J. Group Theory, Ahead of Print
DOI 10.1515/jgth-2020-0046

Conjugacy class sizes in arithmetic progression

Mariagrazia Bianchi, Stephen P. Glasby and Cheryl E. Praeger

Communicated by Andrea Lucchini

Abstract. Let $\mathrm{cs}(G)$ denote the set of conjugacy class sizes of a group G, and let $\mathrm{cs}^*(G) = \mathrm{cs}(G) \setminus \{1\}$ be the sizes of non-central classes. We prove three results. We classify all finite groups for which (1) $\mathrm{cs}(G) = \{a, a+d, \ldots, a+rd\}$ is an arithmetic progression with $r \geqslant 2$; (2) $\mathrm{cs}^*(G) = \{2, 4, 6\}$ is the smallest case where $\mathrm{cs}^*(G)$ is an arithmetic progression of length more than 2 (our most substantial result); (3) the largest two members of $\mathrm{cs}^*(G)$ are coprime. For (3), it is not obvious, but it is true that $\mathrm{cs}^*(G)$ has two elements, and so is an arithmetic progression.

1 Introduction

There is a well-known but mysterious bijection between the set of irreducible characters of a finite group G and the set of conjugacy classes of G. (For the symmetric groups S_n, the bijection is understood via the partitions of n.) It is surprising that the set $\mathrm{cd}(G)$ of degrees of irreducible characters (over $\mathbb{C}$) of G and the set $\mathrm{cs}(G)$ of sizes of conjugacy classes of G both seem to impose strong constraints on the structure of G. Surveys of these topics [6, 12, 19] state theorems where related hypotheses on $\mathrm{cd}(G)$ and $\mathrm{cs}(G)$ give rise to similar structural constraints on G.

Huppert [13] shows that if G satisfies

$$\mathrm{cd}(G) = \{1, 2, \ldots, k\}, \quad \text{then} \quad k \in \{1, 2, 3, 4, 6\},$$

and he describes such groups for each k. An analogous result shows that if

$$\mathrm{cs}(G) = \{1, 2, \ldots, k\}, \quad \text{then} \quad k \in \{1, 2, 3\};$$

see [2, Theorem 1]. In general, it is hard to classify all groups G with a specified set $\mathrm{cs}(G)$. We do this when $\mathrm{cs}(G) = \{a_0, a_1, \ldots, a_r\}$ is an arithmetic progression

SG and CP gratefully acknowledge support from the Australian Research Council Discovery Project DP190100450. MB acknowledges support from G.N.S.A.G.A. (Indam) and thanks the Centre for the Mathematics of Symmetry and Computation (CMSC) for its hospitality. This work began in the CMSC Research Retreat of 2019. CP also thanks the Isaac Newton Institute for Mathematical Sciences for support and hospitality during the programme “Groups, Representations and applications: New Perspectives”. This program was supported by EPSRC grant number EP/R014604/1.

where $a_i = a_0 + id$ for $i \geqslant 0$, and $a_0, d \geqslant 1$ (Proposition 3). The result relies on a classification of groups G whose largest two class sizes are coprime (Theorem 1). The latter strengthens both [3, Theorem] and [9, Theorem (B1)].

Henceforth, all our groups will be finite.

Theorem 1. *Suppose that G is a group with no non-trivial abelian direct factors and the largest two non-central conjugacy class sizes of G are m and n where $m < n$. Then $\gcd(m,n) = 1$ if and only if $\mathrm{cs}(G) = \{1, m, n\}$, $G = K \rtimes L$ where K is abelian $\gcd(|K|, |L|) = 1$, $\mathrm{Z}(G) < L$, $L/\mathrm{Z}(G)$ is cyclic, $G/\mathrm{Z}(G)$ is a Frobenius group with kernel $K\mathrm{Z}(G)/\mathrm{Z}(G)$ and $m = |L : \mathrm{Z}(G)|$, $n = |K|$ satisfy $n \equiv 1 \pmod{m}$.*

To suppress certain details, it is useful to consider the set $\mathrm{cd}^*(G)$ of non-linear character degrees of G and the set $\mathrm{cs}^*(G)$ of non-central conjugacy class sizes. The former "ignores" the derived quotient G/G' and the latter "ignores" the centre $\mathrm{Z}(G)$.

Note that if C is abelian then $\mathrm{cs}(G \times C) = \mathrm{cs}(G)$, and hence

$$\mathrm{cs}^*(G \times C) = \mathrm{cs}^*(G).$$

Our main theorem (Theorem 2) classifies groups G with $\mathrm{cs}^*(G) = \{2, 4, 6\}$. (This is the smallest case when $\mathrm{cs}^*(G) = \{a_0, a_0 + d, a_0 + 2d\}$ as $\mathrm{cs}^*(G) = \{2, 3, 4\}$ is excluded by Proposition 3.) Our proof of Theorem 2 is both delicate and lengthy. The case $\mathrm{cs}^*(G) = \{2, 4, 6, 8\}$ was solved in [4].

Theorem 2. *Suppose that G is a finite group with no abelian direct factors and $\mathrm{cs}^*(G) = \{2, 4, 6\}$. Then $G = AB$, where $B \trianglelefteq G$, $|A| = 2^\alpha$, $|B| = 3$, $|A'| = 2$ and $\mathrm{Z}(A) < C_A(B) < A$. Conversely, if G has these properties, then*

$$\mathrm{cs}^*(G) = \{2, 4, 6\}.$$

The number n_α of groups of order $2^\alpha 3$ with $\mathrm{cs}^*(G) = \{2, 4, 6\}$ and no non-trivial abelian direct factors increases quite rapidly with α. For example, we have $n_\alpha = 4, 16, 46, 104$ when $\alpha = 5, 6, 7, 8$; see Remark 7.

Conjugacy classes x^G of prime power size are important. A beautiful theorem of Kazarin [18] says if $|x^G|$ is a prime power, then $\langle x^G \rangle$ is a solvable subgroup of G.

In Section 2, we first prove Theorem 1. Next we prove that if $\mathrm{cs}(G)$ is an arithmetic progression of length at least 3, then $\mathrm{cs}(G) = \{1, m, n\}$ satisfying the conditions of Theorem 1, and from this, we deduce the detailed structure of G (see Proposition 3). Section 3 explores how number theory constrains possible arithmetic progressions involving precisely two primes; see Lemma 5 and Remark 6.

Sections 4 and 5 give the proof of Theorem 2 when $\mathrm{cs}^*(G) = \mathrm{cs}(G) \setminus \{1\}$ equals $\{2, 4, 6\}$. Call $r = |\mathrm{cs}^*(G)|$ the *conjugacy rank* of G.

We remark that $\mathrm{cs}^*(G)$ can *contain* arbitrarily long arithmetic progressions. Consider $G_k = C_2 \wr C_k$. Since $k, 2^{k-1} \in \mathrm{cs}(G_k)$, we see that

$$\{1, 2, \ldots, n\} \subseteq \mathrm{cs}\left(\prod_{k=1}^{n} G_k\right).$$

Also, $\mathrm{cs}(G)$ can equal a *geometric* progression of arbitrary length by [8, Theorem]. Indeed, given an arbitrary set S of p-powers, [8, Theorem] shows that there is a p-group G of class 2 with $\mathrm{cs}(G) = S$.

2 Conjugacy class sizes

The set $\mathrm{cs}^*(S_n)$ of non-trivial conjugacy class sizes for the symmetric group S_n below suggests that common divisors of class sizes are important. Indeed, the common divisor graph [6] plays a central role. Note that the class equation has the form $|G| = \sum_{k \in \mathrm{cs}(G)} m_k k$, where m_k is the number of classes of G of size k.

n	2	3	4	5	6
$\mathrm{cs}^*(S_n)$	$\{\}$	$\{2, 3\}$	$\{3, 6, 8\}$	$\{10, 15, 20, 24, 30\}$	$\{15, 40, 45, 90, 120, 144\}$

In this section, we study groups G with $\mathrm{cs}(G) = \{1, 1 + d, \ldots, 1 + rd\}$. It seems remarkable to the authors that, building on [3], we can classify such G if $r \geqslant 2$. Before giving our proof, we review some definitions and record some useful facts.

