$(2,m,n)$-groups with Euler characteristic equal to $-2^a s^b$

Nick Gill

Department of Mathematics and Statistics
The Open University
Milton Keynes, MK7 6AA
United Kingdom

n.gill@open.ac.uk

Submitted: May 4, 2012; Accepted: July 22, 2013; Published: August 2, 2013

Abstract

We study those $(2,m,n)$-groups which are almost simple and for which the absolute value of the Euler characteristic is a product of two prime powers. All such groups which are not isomorphic to $PSL_2(q)$ or $PGL_2(q)$ are completely classified.

1 Introduction

Let m and n be positive integers. A $(2,m,n)$*-group* is a triple (G,g,h) where G is a group, g (resp. h) is an element of G of order m (resp. n), and G has a presentation of form

$$\langle g,h \mid g^m = h^n = (gh)^2 = \cdots = 1\rangle. \tag{1.1}$$

We will often abuse notation and simply refer to the group G as a $(2,m,n)$-group. We also exclude the degenerate situation when gh is equal to 1 (and G is cyclic).

The Euler characteristic χ of a $(2,m,n)$-group G is defined by the formula

$$\chi = |G|\left(\frac{1}{m} - \frac{1}{2} + \frac{1}{n}\right) = -|G|\frac{mn-2m-2n}{2mn}. \tag{1.2}$$

It is well known that χ is an even integer and, moreover, that $\chi \leqslant 2$.

In this paper we investigate the situation where $\chi = -2^a s^b$ for some odd prime s and positive integers a and b. We are interested in understanding the structure of the finite $(2,m,n)$-group (G,g,h) in such a situation, particularly when G is non-solvable.

This paper is a follow-up to an earlier paper [Gil]. In particular the main result of this paper was first announced there, and many of the basic ideas needed to prove our main result are first introduced there. We will, therefore, keep exposition and motivation to a minimum in this paper, and refer the reader to [Gil] for futher details.

1.1 Main result

To state our main result we need a definition: a group S is *almost simple* if it contains a finite, simple, non-abelian, normal subgroup T such that $T \leqslant S \leqslant AutT$. We call T the *socle* of S. A $(2,m,n)$-group (S,g,h) is *almost simple* if S is almost simple. Now we can state the main result of this paper.

Theorem 1.1. *Let (S,g,h) be an almost simple $(2,m,n)$-group with Euler characteristic $\chi = -2^a s^b$ for some odd prime s and integers $a, b \geqslant 1$. Let T be the unique non-trivial normal subgroup in S. Then one of the following holds:*

(a) $T = PSL_2(q)$ for some prime power $q \geqslant 5$ and either $S = T$ or $S = PGL_2(q)$ or else one of the possibilities listed in Table 1 holds.

(b) $S = T$, $T.2$ or $T.3$, where T is a finite simple group and all possibilities are listed in Table 2.

Moreover, a $(2,m,n)$-group exists in each case listed in Tables 1 and 2.

Some comments about Tables 1 and 2 are in order. Note, first, that for those entries of Table 2 where we specify only T (rather than S), there are two $(2,m,n)$-groups (S,g,h) in each case: one where $S = T$ and one where $S = T.2$.

Secondly, we note that the single degree 3 extension and the single degree 4 extension listed in the two tables are uniquely defined: up to isomorphism there is only one almost simple group $PSL_3(4).3$ and one almost simple group $PSL_2(9).(C_2 \times C_2)$; the same comment is also true for many of the degree 2 extensions listed, but not all. However, consulting [CCN+85] we find that, in all but one case, the requirement that $S = T.2$ is generated by two elements of orders m and n prescribes the group uniquely, up to isomorphism. (In particular we observe that the entry with group $PSL_2(25).2$ in Table 1 is distinct from $PGL_2(25)$.)

The non-unique case is as follows: there are three distinct groups $S = PSU_4(3).2$, all of which occur as $(2,7,10)$-groups (these are all of the almost simple degree 2 extensions of $PSU_4(3)$).

Theorem 1.1 is proved in §5. To prove Theorem 1.1 we make use of a more general (but weaker) result which is given in §4. This result gives a structure statement for finite $(2,m,n)$-groups G with Euler characteristic χ equal to $-2^a s^b$ for some odd prime s (note that, since χ is always even, this is the only possibility when χ is divisible by exactly two distinct primes).

Group	$\{m,n\}$	χ
$PSL_2(9).2 \cong S_6$	$\{5,6\}$	$-2^5 \cdot 3$
$PSL_2(9).(C_2 \times C_2)$	$\{4,10\}$	$-2^3 \cdot 3^3$
$PSL_2(25).2$	$\{6,13\}$	$-2^5 \cdot 5^3$

Table 1: Some $(2,m,n)$-groups for which $\chi = -2^a s^b$

Group	$\{m,n\}$	χ
$T = SL_3(3)$	$\{4, 13\}$	$-\lvert S:T\rvert \cdot 2^2 \cdot 3^5$
$S = SL_3(3)$	$\{13, 13\}$	$-2^3 \cdot 3^5$
$S = SL_3(5)$	$\{3, 31\}$	$-2^4 \cdot 5^5$
$S = PSL_3(4).2$	$\{5, 14\}$	$-2^{10} \cdot 3^2$
$S = PSL_3(4).2$	$\{10, 7\}$	$-2^7 \cdot 3^4$
$S = PSL_3(4).3$	$\{15, 21\}$	$-2^5 \cdot 3^6$
$S = SU_3(3).2$	$\{4, 7\}$	$-2^4 \cdot 3^4$
$T = SU_3(3)$	$\{6, 7\}$	$-\lvert S:T\rvert \cdot 2^7 \cdot 3^2$
$S = SU_3(3)$	$\{7, 7\}$	$-2^4 \cdot 3^4$
$S = SU_3(4).2$	$\{6, 13\}$	$-2^8 \cdot 5^3$
$S = PSU_3(8)$	$\{7, 19\}$	$-2^8 \cdot 3^8$
$S = G_2(3).2$	$\{13, 14\}$	$-2^{12} \cdot 3^6$
$S = Sp_6(2)$	$\{7, 10\}$	$-2^9 \cdot 3^6$
$S = PSU_4(3).2$	$\{5, 14\}$	$-2^{11} \cdot 3^6$
$S = PSU_4(3).2$	$\{10, 7\}$	$-2^8 \cdot 3^8$
$S = SL_4(2).2 = S_8$	$\{10, 7\}$	$-2^7 \cdot 3^4$
$S = S_7$	$\{10, 7\}$	$-2^4 \cdot 3^4$
$S = A_9$	$\{10, 7\}$	$-2^6 \cdot 3^6$
$T = SU_4(2)$	$\{5, 6\}$	$-\lvert S:T\rvert \cdot 2^7 \cdot 3^3$
$S = SU(4,2).2$	$\{10, 4\}$	$-2^5 \cdot 3^5$
$S = SU(4,2).2$	$\{10, 5\}$	$-2^7 \cdot 3^4$
$S = SU(4,2).2$	$\{10, 10\}$	$-2^6 \cdot 3^5$

Table 2: Some $(2,m,n)$-groups for which $\chi = -2^a s^b$

Theorem 1.1 comes close to classifying all almost simple $(2,m,n)$-groups with χ as given, however the case when $S = PSL_2(q)$ or $PGL_2(q)$ is not fully enumerated. On the other hand the general question of when $PSL_2(q)$ or $PGL_2(q)$ are $(2,m,n)$-groups has been studied in [Sah69] and a complete answer to this question can be found there. Ascertaining when these groups have Euler characteristic divisible by exactly two distinct primes reduces to some difficult number-theoretic questions; we discuss these, along with other open questions, in §6.

1.2 Connection to orientably regular maps

A *map* is a cellular embedding of a graph onto a surface $\mathcal{S}$. It is well known that a $(2,m,n)$-group (G,g,h) can be associated naturally with a map $\mathcal{M}$ in such a way that the surface $\mathcal{S}$ is orientable and the group G acts as a group of orientation-preserving automorphisms of $\mathcal{M}$. This connection is fully explained in the beautiful paper of Jones and Singerman [JS78].

In fact the association just described has an extra property, namely, that the action of G induces a regular action on the 'half-edges' of the associated map. As a consequence the associated map is called *orientably regular* in the literature. (The adjective *rotary* is also used, to mean the same thing.)

In the particular situation where G is finite the surface $\mathcal{S}$ is compact and we can calculate its Euler characteristic. To do this, one considers a CW-complex that is homeomorphic to $\mathcal{S}$ and applies the classical formula $V + E - F$. Indeed the map $\mathcal{M}$ can itself be thought of as a CW-complex and it is, by definition, homeomorphic to $\mathcal{S}$. Thus to calculate the Euler characteristic we need only count the vertices, edges and faces of $\mathcal{M}$.

To do this, we observe that the natural action of G on $\mathcal{M}$ induces a transitive action on the set of vertices (resp. edges, faces) of this complex with vertex-stabilizers (resp. edge-stabilizers, face-stabilizers), the conjugates of the cyclic group $\langle g \rangle$ (resp. $\langle gh \rangle, \langle h \rangle$). By applying the orbit-stabilizer theorem, one immediately obtains that the Euler characteristic of $\mathcal{S}$ is given by (1.2), i.e. it is equal to the quantity that we have defined to be the Euler characteristic of the $(2, m, n)$-group (G, g, h).

There is a natural extension of this group-map-association idea that has also received substantial attention in the literature, via the notion of a *reflexible* map. In this case one naturally encounters a group H of the form

$$H = \langle a, b, c \mid a^2 = b^2 = c^2 = (bc)^2 = (ac)^m = (ab)^n = \cdots = 1 \rangle \tag{1.3}$$

and the quadruple (H, a, b, c) is sometimes, unfortunately, called a $(2, m, n)$-group in the literature. This terminology is inconsistent with that adopted for this paper, and we warn the reader to beware!

1.3 Acknowledgments

I wish to thank Robert Brignall, John Britnell, Ian Short and Jozef Širáň for many useful discussions.

I owe a particular debt to Marston Conder who generously shared his mathematical and computational insight; in particular many of the computer calculations referred to in §5.14 are due to him.

Finally I have been a frequent visitor to the University of Bristol during the period of research for this paper, and I wish to acknowledge the generous support of the Bristol mathematics department.

2 Background on groups

In this section we add to the notation already esablished, and we present a number of well-known results from group theory that will be useful in the sequel.

The following notation will hold for the rest of the paper: (G, g, h) is always a finite $(2, m, n)$-group; (S, g, h) is always a finite almost simple $(2, m, n)$-group; T is always a simple group. We use χ or χ_G to denote the Euler characteristic of the group G.

For groups H, K we write $H.K$ to denote an extension of H by K; i.e. $H.K$ is a group with normal subgroup H such that $H.K/H \cong K$. In the particular situation where the extension is split we write $H \rtimes K$, i.e. we have a semi-direct product. For an integer k write H^k to mean $\underbrace{H \times \cdots \times H}_{k}$.

For an integer $n > 1$ we write C_n for the cyclic group of order n and D_n for the dihedral group of order n. We also sometimes write n when we mean C_n particularly when we are writing extensions of simple groups; so, for instance, $T.2$ is an extension of the simple group T by a cyclic group of order 2.

Let K be a group and let us consider some important normal subgroups. For primes $p_1, \dots, p_k$, write $O_{p_1,\dots,p_k}(K)$ for the largest normal subgroup of K with order equal to $p_1^{a_1} \cdots p_k^{a_k}$ for some non-negative integers $a_1, \dots, a_k$; in particular $O_2(K)$ is the largest normal 2-group in K. We write $Z(K)$ for the centre of K and we write K' for the derived subgroup of K.

Let a and b be positive integers. Write (a, b) for the greatest common divisor of a and b, and $[a, b]$ for the lowest common multiple of a and b; observe that $ab = [a, b](a, b)$. For a prime p write a_p for the largest power of p that divides a; write $a_{p'}$ for a/a_p. For fixed positive integers q and a we define a prime t to be a *primitive prime divisor for* $q^a - 1$ if t divides $q^a - 1$ but t does not divide $q^i - 1$ for any $i = 1, \dots, a - 1$. For fixed q we will write r_a to mean a primitive prime divisor for $q^a - 1$; then we can state (a version of) Zsigmondy's theorem [Zsi92]:

Theorem 2.1. *Let q be a positive integer. For all $a > 1$ there exists a primitive prime divisor r_a unless*

(a) $(a, q) = (6, 2)$*;*

(b) $a = 2$ *and* $q = 2^b - 1$ *for some positive integer* b*.*

Note that r_1 exists whenever $q > 2$; note too that, although r_2 does not always exist, still, for $q > 3$, there are always at least two primes dividing $q^2 - 1$. The following result is of similar ilk to Theorem 2.1; it is Mihăilescu's theorem [Mih04] proving the Catalan conjecture.

