ILLINOIS JOURNAL OF MATHEMATICS
Volume 32, Number 3, Fall 1988

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

BY

T.Y. LAM[1]

**In Memory of Irving Reiner**

## 1. Background

One of the most classical enumeration theorems in the theory of finite $p$-groups is the following:

(1.1) THEOREM OF KULAKOFF [7]. *If $G$ is a noncyclic $p$-group of order $p^n$ where $p > 2$, then for any positive integer $m < n$, the number of subgroups of order $p^m$ in $G$ is* $\equiv 1 + p \pmod{p^2}$.

For $m = 1$, this theorem has the following equivalent form:

(1.2) COROLLARY. *For $G$ as above, the number of solutions of the equation $x^p = 1$ in $G$ is divisible by $p^2$.*

Theorem (1.1) was first stated in Miller's paper [11] in 1923, and (1.2) has appeared as early as 1916 as an exercise in the book of Miller, Blichfeldt and Dickson [12, p. 133]. However, Miller's proof of (1.1) in [11] contained a gap, as was pointed out (and corrected) by Kulakoff [8]. The first complete proof of (1.1) appeared in [7] (1931), which was independent of Miller's work. Other proofs have subsequently been found by O.J. Schmidt [13] and P. Hall [4]. For a modern exposition, see [6, p. 314].

A natural way to extend Kulakoff's Theorem is to try to prove enumeration theorems modulo higher powers of $p$. In this direction, various results have been obtained in the case $m = 1$. Counting modulo $p^3$, the best result is the

Received November 4, 1987.

[1]Supported in part by the National Science Foundation.

following:

(1.3) THEOREM (Huppert [6, p. 339], Berkovich [2]). *Let $G$ be a finite $p$-group which is not metacyclic. If $p > 3$, then the number of solutions of the equation $x^p = 1$ in $G$ is divisible by $p^3$.*

If $G$ is an *irregular* (finite) $p$-group, then even stronger enumeration theorems are possible. In fact, P. Hall [5] has shown that, for such $G$, the number $N$ of solutions of $x^p = 1$ in $G$ is always divisible by $p^{p-1}$, and N. Blackburn [1] has shown that, if $G$ is also not of maximal class, then $N$ is even divisible by $p^p$. These results are, however, considerably deeper.

My own interest in Kulakoff's Theorem stems from the fact that (1.2) has a marvellous application to the computation of the Artin exponent of finite groups. In fact, coupled with a result of Brauer, (1.2) implies that a noncyclic $p$-group of order $p^n$ with $p$ odd has Artin exponent $p^{n-1}$ [10, Th. (5.1)]. In an unpublished part of my thesis [9], I have given another proof of (1.2). Recently, I discovered that the ideas of that proof can be extended to give results on the number of solutions of the equation $x^{p^k} = a$ in a finite group $G$, where $a$ is a given element of $G$. Since these results represent, among other things, generalizations of (1.2), (1.3), and do not seem to have appeared in the literature, I shall record them in this short note.

I wish to thank Professor H. Bass who taught me some of the ideas used here when I wrote my thesis. Shortly thereafter, I had the good fortune of working on representation theory with Professor I. Reiner, through several visits at the University of Illinois. In subsequent years, I have continued to profit from his good counsel, and to receive his warm encouragement and support. His untimely death in October, 1986 was to me a great personal loss.

## 2. Statement and proof of the theorem

Unless stated otherwise, all groups considered in this paper are finite groups. In the following result, the prime $p$ is fixed. However, we do not need to work in a $p$-group, so we take $G$ to be an arbitrary group.

