

SÉMINAIRE DELANGE-PISOT-POITOU. THÉORIE DES NOMBRES

CHRISTIAN RADOUX

Nouvelles propriétés arithmétiques des nombres de Bell

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 16, n° 2 (1974-1975),
exp. n° 22, p. 1-12

http://www.numdam.org/item?id=SDPP_1974-1975__16_2_A1_0

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1974-1975, 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/>

NOUVELLES PROPRIÉTÉS ARITHMÉTIQUES DES NOMBRES DE BELL

par Christian RADOUX [Mons]

1. Périodicité, modulo p premier, de la suite des nombres de Bell.

Notations et propriétés élémentaires [2].

P_n est le n-ième "nombre de Bell" : nombre de partitions d'un ensemble de cardinal n (on pose $P_0 = 1$).

$P_{n,k}$ ($1 \leq k \leq n$) est le nombre de partitions en k classes d'un ensemble de cardinal n . Les $P_{n,k}$ sont les "nombres de Stirling de 2e espèce". Evidemment,

$$(1) \quad P_n = \sum_{k=1}^n P_{n,k}.$$

En outre,

$$(2) \quad P_{n,k} = P_{n-1,k-1} + kP_{n-1,k},$$

$$(3) \quad P_{n+1} = \sum_{k=0}^n C_n^k P_k.$$

Appelons encore $s_{n,k}$ le nombre de surjections d'un ensemble de cardinal n sur un ensemble de cardinal k . Evidemment,

$$(4) \quad s_{n,k} = k! P_{n,k}.$$

* * *

$$(5) \quad \sum_{k=0}^m C_m^k k^n x^k (1-x)^{m-k} = \sum_{k=1}^n C_m^k s_{n,k} x^k \quad (m \geq 0, n \geq 1).$$

En effet,

$$\begin{aligned} \sum_{k=0}^m C_m^k k^n x^k (1-x)^{m-k} &= \sum_{k=0}^m C_m^k \{D_y^n e^{ky}\}_{y=0} x^k (1-x)^{m-k} \\ &= \{D_y^n [\sum_{k=0}^m C_m^k e^{ky} x^k (1-x)^{m-k}]\}_{y=0} \\ &= \{D_y^n [e^y x + (1-x)]^m\}_{y=0} \\ &= \{\sum_{k=1}^n k! C_m^k P_{n,k} x^k e^{ky} [e^y x + (1-x)]^{m-k}\}_{y=0}, \\ &\hspace{20em} \text{par récurrence, vu (2)} \\ &= \sum_{k=1}^n C_m^k k! P_{n,k} x^k = \sum_{k=1}^n C_m^k s_{n,k} x^k. \end{aligned}$$

En identifiant les termes de puissances semblables dans (5), on obtient, après quelques simplifications évidentes,

$$(6) \quad \sum_{l=0}^k (-1)^l C_k^l l^n = (-1)^k s_{n,k} \quad (1 \leq k).$$

* * *

Soit p un nombre premier

$$\begin{aligned}
s_{p,k} &= (-1)^k \sum_{\ell=0}^k (-1)^\ell C_k^\ell \ell^p \\
&\equiv (-1)^k \sum_{\ell=0}^k (-1)^\ell C_k^\ell \ell \pmod{p} \\
&\equiv s_{1,k} \pmod{p} \quad (= 0 \text{ si } k > 1) .
\end{aligned}$$

Ainsi

$$(7) \quad [p \text{ premier et } k > 1] \implies [s_{p,k} \equiv 0 \pmod{p}] .$$

Mais alors, d'après (4),

$$(8) \quad [p \text{ premier et } 1 < k < p] \implies [P_{p,k} \equiv 0 \pmod{p}] .$$