A group G is a *Frobenius group* if it has a proper subgroup H with the property that $H \cap H^g = 1$ for all $g \in G \setminus H$. Using character theory, it can be shown that H determines a normal subgroup K satisfying $K \setminus \{1\} = \bigcap_{g \in G} (G \setminus H^g)$. Observe that $G = KH$. We call K the *Frobenius kernel* and H the *Frobenius complement* as $H \cap K = 1$. The structure of H and K is severely constrained [14, Chapter 6]. For example, K is nilpotent, and if $|H|$ is even, then K is abelian. Moreover, the Sylow subgroups of H are cyclic or generalised quaternion 2-groups [14, Corollary 6.17]. For $x, g \in G$, let $x^g = g^{-1}xg$, $x^G = \{x^g \mid g \in G\}$ and $[x, g] = x^{-1}x^g$.

One way to suppress the role of abelian direct factors is to focus on the classes of $G \setminus \mathrm{Z}(G)$ and study when $\mathrm{cs}^*(G) := \mathrm{cs}(G) \setminus \{1\}$ is an arithmetic progression. Results such as Proposition 3 and Theorem 1 affirm this decision, and experimental evidence shows that there is a much richer family of groups for which $\mathrm{cs}^*(G)$ is an arithmetic progression rather than $\mathrm{cs}(G)$. Recall that $r = |\mathrm{cs}^*(G)|$ is called the *conjugacy rank* of G. Groups with $r \leqslant 2$ have been well studied. Itô proved if $r = 1$, then G is nilpotent [15], and if $r = 2$, then G is solvable [16]. In addition, he proved in [17] that if G is simple and $r = 3$, then $G \cong \mathrm{SL}_2(2^f)$ with $f \geqslant 2$.

We consider conjugacy rank three groups with $\mathrm{cs}^*(G) = \{a_0, a_0 + d, a_0 + 2d\}$. Since $a_0 \geqslant 2$ and $d \geqslant 2$, the smallest example has $\mathrm{cs}^*(G) = \{2, 4, 6\}$. (The possibility $\mathrm{cs}(G) = \{1, 2, 3, 4\}$ with $d = 1$ does not arise by Proposition 3.) There are many groups G with $\mathrm{cs}^*(G) = \{2, 4, 6\}$ (see Remark 7), and determining their common features, to show that our necessary conditions are sufficient, was a challenge.

Proof of Theorem 1. Suppose that G is as in the hypothesis of Theorem 1 (see Section 1), and recall the meaning of m and n. It follows from [3, Corollary 2] that G has conjugacy rank $r = 2$, so $\mathrm{cs}^*(G) = \{m, n\}$. Dolfi and Jabara [9, Theorem A] characterise groups with $r = 2$, into one of four types called (A), (B1), (B2) and (B3), and the connection with the class sizes is given in [9, Lemma 3.3]. Case (A) does not arise since $\gcd(m, n) = 1$. Thus $G = KL$, where $K \trianglelefteqslant G$ and $\gcd(|K|, |L|) = 1$. In case (B2), L is a nonabelian p-group, $|L : O_p(G)| = p$ and $\mathrm{cs}^*(G) = \{p, |O_p(G) : \mathrm{Z}(L)||K|\}$. Since $\gcd(m, n) = 1$, we must have

$$O_p(G) = \mathrm{Z}(L).$$

Hence $L/\mathrm{Z}(L) \cong C_p$ and L is abelian, a contradiction. Thus case (B2) does not occur. In case (B3), $\mathrm{cs}^*(G) = \{p^a, p^b|L/L \cap \mathrm{Z}(G)|\}$ by [9, Lemma 3.3]. However, $a \geqslant 1$ and $b \geqslant 1$ since $p^a = |K : \mathrm{Z}(K)| > 1$ and $\mathrm{cs}^*(K) = \{p^b\}$. Thus we have $\gcd(m, n) \neq 1$, a contradiction.

The only remaining possibility is that G has type (B1). In this case, K and L are abelian, $\mathrm{Z}(G) < L$ and $G/\mathrm{Z}(G)$ is a Frobenius group by [9, Theorem A]. It follows from the proof of [9, Theorem A] that $K\mathrm{Z}(G)/\mathrm{Z}(G)$ is the kernel of $G/\mathrm{Z}(G)$.

Let $\overline{}\colon G \to G/\mathrm{Z}(G)$ be the natural projection, let $\overline{G} = G/\mathrm{Z}(G)$, and write $\overline{G} = \overline{K} \rtimes \overline{L}$. By [9, Lemma 3.3], $\mathrm{cs}^*(\overline{G}) = \{|\overline{K}|, |\overline{L}|\}$ equals $\{m, n\}$. However, $\overline{G}$ is a Frobenius group, so for $1 \neq \overline{k} \in \overline{K}$, $C_{\overline{G}}(\overline{k}) \leqslant \overline{K}$ by [14, Theorem 6.4]. This implies $C_{\overline{G}}(\overline{k}) = \overline{K}$ as $\overline{K}$ is abelian. Therefore $1 < |\overline{k}^{\overline{G}}| \neq |\overline{K}|$, so $|\overline{k}^{\overline{G}}| = |\overline{L}|$. Further, $|\overline{K}| \equiv 1 \pmod{|\overline{L}|}$ by [14, Lemma 6.1], so $m = |\overline{L}| = |L/\mathrm{Z}(G)|$ is less than $n = |\overline{K}| = |K|$ and $n \equiv 1 \pmod{m}$. Since $\overline{L}$ is abelian, its Sylow subgroups are cyclic by [14, Corollary 6.17] and hence $L/\mathrm{Z}(G)$ is cyclic. This proves one implication.

Consider the reverse implication. We first prove that $\mathrm{cs}(G) = \mathrm{cs}(\overline{G})$, that is $|G : C_G(g)| = |\overline{G} : C_{\overline{G}}(\overline{g})|$ for all $g \in G$. Observe that $L/\mathrm{Z}(G)$ being cyclic implies that L is abelian. Since $\mathrm{Z}(G) \leqslant C_G(g)$, we have $|G : C_G(g)| = |\overline{G} : \overline{C_G(g)}|$. It suffices to prove that $\overline{C_G(g)} = C_{\overline{G}}(\overline{g})$. We show that $\overline{C_G(g)} \geqslant C_{\overline{G}}(\overline{g})$ since

$\overline{C_G(g)} \leqslant C_{\overline{G}}(\overline{g})$ is automatic. Consider three cases. (1) If $g \in \mathrm{Z}(G)$, then we have $\overline{C_G(g)} = C_{\overline{G}}(\overline{g}) = \overline{G}$. (2) Suppose $g \in K\mathrm{Z}(G) \setminus \mathrm{Z}(G)$, say $g = g_0 z$ where $g_0 \neq 1$. Then $C_G(g) = C_G(g_0) \geqslant K$ (as K is abelian), so $\overline{C_G(g)} \geqslant \overline{K} \geqslant C_{\overline{G}}(\overline{g})$ by [14, Theorem 6.4 (4)]. (3) If $g \in G \setminus K\mathrm{Z}(G)$, then $\overline{g} \notin \overline{K}$, and so there exists an $x \in G$ such that $\overline{g} \in \overline{xLx^{-1}}$ as $\overline{G}$ is a Frobenius group. Since $\mathrm{Z}(G) \leqslant xLx^{-1}$, we see that $g \in xLx^{-1}$, that is $g^x \in L$. Thus $C_G(g^x) \geqslant L$ (as L is abelian) and $\overline{C_G(g^x)} \geqslant \overline{L} \geqslant C_{\overline{G}}(\overline{g^x})$ by [14, Theorem 6.4 (3)]. Hence $\overline{C_G(g)} \geqslant C_{\overline{G}}(\overline{g})$.

