hexagon:2611.00073v2

TORSION OF ELLIPTIC CURVES OVER NUMBER FIELDS OF DEGREE 6, 7, 8 AND 9

FILIP NAJMAN

Abstract. We determine all the groups that appear as the torsion group of an elliptic curve over a number field of degree d for $d = 6$, 7, 8 and 9. Apart from the groups that occur infinitely often, exactly 4 groups occur in degree 6, 3 in degree 7, 8 in degree 8 and 9 in degree 9, and among them the groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$ over sextic fields, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$ over octic fields and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$ over nonic fields were not known to occur. For 13 of these 24 pairs of a degree and a group we also determine all the elliptic curves that realize them. The proofs combine the global method of Derickx, Hecke sieves, formal immersion criteria at the prime 2 with Hecke operators, 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 [Kam92a], 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]. Finally, $\Phi(5)$ was determined by the author [Naj26a]. In this paper we determine $\Phi(6)$, $\Phi(7)$, $\Phi(8)$ and $\Phi(9)$.

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. A group in $\Phi(d) \setminus \Phi^{\infty}(d)$ will be called a *sporadic torsion group in degree d*. This should not be confused with a *sporadic point* on a curve X, which is a closed point of some degree e such that X has only finitely many closed points of degree at most e. A list of known sporadic and isolated points on the curves $X_1(m, n)$ is maintained on the webpage [Naj26b]. We

Date: November 5, 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.

have $\Phi^\infty(d) = \Phi(d)$ for $d = 1, 2, 4$. The only sporadic torsion group in degree 3 is $\mathbb{Z}/21\mathbb{Z}$ [Naj16, DEvH+21], and the sporadic torsion groups in degree 5 are $\mathbb{Z}/28\mathbb{Z}$, $\mathbb{Z}/30\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ [Naj26a]. The set $\Phi^\infty(6)$ was determined by Derickx and Sutherland [DS17, Theorem 1.1], the cyclic part being due to Derickx and van Hoeij [DvH14, Theorem 3]:

$$\begin{aligned}\Phi^\infty(6) = &\{\mathbb{Z}/n\mathbb{Z} \,:\, 1 \le n \le 30,\ n \ne 23, 25, 29\} \\ &\cup\ \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \,:\, 1 \le n \le 10\} \ \cup\ \{\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z} \,:\, 1 \le n \le 4\} \\ &\cup\ \{\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}\}.\end{aligned} \tag{1}$$

The sets $\Phi^\infty(7)$, $\Phi^\infty(8)$ and $\Phi^\infty(9)$ were determined by Najman and Varivoda [NV26, Theorem 1.1]:

$$\Phi^\infty(7) = \{\mathbb{Z}/n\mathbb{Z} \,:\, 1 \le n \le 30,\ n \ne 25, 29\} \ \cup\ \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \,:\, 1 \le n \le 10\}, \tag{2}$$

$$\begin{aligned}\Phi^\infty(8) = &\{\mathbb{Z}/n\mathbb{Z} \,:\, 1 \le n \le 28 \ \text{ or } \ n \in \{30, 32, 36\}\} \ \cup\ \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \,:\, 1 \le n \le 12\} \\ &\cup\ \{\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z} \,:\, 1 \le n \le 4\} \ \cup\ \{\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4n\mathbb{Z} \,:\, 1 \le n \le 3\} \\ &\cup\ \{\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z},\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}\},\end{aligned} \tag{3}$$

$$\Phi^\infty(9) = \{\mathbb{Z}/n\mathbb{Z} \,:\, 1 \le n \le 28 \ \text{ or } \ n \in \{30, 36\}\} \ \cup\ \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \,:\, 1 \le n \le 12\}. \tag{4}$$

These sets have 44, 38, 52 and 42 elements.

