Atti Accademia Nazionale Lincei Classe Scienze Fisiche Matematiche Naturali

Rendiconti Lincei
Matematica e Applicazioni

Yakov Berkovich

On the number of solutions of equation $x^{p^k} = 1$ in a finite group

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni, *Serie 9*, Vol. **6** (1995), n.1, p. 5–12.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLIN_1995_9_6_1_5_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni, Accademia Nazionale dei Lincei, 1995.

Rend. Mat. Acc. Lincei
s. 9, v. 6:5-12 (1995)

Teoria dei gruppi. — *On the number of solutions of equation $x^{p^k} = 1$ in a finite group.*
Nota di Yakov Berkovich, presentata (*) dal Socio G. Zappa.

Abstract. — Theorem A yields the condition under which the number of solutions of equation $x^{p^k} = 1$ in a finite p-group is divisible by p^{n+k} (here n is a fixed positive integer). Theorem B which is due to Avinoam Mann generalizes the counting part of the Sylow Theorem. We show in Theorems C and D that congruences for the number of cyclic subgroups of order p^k which are true for abelian groups hold for more general finite groups (for example for groups with abelian Sylow p-subgroups).

Key words: Finite groups; p-subgroups; p-elements.

Riassunto. — *Sul numero delle soluzioni dell'equazione $x^{p^k} = 1$ in un gruppo finito.* Il Teorema A fornisce condizioni per cui il numero delle soluzioni dell'equazione $x^{p^k} = 1$ in un gruppo finito è divisibile per p^{n+k} dove n è un fissato intero positivo. Il Teorema B, che è dovuto a Avinoam Mann, è una generalizzazione del teorema di Sylow. Si prova nei teoremi C e D che le congruenze relative al numero dei sottogruppi ciclici di ordine p^k note per i gruppi abeliani valgono in effetti per classi più ampie di gruppi finiti, ad esempio per gruppi a sottogruppi di Sylow abeliani.

1. Introduction

Denote by $N(t, G)$ the number of solutions of $x^t = 1$ in a finite group G. If $t \mid |g|$ then $t \mid N(t, G)$ (Frobenius). But in some cases (see for example Theorems A, C) we can say considerably more about the number $N(t, G)$.

A p-group G is said to be an $L_{n,k}$-group (n, k are positive integers) if $\Omega_1(G) = \langle x \in G \mid x^p = 1\rangle$ is of order p^n and exponent p, $G/\Omega_1(G)$ is cyclic and $\exp G \geq p^k$.

A 2-group G is said to be a $U_{n,k}$-group if it satisfies the following conditions:

(U1) G contains a normal elementary abelian subgroup R of order 2^n;

(U2) G/R is of maximal class, $\exp G \geq 2^k$;

(U3) if T/R is a cyclic subgroup of index 2 in G/R then $\Omega_1(T) = R$ (obviously R is the only normal elementary abelian subgroup of order 2^n in G).

Note that $L_{n,k}$-group and $U_{2,k}$-groups were introduced in [2]. Obviously $U_{1,k}$-groups are 2-groups of maximal class.

A subgroup H of a p-group G, $\exp G \geq p^k$, is said to be k-good if $\exp \Omega_1(\langle x, H\rangle) = p$ for any element x of order p^k in G. Notice that a k-good subgroup is $(k+1)$-good but the converse is not true. If H is k-good in G and $H \leq F \leq G$ then H is k-good in F. Obviously $\Omega_1(G)$ is k-good if G is an $L_{n,k}$-group for any k, or $U_{n,k}$-group for $k > 2$. Moreover $N(p^k, G) \equiv p^{n+k-1} \pmod{p^{n+k}}$ if G is a $L_{n,k}$-group for any k, or $U_{n,k}$-group for $k > 2$. Next if H is k-good in G and $A \leq H$ then A is k-good in G as well. As rule we consider only normal k-good subgroups of exponent p.

