ISRAEL JOURNAL OF MATHEMATICS, Vol. 73, No. 1, 1991

ON THE NUMBER OF ELEMENTS OF GIVEN ORDER IN A FINITE p-GROUP

BY
YAKOV G. BERKOVICH
Department of Mathematics and Computer Science, Bar-Ilan University, 52900 Ramat Gan, Israel

ABSTRACT
A. Kulakoff [9] proved that for $p > 2$ the number $N_k = N_k(G)$ of solutions of the equation $x^{p^k} = e$ in a non-cyclic p-group G is divisible by p^{k+1}. This result is a generalization of the well-known theorem of G. A. Miller asserting that the number $C_k = C_k(G)$ of cyclic subgroups of order $p^k > p > 2$ is divisible by p. In this note we show that, as a rule: (1) if $k > 1$, then $N_k \equiv 0 (\bmod p^{k+p})$; (2) if $k > 2$, then $C_k \equiv 0(\bmod p^p)$. These facts are generalizations of many results from [1–5,8,9].

§1. Let G be a finite p-group with $\exp G \geq p^k$. For $M \subset G$, we put $O_k(M) = \{x \in M \mid x^{p^k} = e\}$, $\Omega_k(M) = \langle O_k(M) \rangle$, $N_k(M) = |O_k(M)|$, $N_k = N_k(G)$. The number C_k was defined in the abstract.

We note that the theorems of Kulakoff and Miller are true for $p = 2$ unless G is cyclic or a 2-group of maximal class ([3], the congruence $N_1 \equiv 0(\bmod 4)$ was proved independently by Alperin–Feit–Thompson using the character theory). The following Lemma is obvious.

LEMMA 1. *If* $\exp G \geq p^k$, *then* $p^{k-1}(p-1)C_k = N_k - N_{k-1}$. ■

A finite p-group G is called *regular* if for all $x, y \in G$ there exists $d \in \langle x, y \rangle'$ such that $(xy)^p = x^p y^p d^p$. G is called *absolutely regular* if $|G : \langle x^p \mid x \in G \rangle| < p^p$. The following facts are due to Ph. Hall.

LEMMA 2. (a) *An absolutely regular p-group is regular.*
(b) *If the nilpotency class* $\mathrm{cl}(G)$ *of G is at most* $p - 1$, *then G is regular.*
(c) *If G is regular, then* $\exp \Omega_k(G) \leq p^k$.

Received August 11, 1989

We note that an absolutely regular 2-group is cyclic and that an absolutely regular 3-group is metacyclic. Recall that a non-abelian p-group G of order p^n is called a *p-group of maximal class* if $\mathrm{cl}(G) = n - 1$. The following facts are due to N. Blackburn [6,7].

LEMMA 3. (a) *A p-group G contains a normal subgroup of order p^p and of exponent p unless G is absolutely regular or of maximal class.*

(b) *Let G be a p-group of maximal class and of order p^n, $n > p + 1$. Then G is non-regular and*
  (b1) *G does not contain a normal subgroup of order p^p and of exponent p;*
  (b2) *if $G_1, \dots, G_{p+1}$ are maximal subgroups of G, then exactly p of them, say $G_1, \dots, G_p$, are of maximal class and G_{p+1} is absolutely regular. Furthermore, $|\Omega_1(G_{p+1})| = p^{p-1}$ and $\exp G_{p+1} = \exp G$.* ■

It is well known that $C_k \equiv 0 (\mathrm{mod}\, p^{p-1})$, $k > 1$, and $N_k \equiv 0(\mathrm{mod}\, p^{k+p-1})$ unless G is absolutely regular or a p-group of maximal class. In [4,5] all p-groups G with $|\Omega_2(G)| \leq p^{2+p}$ and $C_k < p^p$, $k > 1$, were classified. All these results are easy consequences of the main theorem of this note.

§2. In this section we prove three lemmas essential in the sequel.

LEMMA 4. *Let G be a p-group of maximal class and of order p^n, $n \geq 1 + p$. Let $k > 1$ and $\exp G = p^t$, $t \geq k$. If $N_k \not\equiv 0(\mathrm{mod}\, p^{k+p})$, then one and only one of the following assertions takes place*:

(a) $p = 2$;
(b) $k = t = 2$, $n = p + 1$;
(c) $p = 3$, $k = 2$, $t > 2$, $N_2 \equiv 3^4 \,(\mathrm{mod}\, 3^5)$.

PROOF. Since the case $p = 2$ is trivial, we assume that $p > 2$. We prove by induction on n.

