

On Trofimov's Group-Theoretic Numbers (Kourovka Notebook Problem 2.78): The Soluble and the Absolutely Simple Numbers Form Finite Sets

Alper Ferudun*

October 21, 2026

Abstract

P. I. Trofimov (Kourovka Notebook, Problem 2.78, 1967) calls the set of all subgroups of one order of a finite group G an IE -system if it contains a non-normal subgroup, so that the number $k(G)$ of IE -systems is the number of orders of non-normal subgroups of G . A positive integer k is a soluble group-theoretic number if every finite group with exactly k IE -systems is soluble, and an absolutely simple one if some simple group, but no non-soluble non-simple group, has exactly k IE -systems; Trofimov asks whether these two sets are finite, and whether some number is composite (attained by no simple group) but not soluble. We give a partial answer: both sets are finite (the soluble numbers are exactly 1, 2, 3, 4, 5, 6, 8, and the absolutely simple numbers are 7 and possibly 11); the second question stays open (a composite non-soluble number would exceed 323). Our main result is that every $k \geq 9$ with $k \neq 11$ is $k(G)$ for a non-soluble non-simple group G : a group $A_5 \times H$ with metabelian H and a prime from Dirichlet's theorem for large k , and one of 397 explicit groups, checked by computer, for $9 \leq k \leq 406$. Together with $k(\text{PSL}(2, 13)) = 11$ this alone gives the finiteness of both sets. The exact lists also use the theorem that a non-soluble group has $k(G) \geq 7$, with equality only for A_5 , and $k(G) \neq 8$; it is in print (Zhong 2005; Shi, Zhang and Liang 2015), we know these papers only from their reviews and abstracts, and we include a proof based on Thompson's classification of the minimal simple groups. The bound 323 comes from computational data on the groups $\text{PSL}(2, q)$. No printed answer to the problem was found in the sources we searched. This is an unrefereed note.

1 Introduction

1.1 The problem

All groups in this note are finite. For a group G and an integer $n \geq 1$ consider the set of all subgroups of G of order n . Trofimov [KM26, Problem 2.78] calls “any set of all subgroups of the same given order” of G that contains at least one non-normal subgroup an $IE_{\bar{n}}$ -system of G ; we say IE -system. Different orders give different sets, so the number of IE -systems of G is

$$k(G) = \#\{n \geq 1 : G \text{ has a non-normal subgroup of order } n\}.$$

A positive integer k is called a soluble (non-soluble; simple; composite; absolutely simple) “group-theoretic number” if, respectively, (i) every finite group with exactly k IE -systems is soluble; (ii) at least one non-soluble finite group has exactly k IE -systems; (iii) at least one simple finite group has

*Mercury Software GmbH. Email: alper@mercurycodelab.com. GitHub: <https://github.com/AlperTheKing>. Unrefereed preprint. CC BY 4.0.

exactly k IE -systems; (iv) no simple finite group has exactly k IE -systems; (v) at least one simple finite group, and no non-soluble non-simple finite group, has exactly k IE -systems. Thus (ii) is the negation of (i), and (iv) is the negation of (iii). Trofimov asks (Q1) whether the set of soluble and the set of absolutely simple group-theoretic numbers are finite or infinite, and (Q2) whether there are group-theoretic numbers that are “composite, but not soluble”, that is, integers k such that some non-soluble group, but no simple group, has exactly k IE -systems. Groups of prime order are simple and have no non-normal subgroups, so they play no role for positive k .

The problem appeared in the second issue (1967) of the Kourovka Notebook. We read it in the 21st edition [KM26], in the arXiv versions v48 and v49, which have the same text; there it carries no mark and no comment, that is, it is listed as open. The companion Problem 3.57, also due to Trofimov, asks for the “laws of distribution” of the non-soluble and the simple numbers; we claim nothing about it. The problem is record KOU-2.78 of the UnsolvedMath collection [ula26], where it is listed as open.

1.2 Results

Theorem 1.1. *For every integer $k \geq 9$ with $k \neq 11$ there is a non-soluble, non-simple finite group with exactly k IE -systems. Moreover $k(\text{PSL}(2, 13)) = k(\text{PSL}(2, 23)) = 11$.*

For $k \geq 361$ the group can be taken as $A_5 \times H$, where H is a metabelian group $C_q \rtimes C_{7^a}$ or $\mathbb{F}_q^2 \rtimes C_{7^a}$ and the prime q comes from Dirichlet’s theorem (Theorem 4.1); for $9 \leq k \leq 406$ it is one of 397 explicit groups, each a base group or the direct product of a base group with one or two cyclic or metabelian factors of coprime orders, checked by computer (Proposition 4.3).

Theorem 1.2 (Zhong [Zho05]; Shi, Zhang and Liang [SZL15]). *If G is a non-soluble finite group, then $k(G) \geq 7$, with equality only for $G \cong A_5$, and $k(G) \neq 8$.*

Corollary 1.3. (a) *The soluble group-theoretic numbers are exactly 1, 2, 3, 4, 5, 6, 8.* (b) *The number 7 is absolutely simple, every other absolutely simple number is 11, and 11 is absolutely simple if and only if no non-soluble non-simple group has exactly 11 IE -systems.* (c) *Both sets in (Q1) are finite. This already follows from Theorem 1.1 alone: the soluble numbers lie in $\{1, \dots, 8\}$, the absolutely simple numbers in $\{1, \dots, 8, 11\}$.*

So this note gives a partial answer: both sets are finite (the soluble numbers are exactly 1, 2, 3, 4, 5, 6, 8, and the absolutely simple numbers are 7 and possibly 11); the second question stays open (a composite non-soluble number would exceed 323). The bound 323 comes from data (Section 7): every k in $\{7\} \cup [9, 323]$ equals $k(\text{PSL}(2, q))$ for an explicit q . These data are not an answer to (Q2).

1.3 What is in print, what is not, and what stays open

Theorem 1.2 is in print. By the zbMATH review of [Zho05], a non-soluble group has at least seven orders of non-normal subgroups, with equality only for A_5 . By their abstract, Shi, Zhang and Liang [SZL15] prove that a group with at most nine “classes of nonnormal nontrivial subgroups of the same order” is soluble unless it is A_5 , $\text{PSL}(2, 7)$ or $\text{SL}(2, 5)$, which have $k = 7, 9, 9$; this excludes $k(G) = 8$. The zbMATH review of [SZL15] speaks of conjugacy classes, and we did not read the full text, so our reading of their count as a number of orders is an inference: in $\text{PSL}(2, 7)$ the non-normal subgroups of non-prime-power order form six conjugacy classes with only four orders (6, 12, 21, 24), and all non-normal subgroups form 13 conjugacy classes with 9 orders. So the statements of [SZL15] that the non-soluble groups with exactly four such classes of non-prime-power order are $\text{PSL}(2, 7)$ and $\text{PSL}(2, 8)$, and that $\text{PSL}(2, 7)$ has at most nine classes, fit only classes formed by all subgroups of one order. As we know [Zho05, SZL15] only from their reviews and abstracts, we prove Theorem 1.2 in

Section 5, using Thompson’s classification of the minimal simple groups [Tho68]. The invariant $k(G)$ appears as $r(G)$ in [Zho05] and as $J(G)$ in Xiang and Li [XL07]; it has been studied for soluble groups and p -groups, for instance in [HLC24].

