

Immediate Descendants of the Elliptic-Curve Groups of Maglione and Stanojkovski

Alper Ferudun*

October 28, 2026

Abstract

For a prime $p \geq 5$, an elliptic curve $E: y^2 = x^3 + ax + b$ over $\mathbb{F}_p$ and a point $P \in E(\mathbb{F}_p)$ other than the origin, Maglione and Stanojkovski defined a group $G_{E,P}(\mathbb{F}_p)$ of order p^9 , class 2 and exponent p . In the problem session of Oberwolfach Report 27/2025, Maglione asked which pairs (E, P) yield an immediate descendant, defined there as a central extension by $\mathbb{Z}/p\mathbb{Z}$ of class 3 and order p^{10} , and remarked that it would be remarkable if the sum, over the isomorphism classes of these groups, of the numbers of immediate descendants were a PORC function of p . We prove that $G_{E,P}(\mathbb{F}_p)$ has an immediate descendant if and only if P has order 2, and is terminal otherwise; for P of order 2 the nucleus has rank 2. For these pairs we give the number of immediate descendants of order p^{10} , and of those of exponent p , as explicit functions of p , of $|E[3](\mathbb{F}_p)|$ and of the order of the stabilizer of P in the automorphism group of E ; this contains the theorem of du Sautoy and Vaughan-Lee for $y^2 = x^3 - x$ and $P = (0, 0)$. Summed over the isomorphism classes, both numbers are PORC, with moduli 72 and 12: the dependence on $|E[3](\mathbb{F}_p)|$ cancels because the pairs (E, P) with given 3-torsion are parametrized by curves of genus 0. This answers both questions with the source's definition of an immediate descendant. If the descendants of order p^{11} , which are immediate descendants in O'Brien's sense, are counted as well, the PORC question remains open. The question is Maglione's; the groups, their classification and their automorphism groups are due to Maglione and Stanojkovski. This is an unrefereed note.

1 Introduction

1.1 The question

Let $p \geq 5$ be a prime, let $a, b \in \mathbb{F}_p$ with $4a^3 + 27b^2 \neq 0$, let E be the elliptic curve $y^2z = x^3 + axz^2 + bz^3$ with origin $O = (0 : 1 : 0)$, and let $P = (\lambda : \mu : 1) \in E(\mathbb{F}_p)$, so $P \neq O$. Following [DENR25, pp. 1421–1422] and [MS25, (1.3)] put

$$C_{E,P} = \begin{pmatrix} y_1 - \lambda y_3 & y_2 - \mu y_3 & 0 \\ y_2 + \mu y_3 & \lambda y_1 + (a + \lambda^2)y_3 & y_1 \\ 0 & y_1 & -y_3 \end{pmatrix}, \quad B_{E,P} = \begin{pmatrix} 0 & C_{E,P} \\ -C_{E,P}^t & 0 \end{pmatrix} \quad (1)$$

(in [MS25] the matrix $C_{E,P}$ is called $J_{E,P}$). Identify a linear form $c_1y_1 + c_2y_2 + c_3y_3$ with the vector (c_1, c_2, c_3) of $W := \mathbb{F}_p^3$, and let $V := \mathbb{F}_p^6$ with basis $e_1, \dots, e_6$. Then $B_{E,P}$ defines the alternating bilinear map $t = t_{E,P}: V \times V \rightarrow W$ with $t(e_i, e_{3+j}) = (C_{E,P})_{ij} = -t(e_{3+j}, e_i)$ for $1 \leq i, j \leq 3$, and $t = 0$ on $\langle e_1, e_2, e_3 \rangle$ and on $\langle e_4, e_5, e_6 \rangle$. The group $G_{E,P}(\mathbb{F}_p)$ is the Baer group of t [MS25, §2.4]: the set $V \oplus W$ with

$$(v, w)(v', w') = (v + v', w + w' + \tfrac{1}{2}t(v, v')).$$

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

It has order p^9 , class 2 and exponent p , its commutator map is t , and its derived subgroup is W , because t is onto. Let $\mathcal{G}_p$ be the set of all groups $G_{E,P}(\mathbb{F}_p)$, for all a, b and all $P \in E(\mathbb{F}_p) \setminus \{O\}$. By [MS25, Theorem A], for the prime field $G_{E,P}(\mathbb{F}_p) \cong G_{E',P'}(\mathbb{F}_p)$ if and only if there is an isomorphism of elliptic curves $E' \rightarrow E$ mapping P' to P .

In the problem session of [DENR25, pp. 1443–1444] Maglione asks which pairs (E, P) yield an immediate descendant, namely for which pairs there is a central extension

$$1 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow G \longrightarrow G_{E,P}(\mathbb{F}_p) \longrightarrow 1 \quad (2)$$

with G of nilpotency class 3 and order p^{10} . Maglione recalls that du Sautoy and Vaughan-Lee [dSVL12] showed that for $y^2 = x^3 - x$ and $P = (0, 0)$ the number of immediate descendants is not PORC, and adds that it “would be remarkable” if the sum of the numbers of immediate descendants of all groups in $\mathcal{G}_p$, up to isomorphism, were PORC. So there are two questions. (Q1) For which pairs (E, P) does a group G as in (2) exist? (Q2) Is $p \mapsto \sum_{[H]} (\text{number of immediate descendants of } H)$ a PORC function, the sum running over the isomorphism classes $[H]$ of groups in $\mathcal{G}_p$? They form the record OWR-14299292-015 of the UnsolvedMath collection [ula26], where they are listed as open.

Descendants, and two readings of (Q2). In O’Brien’s p -group generation [O’B90], G is an immediate descendant of a p -group H of p -class c if G has p -class $c + 1$ and $G/P_c(G) \cong H$, where $P_0(G) = G$ and $P_{i+1}(G) = [P_i(G), G]P_i(G)^p$; H is terminal if it has none. Du Sautoy and Vaughan-Lee [dSVL12, §1] call immediate descendants of their group the class-3 groups K with $K/\gamma_3(K)$ isomorphic to it; these have order p^{10} or p^{11} . The source defines an immediate descendant as a group G as in (2), of order p^{10} . For the groups $G_{E,P}(\mathbb{F}_p)$ the three notions give the same groups of order p^{10} , of exponent p or p^2 (Lemma 2.1); we count groups up to isomorphism. So in the source’s own sense the numbers in (Q2) count descendants of order p^{10} , and Theorem 1.3 answers (Q2). If one counts all immediate descendants in O’Brien’s sense, those of order p^{11} included, (Q2) remains open; Remark 6.6 only records computed values for order p^{11} .

PORC. A function f on the primes $p \geq 5$ is PORC if there are an integer $N \geq 1$ and polynomials $g_0, \dots, g_{N-1}$ with rational coefficients such that $f(p) = g_k(p)$ whenever $p \equiv k \pmod{N}$; we then say that f is PORC with modulus N . The footnote of the source on PORC [DENR25, p. 1444] does not specify the coefficients, while [MS25, §1.4] requires $g_k \in \mathbb{Z}[x]$. Rational coefficients are the usage of du Sautoy and Vaughan-Lee, whose theorem motivates (Q2): their count of descendants of exponent p is $(p + 1)^2/4 + 3$ for $p \equiv 5 \pmod{12}$ [dSVL12, Theorem 1]; and in the theory around Higman’s PORC conjecture [Hig60a, Hig60b] the polynomials have rational coefficients in general (see [VL18a, §7]). With integer coefficients neither that count nor the totals of Theorem 1.3, whose polynomials have denominators 3 and 27 (and integer values), would be PORC, since two polynomials that agree at infinitely many primes are equal.

1.2 Results

Throughout, $\delta_k := 1$ if $p \equiv 1 \pmod{k}$ and $\delta_k := 0$ otherwise. For a point P of order 2 put $e_3 := |E[3](\mathbb{F}_p)|$ and $s := |\{\sigma \in \text{Aut}_O(E) : \sigma(P) = P\}|$, where $\text{Aut}_O(E)$ is the group of automorphisms of the elliptic curve. Then $s = 4$ if $b = 0$, $P = (0, 0)$ and $p \equiv 1 \pmod{4}$, and $s = 2$ otherwise (Lemma 6.1).

Theorem 1.1 (answer to (Q1)). *Let $p \geq 5$, let E and $P = (\lambda : \mu : 1)$ be as above, and $H = G_{E,P}(\mathbb{F}_p)$. The following are equivalent: (i) there is a group G of order p^{10} and class 3 with a central subgroup Z of order p such that $G/Z \cong H$; (ii) H has an immediate descendant of order p^{10} ; (iii) H is not terminal; (iv) $\mu = 0$, that is, P is a point of order 2. If $\mu = 0$, the nucleus of H has rank 2; then H has immediate descendants of orders p^{10} and p^{11} and of no other order, and among those of order p^{10} there are groups of exponent p and groups of exponent p^2 .*

Theorem 1.2 (the number of descendants of one group). *Let $p \geq 5$ and $P \in E[2](\mathbb{F}_p) \setminus \{O\}$, and put*

$$\begin{aligned} F_1 &= p^6 + 2p^5 + 5p^4 + 8p^3 + 15p^2 + 12p + 9 + 2\delta_3(p^2 + p + 1)^2, \\ F_{\text{refl}} &= 2p^3 + 7p^2 + 16p + 15 + 4\delta_4(p + 2) + 2\delta_3(p + 2)^2, \\ F_{\text{transl}} &= 8 \text{ if } p \equiv 2 \pmod{3}, \quad F_{\text{transl}} = 6p + 46 + 18\delta_9 \text{ if } p \equiv 1 \pmod{3}, \\ F_{\text{ord4}} &= 6p + 34 + 12\delta_8 + 18\delta_3, \end{aligned}$$

and $F_1^e = p^2 + p + 2$, $F_{\text{refl}}^e = p + 3$, $F_{\text{transl}}^e = 2 + 2\delta_3$, $F_{\text{ord4}}^e = 4$. Then the number of immediate descendants of order p^{10} of $G_{E,P}(\mathbb{F}_p)$ is

$$d_{10}(E, P) = \frac{F_1 + e_3 F_{\text{refl}} + (e_3 - 1) F_{\text{transl}} + [s = 4] 2e_3 F_{\text{ord4}}}{e_3 s},$$

and the number $d_{10}^e(E, P)$ of those of exponent p is given by the same formula with F^e in place of F . The type (e_3, s) is one of those in Table 1.

Table 1 lists d_{10}^e for each type; at $p = 5$, $(d_{10}, d_{10}^e) = (13496, 20)$, $(4684, 10)$, $(6780, 12)$ for the types $(1, 2)$, $(3, 2)$, $(1, 4)$. Moreover $d_{10}^e(E, P) = 1 + |\mathbb{P}^2(\mathbb{F}_p)/\Gamma|$ for a natural action of a group $\Gamma \cong E[3](\mathbb{F}_p) \rtimes \text{Stab}(P)$ on the projective plane (Remark 5.4). For $y^2 = x^3 - x$ and $P = (0, 0)$, Theorem 1.2 contains [dSVL12, Theorem 1] and gives the number of all descendants of order p^{10} , for instance 6780, 87328, 365098 and 1451506 for $p = 5, 7, 11, 13$ (Corollary 5.5).

Theorem 1.3 (answer to (Q2) for descendants of order p^{10}). *For $p \geq 5$ let $S_{10}(p)$ be the sum, over the isomorphism classes $[H]$ of groups in $\mathcal{G}_p$, of the number of immediate descendants of H of order p^{10} , and $S_{10}^e(p)$ the same sum for descendants of order p^{10} and exponent p . Then*

$$S_{10}(p) = A(p) + \delta_4(4p^2 + 16p + 60 + 36\delta_3 + 24\delta_8) + \delta_9 \frac{14p-26}{3},$$

where

$$\begin{aligned} A(p) &= \frac{1}{3}(2p^7 + 4p^6 + 10p^5 + 22p^4 + 45p^3 + 51p^2 + 23p - 69) & \text{if } p \equiv 2 \pmod{3}, \\ A(p) &= \frac{1}{27}(20p^7 + 26p^6 + 112p^5 + 196p^4 + 441p^3 + 473p^2 + 213p - 1373) & \text{if } p \equiv 1 \pmod{3}, \end{aligned}$$

and $S_{10}^e(p) = \frac{1}{3}(2p^3 + 5p^2 + 12p - 15) + 8\delta_4$ if $p \equiv 2 \pmod{3}$, $S_{10}^e(p) = \frac{1}{27}(p-1)(20p^2 + 53p + 161) + 8\delta_4$ if $p \equiv 1 \pmod{3}$. In particular S_{10} is PORC with modulus 72 and S_{10}^e is PORC with modulus 12.

For example $S_{10}(5) = 90472$, $S_{10}^e(5) = 148$. The number $d_{10}(E, P)$ itself depends on e_3 , which for a fixed curve over $\mathbb{Q}$ is in general not PORC in p [MS25, Corollary C, Remark 1.2]; this is the mechanism of [dSVL12]. In the sum the dependence on e_3 cancels, because the pairs (E, P) with a point of order 3, or with full 3-torsion, are counted by points on curves of genus 0 (Remark 6.5). So the alternative that the source calls remarkable is what happens, for descendants of order p^{10} .

