The number of subgroups of a finite group (II)

The number of subgroups of a finite group (II)

Yugen Takegahara

Muroran Institute of Technology, 27-1 Mizumoto, Muroran 050-8585, Japan
E-mail: yugen@mmm.muroran-it.ac.jp

Let A be a finite group, and let p be a prime. Suppose that p^s is the highest power of p dividing $|A/A'|$, where A' is the commutator subgroup of A, and that the type $\lambda = (\lambda_1, \lambda_2, \ldots)$ with $\lambda_1 \geq \lambda_2 \geq \cdots$ of a Sylow p-subgroup of A/A' satisfies either $\lambda_2 \leq 1$ or $\lambda_2 = 2$ and $\lambda_3 = 0$. Let $m_A(d)$ denote the number of subgroups of index d in A. If $1 \leq i \leq [(s+1)/2]$ and q is a positive integer such that $\gcd(p, q) = 1$, then $m_A(qp^{i-1}) - m_A(qp^i)$ is a multiple of p^i and $m_A(qp^{[(s+1)/2]}) - m_A(qp^{[(s+1)/2]+1})$ is a multiple of $p^{[s/2]}$.

1. Introduction

For a finite group A, $m_A(d)$ denotes the number of subgroups of index d in A. For a real number x, $[x]$ denotes the largest integer not exceeding x. Let p be a prime. A finite group A is said to admit $\mathbf{C}(p^s)$, where s is a nonnegative integer, if the following conditions hold for any positive integer q such that $\gcd(p, q) = 1$:

(C1) $m_A(qp^{i-1}) \equiv m_A(qp^i) \bmod p^i$ with $i = 1, 2, \ldots, [(s+1)/2]$.

(C2) $m_A(qp^{[(s+1)/2]}) \equiv m_A(qp^{[(s+1)/2]+1}) \bmod p^{[s/2]}$.

A finite group A is said to admit $\mathbf{CP}(p^s)$ if these conditions hold for $q = 1$.

Any finite abelian p-group P admits $\mathbf{CP}(|P|)$ (cf. [4, Note], [7, Theorem 2.1]). Hence we obtain the half p-adic property of an arbitrary finite abelian group:

Theorem 1.1 *Any finite abelian group A admits $\mathbf{C}(|A|_p)$, where $|A|_p$ is the highest power of p dividing $|A|$.*

The following theorem is due to P. Hall [6, Theorem 1.61] and is also a consequence of [8, Lemma 2.2].

Theorem 1.2 *Let P be a finite p-group such that $p^s = |P : \Phi(P)|$, where $\Phi(P)$ denotes the Frattini subgroup of P. Then for any integer i with $0 \leq i \leq s+1$,*

$$m_P(p^i) \equiv m_{P/\Phi(P)}(p^i) \bmod p^{s-i+1}.$$

2000 *Mathematics Subject Classification*: Primary 20B05; Secondary 20D15, 20D40, 20E07.
Keyword : finite p-group; complement; semidirect product; subgroup; homomorphism.

Combining this theorem with Theorem 1.1, we know that any finite p-group P admits $\mathbf{CP}(|P/\Phi(P)|)$. A generalization of this fact is [8, Theorem 1.1]:

THEOREM 1.3 *Let A be a finite group. Then A admits $\mathbf{C}(|A/A' : \Phi(A/A')|_p)$, where A' denotes the commutator subgroup of A.*

Another generalization of a property of finite abelian groups is [8, Theorem 1.2]:

THEOREM 1.4 *Let A be a finite group, and let p^r be the exponent of a Sylow p-subgroup of A/A'. If i is a positive integer less than or equal to r, then*

$$m_A(qp^{i-1}) \equiv m_A(qp^i) \bmod p^i$$

for any positive integer q such that $\gcd(p, q) = 1$.

COROLLARY 1.5 *Under the assumptions of Theorem 1.4, if $r \geq [(s+1)/2]+1$, then A admits $\mathbf{C}(p^s)$.*

A sequence $\lambda = (\lambda_1, \lambda_2, \ldots)$ of nonnegative integers in weakly decreasing order which contains only finitely many non-zero terms is called the type of a finite abelian p-group isomorphic to the direct product of cyclic p-groups of order $p^{\lambda_1}, p^{\lambda_2}, \ldots$.

The purpose of this paper is to establish a refinement of Theorem 1.3:

THEOREM 1.6 *Let A be a finite group, and let $\lambda = (\lambda_1, \lambda_2, \ldots)$ be the type of a Sylow p-subgroup of A/A'. If either $\lambda_2 \leq 1$ or $\lambda_2 = 2$ and $\lambda_3 = 0$, then A admits $\mathbf{C}(|A/A'|_p)$. If $\lambda_2 = 2$, $\lambda_3 = 1$, and $\lambda_1 \geq \lambda_2 + \lambda_3 + \cdots$, then A admits $\mathbf{CP}(|A/A'|_p)$.*

For a finite group C and for a finite group H on which C acts, let $\mathrm{Z}(C, H)$ be the set of complements of H in the semidirect product CH of H by C.