Comme $P_{p,1} = P_{p,p} = 1$, on a donc, d'après (1),

$$(9) \quad [p \text{ premier}] \implies [P_p \equiv 2 \pmod{p}] .$$

On peut encore démontrer (mais c'est beaucoup laborieux) que :

$$[p \text{ premier } > 2 \text{ et } (p-1) | q] \implies [s_{q,p-1} \equiv -1 \pmod{p}]$$

$$[p \text{ premier } > 2 \text{ et } (p-1) \nmid q] \implies [s_{q,p-1} \equiv 0 \pmod{p}]$$

$$[p \text{ premier } > 2 \text{ et } (p-1) | q] \implies [P_{q+1,p} \equiv P_{q,p-1} \equiv 1 \pmod{p}]$$

$$[p \text{ premier } > 2 \text{ et } (p-1) \nmid q] \implies [P_{q+1,p} \equiv P_{q,p-1} \equiv 0 \pmod{p}]$$

$$[n \text{ composé } > 4] \implies [s_{q,n-1} \equiv 0 \pmod{n}] .$$

* * *

THÉORÈME 1. - $\forall p$ premier, $\forall n \in \mathbb{N}$; $\forall \ell \in \mathbb{N}$,

$$(10) \quad P_{n+p}^\ell \equiv P_{n+1} + \ell P_n \pmod{p} .$$

N. B. - Louis COMTET donne dans [2] (t. II, p. 61) le cas particulier $\ell = 1$ de cette congruence. Notre démonstration, pour ce cas $\ell = 1$, diffère totalement de la sienne (Ce résultat (10) n'est donc pleinement original que pour $\ell > 1$).

Démonstration (par récurrence).

(a) La formule est triviale pour $\ell = 0$, et vraie pour $\ell = 1$.

En effet, on vérifie, par une récurrence immédiate, en utilisant (2) que, si $n > 0$,

$$(11) \quad D_x^{n+p}[e^{(e^x)}] = \sum_{k=1}^n P_{n,k} e^{(kx+e^x)} .$$

Ainsi

$$\begin{aligned}
D_x^{n+p}[e^{(e^x)}] &= \sum_{k=1}^n P_{n,k} D_x^p[e^{kx} \times e^{(e^x)}] , \\
D_x^{n+p}[e^{(e^x)}] &= \sum_{k=1}^n P_{n,k} \sum_{\ell=0}^p C_p^\ell D_x^\ell[e^{(e^x)}] D_x^{p-\ell}(e^{kx}) .
\end{aligned}$$

Posons $x = 0$, et divisons par e . Il vient, d'après (11) et (1),

$$P_{n+p} = \sum_{k=1}^n P_{n,k} \sum_{\ell=0}^p C_p^\ell P_\ell k^{p-\ell} .$$

Or p est premier. Donc

$$C_p^1 \equiv \dots \equiv C_p^{p-1} \equiv 0 \pmod{p}$$

$$k^p \equiv k \pmod{p}$$

$$P_p \equiv 2 \pmod{p} \quad (\text{formule (9)}).$$

Ainsi

$$P_{n+p} \equiv \sum_{k=1}^n P_{n,k} (k+2) \pmod{p}$$

$$P_{n+p} \equiv 2P_n + \sum_{k=1}^n k P_{n,k} \pmod{p} \quad (\text{vu (1)})$$

$$P_{n+p} \equiv 2P_n + P_{n,1} + \sum_{k=2}^n (P_{n+1,k} - P_{n,k-1}) \pmod{p} \quad (\text{vu (2)})$$

$$P_{n+p} \equiv 2P_n + P_{n,1} + (P_{n+1} - P_{n+1,1} - P_{n+1,n+1}) - (P_n - P_{n,n}) \pmod{p} \quad (\text{vu (1)})$$

$$P_{n+p} \equiv 2P_n + 1 + (P_{n+1} - 1 - 1) - (P_n - 1) \pmod{p}$$

c'est-à-dire

$$P_{n+p} \equiv P_{n+1} + P_n \pmod{p}.$$

Ceci reste vrai (9) pour $n = 0$.

(b) Hypothèse de récurrence : supposons la formule (10) vraie pour $\ell = k$.

(c) Considérons l'équation $z^{(p^k)} = z + k$. Toutes ses racines sont simples. En effet,

$$\left\{ \begin{array}{l} z^{(p^k)} = z + k \\ p^k z^{(p^k-1)} = 1 \end{array} \right\} \Rightarrow (p^k(z+k) = z) \Rightarrow \left(z = \frac{kp^k}{1-p^k} \right),$$

alors que

$$p^k \left(\frac{kp^k}{1-p^k} \right) \neq 1.$$

Soient donc z_1, \dots, z_{p^k} les p^k -racines de $z^{(p^k)} = z + k$.