Suppose that $k = t$. Then $N_k = |G| < p^{k+p}$. From Lemma 3(b) it follows that $k = 2$ and $n = p + 1$. So we assume that $k < t$. In this case $n > p + 1$. Using notations of Lemma 3(b2), put $G_{p+1} = T$ and $L = G_1 \cap G_2$ (this is the Frattini subgroup of G). Then:

$$(*) \qquad N_k = N_k(G) = N_k(T) + \sum_{i=1}^{p} N_k(G_i) - pN_k(L).$$

In fact, if $x \in G_i \cap G_j$, $i \neq j$, then $x \in L$ and x appears at the right side of (*) exactly $p + 1 - p = 1$ times. We have $|\Omega_k(T)| = p^{k(p-1)}$ since $k < t$ (Lemma 3(b2)).

Suppose that $p > 3$. Then $N_k(T) = |\Omega_k(T)| \equiv 0 (\mathrm{mod}\, p^{k+p})$, and $N_k(G_i) \equiv 0 (\mathrm{mod}\, p^{k+p})$, by induction, $1 \le i \le p$. Since $\Omega_k(L) = \Omega_k(T)$, then $N_k(L) = N_k(T) \equiv 0 (\mathrm{mod}\, p^{k+p})$. Hence, $N_k \equiv 0 (\mathrm{mod}\, p^{k+p})$, by (*), which is a contradiction.

Suppose that $p = 3$. We have $N_2(T) = 3^4$ and $N_2(G_i) \equiv 3^4 (\mathrm{mod}\, 3^5)$ for $i = 1,2,3$, by induction. Since $N_2(L) = N_2(T)$, then $3N_2(L) \equiv 0 (\mathrm{mod}\, 3^5)$ and $N_2 \equiv 3^4 (\mathrm{mod}\, 3^5)$, by(*). Now let $k > 2$. Then $N_k(T) = 3^{2k} \equiv 0 (\mathrm{mod}\, 3^{k+3})$, $N_k(L) = N_k(T)$ and, by induction, $N_k(G_i) \equiv 0 (\mathrm{mod}\, 3^{k+3})$ for $i = 1,2,3$. Hence, $N_k \equiv 0 (\mathrm{mod}\, 3^{k+3})$, by (*), which is a contradiction. ■

Lemma 5. *Let R be a normal subgroup of order p^p and of exponent p in a p-group G. Suppose that G/R is cyclic and $|G/R| > p$. Let* $\exp G \ge p^k$ *and put*

$$\epsilon = \begin{cases} 0 & \text{if } \Omega_1(G) = R; \\ 1 & \text{otherwise.} \end{cases}$$

Then $N_k = p^{k+p-1+\epsilon}$ and $\exp \Omega_k(G) = p^k$.

Proof. Let R_1 be a G-admissible subgroup of order p^{p-2} in R, $G^\circ = G/R_1$, $C^\circ = C_{G^\circ}(R^\circ)$. Then C° is abelian and so C is regular (Lemma 2(b)) and $|G:C| \le p$. Hence $|\Omega_1(C)| = p^{p+\epsilon}$ and $\Omega_1(C) = \Omega_1(G)$. The remaining assertions are now obvious. ■

Lemma 6. *Let R be a normal abelian subgroup of type* (2,2) *of a 2-group G such that G/R is of maximal class and of order 2^{n+1} with a cyclic subgroup T/R of index* 2. *Let* $\exp G > 2^k > 2$. *Then* $N_k \not\equiv 0 (\mathrm{mod}\, 2^{k+2}) \Leftrightarrow \Omega_1(T) = R \Leftrightarrow N_k \equiv 2^{k+1} (\mathrm{mod}\, 2^{k+2})$.

Proof. Let $x \in G - T$, $x^2 \in R$. Then $O_k(xR) = xR$ and the contribution of all such xR in N_k is equal to 0 if G/R is a generalized quaternion group, 2^{n+2} if G/R is dihedral, 2^{n+1} if G/R is semi-dihedral.

Let $y \in G - T$, $y^2 \notin R$ and $y^4 \in R$. Then $|O_k(\langle y, R\rangle) - O_2(T)| = 8\epsilon$ where

$$\epsilon = \begin{cases} 0 & \text{if } \Omega_1(G) = R \text{ and } k = 2; \\ 1 & \text{otherwise.} \end{cases}$$

We note that such y does not exist if G/R is dihedral.

(i) Let $\Omega_1(T) = R$. Then $\exp G = \exp T = 2^{n+1}$. Since $\exp G > 2^k$, we have $n \ge k$ and $N_k(T) = 2^{k+1}$.

Suppose that $k = 2$. Then

$$N_2 = \begin{cases} 2^3 & \text{if } G/R \text{ is a generalized quaternion group;} \\ 2^3 + 2^{n+2} & \text{if } G/R \text{ is dihedral;} \\ 2^3 + 2^{n+1} & \text{if } G/R \text{ is semi-dihedral.} \end{cases}$$

In any case $n \geq 2$ and if G/R is semi-dihedral, then $n \geq 3$. Hence, we have $k + p = 4$, $N_2 \equiv 2^3 \pmod{2^4}$.