What, to our knowledge, is not in print is Theorem 1.1, with Theorem 4.1 and the list of Proposition 4.3, and hence the finiteness of both sets in (Q1) and the exact set of soluble numbers; the searches are described in the paragraph “Scope and priority” in Section 9, and a search that finds nothing is not a proof of novelty. The finiteness follows from Theorem 1.1 alone; Theorem 1.2, which is in print, is needed only for the exact lists in Corollary 1.3(a) and (b). Open are the value 11 (Remark 6.1) and the second question (Section 7). Besides the results named, we use Dickson’s list of the subgroups of $\text{PSL}(2, q)$ [Hup67, Hauptsatz II.8.27], the Schur–Zassenhaus theorem [Isa08, Chapter 3] and Dirichlet’s theorem on primes in arithmetic progressions [Apo76, Chapter 7].

2 Notation and two lemmas

For a group G let $\mathcal{O}(G)$ be the set of orders of subgroups of G , let $\mathcal{U}(G) \subseteq \mathcal{O}(G)$ be the set of orders n such that every subgroup of G of order n is normal, and let $\mathcal{N}(G) = \mathcal{O}(G) \setminus \mathcal{U}(G)$ be the set of orders of non-normal subgroups. Put $o(G) = |\mathcal{O}(G)|$, $u(G) = |\mathcal{U}(G)|$ and

$$k(G) = |\mathcal{N}(G)| = o(G) - u(G),$$

the number of IE -systems of G . Always $1, |G| \in \mathcal{U}(G)$. If G is non-abelian simple, its only normal subgroups are 1 and G , so $\mathcal{U}(G) = \{1, |G|\}$ and $k(G) = o(G) - 2$. We write $\tau(n)$ for the number of divisors of n . For a cyclic group, $\mathcal{O}(C_m) = \mathcal{U}(C_m)$ is the set of divisors of m , so $o(C_m) = u(C_m) = \tau(m)$. For A_5 we have $\mathcal{O}(A_5) = \{1, 2, 3, 4, 5, 6, 10, 12, 60\}$ and $\mathcal{U}(A_5) = \{1, 60\}$, and we put

$$\Lambda = \mathcal{N}(A_5) = \{2, 3, 4, 5, 6, 10, 12\}, \quad k(A_5) = 7.$$

Lemma 2.1 (Monotonicity). *If $H \leq G$, then $\mathcal{N}(H) \subseteq \mathcal{N}(G)$. If $K \trianglelefteq G$, then $|K| \cdot \mathcal{N}(G/K) \subseteq \mathcal{N}(G)$. Hence $k(X) \leq k(G)$ for every section X of G .*

Proof. A subgroup of H that is not normal in H is not normal in G . If L/K is not normal in G/K , then L is not normal in G , and $|L| = |K| |L/K|$. Multiplication by $|K|$ is injective. $\square$

Lemma 2.2 (Coprime direct products). *Let G and H be groups with $\gcd(|G|, |H|) = 1$. Then every subgroup of $G \times H$ is $A \times B$ with $A \leq G$ and $B \leq H$, and $A \times B$ is normal if and only if $A \trianglelefteq G$ and $B \trianglelefteq H$. Consequently $\mathcal{O}(G \times H) = \{ab : a \in \mathcal{O}(G), b \in \mathcal{O}(H)\}$ and $\mathcal{U}(G \times H) = \{ab : a \in \mathcal{U}(G), b \in \mathcal{U}(H)\}$, the map $(a, b) \mapsto ab$ is injective on $\mathcal{O}(G) \times \mathcal{O}(H)$, and*

$$o(G \times H) = o(G) o(H), \quad u(G \times H) = u(G) u(H), \quad k(G \times H) = o(G) o(H) - u(G) u(H).$$

Proof. Let $K \leq G \times H$ and $(g, h) \in K$. The orders of g and h are coprime, so there is an integer e with $e \equiv 1$ modulo the order of g and $e \equiv 0$ modulo the order of h ; then $(g, h)^e = (g, 1) \in K$, and similarly $(1, h) \in K$. Hence $K = A \times B$ with $A = K \cap G$, $B = K \cap H$. Conjugation by (x, y) maps $A \times B$ to $A^x \times B^y$, which gives the criterion for normality. The order ab of $A \times B$ determines $a = \gcd(ab, |G|)$ and b , so the map $(a, b) \mapsto ab$ is injective. If all subgroups of order a of G and all subgroups of order b of H are normal, so are all subgroups of order ab of $G \times H$. If some $A_0 \leq G$ of order a is not normal, then $A_0 \times B$ is a non-normal subgroup of order ab for every $B \leq H$ of order b , and such B exist when $b \in \mathcal{O}(H)$; similarly for H . This gives $\mathcal{U}(G \times H)$. $\square$

In particular, if m is prime to $|G|$, then $k(G \times C_m) = \tau(m) k(G)$. For instance $\mathcal{O}(S_3) = \{1, 2, 3, 6\}$ and $\mathcal{U}(S_3) = \{1, 3, 6\}$ give $k(S_3 \times C_{5^{k-1}}) = k$ for every $k \geq 1$; so every positive integer is the number of IE -systems of a soluble group, and no number is soluble only because no group has that many IE -systems.

3 Two families of metabelian groups

Throughout this section q is a prime, $m \geq 1$ is an integer with $q \nmid m$, and $H = Q \rtimes C$, where Q is an abelian normal Sylow q -subgroup of H and $C = \langle t \rangle$ is cyclic of order m . For $e \mid m$ let $E_e = \langle t^{m/e} \rangle$ be the subgroup of order e of C . We write $D = \tau(m)$ and, for a divisor d of m , $D' = \tau(m/d)$. Note that $d \mid m/e$ if and only if $e \mid m/d$, for divisors d, e of m . We use the Schur–Zassenhaus theorem [Isa08, Chapter 3]: if N is a normal subgroup of a group X with $\gcd(|N|, |X : N|) = 1$, then N has a complement in X , and if moreover N is abelian, all complements of N are conjugate in X .

Lemma 3.1. (a) Every subgroup K of H has the form $K = (K \cap Q)E$, where $K \cap Q$ is the Sylow q -subgroup of K and $E \leq K$ is a subgroup of order $|K : K \cap Q|$. (b) Every subgroup E of H of order e prime to q (so that $e \mid m$) is conjugate to E_e . In particular, for each $e \mid m$ the subgroups of H of order e form one conjugacy class.

Proof. (a) As $Q \trianglelefteq H$, we have $K \cap Q \trianglelefteq K$, and $|K : K \cap Q| = |KQ : Q|$ divides m , which is prime to q . So $K \cap Q$ is a normal Sylow q -subgroup of K , and by the Schur–Zassenhaus theorem it has a complement E in K . (b) Let $L = QE$. Since $H = QC$ and $Q \leq L$, Dedekind’s law gives $L = Q(L \cap C)$. Thus E and $L \cap C$ are complements of the abelian normal Hall subgroup Q of L , and by the Schur–Zassenhaus theorem they are conjugate in L . Finally $L \cap C$ is the subgroup of order e of the cyclic group C , that is, E_e . $\square$

Proposition 3.2 (Block B1). Let $c \geq 1$, let $d > 1$ be a divisor of m with $d \mid q - 1$, and let r be an integer of multiplicative order d modulo q^c ; it exists because q is odd (as $1 < d \mid q - 1$) and $(\mathbb{Z}/q^c\mathbb{Z})^\times$ is cyclic of order $q^{c-1}(q - 1)$. Let $H = C_{q^c} \rtimes C_m$, where t acts on $Q = C_{q^c} = \langle x \rangle$ by $x \mapsto x^r$. Then

$$o(H) = (c + 1)D, \quad u(H) = D + cD'.$$

Proof. For $0 \leq i \leq c$ let Q_i be the subgroup of order q^i of Q ; it is characteristic in Q , hence normal in H . Let $K \leq H$ with $|K| = q^i e$, $q \nmid e$. By Lemma 3.1, $K \cap Q = Q_i$ and $K = Q_i E$ with E conjugate to E_e , so K is conjugate to $Q_i E_e$. Conversely $Q_i E_e$ is a subgroup of order $q^i e$ for all $0 \leq i \leq c$ and $e \mid m$. Hence $o(H) = (c + 1)D$, and for each order the subgroups of that order are conjugate, so the order lies in $\mathcal{U}(H)$ if and only if $Q_i E_e$ is normal.