1.3 What is known, and what is new

The question is Maglione's [DENR25, pp. 1443–1444]. The groups $G_{E,P}(\mathbb{F}_p)$, their isomorphism classification [MS25, Theorem A] and the structure of their automorphism groups [MS25, Theorems 2.15, 5.6, 5.8, Lemmas 5.4, 5.5] are due to Maglione and Stanojkovski; we use these results. The nilpotent group with the arithmetic of $y^2 = x^3 - x$ goes back to du Sautoy [dS01, dS02]; its finite quotient G_p is $G_{E,(0,0)}(\mathbb{F}_p)$ for $E: y^2 = x^3 - x$ (Corollary 5.5). Du Sautoy and Vaughan-Lee [dSVL12] counted the descendants of order p^{10} and exponent p of G_p (their Theorem 1) and proved that the number of

descendants of order p^{10} , with or without the condition on the exponent, is not PORC (their Corollaries 1 and 2). We use O'Brien's p -group generation [O'B90], the Lazard correspondence [Laz54], and the counting of descendants through Lie rings as in [NOVL04, dSVL12].

To our knowledge the following are not in print: the criterion of Theorem 1.1; the counts of Theorem 1.2 for all pairs other than that of [dSVL12], and the count of all descendants of order p^{10} of that group; and Theorem 1.3. The searches are described in the paragraph "Scope and priority" of Section 7; a search that finds nothing is not a proof of novelty, and no priority is claimed.

Table 1: The possible types (e_3, s) , the number d_{10}^e of descendants of order p^{10} and exponent p , and $c d_{10}$ with $c = e_3 s$ on one residue class of p for each type (Theorem 1.2).

type	only if	$d_{10}^e(E, P)$	$c d_{10}(E, P)$	for
(1, 2)	–	$(p^2 + 2p + 5)/2$	$p^6 + 2p^5 + 5p^4 + 10p^3 + 22p^2 + 28p + 24$	$p \equiv 11 \pmod{12}$
(3, 2)	–	$(p^2 + 4p + 15 + 4\delta_3)/6$	$p^6 + 2p^5 + 5p^4 + 14p^3 + 36p^2 + 60p + 70$	$p \equiv 11 \pmod{12}$
(9, 2)	$p \equiv 1 \pmod{3}$	$(p^2 + 10p + 61)/18$	$p^6 + 2p^5 + 7p^4 + 30p^3 + 102p^2 + 280p + 586$	$p \equiv 7, 31 \pmod{36}$
(1, 4)	$p \equiv 1 \pmod{4}$	$(p^2 + 2p + 13)/4$	$p^6 + 2p^5 + 5p^4 + 10p^3 + 22p^2 + 44p + 100$	$p \equiv 5 \pmod{24}$
(9, 4)	$p \equiv 1 \pmod{12}$	$(p^2 + 10p + 133)/36$	$p^6 + 2p^5 + 7p^4 + 30p^3 + 102p^2 + 424p + 1594$	$p \equiv 13, 61 \pmod{72}$

2 The groups, the Lie p -covering ring and descendants

Let $V_1 = \langle e_1, e_2, e_3 \rangle$, $V_2 = \langle e_4, e_5, e_6 \rangle$ and $f_j = e_{3+j}$. Let $\mathfrak{g} = V \oplus W$ be the Lie algebra over $\mathbb{F}_p$ with $[v + w, v' + w'] = t(v, v')$; it has class 2 and $[\mathfrak{g}, \mathfrak{g}] = W$. Let $I = \ker(\Lambda^2 V \rightarrow W, u \wedge v \mapsto t(u, v))$, of dimension 12. Let $\mathcal{L}(V) = \bigoplus_n \mathcal{L}_n(V)$ be the free Lie algebra over $\mathbb{F}_p$ on V , graded by degree; $\mathcal{L}_2(V) = \Lambda^2 V$, and $\dim \mathcal{L}_3(V) = (6^3 - 6)/3 = 70$ by Witt's formula. Let $[I, V]$ be the span of the brackets $[r, v]$ with $r \in I$, $v \in V$, and $N := \mathcal{L}_3(V)/[I, V]$.

The Lazard correspondence [Laz54], [Khu98]. For $p \geq 5$ it is a bijection between finite p -groups of class at most 3 and finite Lie rings of p -power order and class at most 3, on the same underlying set, which preserves isomorphisms, subgroups and Lie subrings, normal subgroups and ideals, quotients, the terms of the lower central series, and $x^n = nx$. The group attached to $\mathfrak{g}$ is $x \circ y = x + y + \frac{1}{2}[x, y]$, which is $G_{E,P}(\mathbb{F}_p)$; so $\text{Aut}(G_{E,P}(\mathbb{F}_p)) = \text{Aut}(\mathfrak{g})$ as sets of maps (see also [MS25, Theorem 2.13 and the proof of Theorem 2.15]). The group $H = G_{E,P}(\mathbb{F}_p)$ has p -class 2: $P_1(H) = H'H^p = W$ and $P_2(H) = 1$.

Lemma 2.1. *Let G be a group with a central subgroup Z of order p and $G/Z \cong H$. (a) G has class at most 3; if it has class 3, then $\gamma_3(G) = Z = P_2(G)$ and $P_3(G) = 1$, so G is an immediate descendant of H in O'Brien's sense and $G/\gamma_3(G) \cong H$. (b) If G has class 2, then $P_2(G) = 1$, and G is not a descendant of H . (c) Every immediate descendant of H of order p^{10} , and every group K of order p^{10} and class 3 with $K/\gamma_3(K) \cong H$, is a group G as in (a). So the three notions of immediate descendant of order p^{10} agree, and both exponents p and p^2 are allowed.*

Proof. (a) As G/Z has class 2, $\gamma_3(G) \leq Z$ and $\gamma_4(G) \leq [Z, G] = 1$. If the class is 3, then $1 \neq \gamma_3(G) \leq Z$ gives $\gamma_3(G) = Z$. Since H has exponent p , $G^p \leq Z \leq G'$, so $P_1(G) = G'G^p = G'$ and $P_2(G) = [G', G](G')^p = \gamma_3(G)(G')^p$. As $G'/Z \cong H'$ has exponent p , $(G')^p \leq Z$; hence $P_2(G) = Z$, and $P_3(G) = [Z, G]Z^p = 1$. (b) If G has class 2, then G' is central and $x^p \in Z$ for all x , so $[x, y]^p = [x^p, y] = 1$ and $(x^p)^p = 1$. Thus $P_1(G) = G'G^p$ is central and generated by elements of order dividing p , and $P_2(G) = [P_1(G), G]P_1(G)^p = 1$. (c) An immediate descendant G of order p^{10} has $G/P_2(G) \cong H$, so $|P_2(G)| = p$; a normal subgroup of order p of a p -group is central, and by (b) the class of G is 3. If K has class 3 and $K/\gamma_3(K) \cong H$, then $\gamma_3(K)$ is normal of order p , hence central. $\square$

The Lie p -covering ring. Let $F_{\mathbb{Z}} = \bigoplus_{n \geq 1} L_n$ be the free Lie ring on $x_1, \dots, x_6$, graded by degree; each L_n is free abelian, and $L_n/pL_n = \mathcal{L}_n(V)$. Let $\pi: F_{\mathbb{Z}} \rightarrow \mathfrak{g}$ map x_i to e_i , $R = \ker \pi$, $R^* = [R, F_{\mathbb{Z}}] + pR$, $L^* = F_{\mathbb{Z}}/R^*$ and $M = R/R^*$. For a Lie ring K let $P_0(K) = K$ and $P_{i+1}(K) = [P_i(K), K] + pP_i(K)$.

Lemma 2.2. (a) $R = pL_1 \oplus \tilde{I} \oplus L_3 \oplus L_4 \oplus \dots$, where $\tilde{I}$ is the preimage of I in L_2 , and $L^* = L_1^* \oplus L_2^* \oplus L_3^*$ with $L_1^* = L_1/p^2L_1 \cong (\mathbb{Z}/p^2\mathbb{Z})^6$, $L_2^* = \Lambda^2 V$ and $L_3^* = N$. (b) M is a central ideal with $pM = 0$, $M = M_1 \oplus M_2 \oplus M_3$ with $M_1 = pL_1^* \cong V$, $M_2 = I \subseteq L_2^*$, $M_3 = L_3^* = N$; moreover $pL^* = M_1$, $P_1(L^*) = L_2^* + L_3^* + pL_1^* \supseteq M$, $P_2(L^*) = \gamma_3(L^*) = N$ and $L^*/M \cong \mathfrak{g}$. (c) Let K be a finite Lie ring with a central ideal Z such that $pZ = 0$ and $Z \subseteq [K, K] + pK$, and let $\psi: K/Z \rightarrow \mathfrak{g}$ be an isomorphism. Then there are a subspace $U \subseteq M$ and an isomorphism $L^*/U \rightarrow K$ which maps M/U onto Z and induces ψ^{-1} .

Proof. (a) The map π is graded (V in degree 1, W in degree 2), so R is graded with $R_1 = pL_1$, $R_2 = \tilde{I}$ and $R_n = L_n$ for $n \geq 3$. Degree by degree, $R_1^* = p^2L_1$; $R_2^* = [pL_1, L_1] + p\tilde{I} = pL_2$; $R_3^* = [pL_1, L_2] + [\tilde{I}, L_1] + pL_3 = [\tilde{I}, L_1] + pL_3$; and $R_n^* = [L_{n-1}, L_1] = L_n$ for $n \geq 4$. Modulo p , $[\tilde{I}, L_1]$ becomes $[I, V]$, so $L_3/R_3^* = \mathcal{L}_3(V)/[I, V] = N$. (b) $[R, F_{\mathbb{Z}}] + pR \subseteq R^*$ gives the first statement, and (a) gives the graded pieces of M . Since $pL_2^* = pL_3^* = 0$, we get $pL^* = pL_1^*$, $P_1(L^*) = L_2^* + L_3^* + pL_1^*$ and $P_2(L^*) = [P_1(L^*), L^*] + pP_1(L^*) = L_3^* + pL_2^* + p^2L_1^* = L_3^*$. (c) Choose $k_i \in K$ with $\psi(k_i + Z) = e_i$ and let $\rho: F_{\mathbb{Z}} \rightarrow K$ map x_i to k_i . Its image S satisfies $S + Z = K$, hence $S + P_1(K) = K$; then $P_1(K) \subseteq [S, S] + pS + P_2(K)$, so $K = S + P_2(K)$, and inductively $K = S + P_j(K)$ for all j . As K is finite and nilpotent, $P_j(K) = 0$ for large j , and ρ is onto. Its kernel lies in R , R maps onto Z , and $[R, F_{\mathbb{Z}}]$ and pR map to $[Z, K] = 0$ and $pZ = 0$. So ρ factors through L^* , with kernel $U = \ker \rho/R^* \subseteq M$. $\square$

O'Brien's p -covering group of $H = \Phi/\mathcal{R}$, with Φ free of rank 6, is $H^* = \Phi/[\mathcal{R}, \Phi]\mathcal{R}^p$; its p -multiplier is $\mathcal{R}/[\mathcal{R}, \Phi]\mathcal{R}^p$ and its nucleus is $P_2(H^*)$. Every 6-generator group which is an extension of H by a central elementary abelian subgroup is a quotient of H^* . H is terminal if and only if the nucleus is trivial, and the immediate descendants of H are the quotients of H^* by the proper subgroups U of the p -multiplier with $U P_2(H^*)$ equal to it; their orders are p^{9+s} , $1 \leq s \leq \log_p |P_2(H^*)|$, and each such s occurs [O'B90].

Lemma 2.3. Under the Lazard correspondence H^* corresponds to L^* , its p -multiplier to M , and its nucleus to N . In particular $|P_2(H^*)| = p^{\dim N}$.

Proof. Both have class at most $3 < p$, as the p -multiplier of H^* is central. The Lazard group of L^* is generated by the images of $x_1, \dots, x_6$ (subgroups and Lie subrings coincide) and contains M as a central subgroup of exponent p with quotient H ; so it is a quotient of H^* , and $|L^*| \leq |H^*|$. Conversely, the Lie ring of H^* satisfies the hypotheses of Lemma 2.2(c), with Z the p -multiplier, which lies in $[H^*, H^*](H^*)^p$; so $|H^*| \leq |L^*|$, and the surjection of Lemma 2.2(c) is an isomorphism mapping M onto the p -multiplier. As $(H^*)^p$ is central, $[P_1(H^*), H^*] = \gamma_3(H^*)$; and $x^p = px = 0$ on the ideal $[L^*, L^*] + pL^*$, which corresponds to $P_1(H^*)$. So $P_2(H^*) = \gamma_3(H^*)$, which corresponds to $\gamma_3(L^*) = N$. $\square$

Lemma 2.4. (a) For a hyperplane U of M with $N \not\subseteq U$, the Lie ring $K_U = L^*/U$ has order p^{10} and class 3, $K_U/\gamma_3(K_U) \cong \mathfrak{g}$, and $pK_U = 0$ if and only if $M_1 \subseteq U$. Every Lie ring K of order p^{10} and class 3 with $K/\gamma_3(K) \cong \mathfrak{g}$ is isomorphic to some K_U . (b) Every $\alpha \in \text{Aut}(\mathfrak{g})$ lifts to an automorphism α^* of L^* inducing α on $L^*/M = \mathfrak{g}$, and $\alpha^*|_M$ depends only on α . (c) $K_U \cong K_{U'}$ if and only if $U' = \alpha^*(U)$ for some $\alpha \in \text{Aut}(\mathfrak{g})$.