Some sporadic torsion groups in these degrees were already known. Van Hoeij [vH14] found points of degree 6 on $X_1(25)$ and $X_1(37)$, of degree 7 on $X_1(25)$, $X_1(33)$ and $X_1(36)$, of degree 8 on $X_1(N)$ for $N = 33, 34, 35, 39, 40$ and 42, and of degree 9 on $X_1(N)$ for $N = 29, 31, 32, 33, 34, 39, 40$ and 42. Derickx, Kamienny, Stein and Stoll proved that every elliptic curve over a sextic field with a point of order 37 has j-invariant -9317 [DKSS23, Proposition 1.4]. González-Jiménez and Najman [GJN23] found that the base change of the rational elliptic curve 162.d2 to a sextic field has torsion group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ (see also [DGJ20, Remark 1]). Clark, Corn, Rice and Stankewicz [CCRS14] determined the torsion groups of elliptic curves with complex multiplication over number fields of small degree. In particular, the groups $\mathbb{Z}/34\mathbb{Z}$, $\mathbb{Z}/39\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ are torsion groups of elliptic curves with complex multiplication over octic fields, while all such groups over nonic fields lie in $\Phi^\infty(9)$.

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. Merel's theorem shows that $S(d)$ is finite. The sets $S(1)$, $S(2)$ and $S(3)$ follow from the work of Mazur, Kamienny, Kenku and Momose and Parent [Maz77, Kam92a, KM88, Par00], the sets $S(4), \dots, S(7)$ were determined by Derickx, Kamienny, Stein and Stoll [DKSS23], and $S(8)$ by Khawaja [Kha24]. Explicitly, $S(6) = \{2, 3, 5, 7, 11, 13, 17, 19, 37\}$ and $S(7)$ is the set of primes up to 23 [DKSS23, Theorem 1.2], and so is $S(8)$ [Kha24, Theorem 1.2]. Derickx and Stoll [DS25] studied the asymptotic behavior of $S(d)$ and developed tools that rule out most primes for any given d, and they have also determined $S(9)$, up to not being able to eliminate 89 from $S(9)$ [DS26]. The author [Naj26c] showed that $S(9)$ is the set of primes up to 31. These results are the starting point of our proofs. Note that in degree 9 our proof depends on [Naj26c].

Our main result is the following theorem.

Theorem 1.1. *Let $d \in \{6, 7, 8, 9\}$, let K be a number field of degree d and let E be an elliptic curve over K. Then $E(K)_{\text{tors}}$ lies in $\Phi^\infty(d)$ or is one of the sporadic groups in degree d given in the following table, and each of these sporadic groups occurs.*

d	*sporadic torsion groups in degree* d	$\#\Phi(d)$
6	$\mathbb{Z}/25\mathbb{Z}$, $\mathbb{Z}/37\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/24\mathbb{Z}$	48
7	$\mathbb{Z}/25\mathbb{Z}$, $\mathbb{Z}/33\mathbb{Z}$, $\mathbb{Z}/36\mathbb{Z}$	41
8	$\mathbb{Z}/33\mathbb{Z}$, $\mathbb{Z}/34\mathbb{Z}$, $\mathbb{Z}/35\mathbb{Z}$, $\mathbb{Z}/39\mathbb{Z}$, $\mathbb{Z}/40\mathbb{Z}$, $\mathbb{Z}/42\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/15\mathbb{Z}$	60
9	$\mathbb{Z}/29\mathbb{Z}$, $\mathbb{Z}/31\mathbb{Z}$, $\mathbb{Z}/32\mathbb{Z}$, $\mathbb{Z}/33\mathbb{Z}$, $\mathbb{Z}/34\mathbb{Z}$, $\mathbb{Z}/39\mathbb{Z}$, $\mathbb{Z}/40\mathbb{Z}$, $\mathbb{Z}/42\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/26\mathbb{Z}$	51

Explicitly, $\Phi(6)$ consists of the groups

$$\begin{aligned}
&\mathbb{Z}/n\mathbb{Z}, && n = 1,\dots,22,\ 24,\dots,28,\ 30,\ 37,\\
&\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z}, && n = 1,\dots,10,\ 12,\\
&\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3n\mathbb{Z}, && n = 1,\dots,4,\\
&\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4n\mathbb{Z}, && n = 1,2,3,\\
&\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}, &&
\end{aligned}$$

$\Phi(7)$ consists of the groups

$$\begin{aligned}
&\mathbb{Z}/n\mathbb{Z}, && n = 1,\dots,28,\ 30,\ 33,\ 36,\\
&\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z}, && n = 1,\dots,10,
\end{aligned}$$