If $i = c$, then QE_e/Q is a subgroup of the cyclic group H/Q , so $QE_e \trianglelefteq H$. Let $i < c$ and write bars for images in $\bar{H} = H/Q_i$, so $\bar{Q} \cong C_{q^{c-i}}$ and $\bar{E}_e \cong E_e$. The integer r has order d also modulo q^{c-i} : if $r^j \equiv 1 \pmod{q^{c-i}}$, then r^j lies in the kernel of $(\mathbb{Z}/q^c\mathbb{Z})^\times \rightarrow (\mathbb{Z}/q^{c-i}\mathbb{Z})^\times$, a q -group, so $r^{jq^i} \equiv 1 \pmod{q^c}$ and $d \mid jq^i$, whence $d \mid j$ as $\gcd(d, q) = 1$. If $\bar{E}_e \trianglelefteq \bar{H}$, then $[\bar{E}_e, \bar{Q}] \leq \bar{E}_e \cap \bar{Q} = 1$, so $t^{m/e}$ centralises $\bar{Q}$, that is $r^{m/e} \equiv 1 \pmod{q^{c-i}}$, and $d \mid m/e$. If $d \mid m/e$, then $t^{m/e}$ centralises $\bar{Q}$ and $\bar{C}$, so $\bar{E}_e$ is central in $\bar{H} = \bar{Q}\bar{C}$ and hence normal. Thus for $i < c$ the subgroup $Q_i E_e$ is normal if and only if $e \mid m/d$, and $\mathcal{U}(H) = \{q^c e : e \mid m\} \cup \{q^i e : i < c, e \mid m/d\}$ has $D + cD'$ elements. $\square$

Proposition 3.3 (Block B2). Let $d > 1$ be a divisor of m with $d \mid q + 1$ and $\gcd(d, q - 1) = 1$ (then d is odd). Let ζ be an element of order d of the cyclic group $\mathbb{F}_{q^2}^\times$, let Q be the additive group of $\mathbb{F}_{q^2}$, so that $Q \cong \mathbb{F}_q^2$, and let $H = Q \rtimes C_m$, where t acts by $v \mapsto \zeta v$. Then

$$o(H) = 2D + D', \quad u(H) = D + D'.$$

Proof. The subgroups of order q of Q are the lines $\mathbb{F}_q v$ with $v \neq 0$. We claim that if $\zeta^j \neq 1$, then multiplication by ζ^j maps no line to itself. Indeed, $\zeta^j v \in \mathbb{F}_q v$ with $v \neq 0$ means $\zeta^j \in \mathbb{F}_q^\times$; then the order of ζ^j divides both d and $q - 1$, so it is 1.

Let $K \leq H$ with $|K| = q^i e$, $q \nmid e$, $i \in \{0, 1, 2\}$. By Lemma 3.1, $K = (K \cap Q)E$ with $E = E_e^g$ for some $g \in H$; then $K^{g^{-1}} = LE_e$, where $L = (K \cap Q)^{g^{-1}}$ has order q^i and is normalised by E_e .

The subgroup E_e acts on Q by multiplication by $\zeta^{m/e}$, which is trivial if and only if $d \mid m/e$, that is $e \mid m/d$.

For $i = 0$: subgroups of order e exist for every $e \mid m$, they are all conjugate, and E_e is normal if and only if it centralises Q (a normal subgroup N of order prime to q satisfies $[N, Q] \leq N \cap Q = 1$, and a subgroup of C centralising Q is central), that is, if and only if $e \mid m/d$. For $i = 2$: $K \supseteq Q$, and QE_e is the unique and normal subgroup of order q^2e , since H/Q is cyclic. For $i = 1$: L is a line mapped to itself by $\zeta^{m/e}$, so $\zeta^{m/e} = 1$ by the claim, and $e \mid m/d$. Conversely, for $e \mid m/d$ the group E_e acts trivially on Q , so LE_e is a subgroup of order qe for every line L ; it is not normal, since otherwise $L = LE_e \cap Q$ would be normal in H and $\zeta L = L$, against the claim.

Hence $\mathcal{O}(H) = \{e : e \mid m\} \cup \{qe : e \mid m/d\} \cup \{q^2e : e \mid m\}$ and $\mathcal{U}(H) = \{e : e \mid m/d\} \cup \{q^2e : e \mid m\}$, of sizes $2D + D'$ and $D + D'$. $\square$

Remark 3.4. The formulas agree with an exhaustive enumeration of all subgroups in 22 instances of Proposition 3.2 and 15 of Proposition 3.3 (Section 9); for $q = 2$ and $m = d = 3$, Proposition 3.3 describes A_4 , with $(o, u) = (5, 3)$. Without $\gcd(d, q - 1) = 1$ a power of ζ may lie in $\mathbb{F}_q^\times$ and fix every line. Both families are metabelian, as Q is abelian and H/Q is cyclic. The groups of Proposition 3.2 are metacyclic; those of Proposition 3.3 are not, since $\zeta - 1$ is invertible, so that the derived subgroup of H is $Q \cong \mathbb{F}_q^2$.

4 Non-soluble non-simple groups with a given number of IE-systems

We write $B_0(m) = C_m$, $B_1(q, c, m, d)$ for the group H of Proposition 3.2 and $B_2(q, m, d)$ for the group H of Proposition 3.3; we call them blocks. By Lemma 2.2, if B is a group and $H_1, \dots, H_j$ are groups such that the orders of $B, H_1, \dots, H_j$ are pairwise coprime, then

$$k(B \times H_1 \times \dots \times H_j) = o(B) \prod_i o(H_i) - u(B) \prod_i u(H_i). \quad (1)$$

If B is not soluble, neither is the product, and if $j \geq 1$ and all $H_i \neq 1$, the product is not simple.

Theorem 4.1. *Let $a \geq 1$ and $1 \leq b \leq a$, and put $A = a + 1$ and $x = a - b + 1$, so that $1 \leq x \leq A - 1$.*

- (a) *If q is a prime with $q \equiv 1 \pmod{7^b}$, then $k(A_5 \times B_1(q, 1, 7^a, 7^b)) = 16A - 2x$.*
- (b) *If q is a prime with $q \equiv -1 \pmod{7^b}$, then $k(A_5 \times B_2(q, 7^a, 7^b)) = 16A + 7x$.*
- (c) *Every even $k \geq 126$ has the form $16A - 2x$, and every odd $k \geq 361$ has the form $16A + 7x$, with a, b as above. Hence every even $k \geq 126$ and every odd $k \geq 361$ is the number of IE-systems of a non-soluble non-simple group.*

Proof. (a) As $q \equiv 1 \pmod{7}$, we have $q \geq 29$, so $|B_1(q, 1, 7^a, 7^b)| = q \cdot 7^a$ is prime to $|A_5| = 60$; the hypotheses of Proposition 3.2 hold with $c = 1$, $m = 7^a$, $d = 7^b$. It gives $o = 2\tau(7^a) = 2A$ and $u = \tau(7^a) + \tau(7^{a-b}) = A + x$, and (1) with $(o(A_5), u(A_5)) = (9, 2)$ gives $9 \cdot 2A - 2(A + x) = 16A - 2x$.

