

SÉMINAIRE DELANGE-PISOT-POITOU. THÉORIE DES NOMBRES

JEAN-LOUIS NICOLAS

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

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 7, n° 2 (1965-1966),
exp. n° 13, p. 1-8

http://www.numdam.org/item?id=SDPP_1965-1966__7_2_A2_0

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1965-1966, 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, I.

par Jean-Louis NICOLAS

Cet exposé a pour but de préciser les résultats décrits par LANDAU ([2], § 61).

On rappelle qu'un élément σ du groupe S_n des permutations de n objets se décompose en cycle de façon unique. Par exemple, pour $n = 9$,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} = (1 \ 9 \ 5)(2 \ 8 \ 4 \ 6)(3 \ 7) .$$

L'ordre d'un élément (le plus petit entier $m \geq 1$ tel que σ^m soit la permutation identique) est donc le p. p. c. m. de la longueur de ses cycles. Dans l'exemple ci-dessus, l'ordre est donc 12 .

Si $\sigma \in S_n$, soient n_1, n_2, \dots, n_k la longueur de ses cycles, on a :

$$n = n_1 + n_2 + \dots + n_k$$

$$\text{ordre de } \sigma = \text{p. p. c. m. } (n_1, n_2, \dots, n_k) .$$

D'autre part, une partition de n est un système quelconque d'entiers ≥ 1 (n_1, n_2, \dots, n_k) tels que $n = n_1 + n_2 + \dots + n_k$. Par exemple, le nombre $n = 5$ a 7 partitions :

$$5 = 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 2 + 1 = 2 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1 .$$

Il est facile de construire une permutation de n objets ayant k cycles de longueur (n_1, n_2, \dots, n_k) . A $5 = 2 + 2 + 1$, on associe, par exemple,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix} .$$

Si $n = n_1 + n_2 + \dots + n_k$ est une partition quelconque de n , il existe donc un élément de S_n dont l'ordre soit : p. p. c. m. (n_1, n_2, \dots, n_k) .

Nous allons nous intéresser à la fonction arithmétique :

$$g(n) = \sup_{\sigma \in S_n} [\text{ordre de } \sigma] = \sup_{\mathcal{P}(n)} [\text{p. p. c. m. } (n_1, n_2, \dots, n_k)] ,$$

$\mathcal{P}(n)$ désignant l'ensemble des partitions de n .

1. Propriétés de $g(n)$.

- $g(n)$ divise $n!$.
- $g(n)$ est croissante (soit $\sigma \in S_n$, l'élément $\sigma' \in S_{n+1}$, qui laisse invariant $(n+1)$ et coïncide ailleurs avec σ , a même ordre que σ) .
- Tableau des valeurs :

n	3	4	5	6	7	8	9	10	11	12	13
$g(n)$	3	4	6	6	12	15	20	30	30	60	60
ρ	3	4	2;3	1;2;3 6	3;4	3;5	4;5	2,3,5	1,2,3,5 5;6	3,4,5	1,3,4,5

La troisième ligne indique la (ou les) partition de n d'ordre $g(n)$. Le calcul de $g(n)$ n'est pas commode dès que n devient grand.

- $g(n)$ n'est pas strictement croissante : $g(12) = g(13)$.
- Pour $n = 6$, $n = 11$, on constate que plusieurs partitions sont d'ordre $g(n)$ (on appelle ordre d'une partition, l'ordre d'un élément σ de S_n associé).
- Parmi les partitions d'ordre $g(n)$ il en existe une, telle que les $(n_i)_{1 \leq i \leq k}$ soient des puissances de nombres premiers ou des 1 . En effet, si

$$n = n_1 + n_2 + \dots + n_k$$

et si $n_1 = ab$, avec $a > 1$, $b > 1$, $(a, b) = 1$, $a, b \in \mathbb{N}$. On a

$$ab - (a + b) = (a - 1)(b - 1) - 1 \geq 0 ,$$

et les partitions

$$n = a + b + n_2 + \dots + n_k + \underbrace{1 + 1 + \dots + 1}_{ab - (a + b)} = ab + n_2 + \dots + n_k$$

ont même ordre, les multiples de ab étant les mêmes que ceux de $a + b$ puisque $(a, b) = 1$.

