New York Journal of Mathematics

New York J. Math. **32** (2026) 1344–1349.

Finite groups with few elements of prime order

Alireza Khalili Asboei

Abstract. Let G be a finite group and let p be an odd prime. We denote by $m_p(G)$ the number of elements of order p in G. If $s_p(G)$ denotes the number of subgroups of order p, then $m_p(G) = (p-1)s_p(G)$. Together with Frobenius' congruence $s_p(G) \equiv 1 \pmod{p}$, this shows that the first two possible positive values of $m_p(G)$ are $p-1$ and p^2-1.

We first investigate the first threshold and obtain a solvability criterion for finite groups satisfying $0 < m_p(G) < p^2-1$. We then study the boundary value $m_p(G) = p^2-1$. In this case, the group has exactly $p+1$ subgroups of order p, and the conjugation action on these subgroups provides a natural permutation representation of degree $p+1$. This action will be the main tool in the analysis of the simple case. Finally, we prove that if S is a finite nonabelian simple group and $p \geq 5$, then $m_p(S) = p^2-1$ if and only if $S \cong \mathrm{PSL}_2(p)$. We also show that no finite nonabelian simple group satisfies $m_3(S) = 8$.

Contents

1. Introduction

Let G be a finite group and let p be a prime. We denote by $m_p(G)$ the number of elements of order p in G. Numerical invariants associated with element orders have long played an important role in the study of finite groups and have proved useful in recognition, classification, and solvability problems.

Received July 24, 2026.
2010 *Mathematics Subject Classification.* 20D60, 20D05, 20D10.
Key words and phrases. Finite groups, finite simple groups, solvable groups, elements of prime order.

ISSN 1076-9803/2026

Let $s_p(G)$ denote the number of subgroups of order p. Since every subgroup of order p contains exactly $p-1$ nonidentity elements and two distinct subgroups of order p intersect trivially, one has $m_p(G) = (p-1)s_p(G)$. Combined with Frobenius' congruence $s_p(G) \equiv 1 \pmod p$, this shows that the smallest positive values of $m_p(G)$ are

$$p-1, \qquad p^2-1, \qquad 2p^2-p-1, \dots .$$

These values naturally motivate the study of finite groups having few elements of order p.

Recognition of finite groups by numerical invariants has been studied extensively. In particular, the author [1] studied characterizations of $\mathrm{PSL}_2(r)$ using its order and the number of its Sylow r-subgroups; in the Mersenne-prime case, additional prime-graph information is required. Related structural results based on the number of involutions were obtained in [2].

The present paper investigates the first two positive values of the invariant $m_p(G)$. Our main result is the following.

Theorem 1.1. *Let S be a finite nonabelian simple group and let $p \geq 5$ be a prime. Then $m_p(S) = p^2 - 1$ if and only if $S \cong \mathrm{PSL}_2(p)$.*

The proof combines elementary counting arguments with Sylow theory, permutation representations, and the Brauer–Reynolds theorem.

2. Preliminaries

Throughout, G denotes a finite group and p denotes an odd prime. We set

$$\Omega_p(G) = \{x \in G \mid |x| = p\}, \qquad m_p(G) = |\Omega_p(G)|.$$

Let

$$\mathcal{S}_p(G) = \{P \leq G \mid |P| = p\}, \qquad s_p(G) = |\mathcal{S}_p(G)|.$$

We also denote by $n_p(G)$ the number of Sylow p-subgroups of G.

Lemma 2.1. *For every finite group G, $m_p(G) = (p-1)s_p(G)$.*

Proposition 2.2. *Suppose that $p \mid |G|$. Then $m_p(G) \equiv -1 \pmod p$. Equivalently, $s_p(G) \equiv 1 \pmod p$.*

Proof. By Frobenius' theorem [4], the number of solutions of $x^p = 1$ is divisible by p. These solutions are the identity and the elements of order p. Hence $1 + m_p(G) \equiv 0 \pmod p$. The second congruence follows from Lemma 2.1. □

Corollary 2.3. *If $p \mid |G|$, then $m_p(G) = (p-1)(1+kp)$ for some integer $k \geq 0$. In particular, the smallest positive values of $m_p(G)$ are*

$$p-1, \qquad p^2-1, \qquad 2p^2-p-1, \qquad 3p^2-2p-1, \dots .$$

Proof. By Proposition 2.2, $s_p(G) = 1 + kp$ for some $k \geq 0$. Now apply Lemma 2.1. □

Proposition 2.4. *The following conditions are equivalent:*

(i) $0 < m_p(G) < p^2 - 1$*;*
(ii) $m_p(G) = p - 1$*;*
(iii) *G has a unique subgroup of order p.*

Proof. Assume that $0 < m_p(G) < p^2 - 1$. Then $p \mid |G|$, and hence $s_p(G) \equiv 1 \pmod{p}$ by Proposition 2.2. Moreover, $(p-1)s_p(G) = m_p(G) < (p-1)(p+1)$, so $s_p(G) < p + 1$. Therefore $s_p(G) = 1$, proving (i)⇒(iii).