(b) As $q \equiv 6 \pmod{7}$, $q \notin \{2, 3, 5, 7\}$, so the order $q^2 \cdot 7^a$ is prime to 60 and $q \nmid 7^a$. Further $7^b \mid q + 1$, and $\gcd(7^b, q - 1) = 1$ because $q - 1 \equiv -2 \pmod{7}$. Proposition 3.3 gives $o = 2A + x$ and $u = A + x$, and $9(2A + x) - 2(A + x) = 16A + 7x$.

(c) Let $k \geq 126$ be even, $A = \lceil (k + 2)/16 \rceil$ and $x = 8A - k/2$. From $k + 2 \leq 16A < k + 18$ we get $1 \leq x \leq 8$, and $A \geq 8$. If $A \geq 9$, then $x \leq 8 \leq A - 1$; if $A = 8$, then $k = 126$ and $x = 1$. So $b = A - x$ lies in $[1, a]$ and $16A - 2x = k$. Let $k \geq 361$ be odd. As $7k$ is odd, there is an odd $x \in [1, 15]$ with $x \equiv 7k \pmod{16}$; then $7x \equiv 49k \equiv k \pmod{16}$, so $A = (k - 7x)/16$ is an integer, and

B	$ B $	o	u	k	lines	B	$ B $	o	u	k	lines
A_5	60	9	2	7	93	$A_5 \times C_{15}$	900	24	3	21	10
$A_5 \times C_2$	120	13	3	10	51	$A_5 \times C_{25}$	1500	21	2	19	24
$A_5 \times C_3$	180	15	3	12	17	$\text{SL}(2, 5)$	120	12	3	9	21
$A_5 \times C_4$	240	17	4	13	33	$\text{PSL}(2, 7) \times C_2$	336	16	3	13	14
$A_5 \times C_5$	300	15	2	13	12	$\text{PSL}(2, 7) \times C_3$	504	17	3	14	12
$A_5 \times C_6$	360	21	4	17	18	$\text{PGL}(2, 9)$	720	19	3	16	10
$A_5 \times C_8$	480	21	5	16	15	$W \rtimes A_5$	960	20	2	18	31
$A_5 \times C_{10}$	600	21	3	18	3	$\text{SL}(2, 13)$	2184	18	3	15	1
$A_5 \times C_{12}$	720	27	5	22	20						

Table 1: The base groups of the certificate whose values $o = o(B)$, $u = u(B)$ were obtained by exhaustive enumeration of all subgroups; W is the even-weight submodule of the permutation module $\mathbb{F}_2^5$ of A_5 , of order 16. The last column gives the number of certificate lines with this base group. Lemma 2.2 does not apply to $A_5 \times C_n$ with $\gcd(n, 60) > 1$.

$A \geq (361 - 105)/16 = 16 > x$. Again $b = A - x \in [1, a]$. Since $\gcd(\pm 1, 7^b) = 1$, Dirichlet's theorem [Apo76, Chapter 7] gives primes $q \equiv 1$ and $q \equiv -1 \pmod{7^b}$. The groups are non-soluble since they contain A_5 , and non-simple since $A_5 \times 1$ is a proper non-trivial normal subgroup. $\square$

Lemma 4.2. *Let $p \geq 5$ be a prime and let Δ_+ , Δ_- be the sets of divisors of $(p+1)/2$ and $(p-1)/2$.*

- (a) $\mathcal{O}(\text{PSL}(2, p))$ consists of 1, p and $|\text{PSL}(2, p)| = p(p^2 - 1)/2$; the elements of $\Delta_+ \cup \Delta_-$; the numbers $2z$ with $z \in \Delta_+ \cup \Delta_-$, $z \geq 2$; the number 12; the number 24 if $p \equiv \pm 1 \pmod{8}$; the number 60 if $p \equiv \pm 1 \pmod{10}$ or $p = 5$; and the numbers pt with $t \in \Delta_-$. Moreover $\mathcal{U}(\text{PSL}(2, p)) = \{1, |\text{PSL}(2, p)|\}$.
- (b) $\mathcal{O}(\text{SL}(2, p)) = \{2n : n \in \mathcal{O}(\text{PSL}(2, p))\} \cup \{n \in \mathcal{O}(\text{PSL}(2, p)) : n \text{ odd}\}$ and $\mathcal{U}(\text{SL}(2, p)) = \{1, 2, |\text{SL}(2, p)|\}$; so $k(\text{SL}(2, p)) = o(\text{SL}(2, p)) - 3$.

Proof. (a) By Dickson's theorem [Hup67, Hauptsatz II.8.27], for a prime p the non-trivial proper subgroups of $\text{PSL}(2, p)$ are, up to isomorphism, the groups of order p , the cyclic groups of order z and the dihedral groups of order $2z$ for $z \mid (p \pm 1)/2$ (with $z \geq 2$ in the dihedral case), A_4 , S_4 if $p^2 \equiv 1 \pmod{16}$, A_5 if $p^2 \equiv 1 \pmod{5}$, and the groups $C_p \rtimes C_t$ with $t \mid (p-1)/2$; and all of them occur. For odd p , $p^2 \equiv 1 \pmod{16}$ means $p \equiv \pm 1 \pmod{8}$, and for $p \neq 5$, $p^2 \equiv 1 \pmod{5}$ means $p \equiv \pm 1 \pmod{10}$. The group $\text{PSL}(2, p)$ is simple.

(b) An element of order 2 of $\text{SL}(2, p)$ is diagonalisable with eigenvalues ± 1 and determinant 1, so it is $-I$. Hence a subgroup of even order contains $-I$ and is the full preimage of its image in $\text{PSL}(2, p)$; this gives the orders $2n$. A subgroup of odd order meets $\{\pm I\}$ trivially and maps isomorphically onto a subgroup of $\text{PSL}(2, p)$. Conversely, if $L \leq \text{PSL}(2, p)$ has odd order, then $\{\pm I\}$ is a normal Hall subgroup of the preimage of L , and by the Schur–Zassenhaus theorem it has a complement, of order $|L|$. A normal subgroup N of $\text{SL}(2, p)$ either lies in $\{\pm I\}$ or satisfies $N\{\pm I\} = \text{SL}(2, p)$, because its image in the simple group $\text{PSL}(2, p)$ is normal. In the second case $|\text{SL}(2, p) : N| \leq 2$, so N contains all elements of odd order, in particular the elementary matrices $\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix}$ of order p , which generate $\text{SL}(2, p)$; so $N = \text{SL}(2, p)$. Thus the normal subgroups are 1, $\{\pm I\}$ and $\text{SL}(2, p)$, and $\{\pm I\}$ is the only subgroup of order 2. $\square$

Proposition 4.3. *For every $k \in [9, 406] \setminus \{11\}$, line k of the file `certificate.txt` names a group $G_k = B \times H_1 \times \cdots \times H_j$ with $0 \leq j \leq 2$ and the following properties: B is a group of Table 1, or $B = \text{SL}(2, p)$ or $\text{PSL}(2, p)$ with p prime; each H_i is a block $B_0(m)$ with $m \geq 2$, $B_1(q, c, m, d)$ or*

k	G_k	$o(B) \prod o(H_i) - u(B) \prod u(H_i)$
18	$W \rtimes A_5$	$20 - 2$
19	$A_5 \times C_{25}$	$21 - 2$
23	$\text{SL}(2, 29)$	$26 - 3$ (19 orders in $\text{PSL}(2, 29)$, 7 of them odd)
39	$(A_5 \times C_4) \times C_{49}$	$17 \cdot 3 - 4 \cdot 3$
59	$(\text{PSL}(2, 7) \times C_3) \times B_1(23, 1, 11, 11)$	$17 \cdot 4 - 3 \cdot 3$
137	$\text{PGL}(2, 9) \times B_1(29, 3, 7, 7)$	$19 \cdot 8 - 3 \cdot 5$
173	$\text{PSL}(2, 13) \times B_1(23, 4, 121, 11)$	$13 \cdot 15 - 2 \cdot 11$
233	$(A_5 \times C_2) \times B_1(29, 1, 7, 7) \times B_2(43, 11, 11)$	$13 \cdot 4 \cdot 5 - 3 \cdot 3 \cdot 3$
359	$(A_5 \times C_6) \times B_2(35573, 5929, 5929)$	$21 \cdot 19 - 4 \cdot 10$
406	$A_5 \times C_{7^{57}}$	$9 \cdot 58 - 2 \cdot 58$

Table 2: Some lines of the certificate, with the values of o and u of the factors.

