A CRITERION FOR NONSOLVABILITY OF A FINITE GROUP AND RECOGNITION OF DIRECT SQUARES OF SIMPLE GROUPS

Zh. Wang, A. V. Vasil'ev, M. A. Grechkoseeva, and A. Kh. Zhurtov

UDC 512.542

Keywords: criterion of nonsolvability, simple exceptional group, element orders, recognition by spectrum.

The spectrum $\omega(G)$ of a finite group $G$ is the set of orders of its elements. The following sufficient criterion of nonsolvability is proved: if, among the prime divisors of the order of a group $G$, there are four different primes such that $\omega(G)$ contains all their pairwise products but not a product of any three of these numbers, then $G$ is nonsolvable. Using this result, we show that for $q \geq 8$ and $q \neq 32$, the direct square $Sz(q) \times Sz(q)$ of the simple exceptional Suzuki group $Sz(q)$ is uniquely characterized by its spectrum in the class of finite groups, while for $Sz(32) \times Sz(32)$, there are exactly four finite groups with the same spectrum.

Dedicated to V. D. Mazurov
on the occasion of his 80th birthday

INTRODUCTION

Let $G$ be a finite group (in what follows, all groups are assumed to be finite). The set of prime divisors of its order and the set of its element orders are denoted by $\pi(G)$ and $\omega(G)$ respectively.

1School of Science, Hainan University, Haikou, Hainan, P.R. China; wzhigang@hainanu.edu.cn.
2Sobolev Institute of Mathematics, Novosibirsk, Russia. School of Science, Hainan University, Haikou, Hainan, P.R. China; vasand@math.nsc.ru.
3Sobolev Institute of Mathematics, Novosibirsk, Russia; grechkoseeva@gmail.com.
4Kabardino-Balkarian State University, Nalchik, Russia; zhurtov_a@mail.ru.

Translated from Algebra i Logika, Vol. 61, No. 4, pp. 424-442, July-August, 2022. Russian DOI: 10.33048/alglog.2022.61.403. Original article submitted February 1, 2022; accepted March 29, 2023.
For brevity, the latter set is called the spectrum of a group $G$. Groups $G$ and $H$ are isospectral if $\omega(G) = \omega(H)$. A group $G$ is recognizable by spectrum if any group isospectral to $G$ is isomorphic to $G$. More details about recognition of simple and related groups by spectrum can be found in a recent survey [1]. The present paper concerns the recognition of direct squares of finite simple groups.

As a rule, the first step in proving the recognizability of nonsolvable groups is to establish that the groups isospectral to these are also nonsolvable, and therefore we start with the following sufficient criterion for nonsolvability of a finite group, which may be of independent interest.

**THEOREM 1.** Let $G$ be a finite group. Suppose that there is a subset $\sigma(G)$ of $\pi(G)$, which contains at least four elements and satisfies the following:

1. $pq \in \omega(G)$ for all distinct $p, q \in \sigma(G)$;
2. $pqr \notin \omega(G)$ for all pairwise distinct $p, q, r \in \sigma(G)$.

Then $G$ is nonsolvable. In particular, there are no groups of odd order satisfying these conditions.

**Remark 1.** Theorem 1 is wrong if $|\sigma(G)| = 3$. It suffices to consider a 3-primary group $G$ with $\pi(G) = \{p, q, r\}$, which is the direct product of two Frobenius groups whose kernels are a $p$-group and a $q$-group, and the complements are $r$-groups.

**Remark 2.** If $|\sigma(G)| \geq 6$, then Theorem 1 follows from [2, Thm. 1]. Indeed, let $G$ satisfy the conditions of Theorem 1 and $\sigma = \sigma(G)$. If $G$ is solvable, then it includes a Hall $\sigma$-subgroup $H$, and by condition (2), the inequality $\alpha(H) \leq 2$ holds. Here, as in [2], we denote by $\alpha(H)$ the maximum of $|\pi(x)|$ for all elements $x$ of $H$. Applying [2, Thm. 1], we obtain

$$|\pi(H)| \leq \alpha(H)(\alpha(H) + 3)/2 \leq 5,$$

a contradiction. If $|\sigma(G)| \leq 5$, then, as examples from [2, 3] show, it is impossible to derive the conclusion of Theorem 1 by applying condition (2) only.

**Remark 3.** If $\sigma(G)$ satisfies the additional condition that $p$ does not divide $q - 1$ for all $p, q \in \sigma(G)$, then the conclusion of Theorem 1 was proved true in [4, Prop. 1].

Before returning to recognition, for convenience we introduce one more concept related to element orders: the prime graph $GK(G)$ of a group $G$ is a graph with vertex set $\pi(G)$, in which two vertices $p$ and $q$ are adjacent iff $p \neq q$ and $pq \in \omega(G)$. Denote by $t(G)$ the maximum number of pairwise nonadjacent vertices in $GK(G)$. If the group $L$ satisfies the condition $t(L) \geq 4$, then it is easy to see that the direct square $L \times L$ satisfies the conditions of Theorem 1, and we derive

**COROLLARY 2.** Let $L$ be a finite group and $t(L) \geq 4$. If $G$ is a finite group such that $\omega(G) = \omega(L \times L)$, then $G$ is nonsolvable.

**Remark 4.** The condition $t(L) \geq 4$ is satisfied for the vast majority of simple groups $L$—namely, for alternating groups of degree at least 19, classical groups of dimension at least 11, all exceptional groups except $G_2(q)$, $^2D_4(q)$, and $^2F_4(2)'$, and for 18 of the 26 sporadic groups (see more in [5]).
Despite the fact that there are a huge number of simple groups recognizable by spectrum (see [1, Thm. 2.1]), there are only two examples of a recognizable group that is a direct square of a simple group: \(Sz(2^7) \times Sz(2^7)\) [6] and \(J_4 \times J_4\) [4]. The reason for this is that conventional methods for proving the nonsolvability of a group isospectral to a simple group are based on properties of its prime graph. Clearly, those methods are not applicable for proving the nonsolvability of a group isospectral to the square of a simple group, since in this case the corresponding graph is always complete. Proposition 1 in [4], mentioned in Remark 3, is a significant advance in this direction, but it is difficult to verify the conditions of that proposition for squares of arbitrary simple groups. As Corollary 2 shows, our Theorem 1 does not have this disadvantage and therefore allows us to hope for new examples of recognizable groups that are squares of simple groups.

