

A CONGRUENCE BETWEEN MULTINOMIAL COEFFICIENTS

by P. DELIGNE

Institut des Hautes Études Scientifiques, Bures sur Yvette

Let p be a prime. For every nonzero integer m , let $v(m)$ denote the exponent of the highest power of p dividing m . Set also $v(0) = \infty$.

For a k -tuple $\mathbf{n} = (n_1, \dots, n_k)$ of nonnegative integers, set

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

and denote by $C(\mathbf{n})$ the coefficient of the monomial $X^{\mathbf{n}}$ in

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

(multinomial coefficients).

Thus

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

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

For $k = 2$, these are the binomial coefficients.

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

Proposition.— Let $\mathbf{n}$ be a k -tuple of nonnegative integers, and let $n = |\mathbf{n}|$. If p is a prime ≥ 5 , then

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

Example.— For $p = 5$, $k = 2$, $l = 1$, and $\mathbf{n} = (1, 1)$, one has

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

Proof.— It is known, or follows from (2), that

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

where Q is a polynomial with *integer* coefficients, of degree $< p^l$ in each variable. The binomial formula then gives

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

with

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

For two polynomials A and B with integer coefficients, write $A \doteq B \pmod{r}$ if the coefficients of $X^{p^l \mathbf{n}}$ in A and B are congruent modulo r . With this notation, (4) becomes

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

Lemma 1.

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

Let the additive group $\mathbb{Z}/(n)$ act on itself by translation¹; if an i -element subset P of $\mathbb{Z}/(n)$ has as stabilizer² a subgroup H of $\mathbb{Z}/(n)$ ($H \cdot P = P$), then P is a union of cosets of H , and $\#H \mid i$. The cardinality $r_p = n/\#H$ of the orbit of P under $\mathbb{Z}/(n)$, in $\mathcal{P}(\mathbb{Z}/(n))$, therefore satisfies

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

hence, since the set of i -element subsets of $\mathbb{Z}/(n)$ is a disjoint union of orbits,

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

Lemma 2. — For $p \neq 2, 3$ and $i \geq 3$, we have

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

We have

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

For $3 \leq i < p$, we have $v(i) = 0$ and $i - v(i) \geq 3$. For $i \geq p$, we have $i - v(i) \geq i - \log i / \log p$. This last function of i is increasing for $i \geq p$, and equals $p - 1 \geq 3$ when $i = p$.

Lemma 3. — The coefficient of $X^{p^l \mathbf{n}}$ in R_1 is zero.

None of the monomials $X^{\mathbf{r}}$ occurring in Q has an exponent $\mathbf{r}$ divisible by p^l . The polynomial

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

inherits this property.

It follows from Lemmas 2 and 3 that

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

It already follows from this congruence, by Lemma 1, that

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

The only monomials $X^{\mathbf{r}}$ with exponent divisible by p^l which occur in $(pQ)^2$ are the monomials

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

¹To each $x \in \mathbb{Z}/(n)$ there is thus associated the permutation of $\mathbb{Z}/(n)$ that sends y to $x + y$.

²If a group G acts on a set E , the stabilizer of a subset P of E is the set of $g \in G$ for which P is stable.

The coefficient of each is

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

and

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

by (12).

Thus

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

with R a polynomial with integer coefficients.

Since

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

the proposition follows from

Lemma 4. — *For a prime $p \geq 5$, one has:*

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

One has

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

for $1 \leq i \leq p-1$, and hence

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

Define $z \in \mathbb{Z}/(p)$ by

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

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

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

and

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

Since $p \neq 2, 3$, there exists u such that $u^2 \neq 1$, and $z = 0$. Formula (14) therefore simplifies to

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

which completes the proof.