TWO PROBLEMS ON FINITE GROUPS
WITH \( k \) CONJUGATE CLASSES

JOHN POLAND

(Received 5 September 1966)

1. Introduction

Let \( G \) be a finite group of order \( g \) having exactly \( k \) conjugate classes. Let \( \pi(G) \) denote the set of prime divisors of \( g \). K. A. Hirsch [4] has shown that

\[ g \equiv k \mod 2 \operatorname{G.C.D.}\{(p^2 - 1) \mid p \in \pi(G)\} \] (provided \( 2 \nmid g \)).

By the same methods we prove \( g \equiv k \mod \operatorname{G.C.D.}\{(p - 1)^2 \mid p \in \pi(G)\} \) and that if \( G \) is a \( p \)-group, \( g \equiv k \mod (p - 1)(p^2 - 1) \). It follows that \( k \) has the form \((n + r(p - 1))(p^2 - 1) + p^e\) where \( r \) and \( n \) are integers \( \geq 0 \), \( p \) is a prime, \( e \) is 0 or 1, and \( g = p^{2n+e} \). This has been established using representation theory by Philip Hall [3] (see also [5]). If

\[ \delta = \operatorname{G.C.D.}\{(p - 1)(p^2 - 1) \mid p \in \pi(G)\} \]

then simple examples show (for \( 6 \nmid g \) obviously) that \( g \equiv k \mod \delta \) or even \( \delta/2 \) is not generally true.

If \( G \) is a \( p \)-group, W. Burnside [2] and N. Blackburn [1] have shown that the statements \( G \) has a conjugate class of maximum order and \( G \) has maximum nilpotent class are equivalent. It seems reasonable that if \( G \) has minimum (conjugate) class number it would have classes of maximum order; indeed, we show that if \( g = p^m \) (\( m = 2n+e \)) and \( k = n(p^2-1) + p^e \) then \( G \) has maximum nilpotent class, and we calculate exactly how many classes \( G \) has of each order. Such strong conditions hold for these groups that we can show that they only exist for \( m < p+3 \). This extends some results we obtained in [5] for 2-groups.

2. Background

Let \( G \) denote a finite group of order \( g \), where \( g \) has prime decomposition \( g = \prod_{i=1}^{n}(p_i^{m_i}) \), and let \( \pi(G) = \{p_i \mid i = 1, \ldots, n\} \) be the set of primes dividing \( g \). The number of conjugate classes of \( G \) will be denoted by \( k(G) \);
often we will simply say that \( k \) is the number of classes of \( G \). The classes of \( G \) are denoted \( K_i \) \((i = 1, \ldots, k)\), as usual ordered, with \( K_1 = \{1\} \); \( K(x) \) means the class containing \( x \). We denote the lower central series of \( G \) by \( G \triangleright \gamma_2 \triangleright \gamma_3 \triangleright \cdots \) (\( \gamma_1 \) is left undefined) and the upper central series by \( \{1\} \triangleleft Z_1 \triangleleft Z_2 \triangleleft \cdots \). The group generated by \( x, y, \cdots \) is denoted \( \langle x, y, \cdots \rangle \).

Most of this paper will be concerned with \( p \)-groups; that is, \( \pi(G) = \{p\} \) and \( g = p^m \). The phrase "\( G \) of order \( p^m \)" will mean that \( G \) is a group, \( p \) a prime, and \( m \) a positive integer; we will write \( m = 2n + e \) to denote that \( m \) and \( n \) are integers \( \geq 0 \) and \( e \) is 0 or 1. In this context we define the function \( f \) by \( f(p^m) = n(p^2 - 1) + p^e \), an important expression. The ordered set \((a_0, a_1, \cdots, a_l)\) is called the \( p \)-class vector of the \( p \)-group \( G \) and is used to indicate that \( G \) has exactly \( a_i \) classes of order \( p^i \) \((0 \leq i \leq l)\) and no classes of order greater than \( p^l \).

