hexagon:2611.00234v2

TORSION OF ELLIPTIC CURVES OVER NUMBER FIELDS OF DEGREE 10

FILIP NAJMAN

Abstract. We determine all the groups that appear as the torsion group of an elliptic curve over a number field of degree 10. There are 69 such groups, and 53 of them appear as the torsion group of infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves over number fields of degree 10. For 4 of the groups, namely $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/26\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/18\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$, we also determine all the elliptic curves over number fields of degree 10 that realize them, and there are only finitely many. These four groups were not known to occur over number fields of degree 10. The proofs combine the global method of Derickx, Hecke sieves, formal immersion criteria at the prime 2, and Riemann-Roch computations on modular curves and their quotients over finite fields.

1. Introduction

Let E be an elliptic curve over a number field K. By the Mordell-Weil theorem $E(K) \simeq E(K)_{\mathrm{tors}} \times \mathbb{Z}^r$, and by Merel's theorem [Mer96] the torsion subgroup $E(K)_{\mathrm{tors}}$ is bounded in terms of $d = [K : \mathbb{Q}]$ alone. Hence, for every $d \geq 1$ the set

$$\Phi(d) := \{\, E(K)_{\mathrm{tors}} \;:\; [K : \mathbb{Q}] = d,\ E/K \text{ an elliptic curve} \,\}$$

is finite. The set $\Phi(1)$ was determined by Mazur [Maz77], building on work of Kubert [Kub76], and $\Phi(2)$ by Kamienny [Kam92], building on work of Kenku and Momose [KM88]. Derickx, Etropolski, van Hoeij, Morrow and Zureick-Brown [DEvH+21] determined $\Phi(3)$, using earlier work of Jeon, Kim and Schweizer [JKS04], Parent [Par00] and Najman [Naj16]. Derickx and Najman [DN25] determined $\Phi(4)$, using earlier work of Jeon, Kim and Park [JKP06] and Bruin and Najman [BN16]. The author determined $\Phi(5)$ in [Naj26a], and $\Phi(6)$, $\Phi(7)$, $\Phi(8)$ and $\Phi(9)$ in [Naj26d]. In this paper we determine $\Phi(10)$.

Write $\Phi^\infty(d) \subseteq \Phi(d)$ for the subset of groups that occur as $E(K)_{\mathrm{tors}}$ for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves E over number fields K of degree d. The sets $\Phi^\infty(d)$ are known for $d \leq 9$: we have $\Phi^\infty(d) = \Phi(d)$ for $d = 1, 2$, the sets $\Phi^\infty(3)$ and $\Phi^\infty(4)$ were determined by Jeon, Kim and Schweizer [JKS04] and Jeon, Kim and Park [JKP06], $\Phi^\infty(5)$ and $\Phi^\infty(6)$ by Derickx and Sutherland [DS17], and $\Phi^\infty(7)$, $\Phi^\infty(8)$ and $\Phi^\infty(9)$ by Najman and Varivoda [NV26]. We also determine $\Phi^\infty(10)$.

Date: November 18, 2026.

2020 *Mathematics Subject Classification.* 11G05, 11G18, 14G05.

Key words and phrases. elliptic curves, torsion, number fields, modular curves, sporadic points.

The author was supported by the Croatian Science Foundation under the project no. IP-2022-10-5008, by the project "Implementation of cutting-edge research and its application as part of the Scientific Center of Excellence for Quantum and Complex Systems, and Representations of Lie Algebras", PK.1.1.10.0004, co-financed by the European Union through the European Regional Development Fund – Competitiveness and Cohesion Programme 2021–2027, and by the European Union – NextGenerationEU through the National Recovery and Resilience Plan 2021–2026, via an institutional grant of the University of Zagreb Faculty of Science, IK IA 1.1.3, Impact4Math.

Closely related is the set $S(d)$ of primes p for which there exists an elliptic curve over a number field of degree d with a point of order p. The sets $S(d)$ for $d \leq 8$ follow from the work of Mazur, Kamienny, Kenku and Momose, Parent, Derickx, Kamienny, Stein and Stoll, and Khawaja [Maz77, Kam92, KM88, Par00, DKSS23, Kha24], and Derickx and Stoll [DS25] developed tools that rule out most primes for any given d. The author [Naj26c, Theorem 1.1] recently determined $S(d)$ for $9 \leq d \leq 22$, and in particular showed that $S(10)$ is the set of primes up to 37. This is the starting point of our proof.

Our main result is the following theorem.

Theorem 1.1. *Let K be a number field of degree 10 and let E be an elliptic curve over K. Then $E(K)_{\mathrm{tors}}$ is isomorphic to one of the following groups:*

$$\begin{aligned}
&\mathbb{Z}/n\mathbb{Z}, && n = 1, \dots, 40,\ 42,\ 45,\ 50,\\
&\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, && n = 1, \dots, 15,\\
&\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z}, && n = 1, \dots, 6,\\
&\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4n\mathbb{Z}, && n = 1, 2, 3,\\
&\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6n\mathbb{Z}, && n = 1, 2.
\end{aligned}$$

Each of these 69 groups occurs as the torsion group of an elliptic curve over a number field of degree 10.

Of these 69 groups, the 35 groups of $\Phi^{\infty}(1) \cup \Phi^{\infty}(2) \cup \Phi^{\infty}(5)$ and the 18 groups

$$\mathbb{Z}/n\mathbb{Z},\ n \in \{23, 26, 27, 28, 30, 32, 33, 34, 36\}, \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n \in \{9, 10, 11, 12\},$$
$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}, \quad \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

occur for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves over number fields of degree 10 (Lemma 3.1 and Proposition 3.3). The groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ occur because the quintic curves with torsion $\mathbb{Z}/28\mathbb{Z}$ and $\mathbb{Z}/30\mathbb{Z}$ of [Naj26a] gain full 2-torsion over a quadratic extension (Proposition 3.5). For $N \in \{29, 31, 35, 37, 38, 39, 40, 42, 45, 50\}$ the group $\mathbb{Z}/N\mathbb{Z}$ is the torsion group of an elliptic curve coming from a point of degree 10 on $X_1(N)$ found by van Hoeij [vH14] (Proposition 3.4). For the remaining 4 groups we also determine all the elliptic curves in question.

Theorem 1.2. *Let G be one of the groups in the following table, let K be a number field of degree 10, and let E/K be an elliptic curve such that $E(K)$ has a subgroup isomorphic to G. Then $E(K)_{\mathrm{tors}} \simeq G$, and up to isomorphism the pair (K, E) is one of the pairs given in Section 11. The number of these pairs and their fields K are as follows.*

G	*pairs* (K, E)	*fields* K
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$	2	*10.6.396320664709.1, 10.2.799905449.1*
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$	1	*10.0.306454347.1*
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$	2	*10.0.2571428187.1*
$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$	1	*10.0.4678854192.1*

In particular, these 4 groups occur for only finitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves over number fields of degree 10.

The two pairs with torsion group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ are defined over the same field, and their elliptic curves are 2-isogenous. All the curves of Theorem 1.2 have j-invariants of degree 5 over $\mathbb{Q}$, which are not algebraic integers, so none of them has complex multiplication.

The elliptic curves of Theorem 1.2 are new, and they are listed in [Naj26b] as the points 2.26.10.a, 2.26.10.b, 3.15.10.a, 3.18.10.a, 3.18.10.b and 6.12.10.a. We found them in the course of this work, so the groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ were not known to occur in degree 10. The elliptic curves with torsion groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ over decic fields of Proposition 3.5 (the points 2.28.10.a, 2.30.10.a and 2.30.10.b), which we obtained from the quintic curves of van Hoeij with torsion $\mathbb{Z}/28\mathbb{Z}$ and $\mathbb{Z}/30\mathbb{Z}$, are also new.

The isomorphism of pairs is defined in Section 2.2. Note that $\mathbb{Z}/37\mathbb{Z}$ occurs in degrees 6 and 10, but in none of the degrees 7, 8 and 9 [Naj26d, Theorem 1.1].

Our second main result is the determination of $\Phi^{\infty}(10)$.

Theorem 1.3. *The set* $\Phi^{\infty}(10)$ *consists of the following* 53 *groups:*

$$\begin{aligned}
&\mathbb{Z}/n\mathbb{Z}, && n = 1, \dots, 28,\ 30,\ 32,\ 33,\ 34,\ 36,\\
&\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, && n = 1, \dots, 12,\\
&\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z}, && n = 1, \dots, 4,\\
&\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4n\mathbb{Z}, && n = 1, 2, 3,\\
&\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.
\end{aligned}$$

Hence the 16 groups of Theorem 1.1 that occur for only finitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves over number fields of degree 10 are

$$\mathbb{Z}/n\mathbb{Z},\ n \in \{29, 31, 35, 37, 38, 39, 40, 42, 45, 50\}, \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n \in \{13, 14, 15\},$$
$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}, \quad \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}.$$

For $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ this is Theorem 1.2, and for the cyclic groups other than $\mathbb{Z}/37\mathbb{Z}$ and for $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}$ it follows from the known ranks and gonalities of the modular curves. The Jacobian of $X_1(2, 30)$ also has rank 0, but the lower bound 10 for its gonality from [NV26, Table 1] is not sufficient, and we show that $X_1(2, 30)$ has no function of degree at most 10 over $\mathbb{Q}$ by computing the classes of all its effective rational cuspidal divisors of degree 10 (Proposition 13.7). The hardest case is $\mathbb{Z}/37\mathbb{Z}$, as $J_1(37)$ has positive rank and $\operatorname{gon}_{\mathbb{Q}} X_1(37) = 18 < 2 \cdot 10$, so neither of the usual criteria applies. As in the proof of [NV26, Proposition 5.7], where Najman and Varivoda showed that $X_1(37)$ has only finitely many points of degree 9, we reduce this case to a computation of Riemann-Roch spaces on $X_1(37)$ over $\mathbb{F}_2$ (Proposition 13.12).

Outline of the proof and of the paper. As in [DN25], [Naj26a] and [Naj26d], the classification reduces to showing that certain modular curves $X_1(m, n)$ have no non-cuspidal points over number fields of degree 10. We introduce the notation and collect the general tools from [Naj26d] in Section 2. In Section 3 we show that the groups of Theorem 1.1 occur, apart from the 4 groups of Theorem 1.2, and in Section 4 we show that 110 groups have to be ruled out. Over a number field K of degree 10 with $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \subseteq E(K)$ we have $m \in \{1, 2, 3, 4, 6, 11, 22\}$, and for $m \in \{3, 4, 6\}$ the problem becomes one about points of degree 5 over $\mathbb{Q}(\zeta_m)$.

The global method of Derickx [DN25, Proposition 4.3], combined with arguments with diamond operators, eliminates the groups $\mathbb{Z}/n\mathbb{Z}$ of $\mathcal{M}_{10}$ with $n \geq 95$ apart from $n \in \{99, 100, 105, 117\}$ (Section 5). The groups $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with $m \geq 3$ are treated in Section 6, and the groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$, together with the cyclic groups that Lemma 4.3 reduces to them, in Section 7. The remaining cyclic groups are treated in Sections 8 to 10:

with the Hecke sieve of [DN25, Proposition 5.5] and computations with the Picard groups of modular curves over finite fields, often after pushing the divisors forward to a curve of smaller level (Section 8), with formal immersion criteria at the prime 2 (Section 9), and, together with $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/39\mathbb{Z}$, with combinations of these methods on quotients of $X_1(n)$ (Section 10). In Section 11 we construct the elliptic curves with torsion groups $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/26\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/18\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ and determine all the points of the relevant degree on the corresponding modular curves, which also rules out the groups properly containing them. We prove Theorems 1.1 and 1.2 in Section 12 and Theorem 1.3 in Section 13, and the computations are described in Section 14.

Data availability and reproducibility. The code, the stored logs and the data of the computations described in this paper are available at

`https://github.com/F-Najman/deg10_torsion`

This paper refers to the revision `f6fd8eb` of this repository, and the links in the paper point to this revision. The `README` file there lists, statement by statement, which scripts establish each claim and which logs they produced, and also the checks that the proofs do not need (see Section 14). In the digital form of this article, the words reporting a computation, such as "we compute", are hyperlinks to the script that carries it out.

AI disclosure and comments. AI models were extensively used in the work leading to this paper. After completing [DN25] (with Derickx) and [Naj26a] and giving talks about this work, I was asked several times whether we could do such a classification for number fields of degree $d > 5$. My answer was that I thought it was not possible as it would require explicit computations that did not seem feasible to me. To check whether this was correct, in mid-October 2026 I asked AI whether this was possible, and whether it could do it. To my surprise, it was able to complete the classifications of possible torsion groups of elliptic curves over number fields, not only in degree 6, but later also in degrees 7, 8, 9 and finally 10. After some initial hesitation about releasing primarily AI-generated mathematics, I decided that the results were simply too interesting and the mathematics too beautiful to just stay on my computer.

OpenAI's GPT-6.1 Sol produced almost all of the mathematical content of the first version of the proof and carried out most of the computations. Anthropic's Claude Opus 5.5 reviewed that version, independently recomputed some of the computations (see Section 14) and the explicit examples, wrote the draft of the present manuscript and organized the code repository.

2. Notation and auxiliary results

We will be using the conventions and notation from [Naj26d, Section 2], which we will essentially repeat here for the convenience of the reader. We also collect the auxiliary results of [Naj26d] that we use. They are stated there for number fields of degree 6, 7, 8 and 9, but most of them are stated for an arbitrary degree d, and their proofs do not use the degree otherwise.

2.1. **Modular curves.** Throughout, $m \mid n$ are positive integers with $mn > 4$. We denote by $X := X_1(m,n)$ the modular curve parametrizing triples (E,P,Q) consisting of a generalized elliptic curve E and points P,Q of orders m and n generating a subgroup of $E[n]$ isomorphic to $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$, such that the Weil pairing of P and $(n/m)Q$ is ζ_m. It is a smooth projective geometrically irreducible curve over $\mathbb{Z}[\zeta_m,\frac{1}{n}]$, and it is a fine moduli space when

$n > 4$ (see [DN25, §2] and [DS17, §2]). Every curve $X_1(m,n)$ that we use has $n \geq 5$, so we use the fine moduli interpretation throughout. We write $Y_1(m,n)$ for the open subscheme obtained by removing the cusps, and $J := J_1(m,n)$ for the Jacobian of X. We abbreviate $X_1(n) := X_1(1,n)$ and $J_1(n) := J_1(1,n)$. For $m \leq 2$ the curve X is defined over $\mathbb{Q}$. For $d \geq 1$ we write $X^{(d)}$ for the d-th symmetric power of X, so that $X^{(d)}(\mathbb{Q}(\zeta_m))$ is the set of effective $\mathbb{Q}(\zeta_m)$-rational divisors of degree d on X. For a curve X over a field F with a set of cusps, such as $X_1(m,n)$ over $\mathbb{Q}(\zeta_m)$ or a quotient of it, we write $\mathrm{Cl}^c_F X$ for the subgroup of $J_X(F)$ generated by the classes of the F-rational divisors of degree 0 supported on the cusps. For a curve X we write $\mathrm{gon}_k X$ for its gonality over a field k, and J_X or $J(X)$ for its Jacobian. For a divisor D on a curve X over a field k we write $L(D) := \{f \in k(X)^\times : \mathrm{div}(f) + D \geq 0\} \cup \{0\}$ for its Riemann-Roch space and $\ell(D) = \dim L(D)$. Similarly, we write $\Omega(D)$ for the space consisting of 0 and the non-zero differentials ω on X with $\mathrm{div}(\omega) \geq D$. Then $\Omega(0) = H^0(X, \Omega^1)$ is the space of holomorphic differentials on X, and if $D = \sum_P m_P P$ is effective, then $\Omega(D)$ is its subspace of the differentials that vanish to order at least m_P at every P. The Riemann-Roch theorem states that $\ell(D) = \deg D + 1 - g + \dim \Omega(D)$, where g is the genus of X.

The cusps of $X_1(m,n)$ correspond to Néron k-gons with $m \mid k \mid n$ together with a level structure (see [DN25, §2]). All cusps are defined over $\mathbb{Q}(\zeta_n)$, and $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_m))$ acts on them through its action on $\mathbb{G}_m$. The cuspidal subscheme is finite étale over $\mathbb{Z}[\zeta_m, \frac{1}{n}]$. We denote by c_0 the cusp given by the Néron n-gon together with the level structure $(a,b) \mapsto (\zeta_m^a, b)$ (see [DN25, Lemma 2.8]), which is $\mathbb{Q}(\zeta_m)$-rational, and by c_* an arbitrary $\mathbb{Q}(\zeta_m)$-rational cusp used as a base point. For a cusp c we write $\sigma_q(c)$ for its image under the automorphism $\zeta_n \mapsto \zeta_n^q$ of $\mathbb{Q}(\zeta_n)$. When we list the degrees of closed cusps or of Galois orbits of cusps, a^r stands for r of them of degree a.

For a congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ we write $\overline{\Gamma}$ for its image in $\mathrm{PSL}_2(\mathbb{Z})$. The curve $X_1(m,n)_{\mathbb{C}}$ is the modular curve of the group $\Gamma_1(n) \cap \Gamma(m)$, and for $n > 2$ we have $[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma_1(n) \cap \Gamma(m)}] = \frac{m}{2} n^2 \prod_{\ell \mid n} (1 - \ell^{-2})$, the product being over the primes dividing n. We write $i(m,n)$ for this index, and $i(n) := i(1,n)$.

For $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ we write $\langle a \rangle$ for the diamond automorphism $(E,P,Q) \mapsto (E, a^{-1}P, aQ)$ of $X_1(m,n)$, which preserves the Weil pairing. For $m \leq 2$ it is the usual diamond operator, which is $(E,P) \mapsto (E, aP)$ on $X_1(n)$ and $(E,P,Q) \mapsto (E,P,aQ)$ on $X_1(2,n)$. It depends only on a modulo ± 1, and we call $\Delta(n) := (\mathbb{Z}/n\mathbb{Z})^\times / \{\pm 1\}$ the group of diamond operators. We write $\mathbb{Z}[\Delta(n)]$ for its group ring, which acts on divisors, on divisor classes and on J. For $a_1, \ldots, a_r \in (\mathbb{Z}/n\mathbb{Z})^\times$ we write $X/\langle a_1, \ldots, a_r \rangle$ for the quotient of X by the subgroup of $\Delta(n)$ generated by $\langle a_1 \rangle, \ldots, \langle a_r \rangle$. For a prime $q \nmid n$ with $q \equiv 1 \pmod m$ we write T_q for the Hecke correspondence $T_q(E,P,Q) = \sum_G (E/G, P \bmod G, Q \bmod G)$, the sum being over the $q+1$ subgroups $G \subseteq E[q]$ of order q, and we set

$$A_q := T_q - q\langle q \rangle - 1.$$

The congruence $q \equiv 1 \pmod m$ ensures that T_q preserves the Weil pairing, and that q splits completely in $\mathbb{Q}(\zeta_m)$. The operator A_q commutes with the diamond operators. For a prime $q \mid n$ we write U_q for the Hecke operator at q.

An automorphism of $X_1(m,n)$ of the form $(E,P,Q) \mapsto (E,P',Q')$, where P', Q' are integral linear combinations of P and Q, will be called a *level automorphism*. The diamond operators are level automorphisms. Some of the level automorphisms are defined over $\mathbb{Q}(\zeta_m)$, namely those that preserve the Weil pairing.

We will use reduction modulo primes of good reduction also for quotients of $X_1(m,n)$, by the following result of Liu and Lorenzini.

Lemma 2.1 ([LL99, Corollary 4.10]). *Let $f : X \to Y$ be a finite morphism of curves over a number field F, and let $\mathfrak{p}$ be a prime of F. Assume that X has good reduction at $\mathfrak{p}$ and that Y has positive genus. Then Y has good reduction at $\mathfrak{p}$, and f extends to a finite morphism of the smooth models over the localization of the ring of integers of F at $\mathfrak{p}$.*

In particular, every quotient of $X_1(m,n)$ of positive genus by a group of automorphisms defined over $\mathbb{Q}(\zeta_m)$ has good reduction at the primes above every prime $p \nmid n$, and we use these smooth models for reduction modulo the primes above p.

2.2. **Trace divisors.** Let K be a number field of degree 10 and E/K an elliptic curve with $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \subseteq E(K)$. By the Weil pairing $\mathbb{Q}(\zeta_m) \subseteq K$, so $\varphi(m) \mid 10$, and we put $d_m := 10/\varphi(m) = [K : \mathbb{Q}(\zeta_m)]$. Hence $m \in \{1,2,3,4,6,11,22\}$, and $d_m = 10$ for $m \leq 2$, $d_m = 5$ for $m \in \{3,4,6\}$ and $d_m = 1$ for $m \in \{11,22\}$. Choosing generators P, Q with the right Weil pairing we obtain a point $x \in Y_1(m,n)(K)$. We write $x^{(d_m)}$ for the sum of the $\mathbb{Q}(\zeta_m)$-conjugates of x, each counted $[K : \mathbb{Q}(\zeta_m)(x)]$ times. It is an effective $\mathbb{Q}(\zeta_m)$-rational divisor of degree d_m on X whose support contains no cusp, and we call it the *trace divisor* of x, usually denoted by D. All the arguments below are applied to trace divisors, so they also cover the case in which the residue field $\mathbb{Q}(\zeta_m)(x)$ is smaller than K.

If $\mathfrak{p}$ is a prime of $\mathbb{Q}(\zeta_m)$ above a prime $p \nmid n$, the reduction of D modulo $\mathfrak{p}$ is $\sum_{\wp \mid \mathfrak{p}} e(\wp/\mathfrak{p})[k_\wp : \kappa(x_\wp)]\, x_\wp$, where $\wp$ runs over the primes of K above $\mathfrak{p}$, $k_\wp$ is the residue field of $\wp$, and $x_\wp$ is the closed point of $X_{k_\mathfrak{p}}$ given by the reduction of x modulo $\wp$, with residue field $\kappa(x_\wp)$. In particular, a non-cuspidal closed point which occurs in the reduction with multiplicity 1 is $x_\wp$ for a prime $\wp$ which is unramified over $\mathfrak{p}$ and satisfies $k_\wp = \kappa(x_\wp)$.

Two pairs (K,E) and (K',E'), consisting of a number field and an elliptic curve over it, are *isomorphic* if there is a field isomorphism $\sigma : K \to K'$ such that $E^\sigma \simeq E'$ over K'.

2.3. **Hecke operators and reduction.**

Proposition 2.2 ([Naj26d, Proposition 2.2]). *Let X be $X_1(m,n)$ or its quotient by a subgroup of $\Delta(n)$, and let $q \nmid 2n$ be a prime with $q \equiv 1 \pmod m$.*

a) (Eichler-Shimura) $T_{q,\mathbb{F}_q} = \mathrm{Frob}_q + \langle q \rangle_{\mathbb{F}_q,*} \mathrm{Ver}_q$ *on $J_{X,\mathbb{F}_q}$, where $\mathbb{F}_q$ is the residue field of a prime of $\mathbb{Q}(\zeta_m)$ above q.*
b) *If $L \supseteq \mathbb{Q}(\zeta_m)$ is a number field in which q splits completely, then $A_q\big(J_X(L)_{\mathrm{tors}}\big) = 0$.*
c) *$A_q(C) = 0$ as a divisor for every $\mathbb{Q}(\zeta_m)$-rational cuspidal divisor C.*
d) *If $J_X(\mathbb{Q}(\zeta_m))$ is finite, then $[A_q(D)] = 0$ for every $\mathbb{Q}(\zeta_m)$-rational divisor D on X. In particular $A_q(D)$ is principal for every $D \in X^{(d)}(\mathbb{Q}(\zeta_m))$ and every d.*

For $m \leq 2$ these are [DN25, (2.2), Proposition 2.6, Lemma 2.8 and Lemma 5.4]. We also need the action of T_q on all the cusps, not only on the rational ones.

Lemma 2.3 ([Naj26d, Lemma 2.3]). *Let X be $X_1(m,n)$ or its quotient by a subgroup of $\Delta(n)$, let $q \nmid n$ be a prime with $q \equiv 1 \pmod m$, and let $\sigma_q \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_m))$ be the automorphism with $\sigma_q(\zeta_n) = \zeta_n^q$. For every cusp c of X we have*

$$T_q c = \sigma_q(c) + q\langle q \rangle \sigma_q^{-1}(c)$$

as divisors. Hence $A_q C = (\sigma_q C - C) + q\langle q \rangle(\sigma_q^{-1} C - C)$ for every cuspidal divisor C, and $A_q C = 0$ if $\sigma_q(C) = C$. The same holds for the reductions modulo a prime $p \nmid qn$, where σ_q

acts on the closed cusps through the reduction of the cusps, and in particular $A_qC = 0$ *for every cuspidal divisor* C *on* $X_{\mathbb{F}_{p^f}}$ *if* $q \equiv p^{fk} \pmod{n}$ *for some* k.

Some of our computations use models of $X_1(n)$ and its quotients given by q-expansions, which parametrize the dual objects $(E/\langle P\rangle,$ the induced μ_n-structure$)$. The isomorphism between the two models conjugates $\langle a\rangle$ to $\langle a\rangle^{-1}$, and on the dual model the Eichler-Shimura relation reads $T_q = \langle q\rangle \operatorname{Frob}_q + q \operatorname{Frob}_q^{-1}$, with annihilator $T_q - \langle q\rangle - q$, and the formula of Lemma 2.3 reads $T_q c = \langle q\rangle \sigma_q(c) + q\sigma_q^{-1}(c)$ (see [Naj26d, Section 2.3]).

We will also use the following results.

- (*Manin-Drinfeld* [Man72, Dri73]) the class of a degree 0 cuspidal divisor on X is torsion in $J(\overline{\mathbb{Q}})$;
- (*Katz* [Kat81, Appendix]) if $p > 2$ is a prime and A is an abelian variety over a number field L with good reduction at a prime $\wp$ of L above p which is unramified in L, then reduction modulo $\wp$ is injective on $A(L)_{\mathrm{tors}}$;
- (*Parent* [Par00, Proposition 2.3]) if A is an abelian variety over a number field L with good reduction at a prime λ above 2 which is unramified in L, then the kernel of reduction modulo λ on $A(L)_{\mathrm{tors}}$ is trivial or of exponent 2 (see [Naj26d, Section 2.3]);
- (*Abramovich* [Abr96, proof of Theorem 0.1]*, with the bound* $\lambda_1 \geq 975/4096$ *of Kim-Sarnak* [Kim03, Appendix 2]) for a congruence subgroup $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$,
$$\operatorname{gon}_{\mathbb{C}} X_\Gamma \geq \tfrac{325}{2^{15}} [\mathrm{PSL}_2(\mathbb{Z}) : \Gamma];$$
- (*Kato* [Kat04, Corollary 14.3]) if A is a quotient of $J_1(n)$ over $\mathbb{Q}$ with $L(A, 1) \neq 0$, then $A(\mathbb{Q})$ is finite.

We use Kato's theorem in the form of the *winding quotient*, as in [Naj26d, Section 2.3]: we compute, for each Galois orbit of even Dirichlet characters χ modulo n, the winding submodule of the space of modular symbols with character χ, and if it is the whole space, then all the factors with character χ have finitely many rational points.

Lemma 2.4 ([Naj26d, Lemma 2.4])**.** *Let* K *be a number field, let* E/K *be an elliptic curve with* $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \subseteq E(K)$*, and let* $\wp$ *be a prime of* K *above a rational prime* $p \nmid n$*. Then* E *does not have additive reduction at* $\wp$*.*

The following proposition is [DN25, Proposition 5.2], stated also for quotients of $X_1(m, n)$ and for one prime of $\mathbb{Q}(\zeta_m)$ above p at a time, as in [Naj26d, Proposition 2.5].

Proposition 2.5 ([Naj26d, Proposition 2.5])**.** *Let* $F = \mathbb{Q}(\zeta_m)$*, let* $p \nmid n$ *be a prime, let* X *be* $X_1(m, n)$ *or its quotient of positive genus by a subgroup of* $\Delta(n)$*, and let* $d \geq 1$*. Assume that* $J_X(F)$ *is finite and that one of the following holds:*

a) $p > 2$ *and* $\operatorname{gon}_F X > d$*;*
b) $p = 2$ *and* $\operatorname{gon}_F X > 2d$*.*

Then no effective F*-rational divisor of degree* d *on* X *whose support contains no cusp reduces to a cuspidal divisor modulo a prime of* F *above* p*. In particular, if* $X = X_1(m, n)$*, then every elliptic curve* E *over a degree* d *extension* K *of* F *with* $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \subseteq E(K)$ *has, for every prime* $\mathfrak{p}$ *of* F *above* p*, good reduction at at least one prime of* K *above* $\mathfrak{p}$*.*

The proof of Proposition 2.5 shows a little more, which we will use when the gonality bound is not available. If $J_X(F)$ is finite, p is odd and D reduces to an effective cuspidal divisor $\overline{C}$ modulo a prime above p, then $D \sim C$ over a number field unramified above p,

where C is the lift of $\overline{C}$, so $\ell(\overline{C}) \geq \ell(C) \geq 2$ by semicontinuity. For $p = 2$ we use the following lemma, which is [Naj26d, Lemma 5.3], whose proof works for any prime $\mathfrak{p}$ of F above 2.

Lemma 2.6 ([Naj26d, Lemma 5.3])**.** *Let $m \mid n$ with n odd and $mn > 4$, let $F = \mathbb{Q}(\zeta_m)$, let $\mathfrak{p}$ be a prime of F above 2 with residue field k, and let $d \geq 1$. Let $X = X_1(m,n)$, and assume that $J_X(F)$ is finite and that*

$$\ell(2\overline{C}) = 1$$

for every effective cuspidal divisor $\overline{C}$ of degree d on X_k. Then no effective F-rational divisor of degree d on X whose support contains no cusp reduces to a cuspidal divisor modulo $\mathfrak{p}$.

Lemma 2.7 ([Naj26d, Lemma 2.6], [DN25, Lemma 5.3])**.** *Let $p \nmid n$ be a prime and let $K \supseteq \mathbb{Q}(\zeta_m)$ be a number field. Suppose that for every prime $\wp$ of K above p there is no elliptic curve E' over the residue field $\mathbb{F}_\wp$ with $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \subseteq E'(\mathbb{F}_\wp)$. Then no elliptic curve E/K with $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \subseteq E(K)$ has good reduction at a prime of K above p.*

Whenever we invoke Lemma 2.7, the hypothesis follows from the Hasse bound, from Waterhouse's description [Wat69, Theorem 4.1] of the possible traces of Frobenius, or from an explicit enumeration of all elliptic curves over the relevant finite fields.

2.4. **Divisors and level automorphisms.**

Lemma 2.8 ([Naj26d, Lemma 2.7])**.** *Let X be a curve over a field F, and let D and A be effective F-rational divisors of degree d on X with $A \sim D$.*

a) *If $\operatorname{gon}_F X > d$, then $A = D$.*
b) *If D is a closed point of degree d and $A \neq D$, then there is a function on X over F of degree exactly d.*

Lemma 2.9 ([Naj26d, Lemma 2.8])**.** *Let G be a finite group of level automorphisms of $X_1(m,n)$, and let D be a divisor on $X_1(m,n)$ whose support consists of non-cuspidal points without complex multiplication. Then no element $g \neq 1$ of G fixes a geometric point in the support of D. If moreover $gD = D$ for all $g \in G$, then the geometric points in the support of D form a union of G-orbits of length $\#G$, and $D = \sum_O m_O \sum_{x \in O} x$, where O runs over these orbits. In particular $\#G \mid \deg D$.*

Lemma 2.10 ([Naj26d, Lemma 2.9])**.** *Let $F = \mathbb{Q}(\zeta_m)$, let $p \nmid n$ be a prime, and let X be $X_1(m,n)$ or its quotient of positive genus by a subgroup of $\Delta(n)$. Let g be a level automorphism of X defined over F, which maps cusps to cusps and extends to the smooth model of X over the primes above p, such that $(g-1)J_X(F)$ is finite. Let D be an effective F-rational divisor of degree d on X, and let C be an effective cuspidal divisor of degree e defined over a number field $L \supseteq F$ which is unramified above p, such that g fixes the reduction of $D - C$ modulo a prime above p. Assume that one of the following holds:*

a) *p is odd, C is F-rational and $\operatorname{gon}_F X > d + e$,*
b) *p is odd and $\operatorname{gon}_{\mathbb{C}} X > d + e$,*
c) *$p = 2$ and $\operatorname{gon}_{\mathbb{C}} X > 2(d + e)$,*
d) *$p = 2$, C is F-rational, g has odd order and acts trivially on $J_X(F)[2]$, and $\operatorname{gon}_F X > d + e$.*

Then $gD + C = D + gC$. In particular, if the support of D contains no cusp, then $gD = D$ and $gC = C$.

Every level automorphism of X defined over F satisfies the assumption on g if $J_X(F)$ is finite. For $m = 1$ and $g = \langle a \rangle$ the assumption holds if all the factors of J_X on which $\langle a \rangle$ acts non-trivially have finitely many rational points, in particular if every character χ for which the winding submodule is not the whole space satisfies $\chi(a) = 1$.

Lemma 2.11 ([Naj26d, Lemma 2.10])**.** *Let C be a smooth projective curve over $\mathbb{F}_q$ with q odd, and let f be a function on C with $\operatorname{div}(f) = 2A$ for a divisor A. For a divisor $Z = \sum n_P P$ whose support is disjoint from that of $\operatorname{div}(f)$ put $\chi_f(Z) = \prod_P N_{\mathbb{F}_{q}(P)/\mathbb{F}_q}(f(P))^{n_P}$ modulo $\mathbb{F}_q^{\times 2}$. Then χ_f induces a homomorphism $\chi_f : \operatorname{Pic}^0(C) \to \mathbb{F}_q^\times/\mathbb{F}_q^{\times 2}$, which is trivial on every subgroup of odd order.*

Lemma 2.12 ([DS25, Proposition 2.2], [Naj26d, Lemma 2.13])**.** *Let X be $X_1(n)$ or its quotient by a subgroup of $\Delta(n)$, and let $q \nmid n$ be a prime. Let L be a divisor on $X_{\mathbb{C}}$ whose support consists of non-cuspidal points at which the elliptic curve has no complex multiplication. If $A_q L = 0$, then $L = 0$.*

Lemma 2.13 ([Naj26d, Lemma 8.1])**.** *Let X be a smooth projective geometrically integral curve over a field k, and let $B = T - U$ with T, U effective divisors of the same degree. Let $\mathcal{L}, \mathcal{M}$ be line bundles on X, and choose $0 \neq F \in H^0(X, \mathcal{L}(-T))$ and $H \in H^0(X, \mathcal{M}(-T))$. If the linear map*

$$H^0(X, \mathcal{L}) \longrightarrow H^0(U, \mathcal{L}|_U) \oplus \frac{H^0(X, \mathcal{L} \otimes \mathcal{M})}{F \cdot H^0(X, \mathcal{M})}, \qquad G \longmapsto \big(G|_U,\ GH \bmod F \cdot H^0(X, \mathcal{M})\big)$$

is injective, then $\ell(B) = 0$. The same holds if several sections H are used.

We will use the following consequence of the results of Clark, Corn, Rice and Stankewicz on torsion of elliptic curves with complex multiplication.

Lemma 2.14. *Let K be a number field whose degree divides 10, and let E/K be an elliptic curve with complex multiplication. Then $E(K)_{\mathrm{tors}}$ is isomorphic to $\mathbb{Z}/m\mathbb{Z}$ for $m \in \{1, 2, 3, 4, 6, 7, 10, 11, 22, 31, 50\}$, to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ for $m \in \{2, 4, 6, 22\}$, or to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.*

Proof. For $[K : \mathbb{Q}] = 10$ this is [CCRS14, Section 4.10]. If $[K : \mathbb{Q}]$ is a proper divisor of 10, then by Lemma 3.1 there is a number field $K' \supseteq K$ of degree 10 with $E(K')_{\mathrm{tors}} = E(K)_{\mathrm{tors}}$. □

All these groups lie in $\mathcal{G}_{10}$ (Section 4), and none of them contains a group of $\mathcal{M}_{10}$ or one of the groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. Hence, in the trace divisor of a point giving such a subgroup over a number field of degree 10, every point corresponds to an elliptic curve without complex multiplication, as its residue field has degree dividing 10, and Lemma 2.9 applies.

The following lemma generalizes [Naj26d, Lemma 11.7].

Lemma 2.15. *Let $F = \mathbb{Q}(\zeta_m)$, let $X = X_1(m, n)$ with $J_X(F)$ finite, let $\mathfrak{p}$ be a prime of F above an odd prime $p \nmid n$, and let g be a level automorphism of X defined over F, of order r. Let D be an effective F-rational divisor on X whose support contains no cusp, and suppose that its reduction modulo $\mathfrak{p}$ is $D' + C'$, where D' has non-cuspidal support and satisfies $gD' = D'$, and C' is an effective cuspidal divisor. If*

$$\ell\Big(D' + \sum_{j=0}^{r-1} g^j C'\Big) = 1$$

on $X_{k_\mathfrak{p}}$, then $gD = D$ and $gC' = C'$. In particular, if g acts on the geometric cusps of X with all orbits of length r, then $r \mid \deg C'$.

Proof. The cusps of X are defined over $\mathbb{Q}(\zeta_n)$, which is unramified above p, so C' lifts to an effective cuspidal divisor C over a number field $L \supseteq F$ which is unramified above p. As in [Naj26d, proof of Lemma 2.9], the class $[gD - D - gC + C] \in J_X(L)$ is torsion, by the finiteness of $J_X(F)$ and the Manin-Drinfeld theorem. It reduces to $[gD' - D'] = 0$ modulo a prime above $\mathfrak{p}$, so it is 0 by Katz's result. Put $\Omega = \sum_{j=0}^{r-1} g^j C$. The divisors $D + \Omega - C$ and $gD + \Omega - gC$ are effective and linearly equivalent, and both reduce to $D' + \sum_j g^j C'$. By semicontinuity $\ell(D+\Omega-C) \leq 1$, so $D+\Omega-C = gD+\Omega-gC$, and hence $D-gD = C-gC$. The left side has non-cuspidal support and the right side is cuspidal, so $gD = D$ and $gC = C$, and hence $gC' = C'$. If all the orbits of g on the geometric cusps have length r, then the coefficients of the g-invariant divisor C' are constant on these orbits, so $r \mid \deg C'$. □

2.5. **The Hecke sieve and push-forwards.** Let $X = X_1(m,n)$ with $J(\mathbb{Q}(\zeta_m))$ finite, let $\mathfrak{p}$ be a prime of $\mathbb{Q}(\zeta_m)$ above a prime $p \nmid n$, with residue field $k = \mathbb{F}_{p^f}$, and let D be the trace divisor of a point $x \in Y_1(m,n)(K)$, where $[K : \mathbb{Q}] = 10$. Reducing modulo $\mathfrak{p}$ we write

$$D_k = D' + C',$$

where D' is effective of degree e with non-cuspidal support and C' is effective and cuspidal of degree $d_m - e$. Note that $e \geq 1$ if and only if the elliptic curve corresponding to x has good reduction at some prime of K above $\mathfrak{p}$. As in [Naj26a, §6] and [Naj26d, Section 6.1] we call the multiset of degrees of the closed points occurring in D', a partition of e, the *type* of the decomposition, and write it in brackets, as in $[3,3]$.

The Hecke sieve [DN25, Proposition 5.5] says that if $[A_q(D')] \neq 0$ and $A_q(C') = 0$ for some prime $q \nmid 2pn$ with $q \equiv 1 \pmod m$, then this decomposition cannot occur, since $[A_q(D)] = 0$ by Proposition 2.2 d) and its reduction is $[A_q(D')] + [A_q(C')]$. By Lemma 2.3, $A_q(C') = 0$ if σ_q fixes every closed cusp occurring in C', and we then call q *admissible* for C'. Every prime $q \equiv p^{fj} \pmod n$, for some $j \geq 0$, is admissible for every C', and every q is admissible for C' if each closed cusp occurring in C' is the reduction of a $\mathbb{Q}(\zeta_m)$-rational cuspidal divisor of the same degree. As A_q commutes with the diamond operators, and more generally with the level automorphisms defined over $\mathbb{Q}(\zeta_m)$, it suffices to test one D' in each orbit of these automorphisms.

Lemma 2.16 ([Naj26d, Lemma 5.6])**.** *Let X be a curve over a number field F with an F-rational cusp c_*, let $\mathfrak{p}$ be a prime of good reduction of X with residue field k, and let $G \subseteq J(k)$ be a subgroup containing the reduction of $J(F)$. Let $D \in X^{(d)}(F)$, and write its reduction modulo $\mathfrak{p}$ as $D' + C'$, where D' is effective of degree e with non-cuspidal support and C' is effective and cuspidal. Then*

$$[D' + C' - d\,\overline{c_*}] \in G.$$

We apply Lemma 2.16 on X itself or after pushing the trace divisor forward to another curve, as in [Naj26d, Section 6.1]. Let $m \leq 2$, let $\pi : X \to Y$ be a morphism of modular curves over $\mathbb{Q}$ which maps cusps to cusps and non-cusps to non-cusps, let p be a prime of good reduction of both curves such that π extends over $\mathbb{Z}_{(p)}$, and let y_0 be a rational cusp of Y. Assume that $J_Y(\mathbb{Q})$ is finite, and let $G \subseteq J_Y(\mathbb{F}_p)$ be a subgroup containing the reduction of $J_Y(\mathbb{Q})$. If the reduction of D is $D' + C'$ as above, with $\deg D' = e$, then Lemma 2.16, applied to $\pi_* D$, gives

$$[\pi_* D' - e\,\overline{y_0}] \in G + \mathcal{S}_{10-e}, \tag{2.1}$$

where $\mathcal{S}_j$ is the set of the classes $[j\overline{y_0} - B]$ for the effective cuspidal divisors B of degree j on $Y_{\mathbb{F}_p}$. Note that we allow all the cuspidal divisors B over $\mathbb{F}_p$, also those that are not reductions of rational cuspidal divisors. If every closed cusp of $Y_{\mathbb{F}_p}$ is the reduction of a rational cuspidal divisor of the same degree, then $\mathcal{S}_j \subseteq G$, and (2.1) reduces to $[\pi_* D' - e\,\overline{y_0}] \in G$.

2.6. **Formal immersion at the prime 2.** Reduction modulo 2 need not be injective on the torsion of the Jacobian. The following lemma shows that a suitable Hecke operator kills the torsion points in the kernel of reduction.

Lemma 2.17 ([Naj26d, Lemma 7.1])**.** *Let A be an abelian scheme over $\mathbb{Z}_2$, and let T and δ be endomorphisms of A such that $T = F + \delta V$ on the special fibre $A_{\mathbb{F}_2}$, where F and V are the Frobenius and the Verschiebung of $A_{\mathbb{F}_2}$. If $z \in A(\mathbb{Q}_2)$ satisfies $2z = 0$ and reduces to 0 modulo 2, then $(T - \delta)z = 0$.*

Let n be odd, let $H \subseteq \Delta(n)$ be a subgroup, and put $Y = X_1(n)/H$. We assume that H has odd order, or that H acts freely on the geometric points of $X_1(n)$ in characteristic 2, cusps included. In both cases Y is the generic fibre of a smooth proper curve over $\mathbb{Z}_{(2)}$, the quotient of the smooth model of $X_1(n)$, and its cuspidal subscheme is finite étale over $\mathbb{Z}_{(2)}$. We write $\mathcal{C}$ for the Cartier operator on the differentials of $Y_{\mathbb{F}_2}$, and $\mathbb{T}_Y$ for the ring of endomorphisms of J_Y generated by the Hecke operators T_ℓ for primes $\ell \nmid n$, the operators U_ℓ for primes $\ell \mid n$, and the diamond operators. For $\psi \in \mathbb{T}_Y$ we write ψ^* for its action on the cotangent space $H^0(Y_{\mathbb{F}_2}, \Omega^1)$ of the special fibre of the Néron model of J_Y over $\mathbb{Z}_2$. By the Eichler-Shimura relation we have $(T_2 - \langle 2\rangle)^* = (\mathcal{C} - 1)\langle 2\rangle^*$ on $H^0(Y_{\mathbb{F}_2}, \Omega^1)$ (see [Naj26d, Section 7]).

Proposition 2.18 ([Naj26d, Proposition 7.3])**.** *Let $Y = X_1(n)/H$ be as above, let $\psi_1, \dots, \psi_r \in \mathbb{T}_Y$ be such that each $\psi_i\big(J_Y(\mathbb{Q})\big)$ is finite, and put*

$$U := (\mathcal{C} - 1)\Big(\sum_{i=1}^{r} \psi_i^* H^0(Y_{\mathbb{F}_2}, \Omega^1)\Big).$$

Let $\overline{C}$ be an effective cuspidal divisor of degree d on $Y_{\mathbb{F}_2}$ such that the restriction map $U \to H^0(\overline{C}, \Omega^1|_{\overline{C}})$ is surjective, i.e. such that $\dim U - \dim\big(U \cap \Omega(\overline{C})\big) = d$. Then no effective rational divisor of degree d on Y with non-cuspidal support reduces to $\overline{C}$ modulo 2.

When $J_Y(\mathbb{Q})$ is finite we take $r = 1$ and $\psi_1 = 1$, and then $U = (\mathcal{C} - 1)H^0(Y_{\mathbb{F}_2}, \Omega^1)$.

3. The groups that occur

Let $\mathcal{G}_{10}$ be the set of the 69 groups listed in Theorem 1.1. In this section we show that 65 of them are torsion groups of elliptic curves over number fields of degree 10: 38 of them already occur in degree 1, 2 or 5 (Section 3.1), 15 occur because the corresponding modular curve has a function of the right degree (Section 3.2), and for the remaining 12 we give explicit elliptic curves (Section 3.3). The remaining 4 groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ are realized in Section 11, where we also determine all the elliptic curves with these torsion groups. In Section 3.2 we also show that 3 of the groups that occur in degree 5, namely $\mathbb{Z}/28\mathbb{Z}$, $\mathbb{Z}/30\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$, occur for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves over number fields of degree 10, which we need in Section 13.

3.1. **Groups from smaller degrees.** The following lemma is well known. We give the proof, which uses the same trick as [Naj26c, Lemma 3.1].

Lemma 3.1. *Let F be a number field of degree e, let E/F be an elliptic curve and let d be a multiple of e. Then there is a number field $K \supseteq F$ of degree d such that $E(K)_{\mathrm{tors}} = E(F)_{\mathrm{tors}}$. In particular, $\Phi(e) \subseteq \Phi(d)$.*

Proof. By Merel's theorem [Mer96] there are only finitely many points $P \in E(\overline{F})_{\mathrm{tors}}$ with $[F(P) : F] \leq d/e$. Let M be the Galois closure over F of the compositum of the fields $F(P)$ for these points P, let ℓ be a rational prime which is unramified in M, and let α be a root of $x^{d/e} - \ell$. This polynomial is Eisenstein at every prime of F above ℓ, so $K = F(\alpha)$ has degree d/e over F, and every prime of F above ℓ is totally ramified in K. If $P \in E(K)_{\mathrm{tors}}$, then $F(P) \subseteq K \cap M$, and $K \cap M$ is an extension of F which is both unramified and totally ramified at the primes above ℓ. Hence $K \cap M = F$ and $P \in E(F)$. □

By Mazur's theorem [Maz77], the theorem of Kamienny [Kam92] and Kenku and Momose [KM88], and [Naj26a, Theorem 1.1], the sets $\Phi(1)$, $\Phi(2)$ and $\Phi(5)$ consist of the groups

$$\begin{aligned}
&\Phi(1): \mathbb{Z}/n\mathbb{Z},\ n = 1, \dots, 10, 12, && \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 1, \dots, 4,\\
&\Phi(2): \mathbb{Z}/n\mathbb{Z},\ n = 1, \dots, 16, 18, && \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 1, \dots, 6,\\
&\qquad \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, &&\\
&\Phi(5): \mathbb{Z}/n\mathbb{Z},\ n = 1, \dots, 22, 24, 25, 28, 30, && \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 1, \dots, 9.
\end{aligned}$$

By Lemma 3.1 all these groups lie in $\Phi(10)$. There are 38 of them: the groups $\mathbb{Z}/n\mathbb{Z}$ for $1 \leq n \leq 25$, $n \neq 23$, and $n \in \{28, 30\}$, the groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ for $1 \leq n \leq 9$, and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

3.2. **Groups from functions on modular curves.**

Lemma 3.2. *Let $m \in \{1, 2, 3, 4, 6\}$, let $m \mid n$ with $n \geq 5$, put $F = \mathbb{Q}(\zeta_m)$, and suppose that $X_1(m, n)$ has a function of degree $d_m = 10/\varphi(m)$ over F. Then there are infinitely many pairs (K, E), consisting of a number field K of degree 10 and an elliptic curve E/K with $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, such that the j-invariants $j(E)$ are pairwise distinct.*

Proof. This is [DS17, Lemma 5.1]. The idea is to apply Hilbert's irreducibility theorem to f and to its compositions with the forgetful maps from the modular curves with larger level structures, which have degree at least 2, so that for infinitely many fibres of f the elliptic curve gains no further torsion over the residue field. □

We use the following model of $X_1(m, n)$, as in Derickx's package `mdsage` [mds]. Let $H \subseteq (\mathbb{Z}/mn\mathbb{Z})^\times$ be the subgroup generated by -1 and by $1 + kn$ for $1 \leq k < m$. The map $X_1(mn) \to X_1(m, n)$, $(E, P) \mapsto \big(E/\langle nP\rangle,\ R \bmod \langle nP\rangle,\ P \bmod \langle nP\rangle\big)$, where $R \in E[m]$ is a point whose Weil pairing with nP is ζ_m, induces an isomorphism over $F = \mathbb{Q}(\zeta_m)$ between the modular curve $X_H(mn)$ of the group $\Gamma_H(mn)$ and $X_1(m, n)$. The curve $X_H(mn)$ is defined over $\mathbb{Q}$, so a rational function of degree d on $X_H(mn)$ gives a function of degree d on $X_1(m, n)$ over F. For $m = 1$ we have $X_H(n) = X_1(n)$.

Proposition 3.3. *Let (m, n) be one of the following pairs:*

$$(1, n) \text{ for } n \in \{23, 26, 27, 28, 30, 32, 33, 34, 36\}, \qquad (2, n) \text{ for } n \in \{18, 20, 22, 24\},$$
$$(3, 9), \quad (3, 12), \quad (4, 8), \quad (4, 12), \quad (6, 6).$$

Then $X_1(m,n)$ has a function of degree d_m over $\mathbb{Q}(\zeta_m)$. Hence each of the 18 groups $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ is the torsion group of infinitely many elliptic curves over number fields of degree 10, with pairwise distinct j-invariants.

Proof. We look for a modular unit of degree d_m, that is, a function on $X_H(mn)$ over $\mathbb{Q}$ whose divisor is supported on the cusps. A divisor of degree 0 supported on the cusps is the divisor of a function over $\overline{\mathbb{Q}}$ if and only if its image under the Abel-Jacobi map, computed with modular symbols, is 0, and if it is moreover invariant under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then by Hilbert's theorem 90 it is the divisor of a function defined over $\mathbb{Q}$. Using the function `has_modular_unit_of_degree` of Derickx's package `mdsage` [mds] we find, for each of the 18 pairs, a Galois-invariant divisor of degree 0 supported on the cusps of $X_H(mn)$ which lies in the lattice of divisors of rational modular units and whose positive part has degree d_m (see `occurrences` for the divisors and the lattices, and the scripts `computations/unit_m_n.py`; for the pairs $(1,28)$, $(1,30)$ and $(2,18)$ see the script `phi_infinity/work/unit_degree10.py` and the files `phi_infinity/outputs/unit_m_n_degree10.json`). The last statement follows from Lemma 3.2. □

3.3. **Explicit curves.** Recall that for b, c in a field, the curve

$$E(b,c): \quad y^2+(1-c)xy-by=x^3-bx^2 \tag{3.1}$$

in Tate normal form has the point $(0,0)$, which is a point of order N exactly when (b,c) comes from a point of $Y_1(N)$. As in [Naj26d, Section 13.1], for a point (x,y) on the model of $X_1(N)$ of van Hoeij [vH14] we put

$$r=\frac{x^2y-xy+y-1}{x^2y-x}, \qquad s=\frac{xy-y+1}{xy}, \qquad b=rs(r-1), \qquad c=s(r-1),$$

and denote by $E(b,c)$ the curve (3.1), on which $(0,0)$ has order N.

Proposition 3.4. *Let N, f and g be one of the following, let x be a root of f, let y be determined by $g(x,y)=0$, and put $K=\mathbb{Q}(x)$ and $E=E(b,c)$.*

N	f *and* g
29	$x^{10}-3x^9+8x^7-5x^6-6x^5+5x^4-2x^2+1$
	$29y-2x^9-x^8+11x^7+8x^6-49x^5+77x^3-35x^2-46x+13$
31	$x^{10}-4x^9+3x^8+6x^7-2x^6-8x^5-8x^4+11x^3+6x^2-5x+1$
	$215y-109x^9+266x^8+207x^7-801x^6-606x^5+304x^4+1470x^3$ $+410x^2-1000x-71$
35	$x^{10}+2x^8+x^7-9x^6-6x^5+7x^4+8x^3-x^2-3x-1$
	$191y-39x^9+192x^8-127x^7+454x^6+452x^5-1286x^4-862x^3+479x^2+443x-7$
37	$x^{10}-5x^8+3x^7+10x^6-8x^5-7x^4+9x^3-3x+1$
	$y-2x^9-x^8+10x^7-x^6-23x^5+6x^4+22x^3-11x^2-9x+5$
38	$x^{10}+3x^9+x^8-6x^7-9x^6-x^5+8x^4+7x^3-2x-1$
	$y-2x^9-5x^8+10x^6+11x^5-2x^4-10x^3-5x^2+x$
39	$x^{10}+2x^8+14x^7-6x^6-20x^5+4x^4+7x^3-2x^2+1$
	$449y-748x^9-643x^8-2185x^7-12166x^6-6406x^5+8021x^4+6917x^3$ $+192x^2-243x+889$
40	$x^{10}-7x^8-5x^7+17x^6+x^5-11x^4+x^3+x^2+2x-1$
	$137y-712x^9-515x^8+4624x^7+6920x^6-7151x^5-6022x^4+3395x^3$ $+1608x^2+565x-912$
42	$x^{10}-5x^9+4x^8+14x^7-24x^6+6x^5+5x^4-6x^3+8x^2-5x+1$
	$3y-16x^9+68x^8-12x^7-237x^6+206x^5+74x^4-35x^3+61x^2-80x+16$
45	$x^{10}-5x^9+11x^8-14x^7+6x^6+10x^5-12x^4+x^3-x^2+3x-1$
	$135y-19x^9+123x^8-335x^7+496x^6-331x^5-243x^4+609x^3-217x^2-157x-158$
50	$x^{10}-2x^9+x^8+7x^6-10x^5+4x^4-2x^3+5x^2-4x+1$
	$49y+255x^9-435x^8+104x^7+45x^6+1804x^5-2005x^4+266x^3$ $-426x^2+1118x-622$

Then $[K:\mathbb{Q}]=10$ and $E(K)_{\mathrm{tors}}\simeq\mathbb{Z}/N\mathbb{Z}$. The fields K are listed in Table 1.

Proof. These points are taken from the lists of van Hoeij [vH14], and they are also listed in [Naj26b]. For each of them we compute that f is irreducible and that $(0,0)$ has order N on E, and we find a prime p and a prime $\wp$ of K above p of residue degree 1, unramified in K, at which E has good reduction and $\#\widetilde{E}(\mathbb{F}_p)=N$ (Table 1). As p is odd and $\wp$ is unramified, $E(K)_{\mathrm{tors}}$ injects into $\widetilde{E}(\mathbb{F}_p)$, so $E(K)_{\mathrm{tors}}\simeq\mathbb{Z}/N\mathbb{Z}$. The computation is done with the model $E(b,c)$ written in terms of another generator of K, given in the scripts `computations/witness_CN.m`, and we check that, after an isomorphism of the fields, it is isomorphic to the curve defined by van Hoeij's coordinates. □

The groups $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/28\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/30\mathbb{Z}$ are obtained from the quintic sporadic points of [Naj26a].

Proposition 3.5. *Let (F,E) be the pair with $E(F)_{\mathrm{tors}}\simeq\mathbb{Z}/28\mathbb{Z}$, respectively the first pair with $E(F)_{\mathrm{tors}}\simeq\mathbb{Z}/30\mathbb{Z}$, of* [Naj26a, Theorem 1.2]*, so that $F=\mathbb{Q}(\alpha)$ with $\alpha^5-\alpha^4-2\alpha^3-$*

N	K	p	$\#\widetilde{E}(\mathbb{F}_p)$	point in [Naj26b]
29	10.2.917035997.1	31	29	1.29.10.b
31	10.0.224415603.1	43	31	1.31.10.a
35	10.2.809040437.1	29	35	1.35.10.b
37	10.2.803282693.1	29	37	1.37.10.a
38	10.2.801214577.1	29	38	1.38.10.a
39	10.4.3393524187.1	31	39	1.39.10.a
40	10.2.2022480784.1	31	40	1.40.10.a
42	10.4.11125027323.1	37	42	1.42.10.b
45	10.2.2630071125.1	37	45	1.45.10.a
50	10.0.400000000.1	37	50	1.50.10.a

TABLE 1. The fields of the elliptic curves of Proposition 3.4, a prime of good reduction of residue degree 1 which bounds the torsion, and the label of the point in [Naj26b].

$\alpha^2+2\alpha+2=0$, *respectively* $\alpha^5+\alpha^4-3\alpha^3+3\alpha+1=0$, *and* $E=E(b,c)$ *with*

$$b=419\alpha^4-759\alpha^3-222\alpha^2-239\alpha+1032,$$
$$c=17\alpha^4-31\alpha^3-8\alpha^2-11\alpha+42,$$

respectively

$$b=-6378\alpha^4-1917\alpha^3+20475\alpha^2-14321\alpha-9118,$$
$$c=-114\alpha^4-34\alpha^3+366\alpha^2-257\alpha-162.$$

The 2-division polynomial of E has exactly one irreducible factor h of degree 2 over F. Let $K=F(\beta)$, where $h(\beta)=0$. Then $[K:\mathbb{Q}]=10$ and $E(K)_{\mathrm{tors}}\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/28\mathbb{Z}$, respectively $E(K)_{\mathrm{tors}}\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/30\mathbb{Z}$. The field K is 10.2.9630499328.1, respectively 10.2.3574086417.1, and the points of $X_1(2,28)$ and $X_1(2,30)$ given by E are 2.28.10.a, respectively 2.30.10.a, in [Naj26b].

Proof. Over K all the points of order 2 of E are rational, and $(0,0)$ has order 28, respectively 30, so $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/28\mathbb{Z}$, respectively $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/30\mathbb{Z}$, is a subgroup of $E(K)$. We find a prime of K of residue degree 1 above 43, unramified in K, at which E has good reduction with 56 points, and similarly a prime above 53 with 60 points in the second case. This proves the claim. □

The same holds for the second curve with torsion $\mathbb{Z}/30\mathbb{Z}$ in [Naj26a, Theorem 1.2], which is 2-isogenous to the first one over F (see `computations/quintic_full2_30b_v2.m`), over the field of the point 2.30.10.b of [Naj26b].

4. The groups that have to be considered

Every finite subgroup of $E(K)$ is isomorphic to $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ with $m\mid n$. The set $\mathcal{G}_{10}$ of the 69 groups of Theorem 1.1 is closed under passing to subgroups, and by Sections 3 and 11 it is contained in $\Phi(10)$. Recall that $S(10)$ is the set of primes up to 37 [Naj26c, Theorem 1.1].

Lemma 4.1. *Let $\mathcal{M}_{10}$ be the set of groups $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with $m \mid n$ such that $\varphi(m) \mid 10$, every prime dividing n lies in $S(10)$, $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \notin \mathcal{G}_{10}$, and every proper subgroup of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ lies in $\mathcal{G}_{10}$. Then $\mathcal{M}_{10}$ consists of the following 110 groups:*

$\mathbb{Z}/n\mathbb{Z}$ *for* $n \in \{44, 46, 48, 49, 51, 52, 54, 55, 56, 57, 58, 60, 62, 63, 64, 65, 66, 68, 69, 70, 72, 74, 75, 76, 77, 78, 80, 81, 84, 85, 87, 90, 91, 93, 95, 99, 100, 105, 111, 115, 117, 119, 121, 125, 133, 135, 143, 145, 155, 161, 169, 175, 185, 187, 203, 209, 217, 221, 247, 253, 259, 289, 299, 319, 323, 341, 361, 377, 391, 403, 407, 437, 481, 493, 527, 529, 551, 589, 629, 667, 703, 713, 841, 851, 899, 961, 1073, 1147, 1369\}$,

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ *for* $n \in \{16, 17, 18, 19, 20, 21, 25\}$,

$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z}$ *for* $n \in \{7, 8, 9, 10, 11, 12, 13, 15\}$,

$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4n\mathbb{Z}$ *for* $n \in \{4, 5, 6, 7\}$,

$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$, $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$.

Every group in $\Phi(10) \setminus \mathcal{G}_{10}$ contains a member of $\mathcal{M}_{10}$.

Proof. By the Weil pairing and by [Naj26c, Theorem 1.1], every group in $\Phi(10)$ is of the form $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with $\varphi(m) \mid 10$, that is, $m \in \{1, 2, 3, 4, 6, 11, 22\}$, and with all the primes dividing n in $S(10)$. As $\mathcal{G}_{10}$ is closed under passing to subgroups, a group in $\Phi(10) \setminus \mathcal{G}_{10}$ contains a subgroup of minimal order which is not in $\mathcal{G}_{10}$, and this subgroup lies in $\mathcal{M}_{10}$. If $\mathbb{Z}/n\mathbb{Z} \in \mathcal{M}_{10}$, then $\mathbb{Z}/(n/p)\mathbb{Z} \in \mathcal{G}_{10}$ for every prime $p \mid n$, so $n \leq 37 \cdot 50$, and if $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \in \mathcal{M}_{10}$ with $m > 1$, then $\mathbb{Z}/n\mathbb{Z} \in \mathcal{G}_{10}$, so $n \leq 50$. It remains to run through these finitely many groups, which we do by computer. □

Note that $\mathbb{Z}/22\mathbb{Z} \times \mathbb{Z}/22\mathbb{Z}$ does not occur in $\mathcal{M}_{10}$, as it contains $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$.

Remark 4.2. Let $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \in \mathcal{M}_{10}$ with $m \leq 2$, and suppose that n is divisible by a prime $p \geq 23$. As $S(1) \cup S(2) \cup S(5)$ consists of the primes up to 19 [Maz77, Kam92, DKSS23], a point $x \in Y_1(m, n)$ defined over a number field of degree 10 has $[\mathbb{Q}(x) : \mathbb{Q}] = 10$, so its trace divisor is a closed point of degree 10.

To rule out a group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \in \mathcal{M}_{10}$ we show that no effective $\mathbb{Q}(\zeta_m)$-rational divisor of degree d_m on $X_1(m, n)$ with non-cuspidal support is the trace divisor (Section 2.2) of a point $x \in Y_1(m, n)(K)$ with $[K : \mathbb{Q}] = 10$.

Several members of $\mathcal{M}_{10}$ are reduced to others by an isogeny.

Lemma 4.3. *Let $m \mid n$, let K be a number field containing μ_m, and let E/K be an elliptic curve with a point of order mn over K. Then there is an elliptic curve E' over K, isogenous to E over K, with $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \subseteq E'(K)$. In particular, if $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}$ is not a subgroup of the torsion of any elliptic curve over a number field K, then neither is $\mathbb{Z}/4k\mathbb{Z}$.*

Proof. Let $P \in E(K)$ have order mn, and let $\phi : E \to E' = E/\langle nP \rangle$, which is defined over K. The kernel of the dual isogeny $\widehat{\phi}$ is $\phi(E[m])$, which is cyclic of order m and, by the Weil pairing, isomorphic to μ_m as a Galois module, as $\langle nP \rangle \simeq \mathbb{Z}/m\mathbb{Z}$. As $\mu_m \subseteq K$, all the points of $\ker \widehat{\phi}$ are defined over K. The point $Q = \phi(P) \in E'(K)$ has order n, and $\widehat{\phi}(Q) = mP$ also has order n, so $\langle Q \rangle \cap \ker \widehat{\phi} = 0$. Hence $\ker \widehat{\phi} + \langle Q \rangle \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is a subgroup of $E'(K)$. For the last statement take $m = 2$ and $n = 2k$. □

By Lemma 4.3, the exclusion of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}$ for $2k \in \{32, 34, 36, 38, 40, 42, 50\}$ in Section 7 also excludes $\mathbb{Z}/4k\mathbb{Z}$ for $4k \in \{64, 68, 72, 76, 80, 84, 100\}$. It does not apply to $\mathbb{Z}/52\mathbb{Z}$, as $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$ lies in $\Phi(10)$, and we treat this group in Proposition 11.25. Section 12 lists where each of the groups in $\mathcal{M}_{10}$ is excluded.

5. The global method and diamond operators

Most of the groups $\mathbb{Z}/n\mathbb{Z}$ with large n are excluded by the global method of Derickx [DN25, Proposition 4.3], which we recall in Section 5.1. With $q = 3$ it excludes the 45 groups $\mathbb{Z}/n\mathbb{Z}$ of Table 2 (Proposition 5.3), and with $q = 2$ the groups $\mathbb{Z}/115\mathbb{Z}$, $\mathbb{Z}/121\mathbb{Z}$ and $\mathbb{Z}/135\mathbb{Z}$ (Section 5.2). For $n = 155$ the global method only shows that the trace divisor is invariant under a diamond operator whose order divides 10, and we conclude by descending the point to a quadratic field (Section 5.3). Finally, the groups $\mathbb{Z}/95\mathbb{Z}$ and $\mathbb{Z}/111\mathbb{Z}$ are excluded in Section 5.4 with a diamond operator of order 3, using that all the reductions modulo the primes above 2 are bad.

We use the following consequence of Kato's theorem, as in [Naj26d, Section 4]. The isogeny decomposition

$$J_1(n) \sim \bigoplus_{n'|n} \bigoplus_{[f]} A_{[f]}^{\sigma_0(n/n')},$$

where the inner sum is over the Galois orbits of newforms of weight 2 and level n', is equivariant for the diamond operators, $\langle a\rangle$ acting on $A_{[f]}$ through $\chi_f(a)$, where χ_f is the nebentypus of f, and $A_{[f]}(\mathbb{Q})$ is finite if $L(f,1) \neq 0$ by Kato's theorem [Kat04, Corollary 14.3]. Hence the group $(\langle a\rangle - 1)J_1(n)(\mathbb{Q})$ is finite if $\chi_f(a) = 1$ for every newform f of weight 2 and level dividing n with $L(f,1) = 0$. We obtain this condition either from the LMFDB [LMF26], where all the analytic ranks that we use are recorded as proved, or from the winding quotient (Section 2.3). For a Galois orbit of even Dirichlet characters χ modulo n we write S_χ for the plus quotient of the space of cuspidal modular symbols of weight 2 and character χ, and W_χ for its winding submodule, the Hecke module generated by the projection of the winding element. If $W_\chi = S_\chi$, then $L(f,1) \neq 0$ for every newform f of level dividing n whose character lies in the orbit of χ. Whenever we compute W_χ for all the orbits, we check that no orbit is missed by verifying that the sum of $\varphi(\operatorname{ord}\chi)\dim S_\chi$ over all of them is the genus of $X_1(n)$. For characters of large order we first check, as in the proof of [Naj26d, Lemma 4.1], whether the vectors $v, vT_2, \dots, vT_2^{k-1}$, where v is the projection of the winding element and $k = \dim S_\chi$, are linearly independent modulo a prime of degree 1 of the field of values of χ at which all the denominators are units. If they are, then $W_\chi = S_\chi$, and if not, we compute W_χ over the field of values of χ.

5.1. The global method.

The main tool is the global method of Derickx [DN25, Proposition 4.3], which we recall for number fields of degree 10, as in [Naj26a, Section 4] and [Naj26d, Section 4.1].

Proposition 5.1 (Derickx [DN25, Proposition 4.3])**.** *Let $n \geq 5$ be an integer, let $q \nmid n$ be a prime and let $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ be such that $(\langle a\rangle - 1)J_1(n)(\mathbb{Q})$ is finite. If $q = 2$, assume also that n is odd and that $(\langle a\rangle - 1)J_1(n)(\mathbb{Q})$ has odd order. Put $k_q = 2q + 1$ if $a \equiv \pm q^{\pm 1} \pmod n$, and $k_q = 2(q+1)$ if not. If $10k_q < \operatorname{gon}_{\mathbb{Q}} X_1(n)$, then every effective $\mathbb{Q}$-rational divisor D of degree 10 on $X_1(n)$ whose support contains no cusp satisfies $\langle a\rangle D = D$. The inequality $10k_q < \operatorname{gon}_{\mathbb{Q}} X_1(n)$ holds as soon as*

$$b(n) := \frac{325}{2^{15}} \cdot \frac{i(n)}{k_q} > 10.$$

Proof. For odd q this is [DN25, Proposition 4.3] with $H = \{\pm 1\}$ and $d = 10$. Its proof applies A_q, which kills the torsion of $J_1(n)(\mathbb{Q})$ and the rational cuspidal divisors by Proposition 2.2 b) and c), to the class of $(\langle a\rangle - 1)(D - 10c_0)$, and $10k_q$ bounds the degree of the

positive part of the resulting principal divisor. For $q = 2$ the proof applies without change, by Lemma 2.3, which allows $q = 2$ as n is odd, and as reduction modulo 2 is injective on the torsion of odd order by Parent's result (Section 2.3). The last statement follows from Abramovich's bound (Section 2.3), as $\operatorname{gon}_{\mathbb{Q}} X_1(n) \geq \operatorname{gon}_{\mathbb{C}} X_1(n) \geq \frac{325}{2^{15}} i(n)$. □

We apply Proposition 5.1 to the trace divisor D of a point of order n over a number field of degree 10 (Section 2.2). By Lemma 2.14 the support of D consists of non-CM points, so if $\langle a \rangle D = D$, then by Lemma 2.9 the order of $\langle a \rangle$ in $\Delta(n)$ divides 10. For the 32 levels of Table 2 that also occur in [Naj26d, Table 1] we use the same elements a as there. For $n = 119$ the inequality $b(119) > 10$ fails with $k_3 = 7$, and we use instead that $J_1(119)(\mathbb{Q})$ is finite (see the proof of Proposition 5.3). The other 11 levels, all of them except 175 divisible by 37, are listed in Table 3.

We check the entries of Table 2 for the levels of Table 3. For the other levels the entries are those of [Naj26d, Table 1], apart from k_3 and $b(n)$ for $n = 119$. They are recorded in `exclusions/global3.json` and `exclusions/global3_additional.json`, where for $n = 133$ and $n = 247$ the elements $a = 27$ and $a = 12$ are used instead, which generate the same subgroups of order 3 of $\Delta(n)$ as 64 and 144.

Lemma 5.2. *Let n and a be as in one of the rows of Table 2. Then $(\langle a \rangle - 1)J_1(n)(\mathbb{Q})$ is finite. The group $J_1(119)(\mathbb{Q})$ is also finite.*

Proof. An LMFDB search shows that every newform of weight 2 and level dividing 119 has analytic rank 0 (see `inputs/global_newforms_cache.json`), so $J_1(119)(\mathbb{Q})$ is finite by Kato's theorem.

For the other 31 levels of Table 2 that occur in [Naj26d, Table 1] with the same element a, the finiteness of $(\langle a \rangle - 1)J_1(n)(\mathbb{Q})$ is shown in the proof of [Naj26d, Proposition 4.2], in a part of that proof which does not depend on the degree. For $n = 341$ and $n = 403$, where [Naj26d, Table 1] uses elements of order 2, the computation of the winding submodules for the proof of [Naj26d, Proposition 4.2] (`inputs/global_archive/winding_probe_minimal.m`, with the logs `inputs/global_archive/winding341.log` and `inputs/global_archive/winding403.log`) shows that $W_\chi = S_\chi$ unless χ has order 1 or 5, respectively order 1, 3, 5 or 15, and it lists the elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ on which all these characters are trivial, among them 56 and 118.

For the 11 levels of Table 3 we compute W_χ for every Galois orbit of even characters χ modulo n, with the scripts linked in Table 3 (for $n = 1147$ the computation is split between `computations/winding1147.m` and `computations/winding1147_resume.m`). In every case the sum of $\varphi(\operatorname{ord}\chi)\dim S_\chi$ is the genus of $X_1(n)$, and $W_\chi = S_\chi$ unless the order of χ is one of those listed in Table 3, and the same scripts check that the element a of Table 2 lies in the kernel of these characters. (For $n = 185$ only one of the two Galois orbits of even characters of order 4, both of conductor 185, has $W_\chi \neq S_\chi$, and it is trivial on 2.) Hence $(\langle a \rangle - 1)J_1(n)(\mathbb{Q})$ is finite. □

Proposition 5.3. *Let n be one of the 45 levels of Table 2. Then the group $\mathbb{Z}/n\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let D be the trace divisor of a point of order n over a number field of degree 10. By Lemma 2.14 the support of D consists of non-CM points.

Suppose first that $n = 119$. As $J_1(119)(\mathbb{Q})$ is finite by Lemma 5.2, the divisor $A_3 D$ is principal by Proposition 2.2 d). Its positive part is contained in $T_3 D$, which has degree 40,

n	a	$\mathrm{ord}\langle a\rangle$	k_3	$i(n)$	$b(n)$
119	–	–	4	6912	17.13
125	3	50	7	7500	10.62
133	64	3	8	8640	10.71
143	67	12	8	10080	12.49
145	3	14	7	10080	14.28
161	3	66	7	12672	17.95
169	3	39	7	14196	20.11
175	18	12	8	14400	17.85
185	2	18	8	16416	20.35
187	122	16	8	17280	21.42
203	6	7	8	20160	24.99
209	34	18	8	21600	26.77
217	3	15	7	23040	32.64
221	3	48	7	24192	34.27
247	144	3	8	30240	37.49
253	3	55	7	31680	44.88
259	3	9	7	32832	46.51
289	3	136	7	41616	58.96
299	3	33	7	44352	62.84
319	3	140	7	50400	71.41
323	101	18	8	51840	64.27
341	56	3	8	57600	71.41
361	3	171	7	64980	92.06
377	5	28	8	70560	87.47
391	3	176	7	76032	107.72
403	118	3	8	80640	99.97
407	10	6	8	82080	101.76
437	3	198	7	95040	134.66
481	3	18	7	114912	162.81
493	3	112	7	120960	171.38
527	3	240	7	138240	195.87
529	3	253	7	139656	197.87
551	12	12	8	151200	187.45
589	3	45	7	172800	244.83
629	6	16	8	196992	244.22
667	3	308	7	221760	314.20
703	3	9	7	246240	348.89
713	2	55	8	253440	314.20
841	12	58	8	353220	437.91
851	3	198	7	361152	511.71
899	3	420	7	403200	571.28
961	3	465	7	461280	653.58
1073	3	252	7	574560	814.08
1147	3	45	7	656640	930.38
1369	6	74	8	936396	1160.92

TABLE 2. The levels n of Proposition 5.3, with $q = 3$. The order of $\langle a\rangle$ is its order in $\Delta(n)$, and $b(n)$ is rounded down to two decimal places. For $n = 119$ the group $J_1(119)(\mathbb{Q})$ is finite, and the column k_3 gives the degree 4 of T_3 instead (see the proof of Proposition 5.3).

n	$g(X_1(n))$	orders of the χ with $W_\chi \neq S_\chi$
175	1033	1, 5
185	1225	1, 4
259	2521	1
407	6481	1, 6
481	9145	1
629	15841	1, 9
703	19873	1
851	29305	1
1073	46873	1
1147	53641	1
1369	77044	1, 3, 9

TABLE 3. The 11 levels of Table 2 that do not occur in [Naj26d, Table 1], the genus of $X_1(n)$, and the orders of the even characters χ modulo n whose winding submodule is not the whole space. Each level is a link to the script that computes the winding submodules.

and $\operatorname{gon}_{\mathbb{Q}} X_1(119) \geq \frac{325}{2^{15}} \cdot 6912 > 68$ by Abramovich's bound, so $A_3 D = 0$. This contradicts Lemma 2.12.