(*) Nella seduta del 16 giugno 1994.

2. The number of cyclic subgroups in a p-group

In this section we prove the following

Theorem A. *Let $n > 1$, $k > 2$ be positive integers. Suppose that a p-group G contains a k-good normal subgroup of order p^n and exponent p. Then if G is not an $L_{n,k}$ – or a $U_{n,k}$ –group and* $\exp G \geqslant p^k$ *then* $N(p^k, G) \equiv 0 \pmod{p^{n+k}}$.

Proof. Suppose that G is a counterexample of minimal order. Take in G a k-good normal subgroup R of order p^n and exponent p.

(*i*) Suppose that G/R is cyclic. Since G is not an $L_{n,k}$-group and $\exp \Omega_1(G) = p$ (in fact $\Omega_1(G) \leqslant RC$ where C is a cyclic subgroup of order p^k in G, and R is k-good) then $|\Omega_1(G)| = p^{n+1}$. Hence $N(p^k, G) = |\Omega_k(G)| = p^{n+k}$ – a contradiction. Thus G/R is not cyclic.

(*ii*) Suppose that G/R is a 2-group of maximal class. Take in G/R a cyclic subgroup T/R of index 2. Since G is not a $U_{n,k}$-group then $\Omega_1(T)$ is of order 2^{n+1} and exponent 2 for some choice of T (if G/R is the ordinary quaternion group then it contains three cyclic subgroups of index 2). It follows from the structure of G/R that all elements from $G - T$ satisfy $x^8 = 1$. Since $k > 2$ one has $N(2^k, G) = N(2^k, T) + |G - T|$. By the above $N(2^k, T) = 2^{n+k}$. Since $|G - T| = |T| = |G|/2$ is divisible by 2^{n+k} (in fact, $|G| = |R|\,|G/R| \geqslant 2^n 2^{1+k} = 2^{n+k+1}$) then 2^{n+k} divides $N(2^k, G)$ – a contradiction. Thus G/R is not a 2-group of maximal class.

It follows from (*i*) that G/R contains a normal subgroup H/R such that G/H is abelian of type (p, p). Let $G_1/R, \ldots, G_{p+1}/R$ be all subgroups of order p in G/R. It is easy to check that the following equality holds:

$$(*) \qquad N(p^k, G) = N(p^k, G_1) + \ldots + N(p^k, G_{1+p}) - pN(p^k, H).$$

Since $|G| \geqslant p^{n+k}$ we may assume without loss of generality that $\exp G \geqslant p^{k+1}$. Then $|G| \geqslant p^{n+k+1}$, $|H| \geqslant p^{n+k-1}$. Since R is k-good in H then $p^{n+k} \mid pN(p^k, H)$ (in fact this is true if H is an $L_{n,k}$- or $U_{n,k}$-group, in the contrary case this follows by induction). Therefore by assumption $p^{n+k} \nmid N(p^k, G_i)$ for some i. By induction G_i is an $L_{n,k}$-group or a $U_{n,k}$-group.

Suppose that G_i is an $L_{n,k}$-group. Since G/R is not a 2-group of maximal class we may assume that $G_1/R, \ldots, G_p/R$ are cyclic, and G_{p+1}/R is non-cyclic abelian with cyclic subgroup of index p (this follows from the classification of p-groups with a cyclic subgroup of index p; it is important that $k > 2$). In particular $i \leqslant p$. Set $S_t = \Omega_1(G_t)$, $t \in \{1, \ldots, p\}$. Since $S_t/R \leqslant \Phi(G_t/R) \leqslant \Phi(G/R) < G_i/R$ then $S_t = S_i = R$ (here $\Phi(G)$ is the Frattini subgroup of G). Hence $G_1, \ldots, G_p$ are $L_{n,k}$-groups. Then by the above $N(p^k, G_t) = p^{n+k-1}$, $t \in \{1, \ldots, p\}$. By induction $N(p^k, G_{p+1}) \equiv 0 \pmod{p^{n+k}}$. Now $(*)$ implies $p^{n+k} \mid N(p^k, G)$ – a contradiction.

