COUNTING GROUP ELEMENTS OF ORDER p MODULO p^2

MARCEL HERZOG

ABSTRACT. Let G be a finite group of order divisible by the prime p . It is shown that the number of elements of G of order p is congruent to -1 modulo p^2 , unless a Sylow p -subgroup of G is cyclic, generalized quaternion, dihedral or quasidihedral.

1. Introduction. In this paper G denotes a finite group, $I_p(G)$ is the set of elements of G of order p and $i_p(G) = |I_p(G)|$. This research originated from an effort to find an elementary proof to the following theorem: if S is a 2-group and if $i_2(S) \equiv 1 \pmod{4}$, then S is cyclic, generalized quaternion, dihedral or quasidihedral. A character theoretical proof, attributed to Alperin, Feit and Thompson, was published in the very interesting book of Isaacs [4, Theorem 4.9]. It appears to be a simplification of Thompson's proof given in [5, Theorem 6.2]. Having found a simple elementary proof of that theorem (basically our Lemma 5), we discovered that a different elementary proof was given by Ja. G. Berkovič in [1, Corollary 5.3]. Moreover, N. Blackburn [2] generalized Berkovič's results from 2-groups to p -groups, using a method similar to ours. The aim of this paper is to determine $i_p(G)$ modulo p^2 for an arbitrary finite group G (Theorem 3 in §3). For $p > 2$ the theorem is known [3, Theorem 4.6]; our short, straightforward proof (basically Lemma 4) is given here for completeness' sake.

Our only nonstandard notation is E_{p^n} for an elementary abelian group of order p^n .

We shall use extensively the following well-known fact (see, for example, [6, Proposition 9.5]): If S is a p -group, and S is not cyclic, generalized quaternion, dihedral or quasidihedral, then S has a normal E_{p^2} .

2. $i_p(G)$ modulo p . The following theorem is well known.

THEOREM 1. *If $p \mid |G|$, then:*

$$(1) \quad i_p(G) \equiv -1 \pmod{p}.$$

PROOF. Let $E \equiv E_{p^n}$ be an elementary abelian p -group of maximal order in G . As $p \mid |G|$, $n \geq 1$. Let E act on $I_p(G)$ by conjugation, and let f be the number of fixed points. Since the length of each E -orbit divides p^n , $i_p(G) \equiv f \pmod{p}$. However, by the maximality of E , it fixes exactly its own $p^n - 1$

Received by the editors March 3, 1977.

AMS (MOS) subject classifications (1970). Primary 20D25.

Key words and phrases. Finite group, element of order p .

© American Mathematical Society 1977

elements in $I_p(G)$. Thus:

$$i_p(G) \equiv f = p^n - 1 \equiv -1 \pmod{p}.$$

3. $i_p(G)$ modulo p^2 . For proving the main result we also need the following reduction theorem.

THEOREM 2. *Let $E \cong E_{p^n}$ be a subgroup of G , and let $T \equiv I_p(N_G(E))$ and $D \equiv I_p(G) \setminus T$. Suppose that:*

- (2) *if $a \in D$ and $H = C_E(a) \times \langle e \rangle$ for some $e \in E \setminus C_E(a)$, then $a \notin N_G(H)$.*

Then:

$$i_p(G) \equiv |T| \pmod{p^n}.$$

PROOF. Clearly if $a \in D$ then $a^x e \in D$ for every $x \in E$ and $e \in C_E(a)$.

Define a relation $\sim$ on D as follows: for $a, b \in D$, $a \sim b$ if $b = a^x e$ for some $x \in E$ and $e \in C_E(a)$. We claim that:

- (i) $\sim$ is an equivalence relation.

This follows easily from the fact that if $a \in D$, $x \in E$ and $e \in C_E(a)$, then $f \in E$ centralizes $a^x e$ if and only if it centralizes a .

Thus D is a disjoint union of equivalence classes with respect to $\sim$. Let $a \in D$, F be the equivalence class to which a belongs, $E_1 \equiv C_E(a)$ and $E = E_1 \times E_2$. Clearly

$$F = \{a^x e | x \in E_2, e \in E_1\}.$$

We claim that:

- (ii) $|F| = p^n$.

In order to prove (ii) it suffices to show that if $a = a^x e$, where $x \in E_2$ and $e \in E_1$, then $x = 1$. As $a = x^{-1} a x e$, it follows that $a^{-1} x a = x e$, hence $a \in N_G\langle x, E_1 \rangle$. By (2) $x \in E_1 \cap E_2 = 1$, as required.

It follows from (ii) that $|D| \equiv 0 \pmod{p^n}$. Thus

$$i_p(G) = |D| + |T| \equiv |T| \pmod{p^n}.$$

REMARK. Condition (2) of Theorem 2 is satisfied in the following cases (S denotes here a Sylow p -subgroup of G):

- (i) $|E| < p^2$;
- (ii) S is abelian;
- (iii) $\Omega_1(S)$ is abelian;
- (iv) S is a TI -group, $E \triangleleft S$.

PROOF. (i) If $a \in N_G(H)$, then $H \neq E$, hence $|E| = p^2$ and $|H| = p$. But then $H \subseteq C_E(a)$, a contradiction.

- (ii) Follows from (iii).

(iii) If $a \in N_G(H)$, then $\langle a, H \rangle \subseteq \Omega_1(S^g)$ for some $g \in G$. Thus $H \subseteq C_E(a)$, a contradiction.

- (iv) If $a \in N_G(H)$ then $a \in S$, hence $a \in T$, a contradiction.

We state now our main result.

THEOREM 3. *Suppose that $p \mid |G|$ and let S be a Sylow p -subgroup of G . Then the following statements hold.*

(a) *If $|S| = p$, then;*

$$(3) \quad i_p(G) \equiv rp - 1 \pmod{p^2}$$

where $0 \leq r \leq p - 1$. Moreover, there exist groups satisfying (3) with respect to each such r .

