

CONGRUENCES FOR THE NUMBER OF SUBGROUPS OF ORDER p^k IN A FINITE GROUP

P. DELIGNE

The method used by Serre [1, p. 147] to prove the Sylow theorem gives results more general than that theorem. We spell them out here.

We use the following notation: p denotes a prime number; for every integer n , $v(n)$ is the exponent of the largest power of p dividing n ; finally, G is a finite group of order g .

For completeness, recall the following lemma (Lazard [2, p. 71]).

Lemma 1.

a) If $n = \sum c_i p^i$, with $0 \leq c_i < p$ the base- p expansion of n , then

$$v(n!) = \frac{1}{p-1} \left(n - \sum c_i \right).$$

b)

$$v\binom{r}{s} \geq v(r) - v(s).$$

For a), one has¹

$$v(p^k!) = \sum_{r=1}^k \left\lfloor \frac{p^k}{p^r} \right\rfloor = \sum_{r=1}^k p^{k-r} = \sum_{i=0}^{k-1} p^i = \frac{p^k - 1}{p - 1},$$

which proves the assertion in this case. It is clear that, if $0 \leq c < p$, then $v((cp^k)!) = cv(p^k!)$, and that, if $m < p^{v(n)}$, then

$$v((n+m)!) = v(n!) + v(m!).$$

These additivity properties are the same as those of the right-hand side, whence the formula.

Part b) follows easily by returning to the definitions and taking account of the algorithm which computes the digits c_i of a sum from the digits of its summands. Equality holds when r is a power of p .

Proposition 1.

$$\binom{p^k n}{p^k m} \equiv \binom{n}{m} \pmod{p^{v(n)+2}}$$

if $p \neq 2$, or if n is odd. The congruence is always true modulo $p^{v(n)+1}$.

Proof. Let X and Y be two indeterminates. One has

$$(X + Y)^{p^k} = X^{p^k} + Y^{p^k} + pQ,$$

where Q is a polynomial of degree $< p^k$ in each variable. The binomial formula then gives

$$(1) \quad (X + Y)^{p^k n} = (X^{p^k} + Y^{p^k})^n + np(X^{p^k} + Y^{p^k})^{n-1}Q$$

¹The source's intermediate sum is negative; we replace it by the exact Legendre calculation (source defect R1).

modulo the largest power of p which divides all the numbers $p^i \binom{n}{i}$, $i \geq 2$. These have valuation at least

$$i + v(n) - v(i) \geq v(n) + 2$$

if $p \neq 2$. If $p = 2$, one always has $i > v(i)$ (Cantor), which gives the exponent $v(n) + 1$.

The binomial coefficient $\binom{p^k n}{p^k m}$ is the coefficient of $X^{p^k m} Y^{p^k(n-m)}$.² The second term on the right-hand side of (1) contains no term of this type, since none of its exponents is divisible by p^k . Thus the coefficient of this monomial on the right-hand side of (1) is $\binom{n}{m}$. This proves the assertion when $p \neq 2$. If $p = 2$, the preceding already proves the congruence modulo $2^{v(n)+1}$. In addition, $Q \equiv X^{2^{k-1}} Y^{2^{k-1}} \pmod{2}$, so $Q^2 \equiv X^{2^k} Y^{2^k} \pmod{4}$, and the next term in the binomial expansion gives

$$\binom{2^k n}{2^k m} \equiv \binom{n}{m} + 2n(n-1) \binom{n-2}{m-1} \pmod{2^{v(n)+2}},$$

which gives the asserted improvement when n is odd. $\square$

Theorem.

Let S be a Sylow p -subgroup of G , let $s = v(g)$, and let d_k be the number of subgroups of G of order p^{s-k} , for $0 \leq k \leq s$. Then:

- (i) $d_k \equiv 1 \pmod{p}$;
- (ii) if S is cyclic or abelian of type $(p, \dots, p)$, then d_k is congruent modulo p^{k+1} to the number of subgroups of S of index p^k ;
- (iii) if S is not cyclic, then

$$d_1 \equiv 1 + p \pmod{p^2}.$$

Let G act by left translations on the set of its subsets with p^k elements. If such a subset P of G has stabilizer H , then P is a union of right cosets of H , and hence H is a group of order p^l with $l \leq k$; one has $l = k$ if and only if P is a translate, on the right or on the left, of a subgroup of order p^k . The number of elements in the orbit of P is divisible by p^{s-l} . Therefore $\binom{g}{p^k}$ is congruent modulo p^{s-k+1} to the number of subsets of G which are translates of a subgroup of order p^k . By Proposition 1, it is also congruent to gp^{-k} . There are $d_{s-k} gp^{-k}$ such subsets. Thus

$$gp^{-k} \equiv d_{s-k} gp^{-k} \pmod{p^{s-k+1}},$$

and the first assertion follows.

