

Groups of Odd Order with Conjugate Deficiency $16m$ (Kourovka Notebook Problem 20.52)

Alper Ferudun*

October 27, 2026

Abstract

For a finite group G let $k(G)$ be its number of conjugacy classes and $r(G) = |G| - k(G)$. Burnside proved that $16 \mid r(G)$ when $|G|$ is odd, and D. MacHale asked (Kourovka Notebook, Problem 20.52) whether every positive multiple $16m$ is $r(G)$ for a non-abelian group G of odd order. Since $r(G \times C_c) = cr(G)$, the question reduces to $m = 2^j$; this is Problem 5 of Buckley and MacHale (2013), who settled $j \leq 8$. We give explicit groups for every $j \leq 13$, so every $m < 16384$ occurs, and, by a computer-assisted search with exact certificates, for every $j \leq 120$ except $j \in \{14, 34, 64\}$. Besides direct products with Frobenius groups, the new examples are semidirect products $(M_1 \times M_2) \rtimes H$ of abelian groups by groups H of order at most 2187, mostly 3-groups, acting through two cyclic quotients; their class numbers are given by a closed formula that we prove: if H acts on M_i through H/K_i , every element outside K_i acting without non-trivial fixed points, then $k(G) = \sum_S \prod_{i \in S} (|M_i| - 1) k(K_S) / |H : K_S|$ with $K_S = \bigcap_{i \in S} K_i$. For example $(C_{13} \times C_{337}) \rtimes 3_+^{1+4}$ has $r(G) = 2^{20}$, which gives $j = 16$. For $j = 14$, that is $m = 16384$, we show that no group in several natural families works, among them $P \times F$ for every group P of odd order and every Frobenius group F with abelian kernel and complement of prime order. The question remains open, first for $m = 2^{14}$. This is an unrefereed note.

1 Introduction

1.1 The problem

Let G be a finite group with $k(G)$ conjugacy classes. Burnside [Bur11, p. 295] proved that $|G| - k(G)$ is divisible by 16 if $|G|$ is odd, and Hirsch [Hir50] showed that it is divisible by 48 if, in addition, $3 \nmid |G|$ (see also Poland [Pol68]). Buckley and MacHale [BM13] called $r(G) = |G| - k(G)$ the *conjugate deficiency* of G ; it vanishes exactly for abelian G , and $|G| \leq 27r(G)/16$ for every non-abelian G of odd order [BM13, (4)]. MacHale asked:

Problem 1.1 (MacHale [KM26, Problem 20.52]). *Is it true that for every integer $m > 0$ there is a finite non-abelian group $G(m)$ of odd order with $|G(m)| - k(G(m)) = 16m$?*

If A is abelian then $k(A \times G) = |A|k(G)$, so $r(A \times G) = |A|r(G)$ [BM13, p. 17]. Writing $m = 2^j c$ with c odd, a group with $r(G) = 2^{j+4}$ gives $r(G \times C_c) = 16m$; conversely an odd m is covered by $j = 0$. So Problem 1.1 asks exactly whether 2^{j+4} is a value of r on groups of odd order for every $j \geq 0$. This is Problem 5 of [BM13] (with $k = j + 4$), where the answer is shown to be positive for $0 \leq j \leq 8$ by groups of orders 21, 39, 75, 147, 291, 579, 1161, 2307, 4221; the authors add that these examples show

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

no pattern that would justify a conjecture. The Notebook prints Problem 20.52 without comment and without a mark in version 49 (October 2026) [KM26], and it is record KOU-20.52 of the UnsolvedMath collection [ula26], where it is listed as open.

1.2 Results

For an odd prime r and a positive integer N prime to r we say that N is an r -norm if $\text{ord}_r(q)$ divides e for every prime power q^e exactly dividing N ($\text{ord}_r(q)$ is the multiplicative order of q modulo r); for $r = 3$ this means that every prime $q \equiv 2 \pmod{3}$ occurs to an even power. More generally, for $o > 1$ an integer s prime to o is an o -size if $\text{ord}_o(q) \mid e$ for every $q^e \parallel s$. By Lemma 2.3 every r -norm, and every o -size, is the order of a fixed-point-free module of the kind used below.

Theorem 1.2. *For every j with $0 \leq j \leq 13$ the group G_j of Table 1 is non-abelian of odd order with $r(G_j) = 2^{j+4}$. Hence for every integer $m > 0$ whose 2-adic valuation is at most 13, in particular for every $m < 16384$, there is a non-abelian group $G(m)$ of odd order with $|G(m)| - k(G(m)) = 16m$.*

Theorem 1.3 (computer-assisted). *For every j with $15 \leq j \leq 120$ and $j \notin \{34, 64\}$ the certificate for j in Table 2 defines a non-abelian group G of odd order with $r(G) = 2^{j+4}$. Hence Problem 1.1 has a positive answer for every m whose 2-adic valuation is at most 120 and is not one of 14, 34, 64.*

The groups of Theorem 1.3 are of four kinds (Section 4): direct products $P \times F$ with F a Frobenius group $A \rtimes C_r$ with abelian kernel or a related group with a 3-part; semidirect products $(K \times A) \rtimes C_3$ in which C_3 acts non-trivially on a non-abelian group K ; and, for 21 of the 104 exponents, semidirect products of abelian groups by small groups H , mostly 3-groups, whose class numbers come from the following formula.

Theorem 1.4. *Let H be a finite group, let $K_1, \dots, K_t$ be normal subgroups of H with H/K_i cyclic, and let $M_1, \dots, M_t$ be finite abelian groups on which H acts so that K_i acts trivially on M_i and every element of $H \setminus K_i$ fixes only the identity of M_i . Put $G = (M_1 \times \dots \times M_t) \rtimes H$ and $K_S = \bigcap_{i \in S} K_i$ for $S \subseteq \{1, \dots, t\}$ ($K_\emptyset = H$). Then*

$$k(G) = \sum_{S \subseteq \{1, \dots, t\}} \prod_{i \in S} (|M_i| - 1) \frac{k(K_S)}{|H : K_S|}.$$

For $t = 1$ this is the familiar $k(G) = k(H) + (|M| - 1)k(K)/|H : K|$; the point is that for $t \geq 2$ only the class numbers of the intersections K_S enter.

Example 1.5. Let $H = 3_+^{1+2}$ be the extraspecial group of order 27 and exponent 3, $K_1 \neq K_2$ two of its subgroups of index 3, and M_1, M_2 modules of orders s_1, s_2 (Lemma 2.3). Here $k(H) = 11$, $k(K_i) = 9$ and $K_1 \cap K_2 = Z(H)$, so $k(G) = (s_1 s_2 + 8(s_1 + s_2) + 16)/3$ and

$$r(G) = 2^{j+4} \iff (10s_1 - 1)(10s_2 - 1) = 15 \cdot 2^{j+2} + 21.$$

For $j = 24$ the factorization $1006632981 = 8409 \cdot 119709$ gives $s_1 = 841 = 29^2$ and $s_2 = 11971$, both 3-norms, so this G of order 271825497 has $k(G) = 3390041$ and $r(G) = 2^{28}$; the same identity covers $j = 86$ and $j = 96$. With $H = 3_+^{1+4}$ and two subgroups of index 3 whose intersection is abelian one gets $k(G) = 3s_1 s_2 + 8(s_1 + s_2) + 64$, i.e. $(30s_1 - 1)(30s_2 - 1) = 15 \cdot 2^{j+2} + 241$; for $j = 16$, $3932401 = 389 \cdot 10109$ gives $(s_1, s_2) = (13, 337)$ and the group $(C_{13} \times C_{337}) \rtimes 3_+^{1+4}$ of order 1064583 with $k(G) = 16007$, $r(G) = 2^{20}$, which we also built and counted in GAP.

For the smallest open exponent we have only negative evidence.