(b) *If $|S| > p$ and S is cyclic, generalized quaternion, dihedral or quasidihedral, then:*

$$(4) \quad i_p(G) \equiv p - 1 \pmod{p^2}.$$

(c) *Otherwise,*

$$(5) \quad i_p(G) \equiv -1 \pmod{p^2}.$$

PROOF. We shall prove Theorem 3 in a series of lemmas.

LEMMA 1. *If $|S| = p$, then (a) holds.*

PROOF. In view of Theorem 1, it suffices to construct examples in which (3) holds for every r between 0 and $p - 1$. By Dirichlet's theorem, there exists a prime $q > p$ such that

$$q \equiv (1 - r)p + 1 \pmod{p^2}.$$

As $q \equiv 1 \pmod{p}$, there exists a Frobenius group G of order pq . Clearly:

$$i_p(G) = (p - 1)q \equiv (p - 1)((1 - r)p + 1) \equiv rp - 1 \pmod{p^2}.$$

LEMMA 2. *If $|S| > p$ and S is either cyclic or generalized quaternion, then $i_p(G) \equiv p - 1 \pmod{|S|}$. In particular, (4) holds.*

PROOF. Let S act on $I_p(G)$ by conjugation. Clearly there are $p - 1$ fixed points, consisting of the elements of $I_p(S)$, and the other orbits are of length $|S|$. The lemma follows.

LEMMA 3. *Suppose that S is either dihedral or quasidihedral. Then (4) holds.*

PROOF. There exists $E \cong E_{2^2} \subseteq S$. By Theorem 2 and the Remark, it suffices to prove Lemma 3 under the assumption: $E \triangleleft G$. The structure of S forces it to be dihedral of order 8. As $E \triangleleft G$,

$$(6) \quad i_2(G) = i_2(E) + \sum (i_2(P) - i_2(E)) = 3 + \sum 2,$$

the summation ranging over all Sylow 2-subgroups P of G . As G has an odd number of P , we get

$$i_2(G) \equiv 3 + 2 \equiv 1 \pmod{4},$$

as required.

LEMMA 4. *Suppose that $p > 2$ and S is noncyclic. Then (5) holds.*

PROOF. There exists $E = E_{p^2} < S$. By Theorem 2 and the Remark, it suffices to prove Lemma 4 under the assumption: $E \triangleleft G$. If $x \in G \setminus E$ and

$x^p \in E$, then $\langle x, E \rangle$ is a regular group of order p^3 and distinct groups of this type intersect in E . Letting Σ range over all such subgroups of G , we get:

$$(7) \quad i_p(G) = i_p(E) + \sum (i_p\langle x, E \rangle - i_p(E)).$$

As $i_p(E) = p^2 - 1$ and $i_p\langle x, E \rangle = p^2 - 1$ or $p^3 - 1$ (as $\langle x, E \rangle$ is regular), (7) yields (5).

LEMMA 5. *Suppose that $p = 2$ and S is none of the following: cyclic, generalized quaternion, dihedral or quasidihedral. Then (5) holds.*

PROOF. There exists $E \equiv E_{2^2} \triangleleft S$ and as S is not dihedral, $C_S(E) \supset E$. By Theorem 2 and the Remark, it suffices to prove Lemma 5 under the assumption: $E \triangleleft G$. As in Lemma 4, we get

$$(8) \quad i_2(G) = 3 + \Sigma_1 (i_2\langle x, E \rangle - 3) + \Sigma_2 (i_2\langle y, E \rangle - 3),$$

where $3 = i_2(E)$, Σ_1 ranges over different $\langle x, E \rangle$ with $x \in C_G(E) \setminus E$, $x^2 \in E$ and Σ_2 ranges over different $\langle y, E \rangle$ with $y \in G \setminus C_G(E)$, $y^2 \in E$. Each $\langle x, E \rangle$ is regular, hence $i_2\langle x, E \rangle = 3$ or 7 . Thus $\Sigma_1 \equiv 0 \pmod{4}$ and it suffices to show that $\Sigma_2 \equiv 0 \pmod{4}$. Each $\langle y, E \rangle$ is a dihedral group of order 8, hence $i_2\langle y, E \rangle - 3 = 5 - 3 = 2$ and it suffices to show that r_2 , the number of summands in Σ_2 , is even. As $2 \mid |C_G(E)/E|$, Theorem 1 yields:

$$r_2 = i_2(G/E) - i_2(C_G(E)/E) \equiv 1 - 1 = 0 \pmod{2},$$

as required.

Theorem 3 follows from Lemmas 1–5.

Note. It follows from (5) and the fact that $(p-1) \mid i_p(G)$, that:

$$i_p(G) = p^2 - 1 + b(p-1)p^2,$$

where b is a nonnegative integer.

REFERENCES

1. Ja. G. Berkovič, *On p -groups of finite order*, Sibirsk. Math. Ž. **9** (1968), 1284–1306.
2. N. Blackburn, *Note on a paper of Berkovich*, J. Algebra **24** (1973), 323–334.
3. P. Hall, *On a theorem of Frobenius*, Proc. London Math. Soc. **40** (1936), 468–501.
4. I. M. Isaacs, *Character theory of finite groups*, Academic Press, New York, 1976.
5. T. Lam, *Artin exponent of finite groups*, J. Algebra **9** (1968), 94–119.
6. D. Passman, *Permutation groups*, Benjamin, New York, 1968.

DEPARTMENT OF MATHEMATICS, INSTITUTE OF ADVANCED STUDIES, AUSTRALIAN NATIONAL UNIVERSITY, CANBERRA, AUSTRALIA