In the present paper, we will look at direct squares of simple Suzuki groups \(Sz(q)\). Recall that \(Sz(q) = 2B_2(q)\), where \(q = 2^\alpha\) with \(\alpha\) odd, is a twisted exceptional group of Lie type. It is well known that \(Sz(q)\) is a non-Abelian simple group if \(q \geq 8\), and a Frobenius group of order \(5 \cdot 4\) if \(q = 2\). As noted, \(Sz(2^7) \times Sz(2^7)\) is uniquely (up to isomorphism) characterized by its spectrum in the class of all finite groups [6]. We prove the following generalization of this result.

**THEOREM 3.** If \(q \geq 8\) and \(q \neq 32\), then the group \(Sz(q) \times Sz(q)\) is recognizable by spectrum.

**THEOREM 4.** Let \(L = Sz(32)\). Then finite groups isospectral to \(L \times L\) are exactly groups of the form \((L \times L) \rtimes \langle \varphi \rangle\), where either \(\varphi = 1\), or \(\varphi\) normalizes each direct factor and induces a field automorphism of order 5 on it. In particular, up to isomorphism, there are four finite groups isospectral to \(L \times L\).

Recognizability by spectrum of the simple Suzuki groups themselves was established by Shi in [7]. It is also worth noting that the proof of Theorem 1 does not depend on the classification of finite simple groups, while the proof of Theorems 3 and 4 uses only the assertion, proved back in 1977 (see [8-10]), that non-Abelian simple groups whose orders are not divisible by 3 are exactly the Suzuki groups.

The paper is organized as follows. In Section 1, necessary preliminary information and results are collected. In Section 2, the nonsolvability criterion from Theorem 1 is proved. In Section 3, recognizability of the squares of Suzuki groups is established.

1. **PRELIMINARIES**

For a natural number \(n\), \(\pi(n)\) denotes the set of prime divisors of \(n\). If \(\pi\) is the set of primes, then \(\pi'\) is the set of primes not in \(\pi\).

Let \(G\) be a group. The set \(\omega(G)\) is closed under taking divisors and is therefore uniquely defined by its subset \(\mu(G)\) consisting of elements maximal with respect to the divisibility relation. The exponent of \(G\) is denoted by \(\exp(G)\). Also, \(\text{Aut} G\) and \(\text{Out} G\) are respectively the automorphism group and the outer automorphism group of \(G\), \(F(G)\) is its Fitting subgroup, and \(\text{Soc}(G)\) is its socle, i.e., the product of the minimal normal subgroups. If \(G\) is a \(p\)-group, then \(\Omega_1(G)\) is its
subgroup generated by elements of order \( p \). If a group \( B \) acts on a group \( A \), then \( A \rtimes B \) denotes their natural semidirect product.

**LEMMA 1.1** (Bang [11], Zsigmondy [12]). Let \( q, n \geq 2 \) be integers. Then either there is a prime number \( r \) that divides \( q^n - 1 \) and does not divide \( q^i - 1 \) for all \( 1 \leq i < n \), or one of the following conditions is satisfied:

1. \( q = 2 \) and \( n = 6 \);
2. \( q \) is a Mersenne prime and \( n = 2 \).

A prime number \( r \) such as in Lemma 1.1 is called a **primitive prime divisor** of \( q^n - 1 \).

**LEMMA 1.2.** If \( G \) is a solvable group, then \( t(G) \leq 2 \).

**Proof.** Otherwise, the spectrum of a Hall \( \sigma \)-subgroup of \( G \), where \( \sigma \) is the set of three vertices of the graph \( GK(G) \) that are not pairwise adjacent to each other, consists only of powers of primes, which contradicts [13, Thm. 1].

A group \( G \) is called a **cover** of a group \( L \) if there exists an epimorphism from \( G \) onto \( L \). Below are four lemmas that deliver known facts on element orders in covers of finite groups. Note that references are given to those papers in which these statements were formulated in a form convenient for further discussion. Say, Lemma 1.6 is a variation of the celebrated Hall–Higman theorem [14].

**LEMMA 1.3** [15, Lemma 10]. Let \( K \) be a normal elementary Abelian subgroup of a group \( G \), \( G/K \cong L \), and \( G_1 = K \rtimes L \) be the natural semidirect product. Then \( \omega(G_1) \subseteq \omega(G) \).

**LEMMA 1.4** [6, Lemma 4]. Let \( G = P \rtimes (R_1 \times \cdots \times R_k) \), where \( P \) is a nontrivial \( p \)-subgroup, \( R_i \) is an elementary Abelian group of order \( r_i^2 \), \( 1 \leq i \leq k \), and primes \( p, r_1, \ldots, r_k \) are pairwise distinct. Then \( G \) contains an element of order \( pr_1 \cdots r_k \).

**LEMMA 1.5** [16, Lemma 1]. Let \( P \) be a normal \( p \)-subgroup of a finite group \( G \) and let \( G/P \) be a Frobenius group with kernel \( F \) and cyclic complement \( C \). If \( p \) does not divide \( |F| \) and \( F \not\subset PC_G(P)/P \), then \( G \) contains an element of order \( p|C| \).

**LEMMA 1.6** [17, Lemma 3.6]. Let \( G = R \rtimes \langle g \rangle \), where \( R \) is an \( r \)-group, \( g \) is of prime order \( s \), \( s \neq r \), and \( [R, g] \neq 1 \). Suppose that \( G \) acts faithfully on an elementary Abelian \( p \)-group \( P \), where \( p \neq r \). Then either the natural semidirect product \( P \rtimes G \) contains an element of order \( ps \), or the following conditions are satisfied:

1. \( C_R(g) \neq 1 \);
2. \( R \) is non-Abelian;
3. \( r = 2 \) and \( s \) is a Fermat prime.

Lemma 1.7 collects well-known facts about Suzuki groups, and the next two lemmas deal with element orders in covers and automorphic extensions of these groups.