(2.1) THEOREM. *Let $G$ be a finite group, and $H \subseteq G$ be a $p$-elementary abelian normal subgroup of order $p^r$. Then, for any central element $a \in Z(G)$ and any integer $k \geq 1$, the number $N$ of solutions of the equation $x^{p^k} = a$ in $G$ is divisible by $p^{r-[r/p^k]}$. ($[d]$ denotes the integral part of a positive number $d$.) In particular, $N$ is divisible by $p^{\min(r, p^k-1)}$.*

Before proceeding to the proof of the theorem, let us first explain how the second conclusion follows from the first. If $r \leq p^k - 1$, then $[r/p^k] = 0$, so

the first conclusion gives the divisibility of $N$ by

$$p^r = p^{\min(r,\, p^k-1)}.$$

If, on the other hand, $r \geq p^k$, then, writing $r = qp^k + r_0$ with $0 \leq r_0 < p^k$, we have $[r/p^k] = q \geq 1$ and so

$$r - [r/p^k] = qp^k + r_0 - q = q(p^k - 1) + r_0 \geq p^k - 1.$$

Then the first conclusion of the Theorem implies that $N$ is divisible by

$$p^{p^k-1} = p^{\min(r,\, p^k-1)}.$$

It is also worth noting that the theorem above is not true if the element $a$ is not assumed to be central in $G$. In fact, if $G$ is the alternating group on four letters, then the 2-Sylow group $H \lhd G$ is 2-elementary abelian of order $2^r$ with $r = 2$, so for $p = 2$ and $k = 1$, we have

$$p^{r-[r/p^k]} = 2^{2-1} = 2.$$

However, for the (noncentral) 3-cycle $a = (123)$, the equation $x^2 = (123)$ has only one solution, namely, $x = (132)$.

*Proof of the theorem.* It is sufficient to prove that, for any element $b \in G$, the number of $N_b$ of solutions of $x^{p^k} = a$ with $x \in H \cdot b$ is divisible by $p^{r-[r/p^k]}$. If such solutions do not exist, then $N_b = 0$ and we have nothing to prove. Therefore, we may as well assume that $b$ itself is a solution, i.e., $b^{p^k} = a$. Now we must count the number $N_b$ of elements $h \in H$ such that $(hb)^{p^k} = a$. Let $\beta \in \mathrm{Aut}(H)$ be defined as the conjugation action of $b$ on $H$, i.e., $\beta(h) = bhb^{-1}$. For any $h \in H$, we have

$$(hb)^2 = h(bhb^{-1})b^2 = h\beta(h)b^2,$$

and so inductively,

$$(hb)^i = h\beta(h)\beta^2(h) \cdots \beta^{i-1}(h)b^i.$$

In particular, $(hb)^{p^k} = h\beta(h) \cdots \beta^{p^k-1}(h)a$. Therefore, $N_b$ *is exactly the number of elements* $h \in H$ *such that* $h\beta(h) \ldots \beta^{p^k-1}(h) = 1$. Next, note that, since $\beta^{p^k}$ is the conjugation action of $b^{p^k} = a$ on $H$ and $a$ is central, we have $\beta^{p^k} = 1$. Letting $\langle B \rangle$ be a cyclic group of order $p^k$ and viewing $H$ as an $\mathbf{F}_p$-vector space, we can then make $H$ into a (left) $\mathbf{F}_p\langle B \rangle$-module by the action $B \cdot h = \beta(h)$ (for any $h \in H$). Using this action, $N_b$ is now the cardinality of

the annihilator of

$$1 + B + B^2 + \cdots + B^{p^k-1} \in \mathbf{F}_p\langle B\rangle$$

on $H$. In order to calculate the sum expression, note that, for any indeterminate $T$ over $\mathbf{F}_p$, we have

$$\begin{aligned} 1 + (1+T) + \cdots + (1+T)^{p^k-1} &= \frac{1-(1+T)^{p^k}}{1-(1+T)} \\ &= \frac{1-1-T^{p^k}}{-T} \\ &= T^{p^k-1}. \end{aligned}$$