While the following theorem is of little use in our argument, certain methods for its proof adapt successfully to the proof of Theorem 1.6.

THEOREM 1.7 ([1, 2, 3]) *Let C be a finite abelian p-group of type $\lambda = (\lambda_1, \lambda_2, \ldots)$, and suppose that either $\lambda_2 \leq 1$ or $p > 2$, $\lambda_2 = 2$, and $\lambda_3 = 0$. Then for any finite p-group H on which C acts, $\sharp\mathrm{Z}(C, H)$ is a multiple of $\gcd(|C|, |H|)$.*

For a finite group A, let $\mathrm{Hom}(A, G)$ be the set of homomorphisms from A to a group G, and set $h_n(A) = \sharp\mathrm{Hom}(A, S_n)$, where S_n is the symmetric group of degree n. If a finite group A admits $\mathbf{C}(p^s)$, then by [7, Theorem 1.2], $h_n(A)$ is a multiple of $\gcd(p^s, n!)$. This fact, together with Theorem 1.1, means that, if A is a finite abelian group, then $h_n(A)$ is a multiple of $\gcd(|A|, n!)$. In general, Yoshida [9] proved that, if A is a finite abelian group, then for any finite group G, $\sharp\mathrm{Hom}(A, G)$ is a multiple of $\gcd(|A|, |G|)$. If A is cyclic, then this fact is due to Frobenius [5]. By an argument analogous to the proof of [2, Theorem D], Theorem 1.7 implies that, if a Sylow p-subgroup of the abelianization A/A' of a finite group A is isomorphic to C given in Theorem 1.7, then for any finite group G, $\sharp\mathrm{Hom}(A, G)$ is a multiple of $\gcd(|A/A'|_p, |G|)$. In this context, we state a corollary to Theorem 1.6:

Corollary 1.8 *Let A be a finite group such that the type of a Sylow p-subgroup of A/A' is $\lambda = (\lambda_1, \lambda_2, \ldots)$. If either $\lambda_2 \leq 1$ or $\lambda_2 = 2$ and $\lambda_3 = 0$, then $h_n(A)$ is a multiple of* $\gcd(|A/A'|_p, n!)$.

Notation The notation is standard. Let G be a finite group. We denote by $|G|$ the order of G, and denote by $\exp G$ the exponent of G, that is, the least common multiple of the orders of the elements of G. The center of G is denoted by $Z(G)$. For $x_1, \ldots, x_n \in G$, $\langle x_1, \ldots, x_n \rangle$ denotes the subgroup generated by $x_1, \ldots, x_n$. Given $x, y \in G$, we set $x^y = y^{-1}xy$ and $[x, y] = x^{-1}y^{-1}xy$. Let H and K be subgroups of G. We denote by $H \times K$ the direct product of H and K. The commutator subgroup of H and K is denoted by $[H, K]$. We denote by $N_G(K)$ and $C_G(K)$ the normalizer and the centralizer of K in G, respectively, and set $N_H(K) = N_G(K) \cap H$ and $C_H(K) = C_G(K) \cap H$. Suppose that $K \subseteq H$. We write $K \leq H$, and denote by H/K the set of left cosets. The index of K in H is denoted by $|H : K|$.

2. Preliminaries

Let A be a finite group and B a normal subgroup such that A/B is a finite abelian p-group of order p^s. We denote by M a normal subgroup of A containing B such that $A/B = \langle \sigma \rangle B/B \times M/B$ with $\sigma \in A$. Let i be a positive integer.

Definition 2.1 For any $R \leq N \leq A$, we define $\mathcal{M}_A(N, R; p^i)$ to be the set of all subgroups C of index p^i in A such that $C \cap N = R$.

Lemma 2.2 *Let R be a subgroup of index p in B. Assume that $A = N_A(R)$ and M/R is abelian. If $|A/M| = p^{[(s+1)/2]}$, then*

$$\sharp\mathcal{M}_A(B, R; p^{[(s+1)/2]}) \equiv \sharp\mathcal{M}_A(B, R; p^{[(s+1)/2]+1}) \bmod p^{[s/2]}.$$

Proof. Suppose that $|A/M| = p^{[(s+1)/2]}$. By the assumption, A/M is cyclic. Hence it follows from [3, Proposition 3.3] that for any subgroup C of A with $A = CM$ and $C \cap B = R$, $\sharp\mathrm{Z}(C/(C \cap M), M/(C \cap M))$ is a multiple of $\gcd(p^{[(s+1)/2]}, |A/C|)$, where $C/(C \cap M)$ acts on $M/(C \cap M)$ by conjugation. In particular, the number of subgroups C of index $p^{[(s+1)/2]}$ or $p^{[(s+1)/2]+1}$ in A with $A = CM$ and $C \cap B = R$ is a multiple of $p^{[(s+1)/2]}$. Given a proper subgroup C of index p^i in A, $A \neq CM$ if and only if $CM \leq \langle \sigma^p \rangle M$ and $|\langle \sigma^p \rangle M : C| = p^{i-1}$, because $A/B = \langle \sigma \rangle B/B \times M/B$. Hence it suffices to verify that

$$\sharp\mathcal{M}_{\langle \sigma^p \rangle M}(B, R; p^{[(s+1)/2]-1}) \equiv \sharp\mathcal{M}_{\langle \sigma^p \rangle M}(B, R; p^{[(s+1)/2]}) \bmod p^{[s/2]}. \qquad (1)$$