Therefore G_i is a $U_{n,k}$-group. We may suppose that $i = 1$. Take in G_1/R a cyclic subgroup T_1/R of index 2. By definition $\Omega_1(T_1) = R$. By supposition $|G/R| \geqslant 2^{k+1} > 8$. As G/R is not a 2-group of maximal class (by (*ii*)) it contains [3] exactly four subgroups of maximal class and index 2: $G_1/R, \dots, G_4/R$. Let T_j/R be a cyclic subgroup of index 2 in G_j/R $(j \leqslant 4)$. If $S_j = \Omega_1(T_j)$ then as above $S_j < T_1$ so $S_j = R$ for $j \leqslant 4$. Thus G_j is a $U_{n,k}$-group for $j \leqslant 4$ and $N(p^k, G_j) = 2^{n+k-1} + |G|/4$ $(j \leqslant 4)$. If M/R is a maximal subgroup of G/R distinct from G_j/R $(j \leqslant 4)$ then by induction $2^{n+k} | N(2^k, M)$. Then $(*)$ implies $N(2^k, G) \equiv 0 \pmod{2^{n+k}}$ and the theorem is proved. ∎

Remark. If G is not cyclic and is not a 2-group of maximal class it contains a normal subgroup R of type (p, p). Obviously R is k-good for any $k > 2$ (but in general it is not 2-good). Hence the main result of [2] for $p = 2$ is a corollary of Theorem A.

Denote by $c_k(G)$ the number of cyclic subgroups of order p^k in a group G. Obviously $c_k(G) = (N(p^k, G) - N(p^{k-1}, G))/p^{k-1}(p-1)$. But it is impossible to apply this formula for proof of the following

Corollary 1. *If G satisfies the condition of Theorem* A *and G is not an $L_{n,k}$- or a $U_{n,k}$-group then $c_k(G) \equiv 0 \pmod{p^n}$.*

It is sufficient to repeat the proof of Theorem A. ∎

Corollary 2 [2]. *Suppose that an irregular p-group G is not a group of maximal class, $k > 2$. If G is not an $L_{p,k}$- or $U_{p,k}$-group then $c_k(G) \equiv 0 \pmod{p^p}$.*

Proof. Take in G a normal subgroup R of order p^p and exponent p [4]. By virtue of Theorem A it suffices to show that R is k-good for $k > 2$. Take in G an element x of order p^k, set $H = \langle x, R\rangle$. Then H/R is cyclic and $|H/R| > p$. Take in H a normal subgroup D of order p^{p-2} such that $D < R$. Let $R < S < H$ such that $|S : R| = p$. Then S/D is abelian so its class is less than p and S is regular. Since $\Omega_1(H) = \Omega_1(S)$ then $\exp \Omega_1(H) = p$ and R is k-good. So Theorem A implies the result. ∎

Corollary 3. *Let a p-group G contains a 2-good normal subgroup R of order $p^n > p$ and exponent p. Then $N(p, G) \equiv 0 \pmod{p^n}$.*

Proof. If x is an element of order p in $G - R$ then $\langle x, R\rangle$ does not contain a cyclic subgroup of order p^2 (since R is 2-good). So the set of all solutions of $y^p = 1$ is a disjoint union of subgroups $\langle x, R\rangle$ for appropriate elements x of order p in $G - R$ (if $G - R$ does not contain elements of order p then $N(p, G) = |R| = p^n$). ∎

3. The theorem of Avinoam Mann

Let θ be a class of finite groups. Denote by $n_\theta(G)$ the number of θ-subgroups in a group G.