We next prove that $\mathrm{cs}(\overline{G}) = \{|\overline{K}|, |\overline{L}|\}$. View $\overline{G}$ as a Frobenius group $\overline{K} \rtimes \overline{L}$ with abelian kernel $\overline{K}$ and abelian complement $\overline{L}$. We show that

$$\mathrm{cs}^*(\overline{K} \rtimes \overline{L}) = \{|\overline{K}|, |\overline{L}|\}.$$

Observe that the cosets of $\overline{K}$ in $\overline{K} \rtimes \overline{L}$, other than $\overline{L}$, form a single conjugacy class [14, p. 185, 6A.4], and as $\overline{K}$ is abelian, the classes in $\overline{K} \setminus \{1\}$ all have size $|\overline{L}|$ by [14, Theorem 6.4 (4)]. Hence

$$\mathrm{cs}^*(G) = \mathrm{cs}^*(\overline{G}) = \{m, n\},$$

where $m = |\overline{L}| < n = |\overline{K}|$ satisfy $n \equiv 1 \pmod{m}$. Thus $\gcd(m, n) = 1$, and the reverse implication holds. □

Proposition 3. *Suppose* $\mathrm{cs}(G) = \{a_0, a_0 + d, \dots, a_0 + rd\}$, *where* $a_0, d \geqslant 1$ *and* $r \geqslant 2$. *Then* $a_0 = d = 1$, $r = 2$, *so* $\mathrm{cs}(G) = \{1, 2, 3\}$, *and* $G \cong G_n \times C$, *where*

$$G_n = \langle a, b \mid a^{2^n} = b^3 = 1,\ b^a = b^{-1} \rangle \tag{2.1}$$

and C *is abelian. Clearly,* $G/\mathrm{Z}(G) \cong \mathrm{S}_3$, *where* $\mathrm{Z}(G) = \langle a^2 \rangle \times C$. *Conversely,* $\mathrm{cs}(G_n \times C) = \{1, 2, 3\}$ *for all* $n \geqslant 1$ *and all abelian groups* C.

Proof. Now $1 \in G$ implies $a_0 = 1$. Hence consecutive terms of

$$\mathrm{cs}^*(G) = \{1 + d, \dots, 1 + rd\}$$

are coprime. It follows from [3, Corollary 2, p. 260] that $r \leqslant 2$, and hence $r = 2$. Thus $\mathrm{cs}(G) = \{1, 1 + d, 1 + 2d\}$. Suppose that $a, b \in G$, where $|a^G| = 1 + d$ and $|b^G| = 1 + 2d$. By [3, Theorem, p. 255], $G = NH$, where $N = C_G(a)$ and $H = C_G(b)$ are abelian, $H \cap N = \mathrm{Z}(G)$, and $G/\mathrm{Z}(G)$ is a Frobenius group with kernel $N/\mathrm{Z}(G)$ and complement $H\mathrm{Z}(G)/\mathrm{Z}(G)$. Since $\mathrm{cs}(X \times C) = \mathrm{cs}(X)$ for all abelian C, we may assume that G has no abelian direct factors, so Theorem 1 applies. However, $1 + 2d \equiv 1 \bmod (1 + d)$ holds by Theorem 1. Thus $2d = k(1 + d)$ for some integer k, so $k = 1, d = 1$. Therefore $\mathrm{cs}(G) = \{1, 2, 3\}$, and the structure of G is determined by [2, Theorem 1]. Paraphrasing this result, G has the form (2.1).

Conversely, the elements of $G = G_n \times C$, see (2.1), have a normal form $a^i b^j c$, where $0 \leqslant i < 2^n$, $0 \leqslant j < 3$ and $c \in C$. A simple calculation shows that

$$|(a^i b^j c)^G| = 3 \quad \text{if } i \neq 0, \quad |(b^j c)^G| = 2 \quad \text{if } j \neq 0, \quad \text{and} \quad |c^G| = 1.$$

Thus $\mathrm{cs}(G) = \{1, 2, 3\}$. Let $N = \langle a^2 \rangle \times C$. Since $G/N \cong \mathrm{S}_3$ and $\mathrm{Z}(\mathrm{S}_3) = 1$, an easy calculation shows that $\mathrm{Z}(G) = N$. □

Having deduced that $d = 1$ in the above proof, we could also invoke [2, Theorem 2] with $p^b = 3$. However, [2, Theorem 1] required less work.

3 Arithmetic progressions involving two primes

In Section 2, we saw that group theory strongly constrains when $\mathrm{cs}(G)$ can be an arithmetic progression. This section explores the extent to which number theory alone imposes constraints.

Most research concerning arithmetic progressions and primes falls in two main areas. The first concerns sets of primes containing arbitrarily long arithmetic progressions [10]. The second concerns quantifying the distribution of smooth numbers in arithmetic progressions, e.g. [1]. (A positive integer is called *y-smooth* if all its prime factors are at most y.) This section is motivated by the latter.

We say that an arithmetic progression $a_0, a_1, \dots, a_r$ *involves* at most two primes if $|\bigcup_{i=0}^{r} \pi(a_i)| \leqslant 2$, where $\pi(a_i)$ denotes the set of prime divisors of a_i.

Let $a_i = a_0 + id$ for $i = 0, 1, \dots, k$, and set $\delta := \gcd(a_0, d)$. For all $i \geqslant 1$, we have

$$\gcd(a_{i-1}, a_i) = \delta \quad \text{and} \quad 2a_i = a_{i-1} + a_{i+1}.$$

An arithmetic progression is called *primitive* if $\delta = \gcd(a_0, d) = 1$.

Lemma 5 relies on an easy number-theoretic lemma of John Thompson.

Lemma 4 ([20, Lemma 3]). *Let p be an odd prime. Then the only solutions to $p^m = 2^n \pm 1$ have $m = 1$ and p a Fermat or Mersenne prime, or $3^2 = 2^3 + 1$.*

Lemma 5. *Suppose $k \geqslant 2$ and $(a_0, a_1, \dots, a_k)$ is a primitive arithmetic progression involving at most two primes and $1 \leqslant a_0 < a_1$. If $k \geqslant 3$, the sequence must be $(1, 2, 3, 4)$. If $k = 2$, then $a_0 \in \{1, 2\}$, and the sequence involves precisely two primes, say p and q. Moreover, (a_0, a_1, a_2) equals one of the following:*

(i) $(1, 2^\alpha, 2^{\alpha+1} - 1)$, *where $2^{\alpha+1} - 1$ is a Mersenne prime,*

(ii) $(1, p^\alpha, q^\beta)$, *where $p > 2$, $q^\beta \equiv 1 \pmod 4$ and $1 + q^\beta = 2p^\alpha$,*

(iii) $(2, q, 2^{\alpha+1})$, *where $q = 2^\alpha + 1$ is a Fermat prime,*

(iv) $(2, 3^2, 2^4)$.

Proof. We first classify the arithmetic sequences (a_0, a_1, a_2) with three terms. Write $a_i = p^{\alpha_i} q^{\beta_i}$ for $i = 0, 1, 2$. Let $d = a_1 - a_0$. Since $\delta = 1$, we have

$$\min\{\alpha_0, \alpha_1\} = \min\{\alpha_1, \alpha_2\} = \min\{\beta_0, \beta_1\} = \min\{\beta_1, \beta_2\} = 0.$$

Case $a_0 = 1$. Here $\alpha_0 = \beta_0 = 0$. Since $a_1 \geqslant 2$, one of α_1 or β_1 is positive. Interchanging p and q if necessary, assume that $\alpha_1 > 0$. This forces $\alpha_2 = 0$, so $a_2 = q^{\beta_2}$. Hence in turn $\beta_2 > 0$, so $\beta_1 = 0$ and $(a_0, a_1, a_2) = (1, p^{\alpha_1}, q^{\beta_2})$. Thus $1 + q^{\beta_2} = 2p^{\alpha_1}$, and so q is odd. If $p > 2$, then $1 + q^{\beta_2} \equiv 2 \pmod 4$ shows (ii) holds. If $p = 2$, then $1 + q^{\beta_2} = 2^{\alpha_1 + 1}$ implies by Thompson's lemma (Lemma 4) that $\beta_2 = 1$, and hence $q = 2^{\alpha_1+1} - 1$ is a Mersenne prime (so $\alpha_1 + 1$ must be prime). This is case (i).

Case $a_0 = 2$. Take $p = 2$. Thus we have $\alpha_0 = 1$ and $\beta_0 = 0$. Therefore the arithmetic sequence $(a_0, a_1, a_2) = (2, 2^0 q^{\beta_1}, 2^{\alpha_2})$ satisfies $2 + 2^{\alpha_2} = 2q^{\beta_1}$, that is $1 + 2^{\alpha_2 - 1} = q^{\beta_1}$. If $\alpha_2 - 1 \geqslant 2$ and $\beta_1 \geqslant 2$, then this equation is $1 + 2^3 = 3^2$ by Thompson's lemma. Hence $(a_0, a_1, a_2) = (2, 3^2, 2^4)$, and case (iv) holds. Suppose now that $\alpha_2 - 1 \in \{0, 1\}$. Then $1 + 2^{\alpha_2 - 1}$ equals 2 or 3. However, $q \neq p$, so the only possibility is $(a_0, a_1, a_2) = (2, 3, 2^2)$, and case (iii) holds. Finally, suppose that $\beta_1 = 1$. Then $1 + 2^{\alpha_2 - 1} = q$ is a Fermat prime. This is case (iii), and $\alpha_2 - 1$ is a power of 2. A specific instance is $(a_0, a_1, a_2) = (2, 3, 2^2)$ which extends to $(1, 2, 3, 4)$.