**LEMMA 1.7.** Let \( G = Sz(q) \), where \( q = 2^\alpha \geq 8 \). Then:

1. \( |G| = q^2(q-1)(q^2+1) \);
2. \( \mu(G) = \{4, q-1, q+\sqrt{2q}+1, q-\sqrt{2q}+1\} \);
(3) \( G \) includes Frobenius groups of orders \( q^2(q - 1) \), \( 4(q + \sqrt{2q} + 1) \), and \( 4(q - \sqrt{2q} + 1) \) with cyclic complements of orders \( (q - 1) \), 4, and 4 respectively;

(4) \( \text{Aut } G = G \rtimes \langle \varphi \rangle \), where \( \varphi \) is a field automorphism of \( G \) of order \( \alpha \), and if \( \psi \in \langle \varphi \rangle \), then \( C_G(\psi) \cong Sz(q^{1/|\psi|}) \);

(5) the Schur multiplier of \( G \) is trivial for \( q > 8 \) and is an elementary Abelian group of order 4 for \( q = 8 \).

**Proof.** Items (1)-(4) were established in [18], and (5), in [19].

**LEMMA 1.8.** Let \( G = Sz(q) \), where \( q \geq 8 \), and \( g \in G \) be an \( r \)-element for an odd prime \( r \). If \( G \) acts faithfully on a \( p \)-group \( V \) and \( p \) is odd, then the coset \( Vg \) of the natural semidirect product \( V \rtimes G \) contains an element of order \( p|g| \).

**Proof.** We can assume that \( V \) is an elementary Abelian \( p \)-group and consider \( V \) as a \( G \)-module.

We may also suppose that \( G \) acts irreducibly on \( V \). By [20, Thm. 1.1], the minimal annihilating polynomial of \( g \) in this representation is equal to \( x^{|g|} - 1 \). Hence there exists \( v \in V \) such that \( v(v^1 + v^2 + \cdots + v^{(q-1)}) \neq 0 \). Then \( (v^q)^{|q|} \neq 0 \). Hence \( |v^q| = p|g| \).

**LEMMA 1.9.** Let \( G = Sz(q) \), where \( q \geq 8 \).

(1) If \( \psi \) is a field automorphism of \( G \), then the set of orders of elements in the coset \( G\psi \) is equal to \( |\psi| \cdot \omega(Sz(q^{1/|\psi|})) \).

(2) If \( g \in \text{Aut } G \), then \( |g| < 2q \).

(3) If \( q \geq 32 \) and \( g \in \text{Aut } G \setminus G \), then \( |g| < q \).

**Proof.** (1) is satisfied by virtue of [21, Thm. 2].

(2), (3) Let \( q = 2^\alpha \). Then the set of element orders of \( \text{Aut } G \setminus G \) is the union of sets \( \gamma \cdot \omega(Sz(q^{1/\gamma})) \) over all nonidentity divisors \( \gamma \) of \( \alpha \). From Lemma 1.7(2) and the fact that \( \mu(Sz(2)) = \{4, 5\} \), it follows that each element of \( \omega(Sz(q^{1/\gamma})) \) is less than \( 2q^{1/\gamma} \) if \( q^{1/\gamma} > 2 \) and is at most \( 5\gamma \) if \( q = 2^\gamma \). Since \( 2\gamma q^{1/\gamma} \leq 2q \) for \( q \geq 8 \) and \( 5\gamma < 2^{\gamma+1} \) for \( \gamma \leq 3 \), and also \( 2\gamma q^{1/\gamma} \leq 6q^{1/3} < q \) for \( q \geq 32 \) and \( 5\gamma < 2^{\gamma} \) for \( \gamma \geq 5 \), we obtain the required estimates.

2. PROOF OF THEOREM 1

Let \( G \) be a minimal (w.r.t. the order) counterexample to the assertion of the theorem. Since \( G \) is a solvable group, Hall’s theorem ensures the existence of a Hall \( \sigma \)-subgroup for any \( \sigma \subseteq \pi(G) \). If we take \( \sigma \) consisting of four primes from the subset \( \sigma(G) \) given in the theorem, then the corresponding Hall \( \sigma \)-subgroup is solvable and satisfies all conditions of the theorem. In view of the assumption on the minimality of the counterexample, therefore, it must coincide with \( G \).

Thus, in what follows, \( G \) is a 4-primary solvable group satisfying the hypotheses of the theorem, i.e., \( \pi(G) = \{p, q, r, s\} \), and the spectrum of \( G \) contains all pairwise products of numbers from \( \pi(G) \) (condition (1) of the theorem), but does not contain any one of the triple products (condition (2)).

**LEMMA 2.1.** For each nontrivial element \( x \) in \( G \), the inequality \( |\pi(C_G(x))| < 4 \) holds.
Proof. Suppose that $G$ has a nontrivial element $x$ with $|\pi(C_G(x))| = 4$. We may assume that $x$ has prime order. By Lemma 1.2, $C_G(x)$ contains an element whose order is divisible by three different primes from $\pi(G)$, which contradicts condition (2) of the theorem.

**Lemma 2.2.** If $p \in \pi(G)$, then $G$ contains a noncyclic subgroup of order $p^2$.

**Proof.** Otherwise, $G$ contains, up to conjugation, a unique subgroup $P$ of order $p$. Condition (1) of the theorem yields $|\pi(C_G(P))| = 4$, where $C_G(P)$ is the centralizer of $P$ in $G$, which contradicts Lemma 2.1.

**Lemma 2.3.** Let $H$ be a Hall subgroup of $G$. Then the Fitting subgroup $F(H)$ of $H$ is not cyclic and $|\pi(F(H))| \leq 2$.

**Proof.** Denote $F(H)$ by $F$. The inequality $|\pi(F)| \leq 2$ follows from condition (2) of the theorem.

Assume that $F$ is cyclic. Then $H \neq F$ by Lemma 2.2. Since the group $H$ is solvable, we have $C_H(F) \subseteq F$ [22, Thm. 6.1.3]. Therefore the quotient group $H/F$ embeds in the group $\text{Aut} F$ and, in particular, is Abelian. If $F$ is a $p$-group, then, by Lemma 2.2, $H/F$ contains a noncyclic $p'$-group, which is impossible because the $p'$-part of $\text{Aut} F$ is cyclic. Let $\pi(F) = \{p, q\}$, where $p > q$, and let $W$ be a Sylow $q$-subgroup of $F$. Since $p > q$, a Sylow $p$-subgroup $P$ of $H$ centralizes $W$. The group $H/F$ is Abelian, so the image of $P$ in $H/F$ is normal in $H/F$, and hence $P \times W$ is normal in $H$. It follows that $P \leq F$, which contradicts Lemma 2.2.

