

# 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  $\mathbf{n} = (n_1, \dots, n_k)$  un  $k$ -uplet d'entiers  $\geq 0$ , on pose

$$|\mathbf{n}| = \sum_1^k n_i, \quad a\mathbf{n} = (an_1, \dots, an_k), \quad X^{\mathbf{n}} = \prod_1^k X_i^{n_i}, \quad \mathbf{n}! = \prod_1^k n_i!$$

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

$$\left( \sum_1^k X_i \right)^{|\mathbf{n}|}$$

(coefficients multinômiaux).

On a donc

$$\left( \sum_1^k X_i \right)^n = \sum_{|\mathbf{n}|=n} C(\mathbf{n}) X^{\mathbf{n}} \quad (1)$$

$$C(\mathbf{n}) = \frac{|\mathbf{n}|!}{\mathbf{n}!} \quad (2)$$

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

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

**Proposition.**— Soient  $\mathbf{n}$  un  $k$ -uplet d'entiers  $\geq 0$ , et  $n = |\mathbf{n}|$ . Si  $p$  est un nombre premier  $\geq 5$ , on a

$$C(p^l \mathbf{n}) \equiv C(\mathbf{n}) \pmod{p^{v(n)+3}} \quad (4)$$

**Exemple.**— Pour  $p = 5$ ,  $k = 2$ ,  $l = 1$  et  $\mathbf{n} = (1, 1)$ , on a

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

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

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

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

$$\left( \sum_1^k X_i \right)^{p^l \cdot n} = \left( \sum_1^k X_i^{p^l} \right)^n + \sum_1^n p^i \binom{n}{i} R_i \quad (6)$$

avec

$$R_i = \left( \sum_1^k X_i^{p^l} \right)^{n-i} \cdot Q^i \quad (7)$$

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

$$\left( \sum_1^k X_i \right)^{p^l \cdot n} \doteq \left( \sum_1^k X_i^{p^l} \right)^n \pmod{p^{v(n)+3}} \quad (8)$$

**Lemme 1.**

$$v \left( \binom{n}{i} \right) \geq v(n) - v(i) \quad (9)$$

Faisons agir le groupe additif  $\mathbb{Z}/(n)$  sur lui-même par translation<sup>1</sup>; si une partie à  $i$  éléments  $P$  de  $\mathbb{Z}/(n)$  a pour stabilisateur<sup>2</sup> un sous-groupe  $H$  de  $\mathbb{Z}/(n)$  ( $H \cdot P = P$ ), 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,

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

**Lemme 2.** — Pour  $p \neq 2, 3$  et  $i \geq 3$ , on a

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

On a

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

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

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

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

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

hérite de cette propriété.

Il résulte des lemmes 2 et 3 que

$$\left( \sum_1^k X_i \right)^{p^l n} \doteq \left( \sum_1^k X_i^{p^l} \right)^n + \binom{n}{2} p^2 R^2, \pmod{p^{v(n)+3}} \quad (11)$$

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

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

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

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

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

<sup>2</sup>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.

Le coefficient de chacun d'eux est

$$\sum_{i \neq 0, p^l} \binom{p^l}{i} \binom{p^l}{p^l - i} = \sum \binom{p^l}{i}^2 - 2 = \binom{2p^l}{p^l} - 2 \quad (13)$$

et

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

d'après (12).

On a donc

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

avec  $R$  polynôme à coefficients entiers.

Puisque

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

la proposition résulte du

**Lemme 4.** — *On a, pour  $p$  premier  $\geq 5$ :*

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

On a

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

pour  $1 \leq i \leq p-1$ , et donc

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

Définissons  $z \in \mathbb{Z}/(p)$  par

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

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.