J. Math. Kyoto Univ. (JMKYAZ)
42-1 (2002), 161–174

On the number of p-subgroups of a finite group

By

Masafumi Murai

Introduction

Let G be a finite group. For each positive integer n, put

$$G(n) = \{x \in G \mid x^n = 1\}$$

and $m(G;n) = |G(n)|/(n, |G|)$. Frobenius proved:

Theorem 1 (Frobenius [Fr1, Section 2.II]). *$m(G;n)$ is always an integer.*

For various generalizations of this result, see Frobenius [Fr2], Hall [Ha2] and Yoshida [Yo]. For recent results in this direction, see Asai-Takegahara [AT].

Let p be a prime. For each integer e, let $S_e(G)$ be the set of subgroups of G of order p^e and put $s_e(G) = |S_e(G)|$. Let P be a Sylow p-subgroup of G of order p^n. Based on Theorem l, Frobenius proved:

Theorem 2 (Frobenius [Fr1, Section 4.I]). *$s_e(G) \equiv 1 \mod p$ for $0 \leq e \leq n$.*

Related to the above theorems, the following results are known.

Theorem 3 (Kulakoff [Ku, Satz 1], Hall [Ha2, Theorem 4.6]). *If p is odd and P is not cyclic, then $s_e(G) \equiv 1 + p \mod p^2$ for $1 \leq e \leq n-1$.*

Theorem 4 (Mi11er [Mi]). *If p is odd and P is not cyclic, the number of cyclic subgroups of G of order p^e is divisible by p for $2 \leq e \leq n$.*

Theorem 5 (Kulakoff [Ku, Satz 2], Hall [Ha2, Theorem 1 (iii)]). *If p is odd and P is not cyclic, then $m(G;p^e)$ is a multiple of p for $1 \leq e \leq n-1$.*

In the present paper, we improve Theorems 3 through 5 by using Theorems 1 and 2. We formulate and prove the counterparts of Theorems 3 through 5 for the case of $p = 2$. We do not exclude the case of odd primes, and Theorems 3 through 5 will be proved simultaneously.

To state our results, it is convenient to introduce the following definition.

Communicated by Prof. T. Hirai, November 5, 1999

Definition. A p-group P is called *exceptional*, if P is cyclic ($p \neq 2$); if P is cyclic, quaternion, dihedral, or semi-dihedral (quasidihedral) ($p = 2$). (Here "dihedral group" means a non-abelian one (of order ≥ 8). Also, "quaternion group" means generalized quaternion of order ≥ 8.)

For a family $\mathcal{X}$ of p-groups, a group G and an integer e, let

$$S_e(G, \mathcal{X}) = \{H \mid H \leq G, |H| = p^e, H \in \mathcal{X}\},$$

and put $s_e(G, \mathcal{X}) = |S_e(G, \mathcal{X})|$.

Let $\mathcal{C}$, $\mathcal{Q}$, $\mathcal{D}$ and $\mathcal{SD}$ be the set of cyclic p-groups, the set of quaternion 2-groups, the set of dihedral 2-groups and the set of semi-dihedral 2-groups, respectively. The statements (i) and (ii) of the following theorem extend Theorems 4 and 5, and determine all *Gegenbeispiele* mentioned on p. 471 of Hall [Ha2].

Theorem A. *Let G be a group with a Sylow p-subgroup P of order p^n.*

(i) *For $1 \leq e \leq n-1$, $m(G; p^e)$ is prime to p if and only if P is cyclic or P is non-cyclic exceptional and $e \leq n-2$.* ($p \geq 2$)

(ii) *For $2 \leq e \leq n$, $s_e(G, \mathcal{C})$ is prime to p if and only if P is cyclic or P is non-cyclic exceptional and $e \leq n-1$.* ($p \geq 2$)

(iii) *For $4 \leq e \leq n$, $s_e(G, \mathcal{SD})$ is odd if and only if P is semi-dihedral and $e = n$.* ($p = 2$)

(iv) *For $3 \leq e \leq n$, $s_e(G, \mathcal{Q}) \not\equiv s_e(G, \mathcal{D}) \mod 2$ if and only if P is quaternion or dihedral, and $e = n$.* ($p = 2$)

As a consequence we obtain the following.

Corollary B. *Let G be a group with a Sylow p-subgroup P of order p^n. Let $p^e r$ be a divisor of $|G|$, where $1 \leq e \leq n-1$ and r is prime to p. Then if $m(G; p^e r)$ is prime to p, P is exceptional.*

Corollary B plays an important role in a reduction to the case of simple groups of the Frobenius conjecture stating that if $m(G; n) = 1$ for a divisor n of $|G|$, then $G(n)$ is a (normal) subgroup of G, cf. [Mu]. The Frobenius conjecture has been shown to be true by Iiyori-Yamaki [IY] on the basis of the classification theorem of finite simple groups. In their proof Corollary B also is useful, cf. Lemma 1 of [IY].

By Theorem 2, whenever p^e divides $|G|$, $(s_e(G)-1)/p$ is an integer. On the other hand, $m(G; p^e)$ also is an integer by Theorem 1. For these two integers, we show that there holds the following congruence.

Theorem C. *Let G be a group with a Sylow p-subgroup P of order p^n ($n \geq 2$). For any e with $1 \leq e \leq n-1$, we have*

$$\frac{s_e(G) - 1}{p} + m(G; p^e) \equiv 1 \mod p.$$

Theorems A and C yield the following.