Letting $t := B - 1$ in the group algebra $R := \mathbf{F}_p\langle B\rangle$ and specializing the above polynomial identity by $T \mapsto t$, we get

$$1 + B + B^2 + \cdots + B^{p^k-1} = t^{p^k-1} \in R,$$

and hence $N_b = \operatorname{Card} \operatorname{ann}_H (t^{p^k-1})$. Now let us invoke our knowledge of the modular representation theory for the group $\langle B\rangle$ (cf. [3, pp. 431–432]). The (finite dimensional) indecomposable left $R$-modules are, up to isomorphism,

$$M_i = R/R \cdot t^i \quad \text{with } \dim_{\mathbf{F}_p} M_i = i \qquad (1 \le i \le p^k),$$

so $H$ (as an $R$-module) has a Krull-Schmidt decomposition

$$H \cong s_1 M_1 \oplus s_2 M_2 \oplus \cdots \oplus s_{p^k} M_{p^k},$$

where the non-negative integers $s_1, \ldots, s_{p^k}$ denote the multiplicities with which the $M_i$'s occur. Since $t^{p^k} = 0$ but $t^{p^k-1} \neq 0$, we have

$$\operatorname{ann}_{M_i}\left(t^{p^k-1}\right) = \begin{cases} M_i & \text{if } i < p^k, \\ tM_i & \text{if } i = p^k. \end{cases}$$

Using the fact that $tM_i$ has codimension 1 in $M_i$, we see that

$$\dim_{\mathbf{F}_p} \operatorname{ann}_H\left(t^{p^k-1}\right) = \dim_{\mathbf{F}_p} H - s_{p^k} = r - s_{p^k}.$$

On the other hand, the fact that $H$ contains $s_{p^k}$ copies of $M_{p^k}$ implies that

$$r \ge \left(\dim_{\mathbf{F}_p} M_{p^k}\right) s_{p^k} = p^k \cdot s_{p^k},$$

and so $s_{p^k} \leq [r/p^k]$. It follows that

$$\dim_{\mathbf{F}_p} \operatorname{ann}_H\left(t^{p^k-1}\right) \geq r - \left[r/p^k\right],$$

and therefore $N_b$ is divisible by $p^{r-[r/p^k]}$, as desired. Q.E.D.

In the proof above, the only property we needed for the element $a$ is that it centralizes the subgroup $H$. Thus, the conclusion of the theorem holds already if we only assume that $C_G(a)$ has a normal $p$-elementary abelian subgroup $H$ of order $p^r$. However, this does not really give a stronger result, since any solution $x$ of the equation $x^{p^k} = a$ lies in $C_G(a)$, so for the purpose of counting the number of solutions of this equation, we could have, in any case, replaced $G$ by $C_G(a)$, in which $a$ is central.

A nice illustration of the method used in the proof of (2.1) is provided by the group $G$ which is a $p$-Sylow group of the symmetric groups $S_{p^2}$. As is well known, $G$ is a regular wreath product $\mathbf{Z}_p \wr \mathbf{Z}_p$; in particular, $G$ is a semidirect product of $H = \mathbf{Z}_p \oplus \cdots \oplus \mathbf{Z}_p$ ($p$ copies) with a cyclic group $\langle b \rangle$ of order $p$. Here we have $r = p$, and we take $a = 1$, $k = 1$. With the element $b$ chosen as above, the $R$-module $H$ referred to in the proof of (2.1) is just the left regular module ${}_RR \cong M_p$ and so $H_0 := \operatorname{ann}_H(t^{p-1})$ is a "hyperplane" in $H$. According to the proof of (2.1), $\{x \in H \cdot b\colon x^p = 1\}$ is just $H_0 \cdot b$. Applying the same consideration to any coset $H \cdot b^i$ ($1 \leq i < p$), we get

$$\left\{x \in H \cdot b^i\colon x^p = 1\right\} = H_0 \cdot b^i.$$

(It is easy to see that the same $H_0$ works for all the non-identity cosets. In fact, $H_0$ is exactly the commutator subgroup of $G$.) Therefore,

$$\{x \in G\colon x^p = 1\} = H \cup \left(H_0 b \cup \cdots \cup H_0 b^{p-1}\right) = H \cup H'$$

where $H' = \langle H_0, b \rangle$ (cf. [6, p. 381, Ex. 36]), and the number of solutions of $x^p = 1$ is $p^p + (p-1)p^{p-1} = p^{p-1}(2p-1)$, as was pointed out already by P. Hall in [5, p. 480].

Even if the element $a \in G$ is not central, the proof of Theorem (2.1) can be used to give divisibility results for the number of solutions of $x^{p^k} = a$ when $a$ is a $p$-element and the integer $k$ is sufficiently large.

