Extrait de « Mathematica & Paedagogia » n° 46.

UNE CONGRUENCE ENTRE COEFFICIENTS MULTINOMIAUX

par P. DELIGNE

Institut des Hautes Études Scientifiques, Bures sur Yvette

Soit p un nombre premier. Pour tout entier $m \neq 0$, on désigne par $v(m)$ l'exposant de la plus haute puissance de p qui divise m. On pose de plus $v(0) = \infty$.

Pour $\mathfrak{n} = (n_1, ..., n_k)$ un k-uple d'entiers $\geqslant 0$, on pose

$$|\mathfrak{n}| = \sum_1^k n_i, \qquad a\mathfrak{n} = (an_1, ..., an_k), \qquad X^{\mathfrak{n}} = \prod_1^k X_i^{n_i}, \qquad \mathfrak{n}! = \prod_1^k n_i!$$

et on désigne par $C(\mathfrak{n})$ le coefficient du monomône $X^{\mathfrak{n}}$ dans

$$(\sum_1^k X_i)^{|\mathfrak{n}|}$$

(coefficients multinômiaux).

On a donc

$$(\sum_1^k X_i)^n = \sum_{|\mathfrak{n}|=n} C(\mathfrak{n}) X^{\mathfrak{n}} \tag{1}$$

$$C(\mathfrak{n}) = \frac{|\mathfrak{n}|!}{\mathfrak{n}!} \tag{2}$$

Pour $k = 2$, ce sont là les coefficients binômiaux.

$$C(n_1, n_2) = \binom{n_1 + n_2}{n_1} \tag{3}$$

PROPOSITION. — *Soient $\mathfrak{n}$ un k-uple d'entiers $\geqslant 0$, et $n = |\mathfrak{n}|$. Si p est un nombre premier $\geqslant 5$, on a*

$$C(p'\mathfrak{n}) \equiv C(\mathfrak{n}) \pmod{p^{v(n)+3}} \tag{4}$$

EXEMPLE. — Pour $p = 5$, $k = 2$, $l = 1$ et $\pi = (1, 1)$, on a

$$\binom{10}{5} = 252 = \binom{2}{1} + 2.5^3$$

PREUVE. — On sait, ou on déduit de (2) que

$$(\sum_1^k X_i)^{p^l} = (\sum_1^k X_i^{p^l}) + pQ \tag{5}$$

où Q est un polynôme à coefficients *entiers*, de degré $< p^l$ en chaque variable. La formule du binôme fournit alors

$$(\sum_1^k X_i)^{p^l.n} = (\sum_1^k X_i^{p^l})^n + \sum_1^n p^i \binom{n}{i} R_i \tag{6}$$

$$R_i = (\sum_1^k x_i^{p^l})^{n-i} \cdot Q^i \tag{7}$$

Pour A et B deux polynômes à coefficients entiers, on écrira $A \doteq B \pmod r$ si les coefficients de $X^{p^l n}$ dans A et B sont congrus modulo r. Avec cette notation, (4) se réécrit

$$(\sum_1^k X_i)^{p^l n} \doteq (\sum_1^k X_i^{p^l})^n \pmod{p^{v(n)+3}} \tag{8}$$

LEMME 1.

$$v\left(\binom{n}{i}\right) \geqslant v(n) - v(i) \tag{9}$$

Faisons agir le groupe additif $\mathbb{Z}/(n)$ sur lui-même par translation (1); si une partie à i éléments P de $\mathbb{Z}/(n)$ a pour stabilisateur (2) un sous-groupe H de $\mathbb{Z}/(n)$ (H.P = P), alors P est réunion de classes latérales de H, et $\# H \mid i$. Le cardinal $r_p = n/\# H$ de l'orbite de P sous $\mathbb{Z}/(n)$, dans $\mathcal{P}(\mathbb{Z}/(n))$, vérifie donc

$$p^{v(n)-v(i)} \mid r_p,$$

d'où, puisque l'ensemble des parties à i éléments de $\mathbb{Z}/(n)$ est somme disjointe d'orbites,

$$p^{v(n)-v(i)} \mid \binom{n}{i}$$

(1) A tout $x \in \mathbb{Z}/(n)$, est donc associée la permutation de $\mathbb{Z}/(n)$ qui applique y sur $x + y$.