**Lemma 2.4.** Every minimal normal subgroup of $G$ is a Sylow subgroup of $G$.

**Proof.** Let $N$ be the minimal normal $p$-subgroup of $G$, and let $H$ be a Hall $p'$-subgroup of $G$. By Lemma 2.2, the group $H$ contains an elementary Abelian $q$-subgroup of order $q^2$ for every $q \in \pi(H)$, and by Lemma 1.4, the subgroup $NH$ contains an element of order $pq$. Thus the group $NH$ satisfies the hypotheses of the theorem. Hence $G = NH$, proving the lemma.

Until the end of the proof of the theorem, we fix the following notation: $F$ is the Fitting subgroup $F(G)$ of $G$ and $H$ is a complement of $F$ in $G$, i.e., a Hall $\pi(F)'$-subgroup of $G$. By Lemma 2.4, the group $F$ is a direct product of Sylow noncyclic elementary Abelian subgroups of $G$.

**Lemma 2.5.** Let $N$ be a normal $r$-subgroup of $H$. Then either $N$ is a Sylow $r$-subgroup of $G$ and $\exp(N) = r$, or $N$ is a cyclic group of odd order, or $N$ has a characteristic subgroup of order 2.

**Proof.** If $N$ is a cyclic group and $r = 2$, then $N$ contains a characteristic subgroup of order 2. If $N$ is not cyclic and does not contain elementary Abelian subgroups of order $r^2$, then $N$ is a generalized quaternion subgroup in view of [22, Thm. 5.4.10], and again it has a characteristic subgroup of order 2. Hence, we may assume that $N$ includes an elementary Abelian subgroup of order $r^2$. By Lemma 1.4, the subgroup $FN$ contains an element of order $rp$ for every $p \in \pi(F)$. Arguing further as in Lemma 2.4, we conclude that $N$ is a Sylow subgroup of $H$, and so of $G$.

By the minimality of $G$, there are no proper noncyclic characteristic Abelian subgroups in $N$. If $N$ is Abelian, then $N = \Omega_1(N)$ and $\exp(N) = r$, as required. Let $N$ be non-Abelian. Then $Z(N)$ is a cyclic group, and for $r = 2$, $N$ has a characteristic subgroup of order 2. If $r \neq 2$, then in virtue
of [22, Thm. 5.5.3] the group $N$ is the central product of a cyclic group and an extraspecial group $M$ of exponent $r$. Then $N = \Omega_1(N) = M$, and we are done.

Recall that $|\pi(F)| \leq 2$ by Lemma 2.3. Therefore Theorem 1 will follow from the next two lemmas.

**Lemma 2.6.** $|\pi(F)| \neq 1$.

**Proof.** Assume the opposite. Then $F$ is a noncyclic elementary Abelian $p$-group which is a Sylow subgroup of $G$, and $H$ is a Hall $p'$-subgroup of $G$.

Let $N$ be a normal primary subgroup of $H$. If $N$ has a characteristic subgroup of order 2, then this subgroup is central in $H$. Therefore $G$ contains an element of order $2rs$ forbidden by condition (2), where $\{r, s\} = \pi(G) \setminus \{2, p\}$. Applying Lemma 2.5, we see that either $N$ is a Sylow subgroup of $G$ of prime exponent, or $N$ is a cyclic group of odd order.

Consider now the Fitting subgroup $U = F(H)$ of $H$. By Lemma 2.3, the group $U$ is not cyclic. Hence, one of the Sylow subgroups of $U$, say, a $q$-subgroup, is not cyclic. Thus, by the previous paragraph, $U$ contains a Sylow $q$-subgroup $Q$ of $G$ and $Q$ is of prime exponent. Below we consider separately the cases when $|\pi(U)| = 2$ and $|\pi(U)| = 1$.

Let $\pi(U) = \{q, r\}$ and $V$ be a Sylow $r$-subgroup of $U$. Then $U = Q \times V$. If $V$ is also a Sylow subgroup of $G$, then, applying Lemma 1.4, we see that $pqr \in \omega(G)$. Hence $V$ is a cyclic group and $r \neq 2$.

Let $S$ be a Sylow $s$-subgroup of $G$, where $\{s\} = \pi(G) \setminus \{p, q, r\}$. If $C_S(V)$ contains a noncyclic elementary Abelian subgroup, then $C_S(V)$ contains an element that centralizes nontrivial elements in both $Q$ and $V$, and so $H$ contains an element of forbidden order $qrs$. Therefore $C_S(V)$ has at most one subgroup of order $s$. In particular, $C_S(V) < S$ due to Lemma 2.2. On the other hand, $S/C_S(V) = N_S(V)/C_S(V)$ is a cyclic group of order dividing $r - 1$. Hence $C_S(V) \neq 1$ and $s < r$. Denote by $Z$ the unique subgroup of order $s$ in $C_S(V)$. It is clear that $Z \leq S$, and therefore $Z \leq Z(S)$.

Let $J$ be a Hall $\{r, s\}$-subgroup of $H$ containing $S$ and let $\overline{J} = J/V$. The images of other subgroups of $J$ in $\overline{J}$ will also be denoted by using an overbar.

Let $\overline{K} = F(\overline{J})$ and $\overline{C} = \overline{C_S(V)} \cap \overline{K}$. Then $\overline{C}$ is normal in $\overline{J}$ because

$$\overline{C} = \overline{C_J(V)} \cap (\overline{S} \cap \overline{K}),$$

while $\overline{C_J(V)}$ and $\overline{S} \cap \overline{K}$ are normal subgroups of $\overline{J}$. Assume that $\overline{Z} \not\cong \overline{K}$. Since $C_{\overline{J}}(\overline{K}) \leq \overline{K}$, $\overline{K}$ must contain a Sylow $r$-subgroup $\overline{T}$ on which $\overline{Z}$ acts nontrivially. Applying Lemma 1.6 to the action of $\overline{T} \times \overline{Z}$ on $Q$ and noting that $r \neq 2$, we obtain an element of order $sq$ in $QZ$. However, $QZ$ centralizes $V$, so $G$ contains an element of forbidden order $sqr$. Thus $\overline{Z} \leq \overline{K}$, whence $\overline{Z} \leq \overline{C}$, and $\overline{Z}$ is normal in $\overline{J}$ as the only subgroup of $\overline{C}$ of order $s$.