Theorem 2.2. *Suppose that $q = p^a$ for some prime p and positive integer a. If $q = 2^a \pm 1$ and $q \neq p$, then $q = 9$.*

If T is a finite simple group of Lie type, then we use notation consistent with [GLS98, Definition 2.2.8] or, equivalently, with [KL90, Table 5.1.A]. In particular we write $T = T_n(q)$ to mean that T has a σ-setup consisting of the simple adjoint $\overline{\mathbb{F}_q}$-algebraic group T_n (of rank n), and a Steinberg endomorphism of level q. We always take q to be a power of a prime p; in particular, for the Suzuki-Ree groups, we choose notation so that q is an integer.

In most cases this notation is enough to specify a unique simple group, however we must exclude eight groups because they are non-simple, namely

$$A_1(2), A_1(3), {}^2A_2(2), {}^2B_2(2), B_2(2), {}^2F_4(2), G_2(2) \text{ and } {}^2G_2(3).$$

Four of these excluded groups, namely $C_2(2), {}^2F_4(2), G_2(2)$ and ${}^2G_2(3)$, have simple derived subgroup; we will include these four derived subgroups in our definition of the finite simple groups of Lie type and will denote them $C_2(2)', {}^2F_4(2)', G_2(2)'$ and ${}^2G_2(3)'$ respectively.

The automorphisms of the finite simple groups of Lie type are well-understood, and are discussed in detail in [GLS98, §2.5]. In particular they come in several types, namely *inner*, *diagonal*, *field*, *graph* and *graph-field*. The definition of these types varies slightly across the literature, in particular when T is a Steinberg group; we will be careful to define automorphisms explicitly in this case.

We need two results that follow from the Lang-Steinberg theorem. For the first we suppose that $T = T_n(q)$ is an untwisted group of Lie type; then T is the fixed set of a Steinberg endomorphism of a simple algebraic group $T_n(\overline{\mathbb{F}_q})$. Suppose that ζ is a non-trivial field automorphism of T or, more generally, the product of a non-trivial field automorphism of T with a graph automorphism of T. Observe that ζ can be thought of as a restriction of an endomorphism of $T_n(\overline{\mathbb{F}_q})$; what is more this endomorphism has the particular property that it has a finite number of fixed points. With the notation just established the Lang-Steinberg theorem implies the following result:

Proposition 2.3. *Any conjugacy class of T which is stable under ζ (i.e. is stabilized set-wise) must intersect X non-trivially, where X is the centralizer in T of ζ.*

Proof. This is well known; see for instance [DM91, 3.10 and 3.12]. □

The Lang-Steinberg theorem also applies to twisted groups, however we will only need it when $T = {}^2B_2(q)$, a twisted group of Lie type and δ is a field automorphism. The situation here is very similar: we observe first that δ can be thought of as a restriction of an endormorphism of the connected algebraic group $B_2(\overline{F_q})$ (restricted first to act on $B_2(q) \cong P\Omega_5(q)$ and then restricted again to act on T) and, again, this endomorphism has a finite number of fixed points. Now the Lang-Steinberg theorem implies the following:

Proposition 2.4. *Any conjugacy class of $B_2(q)$ which is stable under δ must intersect the subfield subgroup $B_2(q_0)$ non-trivially, where $B_2(q_0)$ is the centralizer in $B_2(q)$ of δ.*

For g an element of a group K write $o(g)$ for the order of g; write g^K to mean the conjugacy class of g in K; write $\mathrm{I}rr(K)$ for the set of irreducible characters of K. The following proposition appears as an exercise in [Isa94, p. 45].

Proposition 2.5. *Let g, h, z be elements of a group K. Define the integer*

$$a_{g,h,z} = \left|\{(x,y) \in g^K \times h^K \mid xy = z\}\right|.$$

Then

$$a_{g,h,z} = \frac{|K|}{|C_K(g)| \cdot |C_K(h)|} \sum_{\chi \in \mathrm{I}rr(K)} \frac{\chi(g)\chi(h)\overline{\chi(z)}}{\chi(1)}.$$

3 Lemmas on primes

Recall that (G, g, h) is a $(2, m, n)$-group with Euler characteristic χ. In this section we recall some results from [Gil] concerning primes dividing χ.

Lemma 3.1. *[Gil, Lemma 3.1] Suppose that t is an odd prime dividing $|G|$. If $|G|_t > |[m,n]|_t$, then t divides χ_G.*

An immediate corollary is the following result which is a particular case of Lemma 3.2 in [CPŠ10].

Lemma 3.2. *Suppose that t is an odd prime divisor of $|G|$ such that a Sylow t-subgroup of G is not cyclic. Then $|G|_t > |[m,n]|_t$ and, in particular, t divides χ_G.*

Let N be a normal subgroup of G. Define m_N (resp. n_N) to be the order of gN (resp. hN) in G/N.

Lemma 3.3. *[Gil, Lemma 3.3] Let N be a normal subgroup of the $(2, m, n)$-group (G, g, h). If G/N is not cyclic then $(G/N, gN, hN)$ is a $(2, m_N, n_N)$-group.*

Lemma 3.4. *[Gil, Lemma 3.4] Let N be a normal subgroup of G. If an odd prime t satisfies $|G/N|_t > |[m_N, n_N]|_t$ then t divides χ_G.*

Finally we state the main result which we will use in §4. First some notation. Given a finite group K, let $\pi(K)$ be the set of all prime divisors of its order; let $\pi_{nc}(K) \subseteq \pi(K)$ to be the set of primes for which the corresponding Sylow-subgroups of K are non-cyclic; let $\pi_c(K) = \pi(K)\backslash\pi_{nc}(K)$. A subset $X \subset \pi(K)$ is called an *independent set* if, for all distinct $p, q \in X$ there exists no element in K of order pq. Write $t(K)$ (resp. $t_c(K)$) for the maximum size of an independent set in $\pi(K)$ (resp. $\pi_c(K)$).

Proposition 3.5. *[Gil, Proposition 3.6] Let (G, g, h) be a finite $(2, m, n)$-group. Let N be a normal subgroup of G with non-cyclic Sylow 2-subgroups. Then the number of primes dividing $\frac{|G|}{[m,n]}$ is at least*

$$\max\{0, t_c(N) - 2\} + |\pi_{nc}(N)|.$$

The number of primes dividing $\frac{|G|}{[m,n]}$ is also at least $t(N) - 2$.

Note that Lemma 3.1 implies that if a prime divides $\frac{|G|}{[m,n]}$ then it divides χ_G.

4 Groups with $\chi = -2^a s^b$

In this section we consider those $(2, m, n)$-groups (G, g, h) such that χ_G is divisible by exactly two distinct primes. The first two results reduce the question to studying almost simple groups satisfying a particular property.

Proposition 4.1. *Let G be a non-solvable finite $(2,m,n)$-group with Euler characteristic χ divisible by exactly two primes, 2 and s. Write $\overline{G} = G/O_{2,s}(G)$.*

Then $\overline{G}$ has a normal subgroup isomorphic to $M \times T_1 \times \cdots T_k$ where M is solvable with a cyclic Fitting subgroup of odd order, k is a positive integer, $T_1, \dots, T_k$ are simple groups such that, for all $i \neq j$, $(|T_i|, |T_j|) = 2^a s^b$ for some non-negative integers a, b, and $\overline{G}/(M \times T_1 \dots T_k)$ is isomorphic to a subgroup of $\mathrm{Out}(T_1 \times \cdots \times T_k)$.

Proof. The proof is entirely analogous to that of [Gil, Proposition 4.1] using in addition the fact that $O_{2,s}(G)$ is solvable (a consequence of Burnside's $p^a q^b$-theorem). □

Corollary 4.2. *For $i = 1, \dots, k$, there exists an almost simple group S_i with socle T_i such that S_i is a $(2, m_i, n_i)$-group and $\frac{|S_i|}{[m_i,n_i]} = 2^a s^b$ for some non-negative integers a and b.*

Proof. Note that, since $(|T_i|, T_j|) = 2^a s^b$ for distinct i and j, we have $T_i \ncong T_j$ for distinct i and j. Thus $T_i \trianglelefteq \overline{G}$ for all $i = 1, \dots, k$ and so $C_{\overline{G}}(T_i) \trianglelefteq \overline{G}$ for all $i = 1, \dots, k$. Moreover, for $i = 1, \dots, k$, $\overline{G}/C_{\overline{G}}(T_i)$ is isomorphic to S_i, an almost simple group with socle T_i.

Now Lemma 3.3 implies that there exist integers m_i and n_i such that the group S_i is an almost simple $(2, m_i, n_i)$-group. Furthermore Lemma 3.4 implies that $\frac{|S_i|}{[m_i,n_i]} = 2^a s^b$ for some non-negative integers a and b. □

Our remaining task is to study those almost simple groups $(2,m,n)$-groups S such that $\frac{|S|}{[m,n]} = \pm 2^a s^b$ for some non-negative integers a and b. The next two results give all possibilities.

Lemma 4.3. *Let S be a finite almost simple group with socle $T = T_n(q)$ is simple of Lie type of rank n. Suppose S is a $(2,m,n)$-group such that $\frac{|S|}{[m,n]} = 2^a s^b$ for some non-negative integers a and b. We list the possible isomorphism classes for T, along with restrictions on s.*

T	*Restrictions on s*
$A_n(q) \cong PSL_{n+1}(q), n = 1, 2$	
${}^2A_2(q) \cong PSU_3(q)$	
${}^2B_2(2^{2x+1}), x \in \mathbb{Z}^+$	$s \neq 3$
$A_3(2) \cong SL_4(2), A_3(3) \cong PSL_4(3)$	$s = 3$
${}^2A_3(2) \cong SU_4(2), {}^2A_3(3) \cong PSU_4(3), {}^2A_4(2) \cong SU_5(2)$	$s = 3$
$C_3(2) \cong Sp_6(2)$	$s = 3$
$G_2(3)$	$s = 3$

Proof. Proposition 3.5 implies that

$$\max\{0, t_c(T) - 2\} + |\pi_{nc}(T)| \leqslant 2. \tag{4.1}$$

Now [Gil, Proposition 3.7] gives a list of simple groups of Lie type satisfying (4.1); these are the possibilities that we must consider. In addition to the groups listed above we must rule out

$$A_4(2), B_3(3), C_2(q)', C_3(3), C_4(2), D_4(2), {}^2D_4(2), F_4(2). \tag{4.2}$$

Assume, then, that T is congruent to one of the groups listed in (4.2). In what follows we make frequent use of [KL90, Proposition 2.9.1 and Theorem 5.1.1] in which all isomorphisms between low rank groups of Lie type are listed.

We attend to the infinite family in (4.2) first (note that we write $C_2(q)'$ for the derived subgroup of $C_2(q)$ to take into account the fact that $C_2(q) \cong Sp_4(2)$ is not simple). If $T = C_2(q)'$, then T has non-cyclic Sylow t-subgroups for $t = p, t_1, t_2$ (where t_1, t_2 are distinct primes dividing $q^2 - 1$); thus Lemma 3.2 implies that we can rule out this situation whenever t_1 and t_2 exist, i.e. whenever $q > 3$. If $T = C_2(3)$ then $T \cong {}^2A_3(3)$ and is already listed; if $T = C_2(2)$ then $T \cong A_1(9) \cong PSL_2(9)$ which is already listed.

To rule out the remaining groups in (4.2) we present the following table. For each group T we list a set of primes which lie in $\pi_{nc}(T)$ and an independence set in $\pi(T)$; our sources are [CCN+85, VV05]. In every case we obtain a contradiction with Proposition 3.5.

T	Primes in $\pi_{nc}(T)$	An independence set in $\pi(T)$
$A_4(2)$	2,3	5,7,31
$B_3(3)$	2,3	5,7,13
$C_3(3)$	2,3	5,7,13
$C_4(2)$	2,3,5	
$D_4(2)$	2,3,5	
${}^2D_4(2)$	2,3	5,7,17
$F_4(2)$	2	5,7,13,17

We must now prove the listed restrictions on s. That $s \neq 3$ for $T = {}^2B_2(2^{2x+1})$ follows from the fact that s does not divide $|T|$ and that ${}^2B_2(2^{2x+1})$ is not listed in [Gil, Proposition 4.3]. That $s = 3$ for the last four lines follows from the fact that Sylow 3-subgroups are non-cyclic in every case. □

Lemma 4.4. *Let S be a finite almost simple group with socle T where T is not a finite simple group of Lie type. Suppose S is a $(2, m, n)$-group such that $\frac{|S|}{[m,n]} = 2^a s^b$ for some non-negative integers a and b. Then T is isomorphic to one of the following:*

(a) the alternating groups A_n for $n = 7, 9$ (and $s = 3$);

(b) the sporadic groups M_{11} and M_{12} (and $s = 3$).

Proof. If $n \geqslant 10$ then the Sylow t-subgroups of A_n are non-cyclic for $t = 2, 3$ and 5. Then Lemma 3.2 yields a contradiction. We conclude that, if $T \cong A_n$ is alternating, then $n \leqslant 9$. Now, by [KL90, Proposition 2.9.1], A_5, A_6 and A_8 are all isomorphic to finite simple groups of Lie type; this leaves $n = 7$ and 9.