A. Kulakoff proved that if G is a non-cyclic p-group of order p^n, $p > 2$, and $k \in \{1, \dots, n-1\}$ then $s(p^k, G) \equiv 1 + p \pmod{p^2}$; here $s(p^k, G)$ is the number of subgroups of order p^k in G. The same assertion holds for 2-group G unless it is not cyclic or a 2-group of maximal class [1]. The following theorem which is due to A. Mann permits to transfer some counting theorems from p-groups onto arbitrary finite groups.

THEOREM B. (A. Mann, *Counting p-subgroups,* unpublished manuscript). *Let θ be a class of p-groups of fixed order, let S be a Sylow p-subgroup of G, and assume that any θ-group* M *satisfies* $|M| < |S|$. *Suppose that* $n_\theta(S) \equiv n_\theta(Q) \pmod p$ *for all maximal subgroups Q of S. Then* $n_\theta(G) \equiv n_\theta(S) \pmod{p^2}$.

PROOF. We may assume that all θ-groups are non-identity.

Let $\mathfrak{M}$ be the set of all θ-subgroups of G which are not contained in S.

Consider the action of S on $\mathfrak{M}$ by conjugations. Then the length of an S-orbit equals to p^t for an appropriate positive integer t. Obviously $N_S(A) \neq S$ for any $A \in \mathfrak{M}$. Denote by $\mathfrak{M}_0$ the union of all S-orbits of length p. It is sufficient to show that $|\mathfrak{M}_0| \equiv 0 \pmod{p^2}$. Take $A \in \mathfrak{M}_0$ and set $N_S(A) = Q$. Then $|S:Q| = p$, *i.e.* Q is maximal in S, so by condition $n_\theta(Q) \equiv n_\theta(S) \pmod p$. Denote by $t(Q)$ the number of all elements of $\mathfrak{M}_0$ which are normalized by Q. Note that any element of $\mathfrak{M}_0$ is normalized by exactly one maximal subgroup of S (if X and V, distinct maximal subgroups of S, normalize $A \in \mathfrak{M}_0$ then $\langle X, V\rangle = S$ normalizes A – a contradiction). Therefore $|\mathfrak{M}_0| = \sum t(Q)$ where Q runs over the set of all maximal subgroups of S. If $t(Q) \equiv 0 \pmod{p^2}$ for all maximal in S subgroups Q then $|\mathfrak{M}_0| \equiv 0 \pmod{p^2}$. Let A, Q are taken as before, $T_1 = AQ$. Then $T_1 \in \mathrm{Syl}_p(G)$, A is normal in T_1 and $N_S(T_1) = Q = S \cap T_1$. Let $\{T_1, \dots, T_n, S = T_0\} = \mathrm{Syl}_p(N_G(Q))$. If $B \in \mathfrak{M}_0$ and $N_S(B) = Q$ then $BQ \in \{T_1, \dots, T_n\}$, say $BQ = T_i$. Denote by $m(T_i)$ the number of all elements of $\mathfrak{M}_0$ which are normal in T_i; if B_0 is one of them then $B_0 Q = T_i$ is that element of the set $\{T_1,, \dots, T_n\}$ which contains B_0. Hence $t(Q) = \sum_{i=1}^{n} m(T_i)$. Obviously $m(T_i) \equiv n_\theta(T_i) - n_\theta(Q) \pmod p$ (if $B \in \mathfrak{M}_0$ and $B < T_i$ is not normal in T_i then p divides the number of T_i-conjugates of B; hence the number of such B in T_i is divisible by p). Therefore $p \mid m(T_i)$. Because $N_S(T_i) = Q$ for $i \in \{1, \dots, n\}$ then any S-orbit of the set $\{T_1, \dots, T_n\}$ is of length p. If $\{T_1, \dots, T_p\}$ is such an S-orbit then in view of $m(T_1) = \dots = m(T_p)$ one has $m(T_1) + \dots + m(T_p) = pm(T_1) \equiv 0 \pmod{p^2}$. Summing over all S-orbits of the set $\{T_1, \dots, T_n\}$ one obtains $t(Q) \equiv 0 \pmod{p^2}$, and the theorem is proved (since Q is an arbitrary maximal subgroup of S). ■

COROLLARY 1. *If* $S \in \mathrm{Syl}_p(G)$, $|S| > p^k \geqslant p$ *then the following assertions are equivalent*:

(a) $s(p^k, G) \not\equiv 1 + p \pmod p$,

(b) $s(p^k, G) \equiv 1 \pmod{p^2}$,

(c) *S is either a 2-group of maximal class with* $|S| > 2^{k+1}$, *or S is a cyclic group*.