If \( G \) has order \( p^m \), it is well-known (Blackburn [1], p. 52) that \( G \) has nilpotent class at most \( m - 1 \). If \( G \) has maximum nilpotent class \((m - 1)\) then we return to Blackburn (pp. 54 and 57) for the following concepts. Define \( \gamma_1 = \gamma_1(G) \) by \( \gamma_1 \gamma_4 = C_{\gamma_1 \gamma_4} \gamma_4 \); then \( G \) has the characteristic series \( G \triangleright \gamma_1 \triangleright \gamma_2 = Z_{m-2} \triangleright \gamma_3 = Z_{m-3} \triangleright \cdots \triangleright \gamma_{m-1} = Z_1 \triangleright 1 \) in which successive distinct terms have factor groups of order \( p \). \( G \) is said to have maximum degree of commutativity \( c(G) = c \) if \( \gamma_i, \gamma_j \leq \gamma_{i+j+c} \) for all \( i, j = 1, 2, 3, \cdots \) and \( c \) is the maximum such integer; obviously \( c \geq 0 \).

Burnside ([2], section 98) has shown that the conjugate classes of a non-abelian group \( G \) of order \( p^m \) all have order at most \( p^{m-2} \). In fact the statements that \( G \) contains a class of maximum order and that \( G \) has maximum nilpotent class are equivalent:

2.1 Theorem. (Burnside [2], section 98). If \( G \) is a non-abelian group of order \( p^m \) containing a conjugate class of order \( p^{m-2} \) then \( G \) has nilpotent class \( m - 1 \).

2.2 Theorem. Let \( G \) be a non-abelian group of order \( p^m \) with nilpotent class \( m - 1 \). Then

(i) \( G \) has \( p \)-class vector \((p, p^2 - 1)\) if \( m = 3 \), \((p, p^2 - 1, p^2 - p)\) if \( m = 4 \), and \((p, p^2 - 1, p^2 - p)\) or \((p, p^2 - 1, 0, p^2 - p)\) if \( m = 5 \),

(ii) (Blackburn [1], 2.11 and 3.8) \( c(G) > 0 \) if \( m \) is odd, \( m = 4 \), or \( m \geq p + 2 \), and so

(iii) \( c(G/Z) > 0 \) if \( m \geq 4 \),

(iv) (Blackburn [1], 2.8) \( c(G) > 0 \) if and only if \( \gamma_1 = C_G(Z_2) \), and

(v) (Blackburn [1], 2.14 and the corollaries of 2.15) \( G \) has exactly \((p^2 - p)\) conjugate classes of order \( p^{m-2} \) if \( c(G) > 0 \), and \((p-1)^2\) otherwise.
3. The relation \( g \equiv k \)

K. A. Hirsch [4] has shown that \( g \equiv k \) modulo \( 2 \) (G.C.D. \((p^2-1) \mid p \in \pi(G)\)) if \( g \) is odd, and modulo \( 3 \) if \( g \) is even but \( 3 \nmid g \). Also, for \( p \)-groups, Philip Hall [3] proved by representation theory that \( k = (n+r(p-1))(p^2-1)+p^e \), where \( g = p^{2n+e} \) and \( r \geq 0 \). In this section we wish to use Hirsch's extremely elementary group-theoretic approach to establish Hall's theorem and, in some cases, improve Hirsch's results. Throughout, let \( \delta = \delta(G) = \text{G.C.D.} \{(p^2-1)(p-1) \mid p \in \pi(G)\} \). We assume \( 6 \nmid g \), so that \( \delta > 1 \).

3.1 Lemma. Let \( \{1\} = H_1, H_2, \ldots, H_t \) be the set of all cyclic primary subgroups of \( G \), \( |H_i| = q^i, q \in \pi(G) \), for \( i > 1 \), and let \( \rho(1) = 1, \rho(H_i) = q^{2^{(i-1)}}(q^2-1) \). Then \( gk \equiv \sum_{i=1}^{t} \rho(H_i) \) and \( \rho(H_i) \equiv q^2-1 \) (for \( i > 1 \)) modulo \( 8 \).