Proposition 1.6 (computer-assisted). *No group G of odd order with $r(G) = 2^{18}$, that is $m = 2^{14}$, lies in any of the following classes:*

- (a) $P \rtimes F$, with P an arbitrary group of odd order and F either a Frobenius group $A \rtimes C_r$ with abelian kernel A and r prime, or a group $F_1(X)$ of Lemma 2.5;
- (b) $A \rtimes H$ with A abelian, H non-abelian of odd order at most 375 or $H = C_3^k$ with $k \leq 4$, and $\gcd(|A|, |H|) = 1$;
- (c) the groups of Theorem 1.4 with H abelian and $t \leq 2$; with H non-abelian and $t \leq 2$, if $|H| \leq 2187$ and H/H' has rank at most 4, or if $t = 1$ and either $|H| \leq 2187$ and H/H' has prime order, or $|H : K_1| = 3$ and $|H| \in \{3^6, 3^7\}$; and with H non-abelian and $t \geq 3$, if $|H| > 375$ or every $|M_i|$ is prime to $|H|$;
- (d) $(K \times A) \rtimes \langle s \rangle$ as in Lemma 2.6, with s of order $r \in \{3, 5, 7\}$, $r \nmid |K|$, and K a non-abelian group of odd order at most 4000 in the library that is a 3-group or has order prime to 3, or of order $7^5, 11^4, 13^4$ or p^3 with $17 \leq p \leq 59$ (234 distinct data $(r, |K|, k(K), k(C_K(s)))$).
- (e) every group with an abelian normal subgroup of prime index, and the groups of Theorem 1.4 with $t = 1$, $|H : K_1| \in \{3, 5, 7, 9, 15\}$ and H any group of odd order greater than 2187;

1.3 What is known, what is new, and what stays open

The reduction to $m = 2^j$, the bound $|G| \leq 27r(G)/16$ and the cases $j \leq 8$ are due to Buckley and MacHale [BM13]; the groups for $j \leq 8$ in Table 1 are theirs, except that for $j = 6$ we use $F_1(129)$ instead of their $C_{387} \rtimes C_3$ (both have order 1161 and 137 classes). New are the cases $9 \leq j \leq 13$ (Theorem 1.2), the 104 certificates of Theorem 1.3, Theorem 1.4, which we did not find in the literature in this form, and Proposition 1.6. We do not decide Problem 1.1: neither a family covering all j nor an obstruction for a single j is known to us. Proposition 1.6 does not exclude other structures, and the window $2^{18} < |G| \leq 27 \cdot 2^{14}$ for $j = 14$ contains orders such as $3^{10} \cdot 5$ for which no classification of the groups is available.

2 Class numbers of some semidirect products

All groups are finite. For a group H acting on an abelian group M and $U \leq H$, $\text{Irr}(M)^U$ is the set of U -invariant linear characters of M .

Lemma 2.1 (Burnside, Hirsch). *If $|G|$ is odd then $16 \mid r(G)$, and $48 \mid r(G)$ if moreover $3 \nmid |G|$. In particular a group of odd order with $r(G) = 2^{j+4}$ has order divisible by 3.*

Proof. Since $\sum_{\chi \in \text{Irr}(G)} \chi(1)^2 = |G|$ and $|\text{Irr}(G)| = k(G)$, $r(G) = \sum_{\chi} (\chi(1)^2 - 1)$. For $|G|$ odd the trivial character is the only real-valued irreducible character [Isa76, Problem 3.16], so the non-trivial ones fall into pairs $\{\chi, \bar{\chi}\}$; their degrees are odd, so each pair contributes $2(\chi(1)^2 - 1) \equiv 0 \pmod{16}$. If $3 \nmid |G|$ the degrees are also prime to 3 and each pair contributes a multiple of 48. $\square$

Lemma 2.2. *Let $G = A \rtimes H$ with A abelian. Then*

$$k(G) = \frac{1}{|H|} \sum_{\substack{(x,y) \in H^2 \\ xy=yx}} |\text{Irr}(A)^{\langle x,y \rangle}|.$$

For $h \in H$, $|\text{Irr}(A)^{\langle h \rangle}| = |C_A(h)|$.

Proof. Let $\lambda \in \text{Irr}(A)$ and H_λ its stabilizer. The inertia group of λ in G is $A \rtimes H_\lambda$, and λ extends to it by $\hat{\lambda}(ah) = \lambda(a)$. By Gallagher's theorem [Isa76, Corollary 6.17] the irreducible characters of $A \rtimes H_\lambda$ over λ are the $k(H_\lambda)$ characters $\hat{\lambda}\beta$, $\beta \in \text{Irr}(H_\lambda)$, and by the Clifford correspondence [Isa76, Theorem 6.11] induction maps them bijectively onto $\text{Irr}(G \mid \lambda)$. Summing over the H -orbits on $\text{Irr}(A)$,

$$k(G) = \sum_{\text{orbits}} k(H_\lambda) = \frac{1}{|H|} \sum_{\lambda \in \text{Irr}(A)} |H_\lambda| k(H_\lambda) = \frac{1}{|H|} \sum_{\lambda} \#\{(x, y) \in H_\lambda^2 : xy = yx\},$$

since $|H_\lambda|k(H_\lambda)$ is the number of commuting pairs in H_λ ; exchanging the sums gives the formula. For one element h , the invariant characters are those trivial on the image of the endomorphism $a \mapsto a^{-1}a^h$ of A , whose kernel is $C_A(h)$; so their number is $|A|/|A : C_A(h)| = |C_A(h)|$. $\square$

Proof of Theorem 1.4. Apply Lemma 2.2 with $A = M_1 \times \cdots \times M_t$, so that $\text{Irr}(A) = \text{Irr}(M_1) \times \cdots \times \text{Irr}(M_t)$ and a character is U -invariant if and only if each component is. Let $x, y \in H$ commute and $U = \langle x, y \rangle$. If $x, y \in K_i$ then U acts trivially on M_i and all $|M_i|$ characters of M_i are invariant. Otherwise one of x, y , say h , lies outside K_i ; then $C_{M_i}(h) = 1$, so by Lemma 2.2 only the trivial character of M_i is h -invariant. Hence

$$|\text{Irr}(A)^U| = \prod_{i=1}^t \left(1 + (|M_i| - 1)[x, y \in K_i]\right) = \sum_S \prod_{i \in S} (|M_i| - 1) [x, y \in K_S],$$

where $[\cdot]$ is 1 or 0. The number of commuting pairs in K_S is $|K_S|k(K_S)$, so summing over commuting pairs and dividing by $|H|$ gives the theorem. $\square$

No coprimality between $|A|$ and $|H|$ is needed, and the proof does not use that H/K_i is cyclic; cyclicity enters only through Lemma 2.3. For two modules,

$$k(G) = k(H) + \frac{(s_1 - 1)k(K_1)}{|H : K_1|} + \frac{(s_2 - 1)k(K_2)}{|H : K_2|} + \frac{(s_1 - 1)(s_2 - 1)k(K_1 \cap K_2)}{|H : K_1 \cap K_2|}, \quad s_i = |M_i|, \quad (1)$$

and $r(G) = |H|s_1s_2 - k(G) = 2^{j+4}$ is an equation $\alpha s_1s_2 + \beta s_1 + \gamma s_2 = \rho$ with integer coefficients, that is $(\alpha s_1 + \gamma)(\alpha s_2 + \beta) = \alpha\rho + \beta\gamma$; the search runs over the divisors of the right-hand side.

Lemma 2.3. *Let $o > 1$ and let s be an o -size. There are an abelian group M of order s and an automorphism τ of M of order o such that τ^i fixes only 0 for $0 < i < o$. Consequently, if $K \trianglelefteq H$ with $H/K = \langle gK \rangle$ cyclic of order o , then H acts on M by $h \mapsto \tau^a$ for $hK = g^aK$, with kernel K and with every element of $H \setminus K$ fixing only 0.*

Conversely, if H acts on an abelian group M with kernel containing K , H/K cyclic of order o , and every element of $H \setminus K$ fixes only 0, then $|M|$ is an o -size.

