The probabilistic zeta function of finite simple groups

Erika Damian, Andrea Lucchini *

Università di Brescia, Dipartimento di Matematica, Via Valotti, 25133 Brescia, Italy

Received 17 June 2006
Available online 24 March 2007
Communicated by Martin Liebeck

Abstract

Let \( G \) be a finite group; there exists a uniquely determined Dirichlet polynomial \( P_G(s) \) such that if \( t \in \mathbb{N} \), then \( P_G(t) \) gives the probability of generating \( G \) with \( t \) randomly chosen elements. We show that it may be recognized from the knowledge of \( P_G(s) \) whether \( G/\text{Frat} \ G \) is a simple group.

© 2007 Elsevier Inc. All rights reserved.

Keywords: Probabilistic zeta function; Finite simple groups

1. Introduction

For any finite group \( G \) we may define a sequence of integers \( \{a_n(G)\}_{n\in\mathbb{N}} \) as follows:

\[
\forall n \in \mathbb{N} \quad a_n(G) = \sum_{|G:H|=n} \mu_G(H).
\]

Here \( \mu_G \) is the Möbius function defined on the subgroup lattice \( \mathcal{L}(G) \) of \( G \) as \( \mu_G(G) = 1 \) and \( \mu_G(H) = -\sum_{H<K} \mu_G(K) \) for any \( H < G \). Let

\[
P_G(s) = \sum_{n\in\mathbb{N}} \frac{a_n(G)}{n^s}
\]

be the Dirichlet generating function associated with the sequence \( \{a_n(G)\}_{n\in\mathbb{N}} \).

* Corresponding author.
E-mail addresses: erika.damian@ing.unibs.it (E. Damian), andrea.lucchini@ing.unibs.it (A. Lucchini).
This Dirichlet series associated with a group has been introduced by Boston in [1] and Mann who deals with profinite groups in [18]; both these authors are mainly interested in the probabilistic meaning of this series. In fact, for any \( t \in \mathbb{N} \) the series \( P_G(t) \) gives the probability that \( t \) randomly chosen elements of \( G \) generate \( G \). Since \( \mu_G(H) \neq 0 \) only if \( H \) is an intersection of maximal subgroups of \( G \) (see [10]), the Dirichlet series \( P_G(s) \) can be viewed as a way of encoding in a compact way information concerning the sublattice \( M \) of \( L(G) \) generated by the maximal subgroups of \( G \).

Clearly when we inscribe our information about a finite group \( G \) in the Dirichlet polynomial \( P_G(s) \) we cannot preserve the total amount of our knowledge about \( G \). So it is quite natural to investigate what may be recovered about the group \( G \) from the Dirichlet polynomial \( P_G(s) \). Let us first observe that if \( H \in M \), then \( H \) contains the Frattini subgroup of \( G \); so \( P_G(s) = P_{G/Frat(G)}(s) \) and the knowledge of \( P_G(s) \) may give information only about the structure of the factor group \( G/Frat(G) \). In particular, given two finite groups \( G \) and \( H \) such that \( P_G(s) = P_H(s) \), we are interested in compare \( G/Frat(G) \) and \( H/Frat(H) \). As it was already noted by Gaschütz [8], we cannot infer that \( G/Frat(G) \simeq H/Frat(H) \). However \( G \) and \( H \) have many common properties; for example the first is soluble (respectively perfect) if and only if the latter is soluble (respectively perfect). In this paper we deal with the following question: can we recognize whether \( G/Frat(G) \) is a simple group from the knowledge of the Dirichlet polynomial \( P_G(s) \)?

The result is trivial when \( G = \mathbb{Z}_p \) is an abelian simple group and in a previous paper, [5], it has been proved in the particular case when \( G = Alt(n) \) is an alternating group. Now we deal with the remaining non-abelian simple groups. Our proof for these cases requires new arguments, that are quite different from those used to solve the problem for the alternating groups. We start with proving that \( H/Frat(H) \cong S_1 \times \cdots \times S_t \), a direct product of non-abelian simple groups. Then we consider the Dirichlet polynomial \( Q(s) = \sum_{n \text{ odd}} a_n(G)/n^s = \sum_{n \text{ odd}} a_n(H)/n^s \) and use the previous information to deduce that \( 1 \) is a zero for the complex function \( Q(s) \) with multiplicity at least \( t \). Finally we prove that if \( G \neq Alt(n) \), then the multiplicity of \( 1 \) as zero \( Q(s) = \sum_{n \text{ odd}} a_n(G)/n^s \) is precisely \( 1 \) (this can be done using the fact that the subgroups of odd index in a non-abelian simple group are few and known); but this forces \( t \) to be \( 1 \) and \( H/Frat(H) \) to be simple.

2. Preliminaries

Let \( R \) be the ring of Dirichlet polynomials with integer coefficients:

\[
R = \left\{ f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \mid a_n \in \mathbb{Z} \text{ for all } n \geq 1, \ |\{ n : a_n \neq 0\}| < \infty \right\}.
\]

For any finite set of prime numbers \( \pi \) we may define a ring endomorphism of \( R \) as follows:

\[
\eta_\pi : R \to R, \quad f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \mapsto f^{(\pi)}(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s},
\]

where
We are mainly interested in $P_G^{(p)}(s)$, with $p$ a prime number; besides the series $P_G^{(p')} (s) := P_G^{(\pi(G) \setminus \{p\})}(s)$ will be employed in the proof of a lemma.

As it was noticed by Philip Hall [10] for any positive integer $t$, the number $P_G(t)$ gives the probability that $t$ randomly chosen elements of $G$ generate $G$. It is natural to ask whether $P_G^{(p)}(t)$ has a probabilistic interpretation.

**Proposition 1.** Let $G$ be a finite group, $p$ a prime number and $X$ a fixed Sylow $p$-subgroup of $G$. For any positive integer $t$ the number $P_G^{(p)}(t)$ gives the conditional probability that $t$ randomly chosen elements of $G$ generate $G$ together with the elements of $X$, given that their product normalizes $X$.