Dans la formule de définition de $g(n)$, on peut se restreindre au cas où $n_i = p^r$:

$$g(n) = \sup_{\sum p^r \leq n} \prod p^r ,$$

le "sup" s'étendant à tous les systèmes de couples p, r (p premier, $r \in \mathbb{N}$) de somme $\sum p^r \leq n$.

2. Majoration et minoration de $g(n)$.

p_h étant le h -ième nombre premier ($p_h \sim h \log h$) , on pose :

$$P_j = \sum_{h=1}^j p_h ,$$

j	1	2	3	4	5	6	7	8	9
p_j	2	3	5	7	11	13	17	19	23
P_j	2	5	10	17	28	41	58	77	100

n étant donné, on définit j comme fonction de n par $P_j \leq n < P_{j+1}$.

- Minoration de $g(n)$. - On a

$$2 + 3 + \dots + p_j \leq n ,$$

donc $e^{\theta(p_j)} \leq g(n)$, avec $\theta(x) = \sum_{p \leq x} \log p$ étant la fonction de Čebyšev.

- Majoration de $g(n)$. - Le nombre de facteurs du produit $g(n) = \prod p^r$ est inférieur ou égal à j , sinon :

$$\sum p^r \geq \sum p \geq \sum_{h=1}^{j+1} p_h = P_{j+1} .$$

LEMME. - Le produit de k nombres de somme donnée n est maximum et égal à $(\frac{n}{k})^k$ quand les k nombres sont égaux.

Le résultat est bien connu pour $k = 2$, il se généralise par récurrence.

3. Etude de la fonction $k \mapsto y = (\frac{n}{k})^k$.

On a $\frac{y'}{y} = \log \frac{n}{k} - 1$;

k	1	n/e	∞
y	n	$e^{n/e}$	0

On peut montrer facilement que $j < \frac{n}{e}$ pour $n \geq 7$. Le produit $g(n) = \prod p^r$ a k facteurs ($k \leq j$) de somme n , donc

$$g(n) \leq \left(\frac{n}{k}\right)^k \leq \left(\frac{n}{j}\right)^j \quad \text{pour } n \geq 7 .$$

Finalement, $n \geq 7$, $P_j \leq n < P_{j+1}$,

$$e^{\theta(p_j)} \leq g(n) \leq \left(\frac{n}{j}\right)^j .$$

4. Calcul d'un équivalent de $\log g(n)$.

Pour h, j, n tendant vers l'infini,

$$p_h \sim h \log h ,$$

$$P_j = \sum_{h=1}^j p_h \sim \sum_{h=1}^j h \log h \sim \int_1^j t \log t \, dt = \frac{j^2}{2} \log j - \frac{j^2}{4} + \frac{1}{4} ,$$

$$P_j \sim \frac{j^2}{2} \log j .$$

Ce calcul sera justifié par la suite.

D'autre part, $P_{j+1} - P_j = (j+1) \log(j+1) = o(j^2 \log j)$, donc $P_{j+1} \sim P_j$ et

$$n \sim \frac{j^2}{2} \log j .$$

On en déduit $\log n \sim 2 \log j$, puis

$$\frac{j^2}{2} \sim \frac{2n}{\log n} \quad \text{et} \quad j \sim 2 \sqrt{\frac{n}{\log n}} .$$

Or $\theta(p_j) \leq \log g(n) \leq j[\log n - \log j]$,

$$\theta(p_j) \sim p_j \sim j \log j \sim \sqrt{n \log n} ,$$

$$j[\log n - \log j] \sim j \frac{\log n}{2} \sim \sqrt{n \log n} .$$

On en déduit :

$$\log g(n) \sim \sqrt{n \log n} .$$

5. Développement asymptotique de $\log g(n)$.

Nous allons maintenant chercher un développement asymptotique de $\theta(p_j)$ et de

$j \log \frac{n}{j}$. Il y aura cinq étapes :

- (a) Développement de p_h en fonction de h .
- (b) Développement de P_j en fonction de j .
- (c) Développement de j en fonction de n .
- (d) Développement de $\theta(p_j)$ en fonction de n .
- (e) Développement de $j \log \frac{n}{j}$ en fonction de n .