Clearly, for any nonnegative integer i,

$$\sharp\mathcal{M}_{\langle \sigma^p \rangle M}(B, R; p^i) = m_{\langle \sigma^p \rangle M/R}(p^i) - m_{\langle \sigma^p \rangle M/B}(p^i).$$

By the assumption, $\langle\sigma^p\rangle M/B$ is a finite abelian group of order p^{s-1}. Obviously, $[(s+1)/2] = [s/2]$ if s is even, and $[(s+1)/2] = [s/2]+1$ if s is odd. This, combined with Theorem 1.1, yields

$$m_{\langle\sigma^p\rangle M/B}(p^{[(s+1)/2]-1}) \equiv m_{\langle\sigma^p\rangle M/B}(p^{[(s+1)/2]}) \bmod p^{[s/2]}.$$

Since $[A/R, A/R] \le B/R \le Z(A/R)$ and $|B/R| = p$, it follows that for any $x \in M$,

$$[\sigma^p, x]R = [\sigma^{p-1}, x]^\sigma \cdot [\sigma, x]R = [\sigma^{p-1}, x] \cdot [\sigma, x]R = \cdots = [\sigma, x]^p R = R.$$

Thus $\sigma^p R \in Z(A/R)$, and hence $\langle\sigma^p\rangle M/R$ is a finite abelian group of order p^s. From Theorem 1.1, we know that

$$m_{\langle\sigma^p\rangle M/R}(p^{[(s+1)/2]-1}) \equiv m_{\langle\sigma^p\rangle M/R}(p^{[(s+1)/2]}) \bmod p^{[(s+1)/2]}.$$

Consequently, Eq. (1) holds. This completes the proof. $\square$

Let $I^p(M)$ denote the set of all subgroups of M whose indices are powers of p.

Lemma 2.3 *Let $K_0 \in I^p(M)$, and suppose that the following conditions are satisfied.*

(i) $p^{i+1} \le p^i \cdot |N_B(K_0) : K_0 \cap B| \le |A : K_0|$.

(ii) *Either* $p^i \cdot |N_M(K_0) : K_0| \le |A : K_0|$ *or* $p^i \exp N_B(K_0)/(K_0 \cap B) < |A : K_0|$.

(iii) $p^i \exp N_M(K_0)/K_0 \le |A : K_0|$.

Then

$$\sum_{K \sim_A K_0} \left\{\sharp\mathcal{M}_A(M, K; p^{i-1}) - \sharp\mathcal{M}_A(M, K; p^i)\right\} \equiv 0 \bmod p^i, \qquad (2)$$

where the summation runs over all conjugates K of K_0 in A.

Proof. We may assume that $\mathcal{M}_A(M, K_0; p^i) \ne \emptyset$. Let $C \in \mathcal{M}_A(M, K_0; p^i)$. Then $|C/K_0| = p^{-i} \cdot |A : K_0|$. Set $L = N_A(K_0)$ and $H = N_M(K_0)$. Since L/H is cyclic, it follows that C/K_0 is a cyclic subgroup of L/K_0 which acts on H/K_0 by conjugation. Note that $|C/K_0| \ge p$, $N_B(K_0)/(K_0 \cap B) \simeq K_0 N_B(K_0)/K_0 \le H/K_0$, and $|H/K_0| \ge p$. Set $G = CH/K_0$ and $C_2(G) = [G, G]$. Since $L/N_B(K_0)$ is abelian, it follows that $C_2(G) \le K_0 N_B(K_0)/K_0$. Hence (i) yields $|C_2(G)| \le |C/K_0|$. We define inductively $C_j(G) = [C_{j-1}(G), G]$ for each integer $j \ge 3$, so that $|C_j(G)| < |C_{j-1}(G)|$ if $|C_{j-1}(G)| > 1$. Set $p^u = |C/K_0|$. For each integer j with $3 \le j \le u+2$, $\exp C_j(G) \le |C_j(G)| \le p^{u+2-j}$, because $|C_2(G)| \le p^u$. By [2, Lemma 2.5], $C_2(G)$ is a proper subgroup of H/K_0. Thus (ii) yields $\exp C_2(G) < p^u$. Since $\exp H/K_0 \le p^u$ by (iii), it follows from [2, Lemma 2.7] that

$$\sharp\mathcal{M}_A(M, K_0; p^i) = \sharp\mathrm{Z}(C/K_0, H/K_0) = |H/K_0|.$$

Likewise, if $\mathcal{M}_A(M, K_0; p^{i-1}) \neq \emptyset$, then $\sharp\mathcal{M}_A(M, K; p^{i-1}) = |H/K_0|$. On the other hand, if $\mathcal{M}_A(M, K_0; p^{i-1}) = \emptyset$, then $L = CH$ by [8, Proposition 2.2], which yields

$$\sum_{K \sim_A K_0} \sharp\mathcal{M}_A(M, K; p^i) = |A : L| \cdot |H : K_0| = |A : CH| \cdot |CH : C| = p^i.$$