**Proof.** For any positive integer $t$ let us define the following set:

$$\Theta(G, X, t) = \{ (g_1, \ldots, g_t) \in G^t \mid G = \langle X, g_1, \ldots, g_t \rangle \text{ and } g_1 \cdots g_t \in N_G(X) \}.$$ 

Note that

$$S(t) = \{ (g_1, \ldots, g_t) \in G^t \mid g_1 \cdots g_t \in N_G(X) \} = \bigcup_{X \leq H} \Theta(H, X, t)$$

where clearly the right hand is a disjoint union. Hence

$$|S(t)| = |N_G(X)||G|^{t-1} = \sum_{X \leq H \leq G} |\Theta(H, X, t)|.$$

Thus, by the Möbius Inversion Formula we get

$$|\Theta(G, X, t)| = \sum_{X \leq H \leq G} \mu_G(H)|N_H(X)||H|^{t-1}.$$

Besides, set $\Omega_p = \{ H \leq G \mid |H|_p = |G|_p \}$, then

$$P_G^{(p)}(t) = \sum_{H \in \Omega_p} \frac{\mu_G(H)}{|G : H|^t}$$

$$= \sum_{P \in \text{Syl}_p(G)} \sum_{P \leq H} \frac{\mu_G(H)}{|G : H|^t} \cdot \frac{1}{|H : N_H(P)|}$$

$$= \frac{1}{|N_G(X)|} \sum_{X \leq H} \frac{\mu_G(H)N_H(X)}{|G : H|^t-1}$$

$$= \frac{|\Theta(G, X, t)|}{|G|^{t-1}|N_G(X)|}.$$
hence $P_G^{(p)}(t)$ is the conditional probability that $t$ randomly chosen elements of $G$ generate $G$ together with the elements of $X$, given that their product normalizes $X$. □

As a corollary we obtain a result which can be also deduced from the proof of the main theorem in [19].

**Corollary 2.** Let $G$ be a finite group, $p$ a prime divisor of the order of $G$ and $X \in \text{Syl}_p(G)$. Then $P_G^{(p)}(1) \neq 0$ if and only if $X \subseteq G$ and $G/X$ is a cyclic group.

We remark that if $G$ is a non-cyclic group, then $P_G(1) = 0$. Furthermore, Shareshian [19] proved that the multiplicity of one as a zero of $P_G(s)$ is at least two in most of the cases, in particular when $G$ is a non-abelian simple group. A crucial fact in the proof of our main theorem is that, on the opposite, one is a simple zero of $P_G^{(2)}(s)$ for many non-abelian simple groups.

**Proposition 3.** If $G$ is a non-abelian simple group and it is not an alternating group, then one is a simple zero for $P_G^{(2)}(s)$.

Since the proof of this proposition is long and tricky we defer it to the last section.

3. The main theorem

In this section we shall prove our main result; the proof consists of several subsequent steps so it is convenient to fix notations and hypothesis. Let $G$ be a finite non-abelian simple group and let $H$ be a finite group such that

1. $P_G(s) = P_H(s) = P(s) = \sum_{n \in \mathbb{N}} \frac{a_n}{n^s}$;
2. Frat $H = 1$.

We shall prove that $H$ is a non-abelian simple group.

We start by observing that $H$ is perfect. Indeed for any finite group $X$ and any prime number $p$ we get that $a_p(X) \equiv -1 \pmod{p}$ if and only if $O^p(X) \neq X$, (see [4, Proposition 7]).

Next we prove a couple of lemmas describing how the chief factors of $H$ look like. In these proofs a central role is played by the integer

$$m = \min \{|G:M| \mid M < G\}.$$

Clearly $a_m = -|\{M < G \mid |G:M| = m\}|$; since $P_G(s) = P_H(s)$, then $m$ is the minimal index of a (maximal) subgroup of $H$ and $a_m = -|\{M < H \mid |H:M| = m\}|$.

Lemma 4. Let $K/N$ be a chief factor of $H$. If $K/N$ is not abelian, then it is a simple group.

**Proof.** Let $K/N$ be a non-abelian chief factor of $H$, then there exists a simple group $S$ and $t \in \mathbb{N}$ such that $K/N \cong S^t$. Assume by contradiction that $t > 1$. Hence $H$ has a transitive permutation representation of degree $t$; thus it has a subgroup of index $t$. It follows that $m \leq t$.

Let $L = H/C_H(K/N)$, observe that $L$ is a primitive monolithic group and its minimal normal subgroup $T$ is isomorphic to $S^t$. Consider the following Dirichlet polynomial:
\[ Q(s) := \sum_{n \in \mathbb{N}} \frac{b_n}{n^s} \quad \text{where} \quad b_n = \sum_{|L:X|=n, XT=L} \mu_L(X). \]

It turns out that \( Q(s) \) divides \( P(s) \) in the ring of Dirichlet polynomials with integer coefficients (see for example [2]).

For any prime number \( p \in \pi(T) = \pi(S) \) define

\[ \mathcal{M}_p = \{ X < L \mid XT = L \text{ and } p \nmid |L:X| = |T:X \cap T| \}. \]

Since for any \( p \in \pi(T) = \pi(S) \) and \( P \in \text{Syl}_p(T) \) the Frattini argument gives \( L = TN_L(P) \), we get that \( \mathcal{M}_p \neq \emptyset \); set

\[ m_p = \min\{ |L:X| \mid X \in \mathcal{M}_p \} \]

and note that \( m_p > 1 \) as \( L \notin \mathcal{M}_p \). Observe that the minimality of \( m_p \) gives \( b_{m_p} \neq 0 \) for all \( p \in \pi(S) \). Furthermore, if \( X \notin \mathcal{M}_p \) and \( |L:X| = m_p \), then \( X \) is a maximal subgroup of \( L \) and it is core-free as it cannot contain \( T \) which is the unique minimal normal subgroup of \( L \). Moreover, since \( p \in \pi(T) \) and it does not divide \( |T:X \cap T| \) then \( X \cap T \) contains a Sylow \( p \)-subgroup of \( T \); it follows that \( X \cap T \cong U_t \) where \( U < S \) and it contains a Sylow \( p \)-subgroup of \( S \) (see the proof of O’Nan–Scott Theorem in [16]). As a consequence \( m_p = |L:X| = |T:X \cap T| = [S]/[U]^t = k^t \) where \( k = [S:U] \) is a proper divisor of \( |S| \) which is not divisible by \( p \); then for any prime \( q \in \pi(m_p) \) we get that \( q^t \) divides \( m_p \). Since \( Q(s) \) divides \( P(s) \), there exists a Dirichlet polynomial \( C(s) = \sum c_s/n^s \) such that \( P(s) = C(s)Q(s) \). Now let \( q \) be a prime divisor of \( m_p \); let \( u \) be the degree of \( Q(s) \) with respect to the prime \( q \), i.e. \( u = \max\{ l \mid q^l \text{ divides } n, b_n \neq 0 \} \), and denote by \( v_Q(q) \) the largest \( n \) divisible by \( q^u \) and such that \( b_n \neq 0 \). Define in the same way \( v_C(q) \). If \( n = v_Q(q)v_C(q) \), then \( n = v_p(q) \) and \( a_n \neq 0 \); moreover, since \( q^t \) divides \( b_{m_p} \), then it divides \( v_Q(q) \) and, consequently, \( n \). Hence \( q^t \) divides the order of \( G \). Since \( G \) is a non-abelian simple group with a subgroup of index \( m \), we get that \( G \cong \text{Sym}(m) \), hence \( q^t \) divides \( m! \) but this is impossible since \( m \leq t \). Indeed, \([m!]_q = q^r\) where \( r = \sum_{i=1}^h \lfloor \frac{m}{q^i} \rfloor < \frac{m}{q-1} \leq t \), and \( q^h \) is the maximal power of \( q \) less than \( m \). \( \Box \)