Suppose now that $n \neq 119$, and take $q = 3$ and a as in Table 2. By Lemma 5.2 the hypotheses of Proposition 5.1 are satisfied, and by Table 2 we have $b(n) > 10$, so $\langle a \rangle D = D$. By Lemma 2.9 the order of $\langle a \rangle$ in $\Delta(n)$ divides 10, which contradicts Table 2. □

5.2. **The global method at the prime 2.** For $n = 115$, 121 and 135 we use Proposition 5.1 with $q = 2$. Note that for $n = 115$ this is the argument of [Naj26d, Proposition 4.2] in degree 9, which also works in degree 10. For $n = 121$ the choice $q = 3$ and $a = 2$ gives only $b(121) = 9.0007\ldots$ (see [Naj26d, Table 1]), and 3 divides 135.

Lemma 5.4. *Let (n, a, p) be one of the triples $(115, 16, 3)$, $(121, 2, 3)$ and $(135, 16, 31)$, and let $B_n := (\langle a \rangle - 1)J_1(n)$. Then $B_n(\mathbb{Q})$ is finite and $\#B_n(\mathbb{F}_p)$ is odd. In particular $(\langle a \rangle - 1)J_1(n)(\mathbb{Q})$ is finite of odd order.*

Proof. The abelian variety B_n is isogenous to the product of the parts of $J_1(n)$ with characters χ such that $\chi(a) \neq 1$. These are the characters of order 11, 22 and 44 for $n = 115$, of order 5, 11 and 55 for $n = 121$, and of order 3, 6, 9, 12, 18 and 36 for $n = 135$, and B_n has dimension 400, 520 and 480, respectively.

For $n = 115$ the group $B_n(\mathbb{Q})$ is finite by [Naj26d, Lemma 4.1]. For $n = 121$ the only newform of weight 2 and level dividing 121 with positive analytic rank is 121.2.a.b, which has trivial character (see `inputs/global_newforms_cache.json`). For $n = 135$ we compute that $W_\chi = S_\chi$ for every non-trivial even character χ modulo 135, the sum of $\varphi(\operatorname{ord}\chi)\dim S_\chi$ over all the orbits being $529 = g(X_1(135))$. Hence $B_n(\mathbb{Q})$ is finite in all three cases.

For every Galois orbit of characters χ with $\chi(a) \neq 1$ we compute the norm of $\det\big((1 + p\chi(p)) - T_p\big)$ on S_χ. By the Eichler-Shimura relation it is a power of the number of $\mathbb{F}_p$-points of the part of $J_1(n)$ with characters in the orbit of χ, and we find that all these norms are odd. For $n = 115$ this is the computation in the proof of [Naj26d, Proposition 4.2], and for $n = 121$ and $n = 135$ we compute it with `computations/image121_no2_v2.m`

and computations/cont_image135_a16_no2.m. As the number of points over a finite field is invariant under isogeny, $\#B_n(\mathbb{F}_p)$ is odd. As p is odd and B_n has good reduction at p, reduction modulo p is injective on $B_n(\mathbb{Q})_{\mathrm{tors}}$ by Katz's result, so $B_n(\mathbb{Q})$ has odd order, and so has its subgroup $(\langle a\rangle - 1)J_1(n)(\mathbb{Q})$. □

Proposition 5.5. *The groups $\mathbb{Z}/115\mathbb{Z}$ and $\mathbb{Z}/121\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let $n \in \{115, 121\}$, put $a = 16$ if $n = 115$ and $a = 2$ if $n = 121$, and let D be the trace divisor of a point of order n over a number field of degree 10. By Lemma 5.4 we can apply Proposition 5.1 with $q = 2$. As $16 \not\equiv \pm 2^{\pm 1} \pmod{115}$ we have $k_2 = 6$ for $n = 115$, and $k_2 = 5$ for $n = 121$. As $i(115) = 6336$ and $i(121) = 7260$, we get $b(115) = \frac{10725}{1024} > 10.47$ and $b(121) = \frac{117975}{8192} > 14.40$, so $\langle a\rangle D = D$. By Lemma 2.14 the support of D consists of non-CM points, so by Lemma 2.9 the order of $\langle a\rangle$ in $\Delta(n)$ divides 10. But $\langle 16\rangle$ has order 11 in $\Delta(115)$ and $\langle 2\rangle$ has order 55 in $\Delta(121)$, which is a contradiction. □

Proposition 5.6. *The group $\mathbb{Z}/135\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let D be the trace divisor of a point of order 135 over a number field of degree 10. By Lemma 5.4 we can apply Proposition 5.1 with $q = 2$ and $a = 16$. As $16 \not\equiv \pm 2^{\pm 1} \pmod{135}$ we have $k_2 = 6$, and as $i(135) = 7776$, we get $b(135) = \frac{26325}{2048} > 12.85$, so $\langle 16\rangle D = D$. By Lemma 2.14 the support of D consists of non-CM points, and by Lemma 2.9 the order of $\langle 16\rangle$ in $\Delta(135)$ divides 10. We compute that this order is 9, which is a contradiction. □

5.3. **The group $\mathbb{Z}/155\mathbb{Z}$.** For $n = 155$ we compute that every element a for which $(\langle a\rangle - 1)J_1(155)(\mathbb{Q})$ is known to be finite lies in the subgroup of order 5 of $\Delta(155)$ generated by $\langle 16\rangle$, so the global method only shows that the trace divisor is invariant under $\langle 16\rangle$. We use that a closed point which is mapped to itself by a diamond operator has an image on a modular curve of smaller level which is defined over a smaller field.

Lemma 5.7. *Let $n \geq 5$, let $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, and let r be the order of $\langle a\rangle$ in $\Delta(n)$. Let x be a closed point of $Y_1(n)$ whose geometric points have no complex multiplication, and suppose that $\langle a\rangle$ maps x to itself. Then $\langle a\rangle$ induces an automorphism ϕ of the residue field $\mathbb{Q}(x)$ of x of order r. If $\pi : X_1(n) \to Z$ is a morphism of curves over $\mathbb{Q}$ with $\pi \circ \langle a\rangle = \pi$, then the residue field of $\pi(x)$ is contained in the fixed field $\mathbb{Q}(x)^\phi$, which has degree $[\mathbb{Q}(x) : \mathbb{Q}]/r$.*

Proof. As $\langle a\rangle$ is an automorphism of $X_1(n)$ over $\mathbb{Q}$ which maps the closed point x to itself, it induces an automorphism ϕ of $\mathbb{Q}(x)$, and it acts on the geometric points of x, which correspond to the embeddings $\iota : \mathbb{Q}(x) \to \overline{\mathbb{Q}}$, by $\iota \mapsto \iota \circ \phi$ (or $\iota \mapsto \iota \circ \phi^{-1}$, depending on the convention). If $\phi^k = 1$ for some $0 < k < r$, then $\langle a\rangle^k \neq 1$ fixes the geometric points of x, which contradicts Lemma 2.9. As $\langle a\rangle^r = 1$, the order of ϕ is r. If $\pi \circ \langle a\rangle = \pi$, then the geometric points of $\pi(x)$ given by ι and by $\iota \circ \phi$ coincide for every ι, so ϕ is the identity on the residue field of $\pi(x)$, viewed as a subfield of $\mathbb{Q}(x)$ via π. □

The descent leads to a quadratic point on the curve $Y_{31} := X_1(31)/\langle 2\rangle$, which we exclude with Proposition 2.5 at the prime 2. We first collect the facts that we need about Y_{31} and about the reduction modulo 2.

Lemma 5.8. *The curve $Y_{31} = X_1(31)/\langle 2\rangle$ has genus 6, the group $J_{Y_{31}}(\mathbb{Q})$ is finite, and $\mathrm{gon}_{\mathbb{Q}} Y_{31} \geq 5$.*

Proof. The diamond operator $\langle 2\rangle$ has order 5 in $\Delta(31)$, and Y_{31} is the curve $X_H(31)$ of [Orl25] with $H = \{\pm 1, \pm 2, \pm 4, \pm 8, \pm 16\}$. We compute that its genus is 6. The group $J_1(31)(\mathbb{Q})$ is finite [DEvH+21, Theorem 3.1(2)]. As $J_{Y_{31}}$ is isogenous to an abelian subvariety of $J_1(31)$, the group $J_{Y_{31}}(\mathbb{Q})$ is finite. The curve Y_{31} has good reduction at 2 (Lemma 2.1), and $\operatorname{gon}_{\mathbb{F}_2} Y_{31} \geq 5$ by [Orl25, Proposition 2.6 and Table 1], so $\operatorname{gon}_{\mathbb{Q}} Y_{31} \geq \operatorname{gon}_{\mathbb{F}_2} Y_{31} \geq 5$. □

Lemma 5.9. *For $1 \leq f \leq 10$ no elliptic curve over $\mathbb{F}_{2^f}$ has a point of order 155.*

Proof. The only multiple of 155 in one of the Hasse intervals $\left[2^f + 1 - 2^{f/2+1}, 2^f + 1 + 2^{f/2+1}\right]$ with $f \leq 10$ is $1085 = 7 \cdot 155$, for $f = 10$, which corresponds to the trace of Frobenius -60. It is even, and an elliptic curve over $\mathbb{F}_{2^{10}}$ with even trace of Frobenius is supersingular, so its trace is 0, ± 32 or ± 64 [Wat69, Theorem 4.1]. □

Proposition 5.10. *The group $\mathbb{Z}/155\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let E be an elliptic curve over a number field of degree 10 with a point of order 155, let x be the corresponding closed point of $Y_1(155)$, with residue field $K := \mathbb{Q}(x)$, and let D be the trace divisor, which is a positive multiple of x.

The group $(\langle 16\rangle - 1)J_1(155)(\mathbb{Q})$ is finite, as we compute that $W_\chi = S_\chi$ for every Galois orbit of even characters χ modulo 155 except those of order 1, 3 and 12, the sum of $\varphi(\operatorname{ord}\chi)\dim S_\chi$ being $841 = g(X_1(155))$, and these characters are trivial on 16, which has order 5 in $\Delta(155)$. As $16 \not\equiv \pm 3^{\pm 1} \pmod{155}$ we have $k_3 = 8$, and as $i(155) = 11520$, we get $b(155) = \frac{14625}{1024} > 14$. So $\langle 16\rangle D = D$ by Proposition 5.1, and $\langle 16\rangle$ maps x to itself. By Lemma 2.14, the geometric points of x have no complex multiplication, so by Lemma 5.7 the degree of K is divisible by 5, and $\langle 16\rangle$ induces an automorphism ϕ of K of order 5. As 31 is not in $S(5)$ [DKSS23, Theorem 1.2], we have $[K : \mathbb{Q}] \neq 5$. Hence $[K : \mathbb{Q}] = 10$, and $F := K^\phi$ is a quadratic field.

The residue fields of K at the primes above 2 have at most 2^{10} elements, so by Lemma 5.9, Lemma 2.7 and Lemma 2.4 the curve given by x has multiplicative reduction at every prime of K above 2, and $j(x)$ has negative valuation at each of them. As $16 \equiv 2^4 \pmod{31}$, the composition of $X_1(155) \to X_1(31)$, $(E, P) \mapsto (E, 5P)$, with the quotient map $X_1(31) \to Y_{31}$ is invariant under $\langle 16\rangle$, so by Lemma 5.7 the image y of x on Y_{31} is defined over F. In particular $j(y) = j(x) \in F$, and it has negative valuation at every prime of F above 2. Let D_Y be the sum of the images of y under the two embeddings of F into $\overline{\mathbb{Q}}$. It is an effective $\mathbb{Q}$-rational divisor of degree 2 on Y_{31} whose support contains no cusp, and it reduces to a cuspidal divisor modulo 2. But $J_{Y_{31}}(\mathbb{Q})$ is finite and $\operatorname{gon}_{\mathbb{Q}} Y_{31} \geq 5 > 4$ by Lemma 5.8, so this contradicts Proposition 2.5 b), applied with $X = Y_{31}$, $p = 2$ and $d = 2$. □

5.4. **The groups $\mathbb{Z}/95\mathbb{Z}$ and $\mathbb{Z}/111\mathbb{Z}$.** For $n = 95$ and $n = 111$ we use, as in [Naj26d, Section 4.2], that the elliptic curve has bad reduction at all the primes above 2, together with a diamond operator of order 3 and Lemma 2.10 c).

Lemma 5.11. *Let $n \in \{95, 111\}$, and let $h = \langle 11\rangle$ if $n = 95$ and $h = \langle 10\rangle$ if $n = 111$.*

a) *For $1 \leq f \leq 10$ no elliptic curve over $\mathbb{F}_{2^f}$ has a point of order n.*
b) *The diamond operator h has order 3 in $\Delta(n)$, and $(h-1)J_1(n)(\mathbb{Q})$ is finite.*

Proof. a) For $n = 95$ and $f \leq 7$, and for $n = 111$ and $f \leq 6$ or $f = 8$, the Hasse interval $\left[2^f + 1 - 2^{f/2+1}, 2^f + 1 + 2^{f/2+1}\right]$ contains no multiple of n. The remaining multiples of n in the Hasse intervals are 285, 475 and 1045 for $n = 95$ and $f = 8, 9, 10$, and 111, 555 and

999 for $n = 111$ and $f = 7, 9, 10$, which correspond to the traces of Frobenius -28, 38, -20, respectively 18, -42, 26. These are even, and an elliptic curve over $\mathbb{F}_{2^f}$ with even trace of Frobenius is supersingular, so its trace is 0 or $\pm 2^{(f+1)/2}$ for odd f, and 0, $\pm 2^{f/2}$ or $\pm 2^{f/2+1}$ for even f [Wat69, Theorem 4.1]. None of the six traces above is of this form.

b) The group $\Delta(n)$ is cyclic of order 36, generated by $\langle 2 \rangle$, and $11 \equiv 2^{12} \pmod{95}$ and $10 \equiv 2^{24} \pmod{111}$. So h has order 3, and a character of $\Delta(n)$ is non-trivial on h if and only if its order is 9, 18 or 36. We compute, with `computations/next95_winding.m` and `computations/winding111.m`, that $W_\chi = S_\chi$ for every Galois orbit of even characters χ modulo n except the characters of order 12 for $n = 95$, and of order 1 and 6 for $n = 111$, the sums of $\varphi(\operatorname{ord}\chi) \dim S_\chi$ being $289 = g(X_1(95))$ and $385 = g(X_1(111))$. These characters are trivial on h, so $(h-1)J_1(n)(\mathbb{Q})$ is finite. □

Proposition 5.12. *The groups $\mathbb{Z}/95\mathbb{Z}$ and $\mathbb{Z}/111\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let $n \in \{95, 111\}$, let h be as in Lemma 5.11, let E be an elliptic curve over a number field K of degree 10 with a point of order n, and let D be its trace divisor. The residue fields of K at the primes above 2 are $\mathbb{F}_{2^f}$ with $f \le 10$, so by Lemma 5.11 a) and Lemma 2.7 the curve E has bad reduction at every prime of K above 2. By Abramovich's bound, $\operatorname{gon}_{\mathbb{C}} X_1(95) \ge \frac{325}{2^{15}} \cdot 4320 = \frac{43875}{1024} > 42$ and $\operatorname{gon}_{\mathbb{C}} X_1(111) \ge \frac{325}{2^{15}} \cdot 5472 = \frac{55575}{1024} > 54$, so in both cases $\operatorname{gon}_{\mathbb{C}} X_1(n) > 40$. By Lemma 2.4 the reduction of D modulo a prime above 2 is cuspidal, and as the cusps are defined over $\mathbb{Q}(\zeta_n)$, which is unramified above 2, it lifts to an effective cuspidal divisor C of degree 10 over a number field unramified above 2. By Lemma 5.11 b), Lemma 2.10 c), with $g = h$, $p = 2$ and $d = e = 10$, gives $hD = D$, as the reduction of $D - C$ is 0. By Lemma 2.14 the support of D consists of non-CM points, so by Lemma 2.9 the order 3 of h divides 10, which is a contradiction. □

6. The groups $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with $m \ge 3$

Let E be an elliptic curve over a number field K of degree 10 with $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \subseteq E(K)$ for some $m \ge 3$. By the Weil pairing $m \in \{3, 4, 6, 11, 22\}$, and for $m \in \{3, 4\}$ the trace divisor is an effective $\mathbb{Q}(\zeta_m)$-rational divisor of degree $d_m = 5$ on $X_1(m, n)$ (Section 2.2). We treat here the group $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$, for which $K = \mathbb{Q}(\zeta_{11})$, and the groups $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/33\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}$. The remaining groups $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \in \mathcal{M}_{10}$ (Lemma 4.1) with $m \ge 3$, namely $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/39\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/45\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$, are ruled out in Corollaries 11.11 and 11.19 and Proposition 10.29. For $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$ the Hecke sieve at a single prime suffices, as in [Naj26d, Section 12]. For $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$ we compare the reductions at two primes, for $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$ we use stabilizers of level automorphisms, for $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/33\mathbb{Z}$ we push the trace divisor forward to $X_1(27)$ and $X_1(33)$ (for $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/33\mathbb{Z}$ together with a formal immersion argument at 2 on the part of the Jacobian on which a diamond operator acts by -1), and for $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}$ we work on $X_1(2, 28)$ over $\mathbb{Q}$.

Recall that by [DS17, Theorem 4.1] the group $J_1(m, n)(\mathbb{Q}(\zeta_m))$ is finite for $(m, n) \in \{(3, 21), (3, 24), (3, 27), (4, 16), (4, 20), (4, 24)\}$, and that in the Hecke sieve it suffices to test one point in each orbit of the level automorphisms defined over $\mathbb{Q}(\zeta_m)$ (Section 2.5). If D is the trace divisor of a point $x = (E, P, Q)$ and g is a level automorphism defined over $\mathbb{Q}(\zeta_m)$, then gD is the trace divisor of $g(x)$, which corresponds to the same elliptic curve E.

6.1. **The group $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$.** If $E[11] \subseteq E(K)$ with $[K : \mathbb{Q}] = 10$, then $K = \mathbb{Q}(\zeta_{11})$ by the Weil pairing, and E has a K-rational point of order 11. The modular curve $X_1(11)$ has genus 1, and its Jacobian is the elliptic curve

$$A\colon v^2 + v = u^3 - u^2$$

(11.a3).

Lemma 6.1. *Let $K = \mathbb{Q}(\zeta_{11})$ and let A be the elliptic curve $v^2 + v = u^3 - u^2$. Then $A(K)$ is finite.*

Proof. Let f be the newform of level 11 attached to A. As in the proof of [Naj26d, Lemma 5.1], the restriction of scalars of A_K to $\mathbb{Q}$ is isogenous to a product of the abelian varieties attached to the Galois orbits of the newforms associated with the twists $f \otimes \chi$, where χ runs over the characters of $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/11\mathbb{Z})^\times$, so by Kato's theorem $A(K)$ is finite if $L(f \otimes \chi, 1) \neq 0$ for all χ. As χ has conductor 1 or 11, the newform associated with $f \otimes \chi$ has level 11 or 121, and it has no complex multiplication, as f has none ($j(A) = -2^{12}/11$ is not an integer). The data of the LMFDB [LMF26] (see `inputs/global_newforms_cache.json`) show that every newform of weight 2 and level 11 or 121 without complex multiplication, with any character, has analytic rank 0. Hence $A(K)$ is finite. □

Proposition 6.2. *The group $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Suppose the opposite, that $E[11] \subseteq E(K)$ for an elliptic curve E over a number field K of degree 10. Then $K = \mathbb{Q}(\zeta_{11})$. Let $P \in E(K)$ be a point of order 11, let $x \in Y_1(11)(K)$ be the point given by (E, P), and let $\mathfrak{p}$ be a prime of K above 23. As $23 \equiv 1 \pmod{11}$, the prime 23 splits completely in K, so the residue field of $\mathfrak{p}$ is $\mathbb{F}_{23}$. Every elliptic curve over $\mathbb{F}_{23}$ has at most $(\sqrt{23} + 1)^2 < 34 < 121$ points, so by Lemma 2.7 and Lemma 2.4 the curve E has multiplicative reduction at $\mathfrak{p}$, and x reduces modulo $\mathfrak{p}$ to a cusp. The 10 cusps of $X_1(11)$ are defined over K, and their reductions modulo $\mathfrak{p}$ are the 10 cusps of $X_1(11)_{\mathbb{F}_{23}}$, so the reduction of x is the reduction of a cusp $c \in X_1(11)(K)$. The class $[x - c]$ lies in $J_1(11)(K) \simeq A(K)$, which is finite by Lemma 6.1, and its reduction modulo $\mathfrak{p}$ is 0, so $[x - c] = 0$ by Katz's result. As $X_1(11)$ has genus 1, it follows that $x = c$, which is a contradiction. □

6.2. **The group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z}$.**

Lemma 6.3. *Let $F = \mathbb{Q}(\zeta_3)$, let $X = X_1(3, 21)$ over F, and let $\mathfrak{p}$ be the prime of F above 2, with residue field $\mathbb{F}_4$.*

a) *The curve X has genus 25, and $J_X(F)$ is finite.*
b) *The cusps of X form Galois orbits over F of degrees $1^{24}, 6^4$, and the closed cusps of $X_{\mathbb{F}_4}$ have degrees $1^{24}, 3^8$. In particular, every closed cusp of $X_{\mathbb{F}_4}$ of degree 1 is the reduction of an F-rational cusp.*
c) *The numbers of non-cuspidal closed points of $X_{\mathbb{F}_4}$ of degrees $1, \dots, 5$ are 0, 0, 0, 144 and 216.*
d) *For every effective cuspidal divisor $\overline{C}$ of degree 5 on $X_{\mathbb{F}_4}$ we have $\ell(2\overline{C}) = 1$.*

Proof. Part a) is [DS17, Theorem 4.1]. The Galois orbits of the cusps and their reductions are computed from the description of the cusps in Section 2.1: the Frobenius at $\mathfrak{p}$ acts as σ_4, which has order 3 in $\mathrm{Gal}(\mathbb{Q}(\zeta_{21})/F)$, so each of the 4 orbits of length 6 splits into 2 closed cusps of degree 3. Part c) is a direct computation. For d), there are $\binom{28}{5} + 8\binom{25}{2} = 100680$

effective cuspidal divisors $\overline{C} = \sum_P m_P P$ of degree 5 on $X_{\mathbb{F}_4}$. As explained after [Naj26d, Lemma 5.3], $\ell(2\overline{C}) = 1$ if and only if the 10 linear conditions on $H^0(X_{\mathbb{F}_4}, \Omega^1)$ given by the vanishing of the first $2m_P$ coefficients of the local expansions at each P are linearly independent, and we compute that this holds for all 100680 divisors. □

Proposition 6.4. *The group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree* 10.

Proof. Suppose the opposite, let F, X and $\mathfrak{p}$ be as in Lemma 6.3, and let D be the trace divisor, an effective F-rational divisor of degree 5 on X with non-cuspidal support. By Lemma 6.3 a) and d) and Lemma 2.6, the reduction of D modulo $\mathfrak{p}$ is not entirely cuspidal. By Lemma 6.3 c) it is $D' + C'$, where either D' is one of the 144 non-cuspidal closed points of degree 4 and C' is a cusp of degree 1, or D' is one of the 216 non-cuspidal closed points of degree 5 and $C' = 0$. In both cases C' is 0 or the reduction of an F-rational cusp by Lemma 6.3 b), so 13 is admissible for C', and $[A_{13}(D')] = 0$ (Section 2.5).

Write $Q_3 = 7Q$ and $Q_7 = 3Q$. The 72 level automorphisms $(P, Q) \mapsto (aP + bQ_3,\ cP + dQ_3 + 5uQ_7)$, with $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_3)$ and $u \in (\mathbb{Z}/7\mathbb{Z})^\times$, taken modulo ± 1, are defined over F, and they have 2 orbits on the non-cuspidal closed points of $X_{\mathbb{F}_4}$ of degree 4 and 3 orbits on those of degree 5. For the points of degree 4 we computed in the proof of [Naj26d, Proposition 12.2] that $A_{13}x$ is not principal for a representative x of each of the 2 orbits (see `continuation_20261029/degree_independent_321/sieve_3_21_D4_p2.m`), and we compute that $A_{13}x$ is not principal for a representative x of each of the 3 orbits of points of degree 5. This is a contradiction. □

6.3. The groups $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$.

Lemma 6.5. a) *Let $F = \mathbb{Q}(\zeta_3)$, $X = X_1(3, 24)$ over F, and let $\mathfrak{p}$ be a prime of F above 7, with residue field $\mathbb{F}_7$. Then X has genus 25, $J_X(F)$ is finite and $\mathrm{gon}_{\mathbb{C}} X > 5.71$. The cusps of X form Galois orbits over F of degrees $1^{24}, 2^4, 4^4$, the closed cusps of $X_{\mathbb{F}_7}$ have degrees $1^{24}, 2^{12}$, and those of degree 1 are the reductions of the F-rational cusps. The numbers of non-cuspidal closed points of $X_{\mathbb{F}_7}$ of degrees $1, \dots, 5$ are 0, 0, 48, 456 and 3456.*

b) *Let $F = \mathbb{Q}(i)$, $X = X_1(4, 24)$ over F, and let $\mathfrak{p}$ be a prime of F above 5, with residue field $\mathbb{F}_5$. Then X has genus 33, $J_X(F)$ is finite and $\mathrm{gon}_{\mathbb{C}} X > 7.61$. The cusps of X form Galois orbits over F of degrees $1^{16}, 2^{16}, 4^4$, the closed cusps of $X_{\mathbb{F}_5}$ have degrees $1^{16}, 2^{24}$, and those of degree 1 are the reductions of the F-rational cusps. The numbers of non-cuspidal closed points of $X_{\mathbb{F}_5}$ of degrees $1, \dots, 5$ are 0, 0, 0, 96 and 704.*

Proof. The finiteness of $J_X(F)$ is [DS17, Theorem 4.1], and the gonality bounds follow from Abramovich's bound, as $i(3, 24) = 576$ and $i(4, 24) = 768$. The Galois orbits of the cusps and their reductions are computed from the description of the cusps in Section 2.1, and the numbers of points are computed for $X_1(3, 24)$ and for $X_1(4, 24)$ directly. □

Proposition 6.6. *The groups $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over a number field of degree* 10.

Proof. Suppose first that $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \subseteq E(K)$ for an elliptic curve E over a number field K of degree 10, let F, X and $\mathfrak{p}$ be as in Lemma 6.5 a), and let D be the trace divisor, of degree 5. As $\mathrm{gon}_F X \geq \mathrm{gon}_{\mathbb{C}} X > 5$, Proposition 2.5 a) shows that the reduction of D

modulo $\mathfrak{p}$ is not entirely cuspidal, so it is $D'+C'$ of type [3], with C' effective cuspidal of degree 2, of type [4], with C' a cusp of degree 1, or of type [5], with $C'=0$. Write $R_3=8Q$ and $R_8=3Q$. The 48 level automorphisms $(P,R_3,R_8)\mapsto(aP+bR_3,\ cP+dR_3,\ uR_8)$, with $\begin{pmatrix}a&b\\c&d\end{pmatrix}\in \mathrm{SL}_2(\mathbb{F}_3)$ and $u\in(\mathbb{Z}/8\mathbb{Z})^\times$, taken modulo ±1, have 1, 13 and 72 orbits on the non-cuspidal closed points of $X_{\mathbb{F}_7}$ of degrees 3, 4 and 5. In the types [4] and [5] the prime 13 is admissible for C', and we compute that $A_{13}x$ is not principal for the representatives x of the 13 orbits of degree 4 and of the 72 orbits of degree 5 (the latter computation is split into the six scripts `cont_sieve_3_24_D5_shard`i, $i=0,\dots,5$). In the type [3] the cuspidal part C' may contain cusps of degree 2, which need not be reductions of F-rational cuspidal divisors. But $31\equiv 7 \pmod{24}$, so 31 is admissible for every C' by Lemma 2.3, and we compute that $A_{31}x$ is not principal for a representative x of the single orbit of points of degree 3. This excludes all the possible reductions.

Suppose now that $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/24\mathbb{Z}\subseteq E(K)$ for an elliptic curve E over a number field K of degree 10, and let F, X and $\mathfrak{p}$ be as in Lemma 6.5 b). As $\mathrm{gon}_F X>7.61>5$, the reduction of the trace divisor modulo $\mathfrak{p}$ is not entirely cuspidal by Proposition 2.5 a), so it is of type [4], with C' a cusp of degree 1, or of type [5], with $C'=0$, and in both cases 13 is admissible for C'. The 64 level automorphisms $(P,Q)\mapsto(aP+6bQ,\ cP+dQ)$, with $b,c\in\mathbb{Z}/4\mathbb{Z}$, $d\in\{1,5,7,11\}$ and $a\equiv d^{-1}(1+6bc) \pmod 4$, taken modulo ±1, have 4 orbits on the points of degree 4 and 11 orbits on the points of degree 5, and we compute that $A_{13}x$ is not principal for the representatives x of all of them (see this script for the first orbit of points of degree 4 and this script for the first orbit of points of degree 5, and the analogous scripts `cont_sieve_4_24_D5_d4_r`i and `cont_sieve_4_24_D5_d5_r`i for the others). □

6.4. **The group $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/16\mathbb{Z}$.** For $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/16\mathbb{Z}$ the Hecke sieve at one prime does not suffice, and we compare the reductions at two primes as in [Naj26d, Section 12.4], using the following lemma.

Lemma 6.7 ([Naj26d, Lemma 12.4])**.** *Let X be a curve over a number field F with $J_X(F)$ finite and with an F-rational cusp c_*. Let $\mathfrak{p}_1,\mathfrak{p}_2$ be primes of good reduction, with residue fields k_1,k_2, such that reduction modulo $\mathfrak{p}_1$ is injective on $J_X(F)$, let $H_i\subseteq J_X(k_i)$ be the image of $\mathrm{Cl}^c_F X$ under reduction modulo $\mathfrak{p}_i$, and let $\psi: H_1\to H_2$ be the composite of the inverse of the reduction map $\mathrm{Cl}^c_F X\to H_1$ with the reduction map $\mathrm{Cl}^c_F X\to H_2$. If $J_X(k_1)/H_1$ has exponent e, then for every $D\in X^{(d)}(F)$, with reductions $\overline{D}_i$ and $\overline{c_{*,i}}$ of D and c_* modulo $\mathfrak{p}_i$, we have*

$$\psi\big(e[\overline{D}_1-d\,\overline{c_{*,1}}]\big)=e[\overline{D}_2-d\,\overline{c_{*,2}}].$$

Lemma 6.8. *Let $F=\mathbb{Q}(i)$, let $X=X_1(4,16)$ over F, and let $\mathfrak{p}_5$, $\mathfrak{p}_3$ and $\mathfrak{p}_{13}$ be primes of F above 5, 3 and 13, with residue fields $\mathbb{F}_5$, $\mathbb{F}_9$ and $\mathbb{F}_{13}$.*

a) *The curve X has genus 13, $J_X(F)$ is finite and $\mathrm{gon}_F X\geq 8$.*
b) *The cusps of X form 24 Galois orbits over F, of degrees $1^{16},2^4,4^4$. Modulo $\mathfrak{p}_5$ and modulo $\mathfrak{p}_{13}$ each of them reduces to a single closed cusp of the same degree, and modulo $\mathfrak{p}_3$ the closed cusps have degrees $1^{24},2^8$.*
c) *The numbers of non-cuspidal closed points of degrees $1,\dots,5$ are 0, 0, 64, 160 and 512 on $X_{\mathbb{F}_5}$ and 0, 0, 320, 1808 and 11904 on $X_{\mathbb{F}_9}$.*

d) *Let* H_5 *and* H_9 *be the reductions of* $\mathrm{Cl}_F^c X$ *modulo* $\mathfrak{p}_5$ *and* $\mathfrak{p}_3$*. Then*

$$J_X(\mathbb{F}_5) \simeq (\mathbb{Z}/2\mathbb{Z})^6 \times (\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/40\mathbb{Z})^2 \times (\mathbb{Z}/80\mathbb{Z})^2,$$
$$J_X(\mathbb{F}_9) \simeq (\mathbb{Z}/2\mathbb{Z})^8 \times (\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/8\mathbb{Z})^2 \times (\mathbb{Z}/80\mathbb{Z})^4,$$
$$H_5 \simeq H_9 \simeq \mathrm{Cl}_F^c X \simeq (\mathbb{Z}/2\mathbb{Z})^3 \times (\mathbb{Z}/4\mathbb{Z})^2 \times \mathbb{Z}/20\mathbb{Z} \times (\mathbb{Z}/40\mathbb{Z})^2 \times \mathbb{Z}/80\mathbb{Z},$$

and $J_X(\mathbb{F}_5)/H_5 \simeq (\mathbb{Z}/2\mathbb{Z})^5$*. In particular* $2J_X(F) \subseteq \mathrm{Cl}_F^c X$*.*

e) *The group* G *of the* 64 *level automorphisms* $(P, Q) \mapsto (aP + 4bQ,\ cP + dQ)$*, with* $b, c \in \mathbb{Z}/4\mathbb{Z}$*,* $d \in (\mathbb{Z}/16\mathbb{Z})^\times$ *and* $a \equiv d^{-1} \pmod 4$*, taken modulo* ± 1*, consists of automorphisms defined over* F*, and it has* 5*,* 33 *and* 186 *orbits on the non-cuspidal closed points of* $X_{\mathbb{F}_9}$ *of degrees* 3*,* 4 *and* 5*.*

Proof. Part a) is [DS17, Theorem 4.1] and [NV26, Table 1]. In b), σ_5 and σ_{13} generate $\mathrm{Gal}(\mathbb{Q}(\zeta_{16})/F)$, while the Frobenius σ_9 at $\mathfrak{p}_3$ has order 2, which splits each of the 4 orbits of degree 2 into 2 cusps of degree 1 and each of the 4 orbits of degree 4 into 2 cusps of degree 2. We identify the reductions of each Galois orbit at the three primes using the valuations of integral modular units, in the normal form $y^2 + xy + By = x^3 + Bx^2$ with $P = (0, 0)$ of order 4. The numbers of points in c), the groups in d) and the orbits in e) are computed directly (see also `computations/cont_local_4_16_q5.m`). As 5 is odd and unramified in F, reduction modulo $\mathfrak{p}_5$ is injective on $J_X(F)$, and the last claim of d) follows, as does $H_5 \simeq \mathrm{Cl}_F^c X$. Similarly $H_9 \simeq \mathrm{Cl}_F^c X$. □

Proposition 6.9. *The group* $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$ *is not a subgroup of the torsion of an elliptic curve over a number field of degree* 10*.*

Proof. Suppose the opposite, let F, X, $\mathfrak{p}_5$, $\mathfrak{p}_3$, $\mathfrak{p}_{13}$, H_5, H_9 and G be as in Lemma 6.8, and let D be the trace divisor, of degree 5. As $\mathrm{gon}_F X \geq 8 > 5$, by Proposition 2.5 a) the reductions of D modulo $\mathfrak{p}_5$ and modulo $\mathfrak{p}_3$ are not entirely cuspidal. By Lemma 6.8 c), modulo $\mathfrak{p}_5$ the reduction of D is a closed point of degree 3 plus an effective cuspidal divisor of degree 2, a point of degree 4 plus one of the 16 cusps of degree 1, or a point of degree 5, which gives

$$64\left(\tbinom{17}{2} + 4\right) + 160 \cdot 16 + 512 = 12032$$

possibilities. Modulo $\mathfrak{p}_3$ the reduction has the same types. Replacing D by gD for a suitable $g \in G$, we may assume that its non-cuspidal part modulo $\mathfrak{p}_3$ is one of the representatives of the orbits of Lemma 6.8 e), and this does not affect the set of the 12032 possibilities modulo $\mathfrak{p}_5$, which is stable under G. Allowing all the cuspidal parts, this gives

$$5\left(\tbinom{25}{2} + 8\right) + 33 \cdot 24 + 186 = 2518$$

possibilities for the reduction $\overline{D}_3$ of D modulo $\mathfrak{p}_3$.

Fix an F-rational cusp c_0, and let $\overline{D}_5$ be the reduction of D modulo $\mathfrak{p}_5$. By Lemma 6.7 with $\mathfrak{p}_1 = \mathfrak{p}_5$, $\mathfrak{p}_2 = \mathfrak{p}_3$ and $e = 2$ we have $\psi(2[\overline{D}_5 - 5\overline{c_0}]) = 2[\overline{D}_3 - 5\overline{c_0}]$. We compute that only 158 of the 2518 possibilities for $\overline{D}_3$ satisfy this relation for one of the 12032 possibilities for $\overline{D}_5$: 157 consisting of a point of degree 3 and an effective cuspidal divisor of degree 2, and one point of degree 5. In each of these 158 cases the class $2[D - 5c_0]$, which lies in $\mathrm{Cl}_F^c X$ by Lemma 6.8 d), is determined by its reduction modulo $\mathfrak{p}_3$, so $2D \sim L_v$, where

$$L_v = 10c_0 + \sum_{j=1}^{24} v_j\big(C_j - \deg(C_j)c_0\big)$$

for an explicit $v \in \mathbb{Z}^{24}$, the C_j being the 24 Galois orbits of cusps over F. Reducing modulo $\mathfrak{p}_{13}$, the divisor $2\overline{D}_{13}$, where $\overline{D}_{13}$ is the reduction of D, is an effective $\mathbb{F}_{13}$-rational divisor in the linear system $|\overline{L_v}|$ all of whose multiplicities are even. We compute that $\ell(\overline{L_v}) = 1$ in 150 of the 158 cases and $\ell(\overline{L_v}) = 2$ in the other 8, and that each of the $150 + 8 \cdot 14 = 262$ effective $\mathbb{F}_{13}$-rational divisors in these linear systems has a point of odd multiplicity. This is a contradiction. □

6.5. **The group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$.** For $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$ the Hecke sieve leaves 4 possible reductions whose non-cuspidal parts are fixed by an involution, and we exclude these with Lemma 2.15 and Lemma 2.10.

Lemma 6.10. *Let $F = \mathbb{Q}(i)$, let $X = X_1(4, 20)$ over F, and let $\mathfrak{p}$ be the prime of F above 3, with residue field $\mathbb{F}_9$.*

a) *The curve X has genus 25, $J_X(F)$ is finite and $\operatorname{gon}_{\mathbb{C}} X > 5.71$.*
b) *The cusps of X form Galois orbits over F of degrees $1^{24}, 4^6$, the closed cusps of $X_{\mathbb{F}_9}$ have degrees $1^{24}, 2^{12}$, and those of degree 1 are the reductions of the F-rational cusps.*
c) *The numbers of non-cuspidal closed points of $X_{\mathbb{F}_9}$ of degrees $1, \dots, 5$ are 0, 96, 320, 888 and 11904.*
d) *Let G be the group of the 96 level automorphisms $(P, Q) \mapsto (aP + bQ_4,\ cP + dQ_4 - uQ_5)$, where $Q_4 = 5Q$, $Q_5 = 4Q$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ and $u \in (\mathbb{Z}/5\mathbb{Z})^\times$, taken modulo $(-I, -1)$. Its elements are defined over F, and it has 2, 4, 12 and 124 orbits on the non-cuspidal closed points of $X_{\mathbb{F}_9}$ of degrees 2, 3, 4 and 5.*

Proof. The finiteness of $J_X(F)$ is [DS17, Theorem 4.1], and the gonality bound follows from Abramovich's bound, as $i(4, 20) = 576$. The Galois orbits of the cusps and their reductions are computed from the description of the cusps in Section 2.1, and the numbers of points are computed directly. The orbits of G are computed in the scripts linked in the proof of Proposition 6.11. □

Proposition 6.11. *The group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Suppose the opposite, let F, X, $\mathfrak{p}$ and G be as in Lemma 6.10, and let D be the trace divisor, of degree 5. As $\operatorname{gon}_F X \geq \operatorname{gon}_{\mathbb{C}} X > 5$ by Lemma 6.10 a), the reduction of D modulo $\mathfrak{p}$ is not entirely cuspidal by Proposition 2.5 a), so by Lemma 6.10 c) it is $D' + C'$ with D' of type [2], [3], [4], [5], [2, 2] or [2, 3] and C' effective cuspidal of degree 3, 2, 1, 0, 1 or 0, respectively. In the type [2, 2] the two points may coincide. As $29 \equiv 9 \pmod{20}$, the prime 29 is admissible for every C' by Lemma 2.3, and by Lemma 6.10 b) every prime, in particular 13, is admissible for C' when C' is 0 or a cusp of degree 1. Replacing D by gD for some $g \in G$, we may assume that D' is a representative of an orbit of G, and in the types [2, 3] and [2, 2] that the quadratic point, respectively one of the two quadratic points, is such a representative. This gives the numbers of cases in the following table, and we compute that $A_q D'$ is not principal for one of the listed primes q in all but 4 of them.

type of D'	cases	q	remaining
[2]	2	29	0
[3]	4	29	0
[4]	12	29, 13	2
[5]	124	13	0
[2, 2]	$2 \cdot 96 = 192$	29, 13	2
[2, 3]	$2 \cdot 320 = 640$	13	0

For the types [2], [3] and [4] we compute $A_{29}D'$, and for the 4 points of degree 4 that remain we compute $A_{13}D'$. For the type [5] we compute $A_{13}D'$ (the computation is split into twelve scripts `cont_sieve_4_20_quintic_shard`i, $i = 0, \dots, 11$). For the types [2, 2] and [2, 3] we compute $A_{29}D'$ and $A_{13}D'$, respectively (in eight scripts `cont_sieve_4_20_mixed_shard`i, $i = 0, \dots, 7$), and for the 8 divisors of type [2, 2] that remain we compute $A_{13}D'$.

In each of the 4 remaining cases the reduction of D is $B + \overline{c}$, where B is a closed point of degree 4 or a sum of two closed points of degree 2, and $\overline{c}$ is a closed cusp of degree 1. We compute that the stabilizers in G of the two remaining points of degree 4 have order 8 and both contain the element with $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = -I$ and $u = 1$, and that the stabilizers of the two remaining divisors of type [2, 2] have order 4 and contain the elements with $u = 1$ and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}, \quad \text{respectively} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}.$$

Let g be this element in the case at hand, a level automorphism of order 2 defined over F, which fixes B. We compute that $\ell(B + \overline{c}_1 + \overline{c}_2) = 1$ on $X_{\mathbb{F}_9}$ for each of the 4 divisors B and all the closed cusps $\overline{c}_1, \overline{c}_2$ of degree 1, possibly equal (1200 divisors in total). As $g\overline{c}$ is again a closed cusp of degree 1, we have $\ell(B + \overline{c} + g\overline{c}) = 1$, and Lemma 2.15 with $r = 2$ gives $g\overline{c} = \overline{c}$. So g fixes the reduction $B + \overline{c}$ of D, and as $J_X(F)$ is finite and $\operatorname{gon}_F X \geq \operatorname{gon}_{\mathbb{C}} X > 5$, Lemma 2.10 a), with $C = 0$, gives $gD = D$. By Lemma 2.14, the points in the support of D correspond to elliptic curves without complex multiplication, so Lemma 2.9, applied to the group of order 2 generated by g, shows that $\deg D$ is even. This contradicts $\deg D = 5$. □

6.6. The group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$.

Lemma 6.12. *Let $F = \mathbb{Q}(\zeta_3)$, let $X = X_1(3, 27)$ over F, let $\mathfrak{p}$ be the prime of F above 2, with residue field $\mathbb{F}_4$, and let $\pi : X \to Y = X_1(27)_F$ be the map $(E, P, Q) \mapsto (E, Q)$.*

a) *The curve X has genus 46, $\operatorname{gon}_{\mathbb{C}} X > 9.64$, and $J_X(F)$ is finite of odd order.*
b) *Every Galois orbit of cusps of X over F reduces modulo $\mathfrak{p}$ to a single closed cusp of the same degree. These degrees are $1^{27}, 3^6, 9^3$.*
c) *The numbers of non-cuspidal closed points of $X_{\mathbb{F}_4}$ of degrees $1, \dots, 5$ are 0, 0, 0, 0 and 162.*
d) *The map π sends the 162 non-cuspidal closed points of degree 5 of $X_{\mathbb{F}_4}$ onto 54 closed points of degree 5 of $Y_{\mathbb{F}_4}$, which form 6 orbits under the diamond operators.*

Proof. For a), the gonality bound is Abramovich's bound with $i(3, 27) = 972$, and $J_X(F)$ is finite by [DS17, Theorem 4.1]. Over F the curve X is isomorphic to $X_H(81)$, the quotient of $X_1(81)$ by the subgroup $H = \{1, 28, 55\}$ of the diamond operators [DS17, Section 2], and this isomorphism comes from the moduli interpretation, so it is compatible with reduction at the primes of F above 2 and 37. The Jacobian of $X_H(81)$ has dimension 46, and we

compute the characteristic polynomial of Frobenius at 37 on it and find that $\#J_X(\mathbb{F}_{37})$ is odd. As 37 splits in F and reduction modulo a prime above 37 is injective on $J_X(F)$ by Katz's result, $J_X(F)$ has odd order.

The group $\mathrm{Gal}(\mathbb{Q}(\zeta_{27})/F)$ is cyclic of order 9, and it is generated by the Frobenius σ_4 at $\mathfrak{p}$, as 4 has order 9 modulo 27. So σ_4 acts transitively on each Galois orbit of cusps over F, which proves the first claim of b). The degrees are computed from the description of the cusps in Section 2.1. We compute c) from the Frobenius polynomial of the Jacobian of $X_H(81)$ at 2, and d) by running through all the elliptic curves over $\mathbb{F}_{4^5}$ with a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$ and all their level structures. □

Proposition 6.13. *The group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree* 10.

Proof. Suppose the opposite, let F, X, $\mathfrak{p}$, π and Y be as in Lemma 6.12, and let D be the trace divisor, an effective F-rational divisor of degree 5 on X with non-cuspidal support.

Suppose first that the reduction of D modulo $\mathfrak{p}$ is an effective cuspidal divisor $\overline{C}$. By Lemma 6.12 b), $\overline{C}$ is the reduction of an effective F-rational cuspidal divisor C. The class $[D - C] \in J_X(F)$ reduces to 0, so $2[D - C] = 0$ by Parent's result, and $[D - C] = 0$ as $J_X(F)$ has odd order. So $D \sim C$ and $D \neq C$, which contradicts $\mathrm{gon}_F X \geq \mathrm{gon}_{\mathbb{C}} X > 5$ (Lemma 2.8 a)).

So by Lemma 6.12 c) the reduction of D is one of the 162 non-cuspidal closed points x of degree 5 of $X_{\mathbb{F}_4}$, and the reduction of the effective F-rational divisor $\pi_* D$ of degree 5 on Y is the closed point $N = \pi(x)$ of degree 5. As $\pi^* : J_Y \to J_X$ has finite kernel and $J_X(F)$ is finite, $J_Y(F)$ is finite. Let c_0 be a rational cusp of Y. As 7 splits in F and $7 \nmid 2 \cdot 27$, the operator $A_7 = T_7 - 7\langle 7 \rangle - 1$ on Y kills $J_Y(F)$ and c_0 (Proposition 2.2 b) and c)), so $[A_7(\pi_* D)] = A_7[\pi_* D - 5c_0] = 0$, and $A_7 N$ is principal on $Y_{\mathbb{F}_4}$. As A_7 commutes with the diamond operators, by Lemma 6.12 d) it suffices to check this for 6 representatives N, and we compute that $\ell(A_7 N) = 0$ for each of them. This is a contradiction. □

6.7. **The group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/33\mathbb{Z}$.** The group $J_1(3,33)(\mathbb{Q}(\zeta_3))$ is infinite, as over $\mathbb{Q}(\zeta_3)$ the curve $X_1(3,33)$ is isomorphic to a quotient of $X_1(99)$ [DS17, Section 2], which maps to $X_0(99)$, and the elliptic curve 99.a2, a quotient of $J_0(99)$, has rank 1. So Proposition 2.5 and the Hecke sieve cannot be applied to $X_1(3,33)$ directly. Let $h = \langle 10 \rangle$, which is the involution $(E, P, Q) \mapsto (E, P, 10Q)$ of $X_1(3,33)$, as $10 \equiv 1 \pmod 3$ and $10^2 \equiv 1 \pmod{33}$. We use the part of the Jacobian on which h acts by -1, which has finitely many points over $\mathbb{Q}(\zeta_3)$ (Lemma 6.14), and for the entirely cuspidal reduction modulo 2 a formal immersion argument over the unramified quadratic extension of $\mathbb{Q}_2$, which is a variant of Proposition 2.18 with $\mathcal{C}^2$ in place of $\mathcal{C}$.

Lemma 6.14. *Let $F = \mathbb{Q}(\zeta_3)$, $X = X_1(3,33)$ and $h = \langle 10 \rangle$. Then $(h_* - 1)J_X(F)$ is finite.*

Proof. Over F the curve X is isomorphic to the quotient $X_H(99)$ of $X_1(99)$ by the subgroup $H = \{1, 34, 67\}$ of the diamond operators [DS17, Section 2], and h corresponds to the diamond operator $\langle 10 \rangle$ of $X_H(99)$. The image B of $\langle 10 \rangle_* - 1$ on the Jacobian of $X_H(99)$ is an abelian variety over $\mathbb{Q}$, and the newforms occurring in it are those whose character ε satisfies $\varepsilon(34) = 1$ and $\varepsilon(10) = -1$. Such characters factor through $(\mathbb{Z}/33\mathbb{Z})^\times$, so their conductors divide 33. We compute that they form two Galois orbits, of orders 2 and 10, and that the corresponding spaces of cuspidal modular symbols with sign $+1$ have dimension 8 over the field of values of the character. This accounts for $8 + 4 \cdot 8 = 40 = 81 - 41$ dimensions, where 81 and 41 are the genera of $X_H(99)$ and of its quotient by $\langle 10 \rangle$, which

we also compute, so B has dimension 40. We also compute that in both cases the winding element generates the whole space as a module over the Hecke algebra: the images of the winding element under the products of $T_2, T_3, \dots, T_{23}$ span the space modulo a prime of degree 1 of the field of values, above 5, respectively 11. So $L(f,1) \neq 0$ for every newform f occurring in B.

Let χ_{-3} be the quadratic character of F. By the argument of the proof of [DS17, Theorem 4.1], $B(F)$ is finite if $L(f,1) \neq 0$ and $L(f \otimes \chi_{-3}, 1) \neq 0$ for all such f, and as the conductor of ε divides 33 and $99 = 3 \cdot 33$, the twist $f \otimes \chi_{-3}$ again lies in $S_2(\Gamma_0(99), \varepsilon)$ (see loc. cit.), so it again occurs in B. Hence $B(F)$ is finite, and so is $(h_* - 1)J_X(F)$, as $(h_* - 1)J_X$ corresponds to B under the isomorphism. □

Let R be the ring of integers of the unramified quadratic extension of $\mathbb{Q}_2$, with residue field $k = \mathbb{F}_4$. For an abelian scheme A over R of dimension g we choose coordinates $z = (z_1, \dots, z_g)$ of its formal group. The points of $A(R)$ which reduce to 0 are those with coordinates in $2R$ (see the proof of [Naj26d, Lemma 7.1]), and for such a point P we write $z(P) = 2u$ with $u \in R^g$, and call the reduction $\tau(P) := \overline{u}$ the *first order tangent* of P. We view it as a tangent vector of A_k at 0, which does not depend on the choice of coordinates. We write V_4 for the Verschiebung of A_k relative to k. It satisfies $V_4 \circ \mathrm{Frob}_4 = [4]$, where Frob_4 is the Frobenius endomorphism of A_k, which raises the coordinates to the 4-th power. If A is the Jacobian of a curve $\mathcal{X}$ over R, then $V_4^* = \mathcal{C}^2$ on $H^0(A_k, \Omega^1) = H^0(\mathcal{X}_k, \Omega^1)$, where $\mathcal{C}$ is the Cartier operator [Oda69].

Lemma 6.15. *Let R be the ring of integers of the unramified quadratic extension of $\mathbb{Q}_2$, with residue field $k = \mathbb{F}_4$, let A be an abelian scheme over R, and let $P \in A(R)$ be a torsion point which reduces to 0.*

a) *We have $2P = 0$, and if $\tau(P) = 0$, then $P = 0$.*
b) *For every $\omega \in H^0(A_k, \Omega^1)$ we have $(V_4^*\omega - \omega)(\tau(P)) = 0$.*

Proof. Multiplication by 2 maps the points with coordinates in $2R$ to points with coordinates in $4R$, and a non-zero point v with coordinates in $4R$ is not killed by 2: if $s \geq 2$ is the least valuation of a coordinate of v, then in such a coordinate the linear term of $[2](v)$ has valuation $s+1$, and all the other terms have valuation at least $2s > s+1$. Multiplication by an odd integer is an automorphism of the formal group, so the points with coordinates in $4R$ form a torsion-free group. As $2P$ has coordinates in $4R$ and is torsion, $2P = 0$, and if $\tau(P) = 0$, then P has coordinates in $4R$, so $P = 0$. This proves a).

For b), write $[2](z) = 2z + \mathcal{Q}(z) + \mathcal{S}(z)$, where the coordinates of $\mathcal{Q}$ are homogeneous of degree 2 and $\mathcal{S}$ has only terms of degree at least 3, all with coefficients in R. As $[2] = V \circ \mathrm{Frob}$ on A_k, where $\mathrm{Frob} : A_k \to A_k^{(2)}$ is the relative Frobenius and V the Verschiebung, the reduction of $\mathcal{Q}$ is $\overline{\mathcal{Q}}(z) = \overline{M}(z_1^2, \dots, z_g^2)^t$, where $\overline{M}$ is the matrix of the linear part of V (as in the proof of [Naj26d, Lemma 7.1]). As $2P = 0$, we have $0 = [2](2u) \equiv 4u + 4\mathcal{Q}(u) \pmod 8$, so $\overline{u} = \overline{M}\,\overline{u}^{[2]}$, where $\overline{u}^{[2]}$ is obtained by squaring the coordinates of $\overline{u}$. Applying the Frobenius of k to this identity and using $\overline{u}^{[4]} = \overline{u}$, which holds as $\overline{u} \in \mathbb{F}_4^g$, we get $\overline{u}^{[2]} = \overline{M}^{[2]}\,\overline{u}$, and hence $\overline{u} = \overline{M}\,\overline{M}^{[2]}\,\overline{u}$. The matrix $\overline{M}^{[2]}$ is the matrix of the linear part of $V^{(2)} : A_k^{(4)} \to A_k^{(2)}$, and $A_k^{(4)} = A_k$, so $\overline{M}\,\overline{M}^{[2]}$ is the matrix of the tangent map of $V_4 = V \circ V^{(2)}$ at 0. Hence $\tau(P)$ is fixed by the tangent map of V_4, which is b). □

Lemma 6.16. *Let R be the ring of integers of the unramified quadratic extension of $\mathbb{Q}_2$, with residue field $k = \mathbb{F}_4$. Let $\mathcal{X}$ be a smooth proper curve over R with Jacobian A, let h be*

an automorphism of $\mathcal{X}$ of order 2, and put $\alpha = h_* - 1 \in \mathrm{End}(A)$. Let $\Sigma \subseteq \mathcal{X}$ be a closed subscheme which is finite étale over R and stable under h, such that h fixes no closed point of Σ_k. Let $\overline{C}$ be an effective divisor of degree d on $\mathcal{X}_k$ supported on Σ_k. For each pair $\{c, hc\}$ of closed points of Σ_k let m_c be the smaller of the multiplicities of c and hc in $\overline{C}$, and put $\overline{B} = \sum m_c(c + hc)$, the sum being over these pairs, $\overline{C}_0 = \overline{C} - \overline{B}$ and $k_0 = \deg \overline{B}/2$. Let C and C_0 be the effective divisors on $\mathcal{X}$ supported on Σ which reduce to $\overline{C}$ and $\overline{C}_0$ (they exist and are unique, as Σ is finite étale over R), and put

$$U = (\mathcal{C}^2 - 1)\, \alpha^* H^0(\mathcal{X}_k, \Omega^1) \subseteq H^0(\mathcal{X}_k, \Omega^1).$$

Suppose that the restriction map $U \to H^0(\overline{C}, \Omega^1|_{\overline{C}})$ has rank $d - k_0$. If $D \in \mathcal{X}^{(d)}(R)$ reduces to $\overline{C}$ and $\alpha[D - C]$ is torsion, then $C_0 \leq D$.

Proof. Note first that h^* commutes with $\mathcal{C}$, so $U = \alpha^*(\mathcal{C}^2 - 1)H^0(\mathcal{X}_k, \Omega^1) \subseteq \alpha^* H^0(\mathcal{X}_k, \Omega^1)$. Choose one point c in each pair $\{c, hc\}$ and put $\overline{G} = \sum m_c c$. Then $\overline{B} = \overline{G} + h\overline{G}$ and $\deg \overline{G} = k_0$. Let G_0 be the effective divisor supported on Σ which reduces to $\overline{G}$. Consider the morphisms

$$f : \mathcal{X}^{(d)} \to A, \quad E \mapsto \alpha[E - C], \qquad\qquad \iota : \mathcal{X}^{(k_0)} \to \mathcal{X}^{(d)}, \quad G \mapsto C_0 + G + hG.$$

As $C = C_0 + G_0 + hG_0$ and $h_*(G + hG) = G + hG$, we have $f \circ \iota = 0$. Let $\mathcal{W}$ and $\mathcal{T}$ be the formal completions of $\mathcal{X}^{(d)}$ at $\overline{C}$ and of $\mathcal{X}^{(k_0)}$ at $\overline{G}$, which are formally smooth over R of relative dimensions d and k_0.

We first show that ι induces a closed immersion $\mathcal{T} \to \mathcal{W}$. We may check this after an unramified extension of R, so we may assume that the points of Σ_k are rational. Then $\mathcal{W}$ is the product, over the points P in the support of $\overline{C}$, of the formal completions of the symmetric powers of $\mathcal{X}$ at $n_P P$, where n_P is the multiplicity of P in $\overline{C}$, and the latter are described by the coefficients of a monic polynomial of degree n_P in a local parameter t_P at P. We choose $t_{hc} = t_c \circ h^{-1}$. For a pair $\{c, hc\}$, the polynomials of $\iota(G)$ at c and at hc are $\gamma_c \cdot \gamma$ and $\gamma_{hc} \cdot \gamma$, where γ is the polynomial of G at c and γ_c, γ_{hc} are those of C_0 at c and hc. By the choice of m_c, one of γ_c and γ_{hc} is equal to 1, so the coefficients of γ are among the coordinates of $\iota(G)$. This proves the claim. In particular, the tangent space $\mathcal{T}_0$ of $\iota(\mathcal{T})_k$ at $\overline{C}$ has dimension k_0.

The cotangent space of $\mathcal{W}_k$ at $\overline{C}$ is $H^0(\overline{C}, \Omega^1|_{\overline{C}})$, and the cotangent map of f at $\overline{C}$ is $\omega \mapsto \alpha^*\omega|_{\overline{C}}$ (see the proof of [Naj26d, Proposition 7.3]). As $f \circ \iota = 0$, the space $\mathcal{T}_0$ is contained in the annihilator of the restriction of $\alpha^* H^0(\mathcal{X}_k, \Omega^1)$ to $\overline{C}$, hence in the annihilator of the restriction of U. By assumption the latter has dimension $d - (d - k_0) = k_0$, so it is equal to $\mathcal{T}_0$.

Let $s = (s_1, \dots, s_d)$ be coordinates of $\mathcal{W}$ over R with $s(C) = 0$, choose coordinates z of the formal group of A as above, and write $z(f(E)) = \Phi(s(E))$ with $\Phi \in R[[s]]^{\dim A}$ and $\Phi(0) = 0$. As D reduces to $\overline{C}$, we have $s(D) = 2v$ with $v \in R^d$, and $\overline{v}$ is a tangent vector of $\mathcal{W}_k$ at $\overline{C}$. The point $f(D)$ is torsion and reduces to 0, and $z(f(D)) = \Phi(2v) \equiv 2Jv \pmod 4$, where J is the Jacobian matrix of Φ at 0, so $\tau(f(D)) = df(\overline{v})$. By Lemma 6.15 b), every $\omega \in H^0(\mathcal{X}_k, \Omega^1)$ satisfies

$$0 = \big((\mathcal{C}^2 - 1)\omega\big)\big(df(\overline{v})\big) = \big(\alpha^*(\mathcal{C}^2 - 1)\omega\big)|_{\overline{C}}(\overline{v}),$$

so $\overline{v}$ is annihilated by the restriction of U, and $\overline{v} \in \mathcal{T}_0$. Let t be coordinates of $\mathcal{T}$ over R with $t(G_0) = 0$. As $\overline{v}$ lies in the image of the tangent map of ι, there is $w \in R^{k_0}$ such that the point $G' \in \mathcal{T}(R)$ with $t(G') = 2w$ satisfies $s(\iota(G')) \equiv 2v = s(D) \pmod 4$. Then

$z(f(D)) = \Phi(s(D)) \equiv \Phi(s(\iota(G'))) = z(f(\iota(G'))) = 0 \pmod 4$, as Φ has coefficients in R, so $\tau(f(D)) = 0$, and $f(D) = 0$ by Lemma 6.15 a).

Finally, the restriction of $\alpha^* H^0(\mathcal{X}_k, \Omega^1)$ to $\overline{C}$ has rank at least $d - k_0$, so we can choose $d - k_0$ linear combinations $\phi_1, \dots, \phi_{d-k_0}$ of the coordinates of Φ whose differentials at 0 are linearly independent modulo 2. By the implicit function theorem for formal power series, the closed formal subscheme $\mathcal{Z} \subseteq \mathcal{W}$ defined by $\phi_1 = \cdots = \phi_{d-k_0} = 0$ is formally smooth over R of relative dimension k_0. It contains $\iota(\mathcal{T})$, which is also formally smooth of relative dimension k_0, and the tangent spaces of $\mathcal{Z}_k$ and $\iota(\mathcal{T})_k$ at $\overline{C}$ coincide. So $\iota(\mathcal{T}) = \mathcal{Z}$, as a surjective homomorphism between power series rings over R in k_0 variables is an isomorphism. As $f(D) = 0$, we have $D \in \mathcal{Z}(R) = \iota(\mathcal{T}(R))$, so $D = C_0 + G + hG$ for some G, and $C_0 \le D$. □

Lemma 6.17. *Let $F = \mathbb{Q}(\zeta_3)$, let $X = X_1(3,33)$ over F, let $h = \langle 10 \rangle$, let $\mathfrak{p}$ be the prime of F above 2, with residue field $\mathbb{F}_4$, and let $\pi : X \to Y = X_1(33)_F$ be the map $(E, P, Q) \mapsto (E, Q)$.*

a) *The numbers of non-cuspidal closed points of $X_{\mathbb{F}_4}$ of degrees $1, \dots, 5$ are 0, 0, 0, 0 and 264, and the closed cusps of $X_{\mathbb{F}_4}$ have degrees $1^{40}, 5^8$. The involution h fixes no closed cusp of $X_{\mathbb{F}_4}$, and it interchanges the cusps of degree 1 in 20 pairs and those of degree 5 in 4 pairs.*

b) *Let $U = (\mathcal{C}^2 - 1)(h^* - 1)H^0(X_{\mathbb{F}_4}, \Omega^1)$. Then $\dim U = 36$. For every effective cuspidal divisor $\overline{C}$ of degree 5 on $X_{\mathbb{F}_4}$, the restriction map $U \to H^0(\overline{C}, \Omega^1|_{\overline{C}})$ has rank $5 - k_0$, where k_0 is defined as in Lemma 6.16.*

c) *The map π sends the 264 non-cuspidal closed points of degree 5 of $X_{\mathbb{F}_4}$ onto 88 closed points of degree 5 of $Y_{\mathbb{F}_4}$, which form 12 orbits under the diamond operators.*

Proof. By [Naj26d, Lemma 7.2], the diamond operator $\langle 10 \rangle$ of $X_1(33)$ fixes no geometric cusp in characteristic 2, as $10 \equiv 1 \pmod 3$ and $10 \equiv -1 \pmod{11}$, and as $\pi \circ h = \langle 10 \rangle \circ \pi$, the involution h fixes no geometric cusp of $X_{\mathbb{F}_4}$. As h commutes with the Frobenius, it permutes the closed cusps of each degree, and it fixes none of them, as an involution of the 5 geometric points of a closed cusp of degree 5 has a fixed point. This gives the pairs in a), once we know the degrees of the closed cusps, which we compute from the description of the Galois action on the cusps. We compute the numbers of points in a) from the Frobenius polynomial of the Jacobian of $X_H(99)$ at 2, with $H = \{1, 34, 67\}$ as in the proof of Lemma 6.14. For b) we compute a model of $X_{\mathbb{F}_4}$ as a cyclic cubic cover of $X_1(33)_{\mathbb{F}_4}$: if E is written as $y^2 + A_1xy + A_3y = x^3$ with the point $11Q$ of order 3 at $(0,0)$, then adjoining a cube root r of $A_1^3 - 27A_3$ to the function field of $X_1(33)_{\mathbb{F}_4}$ gives the x-coordinate of a point of order 3 independent of $11Q$, and we check that the resulting curve has genus 81, the genus of X. On this model we compute a basis of $H^0(X_{\mathbb{F}_4}, \Omega^1)$, the matrices of $\mathcal{C}$ and h^* in this basis, and the space U. We then compute the first 5 coefficients of the local expansions of the elements of U at the 40 cusps of degree 1 and the first coefficient at the 8 cusps of degree 5. There are $\binom{44}{5} = 1086008$ effective divisors of degree 5 supported on the cusps of degree 1, and 864008, 213600 and 8400 of them have $k_0 = 0$, 1 and 2, respectively. We compute that the restriction of U to each of them has rank $5 - k_0$, and that the restriction to each of the 8 cusps of degree 5, for which $k_0 = 0$, has rank 5. Part c) is computed by running through all the elliptic curves over $\mathbb{F}_{4^5}$ with a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/33\mathbb{Z}$ and all their level structures. □

Proposition 6.18. *The group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/33\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Suppose the opposite, let F, X, h, $\mathfrak{p}$, π and Y be as in Lemma 6.17, and let D be the trace divisor, an effective F-rational divisor of degree 5 on X with non-cuspidal support. By Lemma 6.17 a), the reduction of D modulo $\mathfrak{p}$ is either an effective cuspidal divisor or a non-cuspidal closed point of degree 5.

Suppose first that D reduces to an effective cuspidal divisor $\overline{C}$. Let R be the completion of the ring of integers of F at $\mathfrak{p}$, the ring of integers of the unramified quadratic extension of $\mathbb{Q}_2$, and let $\mathcal{X}$ be the smooth model of X over R, to which h extends. The cuspidal subscheme Σ of $\mathcal{X}$ is finite étale over R and stable under h, and h fixes no closed point of $\Sigma_{\mathbb{F}_4}$ by Lemma 6.17 a). Let C be the effective divisor supported on Σ which reduces to $\overline{C}$, and let c_0 be an F-rational cusp. The class $\alpha[D-5c_0]$, where $\alpha = h_* - 1$, is torsion by Lemma 6.14, and $[C-5c_0]$ is torsion by the Manin-Drinfeld theorem, so $\alpha[D-C]$ is torsion. As $D \in X^{(5)}(F) \subseteq \mathcal{X}^{(5)}(R)$ and $(h_*-1)^* = h^* - 1$ on differentials, Lemma 6.16 and Lemma 6.17 b) give $C_0 \leq D$. As $\deg C_0 = 5 - 2k_0$ is odd, $C_0 \neq 0$, which contradicts the fact that the support of D contains no cusp.

So the reduction of D is one of the 264 non-cuspidal closed points x of degree 5 of $X_{\mathbb{F}_4}$, and the reduction of the effective F-rational divisor $M = \pi_* D$ of degree 5 on Y is the closed point $N = \pi(x)$ of degree 5. Let σ be the non-trivial automorphism of F. Then $M + M^\sigma$ is an effective rational divisor of degree 10 on $X_1(33)$, and as 2 is inert in F, its reduction modulo 2 is the divisor on $X_1(33)_{\mathbb{F}_2}$ whose base change to $\mathbb{F}_4$ is $N + N^\sigma$, where N^σ is the image of N under the Frobenius of $\mathbb{F}_4$. The group $J_1(33)(\mathbb{Q})$ is finite [DEvH+21, Theorem 3.1(2)], so by Proposition 2.2 d) the divisor $A_5(M+M^\sigma)$ is principal, and hence so is $A_5(N+N^\sigma)$. As A_5 commutes with the diamond operators, by Lemma 6.17 c) it suffices to consider 12 representatives N, and we compute that $\ell(A_5(N+N^\sigma)) = 0$ for 9 of them.

For the remaining 3 representatives we use the other elliptic curves in the isogeny class. Let (E, P, Q) be the point of $Y_1(3,33)(K)$ given by E. As the reduction of D modulo $\mathfrak{p}$ is a closed point of degree $5 = [K:F]$, there is a unique prime $\mathfrak{P}$ of K above $\mathfrak{p}$, its residue field is $\mathbb{F}_{4^5}$, and E has good reduction at $\mathfrak{P}$ (Section 2.2). As $E[3] \subseteq E(K)$, for each of the 3 subgroups $W \subseteq E[3]$ of order 3 different from the subgroup generated by $11Q$, the isogeny $\phi_W : E \to E/W$ is defined over K and $\phi_W(Q)$ has order 33. So $y_W = (E/W, \phi_W(Q))$ is a point of $Y_1(33)(K)$, and the argument above, applied to its trace divisor M_W over F, shows that the reduction of $A_5(M_W + M_W^\sigma)$ modulo 2 is principal. This reduction is determined by the reduction of y_W modulo $\mathfrak{P}$, which depends only on the reduction of (E, Q) and of W, and the construction commutes with the diamond operators. We compute that for each of the 3 remaining representatives N, the dimensions of the Riemann-Roch spaces of these reductions, for the 3 subgroups W, are $(0,0,1)$, $(1,0,0)$ and $(1,0,0)$, respectively. So in each case one of these divisors is not principal, which is a contradiction. □

6.8. **The group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}$.** The group $J_1(4,28)(\mathbb{Q}(i))$ is infinite, as over $\mathbb{Q}(i)$ the curve $X_1(4,28)$ is isomorphic to a quotient of $X_1(112)$ [DS17, Section 2], which maps to $X_0(112)$, and the elliptic curve 112.a2, a quotient of $J_0(112)$, has rank 1. So we work instead with the curve $X_1(2,28)$ over $\mathbb{Q}$, whose Jacobian has rank 0, and with four maps from it to $X_1(28)$. The additional 4-torsion is used twice: through the residue fields of the possible reductions, and through a 2-isogeny.

Lemma 6.19. *Let L be a field of characteristic different from 2 and 7, let E/L be an elliptic curve, and let $P_2, Q, U \in E(L)$ be points such that P_2 has order 2, Q has order 28, $P_2 \neq 14Q$ and $2U = P_2$. Let $\phi : E \to E'$ be the isogeny with kernel $\{0, P_2\}$. Then $\phi(U)$ has order 2, $\phi(Q)$ has order 28 and $\phi(U) \neq 14\phi(Q)$, so $(E', \phi(U), \phi(Q))$ is a point of $Y_1(2,28)(L)$.*

Proof. As $P_2 \neq 14Q$, the kernel of ϕ meets the group generated by Q trivially, so $\phi(Q)$ has order 28. We have $2\phi(U) = \phi(P_2) = 0$, and $\phi(U) \neq 0$ as $U \notin \{0, P_2\}$. The dual isogeny $\widehat{\phi}$ maps $\phi(U)$ to $2U = P_2 \neq 0$ and $14\phi(Q)$ to $28Q = 0$, so $\phi(U) \neq 14\phi(Q)$. □

Lemma 6.20. *Let $Y = X_1(2, 28)$ and $Z = X_1(28)$.*

a) *The curve Y has genus 25, $J_Y(\mathbb{Q})$ is finite and $\operatorname{gon}_{\mathbb{Q}} Y \geq 12$.*
b) *The group $J_Z(\mathbb{Q})$ is equal to $\mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}} Z$, and $J_Z(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/936\mathbb{Z}$. Its reduction modulo 3 has index 4 in $J_Z(\mathbb{F}_3) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/936\mathbb{Z}$.*
c) *The closed cusps of $Y_{\mathbb{F}_3}$ have degrees $1^{12}, 2^6, 3^4, 6^2$, and those of degrees 1 and 2 are the reductions of Galois orbits of cusps of Y over $\mathbb{Q}$ of the same degrees.*
d) *The curve $Y_{\mathbb{F}_3}$ has no non-cuspidal closed points of degree at most 4. The numbers of its non-cuspidal closed points of degrees 5, 6, 8 and 10 are 48, 64, 606 and 6384, and they form 2, 5, 29 and 272 orbits under the group of the 24 automorphisms $(P_2, Q) \mapsto (P_2 + 14bQ,\ cP_2 + aQ)$ of Y, with $b, c \in \{0, 1\}$ and $a \in \{1, 3, 5, 9, 11, 13\}$, which are defined over $\mathbb{Q}$.*

Proof. Part a) is [DEvH+21, Theorem 3.1(3)] and [NV26, Table 1], and b) is [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2] together with a computation of $J_Z(\mathbb{F}_3)$ and of the reduction of $J_Z(\mathbb{Q})$. The degrees in c) are computed directly. We compute that the cusps of Y form Galois orbits over $\mathbb{Q}$ of degrees $1^{12}, 2^6, 6^4$, and that modulo 3 the orbits of degrees 1 and 2 stay irreducible, while those of degree 6 give closed cusps of degree 3 or 6. So the 18 closed cusps of $Y_{\mathbb{F}_3}$ of degrees 1 and 2 are the reductions of the 18 Galois orbits of degrees 1 and 2. An elliptic curve over $\mathbb{F}_{3^j}$ with a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}$ has a number of points divisible by 56, which is impossible for $j \leq 4$ by the Hasse bound, as $(3^{j/2} + 1)^2 < 56$ for $j \leq 3$ and $(9 - 1)^2 = 64 > 56$ and $(9 + 1)^2 = 100 < 112$. The numbers of points and orbits in d) are computed directly. □

Proposition 6.21. *The group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Suppose the opposite, that $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z} \subseteq E(K)$ for an elliptic curve E over a number field K of degree 10. Then $\mathbb{Q}(i) \subseteq K$ by the Weil pairing. Let Y and Z be as in Lemma 6.20, choose $P_2, Q \in E(K)$ of orders 2 and 28 with $P_2 \neq 14Q$, and let D be the trace divisor of the point $(E, P_2, Q) \in Y_1(2, 28)(K)$, an effective rational divisor of degree 10 on Y with non-cuspidal support. As $J_Y(\mathbb{Q})$ is finite and $\operatorname{gon}_{\mathbb{Q}} Y \geq 12 > 10$, the reduction of D modulo 3 is not entirely cuspidal by Proposition 2.5 a). Write it as $D' + C'$ as in Section 2.5.

Let $\mathfrak{P}$ be a prime of K above 3 at which E has good reduction, with ramification index $e(\mathfrak{P})$ and residue degree $f(\mathfrak{P})$. As 3 is inert in $\mathbb{Q}(i) \subseteq K$, $f(\mathfrak{P})$ is even. The reduction $\overline{x}$ of (E, P_2, Q) modulo $\mathfrak{P}$ is a non-cuspidal closed point of $Y_{\mathbb{F}_3}$ whose degree divides $f(\mathfrak{P})$, and it occurs in the reduction of D with multiplicity at least $e(\mathfrak{P})f(\mathfrak{P})/\deg \overline{x}$ (Section 2.2). By Lemma 6.20 d), $\deg \overline{x} \geq 5$. As the numbers $e(\mathfrak{P})f(\mathfrak{P})$ add up to 10, there is exactly one such $\mathfrak{P}$, with $e(\mathfrak{P}) = 1$ and $f(\mathfrak{P}) \in \{6, 8, 10\}$, and D' is a closed point of degree 6, 8 or 10, with C' of degree 4, 2 or 0, respectively, or twice a closed point of degree 5, with $C' = 0$. If $\deg D' \in \{6, 8, 10\}$, then the residue field of D' is the residue field of $\mathfrak{P}$, and as Y is a fine moduli space, the elliptic curve of the point D' is the reduction of E modulo $\mathfrak{P}$, which has full 4-torsion over this field, as $E[4] \subseteq E(K)$. Writing this curve as $y^2 = (x - e_1)(x - e_2)(x - e_3)$, this implies that all the differences $e_i - e_j$ are squares in the residue field, by the usual description of the rational points divisible by 2 on an elliptic curve with full rational 2-torsion over a field of characteristic different from 2 (see [Sil09, Proposition X.1.4 and its

proof]). This condition depends only on the orbit of the point under the 24 automorphisms of Lemma 6.20 d), and it holds for 3 of the 5 orbits of points of degree 6, for 11 of the 29 orbits of degree 8 and for 158 of the 272 orbits of degree 10. Replacing (P_2, Q) by its image under one of these automorphisms, which gives another point of $Y_1(2,28)(K)$ with the same E, we may assume that the closed point under D' is one of the orbit representatives. This leaves $2+3+11+158 = 174$ possibilities for this point.