We examine [VV05, Table 2] and rule out all sporadic simple groups T for which $\pi(T)$ contains an independent set of size 4 with all primes odd. This leaves the groups $M_{11}, M_{12}, J_2, J_3, He, McL, HN$ and HiS. Of these, all but M_{11}, M_{12} and J_3 have non-cyclic Sylow t-subgroups for $t = 2, 3, 5$. Furthermore J_3 has non-cyclic Sylow t-subgroups for $t = 2$ and 3, and also has an independence set $\{5, 17, 19\}$. This leaves M_{11} and M_{12} as listed. □

The results of this section give necessary conditions for a group G to be a $(2,m,n)$-group such that χ_G is divisible by exactly two distinct primes. We can strengthen these results with some simple observations.

First of all, under the assumptions of Lemma 4.3, if $T = PSL_3(q)$ for some odd prime q, then Lemma 3.1 implies that $q = 2^a - 1$ for some integer $a \geqslant 2$; similarly $q = 2^a + 1$ when $T = PSU_3(q)$ with q odd. Using Mihăilescu's theorem (Theorem 2.2) one can also give conditions on even q for both $T = PSL_3(q)$ and $T = PSU_3(q)$.

Secondly, we observe that all of the groups listed in Lemmas 4.3 and 4.4 have order divisible by 2,3 and 5, except for $G_2(3)$ and, possibly, $A_1(q)$, $A_2(q), {}^2A_2(q)$, and ${}^2B_2(q)$. This gives strong conditions on the groups $T_1, \dots, T_k$ in Proposition 4.1 since $(|T_i|, T_j|) = 2^a s^b$ for all $i \neq j$.

5 χ is almost simple and χ is a product of two primes

In this section we assume the following: S is a finite almost simple group with socle T; furthermore (S,g,h) is a $(2,m,n)$-group with corresponding Euler characteristic χ such that $\chi = -2^a s^b$ for some prime s and positive integers a and b. We write $\Lambda = \{m,n\}$.

Now Lemma 3.1 implies that $\frac{|S|}{[m,n]}$ is divisible by at most two primes. Thus the possible isomorphism classes of T are listed in Lemmas 4.3 and 4.4.

Our job in this sectioN is to prove Theorem 1.1. The proof proceeds in the following way: in Sections 5.1 to 5.13 we go through the different possible isomorphism classes for an almost simple group S that are compatible with Lemmas 4.3 and 4.4; in each case we produce a finite list of triples (S,m,n) such that S may possibly occur as a $(2,m,n)$-group (S,g,h) for some $g,h \in S$. Then, in §5.14, we go through each of the listed possibilities and establish which really occur, i.e. when there are elements $g,h \in S$ such that (S,g,h) is a $(2,m,n)$-group.

5.1 $T = PSL_2(q)$

In this situation we need only deal with the situation when $S \neq PSL_2(q)$ or $PGL_2(q)$. We introduce some notation: $q = p^{a_0}$ for some prime p; T' is a group isomorphic to either $PSL_2(q)$ or $PGL_2(q)$ (these coincide with T when q is even); δ is a field automorphism of T (hence also of T') of order $a_1 > 1$; we write $S' = \langle T', \delta \rangle = T' \rtimes \langle \delta \rangle$. We choose T' and δ so that S is a subgroup of S' of index at most 2; if S contains $PGL_2(q)$ or δ then we can choose T' and δ so that $S = S'$, otherwise $S = \langle T, \delta\epsilon \rangle$ where ϵ is a diagonal automorphism of T, and $|S : T| = a_1$.

Observe that $\chi = -2^a p^b$, since the Sylow p-subgroups of T' are non-cyclic whenever T' admits a non-trivial field automorphism. Let x be the order of an element of T'; then x divides at least one of $q-1, p, q+1$. Let u be an element of S' such that uT' generates S'/T'; in semi-direct product notation $u = (t, \delta)$ for some $t \in T'$. The Lang-Steinberg theorem (Proposition 2.3) implies that u has order dividing one of $a_1(q_1-1), a_1 p, a_1(q_1+1)$ where $q = q_1^{a_1}$.

Suppose that $\Lambda = \{\lambda_1, \lambda_2\}$; then we may assume that λ_1 divides one of the orders $a_1(q_1-1), a_1p, a_1(q_1+1)$ where a_1 divides a_0 and q_1 is such that $q = q_1^{a_1}$; similarly λ_2 divides either $a_2(q_2-1), a_2p$ or $a_2(q_2+1)$ for some $a_2|a$ and q_2 is such that $q_2^{a_2} = q$. We assume, without loss of generality, that $a_1 \geqslant a_2$.

In what follows, for an integer k we write $r_{p,k}$ for a primitive prime divisor of $p^k - 1$ (i.e. it is primitive with respect to the prime p rather than with respect to q, as we have written elsewhere).

Lemma 5.1. *$a_1 = 2$.*

Proof. Suppose that $a_1 > 2$. Then the condition $(gh)^2 = 1$ (which implies that $(ghT')^2 = 1 \in S'/T'$) implies that $a_2 > 1$. Consider the primes r_{p,a_0} and $r_{p,2a_0}$; since $a \geqslant a_1 > 2$, Theorem 2.1 implies that at least one of these exist. Observe furthermore that neither r_{p,a_0} nor $r_{p,2a_0}$ divide $(q_1-1)(q_1+1)(q_2-1)(q_2+1)$. Furthermore, by Fermat's little theorem, $a_i|p^{a_i-1}-1$ for $i = 1, 2$ and we conclude that neither r_{p,a_0} nor $r_{p,2a_0}$ divide

$$a_1a_2(q_1-1)(q_1+1)(q_2-1)(q_2+1).$$

But Lemma 3.1 implies that r_{p,a_0} and $r_{p,2a_0}$ must divide $\lambda_1\lambda_2$ and we have a contradiction. □

Lemma 5.2. *If p is odd then one of the following holds:*

(a) $S = PSL_2(25).2$, $\Lambda = \{6, 13\}$, $\chi = -2^5 \cdot 5^3$;

(b) $S = PSL_2(9).2$, $\Lambda = \{4, 5\}$, $\chi = -2^2 \cdot 3^2$;

(c) $S = PSL_2(9).2$, $\Lambda = \{5, 6\}$, $\chi = -2^4 \cdot 3^2$;

(d) $S = PSL_2(9).(C_2 \times C_2)$, $\Lambda = \{4, 10\}$, $\chi = -2^3 \cdot 3^3$;

In all cases the group S is distinct from $PSL_2(q)$ and $PGL_2(q)$.

Proof. Recall that $q = q_1^{a_1} = q_1^2$. Assume first that $q > 25$, and we show a contradiction. Since $a_1 = 2$ we know that λ_1 divides one of $2(\sqrt{q}+1)$, $2(\sqrt{q}-1)$, $2p$. If $a_2 = 2$ then the same can be said of λ_2. But now write $a = 2b$ and observe that $r_{p,4b}$ divides $q+1$; then if $a_2 = 2$ this implies that $r_{p,4b}$ does not divide $\lambda_1\lambda_2$ which is a contradiction. We conclude that $a_2 = 1$ and, moreover, λ_2 divides $q+1$ and is divisible by $r_{p,4b}$.

Now if λ_1 divides $2p$ then we conclude that $|q-1|_{2'}$ does not divide $\lambda_1\lambda_2$. Since $a_0 \geqslant 2$, Theorem 2.2 implies that $|q-1|_{2'}$ is non-trivial; hence we have a contradiction with Lemma 3.1.

Suppose next that λ_1 divides $2(\sqrt{q} \pm 1)$; then we conclude that $|\sqrt{q} \mp 1|_{2'}$ does not divide $\lambda_1\lambda_2$ and we deduce that $|\sqrt{q} \mp 1|_{2'}$ is trivial, i.e. $\sqrt{q} \mp 1 = 2^x$ for some positive integer x; if $\sqrt{q} > 3$, then this implies in particular that $\frac{\sqrt{q}\pm1}{2}$ is odd. Note too that $\frac{q+1}{2}$ is odd and so, since $(\frac{\sqrt{q}\pm1}{2}, \frac{q+1}{2}) = 1$, Lemma 3.1 implies that $\lambda_1 \in \{\frac{\sqrt{q}\pm1}{2}, \sqrt{q}\pm1, 2(\sqrt{q}\pm1)\}$ and $\lambda_2 \in \{\frac{q+1}{2}, q+1\}$. There are, therefore, twelve possibilities for (λ_1, λ_2); in the following table we list them along with a polynomial f which divides χ and which, since $\sqrt{q} > 5$, is divisible by a prime other than 2 and p; note that we write y for $\sqrt{q}$.

λ_1	λ_2	f
$\frac{y+1}{2}$	$\frac{y^2+1}{2}$	y^3-3y^2-3y-7
$\frac{y-1}{2}$	$\frac{y^2+1}{2}$	y^3-5y^2-3y-1
$y+1$	$\frac{y^2+1}{2}$	y^3-y^2-3y-5
$y-1$	$\frac{y^2+1}{2}$	y^3-3y^2-3y+3
$2(y+1)$	$\frac{y^2+1}{2}$	y^3-3y+4
$2(y-1)$	$\frac{y^2+1}{2}$	y^3-2y^2-3y+2
$\frac{y+1}{2}$	y^2+1	y^3-3y^2-y-5
$\frac{y-1}{2}$	y^2+1	y^3-5y^2-y-3
$y+1$	y^2+1	y^3-y^2-y-3
$y-1$	y^2+1	y^3-3y^2-y-1
$2(y+1)$	y^2+1	y^3-y-2
$2(y-1)$	y^2+1	y^2-2y-1

We justify the first line of the above table, the others are similar. In this case

$$\chi = |S:T|q(q^2-1)\left(\frac{2}{\sqrt{q}+1}+\frac{2}{q+1}-\frac{1}{2}\right) = -\frac{1}{2}q(\sqrt{q}-1)(\sqrt{q}^3-3q-3\sqrt{q}-7).$$

Now observe that $(\sqrt{q}^3-3q-3\sqrt{q}-7,q)\big|7$ and $(\sqrt{q}^3-3q-3\sqrt{q}-7,\sqrt{q}-1)\big|12$; since $\sqrt{q}-1$ is a power of 2 in this case, Lemma 3.1 implies that

$$\sqrt{q}^3-3q-3\sqrt{q}-7 \leqslant 28$$

and so $\sqrt{q} \leqslant 5$ which is a contradiction, as required.

Now when $\sqrt{q}=3,5$ we consult [CCN$^+$85]. In the latter case we must have $\lambda_1 \in \{13,26\}$ and $\lambda_2 \in \{6,12\}$; checking these four combinations we find that only $\Lambda = \{6,13\}$ gives a valid value for χ. When $\sqrt{q}=3$ we must have $\lambda_1 \in \{5,10\}$ and $\lambda_2 \in \{4,6,8\}$; checking these six combinations we find that only $\Lambda \in \{\{5,4\},\{5,6\},\{10,4\}\}$ give valid values for χ. The result follows. □

Lemma 5.3. *If $p=2$ then one of the following holds:*

(a) $S=SL_2(16).2$, $\Lambda=\{6,5\}$, $\chi=-2^6\cdot 17$;

(b) $S=SL_2(16).2$, $\Lambda=\{10,3\}$, $\chi=-2^5\cdot 17$;

Proof. We assume that $q>4$ since $SL_2(4).2 \cong PGL_2(5)$. Since $a_1=2$ we know that λ_1 divides one of $2(\sqrt{q}+1)$, $2(\sqrt{q}-1)$, 4. If $a_2=2$ then the same can be said of λ_2; if $a_2=1$ then λ_2 divides one of $q-1$, $q+1$, 2.

Now, since $\sqrt{q}+1,\sqrt{q}-1,q+1$ are pairwise coprime, Lemma 3.1 implies that λ_1 is divisible by one of these, λ_2 is divisible by another, and the third is a power of a prime s (which prime, in turn, divides χ). In fact we know that $\lambda_1 \in \{2(\sqrt{q}-1),2(\sqrt{q}+1)\}$.

Suppose first that $a_2=2$. Then clearly $\{\lambda_1,\lambda_2\}=\{2(\sqrt{q}+1),2(\sqrt{q}-1)\}$. In this case $f=q-2\sqrt{q}-1$ divides χ; furthermore, for $q>4$, f is divisible by a prime other than 2 and s and this case is excluded. We conclude that $a_2 = 1$ and λ_2 divides one of $q-1$ and $q+1$, 2

Suppose that λ_2 divides $q+1$; then $\lambda_2 = q+1$. In this case there are two possibilities for λ_1. We list these possibilities in the table below, along with a polynomial f which χ and which, whenever $\sqrt{q} > 2$, is divisible by a prime other than 2 and s (thus these cases are excluded).

λ_1	λ_2	f
$2(\sqrt{q}+1)$	$q+1$	$(\sqrt{q})^3 - \sqrt{q} - 2$
$2(\sqrt{q}-1)$	$q+1$	$q - 2\sqrt{q} - 1$

We are left with the possibility that λ_2 divides $q-1$ and that $q+1$ is a power of the prime s. Since q is an even power of 2, Theorem 2.1 implies that $q+1 = s$. We assume that $q > 16$ and split into two cases.