Considérons la suite $(R_n)_{n \in \mathbb{N}}$, définie par $R_n = \sum_{j=1}^{p^k} \alpha_j z_j^n$, où $\alpha_1, \dots, \alpha_{p^k}$ sont choisis de telle sorte que $R_i = P_i$ ($i = 0, 1, \dots, p^k - 1$)

$$\forall n \in \mathbb{N}, R_{n+p^k} = \sum_{j=1}^{p^k} \alpha_j z_j^{n+p^k} = \sum_{j=1}^{p^k} \alpha_j z_j^n (z_j + k)^{p^k} = R_{n+1} + kR_n.$$

Ceci montre, d'abord que tous les R_n sont entiers, ensuite que

$$\forall n \in \mathbb{N}, R_n \equiv P_n \pmod{p},$$

vu l'hypothèse de récurrence (b) et le choix des α_j . Mais alors,

$$\begin{aligned} \forall n \in \mathbb{N}, R_{n+p^k} &= \sum_{j=1}^{p^k} \alpha_j z_j^{n+p^k} \\ &= \sum_{j=1}^{p^k} \alpha_j z_j^n [z_j^{(p^k)}]^p \\ &= \sum_{j=1}^{p^k} \alpha_j z_j^n (z_j + k)^p \\ &= \sum_{\ell=0}^p C_p^\ell k^{p-\ell} \sum_{j=1}^{p^k} \alpha_j z_j^{n+\ell} \end{aligned}$$

$$\begin{aligned}
&= \sum_{\ell=0}^p C_p^\ell k^{p-\ell} R_{n+\ell} \\
&\equiv k^p R_n + R_{n+p} \pmod{p} \\
&\equiv kR_n + R_{n+p} \pmod{p} .
\end{aligned}$$

Ceci équivaut à

$$\forall n \in \mathbb{N}, P_{n+p}^{k+1} \equiv kP_n + P_{n+p} \pmod{p} .$$

La formule (10) étant prouvée pour $\ell = 1$, on a donc, modulo p ,

$$\forall n \in \mathbb{N}, P_{n+p}^{k+1} \equiv kP_n + (P_{n+1} + P_n) \equiv P_{n+1} + (k+1)P_n ,$$

ce qui achève la démonstration par récurrence.

* * *

THÉORÈME 2.

(a) La suite P_n est, modulo p premier, périodique, sans début aperiodique.

(b) La période k_p divise $p^p - 1$.

(a) $\forall n \in \mathbb{N}, P_{n+p} \equiv P_{n+1} + P_n \pmod{p} .$

La suite P_n est donc bien connue (mod p) dès que l'on connaît

$$(P_0, P_1, \dots, P_{p-1}) \pmod{p} .$$

Il existe, à priori, p^p façons de former une telle séquence. Considérons les $p^p + 1$ séquences $(P_i, P_{i+1}, \dots, P_{i+p-1})$, $i = 0, 1, \dots, p^p$. Deux (au moins) d'entre elles sont donc égales (mod p).

Soient a et b ($a < b$) les deux valeurs de i qui correspondent à la première répétition :

$$(P_a, P_{a+1}, \dots, P_{a+p-1}) \equiv (P_b, P_{b+1}, \dots, P_{b+p-1}) \pmod{p} .$$

On a nécessairement $a = 0$.

En effet, si $a > 0$, on a successivement

$$P_{a+p-1} \equiv P_{b+p-1} \pmod{p}$$

$$P_a + P_{a-1} \equiv P_b + P_{b-1} \pmod{p}$$

$$P_{a-1} \equiv P_{b-1} \pmod{p}$$

$$(P_{a-1}, P_a, \dots, P_{a+p-2}) \equiv (P_{b-1}, P_b, \dots, P_{b+p-2}) \pmod{p} ,$$

contrairement à l'hypothèse de minimalité de a .