$B_2(q, m, d)$ whose integers satisfy the hypotheses of Proposition 3.2 resp. Proposition 3.3; the orders of $B, H_1, \dots, H_j$ are pairwise coprime; G_k is not simple; and $o(B) \prod_i o(H_i) - u(B) \prod_i u(H_i) = k$. Hence G_k is non-soluble and non-simple, and $k(G_k) = k$.

Proof. The verification of the 397 lines is a finite computation with exact integers. For each line it checks that every q is prime (deterministic Miller–Rabin test; all q are below $1.2 \cdot 10^6$), the hypotheses of the blocks, the coprimality of all orders, and the displayed identity, with $(o(B), u(B))$ taken from Table 1 or from Lemma 4.2, and (o, u) of the blocks from τ and Propositions 3.2 and 3.3; then $k(G_k) = k$ by (1). Every G_k contains the non-soluble group B . If $j \geq 1$, then $B \times 1$ is a proper non-trivial normal subgroup. The 22 lines with $j = 0$ use $\text{SL}(2, p)$ (with centre $\{\pm I\}$) or a group of Table 1 other than A_5 , each of which has a proper non-trivial normal subgroup (a direct factor, $\{\pm I\}$, or W). The computation is done by the program `check_note.py` of this note and by the program `verify_cert.py` with which the list was first checked (Section 9). $\square$

The lines are written as $\mathbf{k}$, the name of B , and the blocks in the form $\mathbf{B0:m}, \mathbf{B1:q:c:m:d}, \mathbf{B2:q:m:d}$; two blocks on one line are separated by a semicolon, as in the six lines $k = 233, 282, 293, 313, 353, 393$. For instance, line 233 reads

233 A5xC2 B1:29:1:7:7;B2:43:11:11

and names $(A_5 \times C_2) \times B_1(29, 1, 7, 7) \times B_2(43, 11, 11)$. In 385 lines B is taken from Table 1; in the other twelve, $(o(B), u(B))$ comes from Lemma 4.2: $B = \text{SL}(2, p)$ for $(k, p) = (23, 29), (25, 167), (29, 1213), (31, 113), (33, 1087), (37, 1019), (41, 1667), (47, 1063), (53, 1151), (61, 1601)$, and $B = \text{PSL}(2, 29), \text{PSL}(2, 13)$, each with a block B_1 , for $k = 157, 173$. The values for $\text{PSL}(2, 13), \text{PSL}(2, 29)$ and $\text{SL}(2, 29)$ were also confirmed by enumeration (the last two in verification runs), and the independent covering found by the second verification run uses enumerated base groups for $k = 23, 29, 31, 33$. So six values, $k = 25, 37, 41, 47, 53, 61$, rest on Dickson’s theorem beyond the range of exhaustive enumeration. Table 2 shows examples.

Proof of Theorem 1.1. For $9 \leq k \leq 406$, $k \neq 11$, use Proposition 4.3, and for $k \geq 407$ use Theorem 4.1(c). By Lemma 4.2(a), $\mathcal{O}(\text{PSL}(2, 13)) = \{1, 2, 3, 4, 6, 7, 12, 13, 14, 26, 39, 78, 1092\}$ and $\mathcal{O}(\text{PSL}(2, 23)) = \{1, 2, 3, 4, 6, 8, 11, 12, 22, 23, 24, 253, 6072\}$, so both groups have $13 - 2 = 11$ IE -systems. For $\text{PSL}(2, 13)$ this was also confirmed by an exhaustive enumeration of its 942 subgroups. $\square$

5 Non-soluble groups with at most eight IE-systems

This section proves Theorem 1.2, which is in print [Zho05, SZL15]; we include the argument because we could not read these papers. A minimal simple group is a non-abelian simple group all of whose proper subgroups are soluble.

Lemma 5.1. *Let $N \neq 1$ be a normal subgroup of G with $G/N \cong A_5$. Then $k(G) \geq 9$.*

Proof. By Lemma 2.1, $\mathcal{N}(G)$ contains the seven numbers $|N|\lambda$, $\lambda \in \Lambda$. For $r \in \{2, 3, 5\}$ let P_r be a Sylow r -subgroup of G . Its image $P_r N/N$ is a Sylow r -subgroup of A_5 , which is not normal, so P_r is not normal and $|P_r| \in \mathcal{N}(G)$. If $|P_r| = |N|\lambda$ with $\lambda \in \Lambda$, then $|N|$ divides the power $|P_r|$ of r , so N is an r -group; this happens for at most one r . The three numbers $|P_2|, |P_3|, |P_5|$ are distinct, and at least two of them lie outside $|N|\Lambda$. Hence $k(G) \geq 7 + 2$. $\square$

Lemma 5.2. *Every minimal simple group $T \not\cong A_5$ satisfies $k(T) \geq 9$.*

Proof. By Thompson's classification [Tho68, Corollary 1], T is one of $\text{PSL}(2, 2^p)$ with p prime, $\text{PSL}(2, 3^p)$ with p an odd prime, $\text{PSL}(2, p)$ with $p > 3$ prime and $5 \mid p^2 + 1$, $\text{Sz}(2^p)$ with p an odd prime, and $\text{PSL}(3, 3)$; and $\text{PSL}(2, 4) \cong A_5$. As T is simple, every order of a proper non-trivial subgroup lies in $\mathcal{N}(T)$. For $\text{PSL}(2, q)$, $q = \ell^f$ with ℓ prime and $\delta = \gcd(2, q-1)$, we use from Dickson's theorem [Hup67, Hauptsatz II.8.27] the elementary abelian subgroups of every order $\ell^i \leq q$, cyclic subgroups of orders $(q \pm 1)/\delta$, dihedral subgroups of orders $2(q \pm 1)/\delta$, A_4 if $\ell > 2$, and a subgroup of order $q(q-1)/\delta$.

$T = \text{PSL}(2, q)$, $q = 2^p$, $p \geq 3$: the orders $2, 4, 8, 3$ (as p is odd, $3 \mid 2^p + 1 = q + 1$); $q - 1, q + 1$; $2(q - 1), 2(q + 1)$; and $q(q - 1)$. They are distinct: $q - 1 \geq 7$ and $q + 1 \geq 9$ are odd; $2(q \pm 1) \equiv 2 \pmod{4}$ and $2(q \pm 1) \geq 14$; $q(q - 1) \geq 56$ is divisible by 8 but is not a power of 2.