Theorem D. *Let G be a group with a Sylow p-subgroup P of order p^n $(n \geq 2)$.*

(i) *If P is non-exceptional,*

$$s_e(G) \equiv 1 + p \mod p^2, \quad \text{for any } e \text{ with } 1 \leq e \leq n-1.$$

(ii) *If P is exceptional,*

$$s_e(G) \equiv 1 \mod p^2, \quad \text{for any } e \text{ with } 1 \leq e \leq n-2,$$

and

$$s_{n-1}(G) \equiv 1 \quad \textit{or} \quad 1 + p \mod p^2 \quad \textit{according as } P \textit{ is cyclic or not.}$$

Theorem D strengthens Theorem 2 and extends Theorem 3. In the proofs of Theorems A and C, Hall's enumeration principle [Ha1, Theorem 1.4] ([Hu, III 8.6]) plays an important role.

The author expresses his thanks to the referee for valuable suggestions.

1. Proofs of Theorem A and Corollary B

The following is well known.

Lemma 1.1. *Let G be a group with a Sylow p-subgroup P. Let $\mathcal{X}$ be a set of p-groups and e an integer.*

(i) $s_e(G, \mathcal{X}) \equiv s_e(P, \mathcal{X}) \mod p$.

(ii) $s_e(P, \mathcal{X}) \equiv \#\{ H \mid H \in S_e(P, \mathcal{X}), H \triangleleft P\} \mod p$.

In particular, if $s_e(P, \mathcal{X})$ is prime to p, then there exists a normal subgroup H of P with $H \in \mathcal{X}$ and $|H| = p^e$.

Proof. Let a be the right hand side of (ii). Considering the conjugation action of P on $S_e(G, \mathcal{X})$, we get $s_e(G, \mathcal{X}) \equiv a \mod p$. Similarly we get $s_e(P, \mathcal{X}) \equiv a \mod p$. So (i) and (ii) follow. □

The following is Lemma 1 of [Mu]. For the convenience of the reader, we recall it here.

Proposition 1.2. *Let G be a group with a Sylow p-subgroup P of order p^n. Let $p^e r$ be a divisor of $|G|$, where $0 \leq e \leq n-1$ and r is prime to p. Then*

(i) $m(G; p^e r) \equiv m(P; p^e) m(G; r) \mod p$.

(ii) $m(G; p^e) \equiv m(P; p^e) \equiv s_{e+1}(G, \mathcal{C}) \equiv s_{e+1}(P, \mathcal{C}) \mod p$.

Proof. If G has no element of order p^{e+1}, then $G(p^e r) = G(p^n r)$. So we have

$$m(G; p^e r) = |G(p^n r)|/p^e r = m(G; p^n r) p^{n-e} \equiv 0 \mod p.$$

Similarly $m(G; p^e) \equiv 0 \mod p$ and $m(P; p^e) \equiv 0 \mod p$. So the result holds in this case. Assume that G has an element of order p^{e+1}. After Frobenius [Fr1], we count the number of elements in $G(p^{e+1} r) - G(p^e r)$. For an element

$x \in G$, x belongs to $G(p^{e+1}r) - G(p^e r)$ if and only if the p-part of x generates a cyclic subgroup, C, of order p^{e+1} and p'-part of x belongs to $C_G(C)(r)$. This shows

$$|G(p^{e+1}r)| - |G(p^e r)| = \sum_C (p^{e+1} - p^e)|C_G(C)(r)|,$$

where C runs through $S_{e+1}(G, \mathcal{C})$. Then we get

$$m(G; p^e r)r \equiv \sum_C |C_G(C)(r)| \mod p. \tag{1}$$

For each $C \in S_{e+1}(G, \mathcal{C})$, let C act on $G(r)$ by conjugation. Then we have

$$|G(r)| \equiv |C_G(C)(r)| \mod p. \tag{2}$$

From (1) and (2), we get

$$\begin{aligned} m(G; p^e r)r &\equiv |G(r)| s_{e+1}(G, \mathcal{C}) \mod p \\ &\equiv m(G; r) s_{e+1}(G, \mathcal{C}) r \mod p. \end{aligned}$$

Since r is prime to p, we get

$$m(G; p^e r) \equiv m(G; r) s_{e+1}(G, \mathcal{C}) \mod p. \tag{3}$$

Letting $r = 1$, we get $m(G; p^e) \equiv s_{e+1}(G, \mathcal{C}) \mod p$. Letting $G = P$ we get $m(P; p^e) \equiv s_{e+1}(P, \mathcal{C}) \mod p$. Since, by Lemma 1.1, $s_{e+1}(G, \mathcal{C}) \equiv s_{e+1}(P, \mathcal{C}) \mod p$, (ii) follows. (i) follows from (ii) and (3). This completes the proof. $\square$

Remark. The congruence $m(G; p^e) \equiv s_{e+1}(G, \mathcal{C}) \mod p$ is implicit in Kulakoff [Ku] (for the case where G is a p-group). It shows that Theorems 4 and 5 are equivalent.

Lemma 1.3 (Hall's enumeration principle [Ha1, Theorem 1.4])**.** *Let P be a p-group. Let $\mathcal{H}$ be the set of subgroups H of P with $H \geq \Phi(P)$. For $H \in \mathcal{H}$ put $p^{d_H} = |P/H|$. Let $\mathcal{S}$ be a set of proper subgroups of P. For $H \in \mathcal{H}$, let $n(H)$ be the number of members of $\mathcal{S}$ which are contained in H. Then we have*

$$\sum_{H \in \mathcal{H}} (-1)^{d_H} p^{\frac{d_H(d_H - 1)}{2}} n(H) = 0.$$

We prepare several lemmas, mainly on 2-groups. Let

$$M(p^n) = \langle a, b \,|\, b^p = a^{p^{n-1}} = 1,\ b^{-1}ab = a^{1+p^{n-2}} \rangle,$$

where $n \geq 3$ if p is odd and $n \geq 4$ if $p = 2$.

