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)
7e année, 1965/66, n° 13

14 mars 1966

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 $m \geqslant 1$ 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 , ... , n_k la longueur de ses cycles, on a :

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

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

D'autre part, une partition de n est un système quelconque d'entiers $\geqslant 1$ $(n_1 , n_2 , \ldots , n_k)$ tels que $n = n_1 + n_2 + \ldots + n_k$. 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 $(n_1 , n_2 , \ldots , n_k)$. 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 $n = n_1 + n_2 + \ldots + n_k$ est une partition quelconque de n , il existe donc un élément de S_n dont l'ordre soit : p. p. c. m. $(n_1 , n_2 , \ldots , n_k)$.

Nous allons nous intéresser à la fonction arithmétique :

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

$\mathcal{P}(n)$ 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
$\mathcal{P}$	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 $(n_i)_{1 \leqslant i \leqslant k}$ 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 $a > 1$, $b > 1$, $(a , b) = 1$, $a , b \in \underset{\sim}{\mathbb{N}}$. On a

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

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 $n_i = p^r$:

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

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

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 $P_j \leqslant n < P_{j+1}$.

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

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

donc $e^{\theta(p_j)} \leqslant g(n)$, avec $\theta(x) = \sum_{p \leqslant x} \log p$ 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 :

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

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 $k \longmapsto y = (\frac{n}{k})^k$.

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 $n \geqslant 7$. Le produit $g(n) = \prod p^r$ a k facteurs $(k \leqslant j)$ de somme n , donc

$$g(n) \leqslant (\frac{n}{k})^k \leqslant (\frac{n}{j})^j \qquad \text{pour} \quad n \geqslant 7 \ .$$

Finalement, $n \geqslant 7$, $P_j \leqslant n < P_{j+1}$,

$$e^{\theta(p_j)} \leqslant g(n) \leqslant (\frac{n}{j})^j \ .$$

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

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

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

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

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

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

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

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

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

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

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

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

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

(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 :

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

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

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

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

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

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

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

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

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

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 $g \geqslant 0$, $f = o(g)$, et $\int_a^{+\infty} g(t)\,dt = +\infty$; alors :

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

Alors :

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

On a, en fait,

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

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

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

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

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

Finalement :

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

(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 :

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

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

On trouve :

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

(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 $k = 1$,

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

$$\theta(p_j) = j[\log j + \log\log j - 1 + o(1)]$$
$$= j[\tfrac{1}{2}\log n + \tfrac{1}{2}\log\log n - 1 + o(1)] .$$

En remplaçant j par sa valeur,

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

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

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

et

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

Résultat :

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

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

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.