Let $R$ be a Sylow $r$-subgroup of $J$ (and $G$). Then $[\overline{R}, \overline{Z}] = 1$ since $r > s$. Therefore $Z$ stabilizes the normal series $1 < V < R$ and so acts trivially on $R$ [22, Thm. 5.3.2]. Consider the action of $R \times Z$ on $QF$. The group $Z$ acts on $Q$ without fixed points, for otherwise $G$ would contain an
element of order $sqr$. Hence $QZ$ is a Frobenius group, and since $C_G(F) = F$, it acts on $F$ faithfully. Therefore $C_F(Z) \neq 1$ in view of Lemma 1.5. The group $R$ acts on $C_F(Z)$, and applying Lemmas 2.2 and 1.4, we obtain an element of order $rpg$, a contradiction.

Now let $\pi(U) = \{q\}$, i.e., $U = Q$ is a Sylow $q$-subgroup of $G$. As above, suppose $J$ is a Hall $\{r, s\}$-subgroup of $H$. Then $G = FUJ$.

Put $V = F(J)$. By Lemma 2.3, the group $V$ is not cyclic. Hence one of its Sylow subgroups, say, the $r$-subgroup $W$, is not cyclic. Denote by $S$ a Sylow $s$-subgroup of $J$ (and $G$).

Assume that $r = 2$ and $W$ contains a unique involution $z$. Then the whole group $S$ centralizes $z$. If $C_U(z) = 1$, then $U \cong \langle z \rangle$ is a Frobenius group and $C_F(z) \neq 1$ by Lemma 1.5. Hence, at least one of the centralizers $C_U(z)$ and $C_F(z)$ is nontrivial. That centralizer is invariant under the action of $S$, and applying Lemma 1.4, therefore, we obtain an element of order $2sq$ or $2sp$, a contradiction. Arguing in the same way as in Lemma 2.5, we conclude that $W$ is a Sylow $r$-subgroup of $G$, and either $W$ is Abelian or the order of $W$ is odd.

Let $\pi(V) = \{r, s\}$ and $T$ be a Sylow $s$-subgroup of $V$, i.e., $V = W \times T$. Repeating the argument of the previous paragraph about the action of $S \times \langle z \rangle$ on $UF$ with $W$ instead of $S$ and any element $x \in T$ instead of $z$, we arrive at a contradiction.

Thus $V = W$. There is a nontrivial element $x$ of order $s$ in $S$ such that $C_V(x) \neq 1$. On the other hand, $[V, x] \neq 1$. The group $V \cong \langle x \rangle$ acts faithfully on $U$ and on $F$. By Lemma 1.6, we conclude that $C_U(x) \neq 1$ and $C_F(x) \neq 1$. Hence $|\pi(C_G(x))| = 4$. This contradiction completes the proof of the lemma.

**Lemma 2.7.** $|\pi(F)| \neq 2$.

**Proof.** Suppose the contrary. Then $F = P \times Q$, where $P$ and $Q$ are noncyclic elementary Abelian Sylow $p$-subgroup and $q$-subgroup of $G$, and $H$ is a Hall $\{r, s\}$-subgroup of $G$.

Assume first that $H$ is of odd order, and let $U = F(H)$ be the Fitting subgroup of $H$. By Lemma 2.3, the group $U$ is not cyclic. Therefore, applying Lemma 2.5, we conclude that $U$ contains a Sylow subgroup of $G$, say, an $r$-subgroup $R$, and $R$ has exponent $r$. Denote by $S$ a Sylow $s$-subgroup of $H$ (and $G$). By the minimality of $G$, the group $S$ is an elementary Abelian group of order $s^2$.

In view of Lemma 1.4, there are $x, y \in S$ such that $C_P(x) \neq 1$ and $C_Q(y) \neq 1$. Condition (2) implies that $C_Q(x) = C_P(y) = 1$. In particular, $x \neq y$. If one of these elements, say $x$, centralizes $R$, then $R$ acts on $C_P(x)$, and we obtain an element of order $prs$. Hence $[R, x] \neq 1$ and $[R, y] \neq 1$.

If $[R, x] \cap C_R(Q) = 1$, then, by Lemma 1.6, we have $C_Q(x) \neq 1$, which is not the case. In particular, $C_R(Q) > 1$. The group $C_R(Q)$ is cyclic; otherwise, by Lemma 1.4, $G$ contains an element of order $rpg$. Thus $C_R(Q)$ is of order $r$ and $[R, x] = C_R(Q)$. Similarly, $[R, y] = C_R(P)$. It is clear that $C_R(Q) \cap C_R(P) = C_R(F) = 1$, so $R$ includes a subgroup $[R, x] \times [R, y]$ of order $r^2$. Let $g, h \in R$ be such that $[g, x] \neq 1$ and $[h, y] \neq 1$. Then $[g, xy] = [g, y][g, x]^y \notin [R, y]$ and $[h, xy] = [h, y][h, x]^x \notin [R, x]$. Consequently, $[R, xy]$ lies neither in $C_R(P)$ nor in $C_R(Q)$, and hence there is an element of order $pqrs$ in $G$, a contradiction.
Now let $2 \in \pi(H)$ and let $s$ be the only odd prime divisor of the order of $H$. By Lemma 2.2, the group $H$ contains a noncyclic subgroup $T$ of order 4. If $t$ is an involution in $T$, then condition (2) of the theorem yields $C_P(t) = 1$ or $C_Q(t) = 1$. From $P$ and $Q$, we now choose a group on which two different involutions $t$ and $u$ of $T$ act fixed-point-freely. Let it be $P$. Then the involution $v = tu$ centralizes $P$ and inverts $Q$. The involution $v^h$ has the same property for every $h \in H$. If $v^h \neq v$, then we obtain an element of forbidden order in $G$: 2pq if the dihedral group $D = \langle v, v^h \rangle$ contains an elementary Abelian subgroup of order 4, and $spq$ otherwise. Thus the involution $v$ lies in the center of $H$. The group $PH$ contains an element $x$ of order $ps$, so $xv$ is an element of order $2ps$. This contradiction proves the lemma, completing the theorem.