Case $a_0 \geqslant 3$. It is not possible that $\alpha_0 > 0$, $\beta_0 > 0$. Otherwise, $\alpha_1 = \beta_1 = 0$, so $a_1 = 1$ and $3 \leqslant a_0 \leqslant a_1 = 1$, a contradiction. Hence one of α_0 and β_0 is zero. Swapping p and q if necessary, we may assume that $\beta_0 = 0$. Arguing as above, we have $(a_0, a_1, a_2) = (p^{\alpha_0}, q^{\beta_1}, p^{\alpha_2})$, where $p^{\alpha_0} + p^{\alpha_2} = 2q^{\beta_1}$. Since $0 < \alpha_0 < \alpha_2$, p^{α_0} divides the left side. Since $p \neq q$, this implies that $p = 2$. However, $a_0 \geqslant 3$ shows $\alpha_0 \geqslant 2$, and so $4 \mid 2q^{\beta_1}$, a contradiction. Thus this case never occurs.

We have now classified the arithmetic progressions with precisely three terms involving at most two primes. If (a_0, a_1, a_2, a_3) involves at most two primes, then it follows from parts (i)–(iv) that $(a_0, a_1, a_2) = (1, 2, 3)$, and hence

$$(a_0, a_1, a_2, a_3) = (1, 2, 3, 4).$$

Finally, $k \leqslant 3$ as $(1, 2, 3, 4, 5)$ involves more than two primes. □

Remark 6. (a) The primitive arithmetic progressions with first term $a_0 = 1$ are therefore the sequences in (i) and (ii) and $(1, 2, 3, 4)$. The work of [3] excludes $(1, 2, 3, 4)$ from occurring as $\mathrm{cs}(G)$, and Proposition 3 shows that only $(1, 2, 3)$ arises. Thus Lemma 5 illustrates the limitations of using number theory only.

(b) Dividing each term of a non-primitive arithmetic progression by

$$\delta = \gcd(a_0, d)$$

gives a primitive one. Thus all non-primitive arithmetic progressions (a_0, a_1, a_2) involving distinct primes p, q can be classified using Lemma 5 by multiplying by $\delta = p^\alpha q^\beta > 1$. We now consider the non-primitive arithmetic progression $(2, 4, 6)$.

4 Examples of groups with $\mathrm{cs}^*(G) = \{2, 4, 6\}$

In this section, we consider groups of the form $3.A$, where A is nilpotent. In particular, we assume that $G = AB$ satisfies

(i) $|A|$ is a power of 2,

(ii) $C_2 \cong A'$,

(iii) $C_3 \cong B \trianglelefteq G$,

(iv) $\mathrm{Z}(A) < C_A(B) < A$.

Remark 7. We used MAGMA [5] to find many groups G, with no (non-trivial) abelian direct factors, satisfying (i)–(iv). Our MAGMA program found that there are 170 such groups whose order divides $2^8 \cdot 3$.

Lemma 8. *If* $G = AB$ *satisfies* ((i))–((iv)) *above, then* $\mathrm{cs}^*(G) = \{2, 4, 6\}$.

Proof. Each element of G can be written uniquely as ab, where $a \in A$ and $b \in B$. Fix a and b, and consider the conjugacy class $(ab)^G = \{(ab)^{a'b'} \mid a' \in A, b' \in B\}$,

$$(ab)^{a'b'} = a^{a'b'} b^{a'b'} = a[a, a'b'] b^{a'b'} = a[a, b'][a, a']^{b'} b^{a'b'}.$$

As A' is normal in the 2-group A and $|A'| = 2$, we have $A' \leqslant \mathrm{Z}(A)$. Further, as $C_A(B) < A$ and $B \cong C_3$, $[A, B] = B$. Also, $[a, a'] \in A' \leqslant \mathrm{Z}(A) \leqslant C_A(B)$, so this expression can be simplified as follows:

$$(ab)^{a'b'} = a[a, b'][a, a'] b^{a'} = a[a, a'][a, b'] b^{a'},$$
$$\text{where} \quad a[a, a'] \in A, [a, b'] b^{a'} \in B.$$

Suppose that $a' \in A$ and $b' \in B$ vary. Then we have

$$[a, A] = \begin{cases} \{1\} & \text{if } a \in \mathrm{Z}(A), \\ A' & \text{otherwise,} \end{cases} \qquad [a, B] = \begin{cases} \{1\} & \text{if } a \in C_A(B), \\ B & \text{otherwise,} \end{cases}$$

$$b^A = \begin{cases} \{1\} & \text{if } b = 1, \\ \{b, b^2\} & \text{otherwise.} \end{cases}$$

The cardinalities of $[a, A]$, $[a, B]$ and b^A are $1, 2$ or $1, 3$ or $1, 2$. This shows that the size of a conjugacy class lies in $\{1, 2, 3, 4, 6, 12\}$. Since $\{[a, b']b^{a'} \mid b' \in B, a' \in A\}$ equals B when $a \notin C_A(B)$, there are no classes of size 12. Observe that $[a, B] = B$ precisely when $a \notin C_A(B)$, and in this case, $a \notin \mathrm{Z}(A)$, so $[a, A] = A'$. This shows that a class size of 3 is also not possible. Thus $\mathrm{cs}(G) \subseteq \{1, 2, 4, 6\}$

Conversely, we show that class sizes 2, 4, 6 do arise. Let $B = \langle w\rangle$. Now A acts non-trivially on B since $C_A(B) < A$. Thus $|w^G| = 2$. Choose $a \in A \setminus C_A(B)$. Then $|[a, B]| = 3$. As $a \notin \mathrm{Z}(A)$, we see that $|[A, a]| = 2$. Thus $|a^G|$ is divisible by 6, so $|a^G| = 6$. Finally, $|(aw)^G| = 4$ for $a \in C_A(B) \setminus \mathrm{Z}(A) \neq \emptyset$. □

In Theorem 2, we prove the converse of Lemma 8, i.e., we prove that a group G satisfying $\mathrm{cs}^*(G) = \{2, 4, 6\}$ must satisfy conditions (i)–(iv) above.

5 Proof of Theorem 2

Lemma 8 gives a class of groups G with $\mathrm{cs}^*(G) = \{2, 4, 6\}$. This is the easy part of the proof of Theorem 2. In this section, we give a detailed proof that these are the only examples. The following lemma paraphrases [7, Proposition 4].

Lemma 9. *Suppose that p is a prime divisor of $|G|$ and $\mathrm{cs}^*(G) = \{n_1, \dots, n_r\}$. Then $p \nmid n_1 \cdots n_r$ if and only if a Sylow p-subgroup of G is central.*

Thus it follows from Burnside's p-complement theorem that

$$p \mid G \quad \text{and} \quad p \nmid n_1 \cdots n_r$$

implies G has a non-trivial abelian direct factor. We henceforth assume that G has no non-trivial abelian direct factor: clearly $\mathrm{cs}(G) = \mathrm{cs}(G \times A)$ for A abelian. Thus, for us, the prime divisors of $n_1 \cdots n_r$ coincide with the prime divisors of G.

Proof of Theorem 2. Let G be a finite group with $\mathrm{cs}^*(G) = \{2, 4, 6\}$ and no abelian direct factors. By the preceding argument, G is a $\{2, 3\}$-group. Since $3 \notin \mathrm{cs}(G)$, it follows that G is not nilpotent, so $F(G) < G$.

A result of Gaschütz [11, Satz III.4.5] says that $F(G)/\Phi(G)$ is a direct product of abelian minimal normal subgroups of $G/\Phi(G)$. Hence the group $\overline{G} := G/\Phi(G)$ may be written as $(P \times Q) \rtimes R$, where $F = F(G)/\Phi(G)$ has Sylow 2-subgroup P, Sylow 3-subgroup Q, and both are elementary abelian and $F = P \times Q$. Now $\overline{G}/F$ acts faithfully on F as $F(G)/\Phi(G) = F$, $C_{\overline{G}}(F) \leqslant F$ by [11, III Satz 4.2]. Hence R acts linearly (perhaps not faithfully) and completely reducibly on both P and Q.