First suppose that $\lambda_1 = 2(\sqrt{q}+1)$ and $\lambda_2 = \frac{q-1}{x}$ for some x dividing $\sqrt{q}+1$. Then

$$\chi = |S|(\frac{1}{2(\sqrt{q}+1)} + \frac{x}{q-1} - \frac{1}{2}) = -\frac{|S|}{2(q-1)}(q - \sqrt{q} - 2x).$$

Let $f = q - \sqrt{q} - 2x$; since x is odd we know that $(f, q) = 2$; we also know that $f < q+1$. We conclude that $f = 2$; but $f \geqslant q - 3\sqrt{q} - 2 > 2$ for $q > 16$, and we have a contradiction as required.

The other possibility is that $\lambda_1 = 2(\sqrt{q}-1)$ and $\lambda_2 = \frac{q-1}{x}$ for some x dividing $\sqrt{q}-1$. Then

$$\chi = |S|(\frac{1}{2(\sqrt{q}-1)} + \frac{x}{q-1} - \frac{1}{2}) = \frac{|S|}{2(q-1)}(q - \sqrt{q} - 2x - 2).$$

Let $f = q - \sqrt{q} - 2x - 2$; since x is odd we know that $(f, q) = 4$; we also know that $f < q+1$. We conclude that $f = 4$; but $f \geqslant q - 3\sqrt{q} > 4$ for $q > 16$, and we have a contradiction as required.

We are left with the case when $q = 16$ and λ_2 divides $q - 1 = 15$. Then $\lambda_1 \in \{6, 10\}$ and the only possibilities are

$$(\lambda_1, \lambda_2) \in \{(6,5), (10,3), (6,15), (10,15)\}.$$

Checking each in turn we exclude the last two cases and the result follows. □

5.2 $T = {}^2B_2(q)$

In this situation $q = 2^{2x+1}$ for some integer $x \geqslant 1$. We refer to [Suz62], in particular Proposition 1 and Theorem 9 of that paper, to conclude that any element in T whose order is not a power of 2 must have order dividing $q-1$, $q-r+1$ or $q+r+1$ where $r = 2^{x+1}$. Note, moreover, that $q-1$, $q-r+1$ and $q+r+1$ are pairwise coprime.

Recall that the outer automorphism group of T is isomorphic to the Galois group of $\mathbb{F}_q$, i.e. it consists of field automorphisms and is a group of odd order. Now write $S = \langle T, \delta \rangle$ where δ is a field automorphism of order a where a divides $2x+1$. Since a is of odd order, for S to be a $(2, m, n)$-group we must have two elements g and h such that gT and hT both have order a in S/T. We conclude that

$$\{o(g^a), o(h^a)\} \subset \{q-1, q-r+1, q+r+1\}.$$

Lemma 5.4. *$S = T$.*

Proof. Suppose that $S = \langle T, \delta\rangle \subset \langle B_2(q), \delta\rangle$ where δ is non-trivial (and we have abused notation slightly by writing δ as a field automorphism of $B_2(q)$). Write $(t, \delta) \in B_2(q) \rtimes \langle\delta\rangle$ and observe that

$$u = (t, \delta)^a = t \cdot t^{\delta} \cdot t^{\delta 2} \cdots t^{\delta^{a-1}}.$$

In particular observe that $u^{\delta} = t^{\delta} \cdots t^{\delta^{a-1}} \cdot t = t^{-1}ut$ and we obtain that u lies in a conjugacy class of $B_2(q)$ that is stable under δ. Now we apply Proposition 2.4 and conclude that u is conjugate in $B_2(q)$ to an element of $B_2(q_0)$ where $q = q_0^a$.

We apply this fact with u equal to g^a or h^a; in both cases u is of odd order and we conclude that $o(u)$ divides $a(q_0^2 - 1)(q_0^4 - 1)$. For $a \geqslant 11$ we have

$$o(u) < q - r + 1 = \min\{q-1, q-r+1, q+r+1\}$$

which is a contradiction. Thus we assume that $a \leqslant 9$.

If $a > 4$, then Theorem 2.1 implies that there is a prime dividing $q-1$ and a prime dividing q^2+1, neither of which divide $q_0^4 - 1$; what is more (since $3|2^2-1$, $5|2^4-1$ and $7|2^3-1$) both of these primes may be taken to be larger than 7. We conclude that neither of these primes divide $o(g) \cdot o(h)$ and so both must divide χ which is a contradiction.

Finally suppose that $a = 3$. Then Theorem 2.1 implies that there is a prime greater than 3 dividing q^2+1 which does not divide q_0^4-1; now $q_0^2 + q_0 + 1$ divides $q-1$ and is coprime to $q_0^4 - 1$ thus there is a prime greater than 3 dividing $q-1$ which does not divide $q_0^4 - 1$. Again we conclude that neither of these primes divide $o(g) \cdot o(h)$ and so both must divide χ which is a contradiction. □

Lemma 5.5. *If $T = {}^2B_2(q)$, then we have a contradiction.*

Proof. We know that $S = T$ and that $\Lambda \subset \{q-1, q-r+1, q+r+1\}$; we go through the possibilities in turn.

If $\Lambda = \{q-r+1, q+r+1\}$ then

$$\begin{aligned}\chi &= |S|(\frac{1}{m} + \frac{1}{n} - \frac{1}{2}) \\ &= q^2(q^2+1)(q-1)\left(\frac{1}{q-r+1} + \frac{1}{q+r+1} - \frac{1}{2}\right) \\ &= -\frac{1}{2}q^2(q-1)(q^2-4q-3).\end{aligned}$$

Now $q^2 - 4q - 3$ is odd thus we require that $(q-1)(q^2-4q-3)$ is a prime power. But $(q^2-4q-3, q-1) = 1$ and we have a contradiction.

If $\Lambda = \{q-r+1, q-1\}$ then

$$\begin{aligned}\chi &= |S|(\frac{1}{m}+\frac{1}{n}-\frac{1}{2})\\ &= q^2(q^2+1)(q-1)\left(\frac{1}{q-r+1}+\frac{1}{q-1}-\frac{1}{2}\right)\\ &= -\frac{1}{2}q^2(q+r+1)(q^2-qr-4q+3r-1).\end{aligned}$$

Now $q^2-qr-4q+3r-1$ is odd thus we require that $(q+r+1)(q^2-qr-4q+3r-1)$ is a prime power. But $(q+r+1, q^2-qr-4q+3r-1) < q+r+1$ and we have a contradiction.

If $\Lambda = \{q+r+1, q-1\}$ then

$$\begin{aligned}\chi &= |S|(\frac{1}{m}+\frac{1}{n}-\frac{1}{2})\\ &= q^2(q^2+1)(q-1)\left(\frac{1}{q+r+1}+\frac{1}{q-1}-\frac{1}{2}\right)\\ &= -\frac{1}{2}q^2(q-r+1)(q^2+qr-4q-3r-1)\end{aligned}$$

Now $(q^2+qr-4q-2r-1)$ is odd thus we require that $(q-r+1)(q^2+qr-4q-3r-1)$ is a prime power. But $(q-r+1, q^2+qr-4q-3r-1) < q-r+1$ and we have a contradiction. □

5.3 $T = PSL_3(q)$

Throughout this section, we assume that $q > 2$ (since $PSL_3(2) \cong PSL_2(7)$). Furthermore we fix γ to be an 'inner diagonal' automorphism of order $(3, q-1)$, δ to be a 'field' automorphism of order $\log_p q$ and σ to be the involutory 'graph' automorphism of T given by $t^\sigma = t^{-T}$ (the inverse transpose of t). We refer to [KL90, §2.2] to see that $\mathrm{Aut}(T) = \langle T, \gamma, \delta, \sigma\rangle$.

Lemma 5.6. *There exists $a \in \mathbb{Z}^+$ such that $q-1 = r^a$ for some prime r.*

Proof. Observe first that the Sylow t-subgroups are non-cyclic for $t = p$ and $t|q-1$. Thus, if t is a prime such that $t|p(q-1)$, then $t|\chi$ and we conclude that $q-1$ is a prime power. □

This result, along with Theorem 2.2 implies that, for $q \neq 4$, the group $SL_3(q)$ has trivial centre; thus $T = SL_3(q)$.

Corollary 5.7. *If q is odd and $q \neq 9$, then q is prime and $T \leqslant S \leqslant \langle T, \sigma\rangle$. If $q = 2^a$ for some integer a, then $q-1$ is prime; what is more, if $q \neq 4$, $T \leqslant S \leqslant \langle T, \delta, \sigma\rangle$.*

Proof. Suppose first that q is odd and $q \neq 9$. By Lemma 5.6, $q = 2^a+1$ for some $a \geqslant 1$. This implies, in particular, that $(3, q-1) = 1$ and so T admits no diagonal outer automorphisms. Now, since $q \neq 9$, Theorem 2.2 implies that $q = p$. Thus T admits no field outer automorphisms, and the result follows.

Now suppose that $q = 2^a$; then $q - 1$ is a prime power, and Theorem 2.2 implies that $q - 1$ is prime. Thus, for $q \neq 4$, T admits no diagonal automorphisms, and the result follows. □

Before we give a classification of maps we give a group-theoretic lemma:

Lemma 5.8. *Suppose $S = \langle T, \sigma\rangle$ with $q > 4$. All elements in S of order divisible by q^2+q+1 have order q^2+q+1. All elements in S of order divisible by $\frac{q+1}{(2,q+1)}$ have order dividing q^2-1. If q is even, then all elements in $S \backslash T$ of order divisible by $q+1$ have order dividing $2(q+1)$.*

Proof. Since $q > 4$ we have $T = SL_3(q)$. Recall that, for $a \in \mathbb{Z}^+$, we write r_a for a primitive prime divisor of $q^a - 1$. Since $q = 2^a$ or $2^a + 1$ we know that r_2 and r_3 exist. Let x (resp. y) be elements of these orders in T.

Observe that x is diagonalizable in $\mathbb{F}_{q^2}$ but not in $\mathbb{F}_q$; we conclude that the eigenvalues of x are equal to λ, λ^q, μ for some $\lambda, \mu \in \mathbb{F}_{q^2}$. If $\lambda = \lambda^q$ then $\lambda \in \mathbb{F}_q$ and so $\mu \in \mathbb{F}_q$ which is a contradiction. If $\lambda = \mu$ then the determinant of x is equal to λ^{q+2}; since $\lambda \in \mathbb{F}^*_{q^2}$ and the determinant of x equals 1 we conclude that $\lambda^3 = 1$. But then $r_2 = 3$ and $\lambda^q = \lambda = \mu$ which is, again, a contradiction. We conclude that all eigenvalues of x are distinct.

Similarly y is diagonalizable in $\mathbb{F}_{q^3}$ but not in $\mathbb{F}_q$; thus the eigenvalues of y are equal to ξ, ξ^2, ξ^3 for some $\xi \in \mathbb{F}_{q^3}$. If these eigenvalues are not distinct then ξ lies either in $\mathbb{F}_{q^2}$ or in $\mathbb{F}_q$ and in both cases we have a contradiction.

Thus the eigenvalues of both elements, x and y, are distinct, i.e. x and y are regular semisimple and, in paricular, both $C_T(x)$ and $C_T(y)$ are maximal tori in $PSL_3(q)$. It follows immediately that $C_T(x)$ (resp. $C_T(y)$) is cyclic of order $q^2 - 1$ (resp. of order q^2+q+1). Now Sylow arguments ensure that all cyclic groups C_{q^2-1} (resp. C_{q^2+q+1}) are conjugate to each other; furthermore $|N_T(C_{q^2+q+1}) : C_{q^2+q+1}| = 3$ and $|N_T(C_{q^2-1}) : C_{q^2-1}| = 2$.

Let us prove first that an element in S of order divisible by q^2+q+1 has order q^2+q+1; the previous paragraph implies that the statement is true for elements in T so we must consider elements in $S \backslash T$. Let $h \in T$ be an element of order q^2+q+1. Since $|S : T| = 2$ and $|N_T(C_{q^2+q+1}) : C_{q^2+q+1}| = 3$ it is sufficient to prove that there exists $g \in S \backslash T$ such that $|\langle h, g\rangle| = 2(q^2+q+1)$ and $\langle h, g\rangle$ is not cyclic.

Now we use the standard fact that h^{-T} is conjugate in $GL_3(q)$ to h^{-1}. Since h^{-1} is an element of order q^2+q+1, the argument above implies that $C_{GL_3(q)}(h^{-1})$ is a maximal torus; indeed $C_{GL_3(q)}(h^{-1} \cong C_{q^3-1}$. Now we appeal to [KL90, (4.3.13)] to conclude that $GL_1(q^3)$ intersects every coset of $SL_3(q)$ in $GL_3(q)$; in other words the conjugacy class of h^{-1} in $GL_3(q)$ does not split when we restrict to $SL_3(q)$. Thus, in particular, there exists $g_0 \in SL_3(q)$ such that $g_0 h^{-T} g_0^{-1} = h^{-1}$; consequently there exists $g (= g_0\sigma)$ in $S \backslash T$ such that $ghg^{-1} = h^{-1}$. Since $\langle g, h\rangle$ is dihedral we are done.

