leq k$, $\alpha_i = v_{p_i}(g(n))$. D'après la propriété précédente, pour n assez grand, on a $\alpha_i \neq 0$ et

$$\frac{m}{2^{\alpha_2}} = \sum_{i=1}^k \frac{p_i^{\alpha_i}}{2^{\alpha_2}} \geq \frac{1}{2} \sum_{i=1}^k \frac{1}{p_i} = \omega_k \quad (\text{définition de } \omega_k) .$$

Pour un n assez grand, on peut appliquer la propriété 7, avec $\mu = q$, q étant le nombre premier suivant p .

$$\frac{q}{2^{\alpha_2}} \geq \frac{q^{1/k} - c_k}{q^{1/k}} \omega_k .$$

En faisant tendre q vers l'infini, on voit que $\frac{q}{2^{\alpha_2}} \geq \omega_k$. Or ω_k est équivalent à $\frac{1}{2} \log \log k$, quand k tend vers l'infini, donc $\frac{q}{2^{\alpha_2}}$ tend vers l'infini avec n .

On peut même préciser : faisant $k = [\sqrt{\log q}]$, on a

$$\log c_k \sim \log k \sim \frac{1}{2} \log \log q ,$$

$$\log q^{1/k} = \frac{1}{k} \log q \sim \sqrt{\log q} ,$$

on a bien $q^{1/k} > c_k$, et on obtient

$$\frac{2^{\alpha_2}}{q} = o\left(\frac{1}{\log \log \log q}\right) ,$$

d'où la propriété puisque $q \sim p$.

PROPRIÉTÉ 10. - Soit p le plus grand nombre premier divisant $g(n)$, soit μ le plus petit nombre premier ne divisant pas $g(n)$. On pose $a_n = \frac{p}{\mu}$. Alors,

$$\lim_{n \rightarrow \infty} a_n = 1 .$$

La démonstration se fait en deux temps.

1er temps : On a $\overline{\lim} a_n < +\infty$, et plus précisément $\overline{\lim} a_n \leq 6$. Reprenant les notations de la propriété 7, on fait $k = 2$, et on étudie :

$$M = \frac{\mu}{p} \frac{\gamma(m+p-\mu)}{\gamma(m)} g(n) .$$

On a $\ell(M) \leq \ell(g(n))$, donc $M < g(n)$.

Soit $\gamma(m+p-\mu) < a_n \gamma(m)$,

$$[m + (a-1)\mu]^2 < 6a_n m^2 ,$$

car $e^{\theta(p_2)} = 6$. Donc,

$$m > \mu \frac{a_n - 1}{\sqrt{6a_n} - 1} .$$

Mais, d'après la propriété 7,

$$\mu \frac{\sqrt{\mu}}{\sqrt{\mu} - \sqrt{6}} > m .$$

S'il existait une sous-suite a_{n_j} de a_n dont la limite soit > 6 , en faisant tendre j vers l'infini, on ne pourrait réaliser simultanément ces deux inégalités.

2e temps : Supposons que $\overline{\lim} a_n > 1$; il existerait alors $\varepsilon > 0$ tel que, pour une infinité de n , on ait $1 + \varepsilon < a_n < 7$. Posons $M = \frac{8\mu}{p} g(n)$. Pour les n vérifiant $1 + \varepsilon < a_n < 7$, $M > g(n)$ et

$$\ell(M) - \ell(g(n)) = 7.2^{\alpha_2} + \mu - p < 7.2^{\alpha_2} - \frac{\varepsilon p}{1 + \varepsilon} \sim -\varepsilon p .$$

Pour p assez grand, $\ell(M) - \ell(g(n)) < 0$, il y aurait contradiction.

Si $a_n < 1$, alors μ est le nombre premier suivant p , et on a $\lim a_n = 1$. La propriété est démontrée.

3. Construction de G (cf. [3], § 32).

Soit G l'ensemble des nombres N qui vérifient la propriété :

Il existe $\rho \in \mathbb{R}^+$ tel que, pour tout $A \in \mathbb{N}^*$, $A \neq N$,

$$\ell(A) - \ell(N) > \rho \log \frac{A}{N} .$$

1° $G \subset g(\mathbb{N})$ (propriété caractéristique).