PROOF. If $S \in \mathrm{Syl}_p(G)$, G is a group from (b), then $s(p^k, S) \equiv 1 \pmod{p^2}$ by Theorem B, and (*a*), (*c*) are true by Kulakoff's Theorem and [1]. Similarly one proves the remaining implications. For example, if S is not a 2-group of maximal class and is not cyclic then $s(p^k, G) \equiv s(p^k, S) \equiv 1 + p \pmod{p^2}$ by [1], Kulakoff's Theorem and Theorem B. ■

Suppose that a p-group G is not cyclic and is not a 2-group of maximal class. If $k > 1$ then $c_k(G) \equiv 0 \pmod p$. This result for $p > 2$ is due to G. A. Miller, and for $p = 2$ to the author [1].

COROLLARY 2. *Let $S \in \mathrm{Syl}_p(G)$. Suppose that S does not contain as a maximal subgroup a cyclic group or 2-group of maximal class. Then $c_k(G) \equiv c_k(S) \pmod{p^2}$ for $k > 1$.*

PROOF. In fact if Q is a maximal subgroup of S then p divides $c_k(S) - c_k(Q)$ by [1] and Miller's Theorem. Now the result follows from Theorem B. ■

As, in Corollary 2, $c_k(G) \equiv c_k(S) \pmod p$ then $c_k(G) \equiv 0 \pmod p$ if S is noncyclic and is not a 2-group of maximal class, $k > 1$.

Corollary 1 was proved by P. Deligne [5] for $|S| = p^{k+1}$, and by M. Herzog [6] for $k = 1$.

4. THE NUMBER OF CYCLIC SUBGROUPS IN A GROUP WITH ABELIAN SYLOW SUBGROUPS

In this section we consider the number of cyclic subgroups of given order in finite groups with Sylow subgroups satisfying certain special conditions.

THEOREM C. *Let $S \in \mathrm{Syl}_p(G)$, $\Omega_1(S)$ is abelian of order p^n. Then $c_1(G) \equiv 1 + p + \dots + p^{n-1} \pmod{p^n}$.*

PROOF. Obviously $\Omega_1(S)$ is elementary abelian.

Denote by $\mathfrak{M}$ the set of all subgroups of order p in G which are not contained in S. Consider, as in the proof of Theorem B, the action of $R = \Omega_1(S)$ on $\mathfrak{M}$ by conjugations. The length of an R-orbit is equal to a power of p. Let $\mathfrak{M}_0 = \{C \in \mathfrak{M} \mid |R : N_R(C)| < p^n\}$. It suffices to prove that $p^n \mid |\mathfrak{M}_0|$.

Set $\mathfrak{N} = \{N_R(C) \mid C \in \mathfrak{M}_0\}$. By definition of $\mathfrak{N}_0$ all elements of the set $\mathfrak{N}$ are nontrivial subgroups of R. We prove that any $Q \in \mathfrak{N}$ normalizes sp^n elements of the set $\mathfrak{M}_0$, s is a non-negative integer. Let $C \in \mathfrak{N}_0$, $Q = N_R(C)$. Then $T_1 = QC = Q \times C$, $|R : Q| = p^r$ $(0 < r < n)$.

