CONGRUENCES SUR LE NOMBRE DE SOUS-GROUPES D'ORDRE p^k DANS UN GROUPE FINI

par P. DELIGNE

La méthode utilisée par Serre [1] p. 147 pour démontrer le théorème de Sylow fournit des résultats plus généraux qu'on se propose d'expliciter.

On utilise les notations suivantes : p désigne un nombre premier ; pour tout entier n, $v(n)$ est l'exposant de la plus grande puissance de p qui divise n ; enfin, G est un groupe fini d'ordre g.

Pour être complet, rappelons le lemme suivant (Lazard [2] p. 71).

Lemme 1 :

a) *Si* $n = \Sigma c_i p^i$ *avec* $0 \leqslant c_i < p$ (*développement de base* p),

$$v(n!) = \frac{1}{p-1}(n - \Sigma c_i)$$

b) $v\binom{r}{s} \geqslant v(r) - v(s)$

Prouvons, *a*), $v(p^k!) = \sum_{i<k} i.(p^{k-i} - p^{k-i+1}) = \sum_{i=0}^{k-1} p^i = \frac{p^k - 1}{p-1}$, ce qui vérifie l'énoncé ; il est clair que si $0 \leqslant c < p$, $v((cp^k)!) = cv(p^k!)$ et que si $m < p^{v(n)}$, $v((n+m)!) = v(n!) + v(m!)$. Ces propriétés d'additivité sont les mêmes que celles du second membre, d'où la formule.

b) s'en déduit aisément en revenant aux définitions et en tenant compte de l'algorithme de calcul des chiffres c_i d'une somme à l'aide de ceux de ses termes. Il y a égalité si r est une puissance de p.

Proposition 1 : $\binom{p^k n}{p^k m} = \binom{n}{m}$ mod. $p^{v(n)+2}$ *si* $p \neq 2$ *ou si* n *est impair. La congruence est toujours vraie modulo* $p^{v(n)+1}$.

Démonstration : Soient X et Y deux indéterminées ; $(X + Y)^{p^k} = X^{p^k} + Y^{p^k} + pQ$ où Q est un polynôme de degré inférieur à p^k en chaque variable. La formule du binôme montre alors que

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

modulo la plus grande puissance de p qui divise tous les $p^i\binom{n}{i}$ ($i \geqslant 2$). Ceux-ci sont de valuation au moins $i + v(n) - v(i) \geqslant v(n) + 2$ si $p \neq 2$; si $p = 2$, on a toujours $i > v(i)$ (Cantor), d'où l'exposant $v(n) + 1$. $\binom{p^k n}{p^k m}$ est le coefficient de $X^{p^k m}Y^{p^k n}$; le second terme du second membre de (1) ne contient aucun terme de ce type (aucun exposant n'y est divisible par p^k), et le coefficient de ce monôme dans le second membre de (1) est donc $\binom{n}{m}$. L'assertion en résulte si $p \neq 2$. Si $p = 2$, ce qui précède prouve déjà $Q = X^{2^{k-1}}Y^{2^{k-1}} \bmod 2$; $Q^2 = X^{2^k}Y^{2^k} \bmod 4$, et le terme suivant dans le développement du binôme donne $\binom{2^k n}{2^k m} = \binom{n}{m} + 2n(n-1)\binom{n-2}{m-1} \bmod 2^{v(n)+2}$, d'où l'assertion.

THÉORÈME :

Soient S *un sous-groupe de* p- *Sylow de* G, $s = v(g)$ et d_k *le nombre de sous-groupes de* G *d'ordre* p^{s-k} *pour* $0 \leqslant k \leqslant s$. *Alors*

(i) $d_k = 1 \bmod p$

(ii) *si* S *est cyclique* ou *abélien de type* (p, ..., p), d_k *est congru* mod p^{k+1} *au nombre de sous-groupes de* S *d'indice* p^k

(iii) *si* S *n'est pas cyclique,*

$$d_1 = 1 + p \bmod p^2.$$

Faisons agir le groupe G par translations à gauche sur l'ensemble de ses parties à p^k éléments. Si une de ces parties soit P de G a un stabiliseur H, elle est réunion de classes à droites de H et H est donc un groupe d'ordre p^l avec $l \leqslant k$; $l = k$ si et seulement si P est translaté (à droite ou à gauche, c'est la même chose) d'un sous-groupe d'ordre p^k. Le nombre d'éléments dans l'orbite de P est divisible par p^{s-l}. $\binom{g}{p^k}$ est donc congru mod

p^{s-k+1} au nombre de parties de G translatées d'un sous-groupe d'ordre p^k, et on sait (prop. 1) qu'il est aussi congru à gp^{-k}. Il y a $d_{s-k}.g.p^{-k}$ telles parties, et $gp^{-k} = d_{s-k}gp^{1-k} \bmod p^{-k+1}$ d'où la première assertion.