Proof. For each prime $q \mid s$ with $q^e \parallel s$ let $f = \text{ord}_o(q)$; the field $\mathbb{F}_{q^f}$ contains a primitive o -th root of unity ζ_q . Let $M = \bigoplus_q \mathbb{F}_{q^f}^{e/f}$ and let τ multiply the q -part by ζ_q . For $0 < i < o$, $\zeta_q^i \neq 1$, so $\tau^i - 1$ is injective. For the converse, let g generate H modulo K and $q \mid |M|$. If $q \mid o$, an element of $\langle g \rangle$ of order q modulo K acts on the q -group M_q with a non-trivial fixed point (orbits of a q -group on $M_q \setminus \{0\}$ have length 1 or a power of q); so $q \nmid o$. On each layer $q^i M_q / q^{i+1} M_q$ the action is coprime, so g^i ($0 < i < o$) has no fixed vectors there either, and every eigenvalue of g is a primitive o -th root of unity; its minimal polynomial over $\mathbb{F}_q$ has degree $\text{ord}_o(q)$, which therefore divides the dimension of the layer. $\square$

Lemma 2.4. *Let r be a prime and $N > 1$ an r -norm. Then $F = A \rtimes C_r$ with $|A| = N$ as in Lemma 2.3 (a Frobenius group) has $|F| = rN$ and $k(F) = r + (N - 1)/r$. If P is any group, $r(P \times F) = |P|rN - k(P)(r + (N - 1)/r)$.*

Proof. Theorem 1.4 with $t = 1$, $H = C_r$, $K = 1$: $k(F) = r + (N - 1)k(1)/r$. $\square$

Lemma 2.5. *Let ω be a primitive cube root of unity, $\pi = 1 - \omega$, $a \geq 1$, and D a 3-norm. Let $A = \mathbb{Z}[\omega]/(\pi^a) \oplus M$ with $|M| = D$ as in Lemma 2.3 ($o = 3$), and let s act as multiplication by ω on the first summand and as τ on M . Then $F_1(X) = A \rtimes \langle s \rangle$ with $X = 3^{a-1}D$ has $|F_1(X)| = 9X$ and $k(F_1(X)) = X + 8$.*

Proof. The fixed points of s form $\pi^{a-1}\mathbb{Z}[\omega]/(\pi^a)$, of order 3. By Lemma 2.2 with $H = \langle s \rangle$ of order 3: the identity pair contributes $|A|$ and each of the 8 other pairs generates $\langle s \rangle$ and contributes $|C_A(s)| = 3$, so $k(F) = (|A| + 24)/3 = X + 8$, where $|A| = 3X$. $\square$

For $a = 1$, $F_1(X) = C_3 \times (M \rtimes C_3)$; for $a = 2$ the 3-part is C_3^2 with s acting as a unipotent Jordan block.

Lemma 2.6. *Let L be a group, s an automorphism of L of prime order r with $r \nmid |L|$, and $G = L \rtimes \langle s \rangle$. Then $k(G) = rc + (k(L) - c)/r$ with $c = k(C_L(s))$. If $L = K \times A$ where s acts on A as in Lemma 2.3 with $|A| = N$, then $k(L) = k(K)N$ and $c = k(C_K(s))$.*

Proof. By Brauer's permutation lemma [Isa76, Theorem 6.32] s fixes as many irreducible characters of L as conjugacy classes, and by Glauberman's lemma [Isa76, Chapter 13] the s -invariant classes of L are in bijection with the classes of $C_L(s)$ (coprime action), so s fixes c characters. These extend to G [Isa76, Corollary 11.22], each in r ways (Gallagher), and the other characters lie in orbits of length r and induce irreducibly. For $L = K \times A$ the s -invariant characters are the products of invariant ones, and only the trivial character of A is invariant (Lemma 2.2). $\square$

Lemma 2.7. *Let G have an abelian normal subgroup A of prime index o , and let $x \in G \setminus A$. Then $k(G) = of + (|A| - f)/o$ with $f = |C_A(x)|$, so $r(G) = (o^2 - 1)(|A| - f)/o$. If $|G|$ is odd and $r(G) = 2^{j+4}$, then $o = 3$ and either $f = 1$ and $3 \cdot 2^{j+1} + 1 = |A|$ is a 3-norm, or $f = 3$ and $2^{j+1} + 1 = |A|/3 = 3^v D$ with D a 3-norm.*

Proof. As G/A is cyclic, the x -invariant characters of A extend to G [Isa76, Corollary 11.22], each in o ways, and the others lie in orbits of length o and induce irreducibly; by Lemma 2.2 there are $|C_A(x)|$ invariant characters. Since $\gcd(o, o^2 - 1) = 1$ and $o^2 - 1$ has an odd prime divisor unless $o = 3$, $r(G) = 2^{j+4}$ forces $o = 3$ and $|A| - f = 3 \cdot 2^{j+1}$; as f divides the odd number $|A|$, $f \in \{1, 3\}$. Conjugation by x induces an automorphism τ of A with $\tau^3 = 1$. On the part of A of order prime to 3, τ has no non-trivial fixed points (they would lie in $C_A(x)$, of order $f \leq 3$), so on each layer $q^i A_q / q^{i+1} A_q$ ($q \neq 3$ prime) its eigenvalues are primitive cube roots of unity, which for $q \equiv 2 \pmod{3}$ come in pairs: that part has 3-norm order D . If $f = 1$, $3 \nmid |A|$ (a 3-group acted on by an element of order 3 has fixed points), so $|A| = D$; if $f = 3$, $|A| = 3^{v+1}D$. $\square$

3 The exponents $j \leq 13$

Proof of Theorem 1.2. By Lemma 2.4, $C_N \rtimes C_3$ has $r = 3N - 3 - (N - 1)/3 = 8(N - 1)/3$, which equals 2^{j+4} if and only if $N = 3 \cdot 2^{j+1} + 1$. This N is a 3-norm for $j \in \{0, 1, 2, 3, 4, 5, 7, 9, 11, 12, 13\}$ (for $j = 2$, $N = 25 = 5^2$ and the module is $\mathbb{F}_{25}$), but not for $j = 6, 8, 10$, where $N = 385 = 5 \cdot 7 \cdot 11$, $1537 = 29 \cdot 53$, $6145 = 5 \cdot 1229$. For $j = 6$, Lemma 2.5 with $a = 2$, $D = 43$ gives $|F| = 9 \cdot 129$ and $k = 137$. For $j = 8$, $k = 5 \cdot 25 = 125$. For $j = 10$, $C_3 \wr C_3 = \text{SG}(81, 7)$ has 17 classes and $C_{41} \rtimes C_5$

j	G_j	$ G_j $	$k(G_j)$
0	$C_7 \rtimes C_3$	21	5
1	$C_{13} \rtimes C_3$	39	7
2	$C_5^2 \rtimes C_3 = \mathbb{F}_{25} \rtimes C_3$	75	11
3	$C_{49} \rtimes C_3$	147	19
4	$C_{97} \rtimes C_3$	291	35
5	$C_{193} \rtimes C_3$	579	67
6	$F_1(129) = (C_3^2 \times C_{43}) \rtimes C_3$	1161	137
7	$C_{769} \rtimes C_3$	2307	259
8	$(C_7 \rtimes C_3) \times (C_{67} \rtimes C_3)$	4221	125
9	$C_{3073} \rtimes C_3, 3073 = 7 \cdot 439$	9219	1027
10	$(C_3 \wr C_3) \times (C_{41} \rtimes C_5)$	16605	221
11	$C_{12289} \rtimes C_3$	36867	4099
12	$C_{24577} \rtimes C_3, 24577 = 7 \cdot 3511$	73731	8195
13	$C_{49153} \rtimes C_3, 49153 = 13 \cdot 19 \cdot 199$	147459	16387

Table 1: Groups with $r(G_j) = |G_j| - k(G_j) = 2^{j+4}$; in $C_N \rtimes C_3$ and $C_N \rtimes C_5$ the generator acts by a root of unity of that order modulo N without fixed points.

has $5 + 40/5 = 13$, so $k = 221$ and $r = 16605 - 221 = 2^{14}$. The values of $k(G_j)$ in Table 1 follow, and $r(G_j) = |G_j| - k(G_j) = 2^{j+4}$ in each row. All fourteen groups were also built in GAP and their classes counted directly (Section 6). The second statement follows from Section 1. $\square$

For $j = 10$ none of the 24319 groups of odd order n with $2^{14} < n \leq 27 \cdot 2^{10}$ in the library has $r(G) = 2^{14}$; of the 147 odd orders in this range that the library does not cover, GrpConst [BE26] was run on 22 and found four groups of order $16605 = 3^4 \cdot 5 \cdot 41$ with $r(G) = 2^{14}$, among them G_{10} . So solutions can be rare, which is one reason why no single family covers all j .