(2.2) THEOREM. *Let $G$ be a finite group and $H \subseteq G$ be a $p$-elementary abelian normal subgroup of order $p^r$. Then, for any $p$-element $a \in G$, the number $N$ of solutions of the equation $x^{p^k} = a$ in $G$ is divisible by $p^{r-1}$ when $p^k = r$, and divisible by $p^r$ when $p^k > r$.*

*Proof.* Going back to the notations used in the proof of (2.1), we fix an element $b \in G$ such that $b^{p^k} = a$ and consider the automorphism $\beta \in \mathrm{Aut}(H)$ induced by the conjugation action of $b$. In order for the proof to work, we need to know that $\beta^{p^k} = 1$. This can be deduced from the assumptions (i) $a$ is a $p$-element, and (ii) $p^k \geq r$, as follows. By (i), we know that $b$ is also a $p$-element, and so $\beta^{p^m} = 1$ for some $m$. Working in $\mathrm{End}(H) \cong \mathbf{M}_r(\mathbf{F}_p)$, $\beta - 1$ is nilpotent and therefore $(\beta - 1)^r = 0$. Using (ii), we have $(\beta - 1)^{p^k} = 0$ and so $\beta^{p^k} = 1$, as desired. Thus, we can conclude as before that $N$ is divisible by $p^{r-[r/p^k]}$, and the theorem follows. Q.E.D.

## 3. Applications

In this section, we shall show how Theorems (2.1) and (2.2) can be used to obtain some generalizations of (1.2) and (1.3). To put the results in better focus, we shall now specialize to $p$-groups. The following is our generalization of (1.2).

(3.1) THEOREM. *Let $G$ be a finite non-cyclic $p$-group, where $p > 2$. Let $a \in G$ and $k$ be any positive integer. Then the number $N$ of solutions of the equation $x^{p^k} = a$ in $G$ is divisible by $p^2$.*

*Proof.* Under the given assumptions on $G$, it is well-known that $G$ contains a normal subgroup $H \cong \mathbf{Z}_p \oplus \mathbf{Z}_p$ [14, pp. 58–59]. Thus, the theorem follows by applying the second conclusion of (2.2) with $r = 2$. Q.E.D.

In the situation of (3.1), if $a = 1$ and $p^k < |G|$, then Kulakoff has proved that $N$ is divisible by $p^{k+1}$ [7, Satz 2]. However, Kulakoff's counting methods do not extend to the case where $a \in G$ is arbitrary. On the other hand, using deeper tools from the structure theory of $p$-groups, P. Hall has proved a much more precise theorem concerning the number of solutions of $x^{p^k} = a$ [5, Th. (2.6)]. Our Theorem (3.1) lacks the depth of Hall's result, but its proof is completely elementary. Note also that the key case in (3.1) is when $k = 1$, because, as is easily seen, the conclusion in this case implies that in the general case.

The case when $p = 2$ is harder and considerably more subtle. It is known that, if a 2-group $G$ is not cyclic, dihedral, semi-dihedral or generalized quaternion, then $G$ has a normal subgroup $H \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2$ [14, pp. 58–59]. For these groups $G$, a result of Alperin, Feit and Thompson (see, for example, [10, Th. (6.1)]) states that the number of solutions of the equation $x^2 = 1$ in $G$ is divisible by 4. (An equivalent statement is that, for any normal subgroup $H \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2$ as above, the number of (normal) subgroups $K \supset H$ isomorphic to the dihedral group of order 8 is even.) It seems likely that, more generally,

for any central element $a \in Z(G)$, the number of solutions of $x^2 = a$ in $G$ is divisible by 4, but we have not been able to find a proof.

In order to get from (2.1) and (2.2) a corresponding counting theorem modulo $p^3$, we would need the existence of a normal $p$-elementary abelian subgroup $H \subseteq G$ of order $p^3$. Fortunately, such a result is available in the literature. (We mention in passing the curious fact that, for $p \geq 3$, a $p$-group $G$ has a $p$-elementary abelian subgroup of order $p^3$ iff it has a *normal* $p$-elementary abelian subgroup of order $p^3$; see [14, p. 63].)