Our argument is similar in parts to [4, pp. 4–6], although our notation differs. Since $\overline{G} := G/\Phi(G)$, $\Phi(\overline{G})$ is trivial. We will write $\overline{G} = F \rtimes R$, where

$F = P \times Q$ are elementary abelian Sylow 2- and Sylow 3-subgroups of F. As $\overline{G}$-conjugacy class sizes are divisors of the G-conjugacy class sizes, we have $\mathrm{cs}^*(\overline{G}) \subseteq \{2, 3, 4, 6\}$.

We split the proof into two cases depending on how R acts on Q.

Case A. R acts non-trivially on Q.

Step A1. *There exists a* 2*-element* $x \in R_2 \setminus C_{R_2}(Q)$*, for* R_2 *a Sylow* 2*-subgroup of* R*, such that* $U := [Q, \langle x \rangle]$ *has order* 3 *and is inverted by* x*, and we have* $Q = C_Q(x) \times U$.

As R acts non-trivially on Q, we have that $C_R(Q)$ is a proper normal subgroup of R. To prove the existence of a suitable element x, let $C_R(Q) < L \trianglelefteq R$ such that $L/C_R(Q)$ is a minimal normal subgroup of $R/C_R(Q)$. Since R is completely reducible on Q (regarded as a vector space over $\mathbb{F}_3$), it follows that $L/C_R(Q)$ is an elementary abelian 2-group. Choose $x \in L \setminus C_R(Q)$. Replacing x by an odd power of itself, we can (and will) assume that x is a 2-element. By definition, x acts non-trivially on Q, and it lies in some Sylow 2-subgroup R_2 of R. Thus $x \in R_2 \setminus C_{R_2}(Q)$.

As x acts non-trivially on Q, we have $U = [Q, \langle x \rangle] \neq 1$ and $C_Q(x) \neq Q$. Also, $Q = C_Q(x) \times U$ since x has order coprime to 3. The $\overline{G}$-conjugacy class size of x, namely $|x^{\overline{G}}| = |\overline{G} : C_{\overline{G}}(x)|$, is divisible by $|Q : C_Q(x)| = |U| = 3^u$ for some $u \geqslant 1$. However, as $|\overline{G} : C_{\overline{G}}(x)|$ is a divisor of one of $2, 4, 6$, it follows that $|\overline{G} : C_{\overline{G}}(x)| = |Q : C_Q(x)| = |U| = 3^u = 3$. Thus U has order 3 and is inverted by x.

Step A2. *Let* x *be as in step* A1. *Then* $R/C_R(Q) = \langle x C_R(Q) \rangle \cong C_2$ *Further, there is a normal subgroup* H *of* G *containing* $\Phi(G)$ *such that* $G/H \cong \mathrm{S}_3$*, and* $\overline{H} := H/\Phi(G) = (P \times C_Q(x)).C_R(Q)$.

It follows from step A1 that x induces a linear transformation of Q with determinant -1, and the same holds for all $y \in R_2 \setminus C_{R_2}(Q)$. In particular, we have $y^2 \in C_{R_2}(Q)$ for all such y, and hence $R_2/C_{R_2}(Q)$ is an elementary abelian 2-group. Further, the product xy of two such elements must have determinant 1, and so xy must lie in $C_{R_2}(Q)$. This implies that $R_2/C_{R_2}(Q) \cong C_2$.

Now $R_2 C_R(Q)/C_R(Q) \cong R_2/C_{R_2}(Q) \cong C_2$, and hence a Sylow 2-subgroup of $R/C_R(Q)$ has order 2. Thus $L/C_R(Q) \cong C_2$ (the minimal normal subgroup in the proof of step A1) and lies in all Sylow 2-subgroups of $R/C_R(Q)$, so $L = R_2 C_R(Q)$. This holds for all minimal normal subgroups of $R/C_R(Q)$, and hence $L/C_R(Q)$ is the unique minimal normal subgroup of $R/C_R(Q)$. Since $R/C_R(Q)$ is a $\{2, 3\}$-group, it follows that $R/C_R(Q) = \langle x C_R(Q) \rangle \cong C_2$.

Since both $C_Q(x)$ and $U = [Q, \langle x \rangle]$ are invariant under $F, C_R(Q)$ and x, it follows that $C_Q(x)$ and U are normal subgroups of $\overline{G}$. Also, $C_R(Q) = C_R(U)$ is centralised by Q and R, and hence by $\overline{H} = (P \times C_Q(x)).C_R(Q) \trianglelefteq \overline{G}$. The quotient is generated by $U\overline{H}/\overline{H} \cong U$ and $x\overline{H}$, and so is nonabelian of order 6. Let H be the full preimage of $\overline{H}$. Then $G/H \cong \overline{G}/\overline{H} \cong \mathrm{S}_3$ as claimed.

Step A3. *Let* $\pi\colon G \to \mathrm{S}_3$ *be the natural projection with kernel* H *as in step* A2. *Let* $T := \{g \in G \mid \pi(g)$ *has order* $2\}$. *Then* $\mathrm{Z}(G) = C_H(T) \leqslant H$, $H/\mathrm{Z}(G)$ *is an elementary abelian* 2*-group, and* $H \neq \mathrm{Z}(G)$. *Also,* $|H : C_H(g)| = 2$ *for each* $g \in T$.

Let $a \in T$, so $Ha = \pi(a)$ has order 2 in $G/H \cong \mathrm{S}_3$. Then Ha lies in an S_3-conjugacy class of size 3, so 3 divides the class size $|a^G|$. Since $\mathrm{cs}(G) = \{2, 4, 6\}$, it follows that $|a^G| = 6$, and hence $|H : C_H(a)| = 2$. The natural map

$$H \to \prod_{a \in T} H/C_H(a)$$

which sends each $h \in H$ to the $|T|$-tuple with a-entry $C_H(a)h$ is a group homomorphism from H to an elementary abelian 2-group with kernel $C_H(T)$. In particular, $H/C_H(T)$ is an elementary abelian 2-group.

We now show that $C_H(T) \leqslant \mathrm{Z}(G)$. Let $g \in G$. We show that $C_H(T)$ centralises g. (i) If $\pi(g)$ has order 1, then $g \in H$. Thus $ga, a^{-1} \in T$ for $a \in T$, so $C_H(T)$ centralises ga and a^{-1} and hence also $gaa^{-1} = g$. (ii) If $\pi(g)$ has order 2, then $g \in T$, and by definition, g centralises $C_H(T)$. (iii) If $\pi(g)$ has order 3, then $\pi(g) = \pi(a)\pi(b)$ for two elements $\pi(a), \pi(b)$ of S_3 or order 2. Thus $g = hab$ for some $h \in H$, $\pi(ha) = \pi(a)$, and so $ha, b \in T$. Therefore $C_H(T)$ centralises ha and b and hence also centralises $hab = g$. This proves that $C_H(T) \leqslant \mathrm{Z}(G)$.

Since S_3 has trivial centre, it follows that $\mathrm{Z}(G) \leqslant H$. If $g \in \mathrm{Z}(G)$, then we just showed that $g \in H$, and since g is in $\mathrm{Z}(G)$, it must in particular centralise T, so $g \in C_H(T)$. Thus $\mathrm{Z}(G) = C_H(T)$. By the first paragraph of this argument, H does not centralise the element a, and so $H \neq \mathrm{Z}(G)$.

Step A4. *Let* A *be a Sylow* 2*-subgroup of* G, *and let* B *be a Sylow* 3*-subgroup of* G. *Then* B *is abelian and normal in* G. *Moreover,* $\mathrm{Z}(G) = (A \cap \mathrm{Z}(G)) \times (B \cap H)$, *and* $F(G) = (A \cap H) \times B$ *has index* 2 *in* G. *Also,* A *is nonabelian and* $A' \cong C_2$.