2° Supposons $N \neq 4$, et soit p le plus grand nombre premier divisant N . On sait (propriété 2) que $v_p(N) = 1$.

Si $A = \frac{N}{p}$, on obtient $\rho > \frac{p}{\log p}$.

Si q est le plus petit nombre premier ne divisant pas N , on pose $A = Nq$, et on obtient $\rho < \frac{q}{\log q}$.

Or la fonction $x \mapsto \frac{x}{\log x}$ est croissante pour $x > e$. On a donc $q > p$, la seule exception possible étant $p = 3$, $q = 2$. On constatera que $3 \in G$ avec la valeur $\rho = 2,8$.

3° Soient $\lambda < p$ un nombre premier, et $\alpha = v_\lambda(N)$.

Etudions $A = N\lambda$ et $A = \frac{N}{\lambda}$, on trouve :

$$\alpha = 1, \quad \frac{\lambda}{\log \lambda} < \rho < \frac{\lambda^2 - \lambda}{\log \lambda},$$

$$\alpha \geq 2, \quad \frac{\lambda^\alpha - \lambda^{\alpha-1}}{\log \lambda} < \rho < \frac{\lambda^{\alpha+1} - \lambda^\alpha}{\log \lambda}.$$

Pour tout λ premier, considérons l'ensemble $E_\lambda \subset \mathbb{R}$:

$$E_\lambda = \left\{ \frac{\lambda}{\log \lambda}, \frac{\lambda^2 - \lambda}{\log \lambda}, \dots, \frac{\lambda^{\alpha+1} - \lambda^\alpha}{\log \lambda}, \dots \right\}.$$

Pour tout $\lambda \neq 2$, la suite constituant E_λ est **strictement** croissante.

Pour $\lambda = 2$, les deux premiers termes sont confondus.

Si on se donne $\mu \notin E_\lambda$, la valeur de $\alpha = v_\lambda(N)$ est donc déterminée par

$$\frac{\lambda^\alpha - \lambda^{\alpha-1}}{\log \lambda} < \rho < \frac{\lambda^{\alpha+1} - \lambda^\alpha}{\log \lambda}.$$

Soit $E = \bigcup_{\lambda \text{ premier}} E_\lambda$. E est un ensemble discret de $\mathbb{R}$ (la quantité de tels nombres inférieurs à x est majorable et donc finie). D'autre part, deux éléments de E sont distincts : si l'on avait

$$\frac{a}{\log \mu} = \frac{b}{\log \lambda},$$

$\frac{\log \mu}{\log \lambda}$ serait rationnel, ce qui est faux.

4° Table des valeurs.

ρ	ρ	N	N	$\ell(N)$
$3/\log 3$	2,73	3	3	3
$2/\log 2 = (4 - 2)/\log 2$	2,88	4.3	12	7
$5/\log 5$	3,11	4.3.5	60	12
$7/\log 7$	3,6	4.3.5.7	420	19
$11/\log 11$	4,58	4.3.5.7.11	4 620	30
$13/\log 13$	5,06	4.3.5.7.11.13	60 060	43
$(9 - 3)/\log 3$	5,46	4.9.5.7.11.13	180 180	49
$(8 - 4)/\log 2$	5,76	8.9.5.7.11.13	360 360	53
$17/\log 17$	6	8.9.5.7.11.13.17	6 126 120	70
$19/\log 17$	6,45	8.9.5.7.11.13.17.19	116 396 280	89
$23/\log 23$	7,33			

Pour chaque valeur de $\rho \in \underline{\mathbb{R}} - E$, tel que $\rho > \frac{3}{\log 3}$, il existe un nombre N_ρ , et un seul, déterminé par sa décomposition en facteurs premiers.