Next we let $f \in S$ be an element in S of order divisible by $\frac{q+1}{(q+1,2)}$ (and hence divisible by r_2); we know, by the centralizer arguments above, that if $f \in T$ then f has order dividing q^2-1. Thus assume that $f \in S\backslash T$; then $k = f^2 \in T$ and k has order divisible by $\frac{q+1}{(q+1,2)}$ and so, once again, k has order dividing q^2-1.

Clearly, then, f has order dividing $2(q^2-1)$. If q is odd, then, since $q-1=2^a$ we conclude that either $o(f)$ divides q^2-1 or else $o(f) = 2(q^2-1)$. If q is even, then, since $q-1$ is an odd prime, either $o(f)$ divides $2(q+1)$ or else $o(f) = 2(q^2-1)$. Thus in both cases to prove the result it suffices to show that S does not contain an element of order $2(q^2-1)$.

First we construct $g \in S\backslash T$ such that $\langle k, g\rangle$ is dihedral of order $2o(k)$. This time things are easier, since k lies in $K < SL_3(q)$ with $K \cong GL_2(q)$ and such that σ normalizes K and takes every element of K to its inverse transpose. As above there exists g_0 in K such that $g_0k^{-T}g_0^{-1} = k^{-1}$ and, setting $g = g_0\sigma$ we obtain $g \in S\backslash T$ such that $gkg^{-1} = k^{-1}$ and so $\langle g, k\rangle$ is dihedral.

To show that no element of order $2(q^2-1)$ exists in $S\backslash T$ we must be sure that the element k is not real, i.e. we must show that k is not conjugate to its inverse in $SL_3(q)$. Observe that the eigenvalues of k are $\{\lambda_1, \lambda_2, \lambda_3\}$ where $\lambda_1, \lambda_2 \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$ and $\lambda_3 \in \mathbb{F}_q$ has multiplicative order equal to $q-1$. Now, since $q > 3$, $\lambda_3 \neq \lambda_3^{-1}$ and thus the eigenvalues of k are not the same as the eigenvalues of k^{-1} and hence cannot be conjugate in $SL_3(q)$. The result follows. □

To make the exposition clearer from this point on, we split into odd and even characteristic cases.

Lemma 5.9. *Suppose that $T = PSL_3(q)$ and $q = 2^a+1$. Then one of the following holds:*

(a) $T = SL_3(3)$, $\Lambda = \{4, 13\}$, $\chi = -|S:T|2^2 \cdot 3^5$;

(b) $S = SL_3(3)$, $\Lambda = \{13, 13\}$, $\chi = -2^3 \cdot 3^5$;

(c) $S = SL_3(5)$, $\Lambda = \{3, 31\}$, $\chi = -2^4 \cdot 5^5$;

Proof. Suppose first that $q > 3$. The two primes dividing χ must be 2 and p, hence Λ must contain elements divisible by primitive prime divisors r_2 and r_3. (Note that, since $q > 3$, both of these exist and both are odd.) Lemma 5.8 implies that no element exists, the order of which is divisible by both r_2 and r_3 so we assume that r_3 divides λ_1. Observe that

$$(q^2+q+1, q-1) = (q^2+q+1, q) = (q^2+q+1, q+1) = 1$$

and we conclude that, in fact, q^2+q+1 must divide λ_1. Now Lemma 5.8 implies that, for $q \neq 9$, $\lambda_1 = q^2+q+1$; [CCN+85] implies that, for $q = 9$, we also have $\lambda_1 = q^2+q+1$.

Similarly we conclude that $\frac{q+1}{2}$ divides λ_2; then Lemma 5.8 implies that, for $q \neq 9$, $\lambda_2 = \frac{q^2-1}{x}$ for some $x = 2^b | 2(q-1)$; [CCN+85] implies that, for $q = 9$, we have the same.

Now we calculate χ:

$$\begin{aligned}\chi &= |S|(\frac{1}{m}+\frac{1}{n}-\frac{1}{2})\\ &= |S:T|q^3(q^2-1)(q^3-1)\left(\frac{x}{q^2-1}+\frac{1}{q^2+q+1}-\frac{1}{2}\right)\\ &= -\frac{1}{2}|S:T|q^3(q-1)\big(q^4+q^3-(2x+2)q^2-(2x+1)q-(2x-1)\big)\end{aligned}$$

Setting $f=q^4+q^3-(2x+2)q^2-(2x+1)q-(2x-1)$, observe that $f\equiv -2x+1\not\equiv 0 \mod q$ for $x<\frac{q-1}{2}$; similarly $f\equiv -6x\not\equiv 0 \mod (q-1)$ for $x<\frac{q-1}{2}$. Thus if $x\leqslant\frac{q-1}{4}$ we must have $|f|<q(q-1)$ which implies that $q<5$.

If $x=\frac{q-1}{2}$ we have

$$f=q^4-2q^2-q+2=(q-1)(q^3+q^2-q-2).$$

Setting $g=q^3+q^2-q-2$, observe that $g\equiv 2\not\equiv 0 \mod q$ for $q>2$; similarly $g\equiv -1\not\equiv 0 \mod (q-1)$ for all q. Thus, since $q>3$, we must have $|g|<q(q-1)$ which implies that $q<5$, a contradiction.

If $x=q-1$ we have

$$f=q^4-q^3-2q^2-q+3=(q-1)(q^3-2q-3).$$

Setting $g=q^3-2q+3$, observe that $g\equiv -3\not\equiv 0 \mod q$ for $q>3$; similarly $g\equiv -4\not\equiv 0 \mod (q-1)$ for $q>5$. Thus, for $q>5$, we must have $|g|<q(q-1)$ which implies that $q<3$, a contradiction.

If $x=2(q-1)$ we have

$$f=q^4-3q^3-2q^2-q+5=(q-1)(q^3-2q^2-4q-5).$$

Setting $g=q^3-2q^2-4q-5$, observe that $g\equiv -5\not\equiv 0 \mod q$ for $q>5$; similarly $g\equiv -10\not\equiv 0 \mod (q-1)$ for $q>5$. Thus, for $q>5$, we must have $|g|<q(q-1)$ which implies that $q<5$, a contradiction.

We are left with the possibility that $q=3$ or $q=5$. When $q=5$ we must have $\Lambda=\{31,\lambda_1\}$ and $\lambda_1=3,6,12$ or 24. Calculating the Euler characteristic in each case we find that $\chi=-|S:T|5^5\cdot 2^4, -|S:T|5^3\cdot 2^7\cdot 7, -|S:T|5^3\cdot 2^3\cdot 11\cdot 13, -|S:T|5^3\cdot 2^2\cdot 317$ respectively. We conclude that $\lambda_2=3$; since there are no elements of order 31 or 3 in $AutT\backslash T$ we conclude that $S=T$ in this situation, as required.

When $q=3$, $|T|=2^4\cdot 3^3\cdot 13$ and we conclude that $\Lambda=\{13,\lambda_1\}$ where λ_1 ranges through the element orders (>2) of elements in S. Using [CCN$^+$85], we go through these one at a time:

λ_1	Prime dividing χ or (S,χ)
3	7
4	$(T,-2^2\cdot 3^5)$ or $(T.2,-2^3\cdot 3^5)$
6	5
8	31
12	53
13	$(T,-2^3\cdot 3^5)$

The result follows. □

From now on we have $q = 2^a$ for some $a \geqslant 1$. In this case we must account for outer automorphisms that are not just graph automorphisms; in what follows we study an automorphism $\zeta = \sigma^x\delta^y$ where x and y satisfy $0 \leqslant x \leqslant 1; 1 \leqslant y \leqslant a-1$. Note, in particular, that ζ can be extended to an automorphism of $SL_3(\overline{\mathbb{F}_q})$ and, in this situation, it has a finite number of fixed points.

Lemma 5.10. *Suppose that $q = 2^a$ with $a > 2$. Any element in S of order divisible by q^2+q+1 has order equal to q^2+q+1. Any element in $S\backslash T$ of order divisible by $q+1$ has order dividing $2(q+1)$.*

Proof. Any element of S lies in a cyclic extension of T; if an element lies in an extension $\langle T, \sigma\rangle$ where σ is a graph automorphism then Lemma 5.8 gives the result. Thus assume this is not the case and consider elements in an extension of form $\langle T, \zeta\rangle$ where ζ is given above.

Let x be the order of ζ; thus x divides $2a$, and consider an element $(t, \zeta) \in T \rtimes \langle\zeta\rangle$. Observe that

$$u = (t, \zeta)^x = g \cdot t \cdot t^2 \cdots g^{\zeta^{x-1}}.$$

In particular observe that $u^\zeta = t^{-1}ut$ and we obtain that u lies in a conjugacy class that is stable under ζ. Now we apply Proposition 2.3, and conclude that u is conjugate to an element of $SL_3(r)$ where $q = r^a$. Observe in particular that $|o(h)|_{2'} \leqslant r^2+r+1$.

Suppose that $g = (t, \zeta)$ is an element of order divisible by q^2+q+1. Then the order of $|o(g)|_{2'}$ divides $a(r^2+r+1)$ and so we have that $q^2+q+1 \leqslant a(r^2+r+1)$ which is a contradiction for $a > 1$. Thus any element of S of order divisible by q^2+q+1 must lie in T and so has order equal to q^2+q+1.

Next suppose that $g = (t, \zeta)$ is an element of S of order divisible by $q+1$. Then, as before, we have that $q+1 \leqslant a(r^2+r+1)$. If $a \geqslant 4$ this implies that $q = 16$ or 32. Then $o(g)$ is divisible by 11 or 17 which does not divide $a|SL_3(r)|$ and we are done. If $a = 3$ then we have $q < 64$ and we conclude that $q = 8$; now [CCN$^+$85] confirms the result. Finally suppose that $a = 2$; then we must have $q+1$ dividing $|SL_3(\sqrt{q}|$. Now $q+1$ is coprime with both $q-1$ and $q+\sqrt{q}+1$, and we have a contradiction. □

Lemma 5.11. *Suppose that $T = PSL_3(q)$ and $q = 2^a$ for some integer $a \geqslant 2$. Then one of the following holds:*

(a) $S = PSL_3(4).2$, $\Lambda = \{5, 14\}$, $\chi = -2^{10} \cdot 3^2$;

(b) $S = PSL_3(4).2$, $\Lambda = \{10, 7\}$, $\chi = -2^7 \cdot 3^4$;

(c) $S = PSL_3(4).3$, $\Lambda = \{15, 21\}$, $\chi = -2^5 \cdot 3^6$;

Proof. The two primes dividing χ must be 2 and $q-1$, hence Λ must contain elements divisible by primitive prime divisors r_2 and r_3. (Note that both of these exist.) Now Lemmas 5.8 and 5.10 imply that $\Lambda = \{q^2+q+1, \lambda_2\}$ where $\lambda_2 \in \{q+1, 2(q+1), q^2-1\}$.

We start by assuming $q > 4$ and we calculate χ for each of the three possibilities. First suppose $\lambda_2 = q+1$:

$$\begin{aligned}\chi &= |S|(\frac{1}{m}+\frac{1}{n}-\frac{1}{2}) \\ &= |S:T|q^3(q^2-1)(q^3-1)\left(\frac{1}{q+1}+\frac{1}{q^2+q+1}-\frac{1}{2}\right) \\ &= -\frac{1}{2}|S:T|q^3(q-1)^2\big(q^3-2q-3\big)\end{aligned}$$

Setting $f = q^3-2q-3$, observe that $f \equiv -3 \not\equiv 0 \mod q$; similarly $f \equiv -4 \not\equiv 0 \mod (q-1)$. Thus we must have $|f| < q(q-1)$ which implies that $q \leqslant 4$, a contradiction.

Next suppose that $\lambda_2 = q^2-1$:

$$\begin{aligned}\chi &= |S|(\frac{1}{m}+\frac{1}{n}-\frac{1}{2}) \\ &= |S:T|q^3(q^2-1)(q^3-1)\left(\frac{1}{q^2-1}+\frac{1}{q^2+q+1}-\frac{1}{2}\right) \\ &= -\frac{1}{2}|S:T|q^3(q-1)\big(q^4+q^3-4q^2-3q-1\big)\end{aligned}$$

Setting $f = q^4+q^3-4q^2-3q-1$, observe that $f \equiv -1 \not\equiv 0 \mod q$; similarly $f \equiv -6 \not\equiv 0 \mod (q-1)$. Thus we must have $|f| < q(q-1)$ which implies that $q \leqslant 4$, a contradiction.

Finally suppose that $\lambda_2 = 2(q+1)$:

$$\begin{aligned}\chi &= |S|(\frac{1}{m}+\frac{1}{n}-\frac{1}{2}) \\ &= |S:T|q^3(q^2-1)(q^3-1)\left(\frac{1}{2(q+1)}+\frac{1}{q^2+q+1}-\frac{1}{2}\right) \\ &= -\frac{1}{2}|S:T|q^3(q-1)^2\big(q^3+q^2-q-2\big)\end{aligned}$$

Setting $f = q^3+q^2-q-2$, observe that $f \equiv -2 \not\equiv 0 \mod q$; similarly $f \equiv -1 \not\equiv 0 \mod (q-1)$. Thus we must have $|f| < q(q-1)$ which implies that $q \leqslant 4$, a contradiction.