Proof. (a) Since $N + U = M$, $\gamma_3(K_U) = (N + U)/U = M/U$ has order p and $K_U/\gamma_3(K_U) = L^*/M = \mathfrak{g}$; $\gamma_4(K_U) = 0$, and $pK_U = (M_1 + U)/U$. Conversely, $Z = \gamma_3(K)$ has order p and is central, and $Z \subseteq [K, K]$; by Lemma 2.2(c), $K \cong L^*/U$ with U a hyperplane of M , and $N \not\subseteq U$ because $\gamma_3(K) \neq 0$.

(b) Define $\tilde{\alpha}: F_{\mathbb{Z}} \rightarrow F_{\mathbb{Z}}$ by choosing $\tilde{\alpha}(x_i) \in \pi^{-1}(\alpha(e_i))$. Then $\pi\tilde{\alpha} = \alpha\pi$, so $\tilde{\alpha}(R) \subseteq R$, $\tilde{\alpha}(R^*) \subseteq R^*$, and $\tilde{\alpha}$ induces an endomorphism α^* of L^* which induces α on L^*/M . Its image S satisfies $S + M = L^*$ and $M \subseteq P_1(L^*)$; as in the proof of Lemma 2.2(c), $L^* = S + P_2(L^*) = S + P_3(L^*) = S$. So α^* is onto, hence bijective. Another lift $\tilde{\beta}$ has $\tilde{\beta}(x_i) - \tilde{\alpha}(x_i) \in R$; for $r = r_1 + r' \in R$ with $r_1 \in pL_1$ and r' of degree at least 2, $\tilde{\beta}(r_1) - \tilde{\alpha}(r_1) \in pR$, and $\tilde{\beta}(r') - \tilde{\alpha}(r')$ is a sum of brackets each containing an element of R . So α^* and β^* agree on M .

(c) An isomorphism $\phi: K_U \rightarrow K_{U'}$ maps $\gamma_3(K_U) = M/U$ onto M/U' and induces some $\alpha \in \text{Aut}(\mathfrak{g})$. Choose $\tilde{\alpha}(x_i) \in F_{\mathbb{Z}}$ with image $\phi(x_i + U)$ in $K_{U'}$. Then $\phi \circ (\text{projection})$ and $(\text{projection}) \circ \tilde{\alpha}$ agree on generators, hence are equal; so $\tilde{\alpha}$ maps R , the preimage of γ_3 , into R , it lifts α , and the induced α^* satisfies $\alpha^*(U) \subseteq U'$, hence $\alpha^*(U) = U'$. The converse is clear. $\square$

So the immediate descendants of order p^{10} of H , up to isomorphism, correspond (by Lemma 2.1 and the Lazard correspondence) to the $\text{Aut}(\mathfrak{g})$ -orbits on the hyperplanes of M not containing N , and those of exponent p to the hyperplanes containing M_1 .

3 Which pairs have immediate descendants

Lemma 3.1. *Let $\varphi: \Lambda^3 V \rightarrow W \otimes V$, $a \wedge b \wedge c \mapsto t(a, b) \otimes c + t(b, c) \otimes a + t(c, a) \otimes b$. Then $[[a, b], c] \mapsto t(a, b) \otimes c$ induces an isomorphism $N \cong (W \otimes V)/\varphi(\Lambda^3 V)$. Hence N^* is the space of bilinear maps $\beta: W \times V \rightarrow \mathbb{F}_p$ with $\beta(t(a, b), c) + \beta(t(b, c), a) + \beta(t(c, a), b) = 0$ for all $a, b, c \in V$, and $N^* = N_1^* \oplus N_2^*$, where N_1^* , resp. N_2^* , consists of the bilinear maps $\beta_1: W \times V_1 \rightarrow \mathbb{F}_p$, resp. $\beta_2: W \times V_2 \rightarrow \mathbb{F}_p$, with*

$$\beta_1(t(e_j, f_k), e_i) = \beta_1(t(e_i, f_k), e_j) \quad (i < j), \quad \beta_2(t(e_i, f_j), f_k) = \beta_2(t(e_i, f_k), f_j) \quad (j < k). \quad (3)$$

Proof. The map $\Lambda^2 V \otimes V \rightarrow \mathcal{L}_3(V)$, $(a \wedge b) \otimes c \mapsto [[a, b], c]$, is onto, and by the Jacobi identity its kernel contains $J(\Lambda^3 V)$, where $J(a \wedge b \wedge c) = (a \wedge b) \otimes c + (b \wedge c) \otimes a + (c \wedge a) \otimes b$. Composing J with the product $\Lambda^2 V \otimes V \rightarrow \Lambda^3 V$ gives 3 times the identity, so J is injective for $p \neq 3$, and $\dim(\Lambda^2 V \otimes V)/J(\Lambda^3 V) = 90 - 20 = 70 = \dim \mathcal{L}_3(V)$. So the kernel is $J(\Lambda^3 V)$. Dividing by the image $I \otimes V$ of $[I, V]$ and identifying $\Lambda^2 V/I$ with W through t gives the isomorphism, with $\varphi = (t \otimes 1) \circ J$. As t vanishes on $V_1 \times V_1$ and on $V_2 \times V_2$, φ vanishes on $\Lambda^3 V_1$ and $\Lambda^3 V_2$; moreover $\varphi(e_i \wedge e_j \wedge f_k) = t(e_j, f_k) \otimes e_i - t(e_i, f_k) \otimes e_j$ lies in $W \otimes V_1$ and $\varphi(e_i \wedge f_j \wedge f_k) = t(e_i, f_j) \otimes f_k - t(e_i, f_k) \otimes f_j$ lies in $W \otimes V_2$. The dual statements follow. $\square$

Let w_1, w_2, w_3 be the standard basis of W , so $t(e_i, f_j) = (C_{E,P})_{ij}$ is the vector of coefficients of the (i, j) entry of (1), and write $\beta_1(w_m, e_i) = K_{mi}$, $\beta_2(w_m, f_i) = L_{mi}$.

Lemma 3.2. *Over every field of characteristic different from 2 and for all values of λ, μ, a , the conditions on β_1 in (3) are the nine equations*

$$\begin{aligned} (k=1) \quad & K_{21} + \mu K_{31} = K_{12} - \lambda K_{32}, \quad K_{13} = \lambda K_{33}, \quad K_{23} = -\mu K_{33}, \\ (k=2) \quad & \lambda K_{11} + (a + \lambda^2) K_{31} + \mu K_{32} = K_{22}, \quad K_{11} = K_{23} - \mu K_{33}, \quad K_{12} = \lambda K_{13} + (a + \lambda^2) K_{33}, \\ (k=3) \quad & K_{11} = 0, \quad K_{31} = 0, \quad K_{32} = -K_{13}, \end{aligned}$$

and those on β_2 are the same equations for L with μ replaced by $-\mu$. If $\mu \neq 0$, the only solution is $K = 0$. If $\mu = 0$, the solutions are the multiples of

$$K_0 = \begin{pmatrix} 0 & a + 2\lambda^2 & \lambda \\ a + 3\lambda^2 & 0 & 0 \\ 0 & -\lambda & 1 \end{pmatrix}. \quad (4)$$

Consequently $N = 0$ if $\mu \neq 0$, and $\dim N = 2$, with $N^* = \{(cK_0, c'K_0) : c, c' \in \mathbb{F}_p\}$, if $\mu = 0$.

Proof. The equations are read off from (1): the k -th column of $C_{E,P}$ is $(w_1 - \lambda w_3, w_2 + \mu w_3, 0)$ for $k = 1$, $(w_2 - \mu w_3, \lambda w_1 + (a + \lambda^2)w_3, w_1)$ for $k = 2$ and $(0, w_1, -w_3)$ for $k = 3$, and the condition on β_1 for the pairs $(i, j) = (1, 2), (1, 3), (2, 3)$ gives the three equations in each line. The equations for $k = 3$ and the last two for $k = 1$ give $K_{11} = K_{31} = 0$, $K_{13} = \lambda K_{33}$, $K_{32} = -\lambda K_{33}$ and $K_{23} = -\mu K_{33}$; the second equation for $k = 2$ then reads $2\mu K_{33} = 0$. If $\mu \neq 0$, then $K_{33} = 0$, and the remaining equations give $K = 0$. If $\mu = 0$, put $c = K_{33}$; then $K_{12} = (a + 2\lambda^2)c$, $K_{22} = 0$ and $K_{21} = K_{12} - \lambda K_{32} = (a + 3\lambda^2)c$, so $K = cK_0$, and every multiple of K_0 solves the system. The same computation applies to β_2 . $\square$

Remark 3.3. The result was found with an exact computation over $\mathbb{Z}[\lambda, \mu, a]$: the diagonal 9×9 blocks of φ have determinants $\mp 2\mu$ and, at $\mu = 0$, 8×8 minors equal to ± 1 ; Lemma 3.2 is a version of this certificate that can be checked by reading.

Proof of Theorem 1.1. (i) $\Leftrightarrow$ (ii) is Lemma 2.1. If (ii) holds, the Lie ring of an immediate descendant of order p^{10} is a ring K as in Lemma 2.4(a), by Lemma 2.1 and the Lazard correspondence; so $K \cong K_U$ with $N \not\subseteq U$, and $N \neq 0$. Conversely, if $N \neq 0$, a hyperplane U of M with $N \not\subseteq U$ gives the Lie ring K_U , whose Lazard group has order p^{10} , class 3 and quotient H by its γ_3 , which is (ii) by Lemma 2.1. By Lemma 2.3 and [O'B90], (iii) holds if and only if $N \neq 0$. By Lemma 3.2, $N \neq 0$ if and only if $\mu = 0$, and $\mu = 0$ if and only if $P = -P = (\lambda : -\mu : 1)$.

Let $\mu = 0$. Then the nucleus has order $p^{\dim N} = p^2$ by Lemmas 2.3 and 3.2, and by [O'B90] the immediate descendants have orders p^{10} and p^{11} and no other order. Write a linear form on $M = M_1 \oplus M_2 \oplus M_3$ as $f = (f_1, f_2, f_3)$. For $f = (0, 0, f_3)$ with $f_3 \neq 0$, $U = \ker f$ contains M_1 but not N , so $pK_U = 0$ and the Lazard group of K_U has exponent p , since $x^p = px$. For $f = (f_1, 0, f_3)$ with $f_1 \neq 0 \neq f_3$, $pK_U \neq 0$ and the group has exponent p^2 , as $p^2 L^* = 0$. $\square$

4 The case of a point of order two

Let Ψ be the group of pseudo-isometries of t , that is, of pairs $(A, B) \in \mathrm{GL}(V) \times \mathrm{GL}(W)$ with $t(Au, Av) = Bt(u, v)$, acting on $\mathfrak{g}$ by $v + w \mapsto Av + Bw$; for $\theta \in \mathrm{Hom}(V, W)$ let $\sigma_\theta(v + w) = v + \theta(v) + w$.