**Lemma 5.** Let \( K/N \) be a chief factor of \( H \). If \( K/N \) is abelian, then \( K/N \leq \text{Frat}(H/N) \).

**Proof.** Assume by contradiction that \( A = K/N \) is an abelian non-Frattini chief factor of \( H \). Since \( A \) is abelian, then \( |A| = p^r \) for some prime number \( p \). Moreover, as \( A \) is a non-Frattini chief factor, then \((1 - \frac{1}{p^r}) \) divides \( P_H^{(p^r)}(s) = P^{(p^r)}(s) = P_G^{(p^r)}(s) \), where \( c \neq 0 \) is the number of complements of \( K/N \) in \( H/N \) (see [2, Corollary 3]). Hence \( P_G^{(p^r)}(s) \neq 1 \); it follows that \( G \) is a finite non-abelian simple group with a subgroup of prime power index. The non-abelian simple groups containing subgroups of prime power index are listed by Guralnick in [9]. By scanning this list we get that \( m = p^r \), being \( m \) the minimal index of a subgroup of \( G \), in all cases except for \( G \cong \text{PSL}(2,7) \); however we proved in [6] that in this case \( H \) is a non-abelian simple group thus it does not have any abelian chief factor.

Let \( L \cong A \rtimes H/C_H(A) \) be the primitive monolithic group associated with \( A \). Set \( V = H/C_H(A) \) and observe that \( V \leq \text{Aut}(A) \cong \text{GL}(r, p) \leq \text{Sym}(p^r - 1) \). Thus \( V \leq \text{Sym}(m - 1) \) and in \( V \) the stabilizer of a point is a subgroup with index at most \( m - 1 \). Since \( m \) is the minimal
index of a subgroup of \( H \) it follows that \( V = 1 \) and \( L = A \) is an epimorphic image of \( H \), but this is impossible as \( H \) is a perfect group. \( \Box \)

**Lemma 6.** \( H \cong S_1 \times \cdots \times S_t \) where \( S_i \) is a non-abelian simple group.

**Proof.** Let us prove that \( \text{Fit} H = 1 \). Assume by contradiction that \( \text{Fit}(H) \neq 1 \). It follows that there exists an abelian minimal normal subgroup \( N \trianglelefteq H \). Since by hypothesis \( \text{Frat} H = 1 \), then \( N \) is a non-Frattini abelian chief factor of \( H \), against Lemma 5. Since \( \text{Fit} H = 1 \), then \( N = \text{F}^*(H) = E(H) = S_1 \times \cdots \times S_t \) where \( S_i \) is a non-abelian simple group. By Lemma 4 we get that \( S_i \trianglelefteq H \) for all \( i = 1, \ldots, t \), hence we may define \( \phi: H \rightarrow \prod_{i=1}^{t} \text{Aut}(S_i) \) the homomorphism induced by the conjugacy action. Note that \( \ker(\phi) = \bigcap C_H(S_i) = C_H(\text{F}^*(H)) \preceq Z(\text{F}^*(H)) \) (Bender \( F^* \)-Theorem) but \( Z(\text{F}^*(H)) = 1 \), hence \( H \cong \prod_{i=1}^{t} \text{Out}(S_i) \), but \( H \) is perfect, hence it cannot have any solvable proper quotient; it follows that \( H = \text{F}^*(H) = \prod_{i=1}^{t} S_i \). \( \Box \)

**Theorem 7.** Let \( G \) be a non-abelian finite simple group and let \( H \) be a finite group such that

1. \( PG(s) = PH(s) = P(s) = \sum_{n \in \mathbb{N}} a_n n^s \);
2. \( \text{Frat} H = 1 \).

Then \( H \) is a non-abelian simple group.

**Proof.** By Lemma 6 we get that \( PH(s) \) can be factorized as follows (see Lemma 5 and Proposition 9 in [12]):

\[
P_H(s) = \prod_{1 \leq i \leq t} \left( P_{S_i}(s) - \frac{n_i |\text{Aut}(S_i)|}{|S_i|^s} \right)
\]

where \( n_i := |\{ j \mid j < i \text{ and } S_i \cong S_j \}| \). Hence

\[
P_H^{(2)}(s) = \prod_{i=1}^{t} P_{S_i}^{(2)}(s). \tag{3.1}
\]

By Corollary 2 we get that \( P_{S_i}^{(2)}(1) = 0 \) for all \( i \in \{1, \ldots, t\} \); thus \( P_G^{(2)}(s) = P_H^{(2)}(s) \) has a zero of multiplicity at least \( t \) in \( s = 1 \). If \( G \) is not an alternating group, then we may employ Proposition 3 to conclude that \( t = 1 \) and \( H \) is a non-abelian simple group. Moreover, in the case of alternating groups the statement has been proved in [5]. \( \Box \)

**4. Proof of Proposition 3**

Let \( G \) be a non-abelian finite simple group and assume that it is not an alternating group, we shall prove that \( P_G^{(2)}(s) \) has a simple zero in \( s = 1 \); in order to obtain this result we need to prove that the derivative of \( P_G^{(2)}(s) \) does not vanish in \( s = 1 \). Set \( \Omega_2(G) := \{ H \trianglelefteq G \mid |H|_2 = |G|_2 \} \), the set of subgroups containing a Sylow 2-subgroup of \( G \), then
\[
D(s) := \frac{d}{ds} P_G^{(2)}(s) = - \sum_{H \in \Omega_2(G)} \frac{\mu_G(H) \log |G : H|}{|G : H|^s}.
\]

Assume by contradiction that \( D(1) = 0 \). Exponentiating both sides of this equality gives the following formulation of our hypothesis:

\[
\prod_{H \in \Omega_2(G)} |G : H|^\frac{\mu_G(H)}{|G : H|^s} = 1.
\] (4.1)

For any odd prime \( p \in \pi(G) \setminus \{2\} \) define the rational number \( \gamma_p(G) \) by

\[
\prod_{H \in \Omega_2(G)} |G : H|^\frac{\mu_G(H)}{|G : H|^s} = \prod_{p \in \pi(G) \setminus \{2\}} p^{\gamma_p(G)}.
\]