3. RECOGNITION OF SQUARES OF SUZUKI GROUPS

In this section, we will prove Theorems 3 and 4. We will use the basic properties of Suzuki groups listed in Lemma 1.7 without explicit reference to that lemma.

Let $L = Sz(q)$, where $q = 2^a \geq 8$. The set $\mu(L)$ consists of numbers $m_1(q) = 4$, $m_2(q) = q - 1$, $m_3(q) = q - \sqrt{2q} + 1$, and $m_4(q) = q + \sqrt{2q} + 1$. Note that $m_3(q)m_4(q) = q^2 + 1$, $q/2 < m_i(q) < 2q$ for $i \neq 1$, and $(m_i(q), m_j(q)) = 1$ for $i \neq j$. In particular, $t(L) = 4$.

Let $G$ be a finite group with $\omega(G) = \omega(L \times L)$. Then

$$\mu(G) = \{m_i(q) \cdot m_j(q) \mid 1 \leq i, j \leq 4 \text{ and } i \neq j\}.$$ 

By virtue of Corollary 2, the group $G$ is nonsolvable. Let $K$ be the solvable radical of $G$ and $G/K = G/K_i$. Then $\text{Soc}(G) \leq G \leq \text{Aut}(\text{Soc}(G))$. Since $3 \not\in \pi(G)$, it follows that $\text{Soc}(G) = L_1 \times L_2 \times \cdots \times L_k$, where $L_i = Sz(2^{a_i})$ and $a_i \geq 3$ for all $1 \leq i \leq k$.

For every $i$, the number $2^{a_i} - 1$ must divide the exponent of $G$, which in turn divides $4(2^{4a_i} - 1)$; so all $a_i$ divide $a$. It is clear that $m_2(2^{a_i})$ divides $m_2(q)$. Also it is not hard to verify that, depending on the residue of $\alpha/a_i$ modulo 8, one of the numbers $m_3(2^{a_i})$ and $m_4(2^{a_i})$ divides $m_3(q)$ and the other divides $m_4(q)$ (cf. [23, p. 18]). These divisibilities immediately imply that $k \leq 2$, since otherwise $4ps \in \omega(G) \setminus \omega(L \times L)$ for some prime divisors $p$ and $s$ of $m_2(2^{a_2})$ and $m_3(2^{a_3})$.

In what follows, we fix some primitive divisors $r_2$ and $r_4$ of the numbers $2^a - 1$ and $2^{4a} - 1$, respectively, and note that each of them is greater than $a$. In particular, none of them divides $|\text{Aut} L_i/L_i|$ for any $i$.

Let $k = 1$. Suppose $a_1 \neq a$. Then $r_2$ and $r_4$ do not divide $|G|$, and so $r_2r_4 \in \omega(K)$. It is clear that $r_4$ divides $m_i(q)$ for some $i \in \{3, 4\}$. Let $j \in \{3, 4\}$ and $j \neq i$. Since $m_j(q) > q/2 = 2^{a-1} > 2^{a+1}$, it follows from Lemma 1.9(2) that $m_j(q) \not\in \omega(G)$. On the other hand, $r_2m_j(q), r_4m_j(q) \in \omega(G)$, and hence $r_2s, r_4s \in \omega(K)$ for some prime divisor $s$ of $m_j(q)/(m_j(q), \exp(G))$. Similarly, if $T$ is a Sylow 2-subgroup of $G$, then $2s \in \omega(KT)$. Thus the solvable group $KT$ satisfies the hypothesis of Theorem 1 with $\sigma(KT) = \{r_2, r_4, 2, s\}$, a contradiction.

Therefore $a_1 = a$ and $L_1 = L$. Let $\alpha \geq 5$. We denote by $G_1$ the preimage of the group $L$ in $G$ and use induction on the order of $K$ to show that $L$ is a direct factor in $G_1$. Let $V$ be a minimal
It is clear that \( \frac{p}{\omega(G)} \) by applying Lemma 1.5 to a Frobenius subgroup of order \( 4m_3(q) \).

If \( p \) is odd, then, by Lemma 1.8, \( G \) contains an element of order \( p^{l+1} \), where \( p^l \) is the greatest power of \( p \) in \( \omega(L) \). Therefore \( C_H(V) = H \). In view of \( \alpha \geq 5 \), the Schur multiplier of \( L \) is trivial, and so \( H = V \times L \). Since \([K,L] \leq V\), the equalities \([K,L,L] = 1\) and \([L,K,L] = 1\) hold, and hence \([L,K] = [L,L,K] = 1\).

Thus \( K \times L = G_1 \leq G \), and so \( \omega(K) \subseteq \omega(L) \). As above, we choose \( j \in \{3,4\} \) so that \( r_4 \) does not divide \( m_j(q) \), and let \( s \in \pi(m_j(q)) \). By virtue of Lemma 1.2 and the inclusion \( \omega(K) \subseteq \omega(L) \), the intersection \( \pi(K) \cap \{2,r_2,r_4,s\} \) does not contain more than two numbers. On the other hand, the numbers \( 2, r_2, \) and \( r_4 \) do not divide \( |G/(K \times L)| \); therefore, two of them must divide \( |K| \). Denote by \( p \) the third one. Then \( pm_j(q) \) is coprime to \( [K] \), so \( pm_j(q) \in \omega(G) \). Applying Lemma 1.9(3), we conclude that \( q > pm_j(q) > pq/2 \), a contradiction.

Let \( \alpha = 3 \). Then the Schur multiplier of \( L \) has order 4, \( m_2(q) = 7 \), \( m_3(q) = 5 \), and \( m_4(q) = 13 \).