We now use the four maps $f_j : Y \to Z$,

$$f_1(E, P_2, Q) = (E, Q), \qquad f_3(E, P_2, Q) = (E/\langle P_2\rangle, \phi_3(Q)),$$
$$f_2(E, P_2, Q) = (E, P_2 + Q), \qquad f_4(E, P_2, Q) = (E/\langle P_2 + 14Q\rangle, \phi_4(Q)),$$

where $\langle T\rangle$ is the subgroup generated by T and ϕ_3, ϕ_4 are the quotient isogenies. They are defined over $\mathbb{Q}$, map cusps to cusps and non-cusps to non-cusps, and extend over $\mathbb{Z}_{(3)}$. By Lemma 6.20 b), (2.1) applied to each f_j, with G the reduction of $J_Z(\mathbb{Q})$, gives four necessary conditions on D', and we compute that only 19 of the 174 possibilities satisfy all four of them: 3 in which D' is a closed point of degree 8, and 16 in which it is a closed point of degree 10.

As $J_Y(\mathbb{Q})$ is finite, $[A_5(D)] = 0$ by Proposition 2.2 d), and by Lemma 6.20 c) and Lemma 2.3, $A_5(C') = 0$ whenever C' has degree at most 2. So $A_5(D')$ is principal (Section 2.5), and we compute (in six scripts `d31b_Y228_A5_v5_s`i, $i = 0, \dots, 5$, with the common part `computations/d31b_Y228_A5_common_v5.m`) that this excludes 15 of the 19 possibilities. The remaining 4 are closed points of degree 10, with $C' = 0$.

In these 4 cases we use the additional 4-torsion once more. In each of them $\mathfrak{P}$ is the only prime of K above 3, with residue field $\mathbb{F}_{3^{10}}$. As $E[4] \subseteq E(K)$, all the 4 points U with $2U = P_2$ are defined over K, and as reduction modulo $\mathfrak{P}$ is injective on $E[4]$, we may choose U such that its reduction is the point $\overline{U}$ with $2\overline{U} = \overline{P_2}$ used in the computation below. By Lemma 6.19, $x_1 = (E/\langle P_2\rangle, \phi_3(U), \phi_3(Q))$ is again a point of $Y_1(2,28)(K)$, and its trace divisor D_1 is an effective rational divisor of degree 10 on Y with non-cuspidal support. As $E/\langle P_2\rangle$ has good reduction at $\mathfrak{P}$, the reduction of D_1 modulo 3 is $(10/\deg \overline{x_1})\,\overline{x_1}$ (Section 2.2), where $\overline{x_1}$ is the closed point of $Y_{\mathbb{F}_3}$ given by the reduction of x_1 modulo $\mathfrak{P}$, and as above A_5 of this divisor has to be principal. We compute that it is not, in each of the 4 cases. This is a contradiction. □

7. The groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$

The groups $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z}$ treated here are those with $2n \in \{32, 34, 36, 38, 40, 42, 50\}$, and we show that none of them is a subgroup of the torsion of an elliptic curve over a number field of degree 10. By Lemma 4.3 this also excludes the cyclic groups $\mathbb{Z}/64\mathbb{Z}$, $\mathbb{Z}/68\mathbb{Z}$, $\mathbb{Z}/72\mathbb{Z}$, $\mathbb{Z}/76\mathbb{Z}$, $\mathbb{Z}/80\mathbb{Z}$, $\mathbb{Z}/84\mathbb{Z}$ and $\mathbb{Z}/100\mathbb{Z}$. The curves $X_1(2, 2n)$ with $2n \in \{32, 34, 36, 40, 42\}$ were used in [Naj26d, Section 11] over number fields of degree at most 9, and we follow the method used there. In all these cases the Jacobian of $X_1(2, 2n)$ has rank 0 over $\mathbb{Q}$, and we study the reduction of the trace divisor modulo $p = 3$ or $p = 5$. The entirely cuspidal reductions are excluded by Proposition 2.5, which needs $\mathrm{gon}_{\mathbb{Q}} X_1(2, 2n) > 10$. For $2n \in \{32, 34, 36\}$ Abramovich's bound does not give this, and we prove it in Lemmas 7.2, 7.10 and 7.17: for $2n = 32$ with the Castelnuovo-Severi inequality, and for $2n = 34, 36$ by specializing a hypothetical pencil of degree 10 modulo p (Lemma 7.1) and computing the short vectors in the lattice of divisors of modular units. The other reductions are excluded by pushing them forward to curves $X_1(m)$ and $X_1(2, m)$ with $m \mid 2n$, to $X_0(42)$ and to quotients of $X_1(2, 2n)$ by groups of level automorphisms (Lemma 2.16 and (2.1)), by the Hecke sieve,

and by showing that a level automorphism which fixes the reduction of the trace divisor also fixes the trace divisor, or the cuspidal part of its reduction (Lemma 2.15).

Let $X = X_1(2, N)$ with $N = 2n$. It parametrizes triples (E, P, Q) with P of order 2 and Q of order N such that $P \neq nQ$. If n is even, the maps

$$(E, P, Q) \longmapsto \big(E, P + n\varepsilon_1 Q,\ \varepsilon_2 P + aQ\big), \qquad \varepsilon_1, \varepsilon_2 \in \{0, 1\},\ a \in (\mathbb{Z}/N\mathbb{Z})^\times, \tag{7.1}$$

are level automorphisms, and taken modulo -1 they form a group of $2\varphi(N)$ automorphisms of X [Naj26d, Section 11]. If n is odd, put $P_1 = P$, $P_2 = nQ$ and $P_3 = P + nQ$. Then the maps $(E, P, Q) \mapsto (E, P_i, P_j + 2aQ)$, with $i \neq j$ and $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, are level automorphisms, and taken modulo -1 they form a group of $3\varphi(n)$ automorphisms of X, isomorphic to $\mathrm{SL}_2(\mathbb{F}_2) \times \Delta(n)$. For $N = 32, 34, 36, 38, 40, 42, 50$ these groups have $32, 48, 24, 54, 32, 36, 60$ elements. These level automorphisms are defined over $\mathbb{Q}$, so they map an effective rational divisor D of degree 10 whose support contains no cusp to another such divisor. Hence in the sieves below we may replace D by its image under a level automorphism, and, as in Section 2.5, it suffices to test one representative of each orbit of the first closed point occurring in the reduction of D, together with all the possibilities for the other closed points.

We also use the four maps $\pi_1, \dots, \pi_4 : X \to X_1(N)$ which keep Q or $P + Q$, or divide E by $\langle P \rangle$ or $\langle P + nQ \rangle$ and keep the image of Q, which has order N in all cases. Sending (E, P, Q) to $(E/\langle P \rangle, R)$, where R is one of the two points with $\widehat{\phi}(R) = Q$ for the dual $\widehat{\phi}$ of the quotient map $\phi : E \to E/\langle P \rangle$, identifies X over $\mathbb{Q}$ with the modular curve $X_\Delta(2N)$ of the group $\Delta = \{\pm 1, \pm(N + 1)\} \subseteq (\mathbb{Z}/2N\mathbb{Z})^\times$. Here R has order $2N$ as $2R = \phi(Q)$ has order N, the two choices of R differ by NR, and $\widehat{\phi}$ recovers (E, P, Q). We describe points of X over finite fields by the model

$$y^2 = x^3 + \gamma x^2 + \beta(1 - \beta - \gamma)x, \qquad P = (0, 0), \quad Q = (\beta, \beta).$$

All the class groups of curves over finite fields that we use are computed with Magma's proven class group algorithm.

By [DEvH+21, Theorem 3.1(3)], $\operatorname{rk} J_1(2, N)(\mathbb{Q}) = 0$ for all the N above. For $N = 38, 40, 42, 50$ we have $i(2, N) = 1080, 1152, 1152, 1800$, so $\operatorname{gon}_{\mathbb{C}} X \geq \frac{325}{2^{15}}\, i(2, N) > 10.7$, and hence $\operatorname{gon}_{\mathbb{Q}} X \geq \operatorname{gon}_{\mathbb{C}} X \geq 11$. For $N = 32, 34, 36$ we have $i(2, N) = 768, 864, 864$, and we prove $\operatorname{gon}_{\mathbb{Q}} X \geq 12$, 11, 11, respectively, in Lemmas 7.2, 7.10 and 7.17. So $\operatorname{gon}_{\mathbb{Q}} X > 10$ in all cases, and by Proposition 2.5 a) the reduction of the trace divisor modulo an odd prime $p \nmid N$ is not entirely cuspidal. In Table 4 we list, for each curve, its genus g, the prime p that we use, the degrees of the closed cusps of $X_{\mathbb{F}_p}$, and the numbers of non-cuspidal closed points of $X_{\mathbb{F}_p}$ of degree at most 10. We find these points by running through all the elliptic curves over $\mathbb{F}_{p^k}$, $k \leq 10$, and all their level structures, and we check the numbers against the zeta functions of the Jacobians. The scripts which carry out these computations are linked in the proofs below.

TABLE 4. Closed cusps and non-cuspidal closed points of $X_1(2,2n)_{\mathbb{F}_p}$.

X	g	p	closed cusps	non-cuspidal closed points of degree $1,\dots,10$
$X_1(2,32)$	37	3	$1^{16},2^8,4^2,8^2$	$0,0,0,0,0,192,320,960,1824,6208$
$X_1(2,34)$	49	3	$1^{24},8^3$	$0,0,0,36,48,48,144,738,2160,6504$
$X_1(2,36)$	41	5	$1^{24},2^8,6^4$	$0,0,48,120,720,2904,10416,50334,218080,979512$
$X_1(2,38)$	64	3	$1^{27},9^3$	$0,0,0,0,54,63,162,756,2270,6129$
$X_1(2,40)$	57	3	$1^{16},2^{12},4^{10}$	$0,0,0,32,96,64,480,504,2048,6000$
$X_1(2,42)$	61	5	$1^{18},2^9,3^6,6^3$	$0,0,0,126,648,2080,11376,48816,211776,983196$
$X_1(2,50)$	109	3	$1^{30},4^6,10^3$	$0,0,0,0,0,0,60,1170,1860,5040$

We will use the following lemma, which turns a lower bound for the gonality over $\mathbb{F}_p$ into a lower bound over $\mathbb{Q}$.

Lemma 7.1. *Let X be a curve over $\mathbb{Q}$ with good reduction at a prime p, let Σ be a finite set of closed points of X, and let $d \geq 1$. Assume that*

a) $\operatorname{gon}_{\mathbb{F}_p} X_{\mathbb{F}_p} \geq d$,
b) *the reduction modulo p of every effective rational divisor of degree d on X whose support is disjoint from Σ is supported on the reduction of Σ, and*
c) *every morphism $X_{\mathbb{F}_p} \to \mathbb{P}^1$ of degree d has a fibre above a point of $\mathbb{P}^1(\mathbb{F}_p)$ which is not supported on the reduction of Σ.*

Then $\operatorname{gon}_{\mathbb{Q}} X > d$.

Proof. Let $\mathcal{X}$ be the smooth proper model of X over $\mathbb{Z}_{(p)}$, and suppose that $f \in \mathbb{Q}(X)$ has degree $e \leq d$. Let $\mathcal{L}$ be the line bundle on $\mathcal{X}$ which extends $\mathcal{O}_X(f^*\infty)$, and let V be the intersection of the span of 1 and f with $H^0(\mathcal{X},\mathcal{L})$. Then V is a saturated submodule of rank 2 of the free $\mathbb{Z}_{(p)}$-module $H^0(\mathcal{X},\mathcal{L})$, so its reduction is a 2-dimensional subspace of $H^0(X_{\mathbb{F}_p},\mathcal{L}_{\mathbb{F}_p})$. It defines a morphism $X_{\mathbb{F}_p} \to \mathbb{P}^1$ of degree $e-b$, where b is the degree of its base locus, and by a) we get $e-b \geq d$. Hence $e=d$ and $b=0$, so V generates $\mathcal{L}$, and it defines a morphism $F : \mathcal{X} \to \mathbb{P}^1_{\mathbb{Z}_{(p)}}$ which extends f and whose special fibre $\overline{f}$ has degree d. By c) there is $\bar{t} \in \mathbb{P}^1(\mathbb{F}_p)$ such that $\overline{f}^*(\bar{t})$ is not supported on the reduction of Σ. Choose $t \in \mathbb{P}^1(\mathbb{Q})$ which reduces to $\bar{t}$ and does not lie in the finite set $f(\Sigma)$. Then $f^*(t)$ is an effective rational divisor of degree d whose support is disjoint from Σ, and its reduction is $\overline{f}^*(\bar{t})$, as the pull-back by F of the closure of t in $\mathbb{P}^1_{\mathbb{Z}_{(p)}}$ is the closure of $f^*(t)$ in $\mathcal{X}$. This contradicts b). □

7.1. **The curve $X_1(2,32)$.** The curve $X_1(2,32)$ has genus 37, and we work at $p=3$. We use the level automorphism $h_{32} : (E,P,Q) \mapsto (E,P,15Q)$, of order 2, and the quotient $Y_{32} = X_1(2,32)/\langle h_{32}\rangle$, with quotient map $\rho_{32} : X_1(2,32) \to Y_{32}$. The diamond operators commute with h_{32}, so they act on Y_{32}.

Lemma 7.2. *Let $X = X_1(2,32)$, let h_{32} be the level automorphism $(E,P,Q) \mapsto (E,P,15Q)$ and let $Y_{32} = X/\langle h_{32}\rangle$. Then Y_{32} has genus 13, $\operatorname{gon}_{\mathbb{Q}} Y_{32} \geq 6$ and $\operatorname{gon}_{\mathbb{Q}} X \geq 12$.*

Proof. Under the identification of X with $X_{\Delta_0}(64)$, $\Delta_0 = \{\pm 1, \pm 31\}$, described at the beginning of the section, h_{32} corresponds to the diamond operator $\langle 15\rangle$, as $\widehat{\phi}(15R) = 15Q$. Hence $Y_{32} \simeq X_{\Delta_1}(64)$ with $\Delta_1 = \{\pm 1, \pm 15, \pm 17, \pm 31\}$, and $\operatorname{gon}_{\mathbb{Q}} Y_{32} \geq 6$ by [Orl25, Proposition 2.7 and Table 2]. We compute that the groups belonging to Δ_0 and Δ_1 have index 768 and 384 in $\mathrm{PSL}_2(\mathbb{Z})$, and that the curves X and Y_{32} have genus 37 and 13. Suppose

that $f \in \mathbb{Q}(X)$ has degree $d \leq 11$. If f is the pull-back of a function on Y_{32}, this function has degree $d/2 \leq 5$, which is impossible. Otherwise $\mathbb{Q}(X)$ is generated by f and $\mathbb{Q}(Y_{32})$, as $[\mathbb{Q}(X) : \mathbb{Q}(Y_{32})] = 2$, and the Castelnuovo-Severi inequality [Sti09, Theorem 3.11.3] gives

$$37 = g(X) \leq 2g(Y_{32}) + (2-1)(d-1) = 25 + d \leq 36,$$

which is a contradiction. □

Lemma 7.3. *Let $X = X_1(2,32)$, let h_{32} and Y_{32} be as in Lemma 7.2, and let $\rho_{32} : X \to Y_{32}$ be the quotient map.*

a) *The closed cusps of $X_{\mathbb{F}_3}$ of degree 1 are the reductions of the 16 rational cusps of X, and h_{32} fixes every geometric point of the closed cusps of $X_{\mathbb{F}_3}$ of degree 2 and 4. The closed cusps of $Y_{32,\mathbb{F}_3}$ have degrees $1^8, 2^8, 4^4$, and those of degree 1 are the images of the closed cusps of degree 1 of $X_{\mathbb{F}_3}$.*

b) *Let $H_{\mathbb{Q}} \subseteq J_{Y_{32}}(\mathbb{Q})$ be the subgroup generated by the classes of the rational cuspidal divisors of degree 0. Then $J_{Y_{32}}(\mathbb{Q})$ is finite and $[J_{Y_{32}}(\mathbb{Q}) : H_{\mathbb{Q}}] \leq 2$.*

c) *We have $J_{Y_{32}}(\mathbb{F}_3) \simeq (\mathbb{Z}/2\mathbb{Z})^4 \times \mathbb{Z}/8\mathbb{Z} \times (\mathbb{Z}/40\mathbb{Z})^2 \times \mathbb{Z}/80\mathbb{Z}$, and the reduction H_{32} of $H_{\mathbb{Q}}$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z} \times (\mathbb{Z}/40\mathbb{Z})^2$. It has order 512000 and index 32.*

Proof. a) We compute the Galois orbits of cusps of X and their reductions, using the valuations of integral modular units, and we check the action of h_{32} on the cusps, using their description by Tate curves. We find 24 geometric cusps of X fixed by h_{32}, namely those in the closed cusps of $X_{\mathbb{F}_3}$ of degree 2 and 4, and we compute the cusps of Y_{32} from this.

b) The Jacobian of Y_{32} is a quotient of J_X, so $J_{Y_{32}}(\mathbb{Q})$ is finite. For the index we use the method of [DEvH+21, Section 4.3]. We work with the model of Y_{32} given by q-expansions, on which the operators A_q of Proposition 2.2 b) become $T_q - \langle q \rangle - q$ (see Section 2.3). Let M be the subgroup of $J_{Y_{32}}(\overline{\mathbb{Q}})_{\mathrm{tors}}$ killed by $T_3 - \langle 3 \rangle - 3$, $T_5 - \langle 5 \rangle - 5$ and $\tau - 1$, where τ is complex conjugation, and let $\mathcal{C} \subseteq J_{Y_{32}}(\overline{\mathbb{Q}})$ be the subgroup generated by the classes of the cuspidal divisors of degree 0. By Proposition 2.2 b), $J_{Y_{32}}(\mathbb{Q}) \subseteq M$. Using modular symbols, we compute that $\#M = 32768000$, that $[M : M \cap \mathcal{C}] = 2$, and that the subgroup of $\mathcal{C}$ fixed by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is $H_{\mathbb{Q}}$, of order 512000. Hence $J_{Y_{32}}(\mathbb{Q}) \cap \mathcal{C} = H_{\mathbb{Q}}$, and $[J_{Y_{32}}(\mathbb{Q}) : H_{\mathbb{Q}}] \leq [M : M \cap \mathcal{C}] = 2$.

c) The curve Y_{32} is the double cover of $X_1(2,16)$ obtained by adjoining w with $w^2 = x(Q_{16}) - x(8Q_{16})$, where (E, P, Q_{16}) is the universal triple over $X_1(2,16)$ in the model above, and we compute $J_{Y_{32}}(\mathbb{F}_3)$ from this model. The 20 closed cusps of $Y_{32,\mathbb{F}_3}$ come from 17 Galois orbits of cusps of Y_{32} over $\mathbb{Q}$, which we identify using the valuations of integral modular units, and we compute the subgroup H_{32} generated by the reductions of these orbits. □

Lemma 7.4. *Let $X = X_1(2,32)$ and let D be an effective rational divisor of degree 10 on X whose support contains no cusp. Suppose that the reduction of D modulo 3 is not entirely cuspidal. Then there is a level automorphism g of X such that the reduction of gD is $x_{32} + C'$, where C' is an effective cuspidal divisor of degree 4 with no closed cusp of degree 1 in its support, and x_{32} is the closed point of degree 6 of $X_{\mathbb{F}_3}$ represented by*

$$\beta = \theta^5, \qquad \gamma = 1 + \theta^2 + \theta^3 + 2\theta^4 + \theta^5, \qquad \text{where } \theta^6 + 2\theta^4 + \theta^2 + 2\theta + 2 = 0.$$

Proof. Write the reduction of D as $D' + C'$ as in Section 2.5, with $D' \neq 0$ of degree e. By Table 4, $X_{\mathbb{F}_3}$ has no non-cuspidal closed points of degree at most 5, so D' is a single closed point of degree $e \in \{6, \ldots, 10\}$. Up to the 32 level automorphisms there are $8, 10, 32, 57, 198$

such points of degree $6, 7, 8, 9, 10$, which we compute, and we replace D by its image under a level automorphism to make D' one of these 305 representatives. The group $J_1(32)(\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z} \times \mathbb{Z}/11640\mathbb{Z}$ is generated by rational cuspidal divisor classes [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], and we compute that its reduction G has index 68 in $J_1(32)(\mathbb{F}_3) \simeq (\mathbb{Z}/2\mathbb{Z})^3 \times (\mathbb{Z}/4\mathbb{Z})^2 \times \mathbb{Z}/120\mathbb{Z} \times \mathbb{Z}/197880\mathbb{Z}$. We apply (2.1) to the four maps $\pi_1, \dots, \pi_4$, allowing all the effective cuspidal divisors on $X_1(32)_{\mathbb{F}_3}$, and we compute that only one of the 305 cases passes all four tests, the point x_{32}. So $D' = x_{32}$ and C' has degree 4. We also compute that, in the notation of (2.1) with a rational cusp y_0 of $X_1(32)$, $[\pi_{i*}x_{32} - 6\overline{y_0}] \notin G + \mathcal{S}_3$ for $i = 1, \dots, 4$.

Suppose that C' contains a closed cusp of degree 1. By Lemma 7.3 a) it is the reduction $\overline{c}$ of a rational cusp c of X. The class $[\pi_{1*}(D - c) - 9y_0]$ lies in $J_1(32)(\mathbb{Q})$, and its reduction is $[\pi_{1*}x_{32} + \pi_{1*}(C' - \overline{c}) - 9\overline{y_0}]$, where $\pi_{1*}(C' - \overline{c})$ is an effective cuspidal divisor of degree 3. Hence $[\pi_{1*}x_{32} - 6\overline{y_0}] \in G + \mathcal{S}_3$, which is a contradiction. □

Lemma 7.5. *Let X, h_{32}, Y_{32}, ρ_{32} and H_{32} be as in Lemma 7.3, let x_{32} be the closed point of $X_{\mathbb{F}_3}$ of Lemma 7.4, and let $\overline{c_*}$ be a closed cusp of degree 1 of $Y_{32,\mathbb{F}_3}$. Then $h_{32}x_{32} = x_{32}$, and $y_{32} := \rho_{32}(x_{32})$ is a closed point of degree 3 with $\rho_{32}^* y_{32} = x_{32}$. For $a \in \{1, 3\}$ let $\mathcal{T}_a$ be the set of the elements z of $J_{Y_{32}}(\mathbb{F}_3)/H_{32}$ with $2z = 0$ which are the classes of the divisors $\langle a \rangle y_{32} + c - 5\overline{c_*}$, with c a closed cusp of degree 2 of $Y_{32,\mathbb{F}_3}$. Then $\mathcal{T}_1 \cap \mathcal{T}_3 = \emptyset$.*

Proof. We check that h_{32} acts on the geometric points of x_{32} as the third power of the Frobenius, which proves the first two claims. In a basis of $J_{Y_{32}}(\mathbb{F}_3)/H_{32} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ we compute

$$\mathcal{T}_1 = \{(1, 1, 0), (1, 0, 4)\} \qquad \text{and} \qquad \mathcal{T}_3 = \{(1, 1, 4), (1, 0, 0)\}.$$

□

Proposition 7.6. *The groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/32\mathbb{Z}$ and $\mathbb{Z}/64\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let $X = X_1(2, 32)$, and let D be the trace divisor of a point of $Y_1(2, 32)$ over a number field of degree 10. As $J_X(\mathbb{Q})$ is finite and $\operatorname{gon}_{\mathbb{Q}} X \geq 12$ by Lemma 7.2, the reduction of D modulo 3 is not entirely cuspidal by Proposition 2.5 a). By Lemma 7.4, after replacing D by its image under a level automorphism, the reduction of D is $x_{32} + C'$, where C' is an effective cuspidal divisor of degree 4 supported on closed cusps of degree 2 and 4. By Lemma 7.3 a) and Lemma 7.5, h_{32} fixes C' and x_{32}, so it fixes the reduction of D, and Lemma 2.10 a), with $C = 0$ and $\operatorname{gon}_{\mathbb{Q}} X > 10$, gives $h_{32}D = D$. By Lemma 2.14, the points in the support of D correspond to elliptic curves without complex multiplication, so by Lemma 2.9 the geometric points in the support of D form orbits of length 2 under h_{32}, on which the coefficients of D are constant. So $D = \rho_{32}^* B$ for an effective rational divisor B of degree 5 on Y_{32}. Its reduction $\overline{B}$ satisfies $\rho_{32}^* \overline{B} = x_{32} + C'$, and as $\rho_{32}^* y_{32} = x_{32}$, we get $\overline{B} = y_{32} + C_Y$ for an effective cuspidal divisor C_Y of degree 2 with $\rho_{32}^* C_Y = C'$. If C_Y contained a closed cusp of degree 1, then so would C', by Lemma 7.3 a). So C_Y is a closed cusp of degree 2.

By Lemma 7.3 a), $\overline{c_*}$ is the reduction of a rational cusp c_* of Y_{32}. Let $H_{\mathbb{Q}}$ be as in Lemma 7.3 b). Reduction modulo 3 is injective on $J_{Y_{32}}(\mathbb{Q})$ and maps $H_{\mathbb{Q}}$ onto H_{32}, and $[J_{Y_{32}}(\mathbb{Q}) : H_{\mathbb{Q}}] \leq 2$, so the class z of $[\overline{B} - 5\overline{c_*}]$ modulo H_{32} satisfies $2z = 0$, and $z \in \mathcal{T}_1$. The diamond operator $\langle 3 \rangle$ is an automorphism of Y_{32} defined over $\mathbb{Q}$ which maps cusps to cusps, so it acts on $J_{Y_{32}}(\mathbb{Q})/H_{\mathbb{Q}}$, trivially as this group has order at most 2. As $[\langle 3 \rangle c_* - c_*] \in H_{\mathbb{Q}}$,

it follows that $[\langle 3\rangle B - 5c_*] - [B - 5c_*] \in H_{\mathbb{Q}}$, so z is also the class of $[\langle 3\rangle y_{32} + \langle 3\rangle C_Y - 5\overline{c_*}]$. As $\langle 3\rangle C_Y$ is a closed cusp of degree 2, we get $z \in \mathcal{T}_3$, which contradicts Lemma 7.5. Finally, $\mathbb{Z}/64\mathbb{Z}$ is excluded by Lemma 4.3. □

7.2. **The curve $X_1(2,34)$.** The curve $X_1(2,34)$ has genus 49, and we work at $p = 3$. We compute that its cusps over $\mathbb{Q}$ form 24 rational cusps and 3 Galois orbits of length 8. The closed cusps of $X_1(2,34)_{\mathbb{F}_3}$ have degrees $1^{24}, 8^3$, so those of degree 1 are the reductions of the rational cusps. Abramovich's bound gives only $\operatorname{gon}_{\mathbb{C}} X_1(2,34) \geq 9$, and we have $\operatorname{gon}_{\mathbb{F}_3} X_1(2,34) \geq 10$ by [NV26, Table 1].

Lemma 7.7. *Let $X = X_1(2,34)$. The reduction modulo 3 of every effective rational divisor of degree 10 on X is supported on the cusps.*

Proof. Let D be such a divisor, and suppose that its reduction is $D' + C'$ as in Section 2.5, with $D' \neq 0$ of degree e. By Table 4, the type of D' is one of $[4], \dots, [10]$, $[4,4]$, $[4,5]$, $[4,6]$ and $[5,5]$. Up to the 48 level automorphisms, the non-cuspidal closed points of degree $4, \dots, 10$ form $2, 1, 2, 3, 18, 45, 138$ orbits, which we compute. Normalizing the first point of D' and taking all the 36, 48, 48 and 48 possibilities for the second point in the types $[4,4]$, $[4,5]$, $[4,6]$ and $[5,5]$, we get $209 + 72 + 96 + 96 + 48 = 521$ cases. The group $J_1(34)(\mathbb{Q}) \simeq \mathbb{Z}/8760\mathbb{Z} \times \mathbb{Z}/595680\mathbb{Z}$ is generated by rational cuspidal divisor classes [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], and we compute that its reduction G has index 128 in $J_1(34)(\mathbb{F}_3) \simeq (\mathbb{Z}/4\mathbb{Z})^3 \times \mathbb{Z}/8760\mathbb{Z} \times \mathbb{Z}/1191360\mathbb{Z}$ and contains the classes of all the cuspidal divisors on $X_1(34)_{\mathbb{F}_3}$. So Lemma 2.16, applied to $\pi_{i*}D$ as in (2.1), gives $[\pi_{i*}D' - e\,\overline{y_0}] \in G$ for $i = 1, \dots, 4$, and we compute that each of the 521 cases fails this for one of the four maps. □

Lemma 7.8. *Let $c_1, \dots, c_{24}$ be the rational cusps of $X = X_1(2,34)$. If $f \in \mathbb{Q}(X)$ is not constant and $\operatorname{div}(f) = \sum_i a_i c_i$, then $\sum_i a_i^2 > 60$.*

Proof. We use the identification of X with $X_\Delta(68)$, $\Delta = \{\pm 1, \pm 33\}$, described at the beginning of the section. A cuspidal divisor of degree 0 is principal if and only if its image under the Abel-Jacobi map, which we compute with modular symbols, lies in the period lattice. This gives the lattice of the principal divisors supported on the cusps, and we compute its intersection with the group of divisors supported on $c_1, \dots, c_{24}$, a lattice of rank 23 in $\mathbb{Z}^{24}$. We compute that it contains no non-zero vector of squared norm at most 60. A function over $\overline{\mathbb{Q}}$ whose divisor is supported on rational points is a constant multiple of a function over $\mathbb{Q}$, so this proves the claim. □

Lemma 7.9. *Let $X = X_1(2,34)$. Every morphism $X_{\mathbb{F}_3} \to \mathbb{P}^1$ of degree 10 has a fibre above a point of $\mathbb{P}^1(\mathbb{F}_3)$ whose support contains a non-cuspidal point.*

Proof. Suppose that $\overline{f} : X_{\mathbb{F}_3} \to \mathbb{P}^1$ has degree 10 and that its fibres $A_1, \dots, A_4$ above the four points of $\mathbb{P}^1(\mathbb{F}_3)$ are cuspidal. By Table 4, $X(\mathbb{F}_3)$ consists of 24 cusps, and each of them lies in exactly one A_i. Let n_i be the number of these cusps in A_i, and order the fibres with $n_1 \geq \cdots \geq n_4$. Then $\sum_i n_i = 24$ and $n_i \leq 10$, so $n_1 \geq 6$ and $n_2 \geq \lceil (24 - n_1)/3 \rceil \geq 5$. The other closed cusps have degree $8 > 10 - 5$, so A_1 and A_2 are supported on rational points. An effective divisor of degree 10 supported on exactly n rational points has squared norm $\sum_i a_i^2 \leq (11 - n)^2 + n - 1$, and checking the possibilities $6 \leq n_1 \leq 10$ and $\lceil (24 - n_1)/3 \rceil \leq n_2 \leq n_1$, we find that the squared norm of $A_1 - A_2$ is at most 60, as A_1 and A_2 have disjoint supports. The divisor $A_1 - A_2$ is principal, and it is the reduction of a rational cuspidal divisor A of degree 0, as the closed cusps of degree 1 of $X_{\mathbb{F}_3}$ are the reductions of the rational

cusps. The class $[A]$ lies in the finite group $J_X(\mathbb{Q})$ and reduces to 0, so $[A] = 0$ by Katz's result, and A is the divisor of a function as in Lemma 7.8 with $\sum_i a_i^2 \leq 60$, which is a contradiction. □

Lemma 7.10. *We have* $\operatorname{gon}_{\mathbb{Q}} X_1(2,34) \geq 11$.

Proof. We apply Lemma 7.1 to $X = X_1(2,34)$ with $p = 3$, $d = 10$ and Σ the set of cusps. Condition a) holds as $\operatorname{gon}_{\mathbb{F}_3} X \geq 10$ [NV26, Table 1], condition b) is Lemma 7.7, and condition c) is Lemma 7.9. □

Proposition 7.11. *The groups* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/34\mathbb{Z}$ *and* $\mathbb{Z}/68\mathbb{Z}$ *are not subgroups of the torsion of an elliptic curve over a number field of degree* 10.

Proof. Let D be the trace divisor of a point of $Y_1(2,34)$ over a number field of degree 10. As $J_1(2,34)(\mathbb{Q})$ is finite and $\operatorname{gon}_{\mathbb{Q}} X_1(2,34) > 10$ by Lemma 7.10, the reduction of D modulo 3 is not entirely cuspidal by Proposition 2.5 a). This contradicts Lemma 7.7. Finally, $\mathbb{Z}/68\mathbb{Z}$ is excluded by Lemma 4.3. □

7.3. **The curve $X_1(2,36)$.** The curve $X_1(2,36)$ has genus 41, and we work at $p = 5$. We use the two maps $X_1(2,36) \to X_1(2,18)$ given by $(E,P,Q) \mapsto (E,P,2Q)$ and $(E,P,Q) \mapsto (E/\langle 18Q\rangle, \phi(P), \phi(Q))$, where $\phi : E \to E/\langle 18Q\rangle$ is the quotient map, the four maps $\pi_1, \dots, \pi_4$ to $X_1(36)$, and two quotients of $X_1(2,36)$ which were also used in [Naj26d, Section 11.5]. The first one is the following.

Lemma 7.12 ([Naj26d, Lemma 11.8 and its proof])**.** *Let* $X = X_1(2,36)$*, let* h_{36} *be the level automorphism* $(E,P,Q) \mapsto (E,P,13Q)$*, of order* 3*, and let* $Z_{36} = X/\langle h_{36}\rangle$*, a curve of genus* 9*. The classes of the cuspidal divisors of degree* 0 *on* $Z_{36,\mathbb{F}_5}$ *generate a subgroup* $H_{36} \simeq (\mathbb{Z}/3\mathbb{Z})^3 \times (\mathbb{Z}/24\mathbb{Z})^3$ *of index* 8 *of* $J_{Z_{36}}(\mathbb{F}_5) \simeq (\mathbb{Z}/3\mathbb{Z})^3 \times (\mathbb{Z}/24\mathbb{Z})^2 \times \mathbb{Z}/192\mathbb{Z}$*, and* H_{36} *contains the reduction modulo* 5 *of* $J_{Z_{36}}(\mathbb{Q})$.

For the second one, let g_{36} be the level automorphism $(E,P,Q) \mapsto (E, P+18Q, P+Q)$ of $X_1(2,36)$, of order 4, with $g_{36}^2(E,P,Q) = (E,P,19Q)$. By [Naj26d, Section 11.5], the group generated by g_{36} acts freely on the non-cuspidal points of $X_1(2,36)$ and acts on the cusps with orbits of length 4, so the quotient $W_{36} = X_1(2,36)/\langle g_{36}\rangle$ is a curve of genus 11 and the quotient map $\rho_{36} : X_1(2,36) \to W_{36}$ is unramified. Let t_9 be the parameter of $X_1(9)$ in Tate normal form,

$$r_9 = t_9^2 - t_9 + 1, \quad c_9 = t_9(r_9 - 1), \quad b_9 = r_9 c_9, \quad E_9 : y^2 + (1 - c_9)xy - b_9 y = x^3 - b_9 x^2,$$

and $j_9(t_9) = j(E_9)$. By [Naj26d, Section 11.5], the function t_9 of $(E,4Q)$ and the function $w_{36} = 4(x(9Q) - x(18Q))/(x(P) - x(P+18Q))$ are invariant under g_{36}, and $\mathbb{Q}(W_{36}) = \mathbb{Q}(t_9, w_{36})$ with $16(w_{36}^2 + 16)^3 = j_9(t_9) w_{36}^4$.

Lemma 7.13. *Let* $X = X_1(2,36)$ *and let* D *be an effective rational divisor of degree* 10 *on* X *whose support contains no cusp. Suppose that the reduction of* D *modulo* 5 *is not entirely cuspidal. Then there is a level automorphism* g *of* X *such that the reduction of* gD *is* $x_{36} + C'$*, where* C' *is an effective cuspidal divisor of degree* 2 *and* x_{36} *is the closed point of degree* 8 *of* $X_{\mathbb{F}_5}$ *represented by*

$$\beta = 2\theta^4 + 3\theta^5 + 4\theta^7, \qquad \gamma = 2 + \theta + 4\theta^3 + 2\theta^5 + \theta^6 + 2\theta^7, \qquad \text{where } \theta^8 + \theta^4 + 3\theta^2 + 4\theta + 2 = 0.$$

Proof. Write the reduction of D as $D' + C'$ as in Section 2.5, with $D' \neq 0$ of degree e. By Table 4, the type of D' is one of $[3], \dots, [10]$, $[3,3]$, $[3,4]$, $[3,5]$, $[3,6]$, $[3,7]$, $[4,4]$, $[4,5]$, $[4,6]$, $[5,5]$, $[3,3,3]$ and $[3,3,4]$. Up to the 24 level automorphisms, the non-cuspidal closed

points of degree $3, \dots, 10$ form $2, 5, 30, 126, 434, 2115, 9088, 40874$ orbits, which we compute. Normalizing one point of D' and taking all the possibilities for the other points, we get 135282 cases. We apply the following three tests, each of them an instance of (2.1).

a) The group $J_1(2,18)(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/42\mathbb{Z} \times \mathbb{Z}/126\mathbb{Z}$ is generated by rational cuspidal divisor classes [DEvH+21, Proposition 4.16 and Table 3], and we compute that its reduction has index 12 in $J_1(2,18)(\mathbb{F}_5) \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z} \times \mathbb{Z}/252\mathbb{Z}$ and contains the classes of all the cuspidal divisors. We compute that only 1251 cases pass the test with both maps to $X_1(2,18)$.

b) By Lemma 7.12, the class of the push-forward of D' to $Z_{36,\mathbb{F}_5}$, relative to a rational cusp, lies in H_{36}. We compute that only 208 of the 1251 cases pass this test.

c) The group $J_1(36)(\mathbb{Q}) \simeq \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/252\mathbb{Z} \times \mathbb{Z}/7812\mathbb{Z}$ is generated by rational cuspidal divisor classes [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], and we compute that its reduction G has index 214272 in $J_1(36)(\mathbb{F}_5) \simeq (\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/12\mathbb{Z})^2 \times \mathbb{Z}/36\mathbb{Z} \times (\mathbb{Z}/7812\mathbb{Z})^2$, and that the images of the sets $\mathcal{S}_0, \dots, \mathcal{S}_7$ of (2.1) in $J_1(36)(\mathbb{F}_5)/G$ have $1, 7, 27, 77, 181, 273, 279, 279$ elements. We compute that only one of the 208 cases passes the test with the four maps $\pi_1, \dots, \pi_4$, the point x_{36} with a cuspidal part of degree 2.

Hence $D' = x_{36}$ and $\deg C' = 2$. □

Lemma 7.14. *Let $X = X_1(2,36)$, let g_{36}, W_{36} and ρ_{36} be as above, and let x_{36} be the closed point of $X_{\mathbb{F}_5}$ of Lemma 7.13. Then $g_{36}x_{36} = x_{36}$, and*

$$\ell\Big(x_{36} + \sum_{j=0}^{3} g_{36}^j C'\Big) = 1$$

on $X_{\mathbb{F}_5}$ for every effective cuspidal divisor C' of degree 2 on $X_{\mathbb{F}_5}$.

Proof. The automorphism g_{36} acts on the geometric points of x_{36} as the sixth power of the Frobenius, as we compute, so it fixes x_{36}, and $x_{36} = \rho_{36}^* z_{36}$ for a closed point z_{36} of degree 2 of $W_{36,\mathbb{F}_5}$. After completing the square in E_9, write its equation as $y^2 = x^3 + a_2x^2 + a_4x + a_6$. The cubic $x^3 + a_2x^2 + a_4x + a_6$ and the polynomial $w_{36}^2(a_2+3x)^2 - 4(w_{36}^2+4)(a_4+2a_2x+3x^2)$ have a unique common root ξ. Put $\kappa = a_4 + 2a_2\xi + 3\xi^2$ and $\Phi_{36} = 16\kappa^3(1 + 4/w_{36})^2$. Over $\mathbb{F}_5$ the cover ρ_{36} is given by $z^4 = \Phi_{36}$, and we check that $\operatorname{div}(\Phi_{36}) = 4\Lambda_{36}$ with $[\Lambda_{36}]$ of order 4. Hence

$$\ell_X(\rho_{36}^*\Theta) = \sum_{j=0}^{3} \ell_{W_{36}}(\Theta + j\Lambda_{36})$$

for every divisor Θ on $W_{36,\mathbb{F}_5}$.

The closed cusps of $X_{\mathbb{F}_5}$ of degree 1 form 6 orbits of length 4 under g_{36}, which map to 6 closed cusps $c_1, \dots, c_6$ of degree 1 of $W_{36,\mathbb{F}_5}$, and the closed cusps of degree 2 form 2 orbits of length 4, which map to 2 closed cusps u_1, u_2 of degree 2. As g_{36} acts freely on the cusps, we have $\sum_j g_{36}^j C' = \rho_{36}^*\rho_{36*}C'$, and $\rho_{36*}C'$ is one of the 21 divisors $c_i + c_k$ with $1 \le i \le k \le 6$ or one of u_1, u_2. In all these 23 cases we compute that $\ell_{W_{36}}(z_{36} + \rho_{36*}C' + j\Lambda_{36}) = 1, 0, 0, 0$ for $j = 0, 1, 2, 3$. Hence $\ell_X(x_{36} + \sum_j g_{36}^j C') = \ell_X(\rho_{36}^*(z_{36} + \rho_{36*}C')) = 1$. □

Lemma 7.15. *Let $X = X_1(2,36)$. The reduction modulo 5 of every effective rational divisor of degree 10 on X whose support contains no cusp is supported on the cusps.*

Proof. Let D be such a divisor, and suppose that its reduction is not supported on the cusps. By Lemma 7.13, after replacing D by its image under a level automorphism, the reduction

of D is $x_{36} + C'$ with C' effective cuspidal of degree 2. By Lemma 7.14, g_{36} fixes x_{36} and $\ell(x_{36} + \sum_{j=0}^{3} g_{36}^j C') = 1$, and g_{36} acts on the geometric cusps with orbits of length 4. As $J_X(\mathbb{Q})$ is finite, Lemma 2.15 gives $4 \mid \deg C' = 2$, which is a contradiction. □

Lemma 7.16. *Let $X = X_1(2, 36)$. Every morphism $X_{\mathbb{F}_5} \to \mathbb{P}^1$ of degree 10 has a fibre above a point of $\mathbb{P}^1(\mathbb{F}_5)$ whose support contains a non-cuspidal point.*

Proof. Suppose that $\overline{f} : X_{\mathbb{F}_5} \to \mathbb{P}^1$ has degree 10 and that its fibres $A_1, \dots, A_6$ above the six points of $\mathbb{P}^1(\mathbb{F}_5)$ are cuspidal. By Table 4, $X(\mathbb{F}_5)$ consists of 24 cusps, and each of them lies in exactly one A_i. Let n_i be the number of these cusps in A_i, and order the fibres with $n_1 \geq \cdots \geq n_6$. Then $\sum_i n_i = 24$, so $n_1 \geq 4$ and $n_2 \geq \lceil (24 - n_1)/5 \rceil$. For a cuspidal divisor $A = \sum_c m_c c$ on $X_{\mathbb{F}_5}$, the sum being over the closed cusps, put $\|A\|^2 = \sum_c \deg(c) m_c^2$, which is the squared norm of the corresponding divisor on the 64 geometric cusps. If A is effective of degree 10 and contains exactly n closed cusps of degree 1, then $\|A\|^2 \leq (11-n)^2 + n - 1$. Checking the possibilities for $4 \leq n_1 \leq 10$ and n_2, we find $\|A_1 - A_2\|^2 \leq 104$, as A_1 and A_2 have disjoint supports.

The closed cusps of $X_{\mathbb{F}_5}$ are the reductions of the orbits of the Frobenius automorphism σ_5 on the geometric cusps of X, which are defined over $\mathbb{Q}(\zeta_{36})$. Let A be the cuspidal divisor over $\mathbb{Q}(\zeta_{36})$ which reduces to the principal divisor $A_1 - A_2$ and has the same multiplicities on each σ_5-orbit. Its class is torsion by the Manin-Drinfeld theorem and reduces to 0 modulo a prime above 5, so A is principal by Katz's result. So the vector of multiplicities of A lies in the lattice of principal divisors supported on the 64 geometric cusps and fixed by σ_5. Using the identification of X with $X_\Delta(72)$, $\Delta = \{\pm 1, \pm 35\}$, and modular symbols as in the proof of Lemma 7.8, we compute this lattice, which has rank 35, and we compute that it contains 24552 pairs $\pm v$ of non-zero vectors of squared norm at most 104, none of which has positive part of degree 10. As the positive part of A is A_1, of degree 10, this is a contradiction. □

Lemma 7.17. *We have* $\operatorname{gon}_{\mathbb{Q}} X_1(2, 36) \geq 11$.

Proof. We apply Lemma 7.1 to $X = X_1(2, 36)$ with $p = 5$, $d = 10$ and Σ the set of cusps. Condition a) holds as $\operatorname{gon}_{\mathbb{F}_5} X \geq 10$ [NV26, Table 1], condition b) is Lemma 7.15, and condition c) is Lemma 7.16. □

Proposition 7.18. *The groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$ and $\mathbb{Z}/72\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let D be the trace divisor of a point of $Y_1(2, 36)$ over a number field of degree 10. As $J_1(2, 36)(\mathbb{Q})$ is finite and $\operatorname{gon}_{\mathbb{Q}} X_1(2, 36) > 10$ by Lemma 7.17, the reduction of D modulo 5 is not entirely cuspidal by Proposition 2.5 a). This contradicts Lemma 7.15. Finally, $\mathbb{Z}/72\mathbb{Z}$ is excluded by Lemma 4.3. □

7.4. **The curves $X_1(2, 38)$, $X_1(2, 40)$ and $X_1(2, 50)$.** For these three curves we work at $p = 3$, and the push-forwards to smaller levels, followed by the Hecke sieve on $X_1(38)$ and $X_1(50)$, exclude all the reductions of the trace divisor which are not entirely cuspidal.

Lemma 7.19. *Let $X = X_1(2, 38)$. The reduction modulo 3 of every effective rational divisor of degree 10 on X whose support contains no cusp is supported on the cusps.*

Proof. Let D be such a divisor, and suppose that its reduction is $D' + C'$ as in Section 2.5, with $D' \neq 0$ of degree e. By Table 4, the type of D' is one of $[5], \dots, [10]$ and $[5, 5]$. Up to the 54 level automorphisms, the non-cuspidal closed points of degree $5, \dots, 10$ form $1, 2, 3, 14, 43, 116$ orbits, which we compute, and normalizing the first point and taking all

the 54 possibilities for the second point in the type $[5,5]$, we get $179+54=233$ cases. Put $V=2Q$, of order 19. We use the four maps $X\to X_1(19)$ which keep V, or divide E by $\langle P\rangle$, $\langle 19Q\rangle$ or $\langle P+19Q\rangle$ and keep the image of V. The group $J_1(19)(\mathbb{Q})\simeq\mathbb{Z}/4383\mathbb{Z}$ is generated by rational cuspidal divisor classes [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], and its reduction G has index 2 in $J_1(19)(\mathbb{F}_3)\simeq\mathbb{Z}/8766\mathbb{Z}$ and contains the classes of all the cuspidal divisors. We compute that only 35 cases satisfy (2.1) for all four maps: one of type $[8]$, two of type $[9]$, fourteen of type $[10]$ and eighteen of type $[5,5]$. In all of them $\deg C'\le 2$.

For these we use the map $\pi_1: X\to X_1(38)$, $(E,P,Q)\mapsto(E,Q)$. We compute that the closed cusps of $X_1(38)_{\mathbb{F}_3}$ have degrees $1^{18},9^2$, and that those of degree 1 are the reductions of rational cusps. So $\pi_{1*}C'$ is the reduction of a rational cuspidal divisor, and $A_5(\pi_{1*}C')=0$ by Proposition 2.2 c). As $J_1(38)(\mathbb{Q})$ is finite [DEvH+21, Theorem 3.1(2)], Proposition 2.2 d) shows that $A_5(\pi_{1*}D)$ is principal, and hence so is $A_5(\pi_{1*}D')$. We compute that $A_5(\pi_{1*}D')$ is not principal in all 35 cases, which is a contradiction. □

Lemma 7.20. *Let $X=X_1(2,40)$. The reduction modulo 3 of every effective rational divisor of degree 10 on X whose support contains no cusp is supported on the cusps.*

Proof. Let D be such a divisor, and suppose that its reduction is $D'+C'$ as in Section 2.5, with $D'\neq 0$ of degree e. By Table 4, the type of D' is one of $[4],\dots,[10]$, $[4,4]$, $[4,5]$, $[4,6]$ and $[5,5]$. Up to the 32 level automorphisms (7.1), the non-cuspidal closed points of degree $4,\dots,10$ form $1,3,2,15,21,64,195$ orbits, which we compute. Normalizing the first point and taking all the possibilities for the second one, we get 301 cases with one point and $32+96+64+288=480$ cases with two points, 781 in total. We use the maps $X\to X_1(2,20)$ given by $(E,P,Q)\mapsto(E,P,2Q)$ and by $(E,P,Q)\mapsto(E/\langle 20Q\rangle,\phi(P),\phi(Q))$, where $\phi: E\to E/\langle 20Q\rangle$ is the quotient map. The group $J_1(2,20)(\mathbb{Q})\simeq\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/60\mathbb{Z}\times\mathbb{Z}/120\mathbb{Z}$ is generated by rational cuspidal divisor classes [DEvH+21, Proposition 4.16 and Table 3], and its reduction has index 4 in $J_1(2,20)(\mathbb{F}_3)\simeq\mathbb{Z}/8\mathbb{Z}\times(\mathbb{Z}/120\mathbb{Z})^2$ and contains the classes of all the cuspidal divisors. We compute that only 288 of the 781 cases satisfy (2.1) for the first map, and we compute that only 118 of these 288 cases satisfy it for the second map. For these we use the four maps $\pi_1,\dots,\pi_4$ to $X_1(40)$. The group $J_1(40)(\mathbb{Q})\simeq(\mathbb{Z}/2\mathbb{Z})^3\times\mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/120\mathbb{Z}\times\mathbb{Z}/895440\mathbb{Z}$ is generated by rational cuspidal divisor classes [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], its reduction G has index 4592 in $J_1(40)(\mathbb{F}_3)\simeq(\mathbb{Z}/2\mathbb{Z})^5\times\mathbb{Z}/16\mathbb{Z}\times\mathbb{Z}/68880\mathbb{Z}\times\mathbb{Z}/895440\mathbb{Z}$, and we compute that each of the 118 cases fails (2.1), with all the effective cuspidal divisors on $X_1(40)_{\mathbb{F}_3}$ allowed, for one of the four maps. □

Lemma 7.21. *Let $X=X_1(2,50)$. The reduction modulo 3 of every effective rational divisor of degree 10 on X whose support contains no cusp is supported on the cusps.*

Proof. Let D be such a divisor, and suppose that its reduction is $D'+C'$ as in Section 2.5, with $D'\neq 0$ of degree e. By Table 4, D' is a single closed point of degree $7,\dots,10$, and up to the 60 level automorphisms there are $1,21,31,84$ of them, which we compute, 137 cases in total. We use the four maps $X\to X_1(25)$ which keep $2Q$ on E or on its quotients by its three subgroups of order 2. The group $J_1(25)(\mathbb{Q})\simeq\mathbb{Z}/227555\mathbb{Z}$ is generated by rational cuspidal divisor classes [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], and its reduction has index 11 in $J_1(25)(\mathbb{F}_3)\simeq\mathbb{Z}/2503105\mathbb{Z}$ and contains the classes of all the cuspidal divisors. We compute that only 3 cases satisfy (2.1) for all four maps, each of them a closed point of degree 8, and hence $\deg C'=2$.

For these we use the map $\pi_1 : X \to X_1(50)$, $(E, P, Q) \mapsto (E, Q)$. We compute that the closed cusps of $X_1(50)_{\mathbb{F}_3}$ have degrees $1^{20}, 4^4, 10^2$, and that those of degree 1 are the reductions of rational cusps. So $\pi_{1*}C'$ is the reduction of a rational cuspidal divisor, and $A_7(\pi_{1*}C') = 0$ by Proposition 2.2 c). As $J_1(50)(\mathbb{Q})$ is finite [DEvH+21, Theorem 3.1(2)], $A_7(\pi_{1*}D')$ is principal by Proposition 2.2 d). We compute that $A_7(\pi_{1*}D')$ is not principal in all 3 cases, which is a contradiction. □

Proposition 7.22. *The groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/38\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/40\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$, $\mathbb{Z}/76\mathbb{Z}$, $\mathbb{Z}/80\mathbb{Z}$ and $\mathbb{Z}/100\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let $N \in \{38, 40, 50\}$ and let D be the trace divisor of a point of $Y_1(2, N)$ over a number field of degree 10. As $J_1(2, N)(\mathbb{Q})$ is finite and $\operatorname{gon}_{\mathbb{Q}} X_1(2, N) \geq 11$, as explained at the beginning of the section, the reduction of D modulo 3 is not entirely cuspidal by Proposition 2.5 a). This contradicts Lemmas 7.19 to 7.21. Finally, the cyclic groups are excluded by Lemma 4.3. □

7.5. **The curve $X_1(2, 42)$.** The curve $X_1(2, 42)$ has genus 61, we work at $p = 5$, and by Abramovich's bound $\operatorname{gon}_{\mathbb{C}} X_1(2, 42) \geq 12$. The cusps of $X_1(2, 42)$ have degrees $1^{18}, 2^9, 6^6$ over $\mathbb{Q}$ [Naj26d, Section 11.6], and the closed cusps of $X_1(2, 42)_{\mathbb{F}_5}$ have degrees $1^{18}, 2^9, 3^6, 6^3$ (Table 4), so those of degree 1 and 2 are the reductions of Galois orbits of cusps of the same degree. We use the two maps $X_1(2, 42) \to X_1(2, 14)$ given by $(E, P, Q) \mapsto (E, P, 3Q)$ and by $(E, P, Q) \mapsto (E/\langle 14Q\rangle, \phi(P), \phi(Q))$, where $\phi : E \to E/\langle 14Q\rangle$ is the quotient map, the four maps $X_1(2, 42) \to X_1(21)$ which keep $2Q$ on E or on its quotients by its three subgroups of order 2, and six maps $X_1(2, 42) \to X_0(42)$. These are the compositions of the natural map $X_1(42) \to X_0(42)$ with the maps $X_1(2, 42) \to X_1(42)$ which keep Q, $P + Q$ or $P + 22Q$, or divide E by $\langle P\rangle$ or $\langle P + 21Q\rangle$ and keep the image of Q, or divide E by $\langle 21Q\rangle$ and keep the image of $P + Q$. All these points have order 42. We denote by $\pi_0 : X_1(2, 42) \to X_0(42)$ the first of these six maps, $(E, P, Q) \mapsto (E, \langle Q\rangle)$. We also use the following quotient.

Lemma 7.23 ([Naj26d, Lemma 11.12 and its proof])**.** *Let $X = X_1(2, 42)$, let G_9 be the group of level automorphisms generated by $s_1 : (E, P, Q) \mapsto (E, 21Q, P + Q)$ and $s_2 : (E, P, Q) \mapsto (E, P, 25Q)$, and let $Y_{42} = X/G_9$. Let v be the parameter of $X_1(7)$ in Tate normal form, evaluated at $(E, 6Q)$, put $t = (v^3 - 3v + 1)/(v(v - 1)) - 8$ and*

$$f_1 = t^2 + 13t + 49, \qquad f_2 = t^2 + 5t + 1, \qquad f_3 = t^4 + 14t^3 + 63t^2 + 70t - 7.$$

Then Y_{42} has genus 5, and its function field is obtained from $\mathbb{Q}(u)$, where $u^2 = t$, by adjoining the coordinates of a point of order 3 on

$$E_u : y^2 = x^3 - \frac{f_2}{48f_1}x + \frac{f_3}{864f_1^2}.$$

The reduction of $J_{Y_{42}}(\mathbb{Q})$ modulo 5, taken relative to a rational cusp, is contained in a subgroup $H_{42} \simeq (\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/24\mathbb{Z}$ of index 18 of $J_{Y_{42}}(\mathbb{F}_5) \simeq \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/6\mathbb{Z})^2 \times \mathbb{Z}/48\mathbb{Z}$.

Lemma 7.24. *Let $\vartheta : X_1(42) \to X_0(42)$ be the natural map, let y_0 be the image of a rational cusp of $X_1(42)$, and let $H_0 \subseteq J_0(42)(\mathbb{F}_5)$ be the reduction modulo 5 of $\vartheta_* J_1(42)(\mathbb{Q})$. Then $J_0(42)(\mathbb{F}_5) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/48\mathbb{Z})^2$, $H_0 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z}$ has index 192, and for $j = 0, \ldots, 6$ the images in $J_0(42)(\mathbb{F}_5)/H_0$ of the sets $\mathcal{S}_j$ of the classes $[j\overline{y_0} - B]$, with B effective cuspidal of degree j on $X_0(42)_{\mathbb{F}_5}$, have $1, 6, 12, 16, 20, 24, 24$ elements.*

Proof. The group $J_1(42)(\mathbb{Q})$ is generated by rational cuspidal divisor classes [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], so $\vartheta_* J_1(42)(\mathbb{Q})$ is generated by the push-forwards of the rational cuspidal divisors of degree 0. All the 8 cusps of $X_0(42)$ are rational, and we compute the push-forwards of the Galois orbits of cusps of $X_1(42)$, the group $J_0(42)(\mathbb{F}_5)$ and its subgroup H_0, and the sets $\mathcal{S}_j$. □

Lemma 7.25. *Let $X = X_1(2, 42)$ and let D be an effective rational divisor of degree 10 on X whose support contains no cusp. Suppose that the reduction of D modulo 5 is not entirely cuspidal. Then there is a level automorphism g of X such that the reduction of gD is $D' + C'$, with C' effective cuspidal, where*

a) *either D' is a closed point of degree 9 which is fixed by a level automorphism of order 3, and $\deg C' = 1$,*
b) *or $D' = x_{42}$, the closed point of degree 6 of $X_{\mathbb{F}_5}$ represented by*

$$\beta = 2\theta^2 + 4\theta^3 + 2\theta^4 + 3\theta^5, \qquad \gamma = 4 + \theta + 4\theta^2 + \theta^5, \qquad \text{where } \theta^6 + \theta^4 + 4\theta^3 + \theta^2 + 2 = 0,$$

and $\deg C' = 4$.

Proof. Write the reduction of D as $D' + C'$ as in Section 2.5, with $D' \neq 0$ of degree e. By Table 4, the type of D' is one of $[4], \dots, [10]$, $[4, 4]$, $[4, 5]$, $[4, 6]$ and $[5, 5]$. Up to the 36 level automorphisms, the non-cuspidal closed points of degree $4, \dots, 10$ form 5, 18, 64, 316, 1372, 5888 and 27374 orbits, which we compute. Normalizing the first point and taking all the 126, 648, 2080 and 648 possibilities for the second point in the types $[4, 4]$, $[4, 5]$, $[4, 6]$ and $[5, 5]$, we get $35037 + 630 + 3240 + 10400 + 11664 = 60971$ cases. We apply the following tests. In i), ii) and iii) we use (2.1), with all the effective cuspidal divisors on the target allowed.

i) The group $J_1(2, 14)(\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ is generated by rational cuspidal divisor classes [DEvH+21, Proposition 4.16 and Table 3], and we compute that its reduction has index 4 in $J_1(2, 14)(\mathbb{F}_5) \simeq (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$ and contains the classes of all the cuspidal divisors. Only 4647 cases pass the test with the two maps to $X_1(2, 14)$, as we compute.
ii) With the subgroup H_{42} of Lemma 7.23, only 752 of them pass the test with the quotient map $X \to Y_{42}$, as we compute.
iii) The group $J_1(21)(\mathbb{Q}) \simeq \mathbb{Z}/364\mathbb{Z}$ is generated by rational cuspidal divisor classes [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], and its reduction has index 6 in $J_1(21)(\mathbb{F}_5) \simeq \mathbb{Z}/2184\mathbb{Z}$. Only 111 of the 752 cases pass the test with the four maps to $X_1(21)$, as we compute. Exactly 3 of them are single closed points of degree 9 (with a cuspidal part of degree 1), and we check that each of them is fixed by one of the level automorphisms $(E, P, Q) \mapsto (E, 21Q, P + 25Q)$ and $(E, P, Q) \mapsto (E, P + 21Q, P + 4Q)$, which have order 3. These 3 cases are the cases in a).
iv) For each of the six maps $\pi : X \to X_0(42)$ described above, the class of $\pi_* D - 10y_0$ lies in $\vartheta_* J_1(42)(\mathbb{Q})$, so Lemma 2.16 gives $[\pi_* D' - e\,\overline{y_0}] \in H_0 + \mathcal{S}_{10-e}$, with the notation of Lemma 7.24. Only 10 of the remaining 108 cases pass this test for all six maps, as we compute: one of type [6], namely x_{42} with $\deg C' = 4$, one of type [10], four of type $[4, 4]$, two of type $[4, 6]$ and two of type $[5, 5]$.
v) Let π' be one of the maps $(E, P, Q) \mapsto (E, Q)$ and $(E, P, Q) \mapsto (E, P + Q)$ from X to $X_1(42)$. As $J_1(42)(\mathbb{Q})$ is finite, $A_q(\pi'_* D)$ is principal for $q = 11$ and $q = 17$ by Proposition 2.2 d), and hence so is its reduction $A_q(\pi'_* D') + A_q(\pi'_* C')$. If $\deg C' = 0$,

then $A_{11}(\pi'_* D')$ is principal. As $17 \equiv 5^5 \pmod{42}$, we have $A_{17} C = 0$ for every cuspidal divisor C on $X_1(42)_{\mathbb{F}_5}$ by Lemma 2.3, so $A_{17}(\pi'_* D')$ is principal in all cases. For the 5 cases of degree 10 we compute that $\ell(A_{11}(\pi'_* D')) = 0$, and for the 4 cases of type $[4,4]$ that $\ell(A_{17}(\pi'_* D')) = 0$, with $\pi'(E,P,Q) = (E,Q)$ except for one case of type $[4,4]$, where we use $\pi'(E,P,Q) = (E, P+Q)$.

So only the case b) remains. □

Lemma 7.26. *Let $X = X_1(2,42)$ and let D be an effective rational divisor of degree 10 on X whose support contains no cusp. Suppose that the reduction of D modulo 5 is $x_{42} + C'$, where x_{42} is the closed point of Lemma 7.25 and C' is an effective cuspidal divisor of degree 4. Then C' consists of a closed cusp of degree 3 and a closed cusp of degree 1.*

Proof. Let π_0, ϑ, y_0 and H_0 be as above and in Lemma 7.24. We compute that $[\pi_{0*} x_{42} - 6\overline{y_0}] \notin H_0$. Suppose that C' contains no closed cusp of degree 3. As C' has degree 4, it is then supported on closed cusps of degree 1 and 2, so it is the reduction of a rational cuspidal divisor C. The class of $\pi_{0*}(D - C) - 6y_0$ lies in $\vartheta_* J_1(42)(\mathbb{Q})$ and reduces to $[\pi_{0*} x_{42} - 6\overline{y_0}]$, which is a contradiction. So C' contains a closed cusp of degree 3, and the remaining part of C' is a closed cusp of degree 1. □

Lemma 7.27. *Let $X = X_1(2,42)$, let h_{42} be the level automorphism $(E,P,Q) \mapsto (E, P + 21Q, P + 4Q)$, and let x_{42} be the closed point of Lemma 7.25. Then h_{42} has order 3, it fixes x_{42}, it acts freely on the 72 geometric cusps of X, and*

$$\ell\big(x_{42} + C' + h_{42} C' + h_{42}^2 C'\big) = 1$$

on $X_{\mathbb{F}_5}$ for every effective cuspidal divisor C' on $X_{\mathbb{F}_5}$ consisting of a closed cusp of degree 3 and a closed cusp of degree 1.

Proof. One checks directly that h_{42} has order 3, and that $h_{42} = s_2 s_1^2$ with s_1, s_2 as in Lemma 7.23. We check that h_{42} acts on the geometric points of x_{42} as the square of the Frobenius, so it fixes x_{42}. The automorphism h_{42} permutes the three points of order 2 cyclically, so it fixes no cusp, as at a cusp one of the points of order 2 is distinguished (see the proof of [Naj26d, Proposition 11.13]). As h_{42} has order 3, it acts freely on the 72 geometric cusps.

Let $W_{42} = X/\langle h_{42} \rangle$, which is the curve V of genus 17 of [Naj26d, proof of Proposition 11.13], as $\langle h_{42} \rangle = \langle s_1 s_2^2 \rangle$, and let $\rho_{42} : X \to W_{42}$ be the quotient map. In the notation of Lemma 7.23, the function field of W_{42} is obtained from that of Y_{42} by adjoining a root w_{42} of

$$w_{42}^3 - \frac{f_2}{48} w_{42} + \frac{f_3(2t+13)}{1728 f_1} - \frac{u}{8 f_1} = 0.$$

Here $w_{42} = r_0 v_0 + r_1 v_1 + r_2 v_2$, where r_0, r_1, r_2 are the x-coordinates of the points of order 2 in a normalized model of E, ordered by the level structure, and $v_0 = v$, $v_1 = (v-1)/v$, $v_2 = 1/(1-v)$. This is the model of the curve V of genus 17 in [Naj26d, proof of Proposition 11.13]: the data `next_cases_20261030/C242/geometry/diagonal17_normalized_model_data.m` and `next_cases_20261030/C242/geometry/diagonal17_parameter_data.m` are those exported by the script `C2x42/diagonal_genus17_lattice/export.m` of the repository of [Naj26d] for degree 9. The function u is regular at x_{42} and satisfies $u^2 + 4u + 2 = 0$ there, and $j = 0$ at x_{42}. We find exactly 2 closed points of degree 2 of $W_{42,\mathbb{F}_5}$ at which $u^2 + 4u + 2 = 0$ and $j = 0$, and both are unramified in ρ_{42}, with a closed point of degree 6 above them. So $x_{42} = \rho_{42}^* z_{42}$ for one of them, z_{42} say, and we treat both possibilities.

The closed cusps of $W_{42,\mathbb{F}_5}$ have degrees $1^6, 2^3, 3^2, 6$. As h_{42} acts freely on the cusps, $C' + h_{42}C' + h_{42}^2C' = \rho_{42}^*\rho_{42*}C'$, and $\rho_{42*}C'$ is the sum of one of the 2 closed cusps of degree 3 and one of the 6 closed cusps of degree 1 of $W_{42,\mathbb{F}_5}$, which gives 12 possibilities. To compute $\ell(\rho_{42}^*\Theta)$ for divisors Θ on W_{42}, we extend the constants to $\mathbb{F}_{25}$. Put $\tilde{t} = t + 8$, $\delta_1 = \tilde{t}^2 - 3\tilde{t} + 9$ and $\delta_2 = 2\tilde{t}^3 - 9\tilde{t}^2 + 27\tilde{t} - 27$, and note that $\delta_2^2 - 4\delta_1^3 = -27\delta_1^2$. The parameter v satisfies $v^3 - \tilde{t}v^2 + (\tilde{t} - 3)v + 1 = 0$, and generates the function field of X over that of W_{42}. For a primitive cube root of unity $\zeta \in \mathbb{F}_{25}$, the cover $X_{\mathbb{F}_{25}} \to W_{42,\mathbb{F}_{25}}$ is the Kummer cover $y^3 = \Phi_{42}$ with $\Phi_{42} = (\delta_2 + 3(\zeta - \zeta^2)\delta_1)/2$, as $3v - \tilde{t} = y + \delta_1/y$. With $\Lambda_j = \lfloor j \operatorname{div}(\Phi_{42})/3 \rfloor$ for $j = 0, 1, 2$, the integral bases of this tame Kummer cover give

$$\ell_X(\rho_{42}^*\Theta) = \sum_{j=0}^{2} \ell_{W_{42}}(\Theta + \Lambda_j)$$

for every divisor Θ on $W_{42,\mathbb{F}_{25}}$. For both choices of z_{42} and all 12 possibilities for $\rho_{42*}C'$ we compute that $\ell_{W_{42}}(z_{42} + \rho_{42*}C' + \Lambda_j) = 1, 0, 0$ for $j = 0, 1, 2$. Hence $\ell_X(x_{42} + \sum_j h_{42}^j C') = \ell_X(\rho_{42}^*(z_{42} + \rho_{42*}C')) = 1$. □

Proposition 7.28. *The groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/42\mathbb{Z}$ and $\mathbb{Z}/84\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let $X = X_1(2, 42)$ and let D be the trace divisor of a point of $Y_1(2, 42)$ over a number field of degree 10. As $J_X(\mathbb{Q})$ is finite and $\operatorname{gon}_{\mathbb{Q}} X \geq \operatorname{gon}_{\mathbb{C}} X \geq 12$, the reduction of D modulo 5 is not entirely cuspidal by Proposition 2.5 a). By Lemma 7.25, after replacing D by its image under a level automorphism, one of the cases a) and b) of that lemma holds.

Suppose first that a) holds, so the reduction of D is $D' + \bar{c}$, where D' is a closed point of degree 9 fixed by a level automorphism h of order 3, and $\bar{c}$ is a closed cusp of degree 1. Let c be a cusp of X which reduces to $\bar{c}$, which is defined over $\mathbb{Q}(\zeta_{42})$. Then h fixes the reduction D' of $D - c$, and Lemma 2.10 b), with $d = 10$, $e = 1$ and $\operatorname{gon}_{\mathbb{C}} X \geq 12 > 11$, gives $hD = D$. By Lemma 2.14, the points in the support of D correspond to elliptic curves without complex multiplication, so Lemma 2.9, applied to the group of order 3 generated by h, shows that $3 \mid \deg D = 10$, which is a contradiction.

Suppose now that b) holds, so the reduction of D is $x_{42} + C'$ with C' effective cuspidal of degree 4. By Lemma 7.26, C' consists of a closed cusp of degree 3 and one of degree 1, so by Lemma 7.27 the automorphism h_{42} fixes x_{42}, acts freely on the geometric cusps, and satisfies $\ell(x_{42} + \sum_{j=0}^{2} h_{42}^j C') = 1$. Lemma 2.15 gives $3 \mid \deg C' = 4$, which is a contradiction. Finally, $\mathbb{Z}/84\mathbb{Z}$ is excluded by Lemma 4.3. □

8. The Hecke sieve and push-forwards to smaller levels

In this section we exclude the groups $\mathbb{Z}/n\mathbb{Z}$ for

$$n \in \{44, 46, 48, 54, 56, 58, 60, 62, 66, 70, 74\}.$$

In most of the cases we reduce the trace divisor D of a point of order n over a decic field (Section 2.2) modulo a small prime p, and we exclude all the possible reductions $D' + C'$ with the Hecke sieve and the push-forward class test of Section 2.5, applied on $X_1(n)$ itself or after pushing D forward to curves of smaller level, such as $X_1(n/2)$ and $X_1(2, n/2)$. For some of the groups, such as $\mathbb{Z}/54\mathbb{Z}$, $\mathbb{Z}/56\mathbb{Z}$ and $\mathbb{Z}/58\mathbb{Z}$, we also use the reduction modulo 2, Riemann-Roch computations on explicit models, or known points of degree 10 on curves of smaller level. Over nonic fields the groups $\mathbb{Z}/44\mathbb{Z}$, $\mathbb{Z}/46\mathbb{Z}$, $\mathbb{Z}/48\mathbb{Z}$, $\mathbb{Z}/54\mathbb{Z}$, $\mathbb{Z}/58\mathbb{Z}$ and $\mathbb{Z}/62\mathbb{Z}$

were excluded in [Naj26d, Propositions 6.7, 6.8, 6.11, 10.4 and 11.15] by the same methods, and for $n = 44$ and $n = 46$ we reuse the computations made there for the reductions whose non-cuspidal part has degree at most 9.

The numbers of non-cuspidal closed points of $X_1(n)_{\mathbb{F}_p}$ that we use for $n \in \{44, 46, 48, 56\}$ are listed in Table 5, together with the numbers of their orbits under the diamond operators. For $n \in \{44, 46, 48\}$ the numbers of points of degree at most 9 are those of [Naj26d, Table 3 and the proof of Proposition 11.15], and for $X_1(44)$ the numbers of orbits of degree $6, \dots, 9$ are those of [Naj26d, proof of Proposition 6.8]. We compute the other numbers by enumerating the closed points of degree 10 on the models of $X_1(44)_{\mathbb{F}_3}$ and $X_1(46)_{\mathbb{F}_3}$ (see also `continuation_20261031a/C46/new_support_filter.m`), and, for $X_1(48)_{\mathbb{F}_5}$ and $X_1(56)_{\mathbb{F}_3}$, by running through all the elliptic curves over $\mathbb{F}_{p^k}$, $k \leq 10$, with a point of order n (see `computations/d31a_even_p5_torsion_common.m` and `computations/d31a_even_p3_census_common.m`).

X	p		degree $1, 2, \dots, 10$
$X_1(44)$	3	points	$0, 0, 0, 0, 60, 160, 240, 920, 2260, 5854$
		orbits	$0, 0, 0, 0, 6, 16, 24, 92, 226, 590$
$X_1(46)$	3	points	$0, 0, 0, 55, 44, 55, 264, 781, 1958, 6292$
		orbits	$0, 0, 0, 5, 4, 5, 24, 71, 178, 572$
$X_1(48)$	5	points	$0, 0, 16, 64, 656, 2712, 10784, 48992, 217520, 977528$
		orbits	$0, 0, 2, 8, 82, 342, 1348, 6172, 27190, 122318$
$X_1(56)$	3	points	$0, 0, 0, 0, 72, 48, 324, 588, 2112, 6300$
		orbits	$0, 0, 0, 0, 6, 4, 27, 54, 176, 530$

TABLE 5. Non-cuspidal closed points of $X_{\mathbb{F}_p}$ of degree at most 10, and the numbers of their orbits under the diamond operators.

8.1. **The curve $X_1(44)$.** Over nonic fields, $\mathbb{Z}/44\mathbb{Z}$ is excluded in [Naj26d, Proposition 6.8], and we reuse the computations made there. The new reductions in degree 10 are treated with the canonical ring of $X_1(44)_{\mathbb{F}_3}$.

Lemma 8.1. *Let D' be an effective divisor on $X_1(44)_{\mathbb{F}_3}$.*

a) *If D' is a closed point of degree 5, or the sum of two (possibly equal) closed points of degree 5, then $A_5 D'$ is not principal.*
b) *If D' is a closed point of degree 10, then $A_5 D'$ or $A_7 D'$ is not principal.*

Proof. As A_q commutes with the diamond operators, we may take a closed point D' of degree 5 or 10 among the 6 and 590 representatives of the diamond orbits of Table 5, and for a sum of two closed points of degree 5 we may take the first one among the 6 representatives and the second one among all the 60 closed points of degree 5. This gives $6 + 590 + 360 = 956$ divisors D'. Write $A_q D' = T - U$ with $T = T_q D'$ and $U = D' + q\langle q \rangle D'$. We compute T from the $q + 1$ isogenies of degree q of the elliptic curves of the points in the support of D', including the residue degrees, and U by multiplying the point of order 44 by q, both on the moduli model. Both are effective, of degree 30 or 60 for $q = 5$ and of degree 80 for $q = 7$.