For any \( H \in \Omega_2(G) \) set \( \lambda_p(H) := \log_p |H| \); then for any \( p \in \pi(G) \setminus \{2\} \) we get

\[
\gamma_p(G) = \sum_{H \in \Omega_2(G)} \left( \lambda_p(G) - \lambda_p(H) \right) \frac{\mu_G(H)}{|G : H|} = \lambda_p(G) P_G^{(2)}(1) - \sum_{H \in \Omega_2(G)} \lambda_p(H) \frac{\mu_G(H)}{|G : H|} = - \sum_{H \in \Omega_2(G)} \lambda_p(H) \frac{\mu_G(H)}{|G : H|},
\]

where the last equality follows from Corollary 2. Note that Eq. (4.1) is equivalent to the following:

\[
\gamma_p(G) = 0 \quad \text{for any } p \in \pi(G) \setminus \{2\}.
\] (4.2)

We shall proceed with a case by case analysis and we shall prove that for any choice of \( G \) there exists an odd prime \( p \) such that \( \gamma_p(G) \neq 0 \) obtaining the desired contradiction. In particular, recall that for any \( H \leq G \), if \( \mu_G(H) \neq 0 \) then \( H \) is an intersection of some maximal subgroups of \( G \); in many cases it turns out that there exists an odd prime number \( p \) such that if \( H \in \Omega_2(G) \) and \( \mu_G(H) \neq 0 \), then either \( H = G \) or \( \lambda_p(H) = 0 \), hence \( \gamma_p(G) \neq 0 \). In other words, in many cases we are able to find an odd prime number \( p \in \pi(G) \) such that there does not exist any maximal subgroup of \( G \) containing both a Sylow 2-subgroup of \( G \) and an element of order \( p \).

4.1. Sporadic simple groups

By looking at the maximal subgroups of the sporadic simple groups (see [3] as a general reference, [20] for the maximal subgroups of the Baby Monster and [11] for the Monster) we find that for almost all of them there exists an odd prime \( p \) such that no maximal subgroup contains both a Sylow 2-subgroup and an element of order \( p \). In Table 1 we list all these sporadic simple groups with the corresponding prime \( p \).

In this list only McL is missing; in fact, McL has a maximal subgroup which is isomorphic to \( M_{22} \) and it contains a Sylow 2-subgroup and elements of order \( p \) for any \( p \) dividing the
order of McL. However, it turns out that the maximal subgroups of McL containing a Sylow 2-
subgroup and an element of order 11 are all isomorphic to M22. As a consequence, if \( H \leq \text{McL} \) has the same property and \( \mu_{\text{McL}}(H) \neq 0 \), then \( H \) is either isomorphic to M22 or it is intersection of maximal subgroups all isomorphic to M22; the latter cannot occur as M22 has no maximal subgroup containing both a Sylow 2-subgroup and an element of order 11. Thus \( \gamma_{11}(\text{McL}) = -1 + \frac{|M22|}{|\text{McL}|}c \) where \( c \) is the number of maximal subgroups of McL isomorphic to M22, and this number is 2\(|\text{McL} : \text{M22}|\) as McL has two conjugacy classes of subgroups isomorphic to M22; hence \( \gamma_{11}(\text{McL}) = 1 \neq 0 \).

### 4.2. Lie groups

In [17] Liebeck and Saxl determine all the primitive permutation groups of odd degree \( G \) together with their stabilizers of a point \( H \). In the case of simple groups of Lie type their result is the following.

**Theorem 8.** Let \( G = L(q) \) be a simple group of Lie type over \( GF(q) \), where \( q = r^\alpha \) and \( r \) is a prime number, and let \( H \) be a maximal subgroup with odd index in \( G \). Then one of the following occurs:

1. if \( q \) is even, then \( H \) is a parabolic subgroup of \( G \);
2. if \( q \) is odd, then one of (a), (b), (c) below holds:
   a. \( H = N_G(L(q_0)) \), where \( q = q_0^c \) and \( c \) is an odd prime.
   b. \( G \) is a classical group with natural projective module \( V = V(n, q) \), and one of the following cases occurs:
      i. \( H \) is the stabilizer of a non-singular subspace \( W \) (any subspace for \( G = \text{PSL}_n(q) \)).
      ii. \( H \) is the stabilizer of an orthogonal decomposition \( V = V_1 \oplus \cdots \oplus V_t \) with all \( V_i \) isometric (any decomposition \( V = \bigoplus V_i \) with \( \dim V_i \) constant for \( G = \text{PSL}_n(q) \)).
      iii. \( H \) is \( \Omega_7(2) \) or \( \Omega^+_8(2) \) and \( G \) is \( \text{PSO}_7(q) \) or \( \text{PSO}^+_8(q) \) respectively, \( q \) is prime and \( q \equiv \pm 3 \text{ mod 8} \).
   c. if \( G = \text{PSL}_2(q) \), and \( H \) is dihedral, Alt(4), Sym(4), Alt(5) or PGL_2(q^\frac{1}{2}).
   d. if \( G = \text{PSU}_3(5) \) and \( H = \text{M}_{10} \).
   e. \( G \) is an exceptional group; \( G \) and \( H \) are as in Table 1 in [17].

<table>
<thead>
<tr>
<th>( G )</th>
<th>( p )</th>
</tr>
</thead>
<tbody>
<tr>
<td>M_{11}</td>
<td>11</td>
</tr>
<tr>
<td>M_{12}</td>
<td>11</td>
</tr>
<tr>
<td>M_{22}</td>
<td>11</td>
</tr>
<tr>
<td>M_{23}</td>
<td>23</td>
</tr>
<tr>
<td>M_{24}</td>
<td>23</td>
</tr>
<tr>
<td>J_1</td>
<td>19</td>
</tr>
<tr>
<td>J_2</td>
<td>7</td>
</tr>
<tr>
<td>J_3</td>
<td>19</td>
</tr>
<tr>
<td>J_4</td>
<td>43</td>
</tr>
<tr>
<td>Suz</td>
<td>11 and 13</td>
</tr>
<tr>
<td>HS</td>
<td>11</td>
</tr>
<tr>
<td>Co_3</td>
<td>23</td>
</tr>
<tr>
<td>Co_2</td>
<td>23</td>
</tr>
<tr>
<td>Co_1</td>
<td>13</td>
</tr>
<tr>
<td>Fi_{22}</td>
<td>13</td>
</tr>
<tr>
<td>Fi_{23}</td>
<td>17</td>
</tr>
<tr>
<td>Fi_{24}</td>
<td>29</td>
</tr>
<tr>
<td>He</td>
<td>17</td>
</tr>
<tr>
<td>Ly</td>
<td>37 and 67</td>
</tr>
<tr>
<td>Ru</td>
<td>29</td>
</tr>
<tr>
<td>O’N</td>
<td>31</td>
</tr>
<tr>
<td>HN</td>
<td>19</td>
</tr>
<tr>
<td>Th</td>
<td>19</td>
</tr>
<tr>
<td>B</td>
<td>47</td>
</tr>
<tr>
<td>M</td>
<td>71</td>
</tr>
</tbody>
</table>
For later use we need to recall definitions and results concerning Zsigmondy primes.