Remarques :

- Si $\rho \leq \rho'$, alors N_ρ divise $N_{\rho'}$.
- Si I et I' sont deux intervalles contigus de $\underline{\mathbb{R}} - E$, séparés par un élément de E_λ , et si $\rho \in I$, $\rho' \in I'$, alors $N_{\rho'} = \lambda N_\rho$.
- $v_p(N_\rho)$ est une fonction décroissante de p , car la fonction $y = \frac{x^{\alpha+1} - x^\alpha}{\log x}$ est croissante pour $x \geq 2$, quelle que soit la valeur du paramètre $\alpha \geq 1$.

5° Réciproque : Montrons que tout N_ρ ainsi construit appartient bien à G .
Soit A un nombre quelconque, et, pour tout nombre premier λ , posons

$$\beta_\lambda = v_\lambda(A) \quad \text{et} \quad \alpha_\lambda = v_\lambda(N) .$$

$$\ell(A) - \ell(N) = \sum_{\lambda} \ell(\lambda^{\beta_\lambda}) - \ell(\lambda^{\alpha_\lambda}) ;$$

il suffit de montrer que, pour tout λ tel que $\beta_\lambda \neq \alpha_\lambda$,

$$\ell(\lambda^\beta) - \ell(\lambda^\alpha) > \rho \log \lambda^{\beta-\alpha}.$$

Il y a cinq cas à considérer :

$$\begin{aligned} \alpha \neq 0, \quad \beta > \alpha : \quad \lambda^\beta - \lambda^\alpha &= (\lambda^{\alpha+1} - \lambda^\alpha)(1 + \lambda + \dots + \lambda^{\beta-\alpha-1}) \\ &\geq (\lambda^{\alpha+1} - \lambda^\alpha)(\beta - \alpha) > \rho \log \lambda^{\beta-\alpha}; \end{aligned}$$

$$\alpha = 0, \quad \beta > \alpha : \quad \ell(\lambda^\beta) - \ell(\lambda^\alpha) = \lambda^\beta \geq \beta \lambda > \beta \rho \log \lambda = \rho \log \lambda^\beta;$$

$$\beta \neq 0, \quad \beta < \alpha, \text{ on a alors } \beta \geq 1 \text{ et } \alpha \geq 2, \text{ donc,}$$

$$\begin{aligned} \ell(\lambda^\beta) - \ell(\lambda^\alpha) &= \lambda^\beta - \lambda^\alpha = (\lambda^{\alpha-1} - \lambda^\alpha)(1 + \frac{1}{\lambda} + \dots + \frac{1}{\lambda^{\alpha-\beta+1}}) \\ &\geq (\lambda^{\alpha-1} - \lambda^\alpha)(\alpha - \beta) > -\rho \log \lambda^{\alpha-\beta} = \rho \log \frac{1}{\lambda^{\alpha-\beta}}; \end{aligned}$$

$$\beta = 0, \quad \alpha = 1 : \quad \ell(\lambda^\beta) - \ell(\lambda^\alpha) = -\lambda > -\rho \log \lambda;$$

$$\begin{aligned} \beta = 0, \quad \alpha \geq 2 : \quad \ell(\lambda^\beta) - \ell(\lambda^\alpha) &= -\lambda^\alpha > -\rho \frac{\lambda}{\lambda-1} \log \lambda > -2\rho \log \lambda \\ \text{et } -2\rho \log \lambda &= \rho \log \frac{1}{\lambda^2} \geq \rho \log \frac{1}{\lambda^\alpha}. \end{aligned}$$

On a ainsi défini une partie G de $g(\mathbb{N})$, et on connaît exactement la décomposition en facteurs premiers des nombres de G .

4. Etude de $\log g(n)$ lorsque $n \rightarrow \infty$.

1° LEMME. - Si $N \in G$, et si p est le plus grand nombre premier divisant N , on a

$$e^{\theta(p)} \leq N \leq e^{\psi(p)},$$

sauf pour $N = 3$ et 12 .

Démonstration. - L'inégalité $e^{\theta(p)} \leq N$ pour $N \neq 3$ résulte du § 3, 2°.