$\Phi(8)$ consists of the groups

$$\begin{aligned}
&\mathbb{Z}/n\mathbb{Z}, && n = 1,\dots,28,\ 30,\ 32,\ 33,\ 34,\ 35,\ 36,\ 39,\ 40,\ 42,\\
&\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z}, && n = 1,\dots,12,\\
&\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3n\mathbb{Z}, && n = 1,\dots,5,\\
&\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4n\mathbb{Z}, && n = 1,2,3,\\
&\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/5n\mathbb{Z}, && n = 1,2,\\
&\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}, &&
\end{aligned}$$

and $\Phi(9)$ consists of the groups

$$\begin{aligned}
&\mathbb{Z}/n\mathbb{Z}, && n = 1,\dots,34,\ 36,\ 39,\ 40,\ 42,\\
&\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z}, && n = 1,\dots,13.
\end{aligned}$$

For many of the sporadic groups we also determine all the elliptic curves in question. Here 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'.

Theorem 1.2. *Let (d,G) be one of the pairs in the following table, let K be a number field of degree d, 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 listed for (d,G) in Table 5. The number of these pairs and their fields K are as follows.*

d	G	pairs (K,E)	fields K
6	$\mathbb{Z}/37\mathbb{Z}$	1	*6.6.300125.1*
	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$	1	*6.2.231852.1*
7	$\mathbb{Z}/25\mathbb{Z}$	1	*7.1.184607.1*
	$\mathbb{Z}/33\mathbb{Z}$	1	*7.3.792873.1*
	$\mathbb{Z}/36\mathbb{Z}$	2	*7.1.1609956.1*, *7.3.3192732.1*
8	$\mathbb{Z}/33\mathbb{Z}$	1	*8.2.7486875.1*
	$\mathbb{Z}/34\mathbb{Z}$	3	*8.0.1257728.1*, *8.0.1265625.1*, *8.4.19360000.1*
	$\mathbb{Z}/35\mathbb{Z}$	1	*8.4.31878125.1*
	$\mathbb{Z}/39\mathbb{Z}$	1	*8.0.1601613.1*
	$\mathbb{Z}/40\mathbb{Z}$	1	*8.2.31500500.1*
	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$	1	*8.0.2313441.1*
9	$\mathbb{Z}/33\mathbb{Z}$	1	*9.3.393718863.1*
	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$	1	*9.3.157505216.1*

The fields and the curves are given explicitly in Section 13, which also contains curves realizing the other sporadic groups. The elliptic curves with torsion groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$ over a sextic field, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$ over an octic field and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$ over a nonic field are new, and they are listed in [Naj26b] as the points 2.24.6.a, 3.15.8.a and 2.26.9.a. We found them in the course of this work, so these three groups were not known to occur in these degrees. We do not determine all the elliptic curves over sextic fields with torsion $\mathbb{Z}/25\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, nor those over octic fields with torsion $\mathbb{Z}/42\mathbb{Z}$ or $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, nor those over nonic fields with the sporadic cyclic torsion groups other than $\mathbb{Z}/33\mathbb{Z}$. This is not needed for Theorem 1.1, since all the groups properly containing these groups can be ruled out directly. The curve with torsion $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$ has j-invariant $1331/8$, so it is a twist of the rational elliptic curve 338.d2, but it is not the base change of an elliptic curve over $\mathbb{Q}$ or $\mathbb{Q}(\zeta_3)$. Note also that $\mathbb{Z}/35\mathbb{Z}$, which is a sporadic torsion group in degree 8, does not occur in degree 9, and that $\mathbb{Z}/37\mathbb{Z}$, which occurs in degree 6, occurs in none of the degrees 7, 8 and 9.

Outline of the proof and of the paper. As in [DN25] and [Naj26a], the classification reduces to showing that certain modular curves $X_1(m,n)$ have no non-cuspidal points over number fields of degree d. We introduce the notation and the general tools in Section 2, and in Section 3 we show that 66, 58, 80 and 81 groups have to be ruled out in degrees 6, 7, 8 and 9. The remaining sections treat these groups by method, most curves once for all the degrees in which they are needed, and often the computation for the largest degree also covers the smaller ones (see Remark 7.4).