If $k > 2$, then in any case $N_k = 2^{k+1} + 2^{n+2} \equiv 2^{k+1} \pmod{2^{k+2}}$.

(ii) Let $\Omega_1(T) > R$. Then $|\Omega_1(T)| = 8$, $|\Omega_k(T)| = 2^{k+2}$, $\exp G = 2^n \geq 2^{k+2}$, $n \geq k + 1$. Then $N_k(G) = N_k = 2^{k+2} + 2^{n+2} \equiv 0 \pmod{2^{k+2}}$.

Hence $N_k \not\equiv 0 \pmod{2^{k+2}} \Leftrightarrow \Omega_1(T) = R \Leftrightarrow N_k \equiv 2^{k+1} \pmod{2^{k+2}}$. ∎

§3. In this section we prove

Main Theorem. *Let* $\exp G \geq p^k > p$. *If* $N_k \not\equiv 0 \pmod{p^{k+p}}$, *then one and only one of the following assertions takes place*:

(a) *G is regular and* $|\Omega_k(G)| < p^{k+p}$;

(b) *G is a 2-group of maximal class*;

(c) *G is 3-group of maximal class*, $k = 2$ *and* $|G| \neq 3^5$;

(d) $k = 2$, $p > 3$, $|G| = p^{p+1}$, *G is a p-group of maximal class*;

(e) $|\Omega_1(G)| = p^p$, $G/\Omega_1(G)$ *is cyclic of order* $> p$;

(f) *G is a 2-group from Lemma* 6.

Proof. Induction on n. By Lemmas 4–6, all groups (a–f) satisfy the condition of the Theorem. Suppose that $G \notin$ (a–f). Then G contains a normal subgroup R of order p^p and of exponent p (Lemma 3(a1)) or G is absolutely regular. By Lemma 2(a), we may assume that G is not absolutely regular. Since G/R is not cyclic (Lemma 5), G/R contains a normal subgroup L/R such that G/L is elementary abelian of order p^2. Let $G_1/L, \ldots, G_{p+1}/L$ be all maximal subgroups of G/L. Then as in Lemma 4 we have

$$(*) \qquad N_k = \sum_{i=1}^{p+1} N_k(G_i) - pN_k(L).$$

Since $\exp G/R \geq p^{k-1}$ and G/R is non-cyclic, then $|G| \geq p^{k+p}$. If $\exp G = p^k$, then $N_k = |G| \equiv 0 \pmod{p^{k+p}}$ which is impossible. Hence $\exp G > p^k$. Then $\exp G_i \geq \exp L \geq p^k$. By [2] (see also [1]), we have $pN_k(L) \equiv 0 \pmod{p^{k+p}}$ if L is not of maximal class. Suppose that L is of maximal class. Then $|L| = p^{p+1}$ (Lemma 3(b1)). Since $\exp G > p^2$, then G/R has a cyclic subgroup G_i/R of order

p^2. Since $L < G_i$, then L is regular (Lemma 5) and this contradicts Lemma 3(b). Since $N_k \not\equiv 0 (\bmod p^{k+p})$, we may assume that $N_k(G_1) \not\equiv 0 (\bmod p^{k+p})$. By induction, $G_1 \in$ (a–f).

Suppose that G_1 is regular. Since $R \leq \Omega_1(G_1)$, then $|\Omega_k(G_1)| \geq p^{k+p-1}$. Since $|\Omega_k(G_1)| < p^{k+p}$, then $|\Omega_k(G_1)| = p^{k+p-1}$ and G_1/R is cyclic (we note that if $p = 2$, then G_1 is abelian). Then $\Omega_1(G_1) = R$ (Lemma 5).

Suppose that G_1 is a p-group of maximal class. Since G_1 contains a normal subgroup R of order p^p and of exponent p, then $|G| = p^{p+1}$ (Lemma 3(a)), $L = R$ and $\exp G = p^2 \leq p^k$ which is a contradiction.

Thus, we have to consider the following cases.