Proof. This is equivalent to a statement of Hirsch [4]; we outline the proof. We note first that \( q(q^2-1) \equiv (q^2-1) \) modulo \( (q-1)(q^2-1) \) so that the last statement is proved.

The number of solutions \( x, y \in G \) of the equation \([x, y] = 1\) is \( \sum_{x \in G} \lambda_0([C_G(x)]) = \sum_{i=1}^{k}(|K_i|)(g/[K_i]) = gk \). The pair \((x, y) \neq (1, 1)\) is a solution of \([x, y] = 1\) if and only if it is a generator of an abelian subgroup \( H \) of \( G \), so \( gk = \sum_{H \text{ abelian}, \rho(H) \leq \delta} \rho(H) \) where \( \rho(H) \) is the number of pairs of generators of \( H \). Let \( H = \prod_{i=1}^{t} H_i, H_i \) a \( p \)-group. Then \( \rho(H) = \prod_{i=1}^{t} \rho(H_i) \) while if \( H_i \) is an abelian \( p \)-group of type \((p^e_1, p^e_2), (p^e_2, p^e_3), \ldots, (p^e_{t-1}, p^e_t)\) then \( \rho(H_i) \equiv \prod_{i=1}^{t} \rho(H_i) \). Since \( (p^e_i-1)(p^e_{i+1}-1) \equiv 0 \) modulo \( \delta \), we are done.

Recall we defined \( f(p^{2n+e}) = n(p^2-1)+p^e \).

3.2 Lemma. \( p^m \equiv f(p^m) \) modulo \( (p^2-1)(p-1) \).

Proof. This is trivially true if \( m \) is 1 or 2. If \( m \geq 3 \), \( f(p^m) = p^{m-2}+p^m-2 \) (\( p^2-1 \)) \equiv \delta \) modulo \( (p^2-1)(p-1) \). Therefore \( p^{2n+e} = (p^e)(p^{2n}) \equiv (p^e)(p^0+n(p^2-1)) \equiv p^e+n(p^2-1) \) modulo \( (p^2-1)(p-1) \).

3.3 Corollary. If \( g = \prod_{i=1}^{t} p_i^{m_i} \) then \( g^2 \equiv 1+\sum_{i=1}^{t} m_i(p^2-1) \) modulo \( \delta \).

Proof. \( g^2 = \prod_{i=1}^{t} p_i^{2m_i} = \prod_{i=1}^{t} (1+m_i(p^2-1)) \equiv 1+\sum_{i=1}^{t} m_i(p^2-1) \) since \( (p_i^2-1)(p_i^2-1) \equiv 0 \) modulo \( \delta \).

The following lemma is of some interest in itself, and is modelled on one of Hirsch ([4], p. 99).

3.4 Lemma. If \( p^m \mid g, p \) odd, and \( t \) is the number of non-trivial cyclic \( p \)-subgroups of \( G \) then \( G \) contains exactly \( \mu p^m \) solutions of the equation \( x^{p^m} = 1 \), \((p-1) \mid (\mu-1)\), and \( t \equiv m+(\mu-1)(p-1) \) modulo \( (p-1) \).

Proof. By Frobenius' Theorem, \( G \) has \( \mu p^m \) solutions of \( x^{p^m} = 1 \). Each non-trivial solution generates a non-trivial cyclic \( p \)-group. Let \( G \) have \( \lambda_i \)
cyclic subgroups of order $p^i$; each has $\varphi(p^i)$ generators. Therefore $\sum_{i \geq 1} (\lambda_i p^{i-1}(p-1)) = \mu p^m - 1 = \mu(p^{m-1} + (\mu - 1)).$ It follows that $(p-1)|(\mu - 1)$ and $\sum_{i \geq 1} (\lambda_i p^{i-1}) = \mu(p^{m-1} + p^{m-2} + \cdots + p + 1 + (\mu - 1))(p-1).$ Since $\mu$ and $p$ are congruent to 1 modulo $(p-1)$, we have $\sum_{i \geq 1} \lambda_i \equiv m + (\mu - 1)/(p-1) \text{ modulo } (p-1)$.