Lemma 1.4. *A p-group P of order p^n has a cyclic maximal subgroup if and only if P is isomorphic to one of the following groups*:

An exceptional group of order p^n, an abelian group of type $(p^{n-1},\ p)$, or $M(p^n)$.

Further, for these groups and $2 \le e \le n$, the following holds.

$$\begin{aligned} s_e(P,\mathcal{C}) = &\ 1 \text{ if } P \text{ is cyclic and } 2 \le e \le n, \\ = &\ p \text{ if } P \text{ is abelian of type } (p^{n-1},p) \text{ or isomorphic to } M(p^n) \\ &\ \text{and } 2 \le e \le n-1, \\ = &\ 1+2^{n-2} \text{ if } P \text{ is quaternion and } e=2, \\ = &\ 1 \text{ if } P \text{ is quaternion and } 3 \le e \le n-1, \\ = &\ 1 \text{ if } P \text{ is dihedral and } 2 \le e \le n-1, \\ = &\ 1+2^{n-3} \text{ if } P \text{ is semi-dihedral and } e=2, \\ = &\ 1 \text{ if } P \text{ is semi-dihedral and } 3 \le e \le n-1, \\ = &\ 0 \text{ if } P \text{ is not cyclic and } e=n. \end{aligned}$$

Proof. The first assertion is well known, cf. [Su, Theorem 4.4.l] for example. Using the formula

$$s_e(P,\mathcal{C}) = \frac{|P(p^e)| - |P(p^{e-1})|}{p^e - p^{e-1}},$$

we can obtain $s_e(P,\mathcal{C})$ by direct computation.

We obtain the following

Corollary 1.5. *Assume that a p-group P has a cyclic maximal subgroup. Put $|P| = p^n$.*

(i) *Let $2 \le e \le n$. Then $s_e(P,\mathcal{C})$ is prime to p if and only if one of the following holds: P is cyclic and $2 \le e \le n$ ($p \ge 2$); P is quaternion, dihedral, or semi-dihedral, and $2 \le e \le n-1$ ($p=2$).*

(ii) *Let $p=2$ and $n \ge 4$. Then P has at least two cyclic maximal subgroups if and only if P is either abelian of type $(2^{n-1},2)$ or isomorphic to $M(2^n)$, each of which has exactly two such subgroups.*

Lemma 1.6. *Let P be a 2-group of order 2^n, $n \le 4$. If $s_e(P,\mathcal{C})$ is odd for some e with $2 \le e \le n$, then P is exceptional.*

Proof. For $n \le 3$, the only non-trivial case to be checked is the case where P is abelian of type $(4,2)$ and $e=2$. In this case, by Lemma 1.4, $s_2(P,\mathcal{C}) = 2$, which contradicts our assumption. So we may assume $n=4$. If P has a cyclic subgroup of order 8, then the result follows by Corollary 1.5. So we assume P has no element of order 8 and obtain a contradiction. Thus $e=2$. Let I be the set of involutions in P. By Proposition 1.2, $m(P;2)$ is odd. Thus

$$|I| \equiv 1 \mod 4. \tag{1}$$

Further, by Lemma 1.1, P has a normal cyclic subgroup C, of order 4. Now $P/C_P(C)$ is identified with a subgroup of $\mathrm{Aut}(C)$, a group of order 2, so either (a) $P = C_P(C)$ or (b) $|C_P(C)| = 8$.

Case (a). If P/C is cyclic, then P is abelian of type $(4,4)$. Then $|I| = 3$, which contradicts (1). Thus P/C is elementary abelian. Let $x \in P - C$. We show $|xC \cap I| = 2$. Let $C = \langle c \rangle$. Since $x^2 \in C$ and P has no element of order 8, $x^2 = 1$ or c^2. In the latter case $(xc^{-1})^2 = 1$. So we may assume $x^2 = 1$. Then $xC \cap I = \{x, xc^2\}$. This implies $|I| = 1 + 2 \times 3 = 7$, which contradicts (1).

Case (b). Clearly $C_P(C)$ is a non-cyclic abelian group, so $C_P(C)$ is of type $(4,2)$. Hence $C_P(C)$ has exactly 3 involutions. Let

$$P = x_1C \cup x_2C \cup x_3C \cup x_4C$$

be the coset decomposition, where $x_1, x_2 \in C_P(C)$. We claim that for $i > 2$, $|x_iC \cap I| \equiv 0 \mod 4$. We may assume $x_iC \cap I \neq \emptyset$. So we may assume $x_i \in I$. Then $\langle x_i, C \rangle$ is dihedral of order 8, so $x_iC \subseteq I$. Thus the claim follows. Hence $|I| \equiv 3 \mod 4$, which contradicts (1). This completes the proof. □

The essential part of the proof of Theorem A is contained in the following.