$T = \text{PSL}(2, q)$, $q = 3^p$, $p \geq 3$: the orders $2, 3, 4, 9, 12, 27$, the orders $(q \pm 1)/2$ and $q \pm 1$, which are at least 13 and prime to 3, and $q(q - 1)/2 \geq 351$; the order 4 occurs because $q \equiv 3 \pmod{8}$, so the dihedral group of order $q + 1$ contains a Klein four-group. These are 11 distinct numbers.

$T = \text{PSL}(2, p)$, $p \geq 7$, $p \equiv \pm 2 \pmod{5}$: by Lemma 4.2(a) the orders $2, 3, 4, 6, 12, p, p - 1, p + 1$ and $p(p - 1)/2$ occur (2 and 3 divide $(p - 1)/2$ or $(p + 1)/2$). For $p \geq 17$ they are distinct. For $p = 13$ we have $p - 1 = 12$, and $(p + 1)/2 = 7$ is a further order; for $p = 7$ we have $p - 1 = 6$, and 24 is a further order, since $7 \equiv -1 \pmod{8}$.

$T = \text{Sz}(q)$, $q = 2^p$, $p \geq 3$ odd: $|T| = q^2(q^2 + 1)(q - 1)$ [Suz62]. By Sylow's theorem every prime power dividing $|T|$ is the order of a proper non-trivial subgroup, so $k(T)$ is at least the number $\Omega(|T|)$ of prime factors of $|T|$ counted with multiplicity. We have $\Omega(q^2) = 2p \geq 6$ and $\Omega(q - 1) \geq 1$. Moreover $5 \mid 4^p + 1 = q^2 + 1$, and $q^2 + 1$ is not a power of 5: if $4^p + 1 = 5^e$, then $5^e \equiv 1 \pmod{8}$, so e is even, and $4^p = (5^{e/2} - 1)(5^{e/2} + 1)$ would be a product of two powers of 2 that differ by 2, which forces $5^{e/2} = 3$. So $\Omega(q^2 + 1) \geq 2$ and $k(T) \geq 9$.

$T = \text{PSL}(3, 3)$, of order $5616 = 2^4 \cdot 3^3 \cdot 13$: the eight prime powers $2, 4, 8, 16, 3, 9, 27, 13$ and the order 108 of the subgroup of upper triangular matrices. $\square$

Proof of Theorem 1.2. Since $k(A_5) = 7$, it suffices to show that every non-soluble group G with $k(G) \leq 8$ is isomorphic to A_5 . Suppose not, and let G be a counterexample of least order.

(1) If X is a non-soluble proper subgroup or a non-soluble proper quotient of G , then $k(X) \leq k(G) \leq 8$ by Lemma 2.1 and $|X| < |G|$, so $X \cong A_5$.

(2) Let $M \leq G$ be a non-soluble subgroup of least order and N a maximal normal subgroup of M . All proper subgroups of M are soluble; so N is soluble, M/N is non-abelian simple, and its proper subgroups, images of proper subgroups of M , are soluble. Thus M/N is minimal simple with $k(M/N) \leq 8$, so $M/N \cong A_5$ by Lemma 5.2, and $N = 1$ by Lemma 5.1. Hence $M \cong A_5$, and $M \neq G$.

(3) Let K be a minimal normal subgroup of G . If K is soluble, then G/K is non-soluble, so $G/K \cong A_5$ by (1), and $k(G) \geq 9$ by Lemma 5.1, a contradiction. If K is non-soluble and $K \neq G$, then $K \cong A_5$ by (1). If $C_G(K) \neq 1$, choose $c \in C_G(K)$ of prime order r ; as $K \cap C_G(K) = 1$, the subgroup $K\langle c \rangle$ is isomorphic to $A_5 \times C_r$. For every non-normal $A \leq A_5$ the subgroups $A \times 1$ and $A \times C_r$ of $A_5 \times C_r$ are not normal, so $\mathcal{N}(A_5 \times C_r) \supseteq \Lambda \cup r\Lambda$, which has at least ten elements (Λ together with 8, 20, 24 for $r = 2$, with 9, 15, 18, 30, 36 for $r = 3$, with 15, 20, 25, 30, 50, 60 for $r = 5$, and $\Lambda \cap r\Lambda = \emptyset$ for $r \geq 7$). So $k(G) \geq 10$ by Lemma 2.1, a contradiction. Hence $C_G(K) = 1$, G embeds into $\text{Aut}(A_5) \cong S_5$, and $G \cong S_5$ as $G \neq K$. But $\mathcal{N}(S_5)$ contains Λ and the orders 8, 20, 24 of non-normal subgroups, so $k(S_5) \geq 10$, a contradiction. Finally, if $K = G$, then G is simple and contains $M \cong A_5$ properly by (2). Then $\mathcal{N}(G) \supseteq \Lambda \cup \{60\}$, and $k(G) \leq 8$ forces $\mathcal{N}(G) = \Lambda \cup \{60\}$. For every prime r and r^e exactly dividing $|G|$, Sylow's theorem gives proper non-trivial, hence non-normal, subgroups of orders $r, r^2, \dots, r^e$. The prime powers in $\Lambda \cup \{60\}$ are 2, 3, 4, 5, so $|G|$ divides 60, against $|G| > |M| = 60$. $\square$

6 The answer to the first question

Proof of Corollary 1.3. (a) A number is non-soluble if and only if some non-soluble group has exactly that many IE -systems. By Theorem 1.2, no $k \in \{1, \dots, 6, 8\}$ is non-soluble; $7 = k(A_5)$ is; and every $k \geq 9$ is, by Theorem 1.1 (for $k = 11$ by $\text{PSL}(2, 13)$). As “soluble” is the negation of “non-soluble”, the soluble numbers are $1, \dots, 6, 8$.

(b) A simple group with $k \geq 1$ IE -systems is non-abelian, hence non-soluble. So by Theorem 1.2 no $k \in \{1, \dots, 6, 8\}$ is simple, and none of them is absolutely simple. Every $k \geq 9$ with $k \neq 11$ is attained by a non-soluble non-simple group (Theorem 1.1), so it is not absolutely simple. The number 7 is attained by the simple group A_5 , and by Theorem 1.2 every non-soluble group with 7 IE -systems is isomorphic to A_5 ; so 7 is absolutely simple. The number 11 is simple, as $k(\text{PSL}(2, 13)) = 11$; it is absolutely simple if and only if no non-soluble non-simple group has exactly 11 IE -systems.

(c) By Theorem 1.1, every $k \geq 9$ is non-soluble, and every $k \geq 9$ with $k \neq 11$ is attained by a non-soluble non-simple group. Hence the soluble numbers lie in $\{1, \dots, 8\}$ and the absolutely simple numbers in $\{1, \dots, 8, 11\}$. Theorem 1.2 is used only in (a) and (b). $\square$

Remark 6.1 (The value 11). We do not know whether a non-soluble non-simple group with exactly 11 IE -systems exists; none of the non-soluble non-simple groups whose subgroups were enumerated for this note or in the verification runs has this property. Settling the question needs the simple groups with at most 11 IE -systems, in all families of finite simple groups, and an analysis of their extensions as in the proof of Theorem 1.2. Among the groups $\text{PSL}(2, p)$ with $p \leq 23$ prime, Lemma 4.2 gives $k = 11$ only for $p = 13$ and $p = 23$.

7 The second question: data

By Corollary 1.3(a) the non-soluble numbers are 7 and all $k \geq 9$, and $7 = k(A_5)$ is simple. So a composite number that is not soluble is an integer $k \geq 9$ such that no simple group has exactly k IE -systems. We record the following data.