In particular $N_R(C) = C_R(C)$. Take $x \in N_R(T_1)$. Since $\langle x, T_1 \rangle$ is contained in a Sylow p-subgroup of G then $\langle x, T_1 \rangle$ is elementary abelian (it is generated by elements of order p). In particular x centralizes C whence $x \in Q$. Therefore $Q = N_R(T_1) = T_1 \cap R$. Now if $x \in T_1 - Q$ then $C_R(x) \geq Q > 1$, *i.e.* $\langle x \rangle \in \mathfrak{M}_0$. We prove that $C_R(x) = Q$. We have $x = yz$ where $C = \langle y \rangle$, $z \in Q$. If $u \in C_R(x)$ then $u \in C_R(y) = Q$, hence $C_R(x) = Q$ for any $x \in T_1 - Q$. Let $\{T_1, \dots, T_m\}$ be the R-orbit of T_1, $m = |R : Q| = p^r$. Obviously $T_i \cap T_j = Q = N_R(T_j) = T_j \cap R$ for $i \neq j$, $i, j \in \{1, \dots, m\}$. By the above $|Q| = p^{n-r}$. Since $|T_1| = p|Q| = p^{n-r+1}$ then T_1 contains exactly $c_1(T_1) - c_1(Q) = p^{n-r}$ elements of the set $\mathfrak{M}$ (moreover by the above these elements are contained in $\mathfrak{M}_0$). The same is true for any subgroup $T_2, \ldots, T_m$. Therefore the subgroups $T_1, \ldots, T_m$ together contain exactly $mp^{n-r} = p^r p^{n-r} = p^n$ elements of the set $\mathfrak{M}_0$ (denote the set of such elements by $\mathfrak{M}_1$). By the above $|\mathfrak{M}_1| = p^n$.

Set $\mathfrak{M}_Q = \{C \in \mathfrak{M}_0 \mid N_R(C) = Q\}$. Assume $\mathfrak{M}_Q \neq \mathfrak{M}_1$; take $C \in \mathfrak{M}_Q - \mathfrak{M}_1$. Then $U_1 = CQ \notin \{T_1, \ldots, T_m\}$. For $\{U_1, \ldots, U_{m(1)}\}$, the R-orbit of U_1, set $\mathfrak{M}_2 = \{C \in \mathfrak{M}_0 \mid C \leqslant U_i, i \in \{1, \ldots, m(i)\}\}$. Then $\mathfrak{M}_1 \cap \mathfrak{M}_2$ is empty (since $T_i \cap U_j = Q$ for all i, j) and $|\mathfrak{M}_2| = p^n$. Continuing so further we present $\mathfrak{M}_Q$ in a disjoint union of sets of length p^n. Hence $p^n \mid |\mathfrak{M}_Q|$.

Then we have by the above the following partition $\mathfrak{M}_0 = \bigcup_{1 \neq Q \in \mathfrak{N}} \mathfrak{M}_Q$ (see definition of the set $\mathfrak{N}$). Therefore $p^n \mid |\mathfrak{M}_0|$, and the theorem is proved. ■

Remark. If S in Theorem C is elementary abelian then the result follows from the Frobenius Theorem since $N(p, G) = N(|S|, G)$.

Corollary. *If* $S \in \mathrm{Syl}_p(G)$, $\Omega_1(S) \leqslant Z(S)$ *(in particular if S is abelian) and* $|\Omega_1(S)| = p^n$ *then* $p^n \mid N(p, G)$.

In the same manner we prove the following

Theorem D. *Let* $S \in \mathrm{Syl}_p(G)$, $k > 1$ *be an integer,* $\exp S \geqslant p^k$. *If* $\Omega_{k-1}(S) \leqslant Z(\Omega_k(S))$ *and* $|\Omega_{k-1}(S)| = p^n$ *then* $c_k(G) \equiv 0 \pmod{p^{n-k+1}}$.

Proof. Set $R = \Omega_{k-1}(S)$. Then R is abelian of exponent p^{k-1} and order p^n. If S is abelian then $\exp \Omega_k(S)/\Omega_{k-1}(S) = p$.