Lemma 1.7. *Let P be a 2-group of order 2^n $(n \geq 5)$ with an exceptional maximal subgroup. Then either of the following holds.*

(i) *P has a cyclic maximal subgroup.*

(ii) *P has exactly two normal cyclic subgroups of order 2^{n-2}, and $s_{n-1}(P, \mathcal{SD}) = 0$, 2, or 4.*

Proof. We assume that (i) is false and prove that (ii) is true. Let M_1 be an exceptional maximal subgroup of P. Since $n - 1 \geq 4$, M_1 has a unique cyclic maximal subgroup, say C. So C is a normal subgroup of P. Put $i = 1 + 2^{n-3}$. Let

$$\phi : P \to \mathrm{Aut}(C) = (\mathbf{Z}/2^{n-2}\mathbf{Z})^{\times}$$

be the map defined by the conjugation action of P on C, where $\mathbf{Z}$ is the integers and $(\mathbf{Z}/2^{n-2}\mathbf{Z})^{\times}$ is the unit group of $\mathbf{Z}/2^{n-2}\mathbf{Z}$.

We claim that P/C is elementary abelian. Assume that P/C is cyclic and put $P = \langle C, a \rangle$ for some $a \in P$. Put $\alpha = \phi(a)$. Then, since $M_1 = \langle C, a^2 \rangle$ is non-cyclic exceptional, $\alpha^2 = \phi(a^2) = -\bar{1}$ or $-\bar{i}$, where bar denotes the residue class modulo 2^{n-2}. Since α has order 4, we get $\alpha^2 = \bar{i}$, a contradiction. Thus the claim follows.

Let $\{M_1, M_2, M_3\}$ be the set of maximal subgroups of P which contain C (with M_1 as above). Let $M_1 = \langle C, a \rangle$, $M_2 = \langle C, b \rangle$ and $M_3 = \langle C, c \rangle$. Put $H = \{\pm\bar{1}, \pm\bar{i}\}$ and $K = \{\bar{1}, \bar{i}\}$. We see $\mathrm{Im}\,\phi \subseteq H$. Here $H = K \cup K(-\bar{1})$ is the coset decomposition of H with respect to K. Since $\phi(a) \in K(-\bar{1})$ and $\phi(b)\phi(c) = \phi(a)$, we may assume $\phi(b) \in K(-\bar{1})$ and $\phi(c) \in K$. Then M_2 is exceptional and M_3 is non-exceptional. By Corollary 1.5, M_3 has exactly two cyclic maximal subgroups, one of which is C. Since C is normal in P, if D is the other cyclic maximal subgroup, then D also is normal in P. Let E be a normal cyclic subgroup of P of order 2^{n-2} with $E \neq C$. Then, since P/C is not cyclic, CE is a maximal subgroup of P. Since C is a unique cyclic maximal subgroup of M_1, $CE \neq M_1$. Likewise, $CE \neq M_2$. So $CE = M_3$, and $E = D$. Thus C and D are the only normal cyclic subgroups of P of order 2^{n-2} .

To compute $s_{n-1}(P, \mathcal{SD})$, we distinguish two cases:

(a) CD is abelian of type $(2^{n-2}, 2)$, (b)$CD \simeq M(2^{n-1})$.

(Note that $CD = M_3$.) Since $\phi(b)\phi(c) = \phi(a)$, we get the following:

($*$) In Case (a), both of M_1 and M_2 are semi-dihedral or neither of them are so, and in Case (b), exactly one of M_1 and M_2 is semi-dihedral.

Let $C = \langle x \rangle$. We claim that $P/\langle x^2 \rangle$ is elementary abelian. Since M_1 is not cyclic, we have that $a^2 \in \langle x^2 \rangle$. We may assume $c^2 = 1$. Write $a^{-1}c^{-1}ac = x^k$ for an integer k. Then $a^{-1}c^{-1}a = x^k c \in M_3$ has order 2, which implies that k is even. Since $P/\langle x^2 \rangle$ is generated by the images of a, c and x, the claim follows.

Since $\langle x^2 \rangle = C \cap D$, P/D is elementary abelian of order 4. Let $\{CD, M_4, M_5\}$ be the set of maximal subgroups of P which contain D. Here M_4 is exceptional. Indeed, if this is not the case, then, by Corollary 1.5, M_4 has exactly two cyclic maximal subgroups, one of which is D. Since D is normal in P, the other cyclic maximal subgroup is also normal in P, a contradiction. So, in the above we can replace (M_1, C) with (M_4, D), and we see that ($*$) is true with $\{M_4, M_5\}$ in place of $\{M_1, M_2\}$. Since $D \not\leq M_1$ and $D \not\leq M_2$, we get $\{M_1, M_2\} \cap \{M_4, M_5\} = \emptyset$. Since any semi-dihedral maximal subgroup of P contains a normal cyclic subgroup of P of order 2^{n-2}, namely C or D, it follows that $s_{n-1}(P, \mathcal{SD})$ equals 0, 2, or 4 in Case (a) and 2 in Case (b). Thus (ii) holds and the proof is complete. □

Now we can prove Theorem A.

Proof of Theorem A. By Proposition 1.2, $m(G; p^e) \equiv s_{e+1}(G, \mathcal{C}) \mod p$, so (i) and (ii) are equivalent to each other, and it suffices to prove (ii) through (iv).

Since, for any set $\mathcal{X}$ of p-groups, $s_e(G, \mathcal{X}) \equiv s_e(P, \mathcal{X}) \mod p$, we may assume $G = P$.

(ii) "if" part: This follows from Corollary 1.5.

"only if" part: It suffices to show the following:

(1) If $s_e(P, \mathcal{C})$ is prime to p for some e with $2 \leq e \leq n$, then P is exceptional.