In either case, Eq. (2) holds. This completes the proof. □

Lemma 2.4 *Let $K \in I^p(M)$, and set $R = K \cap B$. Let $C \in \mathcal{M}_A(M, K; p^i)$. Suppose that either* $\exp M/B \leq |C/K|$ *or $M/B = KB/B \times N/B$ for some subgroup N of M with* $\exp N/B \leq |C/K|$. *Then there exists a subgroup F of C such that $C/R = F/R \times K/R$ and F/R is cyclic.*

Proof. Set $p^u = p^{-i} \cdot |A : K|$. Then C/K is a cyclic group of order p^u. Choose $c \in C$ so that $C/K = \langle c \rangle K/K$, and recall that $A/B = \langle \sigma \rangle B/B \times M/B$. We may assume that $c \in \sigma^{p^e} M$ for some nonnegative integer e. Hence $c = \sigma^{p^e} x$ for some $x \in M$. Observe that $c^{p^u} B = \sigma^{p^{e+u}} x^{p^u} B$ and $c^{p^u} x^{-p^u} B = \sigma^{p^{e+u}} B \leq \langle \sigma \rangle B \cap M = B$. Thus, if $\exp M/B \leq p^u$, then $c^{p^u} \in B$, and hence $C/R = \langle c \rangle R/R \times K/R$. Now let N be a subgroup of M containing B with $\exp N/B \leq p^u$, and suppose that $M/B = KB/B \times N/B$. Since $c^{p^u} x^{-p^u} \in B$, it follows that $c^{p^u} B = x^{p^u} B = y^{p^u} B$ for some $y \in K$. Consequently, $C/R = \langle cy^{-1} \rangle R/R \times K/R$. This completes the proof. □

Definition 2.5 For any $K \in I^p(M)$, we define $\mathcal{M}_A(M, B, K; p^i)$ to be the set of all subgroups C of index p^i in A such that $C \cap B = K \cap B$, $N_M(C \cap M) = N_M(K)$, and $(C \cap M) N_B(C \cap M) = K N_B(K)$. Given $K \in I^p(M)$ and $C \in \mathcal{M}_A(M, B, K; p^i)$, we define $\mathcal{M}_A(M, B, K, C; p^i)$ to be the set consisting of all $D \in \mathcal{M}_A(M, B, K; p^i)$ such that $D N_B(K) = C N_B(K)$.

Remark 2.6 For any $K \in I^p(M)$, there exist $C_j \in \mathcal{M}_A(M, B, K; p^i)$, $j = 1, 2, \ldots$, such that $\mathcal{M}_A(M, B, K; p^i)$ is a disjoint union of $\mathcal{M}_A(M, B, C_j \cap M, C_j; p^i)$, $j = 1, 2, \ldots$.

Lemma 2.7 *Let $K \in I^p(M)$, and set $R = K \cap B$. Let $C \in \mathcal{M}_A(M, K; p^i)$, and suppose that there exists a subgroup F of C such that $C/R = F/R \times K/R$ and F/R is cyclic. If $N_B(K) \neq R$, then*

$$\sharp\mathcal{M}_A(M, B, K, C; p^i) \equiv 0 \bmod \gcd(p^{-i} \cdot |A : K|, |N_B(K) : R|) \cdot |K/R : \Phi(K/R)|.$$

Proof. Suppose that $N_B(K) \neq R$. Set $G = C N_B(K)/R$, $C_1(G) = N_B(K)/R$, and $C_2(G) = [G, G]$. We define inductively $C_j(G) = [C_{j-1}(G), G]$ for each integer $j \geq 3$. Set $p^u = p^{-i} \cdot |A : K|$, and observe that $p^u = |F/R|$. If $u \geq 1$, then we define a subgroup Q of $N_B(K)$ containing R to be

$$Q/R = \begin{cases} N_B(K)/R & \text{if } |N_B(K) : R| \leq p^{u-1}, \\ \Omega_u(C_j(G)) & \text{if } p^{u-1} < |C_j(G)| \text{ and } |C_{j+1}(G)| \leq p^{u-1}, \end{cases}$$

where $\Omega_u(C_j(G))$ is the subgroup of $C_j(G)$ generated by all elements of order at most p^u. (In [2, Definition 2.6], Q/R is denoted by $Q_u(CN_B(K)/R)$.) If $u=0$, then we set $Q=R$. By [2, Proposition 2.8], $|Q/R| \geq \gcd(p^u, |N_B(K):R|)$ and $|\langle x_0 g\rangle R/R| = p^u$ for any $g \in Q$ and $x_0R \in CN_B(K)/R$ with $|\langle x_0\rangle R/R| = p^u$ and $\langle x_0\rangle R \cap N_B(K) = R$. We have $[Q/R, (D\cap M)/R] = 1$ for each $D \in \mathcal{M}_A(M,B,K;p^i)$, because