By step A3, H is an extension of an abelian subgroup $\mathrm{Z}(G)$ by an abelian group $H/\mathrm{Z}(G)$, and hence H is nilpotent, so $H \leqslant F(G)$. Then, since $G/H \cong \mathrm{S}_3$ is not nilpotent, $F(G)$ has index 6 or 2 in G. That is, $F(G)$ equals H or N, where N is the normal subgroup of G satisfying $F(G) \leqslant N$ and $|G : N| = 2$. By step A3, the Sylow 3-subgroup H_3 of H lies in $\mathrm{Z}(G)$. If $F(G) = H$, then $\overline{F(G)} = \overline{H}$ has Sylow 3-subgroup $Q = \overline{H_3} \leqslant \overline{\mathrm{Z}(G)} \leqslant \mathrm{Z}(\overline{G})$. This contradicts step A1. Hence $F(G) = N$, and the Sylow 3-subgroup B of G lies in $F(G)$. Since $B \leqslant N$ and $N = F(G)$, it follows that B is the unique Sylow 3-subgroup of G, and B is normal in G. Moreover, $B \cap H$ has index 3 in B, and by step A3, $B \cap H \leqslant \mathrm{Z}(G)$. Thus B is an extension of a central subgroup $B \cap H$ by a cyclic group, and hence B is abelian.

Recall that A is a Sylow 2-subgroup of G. We have $F(G) = (A \cap H) \times B$ with $A \cap H$ of index 2 in A. Hence

$$H = (A \cap H) \times (B \cap H),$$

and since $B \cap H \leqslant \mathrm{Z}(G) < H$, we have $\mathrm{Z}(G) = (A \cap \mathrm{Z}(G)) \times (B \cap H)$. It was shown in the proof of step A3 that each $a \in A \setminus (A \cap H)$ has $|H : C_H(a)| = 2$. Thus we have $a \notin \mathrm{Z}(A)$, and so A is nonabelian and $\mathrm{Z}(A) \leqslant A \cap H$. Now each $a \in A \setminus (A \cap H)$ lies in the set T of step A3. Since $H = (A \cap H) \times (B \cap H)$ and $B \cap H$ is central, it follows that $C_{A\cap H}(a)$ has index 2 in $A \cap H$. Hence $A' \cong C_2$ by [4, Lemma 1.1].

Step A5. *Using the notation of step* A4, $G = AB$, *where* A *is a* 2-*group,* $B \trianglelefteq G$ *has order* 3, $|A'| = 2$ *and* $\mathrm{Z}(A) < C_A(B) < A$.

First we observe that, for $a, g \in G$, $a^g = a[a, g]$, and hence the conjugacy class a^G equals $a[a, G]$, so $|a^G| = |[a, G]| \leqslant 6$.

By step A4, $B \trianglelefteq G$, B is abelian and $B \cap H \leqslant \mathrm{Z}(G)$. We show that B is cyclic. Suppose to the contrary that B has rank $s > 1$. By the theory of $\mathbb{Z}$-modules, there exist decompositions $B = C_{n_1} \times C_{n_2} \times \cdots \times C_{n_s}$, $B \cap H = C_{n_1/3} \times M$, where $M = C_{n_2} \times \cdots \times C_{n_s} \neq 1$. Then each element $h \in B$ can be written uniquely as $h_1^k m$, where $C_{n_1} = \langle h_1 \rangle$ and $m \in M \leqslant \mathrm{Z}(G)$. Choose $g \in G \setminus F(G)$. Since $B \trianglelefteq G$, the image $(h_1)^g \in B$, and hence $(h_1)^g = h_1^k m$ for some (unique) non-negative $k < |h_1|$ and $m \in M$. If $m = 1$, then, as $G = \langle F(G), g \rangle$ and $F(G)$ centralises B (by step A4), it follows that $\langle h_1 \rangle \trianglelefteq G$, and hence $G = (A\langle h_1 \rangle) \times M$ has a non-trivial abelian direct factor. This is a contradiction. Hence $m \neq 1$. Now $g^2 \in F(G)$ (since $|G : F(G)| = 2$), and since B is abelian and $M \leqslant \mathrm{Z}(G)$, we have

$$h_1 = (h_1)^{g^2} = (h_1^k m)^g = (h_1^g)^k m^g = (h_1^k m)^k m = h_1^{k^2} m^{k+1}.$$

Thus $k^2 \equiv 1 \pmod{n_1}$ and $m^{k+1} = 1$. Since m is a non-trivial 3-element, it follows that 3 divides $k + 1$, and therefore 3 does not divide $k - 1$. However, $n_1 \geqslant 3$ is a power of 3 that divides $k^2 - 1$, and hence n_1 divides $k + 1$. Since $0 \leqslant k < n_1$, this implies that $k = n_1 - 1$ and $(h_1)^g = h_1^{-1} m$ with $m^{n_1} = 1$. Thus we have $[h_1, g] = h_1^{-1} h_1^g = h_1^{-2} m$, and similarly, for each ℓ,

$$[h_1^\ell, g] = h_1^{-\ell} (h_1^\ell)^g = h_1^{-\ell} (h_1^g)^\ell = h_1^{-\ell} (h_1^{-1} m)^\ell = h_1^{-2\ell} m^\ell,$$

and since $|h_1| = n_1$ is coprime to 2, it follows that $|[\langle h_1 \rangle, g]| \geqslant n_1$. However, as we observed above, $|g^G| = |[G, g]| \geqslant |[\langle h_1 \rangle, g]| \geqslant n_1$, and since $|g^G| \leqslant 6$ and n_1 is a power of 3, we conclude that $n_1 = 3$. Also, since $m^{n_1} = 1$, we have $|h_1| = |m| = 3$ and $(h_1)^g = h_1^2 m$. Now the set $\{h_1, h_1^2 m\}$ is invariant under g and is centralised by $F(G)$, and so is G-invariant. Hence $B_0 := \langle h_1, m \rangle \cong C_3 \times C_3$ is normal in G. Now B_0 has exactly four subgroups of order 3, and the two subgroups $\langle m\rangle, \langle h_1 m\rangle$ are G-invariant (recall that $m \in \mathrm{Z}(G)$). Therefore we may replace C_{n_1} by $\langle h_1 m\rangle$ in the decomposition for B, and since $(h_1 m)^g = h_1^2 m^2 = (h_1 m)^2$, we obtain $G = (A\langle h_1 m\rangle) \times M$ with a non-trivial abelian direct factor, which is a contradiction. Thus we have proved that B has one generator, that is, B is cyclic, say $B = \langle b\rangle$.

We now prove $|B| = 3$. Recall that $G = AB$, where $B \trianglelefteq G$ is a cyclic 3-subgroup and A is a Sylow 2-subgroup with $|A'| = 2$ by step A4. By step A3, there exists $a \in A \cap H$ such that a inverts bH, and since $B \trianglelefteq G$, this means $b^a = b^k \neq b$. Since $a^2 \in A \cap F(G) = A \cap H$ centralises B, $k^2 \equiv 1 \bmod |B|$. Since $\mathrm{Aut}(B)$ is cyclic of order $2|B|/3$, it has a unique involution, whence $k \equiv -1 \bmod |B|$. Thus $[b,a] = b^{-1}b^a = b^{k-1} = b^{-2}$. Arguing as in the previous paragraph, we have $6 \geqslant |a^G| = |[G,a]| \geqslant |[B,a]| \geqslant |B|$, and hence $|B| = 3$ as desired.

Finally, we show that $\mathrm{Z}(A) < C_A(B)$. If $\mathrm{Z}(A) = C_A(B)$, then it follows from the proof of Lemma 8 that G has no conjugacy classes of size 4, a contradiction. (Using the notation of Lemma 8, if $|(ab)^G| = 4$, then we have $|[a,B]| = 1$, so $a \in C_B(A) = \mathrm{Z}(A)$, and hence $|[a,A]| = 1$, so $|(ab)^G| \leqslant 2$.)

This completes the proof of step A4, and hence shows that G has the required properties of Theorem 2. This completes the proof of case A.

Case B. R acts trivially on Q.

Since G is not nilpotent, R acts non-trivially on P. As R acts completely reducibly on P, it acts non-trivially on some irreducible subspace V of P.

Step B1. *Let V be an irreducible subspace of P on which R acts non-trivially. Then $|V| = 4$ and $R/C_R(V) \cong C_3$.*

We show first that $|V| = 4$. As $|P|$ is a power of 2, some R-orbit on non-zero elements of V has odd size greater than 1. However, $\mathrm{cs}(G) = \{2,4,6\}$ implies that this orbit has size 3, say $\{a,b,c\}$. Using multiplicative notation, the product abc is then fixed by R, and hence $abc = 1$. By minimality, $V = \langle a,b,c\rangle = \langle a,b\rangle$, and hence $|V| = 4$. Now $R/C_R(V) \leqslant \mathrm{Aut}(V) = \mathrm{GL}_2(2) \cong \mathrm{S}_3$, and since R is irreducible on V, $R/C_R(V)$ equals C_3 or S_3.