Assume (1) is false and choose a counter-example (P, e) so that n is as small as possible and then e as large as possible.

If P has a cyclic maximal subgroup, then the conclusion of (1) is true by Corollary 1.5. So P has no cyclic maximal subgroup. Hence $e \leq n - 2$.

Let $\mathcal{M}$ be the set of maximal subgroups of P. By Lemma 1.3 (with $\mathcal{S} =$

$S_e(P,\mathcal{C})$), we have

$$0 \not\equiv s_e(P,\mathcal{C}) \equiv \sum_{M\in\mathcal{M}} s_e(M,\mathcal{C}) \mod p. \tag{2}$$

Thus there exists a maximal subgroup, say M_1, of P such that $s_e(M_1,\mathcal{C}) \not\equiv 0 \mod p$. By our choice of n, M_1 is exceptional. Since M_1 is not cyclic, $p=2$.

We claim $e=n-2$. Assume $e \le n-3$. By Lemma 1.3, we have

$$s_{e+1}(P,\mathcal{C}) \equiv \sum_{M\in\mathcal{M}} s_{e+1}(M,\mathcal{C}) \mod 2. \tag{3}$$

If $s_{e+1}(P,\mathcal{C})$ is odd, then P is exceptional by our choice of e. Thus $s_{e+1}(P,\mathcal{C})$ is even. Now we show $s_{e+1}(M,\mathcal{C}) \equiv s_e(M,\mathcal{C}) \mod 2$ for all $M\in\mathcal{M}$. It suffices to show $s_{e+1}(M,\mathcal{C})$ is odd if and only if $s_e(M,\mathcal{C})$ is odd. Assume $s_e(M,\mathcal{C})$ is odd. Then M is exceptional. So, since $e+1\le n-2$, $s_{e+1}(M,\mathcal{C})$ is odd by Lemma 1.4. The converse is proved similarly. The above yields that the right hand sides of (2) and (3) are congruent modulo 2. This is a contradiction, since we already see $s_{e+1}(P,\mathcal{C})$ is even. So the claim is proved.

By Lemma 1.6, (1) is true when $n\le 4$. So $n\ge 5$. Since $s_{n-2}(P,\mathcal{C})$ is odd, if a is the number of normal cyclic subgroups of P of order 2^{n-2}, a is also odd by Lemma 1.1. But $a=2$ by Lemma 1.7, a contradiction. This completes the proof of (ii).

(iii) "if" part: This is trivial, since $G=P$.
"only if" part: We must prove the following:

(4) If $s_e(P,\mathcal{SD})$ is odd for some e with $4\le e\le n$, then $e=n$ and P is semi-dihedral.

Let P be a minimal counter-example. If P has a cyclic maximal subgroup, the structure of P is determined by Lemma 1.4, and it is easy to see that (4) is true for P. Thus P has no cyclic maximal subgroup. Clearly $e\le n-1$. Let $\mathcal{M}$ be the set of all maximal subgroups of P. By Lemma 1.3 (with $\mathcal{S}=S_e(P,\mathcal{SD})$), we have

$$s_e(P,\mathcal{SD}) \equiv \sum_{M\in\mathcal{M}} s_e(M,\mathcal{SD}) \mod 2.$$

By the minimality of P, for any $M\in\mathcal{M}$, $s_e(M,\mathcal{SD})$ is odd if and only if M is semi-dihedral and $e=n-1$. Thus the assumption yields that $e=n-1\ge 4$ and that $s_{n-1}(P,\mathcal{SD})$ is odd. In particular, P has a semi-dihedral maximal subgroup. So we can apply Lemma 1.7 to get a contradiction. This completes the proof of (iii).

(iv) "if" part: This is trivial, since $G=P$.
"only if" part: We must prove the following:

If $s_e(P,\mathcal{Q}) \not\equiv s_e(P,\mathcal{D}) \mod 2$ for some e with $3\le e\le n$, then P is quaternion or dihedral, and $e=n$.

Put

$$I = \{(Q,R) \mid Q \le R, Q \in S_{e-1}(P,\mathcal{C}), R \in S_e(P)\}.$$

(Note that $S_{e-1}(P,\mathcal{C})$ is not empty, since $s_e(P,\mathcal{Q}) \not\equiv s_e(P,\mathcal{D}) \mod 2$.) We count $|I|$ in two ways. First, for a given $R \in S_e(P)$, the number of cyclic maximal subgroups of R is odd if and only if R is exceptional by Lemma 1.4. Next, for a given $Q \in S_{e-1}(P,\mathcal{C})$, the number of subgroups of P containing Q as a maximal subgroup equals $s_1(N_P(Q)/Q)$ and hence it is odd by Theorem 2. Thus

$$s_e(P,\mathcal{E}) \equiv s_{e-1}(P,\mathcal{C}) \mod 2, \tag{5}$$

where $\mathcal{E}$ is the set of exceptional 2-groups. On the other hand,

$$s_e(P,\mathcal{E}) = s_e(P,\mathcal{C}) + s_e(P,\mathcal{Q}) + s_e(P,\mathcal{D}) + s_e(P,\mathcal{SD}). \tag{6}$$

If P is non-exceptional, $s_e(P,\mathcal{C})$, $s_{e-1}(P,\mathcal{C})$ and $s_e(P,\mathcal{SD})$ are all even by (ii) and (iii). So (5) and (6) yield that $s_e(P,\mathcal{Q}) \equiv s_e(P,\mathcal{D}) \mod 2$, a contradiction. Hence P is exceptional.