$$Q/R \leq N_B(K)/R = N_B(D\cap M)/R = C_{B/R}((D\cap M)/R).$$

There exists an element z of $N_B(K)$ such that $zR \in Z(N_A(R)/R) \cap N_B(K)/R$ and $|\langle z\rangle R/R| = p$. Now let S be the direct product of Q/R and an elementary abelian p-group $\langle g_1\rangle \times \langle g_2\rangle \times \cdots \times \langle g_k\rangle$, where $p^k = |K/R:\Phi(K/R)|$, and define a monomorphism φ from S to the symmetric group on the set $\mathcal{M}_A(M,B,K,C;p^i)$ by

$$(\langle x_0, x_1, \ldots, x_k\rangle R)^{\varphi(gR, g_1^{e_1}, \ldots, g_k^{e_k})} = \langle x_0 g, x_1 z^{e_1}, \ldots, x_k z^{e_k}\rangle R$$

where $\langle x_0, x_1, \ldots, x_k\rangle R \in \mathcal{M}_A(M,B,K,C;p^i)$ such that $FN_B(K) = \langle x_0\rangle N_B(K)$ and $\langle x_1, \ldots, x_k\rangle N_B(K) = KN_B(K)$. Then S acts on $\mathcal{M}_A(M,B,K,C;p^i)$ via the action φ. Since this action is semiregular (see [2, Lemma 3.1]), we conclude that

$$\sharp\mathcal{M}_A(M,B,K,C;p^i) \equiv 0 \bmod |Q/R|\cdot|K/R:\Phi(K/R)|.$$

This completes the proof. □

Remark 2.8 Let $K \in I^p(M)$, and set $R = K\cap B$. If $N_B(K) \neq R$, then by an argument analogous to the proof of Lemma 2.7, we have

$$\sharp\mathcal{M}_A(M,B,K;p^i) \equiv 0 \bmod |K/R:\Phi(K/R)|. \tag{3}$$

We need one more lemma.

Lemma 2.9 *Let K and T be subgroups of M such that $R := K\cap B = T\cap B \in I^p(M)$, $N_M(K) = N_M(T)$, and $KN_B(K) = TN_B(T)$. Set $p^k = \exp N_M(K)/K$. Assume that $\exp M/B \leq p^2$. Then either $p^k \leq p\exp N_B(T)/R$ or $p^k \leq \exp N_M(T)/T$.*

Proof. By the assumption,

$$KN_B(K)/R = K/R \times N_B(K)/R = T/R \times N_B(T)/R = TN_B(T)/R.$$

Choose $x \in N_M(K)$ so that $|\langle x\rangle K/K| = p^k$. If $|\langle x\rangle KN_B(K)/KN_B(K)| \leq p$, then $p^k \leq p\exp N_B(T)/R$. If $|\langle x\rangle KN_B(K)/KN_B(K)| = p^2$, then $x^{p^2} \in N_B(K) = N_B(T)$ and $|\langle x\rangle T/T| = p^k$. Hence we have $p^k \leq \exp N_M(T)/T$. This completes the proof. □

3. The proof of Theorem 1.6

Recall that $|A/B| = p^s$. Let $\lambda = (\lambda_1, \lambda_2, \ldots)$ be the type of A/B. We show that, if either $\lambda_2 \leq 1$ or $\lambda_2 = 2$ and $\lambda_3 = 0$, then A admits $\mathbf{C}(p^s)$ and that, if $\lambda_2 = 2$, $\lambda_3 = 1$, and $\lambda_1 \geq \lambda_2 + \lambda_3 + \cdots$, then A admits $\mathbf{CP}(p^s)$.

The proof of the following proposition is analogous to that of [8, Theorem 1.1].

Proposition 3.1 *Assume that every subgroup C of A admits $\mathbf{CP}(|C/(C \cap B)|)$. Then A admits $\mathbf{C}(p^s)$.*

Proof. Suppose that $i \leq [(s+1)/2]$, and let q be a positive integer such that $\gcd(p, q) = 1$. In the statement of [8, Proposition 3.2], we may remove the assumption that A/B is elementary abelian, if we assume that every subgroup C of A admits $\mathbf{CP}(|C/(C \cap B)|)$. Hence the statements (1) and (2) of [8, Proposition 3.2] hold under the assumption of this proposition. In particular,

$$m_A(qp^{i-1}) - m_A(qp^i) \equiv \sum_{C \in \mathcal{M}_A(q)} \nu_i^i(C) \bmod p^i, \tag{4}$$

where $\mathcal{M}_A(q)$ is the set of all subgroups of index q in A and $\nu_i^i(C)$ are integers determined by $C \in \mathcal{M}_A(q)$ (see [8, Definition 3.1]). Let $C \in \mathcal{M}_A(q)$. Then $C/(C \cap B) \simeq A/B$. By the above congruence with $A = C$ and $q = 1$, we have

$$m_C(p^{i-1}) - m_C(p^i) \equiv \nu_i^i(C) \bmod p^i.$$

Hence the assumption implies that $\nu_i^i(C) \equiv 0 \bmod p^i$. This, combined with Eq. (4), yields (C1). Likewise, (C2) holds. We have thus proved the proposition. $\square$