The global method of Derickx [DN25, Proposition 4.3] and arguments with several diamond operators at the prime 2 eliminate most of the groups $\mathbb{Z}/n\mathbb{Z}$ with large n (Section 4). In degree 9 we also use that a field of odd degree contains no imaginary quadratic field (Section 2.5). When the Jacobian has rank 0 we use the criterion of [DN25, Proposition 5.2], which shows that the elliptic curve must have good reduction at some prime above a suitable p, together with computations with cuspidal divisor classes over finite fields (Section 5). We exclude the possible good reductions with the Hecke sieve of [DN25, Proposition 5.5], often after pushing the divisors forward to a curve of smaller level whose Mordell-Weil group is known (Section 6). When every elliptic curve with a point of order n has bad reduction at all the primes above 2, but the Jacobian has positive rank or the gonality bound is too

weak, we use a formal immersion criterion at 2 (Section 7). There Lemma 7.1 shows that $T_2 - \langle 2 \rangle$ kills the 2-torsion in the kernel of reduction, and the criterion becomes a condition on the Cartier operator on a quotient of $X_1(n)$ over $\mathbb{F}_2$, combined with elements of the Hecke algebra whose image on the Mordell-Weil group is finite, so that it also applies when the Jacobian has positive rank. When the Hecke sieve has to be applied on curves of large genus, as for $\mathbb{Z}/57\mathbb{Z}$ and $\mathbb{Z}/65\mathbb{Z}$ in degree 9, we replace Riemann-Roch computations over finite fields by linear algebra in the canonical ring (Section 8).

The groups $\mathbb{Z}/57\mathbb{Z}$ and $\mathbb{Z}/65\mathbb{Z}$ in degrees 6, 7 and 8, and the group $\mathbb{Z}/69\mathbb{Z}$, are treated in Section 9, partly on unramified covers of $X_0(57)$ and $X_0(69)$ that we construct over $\mathbb{F}_2$ by class field theory, and $\mathbb{Z}/54\mathbb{Z}$ in Section 10. Most of the groups $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with $m \geq 2$ are treated in Sections 11 and 12. In Section 13 we construct the sporadic points and determine all the points of the relevant degrees on several of the curves $X_1(m, n)$, and in this way we also exclude $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$ in degrees 6, 7 and 8, $\mathbb{Z}/36\mathbb{Z}$ in degree 6 and $\mathbb{Z}/39\mathbb{Z}$ in degrees 6 and 7. We prove Theorems 1.1 and 1.2 in Section 14, and the computations are described in Section 15.

Data availability and reproducibility. The code, the stored logs and the certificates of the computations described in this paper are available in four repositories, one for each degree:

`https://github.com/F-Najman/sextic_torsion`
`https://github.com/F-Najman/septic_torsion`
`https://github.com/F-Najman/octic_torsion`
`https://github.com/F-Najman/nonic-torsion`

This paper refers to the revisions `dbcd360`, `52af365`, `5cac315` and `14d4464` of these repositories, and the links in the paper point to these revisions. The `README` files there list, statement by statement, which script establishes each claim and which log it produced, and also the checks that the proofs do not need (see Section 15). Those of the septic, octic and nonic repositories use the numbering of this paper, and that of the sextic repository uses the numbering of a separate version of the proofs for degree 6. The code in the nonic repository for the prime orders is not used in this paper. 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 versions of the proofs and carried out most of the computations. Anthropic's Claude Opus 5.5 reviewed these versions, independently recomputed some of the computations (see Section 15) and the explicit examples, merged the proofs for the four degrees, wrote the draft

of the present manuscript and organized the code repositories. The degree 6 part of this paper, which I have checked carefully, will appear separately on arXiv.

2. Notation and auxiliary results

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 $\dim L(D) = \deg D + 1 - g + \dim \Omega(D)$, where g is the genus of X. For $i \geq 1$ we put $R_i := H^0(X, iK_X)$, where K_X is a canonical divisor.

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. From the description of the cusps of $X_1(n)$ in [DN25, §2] it follows that a cusp of $X_1(n)$ lying on a Néron k-gon is fixed by the diamond operator $\langle a \rangle$ (defined below) only if $a \equiv \varepsilon \pmod{k}$ and $a \equiv \varepsilon \pmod{n/k}$ for a common sign $\varepsilon = \pm 1$. In particular a is then congruent to ε modulo every prime dividing n. 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 $i(n) := i(1,n)$, so that $i(2,n) = 2i(n)$ for even 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 $(E,P,Q) \mapsto (E, aP, aQ)$, 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. It acts on divisors, on divisor

classes and on J. For $a_1, \dots, a_r \in (\mathbb{Z}/n\mathbb{Z})^\times$ we write $X/\langle a_1, \dots, a_r\rangle$ for the quotient of X by the subgroup of $\Delta(n)$ generated by $\langle a_1\rangle, \dots, \langle a_r\rangle$. 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 $\mathbb{Z}[\Delta(n)]$. For a prime $q \mid n$ we write U_q for the Hecke operator at q.