Every $k \in \{7\} \cup [9, 323]$ equals $k(\text{PSL}(2, q))$ for an explicit q : $q = 27$ for $k = 12$, and a prime $q = p$ otherwise. The table of the smallest such primes, computed from Lemma 4.2(a) for all primes $p \leq 5 \cdot 10^6$, is part of the reproducibility package; the largest of them is $p = 4,022,201$, for $k = 268$. For instance $k = 7, 9, 10, 11, 13, 14$ occur for $p = 5, 7, 11, 13, 47, 17$, and $k = 323$ for $p = 3,243,239$. For $q = 27$, Dickson's theorem gives $\mathcal{O}(\text{PSL}(2, 27)) = \{1, 2, 3, 4, 7, 9, 12, 13, 14, 26, 27, 28, 351, 9828\}$, so $k(\text{PSL}(2, 27)) = 12$. The program `check_note.py` recomputes $k(\text{PSL}(2, q))$ for every listed q . As

a cross-check, the second verification run scanned all prime powers $q \leq 6 \cdot 10^6$ with its own program and found every $k \in \{7\} \cup [9, 331]$; the first value it did not reach is 332, and $k = 324$ first occurs for $q = 5,346,881$. Consequently a composite non-soluble number, if one exists, exceeds 323.

These are data, not a theorem about the second question. Roughly, $k(\text{PSL}(2, p))$ is $3\tau((p-1)/2) + 2\tau((p+1)/2)$, so large values need $p \pm 1$ with many divisors, and a scan reaches new values slowly. An answer would need either a proof that no finite simple group of any family has exactly k *IE*-systems for some k , or simple groups for all $k \geq 324$, for instance through a simultaneous control of the divisors of $p-1$ and $p+1$. We have neither, and the second question stays open.

8 Conclusion

For Problem 2.78 of the Kourovka Notebook this note gives a partial answer: both sets are finite (the soluble numbers are exactly 1, 2, 3, 4, 5, 6, 8, and the absolutely simple numbers are 7 and possibly 11); the second question stays open (a composite non-soluble number would exceed 323). The finiteness rests on Theorem 1.1; the exact lists rest in addition on Theorem 1.2, due to Zhong and to Shi, Zhang and Liang. Two questions remain: whether some non-soluble non-simple group has exactly 11 *IE*-systems, and the second question of the problem.

9 Computations, verification and scope

The proofs of the lemmas, propositions and theorems of Sections 2, 3 and 5 and of Theorem 4.1 use no computation. Computations enter in three places: the values of Table 1, obtained by exhaustive enumeration of all subgroups; the verification of the 397 lines in Proposition 4.3; and the data of Section 7. The reproducibility package has three parts.

The program of this note (`check_note.py`; Python 3, standard library only; about two minutes, or 25 seconds with the option `--quick`, which skips three enumerations of groups of order above 3000) has its own enumeration of all subgroups up to conjugacy. It checks this enumeration against known numbers of subgroups (for instance 59 for A_5 and 179 for $\text{PSL}(2, 7)$); Lemma 2.2 on nine coprime products, among them $A_5 \times B_1(29, 1, 7, 7)$, a member of the family of Theorem 4.1(a), and its failure for $A_5 \times C_5$, where $(o, u) = (15, 2)$ and not $(18, 4)$; Propositions 3.2 and 3.3 in 22 and 15 instances; every row of Table 1, with a non-trivial proper normal subgroup of each base group used without blocks; Lemma 4.2 against enumeration for $\text{PSL}(2, q)$, $q \in \{5, 7, 8, 9, 11, 13\}$, and $\text{SL}(2, p)$, $p \in \{5, 7, 11, 13\}$; every line of the certificate, with the hypotheses of the blocks, primality, coprimality and non-simplicity; the arithmetic of Theorem 4.1(c) for all $k \leq 10^6$; the 942 subgroups of $\text{PSL}(2, 13)$ and the values in Remark 6.1; the data of Section 7; and the counts of conjugacy classes and orders used in Section 1.3. All 644 checks pass.

The programs with which the results were first obtained (`original/`, with their recorded outputs) comprise an exhaustive subgroup enumeration, with which Table 1 and some thirty further groups were computed; an implementation of Dickson's list, compared with enumeration for $\text{PSL}(2, q)$, $\text{SL}(2, q)$ and $\text{PGL}(2, q)$ with $q \leq 13$; checks of Propositions 3.2 and 3.3 in 20 and 11 instances; the search that produced the certificate; the verifier `verify_cert.py`; and the scans of Section 7. In the copies in the package, programs that write files write into a subfolder `rerun/`, so that the recorded outputs are not overwritten, and `verify_cert.py` was changed after the second verification run: it rejects blocks $B_0(m)$ with $m < 2$, and it accepts a line without blocks only if a rule exhibits a non-trivial proper normal subgroup of the base group, instead of consulting a list of names of simple groups. Run again from the package, all programs reproduce the recorded outputs up to running times, except for one intermediate list of witnesses that was recorded before a data file was completed and is not used later (see `README.md`).

The programs of the third verification run (`independent_run_2/`, with their recorded outputs; Python 3 with numpy, and sympy for one program) are described in the next paragraph and in their `README.md`.

Verification. The results were first obtained, with proofs and with the programs in `original/`. Three independent verification runs, all AI-assisted, followed; each re-derived the proofs and wrote its own programs. The first two examined the first write-up of the result, not this text. The first re-derived all proofs line by line. With its own enumeration, by a different method and with its own constructions, it recomputed the enumerated base groups of the certificate and further groups, 22 in all, with the same values of o and u and the same numbers of subgroups; it verified all 397 lines with its own verifier, its own implementation of Lemma 4.2 and its own data, checked 22 instances of the blocks, Lemma 2.2 for products of two non-abelian groups and the arithmetic of Theorem 4.1 up to 20000, and repeated the scan of Section 7. The second wrote its programs before reading those of the first write-up. It enumerated 81 non-soluble groups of order at most 3600, among them the 40 groups of the table of the first write-up; compared its implementation of Dickson’s list with enumeration for $\text{PSL}(2, q)$ with all prime powers $q \leq 31$ and for $\text{SL}(2, q)$, $\text{PGL}(2, q)$ with odd $q \leq 23$; checked Proposition 3.2 in 866 and Proposition 3.3 in 57 instances, Lemma 2.2 on five products of order up to 12180, and Theorem 4.1 in its arithmetic up to $2 \cdot 10^6$ and with explicit groups and probable primes for $k \leq 1200$; found an independent second covering of $[9, 406] \setminus \{11\}$ by other groups; verified all 397 lines with its own data; ran the original programs again with identical outputs; tested the verifier on deliberately wrong inputs; and extended the scan of Section 7 to all prime powers $q \leq 6 \cdot 10^6$. These two runs confirmed the result in the scope stated here and required corrections of the presentation only, all of which were made: among them the status of the value 11, the explicit use of the Schur–Zassenhaus theorem in Section 3, the inference behind our reading of [SZL15], the separation of the results in print from the others, the description of lines with two blocks, and the change of `verify_cert.py`. When this note was written, `check_note.py` was added, the proof of Theorem 1.2 received lower bounds for $k(A_5 \times C_r)$ and $k(S_5)$ that need no computation, and a case of Theorem 4.1 that does not occur for $k \geq 126$ was dropped; the first two runs have not seen this text.