If $s_p(G) = 1$, then Lemma 2.1 gives $m_p(G) = p - 1$. Thus (iii)⇒(ii). Obviously, (ii)⇒(i). □

Proposition 2.5. *The equality $m_p(G) = p^2-1$ holds if and only if $s_p(G) = p+1$.*

Proof. This follows immediately from $m_p(G) = (p-1)s_p(G)$. □

We shall use the following consequence of a theorem of Brauer and Reynolds [3]; see also [1, Corollary 2.2].

Theorem 2.6 (Brauer–Reynolds)**.** *Let G be a finite perfect group, and let p be a prime such that*

$$p \mid |G|, \qquad p^2 \nmid |G|, \qquad n_p(G) = p + 1,$$

where $n_p(G)$ denotes the number of Sylow p-subgroups of G. Then G has a homomorphic image isomorphic to $\mathrm{PSL}_2(p)$*.*

3. Groups with few elements of prime order

3.1. The first threshold. We first recall the structural result needed for the first case. It is a consequence of Burnside's transfer and normal p-complement theorems; see [5, Theorems 7.4.3 and 7.4.4]. An explicit formulation for groups with a unique subgroup of order p is given in [6, Theorem 7].

Lemma 3.1. *Let G be a finite group and let p be an odd prime. Suppose that G has a unique subgroup A of order p. Then G possesses a normal p-nilpotent subgroup N such that G/N is cyclic and $|G/N|$ divides $p-1$. In particular, every nonabelian composition factor of G has order coprime to p.*

Proof. Since A is the unique subgroup of G of order p, it is characteristic in G. Thus $A \trianglelefteq G$ and $A \leq O_p(G)$. Moreover, A is the unique subgroup of $O_p(G)$ of order p; hence, in the notation used in [6], $\Omega(O_p(G)) = A$.

Set $N = C_G(A)$. By [6, Theorem 7], $N = C_G(\Omega(O_p(G)))$ is a normal p-nilpotent subgroup of G. The conjugation action of G on A yields $G/N \hookrightarrow \mathrm{Aut}(A)$. Since $A \cong C_p$ and $\mathrm{Aut}(A) \cong C_{p-1}$, the quotient G/N is cyclic and $|G/N|$ divides $p-1$.

Let $K = O_{p'}(N)$, the unique normal Hall p'-subgroup of N. Hence K is characteristic in N, and since $N \trianglelefteq G$, we have $K \trianglelefteq G$. Moreover, N/K is a p-group and G/N is cyclic. Therefore every nonabelian composition factor of G occurs among the composition factors of the p'-group K, and hence has order coprime to p. □

Theorem 3.2. *Let G be a finite group and let p be an odd prime dividing $|G|$. Suppose that $0 < m_p(G) < p^2 - 1$. If G has no nonabelian composition factor whose order is coprime to p, then G is solvable.*

Proof. By Proposition 2.4, the group G has a unique subgroup of order p. Lemma 3.1 therefore shows that every nonabelian composition factor of G has order coprime to p. By hypothesis, no such composition factor exists. Hence all composition factors of G are cyclic of prime order, and therefore G is solvable. $\square$

We now consider the case $m_p(G) = p^2 - 1$.

Proposition 3.3. *Let G be a finite group and let p be an odd prime. Suppose that $m_p(G) = p^2 - 1$. Then the conjugation action of G on the set of subgroups of order p has degree $p + 1$. Moreover, if K denotes the kernel of this action, then $G/K \leq \mathrm{Sym}(p + 1)$.*

Proof. By Proposition 2.5, one has $s_p(G) = p + 1$. The conjugation action of G on $\mathcal{S}_p(G)$ defines a homomorphism $\varphi : G \longrightarrow \mathrm{Sym}(\mathcal{S}_p(G))$.

Let $K = \ker(\varphi)$. Then the induced action of G/K on $\mathcal{S}_p(G)$ is faithful. Since $|\mathcal{S}_p(G)| = p + 1$, it follows that $G/K \leq \mathrm{Sym}(p + 1)$. $\square$

3.2. The simple boundary case. Throughout this section, let S be a finite nonabelian simple group and let $p \geq 5$ be a prime.

Lemma 3.4. *Suppose that $m_p(S) = p^2 - 1$. Then the conjugation action of S on the set $\mathcal{S}_p(S)$ of subgroups of order p is faithful. Consequently, $S \hookrightarrow \mathrm{Sym}(p + 1)$.*

Proof. By Proposition 2.5, one has $s_p(S) = p + 1$. Conjugation defines a homomorphism $\varphi : S \longrightarrow \mathrm{Sym}(\mathcal{S}_p(S))$.

The kernel of φ is normal in S. Since S is simple, it is either trivial or equal to S. The latter case would imply that every subgroup of order p is normal in S, which is impossible. Thus $\ker \varphi = 1$.