3.5 Corollary. If $G$ has a normal $p$-Sylow subgroup of order $p^m$ ($p \neq 2$) and $t$ is the number of non-trivial cyclic $p$-subgroups of $G$, then $t \equiv m \text{ modulo } p-1$.

3.6 Corollary. If $G$ is a nilpotent group, $g$ odd, then $g \equiv k \text{ modulo } \delta$.

Proof. By Corollary 3.5, we have, in Lemma 3.1, $gk \equiv 1 + \sum_{i \geq 1} m_i (p^i - 1).$ By Corollary 3.3, $gk \equiv g^2 \text{ modulo } \delta$, and the corollary follows since $(g, \delta) = 1$.

By Corollary 3.5 and Lemma 3.2 we have shown that $k = (n + r(p-1)) (p^2 - 1) + p^s$ for a group $G$ of order $p^m$ ($p$ odd, $m = 2n + c$) where $r$ is an integer. By Hirsch's theorem, this is also true for $p = 2$. We will have proved Hall's theorem if we can show that $k \geq f(p^m)$. This is established in (5) but the following useful lemma, which is quite easy to prove, also shows that $r \geq 0$.

Let $f_r(p^{2n+e}) = (n + r(p-1))(p^2 - 1) + p^s$.

3.7 Lemma. Let $G$ have order $p^m$ and let $H$ be a normal subgroup of $G$ of order $p$. If $k(G) \leq f_r(p^m)$, then $k(G/H) \leq f_r(p^{m-1})$; if $k(G/H) \geq f_r(p^{m-1})$, then $k(G) \geq f_r(p^m)$.

Proof. It is straightforward that $f_r(p^m) = f_{r+1}(p^{m-1}) + (-1)^e(1-p)$. Hence $f_r(p^m) < f_{r+1}(p^{m-1})$, or $f_r(p^m) > f_{r-1}(p^m)$. Since $k(G/H) \leq k(G)$, then, if $k(G) \leq f_r(p^m)$, $k(G/H) < f_r(p^m) < f_{r+1}(p^{m-1})$ and so $k(G/H) \leq f_r(p^{m-1})$. Similarly if $k(G/H) \geq f_r(p^{m-1})$ then $k(G) \geq f_r(p^m)$.

This latter statement, combined with the fact that (obviously) $k(G) \geq f(g)$ for groups of order $p$, $p^2$, and $p^3$ gives us by induction

3.8 Corollary. If $G$ has order $p^m$ then $k(G) = (n + r(p-1))(p^2 - 1) + p^s$, $r \geq 0$.

We would like to show that $g \equiv k \text{ modulo } \delta$ for all groups ($6 \nmid g$). By Lemma 3.1 and Corollary 3.3, it seems we would need to extend Corollary 3.5: if $p^m \nmid g$, $p \neq 2$, and $t$ is the number of cyclic non-trivial $p$-subgroups of $G$ then $t \equiv m \text{ modulo } p-1$. We present some counterexamples to these conjectures.

Let $p$ and $q$ be primes such that $p | (q-1)$, and let $1 < \alpha < q$ be such that $\alpha^q \equiv 1 \text{ modulo } q$ then $p | \beta$. Let $Fr(p, q)$ denote the (Frobenius) group $G = \langle x, y \mid x^p = y^q = 1, y^x = y^\alpha \rangle$. Then $G = Fr(p, q)$ contains exactly $q$ $p$-Sylow subgroups, $g = pq$, and the number of non-trivial cyclic
Finite groups with \( k \) conjugate classes