Let K_X be a canonical divisor of $X = X_1(44)_{\mathbb{F}_3}$. We use the canonical model of X, of genus 36 and degree 70 in $\mathbb{P}^{35}$, and the multiplication map $R_2 \times R_2 \to R_4$, where $R_i = H^0(X, iK_X)$, $\dim R_2 = 105$ and $\dim R_4 = 245$, which were computed in the proof of [Naj26d, Proposition 6.8] as the canonical embedding of a plane model of degree 19. From the plane model we also

obtain the local parameters at the points in the support of U. We check with Lemma 2.13, with $\mathcal{L} = \mathcal{M} = \mathcal{O}(2K_X)$ and non-zero sections $F, H \in H^0(X, 2K_X - T)$, that the linear map of Lemma 2.13 has rank $105 = \dim R_2$, and hence $\ell(T - U) = 0$, for $q = 5$ for 954 of the 956 divisors. The remaining 2 divisors are closed points of degree 10, and for them we check in the same way that $\ell(T - U) = 0$ for $q = 7$. □

Proposition 8.2. *The group $\mathbb{Z}/44\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let $X = X_1(44)$, and let D be the trace divisor of a point of order 44 over a decic field. We have $\operatorname{rk} J_1(44)(\mathbb{Q}) = 0$ [DEvH+21, Theorem 3.1(2)] and $\operatorname{gon}_{\mathbb{Q}} X = 15$ [Var26, Theorem D], so by Proposition 2.5 a) with $p = 3$ the reduction of D modulo 3 is $D' + C'$ with $D' \neq 0$. By Table 5, D' is a closed point of degree $5 \leq \deg D' \leq 10$ or the sum of two closed points of degree 5. By Proposition 2.2 d) we have $[A_q(D)] = 0$, and hence $[A_q(D')] = -[A_q(C')]$, for every prime $q \nmid 66$.

We compute that the Galois orbits of cusps of X over $\mathbb{Q}$ have degrees $1^{15}, 2^5, 5, 10^2$, and that the closed cusps of $X_{\mathbb{F}_3}$ have degrees $1^{15}, 2^5, 5^3, 10$. So every closed cusp of $X_{\mathbb{F}_3}$ of degree at most 4 is the reduction of a rational cuspidal divisor of the same degree, and if $\deg C' \leq 4$, then $A_q C' = 0$ for every prime $q \nmid 66$. As $5 \equiv 3^8 \pmod{44}$, Lemma 2.3 also gives $A_5 C' = 0$ for every C'.

Suppose first that $\deg D' \in \{6, 7, 8\}$. Then $\deg C' \leq 4$, and in the proof of [Naj26d, Proposition 6.8] it is computed that for every closed point D' of $X_{\mathbb{F}_3}$ of degree 6, 7 or 8 one of the classes $[A_q(D')]$, $q \in \{5, 7, 13, 17, 19\}$, is non-zero, which is a contradiction. Suppose now that $\deg D' = 9$. Then C' is a closed cusp of degree 1, so $A_5 D'$ is principal, and this is excluded in the proof of [Naj26d, Proposition 6.8], where it is shown that $\ell(T_5 P - P - 5\langle 5\rangle P) = 0$ for all the closed points P of degree 9 of $X_{\mathbb{F}_3}$. Finally, if D' is a closed point of degree 5, then $A_5 D'$ is principal as $A_5 C' = 0$, and if $\deg D' = 10$, then $C' = 0$ and $A_q D'$ is principal for every $q \nmid 66$. Both are impossible by Lemma 8.1. □

8.2. **The curve $X_1(46)$.** Over nonic fields, $\mathbb{Z}/46\mathbb{Z}$ is excluded in [Naj26d, Proposition 6.7], and we reuse the computations made there. Let $\pi : X_1(46) \to X_1(23)$ be the map $(E, P) \mapsto (E, 2P)$, which has degree 3 and commutes with the diamond operators. The group $J_1(23)(\mathbb{Q}) \simeq \mathbb{Z}/408991\mathbb{Z}$ is generated by rational cuspidal divisor classes [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], and its reduction G has index 23 in $J_1(23)(\mathbb{F}_3) \simeq \mathbb{Z}/9406793\mathbb{Z}$ [Naj26d, proof of Proposition 6.7]. Let y_0 be a rational cusp of $X_1(23)$.

Lemma 8.3. *Let D' be an effective divisor of degree 10 on $X_1(46)_{\mathbb{F}_3}$ with non-cuspidal support, of type [10], [6, 4] or [5, 5]. Then $[\pi_* D' - 10\overline{y_0}] \notin G$, or $A_5 D'$ is not principal.*

Proof. Both conditions are invariant under the diamond operators, as these commute with π and A_5, and the diamond operators of $X_1(23)$ preserve G and map $\overline{y_0}$ to reductions of rational cusps, whose differences have classes in G. Taking a representative of each diamond orbit, and for the types [6, 4] and [5, 5] the first point up to the diamond operators and the second one arbitrary, we obtain by Table 5 572 divisors of type [10], $5 \cdot 55 = 275$ of type [6, 4] and $4 \cdot 44 = 176$ of type [5, 5], 1023 in total. We compute that $[\pi_* D' - 10\overline{y_0}] \notin G$ for 552, 264 and 170 of them, respectively. For the remaining 20, 11 and 6 divisors we compute that $\ell(A_5 D') = 0$ on the function field of $X_1(46)_{\mathbb{F}_3}$, which has genus 45, where $T_5 D'$ is computed from the isogenies of degree 5 of the elliptic curves of the points in the support of D' on the moduli model, including the residue degrees. □

Proposition 8.4. *The group $\mathbb{Z}/46\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let D be the trace divisor on $X_1(46)$ of a point of order 46 over a decic field. We have $\operatorname{rk} J_1(46)(\mathbb{Q}) = 0$ [DEvH+21, Theorem 3.1(2)] and $\operatorname{gon}_{\mathbb{Q}} X_1(46) = 19$ [Var26, Theorem D], so by Proposition 2.5 a) with $p = 3$ the reduction of D modulo 3 is $D' + C'$ with $D' \neq 0$ of degree $e \geq 4$ (Table 5). We compute that the Galois orbits of cusps of $X_1(46)$ over $\mathbb{Q}$ and the closed cusps of $X_1(46)_{\mathbb{F}_3}$ both have degrees $1^{22}, 11^2$. So C', which has degree at most 6, is the reduction of a rational cuspidal divisor, and $A_q C' = 0$ for every prime $q \nmid 138$ by Proposition 2.2 c). By Proposition 2.2 d) it follows that $[A_q(D')] = 0$ for all these q. The closed cusps of $X_1(23)_{\mathbb{F}_3}$ have degrees $1^{11}, 11$, so $\pi_* C'$ is the reduction of a rational cuspidal divisor, and (2.1) gives $[\pi_* D' - e\overline{y_0}] \in G$. Note that neither of the two conditions depends on the degree of C'.

By Table 5 the type of D' is one of [4], [5], [6], [7], [8], [9], [4, 4], [5, 4], and [10], [6, 4], [5, 5]. In the proof of [Naj26d, Proposition 6.7] it is computed that every divisor D' of one of the first 8 types, of which there are 782 up to the diamond operators, satisfies $[\pi_* D' - e\overline{y_0}] \notin G$ or $[A_q(D')] \neq 0$ for some $q \in \{5, 7, 11, 13, 17, 19\}$. The last 3 types are excluded by Lemma 8.3. □

8.3. **The curve $X_1(48)$.** Over nonic fields, $\mathbb{Z}/48\mathbb{Z}$ is excluded in [Naj26d, Proposition 11.15]. In degree 10 we push the trace divisor forward to $X_1(2, 24)$, and use A_{13} together with a description of its action on the cusps.

Let $\pi : X_1(48) \to X_1(2, 24)$ be the map $(E, P) \mapsto (E/\langle 24P \rangle, T, \overline{P})$ of [Naj26d, proof of Proposition 11.15], where T is the non-zero point of the kernel of the dual isogeny and $\overline{P}$ is the image of P, which has order 24. It has degree 2 and commutes with the diamond operators. The group $J_1(2, 24)(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^2 \times \mathbb{Z}/120\mathbb{Z} \times \mathbb{Z}/240\mathbb{Z}$ is generated by rational cuspidal divisor classes [DEvH+21, Proposition 4.16 and Table 3], and its reduction H has order 921600 and index 4608 in $J_1(2, 24)(\mathbb{F}_5) \simeq (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/4\mathbb{Z})^2 \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \times (\mathbb{Z}/480\mathbb{Z})^2$ [Naj26d, proofs of Propositions 11.2 and 11.15]. We fix a rational cusp c_* of $X_1(2, 24)$, and we write $\mathcal{S}_j$ for the set of the classes $[j\overline{c_*} - B]$ for the effective cuspidal divisors B of degree j on $X_1(2, 24)_{\mathbb{F}_5}$, as in (2.1). We compute that the images of $\mathcal{S}_0, \ldots, \mathcal{S}_7$ in $J_1(2, 24)(\mathbb{F}_5)/H$ have 1, 5, 23, 75, 178, 378, 661 and 1065 elements.

Lemma 8.5. *For every effective cuspidal divisor C on $X_1(48)_{\mathbb{F}_5}$, the divisor $A_{13}C$ is principal.*

Proof. It is enough to prove this for a closed cusp c. By Lemma 2.3, $A_{13}c = (\sigma_{13}c - c) + 13\langle 13 \rangle(\sigma_{13}^{-1}c - c)$. The 56 geometric cusps of $X_1(48)$ are given by the pairs $(a, b) \in (\mathbb{Z}/48\mathbb{Z})^2$ of order 48 modulo $(a, b) \sim \pm(a + kb, b)$, on which $\sigma_u(a, b) = (ua, b)$ and $\langle u \rangle(a, b) = (ua, u^{-1}b)$. We compute that the closed cusps of $X_1(48)_{\mathbb{F}_5}$ have degrees $1^{16}, 2^{12}, 4^4$, and that σ_{13} fixes 28 of these 32 closed cusps, and hence $A_{13}c = 0$ for them. The remaining 4 are the 2 closed cusps C_2, C_2' of degree 2 at which j has a pole of order 2, and the 2 closed cusps C_4, C_4' of degree 4 at which j has a pole of order 1. Both σ_{13} and $\langle 13 \rangle$ interchange C_i and C_i' for $i = 2, 4$, and as $\sigma_{13}^2 = \sigma_{25} = \sigma_5^2$ fixes every closed cusp, we obtain

$$A_{13}C_i = (C_i' - C_i) + 13(C_i - C_i') = 12(C_i - C_i') = -A_{13}C_i'.$$

Note that this does not depend on the conventions for the diamond operators of Section 2.3. We compute functions f_2 and f_4 on $X_1(48)_{\mathbb{F}_5}$ with $\operatorname{div}(f_i) = 12(C_i - C_i')$, which proves the claim. □

Lemma 8.6. *Let $N \neq 0$ be an effective divisor of degree $r \leq 10$ on $X_1(48)_{\mathbb{F}_5}$ with non-cuspidal support, such that $[\pi_* N - r\overline{c_*}] \in H + \mathcal{S}_{10-r}$. If $r = 10$, then $A_7 N$ is not principal, and if $r < 10$, then $A_{13} N$ is not principal.*

Proof. The diamond operators commute with π, A_7 and A_{13}, and they act on $X_1(2,24)$ by level automorphisms defined over $\mathbb{Q}$, which preserve H and the sets $\mathcal{S}_j$ and map $\overline{c_*}$ to reductions of rational cusps. So both the condition and the conclusion are invariant under the diamond operators. By Table 5 the possible types of N are $[k]$ for $3 \leq k \leq 10$, $[3,3]$, $[3,4]$, $[3,5]$, $[3,6]$, $[3,7]$, $[4,4]$, $[4,5]$, $[4,6]$, $[5,5]$, $[3,3,3]$ and $[3,3,4]$.

Suppose first that N is a closed point of degree 9 or 10. There are $27190+122318 = 149508$ representatives of the diamond orbits of these points. Before computing the classes we use 4 characters χ_f as in Lemma 2.11, for functions f on $X_1(2,24)_{\mathbb{F}_5}$ with $\operatorname{div}(f) = 2A_f$, which we check to be trivial on H (the functions are given in `continuation_20261031b/C48/inputs/four_characters.m`). If N satisfies the condition, then the values of the 4 characters at $[\pi_* N - r\overline{c_*}]$ are those at an element of $\mathcal{S}_{10-r}$. We compute that this holds for 12603 of the representatives, and we keep 1 further representative, at which one of the functions f has a zero or a pole on the support of $\pi_* N$. For these 12604 representatives we compute the classes, and find that the condition holds for only 107 of them, 57 of degree 10 and 50 of degree 9.

For the other types we take the first point of N up to the diamond operators and the others arbitrary. This gives 2, 8, 82, 342, 1348 and 6172 divisors of the types $[3], \ldots, [8]$, and

type	$[3,3]$	$[3,4]$	$[3,5]$	$[3,6]$	$[3,7]$	$[4,4]$	$[4,5]$	$[4,6]$	$[5,5]$	$[3,3,3]$	$[3,3,4]$
divisors	32	128	1312	5424	21568	512	5248	21696	53792	272	2048

of the other types, 119986 in total. We compute that the condition holds for only 243 of them, which form 201 orbits under the diamond operators:

type	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[3,3]$	$[3,5]$	$[3,6]$	$[3,7]$	$[4,4]$	$[4,5]$	$[4,6]$	$[5,5]$
orbits	4	6	20	24	55	4	10	4	8	16	8	12	30

It remains to treat $107 + 201 = 308$ divisors N. For the $57 + 8 + 12 + 30 = 107$ of them of degree 10 we compute that $\ell(A_7 N) = 0$, and for the other 201 we compute that $\ell(A_{13} N) = 0$, on the function field of $X_1(48)_{\mathbb{F}_5}$, which has genus 37. Here $T_q N$ is computed from the cyclic isogenies of degree q of the elliptic curves of the points in the support of N on the moduli model, including the lengths of their Frobenius orbits and the residue degrees. □

Proposition 8.7. *The group $\mathbb{Z}/48\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let D be the trace divisor on $X_1(48)$ of a point of order 48 over a decic field. We have $\operatorname{rk} J_1(48)(\mathbb{Q}) = 0$ [DEvH+21, Theorem 3.1(2)] and $\operatorname{gon}_{\mathbb{Q}} X_1(48) = 16$ [Var26, Theorem D], so by Proposition 2.5 a) with $p = 5$ the reduction of D modulo 5 is $N + C'$ with $N \neq 0$ effective of degree r with non-cuspidal support, and C' effective and cuspidal of degree $10-r$. By (2.1), with $y_0 = c_*$ and $G = H$, we have $[\pi_* N - r\overline{c_*}] \in H + \mathcal{S}_{10-r}$. By Proposition 2.2 d) the classes $[A_7(D)]$ and $[A_{13}(D)]$ are 0. If $r = 10$, then $C' = 0$ and $A_7 N$ is principal. If $r < 10$, then $A_{13} N + A_{13} C'$ is principal, and as $A_{13} C'$ is principal by Lemma 8.5, so is $A_{13} N$. Both contradict Lemma 8.6. □

8.4. **The curve $X_1(54)$.** Over nonic fields, $\mathbb{Z}/54\mathbb{Z}$ is excluded in [Naj26d, Section 10]. We write the points of $X_1(54)$ as triples (E, P_2, Q) with P_2 of order 2 and Q of order 27, and use the two degeneracy maps

$$\alpha, \beta : X_1(54) \to Z := X_1(27), \qquad \alpha(E, P_2, Q) = (E, Q), \qquad \beta(E, P_2, Q) = (E/\langle P_2\rangle, \phi(Q)),$$

where $\phi : E \to E/\langle P_2\rangle$ is the quotient isogeny. Both are defined over $\mathbb{Q}$, have degree 3, map cusps to cusps and non-cusps to non-cusps, and commute with the diamond operators. We write $\delta = \langle 2\rangle$ for the diamond operator of Z. At the unique prime above 2 at which the elliptic curve has good reduction, the reductions of the push-forwards of the trace divisor under α and β have the same non-cuspidal part, and their cuspidal parts are related by δ. We combine this with Riemann-Roch computations on $Z_{\mathbb{F}_2}$ and with class computations on $Z_{\mathbb{F}_5}$.

Lemma 8.8. *We have* $\operatorname{gon}_{\mathbb{Q}} X_1(54) \geq 12$.

Proof. The curve $X_1(54)$ has genus 52 and $i(54) = 972$, so Abramovich's bound gives $\operatorname{gon}_{\mathbb{Q}} X_1(54) \geq \operatorname{gon}_{\mathbb{C}} X_1(54) \geq \frac{325}{2^{15}} \cdot 972 > 9.6$. Let $W_{54} = X_1(54)/\langle 17\rangle$, where $\langle 17\rangle$ has order 3 in $\Delta(54)$, as $17^3 \equiv -1 \pmod{54}$. We compute from the action of $\mathrm{PSL}_2(\mathbb{Z})$ on the cosets that the group of W_{54} has index 324 in $\mathrm{PSL}_2(\mathbb{Z})$, no elliptic points and 36 cusps, so W_{54} has genus $1 + 324/12 - 36/2 = 10$. Suppose that there is a function f on $X_1(54)$ over $\mathbb{Q}$ of degree $n \in \{10, 11\}$. As $[\mathbb{Q}(X_1(54)) : \mathbb{Q}(W_{54})] = 3$ is prime, either $f \in \mathbb{Q}(W_{54})$, in which case $3 \mid n$, or $\mathbb{Q}(X_1(54)) = \mathbb{Q}(W_{54})(f)$, in which case the Castelnuovo-Severi inequality [Sti09, Theorem 3.11.3] gives $52 \leq 3 \cdot 10 + (3-1)(n-1) \leq 50$. Both are impossible. □

Lemma 8.9. *Let E be an elliptic curve over a number field K of degree 10 with a point of order 54. Then E has good reduction at some prime of K above 2. Every such prime is unramified and has residue degree between 6 and 10, and the reduction of E at it is ordinary.*

Proof. This is [Naj26d, Lemma 10.2] for number fields of degree $d \in \{7, 8, 9\}$, and its proof applies verbatim to $d = 10$. It uses only that $J_1(54)(\mathbb{Q})$ is finite of odd order [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], that $\operatorname{gon}_{\mathbb{Q}} X_1(54) > d$, which holds for $d = 10$ by Lemma 8.8, that $Z_{\mathbb{F}_2}$ has no non-cuspidal closed points of degree at most 5, and that the ramification index e and the residue degree $f \geq 6$ of a prime above 2 of good reduction satisfy $ef \leq d$, which forces $e = 1$ also for $d = 10$. The last step of that proof, which shows that the reduction is ordinary, is the case of Lemma 8.30 a) in which the isogeny of degree 2 is the quotient by the subgroup generated by the K-rational point of order 2, as the prime is unramified over 2. □

Lemma 8.10.
a) *The group $J_Z(\mathbb{Q}) \simeq (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/52497\mathbb{Z}$ is generated by rational cuspidal divisor classes. Reduction modulo 2 is an isomorphism $J_Z(\mathbb{Q}) \to J_Z(\mathbb{F}_2)$, and reduction modulo 5 is injective on $J_Z(\mathbb{Q})$.*
b) *The Galois orbits of cusps of Z over $\mathbb{Q}$ have degrees $1^9, 2^3, 6, 9$, and each of them reduces modulo 2 and modulo 5 to a single closed cusp of the same degree. The valuations of the functions b and b^4/Δ, where Δ is the discriminant of the Tate normal form $E(b, c)$ of (3.1), are different at the 14 orbits, and they are the same at the corresponding closed cusps of $Z_{\mathbb{F}_2}$ and $Z_{\mathbb{F}_5}$.*
c) *The curve $Z_{\mathbb{F}_2}$ has no non-cuspidal closed points of degree at most 5. The non-cuspidal closed points of $Z_{\mathbb{F}_2}$ of degree 6, 7, 8, 9 and 10 at which the elliptic curve is ordinary number 9, 9, 18, 90 and 99, and they form 1, 1, 2, 10 and 11 orbits under the diamond operators.*

Proof. a) The first statement is [DEvH+21, Theorem 3.1(2), Theorem 4.13, Corollary 4.14 and Table 2], the statement on the reduction modulo 2 is shown in [Naj26d, Section 10] (the paragraph after Lemma 10.2), and reduction modulo 5 is injective by Katz's result.

b) The cusps are defined over subfields of $\mathbb{Q}(\zeta_{27})$, and both 2 and 5 generate $(\mathbb{Z}/27\mathbb{Z})^\times$, so each Galois orbit stays irreducible modulo 2 and modulo 5. The functions b and b^4/Δ are units on $Y_1(27)$ over $\mathbb{Z}[\frac{1}{27}]$, so their valuations at the cusps do not change under reduction. They are used in [Naj26d, Section 10] (the paragraph after Lemma 10.2) to match the closed cusps modulo 2 and modulo 5, and we compute the degrees of the orbits and that these valuations distinguish them.

c) The first statement is in the proof of [Naj26d, Lemma 10.2], and we compute the second one. Note that an elliptic curve over a finite field of characteristic 2 is ordinary if and only if its j-invariant is non-zero. □

The following lemma describes the reductions modulo 2. By the reduction of a divisor on Z modulo 2 we mean its reduction on the smooth model of Z over $\mathbb{Z}_{(2)}$.

Lemma 8.11. *Let K be a number field of degree 10, and let E/K be an elliptic curve with points $P_2, Q \in E(K)$ of orders 2 and 27. Suppose that E has good ordinary reduction at a prime $\mathfrak{p}$ of K above 2, that P_2 reduces to 0 modulo $\mathfrak{p}$, and that E has bad reduction at all the other primes of K above 2. Let D be the trace divisor of $x = (E, P_2, Q)$ on $X_1(54)$, and put $D_0 = \alpha_* D$ and $D_1 = \beta_* D$. Then the residue degree f of $\mathfrak{p}$ satisfies $6 \le f \le 10$, and there are a non-cuspidal closed point N of $Z_{\mathbb{F}_2}$ of degree f and effective rational cuspidal divisors C_a and C_e on Z with $\deg C_a + \deg C_e = 10 - f$, such that the reductions of D_0 and D_1 modulo 2 are*

$$\overline{D_0} = N + \overline{C_a} + \overline{C_e}, \qquad \overline{D_1} = N + \overline{C_a} + \delta\overline{C_e},$$

and such that $D_1 + C_e \sim D_0 + \delta C_e$.

Proof. The divisors D_0 and D_1 are the trace divisors of the points $\alpha(x)$ and $\beta(x)$ of $Y_1(27)(K)$. For a prime $\mathfrak{q}$ of K above 2 let $y_\mathfrak{q}$ and $y'_\mathfrak{q}$ be the closed points of $Z_{\mathbb{F}_2}$ given by the reductions of $\alpha(x)$ and $\beta(x)$ modulo $\mathfrak{q}$, and let $e_\mathfrak{q}$ and $f_\mathfrak{q}$ be the ramification index and the residue degree of $\mathfrak{q}$. By Section 2.2, $\overline{D_0}$ is the sum of $e_\mathfrak{q} f_\mathfrak{q}/\deg(y_\mathfrak{q}) \cdot y_\mathfrak{q}$ over these primes, and similarly for $\overline{D_1}$, with $\deg(y'_\mathfrak{q}) = \deg(y_\mathfrak{q})$ in all the cases below.

At $\mathfrak{p}$ the point Q, of odd order, reduces to a point of order 27, so $y_\mathfrak{p}$ is non-cuspidal. By Lemma 8.10 c) we have $\deg y_\mathfrak{p} \ge 6$, and as $\deg y_\mathfrak{p}$ divides f and $e_\mathfrak{p} f \le 10$, it follows that $\deg y_\mathfrak{p} = f$ and $e_\mathfrak{p} = 1$. As the reduction is ordinary and P_2 reduces to 0, the subgroup generated by P_2 is the generic fibre of the connected subgroup scheme of order 2 of the 2-torsion of the Néron model of E at $\mathfrak{p}$. Hence ϕ reduces to an isogeny of degree 2 with connected kernel, which is the Frobenius isogeny of the reduction of E, and the reduction of $\beta(x)$ is the image of the reduction of $\alpha(x)$ under the 2-power Frobenius. It follows that $y'_\mathfrak{p} = y_\mathfrak{p} =: N$, with coefficient 1 in both $\overline{D_0}$ and $\overline{D_1}$.

Let $\mathfrak{q} \ne \mathfrak{p}$ be a prime above 2. By Lemma 2.4, applied to the point Q of odd order, E has multiplicative reduction at $\mathfrak{q}$, so $y_\mathfrak{q}$ and $y'_\mathfrak{q}$ are cusps. Over the completion of the maximal unramified extension of $K_\mathfrak{q}$, the curve E is a Tate curve $\mathbb{G}_m/t^\mathbb{Z}$. Its subgroups of order 2 are μ_2 and the 2 subgroups generated by $\pm t^{1/2}$, and the computation in the proof of Lemma 2.3, with $q = 2$, which is prime to 27, shows the following. If $P_2 = -1$, then the cusp to which $\beta(x)$ reduces is $\sigma_2(c)$, where c is the cusp to which $\alpha(x)$ reduces, and otherwise it is $\langle 2\rangle\sigma_2^{-1}(c)$. As σ_2 acts on the reductions of the cusps as the Frobenius, we get $y'_\mathfrak{q} = y_\mathfrak{q}$ in the first case and $y'_\mathfrak{q} = \delta y_\mathfrak{q}$ in the second one. Let $\overline{C_a}$ and $\overline{C_e}$ be the sums of the

contributions of the primes of the first and of the second kind to $\overline{D_0}$. By Lemma 8.10 b) every closed cusp of $Z_{\mathbb{F}_2}$ is the reduction of a rational cuspidal divisor of the same degree, so $\overline{C_a}$ and $\overline{C_e}$ are the reductions of effective rational cuspidal divisors C_a and C_e, and the reductions of D_0 and D_1 are as claimed.

Finally, the classes $[D_1 - D_0]$ and $[\delta C_e - C_e]$ lie in $J_Z(\mathbb{Q})$ and have the same reduction modulo 2, so they are equal by Lemma 8.10 a). □

Lemma 8.12. *Let K be a number field of degree 10, let E/K be an elliptic curve with points $P_2, Q \in E(K)$ of orders 2 and 27, let D be the trace divisor of (E, P_2, Q) on $X_1(54)$, and put $D_0 = \alpha_* D$ and $D_1 = \beta_* D$. Then $D_0 \neq D_1$.*

Proof. As $E(K)$ has a point of order 54, Lemma 2.14 shows that E has no complex multiplication. Suppose that $D_0 = D_1$, and let S be the support of D_0, a set of at most 10 geometric points of Z. Consider the directed graph with vertex set S and an edge from $\alpha(x^\sigma)$ to $\beta(x^\sigma)$ for every embedding σ of K into $\overline{\mathbb{Q}}$, where $x = (E, P_2, Q)$. As $D_0 = D_1$, every vertex has as many incoming as outgoing edges, so the graph contains a directed cycle $s_1 \to s_2 \to \cdots \to s_r \to s_1$ with $r \leq 10$ distinct vertices. Every edge $s_i \to s_{i+1}$ comes with an isogeny of degree 2 between elliptic curves representing s_i and s_{i+1} which maps the point of order 27 of the first to that of the second, up to sign. Composing these isogenies and an isomorphism, we obtain an endomorphism ψ of degree 2^r of an elliptic curve E_1 isogenous to E^σ for some σ, and a point $Q_1 \in E_1$ of order 27 with $\psi(Q_1) = \pm Q_1$. As E_1 has no complex multiplication, $\psi = \pm 2^{r/2}$, so r is even and $2^{r/2} \equiv \pm 1 \pmod{27}$. But 2 has order 18 modulo 27 and $2^9 \equiv -1 \pmod{27}$, so $r \geq 18$, which is a contradiction. □

Lemma 8.13. *Let c_* be a rational cusp of Z, and let $\mathcal{N}$ be a set of representatives of the 25 diamond orbits of the ordinary non-cuspidal closed points of $Z_{\mathbb{F}_2}$ of degree between 6 and 10 (Lemma 8.10 c)). Let $\mathcal{T}$ be the set of the triples (N, C'_a, C'_e) with $N \in \mathcal{N}$ and C'_a, C'_e effective cuspidal divisors on $Z_{\mathbb{F}_2}$ with $\deg N + \deg C'_a + \deg C'_e = 10$, such that*

$$\ell(N + C'_a + C'_e + \delta C'_e) \geq 2,$$

and let $\mathcal{P} \subseteq J_Z(\mathbb{Q})^2$ be the set of the pairs whose reductions modulo 2 are $\big([N + C'_a + C'_e - 10\overline{c_*}], [N + C'_a + \delta C'_e - 10\overline{c_*}]\big)$ for $(N, C'_a, C'_e) \in \mathcal{T}$. Then $\mathcal{P}$ has 4103 elements, and their first coordinates take 800 values.

Proof. As $\deg C'_a + \deg C'_e \leq 4$, the divisors C'_a and C'_e are supported on the 12 closed cusps of degree 1 and 2 (Lemma 8.10 b)). This gives 8825 triples (N, C'_a, C'_e) without the condition on ℓ, and we compute that $\ell(N + C'_a + C'_e + \delta C'_e) = 1$ for 4721 of them. The remaining 4104 triples form $\mathcal{T}$, and we compute that they give 4103 distinct pairs of classes in $J_Z(\mathbb{F}_2)$, with 800 distinct first coordinates. By Lemma 8.10 a) these pairs are the reductions of a unique set of pairs in $J_Z(\mathbb{Q})^2$. □

Lemma 8.14. *Let c_* and $\mathcal{P}$ be as in Lemma 8.13, and write $\overline{\xi}$ for the reduction modulo 5 of $\xi \in J_Z(\mathbb{Q})$. There are no $(\xi, \eta) \in \mathcal{P}$, no non-zero effective divisor L on $X_1(54)_{\mathbb{F}_5}$ with non-cuspidal support and no effective cuspidal divisors B_0, B_1 on $Z_{\mathbb{F}_5}$ of degree $10 - \deg L$ such that*

$$[\alpha_* L + B_0 - 10\overline{c_*}] = \overline{\xi} \qquad \text{and} \qquad [\beta_* L + B_1 - 10\overline{c_*}] = \overline{\eta}.$$

Proof. For each of the 800 first coordinates ξ we construct a divisor on $Z_{\mathbb{F}_5}$ in the class $10\overline{c_*} + \overline{\xi}$ from the expression of ξ in terms of the classes of rational cuspidal divisors (Lemma 8.10 a)), using the identification of the cusps of Lemma 8.10 b), and we compute its Riemann-Roch

space. Only 724 of these 800 spaces are non-zero. We list all the effective divisors in these 724 classes: 217 of them are cuspidal, and 1067 have a non-cuspidal part. If (ξ, η), L, B_0 and B_1 are as in the statement, then $B = \alpha_* L + B_0$ is an effective divisor in the class of $10\overline{c_*} + \overline{\xi}$. As $L \neq 0$ and α maps cusps to cusps and non-cusps to non-cusps, B is one of the 1067 divisors and $\alpha_* L$ is its non-cuspidal part. These 1067 divisors involve 192 distinct non-cuspidal closed points of $Z_{\mathbb{F}_5}$.

Above a non-cuspidal closed point y of $Z_{\mathbb{F}_5}$ of degree k, the closed points of $X_1(54)_{\mathbb{F}_5}$ correspond to the Frobenius orbits of the subgroups of order 2 of the elliptic curve of y, and hence to the irreducible factors of its 2-division polynomial over $\mathbb{F}_{5^k}$. A factor of degree e gives a closed point of degree ke whose push-forward under α is ey. So if y occurs with multiplicity m in $\alpha_* L$, then the points of L above y correspond to factors of degrees e_i with multiplicities n_i such that $\sum_i e_i n_i = m$. We compute that there are 361 closed points of $X_1(54)_{\mathbb{F}_5}$ above the 192 points, that their images under β are 334 distinct closed points, and that there are only 147 pairs (B, L) of one of the 1067 divisors B and an effective divisor L on $X_1(54)_{\mathbb{F}_5}$ such that $\alpha_* L$ is the non-cuspidal part of B: for 59 of them L has degree 10, and for 88 of them degree 9. For each of these pairs we compute the class $[\beta_* L + B_1 - 10\overline{c_*}]$ for every effective cuspidal divisor B_1 of degree $10 - \deg L$ on $Z_{\mathbb{F}_5}$, and find that it is never equal to $\overline{\eta}$ for a pair $(\xi, \eta) \in \mathcal{P}$ with $\overline{\xi} = [B - 10\overline{c_*}]$. □

Proposition 8.15. *The group $\mathbb{Z}/54\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree* 10.

Proof. Suppose the opposite, and let E/K be an elliptic curve over a decic field with a point of order 54. Then $E(K)$ contains points P_2 and Q of orders 2 and 27. By Lemma 8.9, E has good ordinary reduction at a prime $\mathfrak{p}$ of K above 2, of residue degree at least 6, and as two such primes would have residue degrees adding up to more than 10, $\mathfrak{p}$ is the only prime above 2 at which E has good reduction.

Suppose that P_2 does not reduce to 0 modulo $\mathfrak{p}$. Then $\phi : E \to E' = E/\langle P_2 \rangle$ reduces to a separable isogeny, and as the multiplication by 2 on the ordinary reduction of E has inseparable degree 2, the dual isogeny $\widehat{\phi}$ reduces to an inseparable one. The kernel of $\widehat{\phi}$ is $\phi(E[2])$, whose non-zero point R is K-rational, so R reduces to 0 modulo $\mathfrak{p}$. As E' is isogenous to E, it has the same reduction types, and $(E', R, \phi(Q))$ is again a point of $X_1(54)$ over K. So, replacing E by E' if necessary, we may assume that P_2 reduces to 0 modulo $\mathfrak{p}$. Let D be the trace divisor of $x = (E, P_2, Q)$ on $X_1(54)$, and put $D_0 = \alpha_* D$ and $D_1 = \beta_* D$. By Lemma 8.11 the reductions of D_0 and D_1 modulo 2 are $N + \overline{C_a} + \overline{C_e}$ and $N + \overline{C_a} + \delta\overline{C_e}$, and $D_1 + C_e \sim D_0 + \delta C_e$. Replacing Q by aQ for a suitable $a \in (\mathbb{Z}/27\mathbb{Z})^\times$, which replaces x, D, D_0, D_1, N, C_a and C_e by their images under $\langle a \rangle$, we may assume that $N \in \mathcal{N}$.

Suppose first that $\ell(N + \overline{C_a} + \overline{C_e} + \delta\overline{C_e}) = 1$ on $Z_{\mathbb{F}_2}$. The divisors $D_1 + C_e$ and $D_0 + \delta C_e$ are effective, linearly equivalent, and both reduce modulo 2 to $N + \overline{C_a} + \overline{C_e} + \delta\overline{C_e}$. As Z has good reduction at 2, semicontinuity gives $\ell(D_0 + \delta C_e) \leq 1$ over $\mathbb{Q}$, so $D_1 + C_e = D_0 + \delta C_e$. Comparing the non-cuspidal parts we get $D_1 = D_0$, which contradicts Lemma 8.12.

Hence $(N, \overline{C_a}, \overline{C_e})$ lies in the set $\mathcal{T}$ of Lemma 8.13, and the pair $(\xi, \eta) = ([D_0 - 10c_*], [D_1 - 10c_*]) \in J_Z(\mathbb{Q})^2$ lies in $\mathcal{P}$, as its reduction modulo 2 is the pair of classes of this triple. Now we reduce modulo 5. As $J_1(54)(\mathbb{Q})$ is finite [DEvH+21, Theorem 3.1(2)], by Lemma 8.8 and Proposition 2.5 a) with $p = 5$, the reduction of D modulo 5 is $L + \overline{C}$, where $L \neq 0$ is effective with non-cuspidal support and $\overline{C}$ is effective and cuspidal. As α and β map cusps to cusps

and non-cusps to non-cusps, the reductions of D_0 and D_1 modulo 5 are $\alpha_* L + \alpha_* \overline{C}$ and $\beta_* L + \beta_* \overline{C}$, whose classes relative to $10\overline{c_*}$ are $\overline{\xi}$ and $\overline{\eta}$. This contradicts Lemma 8.14. □

8.5. **The curve $X_1(56)$.** The group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/28\mathbb{Z}$ occurs over a decic field (Proposition 3.5), so we cannot exclude $\mathbb{Z}/56\mathbb{Z}$ by Lemma 4.3. We first sieve the reductions modulo 3 with push-forwards to $X_1(2,28)$ and $X_1(28)$, and treat the few remaining cases with Riemann-Roch computations on an explicit model of $X_1(56)$ as a double cover of $X_1(2,28)$.

As in [Naj26d, Section 11], the curve $X_1(2,28)$ parametrizes triples (E,P,Q) with P of order 2 and Q of order 28 such that $P \notin \langle Q\rangle$, and its universal elliptic curve $\mathcal{E}$ has the model

$$y^2 = x^3 + cx^2 + b(1-b-c)x, \qquad P = (0,0), \qquad Q = (b,b). \tag{8.1}$$

The functions b, $b(1-b-c)$ and $c^2 - 4b(1-b-c)$ are units on $Y_1(2,28)$ over $\mathbb{Z}[\frac{1}{56}]$ [Naj26d, Section 11]. The maps

$$(E,P,Q) \longmapsto (E, P + 14\beta Q, \gamma P + aQ), \qquad \beta,\gamma \in \{0,1\},\ a \in (\mathbb{Z}/28\mathbb{Z})^\times, \tag{8.2}$$

taken modulo -1, form a group of 24 level automorphisms of $X_1(2,28)$, which commute with T_q for odd primes $q \nmid 28$ and with the diamond operators [Naj26d, Section 11]. Let

$$\pi : X_1(56) \to X_1(2,28), \qquad (E,R) \longmapsto (E/\langle 28R\rangle, P_2, \phi(R)),$$

where $\phi : E \to E/\langle 28R\rangle$ is the quotient isogeny and P_2 is the non-zero point of the kernel of its dual $\widehat{\phi}$. The point $\phi(R)$ has order 28, and $P_2 \neq 14\phi(R)$, as $\widehat{\phi}(14\phi(R)) = 28R \neq 0$. The map π has degree 2, and it maps the diamond operator $\langle a\rangle$ of $X_1(56)$ to the automorphism (8.2) with $\beta = \gamma = 0$ and the same a. Let $\rho_1,\dots,\rho_4 : X_1(2,28) \to X_1(28)$ be the 4 maps of [Naj26d, Section 11], which keep Q or $P+Q$, or divide E by $\langle P\rangle$ or by $\langle P + 14Q\rangle$ and keep the image of Q.

By [DEvH+21, Theorem 3.1(2) and (3)] the groups $J_1(56)(\mathbb{Q})$ and $J_1(2,28)(\mathbb{Q})$ are finite. The curve $X_1(56)$ has genus 61 and $i(56) = 1152$, so $\operatorname{gon}_{\mathbb{Q}} X_1(56) \geq \operatorname{gon}_{\mathbb{C}} X_1(56) \geq \frac{325}{2^{15}} \cdot 1152 > 11.4$ by Abramovich's bound, and $X_1(2,28)$ has genus 25 and $\operatorname{gon}_{\mathbb{Q}} X_1(2,28) \geq 12$ [NV26, Table 1]. The group $J_1(28)(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}\times\mathbb{Z}/936\mathbb{Z}$ is generated by rational cuspidal divisor classes [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], and its reduction G_{28} has index 4 in $J_1(28)(\mathbb{F}_3) \simeq (\mathbb{Z}/4\mathbb{Z})^2\times\mathbb{Z}/24\mathbb{Z}\times\mathbb{Z}/936\mathbb{Z}$ [Naj26d, Section 11.2] (see also `computations/d31a_C56_target28_setup.m`). We fix a rational cusp z_* of $X_1(28)$, and we write $\mathcal{S}_j \subseteq J_1(28)(\mathbb{F}_3)$ for the sets of (2.1) with $y_0 = z_*$. The closed cusps of $X_1(2,28)_{\mathbb{F}_3}$ have degrees $1^{12}, 2^6, 3^4, 6^2$, those of degree 1 and 2 are reductions of rational cuspidal divisors of the same degree, and for every closed cusp c of degree 3 the divisor $A_5 c$ is one of 17 explicit divisors [Naj26d, Section 11.2]. We write $\mathcal{A}$ for the set of these 17 divisors, which contains 0.

Lemma 8.16. *Let $D' \neq 0$ be an effective divisor of degree $e \leq 10$ on $X_1(56)_{\mathbb{F}_3}$ with non-cuspidal support, and suppose that*

a) $[(\rho_i \circ \pi)_* D' - e\overline{z_*}] \in G_{28} + \mathcal{S}_{10-e}$ *for $i = 1,2,3,4$, and*
b) *there is an effective cuspidal divisor C_Y of degree $10-e$ on $X_1(2,28)_{\mathbb{F}_3}$ such that $A_5(\pi_* D' + C_Y)$ is principal.*

Then, up to the diamond operators, D' is one of the 11 divisors of Table 6.

divisors D'	type	label of $\pi_* D'$
65	[8]	8
271, 327	[10]	14
491, 578	[10]	26
492, 737	[10]	27
818, 837	[5, 5]	36
978, 1009	[5, 5]	41

TABLE 6. The divisors D' of Lemma 8.16, and the labels of their push-forwards to $X_1(2,28)_{\mathbb{F}_3}$ up to the automorphisms (8.2).

Proof. By Table 5 the type of D' is one of $[5], \dots, [10]$ and $[5,5]$. Taking a representative of each diamond orbit, and for the type $[5,5]$ the first point among the 6 representatives and the second one among all the 72 closed points of degree 5, we obtain $797 + 432 = 1229$ divisors D', which we number as in `continuation_20261031a/C56/fourmap_filter.m`. Condition a) is invariant under the diamond operators, as in the proof of Lemma 8.3. We compute that a) holds for only 135 of the 1229 divisors: 2, 6, 11, 8 and 48 of the types $[6], \dots, [10]$, and 60 of type $[5,5]$.

Up to the 24 automorphisms (8.2), the push-forwards $\pi_* D'$ of these 135 divisors give 41 divisors on $X_1(2,28)_{\mathbb{F}_3}$, which we number as in `continuation_20261031b/Y228_shared/union_cases.m`. Condition b) is invariant under these automorphisms, as they commute with A_5 and permute the effective cuspidal divisors of each degree. If $\deg C_Y \le 2$, then C_Y is supported on the closed cusps of degree 1 and 2, and $A_5 C_Y = 0$. If $3 \le \deg C_Y \le 4$, then C_Y contains at most one closed cusp of degree 3, and $A_5 C_Y \in \mathcal{A}$. As $\deg C_Y = 10 - e$, only $A = 0$ occurs if $e \ge 8$. We compute on the function field of $X_1(2,28)_{\mathbb{F}_3}$ that $A_5(\pi_* D') + A$ is not principal for all $A \in \mathcal{A}$ if $e \le 7$, and for $A = 0$ if $e \ge 8$, except for the 6 divisors with labels 8, 14, 26, 27, 36 and 41. These are the push-forwards of 15 of the 135 divisors D', which form the 11 diamond orbits of Table 6 (see `continuation_20261031b/C56/d31b_C56_final_source_subset.py`). □

Next we give a model of $X_1(56)$ as a double cover of $X_1(2,28)$.

Lemma 8.17. *Let k be $\mathbb{Q}$ or $\mathbb{F}_3$, let b, c be the functions of (8.1) on $X_1(2,28)_k$, and put $s = c^2 - 4b(1-b-c)$. Then $k(X_1(56)) = k(X_1(2,28))(z)$ with $z^2 = b$, and π corresponds to this extension. The point*

$$R = \big(2b + c + 2z,\ 2z(2b + c + 2z)\big)$$

on $E'' : y^2 = x^3 - 2cx^2 + sx$ has order 56, and the isogeny $E'' \to \mathcal{E}$, $(x,y) \mapsto \big((x + s/x - 2c)/4,\ y(1 - s/x^2)/8\big)$, whose kernel is generated by $(0,0)$, maps R to Q. Here $E'' = \mathcal{E}/\langle P \rangle$. The map π is unramified outside the cusps.

Proof. Write $u = 2b + c + 2z$. Using $z^2 = b$, a direct computation gives $u^2 - 2cu + s = 4bu$, so $u(u^2 - 2cu + s) = (2zu)^2$ and R lies on E'', and $u^2 - s = 4zu$. Hence the isogeny maps R to the point with coordinates $(u^2 - 2cu + s)/(4u) = b$ and $2zu(u^2 - s)/(8u^2) = b$, which is Q. So R has order 28 or 56, and we check that $28R \neq 0$ in characteristic 3, so also in characteristic 0. Hence $28R$ is a non-zero point which the isogeny maps to $28Q = 0$, so $28R = (0,0)$, and $E''/\langle 28R \rangle \simeq \mathcal{E}$, with the kernel of the dual isogeny generated by P. So (E'', R) is a point of $X_1(56)$ over $k(X_1(2,28))(z)$ whose image under π is the generic point $(\mathcal{E}, P, Q)$ of $X_1(2,28)$.

As π has degree 2 and b is not a square (its divisor has odd valuations at 24 cusps, as we compute), this identifies $k(X_1(56))$ with $k(X_1(2,28))(z)$, and we also check that the genus of this function field over $\mathbb{F}_3$ is 61. As b is a unit on $Y_1(2,28)$, the divisor of b is supported on the cusps, so π is unramified outside the cusps. □

Lemma 8.18. *Let D' be one of the 11 divisors of Table 6, and let $q = 11$ if D' has degree 8 and $q = 5$ otherwise. Then $A_q D'$ is not principal on $X_1(56)_{\mathbb{F}_3}$.*

Proof. Let F_Y be the function field of $X_1(2,28)_{\mathbb{F}_3}$, and $L_Y = F_Y(z)$ that of $X_1(56)_{\mathbb{F}_3}$, with $z^2 = b$ as in Lemma 8.17. We compute $T_q D'$ from the isogenies of degree q of the elliptic curves of the points in the support of D' on the moduli model, including the residue degrees, and we locate the places of L_Y in the support of $G = A_q D'$ using the value of z at the corresponding point of order 56. Write $G = \sum n_{\mathfrak{Q}} \mathfrak{Q}$. Its support contains no cusp, so π is unramified at it by Lemma 8.17. For a place $\mathfrak{q}$ of F_Y put $a_{\mathfrak{q}} = \max(\{0\} \cup \{n_{\mathfrak{Q}} : \mathfrak{Q} \mid \mathfrak{q}\})$ and $H = \sum a_{\mathfrak{q}} \mathfrak{q}$. Then $G \le \pi^* H$. As the divisor $\pi^* H$ is invariant under $z \mapsto -z$ and the characteristic is not 2, we have

$$L(\pi^* H) = L(H) \oplus z\, L(H + R_b), \qquad R_b = \left\lfloor \tfrac{1}{2} \operatorname{div}(b) \right\rfloor,$$

where the spaces on the right are Riemann-Roch spaces on $X_1(2,28)_{\mathbb{F}_3}$. A function $g \in L(\pi^* H)$ lies in $L(G)$ if and only if at every place $\mathfrak{Q} \mid \mathfrak{q}$ with $n_{\mathfrak{Q}} < a_{\mathfrak{q}}$ the first $a_{\mathfrak{q}} - n_{\mathfrak{Q}}$ coefficients of the expansion of $t^{a_{\mathfrak{q}}} g$ vanish, where t is a local parameter at $\mathfrak{Q}$, and these are $(a_{\mathfrak{q}} - n_{\mathfrak{Q}}) \deg \mathfrak{Q}$ linear conditions over $\mathbb{F}_3$. We compute bases of $L(H)$ and $L(H + R_b)$, local parameters at the places in the support of G by Hensel lifting on the plane model, and the matrix of these conditions. For the 2 divisors with label 27 we compute $T_5 D'$ and this matrix in the same way (see `additions/C56/rr56_case492.log` and `additions/C56/rr56_case737.log`). The results are the following:

label	q	$\deg H$	$\ell(H)$	$\ell(H + R_b)$	conditions	rank
$14, 26, 27, 36, 41$	5	60	36	24	120	60
8	11	96	72	60	192	132

In all 11 cases the rank is $\ell(H) + \ell(H + R_b)$, so $L(G) = 0$. □

Proposition 8.19. *The group $\mathbb{Z}/56\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let D be the trace divisor on $X_1(56)$ of a point x of order 56 over a decic field. As $\operatorname{gon}_{\mathbb{Q}} X_1(56) > 10$, Proposition 2.5 a) with $p = 3$ shows that the reduction of D modulo 3 is $D' + C'$ with $D' \neq 0$ of degree e. Applying (2.1) to $(\rho_i \circ \pi)_* D$ shows that D' satisfies condition a) of Lemma 8.16. By Proposition 2.2 d) on $X_1(2,28)$ the divisor $A_5(\pi_* D)$ is principal, so $A_5(\pi_* D' + \pi_* C')$ is principal, and D' satisfies condition b) with $C_Y = \pi_* C'$. Replacing x by its image under a diamond operator, we may assume by Lemma 8.16 that D' is one of the divisors of Table 6.

If D' has degree 8, then C' has degree 2, and we compute that σ_{11} fixes each of the 27 closed cusps of degree at most 2 of $X_1(56)_{\mathbb{F}_3}$, so $A_{11} C' = 0$ by Lemma 2.3. Otherwise $C' = 0$. So by Proposition 2.2 d) on $X_1(56)$ the divisor $A_q D'$ is principal, with q as in Lemma 8.18, which contradicts this lemma. □

8.6. **The curves $X_1(58)$ and $X_1(62)$.** Over nonic fields the groups $\mathbb{Z}/58\mathbb{Z}$ and $\mathbb{Z}/62\mathbb{Z}$ are excluded in [Naj26d, Proposition 6.11] by pushing the trace divisor forward to $X_1(29)$, respectively $X_1(31)$, and comparing the classes of the possible reductions modulo 3 with the

reduction of the Mordell-Weil group. We do the same in degree 10. The new cases are the closed points of degree 10 and, for $X_1(62)$, the sums of two closed points of degree 5. Some classes survive, and they are the reductions of known points of $X_1(29)$ and $X_1(31)$.

Lemma 8.20. *Let $N \in \{29, 31\}$, put $n = 2N$ and $Y = X_1(N)$, and let $\pi : X_1(n) \to Y$ be the morphism $(E, P) \mapsto (E, 2P)$. Let $H \subseteq J_Y(\mathbb{F}_3)$ be the reduction of $J_Y(\mathbb{Q})$.*

a) *We have $\operatorname{gon}_{\mathbb{Q}} X_1(29) = 11$ and $\operatorname{gon}_{\mathbb{Q}} X_1(31) = 12$. The groups*

$$J_1(29)(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/64427244\mathbb{Z}, \qquad J_1(31)(\mathbb{Q}) \simeq \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/1772833370\mathbb{Z}$$

are generated by the classes of rational cuspidal divisors, and reduction modulo 3 is injective on them. We have

$$J_1(29)(\mathbb{F}_3) \simeq (\mathbb{Z}/4\mathbb{Z})^3 \times (\mathbb{Z}/8\mathbb{Z})^2 \times \mathbb{Z}/386563464\mathbb{Z},$$
$$J_1(31)(\mathbb{F}_3) \simeq (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/3352427902670\mathbb{Z},$$

in which H has index $2^9 \cdot 3$, respectively $2^2 \cdot 31 \cdot 61$.

b) *The closed cusps of $Y_{\mathbb{F}_3}$ have degrees $1^{N'}, N'$, where $N' = (N-1)/2$, and those of degree 1 are the reductions of the N' rational cusps of Y.*

c) *Let Q be a non-cuspidal closed point of $X_1(n)_{\mathbb{F}_3}$ of degree $e \leq 10$, and let $P = \pi(Q)$, a closed point of degree k. If $N = 29$, then either $k = e \in \{6, \dots, 10\}$ and the elliptic curve corresponding to P has a point of order 2 over the residue field of P, or $k = 3$, $e = 9$ and $\pi_* Q = 3P$. If $N = 31$, then the elliptic curve corresponding to P has a point of order 2 over the residue field of P, and either $k = e \in \{5, \dots, 10\}$, or $k = 5$, $e = 10$ and $\pi_* Q = 2P$.*

Proof. The gonalities are [DvH14, Theorem 4 and Table 1], the Mordell-Weil groups and their generation by rational cuspidal divisors are [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], and injectivity follows from Katz's result, as $J_Y(\mathbb{Q})$ is finite. The groups $J_Y(\mathbb{F}_3)$ and the indices of H are computed in the proof of [Naj26d, Proposition 6.11], with Magma's proven class group algorithm (see `continuation_20261031a/C58/inputs/C58_X129/build_presentation.m` and its analogue for $N = 31$). Part b) holds as 3 has order $N - 1$ modulo N (see [Naj26d, Proposition 6.11]).

For c), note that the fibre of π above a non-cuspidal point (E, P_N) consists of the points $(E, P'_N + T)$, where P'_N is the unique point of order N with $2P'_N = P_N$ and T runs over $E[2] \setminus \{0\}$. Hence $e = rk$, where $r \in \{1, 2, 3\}$ is the degree of the irreducible factor of the 2-division polynomial of the elliptic curve corresponding to P that belongs to Q, and $\pi_* Q = rP$. By [Naj26d, Table 3], the curve $X_1(58)_{\mathbb{F}_3}$ has no non-cuspidal closed points of degree at most 5, the curve $X_1(62)_{\mathbb{F}_3}$ none of degree at most 4, and $X_1(29)_{\mathbb{F}_3}$ and $X_1(31)_{\mathbb{F}_3}$ none of degree at most 2, respectively 3. If $r = 2$, then the 2-division polynomial at P is the product of a linear and a quadratic factor, and the linear factor gives a non-cuspidal closed point of $X_1(n)_{\mathbb{F}_3}$ of degree $k = e/2 \leq 5$, so $N = 31$ and $k = 5$. If $r = 3$, then $k \leq 3$, so $N = 29$ and $k = 3$. In the remaining case $r = 1$ and $k = e$. In all the cases with $N = 31$ the 2-division polynomial at P has a root, which proves c). □

Lemma 8.21. *Let $Y = X_1(29)$, let c_0 be a rational cusp of Y, and let H be as in Lemma 8.20. Let P be a non-cuspidal closed point of $Y_{\mathbb{F}_3}$ of degree k, and assume that either $k \in \{6, \dots, 10\}$ and the elliptic curve corresponding to P has a point of order 2 over the residue field of P, or $k = 3$. Then $[P - k\,\overline{c_0}] \notin H$ if $k \geq 6$, and $[3P - 9\,\overline{c_0}] \notin H$ if $k = 3$, except for 21 closed points P of degree 10. These 21 points are the reductions of the closed points of degree 10 of $X_1(29)$ in the $\Delta(29)$-orbits of the points 1.29.10.a and 1.29.10.b of*

van Hoeij [vH14, Naj26b]*, and the elliptic curves corresponding to these two points have no point of order* 2 *over their residue fields.*

Proof. For $k \leq 9$ these are the 14, 84, 168, 476 and 1582 tests in degrees 3, 6, 7, 8 and 9 of [Naj26d, Proposition 6.11], none of which lies in H (see `continuation_20261031a/C58/inputs/C58_X129/classify58.m`). Note that H is stable under the diamond operators and contains $[\langle a\rangle\overline{c_0} - \overline{c_0}]$, so $[\langle a\rangle P - k\,\overline{c_0}] = \langle a\rangle[P - k\,\overline{c_0}] + k[\langle a\rangle\overline{c_0} - \overline{c_0}]$ lies in H if and only if $[P - k\,\overline{c_0}]$ does, and it suffices to test one point in each $\Delta(29)$-orbit. We compute that $Y_{\mathbb{F}_3}$ has 5971 non-cuspidal closed points of degree 10, in 430 orbits under $\Delta(29)$, that the elliptic curve has a point of order 2 over the residue field at 4060 of them, which form 293 orbits, and that for the representatives of exactly 2 of these 293 orbits, of lengths 7 and 14, the class $[P - 10\,\overline{c_0}]$ lies in H (see `jobs/d31a_C58_class_filter.log`).

The points 1.29.10.a and 1.29.10.b have residue fields $\mathbb{Q}(a)$ with

$$f_a = a^{10} - 2a^9 + 2a^8 - 5a^7 + 7a^6 - 4a^5 + 4a^4 - 8a^3 + 5a^2 - 1,$$
$$f_b = a^{10} - 5a^9 + 15a^8 - 31a^7 + 47a^6 - 56a^5 + 51a^4 - 37a^3 + 20a^2 - 7a + 1.$$

We compute that f_a and f_b are irreducible modulo 3, and that the reductions of the 14 diamond translates of these two points are the 7, respectively 14, points of the two surviving orbits. We also find that f_a and f_b have the simple roots 11, respectively 5, modulo 29, and at the corresponding primes of degree 1 the elliptic curves have good reduction with 29 points. As reduction is injective on the torsion of order prime to 29, these curves have no point of order 2 over their residue fields. □

Proposition 8.22. *The group $\mathbb{Z}/58\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree* 10.

Proof. Let E/K have a point P_{58} of order 58, where $[K : \mathbb{Q}] = 10$, let D be the trace divisor of $x = (E, P_{58})$ on $X_1(58)$, and let Y, π, H be as in Lemma 8.20 with $N = 29$. Then $D_Y := \pi_* D$ is the trace divisor of $\pi(x) = (E, 2P_{58})$. By Lemma 8.20 a) and Proposition 2.5 a), applied to Y with $p = 3$ and $d = 10$, the reduction of D_Y modulo 3 is not cuspidal. So the reduction of D is $D' + C'$ with $D' \neq 0$, and by Lemma 8.20 c) every non-cuspidal closed point of $X_1(58)_{\mathbb{F}_3}$ of degree at most 10 has degree at least 6, so D' is a single closed point Q of degree $e \in \{6, \ldots, 10\}$ and C' has degree $10 - e \leq 4$. The divisor $\pi_* C'$ is cuspidal of degree at most 4, so by Lemma 8.20 b) it is supported on the reductions of the rational cusps, and its class, normalized at a rational cusp c_0, lies in H. By Lemma 2.16 applied to D_Y we get $[\pi_* Q - e\,\overline{c_0}] \in H$. By Lemma 8.20 c) the divisor $\pi_* Q$ is a closed point P of degree $e \geq 6$ at which the elliptic curve has a point of order 2 over the residue field, or $3P$ with P of degree 3, so by Lemma 8.21, $e = 10$, $C' = 0$, and $\pi_* Q = \overline{B}$ for a closed point B of degree 10 of Y in the $\Delta(29)$-orbit of one of the points 1.29.10.a and 1.29.10.b.

So D_Y and B have the same reduction, and as $[D_Y - B] \in J_Y(\mathbb{Q})$ and reduction modulo 3 is injective on $J_Y(\mathbb{Q})$, we get $D_Y \sim B$. As $\operatorname{gon}_{\mathbb{Q}} Y = 11 > 10$, Lemma 2.8 a) gives $D_Y = B$. Hence $\pi(x)$ is a K-rational point of Y above the closed point B, and as Y is a fine moduli space, E is isomorphic over K to a conjugate of the elliptic curve of B over its residue field. By Lemma 8.21 this curve has no point of order 2 over its residue field, which contradicts $29P_{58} \in E(K)$. □

Lemma 8.23. *Let $Y = X_1(31)$, let c_0 be a rational cusp of Y, and let H be as in Lemma 8.20. Let $\mathcal{P}_k$ be the set of non-cuspidal closed points of $Y_{\mathbb{F}_3}$ of degree k at which the elliptic curve has a point of order* 2 *over the residue field.*

a) *For* $5 \le k \le 10$ *and* $P \in \mathcal{P}_k$ *we have* $[P - k\,\overline{c_0}] \notin H$*, except for* 5 *points of degree* 9*. These* 5 *points are the reductions of the* 15 *diamond translates of the closed point* B_{31} *of degree* 9 *given by the point* x_{31} *of* [Naj26d, Proposition 13.5].
b) *For* $P, P' \in \mathcal{P}_5$*, not necessarily distinct, we have* $[P + P' - 10\,\overline{c_0}] \notin H$.

Proof. For $k \le 9$ there are 90, 90, 180, 630 and 1200 tests in degrees $5, \dots, 9$, and the computation in the proof of [Naj26d, Proposition 6.11] shows that exactly 5 classes lie in H, all of degree 9, and that these 5 points are the reductions of the diamond translates of B_{31} (see `continuation_20261031a/C62/inputs/C62_X131/classify62.m` and `continuation_20261031a/C62/inputs/C62_X131/known31/verify_known31.py`). We also check that the residue field of B_{31} is inert at 3. As in the proof of Lemma 8.21 it suffices to test one point in each orbit under $\Delta(31)$, and we compute that $Y_{\mathbb{F}_3}$ has 5685 non-cuspidal closed points of degree 10, in 379 orbits, that 3795 of them, in 253 orbits, lie in $\mathcal{P}_{10}$, and that none of the 253 representatives has class in H (see `jobs/d31a_C62_class_resume_v2.log`). This proves a).

The set $\mathcal{P}_5$ has 90 elements, so there are 4095 unordered pairs $\{P, P'\}$ with possibly $P = P'$, and we compute that none of the classes $[P + P' - 10\,\overline{c_0}]$ lies in H. □

Proposition 8.24. *The group* $\mathbb{Z}/62\mathbb{Z}$ *is not a subgroup of the torsion of an elliptic curve over a number field of degree* 10.

Proof. Let E/K have a point P_{62} of order 62, where $[K : \mathbb{Q}] = 10$, let D be the trace divisor of $x = (E, P_{62})$ on $X_1(62)$, and let Y, π, H be as in Lemma 8.20 with $N = 31$, and $D_Y = \pi_* D$. As in the proof of Proposition 8.22, Proposition 2.5 a), applied to Y with $p = 3$, $d = 10$ and $\operatorname{gon}_{\mathbb{Q}} Y = 12$, shows that the reduction of D is $D' + C'$ with $D' \neq 0$. The non-cuspidal closed points of $X_1(62)_{\mathbb{F}_3}$ of degree at most 10 have degree at least 5 by Lemma 8.20 c), so D' is either a single closed point Q of degree $e \in \{5, \dots, 10\}$, or a sum $Q + Q'$ of two closed points of degree 5, possibly equal. In both cases C' has degree at most 5, so $\pi_* C'$ is supported on the reductions of the rational cusps by Lemma 8.20 b), and Lemma 2.16 applied to D_Y gives $[\pi_* D' - e\,\overline{c_0}] \in H$, where $e = \deg D'$.

If $D' = Q + Q'$, then $\pi_* D' = P + P'$ with $P, P' \in \mathcal{P}_5$ by Lemma 8.20 c), which is impossible by Lemma 8.23 b). If $D' = Q$ and $\pi_* Q = 2P$ with P of degree 5, then again $P \in \mathcal{P}_5$, and this is excluded by Lemma 8.23 b) with $P' = P$. In the remaining case $\pi_* Q = P \in \mathcal{P}_e$, so by Lemma 8.23 a) we have $e = 9$ and $P = \overline{B'}$ for a diamond translate B' of B_{31}, and C' is a cusp of degree 1, the reduction of a rational cusp c. So D_Y and $B' + c$ have the same reduction, hence $D_Y \sim B' + c$ by the injectivity of reduction on $J_Y(\mathbb{Q})$, and $D_Y = B' + c$ by Lemma 2.8 a), as $\operatorname{gon}_{\mathbb{Q}} Y = 12 > 10$. This is a contradiction, as the support of D_Y contains no cusp. □

8.7. **The curve** $X_1(60)$**.** A point of order 60 gives, after an isogeny of degree 2, a point of $X_1(2, 30)$ over the same field, and we use the quotients of $X_1(2, 30)$ from [Naj26d, Section 11.3], where $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ is excluded in the degrees $6, \dots, 9$. Over number fields of degree 10 the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ occurs (Proposition 3.5), so we have to use the point of order 60 itself. It enters at two places: through the quintic points of $X_1(30)$ (Lemma 8.27) and through a halving condition at the closed points of $X_1(2, 30)$ over finite fields (Lemma 8.28).

The following lemma collects the set-up of [Naj26d, Section 11.3].

Lemma 8.25. *Let* $X = X_1(2, 30)$*, whose points are triples* (E, P, Q) *with* P *of order* 2 *and* Q *of order* 30 *such that* $P \neq 15Q$*. Let* $\alpha : X \to W$ *be the quotient of* X *by the automorphism* $(E, P, Q) \mapsto (E, 15Q, P + Q)$ *of order* 3*, and let* $f : W \to X_1(15)$ *be the morphism through*

which $(E,P,Q)\mapsto(E,2Q)$ factors. Let c_W be a rational cusp of W, and let $H\subseteq J_W(\mathbb{Q})$ be the subgroup generated by the classes $[C-(\deg C)c_W]$, where C runs over the Galois orbits of cusps of W. Let $Y=X_1(30)$, let y_0 be a rational cusp of Y, and let $\pi_1,\pi_2,\pi_3: X\to Y$ be the morphisms

$$\pi_1(E,P,Q)=(E,Q),\qquad \pi_2(E,P,Q)=(E,P+16Q),\qquad \pi_3(E,P,Q)=(E,P+Q).$$

Then W has genus 9, f is the double cover given by a square root of the discriminant of the universal elliptic curve over $X_1(15)$ in Tate normal form, every cusp of $X_1(15)$ is totally ramified in f, the Galois orbits of cusps of W have degrees $1,1,4,2,4,1,2,1$, and the following hold.

a) *The group $J_X(\mathbb{Q})$ is finite and generated by the classes of rational cuspidal divisors, and for every effective rational divisor D of degree d on X we have $[\alpha_*D-d\,c_W]\in H$.*
b) *The group $J_W(\mathbb{Q})$ is finite, reduction modulo 7 is injective on it, and*
$$J_W(\mathbb{F}_7)\simeq(\mathbb{Z}/2\mathbb{Z})^6\times\mathbb{Z}/102\mathbb{Z}\times\mathbb{Z}/10608\mathbb{Z},\qquad H\simeq(\mathbb{Z}/2\mathbb{Z})^5\times\mathbb{Z}/8\mathbb{Z}.$$
c) *Let y be a non-cuspidal closed point of $W_{\mathbb{F}_7}$ of degree k. Then either there are 3 closed points of $X_{\mathbb{F}_7}$ above y, each of degree k, or there is one closed point z above y, of degree $3k$, with $\alpha_*z=3y$.*
d) *We have $J_Y(\mathbb{Q})\simeq\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/8160\mathbb{Z}$, generated by the classes of rational cuspidal divisors, and $J_Y(\mathbb{F}_7)\simeq(\mathbb{Z}/4\mathbb{Z})^3\times\mathbb{Z}/136\mathbb{Z}\times\mathbb{Z}/16320\mathbb{Z}$, in which the reduction G of $J_Y(\mathbb{Q})$ has index 4352. The images in $J_Y(\mathbb{F}_7)/G$ of the sets $\mathcal{S}_0,\dots,\mathcal{S}_6$ of (2.1), for $\overline{y_0}$, have 1, 9, 41, 67, 68, 68 and 68 elements.*

Proof. All of this is in [Naj26d, Section 11.3], apart from the set $\mathcal{S}_6$. The finiteness and the generation in a) are [DEvH+21, Theorem 3.1(3), Proposition 4.16 and Table 3], and $J_Y(\mathbb{Q})$ in d) is [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2]. We compute the images of $\mathcal{S}_0,\dots,\mathcal{S}_6$. □

Lemma 8.26. *Let W, f, c_W and H be as in Lemma 8.25, let ι be the non-trivial automorphism of W over $X_1(15)$, and let $C_1,\dots,C_8$ be the Galois orbits of cusps of W. Every class in H is of the form $[L-10\,c_W]$ for an effective rational cuspidal divisor $L=\sum_i v_iC_i$ of degree 10 on W. For a fixed choice of such divisors L, one for each of the 256 classes, put*

$$B=\sum_i\lfloor v_i/2\rfloor f(C_i),\qquad C=\sum_i(v_i \bmod 2)\,C_i,$$

so that $L=f^*B+C$. Then exactly one of the following holds.

a) *(168 classes) $C\neq 0$, and every effective rational divisor linearly equivalent to L is of the form $f^*B'+C$ for an effective rational divisor B' on $X_1(15)$.*
b) *(4 classes) $C=0$, $\deg B=5$, and every effective rational divisor linearly equivalent to L is of the form f^*B' for an effective rational divisor B' of degree 5 on $X_1(15)$.*
c) *(84 classes) Both eigenspaces of ι on $L(\overline{L})$ over $\mathbb{F}_7$ are non-zero, and $\ell(\overline{L})=2$ for 60 of these classes and $\ell(\overline{L})=3$ for the other 24.*

Proof. We compute the effective rational cuspidal divisors of degree 10, which represent all 256 classes of H, and for the chosen representatives L we compute $\ell(\overline{L})$ on $W_{\mathbb{F}_7}$ and the dimensions of the two eigenspaces of ι on $L(\overline{L})$. As every cusp of $X_1(15)$ is totally ramified in f, the ι-invariant functions in $L(\overline{L})$ are the functions $h\circ f$ with $h\in L(\overline{B})$. We find that for 168 classes the (-1)-eigenspace is 0 and $\ell(\overline{L})=\ell(\overline{B})=k$ with $k=2$, 3 and 4 for 72, 64 and 32 of them, so that $\deg C=10-2k>0$, that for 4 classes the (-1)-eigenspace is

0, $C = 0$ and $\ell(\overline{L}) = \ell(\overline{B}) = 5$, and that for the remaining 84 classes both eigenspaces are non-zero, of dimensions 1 and 1 for 60 classes, and 1 and 2, in some order, for 24 classes.

In the first two cases $\deg B = k \geq 2$, so $\ell(B) = k$ by the Riemann-Roch theorem on the curve $X_1(15)$ of genus 1. Hence $f^*L(B) \subseteq L(L)$ has dimension k over $\mathbb{Q}$, and by semicontinuity [Har77, Theorem III.12.8] $\ell(L) \leq \ell(\overline{L}) = k$, so $L(L) = f^*L(B)$. Every effective rational divisor linearly equivalent to L is $L + \operatorname{div}(h \circ f) = f^*(B + \operatorname{div} h) + C$ for some $h \in L(B)$, which proves a) and b). □

Lemma 8.27. *Let F be a number field of degree 5, let E/F be an elliptic curve with a point of order 30 over F, and let $M = F(E[2])$. Assume that $[M : F] = 2$. Then no elliptic curve over M which is 2-isogenous to E over M has a point of order 60 over M.*

Proof. By [Naj26a, Proposition 9.2], the pair (F, E) is isomorphic to one of the pairs (K_{30}, E_{30}) and (K_{30}, E'_{30}) of [Naj26a, Proposition 9.1], where K_{30} is the quintic field defined by $t^5+t^4-3t^3+3t+1$, so we may assume that E is one of these two curves. As $E[2] \subseteq E(M)$, the curves 2-isogenous to E over M are the 3 curves $E/\langle T\rangle$ with $T \in E[2] \setminus \{0\}$. For both curves E we compute with Magma's function `TorsionSubgroup` that each of these 3 curves has torsion subgroup $\mathbb{Z}/30\mathbb{Z}$ over M (see `additions/C60/tors60.log`). □

Lemma 8.28. *Let X, α, Y, π_1, π_2, π_3, y_0 and G be as in Lemma 8.25, and let $\mathcal{S}_j \subseteq J_Y(\mathbb{F}_7)$ be the sets of (2.1) for $\overline{y_0}$. Let L be one of the 84 divisors of Lemma 8.26 c), and let $\overline{D}$ be an effective divisor of degree 10 on $X_{\mathbb{F}_7}$ which is not entirely cuspidal and satisfies $\alpha_*\overline{D} \sim \overline{L}$. Write $\overline{D} = D' + C'$, with D' non-cuspidal of degree e and C' cuspidal. Then one of the following holds.*

a) *$[\pi_{i*}D' - e\,\overline{y_0}] \notin G + \mathcal{S}_{10-e}$ for some $i \in \{1, 2, 3\}$.*
b) *$C' = 0$, and D' contains with multiplicity 1 a closed point (E_1, P, Q), with residue field κ, such that there is no point $S \in (E_1/\langle P\rangle)(\kappa)$ with $2S = \phi(Q)$ and $\widehat{\phi}(S) = Q$, where $\phi : E_1 \to E_1/\langle P\rangle$ is the quotient map and $\widehat{\phi}$ its dual.*

Proof. As $\alpha_*\overline{D}$ is effective, it is one of the members of the linear system $|\overline{L}|$ over $\mathbb{F}_7$, and there are $60 \cdot 8 + 24 \cdot 57 = 1848$ of them by Lemma 8.26 c). For each member M we run through the effective divisors D' on $X_{\mathbb{F}_7}$ with non-cuspidal support such that α_*D' is the non-cuspidal part of M, using Lemma 8.25 c): above a point y of multiplicity m in M, if there are 3 points of the same degree above y, then m is distributed in all possible ways among them, and if there is one point z above y, then $3 \mid m$ and z has multiplicity $m/3$. The cuspidal part is not restricted. We find 3414 possible non-zero D', supported on 1674 closed points of $X_{\mathbb{F}_7}$. For these we compute the classes $[\pi_{i*}D' - e\,\overline{y_0}]$, and find that all three lie in $G + \mathcal{S}_{10-e}$ for only 24 of them. These 24 divisors have degree 10, so $C' = 0$, and they are sums of distinct closed points with multiplicity 1, of degrees $2+2+3+3$ (12 of them) or $2+4+4$ (12 of them). For each of the 72 closed points occurring in them we compute the points S as in b), and find that each of the 24 divisors contains a point for which there is no such S. □

Proposition 8.29. *The group $\mathbb{Z}/60\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let X, α, W, f, Y, π_1, π_2, π_3, y_0, G and H be as in Lemma 8.25, and let $\mathcal{S}_j \subseteq J_Y(\mathbb{F}_7)$ be the sets of (2.1) for $\overline{y_0}$. Let E_{60}/K have a point R of order 60, where $[K : \mathbb{Q}] = 10$. Let $\phi_0 : E_{60} \to E = E_{60}/\langle 30R\rangle$, let P be the non-zero point of $\ker \widehat{\phi_0} = \phi_0(E_{60}[2])$, and put $Q = \phi_0(R)$, a point of order 30. Then $\widehat{\phi_0}(15Q) = 30R \neq 0 = \widehat{\phi_0}(P)$, so $P \neq 15Q$,

and $x = (E, P, Q)$ is a point of $Y_1(2,30)(K)$. As $\ker \widehat{\phi_0} = \langle P \rangle$, there is an isomorphism $\theta : E/\langle P \rangle \to E_{60}$ over K with $\theta \circ \phi = \widehat{\phi_0}$, where $\phi : E \to E/\langle P \rangle$ is the quotient map, and then $\phi_0 = \widehat{\phi} \circ \theta^{-1}$. Hence

$$S_0 := \theta^{-1}(R) \in (E/\langle P \rangle)(K) \quad \text{satisfies} \quad 2S_0 = \phi(Q) \quad \text{and} \quad \widehat{\phi}(S_0) = Q. \tag{8.3}$$

By [Maz77], [Kam92, KM88] and [Naj26a, Theorem 1.1], the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 1, 2 or 5, so $\mathbb{Q}(x) = K$ and the trace divisor D of x on X is a closed point of degree 10. As α is a cyclic cover of degree 3, also $D_W := \alpha_* D$ is a closed point of degree 10, and by Lemma 8.25 a), b) and Lemma 8.26 it is linearly equivalent to one of the 256 divisors L.

In case a) of Lemma 8.26, $D_W \geq C > 0$, which is impossible as the support of D_W contains no cusp. In case b), $D_W = f^* B'$ with B' effective of degree 5, and as D_W is a closed point of degree 10, B' is a closed point of degree 5, with residue field $F \subseteq K$, $[K : F] = 2$. As $X_1(15)$ is a fine moduli space, there is an elliptic curve E'/F with a point R_{15} of order 15 such that $(E', R_{15}) \simeq (E, 2Q)$ over K. The full 2-torsion of E is defined over K, so the 2-division polynomial of E' splits over K, and as $[K : F] = 2$, it has a root in F. So E' has a point T of order 2 over F, and $T + R_{15}$ has order 30. By [Naj26a, Theorem 1.1], $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \not\subseteq E'(F)$, so $F(E'[2]) = K$. Now $E_{60} \simeq E/\langle P \rangle$ is 2-isogenous over K to $E'_K \simeq E$ and has the point R of order 60 over K, which contradicts Lemma 8.27.