4 The certificates

A certificate for j names one of the following groups and the data from which $|G|$ and $k(G)$ follow by Section 2:

- (i) $P \times (A \rtimes C_r)$, P a named group (or 1), $N = |A|$ an r -norm: $r(G) = |P|rN - k(P)(r + (N-1)/r)$ (Lemma 2.4);
- (ii) $P \times F_1(X)$, $X = 3^v D$ with D a 3-norm: $r(G) = 9|P|X - k(P)(X + 8)$ (Lemma 2.5);
- (iii) $(K \times A) \rtimes \langle s \rangle$, s of order r acting on K with $k(C_K(s))$ given and on A as in Lemma 2.3: $r k(G) = r^2 c + k(K)N - c$ (Lemma 2.6);
- (iv) $(M_1 \times M_2) \rtimes H$ or $M_1 \rtimes H$ as in Theorem 1.4, with $H = \text{SG}(n, i)$, kernels K_i of cyclic quotients of orders o_i , $|M_i| = s_i$ an o_i -size, and the class numbers in (1).

The named groups are $\text{SG}(21, 1) = C_7 \rtimes C_3$, $\text{SG}(93, 1) = C_{31} \rtimes C_3$, $\text{SG}(81, 7) = C_3 \wr C_3$, $\text{SG}(465, 1) = C_{31} \rtimes C_{15}$, $\text{SG}(453, 1) = C_{151} \rtimes C_3$, $\text{SG}(125, 3) = 5_+^{1+2}$, $\text{SG}(1081, 1) = C_{47} \rtimes C_{23}$ for P ; $\text{SG}(125, 3)$ with an automorphism of order 3 centralizing exactly $Z(K)$, and $\text{SG}(1027, 1) = C_{79} \rtimes C_{13}$ with an automorphism of order 3 acting on C_{79} and centralizing a complement C_{13} , for K ; and the groups H of Table 2, which have order 9 to 2187 and, except $\text{SG}(165, 1) = C_3 \times (C_{11} \rtimes C_5)$ and $\text{SG}(117, 3) =$

$C_3 \times (C_{13} \rtimes C_3)$, are 3-groups; $\text{SG}(27, 3) = 3_+^{1+2}$ and $\text{SG}(243, 65) = 3_+^{1+4}$. Of the 104 certificates for $14 \leq j \leq 120$, 67 are of type (i), 14 of type (ii), 2 of type (iii) ($j = 54, 58$) and 21 of type (iv); the full list is Table 2 in the appendix. In every certificate G is non-abelian of odd order (it contains a non-abelian group of odd order, or H acts non-trivially).

Proof of Theorem 1.3. For each row of Table 2 the stated group exists by Lemmas 2.3 to 2.6 and Theorem 1.4 once (1) the sizes N , X , s_i have the stated factorizations into primes and satisfy the norm conditions, and (2) the named groups have the stated class numbers, automorphisms and kernels. Then $r(G) = 2^{j+4}$ is an identity between integers. (1) and the identity were checked in exact arithmetic, with a primality proof for every prime factor (Section 6); (2) was checked in GAP. The second statement follows as in Section 1. $\square$

The certificates were found by searches over these families (Section 6); for type (iv) the data are $k(H)$, $k(K_1)$, $k(K_2)$ and $k(K_1 \cap K_2)$ for all pairs of kernels of cyclic quotients of the non-abelian groups of odd order at most 2187 with H/H' of rank at most 4 (5133 distinct data sets), and the equation (1) was solved over the divisors of $\alpha\rho + \beta\gamma$. For the three exponents 14, 34, 64 all these numbers were completely factored (for 64 with the elliptic curve method), so for them the search over these data sets (and over the 179 groups with H/H' of prime order, which have only one such kernel) is exhaustive and finds nothing. The certificates for $j = 90$ and $j = 91$ were found last, by the same equation with H abelian (Section 5): for $j = 91$ it is simply $C_N \rtimes C_3$ with $N = 3 \cdot 2^{92} + 1 = 1132314641089 \cdot 13119392730926401$, which the first search of type (i) had missed because it factored N only by trial division up to 10^6 ; for $j = 90$ it is $(C_{s_1} \rtimes C_3) \times (C_{s_2} \rtimes C_3)$ ($H = C_3^2$, $K_1 \cap K_2 = 1$). All searches behind Proposition 1.6 and the final runs for $j \in \{34, 64\}$ factor completely.

5 The exponent 14

Proof of Proposition 1.6. Throughout $|G| - k(G) = 2^{18}$ and, by [BM13, (4)], $|G| \leq 27 \cdot 2^{14} = 442368$.

(a) For $P \times (A \rtimes C_r)$ the condition is $N(r^2|P| - k(P)) = r \cdot 2^{18} + (r^2 - 1)k(P)$, and for $P \times F_1(X)$ it is $X(9|P| - k(P)) = 2^{18} + 8k(P)$. If P is abelian, $r(G) = |P|r(F)$ forces $P = 1$; then $r(F) = (N - 1)(r^2 - 1)/r$ is a power of 2 only for $r = 3$, and $N = 3 \cdot 2^{15} + 1 = 5 \cdot 19661$, $X = 2^{15} + 1 = 3^2 \cdot 11 \cdot 331$ are not admissible. For non-abelian P of order at most 2187 all groups of the library were tried with all primes $r \leq 1000$ (for larger r , $|F| > 442368$); the library lacks only the odd orders 2025 and 2079 in this range, and for these no admissible N or X gives an integral value of $k(P)$ at most $11|P|/27$. For $|P| > 2187$ the order bound forces N (or X) to be small, and then $k(P) \leq 11|P|/27$ [BM13, (1)] confines $|P|$ to eleven intervals inside $[2189, 13825]$ ($r = 3$ with $N \in \{7, 13, 19, 25, 31, 37\}$, $r = 5$ with $N = 11$, and $X \in \{3, 7, 9, 13\}$, where for $F_1(X)$ the bound reads $|P| \leq 2^{18}/(9X - 11(X + 8)/27)$). All 4264 non-abelian groups in the library of these orders fail. Of the 56 orders in these intervals that are not in the library, only 13419, 10125 and 13689 give an integral required value of $k(P)$. For $13419 = 3^3 \cdot 7 \cdot 71$ the Sylow 71-subgroup and a subgroup L of order 497 are normal. If $L = C_{71} \rtimes C_7$, it has no automorphism of order 3, so $P = L \times Q$ with $k(P) \in \{17 \cdot 27, 17 \cdot 11\}$; if L is cyclic, C_{71} is central (a 3-group cannot act non-trivially on it), $P = C_{71} \times R$ and $71 \mid k(P)$. Neither gives the required 3931. For $10125 = 3^4 \cdot 5^3$ and $13689 = 3^4 \cdot 13^2$, GrpConst [BE26] constructs all 144, respectively 243, groups, and none has the required class number (1021, respectively 5065).

(b) For a coprime action, A has an H -invariant series whose factors are $\mathbb{F}_q$ -irreducible modules ($q \nmid |H|$), which correspond to the orbits of $\psi \mapsto \psi^{(q)}$ on $\text{Irr}(H)$, and $|C_A(U)|$ is the product of the orders of the fixed points on the factors; by Lemma 2.2, $k(G)$ therefore depends only on the numbers $\langle \psi|_U, 1_U \rangle$ for the abelian subgroups U generated by commuting pairs. For the 160 non-abelian groups H of odd order at most 375 and for C_3^k , $k \leq 4$, all choices compatible with the order bound were enumerated.