In characteristic q, on the ordinary locus, the quotient by the connected subgroup of order q gives the Frobenius, and the other q subgroups all reduce to the kernel of the Verschiebung and send (E,P) to $\langle q\rangle \operatorname{Frob}_q^{-1}(E,P)$. Hence, as correspondences on $X_{\mathbb{F}_q}$ and therefore on its Jacobian,

$$T_{q,\mathbb{F}_q} = \operatorname{Frob}_q + q\langle q\rangle \operatorname{Frob}_q^{-1} = \operatorname{Frob}_q + \langle q\rangle \operatorname{Ver}_q . \tag{5}$$

This is the Eichler-Shimura relation (see [DI95, (10.2.3)]).

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 $d \in \{6,7,8,9\}$ 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 $\varphi(m) \mid d$, and we put $d_m := d/\varphi(m) = [K : \mathbb{Q}(\zeta_m)]$. In particular $m \le 2$ if d is odd, as $\varphi(m)$ is even for $m > 2$. 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 $d = 7$, then the degree of x divides 7, and if $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \notin \Phi(1)$ then x is not rational by Mazur's theorem [Maz77], so D is a closed point of degree 7. This will be the case for all the groups that we have to rule out in degree 7. If $d = 9$, then $\mathbb{Q}(x) = K$ for all the groups that we need to exclude (Remark 3.2), so D is a closed point of degree 9. Isomorphism of pairs (K,E) is as in Section 1.

2.3. **Hecke operators and reduction.**

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 $q \equiv 1 \pmod m$.*

1. (Eichler-Shimura) $T_{q,\mathbb{F}_q} = \operatorname{Frob}_q + \langle q\rangle_{\mathbb{F}_q,*} \operatorname{Ver}_q$ *on $J_{X,\mathbb{F}_q}$, where $\mathbb{F}_q$ is the residue field of a prime of $\mathbb{Q}(\zeta_m)$ above q.*
2. *If $L \supseteq \mathbb{Q}(\zeta_m)$ is a number field in which q splits completely, then $A_q\big(J_X(L)_{\mathrm{tors}}\big) = 0$.*
3. *$A_q(C) = 0$ as a divisor for every $\mathbb{Q}(\zeta_m)$-rational cuspidal divisor C.*

(4) *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.*

Proof. For $X = X_1(m,n)$ with $m \leq 2$ these are, respectively, [DN25, (2.2)], [DN25, Proposition 2.6], [DN25, Lemma 2.8] and [DN25, Lemma 5.4]. For $m \geq 3$ the curve $X_1(m,n)$ is, over $\mathbb{Q}(\zeta_m)$, isomorphic to the quotient of $X_1(mn)$ by the diamond operators congruent to 1 modulo n [DS17, §2], and this isomorphism is compatible with T_q and $\langle q \rangle$ for $q \equiv 1 \pmod{m}$. Hence (1) follows from the Eichler-Shimura relation on $X_1(mn)$ [DI95, (10.2.3)], and the proofs of [DN25, Proposition 2.6, Lemma 2.8 and Lemma 5.4] carry over verbatim. The same proofs work on the quotients by subgroups of $\Delta(n)$, as T_q and $\langle q \rangle$ commute with the diamond operators. Part (3) is also the case $\sigma_q(C) = C$ of Lemma 2.3 below. □

We also need the action of T_q on all the cusps, not only on the rational ones, and also for $q = 2$.

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 $A_q C = 0$ for every cuspidal divisor C on $X_{\mathbb{F}_{p^f}}$ if $q \equiv p^{fk} \pmod{n}$ for some k.