In case c), let $\overline{D}$ be the reduction of D modulo 7. As $J_1(60)(\mathbb{Q})$ is finite [DEvH+21, Theorem 3.1(2)] and $\operatorname{gon}_{\mathbb{Q}} X_1(60) \geq \operatorname{gon}_{\mathbb{C}} X_1(60) \geq \frac{325}{2^{15}} \cdot 1152 > 11.4$ by Abramovich's bound, Proposition 2.5 a), applied to $X_1(60)$ with $p = 7$, shows that E_{60} has good reduction at some prime of K above 7, and so does the isogenous curve E. So $\overline{D}$ is not entirely cuspidal. It satisfies $\alpha_* \overline{D} = \overline{D_W} \sim \overline{L}$, and by Lemma 2.16, applied to $\pi_{i*} D$ as in (2.1), its non-cuspidal part D' satisfies $[\pi_{i*} D' - e\,\overline{y_0}] \in G + \mathcal{S}_{10-e}$ for $i = 1, 2, 3$. By Lemma 8.28, $D' = \overline{D}$ contains with multiplicity 1 a closed point $\overline{x}$ for which there is no point S as in Lemma 8.28 b). As $\overline{x}$ has multiplicity 1 in $\overline{D}$, it is the reduction of x modulo a prime $\mathfrak{p}$ of K above 7 which is unramified and whose residue field is the residue field κ of $\overline{x}$ (Section 2.2). The elliptic curve E has good reduction at $\mathfrak{p}$, and as X is a fine moduli space, the reduction of (E, P, Q) modulo $\mathfrak{p}$ is isomorphic over κ to the triple of $\overline{x}$. The reduction of S_0 of (8.3) modulo $\mathfrak{p}$ is then a point S as in Lemma 8.28 b), which is a contradiction. □

8.8. **The curve $X_1(66)$.** Over number fields of degree 7, 8 and 9 the group $\mathbb{Z}/66\mathbb{Z}$ is excluded in [Naj26d, Proposition 13.7], which determines all the points of these degrees on $X_1(33)$. In degree 10 the curve $X_1(33)$, which has gonality 10, has infinitely many points of degree 10, and the reduction of the trace divisor modulo 2 can lie in a pencil of degree 10. We use the isogenous curve given by the point of order 2, as in the proof of [Naj26d, Proposition 13.17], and the reduction modulo 5 of these pencils. As a field of degree 10 can have automorphisms of even order, we need the following lemma, which we also use for $\mathbb{Z}/74\mathbb{Z}$.

Lemma 8.30. *Let K be a number field, let $\mathfrak{p}$ be a prime of K above 2, let E/K be an elliptic curve with good reduction at $\mathfrak{p}$, and let $\phi : E \to E'$ be an isogeny of degree 2 defined over K.*

a) *If E has supersingular reduction at $\mathfrak{p}$, then $\mathfrak{p}$ is ramified over 2.*
b) *Suppose that E has ordinary reduction at $\mathfrak{p}$ and that $\operatorname{End}_{\overline{K}}(E) = \mathbb{Z}$, and let σ be an automorphism of K with $\sigma(\mathfrak{p}) = \mathfrak{p}$. Then E' is not isomorphic to E^σ over K.*

Proof. Let v be the valuation of K at $\mathfrak{p}$, and put $e = v(2)$. The curve E' also has good reduction at $\mathfrak{p}$. For an isogeny $\psi : E_1 \to E_2$ between elliptic curves over K with good reduction at $\mathfrak{p}$ and invariant differentials ω_1, ω_2 of their smooth models over the local ring at $\mathfrak{p}$, we have $\psi^*\omega_2 = u_\psi \omega_1$ with u_ψ integral at $\mathfrak{p}$, as ψ extends to the smooth models, and $v(u_\psi)$ does not depend on the choice of the ω_i. The reduction of u_ψ is the multiplier of the reduction $\widetilde{\psi}$, so $v(u_\psi) = 0$ if and only if $\widetilde{\psi}$ is separable [Sil09, Proposition II.4.2(c)]. As $\widehat{\phi} \circ \phi = [2]$, we have $v(u_\phi) + v(u_{\widehat{\phi}}) = v(2) = e$.

a) If $\widetilde{E}$ is supersingular, then $\widetilde{E}[2](\overline{\mathbb{F}}_2) = 0$, so $[2]$ is purely inseparable on $\widetilde{E}$, both $\widetilde{\phi}$ and $\widetilde{\widehat{\phi}}$ are inseparable, and $e = v(u_\phi) + v(u_{\widehat{\phi}}) \geq 2$.

b) If $\widetilde{E}$ is ordinary, then $\widetilde{E}[2](\overline{\mathbb{F}}_2)$ has order 2, so $[2]$ has inseparable degree 2 on $\widetilde{E}$. As inseparable degrees are multiplicative, exactly one of $\widetilde{\phi}$ and $\widetilde{\widehat{\phi}}$ is separable, so $v(u_\phi) \in \{0, e\}$. Suppose that $E' \simeq E^\sigma$ over K, and let $\psi : E \to E^\sigma$ be the composition of ϕ with such an isomorphism, so that $v(u_\psi) = v(u_\phi)$, as an isomorphism has a multiplier which is a unit at $\mathfrak{p}$. Let h be the order of σ. The composition

$$\psi^{\sigma^{h-1}} \circ \cdots \circ \psi^\sigma \circ \psi : E \to E^{\sigma^h} = E$$

is an endomorphism of E of degree 2^h, so it is multiplication by an integer m with $m^2 = 2^h$, and h is even and $m = \pm 2^{h/2}$. Choose an invariant differential ω of the smooth model of E over the local ring at $\mathfrak{p}$. As $\sigma(\mathfrak{p}) = \mathfrak{p}$, the differential $\sigma^i(\omega)$ is one for E^{σ^i}, and with these choices the multiplier of ψ^{σ^i} is $\sigma^i(u_\psi)$, whose valuation is $v(u_\psi)$. Hence the multiplier m of the composition has valuation $h\, v(u_\psi) \in \{0, he\}$, while $v(m) = he/2$, which is a contradiction as $he > 0$. □

Lemma 8.31. *Let $X = X_1(33)$, let c_0 be a rational cusp of X, and let $H \subseteq J_X(\mathbb{F}_2)$ be the reduction of $J_X(\mathbb{Q})$. Let $C_1, \ldots, C_{10}$ be the rational cuspidal divisors of degree 9 of the proof of* [Naj26d, Proposition 13.7]*, which are $\mathbb{Z}$-linear combinations of Galois orbits of cusps, not effective. We call the closed points of degree 7, 8 and 9 of X in the $\Delta(33)$-orbits of the points of level 33 of* [Naj26d, Propositions 13.2, 13.3 and 13.5] *the known points of degree 7, 8 and 9. There are 10, 5 and 10 of them, and the following hold.*

a) *We have $\operatorname{gon}_{\mathbb{Q}} X = 10$, the group $J_X(\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/42373650\mathbb{Z}$ is generated by the classes of rational cuspidal divisors, and $J_X(\mathbb{F}_2) \simeq \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/42373650\mathbb{Z}$, in which $H \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/42373650\mathbb{Z}$, so reduction modulo 2 is injective on $J_X(\mathbb{Q})$.*

b) *The Galois orbits of cusps over $\mathbb{Q}$ have degrees $1^{10}, 2^5, 10^2$, and the closed cusps of $X_{\mathbb{F}_2}$ have degrees $1^{10}, 2^5, 5^2, 10$. The non-cuspidal closed points of $X_{\mathbb{F}_2}$ of degrees $1, \ldots, 10$ number*

$$0,\ 0,\ 0,\ 0,\ 2,\ 20,\ 30,\ 25,\ 50,\ 123,$$

and the elliptic curves corresponding to the 2 points of degree 5 are supersingular.

c) *The effective divisors $\overline{B}$ of degree 10 on $X_{\mathbb{F}_2}$ with $[\overline{B} - 10\,\overline{c_0}] \in H$ whose support contains a non-cuspidal point are the following 3224 divisors, and each of them is the only effective divisor in its linear equivalence class.*

   i) *$\overline{S} + C'$, where S is a known point of degree 7, 8 or 9 and C' is an effective cuspidal divisor of degree 3, 2 or 1, respectively, which is the reduction of an effective rational cuspidal divisor (3100 divisors).*

   ii) *$P_i + \overline{c}$, where c is a rational cusp and $P_1, \ldots, P_{10}$ are closed points of degree 9 with $[P_i - 9\,\overline{c_0}] = [\overline{C_i} - 9\,\overline{c_0}]$ (100 divisors).*

iii) 21 *closed points of degree* 10.
iv) 3 *divisors which contain a non-cuspidal closed point of degree* 5 *with multiplicity* 1.

d) *Every effective cuspidal divisor* $\overline{B}$ *of degree* 10 *on* $X_{\mathbb{F}_2}$ *with* $[\overline{B} - 10\,\overline{c_0}] \in H$ *is the reduction of an effective rational cuspidal divisor, and it is the only effective divisor in its linear equivalence class, except for* 10 *classes, each of which contains exactly* 3 *effective divisors.*

Proof. For a) see [DvH14, Theorem 4 and Table 1], [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2] and the proof of [Naj26d, Proposition 13.7], where $J_X(\mathbb{F}_2)$ and H are computed. The Galois orbits of cusps and the closed cusps are as in the proof of [Naj26d, Proposition 13.7], and we compute the non-cuspidal closed points of degree at most 10. An elliptic curve over $\mathbb{F}_{32}$ with a point of order 33 has 33 points by the Hasse bound, so its trace of Frobenius is 0 and it is supersingular.

As every non-cuspidal closed point of $X_{\mathbb{F}_2}$ of degree at most 10 has degree at least 5, the non-cuspidal part of an effective divisor of degree 10 on $X_{\mathbb{F}_2}$ is 0, a single closed point of degree $5, \dots, 10$ (of degree 5 possibly with multiplicity 2), or a sum of two distinct points of degree 5. We run through all the effective divisors of degree 10 on $X_{\mathbb{F}_2}$, with all the cuspidal parts, and determine those with class in H. There are 321230 of them, in 321210 classes. As an effective divisor $\overline{B}$ with $\ell(\overline{B}) = r$ lies in a linear equivalence class with exactly $2^r - 1$ effective divisors over $\mathbb{F}_2$, this shows that $\ell(\overline{B}) = 1$ for all of them except for the 30 divisors in 10 classes with 3 effective divisors each, for which $\ell(\overline{B}) = 2$, and these 30 divisors are cuspidal. Among the 321230 divisors, 318006 are cuspidal, and they are exactly the reductions of the effective rational cuspidal divisors of degree 10 with class in H, which proves d).

The other 3224 divisors are 2700, 300, 200 and 21 divisors whose non-cuspidal part is a closed point of degree 7, 8, 9 and 10, respectively, and the 3 divisors of iv), namely 2 divisors consisting of a closed point of degree 5 and a closed cusp of degree 5, and the sum of the 2 non-cuspidal closed points of degree 5. The points of degree 7, 8 and 9 that occur are 10, 5 and 20 closed points, and every effective cuspidal divisor of degree 3, 2 and 1 occurs with them. By the proof of [Naj26d, Proposition 13.7], these points are the reductions of the known points, together with 10 closed points $P_1, \dots, P_{10}$ of degree 9 with $[P_i - 9\,\overline{c_0}] = [\overline{C_i} - 9\,\overline{c_0}]$. The effective cuspidal divisors of degree at most 3 on $X_{\mathbb{F}_2}$ are reductions of effective rational cuspidal divisors by b). This proves c). □

Lemma 8.32. *Let* $X = X_1(33)$*, and let* $C_1, \dots, C_{10}$ *be as in Lemma 8.31. For every* $i \in \{1, \dots, 10\}$ *and every rational cusp* c *of* X *we have* $\ell(\overline{C_i + c}) = 0$ *on* $X_{\mathbb{F}_5}$*. Hence no effective rational divisor on* X *is linearly equivalent to* $C_i + c$*.*

Proof. We compute the 100 Riemann-Roch spaces over $\mathbb{F}_5$. The last statement follows by semicontinuity [Har77, Theorem III.12.8]. □

For the 10 classes of Lemma 8.31 d) we use the reduction modulo 5 and the morphisms ρ_1 and ρ_2 of the following lemma.

Lemma 8.33. *Let* $X = X_1(33)$*, and let* c_0 *be as in Lemma 8.31. Let* $\rho_1, \rho_2 : X_1(66) \to X$ *be the morphisms*

$$\rho_1(E, R) = (E, 2R), \qquad \rho_2(E, R) = (E/\langle 33R \rangle,\ 2R \bmod \langle 33R \rangle),$$

which are defined over $\mathbb{Q}$, map cusps to cusps and non-cusps to non-cusps, and commute with the diamond operators. There are effective rational cuspidal divisors L_A and L_B of degree 10 on X with the following properties.

a) *The classes $[\langle a\rangle L_A - 10\,c_0]$ and $[\langle a\rangle L_B - 10\,c_0]$, for $a \in (\mathbb{Z}/33\mathbb{Z})^\times$, reduce to the 10 classes of Lemma 8.31 d), 5 of them for L_A and 5 for L_B.*
b) *On $X_{\mathbb{F}_5}$ we have $\ell(\overline{L_A}) = \ell(\overline{L_B}) = 2$, and there are functions $g_A \in L(\overline{L_A})$ and $g_B \in L(\overline{L_B})$ of degree 10.*
c) *The fibres of g_A above 0, 1, ∞ and of g_B above 0, 4, ∞ are entirely cuspidal, and the fibres of g_A above 2, 3, 4 and of g_B above 1, 2, 3 contain no cusp. The latter consist of closed points of degrees $4+6$, 10, 10 and $2+8$, $3+3+4$, $2+8$, respectively, each with multiplicity 1.*
d) *Let $g, g' \in \{g_A, g_B\}$, $a \in (\mathbb{Z}/33\mathbb{Z})^\times$ and $t, t' \in \mathbb{P}^1(\mathbb{F}_5)$, with $g^{-1}(t)$ not containing a cusp. Then there is no effective divisor Z of degree 10 on $X_1(66)_{\mathbb{F}_5}$ with $\rho_{1*}Z = g^{-1}(t)$ and $\rho_{2*}Z = (g' \circ \langle a\rangle)^{-1}(t')$.*

Proof. We take for L_A and L_B effective rational cuspidal divisors representing two of the 10 classes, found in `computations/d31b_C66_prepare_gonal_cusps.py`. We compute $L(\overline{L_A})$ and $L(\overline{L_B})$ on $X_{\mathbb{F}_5}$, the functions g_A and g_B, their diamond translates $g \circ \langle a\rangle$ and the fibres of g_A and g_B above $\mathbb{P}^1(\mathbb{F}_5)$, which proves b) and c), and we check that the polar divisors of the 20 functions $g \circ \langle a\rangle$ represent the 10 classes as stated in a).

For d), suppose that Z is such a divisor. As $\rho_{1*}Z = g^{-1}(t)$ and every point y of $g^{-1}(t)$ has multiplicity 1 by c), above every such y there is exactly one point z_y of Z, and it has multiplicity 1 and the same degree as y. As $\rho_{2*}Z = (g' \circ \langle a\rangle)^{-1}(t')$, every z_y satisfies $(g' \circ \langle a\rangle)(\rho_2(z_y)) = t'$. The closed points of $X_1(66)_{\mathbb{F}_5}$ above a non-cuspidal point y of $X_{\mathbb{F}_5}$ correspond to the irreducible factors of the 2-division polynomial of the elliptic curve of y, and above the 11 non-cuspidal points of the fibres of c) there are 23 of them. For each of these points z we compute $\rho_2(z)$, using the isogeny whose kernel is given by the corresponding factor, and the values at $\rho_2(z)$ of the 20 functions $g' \circ \langle a\rangle$. We find that for all g, t, g', a, t' as in d), the sum of the degrees of the points z above the points of $g^{-1}(t)$ with $(g' \circ \langle a\rangle)(\rho_2(z)) = t'$ is at most 4. But for Z as above this sum is at least $\sum_y \deg z_y = \deg Z = 10$, which is a contradiction. □

The following lemma describes all the effective rational divisors of degree 10 on $X_1(33)$ whose support contains no cusp, in terms of their reductions modulo 2.

Lemma 8.34. *Let $X = X_1(33)$, and let L_A and L_B be as in Lemma 8.33. Let D be an effective rational divisor of degree 10 on X whose support contains no cusp, and let $\overline{D}$ be its reduction modulo 2. Then one of the following holds.*

a) *$\overline{D}$ contains a non-cuspidal closed point of degree 5 with multiplicity 1.*
b) *D and $\overline{D}$ are closed points of degree 10, and $\ell(\overline{D}) = \ell(\langle 2\rangle \overline{D}) = 1$.*
c) *$\overline{D}$ is cuspidal, and $D \sim \langle a\rangle L$ for some $a \in (\mathbb{Z}/33\mathbb{Z})^\times$ and $L \in \{L_A, L_B\}$.*

Proof. Let c_0 and H be as in Lemma 8.31. By Lemma 2.16, $[\overline{D} - 10\,\overline{c_0}] \in H$, so $\overline{D}$ is one of the divisors of Lemma 8.31 c) or d). Recall that reduction modulo 2 is injective on $J_X(\mathbb{Q})$ by Lemma 8.31 a).

Suppose that $\overline{D} = \overline{S} + C'$ as in Lemma 8.31 c) i), and let C be an effective rational cuspidal divisor with $\overline{C} = C'$. Then $[D - S - C] \in J_X(\mathbb{Q})$ reduces to 0, so $D \sim S + C$. By semicontinuity $\ell(D) \le \ell(\overline{D}) = 1$, so $D = S + C$, which is impossible as $C \neq 0$ is cuspidal. If

$\overline{D} = P_i + \overline{c}$ as in c) ii), then in the same way $D \sim C_i + c$, which is impossible by Lemma 8.32. If $\overline{D}$ is one of the divisors of c) iv), then a) holds.

Suppose that $\overline{D}$ is a closed point of degree 10, as in c) iii). The reduction of a closed point of X of degree k is an effective divisor of degree k, and $\overline{D}$ is a single closed point with multiplicity 1, so D is a closed point of degree 10. We have $\ell(\overline{D}) = 1$ by Lemma 8.31 c). The divisor $\langle 2\rangle\overline{D}$ is also a non-cuspidal closed point of degree 10, and its class relative to $\overline{c_0}$ lies in H, as H is stable under the diamond operators and contains $[\langle 2\rangle\overline{c_0} - \overline{c_0}]$. So $\ell(\langle 2\rangle\overline{D}) = 1$ by Lemma 8.31 c), and b) holds.

Suppose finally that $\overline{D}$ is cuspidal, and let C be an effective rational cuspidal divisor with $\overline{C} = \overline{D}$ (Lemma 8.31 d)). Then $D \sim C$, and if $\overline{D}$ is the only effective divisor in its class, then $\ell(D) \leq 1$ and $D = C$, which is impossible. So the class of $\overline{D}$ is one of the 10 classes of Lemma 8.31 d), and by Lemma 8.33 a) and the injectivity of reduction, c) holds. □

Proposition 8.35. *The group $\mathbb{Z}/66\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let $X = X_1(33)$, and let ρ_1, ρ_2 be as in Lemma 8.33. Let E/K have a point R of order 66, where $[K : \mathbb{Q}] = 10$. Put $P = 2R$, of order 33, let $\phi : E \to E_\phi = E/\langle 33R\rangle$, which is defined over K, and $P_\phi = \phi(P)$, of order 33. Let D and D_ϕ be the trace divisors of (E, P) and (E_ϕ, P_ϕ) on X, and D_{66} that of (E, R) on $X_1(66)$, so that $\rho_{1*}D_{66} = D$ and $\rho_{2*}D_{66} = D_\phi$. As $E(K)$ has a point of order 66, Lemma 2.14 shows that $\mathrm{End}_{\overline{K}}(E) = \mathbb{Z}$. We denote reductions modulo 2 by a bar, and apply Lemma 8.34 to D.

Suppose that $\overline{D}$ contains a non-cuspidal closed point y of degree 5 with multiplicity 1. By Section 2.2, y is the reduction of (E, P) modulo a prime $\mathfrak{p}$ of K above 2 which is unramified, with residue field $\mathbb{F}_{32}$. The curve E has good reduction at $\mathfrak{p}$, and it is supersingular there by Lemma 8.31 b). This contradicts Lemma 8.30 a).

Suppose that D and $\overline{D}$ are closed points of degree 10. By Section 2.2, $\overline{D}$ is the reduction of (E, P) modulo a prime $\mathfrak{p}$ of K above 2 which is unramified with residue field $\mathbb{F}_{2^{10}}$, so $\mathfrak{p}$ is the only prime of K above 2, and E has good reduction at $\mathfrak{p}$. By Lemma 8.30 a) the reduction is ordinary. We now argue as in the proof of [Naj26d, Proposition 13.17]. The reduction of ϕ is an isogeny of degree 2 of an ordinary curve, so its kernel is either the connected subgroup of order 2, and it is the Frobenius isogeny, or the étale subgroup of order 2, and it is the Verschiebung up to isomorphism. Hence the reduction of (E_ϕ, P_ϕ) is the image of the reduction of (E, P) under the Frobenius, or under $\langle 2\rangle$ composed with the inverse of the Frobenius (see [Naj26d, Section 2.1]). As closed points are stable under the Frobenius, $\overline{D_\phi}$ is $\overline{D}$ or $\langle 2\rangle\overline{D}$. As $\ell(\overline{D}) = \ell(\langle 2\rangle\overline{D}) = 1$ by Lemma 8.34 b), the injectivity of reduction on $J_X(\mathbb{Q})$ (Lemma 8.31 a)) gives $D_\phi \sim D$, respectively $D_\phi \sim \langle 2\rangle D$, and semicontinuity gives $D_\phi = D$, respectively $D_\phi = \langle 2\rangle D$. Hence the K-points (E_ϕ, P_ϕ) and (E, P), respectively $(E, 2P)$, of X lie above the same closed point with residue field K, so they differ by an automorphism σ of K. As X is a fine moduli space, $E_\phi \simeq E^\sigma$ over K, and $\sigma(\mathfrak{p}) = \mathfrak{p}$ as $\mathfrak{p}$ is the only prime of K above 2. This contradicts Lemma 8.30 b).

Suppose finally that $\overline{D}$ is cuspidal, so that $D \sim \langle a\rangle L$ with a and L as in Lemma 8.34 c). The elliptic curve E has bad reduction at every prime of K above 2, which is multiplicative by Lemma 2.4, and so has the isogenous curve E_ϕ. So $\overline{D_\phi}$ is cuspidal too, and Lemma 8.34, applied to D_ϕ, gives $D_\phi \sim \langle a'\rangle L'$ for some $a' \in (\mathbb{Z}/33\mathbb{Z})^\times$ and $L' \in \{L_A, L_B\}$. Replacing R by bR, where b is coprime to 66 and $b \equiv a^{-1} \pmod{33}$, replaces D, D_ϕ and D_{66} by their diamond translates, so we may assume that $a = 1$.

Now we reduce modulo 5, and denote the reductions by $D^{(5)}$, $D_\phi^{(5)}$ and $D_{66}^{(5)}$. Let $g \in \{g_A, g_B\}$ be the function of Lemma 8.33 b) with $g \in L(\overline{L})$, so that $\overline{L}$ is the polar divisor of g. As $D \sim L$ and $\ell(\overline{L}) = 2$, the divisor $D^{(5)}$ is linearly equivalent to $\overline{L}$ on $X_{\mathbb{F}_5}$, so it equals $\overline{L} + \operatorname{div}(\lambda + \mu g)$ for some $(\lambda, \mu) \neq (0,0)$ in $\mathbb{F}_5^2$, that is, $D^{(5)} = g^{-1}(t)$ for some $t \in \mathbb{P}^1(\mathbb{F}_5)$. In the same way $D_\phi^{(5)} = (g' \circ \langle a' \rangle^{-1})^{-1}(t')$ for some $t' \in \mathbb{P}^1(\mathbb{F}_5)$, where g' is the function with polar divisor $\overline{L'}$. If $g^{-1}(t)$ is entirely cuspidal, then E has bad reduction at all the primes of K above 5, which contradicts Proposition 2.5 a) applied to $X_1(66)$ with $p = 5$, as $J_1(66)(\mathbb{Q})$ is finite [DEvH+21, Theorem 3.1(2)] and $\operatorname{gon}_{\mathbb{Q}} X_1(66) \geq \frac{325}{2^{15}} \cdot 1440 > 14.2$ by Abramovich's bound. Otherwise $g^{-1}(t)$ contains no cusp by Lemma 8.33 c), and $Z = D_{66}^{(5)}$ contradicts Lemma 8.33 d). □

8.9. **The curve $X_1(70)$.** For $X_1(70)$ we push the reduction of the trace divisor forward to $X_1(35)$ along two maps, and use the Hecke operator A_2 there. The prime $q = 2$ is not covered by Proposition 2.2, but the following lemma suffices.

Lemma 8.36. *The operator $A_2 = T_2 - 2\langle 2 \rangle - 1$ annihilates $J_1(35)(\mathbb{Q})$, and $A_2 C = 0$ as a divisor for every rational cuspidal divisor C on $X_1(35)$.*

Proof. By Lemma 2.3 with $q = 2$, we have $A_2 C = (\sigma_2 C - C) + 2\langle 2 \rangle (\sigma_2^{-1} C - C) = 0$ for every rational cuspidal divisor C. The group $J_1(35)(\mathbb{Q})$ is generated by the classes of rational cuspidal divisors of degree 0 [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], so A_2 annihilates it. □

Let $\pi_1, \pi_2 : X_1(70) \to X_1(35)$ be the morphisms

$$\pi_1(E, P) = (E, 2P), \qquad \pi_2(E, P) = (E/\langle 35P \rangle,\ 2P \bmod \langle 35P \rangle).$$

Note that $2P \bmod \langle 35P \rangle$ has order 35, as $\langle 35P \rangle$ has order 2. Both maps are defined over $\mathbb{Q}$, map cusps to cusps and non-cusps to non-cusps, and commute with the diamond operators.

Lemma 8.37. a) *The Galois orbits of cusps of $X_1(70)$ over $\mathbb{Q}$ and the closed cusps of $X_1(70)_{\mathbb{F}_3}$ both have degrees $1^{24}, 4^6, 6^4, 12^2$.*

b) *The non-cuspidal closed points of $X_1(70)_{\mathbb{F}_3}$ of degrees $1, \ldots, 10$ number*

$$0,\ 0,\ 0,\ 0,\ 0,\ 48,\ 408,\ 735,\ 2144,\ 5880,$$

and those of degrees $6, \ldots, 10$ form 4, 34, 65, 180 and 490 orbits under $\Delta(70)$.

c) *For every non-cuspidal closed point P of $X_1(70)_{\mathbb{F}_3}$ of degree between 6 and 10, one of the divisors $A_2(\pi_{1*}P)$ and $A_2(\pi_{2*}P)$ on $X_1(35)_{\mathbb{F}_3}$ is not principal.*

Proof. Part a) is a direct computation with the description of the cusps of $X_1(70)$ in [DN25, Section 2]: the Galois orbits over $\mathbb{Q}$ are the orbits of $\operatorname{Gal}(\mathbb{Q}(\zeta_{70})/\mathbb{Q})$ on the geometric cusps, and the closed cusps of $X_1(70)_{\mathbb{F}_3}$ are the orbits of σ_3. We compute b). As A_2 and the π_i commute with the diamond operators, it suffices to prove c) for one point in each of the 773 orbits. For each of them we compute the divisor $A_2(\pi_{1*}P)$ of degree 0 directly from the moduli interpretation of T_2, using the three subgroups of order 2 of the elliptic curve, and find that $\ell(A_2(\pi_{1*}P)) = 0$ in 770 cases. In the remaining 3 cases, all of degree 8, we find that $\ell(A_2(\pi_{2*}P)) = 0$. □

Proposition 8.38. *The group $\mathbb{Z}/70\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let D be the trace divisor of a point of $Y_1(70)$ over a number field of degree 10. We have $\operatorname{rk} J_1(70)(\mathbb{Q}) = 0$ [DEvH+21, Theorem 3.1(2)], and Abramovich's bound gives $\operatorname{gon}_{\mathbb{Q}} X_1(70) \geq \frac{325}{2^{15}} \cdot 1728 > 17.1$, so by Proposition 2.5 a) with $p = 3$ the reduction of D modulo 3 is $D' + C'$ with $D' \neq 0$ non-cuspidal. By Lemma 8.37 b), D' is a single closed point of degree $6, \ldots, 10$ with multiplicity 1, and C' has degree at most 4. By Lemma 8.37 a), C' is the reduction of a rational cuspidal divisor C.

Let $i \in \{1, 2\}$. The class $[\pi_{i*}D - 10\,c_0]$, for a rational cusp c_0 of $X_1(35)$, lies in $J_1(35)(\mathbb{Q})$, so by Lemma 8.36 the divisor $A_2(\pi_{i*}D)$ is principal, as $A_2 c_0 = 0$. Its reduction modulo 3 is $A_2(\pi_{i*}D') + A_2(\pi_{i*}C')$, and $A_2(\pi_{i*}C')$ is the reduction of $A_2(\pi_{i*}C) = 0$, as $\pi_{i*}C$ is a rational cuspidal divisor. So $A_2(\pi_{i*}D')$ is principal for $i = 1, 2$, which contradicts Lemma 8.37 c). □

8.10. **The curve $X_1(74)$.** The Jacobian $J_1(37)$ has positive rank, so we work with the operator $\gamma := \langle 2 \rangle - 1$ on $J_1(37)$, which has finite image on $J_1(37)(\mathbb{Q})$, and with a formal immersion argument at 2 for the map $B \mapsto \gamma[B - 10\,c_0]$. The cases that it does not cover are treated with the Hecke sieve at 2, with Lemma 2.10, and with the isogenous curve given by the point of order 2, as for $\mathbb{Z}/66\mathbb{Z}$. Some of the computations on $X_1(37)_{\mathbb{F}_2}$ that we use do not depend on the degree, and were carried out together with computations for nonic fields.

Lemma 8.39. *Let $X = X_1(37)$, $J = J_1(37)$, let c_0 be a rational cusp of X, and put $\gamma = \langle 2 \rangle - 1$.*

a) *We have $\operatorname{gon}_{\mathbb{Q}} X = 18$, and $(\langle a \rangle - 1)J(\mathbb{Q})$ is finite for every $a \in (\mathbb{Z}/37\mathbb{Z})^\times$.*
b) *We have $J(\mathbb{Q})[2] = 0$, and reduction modulo 2 is injective on $J(\mathbb{Q})_{\mathrm{tors}}$.*
c) *The Galois orbits of cusps over $\mathbb{Q}$ and the closed cusps of $X_{\mathbb{F}_2}$ both have degrees $1^{18}, 18$. The non-cuspidal closed points of $X_{\mathbb{F}_2}$ of degrees $1, \ldots, 10$ number*

$$0,\ 0,\ 0,\ 0,\ 0,\ 21,\ 18,\ 0,\ 39,\ 99.$$

Under $\Delta(37)$ those of degree 6 form 2 orbits, of lengths 18 and 3, those of degree 7 form 1 orbit, of length 18, and those of degree 9 form 4 orbits, of lengths 18, 18, 2 and 1.
d) *For the representatives P of the orbits of length 18 of the points of degrees 6, 7 and 9, the divisor $\gamma A_3 P$ on $X_{\mathbb{F}_2}$ is not principal.*
e) *The diamond operator $\langle 10 \rangle$ has order 3 in $\Delta(37)$, and it fixes every point in the orbits of lengths 3, 2 and 1 of c).*

Proof. The gonality is [DvH14, Theorem 1]. By [DS25, Proposition 5.2 and Table 2] the prime 37 is not strange, that is, every newform of weight 2 and level 37 with non-trivial character has non-vanishing L-value at 1. By Kato's theorem the factors of J on which the diamond operators act non-trivially have finite Mordell-Weil groups over $\mathbb{Q}$, so $(\langle a \rangle - 1)J(\mathbb{Q})$ is finite. This proves a).

For b), A_3 and A_5 annihilate $J(\mathbb{Q})_{\mathrm{tors}}$ by Proposition 2.2 b), and we compute, using the action of the Hecke algebra on $H_1(J(\mathbb{C}), \mathbb{Z})/2H_1(J(\mathbb{C}), \mathbb{Z}) \simeq J[2]$, that the kernels of A_3 and A_5 on $J[2]$ intersect trivially (see `continuation_20261031b/C74/inputs/work/degree9/prime_orders/continued_20261026/P37/rational_two_delta4.log`). So $J(\mathbb{Q})[2] = 0$, and as the kernel of reduction modulo 2 on $J(\mathbb{Q})_{\mathrm{tors}}$ has exponent dividing 2 by Parent's result, it is trivial.

In c), the statement on the cusps holds as 2 has order 36 modulo 37. An elliptic curve over $\mathbb{F}_{2^k}$ with a point of order 37 does not exist for $k \leq 5$ and for $k = 8$, by the Hasse bound and as the possible even traces of Frobenius over $\mathbb{F}_{2^k}$ are 0 and $\pm 2^{(k+1)/2}$ for odd k and 0,

$\pm 2^{k/2}$ and $\pm 2^{k/2+1}$ for even k [Wat69, Theorem 4.1]. We compute the points of degrees 6, 7 and 9 and their orbits, the lengths of these orbits (see `additions/C74/stab37.log`), and the points of degree 10.

For d) we compute A_3P directly from the moduli interpretation of T_3, and the Riemann-Roch spaces of $\gamma A_3 P$. The representatives are numbered in the same way in the log of this computation and in `additions/C74/stab37.log`.

For e), as $10^3 = 1000 \equiv 1 \pmod{37}$ and $10 \not\equiv \pm 1 \pmod{37}$, the operator $\langle 10\rangle$ has order 3 in $\Delta(37) \simeq (\mathbb{Z}/37\mathbb{Z})^\times/\{\pm 1\}$, which is cyclic of order 18. The stabilizer of a point in an orbit of length 3, 2 or 1 is the subgroup of $\Delta(37)$ of order 6, 9 or 18, which contains the unique subgroup of order 3, generated by $\langle 10\rangle$. □

The image U of $\langle 2\rangle^* - 1$ on $H^0(X_1(37)_{\mathbb{F}_2}, \Omega^1)$, where $\langle 2\rangle^*$ is the pull-back of differentials by the diamond automorphism $\langle 2\rangle$, is the image of the action of γ on the cotangent space at 0 of the special fibre of the Néron model of $J_1(37)$ over $\mathbb{Z}_2$, identified with $H^0(X_1(37)_{\mathbb{F}_2}, \Omega^1)$, and it is stable under the diamond operators. The following is the formal immersion criterion of [Naj26d, Proposition 7.3], in the simpler situation in which reduction is injective on the torsion.

Lemma 8.40. *Let $X = X_1(37)$, $J = J_1(37)$, c_0 and $\gamma = \langle 2\rangle - 1$ be as in Lemma 8.39, and let $U \subseteq H^0(X_{\mathbb{F}_2}, \Omega^1)$ be the image of $\langle 2\rangle^* - 1$. Let $\overline{B}$ be an effective divisor of degree 10 on $X_{\mathbb{F}_2}$ such that the restriction map $U \to H^0(\overline{B}, \Omega^1|_{\overline{B}})$ is surjective. Let D_1 and D_2 be effective rational divisors of degree 10 on X which both reduce to $\overline{B}$ modulo 2, and such that $\gamma[D_1 - D_2]$ is torsion. Then $D_1 = D_2$.*

Proof. The class $\gamma[D_1 - D_2] \in J(\mathbb{Q})_{\mathrm{tors}}$ reduces to $\gamma[\overline{B} - \overline{B}] = 0$, so it is 0 by Lemma 8.39 b). Consider the morphism $h : X^{(10)} \to J$ over $\mathbb{Z}_{(2)}$ given by $h(B) = \gamma[B - 10\,c_0]$, where X and J denote the smooth models. Then $h(D_1) = h(D_2)$, and D_1 and D_2 have the same reduction $\overline{B}$. The cotangent map of $B \mapsto [B - 10\,c_0]$ at $\overline{B}$ is the restriction map $H^0(X_{\mathbb{F}_2}, \Omega^1) \to H^0(\overline{B}, \Omega^1|_{\overline{B}})$, so the image of the cotangent map of h at $\overline{B}$ is the restriction of U to $\overline{B}$. By assumption it is surjective, so h is a formal immersion at $\overline{B}$, and by [DKSS23, Lemma 4.2] (which is due to Parent [Par99, Lemme 4.13]) h is injective on the residue class of $\overline{B}$. Hence $D_1 = D_2$. □

Lemma 8.41. *Let $X = X_1(37)$, and let $U \subseteq H^0(X_{\mathbb{F}_2}, \Omega^1)$ be the image of $\langle 2\rangle^* - 1$. Then $\dim U = 38$, and the restriction map $U \to H^0(\overline{B}, \Omega^1|_{\overline{B}})$ is surjective for the following effective divisors $\overline{B}$ of degree 10 on $X_{\mathbb{F}_2}$:*

a) *every divisor supported on the 18 cusps of degree 1,*
b) *every non-cuspidal closed point of degree 10.*

Proof. We compute a basis of $H^0(X_{\mathbb{F}_2}, \Omega^1)$, which has dimension 40, the matrix of $\langle 2\rangle^*$ on it, of order 18, and its image U, of dimension 38. As U is stable under the diamond operators, which act transitively on the cusps of degree 1, it suffices to compute the expansions at one cusp of degree 1, and to transport them with the diamond operators. We compute the expansions of a basis of U at a cusp of degree 1 up to order 10, and at each of the 99 points of degree 10, and we check that the restriction maps have rank 10 for all the $\binom{27}{10} = 8436285$ divisors of a) (with the program `computations/d31b_C74_prefix_ranks.cpp`), and for all the 99 divisors of b). □

Proposition 8.42. *The group $\mathbb{Z}/74\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let $X = X_1(37)$, $J = J_1(37)$, c_0 and γ be as in Lemma 8.39. Let E/K have a point R of order 74, where $[K : \mathbb{Q}] = 10$. Put $P = 2R$, of order 37, let $\phi : E \to E_\phi = E/\langle 37R\rangle$, which is defined over K, and $P_\phi = \phi(P)$. Let D and D_ϕ be the trace divisors of (E, P) and (E_ϕ, P_ϕ) on X. By Remark 4.2, D is a closed point of degree 10. As $E(K)$ has a point of order 74, Lemma 2.14 shows that E has no complex multiplication. Note that for every effective rational divisor B of degree 10 on X the class $\gamma[D - B]$ lies in $\gamma J(\mathbb{Q})$, which is finite by Lemma 8.39 a). We consider the reduction $\overline{D}$ of D modulo 2.

Suppose first that $\overline{D}$ is cuspidal. Then it is supported on the cusps of degree 1, so it is the reduction of a rational cuspidal divisor C, and Lemma 8.40 and Lemma 8.41 a) give $D = C$, which is impossible. So $\overline{D} = D' + C'$ with $D' \neq 0$, and by Lemma 8.39 c), D' is a single closed point of degree 6, 7, 9 or 10 with multiplicity 1, and C' is supported on the cusps of degree 1. Let C be the rational cuspidal divisor with $\overline{C} = C'$.

The class $\gamma[D - 10\,c_0]$ is torsion, so $A_3\gamma[D - 10\,c_0] = 0$ by Proposition 2.2 b). As γc_0 and γC are rational cuspidal divisors, $A_3\gamma c_0 = A_3\gamma C = 0$ as divisors by Proposition 2.2 c), so $\gamma A_3(D - C)$ is principal, and so is its reduction $\gamma A_3 D'$. As γA_3 commutes with the diamond operators, Lemma 8.39 d) shows that D' lies in one of the orbits of lengths 3, 2 and 1 of Lemma 8.39 c), of degree 6, 9 and 9, or has degree 10.

If $\deg D' \in \{6, 9\}$, then C has degree $10 - \deg D' \leq 4$, and $g = \langle 10\rangle$ fixes the reduction D' of $D - C$ by Lemma 8.39 e). The automorphism g has odd order 3, it acts trivially on $J(\mathbb{Q})[2] = 0$, $(g - 1)J(\mathbb{Q})$ is finite, and $\operatorname{gon}_{\mathbb{Q}} X = 18 > 10 + \deg C$. So Lemma 2.10 d) gives $gD = D$. As E has no complex multiplication, Lemma 2.9 shows that 3 divides $\deg D = 10$, which is a contradiction.

Finally, suppose that $D' = \overline{D}$ is a closed point of degree 10. By Section 2.2, $\overline{D}$ is the reduction of (E, P) modulo a prime $\mathfrak{p}$ of K above 2 which is unramified with residue field $\mathbb{F}_{2^{10}}$, so $\mathfrak{p}$ is the only prime of K above 2, and E has good reduction at $\mathfrak{p}$. By Lemma 8.30 a) the reduction is ordinary. As in the proof of Proposition 8.35, the reduction of D_ϕ is $\overline{D}$ or $\langle 2\rangle\overline{D}$, and both are closed points of degree 10. Applying Lemma 8.40 and Lemma 8.41 b) to D_ϕ and D, respectively $\langle 2\rangle D$, we get $D_\phi = D$, respectively $D_\phi = \langle 2\rangle D$. As in the proof of Proposition 8.35, it follows that $E_\phi \simeq E^\sigma$ over K for an automorphism σ of K with $\sigma(\mathfrak{p}) = \mathfrak{p}$, which contradicts Lemma 8.30 b). □

9. Formal immersion at the prime 2

In this section we show that the groups $\mathbb{Z}/n\mathbb{Z}$ for $n \in \{49, 51, 55, 75, 77, 85, 91, 93\}$ are not subgroups of the torsion of an elliptic curve over a number field of degree 10. These levels were treated in degrees at most 9 in [Naj26d, Sections 7 and 8], and we follow the arguments given there. We reduce the trace divisor D modulo 2 and write its reduction as $D' + C'$ (Section 2.5). The reductions with $D' \neq 0$ are excluded with the Hecke sieve, and for $n \in \{77, 85, 91, 93\}$, where $J_1(n)$ has positive rank, with a variant of it which uses elements of the Hecke algebra with finite image on the Mordell-Weil group. Except for $n \in \{91, 93\}$ there are non-cuspidal closed points of degree 10 on $X_1(n)_{\mathbb{F}_2}$, which play no role in degree 9. The entirely cuspidal reductions are excluded with the formal immersion criterion of Proposition 2.18, except for $n = 49$ and $n = 75$, where Proposition 2.5 b) applies, and $n = 55$, where reduction modulo 2 is injective on $J_1(55)(\mathbb{Q})$. For $n = 91$ and $n = 93$ the argument of [Naj26d, Proposition 8.5], which uses Lemma 2.10 c), would need $\operatorname{gon}_{\mathbb{C}} X_1(n) > 2(10+10) = 40$, which we do not know. For $n = 91$ we replace it by a relative version of Proposition 2.18 (Lemma 9.19), and for $n = 93$ we combine it with a descent to $X_1(31)$ and with Proposition 2.18.

9.1. **The curve $X_1(49)$.**

Lemma 9.1. *The non-cuspidal closed points of $X_1(49)_{\mathbb{F}_2}$ of degree at most 10 are 42 points of degree 9, which form 2 diamond orbits, and 126 points of degree 10, which form 6 diamond orbits. For each of these points P the divisor A_3P is not principal.*

Proof. No elliptic curve over $\mathbb{F}_{2^e}$ with $e \leq 8$ has a point of order 49 (see the proof of [Naj26d, Proposition 7.7]). We compute the non-cuspidal closed points of degree 9 and 10 and their diamond orbits, and that A_3P is not principal for a representative P of each of the 8 orbits. As A_3 commutes with the diamond operators, this proves the lemma. □

Proposition 9.2. *The group $\mathbb{Z}/49\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let $X = X_1(49)$, let D be the trace divisor of a point of order 49 over a number field of degree 10, and let $D' + C'$ be its reduction modulo 2. The group $J_1(49)(\mathbb{Q})$ is finite [DEvH+21, Theorem 3.1(2)], and $\operatorname{gon}_{\mathbb{Q}} X = 21 > 20$ [Var26, Theorem D], so $D' \neq 0$ by Proposition 2.5 b) with $p = 2$. By Lemma 9.1, either D' is a closed point of degree 10 and $C' = 0$, or D' is a closed point of degree 9 and C' is a cusp of degree 1. The cusps of degree 1 of $X_{\mathbb{F}_2}$ are the reductions of the 21 rational cusps of X (see the proof of [Naj26d, Proposition 7.7]), so 3 is admissible for C', and the Hecke sieve (Section 2.5) gives $[A_3D'] = 0$, which contradicts Lemma 9.1. □

9.2. **The curve $X_1(51)$.**

Lemma 9.3. *The non-cuspidal closed points of $X_1(51)_{\mathbb{F}_2}$ of degree at most 10 are 80 points of degree 9, which form 5 diamond orbits, and 64 points of degree 10, which form 4 diamond orbits. For each of these points P the divisor A_5P is not principal.*

Proof. No elliptic curve over $\mathbb{F}_{2^e}$ with $e \leq 8$ has a point of order 51 (see the proof of [Naj26d, Proposition 7.9]). We compute the non-cuspidal closed points of degree 9 and 10 and their diamond orbits, and that A_5P is not principal for a representative P of each of the 9 orbits. □

Lemma 9.4. *Let $X = X_1(51)$ and $U = (\mathcal{C} - 1)H^0(X_{\mathbb{F}_2}, \Omega^1)$. The closed cusps of $X_{\mathbb{F}_2}$ have degrees $1^{16}, 2^8, 8^4$ [Naj26d, Proposition 7.9], and the restriction map $U \to H^0(\overline{C}, \Omega^1|_{\overline{C}})$ is surjective for each of the*

$$[t^{10}](1-t)^{-16}(1-t^2)^{-8}(1-t^8)^{-4} = 9656144$$

effective cuspidal divisors $\overline{C}$ of degree 10 on $X_{\mathbb{F}_2}$.

Proof. The curve X has genus 65, and U has dimension 62. In the proof of [Naj26d, Proposition 7.9] we computed the subspaces $\Omega(m\overline{c})$ for the closed cusps $\overline{c}$ with $m \deg \overline{c} \leq 8$. From them we check that the restriction of U is surjective at each of the 9655880 divisors $\sum_{\overline{c}} m_{\overline{c}}\overline{c}$ of degree 10 with $m_{\overline{c}} \deg \overline{c} \leq 8$ for every $\overline{c}$. The remaining 264 divisors are $10\overline{c}$ and $9\overline{c} + \overline{c}'$ with distinct cusps $\overline{c}, \overline{c}'$ of degree 1, and $5\overline{r}$ with $\overline{r}$ of degree 2. The diamond operator $\langle 5 \rangle$ generates $\Delta(51)$, it acts transitively on the 16 cusps of degree 1 and on the 8 cusps of degree 2, and U is stable under it. So it suffices to consider $10\overline{c_0}$, the 15 divisors $9\overline{c_0} + \overline{c}'$ and $5\overline{r_0}$, where $\overline{c_0}$ is the reduction of the standard cusp c_0 and $\overline{r_0}$ is a fixed cusp of degree 2. We compute the subspaces $\Omega(10\overline{c_0})$ and $\Omega(5\overline{r_0})$, in a common basis of $H^0(X_{\mathbb{F}_2}, \Omega^1)$ with the subspaces above, and that the restriction of U is surjective at these 17 divisors. □

Proposition 9.5. *The group $\mathbb{Z}/51\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree* 10.

Proof. Let $X = X_1(51)$, let D be the trace divisor of a point of order 51 over a number field of degree 10, and let $D' + C'$ be its reduction modulo 2. The group $J_1(51)(\mathbb{Q})$ is finite [DEvH+21, Theorem 3.1(2)].

Suppose first that $D' \neq 0$. By Lemma 9.3, either D' is a closed point of degree 10 and $C' = 0$, or D' is a closed point of degree 9 and C' is a cusp of degree 1, which is the reduction of one of the 16 rational cusps of X. So 5 is admissible for C', and the Hecke sieve gives $[A_5 D'] = 0$, which contradicts Lemma 9.3. So $D' = 0$, and Proposition 2.18 with $H = \{1\}$, $r = 1$ and $\psi_1 = 1$, together with Lemma 9.4, gives a contradiction. □

9.3. **The curve $X_1(55)$.** In degree 10 the formal immersion criterion is not needed for $X_1(55)$, as the gonality is large enough once we know that reduction modulo 2 is injective on the rational torsion of the Jacobian. We use the quotient $Y = X_1(55)/\langle 16 \rangle$ of [Naj26d, Lemma 7.10], which has genus 17 and good reduction at 2.

Lemma 9.6. *Reduction modulo* 2 *is injective on $J_1(55)(\mathbb{Q})$.*

Proof. The group $J_1(55)(\mathbb{Q})$ is finite [DEvH+21, Theorem 3.1(2)], and every torsion point in the kernel of reduction modulo 2 has order a power of 2, so it suffices to consider $J_1(55)(\mathbb{Q})[2^\infty]$, which is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$ [DEvH+21, Theorem 4.13 and Table 2]. Let $\pi : X_1(55) \to Y$ be the quotient map. In the proof of [Naj26d, Proposition 7.11] we computed that $J_Y(\mathbb{F}_2) \simeq (\mathbb{Z}/5\mathbb{Z})^2 \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/1200\mathbb{Z}$ and that the reductions of the rational cuspidal divisors generate a subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/1200\mathbb{Z}$, whose 2-primary part has order 32. The group $J_Y(\mathbb{Q})$ is finite, as J_Y is a quotient of $J_1(55)$, and it contains the classes of the rational cuspidal divisors, so the image of $J_Y(\mathbb{Q})[2^\infty]$ under reduction has order at least 32. As $\pi_*\pi^* = 5$, the map π^* is injective on $J_Y(\mathbb{Q})[2^\infty]$, so this group has order at most 32. Hence $J_Y(\mathbb{Q})[2^\infty]$ has order 32, reduction modulo 2 is injective on it, and π^* maps it isomorphically onto $J_1(55)(\mathbb{Q})[2^\infty]$. If $z = \pi^* y \in J_1(55)(\mathbb{Q})[2^\infty]$ reduces to 0, then so does $\pi_* z = 5y$. So $5y = 0$, and as y has order a power of 2, we get $y = 0$ and $z = 0$. □

Lemma 9.7. *The non-cuspidal closed points of $X_1(55)_{\mathbb{F}_2}$ of degree at most* 10 *are* 20 *points of degree* 7*, which form a single diamond orbit,* 40 *points of degree* 9*, which form* 2 *diamond orbits, and* 100 *points of degree* 10*, which form* 5 *diamond orbits. For each of these points P the divisor $A_3 P$ is not principal.*

Proof. For the points of degree at most 9 this is shown in the proof of [Naj26d, Proposition 7.11]. We compute that exactly 50 elliptic curves over $\mathbb{F}_{2^{10}}$ have a point of order 55, that their j-invariants form 5 Frobenius orbits of length 10, and that their subgroup of order 55 is cyclic. This gives 100 closed points of degree 10, and the 20 generators of the subgroup of order 55 up to sign are permuted transitively by the diamond operators, so they form 5 diamond orbits. For a representative P of each of them we compute $T_3 P$ from the 4 isogenies of degree 3 of an elliptic curve representing P. It consists of a closed point of degree 10 and one of degree 30, or, for one orbit, of 4 closed points of degree 10, each with multiplicity 1, and we compute that $\ell(A_3 P) = 0$ (for the orbits 1, 2, 3, 4 and 5). □

Proposition 9.8. *The group $\mathbb{Z}/55\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree* 10.

Proof. Let $X = X_1(55)$, let D be the trace divisor of a point of order 55 over a number field of degree 10, and let $D' + C'$ be its reduction modulo 2. The group $J_1(55)(\mathbb{Q})$ is finite [DEvH+21, Theorem 3.1(2)]. The Galois orbits of cusps of X and the closed cusps of $X_{\mathbb{F}_2}$ both have degrees $1^{20}, 4^5, 10^2, 20$, and we check that every closed cusp of $X_{\mathbb{F}_2}$ is the reduction of a Galois orbit of cusps of the same degree.

Suppose first that $D' \neq 0$. By Lemma 9.7, D' is a closed point of degree 7, 9 or 10, and C' is a cuspidal divisor of degree 3, 1 or 0, so it is supported on the cusps of degree 1, which are the reductions of the 20 rational cusps. So 3 is admissible for C', and the Hecke sieve gives $[A_3 D'] = 0$, which contradicts Lemma 9.7.

So $D' = 0$, and C' is the reduction of an effective rational cuspidal divisor C of degree 10. The class $[D - C] \in J_1(55)(\mathbb{Q})$ reduces to 0, so $D \sim C$ by Lemma 9.6. As Abramovich's bound gives $\operatorname{gon}_{\mathbb{Q}} X \geq \operatorname{gon}_{\mathbb{C}} X > 14.28 > 10$, Lemma 2.8 gives $D = C$, which is a contradiction. □

9.4. **The curve $X_1(75)$.** We use the quotient $Y = X_1(75)/\langle 26 \rangle$ of [Naj26d, Section 7.6], which has genus 73 and good reduction at 2, and parametrizes elliptic curves with a point of order 25 and a cyclic subgroup of order 3. Its model over $\mathbb{F}_2$ is obtained by adjoining to the function field of $X_1(25)_{\mathbb{F}_2}$ the common x-coordinate x_3 of the non-zero points of a subgroup of order 3 of the universal ordinary elliptic curve $y^2 + xy = x^3 + a_2 x^2 + 1/j$, which satisfies $x_3^4 + x_3^3 + 1/j = 0$. We write $\pi : X_1(75) \to Y$ for the quotient map, and $A_7 = T_7 - 1 - 7\langle 7 \rangle$ also for the operator on Y.

Lemma 9.9. *The non-cuspidal closed points of $X_1(75)_{\mathbb{F}_2}$ of degree at most 10 are 20 points of degree 7, which form a single diamond orbit, and 120 points of degree 10, which form 6 diamond orbits. For each of these points P the image $\pi(P)$ is a closed point of $Y_{\mathbb{F}_2}$ of the same degree as P, and the divisor $A_7\pi(P)$ on $Y_{\mathbb{F}_2}$ is not principal.*

Proof. For the points of degree at most 9 this is shown in the proof of [Naj26d, Proposition 7.13]. We compute that among the 2053 elliptic curves over $\mathbb{F}_{2^{10}}$ up to isomorphism exactly 60 have a point of order 75, that their j-invariants form 6 Frobenius orbits of length 10, and that each of them has $E(\mathbb{F}_{2^{10}}) \simeq \mathbb{Z}/1050\mathbb{Z}$. So each of them has a unique subgroup of order 75, whose 20 generators up to sign are permuted transitively by the diamond operators, which gives 120 closed points of degree 10 in 6 diamond orbits. The degree of $\pi(P)$ divides that of P. For P of degree 10 the j-invariant of P generates $\mathbb{F}_{2^{10}}$, and for P of degree 7 the point $\pi(P)$ is not defined over $\mathbb{F}_2$, as no elliptic curve over $\mathbb{F}_2$ has a point of order 25. So in both cases $\pi(P)$ has the same degree as P. For a representative P of each orbit of points of degree 10 we compute $T_7\pi(P)$ from the 8 isogenies of degree 7 of an elliptic curve representing P, carrying along the point of order 25 and the subgroup of order 3. It consists of 2 closed points of degree 10 and 2 of degree 30, each with multiplicity 1, and we compute that $\ell(A_7\pi(P)) = 0$ (for the orbits 1 and 2, 3 and 4, and 5 and 6). As A_7 commutes with the diamond operators, this proves the lemma. □

Proposition 9.10. *The group $\mathbb{Z}/75\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let D be the trace divisor of a point of order 75 over a number field of degree 10, and let $D' + C'$ be its reduction modulo 2. We have $\operatorname{rk} J_1(75)(\mathbb{Q}) = 0$ [DEvH+21, Theorem 3.1(2)], and Abramovich's bound gives $\operatorname{gon}_{\mathbb{Q}} X_1(75) > 23.80 > 20$. So by Proposition 2.5 b) the reduction of D is not entirely cuspidal, i.e. $D' \neq 0$.

By Lemma 9.9, D' is a closed point P of degree 7 and C' has degree 3, or P has degree 10 and $C' = 0$. The closed cusps of $X_1(75)_{\mathbb{F}_2}$ of degree at most 3 have degrees $1^{20}, 2^{10}$, and we check that they are the reductions of Galois orbits of cusps of $X_1(75)$ of the same degree. So C' is the reduction of an effective rational cuspidal divisor C. The group $J_Y(\mathbb{Q})$ is finite, as J_Y is a quotient of $J_1(75)$, so A_7 annihilates it by Proposition 2.2 b), and $A_7(\pi_* C) = A_7 c_0 = 0$ by Proposition 2.2 c). Hence $[A_7(\pi_* D - 10c_0)] = 0$, and its reduction gives $[A_7 \pi_* P] = 0$. As $\pi_* P = \pi(P)$ by Lemma 9.9, this contradicts Lemma 9.9. □

9.5. **The curve $X_1(77)$.**

Lemma 9.11. *Let $H \subseteq \Delta(77)$ be the subgroup of order 5 generated by $\langle 36 \rangle$, let $Y = X_1(77)/H$, let $\pi : X_1(77) \to Y$ be the quotient map, and let δ be the automorphism of Y induced by $\langle 2 \rangle$.*

a) *The curve Y has genus 37 and good reduction at 2, and $Y \to X_0(77)$ is an unramified cyclic cover of degree 6, also over $\mathbb{F}_2$, whose group of automorphisms is generated by δ. The automorphism of Y induced by $\langle 3 \rangle$ is δ^{-1}.*
b) *The group $T_2 J_Y(\mathbb{Q})$ is finite.*
c) *The closed cusps of $X_1(77)_{\mathbb{F}_2}$ have degrees $1^{30}, 3^{10}, 10^3, 30$. Those of degree 1, 3 and 10 map to the 6 rational cusps of $Y_{\mathbb{F}_2}$ above the cusp of width 77 of $X_0(77)$, to the 2 closed cusps of degree 3 above the cusp of width 11, and to the 3 closed cusps of degree 2 above the cusp of width 7, respectively. In particular the push-forward to $Y_{\mathbb{F}_2}$ of a closed cusp of degree 10 is $5\overline{r}$ for a closed cusp $\overline{r}$ of degree 2.*

Proof. The first two assertions of a) are [Naj26d, Lemma 7.15]. The group $\Delta(77)/H$ has order 6, and as $2^6 \equiv 36^2$ and no smaller positive power of 2 is congruent to $\pm 36^i$ modulo 77, it is generated by $\langle 2 \rangle$. As $36^3 \equiv -6 \pmod{77}$, we have $\langle 2 \rangle \langle 3 \rangle = \langle 6 \rangle \in H$, which proves a). The group $T_2 J_1(77)(\mathbb{Q})$ is finite by [Naj26d, Lemma 7.14]. As π_* commutes with T_2 and $\pi_* \pi^* = 5$, we get $5 T_2 J_Y(\mathbb{Q}) \subseteq \pi_* T_2 J_1(77)(\mathbb{Q})$, which proves b). The Frobenius elements at 2 of the cusps of widths 77, 11, 7 and 1 of $X_0(77)$ in the cover $Y \to X_0(77)$ are δ^0, δ^2, δ^3 and δ^5 (see [Naj26d, Section 7.7]), of orders 1, 3, 2 and 6, so above them there are 6 rational cusps, 2 closed cusps of degree 3, 3 of degree 2 and one of degree 6. The cover $X_1(77) \to X_0(77)$ has degree 30 and is unramified, so the closed cusps of degree 1, 3, 10 and 30 of $X_1(77)_{\mathbb{F}_2}$ lie above the cusps of widths 77, 11, 7 and 1, respectively, which gives c), as we also check with the explicit description of the cusps. □

Lemma 9.12. *Let Y be as in Lemma 9.11, and let $U = \mathcal{C}(\mathcal{C} - 1) H^0(Y_{\mathbb{F}_2}, \Omega^1)$. Then $\dim U = 32$, and the restriction map $U \to H^0(\overline{C}, \Omega^1|_{\overline{C}})$ is surjective for each of the*

$$\sum_{r=0}^{3} (r+1) \tbinom{15-3r}{5} = 4989$$

effective divisors $\overline{C}$ of degree 10 supported on the 6 rational cusps and the 2 closed cusps of degree 3 of Lemma 9.11 c), and for the 3 divisors $5\overline{r}$, where $\overline{r}$ is a closed cusp of degree 2 of Lemma 9.11 c).

Proof. We use the model of $Y_{\mathbb{F}_2}$ constructed after [Naj26d, Lemma 7.15], on which we compute the action of the automorphisms of Y over $X_0(77)$ on $H^0(Y_{\mathbb{F}_2}, \Omega^1)$, which commutes with $\mathcal{C}$, and $\dim U = 32$. We use the subspaces $\Omega(jP)$ for $j \leq 8$ at the rational cusps P from the proof of [Naj26d, Proposition 7.16], and we compute the subspaces $\Omega(jP)$ for $j \in \{9, 10\}$ at a rational cusp, for $j \leq 3$ at a cusp of degree 3 and for $j = 5$ at a cusp of degree 2, which

we transport to the other cusps of the same degree with these automorphisms. From these we check that the restriction of U is surjective at all the 4992 divisors of the lemma. □

Lemma 9.13. *Let Y, π and δ be as in Lemma 9.11. The non-cuspidal closed points of $X_1(77)_{\mathbb{F}_2}$ of degree at most 10 are 90 points of degree 10, which form 3 diamond orbits. For each of these points P the image $Q = \pi(P)$ is a closed point of $Y_{\mathbb{F}_2}$ of degree 10, and the divisor*

$$B = T + 2\delta T - 7Q - 2\delta Q - 3\delta^{-1}Q, \qquad T = T_3 Q,$$

on $Y_{\mathbb{F}_2}$ is not principal.

Proof. No elliptic curve over $\mathbb{F}_{2^e}$ with $e \leq 9$ has a point of order 77 (see the proof of [Naj26d, Lemma 7.14]). We compute that exactly 30 elliptic curves over $\mathbb{F}_{2^{10}}$ have a point of order 77, that each of them has $E(\mathbb{F}_{2^{10}}) \simeq \mathbb{Z}/1078\mathbb{Z}$, and that their j-invariants form 3 Frobenius orbits of length 10. The 30 generators up to sign of the unique subgroup of order 77 of each of them are permuted transitively by the diamond operators, which gives 90 closed points of degree 10 in 3 diamond orbits. As the j-invariant of P generates $\mathbb{F}_{2^{10}}$, the image Q has degree 10.

Our model of $Y_{\mathbb{F}_2}$ is a double cover of $X_1(7) \times_{X(1)} X_0(11)$, given by an Artin-Schreier equation, and its automorphism over this curve is δ^3. We compute the images on $X_1(7) \times_{X(1)} X_0(11)$ of P and of the targets of the 4 isogenies of degree 3 of an elliptic curve representing P, from the Tate normal form of the point of order 7 and the j-invariants of the curve and of its quotient by the subgroup of order 11. So each closed point occurring in T is determined up to δ^3. Replacing Q by $\delta^3 Q$ replaces B by $\delta^3 B$, so we may fix Q, and we test all the possible choices of the closed points in T. For the representatives of the 3 orbits the kernels of the isogenies of degree 3 form Frobenius orbits of lengths $(1,3)$, $(1,1,1,1)$ and $(1,3)$, the corresponding closed points have degrees 10 and 30, each with multiplicity 1, and there are 4, 16 and 4 choices. We compute that $\ell(B) = 0$ in all these 24 cases (for the orbits 1, 2 and 3). As T_3 commutes with the diamond operators, this proves the lemma. □

Proposition 9.14. *The group $\mathbb{Z}/77\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let D be the trace divisor of a point of order 77 over a number field of degree 10, let $D' + C'$ be its reduction modulo 2, and let Y, π and δ be as in Lemma 9.11.

Suppose first that $D' = 0$. As C' has degree 10, it is supported on the closed cusps of degree 1 and 3, or it is a single closed cusp of degree 10. By Lemma 9.11 c), the reduction of $\pi_* D$ is then one of the divisors of Lemma 9.12. The group $T_2 J_Y(\mathbb{Q})$ is finite by Lemma 9.11 b), and we apply Proposition 2.18 with $r = 1$ and $\psi_1 = T_2$. By the Eichler-Shimura relation $T_2^* = \mathcal{C}\langle 2\rangle^*$ on $H^0(Y_{\mathbb{F}_2}, \Omega^1)$, and as $\langle 2\rangle^*$ is invertible and commutes with $\mathcal{C}$, we get

$$(\mathcal{C} - 1) T_2^* H^0(Y_{\mathbb{F}_2}, \Omega^1) = \mathcal{C}(\mathcal{C} - 1) H^0(Y_{\mathbb{F}_2}, \Omega^1).$$

So Lemma 9.12 and Proposition 2.18 give a contradiction.

So $D' \neq 0$, and by Lemma 9.13 the divisor D' is a closed point P of degree 10 and $C' = 0$, and the reduction of $\pi_* D$ is $Q = \pi(P)$. As $T_2 J_Y(\mathbb{Q})$ is finite, the operator $A_3 T_2$ annihilates $J_Y(\mathbb{Q})$ by Proposition 2.2 b). By the Eichler-Shimura relation $T_2 = F + \delta V$ on $J_{Y,\mathbb{F}_2}$, and as the Frobenius F is the identity on $J_Y(\mathbb{F}_2)$ and $VF = 2$, the operator T_2 acts on $J_Y(\mathbb{F}_2)$ as $1 + 2\delta$. By Lemma 2.3 we have $A_3 c_0 = A_3 \delta c_0 = 0$ as divisors. So reducing $A_3 T_2 [\pi_* D - 10 c_0] = 0$ modulo 2 we obtain $[(1 + 2\delta) A_3 Q] = 0$. As $\langle 3\rangle$ acts on Y as δ^{-1}, we have $(1 + 2\delta) A_3 Q = B$, with B as in Lemma 9.13, which is a contradiction. □

9.6. **The curve $X_1(85)$.** For the levels 85 and 93 we compute, as in [Naj26d, Section 8], with the model of $X_1(n)$ given by q-expansions (Section 2.3). The reductions modulo 2 of a basis of the lattice of cusp forms of weight 2 on $\Gamma_1(n)$ with integral q-expansions form a basis of $H^0(X_1(n)_{\mathbb{F}_2}, \Omega^1)$, and we compute the Hecke and diamond operators on it. On q-expansions with coefficients in $\mathbb{F}_2$ the Cartier operator acts as Atkin's operator $\sum_j a_j q^j \mapsto \sum_j a_{2j} q^j$ (see [Naj26d, Section 7]), which is also the reduction modulo 2 of T_2, as n is odd. At each rational cusp c we use the local parameter obtained from the parameter q at the cusp ∞ with a diamond operator, and for $j \geq 1$ we write $\lambda_{c,j}(\omega)$ for the j-th coefficient of the expansion of a differential ω at c, i.e. $\omega = \sum_{j\geq 1} \lambda_{c,j}(\omega) q^{j-1} dq$ near c. If $\overline{C} = \sum_c m_c \overline{c}$ is supported on the rational cusps, then the restriction of a subspace U of $H^0(X_1(n)_{\mathbb{F}_2}, \Omega^1)$ to $\overline{C}$ is surjective if and only if the linear forms $\lambda_{c,j}$ with $1 \leq j \leq m_c$ are linearly independent on U.

Lemma 9.15. *Put $k_2(X) = (X^2+2X-1)(X^2+2X+1)$ and $k_3(X) = (X^2+4X+2)(X^2+2X+2)$. Then the groups $(\langle 2\rangle - 1)J_1(85)(\mathbb{Q})$, $k_2(T_2)J_1(85)(\mathbb{Q})$ and $k_3(T_3)J_1(85)(\mathbb{Q})$ are finite.*

Proof. By the proof of [Naj26d, Proposition 8.5], the factors of $J_1(85)$ outside the winding quotient are 2 factors of dimension 2, whose characters are trivial on $\langle 2\rangle$, and all the other factors have finitely many rational points. This gives the first claim. We compute that the characteristic polynomials of T_2 on these 2 factors are X^2+2X-1 and X^2+2X+1, and those of T_3 are X^2+4X+2 and X^2+2X+2. So $k_2(T_2)$ and $k_3(T_3)$ act as 0 on these factors, which proves the other claims. □

Lemma 9.16. *Let $X = X_1(85)$ and*

$$U = (\mathcal{C}-1)\big(k_2(T_2)^* H^0(X_{\mathbb{F}_2}, \Omega^1) + k_3(T_3)^* H^0(X_{\mathbb{F}_2}, \Omega^1)\big),$$

with k_2, k_3 as in Lemma 9.15. The closed cusps of $X_{\mathbb{F}_2}$ have degrees $1^{32}, 4^8, 8^8$ [Naj26d, Proposition 8.5], and the restriction map $U \to H^0(\overline{C}, \Omega^1|_{\overline{C}})$ is surjective for every effective cuspidal divisor $\overline{C}$ of degree 10 on $X_{\mathbb{F}_2}$.

Proof. As $k_2(X) \equiv X^4+1$ and $k_3(X) \equiv X^4 \pmod 2$, the space U is spanned by the images of $(T_2-1)(T_2^4+1)$ and $(T_2-1)T_3^4$ on the reductions of the q-expansions, and we compute that it has dimension 198. It is stable under the diamond operators, as they commute with $\mathcal{C}$ and with the Hecke operators, so it suffices to prove the claim for one divisor in each diamond orbit.

Suppose first that $\overline{C} = \sum_c m_c \overline{c}$ is supported on the 32 rational cusps. The diamond operators act transitively on them, so we may assume that m_∞ is the largest multiplicity, and then $m_c \leq 5$ for $c \neq \infty$. We compute the 165 linear forms $\lambda_{\infty,j}$ with $j \leq 10$ and $\lambda_{c,j}$ with $j \leq 5$ for the other 31 rational cusps c on U. They span a space of dimension 152. For a linear relation between them let j_c be the largest j for which $\lambda_{c,j}$ occurs in it, with $j_c = 0$ if there is none, and put $w = \max_c j_c + \sum_{c\neq\infty} j_c$. We check that $w \geq 32$ for each of the $2^{13}-1 = 8191$ non-trivial linear relations. A relation between the forms $\lambda_{c,j}$ with $j \leq m_c$ would have $j_c \leq m_c \leq m_\infty$ for every c, and hence $w \leq m_\infty + \sum_{c\neq\infty} m_c = 10$. So these forms are linearly independent on U.

Suppose now that $\overline{C}$ contains a cusp of degree 4 or 8. The diamond operators act transitively on the 8 cusps of degree 4, and the 8 cusps of degree 8 form 2 diamond orbits. So we may assume that $\overline{C}$ is the sum of a fixed cusp of degree 4 and a divisor of degree 6 on the rational cusps, or of a fixed cusp of degree 4, one of the 8 cusps of degree 4 and a divisor of degree 2 on the rational cusps, or of one of 2 fixed cusps of degree 8 and a divisor of degree

2 on the rational cusps. We compute the expansions of the differentials at these cusps, to 2 coefficients at the cusps of degree 4 and to 1 coefficient at the cusps of degree 8, from the Tate curves $E(q^{17})$ with the point $\zeta_5 q$ (degree 4), $E(q^5)$ with the point $\zeta_{17} q$ (degree 8) and $E(q)$ with the point ζ_{85} (degree 8), using the modular units of [DvH14, Sections 2 and 2.1], and we check that the restriction of U is surjective at each of the

$$\binom{37}{6} + 8\binom{33}{2} + 2\binom{33}{2} = 2330064$$

divisors of these forms. □

Lemma 9.17. *The non-cuspidal closed points of $X_1(85)_{\mathbb{F}_2}$ of degree at most 10 are 160 points of degree 9, which form 5 diamond orbits, and 128 points of degree 10, which form 4 diamond orbits. Put $\sigma = \langle 2\rangle^{-1}$, $\tau = \langle 3\rangle$ and $A_3 = T_3 - 1 - 3\tau$. For each of these points P the divisor*

$$B = A_3(\sigma P - P) = \sigma T - T - \sigma P + P - 3\sigma\tau P + 3\tau P, \qquad T = T_3 P,$$

is not principal.

Proof. For the points of degree at most 9 this is shown in the proof of [Naj26d, Proposition 8.5]. We compute that the non-cuspidal closed points of degree 10 come from elliptic curves over $\mathbb{F}_{2^{10}}$ with 1020 points, whose j-invariants form 4 Frobenius orbits of length 10 and whose groups of points are cyclic. This gives 128 closed points of degree 10, which form 4 diamond orbits of length 32. For a representative P of each orbit, T_3P consists of a closed point of degree 10 and one of degree 30, each with multiplicity 1, so B has positive and negative parts of degree 80. As in [Naj26d, Section 8] we compute local parameters at P and at the points of T_3P from the deformation $a_6 \mapsto a_6 + t$ of the corresponding ordinary elliptic curves, and their images on the model given by q-expansions, of genus 225, from the modular units of [DvH14, Sections 2 and 2.1]. On this model we compute σP, τP and $\sigma\tau P$ with the diamond operators, using that the diamond operator $\langle a\rangle$ of this model corresponds to $\langle a\rangle^{-1}$ on the moduli problem, which we verify for $a \in \{2, 3\}$ by comparing the modular units at the points q and q^a of order 85 of the Tate curve $E(q^{85})$. We check with Lemma 2.13, with $\mathcal{L} = \mathcal{M} = K_X$, for which $H^0(X, 2K_X)$ has dimension 672, that $\ell(B) = 0$ for these 4 representatives. As A_3 commutes with the diamond operators, this proves the lemma. □

Proposition 9.18. *The group $\mathbb{Z}/85\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let D be the trace divisor of a point of order 85 over a number field of degree 10, and let $D' + C'$ be its reduction modulo 2.

Suppose first that $D' = 0$. By Lemma 9.15 we may apply Proposition 2.18 with $H = \{1\}$, $r = 2$, $\psi_1 = k_2(T_2)$ and $\psi_2 = k_3(T_3)$, and by Lemma 9.16 it shows that D does not reduce to C', which is a contradiction.

So $D' \neq 0$, and by Lemma 9.17, either D' is a closed point P of degree 10 and $C' = 0$, or D' is a closed point P of degree 9 and C' is a cusp of degree 1, which is the reduction of a rational cusp c. Let σ, τ and A_3 be as in Lemma 9.17. The class $[\sigma D - D] = (\sigma - 1)[D - 10c_0] + 10[\sigma c_0 - c_0]$ is torsion by Lemma 9.15 and by the Manin-Drinfeld theorem, so it is annihilated by A_3 by Proposition 2.2 b). As A_3 annihilates the rational cusps c and σc as divisors, the reduction of $A_3(\sigma D - D)$ is $A_3(\sigma P - P)$, so $A_3(\sigma P - P)$ is principal. This contradicts Lemma 9.17. □

9.7. **The curve $X_1(91)$.** For $n = 91$ we work on a quotient Y of $X_1(91)$ of genus 23 with an automorphism τ of order 3, and use the element $\tau - 1$, which has finite image on $J_Y(\mathbb{Q})$. As it kills the pull-backs of divisors from $Y/\langle\tau\rangle$, the criterion of Proposition 2.18 fails at the cuspidal divisors which contain such pull-backs. The following lemma shows that near such a divisor the fibre of the corresponding map to the Jacobian consists only of divisors of this form.