It is clear that \( G = \text{Soc}(G) \). Suppose \( 7 \not\in \pi(K) \) and let \( x \in G \) be an element of order 7. Since \( \langle x \rangle \) is a Sylow subgroup of \( G \), we have \( \pi(C_K(x)) = \{2,5,13\} \). By Lemma 1.2, \( C_K(x) \) contains an element of order \( pr \) for distinct prime \( p \) and \( r \). Hence \( 7pr \in \omega(G) \), a contradiction. Hence \( 7 \in \pi(K) \). Similarly, \( 5,13 \in \pi(K) \).

Arguing as in the case \( \alpha \geq 5 \), we conclude that either \( L \) is again a direct factor, i.e., \( G = K \times L \), or there is a normal solvable subgroup \( W \) of \( G \) such that the quotient group \( G/W \) is the central product of a solvable group \( N \) and a perfect central extension \( M \) of \( L \), and the center \( Z(M) \) is nontrivial. In the first case, applying Lemma 1.2, we see that the product of two of the numbers \( 5,7,13 \) lies in \( \omega(K) \), and hence the product of all the three numbers lies in \( \omega(G) \), a contradiction.

Let us consider the second case. Since \( Z(M) \neq 1 \), there are no odd numbers in \( \pi(N) \); in particular, \( 7 \in \pi(W) \). Denote by \( J \) the preimage of \( M \) in \( G \). By the Frattini argument, we may assume that a Sylow 7-subgroup \( P \) of \( W \) is normal in \( J \). Also if we replace \( G \) by \( G/\Phi(P) \) we may assume that \( P \) is elementary Abelian. Finally, by Lemma 1.3, we can suppose that \( J \) is a split extension of \( P \) by \( \bar{J} \). If \( C_J(P) = J \), then \( 2 \cdot 5 \cdot 7 \in \omega(G) \), a contradiction.

Let \( C_J(P)W/W \leq Z(M) \) and let \( R \) be a Sylow 2-subgroup of \( \bar{J} \). By the Frattini argument, \( N_{\bar{J}}(R) \) contains an element \( g \) of order 7, and we let \( T = R \times \langle g \rangle \). Since \( C_T(P)W/W \leq Z(M) \), it follows that there is a homomorphism from \( T/C_T(P) \) onto a Borel subgroup of \( L \), which is a Frobenius group of order \( 2^6 \cdot 7 \). Hence an element of \( T/C_T(P) \) of order 7 acts on the normal Sylow 2-subgroup of \( T/C_T(P) \) nontrivially. Applying Lemma 1.6 to the action of \( T/C_T(P) \) on \( P \) and noting that 7 is not a Fermat prime, we obtain an element of order 49 in \( G \). This contradiction completes the proof for the case \( k \neq 1 \).

Thus \( k = 2 \). We suppose \( K \neq 1 \) and show that \( \omega(G) \not\subseteq \omega(L \times L) \). There is no loss of generality in assuming that \( K \) is an elementary Abelian \( p \)-group. By Lemma 1.3, we can also think of \( L_1 \times L_2 \) as being a subgroup of \( G \). Suppose that \( p \neq 2 \) or \( L_1 \times L_2 \) centralizes \( K \). There are odd \( r \in \pi(L_1) \).
and \( s \in \pi(L_2) \) such that \( prs \not\in \omega(L \times L) \), and we let \( x \in L_1 \) and \( y \in L_2 \) be elements of orders \( r \) and \( s \) respectively. Applying Lemma 1.8 to \( L_1 \), we conclude that \( C_K(x) \neq 1 \). The group \( L_2 \) acts on \( C_K(x) \), and appealing to Lemma 1.8 again, we see that \( y \) has a fixed point in \( C_K(x) \). Thus \( prs \in \omega(G) \). Hence \( p = 2 \) and, say, \( L_1 \), acts on \( K \) faithfully. Since \( L_1 \) has Frobenius subgroups with kernels of orders \( m_3(q) \) and \( m_4(q) \) and cyclic complements of order 4, it follows by Lemma 1.5 that \( G \) contains an element of order 8.

Therefore \( K = 1 \). If at least one of the numbers \( \alpha_1 \) and \( \alpha_2 \) is distinct from \( \alpha \), then \( r_2 r_4 \not\in \omega(G) \). Hence, \( L_1 \cong L_2 \cong L \) and \( \text{Aut}(L_1 \times L_2) = (L_1 \times L_2) \rtimes (\langle \varphi \rangle \langle \tau \rangle) \), where \( \varphi \) is some fixed automorphism of \( L_1 \) of odd order \( \alpha \) and \( \tau \) is the automorphism of \( L_1 \times L_2 \) of order 2 interchanging the components. If \( 2 \in \pi(G/\text{Soc}(G)) \), then we may assume that \( \tau \in G \), and taking \( g \) to be an element of \( L_1 \) of order 4, we see that \( 8 = |g\tau| \in \omega(G) \), which is false. Therefore \( G \leq \text{Aut}L_1 \times \text{Aut}L_2 \).

Suppose \( G \neq L_1 \times L_2 \). Then \( G \) contains \( \psi = (\psi_1, \psi_2) \), where \( \psi_i \) is a field automorphism of \( L_i \), \( i = 1, 2 \), and \( |\psi| = p \) is a prime. It is clear that

\[
C_{L_1 \times L_2}(\psi) = C_{L_1}(\psi_1) \times C_{L_2}(\psi_2) \cong S_2(q^{1/|\psi_1|}) \times S_2(q^{1/|\psi_2|}).
\]

Assume that \( q^{1/|\psi_i|} > 2 \) for some \( i \). Then there is \( s \in \pi(C_{L_i}(\psi_i)) \) such that \( s \neq 2 \), \( s \neq p \), and \( ps \not\in \omega(L) \). For this prime \( s \), we have \( 2ps \in \omega(G) \setminus \omega(L \times L) \), a contradiction. It follows that \( |\psi_1| = |\psi_2| = p \) and \( q = 2^p \). On the other hand, \( p \in \pi(G) = \pi(L) \), and so \( p \) divides \((2^p - 1)(2^{2p} + 1)\), which is possible only for \( p = 5 \). Thus if \( q \neq 2^5 \), then \( G \cong L \times L \), completing the proof of Theorem 3.