**Definition 9.** A prime number $p$ is called a *primitive prime divisor* of $a^n - 1$ if it divides $a^n - 1$ but it does not divide $a^e - 1$ for any integer $1 \leq e \leq n - 1$.

The following theorem is due to K. Zsigmondy [21]:

**Theorem 10 (Zsigmondy’s Theorem).** Let $a$ and $n$ be integers greater than 1. There exists a primitive prime divisor of $a^n - 1$ except exactly in the following cases:

1. $n = 2, a = 2^{s} - 1$ (i.e. $a$ is a Mersenne prime), where $s \geq 2$.
2. $n = 6, a = 2$.

Observe that there may be more than one primitive prime divisor of $a^n - 1$; we denote by $\langle a, n \rangle$ the set of these primes. Recall that $x^n - 1 = \prod_{k|m} \Phi_k(x)$, where $\Phi_k(x)$ is the $k$th cyclotomic polynomial; therefore, if $p \in \langle a, m \rangle$, then $|a^m - 1|_p = |\Phi_m(a)|_p$. Furthermore, Lemma 2.1 in [7] states the following:

$$\Phi_m(r) = l^\epsilon \prod_{p \in \langle r, m \rangle} |r^m - 1|_p,$$

(4.3)

where $l$ is the maximum prime divisor of $m$ and $\epsilon \in \{0, 1\}$.

Moreover, the following property is rather easy to prove.

**Lemma 11.** Assume that $a \geq 2, n \geq 3$ and $(a, n) \neq (2, 6)$. Let $p \in \langle a, n \rangle$, then

1. $p \equiv 1 \mod n$.
2. If $p | a^n - 1$, then $n | m$.

In addition, we find it useful to state as a lemma some technical statements we shall use in our proofs. Let $a \in \mathbb{N}, n \in \mathbb{N}$ and $r$ a prime number, we define

$$\langle a, n, r \rangle := \begin{cases} \langle a, n \rangle \setminus \{r\} & \text{if } \langle a, n \rangle \setminus \{r\} \neq \emptyset, \\ \langle a, n \rangle & \text{otherwise.} \end{cases}$$

**Lemma 12.** Let $r$ be an odd prime number and $m \geq 4$.

1. If $p = 2m + 1$ is a prime and $\langle r, 2m, p \rangle = \{p\}$, then $|r^{2m} - 1|_p \neq p$.
2. If $p = 2m + 1$ is a prime and $\langle r, m, p \rangle = \{p\}$, then $|r^m - 1|_p \neq p$.
3. If $p = 2m - 1$ is a prime and $\langle r, 2(m - 1), p \rangle = \{p\}$, then $|r^{2(m-1)} - 1|_p \neq p^2$.

**Proof.** (1) Recall that a Zsigmondy prime $p \in \langle a, n \rangle$ is said to be a large Zsigmondy prime when either $p > n + 1$ or $p^2$ divides $a^n - 1$. By Theorem A in [7] we get that if $\langle r, 2m, p \rangle = \{p\}$, then $p$ is a large Zsigmondy prime in $\langle r, 2m \rangle$, hence $|r^{2m} - 1|_p \geq p^2$.

(2) Assume by contradiction that $|r^m - 1|_p = p$. By (4.3) we get that $\Phi_m(r) = pl^\epsilon$, being $l$ the maximum prime dividing $m$, and $\epsilon \in \{0, 1\}$; hence $2\phi(m) \leq (r - 1)^\phi(m) \leq \Phi_m(r) \leq pm$. Note that if $m = 6$, then $l = 3$ and $p = 13$, thus $\Phi_6(r) = r^2 - r + 1$ should divide 39. This implies $r \in \{3, 5\}$.
but in both cases $p$ does not divide $\Phi_\ell(r)$, against our hypothesis; hence we may assume $m \neq 6$. It is easy to check that for any $k \neq 2, 6$ we get $\phi(k) \geq \sqrt{k}$. It follows that $2^\nu m \leq pm = (2m + 1)m$ but this equality holds only for $m < 308$. As $r \geq 3$ then $\Phi_m(3) \leq \Phi_m(r)$; it is easy to check that for $4 \leq m < 308$ and $m \neq 6$, if $p = 2m + 1$ is a prime number, then $\Phi_m(3) > pl$, against the fact that $\Phi_m(r) \leq pl$.

(3) Assume by contradiction that $|r^{2(m-1)} - 1|_p = p^2$. As above, by (4.3) we obtain that $\Phi_2(m-1)(r)$ divides $p^2l$, being $l$ the maximum prime dividing $2(m - 1)$; note that $l \leq (m - 1)$. Moreover, for any $m \geq 4$ we get that $2^{\nu(m-1)} \leq p^2(m - 1) = (2m - 1)^2(m - 1)$, thus $m < 387$. Again, it can be checked that for $4 \leq m < 387$ the relation $\Phi_2(m-1)(3) \leq p^2(m - 1)$ holds only when $m \in \{4, 6, 7, 10\}$. Furthermore, for $m$ in this list there does not exist any odd prime number $r$ such that $\Phi_2(m-1)(r) \leq p^2(m - 1)$ and $|\Phi_2(m-1)(r)|_p = p^2$. \hfill \Box

Lemma 13. Let $r$ be an odd prime; define $\beta = 6$ if $r \equiv 1 \mod 4$, $\beta = 3$ if $r \equiv 3 \mod 4$. If $(r, \beta, 7) = 7$, then either $r = 5$ or $|r^6 - 1|_7 > 7^3$.

Proof. Let $|r^6 - 1|_7 = 7^m$. By (4.3) we get that $\Phi_\beta(r) = 7^m 3^\epsilon$, with $\epsilon \in \{0, 1\}$; it is easy to check that if $u \leq 3$ then the only case in which the previous equality holds is when $r = 5$. \hfill \Box

We shall go through Theorem 8 and we shall proceed with a case by case analysis showing that $\gamma_p(G) \neq 0$ where $p$ is chosen as described in Tables 2–4. Recall that here we interested only in Lie groups which are simple; we suggest [3] where it is listed which of the groups in our tables are not simple.

**Case 1.** If $G$ is untwisted, then the conjugacy classes of parabolic subgroups correspond to subsets of the set of nodes in the Dynkin diagram. If $J$ is such a subset, then the parabolic subgroup $PJ$ can be written as $PJ = QJLJH$ where $QJ$ is the unipotent radical of $PJ$, $LJH$ is the Levi factor and $H$ is a Cartan subgroup of $G$. In addition $LJ$ is a central product of groups of Lie type corresponding to the subdiagram on $J$.