Lemma 9.19. *Let $Y = X_1(n)/H$ be as in Section 2.6, let τ be an automorphism of Y of order 3 induced by a diamond operator, let $Z = Y/\langle\tau\rangle$, assume that Z has positive genus, and let $\pi : Y \to Z$ be the quotient map. Assume that $(\tau - 1)J_Y(\mathbb{Q})$ is finite, and put*

$$U = (\mathcal{C} - 1)(\tau^* - 1)H^0(Y_{\mathbb{F}_2}, \Omega^1).$$

Let A be an effective rational divisor of degree d on Y, and let C be an effective divisor of degree d on Y defined over $\mathbb{Q}_2$, with the same reduction $\overline{C}$ modulo 2 as A, such that $(\tau - 1)[C - dc_0]$ is torsion. Suppose that $C = C_0 + \pi^*E$ for an effective divisor E of degree k on Z defined over $\mathbb{Q}_2$, such that the morphism $Z^{(k)} \to Y^{(d)}$, $E' \mapsto C_0 + \pi^*E'$, of the smooth models over $\mathbb{Z}_2$ induces a surjection of the completed local rings at $\overline{E}$ and $\overline{C}$. If the restriction map $U \to H^0(\overline{C}, \Omega^1|_{\overline{C}})$ has rank $d - k$, then $A \geq C_0$.

Proof. By Lemma 2.1 the curve Z has good reduction at 2 and π extends to the smooth models over $\mathbb{Z}_2$. Put $\alpha = \tau - 1$ and $M = T_2 - \langle 2\rangle$. The class $\alpha[A - C] = \alpha[A - dc_0] - \alpha[C - dc_0] \in J_Y(\mathbb{Q}_2)$ is torsion by assumption, and it reduces to 0, as A and C have the same reduction. It is killed by 2, by the argument behind the result of Parent recalled in Section 2.3 (see [Naj26d, Section 2.3]), which is local at 2. So $M\alpha[A-C] = 0$ by Lemma 2.17, applied to the Néron model of J_Y over $\mathbb{Z}_2$ with $T = T_2$ and $\delta = \langle 2\rangle$. Consider the morphism

$$\Psi : Y^{(d)} \to J_Y, \qquad B \mapsto M\alpha[B - dc_0]$$

over $\mathbb{Z}_2$. Then $\Psi(A) = \Psi(C)$. As in the proof of [Naj26d, Proposition 7.3], the image of the cotangent map of Ψ at $\overline{C}$ is the restriction to $\overline{C}$ of $(\tau^* - 1)(\mathcal{C} - 1)\langle 2\rangle^* H^0(Y_{\mathbb{F}_2}, \Omega^1)$, which equals U, as $\langle 2\rangle^*$ is invertible and commutes with $\mathcal{C}$ and τ^*. By assumption this restriction has dimension $d - k$. Choose local coordinates $f_1, \dots, f_g$ of J_Y over $\mathbb{Z}_2$ at $\Psi(C)$, vanishing at $\Psi(C)$, such that the differentials of $f_1 \circ \Psi, \dots, f_{d-k} \circ \Psi$ at $\overline{C}$ are linearly independent. As $Y^{(d)}$ is smooth over $\mathbb{Z}_2$ of relative dimension d, the closed formal subscheme $\mathcal{V}$ of the formal neighbourhood of $\overline{C}$ defined by $f_1 \circ \Psi, \dots, f_{d-k} \circ \Psi$ is formally smooth over $\mathbb{Z}_2$ of relative dimension k, i.e. its ring is isomorphic to $\mathbb{Z}_2[[s_1, \dots, s_k]]$. As $\tau\pi^* = \pi^*$ on J_Z, we have $\Psi(C_0 + \pi^*E') = \Psi(C) + M\alpha\pi^*[E' - E] = \Psi(C)$ for every E', so the image of the formal neighbourhood of $\overline{E}$ in $Z^{(k)}$, whose ring is isomorphic to $\mathbb{Z}_2[[e_1, \dots, e_k]]$, lies in $\mathcal{V}$. By assumption the corresponding homomorphism $\mathbb{Z}_2[[s_1, \dots, s_k]] \to \mathbb{Z}_2[[e_1, \dots, e_k]]$ is surjective, and as both rings are integral domains of dimension $k + 1$, it is an isomorphism. So $\mathcal{V}$ is the image of the formal neighbourhood of $\overline{E}$. The point $A \in Y^{(d)}(\mathbb{Z}_2)$ reduces to $\overline{C}$ and $\Psi(A) = \Psi(C)$, so it lies in $\mathcal{V}$, and hence $A = C_0 + \pi^*E'$ for some $E' \in Z^{(k)}(\mathbb{Z}_2)$. In particular $A \geq C_0$. □

Note that for $k = 0$ the conclusion is $A = C$, as in Proposition 2.18 with $r = 1$ and $\psi_1 = \tau - 1$.

Lemma 9.20. *Let $H \subseteq \Delta(91)$ be the subgroup of the $\langle a\rangle$ with $a \equiv \pm 1 \pmod 7$, which has order 12, let $Y = X_1(91)/H$, let $\pi_X : X_1(91) \to Y$ be the quotient map, let τ be the automorphism of Y induced by $\langle 3\rangle$, and let $\pi : Y \to Z = Y/\langle\tau\rangle$ be the quotient map.*

a) *The group H acts freely on the geometric points of $X_1(91)$, in characteristic 0 and 2. The curve Y is the normalization of $X_1(7) \times_{X(1)} X_0(13)$, with $\pi_X(E,P) = (E, 13P, \langle 7P\rangle)$, it has genus 23 and good reduction at 2, and it is a curve as in Section 2.6. The automorphism τ has order 3, and $Z = X_0(91)$ has genus 7. The group $(\tau-1)J_Y(\mathbb{Q})$ is finite.*

b) *The closed cusps of $X_1(91)_{\mathbb{F}_2}$ have degrees $1^{36}, 3^{12}, 12^6$. The push-forward by π_X maps each of those of degree 1 to one of the reductions $\overline{c_1}, \overline{c_2}, \overline{c_3}$ of the 3 rational cusps c_1, c_2, c_3 of Y of width 91, and each of those of degree 3 to the reduction $\overline{q}$, which has degree 3, of a closed cusp q of Y of degree 3 and width 13, in both cases with multiplicity 1. The automorphism τ permutes c_1, c_2, c_3 cyclically and the 3 geometric points of q transitively, and π is unramified at these cusps.*

c) *The fixed points of τ on $Y_{\mathbb{F}_2}$ are 2 closed points p_1, p_2 of degree 2, and τ acts on the tangent spaces at them by a primitive cube root of unity. Each p_i is the reduction of a unique point P_i of Y of degree 2 over $\mathbb{Q}_2$ with $\tau P_i = P_i$, and $\pi^*\pi(P_i) = 3P_i$.*

d) *The non-cuspidal closed points of $X_1(91)_{\mathbb{F}_2}$ of degree at most 10 are 3 points of degree 8 and 144 points of degree 9. The push-forward by π_X of each of the points of degree 8 is $4p_1$ or $4p_2$.*

Proof. a) If $\langle a\rangle \in H$ fixes a geometric point, then by [Naj26d, Lemma 7.2] either it is a cusp and a is congruent to the same sign ± 1 modulo 7 and 13, or it is not a cusp and $a \not\equiv \pm 1 \pmod 7$. As $a \equiv \pm 1 \pmod 7$, in both cases $\langle a\rangle = 1$. The map π_X is invariant under H, and $X_1(91) \to X_1(7) \times_{X(1)} X_0(13)$ has degree $i(91)/(i(7)\cdot 14) = 12$, which proves the second assertion. By the Riemann-Hurwitz formula Y has genus $1 + (265-1)/12 = 23$, as $X_1(91)$ has genus 265, and as H acts freely also in characteristic 2, it is a curve as in Section 2.6, with good reduction at 2. As 3 has order 6 in $(\mathbb{Z}/7\mathbb{Z})^\times$, the automorphism τ generates $\Delta(91)/H$, which has order 3, and $Z = X_1(91)/\Delta(91) = X_0(91)$. The group $(\langle 3\rangle - 1)J_1(91)(\mathbb{Q})$ is finite by the proof of [Naj26d, Proposition 8.5]. As π_{X*} intertwines $\langle 3\rangle$ and τ and $\pi_{X*}\pi_X^* = 12$, we get $12(\tau-1)J_Y(\mathbb{Q}) \subseteq \pi_{X*}(\langle 3\rangle - 1)J_1(91)(\mathbb{Q})$, so $(\tau-1)J_Y(\mathbb{Q})$ is finite.

We construct $Y_{\mathbb{F}_2}$ as follows. Over $\mathbb{F}_2(t)$ put $b = t^3 - t^2$, $c = t^2 - t$ and $E_t : y^2 + (1-c)xy - by = x^3 - bx^2$, on which $(0,0)$ has order 7, and

$$j_{13}(s) = \frac{(s^2+5s+13)(s^4+7s^3+20s^2+19s+1)^3}{s}.$$

We check that $j_{13}(s) = j(E_t)$ defines an irreducible extension of degree 14 of $\mathbb{F}_2(t)$ of genus 23, so its normalization is $Y_{\mathbb{F}_2}$, and that $t \mapsto 1/(t+1)$, $s \mapsto s$ defines an automorphism of $Y_{\mathbb{F}_2}$ of order 3 over $X_0(91)_{\mathbb{F}_2}$. It acts on $X_1(7)$ as a diamond operator and trivially on $X_0(13)$, so it is τ or τ^{-1}, and as all our assertions depend only on the group generated by τ, we may compute with it.

b) The cusps of $Y_{\mathbb{F}_2}$ are the poles of $j(E_t)$, namely 3 rational cusps of width 91, 3 of width 7, and one closed cusp of degree 3 of width 13 and one of width 1, and the Galois orbits of cusps of Y have the same degrees. The degrees of the closed cusps of $X_1(91)_{\mathbb{F}_2}$ and the other assertions follow from the description of the cusps, as we check.

c) The fixed points of τ on $Y_{\mathbb{F}_2}$ are the ramification points of $Y_{\mathbb{F}_2} \to Z_{\mathbb{F}_2}$, which is tamely ramified of degree 3. As $Y_{\mathbb{F}_2}$ and $Z_{\mathbb{F}_2}$ have genus 23 and 7, the Riemann-Hurwitz formula $44 = 3\cdot 12 + 2r$ shows that there are $r = 4$ geometric fixed points. We compute that above the closed point $t^2+t+1=0$ there are 2 closed points of degree 2 of $Y_{\mathbb{F}_2}$ which are fixed by τ, and that τ multiplies a uniformizer at each of them by a primitive cube root of unity,

modulo its square. These are the 4 geometric fixed points. So the fixed point scheme of τ over $\mathbb{Z}_2$ is étale at p_i, which gives the unique lift P_i, and π is totally ramified at P_i.

d) The non-cuspidal closed points of degree at most 9 are given in [Naj26d, Proposition 8.5], and we compute that there are none of degree 10. The points of degree 8 have $j = 0$ and come from 2 elliptic curves over $\mathbb{F}_{2^8}$ with 273 points [Naj26d, Proposition 8.5]. We compute that their groups of points are cyclic, and we check that on each of them an automorphism u of order 3 satisfies $u(P) = 16P$ for a point P of order 91, and hence for every point of order 91 over $\mathbb{F}_{2^8}$, as these are multiples of P. As $16 \equiv 2 \pmod 7$ and $16 \equiv 3 \pmod{13}$, the automorphism u gives an isomorphism between $(E, 13P, \langle 7P\rangle)$ and $(E, 2 \cdot 13P, \langle 7P\rangle)$, which is the image of $(E, 13P, \langle 7P\rangle)$ under the automorphism of Y induced by $\langle 2\rangle$, and this automorphism is τ^{-1}, as $2 \equiv 3^2 \pmod 7$. So the image of a point of degree 8 on $Y_{\mathbb{F}_2}$ is fixed by τ, and by c) it is p_1 or p_2. As it has degree 2, the push-forward is $4p_1$ or $4p_2$. □

Lemma 9.21. *Let Y, τ, c_1, c_2, c_3, q and p_1, p_2 be as in Lemma 9.20, and let $U = (\mathcal{C} - 1)(\tau^* - 1)H^0(Y_{\mathbb{F}_2}, \Omega^1)$. Then $\dim U = 14$, and the following hold.*

a) *For each of the 120 divisors $\overline{C} = a_1\overline{c_1} + a_2\overline{c_2} + a_3\overline{c_3} + b\overline{q}$ with $a_1 + a_2 + a_3 + 3b = 10$, the restriction map $U \to H^0(\overline{C}, \Omega^1|_{\overline{C}})$ has rank $10 - \min(a_1, a_2, a_3) - b$.*

b) *For $i \in \{1, 2\}$ and each of the 6 effective divisors $\overline{R}$ of degree 2 supported on $\overline{c_1}, \overline{c_2}, \overline{c_3}$, the restriction map $U \to H^0(\overline{C}, \Omega^1|_{\overline{C}})$ for $\overline{C} = 4p_i + \overline{R}$ has rank 8.*

Proof. On the model of the proof of Lemma 9.20 we compute the matrices of $\mathcal{C}$ and τ^*, which commute, and of ranks 21 and 16 for $\mathcal{C}$ and $\tau^* - 1$, and $\dim U = 14$. We compute the spaces $\Omega(\overline{C})$ and the ranks for a) and b). □

Lemma 9.22. *Let Y, Z, π, c_1, c_2, c_3, q and P_1, P_2 be as in Lemma 9.20, considered over $\mathbb{Z}_2$, and let $C = C_0 + \pi^*E$ be one of the following divisors.*

a) *$C = a_1c_1 + a_2c_2 + a_3c_3 + bq$ with $a_1 + a_2 + a_3 + 3b = 10$, $E = m\pi(c_1) + b\pi(q)$ with $m = \min(a_1, a_2, a_3)$, and $C_0 = C - \pi^*E$.*

b) *$C = 4P_i + R$ with R an effective divisor of degree 2 supported on c_1, c_2, c_3, $E = \pi(P_i)$ and $C_0 = P_i + R$.*

Then the morphism $Z^{(k)} \to Y^{(10)}$, $E' \mapsto C_0 + \pi^*E'$, where $k = \deg E$, induces a surjection of the completed local rings at $\overline{E}$ and $\overline{C}$.

Proof. Surjectivity can be checked after the unramified base change to the ring of integers W of the unramified extension of $\mathbb{Q}_2$ of degree 6, over which all the points involved split into points defined over W. Near $\overline{E}$ a divisor E' decomposes as a sum of divisors near the geometric points of $\overline{E}$, each of them given by a monic polynomial in a local parameter w of Z whose degree is the multiplicity of the point in $\overline{E}$, and with non-leading coefficients in the maximal ideal. It suffices to show that these polynomials can be recovered from the local equations of $C_0 + \pi^*E'$.

a) As π is unramified at c_1, c_2, c_3 and at the geometric points of q, the pull-back of w is a local parameter u at each of the points above. Some a_i equals m, so C_0 does not contain c_i, and near c_i the divisor $C_0 + \pi^*E'$ is given by $f(u)$, where $f(w)$ is the polynomial of the part of E' near $\pi(c_1)$. Similarly C_0 does not contain q, and near each geometric point of q the divisor $C_0 + \pi^*E'$ is given by the polynomial of the part of E' near $\pi(q)$.

b) Near each of the 2 geometric points of P_i, as τ has order prime to 2 and multiplies the tangent space by a primitive cube root of unity ζ, there is a local parameter z with $\tau^*z = \zeta z$, and $w = z^3$ is a local parameter of Z. The part of E' near the image of this point

is given by $w-a$, and near the point the divisor $C_0+\pi^*E'$ is given by $z(z^3-a)=z^4-az$, whose coefficient of z recovers a. □

Proposition 9.23. *The group $\mathbb{Z}/91\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let D be the trace divisor of a point of order 91 over a number field of degree 10, let $D'+C'$ be its reduction modulo 2, and let Y, π_X, τ and π be as in Lemma 9.20. The divisor $A=\pi_{X*}D$ is an effective rational divisor of degree 10 on Y whose support contains no cusp, and its reduction is $\pi_{X*}(D'+C')$. By Lemma 9.20 d), either $D'=0$, or D' is a closed point of degree 8 and C' has degree 2, or D' is a closed point of degree 9 and C' is a cusp of degree 1.

Suppose first that $D'=0$. By Lemma 9.20 b), the reduction of A is $\overline{C}=a_1\overline{c_1}+a_2\overline{c_2}+a_3\overline{c_3}+b\overline{q}$ with $a_1+a_2+a_3+3b=10$, and it is the reduction of the rational cuspidal divisor $C=a_1c_1+a_2c_2+a_3c_3+bq$. The class $(\tau-1)[C-10c_0]$ is cuspidal, so it is torsion by the Manin-Drinfeld theorem. With m, E and C_0 as in Lemma 9.22 a) we have $k=\deg E=m+b$, and C_0 is cuspidal of degree $10-3k$, which is positive, as $3\nmid 10$. By Lemma 9.21 a) and Lemma 9.22 a), Lemma 9.19 applies and gives $A\geq C_0$, which is impossible, as the support of A contains no cusp.

Suppose now that D' is a closed point of degree 8. The closed cusps of $X_1(91)_{\mathbb{F}_2}$ of degree at most 2 have degree 1, so by Lemma 9.20 b) and d) the reduction of A is $4p_i+\overline{R}$ for some i and an effective divisor $\overline{R}$ of degree 2 supported on $\overline{c_1},\overline{c_2},\overline{c_3}$. It is the reduction of $C=4P_i+R$, where R is the rational cuspidal divisor which reduces to $\overline{R}$. As $\tau P_i=P_i$, the class $(\tau-1)[C-10c_0]=[\tau R-R]-10[\tau c_0-c_0]$ is torsion. With E and C_0 as in Lemma 9.22 b) we have $k=2$, and Lemma 9.21 b), Lemma 9.22 b) and Lemma 9.19 give $A\geq C_0\geq R$, which is impossible.

Suppose finally that D' is a closed point P of degree 9 and C' is the reduction of a rational cusp c. Put $\sigma=\langle 3\rangle^{-1}$. The class $[\sigma D-D]=(\sigma-1)[D-10c_0]+10[\sigma c_0-c_0]$ is torsion, as $(\langle 3\rangle-1)J_1(91)(\mathbb{Q})$ is finite (see the proof of [Naj26d, Proposition 8.5]) and by the Manin-Drinfeld theorem, so it is annihilated by A_3, and as A_3 annihilates the rational cusps c and σc as divisors, the divisor $A_3(\sigma P-P)$ on $X_1(91)_{\mathbb{F}_2}$ is principal. In the proof of [Naj26d, Proposition 8.5] it is shown that this is not the case for any non-cuspidal closed point P of degree 9, which is a contradiction. □

9.8. **The curve $X_1(93)$.**

Lemma 9.24. *Let $X=X_1(93)$, let $h=\langle 32\rangle$, which has order 2 in $\Delta(93)$, and let*

$$U=(\mathcal{C}-1)\big((\langle 2\rangle^*-1)H^0(X_{\mathbb{F}_2},\Omega^1)+(\langle 5\rangle^*-1)H^0(X_{\mathbb{F}_2},\Omega^1)\big).$$

a) *The closed cusps of $X_{\mathbb{F}_2}$ have degrees $1^{30},2^{15},5^6,10^3$, and h maps every closed cusp of degree 2 or 10 to itself. The automorphism h fixes no non-cuspidal geometric point of X in characteristic 0.*

b) *We have $\dim U=248$, and the restriction map $U\to H^0(\overline{C},\Omega^1|_{\overline{C}})$ is surjective for every effective divisor $\overline{C}$ of degree 10 on $X_{\mathbb{F}_2}$ supported on the closed cusps of degree 1 and 5.*

Proof. a) The assertions on the cusps follow from their description, as we check. As $32^2\equiv 1 \pmod{93}$, we have $32^2\not\equiv -1$ and $32^2\pm 32+1\not\equiv 0 \pmod{93}$, so the last assertion follows from [Naj26d, Lemma 7.2].

b) We use the model given by q-expansions, as in Section 9.6, and we compute that $\dim U = 248$. The space U is stable under the diamond operators, so it suffices to prove the claim for one divisor in each diamond orbit. If $\overline{C}$ is supported on the 30 rational cusps, we may assume that ∞ has the largest multiplicity in it, and we compute the 155 linear forms $\lambda_{\infty,j}$ with $j \leq 10$ and $\lambda_{c,j}$ with $j \leq 5$ for the other 29 rational cusps c on U. They span a space of dimension 150, and with w as in the proof of Lemma 9.16 we check that $w \geq 30$ for each of the $2^5 - 1 = 31$ non-trivial linear relations between them. As in the proof of Lemma 9.16, this proves the claim for these divisors. The 6 cusps of degree 5 form one diamond orbit. If $\overline{C}$ contains one of them, we may assume that it contains a fixed one, and then $\overline{C}$ is the sum of this cusp and of a divisor of degree 5 on the rational cusps, or of this cusp and one of the 6 cusps of degree 5. We compute the expansions of the differentials at the cusps of degree 5 to 2 coefficients from the Tate curve $E(q^3)$ with the point $\zeta_{31}q$, using the modular units of [DvH14, Sections 2 and 2.1], and we check that the restriction of U is surjective at each of the $\binom{34}{5} + 6 = 278262$ divisors of these forms. □

Proposition 9.25. *The group $\mathbb{Z}/93\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let $X = X_1(93)$, let D be the trace divisor of a point x of order 93 over a number field of degree 10, and let $D' + C'$ be its reduction modulo 2. By Remark 4.2, D is a closed point of degree 10. By the proof of [Naj26d, Proposition 8.5], the only factor of $J_1(93)$ outside the winding quotient has trivial character, so $(g-1)J_1(93)(\mathbb{Q})$ is finite for every diamond operator g.

The non-cuspidal closed points of $X_{\mathbb{F}_2}$ of degree at most 9 are 10 points of degree 9, which form one diamond orbit [Naj26d, Proposition 8.5], and we compute that there are none of degree 10. Suppose that $D' \neq 0$. Then D' is a closed point P of degree 9, and C' is the reduction of a rational cusp c. Put $\sigma = \langle 2 \rangle^{-1}$, $\tau = \langle 5 \rangle$ and $A_5 = T_5 - 1 - 5\tau$. As in the proof of Proposition 9.18, the class $[\sigma D - D]$ is torsion and annihilated by A_5, and the reduction of $A_5(\sigma D - D)$ is $A_5(\sigma P - P)$, so $A_5(\sigma P - P)$ is principal. In the proof of [Naj26d, Proposition 8.5] it is shown that this is not the case, which is a contradiction.

So $D' = 0$. Let $L = \mathbb{Q}(\zeta_{93})$, over which all the cusps of X are defined, and let λ be a prime of L above 2. As the cuspidal subscheme is finite étale at 2, the divisor C' is the reduction modulo λ of a unique cuspidal divisor C defined over L. Suppose first that C' contains a closed cusp of degree 2 or 10, and let h be as in Lemma 9.24. We follow the proof of Lemma 2.10 c). The class $y = (h-1)[D-C] = (h-1)[D-10c_0] - (h-1)[C-10c_0] \in J_1(93)(L)$ is torsion, by the finiteness of $(h-1)J_1(93)(\mathbb{Q})$ and the Manin-Drinfeld theorem, and it reduces to 0 modulo λ, so $2y = 0$ by the result of Parent recalled in Section 2.3, as L is unramified above 2. So $2hD + 2C \sim 2D + 2hC$ over L. Let G be the largest effective divisor with $G \leq C$ and $G \leq hC$. By Lemma 9.24 a), h fixes the closed cusp of degree 2 or 10 contained in C, so $\deg G \geq 2$. The divisors $2hD + 2(C - G)$ and $2D + 2(hC - G)$ are effective, linearly equivalent and of degree at most 36. As Abramovich's bound gives $\operatorname{gon}_L X \geq \operatorname{gon}_{\mathbb{C}} X > 38.09 > 36$, they are equal by Lemma 2.8, and comparing their non-cuspidal parts we get $hD = D$. So h maps the closed point D to itself, and it induces an automorphism η of its residue field $K = \mathbb{Q}(x)$, of degree 10. As h fixes no geometric point of D by Lemma 9.24 a), η has order 2, and its fixed field K_0 has degree 5. The morphism $f : X_1(93) \to X_1(31)$, $(E, P) \mapsto (E, 3P)$, satisfies $f \circ h = f$, as $32 \equiv 1 \pmod{31}$. So the residue field of the non-cuspidal point $f(x)$ is contained in K_0, and there is an elliptic

curve over a number field of degree 1 or 5 with a point of order 31. This is impossible, as $31 \notin S(1) \cup S(5)$ [Maz77, DKSS23].

Suppose finally that C' is supported on the closed cusps of degree 1 and 5. By the finiteness of $(\langle 2\rangle - 1)J_1(93)(\mathbb{Q})$ and $(\langle 5\rangle - 1)J_1(93)(\mathbb{Q})$ we may apply Proposition 2.18 with $H = \{1\}$, $r = 2$, $\psi_1 = \langle 2\rangle - 1$ and $\psi_2 = \langle 5\rangle - 1$, and by Lemma 9.24 b) it shows that D does not reduce to C', which is a contradiction. □

10. Further cyclic groups

We show that the groups $\mathbb{Z}/n\mathbb{Z}$ for

$$n \in \{57, 63, 65, 69, 78, 81, 87, 90, 99, 105, 117\}$$

and the group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/39\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over a number field of degree 10. For all of them we reduce modulo 2 the trace divisor on $X_1(n)$, or its push-forward to a quotient of $X_1(n)$, to $X_0(n)$ or to $X_1(n')$ for a divisor n' of n. We exclude the reductions with non-cuspidal support mostly with the Eichler-Shimura relation and Riemann-Roch computations over finite fields, often by linear algebra in the canonical ring (Lemma 2.13), and the entirely cuspidal reductions by gonality bounds or by formal immersion at 2. For $n \in \{57, 65\}$ the Jacobian $J_1(n)$ has positive rank, and for these levels and for $n \in \{99, 105\}$ we use elements of the Hecke algebra whose image on $J_1(n)(\mathbb{Q})$ is finite. The groups $\mathbb{Z}/n\mathbb{Z}$ with $n \in \{57, 63, 65, 69, 81, 87\}$ were excluded in some of the degrees 6, 7, 8 and 9 in [Naj26d], where the curves $X_1(39)$ and $X_1(45)$ were also studied, and we reuse the computations from there which do not depend on the degree.

10.1. **The group $\mathbb{Z}/57\mathbb{Z}$.** We largely follow the proof of [Naj26d, Proposition 8.3], which excludes $\mathbb{Z}/57\mathbb{Z}$ over nonic fields. The Jacobians $J_1(57)$ and $J_1(65)$ have positive rank, and we use the following facts about them.

Lemma 10.1. *Let $n \in \{57, 65\}$, let X be $X_1(n)$ or its quotient by a subgroup of $\Delta(n)$, and let a_r be the r-th Fourier coefficient of the newform 57.2.a.a if $n = 57$, and of 65.2.a.a if $n = 65$. Then $(\langle a\rangle - 1)J_X(\mathbb{Q})$ is finite for every $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, and $(T_r - a_r)J_X(\mathbb{Q})$ is finite for $r \in \{2, 5, 7, 11, 13\}$ if $n = 57$ and for $r \in \{2, 3, 7, 11, 17\}$ if $n = 65$, where*

$$(a_2, a_5, a_7, a_{11}, a_{13}) = (-2, -3, -5, 1, 2) \quad \text{for } n = 57,$$
$$(a_2, a_3, a_7, a_{11}, a_{17}) = (-1, -2, -4, 2, 2) \quad \text{for } n = 65.$$

Proof. By [Naj26d, Lemma 9.1], the newform f above is the only newform of level dividing n with $L(f, 1) = 0$, and it has trivial character. By Kato's theorem all the isogeny factors of $J_1(n)$ except the one corresponding to f have finitely many rational points, and the operators $\langle a\rangle - 1$ and $T_r - a_r$ act as 0 on the factor corresponding to f (see the proofs of [Naj26d, Lemma 9.1, Propositions 8.3 and 8.4]). The Jacobian of X is a quotient of $J_1(n)$. □

We first restrict the possible reductions with a quotient of $X_1(57)$ of genus 9. On it we use the model given by q-expansions, which is the dual model of Section 2.3. The diamond operator $\langle 5\rangle$ acts on this quotient as an involution, so it is the same on both models.

Lemma 10.2. *Let $H \subseteq \Delta(57)$ be the subgroup of order 9, which is generated by $\langle 4\rangle$, let $Y_{57} := X_1(57)/H$, let $\pi\colon X_1(57) \to Y_{57}$ be the quotient map, and put $\sigma := \langle 5\rangle$ and $\alpha := \sigma - 1$. Then Y_{57} has genus 9 and good reduction at 2, the group $\alpha J_{Y_{57}}(\mathbb{Q})$ is finite, and*

$$J_{Y_{57}}(\mathbb{F}_2) \simeq \mathbb{Z}/105\mathbb{Z} \times \mathbb{Z}/210\mathbb{Z}.$$

The group $V := \alpha J_{Y_{57}}(\mathbb{F}_2)$ is isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$ and is generated by the images under α of the classes of the cuspidal divisors of degree 0 on $Y_{57,\mathbb{F}_2}$. The reduction modulo 2 of $\alpha J_{Y_{57}}(\mathbb{Q})$ is contained in the kernel $V_0 \simeq \mathbb{Z}/7\mathbb{Z}$ of the operator $T_5 - \langle 5\rangle - 5$ of the dual model on V.

Proof. The genus and the good reduction are [Naj26d, Lemma 9.4], and $\alpha J_{Y_{57}}(\mathbb{Q})$ is finite by Lemma 10.1. The group $J_{Y_{57}}(\mathbb{F}_2)$, the fact that $V \simeq (\mathbb{Z}/7\mathbb{Z})^2$ is generated by the images of the cuspidal classes, and the kernel $V_0 \simeq \mathbb{Z}/7\mathbb{Z}$ of $T_5 - \langle 5\rangle - 5$ on V are computed in Step 1 of the proof of [Naj26d, Proposition 8.3]. By Proposition 2.2 b), in the form for the dual model (Section 2.3), the operator $T_5 - \langle 5\rangle - 5$ annihilates the finite group $\alpha J_{Y_{57}}(\mathbb{Q})$, so the reduction of this group lies in V_0. □

Lemma 10.3. *Let π, α and V_0 be as in Lemma 10.2, and let c_* be a rational cusp of Y_{57}. Let P be a non-cuspidal closed point of $X_1(57)_{\mathbb{F}_2}$ of degree $e \leq 10$ such that $\alpha[\pi_* P - e\,\overline{c_*}] \in V_0$. Then $e \in \{6, 8, 10\}$. The non-cuspidal closed points of $X_1(57)_{\mathbb{F}_2}$ of degree 10 form 12 orbits under $\Delta(57)$, and if $e = 10$, then P lies in one of the 6 orbits whose points (E, R) have the property that $j(E/\langle R\rangle)$ is a root of one of the polynomials*

$$x^{10} + x^7 + 1, \qquad x^{10} + x^9 + x^7 + x^3 + 1, \qquad x^{10} + x^7 + x^6 + x^3 + 1.$$

If c is one of the 2 closed cusps of $X_1(57)_{\mathbb{F}_2}$ of degree 9, then $\alpha[\pi_* c - 9\,\overline{c_*}] \notin V_0$.

Proof. For two rational cusps c_* and c'_* of Y_{57} the class $\alpha[c_* - c'_*]$ lies in $\alpha J_{Y_{57}}(\mathbb{Q})$, so its reduction lies in V_0 by Lemma 10.2, and the conditions do not depend on the choice of c_*. By the Hasse bound $e \geq 6$, as $\#E(\mathbb{F}_{2^k}) \leq 44 < 57$ for every elliptic curve E over $\mathbb{F}_{2^k}$ with $k \leq 5$. For $e \leq 9$ and for the cusps of degree 9 the statement is shown in Step 1 of the proof of [Naj26d, Proposition 8.3].

Let $e = 10$. The point P corresponds to a pair (E, R), where E is an elliptic curve over $\mathbb{F}_{1024}$ and $R \in E(\mathbb{F}_{1024})$ has order 57, and in the dual model $\pi_* P$ lies above $j(E/\langle R\rangle)$, which does not change under $\Delta(57)$. We compute that 60 of the 2053 elliptic curves over $\mathbb{F}_{1024}$, up to isomorphism, have a point of order 57, and that their j-invariants are the roots of 6 irreducible polynomials of degree 10 over $\mathbb{F}_2$, and we compute that 40 of these curves have $E(\mathbb{F}_{1024}) \simeq \mathbb{Z}/1026\mathbb{Z}$ and 20 have $E(\mathbb{F}_{1024}) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/342\mathbb{Z}$, and that their j-invariants form 4 and 2 Frobenius orbits respectively. On a curve of the first kind the points of order 57 generate one cyclic subgroup, and on a curve of the second kind they generate 4. Hence the non-cuspidal closed points of $X_1(57)_{\mathbb{F}_2}$ of degree 10 form $4 + 2 \cdot 4 = 12$ orbits under $\Delta(57)$. As $\#(E/\langle R\rangle)(\mathbb{F}_{1024}) = \#E(\mathbb{F}_{1024})$ and 57 is squarefree, the curve $E/\langle R\rangle$ also has a point of order 57 over $\mathbb{F}_{1024}$, so $\pi_* P$ is a closed point of degree 10 above a root of one of the 6 polynomials. There are 48 such closed points on $Y_{57,\mathbb{F}_2}$, and we find that the condition $\alpha[\pi_* P - 10\,\overline{c_*}] \in V_0$ holds for 6 of them, which lie above the roots of the 3 polynomials in the statement. The second computation above also gives $j(E/\langle R\rangle)$ for a point (E, R) in each of the 12 orbits, and it is a root of one of these 3 polynomials for 6 of the 12 orbits. So P lies in one of these 6 orbits. □

Lemma 10.4. *Let P be a non-cuspidal closed point of $X_1(57)_{\mathbb{F}_2}$ of degree 10 in one of the 6 orbits of Lemma 10.3. Put $\sigma := \langle 5\rangle$ and $T := T_5 P$. Then the divisor*

$$B := \sigma T - T + P + 4\sigma P - 5\sigma^2 P$$

on $X_1(57)_{\mathbb{F}_2}$ is not principal.

Proof. As the divisor B for $\langle a\rangle P$ is $\langle a\rangle B$, it suffices to show that B is not principal for a representative P of each of the 6 orbits.

For each representative we compute T from the 6 isogenies of degree 5 of the corresponding elliptic curve, carrying the level structure through them, and find that T is the sum of 2 closed points, of degrees 10 and 50, with multiplicity 1. So the positive and the negative part of B have degree 110. As in Step 3 of the proof of [Naj26d, Proposition 8.3], the points σP, $\sigma^2 P$ and the points of T are computed on the moduli model, so the identification of the diamond operators of the moduli model and the canonical model plays no role. We apply Lemma 2.13 with $\mathcal{L} = \mathcal{M} = 2K$ on $X_1(57)_{\mathbb{F}_2}$, which has genus 85, as in [Naj26d, Section 8]. Put $R_i := H^0(X_1(57)_{\mathbb{F}_2}, iK)$. We compute the canonical model from an integral basis of $S_2(\Gamma_1(57))$ and its q-expansions up to q^{1100}, and find $\dim R_1 = 85$, $\dim R_2 = 252$ and $\dim R_4 = 588$, where R_2 and R_4 are spanned by products of the elements of the bases of R_1 and R_2, and the identities between these products are checked beyond the Sturm bounds 480 and 960. We obtain local parameters at the points in the support of B from the deformation $a_6 \mapsto a_6 + t$ of the ordinary curves $y^2 + xy = x^3 + a_2x^2 + a_6$, by lifting the point of order 57 by Hensel's lemma, and the canonical coordinates from the modular units of [DvH14, Sections 2 and 2.1] (see `continuation_20261030b/C57/cont57_good10_1.m`). For each of the 6 representatives we compute that the vanishing conditions at the positive and at the negative part of B both have rank 110, that multiplication by the chosen section $F \in R_2$ has rank 252, and that the map of Lemma 2.13 has rank 252, so it is injective and $\ell(B) = 0$. □

Lemma 10.5. *For $r \in \{2, 5, 7, 11, 13\}$ and $\ell \in \{5, 7, 11, 13\}$ let*

$$\Phi_{r,\ell} := (T_r - a_r)(T_\ell - \langle \ell \rangle - \ell)$$

on the dual model of $X_1(57)$, with a_r as in Lemma 10.1, and let c_* be a rational cusp of $X_1(57)$. Then each $\Phi_{r,\ell}$ annihilates $J_1(57)(\mathbb{Q})$, and the morphism

$$f\colon X_1(57)^{(10)} \to J_1(57)^{20}, \qquad B \mapsto \big(\Phi_{r,\ell}[B - 10c_*]\big)_{r,\ell},$$

is a formal immersion modulo 2 at every effective divisor of degree 10 on $X_1(57)_{\mathbb{F}_2}$ supported on the 18 closed cusps of degree 1 and the 9 closed cusps of degree 2.

Proof. The operator $T_r - a_r$ has finite image on $J_1(57)(\mathbb{Q})$ by Lemma 10.1, and $T_\ell - \langle \ell \rangle - \ell$ annihilates $J_1(57)(\mathbb{Q})_{\mathrm{tors}}$ by Proposition 2.2 b) in the form for the dual model (Section 2.3), so $\Phi_{r,\ell}$ annihilates $J_1(57)(\mathbb{Q})$. The image of the cotangent map of f at an effective cuspidal divisor $\overline{C}$ is the image of the restriction map from the space

$$W := \sum_{r,\ell} \Phi_{r,\ell}^* H^0(X_1(57)_{\mathbb{F}_2}, \Omega^1)$$

to $H^0(\overline{C}, \Omega^1|_{\overline{C}})$, so f is a formal immersion at $\overline{C}$ if this restriction has rank 10. As in Step 2 of the proof of [Naj26d, Proposition 8.3], we compute W modulo 2 from the action of the Hecke operators on an integral basis of q-expansions, and find $\dim W = 82$. We use the q-expansions as local expansions at the rational cusps, and at the cusps of degree 2 we use local parameters obtained from the Tate curve $E(q^{19})$ with the point $\zeta_3 q$, which we check up to order 20. As $\Phi_{r,\ell}$ commutes with $\langle a \rangle$, we have $f(\langle a \rangle B) = \langle a \rangle f(B) + f(10\langle a \rangle c_*)$, so f is a formal immersion at $\overline{C}$ if and only if it is one at $\langle a \rangle \overline{C}$. As 57 is squarefree, $\Delta(57)$, of order 18, acts freely on the cusps [Naj26d, Lemma 7.2], so it acts simply transitively on the 18 rational cusps. So, if $\overline{C}$ contains a rational cusp, we may assume that a rational cusp of maximal multiplicity n_0 in $\overline{C}$ is the reduction of c_*. The other rational cusps then have multiplicity at most $\min(n_0, 5)$, and the cusps of degree 2 at most 5. For $n_0 = 1, \dots, 10$ this gives

$$598417,\ 1165590,\ 455634,\ 124979,\ 29835,\ 6267,\ 1122,\ 162,\ 17,\ 1$$

divisors, and there are $\binom{13}{8} = 1287$ divisors supported on the cusps of degree 2. We check that the restriction of W to each of these 2383311 divisors has rank 10. □

Proposition 10.6. *The group $\mathbb{Z}/57\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let $X = X_1(57)$, let D be the trace divisor of a point of order 57 over a number field of degree 10, and let $\overline{D}$ be its reduction modulo 2. Let π, σ, α and V_0 be as in Lemma 10.2, and let c_* be a rational cusp of Y_{57}. The Galois orbits of cusps of X have degrees $1^{18}, 2^9, 18^2$, and the closed cusps of $X_{\mathbb{F}_2}$ have degrees $1^{18}, 2^9, 9^2, 18$ [Naj26d, Section 9.1]. So the closed cusps of degree 1 and 2 are reductions of Galois orbits of cusps of the same degree, and every effective cuspidal divisor on $X_{\mathbb{F}_2}$ supported on them is the reduction of an effective rational cuspidal divisor. For every effective rational cuspidal divisor C of degree k on X, the classes $\alpha[\pi_* D - 10c_*]$ and $\alpha[\pi_* C - kc_*]$ lie in $\alpha J_{Y_{57}}(\mathbb{Q})$, so their reductions lie in V_0 by Lemma 10.2.

Suppose first that $\overline{D}$ contains a non-cuspidal closed point P, of degree e. By the Hasse bound $e \geq 6$ (see the proof of Lemma 10.3), so, as $2 \cdot 6 > 10$, we have $\overline{D} = P + \overline{C}$, where $\overline{C}$ is cuspidal of degree $10 - e \leq 4$. So $\overline{C}$ is supported on the cusps of degree 1 and 2, and it is the reduction of an effective rational cuspidal divisor C. Hence

$$\alpha[\pi_* P - e\,\overline{c_*}] = \alpha[\pi_* \overline{D} - 10\,\overline{c_*}] - \alpha[\pi_* \overline{C} - (10 - e)\,\overline{c_*}] \in V_0,$$

and by Lemma 10.3 we have $e \in \{6, 8, 10\}$, and if $e = 10$, then P lies in one of the 6 orbits of that lemma. Let c be a rational cusp of X. The class $[\sigma D - D] = (\sigma - 1)[D - 10c] + 10[\sigma c - c]$ is torsion by Lemma 10.1 and by Manin-Drinfeld, so it is annihilated by $A_5 = T_5 - 5\sigma - 1$ (Proposition 2.2 b)). As $A_5 C = 0$ by Proposition 2.2 c), we also have $A_5(\sigma C - C) = \sigma A_5 C - A_5 C = 0$. Reducing modulo 2, we get that

$$A_5(\sigma P - P) = \sigma T - T + P + 4\sigma P - 5\sigma^2 P, \qquad T = T_5 P,$$

is principal on $X_{\mathbb{F}_2}$. If $e = 10$, this contradicts Lemma 10.4. If $e \in \{6, 8\}$, then P is one of the 2 non-cuspidal closed points of $X_{\mathbb{F}_2}$ of degree 6, or lies in the single $\Delta(57)$-orbit of non-cuspidal closed points of degree 8 [Naj26d, Section 9.1 and proof of Proposition 9.6], and it is shown in Step 3 of the proof of [Naj26d, Proposition 8.3] that this divisor is not principal for these points. This computation depends only on P, so we again get a contradiction.

Suppose next that $\overline{D}$ is cuspidal and contains one of the 2 closed cusps c of degree 9. Then $\overline{D} = c + \overline{r}$, where r is a rational cusp, and as above $\alpha[\pi_* c - 9\,\overline{c_*}] \in V_0$, which contradicts Lemma 10.3.

Suppose finally that $\overline{D}$ is supported on the cusps of degree 1 and 2. Then $\overline{D}$ is the reduction of an effective rational cuspidal divisor C of degree 10. Let f be the morphism of Lemma 10.5. As $[D - C] \in J_1(57)(\mathbb{Q})$, we have $f(D) = f(C)$, and D and C have the same reduction $\overline{D}$, at which f is a formal immersion by Lemma 10.5. By [DKSS23, Lemma 4.2] (which is due to Parent [Par99, Lemme 4.13]) we get $D = C$, which is a contradiction, as the support of D contains no cusp. □

10.2. **The group $\mathbb{Z}/65\mathbb{Z}$.** We largely follow the proof of [Naj26d, Proposition 8.4], which excludes $\mathbb{Z}/65\mathbb{Z}$ over nonic fields. The following lemma collects the facts about a quotient of genus 9 which we use for a reduction containing a cusp of degree 6. All of them are shown in the proof of [Naj26d, Proposition 8.4].

Lemma 10.7. *Let Y_{65} be the quotient of $X_1(65)$ by the kernel of the character $\langle u \rangle \mapsto \left(\frac{65}{u}\right)$ of $\Delta(65)$, let $\pi\colon X_1(65) \to Y_{65}$ be the quotient map, put $\alpha := \langle 3 \rangle - 1$, and let c_* be a rational*

cusp of Y_{65}. Then Y_{65} has genus 9 and good reduction at 2, and $J_{Y_{65}}(\mathbb{F}_2) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/336\mathbb{Z}$. For each of the 4 closed cusps c of degree 6 of $X_1(65)_{\mathbb{F}_2}$ we have $\pi_* c = 6c_Y$ for a closed cusp c_Y of $Y_{65,\mathbb{F}_2}$ of degree 1, and the class $6\alpha[c_Y - \overline{c_*}]$ is not annihilated by $T_3 - \langle 3\rangle - 3$, the annihilator of the dual model.

Proof. The genus and the remaining statements are shown in the proof of [Naj26d, Proposition 8.4], and Y_{65} has good reduction at 2 by Lemma 2.1. There the classes are normalized at a fixed rational cusp. For another rational cusp c'_* the class $\alpha[c_* - c'_*]$ lies in $\alpha J_{Y_{65}}(\mathbb{Q})$, which is finite by Lemma 10.1, so it is annihilated by $T_3 - \langle 3\rangle - 3$ (Proposition 2.2 b) and Section 2.3), and the last statement does not depend on the choice of c_*. □

Lemma 10.8. *Let P be a non-cuspidal closed point of $X_1(65)_{\mathbb{F}_2}$ of degree 10. Put $\sigma := \langle 3\rangle^{-1}$, $\tau := \langle 3\rangle$ and $T := T_3 P$. Then the divisor*

$$B := \sigma T - T - \sigma P - 2P + 3\tau P$$

on $X_1(65)_{\mathbb{F}_2}$ is not principal.

Proof. We compute that 45 of the 2053 elliptic curves over $\mathbb{F}_{1024}$, up to isomorphism, have a point of order 65, all with $E(\mathbb{F}_{1024}) \simeq \mathbb{Z}/1040\mathbb{Z}$, and that they give 108 non-cuspidal closed points of $X_1(65)_{\mathbb{F}_2}$ of degree 10, which form 5 orbits under $\Delta(65)$, of lengths 24, 24, 24, 12 and 24. (Each closed point in the orbit of length 12 is mapped to itself by a diamond operator of order 2, which permutes its geometric points as a power of the Frobenius.) As the divisor B for $\langle a\rangle P$ is $\langle a\rangle B$, it suffices to treat a representative P of each orbit.

For each representative we compute T from the 4 isogenies of degree 3 of the corresponding elliptic curve, and find that T is the sum of 2 closed points of degree 20 with multiplicity 1. So the positive and the negative part of B have degree 70. As in the proof of [Naj26d, Proposition 8.4], we compute $X_1(65)$, of genus 121, through its canonical forms and the modular units of [DvH14, Sections 2 and 2.1], and apply Lemma 2.13 with $\mathcal{L} = \mathcal{M} = K$. The space $H^0(X_1(65)_{\mathbb{F}_2}, 2K)$ has dimension 360 and is spanned by the products of the canonical forms, which we check beyond the Sturm bound 672. We obtain local parameters from the deformation $a_6 \mapsto a_6 + t$ of the ordinary curves $y^2 + xy = x^3 + a_2 x^2 + a_6$ by lifting the point of order 65 by Hensel's lemma. As the identification of the diamond operators of the moduli model with those of the canonical model is a matter of convention (Section 2.3), we test, as in [Naj26d, Section 8], both B and the divisor $\sigma T - T + 2P + \tau P - 3\sigma P$ obtained from the annihilator of the dual model, for each of the 24 simultaneous diamond translates of the points of T. For each of these $5 \cdot 24 \cdot 2 = 240$ divisors we check that the map of Lemma 2.13, a 121×309 matrix, has rank 121, so it is injective and the divisor is not principal. □

Lemma 10.9. *For $r \in \{2, 3, 7, 11, 17\}$ and $\ell \in \{3, 7, 11, 17\}$ let*

$$\Phi_{r,\ell} := (T_r - a_r)(T_\ell - \langle \ell\rangle - \ell)$$

on the dual model of $X_1(65)$, with a_r as in Lemma 10.1, and let c_* be a rational cusp of $X_1(65)$. Then each $\Phi_{r,\ell}$ annihilates $J_1(65)(\mathbb{Q})$, and the morphism

$$f\colon X_1(65)^{(10)} \to J_1(65)^{20}, \qquad B \mapsto \big(\Phi_{r,\ell}[B - 10c_*]\big)_{r,\ell},$$

is a formal immersion modulo 2 at every effective divisor of degree 10 on $X_1(65)_{\mathbb{F}_2}$ supported on the 24 closed cusps of degree 1 and the 6 closed cusps of degree 4.

Proof. This is proved in the same way as Lemma 10.5. The space

$$W := \sum_{r,\ell} \Phi_{r,\ell}^* H^0(X_1(65)_{\mathbb{F}_2}, \Omega^1)$$

has dimension 106, and at the cusps of degree 4 we use local parameters obtained from the Tate curve $E(q^{13})$ with the point $\zeta_5 q$ and its diamond translates. As $4 \nmid 10$, every effective divisor of degree 10 supported on these cusps contains a rational cusp. As 65 is squarefree, $\Delta(65)$, of order 24, acts freely on the cusps [Naj26d, Lemma 7.2], so it acts simply transitively on the 24 rational cusps, and we may assume that a rational cusp of maximal multiplicity n_0 is the reduction of c_*. The other rational cusps then have multiplicity at most $\min(n_0, 5)$, and the cusps of degree 4 at most 2. For $n_0 = 1, \dots, 10$ this gives

$$1019567,\ 4152510,\ 1521680,\ 377867,\ 80868,\ 14956,\ 2300,\ 276,\ 23,\ 1$$

divisors, 7170048 in total, and we check that the restriction of W to each of them has rank 10 (see also `computations/contc65_cusp_FI_common.py`). □

Proposition 10.10. *The group $\mathbb{Z}/65\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let $X = X_1(65)$, let D be the trace divisor of a point of order 65 over a number field of degree 10, and let $\overline{D}$ be its reduction modulo 2. The Galois orbits of cusps of X have degrees $1^{24}, 4^6, 12^2, 24$, and the closed cusps of $X_{\mathbb{F}_2}$ have degrees $1^{24}, 4^6, 6^4, 12^2$ [Naj26d, Section 9.1]. So the closed cusps of degree 1 and 4 are reductions of Galois orbits of cusps of the same degree, and every effective cuspidal divisor on $X_{\mathbb{F}_2}$ supported on them is the reduction of an effective rational cuspidal divisor. By the Hasse bound and [Naj26d, proof of Proposition 8.4], the non-cuspidal closed points of $X_{\mathbb{F}_2}$ of degree at most 9 have degrees 6, 7, 8 and 9.

Suppose first that $\overline{D}$ contains a non-cuspidal closed point P, of degree e. Then $e \geq 6$, and as $2 \cdot 6 > 10$ we have $\overline{D} = P + \overline{C}$, where $\overline{C}$ is cuspidal of degree $10 - e \leq 4$, so $\overline{C}$ is the reduction of an effective rational cuspidal divisor C. Put $\sigma = \langle 3 \rangle^{-1}$, $\tau = \langle 3 \rangle$ and $A_3 = T_3 - 1 - 3\tau$. As in the proof of Proposition 10.6, the class $[\sigma D - D]$ is torsion by Lemma 10.1 and by Manin-Drinfeld, so it is annihilated by A_3, and $A_3(\sigma C - C) = 0$. Reducing modulo 2, we get that

$$A_3(\sigma P - P) = \sigma T - T - \sigma P - 2P + 3\tau P, \qquad T = T_3 P,$$

is principal on $X_{\mathbb{F}_2}$. For $e = 10$ this contradicts Lemma 10.8. For $e \leq 9$ it is shown in the proof of [Naj26d, Proposition 8.4], for a representative P of each $\Delta(65)$-orbit and hence for all P, that this divisor is not principal (for $e = 6$ it is shown for $A_3(\tau P - P) = -\tau A_3(\sigma P - P)$). This computation depends only on P, so we again get a contradiction.

Suppose next that $\overline{D}$ is cuspidal and contains one of the 4 closed cusps c of degree 6. Then $\overline{D} = c + \overline{C}$, where $\overline{C}$ has degree 4 and is the reduction of an effective rational cuspidal divisor C. Let π, α, c_* and c_Y be as in Lemma 10.7. The classes $\alpha[\pi_* D - 10c_*]$ and $\alpha[\pi_* C - 4c_*]$ lie in $\alpha J_{Y_{65}}(\mathbb{Q})$, which is finite by Lemma 10.1, so they are annihilated by $T_3 - \langle 3 \rangle - 3$ (Proposition 2.2 b) and Section 2.3). The reduction of their difference is $\alpha[\pi_* c - 6\,\overline{c_*}] = 6\alpha[c_Y - \overline{c_*}]$, which is then also annihilated by $T_3 - \langle 3 \rangle - 3$, and this contradicts Lemma 10.7.

Suppose finally that $\overline{D}$ is cuspidal and does not contain a cusp of degree 6. As it has degree 10, it is supported on the cusps of degree 1 and 4, so it is the reduction of an effective rational cuspidal divisor C. As in the proof of Proposition 10.6, the morphism f

of Lemma 10.9 satisfies $f(D) = f(C)$, and it is a formal immersion at $\overline{D}$, so $D = C$ by [DKSS23, Lemma 4.2], which is a contradiction. □

10.3. **The group $\mathbb{Z}/63\mathbb{Z}$.** We work on the quotient Y_{63} of [Naj26d, Lemma 7.8], as in [Naj26d, Proposition 7.12]. In degree 10 the cuspidal part of a reduction can contain a closed cusp of degree 3 which is not the reduction of a rational cuspidal divisor, and we treat it separately.

Lemma 10.11. *Let $Y_{63} := X_1(63)/\langle 8\rangle$ and let $\pi\colon X_1(63) \to Y_{63}$ be the quotient map.*

a) *The diamond operator $\langle 8\rangle$ has order 2 and acts freely on $X_1(63)$, also in characteristic 2, the curve Y_{63} has genus 49 and good reduction at 2, and $J_{Y_{63}}(\mathbb{Q})$ is finite.*
b) *The Galois orbits of cusps of Y_{63} have degrees $1^9, 2^3, 3^6, 6, 9$, and the closed cusps of $Y_{63,\mathbb{F}_2}$ have degrees $1^9, 2^3, 3^9, 6$. The closed cusps of degree 1 and 2, and 6 of the closed cusps of degree 3, are reductions of Galois orbits of cusps of the same degree. The other 3 closed cusps of degree 3, which we denote by C_1, C_2 and C_3, are the closed cusps of degree 3 at which j has a simple pole, and σ_5 acts on them as $\langle 5\rangle$.*
c) *Let P be a non-cuspidal closed point of $X_1(63)_{\mathbb{F}_2}$ of degree $e \leq 10$. Then $e \in \{7, 8, 9, 10\}$, and $\pi_* P$ is a closed point of $Y_{63,\mathbb{F}_2}$ of degree e. For $e = 7, 8, 9, 10$ these closed points of $Y_{63,\mathbb{F}_2}$ are 27, 27, 36 and 27 points, which form 3, 3, 4 and 3 orbits under the diamond operators $\langle 2\rangle$ and $\langle 5\rangle$.*

Proof. Part a) is [Naj26d, Lemma 7.8]. We compute the degrees in b) from the description of the cusps of $X_1(63)$, and we check there that the closed cusps of degree at most 2 are reductions of Galois orbits of cusps of the same degree (see also [Naj26d, proof of Proposition 7.12]). Comparing the two lists of degrees, each Galois orbit of degree 3 reduces to a closed cusp of degree 3, and the orbit of degree 9 splits into the other 3 closed cusps of degree 3. The cusps of $X_1(63)$ at which j has a simple pole are the 18 cusps $(\mathrm{Tate}(q), \zeta)$, with ζ a primitive 63-rd root of unity taken up to sign. As $\langle 8\rangle$ acts freely, their images are the cusps of Y_{63} at which j has a simple pole, and they form the Galois orbit of degree 9. Both σ_5 and $\langle 5\rangle$ map $(\mathrm{Tate}(q), \zeta)$ to $(\mathrm{Tate}(q), \zeta^5)$, so they act in the same way on these cusps.

For $e \leq 9$ part c) is shown in the proof of [Naj26d, Proposition 7.12], where it is also shown that there are no such points of degree at most 6. Let $e = 10$. The function field of Y_{63} is obtained by adjoining to the function field $\mathbb{Q}(t)$ of $X_1(9)$ a root u of the 7-division polynomial of the universal elliptic curve E_t with a point of order 9 in Tate normal form [Naj26d, Lemma 7.8]. We enumerate the pairs (t, u) over $\mathbb{F}_{1024}$ for which E_t is an elliptic curve with $63 \mid \#E_t(\mathbb{F}_{1024})$ and u is the x-coordinate of a point of order 7 of $E_t(\mathbb{F}_{1024})$, which give the images on Y_{63} of all the non-cuspidal points of $X_1(63)$ over $\mathbb{F}_{1024}$. There are 270 of them, and they form 27 Frobenius orbits of length 10, which form 3 orbits under $\langle 2\rangle$ and $\langle 5\rangle$. □

Lemma 10.12. *Let Y_{63} and C_1, C_2, C_3 be as in Lemma 10.11, and put $A_5 := T_5 - 1 - 5\langle 5\rangle$ on Y_{63}.*

a) *For every non-cuspidal closed point P of $Y_{63,\mathbb{F}_2}$ of degree 10 as in Lemma 10.11 c), the divisor $A_5 P$ is not principal.*
b) *For every non-cuspidal closed point P of $Y_{63,\mathbb{F}_2}$ of degree 7 as in Lemma 10.11 c), and all $i \neq j$ in $\{1, 2, 3\}$, the divisor $A_5 P + 4(C_i - C_j)$ is not principal.*

Proof. The diamond operators commute with A_5 and permute C_1, C_2 and C_3, so it suffices to consider a representative P of each of the 3 orbits in each degree, together with all the

ordered pairs (i,j). We use the model of $Y_{63,\mathbb{F}_2}$ described in the proof of Lemma 10.11, and compute T_5P from the 6 isogenies of degree 5 of the corresponding elliptic curve, carrying the points of order 9 and 7 through them. For P of degree 10, T_5P is the sum of 2 closed points of degree 30, and we compute that $\ell(A_5P)=0$ for the 3 representatives. For P of degree 7, T_5P is a closed point of degree 42, and we compute that $\ell(A_5P+4(C_i-C_j))=0$ in all the $3\cdot 6=18$ cases. □

Lemma 10.13. *Let Y_{63} be as in Lemma 10.11, and put $U:=(\mathcal{C}-1)H^0(Y_{63,\mathbb{F}_2},\Omega^1)$. Then $\dim U=45$, and the restriction map $U\to H^0(\overline{C},\Omega^1|_{\overline{C}})$ is surjective for every effective cuspidal divisor $\overline{C}$ of degree 10 on $Y_{63,\mathbb{F}_2}$.*

Proof. The dimension of U is computed in the proof of [Naj26d, Proposition 7.12]. By Lemma 10.11 b) there are $[x^{10}](1-x)^{-9}(1-x^2)^{-3}(1-x^3)^{-9}(1-x^6)^{-1}=239238$ effective cuspidal divisors of degree 10 on $Y_{63,\mathbb{F}_2}$. For a closed cusp c and $m\deg c\le 9$ we use the subspaces $\Omega(mc)$ from the computation for degree 9 in the proof of [Naj26d, Proposition 7.12], and we compute the subspaces $\Omega(10c)$ for the 9 cusps c of degree 1 and $\Omega(5c)$ for the 3 cusps c of degree 2. Using these, we check that $\dim U-\dim\big(U\cap\Omega(\overline{C})\big)=10$ for each of the 239238 divisors $\overline{C}$. □

Proposition 10.14. *The group $\mathbb{Z}/63\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let D be the trace divisor of a point of order 63 over a number field of degree 10, let π, C_1, C_2 and C_3 be as in Lemma 10.11, and let c_* be a rational cusp of Y_{63}. As $J_{Y_{63}}(\mathbb{Q})$ is finite, the operator $A_5=T_5-1-5\langle 5\rangle$ annihilates it (Proposition 2.2 b)), and $A_5c_*=0$ (Proposition 2.2 c)), so $A_5\pi_*D$ is principal, as its class is $A_5[\pi_*D-10c_*]=0$.

Suppose first that the reduction of D modulo 2 is not entirely cuspidal. By Lemma 10.11 c) its non-cuspidal part is a single closed point of degree $e\in\{7,8,9,10\}$, with multiplicity 1 as $2\cdot 7>10$, and the reduction of π_*D is $P+\overline{C}$, where P is one of the closed points of $Y_{63,\mathbb{F}_2}$ of degree e of Lemma 10.11 c) and $\overline{C}$ is cuspidal of degree $10-e\le 3$. If $\overline{C}$ is the reduction of an effective rational cuspidal divisor C, then $A_5C=0$ by Proposition 2.2 c), so A_5P is principal. For $e=10$ this contradicts Lemma 10.12 a), and for $e\le 9$ it is shown in the proof of [Naj26d, Proposition 7.12] that A_5P is not principal for a representative P of each orbit, and hence for all of them. Otherwise, by Lemma 10.11 b), $e=7$ and $\overline{C}=C_i$ for some i. By Lemma 2.3, as σ_5 acts on C_i as $\langle 5\rangle$, we have

$$A_5C_i=\sigma_5C_i-C_i+5\langle 5\rangle\big(\langle 5\rangle^{-1}C_i-C_i\big)=4(C_i-\sigma_5C_i),$$

and $\sigma_5C_i=C_j$ for some j. If $j=i$, then A_5P is principal, which we have just excluded. If $j\neq i$, then $A_5P+4(C_i-C_j)$ is principal, which contradicts Lemma 10.12 b).

So the reduction of π_*D is entirely cuspidal. By Lemma 10.11 a) the curve Y_{63} satisfies the assumptions of Proposition 2.18, and $J_{Y_{63}}(\mathbb{Q})$ is finite, so we may take $r=1$ and $\psi_1=1$. By Lemma 10.13 the restriction of U to the reduction of π_*D is surjective, and Proposition 2.18 gives a contradiction, as π_*D is an effective rational divisor of degree 10 with non-cuspidal support. □

10.4. **The group $\mathbb{Z}/81\mathbb{Z}$.** In degrees 6, 7, 8 and 9 the group $\mathbb{Z}/81\mathbb{Z}$ is excluded in [Naj26d, Proposition 4.8] by showing that $T_2D=D+2\langle 2\rangle D$ for the trace divisor D, which follows from $T_2D\sim D+2\langle 2\rangle D$ as both sides have degree $3d<\operatorname{gon}_{\mathbb{C}}X_1(81)$. In degree 10 both sides have degree 30, and we replace the gonality bound by a Riemann-Roch computation over $\mathbb{F}_2$ on a quotient of $X_1(81)$ of genus 46, after excluding some of the reductions with $X_0(81)$.

Lemma 10.15. *Let $Y_{81} := X_1(81)/\langle 28\rangle$, where $\langle 28\rangle$ has order 3. Then Y_{81} has good reduction at 2. The groups $J_1(81)(\mathbb{Q})$, $J_0(81)(\mathbb{Q})$ and $J_{Y_{81}}(\mathbb{Q})$ are finite and have no non-trivial 2-torsion, reduction modulo 2 is injective on each of them, and $A_2 := T_2 - 1 - 2\langle 2\rangle$ annihilates $J_{Y_{81}}(\mathbb{Q})$.*

Proof. The curve Y_{81} has good reduction at 2 by Lemma 2.1. The group $J_1(81)(\mathbb{Q})$ is finite by [DEvH+21, Theorem 3.1(2)], and $J_1(81)(\mathbb{Q})[2] = 0$ by [Naj26d, proof of Proposition 4.8]. Let ρ be one of the natural maps $X_1(81) \to X_0(81)$ and $X_1(81) \to Y_{81}$, of degrees 27 and 3. As $\rho_*\rho^*$ is multiplication by the odd integer $\deg \rho$ on the Jacobian of the target, the kernel of ρ^* on its rational points is finite of odd order, so the Jacobian of the target has finitely many rational points and no non-trivial rational 2-torsion. By Parent's result (Section 2.3) the kernel of reduction modulo 2 on these finite groups has exponent at most 2, so it is trivial. By the Eichler-Shimura relation [DI95, (10.2.3)] at 2 we have $T_2 = F + \langle 2\rangle V$ on the special fibre of the Néron model of $J_{Y_{81}}$ at 2, and on $J_{Y_{81}}(\mathbb{F}_2)$ the Frobenius F is the identity, so $V = VF = 2$. Hence A_2 annihilates $J_{Y_{81}}(\mathbb{F}_2)$, and as reduction is injective on $J_{Y_{81}}(\mathbb{Q})$ and commutes with T_2 and $\langle 2\rangle$, it annihilates $J_{Y_{81}}(\mathbb{Q})$, as in [Naj26d, proof of Proposition 4.8]. □

Lemma 10.16. *The non-cuspidal closed points of $X_1(81)_{\mathbb{F}_2}$ of degree at most 10 are 135 points of degree 9 and 135 points of degree 10, and the points of each degree form 5 orbits under $\Delta(81)$. Every Galois orbit of cusps of $X_1(81)$ reduces to a single closed cusp of $X_1(81)_{\mathbb{F}_2}$ of the same degree.*

Proof. We compute that no elliptic curve over $\mathbb{F}_{2^e}$ with $e \le 8$ has a point of order 81, that over $\mathbb{F}_{512}$ there are 45 such curves, up to isomorphism, all with $E(\mathbb{F}_{512}) \simeq \mathbb{Z}/486\mathbb{Z}$, and that over $\mathbb{F}_{1024}$ there are 30, of which 20 have $E(\mathbb{F}_{1024}) \simeq \mathbb{Z}/972\mathbb{Z}$ and 10 have $E(\mathbb{F}_{1024}) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/324\mathbb{Z}$. Their points of order 81 give the closed points and the orbits in the statement. The cusps are defined over $\mathbb{Q}(\zeta_{81})$ and the cuspidal subscheme is finite étale over $\mathbb{Z}[\frac{1}{81}]$. As 2 generates $(\mathbb{Z}/81\mathbb{Z})^\times$, the Frobenius at 2 generates $\mathrm{Gal}(\mathbb{Q}(\zeta_{81})/\mathbb{Q})$, so every Galois orbit of cusps reduces to a single closed cusp. □

Lemma 10.17. *Let $\pi_0 \colon X_1(81) \to X_0(81)$ be the natural map, let c_* be a rational cusp of $X_0(81)$, and let G be the subgroup of odd order of $J_0(81)(\mathbb{F}_2)$. Then $J_0(81)(\mathbb{F}_2) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$, and for every non-cuspidal closed point P of $X_1(81)_{\mathbb{F}_2}$ of degree $e \le 10$, the push-forward $\pi_{0*}P$ is a closed point of degree e. For P in 2 of the 5 orbits of Lemma 10.16 of degree 9, and in 3 of the 5 orbits of degree 10, we have $[\pi_{0*}P - e\,\overline{c_*}] \notin G$.*

Proof. The diamond operators act trivially on $X_0(81)$, so $\pi_{0*}P$ depends only on the orbit of P. We compute $J_0(81)(\mathbb{F}_2)$ with Magma's proven class group algorithm on a model of $X_0(81)_{\mathbb{F}_2}$, which has genus 4. For a representative P of each of the 10 orbits we compute $\pi_{0*}P$ from the j-invariants of the corresponding elliptic curve and of its quotient by the cyclic subgroup of order 81, find that it is a closed point of degree e, and compute its class. □

To exclude the remaining reductions we use the following model of Y_{81}. Let (E_{27}, R) be the universal elliptic curve over $X_1(27)$ with a point R of order 27, in Tate normal form, put $S := 9R$, which has order 3, and let $\phi \colon E_{27} \to E_{27}/\langle S\rangle$ be the quotient map and $\widehat{\phi}$ its dual. For a point P of order 81, let ϕ_P be the quotient by $\langle 27P\rangle$. The map $(E, P) \mapsto (E, 3P, \phi_P(P))$ is invariant under $P \mapsto 28P$, as $\phi_P(27P) = 0$, and $\widehat{\phi_P}(\phi_P(P)) = 3P$. So Y_{81} parametrizes the points V of $E_{27}/\langle S\rangle$ with $\widehat{\phi}(V) = R$, and its function field is obtained from that of $X_1(27)$ by adjoining $x(V)$, which is a root of a cubic polynomial.

Lemma 10.18. *Let (E_{27}, R), S and V be as above, let m be the slope of the tangent line to E_{27} at S, and put*

$$f := \big(y(R) - y(S)\big) - m\big(x(R) - x(S)\big).$$

Then the function field of $Y_{81,\mathbb{F}_4}$ is the extension of the function field of $X_1(27)_{\mathbb{F}_4}$ generated by a root w of $w^3 = f$, and $x(V) = a + Aw + Bw^2$ for functions a, A, B on $X_1(27)_{\mathbb{F}_4}$. The map $Y_{81,\mathbb{F}_4} \to X_1(27)_{\mathbb{F}_4}$ is ramified at 9 points and at no other point. These 9 points are the images of the closed cusps of $X_1(81)_{\mathbb{F}_2}$ of degree 1, and Y_{81} has genus 46.

Proof. We compute a model of $X_1(27)_{\mathbb{F}_4}$, which has genus 13, the cubic polynomial of $x(V)$, which is irreducible, and functions a, A, B such that $a + Aw + Bw^2$ is a root of it. The function f has valuation 2 modulo 3 at 9 places, which are cusps, and valuation divisible by 3 at all the other places, so the extension is ramified at these 9 places, and the Riemann-Hurwitz formula gives $g(Y_{81}) = 1 + 3 \cdot 12 + 9 = 46$. By Lemma 10.16, the closed cusps of $X_1(81)_{\mathbb{F}_2}$ of degree 1 are the reductions of the 27 rational cusps $(\mathrm{Tate}(q), q^{b/81})$, with $b \in (\mathbb{Z}/81\mathbb{Z})^\times/\{\pm 1\}$. At these cusps j has a pole of order 81, and at their images $(\mathrm{Tate}(q), q^{b/27})$ on $X_1(27)$ a pole of order 27, so the map $X_1(81) \to X_1(27)$ has ramification index 3 at them. As $\langle 28\rangle$ maps the cusp with label b to the one with label $28b \not\equiv \pm b \pmod{81}$, the map $X_1(81) \to Y_{81}$ is unramified at them, so $Y_{81} \to X_1(27)$ is ramified at their images, which are therefore the 9 ramified cusps. □

Lemma 10.19. *Let $\pi\colon X_1(81) \to Y_{81}$ be the quotient map and $\delta := \langle 2\rangle$. Let P be a non-cuspidal closed point of $X_1(81)_{\mathbb{F}_2}$ of degree $e \in \{9, 10\}$ in one of the 5 orbits of Lemma 10.16 which are not excluded in Lemma 10.17. If $e = 9$, let c be a closed cusp of $X_1(81)_{\mathbb{F}_2}$ of degree 1, and if $e = 10$, put $c = 0$. Then $L := \pi_*(P + c)$ satisfies*

$$\ell(L + 2\delta L) = 1$$

on $Y_{81,\mathbb{F}_2}$.

Proof. For $a \in (\mathbb{Z}/81\mathbb{Z})^\times$ we have $\pi_*(\langle a\rangle P + c) = \langle a\rangle \pi_*(P + \langle a\rangle^{-1} c)$, so it suffices to consider a representative P of each of the 5 orbits, 3 of degree 9 and 2 of degree 10. By Lemma 10.18 there are 9 possibilities for $\pi_* c$ if $e = 9$, so there are $3 \cdot 9 + 2 = 29$ cases. As ℓ does not change under base change, we compute $\ell(L + 2\delta L)$ on $Y_{81,\mathbb{F}_4}$, with the model of Lemma 10.18. Let M be the push-forward of $\pi_* P + 2\delta \pi_* P$ to $X_1(27)_{\mathbb{F}_4}$, and let L' be the space of the functions on $Y_{81,\mathbb{F}_4}$ whose poles are bounded by $L + 2\delta L$ at the cusps and by the pull-back of M at the other points. Under the automorphisms $w \mapsto \zeta w$, with $\zeta^3 = 1$, of $Y_{81,\mathbb{F}_4}$ over $X_1(27)_{\mathbb{F}_4}$, the space L' decomposes as $\bigoplus_{k=0}^{2} V_k\, w^k$, where V_k is a Riemann-Roch space on $X_1(27)_{\mathbb{F}_4}$ determined by M, by the poles allowed at the cusps and by the valuations of f. Above every point p in the support of M only one of the 3 points of $Y_{81,\mathbb{F}_4}$ occurs in $L + 2\delta L$, and $L(L + 2\delta L)$ is the subspace of L' of the functions without poles at the other 2 points. We determine the point which occurs by the formula for $x(V)$ and a computation of the isogenies of degree 3 of the corresponding elliptic curve. We compute that V_0, V_1 and V_2 have dimensions 15, 11 and 13 in the 27 cases with $e = 9$, and 18, 12 and 15 in the 2 cases with $e = 10$, and that the conditions at the other points have rank 38 and 44 respectively. Hence $\ell(L + 2\delta L) = 39 - 38 = 45 - 44 = 1$. □

Proposition 10.20. *The group $\mathbb{Z}/81\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let D be the trace divisor of a point of order 81 over a number field of degree 10, and let $\overline{D}$ be its reduction modulo 2. The group $J_1(81)(\mathbb{Q})$ is finite by Lemma 10.15, and

$\operatorname{gon}_{\mathbb{C}} X_1(81) \geq \frac{325}{2^{15}} \cdot 2916 > 28.92 > 20$, as $i(81) = 2916$. So $\overline{D}$ is not entirely cuspidal by Proposition 2.5 b). By Lemma 10.16, as $2 \cdot 9 > 10$, we have $\overline{D} = P + \bar{c}$, where P is a non-cuspidal closed point of degree $e \in \{9, 10\}$, and c is a rational cusp if $e = 9$, while $c = 0$ if $e = 10$.

Let π_0, c_* and G be as in Lemma 10.17. The class $[\pi_{0*}D - 10c_*]$ lies in $J_0(81)(\mathbb{Q})$, and so does $[\pi_{0*}c - c_*]$ if $e = 9$. As $J_0(81)(\mathbb{Q})$ is finite of odd order by Lemma 10.15, the reductions of these classes lie in G, and hence $[\pi_{0*}P - e\,\overline{c_*}] \in G$. By Lemma 10.17, P lies in one of the 5 orbits of Lemma 10.19.

Let π and δ be as in Lemma 10.19, and let y_* be a rational cusp of Y_{81}. By Lemma 2.3 with $q = 2$ we have $T_2 y_* = y_* + 2\delta y_*$, so $A_2 y_* = 0$, and as A_2 annihilates $J_{Y_{81}}(\mathbb{Q})$ by Lemma 10.15, we get $[A_2\pi_*D] = A_2[\pi_*D - 10y_*] = 0$, so

$$T_2\pi_*D \sim \pi_*D + 2\delta\pi_*D.$$

Both sides are effective of degree 30. The divisor $\pi_*D + 2\delta\pi_*D$ extends to an effective relative divisor on the smooth model of Y_{81} over $\mathbb{Z}_{(2)}$, whose special fibre is $L + 2\delta L$ with $L = \pi_*(P+\bar{c})$, so by the semicontinuity theorem [Har77, Theorem III.12.8] and Lemma 10.19, $\ell(\pi_*D+2\delta\pi_*D) \leq 1$. Hence $\pi_*D+2\delta\pi_*D$ is the only effective divisor in its linear equivalence class, and $T_2\pi_*D = \pi_*D + 2\delta\pi_*D$.

So the finite non-empty set of j-invariants of the points in the support of π_*D is closed under cyclic isogenies of degree 2, as T_2 maps a point to the sum of the points obtained from its 3 isogenies of degree 2, and δ does not change the j-invariant. But for $E_\tau = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ the map $E_\tau \to E_{2\tau}$, $z \mapsto 2z$, is a cyclic isogeny of degree 2, and $j(2^k\tau) = q^{-2^k} + 744 + O(q^{2^k})$, with $q = e^{2\pi i\tau}$, is unbounded as $k \to \infty$, which is a contradiction. □

10.5. **The group $\mathbb{Z}/87\mathbb{Z}$.** Over nonic fields the group $\mathbb{Z}/87\mathbb{Z}$ is excluded in [Naj26d, Proposition 8.2] with a quotient of $X_1(87)$ of genus 33. In degree 10 we work on $X_0(87)$, which has genus 9. As 87 is squarefree, the 4 cusps of $X_0(87)$ are rational.