First we prove that $c_k(S) \equiv 0 \pmod{p^{n-k+1}}$. Let C be a cyclic subgroup of order p^k in S. Then CR is abelian and $|CR : R| = p$. So $c_k(CR) = (|CR| - |R|)/p^{k-1}(p-1) = p^{n-k+1}$. If C_1 is a cyclic subgroup of order p^k in S, C_1 is not contained in CR then $CR \cap C_1 R = R$ and $C_1 R$ contains exactly p^{n-k+1} cyclic subgroups of order p^k. Hence the set of all cyclic subgroups of order p^k in S is a disjoint union of subsets of length p^{n-k+1} and the claim is proved.

Denote by $\mathfrak{M}$ the set of all cyclic subgroups of order p^k in G which are not contained in S. Consider the action of R on $\mathfrak{M}$ by conjugations. Assume that $\mathfrak{M}$ is not empty. Let $\mathfrak{M}_0 = \{C \in \mathfrak{W} \mid N_R(C) > 1\}$. It suffices to prove that $p^{n-k+1} \mid |\mathfrak{M}_0|$.

Take $C \in \mathfrak{M}_0$ and set $Q = N_R(C)$, $|R : Q| = p^r$, $T_1 = CQ$. Then $0 < r < n$. If $T_1 \leqslant S_1 \in \mathrm{Syl}_p(G)$ then $T_1 \leqslant \Omega_k(S_1)$, $Q \leqslant \Omega_{k-1}(S_1) \leqslant Z(\Omega_k(S_1)) \cap T_1 \leqslant Z(T_1)$ and $T_1/\Omega_{k-1}(T_1)$ is cyclic. Therefore T_1 is abelian and $|T_1 : \Omega_{k-1}(T_1)| = p$. Set $|T_1| = p^t$. Then $c_k(T_1) = p^{t-k}$ (see the formula for c_k in section 1). If $x \in N_R(T_1)$ and $\langle x, T_1 \rangle \leqslant S_2 \in \mathrm{Syl}_p(G)$, then $x \in Z(\langle x, T_1 \rangle)$ (since $x \in \Omega_{k-1}(S_2)) \leqslant Z(\Omega_k(S_2))$ and $T_1 \leqslant \Omega_1(S_2))$, so $x \in C_R(C) = N_R(C) = Q$. Thus $N_R(T_1) = Q$ and $T_1 \cap R = Q$. Let Z be a cyclic subgroup of order p^k in T_1; then $ZQ = T_1$, $Q \leqslant N_R(Z) \leqslant N_R(T_1) = Q$ and $N_R(Z) = Q$ (recall that R is abelian). In particular $Z \in \mathfrak{M}_0$. Let $\{T_1, \ldots, T_m\}$ be the R-orbit of T_1, $m = |R : N_R(T_1)| = |R : Q| = p^r$. Obviously $T_1, \ldots, T_m$ are not contained in S and $Q \leqslant T_i \cap T_j \leqslant \Omega_{k-1}(T_i), i \neq j, i, j \in \{1, \ldots, m\}$. Therefore $T_1, \ldots, T_m$ contain together exactly $mc_k(T_1) = p^{r+t-k}$ distinct cyclic subgroups of order p^k (denote the set of these subgroups by $\mathfrak{M}_1$). Set $|Q| = p^s$. Then $r = n - s$, $t - s \geqslant 1$, $r + t - k = n - s + t - k \geqslant n - k + 1$. Therefore $p^{n-k+1} \mid |\mathfrak{M}_1|$.

Set $\mathfrak{N} = \{N_R(C) \mid C \in \mathfrak{M}_0\}$, $\mathfrak{M}_Q = \{C \in \mathfrak{M}_0 \mid N_R(C) = Q\}$ $(Q \in \mathfrak{N})$.

If C, Q as above then $\mathfrak{M}_1 \subseteq \mathfrak{M}_Q$.