Ainsi, $\forall p$ premier, $\exists k \in \{1, \dots, p^p\}$, $\forall n \in \mathbb{N}, P_{n+k} \equiv P_n \pmod{p}$. On appellera k_p le plus petit de ces k . En d'autres termes, k_p est la période de $(P_n)_{n \in \mathbb{N}}$ (mod p).

N. B. - On vérifie sans peine (par récurrence) que $\sum_{k=1}^n R_{n,k} = n!$

(c) La formule

$$(12) \quad P_{(p-1)^*+n} \equiv \sum_{\ell=1}^k (-1)^{\ell+1} R_{k,\ell} P_{(p-k)^*+k-\ell+n} \pmod{p}; \quad k = 1, \dots, p$$

se démontre immédiatement, par récurrence sur k , en tenant compte de la définition de $(p-1)^*$ et de la formule (10).

(d) En particulier, pour $k = p$, il vient

$$P_{(p-1)^*+n} \equiv \sum_{\ell=1}^p (-1)^{\ell+1} R_{p,\ell} P_{0^*+p-\ell+n} \pmod{p}.$$

Si nous tenions pour assuré le fait que

$$(13) \quad [p \text{ premier et } 1 < k < p] \implies [R_{p,k} \equiv 0 \pmod{p}],$$

nous pourrions alors écrire

$$P_{(p-1)^*+n} \equiv R_{p,1} P_{0^*+p-1+n} + R_{p,p} P_{0^*+n} \pmod{p}.$$

Or $R_{p,1} = 1$ et $R_{p,p} = (p-1)! \equiv -1 \pmod{p}$ (WILSON). Ainsi, en remplaçant $(p-1)^*$ et 0^* par leurs valeurs respectives,

$$P_{((p^p-1)/(p-1))+n} \equiv P_{n+p} - P_{n+1} \pmod{p}$$

ou encore, d'après (10),

$$P_{((p^p-1)/(p-1))+n} \equiv P_n \pmod{p},$$

ce qui montre que $(p^p-1)/(p-1)$ est un multiple de k_p .

(e) Reste donc à prouver l'assertion (13).

De $R_{n,2} = (n(n-1))/2$ et de $R_{n+1,k} = nR_{n,k-1} + R_{n,k}$, on déduit, par une récurrence immédiate que, si $k > 1$ est fixé, $R_{n,k}$ est interpolé continûment par un polynôme à coefficients rationnels, de degré $2k-2$, sans terme indépendant :

$$R_{n,2} = (n(n-1))/2,$$

$$R_{n,3} = (n(n-1)(n-2)(3n-1))/24,$$

$$R_{n,4} = (n^2(n-1)^2(n-2)(n-3))/48,$$

$$R_{n,5} = (n(n-1)(n-2)(n-3)(n-4)(15n^3 - 30n^2 + 5n + 12))/5460, \dots$$

En outre, le polynôme exprimant $R_{n,k}$ doit s'annuler pour $n = 0, 1, \dots, k-1$.

Appelons $\mathcal{R}_{2k-2}(n)$ ce polynôme. Tout revient à prouver que, si nous écrivons (comme ci-dessus) $\mathcal{R}_{2k-2}(n)$ sous la forme du quotient d'un polynôme à coefficients entiers par un entier d_{2k-2} , nous pouvons, après simplification, affirmer que d_{2k-2} ne renferme aucun facteur premier $p > k$.

$$R_{n+1,k+1} = nR_{n,k} + R_{n,k+1}. \text{ Donc}$$

$$\mathcal{R}_{2k}(n+1) = n\mathcal{R}_{2k-2}(n) + \mathcal{R}_{2k}(n).$$

Nous pouvons, à titre d'hypothèse de récurrence, supposer que $R_{2k-2}(n)$ vérifie (14). Simplifions par les k facteurs $n, n-1, \dots, n-k+1$. Il vient une identité du type

$$\begin{aligned} \alpha_k(n+1)^k + \alpha_{k-1}(n+1)^{k-1} + \dots + \alpha_1(n+1) + \alpha_0 \\ = n(\beta_{k-2} n^{k-2} + \beta_{k-3} n^{k-3} + \dots + \beta_0) + \alpha_k n^k + \alpha_{k-1} n^{k-1} + \dots + \alpha_0. \end{aligned}$$