Lemma 10.21. *Let $\pi_0 \colon X_1(87) \to X_0(87)$ be the natural map, and let P be a non-cuspidal closed point of $X_1(87)_{\mathbb{F}_2}$ of degree $e \leq 10$. Then $e \in \{9, 10\}$ and $\pi_{0*}P$ is a closed point of $X_0(87)_{\mathbb{F}_2}$ of degree e. These closed points of $X_0(87)_{\mathbb{F}_2}$ are 4 points of degree 9 and 8 points of degree 10.*

Proof. No elliptic curve over $\mathbb{F}_{2^e}$ with $e \leq 8$ has a point of order 87 [Naj26d, proof of Proposition 8.2]. We compute that over $\mathbb{F}_{512}$ there are 36 elliptic curves with a point of order 87, up to isomorphism, all with $E(\mathbb{F}_{512}) \simeq \mathbb{Z}/522\mathbb{Z}$, and that over $\mathbb{F}_{1024}$ there are 50, of which 40 have $E(\mathbb{F}_{1024}) \simeq \mathbb{Z}/1044\mathbb{Z}$ and 10 have $E(\mathbb{F}_{1024}) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/348\mathbb{Z}$. The subgroup of order 29 is unique, and on the curves of the last kind each of the 4 subgroups of order 3 is generated by a rational point. So the points of order 87 generate 36 and $40 + 10 \cdot 4 = 80$ cyclic subgroups of order 87, respectively, and the corresponding points of $X_0(87)$ form 4 Frobenius orbits of length 9 and 8 Frobenius orbits of length 10. □

Lemma 10.22. *Let P be one of the 12 closed points of $X_0(87)_{\mathbb{F}_2}$ of Lemma 10.21, of degree e. Then the divisor $T_5P - 6P$ on $X_0(87)_{\mathbb{F}_2}$ is not principal.*

Proof. We obtain a model of $X_0(87)_{\mathbb{F}_2}$ as the normalization of the fibre product of $X_0(29)_{\mathbb{F}_2}$, which has genus 2, and $X_0(3)_{\mathbb{F}_2}$ over the j-line, by adjoining to the function field of $X_0(29)_{\mathbb{F}_2}$ a root v of $v^4 + v^3 + 1/j = 0$. Here $j = 1/(v^3(v+1))$ is the j-invariant of the curve $y^2 + xy + vy = x^3$, on which $(0, 0)$ has order 3. The point P is determined by the kernel of the isogeny of degree 29 and by the point of order 3 of the corresponding elliptic curve.

We compute T_5P from the 6 cyclic subgroups of order 5, carrying the subgroup of order 87 through the isogenies. For $e = 9$ it is a closed point of degree 54, and for $e = 10$ it is the sum of closed points of degrees 10 and 50, with multiplicity 1. We then compute that $\ell(T_5P - 6P) = 0$ for all the 12 points P. □

Proposition 10.23. *The group $\mathbb{Z}/87\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let D be the trace divisor of a point of order 87 over a number field of degree 10, and let $\overline{D}$ be its reduction modulo 2. The group $J_1(87)(\mathbb{Q})$ is finite [DEvH+21, Theorem 3.1(2)], and $\operatorname{gon}_{\mathbb{C}} X_1(87) \geq \frac{325}{2^{15}} \cdot 3360 > 33 > 20$, as $i(87) = 3360$. So $\overline{D}$ is not entirely cuspidal by Proposition 2.5 b). By Lemma 10.21, as $2 \cdot 9 > 10$, we have $\overline{D} = P + \overline{C}$, where P is a non-cuspidal closed point of degree $e \in \{9, 10\}$ and $\overline{C}$ is cuspidal of degree $10 - e \leq 1$.

Let π_0 be as in Lemma 10.21. The group $J_0(87)(\mathbb{Q})$ is finite, as $J_0(87)$ is a quotient of $J_1(87)$. As the diamond operators act trivially on $X_0(87)$, we have $A_5 = T_5 - 6$ on $X_0(87)$, which annihilates $J_0(87)(\mathbb{Q})$ by Proposition 2.2 b). As all the cusps of $X_0(87)$ are rational, Lemma 2.3 shows that A_5 annihilates every cuspidal divisor on $X_0(87)$ and on $X_0(87)_{\mathbb{F}_2}$. Hence, for a cusp c_* of $X_0(87)$, the class of $A_5\pi_{0*}D$ is $A_5[\pi_{0*}D - 10c_*] = 0$, and reducing modulo 2 we get that $A_5\pi_{0*}P = T_5\pi_{0*}P - 6\pi_{0*}P$ is principal on $X_0(87)_{\mathbb{F}_2}$. As $\pi_{0*}P$ is one of the 12 points of Lemma 10.21, this contradicts Lemma 10.22. □

10.6. **The group $\mathbb{Z}/69\mathbb{Z}$.** Over number fields of degree 7, 8 and 9 the group $\mathbb{Z}/69\mathbb{Z}$ was excluded in [Naj26d, Proposition 9.9] with the unramified double cover $Y_{69} \to Z_{69} = X_0(69)$ of [Naj26d, Lemma 9.4]. Here $Y_{69} = X_1(69)/H$, where H is the subgroup of order 11 of $\Delta(69)$, and we use the model of $Y_{69,\mathbb{F}_2}$ constructed in [Naj26d, Section 9.2]. In degree 10 the reduction of the trace divisor modulo 2 can also be a closed point of degree 10, and for one of the two diamond orbits of such points the double cover does not suffice. For this orbit we use the following quotient of $X_1(69)$ of degree 2, on which the images of a point and of its Hecke translates can be computed from the moduli interpretation.

Lemma 10.24. *The diamond operator $\langle 22\rangle$ has order 2 in $\Delta(69)$ and fixes no geometric point of $X_1(69)$, in characteristic 0 or 2. The curve $W_{69} := X_1(69)/\langle 22\rangle$ has genus 67 and good reduction at 2, and $J(W_{69})(\mathbb{Q})$ is finite. The curve W_{69} parametrizes triples $(E, \pm P_{23}, C_3)$, where P_{23} is a point of order 23 and C_3 a cyclic subgroup of order 3 of E, and the image of (E, P) is $(E, \pm 3P, \langle 23P\rangle)$. Let F_{23} be the function field of $X_1(23)_{\mathbb{F}_2}$, which has genus 12, let $j \in F_{23}$ be the j-invariant, and let v be the coordinate on $X_0(3)_{\mathbb{F}_2}$ for which the pair (E, C_3) is given by the curve $y^2 + xy + vy = x^3$ and the subgroup generated by $(0, 0)$. Then $j = 1/(v^3(v + 1))$ on $X_0(3)_{\mathbb{F}_2}$, and the function field of $W_{69,\mathbb{F}_2}$ is $F_{23}(v)$, where*

$$v^4 + v^3 + 1/j = 0.$$

Proof. We have $22^2 \equiv 1 \pmod{69}$ and $22 \not\equiv \pm 1 \pmod{69}$, so $\langle 22\rangle$ has order 2. As $22 \equiv 1 \pmod 3$ and $22 \equiv -1 \pmod{23}$, and as $22^2 \equiv 1$, $22^2 + 22 + 1 \equiv 24$ and $22^2 - 22 + 1 \equiv 49$ modulo 69, [Naj26d, Lemma 7.2] shows that $\langle 22\rangle$ fixes no cusp and no non-cuspidal geometric point of $X_1(69)$, in characteristic 0 or 2. Hence $\langle 22\rangle$ acts freely on the smooth model of $X_1(69)$ over $\mathbb{Z}_{(2)}$, the quotient is a smooth model of W_{69} with special fibre $X_1(69)_{\mathbb{F}_2}/\langle 22\rangle$, and as $X_1(69)$ has genus 133, the Riemann-Hurwitz formula $2 \cdot 133 - 2 = 2(2g(W_{69}) - 2)$ gives $g(W_{69}) = 67$. Let $\pi : X_1(69) \to W_{69}$ be the quotient map. As $\pi_*\pi^* = 2$ on $J(W_{69})$ and $J_1(69)(\mathbb{Q})$ is finite [DEvH+21, Theorem 3.1(2)], the group $J(W_{69})(\mathbb{Q})$ is finite.

The operator $\langle 22\rangle$ maps (E,P) to $(E,22P)$, so it fixes $23P$ and maps $3P$ to $-3P$. Hence (E,P) and (E,P') have the same image on W_{69} if and only if $P'=aP$ with $a\equiv\pm1 \pmod 3$ and $a\equiv\pm1 \pmod{23}$, i.e. if and only if $\langle 23P'\rangle=\langle 23P\rangle$ and $3P'=\pm 3P$. This proves the moduli description. Over $\mathbb{F}_2$ the maps $(E,P)\mapsto(E,\pm 3P)$ to $X_1(23)$ and $(E,P)\mapsto(E,\langle 23P\rangle)$ to $X_0(3)$ show that the function field of $W_{69,\mathbb{F}_2}$ contains F_{23} and v, and it has degree 4 over F_{23}, as $X_1(69)\to X_1(23)$ has degree $i(69)/i(23)=2112/264=8$. The curve $y^2+xy+vy=x^3$ over $\mathbb{F}_2(v)$ has the point $(0,0)$ of order 3 and j-invariant $1/(v^3(v+1))$, so v is a root of v^4+v^3+1/j. We compute that this polynomial is irreducible over F_{23}, so $F_{23}(v)$ is the function field of $W_{69,\mathbb{F}_2}$, and we also compute that it has genus 67. □

Lemma 10.25. *Let E be an elliptic curve over a number field of degree 10 with a point of order 69, and let D be the trace divisor on $X_1(69)$ of this point. Then the reduction of D modulo 2 is $G+\overline{C}$, where G is a non-cuspidal closed point of $X_1(69)_{\mathbb{F}_2}$ of degree $e\in\{7,8,9,10\}$ and $\overline{C}$ is the reduction of an effective rational cuspidal divisor C of degree $10-e$. The non-cuspidal closed points of $X_1(69)_{\mathbb{F}_2}$ of degree at most 10 have degrees 7, 8, 9 and 10, and there are 66, 44, 44 and 44 of them.*

Proof. By [DEvH+21, Theorem 3.1(2)] the group $J_1(69)(\mathbb{Q})$ is finite. As $i(69)=2112$, Abramovich's bound gives $\operatorname{gon}_{\mathbb{C}} X_1(69)>20.94$, so $\operatorname{gon}_{\mathbb{Q}} X_1(69)>20$, and by Proposition 2.5 b), applied with $p=2$ and $d=10$, the reduction of D modulo 2 is not entirely cuspidal. The numbers of non-cuspidal closed points of degree at most 9 are computed in the proof of [Naj26d, Proposition 9.9]. We compute that there are 20 elliptic curves over $\mathbb{F}_{1024}$ with a point of order 69, all with cyclic group of order 966. Each of them has $\varphi(69)/2=22$ points of order 69 up to sign, which gives 440 geometric points of $X_1(69)$ over $\mathbb{F}_{1024}$, and as there are no non-cuspidal closed points of degree 1, 2 or 5, these form 44 closed points of degree 10. As $2\cdot 7>10$, the non-cuspidal part of the reduction of D is a single closed point G, with multiplicity 1. The Galois orbits of cusps of $X_1(69)$ over $\mathbb{Q}$ have degrees $1^{22},2^{11},22^2$, and the closed cusps of $X_1(69)_{\mathbb{F}_2}$ have degrees $1^{22},2^{11},11^2,22$ (see the proof of [Naj26d, Proposition 9.9]), so the closed cusps of degree 1 and 2 are reductions of Galois orbits of cusps of the same degree. As the cuspidal part of the reduction has degree $10-e\le 3$, it is the reduction of an effective rational cuspidal divisor. □

Proposition 10.26. *The group $\mathbb{Z}/69\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let D be the trace divisor of a point of order 69 over a number field of degree 10, and let G, e and C be as in Lemma 10.25. Let P and P_Y be the images of G on $Z_{69,\mathbb{F}_2}$ and on $Y_{69,\mathbb{F}_2}$. As in the proof of [Naj26d, Proposition 9.9], the groups $J(Y_{69})(\mathbb{Q})$ and $J(Z_{69})(\mathbb{Q})$ are finite, and as $\langle 5\rangle\in H$, the operator $A_5=T_5-6$ annihilates them (Proposition 2.2) and annihilates the images of the rational cuspidal divisors, such as C, as divisors (Lemma 2.3). So T_5P-6P is principal on $Z_{69,\mathbb{F}_2}$ and $T_5P_Y-6P_Y$ is principal on $Y_{69,\mathbb{F}_2}$. The divisor T_5P_Y is one of the effective divisors on $Y_{69,\mathbb{F}_2}$ whose push-forward to $Z_{69,\mathbb{F}_2}$ is T_5P, which we call the lifts of T_5P. The non-trivial automorphism of Y_{69} over Z_{69} commutes with T_5 and exchanges the two points of $Y_{69,\mathbb{F}_2}$ above P, so we may take P_Y to be a fixed one of them.

Suppose first that $e\le 9$. It is shown in the proof of [Naj26d, Proposition 9.9] that the images of the points G on $Z_{69,\mathbb{F}_2}$ are 3 closed points of degree 7, 2 of degree 8 and 2 of degree 9, that the divisor T_5P-6P is not principal for two of those of degree 7, both of degree 8 and one of degree 9, and that for the remaining point of degree 7 and the remaining one of degree 9 the divisor $T-6P_Y$ is not principal for any of the lifts T of T_5P. These tests depend only on G and not on $\overline{C}$, so they exclude these reductions.

Suppose now that $e = 10$. Then the reduction of D is G. The map $X_1(69) \to Z_{69}$ is the quotient by $\Delta(69)$, and we compute that the 44 closed points of degree 10 lie above 2 closed points P_1 and P_2 of $Z_{69,\mathbb{F}_2}$, both of degree 10, so they form 2 diamond orbits of 22 points each. For both $i = 1, 2$, the divisor $T_5P_i - 6P_i$ is principal, and $T_5P_i = Q_i + Q_i'$, where Q_i and Q_i' are closed points of degree 10 and 50 which both split in Y_{69}. So there are 4 lifts of T_5P_i. For $P = P_1$ the divisor $T - 6P_Y$ is not principal for any of them, so G lies above P_2.

We compute that the j-invariants of the points above P_1 and above P_2 have different minimal polynomials over $\mathbb{F}_2$, that those above P_2 are the roots of

$$j^{10} + j^8 + j^7 + j^6 + j^5 + j^4 + j^3 + j + 1,$$

and that for such a root j_0 there is exactly one elliptic curve E_0 over $\mathbb{F}_{1024}$ with $j(E_0) = j_0$ and a point of order 69, and that $E_0(\mathbb{F}_{1024}) \simeq \mathbb{Z}/966\mathbb{Z}$. Let $P_0 \in E_0(\mathbb{F}_{1024})$ be a point of order 69 and G_0 the closed point of (E_0, P_0), which has degree 10 and hence lies above P_1 or P_2, so it lies above P_2. As the closed points above P_2 form one diamond orbit, $G = \langle a \rangle G_0$ for some $a \in (\mathbb{Z}/69\mathbb{Z})^\times$.

Let $\pi : X_1(69) \to W_{69}$ be the quotient map of Lemma 10.24, let P_W be the image of G_0, and put $A_5 = T_5 - 1 - 5\langle 5 \rangle$ on W_{69}. As $J(W_{69})(\mathbb{Q})$ is finite (Lemma 10.24), $A_5\pi_*D$ is principal (Proposition 2.2), and so is its reduction $A_5\pi_*G = \langle a \rangle A_5\pi_*G_0$. We compute below that P_W has degree 10, so $\pi_*G_0 = P_W$ and A_5P_W is principal. We compute A_5P_W on the model of Lemma 10.24 as follows. The image of $(E_0, \pm 3P_0)$ on $X_1(23)_{\mathbb{F}_2}$ is a closed point of degree 10, at which the reduction of v^4+v^3+1/j is the product of a linear and an irreducible cubic polynomial over $\mathbb{F}_{1024}$. The subgroup $\langle 23P_0 \rangle$ is defined over $\mathbb{F}_{1024}$, so P_W is the unique point of degree 10 of $W_{69,\mathbb{F}_2}$ above this point, and in the same way we obtain $\langle 5 \rangle P_W$ from $(E_0, 5P_0)$. The six subgroups of order 5 of E_0 form two orbits under the Frobenius, of lengths 1 and 5. For a subgroup S in each of them, the image of $(E_0/S, \pm 3P_0 \bmod S)$ on $X_1(23)_{\mathbb{F}_2}$ is a closed point of degree 10, respectively 50, and at both of them the quartic again factors as a linear times an irreducible cubic polynomial over the residue field. So $T_5P_W = Q + Q'$, where Q and Q' are the unique points of $W_{69,\mathbb{F}_2}$ of degree 10 and 50 above these two points. We compute that

$$\ell\big(T_5P_W - P_W - 5\langle 5 \rangle P_W\big) = 0,$$

so A_5P_W is not principal, which is a contradiction. □

10.7. **The curve $X_1(39)$.** Over number fields of degree 10 there is an elliptic curve with a point of order 39, and we show that it is the only one up to isomorphism. This excludes $\mathbb{Z}/78\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/39\mathbb{Z}$ and $\mathbb{Z}/117\mathbb{Z}$, as in [Naj26d, Proposition 13.14] over octic fields.

Let $X = X_1(39)$. By [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], $J_X(\mathbb{Q}) \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/31122\mathbb{Z} \times \mathbb{Z}/3236688\mathbb{Z}$, reduction modulo 2 is injective on $J_X(\mathbb{Q})$ [Naj26d, Lemma 13.12], and $\operatorname{gon}_{\mathbb{Q}} X = 14$ [DvH14, Theorem 4 and Table 1]. The Galois orbits of cusps over $\mathbb{Q}$ and the closed cusps of $X_{\mathbb{F}_2}$ both have degrees $1^{12}, 2^6, 12^2$, so every effective cuspidal divisor on $X_{\mathbb{F}_2}$ is the reduction of an effective rational cuspidal divisor of the same degree (see [Naj26d, Section 13.8]). We denote by D_8 the closed point of degree 8 of X given by the octic point of level 39 of [Naj26d, Proposition 13.3], and by D_9 the closed point of degree 9 given by the point x_{39} of [Naj26d, Proposition 13.5]. The point of degree 10 is the following one.

Lemma 10.27. *Let (K_{39}, E_{39}) be the pair of Proposition 3.4 with $N = 39$. The trace divisor D_{10} of $(E_{39}, (0,0))$ on $X_1(39)$ is a closed point of degree 10 (the point 1.39.10.a of [Naj26b]), and its reduction modulo 2 is a closed point of degree 10.*

Proof. We check, with the model of (K_{39}, E_{39}) used in the proof of Proposition 3.4, that the reduction of D_{10} modulo 2 is a closed point of degree 10. (Another model of the pair replaces D_{10} by a diamond translate, as $E_{39}(K_{39})_{\mathrm{tors}} \simeq \mathbb{Z}/39\mathbb{Z}$.) As every closed point in the support of D_{10} reduces to an effective divisor of the same degree, D_{10} is a closed point of degree 10. □

Lemma 10.28. *Let $X = X_1(39)$.*

a) *The non-cuspidal closed points of $X_{\mathbb{F}_2}$ of degrees $1, \dots, 10$ number 0, 0, 0, 0, 0, 12, 0, 49, 52 and 60. Those of degree 6 form one diamond orbit, and those of degree 8, 9 and 10 form 5 diamond orbits each.*

b) *Let P be a non-cuspidal closed point of $X_{\mathbb{F}_2}$ of degree at most 10 such that $A_5 P$ is principal. Then P is the reduction of D_8, or the reduction of a diamond translate of D_9 or of D_{10}.*

Proof. The statements about the points of degree at most 8 are [Naj26d, Section 13.8] and the computation in the proof of [Naj26d, Proposition 13.14]: $A_5 P$ is not principal for the points of degree 6 and for those in 4 of the 5 orbits of degree 8, and the fifth orbit of degree 8 consists of the reduction of D_8 alone. We compute that 39 elliptic curves over $\mathbb{F}_{512}$ have a point of order 39, 36 of them with cyclic group of order 546 and 3 with cyclic group of order 468, and that 50 elliptic curves over $\mathbb{F}_{1024}$ have a point of order 39, all with cyclic group of order 1014. Their points of order 39 give 52 closed points of degree 9 and 60 of degree 10, each forming 5 diamond orbits. As A_5 commutes with the diamond operators, it suffices to test one point in each orbit, and we compute that $\ell(A_5 P) = 0$ for the representatives of 4 of the 5 orbits in each of the degrees 9 and 10. We check that the fifth orbit of degree 9 contains the reduction of D_9, and the fifth orbit of degree 10 that of D_{10}. □

Proposition 10.29. *Every effective rational divisor of degree 10 on $X_1(39)$ with non-cuspidal support is a diamond translate of D_{10}. Hence, if E is an elliptic curve over a number field K of degree 10 with a point of order 39, then (K, E) is isomorphic to the pair (K_{39}, E_{39}) of Proposition 3.4, and $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/39\mathbb{Z}$. In particular, $\mathbb{Z}/78\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/39\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let D be an effective rational divisor of degree 10 on $X = X_1(39)$ with non-cuspidal support. We first note that D is equal to every effective rational divisor B of degree 10 with the same reduction modulo 2: the class $[D - B] \in J_X(\mathbb{Q})$ reduces to 0, so $D \sim B$ by injectivity, and $D = B$ by Lemma 2.8, as $\mathrm{gon}_{\mathbb{Q}} X = 14 > 10$.

Suppose that the reduction of D is entirely cuspidal. It is the reduction of an effective rational cuspidal divisor C of degree 10, so $D = C$, which is impossible as the support of D contains no cusp. So by Lemma 10.28 a) the reduction of D is $P + \overline{C}$, where P is a non-cuspidal closed point of degree 6, 8, 9 or 10 (as $2 \cdot 6 > 10$) and $\overline{C}$ is the reduction of an effective rational cuspidal divisor C of degree $10 - \deg P$. As $J_X(\mathbb{Q})$ is finite, $A_5 D$ is principal (Proposition 2.2), and $A_5 C = 0$ as a divisor, so $A_5 P$ is principal. By Lemma 10.28 b), the reduction of D is the reduction of $D_8 + C$, of $hD_9 + C$ or of hD_{10} for a diamond operator h. These are effective rational divisors of degree 10, so D is equal to one of them, and as the support of D contains no cusp, $D = hD_{10}$.

Now let E be an elliptic curve over a number field K of degree 10 with a point P of order 39, and let D be the trace divisor of (E, P) (Section 2.2). By the first part $D = hD_{10}$ for a diamond operator h, so $(K, E) \simeq (K_{39}, E_{39})$ by Lemma 11.1, applied with $m = 1$ and the point $(E_{39}, (0, 0))$, whose trace divisor D_{10} is a closed point of degree 10 by Lemma 10.27.

Hence $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/39\mathbb{Z}$ by Proposition 3.4. If $E(K)$ contained $\mathbb{Z}/78\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/39\mathbb{Z}$, it would contain a point of order 39, and $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/39\mathbb{Z}$ would contain a point of order 78, respectively two independent points of order 3, which is impossible. □

Proposition 10.30. *The group $\mathbb{Z}/117\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let E be an elliptic curve over a number field K of degree 10 with a point Q of order 117. Then $3Q$ has order 39, so $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/39\mathbb{Z}$ by Proposition 10.29, which contains no point of order 117. □

10.8. **The group $\mathbb{Z}/90\mathbb{Z}$.** The group $\mathbb{Z}/45\mathbb{Z}$ occurs over number fields of degree 10, so we cannot exclude $\mathbb{Z}/90\mathbb{Z}$ on $X_1(45)$ alone. As in the proof of [Naj26d, Proposition 13.17], where $\mathbb{Z}/78\mathbb{Z}$ is excluded over nonic fields, we use the isogeny of degree 2 given by the point of order 2, and show that it would give an isogeny of degree 2 from the curve to one of its Galois conjugates, which is impossible by Lemma 8.30, as in the proofs of Propositions 8.35 and 8.42.

Lemma 10.31. *Let $X = X_1(45)$, which has genus 41.*

a) *The group $J_X(\mathbb{Q})$ is finite, reduction modulo 2 is injective on it, and $\operatorname{gon}_{\mathbb{Q}} X = 18$.*
b) *The Galois orbits of cusps of X over $\mathbb{Q}$ have degrees $1^{12}, 2^4, 4^3, 6^2, 8, 12$, and the closed cusps of $X_{\mathbb{F}_2}$ have degrees $1^{12}, 2^4, 4^5, 6^2, 12$. In particular, every effective cuspidal divisor of degree at most 10 on $X_{\mathbb{F}_2}$ which contains no closed cusp of degree 4 is the reduction of an effective rational cuspidal divisor of the same degree.*
c) *The non-cuspidal closed points of $X_{\mathbb{F}_2}$ of degree at most 10 are 60 points of degree 8, 60 points of degree 9 and 108 points of degree 10. For every point P of degree 8 or 9 there is a prime $q \nmid 90$ such that $A_q P$ is not principal, and $\ell(P) = 1$ for every point P of degree 10.*
d) *The space $U := (\mathcal{C} - 1)H^0(X_{\mathbb{F}_2}, \Omega^1)$ has dimension 39, and its restriction to every effective cuspidal divisor of degree 10 on $X_{\mathbb{F}_2}$ which contains a closed cusp of degree 4 is surjective.*

Proof. a) We have $\operatorname{rk} J_X(\mathbb{Q}) = 0$ [DEvH+21, Theorem 3.1(2)], the injectivity of reduction modulo 2 is shown at the end of the proof of [Naj26d, Proposition 7.6], and $\operatorname{gon}_{\mathbb{Q}} X = 18$ by [Var26, Theorem D].

b) The degrees of the Galois orbits of cusps are given in [DEvH+21, Lemma 2.8], and those of the closed cusps of $X_{\mathbb{F}_2}$ in the proof of [Naj26d, Proposition 7.6]. The cuspidal subscheme is finite étale over $\mathbb{Z}[\frac{1}{45}]$, so distinct geometric cusps have distinct reductions. Hence the 12 rational and the 4 quadratic closed cusps of $X_{\mathbb{F}_2}$ are the reductions of the Galois orbits of degree 1 and 2, and as $X_{\mathbb{F}_2}$ has no closed cusps of degree 3, each of the two Galois orbits of degree 6 reduces to a closed cusp of degree 6. This proves the last statement, as a cuspidal divisor of degree at most 10 on $X_{\mathbb{F}_2}$ which contains no closed cusp of degree 4 is supported on the closed cusps of degree 1, 2 and 6.

c) The points of degree at most 9 and the Hecke tests for them are in the proof of [Naj26d, Proposition 7.6]: the points of degree 8 and 9 form 5 diamond orbits each, for a representative P of each orbit of degree 8 one of the classes $[A_q P]$ with $q \in \{7, 11, 13, 17, 19\}$ is non-zero, and for a representative of each orbit of degree 9 the divisor $A_7 P$ is not principal. As A_q commutes with the diamond operators, this holds for all the points. We compute that the points of order 45 of the elliptic curves over $\mathbb{F}_{1024}$ give 108 closed points of degree 10 of $X_{\mathbb{F}_2}$, which form 10 orbits under the diamond operators, and we compute that $\ell(P) = 1$ for

a representative P of each orbit. As the diamond operators are automorphisms of $X_{\mathbb{F}_2}$, it follows that $\ell(P) = 1$ for all the 108 points.

d) The dimension of U is computed in the proof of [Naj26d, Proposition 7.6], together with the restrictions of U to the divisors mc for every closed cusp c of $X_{\mathbb{F}_2}$ and every m with $m \deg c \leq 8$. In an effective cuspidal divisor of degree 10 which contains a closed cusp of degree 4, this cusp has multiplicity at most 2, and every other closed cusp c occurs with a multiplicity m with $m \deg c \leq 6$. So the restriction of U to such a divisor is determined by these data. There are 94420 such divisors, and we compute that the restriction of U to each of them has rank 10. □

Lemma 10.32. *Let E be an elliptic curve over a number field K of degree 10 with a point P of order 45, and let D be the trace divisor of (E, P) on $X_1(45)$. Then D is a closed point of degree 10 with residue field K, the field K has a unique prime $\mathfrak{p}$ above 2, which is unramified with residue field $\mathbb{F}_{1024}$, E has good reduction at $\mathfrak{p}$, and the reduction of D modulo 2 is a non-cuspidal closed point of degree 10.*

Proof. Let $X = X_1(45)$. Suppose first that the reduction $\overline{D}$ of D is entirely cuspidal. If $\overline{D}$ contains no closed cusp of degree 4, then by Lemma 10.31 b) it is the reduction of an effective rational cuspidal divisor C of degree 10, so $D \sim C$ by Lemma 10.31 a), and $D = C$ by Lemma 2.8, as $\operatorname{gon}_{\mathbb{Q}} X = 18 > 10$. This is impossible, as the support of D contains no cusp. If $\overline{D}$ contains a closed cusp of degree 4, then Proposition 2.18, applied with $Y = X$, $r = 1$ and $\psi_1 = 1$ (as $J_X(\mathbb{Q})$ is finite), and Lemma 10.31 d) give a contradiction.

So $\overline{D}$ is not entirely cuspidal, and by Lemma 10.31 c), as $2 \cdot 8 > 10$, it is $G + \overline{C}$ with G a non-cuspidal closed point of degree 8, 9 or 10 and $\overline{C}$ cuspidal of degree at most 2. If $\deg G \leq 9$, then by Lemma 10.31 b) $\overline{C}$ is the reduction of an effective rational cuspidal divisor C. As $J_X(\mathbb{Q})$ is finite, $A_q D$ is principal for every prime $q \nmid 90$ (Proposition 2.2), and $A_q C = 0$ as a divisor, so $A_q G$ is principal, which contradicts Lemma 10.31 c). Hence $\overline{D} = G$ is a closed point of degree 10 with multiplicity 1. If $x \in X(K)$ is the point given by (E, P), then D is the sum of the conjugates of x, each counted $[K : \mathbb{Q}(x)]$ times, so $[K : \mathbb{Q}(x)] = 1$ and D is a closed point with residue field K. By Section 2.2, G is the reduction of x modulo a prime $\mathfrak{p}$ of K above 2 which is unramified and has residue field $\kappa(G) = \mathbb{F}_{1024}$, so $\mathfrak{p}$ is the only prime of K above 2. As G is not a cusp and X is a fine moduli space, E has good reduction at $\mathfrak{p}$. □

Proposition 10.33. *The group $\mathbb{Z}/90\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let E be an elliptic curve over a number field K of degree 10 with a point Q of order 90. Put $P = 2Q$ and $R = 45Q$, let $\phi : E \to E' = E/\langle R \rangle$, which is defined over K, and put $P' = \phi(P)$, which has order 45. Let D and D' be the trace divisors of (E, P) and (E', P') on $X = X_1(45)$. By Lemma 10.32, applied to both of them, the prime $\mathfrak{p}$ of K above 2 is unique and unramified with residue field $\mathbb{F}_{1024}$, E and E' have good reduction at $\mathfrak{p}$, and D and D' are closed points of degree 10 with residue field K which reduce to non-cuspidal closed points of degree 10. As $\mathfrak{p}$ is unramified over 2, the reduction of E at $\mathfrak{p}$ is ordinary by Lemma 8.30 a).

The reduction of ϕ at $\mathfrak{p}$ is an isogeny of degree 2 of an ordinary elliptic curve, so its kernel is either the connected subgroup of order 2, in which case it is the Frobenius isogeny, or the unique étale subgroup of order 2, in which case it is the Verschiebung up to isomorphism. Hence, as in the proof of [Naj26d, Proposition 13.17], the reduction of (E', P') is the image

of the reduction of (E,P) under the Frobenius, or under $\langle 2\rangle$ composed with the inverse of the Frobenius. As closed points are stable under the Frobenius, the reduction of D' is that of D or of $\langle 2\rangle D$. These are effective rational divisors of degree 10, so the class of $D'-D$, respectively of $D'-\langle 2\rangle D$, lies in $J_X(\mathbb{Q})$ and reduces to 0, and by Lemma 10.31 a) we get $D'\sim D$, respectively $D'\sim\langle 2\rangle D$. The reductions of D and $\langle 2\rangle D$ are non-cuspidal closed points of degree 10, so $\ell(D)=\ell(\langle 2\rangle D)=1$ by Lemma 10.31 c) and semicontinuity [Har77, Theorem III.12.8], and hence $D'=D$, respectively $D'=\langle 2\rangle D$.

Note that $\langle 2\rangle D$ is the trace divisor of $(E,2P)$. So the K-point of X given by (E',P') and the one given by (E,P), respectively $(E,2P)$, lie on the same closed point with residue field K, and they differ by an automorphism σ of K. As X is a fine moduli space, $E'\simeq E^\sigma$ over K, and $\sigma(\mathfrak{p})=\mathfrak{p}$, as $\mathfrak{p}$ is the only prime of K above 2. As $\mathbb{Z}/90\mathbb{Z}$ is not a subgroup of any of the groups of Lemma 2.14, the curve E has no complex multiplication, so $\mathrm{End}_{\overline{K}}(E)=\mathbb{Z}$, and this contradicts Lemma 8.30 b). □

10.9. **The groups $\mathbb{Z}/99\mathbb{Z}$ and $\mathbb{Z}/105\mathbb{Z}$.** For $n=99$ and $n=105$ we do not show that $J_1(n)(\mathbb{Q})$ is finite, and we only use that $(\langle a\rangle-1)J_1(n)(\mathbb{Q})$ is finite for a suitable a. The entirely cuspidal reductions modulo 2 are then excluded by the following lemma, and the non-cuspidal ones with Hecke operators on $X_1(33)$ and on a quotient of $X_1(99)$ of genus 29, respectively on $X_1(35)$.

Lemma 10.34. *Let n be odd, let $X=X_1(n)$, and let $a\in(\mathbb{Z}/n\mathbb{Z})^\times$ be such that $(\langle a\rangle-1)J_X(\mathbb{Q})$ is finite, $\mathrm{gon}_{\mathbb{C}}X>40$, and the order of $\langle a\rangle$ in $\Delta(n)$ does not divide 10. Then no effective rational divisor of degree 10 on X whose support contains no cusp reduces modulo 2 to a cuspidal divisor.*

Proof. Let D be such a divisor, and suppose that its reduction modulo 2 is cuspidal. The cusps of X are defined over $\mathbb{Q}(\zeta_n)$, which is unramified above 2, and the cuspidal subscheme is finite étale over $\mathbb{Z}[\frac{1}{n}]$, so the reduction of D lifts to an effective cuspidal divisor C of degree 10 defined over $\mathbb{Q}(\zeta_n)$. The operator $g=\langle a\rangle$ fixes the reduction of $D-C$, which is 0. By Lemma 2.10 c), applied with $p=2$ and $d=e=10$, as $\mathrm{gon}_{\mathbb{C}}X>40$, we get $gD+C=D+gC$, and as the support of D contains no cusp, $gD=D$. Every point in the support of D reduces to a cusp modulo a prime above 2, so its j-invariant is not integral, and the corresponding elliptic curve has no complex multiplication. By Lemma 2.9, applied to the group generated by g, the order of g in $\Delta(n)$ divides $\deg D=10$, which is a contradiction. □

Lemma 10.35. *Let $X=X_1(99)$, which has genus 281.*

a) *The group $(\langle a\rangle-1)J_X(\mathbb{Q})$ is finite for every $a\in(\mathbb{Z}/99\mathbb{Z})^\times$.*
b) *The curve $X_{\mathbb{F}_2}$ has no non-cuspidal closed points of degree at most 9, and 120 of degree 10, which form 4 diamond orbits.*
c) *We have $\mathrm{gon}_{\mathbb{C}}X>42.84$.*

Proof. a) We compute, for each Galois orbit of even Dirichlet characters modulo 99, the winding submodule of the space of cuspidal modular symbols of weight 2 with that character. The dimensions of these spaces, counted with the sizes of the orbits, add up to 281. The winding submodule is the whole space for every non-trivial character, and it has codimension 1 for the trivial character. By Kato's theorem [Kat04, Corollary 14.3], every factor of J_X with non-trivial character has finitely many rational points, and $\langle a\rangle$ acts trivially on the factor with trivial character, so $(\langle a\rangle-1)J_X(\mathbb{Q})$ is finite.

b) We compute that no elliptic curve over $\mathbb{F}_{2^k}$ with $k\le 9$ has a point of order 99, and that 40 elliptic curves over $\mathbb{F}_{1024}$ have one, all with cyclic group of order 990. Their points

of order 99 give 120 closed points of degree 10, which form 4 orbits under $\Delta(99)$, a group of order 30.

c) As $i(99) = 4320$, Abramovich's bound gives $\operatorname{gon}_{\mathbb{C}} X \geq \frac{325}{2^{15}} \cdot 4320 > 42.84$. □

For the remaining orbit of $\mathbb{Z}/99\mathbb{Z}$ we use the following quotient of $X_1(99)$.

Lemma 10.36. *Let $H_{99} \subseteq \Delta(99)$ be the subgroup of the $\langle a\rangle$ with $a \equiv \pm 1 \pmod 9$, which has order 10, let $V_{99} = X_1(99)/H_{99}$, and let $\pi : X_1(99) \to V_{99}$ be the quotient map.*

a) *The curve V_{99} parametrizes triples $(E, \pm P_9, C_{11})$, where P_9 is a point of order 9 and C_{11} a cyclic subgroup of order 11 of E, and $\pi(E, P) = (E, \pm 11P, \langle 9P\rangle)$. It is the normalization of $X_1(9) \times_{X(1)} X_0(11)$, it has good reduction at 2, and every $\langle a\rangle$ induces an automorphism δ_a of V_{99}, which depends only on a modulo 9 up to sign. In particular $\delta_{10} = 1$.*

b) *The group $(\delta_2 - 1)J(V_{99})(\mathbb{Q})$ is finite.*

c) *Let t be the coordinate on $X_1(9)$ for which the pair (E, P_9) is given by the curve*

$$E_t : y^2 + (1-c)xy - by = x^3 - bx^2, \qquad c = t^2(t-1), \quad b = c(t^2 - t + 1),$$

and the point $(0, 0)$. Then the function field of $V_{99,\mathbb{F}_2}$ is generated over $\mathbb{F}_2(t)$ by the function field of $X_0(11)_{\mathbb{F}_2}$, it has degree 12 over $\mathbb{F}_2(t)$, and the curve V_{99} has genus 29.

Proof. a) Two points (E, P) and (E, P') of $X_1(99)$ satisfy $11P' = \pm 11P$ and $\langle 9P'\rangle = \langle 9P\rangle$ if and only if $P' = aP$ with $a \equiv \pm 1 \pmod 9$, i.e. if and only if $(E, P') = \langle a\rangle(E, P)$ with $\langle a\rangle \in H_{99}$. This proves the moduli description, and hence V_{99} is the normalization of $X_1(9) \times_{X(1)} X_0(11)$. It has good reduction at 2 by Lemma 2.1, as its genus is positive by c). As $\Delta(99)$ is abelian, every $\langle a\rangle$ induces an automorphism δ_a of V_{99}, which acts by $(E, \pm P_9, C_{11}) \mapsto (E, \pm aP_9, C_{11})$. As $10 \equiv 1 \pmod 9$, we have $\delta_{10} = 1$.

b) We have $\pi_*\pi^* = 10$ on $J(V_{99})$ and $\pi_*\langle 2\rangle = \delta_2\pi_*$. So for $y \in J(V_{99})(\mathbb{Q})$ we get $10(\delta_2 - 1)y = \pi_*\big((\langle 2\rangle - 1)\pi^* y\big)$, which lies in the finite group $\pi_*\big((\langle 2\rangle - 1)J_1(99)(\mathbb{Q})\big)$ by Lemma 10.35 a). As $J(V_{99})(\mathbb{Q})$ is finitely generated, $(\delta_2 - 1)J(V_{99})(\mathbb{Q})$ is finite.

c) The map $V_{99} \to X_1(9)$ has degree $i(99)/(10\, i(9)) = 4320/360 = 12$, which is also the degree of $X_0(11) \to X(1)$. Over $\mathbb{F}_2$ the maps $(E, \pm P_9, C_{11}) \mapsto (E, \pm P_9)$ and $(E, \pm P_9, C_{11}) \mapsto (E, C_{11})$ to $X_1(9)$ and $X_0(11)$ show that the function field of $V_{99,\mathbb{F}_2}$ contains $\mathbb{F}_2(t)$ and the function field of $X_0(11)_{\mathbb{F}_2}$. We compute that $(0, 0)$ has order 9 on E_t over $\mathbb{F}_2(t)$, and, eliminating the j-invariant between E_t and the j-map of a model of $X_0(11)_{\mathbb{F}_2}$, that the compositum of these two fields is given by an irreducible polynomial of degree 12 over $\mathbb{F}_2(t)$. So it is the function field of $V_{99,\mathbb{F}_2}$, and we compute that it has genus 29. On this model we also express $j(E/C_{11})$, using the Atkin-Lehner involution of $X_0(11)$. The image on $V_{99,\mathbb{F}_2}$ of a point (E, P) of $X_1(99)_{\mathbb{F}_2}$ is then determined by the value of t at $(E, \pm 11P)$ and by the point $(E, \langle 9P\rangle)$ of $X_0(11)_{\mathbb{F}_2}$, which we compute from $j(E)$ and $j(E/\langle 9P\rangle)$. □

Proposition 10.37. *The group $\mathbb{Z}/99\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let D be the trace divisor of a point of order 99 over a number field of degree 10. As $2^{15} \equiv -1 \pmod{99}$ and $2, 2^3, 2^5 \not\equiv \pm 1 \pmod{99}$, the operator $\langle 2\rangle$ has order 15 in $\Delta(99)$. By Lemma 10.35 and Lemma 10.34, applied with $a = 2$, the reduction $\overline{D}$ of D modulo 2 is not entirely cuspidal, so by Lemma 10.35 b) it is a non-cuspidal closed point G of degree 10. Then $G = \langle a\rangle G_i$ for some a and i, where $G_1, \dots, G_4$ are representatives of the 4 diamond orbits of such points.

We first use the map $\pi_{33} : X_1(99) \to X_1(33)$, $(E, P) \mapsto (E, 3P)$, which commutes with the diamond operators. We have $\operatorname{rk} J_1(33)(\mathbb{Q}) = 0$ [DEvH+21, Theorem 3.1(2)], so for $A_5 = T_5 - 1 - 5\langle 5\rangle$ on $X_1(33)$ the divisor $A_5\pi_{33*}D$ is principal (Proposition 2.2 d)), and so is its reduction $\langle a\rangle A_5\pi_{33*}G_i$. We compute that for every i the image $P_i = \pi_{33*}G_i$ is a closed point of degree 10, that the six subgroups of order 5 form Frobenius orbits of lengths 1, 1, 2 and 2, which give T_5P_i as a sum of closed points of degrees 10, 10, 20 and 20, each with multiplicity 1, and that $\ell(A_5P_i) = 0$ for $i = 1, 2, 4$. So $G = \langle a\rangle G_3$.

Let $\pi : X_1(99) \to V_{99}$ be as in Lemma 10.36, let c_0 be the image of the standard cusp, which is rational, and put $A_5 = T_5 - 1 - 5\delta_5$ on V_{99}. We have

$$(\delta_2 - 1)\pi_*D = (\delta_2 - 1)(\pi_*D - 10c_0) + 10(\delta_2c_0 - c_0).$$

The class of the first term lies in the finite group $(\delta_2 - 1)J(V_{99})(\mathbb{Q})$ (Lemma 10.36 b)), and the second term is a rational cuspidal divisor of degree 0, whose class is torsion by the Manin-Drinfeld theorem. So the class of $(\delta_2 - 1)\pi_*D$ is a rational torsion point of $J(V_{99})$, and it is annihilated by A_5 (Proposition 2.2). Hence the reduction $(\delta_2-1)A_5\pi_*G$ of $A_5(\delta_2-1)\pi_*D$ is principal. As the operators δ_b are automorphisms of V_{99} which commute with A_5, it follows that $B = (\delta_2 - 1)A_5P_V$ is principal, where $P_V = \pi_*G_3$. Writing $T = T_5P_V$, and using $\delta_{10} = 1$, we have

$$B = \delta_2T - T - \delta_2P_V + 5\delta_5P_V - 4P_V.$$

We compute B on the model of Lemma 10.36 c), carrying the level structure of a point of G_3 through the six isogenies of degree 5: the point P_V has degree 10, T and δ_2T are sums of closed points of degrees 10, 10, 20 and 20, each with multiplicity 1, and the positive and negative parts of B have degree 110. We compute that $\ell(B) = 0$, so B is not principal, which is a contradiction. □

Lemma 10.38. *Let $X = X_1(105)$, which has genus 289.*

a) *The group $(\langle 22\rangle - 1)J_X(\mathbb{Q})$ is finite.*
b) *The curve $X_{\mathbb{F}_2}$ has no non-cuspidal closed points of degree at most 9, and 144 of degree 10, which form 6 diamond orbits.*
c) *We have $\operatorname{gon}_{\mathbb{C}} X > 45.70$.*

Proof. a) We compute the winding submodules as in the proof of Lemma 10.35. The dimensions add up to 289, and the winding submodule is the whole space for every Galois orbit of even characters except one, which consists of characters of order 6 and conductor 21, and for which it has codimension 1. As $22 \equiv 1 \pmod{21}$, these characters are trivial at 22, so $\langle 22\rangle$ acts trivially on the corresponding factor of J_X, and by Kato's theorem [Kat04, Corollary 14.3] the group $(\langle 22\rangle - 1)J_X(\mathbb{Q})$ is finite.

b) We compute that no elliptic curve over $\mathbb{F}_{2^k}$ with $k \leq 9$ has a point of order 105, and that 60 elliptic curves over $\mathbb{F}_{1024}$ have one, all with cyclic group of order 1050. Their points of order 105 give 144 closed points of degree 10, which form 6 orbits under $\Delta(105)$, a group of order 24.

c) As $i(105) = 4608$, Abramovich's bound gives $\operatorname{gon}_{\mathbb{C}} X \geq \frac{325}{2^{15}} \cdot 4608 > 45.70$. □

Proposition 10.39. *The group $\mathbb{Z}/105\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Let D be the trace divisor of a point of order 105 over a number field of degree 10. We have $22^2 \equiv 64$ and $22^4 \equiv 1$ modulo 105, and $64 \not\equiv -1 \pmod{105}$, so $\langle 22\rangle$ has order 4 in $\Delta(105)$. By Lemma 10.38 and Lemma 10.34, applied with $a = 22$, the reduction of D

modulo 2 is not entirely cuspidal, so by Lemma 10.38 b) it is a non-cuspidal closed point G of degree 10, and $G = \langle a \rangle G_i$ for a representative G_i of one of the 6 diamond orbits.

Let $\pi_{35} : X_1(105) \to X_1(35)$ be the map $(E, P) \mapsto (E, 3P)$, which commutes with the diamond operators. We have $\operatorname{rk} J_1(35)(\mathbb{Q}) = 0$ [DEvH+21, Theorem 3.1(2)], so for $A_3 = T_3 - 1 - 3\langle 3 \rangle$ on $X_1(35)$ the divisor $A_3 \pi_{35*} D$ is principal (Proposition 2.2 d)), and so is its reduction $\langle a \rangle A_3 \pi_{35*} G_i$. We compute that for each of the 6 representatives the image $P_i = \pi_{35*} G_i$ is a closed point of degree 10, that the four subgroups of order 3 form Frobenius orbits of lengths 1 and 3, which give $T_3 P_i$ as a sum of closed points of degrees 10 and 30, each with multiplicity 1, and that

$$\ell\big(T_3 P_i - P_i - 3\langle 3 \rangle P_i\big) = 0.$$

So $A_3 P_i$ is not principal for any i, which is a contradiction. □

11. Sporadic points and complete classifications

We treat the groups $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$. Each of them is the torsion group of an elliptic curve over a number field of degree 10, but only of finitely many. For each of them we give explicit elliptic curves over explicit decic fields with exactly this torsion group, and we determine all the effective $\mathbb{Q}(\zeta_m)$-rational divisors of degree d_m on $X_1(m, n)$ whose support contains no cusp. This shows that the curves we give are, up to isomorphism, the only elliptic curves over decic fields with a subgroup isomorphic to these groups, and it excludes the groups $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/45\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ and $\mathbb{Z}/52\mathbb{Z}$. Table 7 lists the curves.

In all four cases the Jacobian of the modular curve X is finite over $F = \mathbb{Q}(\zeta_m)$ by [DS17, Theorem 4.1] (for $X_1(2, 26)$ see also [DEvH+21, Theorem 3.1(3)]), and $\operatorname{gon}_F X > d_m$. Hence, by Lemma 2.8, distinct effective F-rational divisors of degree d_m on X have distinct classes, and X has only finitely many such divisors. We work at primes $\mathfrak{p}$ of F not dividing n, at which X has good reduction, which are odd except in one step for $X_1(3, 15)$, so that reduction is injective on $J_X(F)$ by Katz's result. We identify the Galois orbits of cusps over F with their reductions using the valuations of integral modular units, as in [Naj26d, Sections 11, 12 and 13]. The arguments below then show that the class of the trace divisor D is, after applying a level automorphism, the class of a known effective divisor, which is then equal to D. By Lemma 2.14, an elliptic curve over a number field of degree 10 whose torsion contains one of the four groups has no complex multiplication. Finally, the following lemma shows that the pair (K, E) is determined up to isomorphism.

Lemma 11.1. *Let $m \mid n$ with $n \geq 4$, let $F = \mathbb{Q}(\zeta_m)$ and $X = X_1(m, n)$ over F, and put $d_m = 10/\varphi(m)$. Let E_0 be an elliptic curve over a number field K_0 of degree 10, and let $x_0 = (E_0, P_0, Q_0) \in Y_1(m, n)(K_0)$ be a point whose trace divisor D_0 is a closed point of degree d_m. Let E be an elliptic curve over a number field K of degree 10, and let $x = (E, P, Q) \in Y_1(m, n)(K)$ be a point whose trace divisor is gD_0 for a level automorphism g of X defined over F. Then (K, E) is isomorphic to (K_0, E_0).*

Proof. As D_0 is a closed point of degree $d_m = [K_0 : F]$, the residue field $F(x_0) \subseteq K_0$ of x_0 is K_0. The automorphism g is defined over F, so $g(x_0) \in Y_1(m, n)(K_0)$ also has residue field K_0, and its closed point is gD_0. The trace divisor of x is the sum of the F-conjugates of x, each counted $[K : F(x)]$ times (Section 2.2), and as it is a closed point with multiplicity 1, we have $F(x) = K$. So x and $g(x_0)$ lie above the same closed point of X, and there is an

isomorphism $\sigma\colon K_0 \to K$ over F such that x is the image of $g(x_0)$ under σ. As $Y_1(m,n)$ is a fine moduli space and g does not change the elliptic curve, $E \simeq E_0^\sigma$ over K. □

For b, c in a field we write

$$E(b,c): \quad y^2 + (1-c)xy - by = x^3 - bx^2 \tag{11.1}$$

for the curve in Tate normal form, on which $(0,0)$ has order n when (b,c) comes from a point of $Y_1(n)$, and

$$E'(b,c): \quad y^2 = x^3 + cx^2 + b(1-b-c)x, \tag{11.2}$$

on which $(0,0)$ has order 2 and (b,b) has order n when (b,c) comes from a point of $Y_1(2,n)$.

G	K	pairs	E	[Naj26b]	
$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$	10.0.4678854192.1	1	$E_{6,12}$	6.12.10.a	Proposition 11.7
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$	10.0.306454347.1	1	$E_{3,15}$	3.15.10.a	Proposition 11.10
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$	10.0.2571428187.1	2	$E_{3,18}$	3.18.10.a	Proposition 11.18
			$E'_{3,18}$	3.18.10.b	
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$	10.6.396320664709.1	1	$E_{2,26}$	2.26.10.a	Proposition 11.24
	10.2.799905449.1	1	$E'_{2,26}$	2.26.10.b	

TABLE 7. The elliptic curves E over number fields K of degree 10 with $E(K)_{\mathrm{tors}} \simeq G$, for the four groups G of this section, the number of pairs (K,E) up to isomorphism over each field, and the labels of the corresponding points in [Naj26b]. These are all the pairs with $G \subseteq E(K)_{\mathrm{tors}}$. The curves $E_{3,18}$ and $E'_{3,18}$ are 2-isogenous. In all cases $j(E)$ has degree 5 over $\mathbb{Q}$ and is not an algebraic integer, so E has no complex multiplication.

11.1. **The curve $X_1(6,12)$.** Let $F = \mathbb{Q}(z)$ with $z^2 - z + 1 = 0$, so that z is a primitive sixth root of unity, and let $X = X_1(6,12)$ over F. It is a curve of genus 9, $J_X(F)$ is finite [DS17, Theorem 4.1], and $\mathrm{gon}_F X \geq 6$ [NV26, Table 1]. We use the plane model of X from [mdm] (see `shared/mdmagma/models_X1_m_n/X1_6_12.txt`), with affine coordinates u, v. On it the point Q of order 12 is the point $(0,0)$ of the curve $E(b,c)$ of (11.1), where

$$r = \frac{u^2+1}{u^2-u}, \qquad s = \frac{u^2+u+1}{u^2}, \qquad b = rs(r-1), \qquad c = s(r-1). \tag{11.3}$$

So u is a coordinate on $X_1(12) \simeq \mathbb{P}^1$, and $u : X \to \mathbb{P}^1$ is the map forgetting P, which has degree 6.

The level automorphisms of X defined over F are the maps

$$(P,Q) \longmapsto (\alpha P + 2\beta Q,\ \gamma P + \delta Q), \qquad \alpha,\beta,\gamma \in \mathbb{Z}/6\mathbb{Z},\ \ \delta \in \mathbb{Z}/12\mathbb{Z},\ \ \alpha\delta - 2\beta\gamma \equiv 1 \pmod 6, \tag{11.4}$$

which preserve the Weil pairing of P and $2Q$. Taken modulo ± 1 they form a group $G_{6,12}$ of order 96, as we compute.

Lemma 11.2. *Let $F = \mathbb{Q}(\zeta_6)$, let $X = X_1(6,12)$ over F, and let $\mathfrak{p}_7$ be a prime of F above 7, with residue field $\mathbb{F}_7$.*

a) *The closed cusps of $X_{\mathbb{F}_7}$ have degrees $1^{16}, 2^8$, and each of them is the reduction of a Galois orbit of cusps over F of the same degree.*

b) *We have*

$$J_X(\mathbb{F}_7) \simeq \mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}\times(\mathbb{Z}/24\mathbb{Z})^2\times(\mathbb{Z}/48\mathbb{Z})^2, \qquad \mathrm{Cl}^c_F X \simeq \mathbb{Z}/6\mathbb{Z}\times(\mathbb{Z}/12\mathbb{Z})^3\times(\mathbb{Z}/24\mathbb{Z})^2,$$

so $\#\,\mathrm{Cl}^c_F X = 5971968$*, and reduction modulo* $\mathfrak{p}_7$ *is injective on* $J_X(F)$*.*

c) *The kernel of* $A_{13} = T_{13} - 14$ *on* $J_X(\mathbb{F}_7)$ *contains the reduction of* $\mathrm{Cl}^c_F X$*, with quotient isomorphic to* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$*. In particular* $2J_X(F) \subseteq \mathrm{Cl}^c_F X$*.*

d) *The non-cuspidal closed points of* $X_{\mathbb{F}_7}$ *of degrees* $1,\dots,5$ *number* 0, 0, 96, 468 *and* 3264*.*

Proof. Parts a) and b) and the first four numbers in d) are in the proof of [Naj26d, Proposition 12.7], and reduction modulo $\mathfrak{p}_7$ is injective on $J_X(F) = J_X(F)_{\mathrm{tors}}$ by Katz's result, as 7 is odd, unramified in F and prime to 12. We compute the number 3264 of closed points of degree 5. As $13 \equiv 1 \pmod{12}$, the diamond operator $\langle 13\rangle$ is trivial and $A_{13} = T_{13} - 14$. We compute the kernel of A_{13} on $J_X(\mathbb{F}_7)$, and that its quotient by the reduction of $\mathrm{Cl}^c_F X$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. As 13 splits completely in F, A_{13} annihilates $J_X(F)$ by Proposition 2.2 b), so the reduction of $J_X(F)$ lies in this kernel. As reduction is injective on $J_X(F)$, it follows that $J_X(F)/\mathrm{Cl}^c_F X$ embeds into $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, which proves c). □

Lemma 11.3. *Let* $F = \mathbb{Q}(\zeta_6)$ *and* $X = X_1(6,12)$ *over* F*. There are* 3360 *explicit* F*-rational cuspidal divisors* $L_1,\dots,L_{3360}$ *of degree* 10 *on* X *(not necessarily effective), given in* `continuation_20261029/M6N12_D5_all_source_lifts.m`*, such that for every effective* F*-rational divisor* D *of degree* 5 *on* X *whose support contains no cusp we have* $2D \sim L_k$ *for some* k*.*

Proof. Let D be such a divisor, let $\mathfrak{p}_7$ be as in Lemma 11.2, and fix an F-rational cusp c_*. As $\mathrm{gon}_F X \geq 6 > 5$, by Proposition 2.5 a) the reduction of D modulo $\mathfrak{p}_7$ is not cuspidal, so by Lemma 11.2 d) it is $x + C'$, where x is a closed point of degree 3, 4 or 5 and C' is an effective cuspidal divisor of degree $5 - \deg x$. By Lemma 11.2 a) there are $\binom{17}{2} + 8 = 144$ effective cuspidal divisors of degree 2 and 16 of degree 1, so there are

$$96\cdot 144 + 468\cdot 16 + 3264 = 24576$$

possibilities for $x + C'$. The class $[D - 5c_*]$ lies in $J_X(F)$, so it is killed by A_{13}, and hence so is its reduction $[x + C' - 5\overline{c_*}]$. We compute that this holds for 3552 of the 24576 possibilities, and that they give 3360 distinct classes $2[x + C' - 5\overline{c_*}]$. By Lemma 11.2 c) these classes lie in the reduction of $\mathrm{Cl}^c_F X$, and by the injectivity of reduction we obtain 3360 explicit F-rational cuspidal divisors $L_1,\dots,L_{3360}$ of degree 10 such that $2D \sim L_k$ for some k. □

Lemma 11.4. *Let* $F = \mathbb{Q}(z)$ *with* $z^2 - z + 1 = 0$*, let* $X = X_1(6,12)$ *over* F*, let* $L_1,\dots,L_{3360}$ *be as in Lemma 11.3, and let* $\mathfrak{p}_{13} = (13, z-4)$*, a prime of* F *above* 13*, with residue field* $\mathbb{F}_{13}$*. For exactly* 192 *of the* 3360 *indices* k *the linear system* $|\overline{L_k}|$ *on* $X_{\mathbb{F}_{13}}$ *contains a divisor of the form* $2A$*, where* A *is effective and its support is not contained in the cusps, and for these* $\ell(L_k) = 2$*.*

Proof. We compute all the effective $\mathbb{F}_{13}$-rational divisors in the linear systems $|\overline{L_k}|$ (we have $\ell(\overline{L_k}) = 2$ for 2880 of them and $\ell(\overline{L_k}) = 3$ for the other 480), and find that such a divisor $2A$ exists for exactly 192 of the 3360 classes, and that $\ell(\overline{L_k}) = 2$ for all of these. For these 192 divisors L_k we have $\ell(L_k) \geq 10 + 1 - 9 = 2$ by the Riemann-Roch theorem, and $\ell(L_k) \leq \ell(\overline{L_k}) = 2$ by semicontinuity [Har77, Theorem III.12.8], so $\ell(L_k) = 2$. □

Lemma 11.5. *Let* $F = \mathbb{Q}(\zeta_6)$*, let* $X = X_1(6,12)$ *over* F*, and let* $L_{8,1},\dots,L_{8,6}$ *be the six effective cuspidal divisors of degree* 8 *with* $\ell(L_{8,i}) = 2$ *of the proof of* [Naj26d, Proposition

12.7]. *Then* 96 *of the* 192 *divisors* L_k *of Lemma 11.4 are linearly equivalent to divisors* $L_{8,i}+2c$*, where* c *is an* F*-rational cusp, and no effective* F*-rational divisor* D *of degree* 5 *on* X *whose support contains no cusp satisfies* $2D \sim L_{8,i}+2c$*.*

Proof. We find that 96 of the 192 classes are the classes of the divisors $L_{8,i}+2c$, where c runs over the 16 F-rational cusps. We verify these identities of classes with the divisors of 141 modular units. They span a sublattice of rank 23 and index $5971968 = \#\operatorname{Cl}_F^c X$ of the lattice of F-rational cuspidal divisors of degree 0, which is also the index of the sublattice of principal divisors, so the two sublattices are equal. By Lemma 11.4 we have $\ell(L_{8,i}+2c) = 2 = \ell(L_{8,i})$, so every effective divisor linearly equivalent to $L_{8,i}+2c$ is of the form $B+2c$ with $B \in |L_{8,i}|$. So $2D \sim L_{8,i}+2c$ would imply that c lies in the support of D, which is impossible. □

Lemma 11.6. *Let* $F = \mathbb{Q}(\zeta_6)$ *and* $X = X_1(6,12)$ *over* F*, and let* D *be an effective* F*-rational divisor of degree* 5 *on* X *whose support contains no cusp. Then there is* $g \in G_{6,12}$ *such that* $2gD \sim L$*, where* L *is the effective cuspidal divisor of degree* 10 *given in* `jobs/cont_reduce612_quintic_lattice_v2.log`*.*

Proof. By Lemma 11.3 we have $2D \sim L_k$ for some k. Let $\mathfrak{p}_{13}$ be as in Lemma 11.4. As $\operatorname{gon}_F X \geq 6 > 5$, by Proposition 2.5 a) the reduction of D modulo $\mathfrak{p}_{13}$ is not cuspidal, so the reduction of $2D$ is a divisor in $|\overline{L_k}|$ of the form $2A$, where A is effective and its support is not contained in the cusps. So L_k is one of the 192 divisors of Lemma 11.4, and by Lemma 11.5 it is not linearly equivalent to any of the divisors $L_{8,i}+2c$. We compute that the remaining 96 classes are the classes of the divisors gL, $g \in G_{6,12}$. As the elements of $G_{6,12}$ are automorphisms of X over F which map cusps to cusps, $2D \sim gL$ is equivalent to $2g^{-1}D \sim L$. □

Proposition 11.7. *Let* $F = \mathbb{Q}(z)$ *with* $z^2 - z + 1 = 0$*, let* w *be a root of*

$$3w^5 + (4-5z)w^4 + (7-8z)w^3 - 7(z+1)w^2 + 6(z-1)w + 2z - 1,$$

and put $K_{6,12} = F(w)$*, which is the field 10.0.4678854192.1. Let* $E_{6,12} = E(b,c)$ *be the curve* (11.1) *with* r*,* s*,* b *and* c *given by* (11.3) *with* $u = w$*, i.e.*

$$E_{6,12}:\ y^2+(1+s-rs)xy+rs(1-r)y = x^3+rs(1-r)x^2, \qquad r = \frac{w^2+1}{w^2-w},\ \ s = \frac{w^2+w+1}{w^2}.$$

a) *We have* $E_{6,12}(K_{6,12})_{\mathrm{tors}} \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$*. The point* $Q = (0,0)$ *has order* 12*, the point* P *with*

$$2x(P) = (25z+10)w^4 + (45-20z)w^3 + (79-17z)w^2 + (22-109z)w + 39z - 46,$$

$$2y(P) = (222z+237)w^4 + (651-537z)w^3 + (1012-601z)w^2 - (1518z+223)w + 808z - 861$$

has order 6*, and* $e_6(P,2Q) = z$*. The* j*-invariant of* $E_{6,12}$ *has degree* 5 *over* $\mathbb{Q}$ *and is not an algebraic integer.*

b) *Every effective* F*-rational divisor of degree* 5 *on* $X_1(6,12)$ *whose support contains no cusp is one of the* 96 *closed points of degree* 5 *in the orbit under* $G_{6,12}$ *of the trace divisor* $D_{6,12}$ *of* $(E_{6,12}, P, Q)$*.*

c) *If* E *is an elliptic curve over a number field* K *of degree* 10 *with* $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \subseteq E(K)$*, then* (K,E) *is isomorphic to* $(K_{6,12}, E_{6,12})$*, and* $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$*. In particular, no group properly containing* $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ *is a subgroup of the torsion of an elliptic curve over a number field of degree* 10*.*

Proof. We compute that the quintic polynomial is irreducible over F, that Q and P have orders 12 and 6, and that $e_6(P,2Q) = z$, so $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \subseteq E_{6,12}(K_{6,12})$. The prime of $K_{6,12}$ given by $z \mapsto 14$, $w \mapsto 8$ has residue field $\mathbb{F}_{61}$, and it is unramified, as both defining polynomials have simple roots modulo 61. The curve has good reduction $y^2 - 4xy + 4y = x^3 + 4x^2$ there, with 72 points over $\mathbb{F}_{61}$. As 61 is odd, reduction is injective on $E_{6,12}(K_{6,12})_{\mathrm{tors}}$, so its order divides 72, which proves the first claim of a). The same computation shows that the minimal polynomial of $j(E_{6,12})$ over F has rational, non-integral coefficients and degree 5.

We prove b). By (11.3) the point $(E_{6,12}, P, Q)$ of X has u-coordinate w, so its residue field is $F(w) = K_{6,12}$, and $D_{6,12}$ is a closed point of degree 5. Let D be as in b). By Lemma 11.6, applied to D and to $D_{6,12}$, there are $g, g_0 \in G_{6,12}$ with $2gD \sim L$ and $2g_0 D_{6,12} \sim L$. Let $\mathfrak{p}_{13} = (13, z-4)$ be the prime of F above 13 of Lemma 11.4. We compute that $\ell(\overline{L}) = 2$ on $X_{\mathbb{F}_{13}}$, and that exactly one of the 14 effective divisors in $|\overline{L}|$ is of the form $2A$ with A effective and its support not contained in the cusps (and A is the sum of a closed point of degree 2 and a closed point of degree 3). By Proposition 2.5 a), as $\mathrm{gon}_F X \geq 6 > 5$, the reductions of gD and of $g_0 D_{6,12}$ modulo $\mathfrak{p}_{13}$ are not entirely cuspidal, and twice each of them lies in $|\overline{L}|$, so both are equal to A. Hence $[gD - g_0 D_{6,12}] \in J_X(F)$ reduces to 0, so $gD \sim g_0 D_{6,12}$ by Katz's result, as 13 is odd, unramified in F and prime to 12, and $gD = g_0 D_{6,12}$ by Lemma 2.8, as $\mathrm{gon}_F X \geq 6 > 5$. So every D as in b) is in the orbit of $D_{6,12}$ under $G_{6,12}$. If $S \subseteq G_{6,12}$ is the stabilizer of $D_{6,12}$, then $\#S$ divides $\deg D_{6,12} = 5$ by Lemma 2.9, as $E_{6,12}$ has no complex multiplication by Lemma 2.14, and $\#S$ divides 96, so S is trivial and the orbit has 96 elements. This proves b).

For c), let E/K be as in c). By the Weil pairing $F \subseteq K$, and choosing $P', Q' \in E(K)$ of orders 6 and 12 with $e_6(P', 2Q') = z$ we obtain a point of $Y_1(6,12)(K)$, whose trace divisor has degree 5. By b) it is $gD_{6,12}$ for some $g \in G_{6,12}$, so $(K, E) \simeq (K_{6,12}, E_{6,12})$ by Lemma 11.1. The last claim of c) follows from a). □

11.2. **The curve $X_1(3,15)$.** Let $F = \mathbb{Q}(z)$ with $z^2 + z + 1 = 0$, and let $X = X_1(3,15)$ over F. It is a curve of genus 9, $J_X(F)$ is finite [DS17, Theorem 4.1], and $\mathrm{gon}_F X \geq 6$ [NV26, Table 1]. As in [Naj26d, Lemma 5.4] we use the normal form $y^2 + a_1 xy + a_3 y = x^3$, in which $P = (0,0)$ has order 3, and we write Q for the point of order 15. The cusps are defined over $\mathbb{Q}(\zeta_{15}) = F(\zeta_5)$, and the 20 Galois orbits of cusps over F have degrees $1^{16}, 4^4$. We identify them with their reductions at the primes of F above 2 and 7 using the valuations of integral modular units, as in the proof of [Naj26d, Lemma 5.4]. Modulo the prime above 7 these orbits stay irreducible, and modulo the prime above 2, whose residue field is $\mathbb{F}_4$, each orbit of degree 4 splits into two closed cusps of degree 2.

Put $Q_3 = 5Q$ and $Q_5 = 3Q$, of orders 3 and 5. The level automorphisms of X defined over F are the maps

$$(P,Q) \longmapsto \big(\alpha P + \beta Q_3,\ 2(\gamma P + \delta Q_3) + 2\varepsilon Q_5\big), \qquad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_3), \quad \varepsilon \in \mathbb{F}_5^\times, \quad (11.5)$$

taken modulo ± 1, and they form a group $G_{3,15} \simeq (\mathrm{SL}_2(\mathbb{F}_3) \times \mathbb{F}_5^\times)/\langle(-I,-1)\rangle$ of order 48 (see [Naj26d, proof of Proposition 13.23], where the representatives with $\varepsilon \in \{1,2\}$ are used).

Lemma 11.8. *Let $F = \mathbb{Q}(\zeta_3)$ and $X = X_1(3,15)$ over F. Then*

$$J_X(F) = \mathrm{Cl}_F^c X \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/96\mathbb{Z} \times \mathbb{Z}/96\mathbb{Z},$$

and reduction modulo the prime of F above 2 is injective on $J_X(F)$.

Proof. By [Naj26d, Lemma 5.4], $\mathrm{Cl}^c_F X$ has these invariant factors, $J_X(F)/\mathrm{Cl}^c_F X$ has order dividing 3, and reduction modulo the prime $\mathfrak{p}$ of F above 2 is injective on $J_X(F)$. It remains to show that $J_X(F)[3^\infty] \subseteq \mathrm{Cl}^c_F X$.

We compute that $J_X(\mathbb{F}_4) \simeq (\mathbb{Z}/3\mathbb{Z})^3 \times \mathbb{Z}/24\mathbb{Z} \times (\mathbb{Z}/96\mathbb{Z})^2$, so its 3-primary part is $(\mathbb{Z}/3\mathbb{Z})^6$, and that the classes $[\overline{C} - \deg(\overline{C})\overline{c_*}]$ of the closed cusps $\overline{C}$ of $X_{\mathbb{F}_4}$ generate a subgroup whose 3-primary part is all of $(\mathbb{Z}/3\mathbb{Z})^6$. Let $L_0 \subseteq F(\zeta_5)$ be the quadratic extension of F. As 4 has order 2 modulo 5, the decomposition group of a prime of $F(\zeta_5)$ above $\mathfrak{p}$ is $\mathrm{Gal}(F(\zeta_5)/L_0)$, so $\mathfrak{p}$ splits in L_0 into two primes with residue field $\mathbb{F}_4$. Let λ be one of them. As in the proof of Lemma 2.6, every closed cusp of $X_{\mathbb{F}_4}$ is the reduction modulo λ of an L_0-rational cuspidal divisor of the same degree. Let $C_1, \dots, C_r$ be such lifts of all the closed cusps, let c_* be an F-rational cusp, and let N be the prime-to-3 part of the order of the subgroup of $J_X(L_0)$ generated by the classes $y_i = [C_i - \deg(C_i)c_*]$, which are torsion by the Manin-Drinfeld theorem. The reductions of the classes Ny_i generate the 3-primary part of $J_X(\mathbb{F}_4)$.

Let $y \in J_X(F)[3^\infty]$. As reduction modulo λ is injective on the torsion of odd order of $J_X(L_0)$ (the kernel of reduction is the group of points of a formal group over a 2-adic ring, which has no torsion of odd order), and the 3-primary part of $J_X(\mathbb{F}_4)$ is killed by 3, we have $3y = 0$, and $y = \sum_i n_i N y_i$ for some integers n_i. Let σ be the non-trivial element of $\mathrm{Gal}(L_0/F)$. As y is F-rational,

$$2y = y + \sigma(y) = \sum_i n_i N\,[C_i + \sigma(C_i) - 2\deg(C_i)c_*],$$

and the divisors $C_i + \sigma(C_i)$ are F-rational and cuspidal. So $2y \in \mathrm{Cl}^c_F X$, and as $3y = 0$, also $y = -2y \in \mathrm{Cl}^c_F X$. □

Lemma 11.9. *Let $F = \mathbb{Q}(\zeta_3)$, let $X = X_1(3,15)$ over F, and fix an F-rational cusp c_*. Let D be an effective F-rational divisor of degree 5 on X whose support contains no cusp. Then $[D - 5c_*]$ is one of 48 explicit elements of $\mathrm{Cl}^c_F X$.*

Proof. We consider the reductions D_2 and D_7 of D modulo the primes $\mathfrak{p}_2$ and $\mathfrak{p}_7$ of F above 2 and 7, with residue fields $\mathbb{F}_4$ and $\mathbb{F}_7$. We compute that the numbers of non-cuspidal closed points of degrees $1, \dots, 5$ are $0, 0, 0, 102, 192$ on $X_{\mathbb{F}_4}$ and $0, 24, 144, 396, 3312$ on $X_{\mathbb{F}_7}$. Modulo $\mathfrak{p}_2$ we allow all the effective divisors of degree 5: there are 22608 cuspidal ones, $102 \cdot 16$ which are a point of degree 4 plus one of the 16 cusps of degree 1, and the 192 points of degree 5, 24432 in all. Modulo $\mathfrak{p}_7$ the reduction is not cuspidal by Proposition 2.5 a), as $\mathrm{gon}_F X > 5$. So D_7 is a point of degree 2, 3, 4 or 5 plus an effective cuspidal divisor of the complementary degree, which gives 19584, 19584, 6336 and 3312 possibilities, or a sum of two points of degree 2 (possibly equal) and a cusp of degree 1, which gives 4800 possibilities, or the sum of a point of degree 2 and a point of degree 3, which gives 3456 possibilities. This makes 57072 possibilities for D_7.

By Lemma 11.8, the class $y = [D - 5c_*]$ lies in $\mathrm{Cl}^c_F X$, and its reductions modulo $\mathfrak{p}_2$ and $\mathfrak{p}_7$ are $[D_2 - 5\overline{c_*}]$ and $[D_7 - 5\overline{c_*}]$. We compute, for all the pairs (D_2, D_7) above, whether there is an element of $\mathrm{Cl}^c_F X$ whose reductions are these two classes, and find that this leaves 240 elements of $\mathrm{Cl}^c_F X$ for y.

By [Naj26d, Proposition 13.23 and its proof] there is a closed point A_0 of degree 4 on X, coming from an elliptic curve over an octic field, whose orbit under $G_{3,15}$ consists of 12 closed points $A_1, \dots, A_{12}$ of degree 4 (see `exclusions/315d5/M3N15_D4_exact_cusp_lifts.txt` for their classes). We compute that 192 of the 240 elements above are the classes $[A_i + c - 5c_*]$, where c runs over the 16 F-rational cusps. If y is one of them, then $D \sim A_i + c$, so $D = A_i + c$

by Lemma 2.8, as $\mathrm{gon}_F X > 5$. This is impossible, as the support of D contains no cusp. So y is one of the remaining 48 elements. □

Proposition 11.10. *Let $F = \mathbb{Q}(z)$ with $z^2 + z + 1 = 0$, let w be a root of*

$$w^5 + 13(z+1)w^4 - (24z+22)w^3 + 4(z+1)w^2 + (z+4)w + z + 1,$$

and put $K_{3,15} = F(w)$, which is the field 10.0.306454347.1. Let

$$q = \frac{(293z+23)w^2 + (105-238z)w + 357 - 28z}{217w^2 + (603z+271)w + 283 + 86z}$$

and

$$E_{3,15}: \quad y^2 + \big((1+q)w + 2 - q\big)xy + \big(qw^2 + (1-q)w\big)y = x^3.$$

a) *We have $E_{3,15}(K_{3,15})_{\mathrm{tors}} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$. The points $P = (0,0)$ and $Q = (-w, w^2)$ have orders 3 and 15, and $e_3(P, 5Q) = z^2$. The j-invariant of $E_{3,15}$ has degree 5 over $\mathbb{Q}$ and is not an algebraic integer.*

b) *Every effective F-rational divisor of degree 5 on $X_1(3,15)$ whose support contains no cusp is one of the 48 closed points of degree 5 in the orbit under $G_{3,15}$ of the trace divisor $D_{3,15}$ of $(E_{3,15}, P, Q)$.*

c) *If E is an elliptic curve over a number field K of degree 10 with $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \subseteq E(K)$, then (K, E) is isomorphic to $(K_{3,15}, E_{3,15})$, and $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$.*

Proof. We compute that the quintic polynomial is irreducible over F, that P and Q have orders 3 and 15, and that $e_3(P, 5Q) = z^2$, so $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \subseteq E_{3,15}(K_{3,15})$. The prime of $K_{3,15}$ given by $z \mapsto 6$, $w \mapsto 28$ has residue field $\mathbb{F}_{43}$ and is unramified, and the curve has good reduction $y^2 + 36xy + 24y = x^3$ there, with group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$. As reduction at an odd unramified prime is injective on the torsion, this proves the first claim of a). The same computation gives the minimal polynomial of $j(E_{3,15})$ over F, which has rational, non-integral coefficients and degree 5. The computation uses an expression of q as a polynomial in w, and we check that it is equal to the formula above.