Plaçons-nous dans le cas (*ii*), avec S abélien de type $(p \dots p)$. Le nombre G_{ij} de sous-groupes d'ordre p^i d'un sous-groupe d'ordre p^j est le nombre d'éléments d'une grassmannienne. Pour $i > j$, $G_{ij} = 0$; pour $i \leqslant j$,

$$G_{ij} = \frac{(p^j - 1) \dots (p^j - p^{i-1})}{(p^i - 1) \dots (p^i - p^{i-1})} = G_i G_{j-i} G_j^{-1}, \text{ où on pose}$$

$$G_i = [(p^j - 1) \dots (p - 1)]^{-1} \text{ si } i \geqslant 0, \; G_i = 0 \text{ si } i < 0.$$

On sait que p^i divise le nombre u_i de parties de G à p^s éléments dont le stabiliseur est d'ordre p^{s-i}. Posons $g = p^s h$; si on compte de deux façons différentes le nombre des couples formés d'un sous-groupe d'ordre p^{s-i} et d'une partie à p^s éléments qu'il laisse fixe, on trouve, pour $0 \leqslant i, j \leqslant s$,

$$\left\{ \begin{array}{ll} d_i \binom{p^s h}{p^i} = \sum_j G_{s-i,s-j} u_j & (2) \\ p^i \mid u_i & (3) \\ d_s = 1 & (4) \end{array} \right.$$

Travaillons maintenant dans le localisé de $\mathbf{Z}$ en p (ou dans $\mathbf{Z}_p$). Soit e_i le quotient par $\binom{p^s h}{p^s} G_i$ du premier membre de (2). En vertu de la proposition 1 et du fait que G_i est premier avec p pour $i \geqslant 0$, on voit qu'il existe des nombres $v_i (0 \leqslant i \leqslant s)$ tels que

$$\left\{ \begin{array}{ll} d_i = G_i e_i \bmod p^{i+1} & (5) \\ e_i = \sum_j G_{i-j} v_j & (2') \\ p^i \mid v_i & (3') \\ e_s = G_s^{-1} & (4') \end{array} \right.$$

Des identités analogues sont vérifiées dans le groupe S ; pour montrer qu'elles déterminent $d_i \bmod p^{i+1}$, il suffit de vérifier que les identités (pour $0 \leqslant i, j \leqslant s$)

$$\begin{cases} e_i = \Sigma\, G_{i-j} v_j & (2'') \\ p^i \mid v_i & (3'') \\ e_s = 0 & (4'') \end{cases}$$

impliquent que $p^{i+1} \mid e_i$.
De $(2'')$ on tire

$$e_i - e_{i+1} = \Sigma\,(G_{i-j} - G_{i+1-j}) v_j$$

Comme trivialement $G_k^{-1} = G_{k+1}^{-1} \bmod p^{k+1}$, on a aussi

$$p^{i+1-j} \mid G_{i-j} - G_{i+1-j} \text{ et } p^{i+1} \mid e_i - e_{i+1}.$$

On conclut par $(4'')$.

La même technique, en plus simple, s'applique si S est cyclique.

Passons au cas (*iii*). Les sous-groupes d'indice p de S sont tous distingués. Leur intersection S′ est le sous-groupe de Fratini de S. Pour tout sous-groupe T de S, si TS′ = S, alors T = S. En particulier, si S n'est pas cyclique, S/S′ ne l'est pas non plus et les sous-groupes d'indice p de S s'identifient aux hyperplans d'un $\mathbf{Z}/p$-vectoriel de dimension > 1 ; leur nombre est congru à $1 + p \bmod p^2$.

Des équations précédentes subsiste

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

Or (prop. 1), $\binom{p^s h}{p^s} = \binom{ph}{p} = h \bmod p^2$, donc

$$d_1 h = (1+p) d_0 h + (h - d_0 h) \bmod p^2 \text{ et}$$

$$d_1 = 1 + p d_0 \bmod p^2,$$

d'où l'assertion puisque $d_0 = 1 \bmod p$.

BIBLIOGRAPHIE

[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.*, n° 26, 1965.