(a) Développement de p_h en fonction de h . - On sait que

$$\Pi(x) = \sum_{p \leq x} 1 = \text{li}(x) + o\left(\frac{x}{\log^k(x)}\right) \quad \forall k ,$$

et, en intégrant $\text{li}(x) = \int_2^x \frac{dx}{\log x}$ par parties, on obtient

$$\Pi(x) = \frac{x}{\log x} + \frac{x}{\log^2 x} + \dots + \frac{(k-1)! x}{\log^k x} + o\left(\frac{x}{\log^k x}\right) .$$

Pour $x = p_h$, $\Pi(x) = h$, en prenant $k = 2$, on a :

$$h = \frac{p_h}{\log p_h} + \frac{p_h}{\log^2 p_h} + o\left(\frac{p_h}{\log^2 p_h}\right) .$$

De $p_h \sim h \log h$, on déduit que

$$o\left(\frac{p_h}{\log^2 p_h}\right) = o\left(\frac{h}{\log h}\right) ,$$

$$p_h = h \log h [1 + o(1)] ,$$

$$\log p_h = \log h + \log \log h + o(1) ,$$

d'où

$$h[1 + o\left(\frac{1}{\log h}\right)] = \frac{p_h}{\log p_h} \left[1 + \frac{1}{\log p_h}\right] ,$$

$$p_h = h[1 + o\left(\frac{1}{\log h}\right)] \log p_h \left[1 - \frac{1}{\log p_h} + o\left(\frac{1}{\log p_h}\right)\right] ,$$

$$p_h = h[\log h + \log \log h - 1 + r_h] \quad \text{avec } r_h = o(1) .$$

(b) Développement de P_j en fonction de j .

$$P_j = \sum_{h=1}^j p_h = \sum_1^j h \log h + \sum_1^j h \log \log h - \sum_1^j h + \sum_1^j h r_h .$$

Utilisons la formule sommatoire d'Euler-MacLaurin ([1], chapitre VI, § 3, n° 1) à l'ordre 1 :

$$f(x) + f(x+1) + \dots + f(x+m) = \int_x^{x+m+1} f(t) dt - \frac{1}{2}[f(x+m+1) - f(x)] + \frac{1}{12}[f'(x+m+1) - f'(x)] + R(x, m) ,$$

$$\text{avec } R \leq C \int_x^{x+m+1} |f'''(t)| dt \text{ et } C = \frac{4e^{2\pi}}{(2\pi)^3} .$$

(α) Posons $f(t) = t \log t$; $f'(t) = \log t + 1$; $f''(t) = \frac{1}{t}$; $f'''(t) = -\frac{1}{t^2}$;
 $x = 1$; $m = j - 2$, on obtient :

$$\sum_{h=1}^{j-1} h \log h = \int_1^j t \log t dt - \frac{1}{2} j \log j + \frac{1}{12} \log j + R .$$

On voit que R est majoré par C . On trouve :

$$\sum_{h=1}^j h \log h = \frac{j^2}{2} \log j - \frac{j^2}{4} + o(j^2) .$$

(β) Posons $f(t) = t \log \log t$; $f'(t) = \log \log t + \frac{1}{\log t}$; $f''(t) = \frac{\log t - 1}{t \log^2 t}$;
 $f'''(t) = \frac{2 \log^2 t - 1}{t^2 \log^3 t}$; $x = 3$; $m = j - 2$. Comme dans cet exemple, f et ses dérivées sont plus petites que précédemment, tous les termes, qui étaient négligeables, le sont encore, et

$$\sum_{h=3}^j h \log \log h = \int_3^j t \log \log t dt + o(j^2) ,$$

$$\int_3^j t \log \log t dt = \frac{j^2}{2} \log \log j - \int_3^j \frac{t dt}{2 \log t} + o(j^2) .$$

Nous utilisons le théorème ([1], chapitre V, § 3, n° 3, prop. 6) :