By Proposition 3.1, it suffices to verify that, if either $\lambda_2 \leq 1$ or $\lambda_2 = 2 > \lambda_3$ and $\lambda_1 \geq \lambda_2 + \lambda_3 + \cdots$, then A admits $\mathbf{CP}(p^s)$ (see the end of this section). We owe the first half of the proof to [8, Proposition 2.1]:

Proposition 3.2 *Let R_0 be a subgroup of B with $N_B(R_0) = R_0$. If $i \leq [(s+1)/2]$, then*

$$\sum_{R \sim_A R_0} \{\sharp\mathcal{M}_A(B, R; p^{i-1}) - \sharp\mathcal{M}_A(B, R; p^i)\} \equiv 0 \bmod p^i.$$

Moreover,

$$\sum_{R \sim_A R_0} \left\{\sharp\mathcal{M}_A(B, R; p^{[(s+1)/2]}) - \sharp\mathcal{M}_A(B, R; p^{[(s+1)/2]+1})\right\} \equiv 0 \bmod p^{[s/2]}.$$

The following proposition completes the second half of the proof.

Proposition 3.3 *Assume that either $\lambda_2 \leq 1$ or $\lambda_1 = [(s+1)/2]$ and $\lambda_2 = 2 > \lambda_3$. Let $\widetilde{\mathcal{M}}_A(B; p^i)$ be the set of all subgroups C of index p^i in A with $N_B(C \cap B) \neq C \cap B$. Then*

$$\sharp\widetilde{\mathcal{M}}_A(B; p^{[(s+1)/2]}) \equiv \sharp\widetilde{\mathcal{M}}_A(B; p^{[(s+1)/2]+1}) \bmod p^{[s/2]}.$$

Moreover, if $i \leq [(s+1)/2]$ and $\lambda_2 \leq 1$, then

$$\sharp\widetilde{\mathcal{M}}_A(B; p^{i-1}) \equiv \sharp\widetilde{\mathcal{M}}_A(B; p^i) \bmod p^i.$$

Proof. For each $K \in I^p(M)$ with $N_B(K \cap B) \neq K \cap B$, we have

$$KN_B(K)/(K \cap B) = N_{KN_B(K\cap B)/(K\cap B)}(K/(K \cap B)) \neq K/(K \cap B),$$

whence $N_B(K) \neq K \cap B$. Suppose that $1 \leq i \leq [(s+1)/2] + 1$. Let $\mathcal{X}$ be the set of all $K \in I^p(M)$ with $N_B(K \cap B) \neq K \cap B$ and $\mathcal{Y}$ the set consisting of all $K \in \mathcal{X}$ which satisfy the following conditions.

(i) $p^i \cdot |N_B(K) : K \cap B| \leq |A : K|$.

(ii) Either $p^i \cdot |N_M(K) : K| \leq |A : K|$ or $p^i \exp N_B(K)/(K \cap B) < |A : K|$.

(iii) $p^i \exp N_M(K)/K \leq |A : K|$.

Obviously, both $\mathcal{X}$ and $\mathcal{Y}$ are closed under conjugation. Given $K_0 \in \mathcal{Y}$, it follows from Lemma 2.3 that

$$\sum_{K \sim_A K_0} \left\{\sharp\mathcal{M}_A(M, K; p^{i-1}) - \sharp\mathcal{M}_A(M, K; p^i)\right\} \equiv 0 \bmod p^i.$$

Assume that M/B is of type $(\lambda_2, \lambda_3, \ldots)$. If $\lambda_1 = [(s+1)/2]$, then by Lemma 2.2,

$$\sharp\mathcal{M}_A(B, R; p^{[(s+1)/2]}) \equiv \sharp\mathcal{M}_A(B, R; p^{[(s+1)/2]+1}) \bmod p^{[s/2]}$$

for any subgroup R of index p in B such that $A = N_A(R)$ and M/R is abelian. For each $K \in \mathcal{X} - \mathcal{Y}$ with $|A : K| \geq p^{i-1}$, we consider the two conditions

$$\sharp\mathcal{M}_A(M, B, K; p^{i-1}) \equiv \sharp\mathcal{M}_A(M, B, K; p^i) \equiv 0 \bmod p^{s-i+1} \tag{5}$$

and

$$\sum_{aN_A(R) \in A/N_A(R)} \left\{\sharp\mathcal{M}_A(M, B, {}^aK; p^{[(s+1)/2]}) - \sharp\mathcal{M}_A(M, B, {}^aK; p^{[(s+1)/2]+1})\right\} \equiv 0 \bmod p^{[s/2]}, \tag{6}$$