\( p \)-subgroups of \( G \) is \( q \). But it is not necessarily true (for example: \( p = 7, q = 29 \)) that \( q \equiv 1 \) modulo \( p-1 \), or even modulo \( (p-1)/2 \), so Corollary 3.5 cannot be extended to all groups, except in the form of Lemma 3.4. If \( p = 61, q = 367 \), then \( g = 22,387, k = 67, g-k = 22,320 = 16 \cdot 9 \cdot 5 \cdot 31 \), while \( \delta = 32 \cdot 9 \) so that \( g \equiv k \) modulo \( \delta/2 \) but not \( \delta \). If \( p = 7, q = 71 \), then \( g = 497, k = 17, g-k = 480 = 32 \cdot 3 \cdot 5 \), while \( \delta = 32 \cdot 9 \) so that \( g \equiv k \) modulo \( \delta/3 \) but not \( \delta \).

Although we cannot show that \( g \equiv k \) modulo \( \delta \) or even \( \delta/2 \) in general then, we can still extend Hirsch’s result slightly.

3.9 Proposition. \( g \equiv k \) modulo \( \text{G.C.D.}\{(p-1)^2 \mid p \in \pi(G)\} \) if \( g \) is odd.

Proof. Let

\[ \tau = \text{G.C.D.}\{(p-1)^2 \mid p \in \pi(G)\} = \left[ \text{G.C.D.}\{(p-1) \mid p \in \pi(G)\} \right]^2 \]

say. As every element of \( G \) generates a cyclic subgroup of \( G \),

\[ g = \sum_{H \text{cyclic}} \varphi(|H|) = \sum_{i=1}^{\lambda} \varphi(|H_i|) \]

modulo \( \tau \), where \( H \) and \( \lambda \) are as in Lemma 3.1, taking \( \varphi(1) = 1 \). Note that if \( |H_i| = q_i^t, q_i \in \pi(G) \), then \( \varphi(|H_i|) = q_i^t - 1 \equiv q_i - 1 \) modulo \( \tau \). Therefore \( g^2 = \left[ 1 + \sum_{i=2}^{\lambda} (q_i - 1)^2 \right] = 1 + \sum_{i=2}^{\lambda} (q_i - 1) = 1 + \sum_{i=2}^{\lambda} (q_i + 1)(q_i - 1) \equiv gk \) modulo \( \tau \) by Lemma 3.1. Since \( (g, \tau) = 1 \), the proposition follows.

3.10 Corollary. \( g \equiv k \) modulo \( \text{L.C.M.}[\text{G.C.D.}\{(p-1)^2 \mid p \in \pi(G)\}], 2(\text{G.C.D.}\{p^2 - 1 \mid p \in \pi(G)\}) \) if \( g \) is odd.

Proposition 3.9 says, for example, if \( \pi(G) = \{19, 37\} \), then \( g \equiv k \) modulo \( 18^2 \), whereas Hirsch’s theorem states \( g \equiv k \) modulo \( 16 \cdot 18 \).

4. \( k(G) = f(g) \)

In this section, \( G \) will always denote a group of order \( p^m \), \( p \) prime. We have shown that if \( f_r(p^m) = (n+r(p-1))(p^2-1)+p^e \) (where \( m = 2n+e \)), then \( k(G) = f_r(p^m) \) for some integer \( r \geq 0 \). Denote \( f_0(p^m) \) by \( f(p^m) \); what is the structure of \( G \) if \( k(G) = f(g) \)?

4.1 Lemma. Let \( N \) be a normal subgroup of \( G \) of order \( p \). Let \( k(G/N) = f_r(p^{m-1}), c(G) = f_r(p^m) \), and let \( G/N \) have \( p \)-class vector \((a_0, a_1, \ldots, a_\lambda)\). Then \( G \) has \( p \)-class vector \((\lambda^{p-1}, (a_0 - 1) + (e - 1)(p - 1), a_1, a_2, \ldots, a_\lambda) \) or \((\lambda, (a_0 - 1), a_1, \ldots, a_{i-1}, a_i + (1 - e)(p^2 - p), a_{i+1} + (e - 1)(p - 1), a_{i+2}, \ldots, a_\lambda)\) for some \( 0 \leq i < \lambda \).