We are left with the possibility that $q = 4$; in this case we know that $s = 3$ and we must have $\Lambda = \{\lambda_1, \lambda_2\}$ with $5|\lambda_1$ and $7|\lambda_2$. Consulting [CCN+85] we see that $\lambda_1 \in \{5, 10, 15\}$ and $\lambda_2 \in \{7, 14, 21\}$. Now we go through the nine possibilities; all cases but three may be excluded:

Λ	Prime dividing χ	Λ	Prime dividing χ	Λ	Prime dividing χ
{5,7}	11	{5,14}	*	{5,21}	53
{10, 7}	*	{10, 14}	23	{10, 21}	37
{15,7}	61	{15, 14}	19	{15, 21}	*

Note that the outer automorphism group of $PSL_3(4)$ has order 12. If $\Lambda = \{5, 14\}$ or $\{10, 7\}$ then $(\lambda, 12) \leqslant 2$ for $\lambda \in \Lambda$. What is more in both $PSL_3(4)$ does not contain elements of order 10 nor of order 14; thus, in both cases we must generate a degree 2 extension, $T.2$. If $\Lambda = \{15, 21\}$ then $(\lambda, 12) = 3$ for all $\lambda \in \Lambda$; furthermore there are no elements of order 15 nor of order 21 in $PSL_3(4)$. Thus, since $(ghT)^2 = 1$ we conclude that $gT = (hT)^{-1} \in S/T$; thus g and h generate a degree 3 extension, $T.3$. The result follows. □

5.4 $T = PSU_3(q)$

In this section we proceed very similarly to the previous. We assume throughout that $q > 2$ (since $PSU_3(2)$ is solvable). Furthermore we fix γ to be an 'inner diagonal' automorphism of order $(3, q+1)$ and δ to be an automorphism of order $2\log_p q$ induced by a Galois automorphism of $\mathbb{F}_{q^2}$ of order $2\log_p q$. We refer to [KL90, §2.2] to see that $\mathrm{Aut}(T) = \langle T, \gamma, \delta \rangle$. We start with an easy result:

Lemma 5.12. *There exists $a \in \mathbb{Z}^+$ such that $q + 1 = r^a$ for some prime r.*

Proof. Observe first that the Sylow t-subgroups are non-cyclic for $t = p$ and $t | q + 1$. Thus, if t is a prime such that $t | p(q + 1)$, then $t | \chi$ and we conclude that $q - 1$ is a prime power. □

Once again we use Theorem 2.2 to limit the possibilities.

Corollary 5.13. *One of the following holds:*

(a) q is an odd prime and $S = T$ or $S = \langle T, \delta^{\log_p q} \rangle$;

(b) $q = 2^a$ for some positive integer $a \neq 1, 3$ and $S \leqslant \langle T, \delta \rangle$;

(c) $q = 8$.

Note that, since δ has order $2\log_p q$, the group $\langle T, \delta^{\log_p q} \rangle$ is a degree 2 extension of T.

Proof. Suppose first that q is odd. Since $q = 2^a - 1$ we know that T admits no diagonal outer automorphisms. Now Theorem 2.2 implies that q is prime; thus T has an outer automorphism group of size 2, and the result follows.

Now suppose that $q = 2^a$ with $a \neq 1, 3$; then $q + 1$ is a prime power and Theorem 2.2 implies that $q + 1$ is a prime. In particular $q + 1$ is not divisible by 3 and so T admits no diagonal automorphisms; the result follows. □

Let us deal with the last situation first.

Lemma 5.14. *If $T = PSU_3(8)$ then $S = T$, $\Lambda = \{7, 19\}$ and $\chi = -2^8 \cdot 3^8$.*

Proof. Observe first that $\pi(T) = \{2, 3, 7, 19\}$ and that $\pi_{nc}(T) = \{2, 3\}$. Thus Λ must contain elements divisible by 7 and 19. Consulting [CCN$^+$85] for almost simple groups S with socle T we see that the possible element orders are 7, 14, 21, 63, 19 and 57. Now we go through the eight possibilities; all cases but one may be excluded:

Λ	Prime dividing χ or (S,χ)	Λ	Prime dividing χ or (S,χ)
$\{7{,}19\}$	$(T, -2^8 \cdot 3^8)$	$\{7, 57\}$	271
$\{14{,}19\}$	5	$\{14{,}57\}$	139
$\{21{,}19\}$	11	$\{21{,}57\}$	347
$\{63{,}19\}$	1033	$\{63{,}57\}$	1117

The result follows. □

We are interested in the order of elements in $S\backslash T$; we will need to use the Lang-Steinberg theorem in much the same way as we have already seen it with $T = {}^2B_2(q)$ and $T = PSL_3(q)$.

Lemma 5.15. *Suppose that we are in one of the first two situations of Cor. 5.13 and that $q > 3$. Any element in S of order divisible by $q^2 - q + 1$ has order equal to $q^2 - q + 1$. Any element in S of order divisible by $\frac{q-1}{(2,q-1)}$ has order dividing $\frac{4}{(2,q-1)}(q^2 - 1)$.*

Proof. Since $T = SU_3(q) < SL_3(q^2)$ we know that every element of T is diagonalizable (in $GL_3(q)$) over a field of order q^2, q^4 or q^6; furthermore, elements in T that are diagonalizable over $\mathbb{F}_{q^2}$ and not $\mathbb{F}_q$ have order dividing $q + 1$. We conclude that if an element of T is divisible by an odd prime dividing $q - 1$ or by a primitive prime divisor r_2, then it is not diagonalizable over $\mathbb{F}_{q^2}$.

Proceeding now as per the proof of Lemma 5.8 we conclude that such elements have distinct eigenvalues and thus their centralizers are both maximal tori of T; in particular $C_T(x) \cong C_{q^2-1}$ and $C_T(y) \cong C_{q^2-q+1}$. We conclude, in particular, that any element in T of order divisible by $q^2 - q + 1$ has order equal to $q^2 - q + 1$; similarly any element in T of order divisible by $\frac{q-1}{(2,q-1)}$ has order dividing $q^2 - 1$.

Suppose, next, that $S = \langle T, \delta^y \rangle$ where $y = \frac{2 \log_p q}{x}$ for some $x > 1$; in particular δ^y has order x. Let (t, δ^y) be an element of S; proceeding as per the proof of Lemma 5.10, and using Proposition 2.3 we conclude that $(t, \delta^y)^x$ lies in $SL_3(q_1^2)$ where $q_1^t = q$. Thus (t, δ^y) has order xv where v is the order of an element in $SL_3(q_1^2)$.

Suppose first that (t, δ^y) has order divisible by $q^2 - q + 1$. If x is even then we conclude that $q^2 - q + 1$ has order xv where v is the order of an element in $SL_3(q)$. But now observe that $(q^2 - q + 1, |SL_3(q)|) = 1$ and we have a contradiction.

If x is odd then $q_1^{2x} - q_1^x + 1 = xv$ where v is the order of an element in $SL_3(q_1^2)$. Since $|v|_{p'} \leqslant q_1^4 + q_1^2 + 1$ we have

$$q_1^{2x} - q_1^x + 1 \leqslant x(q_1^4 + q_1^2 + 1)$$

which is a contradiction unless $q_1 = 2$ and $x = 3$. But in this case $q = 8$ which is excluded.

Suppose next that (g, δ^y) has order divisible by $\frac{q-1}{(2,q-1)}$. If δ^y has order at most 2 then the result follows immediately; in particular the result is true for q odd and we suppose that q is even. Then, as above, we have that $q_1^x - 1$ divides xv where v is the order of an element in $SL_3(q_1^2)$. This implies immediately that $q_1^x - 1 \leqslant x(q_1^4 + q_1^2 + 1)$ which is a contradiction for $x \geqslant 8$.

For $x = 6, 7$ we conclude that $q_1 = 2$. Since $2^7 - 1$ is a prime we know that it does not divide the order of an element of $SL_3(4)$ so we exclude $x = 7$. If $x = 6$, $q = 2^x + 1 = 65$ which is not a prime and so is excluded. If $x = 5$ then $q_1^5 - 1$ divides either $5(q_1^4 - 1)$ or $5(q_1^4 + q_1^2 + 1)$ which is a contradiction. If $x = 4$ then $q_1^4 - 1$ divides either $4(q_1^4 - 1)$ or $4(q_1^4 + q_1^2 + 1)$; the latter is impossible, the former gives the result.

We are left with $x = 3$. In this case $q_1^3 - 1$ divides either $3(q_1^4 - 1)$ (impossible) or $3(q_1^4 + q_1^2 + 1)$; this in turn implies that $q_1^3 - 1$ divides $3(q_1^2 + q_1 + 1)$ and we conclude that $q_1 \leqslant 4$. If $q_1 = 2$ then $q = 8$ which is excluded; if $q_1 = 4$ then the order of (g, δ^y) divides $q_1^3 - 1$ as required. □

Lemma 5.16. *If q is odd, then $PSU_3(3) = T \leqslant S \leqslant PSU_3(3).2$ and one of the following holds:*

(a) $S = T$, $\Lambda = \{3, 7\}$, $\chi = -2^4 \cdot 3^2$;

(b) $\Lambda = \{4, 7\}$, $\chi = -|S : T|2^3 \cdot 3^4$;

(c) $\Lambda = \{6, 7\}$, $\chi = -|S : T|2^7 \cdot 3^2$;

(d) $S = T$, $\Lambda = \{7, 7\}$, $\chi = -2^4 \cdot 3^4$;

Proof. Suppose first that $q > 3$. The two primes dividing χ must be 2 and p hence, writing $\Lambda = \{\lambda_1, \lambda_2\}$ we must have $(\frac{q-1}{2})(q^2 + 1 + 1)$ dividing $\lambda_1\lambda_2$. Now Lemma 5.15 implies that $\Lambda = \{q^2 + q + 1, \lambda_2\}$ where $\lambda_2 = \frac{2(q^2-1)}{x}$ for some $x = 2^b | 4(q + 1)$. Now we calculate χ:

$$\begin{aligned}
\chi &= |S|(\frac{1}{m} + \frac{1}{n} - \frac{1}{2}) \\
&= |S : T|q^3(q^2 - 1)(q^3 + 1)\left(\frac{x}{2(q^2 - 1)} + \frac{1}{q^2 - q + 1} - \frac{1}{2}\right) \\
&= -\frac{1}{2}|S : T|q^3(q + 1)\big(q^4 - q^3 - (x + 2)q^2 + (x + 1)q - (x - 1)\big)
\end{aligned}$$

Setting $f = q^4 - q^3 - (x + 2)q^2 + (x + 1)q - (x - 1)$, observe that $f \equiv -(x - 1) \not\equiv 0 \mod q$ for $x < q + 1$; similarly $f \equiv -3x \not\equiv 0 \mod (q + 1)$ for $x < q + 1$. Thus if $x \leqslant \frac{q+1}{2}$ we must have $|f| < q(q + 1)$ which implies that $q < 7$, a contradiction.

If $x = q + 1$ we have

$$f = q^4 - 2q^3 - 2q^2 + q = q(q + 1)(q^2 - 3q + 1).$$

Setting $g = q^2 - 3q + 1$, observe that $(g, q) = 1$ and $(g, q + 1) \leqslant 5$. Thus $q^2 - 3q + 1 \leqslant 5$ which is a contradiction.

If $x = 2(q + 1)$ we have

$$f = q^4 - 3q^3 - 2q^2 + q - 1 = (q + 1)(q^3 - 4q^2 + 2q - 1).$$

Setting $g = q^3 - 4q^2 + 2q - 1$, observe that $g \equiv -1 \not\equiv 0 \mod q$; similarly $g \equiv -8 \not\equiv 0 \mod (q-1)$ for $q > 7$. Thus, for $q > 7$, we must have $|g| < q(q-1)$ which implies that $q < 5$, a contradiction. If $q = 7$ then f is divisible by 5 which is a contradiction.

If $x = 4(q+1)$ we have

$$f = q^4 - 5q^3 - 2q^2 + q - 3 = (q+1)(q^3 - 6q^2 + 4q - 3).$$

Setting $g = q^3 - 6q^2 + 4q - 3$, observe that $g \equiv -3 \not\equiv 0 \mod q$ for $q > 3$; similarly $g \equiv -14 \not\equiv 0 \mod (q+1)$ for all $q \neq 13$ (and we know that $q \neq 13$ since $q + 1$ is a power of 2). Thus, for $q > 3$, we must have $|g| < q(q+1)$ which implies that $q < 7$, a contradiction.