Besides, if $G$ is a twisted group, then it consists of elements centralized by an automorphism $\tau$ of the corresponding untwisted group. This automorphism $\tau$ induces a non-trivial symmetry $\rho$ on the Dynkin diagram and the $J$ described above should be a $\rho$-invariant subset of the Dynkin diagram. The Levi factor of $PJ$ is obtained by taking the fixed points of the automorphism $\tau$ on the Levi factor for the corresponding untwisted group.

If $G \notin \{A_5(2), C_3(2), D_4(2), 2A_3(2)\}$ and $p$ is chosen as described in the tables above, then $\gamma_p(G) = -\lambda_p(G) \neq 0$. Indeed, no subgroup of odd index contains an element of order $p$. Otherwise there would exist a maximal parabolic subgroup $PJ = QJLJH$ of order divisible by $p$, but this is not the case. In fact, $QJ$ is a 2-group, $LJ$ is described in the tables and $\exp(H)$ divides respectively $(q - 1)$ in the untwisted case and $(q^{|\rho|} - 1)$ in the other.

We need more careful computations to handle the remaining cases. In fact, it is not possible to find a prime which behaves as above. However it is easy to compute $\gamma_p(G)$ as there are only few subgroups $K \leq G$ such that $K$ has odd index and $\mu_G(K) \neq 0$ (in particular, $K$ is a parabolic subgroup). For example, for $G = A_5(2)$ the only proper subgroups of odd index and with order divisible by 31 are those associated to the Dynkin subdiagrams of type $A_4$; as there are two conjugacy classes of these subgroups we get that $\gamma_{31}(G) = 1$. Analogously it can be checked that $\gamma_3(C_3(2)) = -2$, $\gamma_5(D_4(2)) = 1$, $\gamma_3(2A_3(2)) = -2$.

**Case 2.** Let $G$ be a classical group and $p$ as described in the tables, then the following holds.
Step 1. If $H$ is as in case (2)(a), then $p$ does not divide $|H|$.

As $C_G(L(q_0)) = 1$, then $H \leqslant \text{Aut}(L(q_0))$ but $p$ does not divide $|\text{Aut}(L(q_0))|$. Indeed, suppose, by contradiction, that $p$ divides $|\text{Aut}(L(q_0))|$. By using Lemma 11 we obtain that $p$ cannot divide neither the order of a graph automorphism (which is at most 3) nor that of a field automorphism (which divides $\alpha$). So $p$ must divide the order of an inner-diagonal automorphism, but this is impossible because of our choice of $p$ in each case. For example, let $G = B_m(q)$ and $q_0 = r^{\alpha_0}$, then, as described in the statement of Theorem 8, $\alpha = \alpha_0c$ with $c$ an odd prime. Not that any prime different from $r$ and dividing the order of an inner-diagonal automorphism divides $r^{i\alpha_0} - 1$ with $i \leqslant 2m$. If $q^m \equiv \pm 1 \mod 4$, this cannot occur since $p \in \langle r, 2m\alpha \rangle$ or $p \in \langle r, m\alpha \rangle$.

| $G$ | $|G|d$ | Levi factors | $p$ |
|-----|-------|--------------|-----|
| $A_n(q) = \text{PSL}_n(q)$ | $q^{mn/2} \prod_{i=1}^{m}(q^{j+1} - 1)$ | $A_r(q) \times A_{m-r-1}(q)$ | 31 if $(q, n) = (2, 6)$ |
| $n = m + 1$ | $d = (m + 1, q - 1)$ | $1 \leqslant r \leqslant \lfloor \frac{m-1}{2} \rfloor$ | 7 if $(q, n) = (4, 3)$ |
| $n \geqslant 3$ or $q$ even | | | 3 if $(q, n) = (8, 2)$ |
| | | | \{$(r, \alpha n)$\} else |
| | | | |
| $A_1(q) = \text{PSL}_2(q)$ | $q(q^2 - 1)$ | $\emptyset$ | $r$ if $\alpha = 1$ |
| $q$ odd | $d = 2$ | | $(r, \alpha)$ if $q \equiv 3 \mod 4$ |
| | | | $(r, 2\alpha)$ if $q \equiv 1 \mod 4$ |
| | | | |
| $B_m(q) = \Omega_n(q)$ | $q^{m^2} \prod_{i=1}^{m}(q^{2i} - 1)$ | $A_r(q) \times B_{m-r-1}(q)$ | $(r, \alpha(n-1), n)$ if $q^m \equiv 1 \mod 4$ |
| $n = 2m + 1$ | $d = 2$ | $1 \leqslant r \leqslant m - 3$ | 13 if $(q, n) = (5, 7)$ |
| $n \geqslant 5$ and $q$ odd | | $A_{m-2}(q) \times A_1(q)$ | $(r, \alpha(n-1), n)$ if $q^m \equiv 1 \mod 4$ |
| | | $A_{m-1}(q), B_{m-1}(q)$ | | |
| | | | |
| $C_m(q) = \text{PSp}_n(q)$ | $q^{m^2} \prod_{i=1}^{m}(q^{2i} - 1)$ | $A_r(q) \times C_{m-r-1}(q)$ | $(r, \alpha n)$ if $(q, n) \neq (2, 6)$ |
| $n = 2m$ | $d = (2, q - 1)$ | $1 \leqslant r \leqslant m - 4$ | 3 if $(q, n) = (2, 6)$ |
| $n \geqslant 6$ | | $A_{m-3}(q) \times B_2(q)$ | | |
| | | $A_{m-2}(q) \times A_1(q)$ | | |
| | | $A_{m-1}(q), C_{m-1}(q)$ | | |
| | | | |
| $D_m(q) = \text{PO}_n(q)$ | $q^{m(m-1)}(q^m - 1)$ | $A_r(q) \times D_{m-r-1}(q)$ | $(r, \alpha(n-2))$ if $(q, n) \neq (2, 8)$ and $q$ even |
| $n = 2m$ | $\prod_{i=1}^{m-1}(q^{2i} - 1)$ | $1 \leqslant r \leqslant m - 5$ | 5 if $(q, n) = (2, 8)$ |
| $n \geqslant 8$ | $d = (4, q^m - 1)$ | $A_{m-4}(q) \times A_3(q)$ | $(r, 4\alpha)$ if $n = 8, q$ odd |
| | | $A_{m-3}(q) \times A_1(q) \times A_1(q)$ | $(r, \alpha(n-2), n-1)$ if $q^m \equiv 1 \mod 4$ |
| | | $A_{m-1}(q)$ | $(r, \alpha n/2)$ if $q^m \equiv 3 \mod 4$ |
Table 3