Lemma 4.1. *Every $\alpha \in \mathrm{Aut}(\mathfrak{g})$ is uniquely $\sigma_\theta \circ (A, B)$ with $(A, B) \in \Psi$ and $\theta \in \mathrm{Hom}(V, W)$. On $M = M_1 \oplus M_2 \oplus M_3$, (A, B) acts as A on $M_1 = V$, as $\Lambda^2 A$ on $M_2 = I$ and as $B \otimes A$ on $M_3 = (W \otimes V)/\varphi(\Lambda^3 V)$; σ_θ fixes M_1 and M_3 pointwise and maps $r \in M_2$ to $r + \delta_\theta(r)$, where $\delta_\theta(u \wedge v) = \theta(u) \otimes v - \theta(v) \otimes u$ modulo $\varphi(\Lambda^3 V)$.*

Proof. $W = [\mathfrak{g}, \mathfrak{g}]$ is invariant; with A induced on $\mathfrak{g}/W = V$ and $B = \alpha|_W$, $(A, B) \in \Psi$, and $\alpha \circ (A, B)^{-1}$ is the identity on $\mathfrak{g}/W$ and on W , so it is some σ_θ (compare the proof of [MS25, Theorem 2.15]). A lift of (A, B) as in Lemma 2.4(b) is the graded endomorphism of $F_{\mathbb{Z}}$ given by an integer matrix lifting A ; it acts as A on $M_1 = pL_1^*$, as $\Lambda^2 A$ on L_2^* , and maps $[[a, b], c]$ to $[[Aa, Ab], Ac]$, which corresponds to $Bt(a, b) \otimes Ac$ under Lemma 3.1. A lift of σ_θ is $x_i \mapsto x_i + \tilde{\theta}(x_i)$ with $\tilde{\theta}(x_i) \in L_2$ mapping to $\theta(e_i)$; it fixes M_1 ($pL_2^* = 0$) and L_3^* ($L_4^* = 0$), and maps $r = \sum c_{ij}[x_i, x_j] \in \tilde{I}$ to $r + \sum c_{ij}([\tilde{\theta}x_i, x_j] + [x_i, \tilde{\theta}x_j])$ plus terms of degree 4; the sum corresponds to $\delta_\theta(r)$. $\square$

A hyperplane of M is the kernel of a linear form $f \neq 0$, unique up to a factor, and $\alpha^*(\ker f) = \ker(f \circ \alpha^{*-1})$. Write $f = (f_1, f_2, f_3)$ with $f_i \in M_i^*$. By Lemmas 2.4 and 4.1, $d_{10}(H)$ is the number of orbits of $(\{\sigma_\theta\} \rtimes \Psi) \times \mathbb{F}_p^\times$, acting by $f \mapsto cf \circ \alpha^{*-1}$, on $Y = \{f \in M^* : f_3 \neq 0\}$, and $d_{10}^e(H)$ the number of orbits on $\{f \in Y : f_1 = 0\}$. The map σ_θ sends f to $(f_1, f_2 - f_3 \circ \delta_\theta, f_3)$; let $D(f_3) = \{f_3 \circ \delta_\theta|_I : \theta \in \mathrm{Hom}(V, W)\} \subseteq I^*$.

Tensor structure. From now on $\mu = 0$. Then $P = (\lambda, 0)$, $b = -\lambda^3 - a\lambda$, $3\lambda^2 + a \neq 0$ (λ is a simple root of $x^3 + ax + b$), and $C = C_{E,P}$ is symmetric. Let $S: V_1 \times V_1 \rightarrow W$ be the symmetric bilinear

map with $S(e_i, e_j) = C_{ij}$, let $U = \mathbb{F}_p^2$ with basis u_1, u_2 and $\omega(u_1, u_2) = 1$ for the standard alternating form, and identify $V = V_1 \otimes U$ by $e_i = e_i \otimes u_1$, $f_i = e_i \otimes u_2$.

Lemma 4.2. (a) $t(v \otimes x, v' \otimes x') = S(v, v')\omega(x, x')$. (b) $\kappa(w, v) = w^t K_0 v$, with K_0 from (4), is a perfect pairing $W \times V_1 \rightarrow \mathbb{F}_p$ ($\det K_0 = -(a + 3\lambda^2)^2$), the form $\kappa(S(u, v), v')$ is symmetric, and $N^* = \{\tau_\xi : \xi \in U^*\}$ with $\tau_\xi(w \otimes (v \otimes x)) = \kappa(w, v)\xi(x)$. (c) Let Ψ_S be the group of pairs $(a, b) \in \text{GL}(V_1) \times \text{GL}(W)$ with $S(av, av') = bS(v, v')$. There is a homomorphism $\chi : \Psi_S \rightarrow \mathbb{F}_p^\times$ with $\kappa(bw, av) = \chi(a, b)\kappa(w, v)$, and $\chi(s, s^2) = s^3$ for $s \in \mathbb{F}_p^\times$. (d) $(a, b, g) \mapsto (a \otimes g, \det(g)b)$ is a homomorphism $\Psi_S \times \text{GL}(U) \rightarrow \Psi$ with kernel $\{(s, s^2, s^{-1})\}$, and for its image (A, B) , $\tau_\xi \circ (B \otimes A) = \det(g)\chi(a, b)\tau_{\xi \circ g}$.

Proof. (a) Both sides agree on the basis, as C is symmetric. (b) Expand $\det K_0$ along the second row. By Lemma 3.2, N_1^* and N_2^* consist of the forms $(w, e_i \otimes u_1) \mapsto c\kappa(w, e_i)$ and $(w, e_i \otimes u_2) \mapsto c'\kappa(w, e_i)$; and the condition (3) for $\beta_1 = \kappa$, with the symmetry of S , gives the symmetry. (c) For $(a, b) \in \Psi_S$, $(a \otimes 1, b) \in \Psi$ by (a), and φ is Ψ -equivariant, so $f \mapsto f \circ (b \otimes a \otimes 1)$ preserves the 2-dimensional space N^* , and $\tau_{u_1^*} \circ (b \otimes a \otimes 1) = \tau_{\xi'}$ for some ξ' . Evaluating at $w \otimes (v \otimes u_2)$ gives $\xi'(u_2) = 0$, so $\xi' = \chi u_1^*$, and evaluating at $w \otimes (v \otimes u_1)$ gives $\kappa(bw, av) = \chi\kappa(w, v)$. This uses only that the τ_ξ span N^* , which Lemma 3.2 proves over every $\mathbb{F}_p$. (d) By (a), $t((a \otimes g)(v \otimes x), (a \otimes g)(v' \otimes x')) = \det(g)bS(v, v')\omega(x, x')$; if $a \otimes g = 1$, then $a = s$, $g = s^{-1}$ and $b = s^2$; the last formula follows from (c). $\square$

The group Ψ . For $(a, b) \in \Psi_S$ the identity $S(av, av') = bS(v, v')$ reads $a^t C(y)a = C(b^t y)$ for the matrix $C(y)$ of linear forms. As $\det C(y) = y_2^2 y_3 - y_1^3 - ay_1 y_3^2 - by_3^3$, the curve $\det C(y) = 0$ is E in the coordinates $(y_1 : y_2 : y_3) = (x : y : z)$, and $y \mapsto b^{-t}y$ maps E to itself. This gives a homomorphism ε from Ψ_S to the automorphism group $\text{Aut}(E)$ of the projective curve, trivial on the scalars $\{(s, s^2)\}$; let $\Gamma = \Psi_S / \mathbb{F}_p^\times$.

Lemma 4.3 (Maglione–Stanojkovski). *Let $e_3 = |E[3](\mathbb{F}_p)|$, $\text{Stab}(P) = \{\sigma \in \text{Aut}_O(E) : \sigma(P) = P\}$ and $s = |\text{Stab}(P)|$. Then $|\Psi_S| = (p-1)e_3s$, the map of Lemma 4.2(d) is onto Ψ , and ε induces an isomorphism of Γ onto $\{\sigma \circ \tau_T : \sigma \in \text{Stab}(P), T \in E[3](\mathbb{F}_p)\} \cong E[3](\mathbb{F}_p) \rtimes \text{Stab}(P)$, where τ_T is the translation by T .*

Proof. We use [MS25, Theorem 5.8 and its proof] with $F = \mathbb{F}_p$; their $\Psi\text{Isom}_F(B_{E,P})$ is our Ψ , and their U, W are our V_1, V_2 . There, Ψ acts 2-transitively on the set $\mathcal{T}(t)$ of totally isotropic 3-dimensional subspaces (by Lemmas 5.4 and 5.5 there), which has $p+1$ elements for $P \in E[2](\mathbb{F}_p)$ ([MS25, Corollary 3.6] together with the end of the proof of Theorem D there; this is used in (5.3) of the proof of Theorem 5.8); the stabilizer of (V_1, V_2) is the group $\text{Aut}_V^f(\mathfrak{g})$ of the $\text{diag}(X, Y, Z)$ with $X^t C(Zy)Y = C(y)$; and $\phi : \text{diag}(X, Y, Z) \mapsto Z \in \text{Aut}(E)$ has kernel $\{\text{diag}(xI, yI, (xy)^{-1}I)\}$ and an image of order e_3s . So $|\Psi| = p(p+1)(p-1)^2 e_3s = e_3s|\text{GL}_2(\mathbb{F}_p)|$. By the proof of [MS25, Theorem 5.6] every element of the image is some $\sigma \circ \tau_T$ (the map δ there is $\sigma \circ \tau_T$ with $T = -\delta^{-1}(O)$); these e_3s maps are pairwise distinct, as $\sigma \circ \tau_T(O) = \sigma(T)$, so the image is the whole set.

Dictionary. $(a, b) \in \Psi_S$ if and only if $\text{diag}(a^{-1}, a^{-1}, b^t) \in \text{Aut}_V^f(\mathfrak{g})$, as $a^{-t}C(b^t y)a^{-1} = C(y)$ means $a^t C(y)a = C(b^t y)$; and $\varepsilon(a, b)$ is the inverse of $\phi(\text{diag}(a^{-1}, a^{-1}, b^t))$. As C is symmetric, transposing $X^t C(Zy)Y = C(y)$ shows that $\text{diag}(Y, X, Z) \in \text{Aut}_V^f(\mathfrak{g})$ with $\text{diag}(X, Y, Z)$; so $\text{diag}(XY^{-1}, YX^{-1}, I) \in \ker \phi$ and $X = xY$ for a scalar x . Hence $\text{diag}(xY, Y, Z)$ is the product of $\text{diag}(xI, I, x^{-1}I) \in \ker \phi$ and $\text{diag}(Y, Y, xZ)$: $\text{Aut}_V^f(\mathfrak{g})$ is the product of $\ker \phi$ and the image A_0 of Ψ_S , the subgroup of elements with $X = Y$, and $A_0 \cap \ker \phi$ consists of the $\text{diag}(yI, yI, y^{-2}I)$. Therefore $|\Psi_S| = |\text{Aut}_V^f(\mathfrak{g})|/(p-1) = (p-1)e_3s$, $\phi(A_0)$ is the whole image, and ε maps Γ isomorphically onto it. Finally the image of $\Psi_S \times \text{GL}(U)$ in Ψ has order $|\Psi_S||\text{GL}_2(\mathbb{F}_p)|/(p-1) = |\Psi|$. $\square$

Remark 4.4. The order $|\Psi| = e_3s|\text{GL}_2(\mathbb{F}_p)|$, that is $|\text{Aut}(G_{E,P}(\mathbb{F}_p))| = p^{18}e_3s|\text{GL}_2(\mathbb{F}_p)|$ [MS25, Theorem B], was confirmed by an exhaustive computation of Ψ assuming no structure for all 182 classes

with $P \in E[2]$ and $p \leq 23$ in the second verification run, and $|\Psi_S| = (p-1)e_3s$ by the programs of this note. The third verification run found $|\Psi| = e_3s|\text{GL}_2(\mathbb{F}_p)|$ again, for the 22 classes with $p \leq 7$, by an exhaustive search of $\mathcal{T}(t)$ and of the stabilizer of (V_1, V_2) . The structural statements used below (Lemma 4.3) rest on the proofs of [MS25, Theorems 5.6, 5.8]; the first and the third verification run checked the reading above against their text.

Lifts. As S maps onto W , b is determined by a , and we write a for $(a, b) \in \Psi_S$.

Lemma 4.5. (a) $a = \text{diag}(-1, 1, 1)$, $b = \text{diag}(1, -1, 1)$ lies in Ψ_S , with $\chi(a) = 1$ and $\varepsilon(a) = [-1]$ (cf. [MS25, Lemma 5.4]). (b) If $\lambda = 0$ and $i^2 = -1$ in $\mathbb{F}_p$, then $a = \text{diag}(i, 1, -1)$, $b = \text{diag}(-1, i, 1)$ lies in Ψ_S , $\chi(a) = -1$, and $\varepsilon(a)$ is an automorphism of order 4 fixing $P = (0, 0)$. (c) For $T \in E[3](\mathbb{F}_p) \setminus \{O\}$ there is $a_T \in \Psi_S$ with $\varepsilon(a_T) = \tau_T$ and $a_T^3 = 1$; it has the three distinct eigenvalues $1, \omega, \omega^2$ (ω a primitive cube root of unity in $\overline{\mathbb{F}_p}$), and $\chi(a_T) = 1$.