(i) G_1/R is cyclic. If $|G_1/R| = p$, then $R = L$ and $\exp G = p^2$ which is a contradiction. Hence $|G_1/R| > p$. Then exactly p maximal subgroups of G/R, say $G_1/R, \dots, G_p/R$, are cyclic (G/R has exactly $p + 1$ maximal subgroups and they are G_i/R, $1 \leq i \leq p + 1$) and G_{p+1}/R is non-cyclic abelian (since, by Lemma 6, the factorgroup G/R is not a generalized quaternion group). By induction, we have $N_k(G_{p+1}) \equiv 0 (\bmod p^{k+p})$. Let S/R be a subgroup of order p in G_1/R. Then $S/R \leq \Phi(G_1/R) \leq G_i/R$, $1 \leq i \leq p + 1$. So we have $N_k(G_i) = p^{k+p-1+\epsilon}$ for all $1 \leq i \leq p$ (ϵ has the same value as in Lemma 5). By (*), we have $N_k \equiv pN_k(G_1) = p^{k+p+\epsilon} \equiv 0 (\bmod p^{k+p})$ which is a contradiction.

(ii) G_1/R is a 2-group of maximal class and of order 2^{n+1}, all G_i/R are noncyclic. Let T_1/R be a cyclic subgroup of index 2 in G_1/R which is normal in G/R (such T_1/R exists since G_1/R contains an odd number of cyclic subgroups of index 2). We have $|G : T_1| = 4$. One verifies as in Lemma 5 that G/T_1 is abelian of type (2,2). So we may assume that $L = T_1$. By Lemma 15 from [2] we may assume that G_2/R is of maximal class and G_3/R is not of maximal class. Hence, by induction, $N_k(G_3) \equiv 0 (\bmod 2^{k+2})$. Let S/R be a subgroup of order 2 in T_1/R and let T_2/R be a cyclic subgroup of index 2 in G_2/R. We have $\Omega_1(T_1) = R$, hence $\Omega_1(T_2) = \Omega_1(S) = R$. Then $N_k(G_2) \equiv 2^{k+1} (\bmod 2^{k+2})$, by Lemma 6. Therefore, $N_k \equiv 0 (\bmod 2^{k+2})$, by (*), which is a contradiction. ■

As a consequence of Main Theorem we obtain the following result.

Corollary 1. *Let $k > 2$. Then $C_k \not\equiv 0 (\bmod p^p) \Leftrightarrow G \in$ (a,b,c′,d–f) where* (c′) *G is a 3-group of maximal class, $k = 3$.*

Proof. We may assume that $\exp G \geq p^k$. Suppose that $G \notin$ (a,b,c′,d–f). By the Main Theorem, we have $N_k = xp^{k+p}, N_{k-1} = yp^{k+p-1}$ for certain natural numbers x,y. Then, by Lemma 1, we have $C_k = (N_k - N_{k-1})/(p-1)p^{k-1} = (px - y)p^p \equiv 0 (\bmod p^p)$. ■

One can give a proof of Corollary 1 independent of the Main Theorem. For this one has to prove analogs of Lemmas 4–6 for C_k and to use an analog of (*) for C_k.

COROLLARY 2. *If* $G \notin$ (a,b,c′,d–f), *then the number of elements of order* p^k, $k > 2$, *in* G *is divisible by* p^{k+p-1}. ■

I believe that Corollary 1 is not true for $k = 2$. For a regular p-group H we put $w(H) = \log_p |\Omega_1(H)|$. For $1 \leq s \leq p-1$, we denote by $M_k(s)$ the number of absolutely regular subgroups F in G with $w(F) = s$, $|F| = p^k$ and $\exp F > p^2$.

CONJECTURE. If $M_k(s) \not\equiv 0 (\mathrm{mod}\, p^{p-s})$, then G is absolutely regular or a p-group of maximal class.

REFERENCES

1. Ya. G. Berkovich, *On the number of solutions of the equation* $x^{p^k} = a$ *in a finite p-group*, to appear.
2. Ya. G. Berkovich, *A generalization of the theorems of Hall and Blackburn and their applications to nonregular p-groups*, Math. USSR Izvestiya **5** (1971), 815–844.
3. Ya. G. Berkovich, *On p-groups of finite order*, Siberian Math. J. **9** (1968), 963–978.
4. Ya. G. Berkovich, *Finite p-groups containing at most* $p^p - 1$ *cyclic subgroups of order* p^n, Voprosy teorii grup i gomologicheskoi algebry **2** (1979), Yaroslavl.
5. Ya. G. Berkovich, II, Matematicheski analis i ego prilozenia, Rostov University (1981), 10–16, Rostov-Don (in Russian).
6. N. Blackburn, *On a special class of p-groups*, Acta Math. **100** (1958), 45–92.
7. N. Blackburn, *Generalizations of certain elementary theorems on p-groups*, Proc. London Math. Soc. **11** (1961), 1–22.
8. N. Blackburn, *Note on a paper of Berkovich*, J. Algebra **24** (1973), 323–334.
9. A. Kulakoff, *Uber die Anzahl der eigentlichen Untergruppen und der Elemente von gegeberen Ordnung in p-Gruppen*, Math. Ann. **104** (1931), 778–793.