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)
8e année, 1966/67, n° 11

6 février 1967

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 ;

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

$g(n) = \sup_{\sum p^r \leqslant n} \prod p^r$ (p premier, $r \in \underset{\sim}{N}^*$).

Définition. - Soit $\ell : \underset{\sim}{N}^* \to \underset{\sim}{N}$.

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

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

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, $\alpha \in \underset{\sim}{N}^*$) est l'application identique. On a $\ell(k) \leqslant k$ 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 :

$$g(n) = \sup_{\ell(k) \leqslant n} k . \tag{1}$$

Ce qui équivaut à

$$\begin{cases} \ell(g(n)) \leqslant n & (2) \\ M > g(n) \implies \ell(M) > n . & (3) \end{cases}$$

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

$$M > g(n-1) \implies \ell(M) \geqslant n . \tag{3'}$$

Propriété caractéristique. - Les deux propriétés suivantes sont équivalentes :

$$(a) \quad m \in g(\underset{\sim}{N}) \ ,$$

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

Démonstration.

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

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

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

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

(3') et (2) donnent :

$$\ell(m) \geqslant n \geqslant \ell(g(n)) \ .$$

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

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

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

Remarque. - Soit $f : \underset{\sim}{N}^* \to \underset{\sim}{R}$ 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 $n \in \underset{\sim}{N}^*$, où ℓ est petite, est exactement $g(\underset{\sim}{N})$.

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 $\underset{\sim}{N}$ la relation d'équivalence

$$n \backsim n' \iff g(n) = g(n') \ .$$

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

$$g(\hat{n}) = g(n) \ ; \qquad \hat{n} \leqslant n \ ; \qquad g(\hat{n} - 1) < g(\hat{n}) \ .$$

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

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

On a en fait démontré les équivalences :

$$n = \hat{n} \iff \ell(g(n)) = n \iff g(n) > g(n-1) \iff n \in \ell \circ g(\underset{\sim}{N}) \quad .$$

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

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

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

Si $N \notin g(\underset{\sim}{N})$, il ne peut y avoir égalité, car $g(\ell(N)) \in g(\underset{\sim}{N})$.
Si $N = g(n)$, $g(\ell(g(n))) = g(\hat{n}) = g(n)$.

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

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

On a $g(n) \leqslant g[\ell(A^*) - 1] < g(\ell(A^*)) = A^*$, car $\ell(A^*) \in \ell(g(\underset{\sim}{N}))$. D'autre part, $g(n) \geqslant g(\ell(A)) = A$, donc $g(n) = A$.

5° On a

(5) $$\underline{A < N \leqslant A^* \implies \ell(N) \geqslant \ell(A^*)} \quad ,$$

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

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

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

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

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

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

Démonstration. - On peut supposer $\beta \geqslant 2$ (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 $\alpha \neq 0$,

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

ce qui entraîne

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Si $\alpha \geqslant 3$, $M = 2^{\alpha-1} 3 > g(n)$ 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 $q \geqslant p + p'$ ne divise pas $g(n)$.

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

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

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

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

D'autre part,

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

et

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

donc $M \geqslant g(n)$, 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 $\ell(M) - \ell(g(n)) \leqslant 4 + 6 - 11 < 0$. D'après le lemme, tout nombre premier supérieur ou égal à 13 ne divise pas $g(n)$. Donc $g(n)$ divise $3.5.7 = 105$. 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 $n \in \underset{\sim}{\mathbb{N}}^*$, $\frac{g(n+1)}{g(n)} \leqslant 2$ ou, ce qui est équivalent, pour tout $A \in g(\underset{\sim}{\mathbb{N}})$, $\frac{A^*}{A} \leqslant 2$.

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), $\ell(\frac{A^*}{2}) \geqslant \ell(A^*)$, 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 :

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

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

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

donc

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

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 $\alpha \geqslant 1$ et $\beta \geqslant 2$.

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

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

Si $\alpha = 0$:

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

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

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 $\alpha = v_\lambda(g(n)) \geqslant 2$, alors,

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

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 $g(\underset{\sim}{N})$, p le plus grand nombre premier divisant A, q son suivant. On a

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

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

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

et

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

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 $\lambda \leqslant p$, on a $\lambda^{\alpha} < \frac{q\lambda}{\lambda - 1}$, donc

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

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

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

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

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

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

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 $\mu > e^{\theta(p_k)}$, alors

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

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

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

On a, pour tout j ,

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

$\gamma(j)$ 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

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

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

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

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

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

donc $M < g(n)$,

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

On en déduit

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

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

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

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

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

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

$$(1 - \tfrac{1}{k}) \log p + \log 2P_k\, c_k \leqslant \alpha_2 \log 2 \leqslant \log p + \log 2 .$$

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

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

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

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

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

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

$$\frac{m}{2^{\alpha_2}} = \sum_{i=1}^{k} \frac{p_i^{\alpha_{p_i}}}{2^{\alpha_2}} \geqslant \frac{1}{2} \sum_{i=1}^{k} \frac{1}{p_i} = \omega_k \qquad \text{(définition de } \omega_k \text{)} .$$

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

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

En faisant tendre q vers l'infini, on voit que $\frac{q}{2^{\alpha_2}} \geqslant \omega_k$. 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,

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

La démonstration se fait en deux temps.

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

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

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

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

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

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

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

Mais, d'après la propriété 7,

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

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

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

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 $\rho \in \underset{\sim}{R}^+$ tel que, pour tout $A \in \underset{\sim}{N}^*$, $A \neq N$,

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

1° $G \subset g(\underset{\sim}{N})$ (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 $x \longmapsto \frac{x}{\log x}$ 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 :

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

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

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

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

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 $\underset{\sim}{R}$ (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 $\rho \in \underset{\sim}{R} - E$, 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 $\rho \leqslant \rho'$, alors N_ρ divise $N_{\rho'}$.
- Si I et I' sont deux intervalles contigus de $\underset{\sim}{R} - E$, 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 $x \geqslant 2$, quelle que soit la valeur du paramètre $\alpha \geqslant 1$.

