ON THE NUMBER OF SOLUTIONS OF THE EQUATION $x^{p^k} = a$
IN A FINITE $p$-GROUP

YAKOV G. BERKOVICH

(Communicated by Warren J. Wong)

Dedicated to Professor Gregory A. Freiman

Abstract. A. Kulakoff (Math. Ann. 104 (1931), 778–793) proved that for $p > k^2$ the number of solutions of the equation $x^{p^k} = e$ ($e$ is a unit element of $G$) in a finite noncyclic $p$-group $G$ is divisible by $p^{k+1}$ if $\exp G \geq p^k$. In this note we consider the number $N(a, G, k)$ of solutions of the equation $x^{p^k} = a$ in $G$, $a \in G$. Our results cover the case $p = 2$ also.

1. Introduction

In this note $p$ denotes a prime and $G$ denotes a finite $p$-group.

A $p$-group $G$ is called regular (Hall [8]) if for all $x, y \in G$ there exists $z \in \langle x, y \rangle$ such that $(xy)^p = x^py^pz^p$. By a well-known theorem of Hall [8] for an irregular $p$-group $G$ we have

$$|G: \langle x^p | x \in G \rangle| \geq p^p.$$ 

A $p$-group $G$ is called absolutely regular (Blackburn [6]) if $|G: \langle x^p | x \in G \rangle| < p^p$. Hence an absolutely regular $p$-group is regular.

If a $p$-group $G$ is regular and $k$ is a positive integer, then

$$N(e, G, k) = |\{x \in G | x^{p^k} = e\}|,$n
i.e., $N(e, G, k)$ depends on the power structure of $G$ only. We note that for a regular $p$-group $G$ we have

$$\langle x \in G | x^{p^k} = e \rangle = \{x \in G | x^{p^k} = e\},$$

i.e., $\exp(x \in G | x^{p^k} = e) \leq p^k$.

Hence $N(e, G, k)$ is hard to determine only for irregular $p$-groups.

Obviously an absolutely regular 2-group is cyclic. We note that an absolutely regular 3-group is metacyclic.

If $p > 2$ and a $p$-group $G$ is noncyclic, $\exp G \geq p^k$, then $N(e, G, k)$ is divisible by $p^{k+1}$ (Kulakoff [10]).

We call a $p$-group $G$ exceptional if it is absolutely regular or of maximal class. Blackburn [6] showed that any nonexceptional $p$-group contains a normal...
subgroup of order $p^s$ and exponent $p$. If a 2-group $G$ is nonexceptional then $N(e, G, 1)$ is divisible by 4 [2; 11, Theorem 6; 9, Theorem 4.9]. This result was generalized by Berkovich [1] and Blackburn [7]: if $G$ is a nonexceptional $p$-group then $N(e, G, 1)$ is divisible by $p^s$. This is the best-possible result.

If $a \neq e$ the counting of $N(a, G, k)$ is harder and considerably more subtle. If $p > 2$ and a $p$-group $G$ is noncyclic then $N(a, G, k)$ is divisible by $p^2$ (Lam [12]). On pp. 580–581 of paper [12] Lam writes: “It seems likely that, more generally, for any central element $a \in Z(G)$ the number of solutions of $x^2 = a$ in (nonexceptional 2-group) $G$ is divisible by 4, but we have not been able to find a proof.”

Theorem A shows that Lam’s conjecture is true. This theorem shows that as a rule $N(e, G, k)$ is divisible by $p^{k+1}$ if $\exp G \geq p^k$. Theorem B shows that in a nonexceptional $p$-group $G$ the number $N(e, G, k)$ is divisible by $p^{k+p-1}$ if $\exp G \geq p^k$. Both these theorems extend results mentioned earlier.

We denote by $G'$ the commutator subgroup of $G$ and by $\varphi(G)$ the Frattini subgroup of $G$. Since in a $p$-group we have
$$\varphi(G) = G'(x^p | x \in G),$$
it follows that $H < G \Rightarrow \varphi(H) \leq \varphi(G)$. If $A$ is a subset of $G$ then $C_G(A), \text{ resp. } N_G(A)$, denotes the centralizer, resp. normalize, of $A$ in $G$. By $|M|$ we denote the number of elements of a set $M$.

2. Results

In this section we state our main results.

**Theorem A.** Let a $p$-group $G$ be noncyclic and not a 2-group of maximal class. Let $k$ be a positive integer, $a \in G$, and $\exp G \geq p^k |(a)|$. Then $N(a, G, k)$ is divisible by $p^{k+1}$.