(3.2) PROPOSITION. *Let $G$ be a finite $p$-group where $p > 3$. If $G$ is not regular, then $G$ has a normal $p$-elementary abelian subgroup $H$ of order $p^3$.*

This can be seen by using the short argument from the first part of the proof of Satz 12.4 in [6, p. 344], due to Blackburn. In fact, if $G$ does not have a (normal) $p$-elementary abelian subgroup of order $p^3$ ($p \geq 3$), the structure of $G$ has been completely determined by Blackburn. However, we only need to know that such $G$ must be regular when $p > 3$, for which the beginning part of the proof of Satz 12.4 suffices. Note also that Prop. (3.2) does not hold for the prime $p = 3$; in fact, there exists an irregular 3-group of order $3^4$ for which $x^3 = 1$ has exactly nine solutions, so clearly $G$ has no subgroup isomorphic to $\mathbf{Z}_3 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3$ (see [6, Bem. (11.7), p. 339], or [14, Ex. 9, p. 99]).

With the aid of Prop. (3.2), we can now generalize the theorem of Huppert and Berkovich stated in (1.3).

(3.3) THEOREM. *Let $G$ be a finite $p$-group which is not metacyclic, $a \in G$, and $k$ be a positive integer. Assume that* (i) $p > 3$, *or* (ii) $p = 3$, $k \geq 2$, *and $G$ is not one of the 3-groups determined by Blackburn which do not have a normal subgroup $\cong \mathbf{Z}_3 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3$. Then the number $N$ of solutions of the equation $x^{p^k} = a$ in $G$ is divisible by $p^3$.*

*Proof.* First assume that $G$ is *regular*. Then $\Omega_1(G) = \{ y \in G\colon\ y^p = 1\}$ is a subgroup of $G$. If $|\Omega_1(G)| \leq p^2$, then $G$ has at most $p + 1$ subgroups of order $p$ (since these subgroups must all lie in $\Omega_1(G)$). By [6, (11.6), p. 338], $G$ is then metacyclic, a contradiction. Thus, $|\Omega_1(G)| \geq p^3$. Fix an element $b \in G$ such that $b^{p^k} = a$. (We may assume that $b$ exists, for otherwise $N = 0$ and we have nothing to prove.) For any $x \in G$, the regularity of $G$ implies that $x^{p^k} = a = b^{p^k}$ iff $(b^{-1}x)^{p^k} = 1$ (see [14, p. 47]). Thus,

$$N = |\Omega_k(G)| \quad \text{where } \Omega_k(G) = \left\{ y \in G\colon\ y^{p^k} = 1 \right\}.$$

Since $\Omega_k(G)$ is a subgroup of $G$ containing $\Omega_1(G)$, we have $N = p^m$ for some $m \geq 3$.

Now let us treat case (i), where $p > 3$. By the above, we may assume that $G$ is irregular. Then by (3.2) $G$ has a normal $p$-elementary abelian subgroup $H$

of order $p^3$. If $p = 3$, we simply assume that such an $H$ exists, as in case (ii). In either case, taking $r = 3$ in (2.2), we are in the situation $p^k > r$. Applying the second conclusion of Theorem (2.2), we see that $N$ is divisible by $p^3$. Q.E.D.

To conclude this paper, let us make some remarks about the case when $p = 3$ and $k = 1$. We shall limit ourselves to the situation $a = 1$. In this case, we claim the following:

(A) *The theorem need not hold for* 3*-groups of order* $3^4$.

(B) *But the theorem remains valid for all* 3*-groups* (*as in* (3.3)(ii)) *of order* $> 3^4$.