We prove b). As $j(E_{3,15})$ is a function on X and has degree 5 over F, the residue field of the point $(E_{3,15}, P, Q)$ is $F(j(E_{3,15})) = K_{3,15}$, so $D_{3,15}$ is a closed point of degree 5. If $S \subseteq G_{3,15}$ is its stabilizer, then $\#S$ divides 5 by Lemma 2.9, as $E_{3,15}$ has no complex multiplication by Lemma 2.14, and $\#S$ divides 48. So S is trivial, and the orbit of $D_{3,15}$ consists of 48 distinct closed points of degree 5. By Lemma 2.8 their classes $[gD_{3,15} - 5c_*]$ are distinct, and by Lemma 11.9 they are among the 48 elements of $\mathrm{Cl}^{\mathrm{c}}_F X$ of that lemma, so they are all of them. Now let D be as in b). By Lemma 11.9, $D \sim gD_{3,15}$ for some $g \in G_{3,15}$, and $D = gD_{3,15}$ by Lemma 2.8.

Part c) follows from a), b) and Lemma 11.1 as in the proof of Proposition 11.7 c), using the Weil pairing $e_3(P', 5Q') = z^2$. □

Corollary 11.11. *The groups $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/45\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over a number field of degree 10.*

Proof. Both groups contain $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$, so by Proposition 11.10 c) such a curve would have torsion group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$. □

Remark 11.12. The 5 conjugates of $j(E_{3,15})$ give 5 elliptic curves over $\overline{\mathbb{Q}}$ which are pairwise not isomorphic, but by Proposition 11.10 they all come from the single pair $(K_{3,15}, E_{3,15})$.

11.3. **The curve $X_1(3,18)$.** Let $F=\mathbb{Q}(\zeta_3)$ and $X=X_1(3,18)$ over F, a curve of genus 10 with $J_X(F)$ finite [DS17, Theorem 4.1] and $\mathrm{gon}_F X\geq 6$ [NV26, Table 1]. We use the model of [Naj26d, Section 12.4], on which the universal curve is $y^2+a_1xy+a_3y=x^3$ with $P=(0,0)$ of order 3, normalized by $y(Q)=x(Q)^2$ for the point Q of order 18. We work at primes $\mathfrak{p}_7$ and $\mathfrak{p}_{13}$ of F above 7 and 13, with residue fields $\mathbb{F}_7$ and $\mathbb{F}_{13}$. As in [Naj26d, Section 12.4], at both primes the closed cusps have degrees $1^{18},3^6$, every closed cusp is the reduction of a Galois orbit of cusps over F of the same degree, and we identify these orbits at the two primes using the valuations of integral modular units. Reduction modulo $\mathfrak{p}_7$ and modulo $\mathfrak{p}_{13}$ is injective on $J_X(F)$ by Katz's result.

The level automorphisms of X defined over F are the maps

$$(P,Q)\longmapsto(\alpha P+6\beta Q,\ \gamma P+\delta Q),\qquad \beta,\gamma\in\mathbb{Z}/3\mathbb{Z},\quad \delta\in(\mathbb{Z}/18\mathbb{Z})^\times,\quad \alpha\equiv\delta^{-1}\pmod 3, \tag{11.6}$$

taken modulo ±1, so that we may take $\delta\in\{1,5,7\}$. They form a group $G_{3,18}$ of order 27 (these are the automorphisms of [Naj26d, proof of Proposition 12.5]). Every element of $G_{3,18}$ fixes the point $9Q$ of order 2. If $g\neq1$ fixed a geometric non-cuspidal point (E,P,Q) in characteristic 0 or $p\geq5$, it would be induced by an automorphism u of E whose image in $\mathrm{Aut}(E)/\{\pm1\}$ is non-trivial of order dividing 27, hence of order 3, and such a u fixes no non-zero point T of order 2: replacing u by $-u$, which acts in the same way on $E[2]$, we may assume that $u^2+u+1=0$, and then $uT=T$ gives $3T=0$. So $G_{3,18}$ acts freely on the non-cuspidal geometric points of X, also those with complex multiplication, and of $X_{\mathbb{F}_7}$ and $X_{\mathbb{F}_{13}}$.

We also need an involution of X which is not a level automorphism. For a point (E,P,Q) of $Y_1(3,18)$ let $\phi:E\to E'=E/\langle 9Q\rangle$ and let T' be the point of order 2 in the kernel of the dual isogeny. Then

$$\tau(E,P,Q)=(E',\ \phi(P),\ 2\phi(Q)+T') \tag{11.7}$$

defines an involution τ of X over F: the point $2\phi(Q)+T'$ has order 18, the Weil pairing is raised to the power $2\deg\phi=4\equiv1\pmod 3$, and $\tau^2(E,P,Q)=(E,-P,-Q)$.

Lemma 11.13. *Let $F=\mathbb{Q}(\zeta_3)$, $X=X_1(3,18)$ over F, and let $\mathfrak{p}_7$ be a prime of F above 7.*

a) *We have $J_X(\mathbb{F}_7)\simeq(\mathbb{Z}/3\mathbb{Z})^3\times(\mathbb{Z}/9\mathbb{Z})^2\times(\mathbb{Z}/63\mathbb{Z})^2\times\mathbb{Z}/189\mathbb{Z}$ and $\mathrm{Cl}^c_F X\simeq(\mathbb{Z}/3\mathbb{Z})^4\times(\mathbb{Z}/63\mathbb{Z})^3$, of order 20253807.*

b) *The common kernel of A_{13} and A_{19} on $J_X(\mathbb{F}_7)$ contains the reduction of $\mathrm{Cl}^c_F X$, with quotient isomorphic to $(\mathbb{Z}/3\mathbb{Z})^3$. In particular $3J_X(F)\subseteq\mathrm{Cl}^c_F X$.*

c) *The numbers of non-cuspidal closed points of degrees $1,\dots,5$ are $0,27,144,513,3672$ on $X_{\mathbb{F}_7}$ and $0,54,846,7506,75384$ on $X_{\mathbb{F}_{13}}$. The numbers of orbits of $G_{3,18}$ on them in degrees $2,\dots,5$ are $1,8,19,136$ on $X_{\mathbb{F}_7}$ and $2,38,278,2792$ on $X_{\mathbb{F}_{13}}$.*

Proof. The invariants of $\mathrm{Cl}^c_F X$ are also given in [Naj26d, Section 12.4]. We compute $J_X(\mathbb{F}_7)$ and the reduction of $\mathrm{Cl}^c_F X$. As 13 and 19 are $\equiv1\pmod 3$, the operators A_{13} and A_{19} annihilate $J_X(F)$ and the F-rational cuspidal divisors by Proposition 2.2. We compute their common kernel on $J_X(\mathbb{F}_7)$, and as in the proof of Lemma 11.2 c) the injectivity of reduction gives $3J_X(F)\subseteq\mathrm{Cl}^c_F X$. We compute the numbers of closed points from the zeta functions of $X_{\mathbb{F}_7}$ and $X_{\mathbb{F}_{13}}$, and the numbers of orbits by enumerating the closed points at 7 and at 13 (in degree 5 at 13 see `computations/d31b_m318_p13_lean_s0.m`). □

We use the following formal argument, which replaces Lemma 2.10 when the gonality is too small for it. Let $p\in\{7,13\}$, let $R=\mathbb{Z}_p$ be the completion of the ring of integers of F at $\mathfrak{p}_p$, and let h be an automorphism of X over F which maps cusps to cusps. We denote by

$\alpha = h_* - 1$ the induced endomorphism of J_X. Recall that the cotangent space of $X^{(5)}_{\mathbb{F}_p}$ at an effective divisor $\overline{D}$ is $H^0(\overline{D}, \Omega^1|_{\overline{D}})$, and that, after identifying the cotangent space of J_X at 0 with $H^0(X_{\mathbb{F}_p}, \Omega^1)$, the cotangent map at $\overline{D}$ of the map $X^{(5)} \to J_X$, $Z \mapsto [\alpha(Z)] = [hZ - Z]$, is $\omega \mapsto ((h^* - 1)\omega)|_{\overline{D}}$.

Lemma 11.14. *Let $F = \mathbb{Q}(\zeta_3)$, $X = X_1(3,18)$ over F, $p \in \{7, 13\}$, and let h be an automorphism of X over F of order $r \in \{2, 3\}$ which maps cusps to cusps and extends to the smooth model of X over $R = \mathbb{Z}_p$. Let $\overline{N}$ be a non-cuspidal effective divisor on $X_{\mathbb{F}_p}$ with $h\overline{N} = \overline{N}$ such that h acts freely on the geometric points of $\overline{N}$, and let $\overline{C}$ be an effective cuspidal divisor on $X_{\mathbb{F}_p}$ which is the reduction of an F-rational cuspidal divisor C, with $\deg \overline{N} + \deg \overline{C} = 5$. Let $Y = X/\langle h \rangle$ and $\pi : X \to Y$ the quotient map, and assume that*

a) *$\overline{N} = \pi^*(\overline{M})$ for an effective divisor $\overline{M}$ on $Y_{\mathbb{F}_p}$ of degree $k = \deg \overline{N}/r$, which is a sum of k distinct points or a single closed point of degree k, and*
b) *the restriction map $(h^* - 1)H^0(X_{\mathbb{F}_p}, \Omega^1) \to H^0(\overline{N} + \overline{C}, \Omega^1|_{\overline{N}+\overline{C}})$ has rank $5 - k$.*

Then no effective F-rational divisor D of degree 5 on X whose support contains no cusp reduces to $\overline{N} + \overline{C}$ modulo $\mathfrak{p}_p$.

Proof. Suppose that D reduces to $\overline{N} + \overline{C}$. As h acts freely on the points of $\overline{N}$, it acts freely on a neighbourhood of them in the smooth model of X over R, so π is étale there and Y is smooth over R at the support of $\overline{M}$. Hence $\overline{M}$ lifts to an effective divisor M on Y over R of the same shape. The class

$$y = [hD - D - hC + C] \in J_X(F)$$

is torsion, as $J_X(F)$ is finite, and its reduction is $[h\overline{N} - \overline{N}] = 0$. As p is odd and unramified in F, $y = 0$ by Katz's result. So D lies in the fibre $V = \{Z : [hZ - Z - hC + C] = 0\}$ of the map $X^{(5)}_R \to J_{X,R}$ over 0. For every effective divisor M' on Y in a formal neighbourhood of M, the divisor $C + \pi^*M'$ lies in V, as π^*M' is h-invariant. These divisors form a closed formal subscheme W of V through $\overline{N} + \overline{C}$ which is smooth of relative dimension k over R, as M' is determined by π^*M', and π is étale at the points of $\overline{N}$, whose support is disjoint from that of $\overline{C}$. On the other hand, by b) and the description of the cotangent map above, the formal neighbourhood of $\overline{N} + \overline{C}$ in V is contained in the zero locus of $5 - k$ functions on the formal neighbourhood of $\overline{N} + \overline{C}$ in $X^{(5)}_R$ (which is smooth of relative dimension 5 over R) with linearly independent differentials. This zero locus is formally smooth of relative dimension k over R and integral, and it contains W, which has the same dimension, so it equals W. So $D = C + \pi^*M'$ for some M', and the support of D contains the cusps in the support of C, which is a contradiction. □

Lemma 11.15. *Let $F = \mathbb{Q}(\zeta_3)$, $X = X_1(3,18)$ over F, $p \in \{7, 13\}$, and let $\mathfrak{p}_p$ be a prime of F above p. Let $\overline{N}$ be a non-cuspidal closed point of degree 3 of $X_{\mathbb{F}_p}$ whose orbit under $G_{3,18}$ has length 9, and let $\overline{C}$ be an effective cuspidal divisor of degree 2 on $X_{\mathbb{F}_p}$. Then no effective F-rational divisor of degree 5 on X whose support contains no cusp reduces to $\overline{N} + \overline{C}$ modulo $\mathfrak{p}_p$.*

Proof. As the closed cusps of $X_{\mathbb{F}_p}$ have degrees 1 and 3, the divisor $\overline{C}$ is a sum of cusps of degree 1, and it is the reduction of an F-rational cuspidal divisor, as every closed cusp is the reduction of a Galois orbit of cusps over F of the same degree. There are $\binom{19}{2} = 171$ such divisors. If D reduces to $\overline{N} + \overline{C}$, then gD reduces to $g\overline{N} + g\overline{C}$ for every $g \in G_{3,18}$,

so we may assume that $\overline{N}$ is one of the orbit representatives of Lemma 11.13 c). As $G_{3,18}$ acts freely on the non-cuspidal geometric points of $X_{\mathbb{F}_p}$, the stabilizer of a closed point of degree 3 acts freely on its 3 geometric points, so the orbits of these points have length 9 or 27, and by the numbers in Lemma 11.13 c), 4 of the 8 orbits at 7 and 10 of the 38 orbits at 13 have length 9. The stabilizer of $\overline{N}$ in $G_{3,18}$ has order 3. Let h be a generator of it. Then h permutes the 3 geometric points of $\overline{N}$ freely, so $\overline{N}$ is the fibre of $X \to X/\langle h\rangle$ over a point of degree 1. As a level automorphism, h maps cusps to cusps and extends to the smooth model of X over $\mathbb{Z}_p$. We compute that the assumption b) of Lemma 11.14, with $r = 3$ and $k = 1$, holds in all the $4 \cdot 171 = 684$ cases at 7, and in all the $10 \cdot 171 = 1710$ cases at 13, so Lemma 11.14 gives the claim. □

Lemma 11.16. *Let $F = \mathbb{Q}(\zeta_3)$, $X = X_1(3,18)$ over F, and let $\mathfrak{p}_7$ be a prime of F above 7. Let $\overline{N}_{12}$ and $\overline{N}_{17}$ be the representatives number 12 and 17 of the 19 orbits of $G_{3,18}$ on the non-cuspidal closed points of degree 4 of $X_{\mathbb{F}_7}$ listed in `continuation_20261031b/M3N18/paired_p7_degree4_data.m`. Let $i \in \{12, 17\}$, $g \in G_{3,18}$, and let $\overline{c}$ be a cusp of $X_{\mathbb{F}_7}$ of degree 1. Then no effective F-rational divisor of degree 5 on X whose support contains no cusp reduces to $g(\overline{N}_i + \overline{c})$ modulo $\mathfrak{p}_7$.*

Proof. Suppose that D is such a divisor. Replacing D by $g^{-1}D$, we may assume that $g = 1$. The points $\overline{N}_{12}$ and $\overline{N}_{17}$ are fixed by the involutions $h_{12} = g_{12}^{-1}\tau g_{12}$ and $h_{17} = g_{17}^{-1}\tau g_{17}$ respectively, where $g_{12}(P,Q) = (P + 12Q, Q)$ and $g_{17}(P,Q) = (P + 12Q, P + Q)$, which act on their residue field $\mathbb{F}_{7^4}$ as the square of the Frobenius, as we compute (see also `computations/d31b_m318_tau_frame_p7.m` for τ). As τ is defined by an isogeny of degree 2, the involutions h_i map cusps to cusps and extend to the smooth model of X over $\mathbb{Z}_7$. So h_i acts freely on the geometric points of $\overline{N}_i$, and $\overline{N}_i = \pi^*(\overline{M}_i)$ for a closed point $\overline{M}_i$ of degree 2 of $X/\langle h_i\rangle$, where π is the quotient map. The cusp $\overline{c}$ is the reduction of an F-rational cusp. The space $(h_i^* - 1)H^0(X_{\mathbb{F}_7}, \Omega^1)$ has dimension 6, and we compute (and for $\overline{N}_{17}$) that its restriction to $\overline{N}_i + \overline{c}$ has rank 3 for each of the 18 cusps $\overline{c}$ of degree 1. So Lemma 11.14, with $r = 2$ and $k = 2$, gives a contradiction. □

Lemma 11.17. *Let $F = \mathbb{Q}(\zeta_3)$, $X = X_1(3,18)$ over F, and let D be an effective F-rational divisor of degree 5 on X whose support contains no cusp. Then there are $g \in G_{3,18}$ and $i \in \{1,2\}$ with $gD \sim A_i$, where A_1 and A_2 are the F-rational cuspidal divisors of degree 5 given in `jobs/d31b_m318_short_cusp_divisors.log` (see also `continuation_20261031b/M3N18/endomorphism_gluing/short_cusp_divisors.m`).*

Proof. Fix an F-rational cusp c_*. As $\operatorname{gon}_F X \geq 6 > 5$, by Proposition 2.5 a) the reductions of D modulo $\mathfrak{p}_7$ and $\mathfrak{p}_{13}$ are not cuspidal. By Lemma 11.13 c), the non-cuspidal part of each of them is a closed point of degree $2, \dots, 5$ or a sum of two points of degree 2 (possibly equal) or of a point of degree 2 and a point of degree 3, and its cuspidal part is an effective cuspidal divisor of the complementary degree, which may contain cusps of degree 3. Applying an element of $G_{3,18}$, we may assume that at $\mathfrak{p}_7$ the first point of the non-cuspidal part is one of the orbit representatives of Lemma 11.13 c), and we do the same separately at $\mathfrak{p}_{13}$. This gives the following numbers of cases, according to the type of the non-cuspidal part.

p	[2]	[3]	[4]	[5]	[2, 2]	[2, 3]	total
7	1146	1368	342	136	486	144	3622
13	2292	6498	5004	2792	1944	1692	20222

By the Hecke sieve (Section 2.5), with $q = 13$ and $q = 19$, which are admissible for every cuspidal part as every closed cusp is the reduction of an F-rational cuspidal divisor of the

same degree, the class of the reduction modulo $\mathfrak{p}_7$ of $D - 5c_*$ lies in the common kernel of A_{13} and A_{19}. By Lemma 11.15, the cases of a point of degree 3 in an orbit of length 9 with a cuspidal part, $4 \cdot 171 = 684$ at $\mathfrak{p}_7$ and $10 \cdot 171 = 1710$ at $\mathfrak{p}_{13}$, do not occur. We compute that the Hecke sieve and these exclusions leave 242 of the 3622 cases at $\mathfrak{p}_7$. Here, for the types $[2,2]$ and $[2,3]$, we use the classes of all the closed points of degree 2 and 3 of $X_{\mathbb{F}_7}$ and $X_{\mathbb{F}_{13}}$, not only those of the orbit representatives, which we compute from the model of X.

By Lemma 11.13 b), the class $v = 3[D - 5c_*]$ lies in $\mathrm{Cl}^c_F X$, so its reductions modulo $\mathfrak{p}_7$ and $\mathfrak{p}_{13}$ are the reductions of the same element of $\mathrm{Cl}^c_F X$. As we normalized the reductions by $G_{3,18}$ at the two primes separately, we compare each case at $\mathfrak{p}_{13}$ with the 27 translates of each of the 242 cases at $\mathfrak{p}_7$, computing the action of $G_{3,18}$ on the classes from its action on the cusps. We find that only 78 of the cases at $\mathfrak{p}_{13}$ admit such a match, with 53 distinct non-cuspidal parts $\overline{N}$. For these we use the Hecke sieve at $\mathfrak{p}_{13}$ with $q = 7$: as 7 is admissible for every cuspidal part, $A_7\overline{N}$ has to be principal, and we compute that it is not for 43 of the 53 divisors $\overline{N}$. The remaining 10 give 12 cases at $\mathfrak{p}_{13}$. The cases at $\mathfrak{p}_7$ which match them are of type $[4]$, with a point in the orbit of $\overline{N}_{12}$ or of $\overline{N}_{17}$ plus a cusp of degree 1, which Lemma 11.16 excludes, or one of two cases of type $[2,3]$.

There remain 4 pairs of cases at $\mathfrak{p}_7$ and $\mathfrak{p}_{13}$, with 2 cases of type $[2,3]$ at $\mathfrak{p}_7$. For both of these, we compute that the class of the reduction of $D - 5c_*$ itself (not only its multiple by 3) lies in the reduction of $\mathrm{Cl}^c_F X$, so by the injectivity of reduction $[D - 5c_*] \in \mathrm{Cl}^c_F X$. Comparing the classes $[D - 5c_*]$ at the two primes, with the action of $G_{3,18}$ on the cusps taken into account, two of the 4 pairs are excluded, as their classes at $\mathfrak{p}_{13}$ do not lie in the reduction of $\mathrm{Cl}^c_F X$, and the other two give the classes $[A_1 - 5c_*]$ and $[A_2 - 5c_*]$. By injectivity, $gD \sim A_1$ or $gD \sim A_2$ for some $g \in G_{3,18}$. □

Proposition 11.18. *Let $F = \mathbb{Q}(\zeta_3)$, let u be a root of*

$$3u^5 + (1 + 5\zeta_3)u^4 + (6\zeta_3 - 3)u^3 - (6\zeta_3 + 9)u^2 - (5\zeta_3 + 4)u + 3,$$

and put $K_{3,18} = F(u)$, which is the field 10.0.2571428187.1. Let

$$19t = (4\zeta_3 - 25)u^4 + (12 - 65\zeta_3)u^3 + (20 + 31\zeta_3)u^2 + (69 + 30\zeta_3)u + 3\zeta_3 - 33,$$

$$E_{3,18}: \quad y^2 + \big((u+2)t + 1 - u\big)xy + \big((u+1)t^2 - ut\big)y = x^3,$$

$P = (0,0)$, $Q = (-t, t^2)$, and let $E'_{3,18} = E_{3,18}/\langle 9Q \rangle$.

a) *The points P and Q have orders 3 and 18 and generate a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$, and $E_{3,18}(K_{3,18})_{\mathrm{tors}} \simeq E'_{3,18}(K_{3,18})_{\mathrm{tors}} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$. The j-invariants of $E_{3,18}$ and $E'_{3,18}$ have degree 5 over $\mathbb{Q}$, they are not algebraic integers, and their minimal polynomials over $\mathbb{Q}$ are different.*

b) *Every effective F-rational divisor of degree 5 on $X_1(3,18)$ whose support contains no cusp is one of the 54 closed points of degree 5 in the two orbits under $G_{3,18}$ of the trace divisor $D_{3,18}$ of $(E_{3,18}, P, Q)$ and of $\tau(D_{3,18})$, each of which has 27 elements.*

c) *If E is an elliptic curve over a number field K of degree 10 with $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z} \subseteq E(K)$, then the pair (K, E) is isomorphic to $(K_{3,18}, E_{3,18})$ or to $(K_{3,18}, E'_{3,18})$, and $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$. These two pairs are not isomorphic.*

Proof. We compute that the quintic polynomial is irreducible over F, that P and Q have orders 3 and 18, and that their Weil pairing is primitive, so $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z} \subseteq E_{3,18}(K_{3,18})$. The image of (P, Q) under the isogeny gives $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z} \subseteq E'_{3,18}(K_{3,18})$, as in (11.7). We compute that an absolute defining polynomial of $K_{3,18}$ is squarefree modulo 7, with irreducible factors of degrees $2, 2, 3, 3$, and that at the two primes of $K_{3,18}$ of residue degree

2 above 7 both curves have good reduction with 54 points over $\mathbb{F}_{49}$. As 7 is odd and unramified in $K_{3,18}$, the torsion of both curves has order dividing 54. We compute the minimal polynomials of $j(E_{3,18})$ and $j(E'_{3,18})$, which proves the rest of a).

We prove b). As $j(E_{3,18})$ has degree 5 over $\mathbb{Q}$ and $[F:\mathbb{Q}]=2$, it has degree 5 over F. The residue field of the point $(E_{3,18},P,Q)$ contains $F(j(E_{3,18}))$ and is contained in $K_{3,18}$, so it is $K_{3,18}$, and $D_{3,18}$ is a closed point of degree 5. As τ is an automorphism of X over F which maps cusps to cusps, $\tau(D_{3,18})$ is a closed point of degree 5 whose support contains no cusp, and its elliptic curve is $E'_{3,18}$. By Lemma 11.17 there are $g_1,g_2\in G_{3,18}$ and $i_1,i_2\in\{1,2\}$ with $g_1D_{3,18}\sim A_{i_1}$ and $g_2\tau(D_{3,18})\sim A_{i_2}$. If $i_1=i_2$, then $g_1D_{3,18}=g_2\tau(D_{3,18})$ by Lemma 2.8, as $\operatorname{gon}_F X\geq 6>5$, and as the level automorphisms do not change the elliptic curve, $j(E_{3,18})$ and $j(E'_{3,18})$ would be conjugate, which contradicts a). So $\{i_1,i_2\}=\{1,2\}$. Now let D be as in b). By Lemma 11.17 there are $g\in G_{3,18}$ and $i\in\{1,2\}$ with $gD\sim A_i$, so gD is linearly equivalent, and by Lemma 2.8 equal, to $g_1D_{3,18}$ or to $g_2\tau(D_{3,18})$. By Lemma 2.9, as $E_{3,18}$ and $E'_{3,18}$ have no complex multiplication by Lemma 2.14, the stabilizers of $D_{3,18}$ and of $\tau(D_{3,18})$ in $G_{3,18}$ have order dividing $\gcd(27,5)=1$, so both orbits have 27 elements. As the level automorphisms do not change the elliptic curve, and the j-invariants of $E_{3,18}$ and $E'_{3,18}$ are not conjugate by a), the two orbits are distinct.

Part c) follows from a), b) and Lemma 11.1, applied to the point $(E_{3,18},P,Q)$ and to its image under τ, as in the proof of Proposition 11.7 c). As the minimal polynomials of $j(E_{3,18})$ and $j(E'_{3,18})$ are different, no field automorphism maps one to the other, so the two pairs are not isomorphic. □

Corollary 11.19. *The groups $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/36\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/18\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over a number field of degree* 10.

Proof. Both groups contain $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/18\mathbb{Z}$, so by Proposition 11.18 c) the torsion group of such a curve would be $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/18\mathbb{Z}$, of order 54. □

Remark 11.20. For the curve $X_1(3,18)$ over sextic and octic fields, where the trace divisor has degree 3 or 4, the stabilizer argument of Lemma 2.10 a) was enough to deal with the points of degree 3 fixed by an element of order 3 of $G_{3,18}$ (see the proof of [Naj26d, Proposition 12.5]). Here it would require $\operatorname{gon}_F X>7$, which is why we use Lemma 11.14 instead. Note also that the field $K_{3,18}$ has an automorphism which acts non-trivially on F (we compute that $\operatorname{Aut}(K_{3,18})$ has order 2 and that its non-trivial element does not fix ζ_3), so the last claim of Proposition 11.18 c) does not follow from b) alone.

11.4. **The curve $X_1(2,26)$.** Let $X=X_1(2,26)$ over $\mathbb{Q}$, a curve of genus 25. We use the normal form (11.2), with $P=(0,0)$ and $Q=(b,b)$. By [DEvH+21, Theorem 3.1(3), Proposition 4.16 and Table 3], $J_X(\mathbb{Q})\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/14\mathbb{Z}\times\mathbb{Z}/266\mathbb{Z}\times\mathbb{Z}/3990\mathbb{Z}\times\mathbb{Z}/11970\mathbb{Z}$ is generated by rational cuspidal divisor classes, and $\operatorname{gon}_{\mathbb{Q}} X\geq 12$ [NV26, Table 1]. As in the proof of [Naj26d, Proposition 13.22], the closed cusps of $X_{\mathbb{F}_3}$ have degrees $1^{18},3^6$, the 18 cusps of degree 1 are the reductions of the 18 rational cusps, and their differences generate the reduction of $J_X(\mathbb{Q})$, which is a subgroup of index 350 of

$$J_X(\mathbb{F}_3)\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/14\mathbb{Z}\times\mathbb{Z}/70\mathbb{Z}\times\mathbb{Z}/1330\mathbb{Z}\times\mathbb{Z}/3990\mathbb{Z}\times\mathbb{Z}/11970\mathbb{Z}$$

Reduction modulo 3 is injective on $J_X(\mathbb{Q})$ by Katz's result. The level automorphisms of X permute the three points of order 2 and act by $\Delta(13)$ on the point of order 13, and they form a group $G_{2,26}\simeq S_3\times\Delta(13)$ of order 36 (see [Naj26d, Section 11]). They are defined over $\mathbb{Q}$.

Lemma 11.21. *Let K be a number field of degree at most 10 and E/K an elliptic curve with $j(E) = 0$. Then $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z} \not\subseteq E(K)$.*

Proof. Suppose the opposite. Then E has a model $y^2 = x^3 - \lambda^3$ with $\lambda \in K^\times$, and as the other two roots $\lambda\zeta_3^{\pm 1}$ of $x^3 - \lambda^3$ lie in K, we have $F = \mathbb{Q}(\zeta_3) \subseteq K$, so $[K : F] \leq 5$. The curve E is the quadratic twist by λ of $E_0 : y^2 = x^3 - 1$, so the x-coordinate of a point of order 13 in $E(K)$, divided by λ, is the x-coordinate of a point of order 13 of E_0, and lies in K. So the 13-division polynomial of E_0 has a root of degree at most 5 over F. We compute that its irreducible factors over F have degrees $6, 6, 72$, which is a contradiction. □

Lemma 11.22. *Let $X = X_1(2, 26)$ and let D be an effective rational divisor of degree 10 on X whose support contains no cusp. Then there is $g \in G_{2,26}$ such that the reduction of gD modulo 3 is one of the following divisors, where $\overline{N_9}$, $\overline{N_5}$, $\overline{N_5'}$ and $\overline{N_{10}}$ are closed points of $X_{\mathbb{F}_3}$ of degrees 9, 5, 5 and 10 determined in the proof:*

a) $\overline{N_9} + \overline{c}$, *where $\overline{c}$ is a cusp of degree 1,*
b) $\overline{N_5} + \overline{N_5'}$,
c) $\overline{N_{10}}$.

Proof. As $\operatorname{gon}_{\mathbb{Q}} X \geq 12 > 10$, by Proposition 2.5 a) the reduction of D modulo 3 is not cuspidal. We compute that the numbers of non-cuspidal closed points of $X_{\mathbb{F}_3}$ of degrees $1, \dots, 10$ are $0, 0, 0, 0, 36, 122, 288, 936, 2328, 5382$ (the first nine are also in [Naj26d, Table 4]). So the reduction of D is $x + C'$, where x is a closed point of degree $e \in \{5, \dots, 10\}$ or a sum of two closed points of degree 5, and C' is an effective cuspidal divisor of degree $10 - \deg x$, which may contain cusps of degree 3. The 36 points of degree 5 form a single orbit under $G_{2,26}$, and the points of degrees $6, \dots, 10$ form 7, 8, 29, 66 and 154 orbits. Applying an element of $G_{2,26}$, we may assume that x, or its first summand of degree 5, is one of these 265 orbit representatives, which gives $265 + 36 = 301$ possibilities for x.

By Lemma 2.16, applied with the reduction of $J_X(\mathbb{Q})$, the class $[x + C' - 10\overline{c_*}]$ lies in the reduction of $J_X(\mathbb{Q})$, so a possibility for x can only occur if this holds for some effective cuspidal divisor C' of degree $10 - \deg x$ on $X_{\mathbb{F}_3}$. To speed up the computation, we first apply the analogous condition (2.1) to the push-forwards of x by the four maps $X \to X_1(26)$ of [Naj26d, Section 11], which keep Q or $P + Q$, or divide E by $\langle P \rangle$ or $\langle P + 13Q \rangle$ and keep the image of Q, with the reduction of $J_1(26)(\mathbb{Q})$, which is finite and generated by the rational cuspidal divisor classes [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2]. This leaves 32 of the 301 possibilities. For these we test the condition on X itself, allowing all the effective cuspidal divisors C' over $\mathbb{F}_3$, and find that only the three divisors in the statement satisfy it (see `continuation_20261029b/C226/picard_template.m` and the logs of the eight runs). □

Lemma 11.23. *Let $X = X_1(2, 26)$. No effective rational divisor D of degree 10 on X whose support contains no cusp reduces modulo 3 to the divisor $\overline{N_9} + \overline{c}$ of Lemma 11.22 a).*

Proof. Suppose the opposite. Let $g \in G_{2,26}$ be the level automorphism $(P, Q) \mapsto (13Q, P + 17Q)$. As $g^3(P, Q) = (-P, -Q)$, it has order 3 in $G_{2,26}$, and we compute that it fixes $\overline{N_9}$, on which it acts as the cube of the Frobenius. Let c be the rational cusp which reduces to $\overline{c}$. By Lemma 2.10 a), with $p = 3$, $C = c$ and $\operatorname{gon}_{\mathbb{Q}} X \geq 12 > 11$, we get $gD = D$.

If g fixed a geometric point (E, P, Q) in the support of D, there would be an automorphism u of E with $u(P, Q) = \pm g(P, Q)$, whose image in $\operatorname{Aut}(E)/\{\pm 1\}$ has order 3, so $j(E) = 0$. All the geometric points in the support of D are conjugate to a non-cuspidal point defined

over a number field of degree at most 10, over which, as X is a fine moduli space, its elliptic curve has a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$, so this is impossible by Lemma 11.21. So g acts freely on the geometric points in the support of D, and as $gD = D$, these points form orbits of length 3 on which the coefficients of D are constant. Hence $3 \mid \deg D = 10$, which is a contradiction. □

Let $K_{2,26} = \mathbb{Q}(a_1)$ and $K'_{2,26} = \mathbb{Q}(a_2)$, where a_1 and a_2 are roots of

$$F_1(x) = 2x^{10} + 11x^9 + 17x^8 - 7x^7 - 42x^6 - 20x^5 + 9x^4 + 9x^3 + 10x^2 + 6x + 1,$$
$$F_2(x) = x^{10} + 3x^9 - 3x^8 - 23x^7 - 26x^6 + 3x^5 + 13x^4 - 2x^3 - 9x^2 - 5x - 1,$$

which are the fields 10.6.396320664709.1 and 10.2.799905449.1. Put

$$b_1 = \frac{B_1(a_1)}{406832}, \qquad c_1 = \frac{C_1(a_1)}{203416}, \qquad b_2 = \frac{B_2(a_2)}{784}, \qquad c_2 = \frac{C_2(a_2)}{1960},$$

where the coefficients of the polynomials B_i and C_i are given in Table 8, and let $E_{2,26} = E'(b_1, c_1)$ over $K_{2,26}$ and $E'_{2,26} = E'(b_2, c_2)$ over $K'_{2,26}$ be the curves (11.2), with $P = (0, 0)$ and $Q = (b_i, b_i)$.

j	$[x^j]B_1$	$[x^j]C_1$	$[x^j]B_2$	$[x^j]C_2$
0	−621631	129155	−27507	90619
1	−2586377	551533	−95105	307177
2	−2555940	1269576	−100181	325777
3	−4632176	2528052	101187	−321491
4	2207386	1757370	190643	−622235
5	13819447	−2078127	−236919	755143
6	4462921	−1932589	−349828	1128928
7	−4689287	−133261	−76640	249316
8	−3688261	347217	41312	−133040
9	−721870	92982	17265	−55877

TABLE 8. The coefficients of the polynomials B_1, C_1, B_2, C_2 defining the curves $E_{2,26}$ and $E'_{2,26}$.

Proposition 11.24. *Let $K_{2,26}$, $K'_{2,26}$, $E_{2,26}$ and $E'_{2,26}$ be as above.*

a) *We have $E_{2,26}(K_{2,26})_{\mathrm{tors}} \simeq E'_{2,26}(K'_{2,26})_{\mathrm{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$, generated by P and Q. The j-invariants of $E_{2,26}$ and $E'_{2,26}$ have degree 5 over $\mathbb{Q}$, they are not algebraic integers, and their minimal polynomials over $\mathbb{Q}$ are different.*

b) *Every effective rational divisor of degree 10 on $X_1(2, 26)$ whose support contains no cusp is one of the 36 closed points of degree 10 in the orbits under $G_{2,26}$ of the trace divisors $D_{2,26}$ and $D'_{2,26}$ of $(E_{2,26}, P, Q)$ and $(E'_{2,26}, P, Q)$. Each of the two orbits has 18 elements.*

c) *If E is an elliptic curve over a number field K of degree 10 with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z} \subseteq E(K)$, then the pair (K, E) is isomorphic to $(K_{2,26}, E_{2,26})$ or to $(K'_{2,26}, E'_{2,26})$, and $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$.*

Proof. We compute that F_1 and F_2 are irreducible, that P and Q have orders 2 and 26 on both curves, and that $P \neq 13Q$, so $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z} \subseteq E_{2,26}(K_{2,26})$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z} \subseteq E'_{2,26}(K'_{2,26})$. At the prime of $K_{2,26}$ given by $a_1 \mapsto 23 \in \mathbb{F}_{41}$ and at the prime of $K'_{2,26}$ given by $a_2 \mapsto 39 \in \mathbb{F}_{43}$, which are unramified as the defining polynomials are separable modulo

41 and 43, the curves have good reduction, with $b_1 \mapsto 6$, $c_1 \mapsto 25$, respectively $b_2 \mapsto 21$, $c_2 \mapsto 11$, and 52 points. So both torsion groups have order 52. We compute the minimal polynomials of the j-invariants, which proves the rest of a).

We compute that $\mathbb{Q}(b_1, c_1) = K_{2,26}$ and $\mathbb{Q}(b_2, c_2) = K'_{2,26}$, so $D_{2,26}$ and $D'_{2,26}$ are closed points of degree 10 with these residue fields. Modulo 3, F_1 and F_2 factor into irreducible factors of degrees $5, 5$ and 10, and we compute, by evaluating b_i and c_i at the roots of these factors, that $D_{2,26}$ reduces to the divisor of Lemma 11.22 b) and $D'_{2,26}$ to the divisor of Lemma 11.22 c).

Now let D be as in b). By Lemmas 11.22 and 11.23, there is $g \in G_{2,26}$ such that gD and $D_{2,26}$, or gD and $D'_{2,26}$, have the same reduction modulo 3. Then $[gD - D_{2,26}]$, respectively $[gD - D'_{2,26}]$, lies in $J_X(\mathbb{Q})$ and reduces to 0, so it is 0, and $gD = D_{2,26}$, respectively $gD = D'_{2,26}$, by Lemma 2.8, as $\operatorname{gon}_{\mathbb{Q}} X \geq 12 > 10$. The two orbits are distinct, as the j-invariants are not conjugate. We compute that the reductions of $D_{2,26}$ and $D'_{2,26}$ are fixed by the elements $(P, Q) \mapsto (P, P+5Q)$ and $(P, Q) \mapsto (13Q, P+18Q)$ of $G_{2,26}$, respectively, which have order 2. By Lemma 2.10 a), with $C = 0$, these elements fix $D_{2,26}$ and $D'_{2,26}$. On the other hand, by Lemma 2.9, the stabilizers have order dividing $\gcd(36, 10) = 2$, as the curves have no complex multiplication by Lemma 2.14. So both stabilizers have order 2 and both orbits have 18 elements. This proves b), and c) follows from a), b) and Lemma 11.1, applied to the points $(E_{2,26}, P, Q)$ and $(E'_{2,26}, P, Q)$, as in the proof of Proposition 11.7 c). □

Proposition 11.25. *The group $\mathbb{Z}/52\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree* 10.

Proof. Suppose the opposite, and let E_0 be an elliptic curve over a number field K of degree 10 with a point R of order 52. Let $\phi : E_0 \to E = E_0/\langle 26R \rangle$. As in Lemma 4.3 (or the proof of [Naj26d, Proposition 11.16]), the point $\phi(R)$ has order 26 and is independent of the generator of the kernel of the dual isogeny $\widehat{\phi}$, as $\widehat{\phi}(13\phi(R)) = 26R \neq 0$, so $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z} \subseteq E(K)$. By Proposition 11.24 c), after replacing (K, E_0, E) by an isomorphic triple, we may assume that (K, E) is $(K_{2,26}, E_{2,26})$ or $(K'_{2,26}, E'_{2,26})$. Then $E_0 \simeq E/\ker\widehat{\phi}$, where $\ker\widehat{\phi}$ is one of the three subgroups of order 2 of E, and the kernel $\langle 26R \rangle$ of the dual of $E \to E/\ker\widehat{\phi}$ is generated by the point $26R = 2 \cdot 13R$, which is divisible by 2 in $E_0(K)$.

Let $r_0 = 0$, $r_1 = x(13Q)$ and $r_2 = -c_i - r_1$ be the x-coordinates of the points of order 2 of $E'(b_i, c_i)$, let $\{s, t, w\} = \{0, 1, 2\}$, and put $u = r_t - r_s$ and $v = r_w - r_s$. Moving $(r_s, 0)$ to $(0, 0)$, the curve becomes $y^2 = x(x-u)(x-v)$, and its quotient by $\langle (0,0) \rangle$ is

$$y^2 = x^3 + 2(u+v)x^2 + (u-v)^2 x,$$

on which the kernel of the dual isogeny is generated by $(0, 0)$. A point T with $2T = (0, 0)$ satisfies $x(T)^2 = (u-v)^2$, and $y(T)^2 = 4(u-v)^2 u$ if $x(T) = u-v$, and $y(T)^2 = 4(u-v)^2 v$ if $x(T) = v-u$. So $(0, 0)$ is divisible by 2 over K only if u or v is a square in K. We compute that none of the 6 differences $r_t - r_s$, $s \neq t$, is a square in $K_{2,26}$, respectively $K'_{2,26}$: their

residues at the degree 1 primes given in the following table are non-zero non-squares.

(s,t)	$K_{2,26}: \ p=41, \ a_1 \mapsto 23$	$K'_{2,26}: \ p=43$	
	$r_t - r_s$	$a_2 \mapsto$	$r_t - r_s$
$(0,1)$	38	16	33
$(0,2)$	19	39	18
$(1,0)$	3	39	29
$(1,2)$	22	16	19
$(2,0)$	22	16	34
$(2,1)$	19	39	39

As a square in K which is a unit at such a prime has a square residue, this is a contradiction. □

Remark 11.26. The points of $X_1(m,n)$ of degree d_m over $\mathbb{Q}(\zeta_m)$ found in this section are sporadic, as by the finiteness of $J_X(\mathbb{Q}(\zeta_m))$ and $\mathrm{gon}_{\mathbb{Q}(\zeta_m)} X > d_m$ the curve X has only finitely many points of degree at most d_m over $\mathbb{Q}(\zeta_m)$ (see the beginning of the section). They are listed in [Naj26b] as the points 6.12.10.a, 3.15.10.a, 3.18.10.a, 3.18.10.b, 2.26.10.a and 2.26.10.b, with one representative for each pair (K,E).

12. Proof of the main theorems

Table 9 lists, for each of the 110 groups of $\mathcal{M}_{10}$, where it is shown that it is not a subgroup of the torsion of an elliptic curve over a number field of degree 10.

$G \in \mathcal{M}_{10}$	treated in
$\mathbb{Z}/n\mathbb{Z}$ for the 45 levels n of Table 2	Proposition 5.3 (global method)
$\mathbb{Z}/n\mathbb{Z}$, $n = 115, 121, 135$	Propositions 5.5 and 5.6
$\mathbb{Z}/155\mathbb{Z}$	Proposition 5.10 (descent)
$\mathbb{Z}/n\mathbb{Z}$, $n = 95, 111$	Proposition 5.12
$\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$	Proposition 6.2
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$	Propositions 6.4 and 6.6
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$	Propositions 6.9 and 6.11
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/33\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}$	Propositions 6.13, 6.18 and 6.21
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/45\mathbb{Z}$	Corollary 11.11
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$	Corollary 11.19
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/39\mathbb{Z}$, $\mathbb{Z}/78\mathbb{Z}$	Proposition 10.29
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/32\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/34\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$	Propositions 7.6, 7.11 and 7.18
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/38\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/40\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$	Proposition 7.22
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/42\mathbb{Z}$	Proposition 7.28
$\mathbb{Z}/n\mathbb{Z}$, $n = 64, 68, 72, 76, 80, 84, 100$	Lemma 4.3 and Section 7
$\mathbb{Z}/52\mathbb{Z}$	Proposition 11.25
$\mathbb{Z}/n\mathbb{Z}$, $n = 44, 46, 48, 54, 56$	Propositions 8.2, 8.4, 8.7, 8.15 and 8.19
$\mathbb{Z}/n\mathbb{Z}$, $n = 58, 60, 62, 66, 70, 74$	Propositions 8.22, 8.24, 8.29, 8.35, 8.38 and 8.42
$\mathbb{Z}/n\mathbb{Z}$, $n = 49, 51, 55, 75$	Propositions 9.2, 9.5, 9.8 and 9.10
$\mathbb{Z}/n\mathbb{Z}$, $n = 77, 85, 91, 93$	Propositions 9.14, 9.18, 9.23 and 9.25
$\mathbb{Z}/n\mathbb{Z}$, $n = 57, 63, 65, 81, 87$	Propositions 10.6, 10.10, 10.14, 10.20 and 10.23
$\mathbb{Z}/n\mathbb{Z}$, $n = 69, 90, 99, 105, 117$	Propositions 10.26, 10.30, 10.33, 10.37 and 10.39

Table 9. Treatment of the 110 groups of $\mathcal{M}_{10}$.

Proof of Theorem 1.1. By Lemma 3.1 and Propositions 3.3 to 3.5 and by Propositions 11.7, 11.10, 11.18 and 11.24, every group of $\mathcal{G}_{10}$ is the torsion group of an elliptic curve over a

number field of degree 10. Conversely, let E be an elliptic curve over a number field K of degree 10. If $E(K)_{\mathrm{tors}} \notin \mathcal{G}_{10}$, then by Lemma 4.1 it contains a group of $\mathcal{M}_{10}$, which is impossible by the results listed in Table 9. □

Proof of Theorem 1.2. This is Propositions 11.7, 11.10, 11.18 and 11.24. □

13. Torsion groups that occur infinitely often

In this section we prove Theorem 1.3. The groups listed there occur for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves over number fields of degree 10 by the results of Section 3, so we have to show that each of the other 16 groups of Theorem 1.1 occurs for only finitely many. For a curve X over $\mathbb{Q}$ and $d \geq 1$ we write $W_d(X) \subseteq \mathrm{Pic}^d(X)$ for the image of $X^{(d)}$ under the map $D \mapsto [D]$.

Lemma 13.1. *Let X be a curve over $\mathbb{Q}$ with $J_X(\mathbb{Q})$ finite, and let $d \geq 1$ be such that $\mathrm{gon}_{\mathbb{Q}} X > d$. Then X has only finitely many closed points of degree at most d.*

Proof. Let $e \leq d$ and suppose that X has a closed point D_0 of degree e. By Lemma 2.8 a) the map $X^{(e)}(\mathbb{Q}) \to J_X(\mathbb{Q})$, $D \mapsto [D - D_0]$, is injective, so $X^{(e)}(\mathbb{Q})$ is finite. □

Lemma 13.2. *Let $m \in \{1, 2\}$ and $n \geq 5$ with $m \mid n$, and suppose that for every $e \mid 10$ the curve $X_1(m, n)$ has only finitely many closed points of degree e. Then the elliptic curves E over number fields K of degree 10 with $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \subseteq E(K)$ have only finitely many j-invariants. In particular, no group containing $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ lies in $\Phi^{\infty}(10)$.*

Proof. Such a curve E gives a point $x \in Y_1(m, n)(K)$ with $j(x) = j(E)$ (see Section 2.2), and the closed point of $X_1(m, n)$ below x has degree $[\mathbb{Q}(x) : \mathbb{Q}]$, which divides 10. □

13.1. Rank 0 and gonality.

Proposition 13.3. *Let (m, n) be one of the pairs*

$$(1, N) \text{ for } N \in \{29, 31, 35, 38, 39, 40, 42, 45, 50\}, \qquad (2, 28).$$

Then $X_1(m, n)$ has only finitely many closed points of degree at most 10, and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \notin \Phi^{\infty}(10)$.

Proof. The group $J_1(N)(\mathbb{Q})$ is finite for these N by [DEvH+21, Theorem 3.1(2)], and $J_1(2, 28)(\mathbb{Q})$ is finite by [DS17, Theorem 4.1]. By [DvH14, Theorem 4 and Table 1] for $N \leq 40$ and by [Var26, Theorem D] for $N \in \{42, 45, 50\}$ we have

N	29	31	35	38	39	40	42	45	50
$\mathrm{gon}_{\mathbb{Q}} X_1(N)$	11	12	12	12	14	12	12	18	15

and $\mathrm{gon}_{\mathbb{Q}} X_1(2, 28) \geq 12$ by [NV26, Table 1]. All these numbers are larger than 10, so the result follows from Lemmas 13.1 and 13.2. □

13.2. The group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$.

The Jacobian of $X_1(2, 30)$, a curve of genus 25, has finitely many rational points [DS17, Theorem 4.1], but the bound $\mathrm{gon}_{\mathbb{Q}} X_1(2, 30) \geq 10$ of [NV26, Table 1] is not sufficient for Lemma 13.1. We use the model $X_H(60)$ of $X_1(2, 30)$ with $H = \langle -1, 31 \rangle$ of Section 3.2. The Galois orbits of the cusps over $\mathbb{Q}$ have degrees $1^{12}, 2^6, 4^6$ (see `phi_infinity/outputs/cusp_lattice_2_30.json`), so $X_1(2, 30)$ has 12 rational cusps.

Lemma 13.4. *Every closed point of $X_1(2, 30)$ of degree at most 9 is a cusp.*

Proof. A non-cuspidal closed point x of degree e gives an elliptic curve E over the field $\mathbb{Q}(x)$ of degree e with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \subseteq E(\mathbb{Q}(x))$, so it suffices to show that for $e \leq 9$ no group of $\Phi(e)$ contains $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$. By Lemma 3.1 we have $\Phi(1) \subseteq \Phi(2) \subseteq \Phi(4) \subseteq \Phi(8)$ and $\Phi(3) \subseteq \Phi(6)$, so we only need to consider $5 \leq e \leq 9$. By [Naj26a, Theorem 1.1] and [Naj26d, Theorem 1.1], the groups of these sets $\Phi(e)$ which contain $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are among the groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ with $n \leq 13$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4n\mathbb{Z}$ with $n \leq 3$ and $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. None of them contains $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$. □

Lemma 13.5. *If $X_1(2,30)$ has a function of degree $e \leq 10$ over $\mathbb{Q}$, then it has a modular unit of degree e over $\mathbb{Q}$, that is, a function of degree e over $\mathbb{Q}$ whose divisor is supported on the cusps.*

Proof. Let f be a function of degree $e \leq 10$ over $\mathbb{Q}$, and let c be a rational cusp. If c is not a pole of f, we replace f by $1/(f - f(c))$, which also has degree e. Then the polar divisor of f is an effective $\mathbb{Q}$-rational divisor of degree e which contains c, so removing c from it leaves an effective $\mathbb{Q}$-rational divisor of degree $e-1 \leq 9$, which is supported on the cusps by Lemma 13.4. Hence all the poles of f are cusps. At most $e \leq 10$ of the 12 rational cusps are poles of f, so there is a rational cusp c' which is not a pole of f. The function $g = f - f(c')$ has the same poles as f, and its divisor of zeros contains c', so by the same argument all the zeros of g are cusps. Hence g is a modular unit of degree e. □

Lemma 13.6. *No two distinct effective $\mathbb{Q}$-rational cuspidal divisors of degree 10 on $X_1(2,30)$ are linearly equivalent.*

Proof. As in the proof of Proposition 3.3, a $\mathbb{Q}$-rational cuspidal divisor of degree 0 on $X_H(60)$ is principal if and only if it lies in the lattice of divisors of rational modular units, which we compute with the function `rational_modular_unit_lattice` of `mdsage` [mds]. It follows that the group of classes of $\mathbb{Q}$-rational cuspidal divisors of degree 0 is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^5 \times \mathbb{Z}/24\mathbb{Z} \times (\mathbb{Z}/8160\mathbb{Z})^2$. Writing the effective $\mathbb{Q}$-rational cuspidal divisors of degree 10 as non-negative combinations of the 24 Galois orbits of cusps, we find 1287948 of them, and we compute that their classes, relative to 10 times a fixed rational cusp, are pairwise distinct. □

Proposition 13.7. *We have $\operatorname{gon}_{\mathbb{Q}} X_1(2,30) > 10$. Hence $X_1(2,30)$ has only finitely many closed points of degree at most 10, and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \notin \Phi^{\infty}(10)$.*

Proof. Suppose that $X_1(2,30)$ has a function of degree $e \leq 10$ over $\mathbb{Q}$. By Lemma 13.5 it then has a modular unit g of degree e over $\mathbb{Q}$. Write $\operatorname{div}(g) = D_0 - D_\infty$, where D_0 and D_∞ are distinct effective $\mathbb{Q}$-rational cuspidal divisors of degree e, and let c be a rational cusp. Then $D_0 + (10-e)c$ and $D_\infty + (10-e)c$ are distinct and linearly equivalent, which contradicts Lemma 13.6. As $J_1(2,30)(\mathbb{Q})$ is finite [DS17, Theorem 4.1], the remaining claims follow from Lemmas 13.1 and 13.2. □

13.3. **The group $\mathbb{Z}/37\mathbb{Z}$.** The curve $X_1(37)$ has genus 40 and $\operatorname{gon}_{\mathbb{Q}} X_1(37) = 18$ [DvH14, Theorem 4 and Table 1], but $J_1(37)(\mathbb{Q})$ is infinite, so Lemma 13.1 does not apply. We follow the proof of [NV26, Proposition 5.7], where Najman and Varivoda showed that $X_1(37)$ has only finitely many points of degree 9. We will use the following consequence of Faltings' theorem (see also [NV26, Theorem 2.4]).

Lemma 13.8. *Let X be a curve over $\mathbb{Q}$ and let $d \geq 1$ be such that $\operatorname{gon}_{\mathbb{Q}} X > d$. If X has infinitely many closed points of degree d, then there are an abelian subvariety $A \subseteq J_X$ defined over $\mathbb{Q}$ with $A(\mathbb{Q})$ infinite and a point $y \in W_d(X)(\mathbb{Q})$ such that $y + A \subseteq W_d(X)$.*

Proof. By Lemma 2.8 a), distinct effective $\mathbb{Q}$-rational divisors of degree d on X have distinct classes, so $W_d(X)(\mathbb{Q})$ is infinite. Fix $y_0 \in W_d(X)(\mathbb{Q})$ and put $Z = W_d(X) - y_0 \subseteq J_X$. By Faltings' theorem [Fal94], $Z(\mathbb{Q})$ is a finite union of sets $z_i + B_i(\mathbb{Q})$, where $z_i \in Z(\mathbb{Q})$ and $B_i \subseteq J_X$ are abelian subvarieties with $z_i + B_i \subseteq Z$. One of the sets $B_i(\mathbb{Q})$ is infinite. Let A be the identity component of the Zariski closure of $B_i(\mathbb{Q})$. It is an abelian subvariety of B_i defined over $\mathbb{Q}$, and $A(\mathbb{Q})$ has finite index in a group containing $B_i(\mathbb{Q})$, so it is infinite. Hence $y = y_0 + z_i$ has the required properties. □

Let $\pi : X_1(37) \to X_0^+(37)$ be the quotient map, of degree 36, and identify the curve $X_0^+(37)$ with the elliptic curve $E : y^2 + y = x^3 - x$ (37.a1). We write π^*E for the image of $\pi^* : \mathrm{Pic}^0(E) \to J_1(37)$.

Lemma 13.9. *Every abelian subvariety $A \subseteq J_1(37)$ defined over $\mathbb{Q}$ with $A(\mathbb{Q})$ infinite contains π^*E.*

Proof. By [NV26, proof of Proposition 5.7], the only simple factor of $J_1(37)$ of positive rank, up to isogeny, is π^*E. As $A(\mathbb{Q})$ is infinite, one of the simple factors of A has positive rank, so A contains an abelian subvariety B isogenous to E. As 37 is prime and there are no cusp forms of weight 2 and level 1, every simple factor of $J_1(37)$ occurs in it with multiplicity 1 up to isogeny, so $B = \pi^*E$. □

Let $C = X_1(37)_{\mathbb{F}_2}$ and $\overline{E} = E_{\mathbb{F}_2}$. By Lemma 2.1, π extends to the smooth models over $\mathbb{Z}_{(2)}$, and we denote its reduction $C \to \overline{E}$ again by π. The group $\overline{E}(\mathbb{F}_2)$ has order 5. Let $e_\infty \in \overline{E}(\mathbb{F}_2)$ be the reduction of the cusp of $X_0^+(37)$, which is the image of all the cusps of $X_1(37)$, and let $e_0 \in \overline{E}(\mathbb{F}_2)$ be the point above $S = T = 0$ on the plane model of $X_0^+(37)_{\mathbb{F}_2}$ with coordinates $S = j(\mathcal{E}) + j(\mathcal{E}/\langle P\rangle)$ and $T = j(\mathcal{E})j(\mathcal{E}/\langle P\rangle)$ of [NV26, proof of Proposition 5.7], where $(\mathcal{E}, P)$ is the universal pair. Put $F_\infty = \pi^*e_\infty$, $F_0 = \pi^*e_0$ and $\Delta = F_\infty - F_0$, a divisor of degree 0 on C. As $e_0 \neq e_\infty$, the class $[e_\infty - e_0]$ generates $\mathrm{Pic}^0(\overline{E}) \simeq \overline{E}(\mathbb{F}_2)$, where $\mathrm{Pic}^0(\overline{E})$ is the group of classes of $\mathbb{F}_2$-rational divisors of degree 0, so its image $[\Delta] = \pi^*[e_\infty - e_0]$ satisfies $5[\Delta] = 0$.

Lemma 13.10. *Let D and D' be effective $\mathbb{F}_2$-rational divisors of degree 10 on C with $D' \sim D + \Delta$. Then D or D' contains a closed point of degree larger than 1.*

Proof. No elliptic curve over $\mathbb{F}_2$ has a point of order 37, as it has at most 5 points, so every $\mathbb{F}_2$-rational point of C is a cusp and is mapped to e_∞ by π. If D and D' are supported on $\mathbb{F}_2$-rational points, it follows that $\pi_*D = \pi_*D' = 10e_\infty$. On the other hand, $\pi_*D' \sim \pi_*D + \pi_*\pi^*(e_\infty - e_0) = \pi_*D + 36(e_\infty - e_0)$, and $36[e_\infty - e_0] = [e_\infty - e_0] \neq 0$ in $\mathrm{Pic}^0(\overline{E})$, which has order 5. This is a contradiction. □

Lemma 13.11. *For every effective $\mathbb{F}_2$-rational divisor D of degree 10 on C which contains a closed point of degree larger than 1, there is a $k \in \{1, 2, 3, 4\}$ with $\ell(D + k\Delta) = 0$.*

Proof. We use the plane model of $X_1(37)$ and the map π of [NV26, proof of Proposition 5.7] (see `phi_infinity/work/x1_37/driver_fast.m` and `phi_infinity/work/x1_37/X1_37_X0plus_map_data.m`). We compute that C has genus 40 and that the numbers of its closed points of degree $1, 2, \ldots, 10$ are

$$18,\ 0,\ 0,\ 0,\ 0,\ 21,\ 18,\ 0,\ 39,\ 99.$$

We compute F_0 and the fibre of π over the point at infinity of the plane model of $X_0^+(37)_{\mathbb{F}_2}$, check that both have degree 36, and check that the latter contains the 18 points of degree

1, which are cusps, so that it is F_∞. Hence $D = P + R$, where P is a closed point of degree $i \in \{6, 7, 9, 10\}$ and R is an effective divisor of degree $10 - i$ supported on the 18 points of degree 1, and there are $21\binom{21}{4} + 18\binom{20}{3} + 39 \cdot 18 + 99 = 147006$ such divisors D. For each closed point P of degree i put $H = P + (10 - i)\sum_{c \in C(\mathbb{F}_2)} c$. Every divisor $D = P + R$ satisfies $D \leq H$, and $H - D$ is supported on $C(\mathbb{F}_2)$, so $L(D + k\Delta) = L(H + k\Delta - (H - D))$ is the subspace of $L(H + k\Delta)$ cut out by vanishing conditions at the points of $C(\mathbb{F}_2)$. We compute a basis of $L(H + k\Delta)$ and the Laurent expansions of its elements at the points of $C(\mathbb{F}_2)$, so that $\ell(D + k\Delta)$ is the dimension of the kernel of a matrix over $\mathbb{F}_2$. In this way we find, for each of the 147006 divisors D, a $k \in \{1, 2, 3, 4\}$ with $\ell(D + k\Delta) = 0$. For one divisor D for every P, we also compute $\ell(D + \Delta)$ directly, with the same result. □

Proposition 13.12. *The curve $X_1(37)$ has only finitely many closed points of degree 10, and $\mathbb{Z}/37\mathbb{Z} \notin \Phi^\infty(10)$.*

Proof. Suppose that $X_1(37)$ has infinitely many closed points of degree 10. As $\operatorname{gon}_{\mathbb{Q}} X_1(37) = 18 > 10$, by Lemmas 13.8 and 13.9 there is a $y \in W_{10}(X_1(37))(\mathbb{Q})$ with $y + \pi^* E \subseteq W_{10}(X_1(37))$. Let $a \in E(\mathbb{Q})$. Then $y + \pi^*[a - O]$ is a rational point of $W_{10}(X_1(37))$, and as $X_1(37)$ has a rational cusp, it is the class of an effective $\mathbb{Q}$-rational divisor D_a of degree 10. Reduction of divisors from $X_1(37)$ to C, through their closures in the smooth model over $\mathbb{Z}_{(2)}$, preserves effectivity and linear equivalence and commutes with π^* (compare [NV26, Lemma 2.5]). Hence the reduction $\overline{D}_a$ of D_a is an effective $\mathbb{F}_2$-rational divisor in the class $\overline{y} + \pi^*[\overline{a} - \overline{O}]$. The group $E(\mathbb{Q})$ is generated by the point $(0, 0)$ [LMF26], whose reduction is not $\overline{O}$, so the reduction map $E(\mathbb{Q}) \to \overline{E}(\mathbb{F}_2)$ is surjective. Hence for every $k \in \{0, \dots, 4\}$ there is an effective $\mathbb{F}_2$-rational divisor D_k of degree 10 on C with $D_k \sim D_0 + k\Delta$. By Lemma 13.10, D_0 or D_1 contains a closed point of degree larger than 1. As $5[\Delta] = 0$, every class $[D_0 + k\Delta]$ is the class of one of $D_0, \dots, D_4$, so $\ell(D_0 + k\Delta) \geq 1$ and $\ell(D_1 + k\Delta) \geq 1$ for all k, which contradicts Lemma 13.11.

Hence $X_1(37)$ has only finitely many closed points of degree 10. Its closed points of degree 1, 2 and 5 are cusps, as $\mathbb{Z}/37\mathbb{Z}$ does not lie in $\Phi(1)$, $\Phi(2)$ and $\Phi(5)$ (Section 3.1), so the second claim follows from Lemma 13.2. □

Proof of Theorem 1.3. By Lemma 3.1, applied to infinitely many elliptic curves with pairwise distinct j-invariants, we have $\Phi^\infty(e) \subseteq \Phi^\infty(10)$ for every $e \mid 10$. We have $\Phi^\infty(1) = \Phi(1)$ and $\Phi^\infty(2) = \Phi(2)$ (see [DS17, Section 1]), and $\Phi^\infty(5)$ consists of the groups $\mathbb{Z}/n\mathbb{Z}$ with $1 \leq n \leq 25$, $n \neq 23$, and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ with $1 \leq n \leq 8$ [DS17, Theorem 1.1]. With the lists of $\Phi(1)$ and $\Phi(2)$ in Section 3.1, these are 35 of the groups of Theorem 1.3, and the other 18 lie in $\Phi^\infty(10)$ by Proposition 3.3. The remaining 16 groups of Theorem 1.1 do not lie in $\Phi^\infty(10)$ by Theorem 1.2 for $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, by Proposition 13.3 for $\mathbb{Z}/n\mathbb{Z}$ with $n \in \{29, 31, 35, 38, 39, 40, 42, 45, 50\}$ and for $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}$, and by Propositions 13.7 and 13.12 for $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ and $\mathbb{Z}/37\mathbb{Z}$. □

14. The computations

Our computations were performed in Magma V2.30-1 [BCP97], apart from some auxiliary ones in Python and in SageMath 10.7 (such as the lists of groups, the values of Abramovich's bound, the modular units of Proposition 3.3, which were found with the package `mdsage` [mds], and the replay of data exported from Magma). They were run on the *Mordell* server at the Department of Mathematics, University of Zagreb, with an AMD EPYC 9175F CPU and 384 GB of RAM, between 29 and 31 October 2026, apart from the

computations of Section 13, which were made on 17 and 18 November 2026. We used the package `mdmagma` [mdm] for the moduli-theoretic operations, Sutherland's optimized models of $X_1(n)$ [Sut12a, Sut12b], the Derickx-Sutherland models of $X_1(m,n)$ [DS16], the low degree points of van Hoeij [vH14], and the LMFDB [LMF26] for the analytic ranks of newforms. The jobs recorded in the repository took about 66 hours of CPU time in total. This includes exploratory and diagnostic runs which the proofs do not use, and does not include the computations from [Naj26d] that we reuse. Those are copied into the repository together with the scripts that produced them.

Several results were also checked by computations that their proofs do not need. They are listed, result by result and with their logs, in the section "Further checks" of the `README` file of the repository. Most of them repeat a computation by an independent program, usually in SageMath or Python with integer or finite field linear algebra, starting from the data exported by the Magma computation. For example, the 1086016 restriction ranks for $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/33\mathbb{Z}$, the 262 parity decisions for $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$, the classes and matches in the proofs for $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$, the determinants and norms in Lemma 5.4, and the linear independence of the vectors $v, vT_2, \dots$ in the winding computations of Section 5 were all recomputed in this way. Other results were checked by a second method or at other primes: for example the isogenies used in the Hecke operators were recomputed from the division polynomials with Vélu's formulas, the Riemann-Roch computations at 13 for $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ were repeated at 19 and 31, and the divisor classes were recomputed from ideal identities in the function fields. In all cases the results agree.

A few computations were made for the final version of the paper, when some of the original arguments were replaced by shorter ones. They are in the folder `additions` of the repository, and they are linked in the proofs of Propositions 6.11, 8.19 and 8.42 and Lemma 8.27 and in Section 11. Some arguments of the original computational record are therefore no longer needed in the paper: for example the formal immersion computations for the entirely cuspidal reductions on $X_1(49)$, and the computation of the gonality of $X_1(4,20)$ over $\mathbb{F}_9$, which needed 11156288 rank computations.

The computations of Section 13 are in the folder `phi_infinity`, apart from the computation in the proof of Lemma 13.11, which is in `additions/phi_infinity`. The computation for $\mathbb{Z}/37\mathbb{Z}$ in `phi_infinity/work/x1_37` checks only one closed point P in each orbit of the diamond operators, which preserve Δ as $\pi \circ \langle a \rangle = \pi$, so it needs only 13188 divisors D. It uses that, for every $i \leq 10$, the closed points of C of degree i whose j-invariants are non-zero and conjugate form one orbit. This holds because for an elliptic curve over $\mathbb{F}_{2^i}$ with non-zero j-invariant, the points Q of order 37 with $\varphi(Q) = \pm Q$, where φ is its Frobenius endomorphism of degree 2^i, lie on one line of its 37-torsion, as $\deg \varphi = 2^i \not\equiv \pm 1 \pmod{37}$. The computation in the proof of Lemma 13.11, which checks all the 147006 divisors and does not need this argument, took about 4 hours of CPU time.

We also checked some of the computations a second time, with code written independently of the first implementation. These are the list of Lemma 4.1, which we recomputed from scratch, and the explicit examples of Propositions 3.4 and 3.5, for which we computed the torsion groups with Magma's function `TorsionSubgroup`, which does not use the reductions of Table 1, both from the models used in the proofs and, for the points of Proposition 3.4, directly from van Hoeij's coordinates. We also checked the field automorphism and the j-invariants used in Section 11 (`independent_checks/aut_318_check.m`, `independent_checks/sporadic_check.m`). For Section 13, we recomputed the numbers of closed points of C of degree at most 10 from the moduli interpretation, by counting the

elliptic curves over $\mathbb{F}_{2^k}$ with $k \leq 10$ that have a point of order 37, instead of using the plane model. We also recomputed the classes in the proof of Lemma 13.6 with the Hermite normal form of the lattice of divisors of modular units instead of its Smith normal form, and checked that the order 51137740800 of the group of classes of rational cuspidal divisors of degree 0 on $X_1(2,30)$ divides $\#J_1(2,30)(\mathbb{F}_p)$ for $p \in \{7,11,13,17,19,23\}$, as it should. An LMFDB search also shows that the newform 37.2.a.a of E is the only newform of weight 2 and level 37 with positive analytic rank, in accordance with Lemma 13.9. In all cases the results agree. Finally, we checked that every file of the repository that is used as evidence in the original record has the hash recorded there (`independent_checks/check_ledger_hashes.py`). The files that are only in the release archive of the repository, or that are copies of other papers, are listed there.

References

[Abr96] Dan Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices (1996), no. 20, 1005–1011.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

[BN16] Peter Bruin and Filip Najman, *A criterion to rule out torsion groups for elliptic curves over number fields*, Res. Number Theory **2** (2016), Paper No. 3, 13 pp.

[CCRS14] Pete L. Clark, Patrick Corn, Alex Rice, and James Stankewicz, *Computation on elliptic curves with complex multiplication*, LMS J. Comput. Math. **17** (2014), no. 1, 509–535.

[DEvH+21] Maarten Derickx, Anastassia Etropolski, Mark van Hoeij, Jackson S. Morrow, and David Zureick-Brown, *Sporadic cubic torsion*, Algebra Number Theory **15** (2021), no. 7, 1837–1864.

[DI95] Fred Diamond and John Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), CMS Conf. Proc. **17** (1995), 39–133.

[DKSS23] Maarten Derickx, Sheldon Kamienny, William Stein, and Michael Stoll, *Torsion points on elliptic curves over number fields of small degree*, Algebra Number Theory **17** (2023), no. 2, 267–308.

[DN25] Maarten Derickx and Filip Najman, *Classification of torsion of elliptic curves over quartic fields*, J. Reine Angew. Math. **829** (2025), 123–156.

[Dri73] V. G. Drinfel'd, *Two theorems on modular curves*, Funktsional. Anal. i Prilozhen. **7** (1973), no. 2, 83–84.

[DS16] Maarten Derickx and Andrew V. Sutherland, *Explicit models of $X_1(m,mn)$*, `https://math.mit.edu/~drew/X1mn.html`, 2016.

[DS17] ———, *Torsion subgroups of elliptic curves over quintic and sextic number fields*, Proc. Amer. Math. Soc. **145** (2017), no. 10, 4233–4245.

[DS25] Maarten Derickx and Michael Stoll, *Prime order torsion on elliptic curves over number fields. Part I: Asymptotics*, Preprint, arXiv:2505.14109v1, 2025.

[DvH14] Maarten Derickx and Mark van Hoeij, *Gonality of the modular curve $X_1(N)$*, J. Algebra **417** (2014), 52–71.

[Fal94] Gerd Faltings, *The general case of S. Lang's conjecture*, Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), Perspect. Math., vol. 15, Academic Press, San Diego, CA, 1994, pp. 175–182.

[Har77] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York-Heidelberg, 1977.

[JKP06] Daeyeol Jeon, Chang Heon Kim, and Euisung Park, *On the torsion of elliptic curves over quartic number fields*, J. London Math. Soc. (2) **74** (2006), no. 1, 1–12.

[JKS04] Daeyeol Jeon, Chang Heon Kim, and Andreas Schweizer, *On the torsion of elliptic curves over cubic number fields*, Acta Arith. **113** (2004), no. 3, 291–301.

[Kam92] Sheldon Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229.

[Kat81] Nicholas M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), no. 3, 481–502.

[Kat04] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque (2004), no. 295, ix, 117–290, Cohomologies p-adiques et applications arithmétiques. III.

[Kha24] Maleeha Khawaja, *Torsion primes for elliptic curves over degree* 8 *number fields*, Res. Number Theory **10** (2024), no. 2, Paper No. 48.

[Kim03] Henry H. Kim, *Functoriality for the exterior square of* GL_4 *and the symmetric fourth of* GL_2, J. Amer. Math. Soc. **16** (2003), no. 1, 139–183, With appendix 1 by Dinakar Ramakrishnan and appendix 2 by Henry H. Kim and Peter Sarnak.

[KM88] M. A. Kenku and Fumiyuki Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.

[Kub76] Daniel Sion Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) **33** (1976), no. 2, 193–237.

[LL99] Qing Liu and Dino Lorenzini, *Models of curves and finite covers*, Compositio Math. **118** (1999), 61–102.

[LMF26] *The L-functions and modular forms database*, https://www.lmfdb.org, 2026, The LMFDB Collaboration; online, accessed September 2026.

[Man72] Ju. I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66.

[Maz77] Barry Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978), With an appendix by Mazur and M. Rapoport.

[mdm] *mdmagma*, https://github.com/nt-lib/mdmagma, M. Derickx and A. V. Sutherland, `Magma` package.

[mds] *mdsage*, https://github.com/koffie/mdsage, M. Derickx, `SageMath` package.

[Mer96] Loïc Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1-3, 437–449.

[Naj16] Filip Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on* $X_1(n)$, Math. Res. Lett. **23** (2016), no. 1, 245–272.

[Naj26a] ———, *Classification of torsion of elliptic curves over quintic fields*, Preprint, https://arxiv.org/abs/2609.12846, 2026.

[Naj26b] ———, *Isolated and sporadic points on* $X_1(m,n)$, https://x1mn-sporadic.github.io, 2026.

[Naj26c] ———, *Points of prime order on elliptic curves over number fields of degree* 9 *to* 22, Preprint, https://hexagonmath.org/2611.00120v1, 2026.

[Naj26d] ———, *Torsion of elliptic curves over number fields of degree* 6*,* 7*,* 8 *and* 9, Preprint, https://hexagonmath.org/2611.00073v2, 2026.

[NV26] Filip Najman and Marin Varivoda, *Torsion groups of elliptic curves that appear infinitely often over septic, octic and nonic fields*, Preprint, https://arxiv.org/abs/2602.03513, 2026.

[Oda69] Tadao Oda, *The first de Rham cohomology group and Dieudonné modules*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 63–135.

[Orl25] Petar Orlić, *Tetragonal intermediate modular curves*, Acta Arith. **220** (2025), no. 3, 263–288.

[Par99] Pierre Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math. **506** (1999), 85–116.

[Par00] ———, *Torsion des courbes elliptiques sur les corps cubiques*, Ann. Inst. Fourier (Grenoble) **50** (2000), no. 3, 723–749.

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[Sti09] Henning Stichtenoth, *Algebraic function fields and codes*, second ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009.

[Sut12a] Andrew V. Sutherland, *Constructing elliptic curves over finite fields with prescribed torsion*, Math. Comp. **81** (2012), no. 278, 1131–1147.

[Sut12b] ———, *Optimized equations for* $X_1(N)$, https://math.mit.edu/~drew/X1_altcurves.html, 2012.

[Var26] Marin Varivoda, *Gonality and quintic points on intermediate modular curves*, Preprint, https://hexagonmath.org/2610.00219v1, 2026.

[vH14] Mark van Hoeij, *Low degree places on the modular curve* $X_1(N)$, Preprint, https://arxiv.org/abs/1202.4355; data at https://www.math.fsu.edu/~hoeij/files/X1N/, 2014.

[Wat69] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560.

University of Zagreb Faculty of Science, Department of Mathematics, Bijenička cesta 30, 10000 Zagreb, Croatia

Email address: fnajman@math.hr