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

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

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

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

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

Il y a cinq cas à considérer :

$\alpha \neq 0$, $\beta > \alpha$: $\lambda^\beta - \lambda^\alpha = (\lambda^{\alpha+1} - \lambda^\alpha)(1 + \lambda + \ldots + \lambda^{\beta-\alpha-1})$
$\geqslant (\lambda^{\alpha+1} - \lambda^\alpha)(\beta - \alpha) > \rho \log \lambda^{\beta-\alpha}$;

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

$\beta \neq 0$, $\beta < \alpha$, on a alors $\beta \geqslant 1$ et $\alpha \geqslant 2$, donc,

$$\ell(\lambda^\beta) - \ell(\lambda^\alpha) = \lambda^\beta - \lambda^\alpha = (\lambda^{\alpha-1} - \lambda^\alpha)(1 + \frac{1}{\lambda} + \ldots + \frac{1}{\lambda^{\alpha-\beta+1}})$$

$$\geqslant (\lambda^{\alpha-1} - \lambda^\alpha)(\alpha - \beta) > -\rho \log \lambda^{\alpha-\beta} = \rho \log \frac{1}{\lambda^{\alpha-\beta}} \quad ;$$

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

$\beta = 0$, $\alpha \geqslant 2$: $\ell(\lambda^\beta) - \ell(\lambda^\alpha) = -\lambda^\alpha > -\rho \frac{\lambda}{\lambda - 1} \log \lambda > -2\rho \log \lambda$

et $-2\rho \log \lambda = \rho \log \frac{1}{\lambda^2} \geqslant \rho \log \frac{1}{\lambda^\alpha}$.

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

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

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

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

sauf pour $N = 3$ et 12 .

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

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

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

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 $p \geqslant 29$, $q \leqslant \frac{6}{5} p$. On démontre ainsi que, pour $\lambda = p^{1/\alpha}$,

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

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

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

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

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

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

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

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 $g(\underset{\sim}{\mathbb{N}})$. On est en fait limité par la connaissance de θ et ψ. L'hypothèse de Riemann permettrait d'obtenir de meilleurs résultats.

5. THÉORÈME. - 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

$$\overline{\lim_{A \in g(\underset{\sim}{\mathbb{N}})}} \ \ell(A^*) - \ell(A) = +\infty \quad .$$

En fait, on va démontrer

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

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

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

en tenant compte du § 4, 2°.

La démonstration du théorème résulte de deux lemmes :

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

$$\ell(\tfrac{r}{s} N) - \ell(N) \geqslant \rho^- \log \tfrac{r}{s} + (\rho^+ - \rho^-) \log r \quad ,$$

où $]\rho^- , \rho^+[$ est la composante connexe de ρ dans $\underset{\sim}{R} - E$.

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 $\lambda^{\alpha-1} - \lambda^\alpha \geqslant - \rho^- \log \lambda$. On a ainsi

$$\ell(\tfrac{N}{s}) - \ell(N) \geqslant \rho^- \log \tfrac{1}{s} \quad ,$$

$$\ell(\tfrac{rN}{s}) - \ell(\tfrac{N}{s}) \geqslant \rho^+ \log r \quad .$$

En ajoutant, on obtient :

$$\ell(\tfrac{r}{s} N) - \ell(N) \geqslant \rho^- \log \tfrac{1}{s} + \rho^+ \log r = \rho^- \log \tfrac{r}{s} + (\rho^+ - \rho^-) \log r \quad .$$

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

Démonstration. - Soit

$$\varphi(x) = \mathrm{Card}\{\rho \in E \mid \tfrac{x}{\log x} < \rho \leqslant \tfrac{2x}{\log x}\} \quad .$$

Soient

$$E_1 = \{\tfrac{\lambda}{\log \lambda} , \ \lambda \text{ premier } \geqslant 3\} \qquad \text{et} \qquad E_2 = \{\tfrac{\lambda^\alpha - \lambda^{\alpha-1}}{\log \lambda} , \ \lambda \text{ premier}, \ \alpha \geqslant 2\} \ .$$

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

$$\varphi_1(x) = \mathrm{Card}\{\rho \in E_1 \mid \tfrac{x}{\log x} < \rho \leqslant \tfrac{2x}{\log x}\}$$

et

$$\varphi_2(x) = \mathrm{Card}\{\rho \in E_2 \mid \tfrac{x}{\log x} < \rho \leqslant \tfrac{2x}{\log x}\} \quad .$$

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

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

D'autre part, $\varphi_2(x) \leqslant \mathrm{Card}\{\rho \in E_2 \mid \rho \leqslant \frac{2x}{\log x}\}$.

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

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

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

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

Finalement, $\varphi_2(x) \leqslant \sqrt{2x} + \sqrt[3]{x}\,\frac{\log x}{\log 2}$ et $\varphi_2(x) = O(\sqrt{x})$,

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

Si pour tout $\rho > \frac{x}{\log x}$, on avait $\rho^+ - \rho^- \leqslant 1$, entre $\frac{x}{\log x}$ et $\frac{2x}{\log x}$ il y aurait seulement $\varphi(x)$ 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 $\rho^+ - \rho^- \geqslant 1$.

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

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

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

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

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

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 $n_0 \leqslant n' < n_1$, avec n_0 et n_1 consécutifs dans la table, $g(n) = g(n_0)$.

Un astérisque signale les nombres de G.