We will show $R/C_R(V) = C_3$. Suppose not. Then $R/C_R(V) = \mathrm{S}_3$. Let U be an R-invariant complement to V in P, so $P = U \times V$ by complete reducibility and $U \trianglelefteq \overline{G}$. Observe that $F = P \times Q$, and so

$$\begin{aligned} FC_R(V)/((U \times Q)C_R(V)) &\cong F/(U \times Q) \cong (P \times Q)/(U \times Q) \\ &\cong P/U \cong V \end{aligned}$$

is normal in $\overline{G}/((U \times Q)C_R(V))$. The quotient is isomorphic to

$$\overline{G}/FC_R(V) \cong R/C_R(V) \cong \mathrm{S}_3.$$

Moreover, we have $\overline{G}/((U \times Q)C_R(V)) \cong V \rtimes \mathrm{S}_3 \cong \mathrm{S}_4$. However, the 3-cycles of S_4 form a conjugacy class of size 8, and this conjugacy class size must divide some G-conjugacy class size. This is a contradiction since $\mathrm{cs}(G) = \{2, 4, 6\}$. Hence $R/C_R(V) \cong C_3$ as claimed.

Step B2. *Suppose that V is as in step* B1. *Then $R \cong C_3$, $F = \mathrm{Z}(\overline{G}) \times V$ and $\overline{G}/\mathrm{Z}(\overline{G}) \cong V \rtimes R \cong A_4$.*

Recall that R centralises Q. By step B1, $R/C_R(V) \cong C_3$ for each non-central minimal normal subgroup V of F. Since R is faithful on F, it follows that R is an elementary abelian 3-group. Let $1 \neq x \in R$. Then $C_{\overline{G}}(x)$ contains R and Q, and so

$$|\overline{G} : C_{\overline{G}}(x)| = |\overline{G} : RC_F(x)| = |F : C_F(x)| = |P : C_P(x)|$$

which is a power of 2. Since $x \neq 1$ and R is faithful on P, x acts non-trivially on some minimal normal subgroup V of P. Using the multiplicative notation of step B1, we may write $V \setminus \{1\}$ as $\{a, b, c\}$ and assume that $a^x = b$, $b^x = c$, $c^x = a$. It is straightforward to show that the elements x, x^a, x^b, x^c are pairwise distinct: for example, if $x^a = x^b$, then x centralises $ab = c \in V$, which is not the case. Hence the $\overline{G}$-class of x has size at least 4, and since the size is a 2-power, it must be 4. Thus $P = C_P(x) \times V$. Since, for any given $g \in \overline{G}$, $x^g = x^h$ for some $h \in P$, we have $C_P(x)^g = C_{P^g}(x^g) = C_P(x^h)$. Now $y \in C_P(x^h)$ if and only if $yh^{-1}xh = h^{-1}xhy$, and since h, y commute (because P is abelian), this is equivalent to $yx = xy$, that is, $y \in C_P(x)$. Thus $C_P(x^h) = C_P(x)$, and hence $C_P(x) \trianglelefteq \overline{G}$.

We now show that R acts trivially on $C_P(x)$. Suppose not. Then R acts non-trivially on $C_P(x)$, so there exists a non-central minimal normal subgroup W of $\overline{G}$ contained in $C_P(x)$. If $C_R(V) = C_R(W)$, then $\langle C_R(V), x\rangle = R$ would centralise W, which is not the case, so $C_R(V), C_R(W)$ are distinct proper subgroups of R, and hence there exists $y \in R \setminus (C_R(V) \cup C_R(W))$. This means that y acts non-trivially on both V and W, and hence $|F : C_F(y)| \geqslant |VW| = 16$, implying that the $\overline{G}$-conjugacy class size of y is at least 16, a contradiction. Hence R centralises $C_P(x)$, and since R centralises Q and acts faithfully on F, it follows that $R \cong C_3$ and $C_P(x) = C_P(R) = C_P(\overline{G})$. This implies that $C_F(\overline{G}) = \mathrm{Z}(\overline{G})$ has index 4 in F, and $F = \mathrm{Z}(\overline{G}) \times V$. Hence $\overline{G}/\mathrm{Z}(\overline{G}) \cong V \rtimes R \cong A_4$. This proves step B2.

We now define some more notation.

(1) Step B2 implies that $|G : F(G)| = 3$. Hence the unique Sylow 2-subgroup S of $F(G)$ is the unique Sylow 2-subgroup of G, and $\overline{S} = P$. Further, by step B2, G has four Sylow 3-subgroups; let T be one of them, and suppose without loss of generality that $\overline{T} = Q \times R$. Then $G = S \rtimes T$, and $T_0 := T \cap F(G)$ is the

unique Sylow 3-subgroup of $F(G)$ with $|T : T_0| = 3$. Thus $F(G) = S \times T_0$, $T_0 = C_T(S)$ and $\overline{T_0} = Q$.

(2) By step B2, $Z(\overline{G}) = U \times Q$, where $U = Z(\overline{G}) \cap P$, so $\overline{S} = P = U \times V$, and $C_F(R) = U \times Q$ (recall $F = \overline{F(G)} = P \times Q$).

(3) Let π be the composition of the natural projection $\pi_0 \colon G \to \overline{G}$ and the projection $\pi_1 \colon \overline{G} \to \overline{G}/(U \times Q)$. Let $M := \ker(\pi)$ and $B := \ker(\pi) \cap S$. Since $S \trianglelefteq G$, both M and B are normal in G. Also,

$$\begin{aligned} G/M &\cong \pi(G) = \overline{G}/(U \times Q) \cong V \rtimes R \cong A_4, \\ S/B &\cong \pi(S) = \pi_1(P) \cong V \cong (C_2)^2, \\ \pi(T) &\cong \pi_1(T)/Q \cong R \cong C_3. \end{aligned}$$

In particular, T permutes cyclically the three non-trivial elements of S/B.

(4) In fact, $T \cap \ker(\pi) = T_0$, so $M = B \times T_0 \leqslant F(G)$. We let $H := BT$, so $|G : H| = |ST : BT| = |S : B| = 4$ and $|H : M| = 3$.

Step B3. *If* $x \in H \setminus M$, *then* $C_G(x) = H$ *and* $|x^G| = 4$.

Let $x \in H \setminus M$, so $x = bt$ for unique $b \in B$, $t \in T \setminus T_0$. Suppose $y \in C_G(x)$. Thus $[y, x] = 1$ and $y = sr$ for unique $s \in S$, $r \in T$. Since $[sr, bt] = 1$, computing modulo the normal subgroup B shows that $[sr, t] \in B$. However,

$$[sr, t] = r^{-1}s^{-1}t^{-1}srt = r^{-1}[s, t]t^{-1}rt = [s, t]^r[r, t].$$

Further, $[s, t]^r \in S$ (since $S \trianglelefteq G$) and $[r, t] \in T$. Since $[sr, t] \in B \subseteq S$, it follows that $[r, t] = 1$, and hence that $[s, t]^r \in B$, which implies that $[s, t] \in B$ (since $B \trianglelefteq G$).

We claim that $s \in B$. If not, then $s \in S \setminus B$, and since $t \in T \setminus T_0$, the element t maps the non-trivial coset sB to $(sB)^t = s^tB \neq sB$, which implies that $s^{-1}s^t = [s, t] \notin B$, a contradiction. Thus $s \in B$, and hence $y = sr \in BT = H$. This means that $|x^G| = |G : C_G(x)|$ is divisible by $|G : H| = 4$, and we conclude that $|x^G| = 4$ and $H = C_G(x)$ since $\mathrm{cs}(G) = \{2, 4, 6\}$.

Step B4. *With the above notation,* $H = B \times T$ *is abelian, and* $B = C_S(T)$. *Further,* $S = [S, T] \circ B$ *is a central product, and* $B \leqslant Z(S)$.

By step B3, H centralises each element of $H \setminus M$. Let $h \in M$ and $x \in H \setminus M$. Then $xh \in H \setminus M$, so H centralises both x^{-1} and xh, and hence H also centralises $x^{-1}(xh) = h$. Thus H is abelian, and hence $H = B \times T$, with B, T abelian. Next, since T acts fixed-point freely on S/B and centralises B, it follows that $B = C_S(T)$.