The third run examined the text of this note. It read Problem 2.78 again in v49 of [KM26], compared the record, the zbMATH reviews of [Zho05, XL07, SZL15] and the abstract of [SZL15] with the text, and re-derived all proofs line by line. Before reading `check_note.py` it wrote its own programs: an enumeration of all subgroups up to conjugacy, its own constructions of the groups, its own coding of Dickson’s list and its own verifier of the certificate. It enumerated the 17 groups of Table 1, with the values of the table; $\text{PSL}(2, q)$ for 13 values $q \leq 29$, among them $q = 13$ (942 subgroups), 23 and 27; and $\text{SL}(2, q)$ for $q \in \{5, 7, 9, 11, 13, 17, 29\}$, all in agreement with Dickson’s list and Lemma 4.2. Among these groups is $\text{SL}(2, 29)$, of order 24360, the base group of line $k = 23$. It also enumerated the whole groups of the lines $k = 26, 32, 34, 36$ (orders 1680 to 6720), 20 instances of Proposition 3.2 and 15 of Proposition 3.3, three instances that violate their hypotheses (they disagree with the formulas, as they must), and three coprime products of order up to 18060, among them $A_5 \times B_1(43, 1, 7, 7)$ from Theorem 4.1(a). It verified all 397 lines of the certificate with its own verifier and data, the arithmetic of Theorem 4.1(c) up to $2 \cdot 10^6$, and explicit groups with primes (probable primes above 2^{64}) for $k \leq 800$; it repeated the scan of Section 7 for all primes up to $5 \cdot 10^6$, with the same least primes for all 422 values found; it repeated the literature search; and it ran the whole package again from the source archive, with the recorded outputs reproduced as described above. It found no error in the statements or proofs. Its corrections, all made, are these: the groups of Proposition 3.3 are metabelian but not metacyclic (this text had called both families metacyclic); the invariant $k(G)$ is not due to Xiang and Li, who introduced the notation $J(G)$ for it; two short

justifications were added in Section 3; and this run is recorded here and in the package.

Scope and priority. The note answers the first question of Problem 2.78 (Corollary 1.3): both sets are finite, the soluble numbers are determined, and the absolutely simple numbers are determined up to the value 11. The second question is open; Section 7 gives data only. Problem 3.57 is not treated. The problem and its notions are due to Trofimov [KM26]. Theorem 1.2 is due to Zhong [Zho05] and to Shi, Zhang and Liang [SZL15], and the invariant $k(G)$ appears as $r(G)$ in [Zho05] and as $J(G)$ in Xiang and Li [XL07]. We use Thompson’s classification [Tho68], Dickson’s theorem [Hup67], the Schur–Zassenhaus theorem [Isa08], Dirichlet’s theorem [Apo76] and the order of the Suzuki groups [Suz62]. Only Theorem 1.1, with Theorem 4.1 and Proposition 4.3, and hence the finiteness of the two sets and the exact set of soluble numbers, are, to our knowledge, not in print.

What was read: Problems 2.78 and 3.57 in the arXiv versions v48 and v49 of [KM26]; the zbMATH reviews of [Zho05, SZL15], the abstract of [SZL15], the zbMATH summary of [XL07] and the abstract of [HLC24]. We did not read the full texts of [Zho05, XL07, SZL15], nor Trofimov’s papers of 1962 and 1964 [Tro62, Tro64] and his notes of 1975 [Tro75], where group-theoretic numbers may have been introduced or studied; these are the main residual risk for the statement on novelty. The cited theorems of [Tho68, Hup67, Isa08, Apo76, Suz62] were not re-read for this note.

The searches were made on 21 October 2026: the zbMATH Open API (Trofimov’s papers; orders of non-normal subgroups; non-normal subgroups and solubility; the phrases “group-theoretic number” and “IE-system”; citing works), OpenAlex (topic searches and citing works), Crossref, the arXiv API, and a few web searches; the third verification run repeated them in part on the same day. The site mathnet.ru, which holds the Russian journal, was unreachable from our machine; the zbMATH web pages refused automated access (HTTP status 403), Project Euclid answered with a bot check, Semantic Scholar with HTTP status 429, and the site of the AMS refused the file of [Tho68] (HTTP status 403); none of this was worked around. No printed answer to the question was found in these sources; a search that finds nothing is not a proof of novelty, and we claim no priority. The Notebook v49 lists Problem 2.78 without comment.

AI-assisted tools were used to search the problem corpus and the literature, to find the arguments, to write and run the verification programs, and to help prepare this manuscript. The author has reviewed the proofs, the computations and the sources and is responsible for all claims. The note has not been peer reviewed.

References

- [Apo76] Tom M. Apostol. *Introduction to Analytic Number Theory*. Undergraduate Texts in Mathematics. Springer, New York, 1976. doi:10.1007/978-1-4757-5579-4.
- [HLC24] Lijuan He, Heng Lv, and Guiyun Chen. Solvable groups whose nonnormal subgroups have few orders. *Bulletin of the Australian Mathematical Society*, 110(1):121–128, 2024. doi:10.1017/S0004972723001168.
- [Hup67] Bertram Huppert. *Endliche Gruppen I*, volume 134 of *Grundlehren der mathematischen Wissenschaften*. Springer, Berlin, Heidelberg, 1967. doi:10.1007/978-3-642-64981-3.
- [Isa08] I. Martin Isaacs. *Finite Group Theory*, volume 92 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2008. doi:10.1090/gsm/092.
- [KM26] E. I. Khukhro and V. D. Mazurov. Unsolved Problems in Group Theory. The Kurovka Notebook, No. 21, 2026. Versions v48 (6 October 2026) and v49 (20 October 2026); Problems 2.78 and 3.57. arXiv:1401.0300.

- [Suz62] Michio Suzuki. On a class of doubly transitive groups. *Annals of Mathematics*, 75(1):105–145, 1962. doi:10.2307/1970423.
- [SZL15] Jiangtao Shi, Cui Zhang, and Dengfeng Liang. Finite groups with some nonnormal subgroups of non-prime-power order. *Hokkaido Mathematical Journal*, 44(3):387–396, 2015. zbMATH 1343.20020; only the abstract and the review were read. doi:10.14492/hokmj/1470053370.
- [Tho68] John G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. *Bulletin of the American Mathematical Society*, 74(3):383–437, 1968. doi:10.1090/S0002-9904-1968-11953-6.
- [Tro62] P. I. Trofimov. Zeichen für die Nichteinfachheit und Auflösbarkeit endlicher Gruppen. *Sibirskiiĭ Matematičeskiiĭ Žurnal*, 3:876–881, 1962. In Russian; title as in zbMATH 0122.03104; not read.
- [Tro64] P. I. Trofimov. Zur Frage der Auflösbarkeit endlicher Gruppen. *Sibirskiiĭ Matematičeskiiĭ Žurnal*, 5:192–200, 1964. In Russian; title as in zbMATH 0267.20009; not read.
- [Tro75] P. I. Trofimov. Zur Theorie der endlichen nichtauflösbaren Gruppen. *Sibirskiiĭ Matematičeskiiĭ Žurnal*, 16:416, 1975. In Russian; title as in zbMATH 0323.20014; English translation: On the theory of unsolvable groups, *Siberian Math. J.* 16 (1975), 321, zbMATH 0349.20005; not read.
- [ula26] ulamai. UnsolvedMath. Hugging Face dataset, <https://huggingface.co/datasets/ulamai/UnsolvedMath>, 2026. Version 1.8.0; record KOU-2.78.
- [XL07] Jianguo Xiang and Yangming Li. The number of the orders of non-normal subgroups and the structure of finite groups. *Journal of Foshan University (Natural Science Edition)*, 25(6):7–10, 2007. In Chinese; zbMATH 1144.20304; only the summary was read.
- [Zho05] Xianggui Zhong. A characteristic property of A_5 and the solvability of finite groups. *Journal of Applied Algebra and Discrete Structures*, 3(1):33–39, 2005. zbMATH 1070.20016; only the review was read.