Assume that P is semi-dihedral. If $e < n$, $s_{e-1}(P,\mathcal{C})$ and $s_e(P,\mathcal{C})$ are odd by (ii) and $s_e(P,\mathcal{SD}) = 0$, so we get a contradiction in the same way as above. If $e = n$, $s_e(P,\mathcal{Q}) = s_e(P,\mathcal{D}) = 0$, a contradiction.

If P is cyclic, $s_e(P,\mathcal{Q}) = s_e(P,\mathcal{D}) = 0$, a contradiction.

If P is quaternion, $s_e(P,\mathcal{D}) = 0$. However, if $e < n$, then $s_e(P,\mathcal{Q})$ is even by Lemma 1.4 and Theorem 2, a contradiction. Hence $e = n$.

If P is dihedral, $s_e(P,\mathcal{Q}) = 0$. However, if $e < n$, then $s_e(P,\mathcal{D})$ is even by Lemma 1.4 and Theorem 2, a contradiction. Hence $e = n$.

Thus the proof is complete. □

Now we prove Corollary B.

Proof of Corollary B. By Proposition 1.2, $m(G;p^e r) \equiv m(P;p^e)m(G;r) \mod p$. So $m(P;p^e)$ is prime to p. Thus the result follows from Theorem A. □

Remark. Theorem 6.2 (Thompson) of Lam [La] (see also [Is, Theorem 4.9 (Alperin-Feit-Thompson)]) says that if the number of solutions of the equation $x^2 = 1$ in a 2-group P is not divisible by 4, then P is exceptional. This theorem is a special case of Corollary B, since the assumption is equivalent to the fact that $m(G;2)$ is odd. We note that the proof in [La] (or [Is]) needs character theory (especially the Frobenius-Schur theorem), while our proof is purely group-theoretical.

Some well-known elementary facts on p-groups involving exceptional p-groups follow immediately from Theorem A.

Corollary 1.8. *Let P be a p-group.*

(i) ([*Hu*, III 8.2], [*Su*, 4.4.4]) *If P has a unique subgroup of order p, then P is cyclic or $p = 2$ and P is quaternion.*

(ii) ([*Go, Theorem* 5.4.10 (i)], [*Hu*, III 7.6], [*Su*, 4.4.3]) *If every normal abelian subgroup of P is cyclic, then P is cyclic or $p = 2$ and P is quaternion, dihedral of order ≥ 16 or semi-dihedral.*

Proof. We may assume $|P| \geq p^2$.

(i) By assumption $m(P;p) = 1$. Thus P is exceptional by Theorem A, and the result follows.

(ii) Let a be the number of normal subgroups of P of order p^2. By Lemma 1.1, $a \equiv s_2(P) \mod p$. By assumption and Lemma 1.1, $a \equiv s_2(P, \mathcal{C}) \mod p$. Thus $s_2(P, \mathcal{C}) \equiv s_2(P) \equiv 1 \mod p$ by Theorem 2. So P is exceptional by Theorem A, and the result follows. □

2. Proofs of Theorems C and D

First we prove Theorem D.

Proof of Theorem D (*under Theorem* C). If P is cyclic, the result follows from Theorem C and Proposition 1.2. If P is not cyclic, the result follows from Theorems A and C. □

Remark. Hall [Ha2, Lemma 4.61] proved that if G has a cyclic Sylow p-subgroup of order p^n, then $s_e(G) \equiv 1 \mod p^{n-e+1}$ for $1 \leq e \leq n$. When G has a non-cyclic exceptional Sylow 2-subgroup, we can obtain similar congruences which are better than Theorem D (ii). Indeed, $s_e(G) \equiv s_e(G, \mathcal{C}) \equiv 1 \mod 2^{n-e}$ for $3 \leq e \leq n-1$ for example.

We begin with a special case of Theorem C.

Lemma 2.1. *Let P be a p-group of order p^n $(n \geq 2)$. For any e with $1 \leq e \leq n-1$, we have*

$$\frac{s_e(P) - 1}{p} + m(P; p^e) \equiv 1 \mod p.$$

Proof. The congruence is rewritten as

$$s_e(P) + m(P; p^e)p \equiv 1 + p \mod p^2. \tag{1}$$

We argue by induction on n. If P is cyclic, then (1) is true. So we assume P is not cyclic. If $n = 2$, then P is elementary abelian of order p^2, so $s_1(P) = p + 1$ and $m(P;p) = p$. Thus (1) is true in this case. Assume $n \geq 3$. Since P is not cyclic, a standard argument yields $s_{n-1}(P) \equiv 1 + p \mod p^2$. Since $m(P; p^{n-1}) = p$, (1) is true if $e = n-1$. Assume $e \leq n-2$. Since P is not cyclic, $|P/\Phi(P)| \geq p^2$. Let $\mathcal{M}$ be the set of maximal subgroups of P. Let $\mathcal{M}'$ be the set of subgroups Q of P such that $\Phi(P) \leq Q$ and that $|P/Q| = p^2$. Then, by Lemma 1.3 (with $\mathcal{S} = S_e(P)$)

$$s_e(P) \equiv \sum_{M \in \mathcal{M}} s_e(M) - p \sum_{Q \in \mathcal{M}'} s_e(Q) \mod p^2.$$