(c) and (d): for $j = 14$ the divisor searches of Section 4 and the analogous linear equations have small right-hand sides and were complete, also without the condition that the $|M_i|$ be prime to $|H|$; the 179 non-abelian groups of order at most 2187 with H/H' of prime order, which have a single kernel of a cyclic quotient and are therefore not in the data of pairs of kernels, were treated separately. For abelian H and $t = 1$, $k(G) = |H| + (s - 1)|K|/o$ gives $r(G) = (s - 1)|K|(o^2 - 1)/o$, a power of 2 only if $o = 3$ and $|K| \leq 3$, and then $s = 3 \cdot 2^{15} + 1$ or $s = 2^{15} + 1$ is not a 3-size. For abelian H and $t = 2$, $K_1 \cap K_2$ is central in G and meets $G' \leq M_1 \times M_2$ trivially, so $r(G) = |K_1 \cap K_2| r(G/(K_1 \cap K_2))$ forces $K_1 \cap K_2 = 1$; then H embeds in $C_{o_1} \times C_{o_2}$ and (1) reads $k(G) = h + (s_1 - 1)h/o_1^2 + (s_2 - 1)h/o_2^2 + (s_1 - 1)(s_2 - 1)/h$ with $h = |H|$; the order bound gives $o_1, o_2 \leq 333$, and all 17363 cases (o_1, o_2, h) with $o_i \leq 333$ fail (only 176 of them leave room for sizes s_i at least the smallest o_i -sizes); for $t = 1$ and $|H| \in \{3^6, 3^7\}$ all maximal subgroups of all non-abelian groups of these orders were used (116 distinct pairs $(k(H), k(K))$). For $t \geq 3$ the sizes are at least 7, so $|H| \leq 442368/7^3 < 1290$, and $|H| \leq 184$ if $t \geq 4$; the case $|H| \leq 375$ is part of (b). The K_i may be taken distinct, since two modules with the same kernel combine into one. For $t = 3$ and $375 < |H| \leq 1289$ the bound leaves the size multisets $\{7, 7, 7\}$, $\{7, 7, 11\}$, $\{7, 7, 13\}$, $\{7, 7, 19\}$, $\{7, 7, 23\}$, $\{7, 11, 11\}$, $\{7, 11, 13\}$ (7, 13, 19 are 3-sizes, 11 a 5-size, 19 also a 9-size, 23 an 11-size). All 886 non-abelian groups of these orders in the library with at least three kernels of cyclic quotients fail for the multisets with sizes 7, 13, 19 (2689776 choices of kernels and sizes prime to $|H|$, and 56514 further choices with a size dividing $|H|$), and the 167 such groups with a quotient of order 5 or 11 fail for the other four multisets (924 choices); the library contains all groups of odd order up to 2000. (e) For $t = 1$, Theorem 1.4 gives $ok(H) + (s - 1)k(K) = os|H| - o2^{18}$ with $o = |H : K|$ and $s \geq 7$ an o -size; abelian H was excluded under (c). Since $k(H) \leq 11|H|/27$ and $k(K) \leq |K| = |H|/o$, $|H|$ lies in $2^{18}/s < |H| \leq 2^{18}/(s - 11/27 - (s - 1)/o^2)$; if K is non-abelian, $k(K) \leq 11|K|/27$ gives narrower intervals. For $|H| > 2187$ this leaves 37 intervals. All 14390 library groups of the orders in the narrower intervals (all kernels) and all 18084 library groups of the further orders (abelian kernels) fail. If K is abelian, $M \times K$ is an abelian normal subgroup of G of index o , so Lemma 2.7 applies (for $o \in \{9, 15\}$ no case is arithmetically possible for the orders outside the library); for $j = 14$, $N = 98305 = 5 \cdot 19661$ and $2^{15} + 1 = 3^2 \cdot 11 \cdot 331$ are not admissible, which also proves the first part of (e). Of the 129 orders in the narrower intervals that the library does not cover, all groups of 127 orders were built with GrpConst and fail. For $21609 = 3^2 \cdot 7^4$ only $(o, s) = (3, 13)$ is possible and forces $k(K) \geq 2493$ for the non-abelian K of order $3 \cdot 7^4$; but $K/Z(K)$ is non-cyclic, and $K/Z(K) \cong C_7 \rtimes C_3$ gives $k(K) = 1715$, $K/Z(K) \cong C_7^2$ gives $k(K) = 1155$, and $|K : Z(K)| \geq 147$ gives $k(K) \leq \frac{149}{441}|K| < 2434$ by [BM13, Lemma 9]. For $10935 = 3^7 \cdot 5$ only $(o, s) = (3, 25)$ is possible, i.e. $k(H) + 8k(K) = 11231$: if the Sylow 5-subgroup is normal, $H = C_5 \times Q$ and 5 divides the left side; otherwise $H = P \rtimes C_5$ with P of order 3^7 and $P/\Phi(P)$ of rank at least 4, and the 52 groups obtained from the 13 groups P with $5 \mid |\text{Aut}(P)|$ fail. $\square$

6 Computations and reproducibility

The computations used GAP 4.16.1 [GAP26] with the packages SmallGrp 1.7.0 [BEO02], GrpConst 2.7.0 [BE26] and AutPGrp 1.12.0 [EO26], and Python 3.13.5 with SymPy 1.14.0 [M⁺17]; all scripts and outputs are in the source archive, whose `README.md` describes each program.

Direct checks. The groups $G_0, \dots, G_{13}$ of Table 1 were built and their classes counted (`verify_j1e13.g`). The group $(C_{13} \times C_{337}) \rtimes 3_+^{1+4}$ of Example 1.5 was built for both extraspecial groups of order 243, with $k(G) = 16007$ (`k_verify_j16.g`). For every group H used in type (iv) a small instance of the same shape (primes $q_i \equiv 1 \pmod{o_i}$) was built and its class number counted and compared with (1); they agree in all cases, as do small instances of Lemma 2.5 ($X = 21$: $k = 29$) and of $A \rtimes C_5$ ($N = 31$: $k = 11$), and Lemma 2.6 on two examples.

The certificates. The file `certificates.json` contains one certificate for each of the 118 exponents

$j \leq 120$ outside $\{14, 34, 64\}$. The program `check_certificates.py` reads only this file; it recomputes $|G|$ and $k(G)$ from the formulas of Section 2, checks $|G| - k(G) = 2^{j+4}$, checks the norm conditions, and proves each of the 242 distinct prime factors prime: by trial division below 10^6 and otherwise by Pocklington’s criterion [Poc14, BLS75] with $p - 1$ completely factored, recursively (247 primes above 10^6 are proved in this way, the largest with 33 digits); no probabilistic test is used. The GAP program `check_certificates.g` checks the group data: the class numbers of the named groups P , K and H , the existence of an automorphism of K of the stated order with the stated $k(C_K(s))$, and the existence of kernels with the stated indices, class numbers and intersections. All checks pass.

The searches. The certificates were found by the programs `cover_products*.py` (types (i), (ii)), `k_triples.g` and `cover_products5.py` (type (iii)), and `k_Hdata.g`, `cover_nonabH*.py`, `k_bilin_data.g`, `cover_bilin2.py` (type (iv)); the searches behind Proposition 1.6 are `windows_j14.txt`, `k_window_pairs.g`, `k_grpconst_j14.g`, `cover_elemH2.py`, `k_HK_pairs.g`, `k_three_j14*.g`, `cover_abelianH.py`, `k_t1_windows_j14*.g` and `k_t1_missing_j14*.g`, `k_10935_direct.g`, and, after the verification runs, `windows_j14_corr.txt`, `k_window_pairs_corr.g`, `k_three_j14_sizes11.g`, `k_t1_primequot.g` and `cover_elemH2_k*_j14.out`. A search that finds nothing proves nothing beyond its stated scope.