Proof. (a), (b): in (a), $a^t C(y)a$ is $C(y)$ with the signs of the entries $(1, 2)$, $(2, 1)$ changed, which is $C(y_1, -y_2, y_3)$ as $\mu = 0$, and $b^t K_0 a = K_0$; in (b), $a^t C(y)a = C(-y_1, iy_2, y_3)$ and $b^t K_0 a = -K_0$. (c) Let $\varepsilon(a) = \tau_T$. As $\tau_T^3 = 1$, $a^3 = t$ is a scalar. With a_i from (a), $a_i a a_i^{-1}$ lies over $[-1]\tau_T[-1] = \tau_T^{-1}$, so it is $e a^{-1}$ for a scalar e . Cubing gives $t = e^3 t^{-1}$, so $t = (t/e)^3$, and $a_T = (e/t)a$ satisfies $a_T^3 = 1$; again $a_i a_T a_i^{-1} = e' a_T^{-1}$, now with $e'^3 = 1$. So a_T is semisimple with eigenvalues in μ_3 , and not scalar. Eigenvalues ζ, ζ, ζ' with $\zeta \neq \zeta'$ would give $e' = \zeta^2 = \zeta'^2$, which is impossible. Finally $\chi(a_T)^3 = 1$ and $\chi(a_T) = \chi(a_i a_T a_i^{-1}) = \chi(e')\chi(a_T)^{-1} = \chi(a_T)^{-1}$. $\square$

In Γ , identified with $\{\sigma \circ \tau_T\}$, one has $\tau_S[-1]\tau_{-S} = \tau_{2S}[-1]$ and, if $s = 4$ and $[i] \in \text{Stab}(P)$ has order 4, $\tau_S[i]\tau_{-S} = \tau_{(1-[i])S}[i]$; and 2 and $1 - [i]$ are bijective on $E[3](\mathbb{F}_p)$, since $(1 - [i])(1 + [i]) = 2$. So every element of Γ is the identity, a translation τ_T with $T \neq O$ ($e_3 - 1$ elements), conjugate to $[-1]$ (e_3 elements), or, if $s = 4$, conjugate to an element of order 4 of $\text{Stab}(P)$ ($2e_3$ elements). We call these the four *types*.

5 The number of descendants of one group

By Lemma 4.2(d) and Lemma 4.3, $\Psi \times \mathbb{F}_p^\times$ is transitive on $N^* \setminus \{0\}$, as $\text{SL}(U)$ is transitive on $U^* \setminus \{0\}$. So $d_{10}(H)$ is the number of orbits of the stabilizer of $f_3 := \tau_{u_2^*}$ on the fibre $\{f \in Y : f|_N = f_3\}$ modulo the σ_θ , which is $M_1^* \times I^*/D(f_3)$. Let $B \subseteq \text{GL}(U)$ be the group of upper triangular $g = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$, of order $p(p-1)^2$.

Proposition 5.1. (i) $(a, g, c) \in \Psi_S \times \text{GL}(U) \times \mathbb{F}_p^\times$ fixes f_3 if and only if $g \in B$ and $c = xz^2\chi(a)$. (ii) $D(f_3)$ is the annihilator in I^* of the subspace $\Lambda^2(V_1 \otimes u_1)$ of I ; so $\dim D(f_3) = 9$, and restriction identifies $I^*/D(f_3)$ with $(\Lambda^2(V_1 \otimes u_1))^*$. (iii) Write $f_1 = \phi_1 \otimes u_1^* + \phi_2 \otimes u_2^*$ with $\phi_i \in V_1^*$, and let q be the restriction of f_2 to $\Lambda^2(V_1 \otimes u_1)$. An element as in (i) acts by

$$\phi_1 \mapsto z^2\chi\phi_1a^{-1}, \quad \phi_2 \mapsto xz\chi\phi_2a^{-1} - yz\chi\phi_1a^{-1}, \quad q \mapsto x^{-1}z^2\chi q \circ (\Lambda^2a)^{-1}, \quad \chi = \chi(a).$$

(iv) Every element of Ψ_S is semisimple. For $a \in \Psi_S$ and $\varepsilon \in \mathbb{F}_p^\times$ let $e(\varepsilon)$ and $e'(\varepsilon)$ be the dimensions of the ε -eigenspaces of a and of Λ^2a , and put $\varepsilon_1 = z^2\chi$, $\varepsilon_2 = xz\chi$, $\varepsilon_3 = z^2\chi/x$. The number of fixed points of $(a, g, xz^2\chi)$ on the fibre is $\text{Fix}(a, g) = p^{e(\varepsilon_1)+e(\varepsilon_2)+e'(\varepsilon_3)}$ if $x \neq z$ or $y = 0$, and $\text{Fix}(a, g) = p^{e(\varepsilon_1)+e'(\varepsilon_3)}$ if $x = z$ and $y \neq 0$; on the part with $f_1 = 0$ it is $p^{e'(\varepsilon_3)}$. Hence $d_{10}(H)$ is the average of $\text{Fix}(a, g)$ over $\Psi_S \times B$, and $d_{10}^e(H)$ the average of $p^{e'(\varepsilon_3)}$.

Proof. (i) By Lemma 4.2(d), $c\tau_{u_2^*} \circ (B \otimes A)^{-1} = c(\det(g)\chi)^{-1}\tau_{u_2^* \circ g^{-1}}$. This is $\tau_{u_2^*}$ only if g^{-1} preserves $\ker u_2^* = \langle u_1 \rangle$, that is $g \in B$; then $u_2^* \circ g^{-1} = z^{-1}u_2^*$, and the condition is $c = xz^2\chi$.

(ii) $f_3(\delta_\theta(e \wedge e')) = \beta_\theta(e, e') - \beta_\theta(e', e)$ with $\beta_\theta(e, v \otimes x) = \kappa(\theta(e), v)u_2^*(x)$. As κ is perfect, β_θ runs over $V^* \otimes L$, $L = V_1^* \otimes u_2^* \subseteq V^*$. So $D(f_3)$ is the restriction to I of the space $V^* \wedge L$ of alternating

forms, which are the forms vanishing on $\Lambda^2(L^\perp)$, $L^\perp = V_1 \otimes u_1$; it has dimension $15 - 3 = 12$ and contains the 3-dimensional kernel $\{w^* \circ t\}$ of the restriction to I , since t vanishes on $L^\perp \times L^\perp$. So $\dim D(f_3) = 9$, which is also the dimension of the annihilator of $\Lambda^2(V_1 \otimes u_1)$, which contains $D(f_3)$.

(iii) We have $u_1^* \circ g^{-1} = x^{-1}u_1^* - y(xz)^{-1}u_2^*$, $u_2^* \circ g^{-1} = z^{-1}u_2^*$, and $(a \otimes g)^{-1}(v \otimes u_1) = x^{-1}a^{-1}v \otimes u_1$; now compute $c f \circ (a \otimes g)^{-1}$ and $c f_2 \circ \Lambda^2(a \otimes g)^{-1}$ with $c = xz^2\chi$. Since $\Lambda^2(a \otimes g)$ preserves $\Lambda^2(V_1 \otimes u_1)$, the coordinate q is well defined on the fibre modulo the σ_θ .

(iv) $|\Psi_S| = (p-1)e_3s$ is prime to p . The fixed ϕ_1 solve $\phi_1 a = \varepsilon_1 \phi_1$, the fixed q solve $q \circ \Lambda^2 a = \varepsilon_3 q$, and the fixed ϕ_2 solve $\phi_2(\varepsilon_2 - a) = yz\chi \phi_1$. As a is semisimple, the image of $\phi \mapsto \phi(\varepsilon_2 - a)$ is a complement of the ε_2 -eigenspace containing all eigenvectors for other eigenvalues. So for $\varepsilon_1 \neq \varepsilon_2$, that is $x \neq z$, there are $p^{e(\varepsilon_2)}$ solutions for each ϕ_1 , and for $x = z$ there are $p^{e(\varepsilon_2)}$ if $y\phi_1 = 0$ and none otherwise. By (i) and Lemma 4.3 the stabilizer of f_3 in $\Psi \times \mathbb{F}_p^\times$ is the image of $\Psi_S \times B$, and Burnside's lemma applies to a group acting through a homomorphism. $\square$

Reduction to two variables. Fix $\gamma \in \Gamma$ and an element $a_0 \in \Psi_S$ over γ , and let $\chi_0 = \chi(a_0)$. The elements over γ are sa_0 ($s \in \mathbb{F}_p^\times$), with $\chi(sa_0) = s^3\chi_0$; the ε -eigenspace of sa_0 is the ε/s -eigenspace of a_0 , and that of $\Lambda^2(sa_0) = s^2\Lambda^2 a_0$ is the ε/s^2 -eigenspace of $\Lambda^2 a_0$. Let $e_0(\varepsilon)$, $e'_0(\varepsilon)$ be the eigenvalue multiplicities of a_0 and $\Lambda^2 a_0$ in $\mathbb{F}_p^\times$. With $u = zs$ and $t' = xs$ the three exponents in Proposition 5.1(iv) become

$$f_1(u) = e_0(u^2\chi_0), \quad f_2 = e_0(t'u\chi_0), \quad f_3 = e'_0(u^2\chi_0/t'),$$

and $x = z$ if and only if $t' = u$. For fixed s , $(x, z) \mapsto (t', u)$ is a bijection of $(\mathbb{F}_p^\times)^2$, and summing over y gives

$$F_\gamma := \frac{1}{(p-1)|B|} \sum_{s,g} \text{Fix}(sa_0, g) = \frac{1}{p(p-1)^2} \sum_{u,t' \in \mathbb{F}_p^\times} T(u, t'), \quad F_\gamma^e = \frac{1}{(p-1)^2} \sum_{u,t'} p^{f_3}, \quad (5)$$

where $T(u, t') = p^{1+f_1+f_2+f_3}$ for $t' \neq u$ and $T(u, u) = p^{2f_1+f_3} + (p-1)p^{f_1+f_3}$ (for $t' = u$ one has $f_2 = f_1$). By Proposition 5.1, $d_{10}(H) = \frac{1}{e_3s} \sum_{\gamma \in \Gamma} F_\gamma$ and $d_{10}^e(H) = \frac{1}{e_3s} \sum_{\gamma} F_\gamma^e$. F_γ depends only on the conjugacy class of γ , and $F_{\gamma^{-1}} = F_\gamma$, because h and h^{-1} have the same fixed points. Moreover, by (5), F_γ and F_γ^e depend only on χ_0 and on the functions e_0 , e'_0 , and these are the same for all translations τ_T , $T \neq O$, by Lemma 4.5(c) (the translations need not be conjugate to each other when $e_3 = 9$). So F_γ is constant on each of the four types of Section 4.

Lemma 5.2. *Let $\Lambda_1, \Lambda_2 \subseteq \mathbb{F}_p^\times$ be the sets of eigenvalues of a_0 and of $\Lambda^2 a_0$ in $\mathbb{F}_p^\times$, and put $\sigma_i = \sum_{\lambda \in \Lambda_i} (p^{e_0^{(i)}(\lambda)} - 1)$, where $e_0^{(1)} = e_0$, $e_0^{(2)} = e'_0$, and $\nu(u) = \sum_{\lambda \in \Lambda_1} (p^{e_0(\lambda)} - 1)(p^{e'_0(u^3\chi_0^2/\lambda)} - 1)$. Then for every $u \in \mathbb{F}_p^\times$*

$$\sum_{t' \in \mathbb{F}_p^\times} T(u, t') = p^{1+f_1(u)} (p-1 + \sigma_1 + \sigma_2 + \nu(u)) - (p-1) p^{f_1(u)+e'_0(u\chi_0)} (p^{f_1(u)} - 1),$$

and $F_\gamma^e = 1 + \sigma_2/(p-1)$.

Proof. Write $p^{f_2+f_3} = 1 + X + Y + XY$ with $X = p^{f_2} - 1$ and $Y = p^{f_3} - 1$. As t' runs over $\mathbb{F}_p^\times$, so do $t'u\chi_0$ and $u^2\chi_0/t'$; hence $\sum_{t'} X = \sigma_1$ and $\sum_{t'} Y = \sigma_2$. The product XY is non-zero only if $\lambda = t'u\chi_0 \in \Lambda_1$ and $\lambda' = u^2\chi_0/t' \in \Lambda_2$; then $\lambda\lambda' = u^3\chi_0^2$, and λ determines t' , so $\sum_{t'} XY = \nu(u)$. This gives $\sum_{t'} p^{1+f_1+f_2+f_3}$. At $t' = u$ the true value $T(u, u)$ differs from $p^{1+2f_1+f_3}$ by $-(p-1)p^{f_1+f_3}(p^{f_1} - 1)$, with $f_3 = e'_0(u\chi_0)$. For F_γ^e , $\sum_{t'} p^{f_3} = p-1 + \sigma_2$ for every u . $\square$

Proposition 5.3. *For the four types, F_γ and F_γ^e are the functions $F_1, F_{\text{refl}}, F_{\text{transl}}, F_{\text{ord4}}$ and $F_1^e, \dots, F_{\text{ord4}}^e$ of Theorem 1.2.*

Proof. By Lemma 4.5 we may take $a_0 = 1$, $a_0 = \text{diag}(-1, 1, 1)$, $a_0 = a_T$, and $a_0 = \text{diag}(i, 1, -1)$ with $\chi_0 = 1, 1, 1, -1$. Write Σ for $\sum_{u, t'} T(u, t')$, computed with Lemma 5.2 as the sum of a main part $\sum_u p^{1+f_1}(p-1+\sigma_1+\sigma_2)$, a part $\sum_u p^{1+f_1}\nu(u)$, and a diagonal part D , to be subtracted. We use that $\mathbb{F}_p^\times$ is cyclic of order $p-1$, so the group μ_n of n -th roots of unity in $\mathbb{F}_p^\times$ has $\gcd(n, p-1)$ elements.