Since, by Theorem 2, $s_e(Q) \equiv 1 \mod p$ for $Q \in \mathcal{M}'$ and $|\mathcal{M}'| \equiv 1 \mod p$, we get

$$s_e(P) \equiv \sum_{M \in \mathcal{M}} s_e(M) - p \mod p^2.$$

By Lemma 1.3

$$s_{e+1}(P,\mathcal{C}) \equiv \sum_{M\in\mathcal{M}} s_{e+1}(M,\mathcal{C}) \mod p.$$

So by Proposition 1.2,

$$m(P;p^e) \equiv \sum_{M\in\mathcal{M}} m(M;p^e) \mod p.$$

Thus

$$\begin{aligned} s_e(P) + m(P;p^e)p &\equiv \sum_{M\in\mathcal{M}} \{s_e(M) + m(M;p^e)p\} - p \mod p^2 \\ &\equiv (1+p)|\mathcal{M}| - p \mod p^2 (\text{by induction}) \\ &\equiv (1+p)^2 - p \mod p^2 (\text{since } |\mathcal{M}| \equiv 1+p \mod p^2) \\ &\equiv 1 + p \mod p^2. \end{aligned}$$

Thus the lemma is proved. □

We need the following

Lemma 2.2. *Let G be a group with a Sylow p-subgroup P of order p^n $(n \geq 2)$.*
(i) *If P is non-exceptional, $s_1(G) \equiv 1+p \mod p^2$.*
(ii) *If P is exceptional, $s_1(G) \equiv 1 \mod p^2$.*

Proof. We have

$$s_1(G)(p-1) + 1 = |G(p)| = m(G;p)p.$$

Thus the result follows from Theorem A. (Note that, by Proposition 1.2, $m(G;p) \equiv 1 \mod p$ if P is cyclic.) □

In the following we write $C_e(G)$ instead of $S_e(G,\mathcal{C})$ and put $c_e(G) = |C_e(G)|$.

Proof of Theorem C. By Proposition 1.2 and Lemma 2.1, it suffices to show the following:

(1) $$s_e(G) \equiv s_e(P) \mod p^2 \quad \text{for any } e \text{ with } 1 \leq e \leq n-1.$$

By Lemma 2.2,

(2) $$s_1(G) \equiv s_1(P) \mod p^2.$$

So (1) is true when $n = 2$. Assume $n \geq 3$. We shall show

(3) $$s_{e+1}(G) - s_{e+1}(P) \equiv s_e(G) - s_e(P) \mod p^2 \quad \text{for} \quad 1 \leq e \leq n-2.$$

Then (1) follows from (2) and (3).

Let $1 \le e \le n-2$. Let $X_e(G)$ be the set of all subgroups Q of G of order p^e such that $N_G(Q)/Q$ has an exceptional Sylow p-subgroup. Let $Y_e(G)$ be the set of all subgroups Q of G of order p^e such that $N_G(Q)/Q$ has a Sylow p-subgroup of order p. So $Y_e(G) \subseteq X_e(G) \subseteq S_e(G)$. Put $x_e(G) = |X_e(G)|$ and $y_e(G) = |Y_e(G)|$. Let

$$I = \{(Q,R) \,|\, Q \le R,\, Q \in S_e(G),\, R \in S_{e+1}(G)\}.$$

We count $|I|$ in two ways. For a given $R \in S_{e+1}(G)$, the number of $Q \in S_e(G)$ with $Q \le R$ equals $s_e(R)$, which equals 1 if R is cyclic. On the other hand, for a given $Q \in S_e(G)$, the set of $R \in S_{e+1}(G)$ with $Q \le R$ is identified with $S_1(N_G(Q)/Q)$. Thus we get

$$c_{e+1}(G) + \sum_R s_e(R) = \sum_Q s_1(N_G(Q)/Q), \tag{4}$$

where R and Q run over $S_{e+1}(G) - C_{e+1}(G)$ and $S_e(G)$, respectively. We have $s_e(R) \equiv 1+p \mod p^2$ for $R \in S_{e+1}(G) - C_{e+1}(G)$. On the other hand, by Lemma 2.2,

$$\begin{aligned} s_1(N_G(Q)/Q) &\equiv 1+p \mod p^2, \quad \text{if} \quad Q \in S_e(G) - X_e(G), \\ &\equiv 1 \mod p^2, \quad \text{if} \quad Q \in X_e(G) - Y_e(G). \end{aligned}$$

Let $\{Q_i\}$ be a set of representatives of G-conjugacy classes in $Y_e(G)$. Then

$$\begin{aligned} \sum_{Q \in Y_e(G)} s_1(N_G(Q)/Q) &= \sum_i s_1(N_G(Q_i)/Q_i)|G : N_G(Q_i)| \\ &\equiv \sum_i |G : N_G(Q_i)| \mod p^2 \\ &\equiv y_e(G) \mod p^2. \end{aligned}$$

Here we have used the fact that $s_1(N_G(Q_i)/Q_i) \equiv 1 \mod p$(Sylow's theorem) and the fact that $|G : N_G(Q_i)| \equiv 0 \mod p$ since $e \le n-2$. Thus (4) yields

$$\begin{aligned} &c_{e+1}(G) + (1+p)\{s_{e+1}(G) - c_{e+1}(G)\} \\ &\equiv (1+p)\{s_e(G) - x_e(G)\} + \{x_e(G) - y_e(G)\} + y_e(G) \mod p^2. \end{aligned}$$