We are left with the possibility that $q = 3$. Then $|T| = 2^5 \cdot 3^3 \cdot 7$ and we conclude that $\Lambda = \{7, \lambda_1\}$ where λ_1 ranges through the element orders (> 2) of elements in S. Using [CCN+85], we go through these one at a time:

λ_1	Prime dividing χ or (S, χ)
3	$(T, -2^4 \cdot 3^2)$
4	$(T, -2^3 \cdot 3^4)$ or $(T.2, -2^4 \cdot 3^4)$
6	$(T, -2^7 \cdot 3^2)$ or $(T.2, -2^8 \cdot 3^2)$
7	$(T, -2^4 \cdot 3^4)$
8	13
12	23

The result follows. □

Lemma 5.17. *Suppose that $q = 2^a$ with a a positive integer not equal to 3. Then*

(a) $S = PSU_3(4).2$, $\Lambda = \{6, 13\}$, $\chi = -2^8 \cdot 5^3$;

Proof. Assume first that $q > 4$; hence, in particular, $q \geqslant 16$. The two primes dividing χ must be 2 and $q+1$, hence, writing $\Lambda = \{\lambda_1, \lambda_2\}$, we must have $(\frac{q-1}{2})(q^2+1+1)$ dividing $\lambda_1\lambda_2$. Now Lemma 5.15 implies that $\Lambda = \{q^2+q+1, \lambda_2\}$ where $\lambda_2 = \frac{2(q^2-1)}{x}$ for some $x = 2^b | 4(q+1)$. Now we calculate χ:

$$\begin{aligned}\chi &= |S|(\frac{1}{m} + \frac{1}{n} - \frac{1}{2}) \\ &= |S:T|q^3(q^2-1)(q^3+1)\left(\frac{x}{4(q^2-1)} + \frac{1}{q^2-q+1} - \frac{1}{2}\right) \\ &= -\frac{1}{4}|S:T|q^3(q+1)\big(2q^4 - 2q^3 - (x+4)q^2 + (x+2)q - (x-2)\big)\end{aligned}$$

Setting $f = 2q^4 - 2q^3 - (x+4)q^2 + (x+2)q - (x-2)$, observe that $f \equiv -(x-2) \not\equiv 0 \mod q$ for $x \leqslant q+1$; similarly $f \equiv -3x \not\equiv 0 \mod (q+1)$ for $x < q+1$. Thus if $x < q+1$ we must have $|f| < q(q+1)$ which implies that $q < 16$, a contradiction.

Now suppose that $x \geqslant q+1$; this implies that $\lambda_2 \in \{q-1, 2(q-1), 4(q-1)\}$ and we go through these in turn.

If $\lambda_2 = q-1$ then we have

$$\begin{aligned}\chi &= |S|(\frac{1}{m}+\frac{1}{n}-\frac{1}{2})\\ &= |S:T|q^3(q^2-1)(q^3+1)\left(\frac{1}{q-1}+\frac{1}{q^2-q+1}-\frac{1}{2}\right)\\ &= -\frac{1}{2}|S:T|q^3(q+1)\big(q^3-4q^2+2q-1\big)\end{aligned}$$

Now, since $(q^3-4q^2-2q+1, q+1)=1$ we have a contradiction.

If $\lambda_2 = 2(q-1)$ then we have

$$\begin{aligned}\chi &= |S|(\frac{1}{m}+\frac{1}{n}-\frac{1}{2})\\ &= |S:T|q^3(q^2-1)(q^3+1)\left(\frac{1}{2(q-1)}+\frac{1}{q^2-q+1}-\frac{1}{2}\right)\\ &= -\frac{1}{2}|S:T|q^4(q+1)\big(q^2-3q+1\big)\end{aligned}$$

Now, since $(q+1, q^2-3q+1) \leqslant 5 < q^2-3q+1$ we have a contradiction.

If $\lambda_2 = 4(q-1)$ then we have

$$\begin{aligned}\chi &= |S|(\frac{1}{m}+\frac{1}{n}-\frac{1}{2})\\ &= |S:T|q^3(q^2-1)(q^3+1)\left(\frac{1}{2(q-1)}+\frac{1}{q^2-q+1}-\frac{1}{2}\right)\\ &= -\frac{1}{4}|S:T|q^3(q+1)\big(2q^3-5q^2+q+1\big)\end{aligned}$$

Now, since $(q+1, 2q^3-5q^2+q+1)$ divides 7 we have a contradiction.

We are left with the possibility that $q=4$. Thus, writing $\Lambda = \{\lambda_1, \lambda_2\}$ we assume that λ_1 is divisible by 3 and λ_2 is divisible by 13. Consulting [CCN$^+$85] we obtain that $\lambda_2 = 13$ and $\lambda_1 \in \{3, 6, 12, 15\}$; we go through these one at a time:

λ_1	Prime dividing χ or (S, χ)
3	7
6	$(T.2, -2^8 \cdot 5^3)$
12	53
15	139

The result follows. □

5.5 $T = G_2(3)$

Recall that $s=3$. Thus, writing $\Lambda = \{\lambda_1, \lambda_2\}$ we assume that λ_1 divisible by 7 and λ_2 is divisible by 13. We consult [CCN$^+$85] and find that there are two possibilities:

Suppose that $S = T = G_2(3)$; then $\Lambda = \{7, 13\}$. In this case $17|\chi$ and we exclude this case. Alternatively we have $S = G_2(3).2$ and $= \{13, 14\}$. In this case $\chi = -2^{12} \cdot 3^6$, a valid possibility.

5.6 $T = Sp_6(2)$

Recall that $s = 3$. Thus, writing $\Lambda = \{\lambda_1, \lambda_2\}$ we assume that λ_1 is divisible by 5 and λ_2 is divisible by 7. The outer automorphism group is trivial here so $S = T$. There are three possibilities: $\Lambda = \{5, 7\}$ in which case $11|\chi$ and we exclude this case; $\Lambda = \{15, 7\}$ in which case $61|\chi$ and we exclude this case; $\Lambda = \{7, 10\}$ in which case $\chi = -2^9 \cdot 3^6$, a valid possibility.

5.7 $T = SU_5(2)$

Recall that $s = 3$. Thus, writing $\Lambda = \{\lambda_1, \lambda_2\}$ we assume that λ_1 is divisible by 5 and λ_2 is divisible by 11. There are three possibilities, all of which are invalid: $\Lambda = \{5, 11\}$ in which case $23|\chi$; $\Lambda = \{10, 11\}$ in which case $17|\chi$; $\Lambda = \{15, 11\}$ in which case $113|\chi$.

5.8 $T = PSL_4(3)$

Recall that $s = 3$. Thus, writing $\Lambda = \{\lambda_1, \lambda_2\}$ we assume that λ_1 is divisible by 5 and λ_2 is divisible by 13. Consulting [CCN+85] we see that $\lambda_1 \in \{5, 10, 20, 40\}$ and $\lambda_2 \in \{13, 26\}$. In all cases we find that a prime other than 2 or 3 divides χ:

Λ	Prime dividing χ	Λ	Prime dividing χ
{5,13}	29	{5,26}	17
{10, 13}	7	{10, 26}	47
{20,13}	97	{20, 26}	107
{40,13}	23	{40, 26}	227

5.9 $T = PSU_4(3)$

Recall that $s = 3$. Thus, writing $\Lambda = \{\lambda_1, \lambda_2\}$ we assume that λ_1 is divisible by 5 and λ_2 is divisible by 7. Consulting [CCN+85] we see that $\lambda_1 \in \{5, 10, 20\}$ and $\lambda_2 \in \{7, 14, 28\}$. In all cases but two we find that a prime other than 2 or 3 divides χ:

Λ	Prime dividing χ	Λ	Prime dividing χ	Λ	Prime dividing χ
{5,7}	11	{5,14}	*	{5,28}	37
{10, 7}	*	{10, 14}	23	{10, 28}	17
{20,7}	43	{20, 14}	53	{20, 28}	29

Since T does not contain an element of order 10 nor an element of order 14, we conclude that $S = T.2$ in both cases. When $\Lambda = \{7, 10\}$ we have $\chi = -2^8 \cdot 3^8$; when $\lambda = \{5, 14\}$ we have $\chi = -2^{11} \cdot 3^6$.

5.10 $T = SL_4(2)$

Recall that $s = 3$. Thus, writing $\Lambda = \{\lambda_1, \lambda_2\}$ we assume that λ_1 is divisible by 5 and λ_2 is divisible by 7. There are three possibilities: $\Lambda = \{5, 7\}$ in which case $11|\chi$ and we exclude this case; $\Lambda = \{15, 7\}$ in which case $61|\chi$ and we exclude this case; $\Lambda = \{7, 10\}$ in which case $\chi = -2^7 \cdot 3^4$; since t does not contain an element of order 10 we conclude that $S = T.2$ in this case.

5.11 $T = SU_4(2)$

Once again $s = 3$. Since $|T| = 2^6 \cdot 3^4 \cdot 5$ and writing $\Lambda = \{\lambda_1, \lambda_2\}$, we assume that λ_1 is divisible by 5, while λ_2 may be any order greater than 2. Consulting [CCN$^+$85] for T and $T.2$ we conclude that $m \in \{5, 10\}$, $n \in \{3, 4, 5, 6, 8, 9, 10, 12\}$. If $m = 5$ we exclude $n = 3$ since it is well known that

$$\langle x, y \mid x^3 = y^5 = (xy)^2 = 1\rangle \cong A_5.$$

In the table below we list all possible combinations for m and n; if χ is divisible by a prime greater than 3 we list it, otherwise we list the value of χ as well as the isomorphism class of S (either T or $T.2$ or, in two cases, both):

Λ	Prime dividing χ or (S, χ)	Λ	Prime dividing χ or (S, χ)
{5,3}	Excluded	{10, 3}	$(T.2, -2^7 \cdot 3^3)$
{5,4}	$(T, -2^4 \cdot 3^4)$, $(T.2, -2^5 \cdot 3^4)$	{10,4}	$(T.2, -2^5 \cdot 3^5)$
{5,5}	$(T, -2^5 \cdot 3^4)$	{10,5}	$(T.2, -2^7 \cdot 3^4)$
{5,6}	$(T, -2^7 \cdot 3^3)$, $(T.2, -2^8 \cdot 3^3)$	{10,4}	7
{5,8}	7	{10,8}	11
{5,9}	17	{10,9}	13
{5,10}	Already covered	{10, 10}	$(T.2, -2^6 \cdot 3^5)$
{5,12}	13	{10,12}	19

5.12 Alternating groups

We must consider $S = A_7, S_7, A_9, S_9$; in all cases $s = 3$ thus, writing $\Lambda = \{\lambda_1, \lambda_2\}$ we assume that λ_1 is divisible by 5 and λ_2 is divisible by 7. Consulting [CCN$^+$85] we see that $\lambda_1 \in \{5, 10, 15, 20\}$ and $\lambda_2 \in \{7, 14\}$. In all but two cases we see that a prime greater than 3 divides χ:

Λ	Prime dividing χ	Λ	Prime dividing χ
{5,7}	11	{5,14}	*
{10, 7}	*	{10, 14}	23
{15,7}	61	{15,14}	19
{20,7}	43	{20, 14}	53

Thus we must check $\Lambda = \{10, 7\}$ and $\{5, 14\}$ for the four different groups. When $S = A_7$ neither of these are possible. When $S = S_7$ only $\Lambda = \{10, 7\}$ is possible and we obtain $\chi = -2^4 \cdot 3^4$. When $S = A_9$ only $\Lambda = \{10, 7\}$ is possible and we obtain $\chi = -2^6 \cdot 3^6$. Finally when $S = S_9$ both cases are possible and we obtain $\chi = -2^9 \cdot 3^4$ when $\Lambda = \{5, 14\}$ and $\chi = -2^7 \cdot 3^6$) when $\Lambda = \{10, 7\}$.

5.13 Sporadic groups

We must consider $S = M_{11}, M_{12}, M_{12}.2$. Since $s = 3$ the elements of Λ must be divisible by 5 and 11. Examining [CCN+85] we see that there are only two possibilities in total: $\Lambda = \{5, 11\}$ (in which case 23 divides χ) or $\Lambda = \{10, 11\}$ (in which case 17 divides χ).

5.14 Existence

The work of Sections 5.1 to 5.13 has yielded a number of putative $(2, m, n)$-groups for which we must now establish existence or otherwise. When $T = PSL_2(q)$ for some $q \geqslant 4$ we have the following possibilities for S provided $S \neq PSL_2(q)$ or $PGL_2(q)$:

S	$\{m, n\}$	χ
$PSL_2(9).2$	$\{4, 5\}$	$-2^2 \cdot 3^2$
$PSL_2(9).2$	$\{5, 6\}$	$-2^5 \cdot 3$
$PSL_2(9).(C_2 \times C_2)$	$\{4, 10\}$	$-2^3 \cdot 3^3$
$SL_2(16).2$	$\{6, 5\}$	$-2^6 \cdot 17$
$SL_2(16).2,$	$\{10, 3\}$	$-2^5 \cdot 17$
$PSL_2(25).2$	$\{6, 13\}$	$-2^5 \cdot 5^3$

In all cases bar the first the requirement that S be generated by a pair of elements of order m and n uniquely prescribes the group up to isomorphism.

Let us consider the exceptional first case. Then $S = PSL_2(9).2$, $\{m, n\} = \{4, 5\}$ and there are two isomorphism classes for S that we must consider, namely $S = M_{10}$ and $S = S_6$. Suppose that $S = M_{10}$ and let $S = \langle g, h\rangle$ where $o(g) = 4$ and $o(h) = 5$. Then $g \notin PSL_2(9)$ and $h \in PSL_2(9)$. Thus $gh \notin PSL_2(9)$. But M_{10} is a non-split extension and so $o(gh) \neq 2$ which is a contradiction.