As in Theorem C the set $\mathfrak{M}_Q\,(Q \in \mathfrak{N})$ is a disjoint union of subsets of lengths divisible by p^{n-k+1} (one of them is $\mathfrak{M}_1$). Therefore $p^{n-k+1} \mid |\mathfrak{M}_Q|$. Let $Z \in \mathfrak{M} - \mathfrak{M}_Q$, $N_R(Z) = Q(1)$. Then $\mathfrak{M}_Q \cap \mathfrak{M}_{Q(1)}$ is empty and $p^{n-k+1} \mid |\mathfrak{M}_{Q(1)}|$. So $\mathfrak{M}_0 = \bigcup_{Q \in \mathfrak{N}} \mathfrak{M}_Q$ is a partition. Therefore $p^{n-k+1} \mid |\mathfrak{M}_0|$ and the theorem is proved. ■

COROLLARY. *If $S \in \mathrm{Syl}_p(G)$, $\exp S \geqslant p^k > p$. $|\Omega_{k-1}(S)| = p^n$, and $\Omega_k(S)$ is abelian then $c_k(G) \equiv 0 \pmod{p^{n-k+1}}$.*

QUESTION 1. *Let G, S, n be as in Theorem C, $1 < k < n$. Denote by $e(p^k, G)$ the number of elementary abelian subgroups of order p^k in G. Whether is the congruence $e(p^k, G) \equiv e(p^k, S) \pmod{p^{n-k+1}}$ true?*

The answer on Question 1 is affirmative if S is elementary abelian itself [5]. If $S \in \mathrm{Syl}_p(G)$ is abelian of rank $n > 1$ and $k > 1$ then, as follows from Theorem D, $c_k(G) \equiv c_k(S) \pmod{p^n}$.

QUESTION 2. *Let $S \in \mathrm{Syl}_p(G)$, $d = \log_p |S : \Phi(S)|$, $|S| = p^t$. Whether is the congruence $s(p^{t-1}, G) \equiv s(p^{t-1}, S) \pmod{p^d}$ true?*

QUESTION 3. *Is it true Theorem C if $\Omega_1(S)$ is of order p^n and exponent p?*

QUESTION 4. *Suppose that $S \in \mathrm{Syl}_p(G)$, $|S : \langle x^p \mid x \in S \rangle| \geqslant p^p$ and S is not of maximal class. Whether is true that $c_1(G) \equiv 1 + p + \ldots + p^{p-1} \pmod{p^p}$?*

ACKNOWLEDGEMENTS

I am indebted to Prof. A. Mann for permission to include his Theorem B, which inspired this investigation, in this *Note* and useful discussions.

Supported in part by the Rashi Foundation and the Ministry of Science and Technology of Israel.

REFERENCES

[1] YA. G. BERKOVICH, *On p-groups of finite order.* Sibirsk. Math. J., 9, 6, 1968, 1284-1306 (in Russian).

[2] YA. G. BERKOVICH, *On the number of elements of given order in a finite p-group.* Israel J. Math., 73, 1991, 107-112.

[3] YA. G. BERKOVICH, *Counting theorems for finite p-groups.* Arch. Math., 59, 1992, 215-222.

[4] N. BLACKBURN, *Generalizations of certain elementary theorems on p-groups.* Proc. London Math. Soc., 11, 1961, 1-22.

[5] P. DELIGNE, *Congruences sur le nombre de sous-groupes d'ordre p^k dans un groupe fini.* Bull. Soc. Math. Belg., 18, 1966, 129-132.
[6] M. HERZOG, *Counting group elements of order p modulo p^2.* Proc. Amer. Math. Soc., 66, 1977, 247-250.

Department of Mathematics and Computer Science
Research Institute of Afula
University of Haifa
31905 HAIFA (Israele)

Einstein Institute of Mathematics
The Hebrew University of Jerusalem
Givat Ram
91904 JERUSALEM (Israele)