Let \( q = 2^5 \) and \( M = (L_1 \times L_2) \rtimes (\psi) \), where \( \psi \) induces a field automorphism of order 5 on each factor \( L_i \). We claim that \( \omega(M) = \omega(L \times L) \). Let \( g \in M \setminus (L_1 \times L_2) \). Then \( g = (g_1\psi_1, g_2\psi_2) \), where \( |\psi_1| = |\psi_2| = 5 \). By Lemma 1.9(1), for every \( i = 1, 2 \), the order of \( g_i\psi_i \) lies in \( 5 \cdot \omega(S_2(2)) \) and, hence, divides 20 or 25. Since the order of \( g \) is equal to the least common multiple of \( |g_1\psi_1| \) and \( |g_2\psi_2| \), this order divides 100 and, therefore, lies in \( \omega(L \times L) \).

It remains to find the number of pairwise nonisomorphic groups \( M \). Groups \( A \) and \( B \) such that \( L_1 \times L_2 \leq A, B \leq \text{Aut}(L_1 \times L_2) \) are isomorphic iff their images in \( \text{Out}(L_1 \times L_2) \) are conjugate. Recall that \( \text{Aut}(L_1 \times L_2) = (L_1 \times L_2) \rtimes (\langle \varphi \rangle \langle \tau \rangle) \). We denote the images of \( \varphi \) and \( \tau \) in \( \text{Out}(L_1 \times L_2) \) by the same symbols. Then the image of \( M \) in \( \text{Out}(L_1 \times L_2) \) is the cyclic group \( X_l \) generated by \( (\varphi^l, \varphi^{-l}) \) for some \( 1 \leq l \leq 4 \). It is clear that \( X_l \) and \( X_m \), with \( l \neq m \), are conjugate if \( X_l^\tau = X_m \). It follows that \( X_2 \) and \( X_3 \) are conjugate, while \( X_1 \), \( X_2 \), and \( X_4 \) are pairwise not conjugate. Thus, up to isomorphism, there are four groups isospectral to \( L \times L \): \( L_1 \times L_2 \) and the full preimages of \( X_l \), with \( l = 1, 2, 4 \), in \( \text{Aut}(L_1 \times L_2) \). This completes the proof of Theorem 4.

Acknowledgments. The authors would like to express their deep gratitude and admiration to V. D. Mazurov whose article [6] served as a source of inspiration for this paper. Thanks also are due to A. A. Buturlakin and the reviewer for valuable comments.

REFERENCES

1. M. A. Grechkoseeva, V. D. Mazurov, W. Shi, A. V. Vasil’ev, and N. Yang, “Finite groups isospectral to simple groups,” Comm. Math. Stat., 2022; DOI: 10.1007/s40304-022-00288-5.
2. J. Zhang, “Arithmetical conditions on element orders and group structure,” *Proc. Am. Math. Soc.*, 123, No. 1, 39-44 (1995).

3. T. M. Keller, “Solvable groups with a small number of prime divisors in the element orders,” *J. Alg.*, 170, No. 2, 625-648 (1994).

4. I. B. Gorshkov and N. V. Maslova, “The group $J_4 \times J_4$ is recognizable by spectrum,” *J. Alg. Appl.*, 20, No. 4 (2021), Article ID 2150061.

5. A. V. Vasil’ev and E. P. Vdovin, “Cocliques of maximal size in the prime graph of a finite simple group,” *Algebra and Logic*, 50, No. 4, 291-322 (2011).

6. V. D. Mazurov, “Recognition of finite nonsimple groups by the set of orders of their elements,” *Algebra and Logic*, 36, No. 3, 182-192 (1997).

7. W. Shi, “A characterization of Suzuki’s simple groups,” *Proc. Am. Math. Soc.*, 114, No. 3, 589-591 (1992).

8. N. D. Podufalov, “Finite simple groups without elements of sixth order,” *Algebra and Logic*, 16, No. 2, 133-135 (1977).

9. L. M. Gordon, “Finite simple groups with no elements of order six,” *Bull. Aust. Math. Soc.*, 17, No. 2, 235-246 (1977).

10. L. R. Fletcher, B. Stellmacher, and W. B. Stewart, “Endliche Gruppen, die kein Element der Ordnung 6 enthalten,” *Q. J. Math., Oxford II. Ser.*, 28, No. 110, 143-154 (1977).

11. A. S. Bang, “Talteoretiske undersøgelser,” *Tidsskrift for Math.*, 5. Ser., 4, 70-80 (1886); 4, 130-137 (1886).

12. K. Zsigmondy, “Zur Theorie der Potenzreste,” *Monatsh. Math. Phys.*, 3, 265-284 (1892).

13. G. Higman, “Finite groups in which every element has prime power order,” *J. London Math. Soc.*, 32, 335-342 (1957).

14. P. Hall and G. Higman, “On the $p$-length of $p$-soluble groups and reduction theorems for Burnside’s problem,” *Proc. London Math. Soc.*, III. Ser., 6, No. 1, 1-42 (1956).

15. A. V. Zavarnitsine and V. D. Mazurov, “Element orders in coverings of symmetric and alternating groups,” *Algebra and Logic*, 38, No. 3, 159-170 (1999).

16. V. D. Mazurov, “Characterizations of finite groups by sets of orders of their elements,” *Algebra and Logic*, 36, No. 1, 23-32 (1997).

17. A. V. Vasil’ev, “On finite groups isospectral to simple classical groups,” *J. Alg.*, 423, 318-374 (2015).

18. M. Suzuki, “On a class of doubly transitive groups,” *Ann. Math.*, II. Ser., 75, No. 1, 105-145 (1962).
19. J. L. Alperin and D. Gorenstein, “The multiplicators of certain simple groups,” *Proc. Am. Math. Soc.*, **17**, 515-519 (1966).

20. P. H. Tiep and A. E. Zalesski, “Hall–Higman type theorems for exceptional groups of Lie type, I,” *J. Alg.*, **607**, Part A, 755-794 (2022).

21. M. A. Grechkoseeva, “Orders of elements of finite almost simple groups,” *Algebra and Logic* **56**, No. 6, 502-505 (2018).

22. D. Gorenstein, *Finite Groups*, Harper’s Ser. Modern Math., Harper & Row, New York (1968).

23. M. S. Lucido, “Prime graph components of finite almost simple groups,” *Rend. Semin. Mat. Univ. Padova*, **102**, 1-22 (1999).