Identity. $\Lambda_1 = \Lambda_2 = \{1\}$ with multiplicity 3, so $\sigma_1 = \sigma_2 = p^3 - 1$; $f_1(u) = 3$ if $u^2 = 1$ and 0 otherwise; $\nu(u) = (p^3 - 1)^2$ if $u^3 = 1$ and 0 otherwise. The main part is $p(2p^3 + p - 3)^2$; the ν -part is $p(p^3 - 1)^2(p^3 + 2\delta_3)$, since $u = 1$ has $f_1 = 3$ and the other cube roots of 1 have $f_1 = 0$; $D = (p-1)(p^3 - 1)(p^6 + p^3)$ from $u = \pm 1$. So $\Sigma = p^9 + 2p^7 + 4p^5 - 10p^4 - 6p^2 + 9p + 2\delta_3 p(p^3 - 1)^2$, and $\Sigma/(p(p-1)^2) = F_1$.

Reflection. $\Lambda_1 = \{1, -1\}$ with multiplicities 2, 1 and $\Lambda_2 = \{-1, 1\}$ with multiplicities 2, 1, so $\sigma_1 = \sigma_2 = p^2 + p - 2$; $f_1(u) = 2, 1, 0$ according as $u^2 = 1, u^2 = -1$, or neither; $\nu(u) = 2(p^2 - 1)(p - 1)$ if $u^3 = 1$, $(p^2 - 1)^2 + (p - 1)^2$ if $u^3 = -1$, and 0 otherwise. The main part is $p(2p^2 + 3p - 5)(2p^2 + p - 3 + 2\delta_4(p - 1))$. The solutions of $u^3 = \pm 1$ are $u = \pm 1$, with $f_1 = 2$, and, if $\delta_3 = 1$, four more with $f_1 = 0$; so the ν -part is $p(p^2 + 2\delta_3)(p^2 + p - 2)^2$. The diagonal part comes from $u = 1, u = -1$ and $u^2 = -1$: $D = (p-1)((p^3 + p^4)(p^2 - 1) + 2\delta_4 p(p - 1))$. So $\Sigma = 2p^6 + 3p^5 + 4p^4 - 10p^3 - 14p^2 + 15p + 4\delta_4 p(p - 1)^2(p + 2) + 2\delta_3 p(p - 1)^2(p + 2)^2$, and $\Sigma/(p(p-1)^2) = F_{\text{refl}}$.

Translation, $p \equiv 2 \pmod{3}$. a_T has the eigenvalue 1 in $\mathbb{F}_p$ and $\omega, \omega^2 \notin \mathbb{F}_p$, and so has $\Lambda^2 a_T$; so $\Lambda_1 = \Lambda_2 = \{1\}$ with multiplicity 1 and $\sigma_1 = \sigma_2 = p - 1$; $f_1(u) = 1$ if and only if $u = \pm 1$; $\nu(u) = (p - 1)^2$ if $u = 1$, and 0 otherwise. Then $\Sigma = 9p(p - 1)^2 + p^2(p - 1)^2 - (p - 1)^2(p^2 + p) = 8p(p - 1)^2$.

Translation, $p \equiv 1 \pmod{3}$. $\Lambda_1 = \Lambda_2 = \mu_3$ with multiplicity 1 (the eigenvalues of $\Lambda^2 a_T$ are $\omega \cdot \omega^2, \omega, \omega^2$), $\sigma_1 = \sigma_2 = 3(p - 1)$; $f_1(u) = 1$ if and only if $u \in \mu_6$; $\nu(u) = 3(p - 1)^2$ if $u^3 \in \mu_3$, that is $u \in \mu_9$, and 0 otherwise; $|\mu_9| = 3 + 6\delta_9$ and $\mu_9 \cap \mu_6 = \mu_3$. The main part is $49p(p - 1)^2$, the ν -part $3p(p - 1)^2(3p + 6\delta_9)$, and $D = (p - 1)^2(3p^2 + 3p)$, from $u \in \mu_3$ and $u \in \mu_6 \setminus \mu_3$. So $\Sigma = p(p - 1)^2(6p + 46 + 18\delta_9)$.

Order four ($p \equiv 1 \pmod{4}$). $a_0 = \text{diag}(i, 1, -1)$, $\chi_0 = -1$, $\Lambda_1 = \{i, 1, -1\}$ and $\Lambda_2 = \{i, -i, -1\}$, all with multiplicity 1, so $\sigma_1 = \sigma_2 = 3(p - 1)$. Here $f_1(u) = e_0(-u^2) = 1$ if and only if $u^2 \in \{1, -1, -i\}$, which has $4 + 2\delta_8$ solutions ($-i$ is a square if and only if $p \equiv 1 \pmod{8}$); so the main part is $7p(p - 1)^2(5 + 2\delta_8)$. Next $\nu(u) = (p - 1)^2 m(u^3)$, where $m(c)$ is the number of pairs $(\lambda, \lambda') \in \Lambda_1 \times \Lambda_2$ with $\lambda\lambda' = c$: $m(1) = m(-1) = m(i) = 2$, $m(-i) = 3$, and $m(c) = 0$ for $c \notin \mu_4$. So $\nu(u) \neq 0$ only for $u \in \mu_{12}$, and for such u , $f_1(u) = 1$ if and only if $u \in \mu_4$. Cubing maps μ_4 bijectively onto μ_4 , and μ_{12} onto μ_4 with fibres of size $1 + 2\delta_3$; hence $\sum_u p^{f_1(u)} m(u^3) = 9p + 18\delta_3$, and the ν -part is $p(p - 1)^2(9p + 18\delta_3)$. For the diagonal part, $e'_0(-u) = 1$ for $u \in \{1, i, -i\}$ and $e'_0(-u) = 0$ for $u = -1$ and for the two u with $u^2 = -i$; so $D = (p - 1)^2 p(3p + 1 + 2\delta_8)$. Altogether $\Sigma = p(p - 1)^2(6p + 34 + 12\delta_8 + 18\delta_3)$.

Exponent p . By Lemma 5.2, $F_\gamma^e = 1 + \sigma_2/(p - 1)$, which is $p^2 + p + 2, p + 3, 1 + |\mu_3| = 2 + 2\delta_3$ and 4 for the four types. $\square$

Proof of Theorem 1.2. The formula follows from Propositions 5.1 and 5.3 and the count of the types. $E[3](\mathbb{F}_p)$ has order 1, 3 or 9, and 9 only if $\mathbb{F}_p$ contains the cube roots of unity (Lemma 6.3); $s = 4$ only if $p \equiv 1 \pmod{4}$; and then $e_3 \neq 3$: $[i]$ is defined over $\mathbb{F}_p$, and $E[3](\mathbb{F}_p) = \langle T \rangle$ of order 3 would give $[i]T = \pm T$, so $-T = [i]^2 T = T$. $\square$

Remark 5.4. As g runs over B , $x^{-1}z^2\chi$ takes each value in $\mathbb{F}_p^\times$ exactly $p(p - 1)$ times. So $d_{10}^e(H)$ is the number of orbits of $\Lambda^2 \Psi_S$ and the scalars on $(\Lambda^2 V_1)^* \cong V_1 \otimes \det^{-1}$, that is $d_{10}^e(H) = 1 + |\mathbb{P}(V_1)/\Gamma|$ for $\Gamma = \Psi_S/\mathbb{F}_p^\times$ acting on $\mathbb{P}(V_1) = \mathbb{P}^2(\mathbb{F}_p)$.

Corollary 5.5 (du Sautoy–Vaughan–Lee). *Let $E: y^2 = x^3 - x$, $P = (0, 0)$. The group G_p of $[d\text{SVL12}]$ ($[x_1, x_4] = y_3$, $[x_1, x_5] = y_1$, $[x_1, x_6] = y_2$, $[x_2, x_4] = y_1$, $[x_2, x_5] = y_3$, $[x_3, x_4] = y_2$, $[x_3, x_6] = y_1$) is isomorphic to $G_{E,P}(\mathbb{F}_p)$. Its type is $(1, 4), (1, 2), (3, 2)$ for $p \equiv 5, 7, 11 \pmod{12}$, and for $p \equiv 1$*

(mod 12) it is (1, 4) or (9, 4) according as the number V_p of [dSVL12, Theorem 1] vanishes or not. In all five cases d_{10}^e is the number D_p of [dSVL12, Theorem 1]. The number of all descendants of order p^{10} is $\frac{1}{6}(p^6 + 2p^5 + 5p^4 + 14p^3 + 36p^2 + 60p + 70)$ for $p \equiv 11 \pmod{12}$, $\frac{1}{2}(p^6 + 2p^5 + 7p^4 + 14p^3 + 30p^2 + 40p + 34)$ for $p \equiv 7 \pmod{12}$, $\frac{1}{4}(p^6 + 2p^5 + 5p^4 + 10p^3 + 22p^2 + 44p + 100)$ for $p \equiv 5 \pmod{24}$ (124 instead of 100 for $p \equiv 17 \pmod{24}$), and Theorem 1.2 with type (1, 4) or (9, 4) for $p \equiv 1 \pmod{12}$.

Proof. Let $A(y)$ be the matrix of the commutators $[x_i, x_{3+j}]$ as linear forms in y_1, y_2, y_3 , and $C(y)$ that of (1) with $a = -1$, $b = \lambda = \mu = 0$. For the permutation matrix Q of $e_1 \mapsto x_3$, $e_2 \mapsto x_1$, $e_3 \mapsto x_2$ one checks $Q^t A(y_1, y_2, -y_3) Q = C(y)$; this gives a pseudo-isometry, so the groups are isomorphic [MS25, Theorem 2.13]. For $p \equiv 3 \pmod{4}$, -1 is not a square and $x^3 - x$ is odd, so $|E(\mathbb{F}_p)| = p + 1$; hence $e_3 = 3$ for $p \equiv 11 \pmod{12}$ and $e_3 = 1$ for $p \equiv 7 \pmod{12}$. For $p \equiv 1 \pmod{4}$, $s = 4$ and $e_3 \in \{1, 9\}$. For $p \equiv 1 \pmod{12}$, $x^4 + 6x^2 - 3$ is, up to sign, the reverse of the 3-division polynomial $3x^4 - 6x^2 - 1$ of E , its roots are not in $\{0, \pm 1\}$, and $x_0 = 1/x$ gives $x_0^3 - x_0 = -(x^3 - x)/x^4$; as -1 is a square, $V_p > 0$ if and only if E has a rational point of order 3, that is $e_3 = 9$. The identities $D_p = d_{10}^e$ follow from Table 1, for instance $(p - 1)^2/36 + (p - 1)/3 + 4 = (p^2 + 10p + 133)/36$. $\square$

This is the mechanism of [dSVL12, Corollary 2]: $V_p > 0$ is not given by a congruence condition [dSVL12, Theorem 2], and the polynomials for the types (1, 4) and (9, 4) differ.

6 The sum over the isomorphism classes

For $p \geq 5$ every elliptic curve over $\mathbb{F}_p$ has a model $y^2 = x^3 + ax + b$, and the isomorphisms between such models are the maps $(x, y) \mapsto (u^2x, u^3y)$; these are the changes of variables $x = u^2x' + r$, $y = u^3y' + su^2x' + t$ between Weierstrass equations [Sil09, Chapter III] that preserve the short form.