(2) Si un groupe G opère dans un ensemble E, le stabilisateur d'une partie P de E est l'ensemble des $g \in G$ pour lesquels P est stable.

LEMME 2. — *Pour $p \neq 2, 3$ et $i \geqslant 3$, on a*

$$p^i \binom{n}{i} \equiv 0 \pmod{p^{v(n)+3}} \tag{10}$$

On a

$$v\left(p^i \binom{n}{i}\right) = i + v\binom{n}{i} \geqslant v(n) + (i - v(i)) \text{ (lemme 1)}$$

Pour $3 \leqslant i < p$, on a $v(i) = 0$ et $i - v(i) \geqslant 3$. Pour $i \geqslant p$, on a $i - v(i) \geqslant i - \log i/\log p$. Cette dernière fonction de i est croissante pour $i \geqslant p$, et vaut $p - 1 \geqslant 3$ pour $i = p$.

LEMME 3. — *Le coefficient de $X^{p^l \mathfrak{n}}$ dans R_1 est nul.*

Aucun des monômes $X^{\mathfrak{r}}$ apparaissant dans Q n'a un exposant $\mathfrak{r}$ divisible par p^l. Le polynôme

$$R_1 = (\sum_1^k X_i^{p^l})^{n-1} \cdot Q$$

hérite de cette propriété.

Il résulte des lemmes 2 et 3 que

$$(\sum_1^k X_i)^{p^l n} \doteq (\sum_1^k X_i^{p^l})^n + \binom{n}{2} p^2 R^2, \quad (\mathrm{mod}\ p^{v(n)+3}) \tag{11}$$

De cette congruence résulte déjà (d'après le lemme) 1 que

$$C(p^l \mathfrak{n}) \equiv C(\mathfrak{n}) \pmod{p^{v(n)+2}} \tag{12}$$

Les seuls monômes $X^{\mathfrak{r}}$ d'exposant divisible par p^l qui figurent dans $(pQ)^2$ sont les monômes

$$X_i^{p^l} \cdot X_j^{p^l} \qquad (i < j)$$

Le coefficient de chacun d'eux est

$$\sum_{i \neq 0, p^l} \binom{p^l}{i}\binom{p^l}{p^l - 1} = \sum \binom{p^l}{i}^2 - 2 = \binom{2p^l}{p^l} - 2 \tag{13}$$

et

$$\binom{2p^l}{p^l} - 2 \equiv \binom{2p}{p} - 2 \pmod{p^3}$$

d'après (12).

On a donc

$$(\sum_1^k X_i)^{p^l.n} \doteq (\sum_1^k X_i^{p^l})^n + \binom{n}{2}\left[\binom{2p}{2} - 2\right] \cdot R_2 \pmod{p^{v(n)+3}}$$

avec R polynôme à coefficients entiers.

Puisque

$$v\left(\binom{n}{2}\right) \geqslant v(n) \text{ (lemme 1)},$$

la proposition résulte du

LEMME 4. — *On a, pour p premier* $\geqslant 5$:

$$\binom{2p}{p} \equiv 2 \pmod{p^3}.$$

On a

$$p^{-1}\binom{p}{i} \equiv (-1)^{i-1} \cdot i^{-1} \pmod{p}$$

pour $1 \leqslant i \leqslant p-1$ et donc

$$p^{-2}\left[\binom{2p}{p} - 2\right] = \sum_1^{p-1} p^{-2}\binom{p}{i}^2 \equiv \sum_1^{p-1} (1/i)^2 \pmod{p} \qquad (14)$$

Définissons

$$z \in \mathbb{Z}/(p) \quad \text{par} \quad z = \sum_{i \in \mathbb{Z}/(p)^*} 1/i^2$$

Pour

$$u \in \mathbb{Z}/(p)^*,$$

on a

$$z = \sum_{i \in \mathbb{Z}/(p)^*} 1/(u^{-1}i)^2 = u^2 z$$

et

$$(u^2 - 1)z = 0.$$

Puisque $p \neq 2, 3$, il existe u tel que $u^2 \neq 1$, et $z = 0$.

La formule (14) se simplifie donc en

$$p^{-2}\left[\binom{2p}{p} - 2\right] \equiv 0 \pmod{p},$$

ce qui achève la démonstration.