Verification runs. Two independent verification runs (AI-assisted, each with its own programs) re-derived the statement, the reduction and the proofs of Section 2, rebuilt the fourteen groups of Table 1 in GAP, re-checked all 118 certificates with their own checkers (arithmetic, Pocklington proofs of all 242 prime factors, the group data in GAP), counted classes directly in 32 built groups, among them the group of order 1064583 for $j = 16$, rejected deliberately wrong certificates, and searched the literature. They found gaps in the proof of Proposition 1.6: the intervals for $F_1(X)$, the size list for $t = 3$, the cyclic subgroup of order 497 for $|P| = 13419$, the groups with H/H' of prime order, and the missing archives of the searches with C_3^2 , C_3^3 . They are corrected here; none of the added cases gives a solution.

Sources. We read [BM13] in full (the open copy of the Irish Mathematical Society) and Problem 20.52 in version 49 of [KM26]. The results of Burnside, Hirsch and Poland are quoted from [BM13]; the part we use is proved in Lemma 2.1. Searches on 25 October 2026 of the arXiv, zbMATH Open and OpenAlex (including the works citing [BM13]; OpenAlex lists one, on a different invariant) found no further work on Problem 5 of [BM13] or on Problem 20.52; a search that finds nothing is not a proof of novelty, and we claim no priority.

AI-assisted tools were used to search the literature, to find the constructions and the formula of Theorem 1.4, to write and run the 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

- [BE26] Hans Ulrich Besche and Bettina Eick. GrpConst, Constructing the groups of a given order, Version 2.7.0. GAP package, 2026.
- [BEO02] Hans Ulrich Besche, Bettina Eick, and E. A. O’Brien. A millennium project: constructing small groups. *International Journal of Algebra and Computation*, 12(5):623–644, 2002.
doi:10.1142/S0218196702001115.
- [BLS75] John Brillhart, D. H. Lehmer, and J. L. Selfridge. New primality criteria and factorizations of $2^m \pm 1$. *Mathematics of Computation*, 29(130):620–647, 1975.
doi:10.1090/S0025-5718-1975-0384673-1.

- [BM13] Stephen M. Buckley and Desmond MacHale. Conjugate deficiency in finite groups. *Irish Mathematical Society Bulletin*, 71:13–19, 2013. Problem 5. doi:10.33232/BIMS.0071.13.19.
- [Bur11] W. Burnside. *Theory of Groups of Finite Order*. Cambridge University Press, 2nd edition, 1911. Reprinted by Dover, New York, 1955.
- [EO26] Bettina Eick and E. A. O’Brien. AutPGrp, Computing the automorphism group of a p -group, Version 1.12.0. GAP package, 2026.
- [GAP26] GAP. GAP – Groups, Algorithms, and Programming, Version 4.16.1. The GAP Group, <https://www.gap-system.org>, 2026.
- [Hir50] K. A. Hirsch. On a theorem of Burnside. *The Quarterly Journal of Mathematics*, 1:97–99, 1950. doi:10.1093/qmath/1.1.97.
- [Isa76] I. Martin Isaacs. *Character Theory of Finite Groups*, volume 69 of *Pure and Applied Mathematics*. Academic Press, New York, 1976. Reprinted by AMS Chelsea, 2006.
- [KM26] E. I. Khukhro and V. D. Mazurov (eds.). Unsolved Problems in Group Theory. The Kourovka Notebook. No. 21, <https://arxiv.org/abs/1401.0300>, 2026. Version 49 (20 October 2026); Problem 20.52 (D. MacHale, 20th issue, 2022).
- [M⁺17] Aaron Meurer et al. SymPy: symbolic computing in Python. *PeerJ Computer Science*, 3:e103, 2017. doi:10.7717/peerj-cs.103.
- [Poc14] H. C. Pocklington. The determination of the prime or composite nature of large numbers by Fermat’s theorem. *Proceedings of the Cambridge Philosophical Society*, 18:29–30, 1914.
- [Pol68] John Poland. Two problems on finite groups with k conjugate classes. *Journal of the Australian Mathematical Society*, 8:49–55, 1968. doi:10.1017/S1446788700004596.
- [ula26] ulamai. UnsolvedMath. Hugging Face dataset, <https://huggingface.co/datasets/ulamai/UnsolvedMath>, 2026. Version 1.8.0; record KOU-20.52.

A The certificates for $14 \leq j \leq 120$

In type (i) with $P = 1$, $G = A \rtimes C_r$ with $|A| = N$ as in Lemma 2.3 (so $G = C_N \rtimes C_r$ if N is square-free); in type (iv), $(o_i, k(K_i))$ are the order of H/K_i and the class number of K_i , and $K_{12} = K_1 \cap K_2$.

j	type	group data	parameters
15	(i)	$P = 1, r = 3$	$N = 196609 = 7 \cdot 28087$
16	(iv)	$H = \text{SG}(243, 65), k(H) = 83; (o_1, k(K_1)) = (3, 33),$ $(o_2, k(K_2)) = (3, 33); H : K_{12} = 9, k(K_{12}) = 27$	$s_1 = 13$ (prime), $s_2 = 337$ (prime)
17	(i)	$P = 1, r = 3$	$N = 786433$ (prime)
18	(ii)	$P = 1$	$X = 524289 = 3 \cdot 174763$
19	(i)	$P = 1, r = 3$	$N = 3145729 = 727 \cdot 4327$
20	(ii)	$P = 1$	$X = 2097153 = 3^2 \cdot 43 \cdot 5419$
21	(i)	$P = 1, r = 3$	$N = 12582913 = 7 \cdot 313 \cdot 5743$
22	(i)	$P = 1, r = 3$	$N = 25165825 = 5^2 \cdot 1006633$
23	(i)	$P = 1, r = 3$	$N = 50331649 = 61 \cdot 825109$
24	(iv)	$H = \text{SG}(27, 3), k(H) = 11; (o_1, k(K_1)) = (3, 9),$ $(o_2, k(K_2)) = (3, 9); H : K_{12} = 9, k(K_{12}) = 3$	$s_1 = 841 = 29^2, s_2 = 11971$ (prime)
25	(i)	$P = 1, r = 3$	$N = 201326593 = 13 \cdot 1567 \cdot 9883$
26	(ii)	$P = 1$	$X = 134217729 = 3^4 \cdot 19 \cdot 87211$
27	(i)	$P = 1, r = 3$	$N = 805306369 = 7 \cdot 37 \cdot 139 \cdot 22369$
28	(i)	$P = 1, r = 3$	$N = 1610612737 = 79 \cdot 20387503$
29	(i)	$P = 1, r = 3$	$N = 3221225473$ (prime)
30	(ii)	$P = 1$	$X = 2147483649 = 3 \cdot 715827883$
31	(i)	$P = 1, r = 3$	$N = 12884901889 = 19^2 \cdot 35692249$
32	(iv)	$H = \text{SG}(2187, 8693), k(H) = 139; (o_1, k(K_1)) =$ $(3, 73), (o_2, k(K_2)) = (3, 153); H : K_{12} = 9,$ $k(K_{12}) = 51$	$s_1 = 95179 = 7 \cdot 13597, s_2 = 331$ (prime)
33	(i)	$P = 1, r = 3$	$N = 51539607553 = 7 \cdot 181 \cdot 40678459$
35	(i)	$P = 1, r = 3$	$N = 206158430209$ (prime)
36	(ii)	$P = 1$	$X = 137438953473 = 3 \cdot 1777 \cdot 25781083$
37	(i)	$P = 1, r = 3$	$N = 824633720833 = 13 \cdot 829 \cdot 1063 \cdot 71983$
38	(i)	$P = C_{31} \rtimes C_3, r = 3$	$N = 16012305259 = 37 \cdot 11353 \cdot 38119$
39	(i)	$P = 1, r = 3$	$N = 3298534883329 = 7 \cdot 10243 \cdot 46004029$
40	(i)	$P = 1, r = 3$	$N = 6597069766657$ (prime)
41	(i)	$P = 1, r = 3$	$N = 13194139533313 = 103 \cdot 128098442071$
42	(ii)	$P = 1$	$X = 8796093022209 = 3 \cdot 2932031007403$
43	(i)	$P = 1, r = 3$	$N = 52776558133249 = 128413 \cdot 410990773$
44	(i)	$P = 1, r = 3$	$N = 105553116266497 = 859783 \cdot 122767159$
45	(i)	$P = 1, r = 3$	$N = 211106232532993 = 7^2 \cdot 4308290459857$
46	(iv)	$H = \text{SG}(243, 3), k(H) = 35; (o_1, k(K_1)) = (3, 33)$	$s_1 = 4853016839839 = 7 \cdot 693288119977$
47	(i)	$P = 1, r = 3$	$N = 844424930131969 = 367 \cdot 2300885368207$
48	(i)	$P = C_{151} \rtimes C_3, r = 3$	$N = 3357554394163 = 3217 \cdot 1043691139$
49	(i)	$P = 1, r = 3$	$N = 3377699720527873 = 13 \cdot 19 \cdot 51307 \cdot 266530837$