Now $S = [S,T]C_S(T)$ by [14, Lemma 4.28], and since $B = C_S(T)$, we have $S = [S,T]B$. Using the three-subgroup lemma [14, Lemma 4.9], since

$$[[T,B],S] = [1,S] = 1 \quad \text{and} \quad [[B,S],T] \leqslant [B,T] = 1,$$

we conclude that $[[S,T],B] = 1$. Thus $S = [S,T] \circ B$ is a central product, and as B is abelian, this implies $B \leqslant \mathrm{Z}(S)$.

Step B5. *Set* $Z := [S,T] \cap B$. *Then* $[S,T]/Z \cong S/B \cong (C_2)^2$, $S' = [S,T]' \cong C_2$, $\mathrm{Z}(S) = B$, $\mathrm{Z}([S,T]) = Z$, *and* $\mathrm{Z}(G) = B \times T_0 = M$.

By definition, since $Z \leqslant B$, it follows from step B4 that Z centralises $[S,T]$, and since also B is abelian, we have $Z \leqslant \mathrm{Z}(S) \leqslant \mathrm{Z}([S,T])$. Also, by step B4 and (3) above,

$$[S,T]/Z = [S,T]/([S,T] \cap B) \cong ([S,T]B)/B = S/B \cong C_2^2.$$

Let $a \in [S,T] \setminus Z$ (or more generally, let $a \in S \setminus B$) and $x \in T \setminus T_0$. Then x acts fixed-point freely on $S/B \cong [S,T]/Z$, so, under the homomorphism $\pi\colon G \to A_4$ defined in (3) above, $\pi(a)$ is an involution in the fours group $\pi(S)$ of A_4, and $\pi(x)$ acts fixed-point freely on $\pi(S)$. Hence $\pi(a)$ lies in an A_4-conjugacy class of size 3, and so $|a^G|$ is divisible by 3 and hence is equal to 6 since $\mathrm{cs}(G) = \{2,4,6\}$. It follows that $C_G(a) \leqslant F(G) = S \times T_0$, and hence $C_G(a) = C_{F(G)}(a) = C_S(a) \times T_0$ with $C_S(a)$ of index 2 in S. By step B4, $B \leqslant \mathrm{Z}(S)$, and so $C_S(a) = \langle B, a\rangle$, of index 2 in S. In particular, $C_S(a)$ does not contain $[S,T]$. Thus $[S,T]$ is nonabelian, and for each $a \in [S,T] \setminus Z$, $C_{[S,T]}(a)$ has index 2 in $[S,T]$; also, if $a \in S \setminus B$, then $C_S(a)$ has index 2 in S. Applying [4, Lemma 1.1] to the nonabelian group $[S,T]$ with proper subgroup Z, and to the nonabelian group S with proper subgroup B, we conclude that $|[S,T]'| = |S'| = 2$. Thus $S' = [S,T]' \cong C_2$.

We have just shown that no element of $[S,T] \setminus Z$ is central in $[S,T]$, and hence $\mathrm{Z}([S,T]) \subseteq Z$. We proved the reverse inclusion above, and hence $\mathrm{Z}([S,T]) = Z$. An analogous argument shows that $\mathrm{Z}(S) = B$. Finally, B centralises both S and T by step B4, so $B \leqslant \mathrm{Z}(G)$. Also, $T_0 = C_T(S)$ centralises both S and T (since T is abelian by step B4), so $T_0 \leqslant \mathrm{Z}(G)$. Hence $M = B \times T_0 \leqslant \mathrm{Z}(G)$, and equality holds since $G/M \cong A_4$ has trivial centre.

Step B6. We can now eliminate case B. Since $\mathrm{cs}^*(G/\mathrm{Z}(G)) = \mathrm{cs}^*(A_4) = \{3,4\}$, it follows that any conjugacy class of G of size 2 is contained in $\mathrm{Z}(G)$. This is a contradiction as every conjugacy class in $\mathrm{Z}(G)$ has size 1. This eliminates case B and completes our rather long proof. □

Acknowledgments. We are most grateful to Rachel Camina for suggesting an improvement to Proposition 3 and to Avinoam Mann for alerting us to a number-theoretic lemma of John Thompson. We thank the referee for carefully reading our paper and suggesting improvements.

Bibliography

[1] A. Balog and C. Pomerance, The distribution of smooth numbers in arithmetic progressions, *Proc. Amer. Math. Soc.* **115** (1992), no. 1, 33–43.

[2] M. Bianchi, D. Chillag, A. G. B. Mauri, M. Herzog and C. M. Scoppola, Applications of a graph related to conjugacy classes in finite groups, *Arch. Math. (Basel)* **58** (1992), no. 2, 126–132.

[3] M. Bianchi, A. Gillio and C. Casolo, A note on conjugacy class sizes of finite groups, *Rend. Semin. Mat. Univ. Padova* **106** (2001), 255–260.

[4] M. Bianchi, A. Gillio and P. P. Pálfy, A note on finite groups in which the conjugacy class sizes form an arithmetic progression, in: *Ischia Group Theory 2010*, World Scientific, Hackensack (2012), 20–25.

[5] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), no. 3–4, 235–265,

[6] A. R. Camina and R. D. Camina, The influence of conjugacy class sizes on the structure of finite groups: A survey, *Asian-Eur. J. Math.* **4** (2011), no. 4, 559–588.

[7] D. Chillag and M. Herzog, On the length of the conjugacy classes of finite groups, *J. Algebra* **131** (1990), no. 1, 110–125.

[8] J. Cossey and T. Hawkes, Sets of p-powers as conjugacy class sizes, *Proc. Amer. Math. Soc.* **128** (2000), no. 1, 49–51.

[9] S. Dolfi and E. Jabara, The structure of finite groups of conjugate rank 2, *Bull. Lond. Math. Soc.* **41** (2009), no. 5, 916–926.

[10] B. Green and T. Tao, The primes contain arbitrarily long arithmetic progressions, *Ann. of Math. (2)* **167** (2008), no. 2, 481–547.

[11] B. Huppert, *Endliche Gruppen. I*, Grundlehren Math. Wiss. 134, Springer, Berlin, 1967.

[12] B. Huppert, Character degrees, *Rend. Circ. Mat. Palermo (2) Suppl.* **19** (1988), 113–118.

[13] B. Huppert, A characterization of $\mathrm{GL}(2,3)$ and $\mathrm{SL}(2,5)$ by the degrees of their representations, *Forum Math.* **1** (1989), no. 2, 167–183.

[14] I. M. Isaacs, *Finite Group Theory*, Grad. Stud. Math. 92, American Mathematical Society, Providence, 2008.

[15] N. Itô, On finite groups with given conjugate types. I, *Nagoya Math. J.* **6** (1953), 17–28.

[16] N. Itô, On finite groups with given conjugate types. II, *Osaka Math. J.* **7** (1970), 231–251.

[17] N. Itô, On finite groups with given conjugate types. III, *Math. Z.* **117** (1970), 267–271.

[18] L. S. Kazarin, Burnside's p^α-lemma, *Mat. Zametki* **48** (1990), no. 2, 45–48, 158; translation in *Math. Notes* **48** (1990), no. 1–2, 749–751.

[19] M. L. Lewis, An overview of graphs associated with character degrees and conjugacy class sizes in finite groups, *Rocky Mountain J. Math.* **38** (2008), no. 1, 175–211.

[20] J. G. Thompson, A special class of non-solvable groups, *Math. Z* **72** (1959/1960), 458–462.

Received March 25, 2020; revised May 11, 2020.

Author information

Mariagrazia Bianchi, Dipartimento di Matematica, Universita degli Studi di Milano,
Via Saldini 50, 20133 Milano, Italy.
E-mail: mariagrazia.bianchi@unimi.it

Stephen P. Glasby, Centre for the Mathematics of Symmetry and Computation,
University of Western Australia, 35 Stirling Highway, Perth 6009, Australia.
E-mail: stephen.glasby@uwa.edu.au

Cheryl E. Praeger, Centre for the Mathematics of Symmetry and Computation,
University of Western Australia, 35 Stirling Highway, Perth 6009, Australia.
E-mail: cheryl.praeger@uwa.edu.au