On the other hand suppose that $S = S_6$; then [Con90] implies that S is not a $(2, 4, 5)$-group and this case is also excluded. On the other hand [Con90] implies that S is a $(2, 5, 6)$-group which confirms the existence of the group in the second line of the table.

For the next three lines we use a combination of [GAP08] and [BCP97]; these rule out both possibilities when $S = SL_2(16).2$. On the other hand they confirm that the group $PSL_2(9).(C_2 \times C_2)$ is a $(2, 4, 10)$-group.

We are left with the case when $S = PSL_2(25).2$. Note first that the list of maximal subgroups of $PSL_2(25)$ given in [CCN+85] implies that any pair of elements of order 3 and 13 in $PSL_2(25)$ must generate $PSL_2(15)$. Thus it is enough to show that there are elements $g, h \in S\backslash PSL_2(25)$ such that $o(g) = 2, o(h) = 6$ and $gh \in PSL_3(4)$ is of order

13; a simple application of Proposition 2.5 confirms that such elements exist. We have justified the entries in Table 1.

Now we turn to the situation where $T \neq PSL_2(q)$ for any $q \geqslant 4$. Table 2 lists twenty-seven pairs $(S, \{m,n\})$ such that S is a $(2,m,n)$-group. (The total of twenty-seven takes into account two key facts: when only T is specified, there are two groups to consider for S; when $(S, \{m,n\}) = (PSU_4(3).2, \{10,7\})$, we must consider three isomorphism classes for S.)

Our work in Sections 5.1 to 5.13 implies that there are a number of other possible pairs to consider. We list them as follows:

Group	$\{m,n\}$	χ
$S = SU_3(3)$	$\{3,7\}$	$-2^4 \cdot 3^2$
$S = SU_3(3)$	$\{4,7\}$	$2^3 \cdot 3^4$
$T = SU_4(2)$	$\{5,4\}$	$-\lvert S:T\rvert \cdot 2^4 \cdot 3^4$
$S = SU_4(2)$	$\{5,5\}$	$-2^5 \cdot 3^4$
$S = SU_4(2).2$	$\{10,3\}$	$-2^7 \cdot 3^3$
$S = S_9$	$\{10,7\}$	$-2^7 \cdot 3^6$
$S = S_9$	$\{5,14\}$	$-2^{10} \cdot 3^4$

We follow the conventions of Table 2; in particular when we specify only T we must consider two groups $S = T$ and $S = T.2$. Our first job is to rule out the eight possibilities listed in this table. The first possibility is excluded by [Con87] in which it is shown that $SU_3(3)$ is not a Hurwitz group.

Now consider the second possibility when $S = SU_3(3)$ and $\{m,n\} = \{4,7\}$. We consult [CCN+85] to find that $SU_3(3)$ has a unique conjugacy class of involutions and three conjugacy classes of elements of order 4 which we label, as per [CCN+85], 4A, 4B and 4C. Let g be an involution and h an element of order 4; Proposition 2.5 implies that if h is in conjugacy class 4B or 4C then gh is never of order 7, so suppose that h is in conjugacy class 4A. Then Proposition 2.5 implies that, for any $z \in S$ of order 7 there are seven pairs $(x,y) \in g^S \times h^S$ such that $xy = z$. Now an application of Proposition 2.5 to $H = PSL_2(7)$ implies that, for any $z \in S$ of order 7 there are seven pairs $(x,y) \in H$ such that $o(x) = 2$, $o(y) = 4$ and $xy = z$. Furthermore [CCN+85] implies that S has a subgroup isomorphic to $PSL_2(7)$. Since a Sylow 7-subgroup of H is cyclic of order 7, every element of order 7 in S lies in a subgroup of S isomorphic to H and we conclude that any pair $(x,y) \in S$ such that $o(x) = 2, o(y) = 4$ and $o(xy) = 7$ must lie in a subgroup isomorphic to $PSL_2(7)$ and so cannot generate S.

The four almost simple groups S with socle $T \cong SU_4(2)$ can all be ruled out using [GAP08] or [BCP97]. The same is true of the final two cases involving S_9, although we give an alternative proof using the following result [CM88].

Proposition 5.18. *Suppose that $G \leqslant S_n$ and G is generated by elements $g_1, g_2, ..., g_s$ where $g_1 \cdots g_s = 1$. Suppose that, for $i = 1, \ldots, s$, the generator g_i has exactly c_i cycles on $\Omega = \{1, \ldots, n\}$ and that G is transitive on Ω, then*

$$\sum_{i=1}^{s} c_i + 2 \leqslant n(s-2).$$

We apply this to $G = S_9$ with $s = 3$; observe that if $z \in G$ is an involution, then z has at least 5 cycles. If g is of order 10 then it has at least 3 cycles and if h has order 7 then it has at least 3 cycles; since $5 + 3 + 3 > 9$ we conclude that G is not a $(2, 7, 10)$-group. Similarly if g is of order 5 then it has at least 5-cycles; since $5 + 5 > 9$ we conclude that G is not a $(2, 5, k)$-group for any k.

All that remains is to show that the twenty-seven pairs listed in Table 2 correspond to a $(2, m, n)$-group. In nearly all cases we can confirm this easily using [GAP08] or [BCP97]; we mention three cases that are slightly tricky and which we prefer to do “by hand”.

Consider first the two cases

$$(S, \{m, n\}) = (PSL_3(4).2_2, \{5, 14\}) \text{ and } (S, \{m, n\}) = (PSL_3(4).2_3, \{7, 10\}).$$

(We use [CCN$^+$85] notation to single out the particular degree 2 extension to be studied in each case.) Note first that the list of maximal subgroups of $PSL_3(4)$ given in [CCN$^+$85] implies that any pair of elements of order 5 and 7 in $PSL_3(4)$ must generate $PSL_3(4)$. Thus in the first instance it is enough to show that there are elements $g, h \in S\backslash PSL_3(4)$ such that $o(g) = 2, o(h) = 14$ and $gh \in PSL_3(4)$ is of order 5; a simple application of Proposition 2.5 confirms that such elements exist. Similarly in the second instance it is enough to show that there are elements $g, h \in S\backslash PSL_3(4)$ such that $o(g) = 2, o(h) = 10$ and $gh \in PSL_3(4)$ is of order 7; again Proposition 2.5 confirms that such elements exist.

Finally suppose that $(S, \{m, n\}) = (G_2(3).2, \{13, 14\})$. Let z be an element of order 13 in $G_2(3)$. Proposition 2.5 implies that the number of pairs of elements $g, h \in S$ such that $o(g) = 2$ and $o(h) = 14$ is 286.

Now [CCN$^+$85] implies that the only maximal subgroup of $G_2(3).2$ that contains elements of order 13 and of order 14 is $PSL_2(13) : 2 = PGL_2(13)$. Let M be a maximal subgroup isomorphic to $PGL_2(13)$ that contains z. The number of pairs of elements $g, h \in M$ such that $o(g) = 2$ and $o(h) = 14$ is 13.

Let P be a Sylow 13-subgroup of S lying in M. Then $N_S(P) < M$ and we conclude that every Sylow 13-subgroup lies in a unique maximal subgroup isomorphic to $PGL_2(13)$. Thus there are $286 - 13 = 273$ pairs of elements $g, h \in S$ such that $o(g) = 2$, $o(h) = 14$, $gh = z$ and $\langle g, h\rangle \not\leq M$. Thus $\langle g, h\rangle$ does not lie in any maximal subgroup and we conclude that $\langle g, h\rangle = S$ as required.

6 Closing remarks

There are a number of obvious avenues for future research; we briefly run through some of them.

6.1 Improving Theorem 1.1

The obvious weakness with Theorem 1.1 is that those $(2, m, n)$-groups (S, g, h) for which $\chi = -2^a s^b$ and $S = PSL_2(q)$ or $S = PGL_2(q)$, for some q, are not classified. This is despite the fact that, thanks to Sah, we have a full enumeration of all $(2, m, n)$ groups

(S, g, h) for which $S = PSL_2(q)$ or $S = PGL_2(q)$ [Sah69]. Thus one needs only to extract from this enumeration the $(2, m, n)$-groups for which $\chi = -2^a s^b$. Unfortunately this seems hard, indeed we have not even been able to establish whether or not there are an infinite number of such $(2, m, n)$-groups.

The nature of the problem is illustrated by the following example: suppose that $S = PSL_2(2^x)$ for some integer $x > 1$. Set $m = 2^x + 1$ and $n = 2^x - 1$; using a knowledge of the subgroups of S, the character table of S, and Proposition 2.5 one can quickly deduce that S is a $(2, m, n)$-group. Writing $q = 2^x$, the Euler characteristic χ is equal to $-\frac{1}{2}q(q^2 - 4q + 1)$. Thus, if χ is to be divisible by exactly two distinct primes, then we must have

$$q^2 - 4q + 1 = s^b \tag{6.1}$$

for some odd prime s and positive integer b. The number theoretic task of describing those q, s and b such that (6.1) holds true appears to be difficult.

6.2 Three primes

Consider those $(2, m, n)$-groups G with associated Euler characteristic divisible by exactly three distinct primes. In this case the analogue of Proposition 4.1 is slightly more complicated as the group G may have non-simple non-abelian chief factors.

In particular, if $\chi = -2^a s^b t^c$ then the group G may have a chief factor isomorphic to T^k for some simple group T and $k > 1$; in this case $|T|$ must be divisible by exactly three primes (namely $2, s$ and t) and such groups do exist. (There are precisely eight simple groups whose orders are divisible by exactly three primes, namely A_5, A_6, $\mathrm{PSp}_4(3)$, $PSL_2(7)$, $PSL_2(8)$, $PSU_3(3)$, $PSL_3(3)$ and $PSL_2(17)$; this fact is not dependent on the classification of finite simple groups; see, for example, [BCM01].)

6.3 Other possibilities

Each entry of Tables 1 and 2 warrants further investigation. Although we know that each entry corresponds to at least one $(2, m, n)$-group we have not established how many distinct $(2, m, n)$-groups occur in each case. Once we have established this fact, there are a plethora of further questions: for instance, which of them are *reflexible* (i.e. admit an orientation-reversing automorphism)?

In a different direction much of the work of this paper will carry over to the study of groups associated with *non-orientable* regular maps; indeed in this situation the structure of the group has more properties that we can exploit (for instance it is generated by three involutions) and we intend to address this question in a future paper.

References

[BCM01] Y. Bugeaud, Z. Cao, and M. Mignotte, *On simple K_4-groups*, J. Algebra **241** (2001), no. 2, 658–668.

[BCP97] 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, Computational algebra and number theory (London, 1993).

[CCN$^+$85] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson, *Atlas of finite groups*, Oxford University Press, 1985.

[CM88] M. Conder and J. McKay, *A necessary condition for transitivity of a finite permutation group*, Bull. London Math. Soc. **20** (1988), no. 3, 235–238.

[Con87] M. Conder, *The genus of compact Riemann surfaces with maximal automorphism group*, J. Algebra **108** (1987), no. 1, 204–247.

[Con90] ______, *Hurwitz groups: a brief survey*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 2, 359–370.

[CPŠ10] M. Conder, P. Potočnik, and J. Širáň, *Regular maps with almost Sylow-cyclic automorphism groups, and classification of regular maps with Euler characteristic $-p^2$*, J. Algebra **324** (2010), no. 10, 2620–2635.

[DM91] F. Digne and J. Michel, *Representations of finite groups of Lie type*, London Mathematical Society Student Texts, vol. 21, Cambridge Univ. Press, 1991.

[GAP08] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008.

[Gil] N. Gill, *Orientably regular maps with Euler characteristic divisible by few primes*, To appear in *J. London Math. Soc.* doi:10.1112/jlms/jdt010.

[GLS98] D Gorenstein, R Lyons, and R Solomon, *The classification of the finite simple groups. Number 3. Part I. Chapter A*, Mathematical Surveys and Monographs, vol. 40, American Mathematical Society, Providence, RI, 1998, Almost simple K-groups.

[Isa94] I. M. Isaacs, *Character theory of finite groups*, Dover Publications Inc., New York, 1994, Corrected reprint of the 1976 original [Academic Press, New York].

[JS78] G. A. Jones and D. Singerman, *Theory of maps on orientable surfaces*, Proc. London Math. Soc. (3), **37** (1978), no. 2, 273–307.

[KL90] P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series, vol. 129, Cambridge University Press, 1990.

[Mih04] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. **572** (2004), 167–195.

[Sah69] C-H. Sah, *Groups related to compact Riemann surfaces*, Acta Math. **123** (1969), 13–42.

[Suz62] M. Suzuki, *On a class of doubly transitive groups*, Ann. of Math. **75** (1962), no. 1, 105–145.

[VV05] A. V. Vasilév and E. P. Vdovin, *An adjacency criterion in the prime graph of a finite simple group*, Algebra Logika **44** (2005), no. 6, 682–725, 764.

[Zsi92] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys. **3** (1892), no. 1, 265–284.