Table 2: Certificates for $15 \leq j \leq 120, j \notin \{34, 64\}$; types as in Section 4; $\text{SG}(n, i)$ is $\text{SmallGroup}(n, i)$.

j	type	group data	parameters
50	(iv)	$H = \text{SG}(243, 3)$, $k(H) = 35$; $(o_1, k(K_1)) = (3, 33)$, $(o_2, k(K_2)) = (3, 33)$; $ H : K_{12} = 9$, $k(K_{12}) = 27$	$s_1 = 25 = 5^2$, $s_2 = 3006408295975 = 5^2 \cdot 7 \cdot 1489 \cdot 11537593$
51	(i)	$P = 1$, $r = 3$	$N = 13510798882111489 = 7 \cdot 379 \cdot 997 \cdot 5107973329$
52	(i)	$P = C_7 \rtimes C_3$, $r = 3$	$N = 1174852076705347 = 43 \cdot 21787 \cdot 1254057067$
53	(i)	$P = 1$, $r = 3$	$N = 54043195528445953 = 3373 \cdot 179209 \cdot 89405629$
54	(iii)	$K = \text{SG}(125, 3)$, $r = 3$, $k(C_K(s)) = 5$	$N = 788951759539357$ (prime)
55	(i)	$P = 1$, $r = 3$	$N = 216172782113783809 = 109453 \cdot 1975028387653$
56	(i)	$P = C_{31} \rtimes C_{15}$, $r = 3$	$N = 829837935177673 = 2908771 \cdot 285288163$
57	(i)	$P = 1$, $r = 3$	$N = 864691128455135233 = 7 \cdot 49081 \cdot 2516804956399$
58	(iii)	$K = \text{SG}(1027, 1)$, $r = 3$, $k(C_K(s)) = 13$	$N = 1499897881101709$ (prime)
59	(i)	$P = 1$, $r = 3$	$N = 3458764513820540929 = 67 \cdot 307 \cdot 168154237630441$
60	(ii)	$P = 1$	$X = 2305843009213693953 = 3 \cdot 768614336404564651$
61	(i)	$P = 1$, $r = 3$	$N = 13835058055282163713 = 13 \cdot 211 \cdot 5295463 \cdot 952469857$
62	(i)	$P = 1$, $r = 3$	$N = 27670116110564327425 = 5^2 \cdot 39679 \cdot 27893965181143$
63	(i)	$P = 1$, $r = 3$	$N = 55340232221128654849 = 7 \cdot 37 \cdot 751 \cdot 284512450432261$
65	(i)	$P = 1$, $r = 3$	$N = 221360928884514619393$ (prime)
66	(ii)	$P = 1$	$X = 147573952589676412929 = 3 \cdot 7327657 \cdot 6713103182899$
67	(i)	$P = 1$, $r = 3$	$N = 885443715538058477569 = 19 \cdot 79 \cdot 150427 \cdot 3921520352047$
68	(iv)	$H = \text{SG}(81, 7)$, $k(H) = 17$; $(o_1, k(K_1)) = (3, 11)$, $(o_2, k(K_2)) = (3, 11)$; $ H : K_{12} = 9$, $k(K_{12}) = 9$	$s_1 = 91 = 7 \cdot 13$, $s_2 = 648914412266807239 = 7 \cdot 109 \cdot 14731 \cdot 57733867663$
69	(i)	$P = 1$, $r = 3$	$N = 3541774862152233910273 = 7 \cdot 505967837450319130039$
70	(iv)	$H = \text{SG}(2187, 5862)$, $k(H) = 75$; $(o_1, k(K_1)) = (3, 89)$, $(o_2, k(K_2)) = (3, 89)$; $ H : K_{12} = 9$, $k(K_{12}) = 243$	$s_1 = 1378658209 = 32587 \cdot 42307$, $s_2 = 6343213321$ (prime)
71	(i)	$P = 1$, $r = 3$	$N = 14167099448608935641089 = 271 \cdot 247854961 \cdot 210918189919$
72	(ii)	$P = 1$	$X = 9444732965739290427393 = 3 \cdot 1753 \cdot 1795918038741070627$
73	(i)	$P = 1$, $r = 3$	$N = 56668397794435742564353 = 13 \cdot 9907 \cdot 2489413 \cdot 176749610491$
74	(iv)	$H = \text{SG}(729, 398)$, $k(H) = 57$; $(o_1, k(K_1)) = (3, 35)$, $(o_2, k(K_2)) = (3, 51)$; $ H : K_{12} = 9$, $k(K_{12}) = 17$	$s_1 = 232852036459 = 7 \cdot 2221 \cdot 14977297$, $s_2 = 1785084751 = 19 \cdot 93951829$
75	(i)	$P = 1$, $r = 3$	$N = 226673591177742970257409 = 7 \cdot 4561 \cdot 34369 \cdot 206574122607943$
76	(i)	$P = 1$, $r = 3$	$N = 453347182355485940514817 = 11^2 \cdot 3746670928557735045577$
77	(i)	$P = 1$, $r = 3$	$N = 906694364710971881029633 = 6271 \cdot 144585291773396887423$
78	(ii)	$P = 1$	$X = 604462909807314587353089 = 3 \cdot 201487636602438195784363$
79	(i)	$P = 1$, $r = 3$	$N = 3626777458843887524118529 = 2521 \cdot 1438626520763144595049$
80	(ii)	$P = 1$	$X = 2417851639229258349412353 = 3^5 \cdot 19 \cdot 163 \cdot 87211 \cdot 135433 \cdot 272010961$
81	(i)	$P = 1$, $r = 3$	$N = 14507109835375550096474113 = 7 \cdot 165804817111 \cdot 12499300673569$
82	(i)	$P = 1$, $r = 3$	$N = 29014219670751100192948225 = 5^2 \cdot 439 \cdot 33961 \cdot 131449 \cdot 592200281599$
83	(i)	$P = 1$, $r = 3$	$N = 58028439341502200385896449 = 61 \cdot 1336519 \cdot 711763836387135811$
84	(i)	$P = 1$, $r = 3$	$N = 116056878683004400771792897 = 7 \cdot 2161 \cdot 7672167560190678969511$

Table 3: Certificates for $15 \leq j \leq 120$, $j \notin \{34, 64\}$ (continued).