In particular we see that Lam’s conjecture holds.

**Theorem B.** Let a $p$-group $G$ be nonexceptional, $k$ be a positive integer, and $\exp G \geq p^k$. Then $N(e, G, k)$ is divisible by $p^{k+p-1}$.

In particular in the case when $a = e$ and $p = 2$, Theorem B implies Theorem A. We note that the proof of Theorem A is completely elementary, but the proof of Theorem B uses deep results of $p$-group theory.

3. Proofs

In this section we prove Theorems A and B.

**Lemma 1.** Let $G$ be a cyclic $p$-group, let $k$ be a positive integer, $a \in G$, and $|G| \geq p^k |(a)|$. Then $N(a, G, k) = p^k$.

This is obvious.

**Lemma 2.** Let $G$ be a 2-group of maximal class, $k$ be a positive integer, $a \in G$. If $a = e$ then let $k > 1$. Then $N(a, G, k) = 0$ or $N(a, G, k) \equiv 2^k \pmod{2^{k+1}}$.

This is proved by easy checking since a 2-group of maximal class is dihedral, semi-dihedral, or generalized quaternion.

We note that, in Lemma 2, if $N(a, G, k) > 0$ then $a \in \varphi(G)$.
Lemma 3. Let $A$ be a cyclic subgroup of a $p$-group $G$, $C_G(A) > A$. If $C_G(A)$ is cyclic then $G$ is cyclic or a 2-group of maximal class.

Proof. Suppose that $G$ is noncyclic and not a 2-group of maximal class. Then by Roquette's theorem (see, e.g., [3]) $G$ contains a normal subgroup $R$ of type $(p, p)$. Then $RC_G(A)$ is a nonabelian $p$-group with a cyclic subgroup of index $p$ and $A \not\subseteq Z(RC_G(A))$. Since $A < C_G(A)$,

$$A \leq \varphi(C_G(A)) \leq \varphi(RC_G(A)) = Z(RC_G(A))$$

(the equality follows from the classification of $p$-groups with a cyclic subgroup of index $p$), a contradiction. □

Note that if $A$ is a cyclic subgroup of a 2-group of maximal class and $|A| > 2$ then $C_G(A)$ is cyclic (see remark after Lemma 2).

Lemma 4. Let $A$ be a cyclic subgroup of a noncyclic $p$-group $G$, where $G$ is not a 2-group of maximal class. Let $k$ be a positive integer and $k > 1$ if $|A| = 1$. Let $\mathfrak{M} = \mathfrak{M}(A, G, k)$ denote the set of all cyclic subgroups containing $A$ of order $p^k|A|$ in $G$. Then $|\mathfrak{M}| \equiv 0 \pmod{p}$.

Proof. For $|A| = 1$ this result is well known (for $p > 2$ it is due to Miller and for $p = 2$ it is due to Berkovich; for details see [1, 3]). Now let $|A| > 1$.

Induct on $|G|$. For $D \leq G$ let $c(D)$ denote the number of elements of $\mathfrak{M}$ contained in $D$ (if $A \leq D$ then $c(D) = |\mathfrak{M}(A, D, k)|$ and if $A \not\leq D$ then $c(D) = 0$).

We may assume that the set $\mathfrak{M}$ is nonempty. Obviously $\mathfrak{M}(A, G, k) = \mathfrak{M}(A, C_G(A), k)$. Since $\mathfrak{M}$ is nonempty, $C_G(A) > A$ and $C_G(A)$ is noncyclic by Lemma 3. If $C_G(A)$ is a 2-group of maximal class then $|A| = 2$ and elementary results of $p$-group theory imply $G = C_G(A)$, a contradiction to the assumption that $G$ is not a 2-group of maximal class.

If $C_G(A) < G$ then $|\mathfrak{M}| \equiv 0 \pmod{p}$ by induction. Hence we may assume that $C_G(A) = G$, i.e., $A \leq Z(G)$.