Finalement, nous savons encore que $\alpha_k n^k + \dots + \alpha_0$ doit s'annuler pour $n = k$. D'où une dernière identité du type

$$(n+1-k)(\gamma_{k-1}(n+1)^{k-1} + \dots + \gamma_0) = n(\beta_{k-2} n^{k-2} + \dots + \beta_0) + (n-k)(\gamma_{k-1} n^{k-1} + \dots + \gamma_0).$$

D'après notre hypothèse de récurrence, l'identification donnera pour $R_{2k}(n)$ des coefficients du type attendu.

* * *

THÉOREME 4. - $\forall p$ premier, $\forall n, a \in \mathbb{N}$,

$$(15) \quad P_{np+a} \equiv (-1)^a \sum_{\ell=0}^a (-1)^\ell C_a^\ell P_{n+1+\ell} \pmod{p}.$$

(cette congruence est évidemment essentiellement intéressante pour $0 \leq a < p$.)

Démontrons (par récurrence) la formule équivalente, $\forall p$ premier, $\forall n, a \in \mathbb{N}$,

$$(15') \quad P_{np+a} \equiv \sum_{\ell=0}^a (-1)^\ell C_a^\ell P_{n+a+1-\ell} \pmod{p}.$$

(a) La formule est vraie pour $a = 0$:

$$(16) \quad \forall p \text{ premier, } \forall n \in \mathbb{N}, P_{np} \equiv P_{n+1} \pmod{p}.$$

Prouvons d'abord (par récurrence également) la forme auxiliaire

$$(17) \quad \forall p \text{ premier, } \forall n \in \mathbb{N}, P_{np} \equiv \sum_{\ell=0}^k C_k^\ell P_{(n-k)p+\ell} \pmod{p}, \quad k=0, \dots, n$$

1° La formule (17) est triviale pour $k = 0$, et vraie pour $k = 1$ (cf. (10))

2° Supposons ensuite (hypothèse de récurrence) cette assertion vraie pour $k = m$ (m fixé, $m < n$) :

$$P_{np} \equiv \sum_{\ell=0}^m C_m^\ell P_{(n-m)p+\ell} \pmod{p}$$

3° Alors

$$\begin{aligned} P_{np} &\equiv \sum_{\ell=0}^m C_m^\ell P_{\{[n-(m+1)]p+\ell\}+p} \pmod{p} \\ &\equiv \sum_{\ell=0}^m C_m^\ell (P_{[n-(m+1)]p+\ell+1} + P_{[n-(m+1)]p+\ell}) \pmod{p} \quad (\text{vu (10)}) \\ &\equiv \sum_{\ell=1}^{m+1} C_m^{\ell-1} P_{[n-(m+1)]p+\ell} + \sum_{\ell=0}^m C_m^\ell P_{[n-(m+1)]p+\ell} \pmod{p} \\ &\equiv P_{[n-(m+1)]p} + \sum_{\ell=1}^m (C_m^{\ell-1} + C_m^\ell) P_{[n-(m+1)]p+\ell} + P_{[n-(m+1)]p+(m+1)} \pmod{p} \\ &\equiv \sum_{\ell=0}^{m+1} C_{m+1}^\ell P_{[n-(m+1)]p+\ell} \pmod{p}. \end{aligned}$$

Ceci achève de prouver (17). Posons $k = n$ dans cette formule. Il vient

$$\forall p \text{ premier}, \forall n \in \underline{\mathbb{N}}, P_{np} \equiv \sum_{\ell=0}^n C_n^\ell P_\ell \pmod{p},$$

c'est-à-dire, d'après la formule (3),

$$\forall p \text{ premier}, \forall n \in \underline{\mathbb{N}}, P_{np} \equiv P_{n+1} \pmod{p}.$$

La formule (16) est ainsi prouvée.