Lemma 6.1. *Let $X = \{(a, \lambda) \in \mathbb{F}_p^2 : 4a^3 + 27b^2 \neq 0 \text{ for } b = -\lambda^3 - a\lambda\}$, with the action $u \cdot (a, \lambda) = (u^4a, u^2\lambda)$ of $\mathbb{F}_p^\times$. Then $|X| = (p - 1)^2$, and the orbits are the isomorphism classes of pairs (E, P) with $P \in E[2](\mathbb{F}_p) \setminus \{O\}$, hence, by [MS25, Theorem A], of the groups $G_{E,P}(\mathbb{F}_p)$ with P of order 2. The stabilizer of (a, λ) is $\text{Stab}(P)$, of order $s = 4$ if $\lambda = 0$ and $p \equiv 1 \pmod{4}$, and $s = 2$ otherwise. There are $2(p - 1) + 2\delta_4$ classes, $4\delta_4$ of them with $s = 4$, and $\sum 1/s = p - 1$.*

Proof. $x^3 + ax + b = (x - \lambda)(x^2 + \lambda x + \lambda^2 + a)$ has a repeated root if and only if $3\lambda^2 + a = 0$ or $3\lambda^2 + 4a = 0$; for $\lambda \neq 0$ these are two values of a , and for $\lambda = 0$ one. So $|X| = p^2 - 2(p - 1) - 1$. The stabilizer of (a, λ) consists of the u with $u^4a = a$ and $u^2\lambda = \lambda$, which are the automorphisms of E fixing P ; it is $\{\pm 1\}$ if $\lambda \neq 0$, and μ_4 if $\lambda = 0$ (then $b = 0 \neq a$). Summing $s/(p - 1)$, resp. $1/(p - 1)$, over X gives the number of classes, resp. $\sum 1/s$; the classes with $s = 4$ are those of $(a, 0)$ with a modulo fourth powers. $\square$

Lemma 6.2 (Tate normal form of level 6; Kubert [Kub76]). *Let K be a field of characteristic prime to 6, and for $c \in K$ let $E_c: y^2 + (1 - c)xy - (c + c^2)y = x^3 - (c + c^2)x^2$ and $\Delta(c) = c^6(c + 1)^3(9c + 1)$. For every c with $\Delta(c) \neq 0$, E_c is an elliptic curve on which $Q = (0, 0)$ has order exactly 6. Conversely, for every elliptic curve E/K and $Q \in E(K)$ of order exactly 6 there is exactly one $c \in K$ with $\Delta(c) \neq 0$ such that $(E, Q) \cong (E_c, (0, 0))$ over K .*

Proof. On $E(b, c): y^2 + (1 - c)xy - by = x^3 - bx^2$ with $b \neq 0$, the tangent at $Q = (0, 0)$ is $y = 0$, which meets the curve again at $(b, 0)$; so $2Q = -(b, 0) = (b, bc)$. The line $y = cx$ through Q and $2Q$ meets the curve where $x(x - b)(x - c) = 0$, so $3Q = -(c, c^2) = (c, b - c)$, and $-3Q = (c, c^2)$. Hence $6Q = O$ if and only if $b = c + c^2$, and then $2Q, 3Q$ are affine points, so Q has order 6. The discriminant of E_c is $\Delta(c)$, by the usual formula for Weierstrass equations [Sil09, Chapter III].

Let $E: y^2 = x^3 + Ax + B$ and $Q = (x_0, y_0)$ of order 6; then $y_0 \neq 0$. With $m = (3x_0^2 + A)/(2y_0)$, the substitution $x = X + x_0$, $y = Y + mX + y_0$ gives $Y^2 + 2mXY + a_3Y = X^3 + a_2X^2$ with $a_3 = 2y_0 \neq 0$ and

$a_2 = 3x_0 - m^2$; here $a_2 \neq 0$, since otherwise the tangent $Y = 0$ would meet E only at Q and $3Q = O$. The substitution $X = u^2x$, $Y = u^3y$ with $u = a_3/a_2$ then gives $y^2 + (2m/u)xy + a'y = x^3 + a'x^2$ with $a' = a_2^3/a_3^2$, which is $E(b, c)$ with $b = -a'$ and $c = 1 - 2m/u$, and $b = c + c^2$ by the first part. Finally, an isomorphism between two curves $y^2 + a_1xy + a_3y = x^3 + a_2x^2$ is a change of variables $x = u^2x' + r$, $y = u^3y' + su^2x' + t$ [Sil09, Chapter III], and $r = t = 0$ if it fixes $(0, 0)$; the new equation has the term a_3su^2x' of degree one, so $s = 0$, and then $a'_i = a_iu^{-i}$. If both curves have $a_2 = a_3$, then $u = 1$; so c is unique. $\square$

Lemma 6.3. *Let K be a field of characteristic prime to 6 and $E: y^2 + a_1xy + a_3y = x^3$ an elliptic curve over K , so that $T = (0, 0)$ has order 3, $\Delta(E) = a_3^3D$ with $D = a_1^3 - 27a_3 \neq 0$. Then $E[3] \subseteq E(K)$ if and only if K contains a primitive cube root of unity and D is a cube in K . Every elliptic curve over K with a point of order 3 in $E(K)$ has such a model; for it, the condition reads: K contains a primitive cube root of unity and $\Delta(E)$ is a cube.*

Proof. The abscissae of the points of order 3 are the roots of the 3-division polynomial $3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8$ (a point R of order 3 satisfies $x(2R) = x(-R) = x(R)$, and the duplication formula turns this into the vanishing of this polynomial [Sil09, Chapter III]), here $x(3x^3 + a_1^2x^2 + 3a_1a_3x + 3a_3^2)$. The root 0 belongs to $\pm T$. With $x = a_3/w$ the cubic factor becomes $(3w^3 + 3a_1w^2 + a_1^2w + 3a_3)a_3^2/w^3$, and $9(3w^3 + 3a_1w^2 + a_1^2w + 3a_3) = (3w + a_1)^3 - D$. The four subgroups of order 3 have distinct abscissae, so the three values $3w + a_1$ belonging to the subgroups other than $\langle T \rangle$ are the three distinct cube roots of D . If $E[3] \subseteq E(K)$, they lie in K , and their ratios are primitive cube roots of unity. Conversely, if K contains the cube roots of unity and D is a cube, all abscissae lie in K , so every $\sigma \in \text{Gal}(\bar{K}/K)$ maps each $R \in E[3] \setminus \langle T \rangle$ to $\pm R$; if $\sigma R = -R$, then $\sigma(R + T) = -R + T$ would equal $R + T$ or $-R - T$, forcing $2R = O$ or $2T = O$. So σ fixes $E[3]$. For the last statement, move a point of order 3 to $(0, 0)$ and make its tangent horizontal; as the point is a flex, the tangent meets E only there, and the equation takes the form $y^2 + a_1xy + a_3y = x^3$. The class of Δ modulo cubes does not depend on the model, since Δ changes by twelfth powers. $\square$

Lemma 6.4. *For $x \in X$ let $e_3(x) = |E[3](\mathbb{F}_p)|$ for the curve of x . Then*

$$\sum_{x \in X} (e_3(x) - 1) = (p - 1)(p - 3), \quad \#\{x \in X : e_3(x) = 9\} = \delta_3 \frac{(p - 1)(p - 7)}{24},$$

$$\sum_{x \in X} \frac{1}{e_3(x)} = (p - 1) \alpha(p), \quad \alpha(p) = \frac{2p}{3} + \frac{2}{27}(p - 7) \delta_3.$$

Proof. The triples (a, λ, T) with $(a, \lambda) \in X$ and $T \in E[3](\mathbb{F}_p) \setminus \{O\}$ correspond to the triples (a, b, Q) with $Q \in E(\mathbb{F}_p)$ of order 6, by $Q = P + T$, $P = 3Q$, $T = -2Q$, where $P = (\lambda, 0)$. The group $\mathbb{F}_p^\times$ acts freely on them: if u fixes (a, λ, T) with $T = (x_T, y_T)$, then $y_T \neq 0$ gives $u^3 = 1$, and $u^2x_T = x_T$, $u^2\lambda = \lambda$ give $u^2 = 1$ unless $x_T = \lambda = 0$, which is impossible, because then $b = 0$ and $y_T^2 = x_T^3 + ax_T = 0$. The orbits are the isomorphism classes of pairs (E, Q) with Q of order 6, and by Lemma 6.2 there are $p - 3$ of them, as $0, -1, -1/9$ are distinct. This gives the first formula. By Lemma 6.3, the curve E_c , which has the point $2Q$ of order 3, has full rational 3-torsion if and only if $p \equiv 1 \pmod{3}$ and $\Delta(c)$ is a cube, that is $9c + 1$ is a cube. As c runs over $\mathbb{F}_p \setminus \{0, -1, -1/9\}$, $9c + 1$ runs over $\mathbb{F}_p^\times \setminus \{1, -8\}$, and 1 and -8 are cubes; so for $p \equiv 1 \pmod{3}$ there are $(p - 1)/3 - 2 = (p - 7)/3$ such classes. Each x with $e_3(x) = 9$ gives 8 triples, all in these classes, so $8 \#\{e_3 = 9\} = (p - 1)(p - 7)/3$; for $p \equiv 2 \pmod{3}$ there is no such x . Finally, with $n_k = \#\{x : e_3(x) = k\}$, $n_1 + n_3 + n_9 = (p - 1)^2$ and $2n_3 + 8n_9 = (p - 1)(p - 3)$ give $\sum 1/e_3 = (p - 1)^2 - (p - 1)(p - 3)/3 + \frac{16}{9}n_9 = (p - 1)\alpha(p)$. $\square$

Proof of Theorem 1.3. By Theorem 1.1 only the classes with P of order 2 contribute, and by Theorem 1.2, $d_{10} = (F_1 - F_{\text{transl}})/(e_3s) + (F_{\text{refl}} + F_{\text{transl}})/s + [s = 4]F_{\text{ord4}}/2$. Summed over the classes of

Lemma 6.1, $\sum 1/s = p - 1$; an orbit of size $(p - 1)/s$ contributes $1/(e_3 s) = \sum_x 1/((p - 1)e_3(x))$ over its points, so $\sum 1/(e_3 s) = \alpha(p)$ by Lemma 6.4; and there are $4\delta_4$ classes with $s = 4$. Hence

$$S_{10}(p) = (F_{\text{refl}} + F_{\text{transl}})(p - 1) + (F_1 - F_{\text{transl}})\alpha(p) + 2\delta_4 F_{\text{ord}4},$$

and S_{10}^e is given by the same formula with F^e in place of F . Inserting the closed forms gives the polynomials of Theorem 1.3. All ingredients are polynomials in p on the residue classes determined by $\delta_3, \delta_4, \delta_8, \delta_9$, that is modulo 72, and for the exponent- p count by δ_3, δ_4 , that is modulo 12. $\square$

Remark 6.5 (why the dependence on e_3 cancels). For one curve over $\mathbb{Q}$, e_3 depends on how p splits in $\mathbb{Q}(E[3])$, which is in general not PORC [MS25, Corollary C, Remark 1.2]; for $y^2 = x^3 - x$ this is [dSVL12, Theorem 2]. The sum over all classes only involves the numbers of Lemma 6.4, which count points on curves of genus 0: the pairs (E, Q) with Q of order 6 are parametrized by Kubert’s c -line, an open part of the modular curve $X_1(6)$, and those with full rational 3-torsion by the curve $w^3 = 9c + 1$, which is the w -line. The count n_9 was first obtained with the Hesse pencil $x^3 + y^3 + z^3 = 3mxyz$, the universal family of elliptic curves with a level-3 structure [AD09, §2]: with origin $(1 : -1 : 0)$ its points of order 2 are $(1 : 1 : t)$, $t^3 - 3mt + 2 = 0$, and $m^3 = 1$ exactly for $t \in \mu_3 \cup -2\mu_3$; this gives $p - 7$ pairs (m, P) , and n_9 after dividing by the 24 bases of $E[3]$ of given Weil pairing (over $\mathbb{F}_p$ this uses the rigidity of level 3, which the proof above avoids).

Remark 6.6 (descendants of order p^{11} ; data only). The immediate descendants of order p^{11} correspond to the $\text{Aut}(\mathfrak{g})$ -orbits on the complements of N in M . A program counts them by Burnside’s lemma over $\Psi_S \times \text{GL}_2(\mathbb{F}_p)$; the numbers d_{11} and their sums $S_{11}(p)$ over the classes are:

p	type (1, 2)	type (3, 2)	type (1, 4)	$S_{11}(p)$
5	62088351503793	20696228400858	31044175770943	413922565900660
7	47515195180766327	15838404019120346	–	443475177522612000
11	373095936474912917119	124365313329192913402	–	5472073744332498312644

All these values were recomputed by the third verification run with its own programs (Burnside’s lemma over Ψ acting on the complements of N modulo the σ_θ , for all classes with $p = 5, 7, 11$), but nothing is proved about them; we do not know whether S_{11} , or $S_{10} + S_{11}$, is PORC. In the computed cases d_{11} again splits over the four types, so the argument of Theorem 1.3 would reduce the question to four functions of p , for which we have no closed forms.

7 Computations, verification and scope

Apart from expansions of polynomials, which the programs also check, no proof depends on a computation. The package has three parts; its `README.md` gives commands, running times and what each program checks. *The program written with this note*, `check_note.py` (25 seconds; “TOTAL failures: 0”), checks (A) Remark 3.3 and Lemma 3.2 and Lemma 4.2(b) over $\mathbb{Z}[\lambda, \mu, a]$, (B) $\dim N$ from the definition for all pairs with $p = 5, 7$, (C) Lemma 5.2 and Proposition 5.3 for $5 \leq p < 100$, (D) Lemmas 6.1 to 6.4 for $5 \leq p < 60$, (E) Theorem 1.2 for $p = 5, 7$ by a direct Burnside count on M^* , with an exhaustive search for Ψ_S , (F) Theorem 1.3 for $p \leq 23$ and Table 1, and (G) Corollary 5.5. *The programs with which the results were first obtained* (`original/`) include $\dim N$ from the definition and GAP’s p -quotient algorithm [GAP26] (no Lie theory) for all 3632 pairs with $p \leq 13$; direct counts of d_{10} , d_{10}^e for all 182 classes with P of order 2 and $p \leq 23$; the closed forms for the 76 primes below 400; the data of Remark 6.6; and a GAP pipeline without Lie theory (AutPGrp [ELGO02], lifts to the p -covering group, Burnside’s lemma), which confirmed d_{10} , d_{10}^e for 9 of the 10 classes at $p = 5$ (for $y^2 = x^3 + 2x$, $P = (0, 0)$, AutPGrp did not finish within 11 minutes). *The programs of the three verification runs* are in `verification_run_A/`, `verification_run_B/` and `independent_run_2/` (the

third run). The quick programs of the first two parts and of the first two runs were run again from a copy of the package, twice (when this note was written, and by the third run), and reproduced the recorded outputs, up to running times.