We now consider case (ii), with S abelian of type $(p, \dots, p)$. Let $G_{i,j}$ be the number of subgroups of order p^i in a subgroup of order p^j ; this is the number of points of a Grassmannian. For $i > j$, $G_{i,j} = 0$; for $i \leq j$,

$$G_{i,j} = \frac{(p^j - 1) \cdots (p^j - p^{i-1})}{(p^i - 1) \cdots (p^i - p^{i-1})} = \tilde{G}_i \tilde{G}_{j-i} \tilde{G}_j^{-1},$$

where

$$\tilde{G}_i = [(1 - p^i) \cdots (1 - p)]^{-1} \quad (i \geq 0), \quad \tilde{G}_i = 0 \quad (i < 0).$$

Here $\tilde{G}_i = (-1)^i G_i$, where the source defines $G_i = [(p^i - 1) \cdots (p - 1)]^{-1}$. This sign normalization leaves $G_{i,j}$ unchanged.³

²The printed source instead has $X^{p^k m} Y^{p^k n}$. For $m > 0$ that monomial has total degree $p^k(m + n) > p^k n$, so its coefficient in $(X + Y)^{p^k n}$ is zero. The displayed $Y^{p^k(n-m)}$ is the source repair recorded as R2 in the editorial register.

³The source later claims $G_k^{-1} \equiv G_{k+1}^{-1} \pmod{p^{k+1}}$, which is false for its printed definition. The displayed normalization gives $\tilde{G}_{k+1}^{-1} = \tilde{G}_k^{-1}(1 - p^{k+1})$ and repairs the argument exactly (source defect A1).

We know that p^i divides the number u_i of subsets of G with p^s elements whose stabilizer has order p^{s-i} . Put $g = p^s h$. Counting in two ways the pairs formed by a subgroup of order p^{s-i} and a subset with p^s elements fixed by it gives, for $0 \leq i, j \leq s$,

$$(2) \quad d_i \binom{p^i h}{p^i} = \sum_j G_{s-i, s-j} u_j,$$

$$(3) \quad p^i \mid u_i,$$

$$(4) \quad d_s = 1.$$

Now work in the localization of $\mathbf{Z}$ at p , or in $\mathbf{Z}_p$. Let e_i be the quotient of the left-hand side of (2) by $\binom{p^s h}{p^s} \tilde{G}_i$. By Proposition 1, and since $\tilde{G}_i$ is prime to p for $i \geq 0$, there are numbers v_i , $0 \leq i \leq s$, such that

$$(5) \quad d_i \equiv \tilde{G}_i e_i \pmod{p^{i+1}},$$

$$(2') \quad e_i = \sum_j \tilde{G}_{i-j} v_j,$$

$$(6) \quad p^i \mid v_i,$$

$$(7) \quad e_s = \tilde{G}_s^{-1}.$$

Analogous identities hold in the group S . To show that they determine d_i modulo p^{i+1} , it is enough to check that the identities

$$(8) \quad e_i = \sum_j \tilde{G}_{i-j} v_j,$$

$$(9) \quad p^i \mid v_i,$$

$$(10) \quad e_s = 0$$

for $0 \leq i, j \leq s$ imply $p^{i+1} \mid e_i$.

From (2'') one obtains

$$e_i - e_{i+1} = \sum_j (\tilde{G}_{i-j} - \tilde{G}_{i+1-j}) v_j.$$

Since $\tilde{G}_k^{-1} \equiv \tilde{G}_{k+1}^{-1} \pmod{p^{k+1}}$, one also has

$$p^{i+1-j} \mid \tilde{G}_{i-j} - \tilde{G}_{i+1-j}, \quad p^{i+1} \mid e_i - e_{i+1}.$$

The conclusion follows from (4'').

The same technique, in a simpler form, applies when S is cyclic.

We turn to case (iii). The subgroups of S of index p are all normal. Their intersection S' is the Frattini subgroup of S . For every subgroup T of S , if $TS' = S$, then $T = S$. In particular, if S is not cyclic, then S/S' is not cyclic either, and the subgroups of S of index p are identified with the hyperplanes of a vector space over $\mathbf{Z}/p$ of dimension > 1 ; their number is congruent to $1 + p \pmod{p^2}$.

The preceding equations leave the following system.⁴

$$\begin{cases} d_0 h = u_0, \\ d_1 \binom{ph}{p} = (1+p)u_0 + u_1 \pmod{p^2}, \\ \binom{p^s h}{p^s} = u_0 + u_1 \pmod{p^2}. \end{cases}$$

By Proposition 1, $\binom{p^s h}{p^s} \equiv \binom{ph}{p} \equiv h \pmod{p^2}$. Hence

$$\begin{aligned} d_1 h &\equiv (1+p)d_0 h + (h - d_0 h) \pmod{p^2}, & \text{and} \\ d_1 &\equiv 1 + p d_0 \pmod{p^2}. \end{aligned}$$

The assertion follows because $d_0 \equiv 1 \pmod{p}$.

REFERENCES

- [1] SERRE, J.-P., *Corps locaux. Act. sc. et ind.* Hermann, 1962.
- [2] LAZARD, M., Groupes analytiques p -adiques. *Publ. Math. I.H.E.S.*, no. 26, 1965.

⁴In its third line the source prints the lower argument p ; the next source line itself uses p^s . We restore p^s here (source defect R3). The final subscript after u is damaged in the scan; the counting identities force the intended right-hand side $u_0 + u_1$.