Proof. Let \( \xi \) be the canonical map of \( G \to G/N \) and let \( \overline{K} \) be any conjugate class of \( G/N \). If \( 1 \neq \xi(x) \in \overline{K} \) then \( \xi^{-1}(\overline{K}) = K(x) \cdot N \) is a union of classes of \( G \), and since \( |N| = p \), \( \xi^{-1}(\overline{K}) \) then must be a single class of \( G \).
or a union of $p$ classes of $G$ (obviously $\xi^{-1}(1) = N$ is a union of $p$ classes of order 1). $\xi^{-1}(\bar{K}) \neq N$ is a union of $p$ classes of $G$ if and only if $\bar{K}$ is, where $\bar{x} \in \bar{K}$ and $\bar{x}^p \in \bar{K}'$ for some $1 < a < p$, so this happens in sets of $p-1$ classes of the same order, over $G/N$. If we let $\beta$ denote the number of such sets, then $k(G) = k(G/N) + (p-1) + \beta[\beta(p-1) - (p-1)]$. Straightforward substitution shows that if $m = 2n+e$, $\beta = 1 - e$, and we are done.

4.2 Theorem. If $G$ has order $p^m$ ($m > 1$) and $k(G) = f(p^m)$ then $G$ has nilpotent class $m-1$.

Proof. The theorem is obviously true for $m = 2$ and 3, so suppose $m > 3$, $k(G) = f(p^m)$, and that the theorem is proved for all groups of order $p^{m-t}$ ($1 \leq t \leq m-2$). Take $N \leq Z_1(G)$, $|N| = p$. By Lemma 3.7 and Corollary 3.8, $k(G/N) = f(p^{m-1})$. By the induction hypothesis, $G/N$ has maximum nilpotent class, so by part (v) of Theorem 2.2, $G$ has $p^2 - p$ classes of maximum order, or $(p-1)^2$ perhaps if $p > 2$. By Lemma 4.1 then $G$ has $(p^2 - p) - (p-1)$, or $(p-1)^2 - (p-1)$ if $p > 2$, classes of order $p^{m-2}$, at least; that is, $G$ has at least one class of maximum order. The theorem follows by Theorem 2.1.

The $p$-Sylow subgroup of Sym($p^2$) shows that the converse of Theorem 4.2 is not true. In fact, we must place rather strong conditions upon $G$ in order that $k(G) = f(g)$.

4.3 Theorem. If $k(G) = f(p^m)$ for a group $G$ of order $p^m$ ($m \geq 3$) then either

(i) $c(G) = 0$ and $G$ has $p$-class vector

\[
(p, p-1, \ldots, p-1, p^2-\bar{p}, \ldots, p^2-\bar{p}, 2(p^2-\bar{p}), (p-1)^2) \text{ if } n \geq 4,
\]

or $(p, p-1, p-1, 2p^2-p-1, (p-1)^2)$ if $n = 3$; or

(ii) $c(G) = 1$; for $1 \leq i \leq m-2$, if $x \in \gamma_i - \gamma_{i+1}$ then $C_G(x) = \langle x, \gamma_{m-i-1} \rangle$ and $x^p \in \gamma_{m-i-1}$; and $G$ has $p$-class vector

\[
(p, p-1, \ldots, p-1, p^2-\bar{p}, \ldots, p^2-\bar{p}).
\]

Proof. Since each $\gamma_i$ is a normal subgroup of $G$ and so a union of conjugate classes of $G$, then $G - \gamma_1$ and $\gamma_i - \gamma_{i+1}$ ($i > 0$) are unions of classes of $G$. Note that $|\gamma_i| = p^{m-i}$.