Since $\mathfrak{M}$ is nonempty, for $B \in \mathfrak{M}$ we have $A \leq \varphi(B) \leq \varphi(G)$. Let $T_1, \ldots, T_m$ be all maximal subgroups of $G$. Then by Hall’s enumeration principle [8] we have

$$|\mathfrak{M}| = c(G) \equiv \sum_{i=1}^{m} c(T_i) \pmod{p}. \tag{1}$$

Suppose that one of the $T_i$’s, say $T_1$, is cyclic. Then $m = p + 1$ and exactly $p$ of the $T_i$’s are cyclic (this follows from the classification of $p$-groups with a cyclic subgroup of index $p$). Since $A \leq \varphi(G)$, $c(T_i) = 1$ for all cyclic $T_i$. If $T_j$ is noncyclic (then $T_j$ is abelian) then $c(T_j) = 0$ or $p$, and (1) gives $|\mathfrak{M}| \equiv 0 \pmod{p}$. Hence we may assume that any $T_i$ is noncyclic. Suppose that one of the $T_i$’s, say $T_1$, is a 2-group of maximal class. By a result of Berkovich (see §5 in [3]) among $T_i$’s there are $4t$ ($t \geq 1$ is an integer) subgroups of maximal class. Then $c(T_i)$ is odd for $i \in [1, 4t]$ and $c(T_j)$ is even for $j \in [4t + 1, m]$. In this case, by (1), we have $|\mathfrak{M}| \equiv 0 \pmod{p}$. If all the $T_i$ are not 2-groups of maximal class then by induction $c(T_i) \equiv 0 \pmod{p}$ for all $i$, and $|\mathfrak{M}| \equiv 0 \pmod{p}$ by (1). □

There is a little hope to find $|\mathfrak{M}| \pmod{p^2}$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Proof of Theorem A. Induct on \(|G|\).

(i) Let \(a = e\). Our result is known if \(k = 1\) (see §1). Let \(k > 1\). We may assume that \(\exp G > p^k\) (since in the contrary case \(N(e, G, k) = |G| \geq p^{k+1}\)). By supposition and Roquette's theorem (see proof of Lemma 4) \(G\) contains a normal subgroup \(R\) of type \((p, p)\). Suppose that \(G/R\) is cyclic. Then \(C_G(R)\) is abelian, and its index in \(G\) is at most \(p\). If \(C_G(R) = G\) the result is obvious. Let \(C_G(R) < G\). Take an element \(x \in G\) with \(|\langle x \rangle| \leq p^k\). Consider the subgroup \(T = R(x)\). Obviously \(\exp T \leq p^k < \exp G \Rightarrow T < G \Rightarrow T \leq C_G(R)\). Hence any element of \(G\) of order not exceeding \(p^k\) is contained in \(C_G(R)\). So \(N(e, G, k) = N(e, C_G(R), k)\). Since \(C_G(R)\) is abelian, \(N(e, C_G(R), k) = p^{k+1}\) or \(p^{k+2}\).

So we may assume that \(G/R\) is noncyclic. Then \(G/R\) contains a normal subgroup \(L/R\) such that \(G/L\) is abelian of type \((p, p)\). Since \(\exp G > p^k > p^2\), it follows that \(L > R\). Hence all maximal subgroups of \(G\) containing \(L\), say \(T_1, \ldots, T_{p+1}\), are not 2-groups of maximal class (if a 2-group of maximal class contains a normal subgroup of type \((2, 2)\) then its order is equal to 8).

Since \(x^p \in L\) for all \(x \in G\),

\[ T_1 \cup \cdots \cup T_{p+1} = G \]

and

\[
N(e, G, k) = \sum_{i=1}^{p+1} N(e, T_i, k) - pN(e, L, k).
\]

By Frobenius's theorem of elementary group theory we have \(N(e, L, k) \equiv 0 \pmod{p^k}\). By induction \(N(e, T_i, k) \equiv 0 \pmod{p^{k+1}}\) since all \(T_i\) are not 2-groups of maximal class. Hence by (2) we have \(N(e, G, k) \equiv 0 \pmod{p^{k+1}}\).

(ii) Let \(a \neq e\) and let \(\mathcal{M}\) be the set of all cyclic subgroups containing \(\langle a \rangle\) of order \(p^k|\langle a \rangle|\) in \(G\). Then by Lemma 1 we have

\[
N(a, G, k) = \sum_{Z \in \mathcal{M}} N(a, Z, k) = p^k|\mathcal{M}|.
\]

Since \(|\mathcal{M}| \equiv 0 \pmod{p}\) by Lemma 4, \(N(a, G, k) \equiv 0 \pmod{p^{k+1}}\). \(\square\)

Lemma 5. Let \(R\) be a normal subgroup of order \(p^n\) and exponent \(p\) in a \(p\)-group \(G\); \(G/R\) be cyclic of order \(p^m\), \(m > 1\); \(T/R\) be a subgroup of index \(p\) in \(G/R\). Then the nilpotence class of \(T\) is at most \(p - 1\). In particular \(T\) is regular.