Hence

$$(1+p)s_{e+1}(G) - c_{e+1}(G)p \equiv (1+p)s_e(G) - x_e(G)p \mod p^2. \tag{5}$$

Applying (5) to the case where $G = P$, we get

$$(1+p)s_{e+1}(P) - c_{e+1}(P)p \equiv (1+p)s_e(P) - x_e(P)p \mod p^2, \tag{6}$$

where $x_e(P)$ is defined in a manner similar to $x_e(G)$. Now $c_{e+1}(G) \equiv c_{e+1}(P) \mod p$ by Proposition 1.2. Further, $x_e(G) \equiv x_e(P) \mod p$. Indeed, considering the conjugation action of P on $X_e(G)$, we get

$$x_e(G) \equiv \#\{\, Q \,|\, Q \lhd P,\, |Q| = p^e,\, P/Q \text{ is exceptional} \,\} \mod p. \tag{7}$$

We can obtain a similar formula for $x_e(P)$ in a similar way. Thus $x_e(G) \equiv x_e(P) \mod p$. So, by (5) and (6), we get

$$s_{e+1}(G) - s_{e+1}(P) \equiv s_e(G) - s_e(P) \mod p^2.$$

Thus (3) is proved and the proof is complete. □

Remark. Theorem C shows that Theorems 3 and 5 are equivalent.

We obtain another congruence for $m(G; p^e)$.

Corollary 2.3. *Let G be a group with a Sylow p-subgroup P of order p^n. For any e with $1 \le e \le n-3$, we have*

$$m(G; p^e) \equiv \#\{\, Q \mid Q \triangleleft P,\ |Q| = p^e,\ P/Q \text{ is exceptional} \,\} \mod p.$$

Proof. By Proposition 1.2,

$$m(G; p^e) \equiv m(P; p^e) \equiv c_{e+1}(P) \mod p.$$

By (6) in the proof of Theorem C, we have

$$(1+p)s_{e+1}(P) - c_{e+1}(P)p \equiv (1+p)s_e(P) - x_e(P)p \mod p^2.$$

By Theorem D, $s_{e+1}(P) \equiv s_e(P) \mod p^2$. Thus it follows that $m(G; p^e) \equiv x_e(P) \mod p$. Hence the assertion follows from (7) in the proof of Theorem C (with $G = P$). This completes the proof. □

We give a new proof to a well-known theorem of Taussky. See [Hu, III 11.9], [Go, Theorem 5.4.5] for other proofs.

Proposition 2.4 (Taussky [Ta]). *Let P be a non-abelian 2-group with $|P : P'| = 4$, where P' is the commutator subgroup of P. Then P is quaternion, dihedral, or semi-dihedral.*

Proof. Put $|P| = 2^n$. The result is clear when $n = 3$. Assume $n \ge 4$. Let X be the set of normal subgroups of P of order 2^{n-3}. For any $Q \in X$, P/Q is either quaternion or dihedral of order 8, since $|P : P'| = 4$. Thus P/Q is exceptional. Hence $m(G; 2^{n-3}) \equiv |X| \mod 2$ by Corollary 2.3. On the other hand, $|X|$ is odd by Theorem 2 and Lemma 1.1. Hence $m(G; 2^{n-3})$ is odd, and P is exceptional by Theorem A. Since P is not cyclic, the result follows. □

Meiji-machi 2-27
Izumi Toki-shi
Gifu 509-5146, Japan

References

[AT] T. Asai and Y. Takegahara, |Hom(A, G)|, IV, J. Algebra, **246** (2001), 543-563.

[Fr1] G. Frobenius, Verallgeminerung des Sylowschen Satzes, Sitzungsberichte der Koniglich Preußischen Akademie der Wissenschaften zu Berlin, 1895, pp. 981–993. (= Gesammelte Abhandlungen, Bd. II, pp. 664–676.)

[Fr2] G. Frobenius, Über einen Fundamentalsatz der Gruppentheorie, Sitzungsberichte der Koniglich Preußischen Akademie der Wissenschaften zu Berlin, 1903, pp. 987–991. (= Gesammelte Abhandlungen, Bd. III, pp. 330–334.)

[Go] D. Gorenstein, Finite Groups, Harper and Row, 1968. (Chelsea, 1980)

[Ha1] P. Hall, A contribution to the theory of groups of prime power order, Proc. London Math. Soc., **36** (1933), 29–95.

[Ha2] P. Hall, On a theorem of Frobenius, Proc. London Math. Soc., **40** (1935), 468–501.

[Hu] B. Huppert, Endliche Gruppen I, Springer-Verlag, Berlin, 1967.

[IY] N. Iiyori and H. Yamaki, On a conjecture of Frobenius, Bull. Amer. Math. Soc., **25** (1991), 413–416.

[Is] I. M. Isaacs, Character Theory of Finite Groups, Academic Press, New York, 1976.

[Ku] A. Kulakoff, Über die Anzahl der eigentlichen Untergruppen und der Elemente von gegebener Ordnung in p-Gruppen, Math. Ann., **104** (1931), 778–793.

[La] T. Y. Lam, Artin exponent of finite groups, J. Algebra, **9** (1968), 94–119.

[Mi] G. A. Miller, An extension of Sylow's theorem, Proc. London Math. Soc., **2** (1905), 142–143.

[Mu] M. Murai, On a conjecture of Frobenius, Sugaku, **35** (1983), 82–84. (in Japanese)

[Su] M. Suzuki, Group Theory II, Springer-Verlag, Berlin, 1986.

[Ta] O. Taussky, A remark on the class field tower, J. London Math. Soc., **12** (1937), 82–85.

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

Added in proof: For a generalization of Theorem A (i), see M. Murai and Y. Takegahara, Hall's relations in finite groups, preprint.