Pour montrer $N \leq e^{\psi(p)}$ où $\psi(x) = \sum_{p^m \leq x} \log p$, il faut montrer que, pour $\alpha \geq 2$,

$$\frac{\lambda^\alpha - \lambda^{\alpha-1}}{\log \lambda} < \rho \quad \text{entraîne} \quad \lambda < p^{1/\alpha}.$$

Soit q le nombre premier suivant p , on sait que $\rho < \frac{q}{\log q}$. On utilise le résultat suivant ([1], § 23) qui améliore le postulat de Bertrand : pour $p \geq 29$, $q \leq \frac{6}{5}p$. On démontre ainsi que, pour $\lambda = p^{1/\alpha}$,

$$\frac{\lambda^\alpha - \lambda^{\alpha-1}}{\log \lambda} > \frac{q}{\log q} .$$

La fonction $\lambda \mapsto \frac{\lambda^\alpha - \lambda^{\alpha-1}}{\log \lambda}$ étant croissante pour tout $\alpha \geq 2$, cela démontre la propriété pour $p \geq 29$; pour $p \leq 23$, on regarde les valeurs numériques.

2° Etude de $\log g(n)$ quand $g(n) \in G$. On a

$$e^{\theta(p)} \leq g(n) \leq e^{\psi(p)} ,$$

$$P \leq n \leq P + p\sqrt{p} \quad \text{avec} \quad P = \ell(e^{\theta(p)}) = \sum_{\substack{\lambda \leq p \\ \lambda \text{ premier}}} \lambda .$$

Le calcul est le même que dans [2], l'inégalité sur n est un peu plus large, mais cela ne gêne en rien les calculs, l'inégalité sur $g(n)$ est meilleure. On obtient ainsi

$$\log g(n) = \sqrt{n \log n} \left[1 + \frac{\log \log n}{2 \log n} - \frac{1 + o(1)}{2 \log n} \right] ,$$

et on peut prolonger le développement à un ordre $\frac{\sqrt{n}}{(\log n)^k}$ pour tout k . Comme on obtient le même résultat pour deux éléments consécutifs de G , le résultat s'étend à $g(\mathbb{N})$. On est en fait limité par la connaissance de θ et ψ . L'hypothèse de Riemann permettrait d'obtenir de meilleurs résultats.

5. THÉOREME. - Il existe des intervalles aussi grands que l'on veut sur lesquels $g(n)$ est constante.

D'après le § 1, 4°, cela revient à démontrer

$$\overline{\lim}_{A \in g(\mathbb{N})} \ell(A^*) - \ell(A) = +\infty .$$

En fait, on va démontrer

$$\overline{\lim} \frac{\ell(A^*) - \ell(A)}{\log p} \geq 1 ,$$

où p est le plus grand nombre premier divisant A et, comme dans la démonstration $A \in G$, d'après le § 4, 1°, $p \sim \log A$, donc on démontre en même temps

$$\overline{\lim} \frac{\ell(A^*) - \ell(A)}{\log \log A} \geq 1 \quad \text{et} \quad \overline{\lim} \frac{\ell(g(n)) - \ell(g(n-1))}{\log n} \geq \frac{1}{2} ,$$

en tenant compte du § 4, 2°.

La démonstration du théorème résulte de deux lemmes :

LEMME 1. - Soit $N = N_\rho \in G$; soient $r, s \in \mathbb{N}^*$ deux nombres premiers entre eux,
tels que s divise N , on a

$$\ell\left(\frac{r}{s}N\right) - \ell(N) \geq \rho^- \log \frac{r}{s} + (\rho^+ - \rho^-) \log r ,$$

où ρ^- , ρ^+ est la composante connexe de ρ dans $\mathbb{R} - E$.