Verification. The results were first obtained, with proofs and with the programs in `original/`. Three independent verification runs, all AI-assisted, followed; each wrote its own programs. The first two examined the first written version of the results, the third examined this note. The first run re-derived the proofs line by line; compared the statements used from [MS25] (Theorems A, B, 2.13, 2.15, 5.6, 5.8 with their proofs, Lemmas 5.4, 5.5, Corollary 3.6) and [dSVL12] with the texts; redid the case analyses for F_1 , F_{refl} , F_{transl} and the exponent- p functions; re-ran ten programs of `original/` with identical outputs; and computed $\dim N$ from the definitions for all $(\lambda, \mu, a) \in \mathbb{F}_p^3$, $p = 5, 7, 11$. It found no error and required seven corrections, all made, among them that χ in Lemma 4.2(c) be obtained over every $\mathbb{F}_p$, that F_{ord4} , first obtained by interpolation at primes, be derived, and that the dictionary with [MS25] be given.

The second run did not use the report of the first and, apart from re-running two programs of `original/`, used only its own programs. It proved Theorem 1.1 again with its own certificate (the 18×18 system for N^* has determinant $-4\mu^2$, with a 16×16 minor equal to 1 at $\mu = 0$), and confirmed it at the group level with GAP's `TwoCocycles` and `TwoCoboundaries` for all 3632 pairs with $p \leq 13$. It computed Ψ by an exhaustive search assuming no structure, with $|\Psi| = e_3 s |\text{GL}_2(\mathbb{F}_p)|$, for all 182 classes with P of order 2 and $p \leq 23$, and counted their descendants of order p^{10} in its own model, by enumerating the orbits ($p = 5$, and a fibre at $p = 7$) and by Burnside's lemma; all values agree with Theorem 1.2. At the group level, for all 68 classes with $p \leq 13$, among them $y^2 = x^3 + 2x$, $P = (0, 0)$ at $p = 5$ (6780 descendants, 12 of exponent p), and for one class of each type at $p = 17$, it computed the p -covering group with GAP's p -quotient algorithm, lifted its own generators of $\text{Aut}(H)$ to it, and found an invertible intertwiner, respecting the nucleus and the p -th powers, between the action on the multiplier and the one used in its counts. It also reproduced $D_p = 12, 34, 30, 52$ on the presentation of [dSVL12], checked $V_p > 0 \Leftrightarrow e_3 = 9$ for the 99 primes $p \equiv 1 \pmod{12}$ below 3000, and tested Lemmas 6.1 and 6.4 for $p \leq 97$ and [MS25, Theorem A] at $p = 5, 7$, and checked the polynomials of Theorem 1.3 against the general formula below 5000. It required four corrections, all made: the PORC convention, the derivation of F_{ord4} , the attribution of the group-level confirmation, and Remark 4.4.

When this note was written, after the two runs, the following were added: Lemma 3.2; Lemma 5.2 and the derivation of the four closed forms from it; Lemmas 6.2 and 6.3, which give Lemma 6.4 without the Hesse pencil; and the proofs of Lemma 2.3 and Lemma 2.4(b). `check_note.py` checks their statements (parts A, C, D).

The third run examined the final text, and these additions first. It re-derived all proofs line by line (among them the elimination of Lemma 3.2, the case analyses of Proposition 5.3 for all four types, the dictionary of Lemma 4.3, Lemmas 6.2 and 6.3 and the isomorphism of Corollary 5.5), compared the quoted statements with the texts of [DENR25, MS25, dSVL12, AD09, VL18a], and wrote its own programs: $\dim N$ from the definition for all 3632 pairs with $p \leq 13$; Ψ by an exhaustive search of all 3-dimensional subspaces of $\mathbb{F}_p^6$ (for $\mathcal{T}(t)$) and of the stabilizer of (V_1, V_2) , with $|\Psi| = e_3 s |\text{GL}_2(\mathbb{F}_p)|$, for the 22 classes with $p \leq 7$; d_{10} and d_{10}^e by Burnside's lemma in its own model of M , for all 68 classes with $p \leq 13$ and for one class of each type at $p = 17$ and $p = 19$, where the terms with δ_8 and δ_9 occur, all equal to Theorem 1.2, and with sums equal to Theorem 1.3 for $p \leq 13$; the order- p^{11} counts for all classes with $p = 5, 7, 11$, which reproduce every value of Remark 6.6; Lemma 5.2 and Proposition 5.3 against direct sums, and Lemmas 6.1 and 6.4 and the class sums of Theorem 1.3 by brute force, for all primes $5 \leq p < 100$; and exact checks of the polynomial identities in the proofs. It ran `check_note.py` and nineteen programs of `original/` and of the first two runs again from the

archive, with identical outputs, and repeated the literature search. It found no wrong statement and no gap that could not be closed, and required corrections that were made: the references to [Sil09] were reduced to the chapter, the constancy of F_γ on the translations was justified (before Lemma 5.2), two citations of [MS25] were made precise, and the text was updated for its results.

Scope and priority. The note answers (Q1) for every $p \geq 5$ and every pair (E, P) , and (Q2) for the immediate descendants of order p^{10} , which is the source’s definition, and for those of order p^{10} and exponent p . If all immediate descendants in O’Brien’s sense are counted, those of order p^{11} included, (Q2) remains open (Remark 6.6). Only prime fields are treated, as in the question. The question is Maglione’s [DENR25]; the groups, their classification and the structure of their automorphisms are Maglione and Stanojkovski’s [MS25]; the group of $y^2 = x^3 - x$ goes back to du Sautoy [dS01, dS02], its exponent- p count and the non-PORC results to du Sautoy and Vaughan-Lee [dSVL12]; we use O’Brien’s p -group generation [O’B90], Lazard’s correspondence [Laz54] and Kubert’s normal form [Kub76].

What was read: [DENR25], pp. 1421–1422 and 1443–1444 with the footnote on PORC; [MS25] in the arXiv version v4, whose numbering we use (the journal version was not compared): Sections 1, 2.4, 4, 5, Definition 3.2, Corollary 3.6, Conjecture 6.9; [dSVL12] in the arXiv version v2: Sections 1, 2 and the beginnings of 4, 5; [AD09, §2] (arXiv:math/0611590) and [VL18a, §§1, 7, 8]. Kubert [Kub76] and Higman [Hig60a, Hig60b] were not read; Lemma 6.2 proves what we use of [Kub76]. O’Brien [O’B90], Lazard [Laz54], Khukhro [Khu98] and Silverman [Sil09] are cited for standard definitions and facts and were not consulted for this note. Of [Lee16, VL18b, VL17, SV21, OS26] only the abstracts were read.

The searches (27 October 2026, repeated in part on the same day by the third verification run) used the arXiv API (authors Maglione, Stanojkovski, Vaughan-Lee, du Sautoy, S. Lee; abstracts with “immediate descendants”, “PORC”, “descendants” and “elliptic”, “smooth cuboids”), citing works in OpenAlex (15 for [dSVL12], one for [MS25], none for [DENR25], three for [SV21], ten for [Lee16]) and Semantic Scholar, zbMATH Open, Crossref, and four web searches. No printed answer to (Q1) or (Q2) was found: [MS25] mentions immediate descendants only in passing (§1.2 there); [OS26], the only work found that cites it, concerns isomorphism invariants by its abstract; [dSVL12] treat only $y^2 = x^3 - x$ with $P = (0, 0)$; and [Evs08, Lee16, VL18b, VL17] concern other families of groups. A search that finds nothing is not a proof of novelty, and no priority is claimed.

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

- [AD09] Michela Artebani and Igor V. Dolgachev. The Hesse pencil of plane cubic curves. *L’Enseignement Mathématique (2)*, 55(3):235–273, 2009. doi:10.4171/LEM/55-3-3.
- [DENR25] Heiko Dietrich, Bettina Eick, Gabriele Nebe, and Colva Roney-Dougla. Computational group theory. *Oberwolfach Reports*, 22(2):1389–1450, 2025. Report No. 27/2025. doi:10.4171/OWR/2025/27.
- [dS01] Marcus du Sautoy. A nilpotent group and its elliptic curve: non-uniformity of local zeta functions of groups. *Israel Journal of Mathematics*, 126:269–288, 2001. doi:10.1007/BF02784157.

- [dS02] Marcus du Sautoy. Counting subgroups in nilpotent groups and points on elliptic curves. *Journal für die reine und angewandte Mathematik*, 549:1–21, 2002. doi:10.1515/crll.2002.063.
- [dSVL12] Marcus du Sautoy and Michael Vaughan-Lee. Non-PORC behaviour of a class of descendant p -groups. *Journal of Algebra*, 361:287–312, 2012. arXiv:1106.5530, doi:10.1016/j.jalgebra.2012.03.038.
- [ELGO02] Bettina Eick, C. R. Leedham-Green, and E. A. O’Brien. Constructing automorphism groups of p -groups. *Communications in Algebra*, 30(5):2271–2295, 2002. doi:10.1081/AGB-120003468.
- [Evs08] Anton Evseev. Higman’s PORC conjecture for a family of groups. *Bulletin of the London Mathematical Society*, 40(3):415–431, 2008. doi:10.1112/blms/bdn021.
- [GAP26] The GAP Group. GAP – Groups, Algorithms, and Programming, Version 4.16.1. <https://www.gap-system.org>, 2026.
- [Hig60a] Graham Higman. Enumerating p -groups. I: Inequalities. *Proceedings of the London Mathematical Society* (3), 10:24–30, 1960. doi:10.1112/plms/s3-10.1.24.
- [Hig60b] Graham Higman. Enumerating p -groups, II: Problems whose solution is PORC. *Proceedings of the London Mathematical Society* (3), 10:566–582, 1960. doi:10.1112/plms/s3-10.1.566.
- [Khu98] Evgenii I. Khukhro. *p -Automorphisms of Finite p -Groups*, volume 246 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1998. doi:10.1017/CB09780511526008.
- [Kub76] Daniel Sion Kubert. Universal bounds on the torsion of elliptic curves. *Proceedings of the London Mathematical Society* (3), 33(2):193–237, 1976. doi:10.1112/plms/s3-33.2.193.
- [Laz54] Michel Lazard. Sur les groupes nilpotents et les anneaux de Lie. *Annales scientifiques de l’École normale supérieure*, 71(2):101–190, 1954. doi:10.24033/asens.1021.
- [Lee16] Seungjai Lee. A class of descendant p -groups of order p^9 and Higman’s PORC conjecture. *Journal of Algebra*, 468:440–447, 2016. doi:10.1016/j.jalgebra.2016.08.042.
- [MS25] Joshua Maglione and Mima Stanojkovski. Smooth cuboids in group theory. *Algebra & Number Theory*, 19(5):967–1006, 2025. arXiv:2212.03941, doi:10.2140/ant.2025.19.967.
- [NOVL04] M. F. Newman, E. A. O’Brien, and M. R. Vaughan-Lee. Groups and nilpotent Lie rings whose order is the sixth power of a prime. *Journal of Algebra*, 278(1):383–401, 2004. doi:10.1016/j.jalgebra.2003.11.012.
- [O’B90] E. A. O’Brien. The p -group generation algorithm. *Journal of Symbolic Computation*, 9(5–6):677–698, 1990. doi:10.1016/S0747-7171(08)80082-X.
- [OS26] E. A. O’Brien and Mima Stanojkovski. Geometric invariants for p -groups of class 2 and exponent p . *Journal of Algebra*, 703:266–278, 2026. doi:10.1016/j.jalgebra.2025.08.029.

- [Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2009.
doi:10.1007/978-0-387-09494-6.
- [SV21] Mima Stanojkovski and Christopher Voll. Hessian matrices, automorphisms of p -groups, and torsion points of elliptic curves. *Mathematische Annalen*, 381(1–2):593–629, 2021.
doi:10.1007/s00208-021-02193-8.
- [ula26] ulamai. UnsolvedMath. Hugging Face dataset,
<https://huggingface.co/datasets/ulamai/UnsolvedMath>, 2026. Version 1.8.0; record OWR-14299292-015.
- [VL17] Michael Vaughan-Lee. The class three groups of order p^9 with exponent p . Preprint, 2017.
arXiv:1702.04898.
- [VL18a] Michael Vaughan-Lee. Graham Higman’s PORC theorem. Preprint, 2018.
arXiv:1808.04145.
- [VL18b] Michael Vaughan-Lee. Non-PORC behaviour in groups of order p^7 . *Journal of Algebra*, 500:30–45, 2018. doi:10.1016/j.jalgebra.2016.07.042.