(b) Hypothèse de récurrence : la formule (15') est vraie pour $a = k$:

$$\forall p \text{ premier}, \forall n \in \underline{\mathbb{N}}, P_{np+k} \equiv \sum_{\ell=0}^k (-1)^\ell C_k^\ell P_{n+k+1-\ell} \pmod{p}.$$

(c) Alors elle subsiste pour $a = k + 1$. En effet,

$$\begin{aligned} P_{np+k+1} &= 2 \sum_{\ell=1}^{k+1} (-1)^\ell C_k^{\ell-1} P_{n+k-(\ell-2)} \\ &= P_{np+k+1} + 2 \sum_{\ell=0}^k (-1)^\ell C_k^\ell P_{n+k+1-\ell} \\ &\equiv P_{np+k+1} + 2P_{np+k} \pmod{p} \quad (\text{vu l'hypothèse de récurrence}) \\ &\equiv P_{np+k+p^2} \pmod{p} \quad (\text{vu (10)}) \\ &\equiv \sum_{\ell=0}^k (-1)^\ell C_k^\ell P_{n+p+k+1-\ell} \pmod{p} \quad (\text{vu l'hypothèse de récurrence}) \\ &\equiv \sum_{\ell=0}^k (-1)^\ell C_k^\ell (P_{n+k+2-\ell} + P_{n+k+1-\ell}) \pmod{p} \quad (\text{vu (10)}) \\ &\equiv \sum_{\ell=0}^k (-1)^\ell C_k^\ell (P_{n+k-(\ell-2)} + P_{n+k-(\ell-1)}) \pmod{p} \\ &\equiv \sum_{\ell=0}^k (-1)^\ell C_k^\ell P_{n+k-(\ell-2)} + \sum_{\ell=1}^{k+1} (-1)^{\ell-1} C_k^{\ell-1} P_{n+k-(\ell-2)} \pmod{p} \\ &\equiv P_{n+k+2} + \left[\sum_{\ell=1}^k (-1)^\ell (C_k^\ell - C_k^{\ell-1}) P_{n+k-(\ell-2)} \right] + (-1)^k P_{n+1} \pmod{p}. \end{aligned}$$

Ainsi, en comparant les membres extrêmes de cette suite de congruences,

$$P_{np+k+1} \equiv P_{n+k+2} + \left[\sum_{\ell=1}^k (-1)^\ell (C_k^\ell + C_k^{\ell-1}) P_{n+k-(\ell-2)} \right] - (-1)^k P_{n+1} \pmod{p},$$

c'est-à-dire

$$P_{np+k+1} \equiv \sum_{\ell=0}^{k+1} (-1)^\ell C_{k+1}^\ell P_{n+k+2-\ell} \pmod{p}.$$

Ceci achève la démonstration de (15).

2. Nombre de topologies de Kolmogorov sur un ensemble de p éléments (p premier).

Soit E un ensemble fini à n éléments. Soit \mathcal{C} une topologie sur E . Si $x \in E$, nous noterons $t(x)$ la fermeture topologique de x (vis à vis de \mathcal{C}), c'est-à-dire le plus petit fermé de \mathcal{C} dont x est élément. Evidemment $t(x)$ est l'intersection (finie) de tous les fermés dont x est élément.

\mathcal{C} est une "topologie de Kolmogorov" ou " T_0 -topologie" lorsque $t : x \mapsto t(x)$ est injective.

On sait que le demi-treillis des ordres sur E est dual du demi-treillis des topologies de Kolmogorov sur cet ensemble [1]. Dénombrer les topologies de Kolmogorov sur E revient donc à dénombrer les ordres sur E . Soit donc O_n le nombre de ces ordres.

On a

| | | | | | | | | |
|------------|---|---|----|-----|-------|---------|-----------|-----|
| $n = \# E$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | ... |
| 0_n | 1 | 3 | 19 | 219 | 4.231 | 130.023 | 6.129.859 | ... |

THÉORÈME. - $[p \text{ premier}] \implies [0_p \equiv 1 \pmod{p}]$.

Démonstration.