Proof. This is the computation in the proof of [DN25, Lemma 2.8], carried out for an arbitrary cusp. Near a cusp the universal generalized elliptic curve is the Tate curve $\mathrm{Tate}(t) = \mathbb{G}_m/t^{\mathbb{Z}}$, and the points of the level structure are of the form $\zeta_n^a t^{b/n}$. The subgroups of order q of $\mathrm{Tate}(t)$ are μ_q, with quotient map $x \mapsto x^q$ to $\mathrm{Tate}(t^q)$, and the q subgroups generated by $\zeta_q^i t^{1/q}$, with quotient maps induced by the identity of $\mathbb{G}_m$ to $\mathrm{Tate}(\zeta_q^i t^{1/q})$. The first sends $\zeta_n^a t^{b/n}$ to $\zeta_n^{qa}(t^q)^{b/n}$, which gives the cusp $\sigma_q(c)$. The others send it to $\zeta_n^{a-ib} u^{qb/n}$ with $u = \zeta_q^i t^{1/q}$, and as the label a is only defined modulo multiples of b and q is invertible modulo n, all q of them give the same cusp, with labels (a, qb) for every point of the level structure. This is $\langle q \rangle \sigma_q^{-1}(c)$, as $\langle q \rangle$ multiplies both labels by q (for $m \geq 3$ note that $q \equiv 1 \pmod{m}$, so $\langle q \rangle$ fixes the point of order m). Letting $t \to 0$ gives the formula on $X_1(m,n)$. As T_q, $\langle q \rangle$ and σ_q commute with the diamond operators, the formula also holds on the quotients. The cuspidal subscheme is finite étale over $\mathbb{Z}[\zeta_m, \frac{1}{n}]$ and T_q extends over it, so the formula reduces modulo p, and if $q \equiv p^{fk} \pmod{n}$ then σ_q acts on the geometric cusps as a power of the Frobenius of $\mathbb{F}_{p^f}$, which fixes every closed cusp. □

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 $T_q = \langle q \rangle \mathrm{Frob}_q + q\,\mathrm{Frob}_q^{-1}$, with annihilator $T_q - \langle q \rangle - q$, and the formula of Lemma 2.3 reads $T_q c = \langle q \rangle \sigma_q(c) + q\sigma_q^{-1}(c)$. When we use such a model, we test both forms of the relevant divisors, so the results do not depend on the identification of the two conventions.

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. Indeed, this kernel is contained in the group of points of the formal group of the Néron model of A at λ with coordinates in the maximal ideal, and multiplication by 2 maps it into the subgroup of points with coordinates in the square of the maximal ideal, which is torsion-free as λ is unramified over 2. We apply this to J for $2 \nmid n$ and to the Jacobians of the quotients of $X_1(n)$ of positive genus (see Lemma 2.1);
- (*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 $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$,

$$\mathrm{gon}_{\mathbb{C}} X_\Gamma \geq \tfrac{325}{2^{15}} [\mathrm{PSL}_2(\mathbb{Z}) : \Gamma];$$

- (*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;
- (*Clark-Genao-Pollack-Saia* [CGPS22]) the exact values of the least degree $d_{\mathrm{CM}} X_1(n)$ of a CM point on $X_1(n)$ that we quote are taken from the list `dcm_list_all_min_orders_X1_10k.m` in the repository accompanying [CGPS22].

In degree 6 we compute all the values of Abramovich's bound and all the orders of diamond operators that we quote, and in degrees 7, 8 and 9 they are computed by the scripts linked in the corresponding proofs and tables.

We use Kato's theorem in the form of the *winding quotient*: 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.

Finally, we state the standard reduction results.

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 $\wp$.*

Proof. This is contained in the proof of [DN25, Proposition 5.2]. If E had additive reduction at $\wp$, the special fibre of the Néron model would have $a \cdot \#\mathbb{F}_\wp$ points over $\mathbb{F}_\wp$, where $a \leq 4$ is the order of the component group and $\#\mathbb{F}_\wp$ is a power of p. Reduction is injective on the prime-to-p torsion of $E(K)$, so $mn \mid a \leq 4$, contradicting $mn > 4$. □

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. We include the short proof.

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

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 $\mathfrak{p}$.

Here d plays the role of d_m in Section 2.2.

Proof. Let D be such a divisor, and suppose that its reduction modulo a prime $\mathfrak{p}$ of F above p is cuspidal. The cusps are defined over $\mathbb{Q}(\zeta_n)$, which is unramified above p, so the reduction of D lifts to a cuspidal divisor C over a number field $L \supseteq F$ which is unramified above p. The classes $[D - dc_0]$ and $[C - dc_0]$ are torsion, by assumption and by the Manin-Drinfeld theorem, so $[D - C]$ is a torsion point of $J_X(L)$ which reduces to 0 modulo a prime above $\mathfrak{p}$. If p is odd, then $[D-C] = 0$ by Katz's result, so $D \sim C$ over L, and $\ell(D) \geq 2$ as $D \neq C$. If $p = 2$, then $2[D - C] = 0$ by Parent's result, so $2D \sim 2C$ over L, and $\ell(2D) \geq 2$. As D is F-rational, $\ell(D)$ and $\ell(2D)$ do not change under extension of scalars from F to L, which contradicts $\operatorname{gon}_F X > d$, respectively $\operatorname{gon}_F X > 2d$.