Since $|\mathcal{S}_p(S)| = p + 1$, it follows that $S \hookrightarrow \mathrm{Sym}(p + 1)$. $\square$

Lemma 3.5. *Suppose that $m_p(S) = p^2 - 1$. Then $v_p(|S|) = 1$. Equivalently, $|S|_p = p$. In particular, $p^2 \nmid |S|$.*

Proof. By Lemma 3.4, $S \hookrightarrow \mathrm{Sym}(p + 1)$, and hence $|S|$ divides $(p + 1)!$. Since $p < p + 1 < 2p$, the only multiple of p among $1, 2, \dots, p + 1$ is p. Therefore $v_p((p + 1)!) = 1$, and hence $v_p(|S|) \leq 1$.

On the other hand, $m_p(S) > 0$, so $p \mid |S|$. Thus $v_p(|S|) = 1$. $\square$

Corollary 3.6. *Suppose that $m_p(S) = p^2 - 1$. Then every subgroup of order p in S is a Sylow p-subgroup, and $n_p(S) = p + 1$.*

Proof. By Lemma 3.5, $|S|_p = p$. Hence every subgroup of order p is a Sylow p-subgroup. Since Proposition 2.5 gives $s_p(S) = p + 1$, one has $n_p(S) = p + 1$. $\square$

Theorem 3.7. *Let $p \geq 5$ be a prime and let S be a finite nonabelian simple group. Then $m_p(S) = p^2 - 1$ if and only if $S \cong \mathrm{PSL}_2(p)$.*

Proof. Assume first that $m_p(S) = p^2 - 1$. By Corollary 3.6, $n_p(S) = p + 1$, and by Lemma 3.5, $p^2 \nmid |S|$. Moreover, $p \mid |S|$, and S is perfect. Hence Theorem 2.6 implies that S has a homomorphic image isomorphic to $\mathrm{PSL}_2(p)$. Since S is simple, it follows that $S \cong \mathrm{PSL}_2(p)$.

Conversely, let $S = \mathrm{PSL}_2(p)$ and let P be a Sylow p-subgroup of S. Then $|P| = p$ and $|N_S(P)| = p(p-1)/2$. Since $|S| = p(p^2-1)/2$, one obtains $n_p(S) = |S|/|N_S(P)| = p + 1$.

Distinct Sylow p-subgroups intersect trivially, and each contains $p - 1$ non-identity elements. Therefore $m_p(S) = (p+1)(p-1) = p^2 - 1$. $\square$

Proposition 3.8. *Let S be a finite nonabelian simple group. Then*

$$m_3(S) \neq 3^2 - 1 = 8.$$

Proof. Assume that $m_3(S) = 8$. By Lemma 2.1, $s_3(S) = 4$. Thus conjugation on the four subgroups of order 3 gives a homomorphism $S \longrightarrow \mathrm{Sym}(4)$.

Its kernel is normal in S. It cannot be equal to S, since this would make every subgroup of order 3 normal in S. Hence the action is faithful, and $S \hookrightarrow \mathrm{Sym}(4)$. This is impossible because $\mathrm{Sym}(4)$ has no nonabelian simple subgroup. Therefore $m_3(S) \neq 8$. $\square$

4. Open problems

The results of this paper suggest several directions for further research.

(1) Classify finite groups satisfying $m_p(G) = 2p^2 - p - 1$, or more generally, $m_p(G) = (p-1)(kp+1)$, where $k \geq 2$.
(2) Investigate analogous extremal problems for elements of prime-power order.
(3) Determine whether similar characterization results hold for almost simple groups.

Acknowledgements

The author would like to thank the anonymous referee for the careful reading of the manuscript and for the constructive comments and insightful suggestions, which significantly improved the presentation and exposition of this paper.

References

[1] Asboei, Alireza K. Characterizing $\mathrm{PSL}_2(r)$ by its order and the number of its Sylow r-subgroups. *J. Algebra Appl.* **13** (2014), no. 1, 1350065 (6 pages). MR3096846, doi: 10.1142/S0219498813500655. 1345, 1346

[2] Asboei, Alireza K. Groups with fewer than 15 involutions. *Commun. Algebra* **51** (2023), no. 10, 4171–4175. MR4613261, Zbl 1521.20049, doi: 10.1080/00927872.2023.2198027. 1345

[3] Brauer, R.; Reynolds, W. F. On a problem of E. Artin. *Ann. of Math. (2)* **68** (1958), 713–720. MR0100635, Zbl 0082.24803, doi: 10.2307/1970164. 1346

[4] Frobenius, Ferdinand G. Verallgemeinerung des Sylowschen Satzes. Berlin (1895), 981–993. JFM 26.0158.01, doi: 10.3931/e-rara-18880. 1345

[5] GORENSTEIN, D. *Finite Groups*, 2nd ed., Chelsea Publishing Company, New York, 1980. MR0569209, Zbl 0463.20012. 1346

[6] SCHMIDT, J. *Finite groups with a unique subgroup of order p*, University of Kentucky, 2009. https://www.ms.uky.edu/~jack/2009-07-08-UniqueSubgroupOfOrderP.pdf. 1346

(Alireza Khalili Asboei) DEPARTMENT OF MATHEMATICS EDUCATION, FARHANGIAN UNIVERSITY, P.O. BOX 14665-889, TEHRAN, IRAN
a.khalili@cfu.ac.ir

This paper is available via http://nyjm.albany.edu/j/2026/32-54.html.