(A) Soit r une relation d'ordre sur E , avec $\# E = p$, premier. s , fermeture transitive de $r \cup r^{-1}$, est la plus petite équivalence sur E incluant r . Elle détermine une partition de E en les classes C_1, \dots, C_k . Posons $\# C_i = n_i$.

La restriction de r à chacune de ces classes l'érige en ensemble ordonné. On regroupe ceux de ces ensembles qui sont isomorphes : on obtient ainsi les ensembles $\Omega_1, \dots, \Omega_j$.

Posons encore $\# \Omega_i = l_i$. Evidemment, $\sum_{i=1}^j l_i = k$.

(B) On sait que

$$[r' \text{ isomorphe à } r] \iff [\exists \rho \in \mathcal{S}_E, r' = \rho^{-1} \circ r \circ \rho].$$

Appelons Z_r le "centralisateur" (dans une acception assez libre, puisque $r \notin \mathcal{S}_E$) de r :

$$Z_r = \{\rho \in \mathcal{S}_E ; \rho^{-1} \circ r \circ \rho = r\}.$$

Posons $\# Z_r = q_r$ ($Z_r \neq \emptyset$, puisque $1_E \in Z_r$. Ainsi $q_r > 0$). Z_r est un sous-groupe de \mathcal{S}_E . D'après le théorème de Lagrange, on a donc $q_r \mid \# E$, c'est-à-dire $q_r \mid p!$.

Soit maintenant r' isomorphe à r .

$$Z_{r,r'} = \{\rho \in \mathcal{S}_E ; \rho^{-1} \circ r \circ \rho = r'\}$$

est une classe latérale de Z_r . En effet,

- si $\rho^{-1} \circ r \circ \rho = r'$, alors $r = \rho \circ r' \circ \rho^{-1}$, de sorte que si ρ^* est fixé dans $Z_{r,r'}$, on a

$$\forall \rho \in Z_{r,r'}, \rho \rho^{*-1} \in Z_r, \text{ c'est-à-dire } \rho \in Z_r \rho^*.$$

- réciproquement, il est clair que $[\rho \in Z_r \rho^*] \implies [\rho \in Z_{r,r'}]$.

Chaque ordre isomorphe à r sera ainsi obtenu q_r fois.

Il existe par conséquent, sur l'ensemble E , $(p!/q_r)$ ordres distincts isomorphes à r .

(G) Un élément de Z_r est nécessairement une permutation des classes C_i dans chaque $\Omega_1, \dots, \Omega_j$, composée avec une permutation des éléments de chaque C_i . Par conséquent, Z_r est un sous-groupe du groupe Z_r^* de toutes les permutations de ce type, et q_r est un diviseur de $q_r^* = \# Z_r^* = l_1! \dots l_j! n_1! \dots n_k!$.

(D) 1er cas : $1 < k < p$. - p , étant premier, ne peut diviser q_r^* , puisque $n_1 < p , \dots , n_k < p , l_1 < p , \dots , l_j < p$. A fortiori, p ne peut diviser q_r . Ainsi $(p!/q_r) \equiv 0 \pmod{p}$.

2e cas : $k = 1$. - Dans ce cas, le graphe de r ne peut comporter de parties connexes disjointes, et $s = E^2$. En outre, tout élément de Z_r permute entre eux (par la transformation $r \rightarrow \varphi^{-1} \circ r \circ \varphi$), d'une part les m_r éléments minimaux de E , d'autre part les $p - m_r$ éléments non minimaux de E (minimalité par rapport à r , bien entendu).

Appelons Z_r^{**} le groupe de toutes les permutations de ce type. Z_r est évidemment un sous-groupe de Z_r^{**} . Donc

$$q_r \mid \# Z_r^{**} = m_r! (p - m_r)!$$

Comme $0 < m_r < p$, $p \nmid q_r$, et l'on a encore $(p!/q_r) \equiv 0 \pmod{p}$.

3e cas : $k = p$ (c'est-à-dire $n_1 = \dots = n_k = 1$, $j = 1$ et $l_1 = p$) . - En d'autres termes, $Z_r = \mathcal{S}_E$ et $(p!/q_r) = 1$ ($\underline{1}_E$ est le seul ordre sur E isomorphe à $\underline{1}_E$).