An example for (A) is provided by the regular wreath product group $\mathbf{Z}_3 \wr \mathbf{Z}_3$. As we have mentioned earlier, this 3-group has a maximal (normal) subgroup $\cong \mathbf{Z}_3 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3$, but the number of solutions for $x^3 = 1$ is $3^2(6 - 1) = 45$ which is not divisible by 27. As for (B), we do not have a direct proof, but it is a special case of the following much more general statement (cf. [1]):

(3.4) THEOREM (Blackburn). *Let $G$ be a $p$-group which has a normal subgroup $H$ of order $p^p$ and exponent $p$. If $|G| \geq p^{p+2}$, then the number of solutions of the equation $x^p = 1$ in $G$ is divisible by $p^p$.*

This theorem is not explicitly stated in [1], but a careful analysis of the proofs of Corollary 2 and Theorem 6 in [1] shows that (3.4) is, in fact, what Blackburn has proved. This theorem applies, in particular, to $p$-groups which are neither regular nor of maximal class, because such groups always have order $\geq p^{p+2}$ [6, (10.11), p. 331], and Blackburn has shown earlier that they always have normal subgroups of order $p^p$ and exponent $p$. Also, it is worth noting that, for $p = 2$, (3.4) essentially coincides with the theorem of Alperin, Feit and Thompson referred to earlier in the remark following the proof of (3.1).

*Note added in proof.* The method of proof of Theorems (2.1) and (2.2) in this paper is already applicable under the more general assumption that $a \in G$ gives a $p$-element in the quotient group $G/C_G(H)$, say of order $p^m$. In this case, our method can be used to show that the number $N$ of solutions of the equation $x^{p^k} = a$ in $G$ is divisible by $p^d$ where $d$ is an integer $\geq r(p^k - 1)/p^{k+m}$. For $m = 0$, this gives back the estimate in (2.1). In any case, it is straightforward to show that $N$ is always divisible by $p^{\min(r, p^k - 1)}$ independently of $m$; this subsumes (2.2) as well as the last conclusion of (2.1). The nilpotency argument used in the proof of (2.2) can thus be avoided.

## REFERENCES

1. N. BLACKBURN, *Note on a paper of Berkovich*, J. Algebra, vol. 24 (1973), pp. 323–334.
2. YA.G. BERKOVICH, *On p-groups of finite order*, Sibirsk. Math., vol. 9 (1968), 1284–1306 (in Russian).

3. C. CURTIS, and I. REINER, *Representation theory of finite groups and associative algebras*, Interscience, J. Wiley, N.Y., 1962.
4. P. HALL, *A contribution to the theory of groups of prime power order*, Proc. Lond. Math. Soc., vol. 36 (1933), pp. 29–95.
5. _____, *On a theorem of Frobenius*, Proc. Lond. Math. Soc., vol. 40 (1936), pp. 468–501.
6. B. HUPPERT, *Endliche Gruppen*, Vol. 1, Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, New York, 1967.
7. A. KULAKOFF, *Über die Anzahl der eigentlichen Untergruppen und der Elemente von gegebener Ordnung in p-Gruppen*, Math. Ann., vol. 104 (1931), pp. 778–793.
8. _____, *Einige Bemerkungen zur Arbeit: "Form of the number of the subgroups of a prime power group" von G.A. Miller*, Rec. Math. (Mat. Sbornik), vol. 50 (1940), pp. 73–75.
9. T.Y. LAM, *Induction theorems for Grothendieck groups and Whitehead groups of finite groups*, Doctoral Dissertation, Columbia University, 1967.
10. _____, *Artin exponents of finite groups*, J. Algebra, vol. 9 (1968), pp. 94–119.
11. G.A. MILLER, *Form of the number of the subgroups of a prime power group*, Proc. Nat. Acad. Sci., vol. 9 (1923), pp. 237–238.
12. G.A. MILLER, H.F. BLICHFELDT and L.E. DICKSON, *Theory and applications of finite groups*, John Wiley and Sons, New York, 1916 (Reprinted by Dover Publications, 1961).
13. O.J. SCHMIDT, *A new proof of a group theoretic theorem of A. Kulakoff*, Rec. Math. [Mat. Sbornik], vol. 39 (1932), pp. 66–71 (in Russian).
14. M. SUZUKI, *Group theory*, Vol. 2, Grundlehren der Mathematischen Wissenschaften, Band 247, Springer-Verlag, New York, 1986.

UNIVERSITY OF CALIFORNIA
BERKELEY, CALIFORNIA