Démonstration. - Il suffit d'examiner de plus près la réciproque (§ 3, 5°). Lorsqu'on minore $\lambda^{\alpha+1} - \lambda^\alpha$ par $\rho \log \lambda$, on peut aussi bien minorer par $\rho^+ \log \lambda$, et de même $\lambda^{\alpha-1} - \lambda^\alpha \geq -\rho^- \log \lambda$. On a ainsi

$$\ell\left(\frac{N}{s}\right) - \ell(N) \geq \rho^- \log \frac{1}{s} ,$$

$$\ell\left(\frac{rN}{s}\right) - \ell\left(\frac{N}{s}\right) \geq \rho^+ \log r .$$

En ajoutant, on obtient :

$$\ell\left(\frac{r}{s}N\right) - \ell(N) \geq \rho^- \log \frac{1}{s} + \rho^+ \log r = \rho^- \log \frac{r}{s} + (\rho^+ - \rho^-) \log r .$$

LEMME 2. - Il existe une infinité d'intervalles (ρ^-, ρ^+) de longueur supérieure à 1 .

Démonstration. - Soit

$$\varphi(x) = \text{Card}\{\rho \in E \mid \frac{x}{\log x} < \rho \leq \frac{2x}{\log x}\} .$$

Soient

$$E_1 = \left\{ \frac{\lambda}{\log \lambda} , \lambda \text{ premier } \geq 3 \right\} \quad \text{et} \quad E_2 = \left\{ \frac{\lambda^\alpha - \lambda^{\alpha-1}}{\log \lambda} , \lambda \text{ premier, } \alpha \geq 2 \right\} .$$

On a $\varphi(x) = \varphi_1(x) + \varphi_2(x)$ avec

$$\varphi_1(x) = \text{Card}\{\rho \in E_1 \mid \frac{x}{\log x} < \rho \leq \frac{2x}{\log x}\}$$

et

$$\varphi_2(x) = \text{Card}\{\rho \in E_2 \mid \frac{x}{\log x} < \rho \leq \frac{2x}{\log x}\} .$$

Si $\pi(x)$ est le nombre des nombres premiers inférieurs ou égaux à x ,

$$\varphi_1(x) = \pi(2x) - \pi(x) = \frac{x}{\log x} \left(1 - \frac{3 + 2 \log 2 + o(1)}{\log x} \right) .$$

D'autre part, $\omega_2(x) \leq \text{Card}\{\rho \in E_2 \mid \rho \leq \frac{2x}{\log x}\}$.

$$\text{Si } \frac{\lambda^2 - \lambda}{\log \lambda} \leq \frac{2x}{\log x}, \quad \text{alors } \lambda \leq \sqrt{2x};$$

$$\text{Si } \frac{\lambda^\alpha - \lambda^{\alpha-1}}{\log \lambda} \leq \frac{2x}{\log x}, \quad \text{alors } \lambda \leq x^{1/\alpha} \text{ pour } \alpha \geq 3.$$

Et le plus grand α possible est l'exposant de 2 :

$$\frac{2^\alpha - 2^{\alpha-1}}{\log 2} \leq \frac{2x}{\log x} \quad \text{qui donne} \quad \alpha \leq \frac{\log x}{\log 2}.$$

Finalement, $\omega_2(x) \leq \sqrt{2x} + \sqrt[3]{x} \frac{\log x}{\log 2}$ et $\omega_2(x) = O(\sqrt{x})$,

$$\varphi(x) = \frac{x}{\log x} \left(1 - \frac{3 + 2 \log 2 + o(1)}{\log x}\right).$$

Si pour tout $\rho > \frac{x}{\log x}$, on avait $\rho^+ - \rho^- \leq 1$, entre $\frac{x}{\log x}$ et $\frac{2x}{\log x}$ il y aurait seulement $\omega(x)$ intervalles de longueur au plus 1, ce serait insuffisant puisque $\frac{x}{\log x} - \varphi(x)$ est positif pour x assez grand.

Démonstration du théorème. - Appliquons le lemme 1 à la famille infinie de nombres N_ρ tels que $\rho^+ - \rho^- \geq 1$.

$$\ell\left(\frac{r}{s} N\right) - \ell(N) \geq \rho^- \log \frac{r}{s} + \log r.$$

$r \rho^- \geq \frac{p}{\log p}$. Si on suppose $\frac{r}{s} > 1$, alors $\frac{r}{s} \geq \frac{r}{r-1}$ et

$$\ell\left(\frac{r}{s} N\right) - \ell(N) \geq \frac{p}{\log p} \log \frac{r}{r-1} + \log r.$$

Or la fonction $y = a \log \frac{x}{x-1} + \log x$ admet un minimum pour $x = a + 1$, et ce minimum est minoré par $\log a$, donc

$$\ell\left(\frac{r}{s} N\right) - \ell(N) \geq \log p - \log \log p.$$

Cette relation vaut en particulier pour $N^* = \frac{r}{s} N$, et le théorème est établi.