For the last statement, let $x \in Y_1(m,n)(K)$ be the point given by E, and let D be its trace divisor (Section 2.2), which has degree d. If E had bad reduction at all the primes of K above $\mathfrak{p}$, then by Lemma 2.4 it would have multiplicative reduction at all of them, so all the geometric points of D would reduce to cusps modulo the primes above $\mathfrak{p}$, and the reduction of D modulo $\mathfrak{p}$ would be cuspidal. □

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 2.6, 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, which we carry out separately in each degree (the scripts for the degrees 6, 7, 8 and 9 are linked). For example, over $\mathbb{F}_{64}$ the possible traces of Frobenius are the odd integers t with $|t| \leq 16$ together with $t \in \{0, \pm 8, \pm 16\}$, so no elliptic curve over $\mathbb{F}_{64}$ has exactly 51, 55, 63, 75 or 77 points. If $\#E(\mathbb{F}_{64}) = 81$, then the Frobenius π satisfies $(\pi + 8)^2 = 0$, so $\pi = -8$ as $\operatorname{End}(E)$ has no non-zero nilpotents, and $E(\mathbb{F}_{64}) = \ker(1 - \pi) = E[9]$. Similarly, if $\#E(\mathbb{F}_{64}) = 49$, then $\pi = 8$ and $E(\mathbb{F}_{64}) = E[7]$. In general, an elliptic curve over $\mathbb{F}_{2^e}$ with even trace of Frobenius is supersingular, so its trace is 0 or $\pm 2^{(e+1)/2}$ for odd e, and 0, $\pm 2^{e/2}$ or $\pm 2^{e/2+1}$ for even e [Wat69, Theorem 4.1].

2.4. **Divisors and level automorphisms.**

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 $A \sim D$.*

1. *If $\operatorname{gon}_F X > d$, then $A = D$.*
2. *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.*

Proof. If $A \neq D$, a function f with $\operatorname{div}(f) = A - D$ is non-constant, and its degree is at most d. This proves (1). For (2), if D were contained in the support of A, then $A = D$ as both have degree d. So the supports of A and D are disjoint, and a function with divisor $D - A$ has degree exactly d. □

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. We will often use the following simple lemma. For subgroups of $\Delta(n)$, its first part is the argument at the end of the proof of [Naj26a, Proposition 7.2].

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 $\#G \mid \deg D$.*

Proof. If g fixes a geometric point (E,P,Q) in the support of D, then there is an automorphism u of E with $u(P,Q) = g(P,Q)$. As E has no complex multiplication, $u = \varepsilon$ with $\varepsilon = \pm 1$, so $g(P,Q) = (\varepsilon P, \varepsilon Q)$. As g is given by integral linear combinations which do not depend on the point, and P,Q generate a group isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, it follows that g maps every triple (E',P_1,Q_1) to $(E',\varepsilon P_1, \varepsilon Q_1)$, which is isomorphic to (E',P_1,Q_1). So g is the identity of $X_1(m,n)$. If $gD = D$ for all $g \in G$, then D has the same coefficient at x and at gx, so the geometric points in the support of D form a union of G-orbits and the coefficients of D are constant on each of them. By the first part, each orbit has length $\#G$. □

We will also often use the following lemma, whose proof is the same as that of Proposition 2.5.

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 $gC = C$.

Proof. The class $y := [gD - D - gC + C] \in J_X(L)$ equals $(g-1)[D - dc_0] - (g-1)[C - ec_0] + (d-e)[gc_0 - c_0]$, so it is torsion, by the assumption on g and by the Manin-Drinfeld theorem. It reduces to 0, so $y = 0$ if p is odd and $2y = 0$ if $p = 2$. In case (d) the class y lies in $J_X(F)[2]$, so $gy = y$, and if r is the order of g, then $ry = (1 + g + \cdots + g^{r-1})y$ is the class of the divisor $(g^r - 1)(D - C) = 0$. As r is odd and $2y = 0$, it follows that $y = 0$. Hence $gD + C \sim D + gC$ in cases (a), (b) and (d), and $2gD + 2C \sim 2D + 2gC$ in case (c), over L, and over F in cases (a) and (d). Lemma 2.7 gives the claim. □

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 $\chi(a) = 1$.