where $R = K \cap B$. (Note that $s = [s/2] + [(s+1)/2]$.) Given $K \in \mathcal{X}$ and $C \in \mathcal{M}_A(M, B, K; p^i)$, it follows from Lemma 2.9 that $K \in \mathcal{Y}$ if and only if $C \cap M \in \mathcal{Y}$. Hence it suffices to verify that for any $K \in \mathcal{X} - \mathcal{Y}$ with $|A : K| \geq p^{i-1}$, Eq. (5)

holds if $\lambda_2 \leq 1$, and either Eq. (5) or Eq. (6) holds if $\lambda_1 = [(s+1)/2]$, $\lambda_2 = 2 > \lambda_3$, $i = [(s+1)/2]+1$, and $R(= K \cap B)$ does not satisfy the assumptions of Lemma 2.2.

Suppose that $K \in \mathcal{X} - \mathcal{Y}$ with $|A : K| \geq p^{i-1}$, and set $R = K \cap B$. We complete the proof by three steps.

Step 1. We first assume that $|A : K| = p^{i-1}$. Obviously, $\mathcal{M}_A(M, B, K; p^i) = \emptyset$. By the assumption, we have $|N_B(K) : R| \geq p > p^{-i+1}|A : K|$. Moreover,

$$|A : K| \cdot |K/R : \Phi(K/R)| \geq p^{-1} \cdot |A : R| \geq p^s.$$

Hence it follows from Lemma 2.7 that $\sharp\mathcal{M}_A(M, B, K; p^{i-1}) \equiv 0 \bmod p^{s-i+1}$.

Step 2. We next assume that $p^i \cdot |N_B(K) : R| \geq |A : K| \geq p^i$ and one of the following conditions are satisfied.

(i) $|B : R| \geq p^2$.

(ii) Either $|A : K| = p^i$ and $\exp K/R \leq p$ or $|A : K| = p^{i+1}$ and $\exp M/B \leq p$.

By the assumption, $|A : K| \cdot |K/R : \Phi(K/R)| \geq p^{s+1}$. Hence, if $|A : K| = p^i$, then Eq. (5) follows from Eq. (3). Suppose now that $|A : K| \geq p^{i+1}$. If $|B : R| \geq p^2$, $\exp K/R \leq p$, and $|A : K| = p^{i+1}$, then

$$p^{i+1} \cdot |K/R : \Phi(K/R)| = |A : K| \cdot |K/R : \Phi(K/R)| = |A : R| \geq p^{s+2},$$

and hence Eq. (5) follows from Eq. (3). Excepting the case where $|B : R| \geq p^2$, $\exp K/R \leq p$, and $|A : K| = p^{i+1}$, Eq. (5) follows from Lemmas 2.4 and 2.7. Thus Eq. (5) holds in any case.

Step 3. In the situation apart from the assumptions for Steps 1 and 2, the remaining cases are as follows.

(a) $p^i = p^{i-1} \cdot |B : R| = |A : K|$ and $\exp K/R = p^2$.

(b) $p^{i+1} = p^i \cdot |B : R| = |A : K| \leq p^{i-1} \cdot |N_M(K) : K|$ and $\exp M/B = p^2$.

(c) $p^{i+1} \cdot |N_B(K) : R| \leq |A : K| \leq p^{i-1} \exp N_M(K)/K$.

(In the cases (a), (b), and (c), we assume that $|A : K| = p^i$, $|A : K| = p^{i+1}$, and $|A : K| \geq p^{i+2}$, respectively. By the hypothesis, $K \in \mathcal{X} - \mathcal{Y}$, which is reflected in the conditions.) Obviously, $\exp N_M(K)/K \leq p^2 \exp N_B(K)/R$. If either $\exp M/B \leq p$ or $\exp K/R = p^2$, then $x^p \in KN_B(K)$ for any $x \in N_M(K)$, which implies that $\exp N_M(K)/K \leq p \exp N_B(K)/R$. Hence the case (c) is rewritten as

(c)′ $p^{i+1} \cdot |N_B(K) : R| = |A : K| = p^{i-1} \exp N_M(K)/K$, $\exp M/B = p^2$, and $\exp K/R \leq p$.

In this case, if $|B : R| \geq p^2$, then Lemmas 2.4 and 2.7 yield Eq. (5). Hence we may restrict the case (c) to the following.

(d) $p^{i+2} = p^{i+1} \cdot |B : R| = |A : K| = p^{i-1} \exp N_M(K)/K$, $\exp M/B = p^2$, and $\exp K/R \leq p$.