BIBLIOGRAPHIE

- [1] LANDAU (Edmund). - Handbuch der Lehre von der Verteilung der Primzahlen, Bände 1 und 2. - Leipzig und Berlin, B. G. Teubner, 1909 [2te Auflage, New York, Chelsea publishing Company, 1953].

- [2] NICOLAS (Jean-Louis). - Sur l'ordre maximum d'un élément dans le groupe S_n des permutations, I., Séminaire Delange-Pisot-Poitou : Théorie des nombres, 7e année, 1965/66, n° 13, 8 p.
- [3] RAMANUJAN (Srinivasa). - Highly composite numbers, Proc. London math. Soc., Series 2, t. 14, 1915, p. 347-400 ; Collected papers, p. 78-128. - Cambridge, at the University Press, 1927.

Table numérique

n	g(n)	facteurs premiers de g(n)	n	g(n)	facteurs premiers de g(n)
1	1				
2	2	2	*53	360 360	8 9 5 7 11 13
*3	3	3	57	471 240	8 9 5 7 11 17
4	4	4	58	510 510	2 3 5 7 11 13 17
5	6	2 3	59	556 920	8 9 5 7 13 17
*7	12	4 3	60	1 021 020	4 3 5 7 11 13 17
8	15	3 5	62	1 141 140	4 3 5 7 11 13 19
9	20	4 5	64	2 042 040	8 3 5 7 11 13 17
10	30	2 3 5	66	3 063 060	4 9 5 7 11 13 17
*12	60	4 3 5	68	3 423 420	4 9 5 7 11 13 19
14	84	4 3 7	*70	6 126 120	8 9 5 7 11 13 17
15	105	3 5 7	72	6 846 840	8 9 5 7 11 13 19
16	140	4 5 7	76	8 953 560	8 9 5 7 11 17 19
17	210	2 3 5 7	77	9 699 690	2 3 5 7 11 13 17 19
*19	420	4 3 5 7	78	12 252 240	16 9 5 7 11 13 17
23	840	8 3 5 7	79	19 399 380	4 3 5 7 11 13 17 19
25	1 260	4 9 5 7	83	38 798 760	8 3 5 7 11 13 17 19
27	1 540	4 5 7 11	85	58 198 140	4 9 5 7 11 13 17 19
28	2 310	2 3 5 7 11	*89	116 396 280	8 9 5 7 11 13 17 19
29	2 520	8 9 5 7	93	140 900 760	8 9 5 7 11 13 17 23
*30	4 620	4 3 5 7 11	95	157 477 320	8 9 5 7 11 13 19 23
32	5 460	4 3 5 7 13	97	232 792 560	16 9 5 7 11 13 17 19
34	9 240	8 3 5 7 11	101	281 801 520	16 9 5 7 11 13 17 23
36	13 860	4 9 5 7 11	102	446 185 740	4 3 5 7 11 13 17 19 23
38	16 380	4 9 5 7 13	106	892 371 480	8 3 5 7 11 13 17 19 23
40	27 720	8 9 5 7 11	108	1 338 557 220	4 9 5 7 11 13 17 19 23
41	30 030	2 3 5 7 11 13	*112	2 677 114 440	8 9 5 7 11 13 17 19 23
42	32 760	8 9 5 7 13	118	3 375 492 120	8 9 5 7 11 13 17 19 29
*43	60 060	4 3 5 7 11 13			
47	120 120	8 3 5 7 11 13			
*49	180 180	4 9 5 7 11 13			

Si n n'est pas dans la table, si $n_0 \leq n' < n_1$, avec n_0 et n_1 consécutifs dans la table, $g(n) = g(n_0)$.

Un astérisque signale les nombres de G .