Proof. Let \(K\) be a \(G\)-admissible subgroup of order \(p^{n-2}\) in \(R\) (if \(p = 2\) then \(K = 1\)). We set \(G^o = G/K, R^o = R/K, T^o = T/K\). Then \(C_{G^o}(R^o) \geq T^o\) and \(C_{G^o}(R^o) = D/K\) is abelian (see the proof of Theorem A). So the nilpotency class of \(D\) is at most \(p - 1\), and \(D\) is regular by a well-known theorem of Hall [8]. Since \(D \geq T^o, T^o\) is regular also. \(\square\)

Lemma 6. Let \(G, R, T\) be as in Lemma 5, \(\exp G \geq p^k\). Then \(N(e, G, k) = p^{k+p-1}\) or \(p^{k+p}\) (here \(k\) is a positive integer).

Proof. If \(\exp G = p^k\) then \(|G| = p^{k+p-1}\) or \(p^{k+p}\) and \(N(e, G, k) = |G|\). Hence we may assume that \(\exp G > p^k\). If \(\exp T > p^k\) then \(T \geq \langle x \in G| x^{p^k} = e \rangle\) and the lemma is true since \(T\) is regular (Lemma 5). Let \(\exp T = p^k\).
ON THE NUMBER OF SOLUTIONS OF THE EQUATION \( x^k = a \)

Then \( \exp G = p^{k+1} \). Let \( x \) be an element of \( G \) with \( |\langle x \rangle| \leq p^k \). Suppose that \( x \notin T \). Then \( G = R(x) \) with \( R \cap \langle x \rangle = 1 \). Then \( T = R(x^p) \) and \( \exp T < p^k \), a contradiction. Hence all elements of \( G \) of order at most \( p^k \) lie in \( T \). Since \( T \) is regular, \( T = \langle x \in G | x^{p^k} = e \rangle \) and \( N(e, G, k) = |T| = p^{k+p-1} \) or \( p^{k+p} \). □

**Proof of Theorem B.** By Blackburn’s theorem [6] any nonexceptional \( p \)-group \( G \) contains a normal subgroup \( R \) of order \( p^p \) and exponent \( p \) (see also [1, 2]). Our result is true if \( k = 1 \) (see [1] or [7]). Now let \( k > 1 \). In virtue of Lemma 6 we may assume that \( G/R \) is noncyclic. Hence \( G/R \) contains a normal subgroup \( L/R \) such that \( G/L \) is abelian of type \((p, p)\). Let \( T_1, \ldots, T_{p+1} \) be all maximal subgroups of \( G \) containing \( L \). Then, as in the proof of Theorem A, we have

\[
N(e, G, k) = \sum_{i=1}^{p+1} N(e, T_i, k) - pN(e, L, k).
\]

1. **If** \( L = R \) **then** \( \exp G = p = p^k \), \( k = 2 \), and \( N(e, G, k) = |G| = p^{p+2} = p^{k+p} \equiv 0 \) (mod \( p^{k+p-1} \)). So we may assume that \( R < L \). Then all \( T_i \) are nonexceptional. We may assume that \( \exp G > p^k \). Then \( \exp T_i \geq p^k \) for all \( i \), and by induction we have \( N(e, T_i, k) \equiv 0 \) (mod \( p^{k+p-1} \)). We note that \( \exp L \geq p^k \). If \( L \) is of maximal class then \( |L| = p^{p+1} \) (since a \( p \)-group of maximal class and order larger than \( p^{p+1} \) does not contain a normal subgroup of order \( p^p \) and exponent \( p \)). In this case \( k = 2 \) and \( N(e, L, k) = p^{p+1} = p^{k+p-1} \) and \( N(e, G, k) \equiv 0 \) (mod \( p^{k+p-1} \)) by (2'). If \( L \) is not a group of maximal class then \( N(e, L, k) \equiv 0 \) (mod \( p^{k+p-1} \)) by induction, and again \( N(e, G, k) \equiv 0 \) (mod \( p^{k+p-1} \)). □

We note that if \( G \) is a nonregular \( p \)-group of maximal class then \( N(e, G, k) \equiv 0 \) (mod \( p^{k+p-2} \)) (here \( \exp G \geq p^k \)). A proof of this result is analogous to the proof of Theorem B. If \( G \) is of maximal class, \( \exp G \geq p^k \), \( |G| > p^{p+1} \), then we may prove that \( N(e, G, k) \equiv p^{k+p-2} \) (mod \( p^{p+k-1} \)) (for \( p = 2 \) see Lemma 2).

Many related results were proved in [1–5, 7].

**References**


License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use


Department of Mathematics, Afula Research Institute, University of Haifa, 31905 Haifa, Israel