(E) Finalement,

$$O_p = \sum_{\substack{\text{système de représentants} \\ \text{des } r \text{ non isomorphes}}} \frac{p!}{q_r} \equiv 1 \pmod{p} ,$$

comme annoncé.

Remarque. - En fait, nous avons démontré un résultat plus précis. Soit E un ensemble fini à p éléments, p premier. Si $r \neq \underline{1}_E$ est un ordre sur E , le nombre d'ordres sur E isomorphes à r (y compris r lui-même) est un multiple de p .

Conjectures. - Définissons la suite (r_n) par

$$\forall n \geq 1, \quad O_n = \sum_{k=1}^n k P_{n,k} r_k .$$

- Tous les r_n sont-ils entiers ?

- Si oui, a-t-on $r_p \equiv 1 \pmod{p}$ lorsque p est premier ?

$$(r_1=1, r_2=1, r_3=4, r_4=33, r_5=516, r_6=13600, r_7=572160, \dots)$$

Comme on a vu que

$$[p \text{ premier et } 1 < k < p] \implies [P_{p,k} \equiv 0 \pmod{p}] ,$$

une réponse affirmative à la première de ces questions entraînerait de façon immédiate le théorème précédent.

3. Nombre de topologies sur un ensemble de p éléments (p premier).

On sait que le treillis des préordres sur un ensemble E est dual du treillis des topologies sur E [1]. Dénombrer les topologies sur l'ensemble fini E de cardinal n revient donc à rechercher le nombre π_n de préordres sur E .

On a

| $n = \# E$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | ... |
|------------|---|---|----|-----|-------|---------|-----------|-----|
| π_n | 1 | 4 | 29 | 355 | 6.942 | 209.527 | 9.535.241 | ... |

THÉOREME. - $[p \text{ premier}] \Rightarrow [\pi_p \equiv 2 \pmod{p}]$.

Si nous appelons $\pi_{n,k}$ le nombre de préordres à k classes sur un ensemble à n éléments, nous avons

$$\pi_{n,k} = P_{n,k} O_k,$$

et par conséquent

$$\pi_n = \sum_{k=1}^n P_{n,k} O_k.$$

(Se rappeler la décomposition canonique d'un préordre en une équivalence et un ordre quotient.)

Or nous savons déjà que

$$[p \text{ premier et } 1 < k < p] \Rightarrow [P_{p,k} \equiv 0 \pmod{p}]$$

$$[p \text{ premier}] \Rightarrow [O_p \equiv 1 \pmod{p}].$$

Comme $P_{p,1} = P_{p,p} = 1$ et $O_1 = 1$, le théorème est alors évident.

A noter que Louis COMTET [2] a démontré que

$$\lim_{n \rightarrow \infty} \left[\frac{\log(\log \pi_n)}{2 \log n} \right] = 1.$$

(On sait également que si $\text{Re } R = n \rightarrow \infty$, $P_n \sim \exp[n(R + (1/R) - 1) - 1] / \sqrt{R + 1}$ [3].)

4. Considérations générales sur un usage des congruences précédentes.

A partir des dernières formules données (sans démonstration) au §1 avant le théorème 1, on peut retrouver le théorème de von Staudt sur les nombres de Bernoulli.

(Nous utilisons la notation

$$B_1 = \frac{1}{6}, \quad B_2 = \frac{1}{30}, \quad B_3 = \frac{1}{42}, \quad B_4 = \frac{1}{30},$$

$$B_5 = \frac{5}{66} \dots \frac{z}{e^z - 1} = 1 - \frac{z}{2} + \sum_{n=1}^{\infty} ((-1)^{n+1} B_n) / (2n)! z^{2n},$$

où $|z| < 2\pi$.)

Il suffit pour cela de démontrer que

$$B_n = (-1)^n \sum_{k=1}^{2n} ((-1)^{k+1} s_{2n,k}) / (k+1),$$

ce qui est relativement facile.

D'où l'on tire bien

$$\forall n \geq 1, \quad B_n = A_n + (-1)^n \sum \frac{1}{p},$$