Note that $\exp M/B = p^2$ in the cases (a), (b), and (d). Hence Eq. (5) already holds in any case if $\lambda_2 \leq 1$. We assume that $\lambda_1 = [(s+1)/2]$, $\lambda_2 = 2 > \lambda_3$, and $i = [(s+1)/2]+1$. If K satisfies one of the conditions in the cases (a), (b), and (d), then by an argument analogous to Step 2, we have

$$\sharp\mathcal{M}_A(M, B, K; p^{\lambda_1}) \equiv \sharp\mathcal{M}_A(M, B, K; p^{\lambda_1+1}) \equiv 0 \bmod p^{[s/2]-1}.$$

Moreover, if $A \neq N_A(R)$, then Eq. (6) holds in the cases (a), (b), and (d). Thus we may assume that $A = N_A(R)$. If $|B : R| = p$ and M/R is abelian, then R satisfies the assumptions of Lemma 2.2. We conclude the proof with the assertion that M/R is abelian in each of the cases (a), (b), and (d). Recall that $|A : M| = p^{\lambda_1}$.

(**a**) Assume that $p^{\lambda_1+1} = p^{\lambda_1} \cdot |B : R| = |A : K|$. We have $|M/K| = p = |B/R|$, whence $M/R = KB/R$. Since $B/R \leq Z(A/R)$, it follows that M/R is abelian.

(**b**) Assume that $p^{\lambda_1+2} = |A : K| \leq p^{\lambda_1} \cdot |N_M(K) : K| \leq p^{\lambda_1} \cdot |M : K| = p^{\lambda_1+2}$. Then $|M/K| = p^2$ and $M = N_M(K)$. Since M/B and M/K are abelian, it turns out that

$$[M/R, M/R] \leq B/R \cap K/R = R/R.$$

Thus M/R is abelian.

(d) Assume that $p^{\lambda_1+3} = |A : K| = p^{\lambda_1} \exp N_M(K)/K \leq p^{\lambda_1}|M : K| = p^{\lambda_1+3}$. Then $|M/K| = p^3$, $M = N_M(K)$, and M/K is a cyclic group of order p^3. Consequently, M/R is abelian.

This completes the proof. □

Remark 3.4 Assume that $\lambda_1 \geq \lambda_2 + \lambda_3 + \cdots$. Then $\lambda_1 \geq [(s+1)/2]$. If $\lambda_1 \geq [(s+1)/2]+1$, then by Corollary 1.5, A admits $\mathbf{C}(p^s)$. If $\lambda_1 = [(s+1)/2]$ and i is a positive integer less than or equal to $[(s+1)/2]$, then by Theorem 1.4,

$$m_A(qp^{i-1}) \equiv m_A(qp^i) \bmod p^i$$

for any positive integer q such that $\gcd(p, q) = 1$.

We are now in a position to prove an analogy of Theorem 1.6 stated at the beginning of this section.

Theorem 3.5 *Let A be a finite group and B a normal subgroup such that A/B is a finite abelian p-group of order p^s. Let $\lambda = (\lambda_1, \lambda_2, \ldots)$ be the type of A/B. If either $\lambda_2 \leq 1$ or $\lambda_2 = 2$ and $\lambda_3 = 0$, then A admits $\mathbf{C}(p^s)$. If $\lambda_2 = 2$, $\lambda_3 = 1$, and $\lambda_1 \geq \lambda_2 + \lambda_3 + \cdots$, then A admits $\mathbf{CP}(p^s)$.*

Proof. Assume that either $\lambda_2 \leq 1$ or $\lambda_2 = 2 > \lambda_3$ and $\lambda_1 \geq \lambda_2 + \lambda_3 + \cdots$. Then by Propositions 3.2 and 3.3 and Remark 3.4, A admits $\mathbf{CP}(p^s)$. Moreover, if either $\lambda_2 \leq 1$ or $\lambda_2 = 2$ and $\lambda_3 = 0$, then A satisfies the assumption of Proposition 3.1, whence A admits $\mathbf{C}(p^s)$. This completes the proof. □

Proof of Theorem 1.6. The assertions follow from Theorem 3.5 with $B = A'$. □

REFERENCES

1. T. Asai and Y. Takegahara, On the number of crossed homomorphisms, *Hokkaido Math. J.* **28** (1999), 535–543.

2. T. Asai and Y. Takegahara, $|\mathrm{Hom}(A, G)|$, IV, *J. Algebra* **246** (2001), 543–563.

3. T. Asai and T. Yoshida, $|\mathrm{Hom}(A, G)|$, II, *J. Algebra* **160** (1993), 273–285.

4. L. M. Butler, A unimodality result in the enumeration of subgroups of a finite abelian group, *Proc. Amer. Math. Soc.* **101** (1987), 771–775.

5. G. Frobenius, Verallgemeinerung des Sylowschen Satzes, *Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin* (1895), 981–993; in :"Gesammelte Abhandlungen," Bd. II, pp. 664–676, Springer-Verlag, Berlin, 1968.

6. P. Hall, A contribution to the theory of groups of prime-power order, *Proc. London Math. Soc.* (2) **36** (1933), 29–95.

7. Y. Takegahara, On the Frobenius numbers of symmetric groups, *J. Algebra* **221** (1999), 551–561.

8. Y. Takegahara, The number of subgroups of a finite group, *J. Algebra* **227** (2000), 783–796.

9. T. Yoshida, $|\mathrm{Hom}(A, G)|$, *J. Algebra* **156** (1993), 125–156.