Soient f et g deux fonctions numériques réglées (limite uniforme sur tout compact de fonctions en escalier) définies sur $]a, +\infty[$, telles que $g \geq 0$, $f = o(g)$, et $\int_a^{+\infty} g(t) dt = +\infty$; alors :

$$\int_a^x f(t) dt = o\left[\int_a^x g(t) dt\right] .$$

Alors :

$$\int_3^j \frac{t}{2 \log t} dt = o\left[\int_3^j t dt\right] = o(j^2) .$$

On a, en fait,

$$\int_3^j \frac{t}{2 \log t} dt \sim \frac{j^2}{4 \log j} \quad ([1], \text{n}^\circ 5, \text{prop. 8}) .$$

$$(\gamma) \quad \sum_{h=1}^j h = \frac{j(j+1)}{2} = \frac{j^2}{2} + o(j^2) .$$

$$(\delta) \quad \sum_{h=1}^j hr_h = \int_1^{j+1} r(t) dt , \quad r(t) \text{ étant défini par } h \leq t < h+1 , \quad r(t) = hr_h .$$

Comme $r(t) = o(t)$ d'après le théorème précédent,

$$\sum_{h=1}^j hr_h = o(j^2) .$$

Finalelement :

$$P_j = \frac{j^2}{2} \log j + \frac{j^2}{2} \log \log j - \frac{3j^2}{4} + o(j^2) .$$

(c) Développement de j en fonction de n . - Comme $P_{j+1} - P_j = o(j^2)$,

$$n = \frac{j^2}{2} \log j + \frac{j^2}{2} \log \log j - \frac{3j^2}{4} + o(j^2) .$$

On avait vu que $j = 2 \sqrt{\frac{n}{\log n}} (1 + o(1))$, d'où

$$\log j = \frac{1}{2} \log n - \frac{1}{2} \log \log n + \log 2 + o(1) ,$$

$$\log \log j = \log \log n - \log 2 + o(1) .$$

Comme $j^2 \sim 4 \frac{n}{\log n}$, $o(j^2) = o(\frac{n}{\log n})$, d'où :

$$n(1 + o(\frac{1}{\log n})) = \frac{j^2}{4} [2 \log j + 2 \log \log j - 3] = \frac{j^2}{4} [\log n + \log \log n - 3] ,$$

$$\frac{j^2}{4} = \frac{n}{\log n} \frac{1}{1 + \frac{\log \log n}{\log n} - \frac{3}{\log n}} [1 + o(\frac{1}{\log n})] .$$

On trouve :

$$j = 2 \sqrt{\frac{n}{\log n}} \left[1 - \frac{\log \log n}{2 \log n} + \frac{3}{2 \log n} + o(\frac{1}{\log n}) \right] .$$

(d) Développement de $\theta(p_j)$ en fonction de n . - On sait que :

$$\theta(x) = x + o\left(\frac{x}{\log^k x}\right) .$$

Pour $k = 1$,

$$\theta(p_j) = p_j + o\left(\frac{p_j}{\log p_h}\right) = p_j + o(j) ,$$

$$\begin{aligned} \theta(p_j) &= j[\log j + \log \log j - 1 + o(1)] \\ &= j\left[\frac{1}{2} \log n + \frac{1}{2} \log \log n - 1 + o(1)\right] . \end{aligned}$$

En remplaçant j par sa valeur,

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

(e) Développement de $j[\log n - \log j]$.

$$\log n - \log j = \frac{1}{2} \log n + \frac{1}{2} \log \log n - \log 2 + o(1)$$

et

$$j[\log n - \log j] = \sqrt{n \log n} \left[1 + \frac{\log \log n}{2 \log n} + \frac{\frac{3}{2} - 2 \log 2}{\log n} + o\left(\frac{1}{\log n}\right)\right] .$$

Résultat :

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

avec $-\frac{1}{2} \leq \liminf a_n \leq \limsup a_n \leq \frac{3}{2} - 2 \log 2 \neq 0,1$.

BIBLIOGRAPHIE

- [1] BOURBAKI (Nicolas). - Fonctions d'une variable réelle, chap. 4 à 7. - Paris, Hermann, 1951 (Act. scient. et ind. 1132, Bourbaki, 12).
- [2] LANDAU (Edmund). - Handbuch der Lehre von der Verteilung der Primzahlen. - Leipzig und Berlin, B. G. Teubner, 1909.