First, suppose $c(G) > 0$. By part (v) of Theorem 2.2, $G - \gamma_1$ splits into $p^2 - p$ classes of $p^{m-2}$ elements each. Since $[\gamma_i, \gamma_j] \leq \gamma_{i+j-1}$ then $[\gamma_i, \gamma_{m-i}] = 1$ so if $x \in \gamma_i - \gamma_{i+1}$ then $C_G(x) \cong \langle x, \gamma_{m-i-1} \rangle$. Now $x \in \gamma_{m-i-1}$ if and only if $i \leq (m-1)/2$. Therefore if $1 \leq i < n$, then $|C_G(x)| \geq p \cdot i + 1$ so $|K(x)| \leq p^{m-i-2}$. It follows that $\gamma_i - \gamma_{i+1}$ splits into at least $(p^{m-i} - p^{m-2})/p^{m-i-2} = p^2 - p$ classes of $G$ if $1 \leq i \leq n$. In the same
way if \( n \leq i \leq m \), \( \gamma_i - \gamma_{i+1} \) splits into at least \( p-1 \) classes. Finally \( \gamma_m = \{1\} \) is a class of \( G \). Therefore \( k(G) \geq n(p^2 - p) + (m-n)(p-1) + 1 = f(p^m) \), with equality only if \( x \in \gamma_i - \gamma_{i+1} \) implies that \( C(x) = \langle x, \gamma_{m-i-1} \rangle \) and \( x^p \in \gamma_{m-i-1} \) for \( i = 1, \ldots, m-2 \). In particular \( \{\gamma_2, \gamma_m-3\} = 1 \) but \( \{\gamma_1, \gamma_m-3\} \neq 1 \) so \( c(G) = 1 \). We note that we have \( \gamma_{n-1} - \gamma_n \) splitting into \( p^2 - p \) classes of order \( p^{m-n-2} \) and \( \gamma_n - \gamma_{n+1} \) splitting into \( p-1 \) classes of the same order. To summarize, \( G \) must have \( p \)-class vector

\[
(p, p-1, \ldots, p-1, p^2-p, \ldots, p^2-p).
\]

Suppose now \( c(G) = 0 \). By part (ii) of Theorem 2.2 \( m = 2n \) and \( 6 \leq m \leq p+2 \), while by part (iii), \( c(G/Z) > 0 \). By Lemma 3.7 and Corollary 3.8, \( k(G/Z) = f(p^{m-1}) \). Hence we can apply the above results and \( G/Z \) must have \( p \)-class vector

\[
(p, p-1, \ldots, p-1, p^2-p, \ldots, p^2-p).
\]

Now by part (v) of Theorem 2.2, \( G \) has exactly \( (p-1)^2 = (p^2-p) - (p-1) \) classes of order \( p^{m-2} \). The \( p \)-class vector of \( G \) now follows by Lemma 4.1, and we are done.

4.4 Theorem. If \( G \) is a group of order \( p^m \) and \( m \geq p+3 \) then \( k(G) \geq f_1(p^m) \).

Proof. Suppose \( g = p^m, m \geq p+3 \), and \( k(G) = f(p^m) \). Define \( s \) and \( s_1 \) as generators of \( G \) modulo \( \gamma_1 \) and \( \gamma_1 \) modulo \( \gamma_2 \) respectively; define \( s_i = [s_{i-1}, s] \) for \( i > 1 \). Blackburn ([1], 2.9 and 3.8) has shown that \( s_i \) and \( \gamma_{i+1} \) generate \( \gamma_i \) then because of Theorem 4.2. By Theorem 4.3, \( s_i^p \in \gamma_{m-2} \subseteq \gamma_{p+1} \) since \( m \geq p+3 \). Therefore \( s_i^p s_j \notin \gamma_{p+1} \), contradicting Lemma 3.3 of Blackburn. The theorem follows by Corollary 3.8.

The case of \( p = 2 \) and \( k(G) = f_1(g) \) has been examined in [5].

Bibliography


Institute of Advanced Studies
Australian National University
Canberra, A.C.T.