| $G$    | $|G|d$                                      | Levi factors                        | $p$       |
|--------|-------------------------------------------|-------------------------------------|-----------|
| $G_2(q)$ | $q^6(q^6 - 1)(q^2 - 1)$                    | $A_1(q)$                            | ($q, 6$)  |
|        | $d = 1$                                   |                                     | $q$ even  |
|        |                                            |                                     | ($r, 6\alpha, 7$) if $q \equiv 1 \mod 4$ |
|        |                                            |                                     | ($r, 3\alpha, 7$) if $q \equiv 3 \mod 4$ |
| $F_4(q)$ | $q^{24}(q^{12} - 1)(q^8 - 1)$              | $C_3(q), B_3(q), A_1(q) \times A_2(q)$ | ($r, 12\alpha$) |
|        | $d = 1$                                   |                                     |           |
| $E_6(q)$ | $q^{36}(q^{12} - 1)(q^9 - 1)(q^8 - 1)$    | $D_5(q), A_5(q), A_2(q) \times A_2(q) \times A_1(q)$ | ($r, 12\alpha$) |
|        | $d = (3, q - 1)$                           | $A_1(q) \times A_4(q)$             |           |
| $E_7(q)$ | $q^{63}(q^{18} - 1)(q^{14} - 1)(q^{12} - 1)$ | $E_6(q), A_1(q) \times D_5(q)$, $A_2(q) \times A_4(q), D_6(q)$ | ($r, 18\alpha$) |
|        | $d = (2, q - 1)$                           | $A_3(q) \times A_2(q) \times A_1(q)$, $A_1(q) \times A_5(q), A_6(q)$ |           |
| $E_8(q)$ | $q^{120}(q^{20} - 1)(q^{24} - 1)(q^{20} - 1)$ | $E_7(q), A_1(q) \times E_6(q)$, $A_3(q) \times A_4(q), A_7(q)$ | ($r, 30\alpha$) |
|        | $d = 1$                                   | $A_4(q) \times A_2(q) \times A_1(q)$, $A_1(q) \times A_6(q), D_7(q)$ |           |
|        |                                            | $A_2(q) \times D_5(q)$             |           |

and $2m\alpha_0 = 2m\alpha/c < m\alpha$, as $c$ is an odd prime. The other cases can be discussed with similar arguments.

**Step 2.** Assume that $H$ is as in case (2)(b)(i). If $G \neq \Omega_7(5)$, then $p$ does not divide $|H|$. If $(G, p) = (\Omega_7(5), 13)$, and $p$ divides $|H|$, then either $H \simeq \Omega_6^+(5).2$ or $H \simeq (\Omega_7(5) \times \Omega_5(5)).[4]$ and in both cases there is a unique conjugacy class of these subgroups.

Set $k := \dim W$; clearly

$$|H| \text{ divides } |\text{GL}(k, q^\epsilon)||\text{GL}(n - k, q^\epsilon)|(q^\epsilon)^{k(n-k)},$$

where $\epsilon = 2$ when $G = \text{PSU}_n(q)$ and $\epsilon = 1$ otherwise. Assume that $G \neq \Omega_7(5)$ and $G \neq P\Omega_8^+(q)$. It can be easily seen that $p$ does not divide $|H|$ except when $G = \text{PSL}(2, q)$ and $q = r$, $G = \text{PSU}(n, q)$ with $n$ even and $k \in \{1, n - 1\}$ or $G$ is orthogonal. However $|\text{PSL}(2, q) : H| = q + 1$ is even; in the same way, if $G = \text{PSU}(n, q)$ and $k \in \{1, n - 1\}$ then, using Proposition 4.1.4 in [13], we get $|G : H| = q^{n-1}(q^n - 1)/(q + 1)$, which is again an even number when $n$ is even. The structure of $H$ in the orthogonal cases is described by Proposition 4.1.6 in [13]: $p$ can divide $|H|$ only if it divides the order of an orthogonal subgroup of $\text{GL}(u, q)$ with $u \in \{k, n - k\}$; applying Lemma 11 we get that this is possible only when $k \leq 2$ or $k \geq n - 2$, but in those cases the index $|G : H|$ turns out to be even.

Besides, using Proposition 4.1.6 in [13] we obtain the following: if $G = P\Omega_8^+(q)$, then $p$ cannot divide $|H|$; when $(G, p) = (\Omega_7(5), 13)$, then $H$ is as described in the statement.

**Step 3.** If $H$ is as in case (2)(b)(ii) and $p$ divides $|H|$, then
Table 4
Twisted Lie groups

| $G$ | $|G|d$ | Levi factors | $p$ |
|-----|--------|--------------|-----|
| $2A_n(q) = \text{PSU}_n(q)$ | $q^{\frac{m}{2}} \prod_{i=1}^{m} (q^{i+1} - (-1)^{i+1})$ | $A_m(q) \times A_{m-2}(q^2)$, $1 \leq r \leq \frac{m-4}{2}$ | $\langle r, 2an \rangle$ |
| $n = m + 1$ | $d = (n, q + 1)$ | $A_m(q^2)$, $2A_m(q)$ | |
| $n$ odd | | $A_m(q^2)$, $2A_m(q)$ | |
| $n$ even | | $A_m(q^2)$, $2A_m(q)$ | |
| $n \geq 4$ | | $A_m(q^2)$, $2A_m(q)$ | |
| $2B_2(q) = 2C_2(q)$ | $q^2(q^2 + 1)(q - 1)$ | $\emptyset$ | $\langle r, 4a \rangle$ |
| $r = 2$, $\alpha$ odd | $d = 1$ | | |
| $2D_m(q) = \text{PO}_m^-(q)$ | $q^{m(m-1)}(q^m + 1)$ | $A_r(q) \times 2D_{m-r-1}(q)$, $1 \leq r \leq m - 5$ | $\langle r, an \rangle$ |
| $n = 2m$ | $\prod_{i=1}^{m} (q^{2i} - 1)$ | $A_m(q)$, $2A_m(q)$ | $\langle r, 2an \rangle$ |
| $n \geq 8$ | $d = (4, q^m + 1)$ | $A_3(q)$, $2A_3(q)$ | $\langle r, 2an \rangle$ |
| $2D_4(q)$ | $q^{12}(q^8 + q^4 + 1)$ | $A_1(q^3), A_1(q)$ | $\langle r, 12a \rangle$ |
| $q^0(q - 1)(q^2 - 1)$ | $d = 1$ | | |
| $2G_2(q)$ | $q^3(q^3 + 1)(q - 1)$ | $\emptyset$ | $\langle r, 6a \rangle$ |
| $r = 3$, $\alpha$ odd | $d = 1$ | | |
| $2F_4(q)$ | $q^{12}(q^6 + 1)(q^4 - 1)$ | $2B_2(q), A_1(q)$ | $\langle r, 12a \rangle$ |
| $r = 2$, $\alpha$ odd | $q^{3}(q^3 + 1)(q - 1)$ | $d = 1$ | |
| $T = 2F_4(2)'$ | $2^{11} \cdot 3^3 \cdot 5^2 \cdot 13$ | $2B_2(q), A_1(q)$ | $\langle r, 12a \rangle$ |
| Tits group | $d = 1$ | | |
| $2E_6(q)$ | $q^{36}(q^{12} - 1)$ | $2D_3(q), A_1(q) \times 2A_2(q^2), 2A_5(q), A_2(q) \times A_1(q^2)$ | $\langle r, 18a \rangle$ |
| $(q^{6} - 1)(q^2 + 1)$ | $d = (3, q + 1)$ | | |
| $(q^3 + 1)(q^6 - 1)$ | | | |
| $(q^3 + 1)(q^6 - 1)$ | | | |