j	type	group data	parameters
85	(i)	$P = 1, r = 3$	$N = 232113757366008801543585793 = 13 \cdot 19 \cdot 939731811198416200581319$
86	(iv)	$H = \text{SG}(27, 3), k(H) = 11; (o_1, k(K_1)) = (3, 9), (o_2, k(K_2)) = (3, 9); H : K_{12} = 9, k(K_{12}) = 3$	$s_1 = 1453$ (prime), $s_2 = 31951787096979668462191 = 349 \cdot 2427777223 \cdot 37710378733$
87	(i)	$P = 1, r = 3$	$N = 928455029464035206174343169 = 7^2 \cdot 3370243 \cdot 236223769 \cdot 23800165843$
88	(iv)	$H = \text{SG}(729, 95), k(H) = 89; (o_1, k(K_1)) = (3, 35), (o_2, k(K_2)) = (3, 35); H : K_{12} = 9, k(K_{12}) = 81$	$s_1 = 1181030296608889 = 109267 \cdot 10808664067, s_2 = 5823258457 = 31 \cdot 187847047$
89	(i)	$P = 1, r = 3$	$N = 3713820117856140824697372673 = 5227 \cdot 865890601 \cdot 820550546108299$
90	(iv)	$H = \text{SG}(9, 2), k(H) = 9; (o_1, k(K_1)) = (3, 3), (o_2, k(K_2)) = (3, 3); H : K_{12} = 9, k(K_{12}) = 1$	$s_1 = 25958731291$ (prime), $s_2 = 85839791080037359 = 167230543 \cdot 513302113$
91	(i)	$P = 1, r = 3$	$N = 14855280471424563298789490689 = 1132314641089 \cdot 13119392730926401$
92	(ii)	$P = 1$	$X = 9903520314283042199192993793 = 3^2 \cdot 529510939 \cdot 715827883 \cdot 2903110321$
93	(i)	$P = 1, r = 3$	$N = 59421121885698253195157962753 = 7 \cdot 51109 \cdot 166090741316732734226731$
94	(iv)	$H = \text{SG}(729, 95), k(H) = 89; (o_1, k(K_1)) = (3, 35), (o_2, k(K_2)) = (3, 35); H : K_{12} = 9, k(K_{12}) = 81$	$s_1 = 23515172137$ (prime), $s_2 = 18717977306238121$ (prime)
95	(i)	$P = C_{47} \rtimes C_{23}, r = 3$	$N = 195947640183671074015360141 = 7 \cdot 31 \cdot 1051 \cdot 1777 \cdot 7297 \cdot 66259142888767$
96	(iv)	$H = \text{SG}(27, 3), k(H) = 11; (o_1, k(K_1)) = (3, 9), (o_2, k(K_2)) = (3, 9); H : K_{12} = 9, k(K_{12}) = 3$	$s_1 = 109$ (prime), $s_2 = 436518801731483953683437743 = 13 \cdot 433 \cdot 1093 \cdot 9181 \cdot 7727901116581099$
97	(i)	$P = 1, r = 3$	$N = 950737950171172051122527404033 = 13 \cdot 499 \cdot 24781 \cdot 5914228559997646913539$
98	(iv)	$H = \text{SG}(243, 28), k(H) = 19; (o_1, k(K_1)) = (3, 33), (o_2, k(K_2)) = (3, 17); H : K_{12} = 9, k(K_{12}) = 27$	$s_1 = 13986866825048041 = 73 \cdot 6121 \cdot 31302224377, s_2 = 1510524856501$ (prime)
99	(i)	$P = 1, r = 3$	$N = 3802951800684688204490109616129 = 7 \cdot 37 \cdot 12439951 \cdot 358252591 \cdot 3294678541291$
100	(i)	$P = 1, r = 3$	$N = 7605903601369376408980219232257 = 97 \cdot 57735121 \cdot 1358122681230804234961$
101	(i)	$P = 1, r = 3$	$N = 15211807202738752817960438464513 = 193 \cdot 78817653900200791802903826241$
102	(i)	$P = 1, r = 3$	$N = 30423614405477505635920876929025 = 5^2 \cdot 7 \cdot 173849225174157175062405011023$
103	(i)	$P = 1, r = 3$	$N = 60847228810955011271841753858049 = 19 \cdot 2437 \cdot 387466563223 \cdot 3391543900660921$
104	(iv)	$H = \text{SG}(729, 276), k(H) = 153; (o_1, k(K_1)) = (9, 17), (o_2, k(K_2)) = (3, 99); H : K_{12} = 27, k(K_{12}) = 11$	$s_1 = 19079831794123$ (prime), $s_2 = 23344266818848357 = 151 \cdot 3011221 \cdot 51340567$
105	(i)	$P = 1, r = 3$	$N = 243388915243820045087367015432193 = 7 \cdot 13567 \cdot 12417571 \cdot 206386971472536639907$
106	(iv)	$H = \text{SG}(729, 188), k(H) = 57; (o_1, k(K_1)) = (3, 35), (o_2, k(K_2)) = (3, 35); H : K_{12} = 9, k(K_{12}) = 33$	$s_1 = 10590184498806485155547351917 = 19 \cdot 557378131516130797660386943, s_2 = 169 = 13^2$
107	(iv)	$H = \text{SG}(81, 12), k(H) = 33; (o_1, k(K_1)) = (3, 27), (o_2, k(K_2)) = (3, 11); H : K_{12} = 9, k(K_{12}) = 9$	$s_1 = 1019056616555019901 = 19 \cdot 601 \cdot 89242194286279, s_2 = 31844997460051 = 67 \cdot 163 \cdot 2915941531$
108	(ii)	$P = 1$	$X = 649037107316853453566312041152513 = 3 \cdot 104124649 \cdot 2077756847362348863128179$
109	(i)	$P = 1, r = 3$	$N = 3894222643901120721397872246915073 = 13^2 \cdot 7603 \cdot 44317579 \cdot 68386921674510929641$
110	(i)	$P = 5_+^{1+2}, r = 3$	$N = 56849965604395922940114923312629 = 229 \cdot 248253124910025864367314075601$
111	(i)	$P = 1, r = 3$	$N = 15576890575604482885591488987660289 = 7 \cdot 5526931 \cdot 319534819 \cdot 388369171 \cdot 3244410133$
112	(iv)	$H = \text{SG}(165, 1), k(H) = 21; (o_1, k(K_1)) = (3, 7), (o_2, k(K_2)) = (15, 11); H : K_{12} = 15, k(K_{12}) = 11$	$s_1 = 547322769298546249479829387 = 18897883 \cdot 28962120746463836689, s_2 = 924031$ (prime)
113	(i)	$P = 1, r = 3$	$N = 62307562302417931542365955950641153 = 3067 \cdot 344917 \cdot 11667127 \cdot 5048338402742350801$
114	(iv)	$H = \text{SG}(729, 276), k(H) = 153; (o_1, k(K_1)) = (9, 17), (o_2, k(K_2)) = (3, 243); H : K_{12} = 27, k(K_{12}) = 27$	$s_1 = 3709$ (prime), $s_2 = 123073384319465913585249491521 = 409 \cdot 300912920096493676247553769$
115	(i)	$P = 1, r = 3$	$N = 249230249209671726169463823802564609 = 1993 \cdot 2659 \cdot 10677478723 \cdot 4404599255303259409$
116	(ii)	$P = 1$	$X = 166153499473114484112975882535043073 = 3^3 \cdot 19 \cdot 2731 \cdot 22366891 \cdot 5302306226370307681801$
117	(i)	$P = 1, r = 3$	$N = 996920996838686904677855295210258433 = 7 \cdot 29582727613 \cdot 4814203988413999592172163$
118	(iv)	$H = \text{SG}(117, 3), k(H) = 21; (o_1, k(K_1)) = (3, 7), (o_2, k(K_2)) = (3, 7); H : K_{12} = 9, k(K_{12}) = 13$	$s_1 = 7$ (prime), $s_2 = 6580336612796613232197064654853191 = 7 \cdot 940048087542373318885294950693313$

Table 4: Certificates for $15 \leq j \leq 120, j \notin \{34, 64\}$ (continued).

j	type	group data	parameters
119	(i)	$P = 1, r = 3$	$N = 3987683987354747618711421180841033729 = 7591 \cdot 743329565653 \cdot 706708534276472766523$
120	(iv)	$H = \text{SG}(81, 7), k(H) = 17; (o_1, k(K_1)) = (3, 27),$ $(o_2, k(K_2)) = (3, 11); H : K_{12} = 9, k(K_{12}) = 9$	$s_1 = 280873 = 157 \cdot 1789, s_2 = 946497636678870511618341620593 = 484327 \cdot 8326896181 \cdot 234691685200939$

Table 5: Certificates for $15 \leq j \leq 120, j \notin \{34, 64\}$ (continued).