- $q$ is a prime number and $q \equiv \pm 3 \mod 8$;
- $H \simeq \begin{cases} 2^{n-1} \cdot \text{Alt}(n) & \text{if } n \text{ odd}, \\ 2^{n-2} \cdot \text{Alt}(n) & \text{if } n \text{ even}. \end{cases}$
- $(G, p) \in \{(\Omega_n(q), n), (\text{PO}_n^+(q), n - 1), (\text{PO}_n^+(q), 5).\}$

As $H$ is the stabilizer of the decomposition $V = V_1 \oplus \cdots \oplus V_t$ and $\dim V_i = k = n/t$ for each $1 \leq i \leq t$, we get that $|H|$ divides $\left|\text{GL}(k, q^\epsilon) \cdot \text{Sym}(t)\right| = \left|\text{GL}(k, q^\epsilon)\right|^t t!.$

where $\epsilon = 2$ when $G = \text{PSU}_n(q)$ and $\epsilon = 1$ otherwise. Assume $G \neq \text{PO}_n^+(q)$. The previous observation allows us to conclude that if $p$ divides $|H|$, then it must divide $t!$ and, by using Lemma 11, we conclude that this is possible only when $n = t$, $q$ is a prime and
(G, p) ∈ ((Ωn(q), n), (PΩn+(q), n − 1)). By [13] Proposition 4.2.15, H has odd index only when q ≡ ±3 mod 8, and this implies H ≃ 2p−1. Alt(n). The case G = PΩ8+(q) can be easily discussed by using Propositions 4.2.11 and 4.2.15 in [13].

**Step 4.** In cases (2)(b)(iv) and (2)(b)(v) H does not contain any element of order p.

This is easy to check.

**Step 5.** If G is a classical group, then γp(G) ≠ 0.

By the previous remarks, it follows that no proper subgroup of G with odd index has order divisible by p (hence γp(G) = −λp(G) ≠ 0) except when q is a prime, q ≡ ±3 mod 8 and (G, p) ∈ {((Ωn(q), n), (PΩn+(q), n − 1)), (PΩ8+(q), 5)}. A more careful analysis is needed in these last cases. We first assume n > 8. Any maximal subgroup H ∈ Ω2(G) such that λp(H) ≠ 0, is isomorphic to 2p−1. Alt(n). Furthermore, as Alt(n) does not contain any subgroup of odd index and order divisible by p, we get that contributions to γp(G) are given only by G itself and by subgroups isomorphic to 2p−1. Alt(n). These subgroups are all conjugated when n is odd, whereas there are two conjugacy classes in the even case. As λp(2p−1. Alt(n)) = 1, we have

$$γ_p(G) = \begin{cases} -λ_p(G) + 1 & \text{if } n \text{ is odd}, \\ -λ_p(G) + 2 & \text{if } n \text{ is even} \end{cases}$$

and the conclusion follows directly from Lemma 12. Assume now that G = Ω7(q), and H ∈ Ω2(G) with order divisible by p. If q is not a prime or q ≡ ±3 mod 8, then H = G and γp(G) = −λp(G) ≠ 0. Assume now that q is a prime, q ≡ ±3 mod 8 and q ≠ 5. By Lemma 12 we get that p ≥ 7; if p > 7, then H = G and γp(G) = −λp(G) ≠ 0. So we consider the case (G, p) = (Ω7(q), 7). There are three conjugacy classes of maximal subgroups with odd index and order divisible by 7; two of them consists of subgroups isomorphic to Ω7(2), the third contains subgroups isomorphic to 26. Alt(7); moreover, if H ∈ Ω2(G) is a proper subgroup of G with μG(H) ≠ 0 and λ7(H) ≠ 0, then either H is a maximal of G or H ≃ 26. PSL(2, 7) and in this last case μG(H) > 0 (indeed μG(H) + 1 coincides with the number of maximal subgroups of G containing H). Therefore

$$γ_7(G) = -λ_7(G) + 2λ_7(Ω_7(2)) + λ_7(2^6 \cdot \text{Alt}(7)) - a(λ_7(2^6 \cdot \text{PSL}(2, 7))) = 3 - a - λ_7(G),$$

where a ≥ 0. By Lemma 13, either (q^6 − 1)7 > q^3 (and consequently γ7(G) < 0) or q = 5. We now study (G, p) = (Ω7(5), 13). Then H is described in Step 2 and γ13(G) = 1.

Let us now consider G = PΩ8+(q) and let H ≤ G a subgroup of odd index and order divisible by p. If q is not a prime or q ≡ ±3 mod 8, then H = G and γp(G) = −λp(G) ≠ 0. Assume now that q is a prime and q ≡ ±3 mod 8. Note that if p > 7, then H = G and γp(G) ≠ 0. Assume that p ≤ 7; since p ∈ {r, 4} then p = 5. In this last case the set of subgroups ∈ Ω2(G) whose order is divisible by p consists of G itself, four conjugacy classes of maximal subgroups isomorphic with PΩ8+(2) and six conjugacy classes of subgroups isomorphic with 26. Alt(8), which have Möbius function equal 1 (see [14]). Therefore

$$γ_7(G) = -λ_7(G) + 4λ_7(PΩ_8^+(2)) - 6λ_7(2^6 \cdot \text{Alt}(8)) = -2 - λ_7(G) ≠ 0.$$
Step 6. If $G$ is an exceptional group, then $\gamma_p(G) \neq 0$.

By step 1 and analyzing the possibilities listed in [17, Table 1], we get that if $G \neq G_2(q)$, then no proper subgroup of odd index has order divisible by $p$, hence $\gamma_p(G) \neq 0$. The case $G = G_2(q)$ requires more attention when $q$ is a prime with $q = \pm 3 \mod 8$ and $p = 7$. In this case the set of subgroups in $\Omega_2(G)$ whose order is divisible by 7 consists of $G$ itself, a conjugacy class of maximal subgroups isomorphic with $G_2(2)$ and a conjugacy class of maximal subgroups isomorphic with $2^3 \cdot \text{SL}(3,2)$ (see [15]). Thus $\gamma_7(G) = -\lambda_7(G) + 2 \neq 0$ by Lemma 13.

References