We also use the following form of the Mordell-Weil sieve with quadratic characters.

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.*

Proof. By Weil reciprocity, for a function g whose divisor is disjoint from that of f we have $\chi_f(\operatorname{div} g) = g(\operatorname{div} f) = g(A)^2$, which is a square. So χ_f is trivial on principal divisors, and by the moving lemma it induces a homomorphism on $\operatorname{Pic}^0(C)$, whose values have order dividing 2. □

2.5. **Complex multiplication and fields of odd degree.**

Lemma 2.11. *Let E be an elliptic curve with complex multiplication over a number field K of degree d.*

1. *If $d = 7$, then $E(K)_{\mathrm{tors}}$ is isomorphic to one of $\{0\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*
2. *If $d = 8$, then $E(K)_{\mathrm{tors}}$ belongs to $\Phi^\infty(8) \cup \{\mathbb{Z}/34\mathbb{Z}, \mathbb{Z}/39\mathbb{Z}, \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}\}$.*
3. *If $d = 9$, then $E(K)_{\mathrm{tors}}$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ with $n \in \{1, 2, 3, 4, 6, 9, 14, 18, 19, 27\}$ or to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In particular it lies in $\Phi^\infty(9)$.*

Proof. Part (1) follows from the Strong Odd Degree Theorem of Bourdon and Pollack [BP17, Theorem 1.2]. Apart from the four groups $\{0\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the possible groups are $\mathbb{Z}/\ell^k\mathbb{Z}$ and $\mathbb{Z}/2\ell^k\mathbb{Z}$ for primes $\ell \equiv 3 \pmod 4$, and these occur in degree 7 only if 7 is divisible by $\frac{\ell-1}{2}$ times the class number of $\mathbb{Q}(\sqrt{-\ell})$. This leaves $\ell = 3$, and for $\ell = 3$ and $k \geq 2$ the degree has to be divisible by 3.

For (2), by [CCRS14, Section 4.8], $E(K)_{\mathrm{tors}}$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ with

$$n \in \{1, \dots, 8, 10, 12, 13, 15, 16, 20, 21, 28, 30, 34, 39\},$$

to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with $n \in \{2, 4, 6, 8, 10, 12, 16, 20\}$, to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with $n \in \{4, 8, 12\}$, or to one of $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Comparing with (3) proves (2).

Part (3) is [CCRS14, Section 4.9]. □

Let $d \in \{7, 8, 9\}$, and let $\mathcal{G}_d$ be the union of $\Phi^\infty(d)$ and the sporadic groups of Theorem 1.1 in degree d, which is closed under passing to subgroups (see Section 3). By Lemma 2.11, if $E(K)$ contains a subgroup which is not in $\mathcal{G}_d$, then E does not have complex multiplication, so in degrees 7, 8 and 9 Lemma 2.8 applies to all the trace divisors that we consider. For fields of odd degree we have the following stronger statement, which we use in degree 9.

Lemma 2.12. *Let K be a number field of odd degree and let E/K be an elliptic curve. Then $\operatorname{End}_K(E) = \mathbb{Z}$ and $\operatorname{Aut}_K(E) = \{\pm 1\}$. Let x be a point of odd degree on $Y_1(m, n)$ and let g be a level automorphism of $X_1(m, n)$ which is not the identity. Then g fixes no geometric point above x. In particular, if D is an effective divisor whose support consists of non-cuspidal points of odd degree and $gD = D$, then every orbit of the group generated by g*

on the geometric points in the support of D has length equal to the order of g, so the order of g divides $\deg D$.

Proof. An endomorphism of E acts on the invariant differential by multiplication by an element of K, which gives an injection $\mathrm{End}_K(E) \to K$. The image of an endomorphism outside $\mathbb{Z}$ would generate an imaginary quadratic subfield of K, which is impossible as $[K : \mathbb{Q}]$ is odd. If g fixes a geometric point (E, P, Q) above x, then there is an automorphism α of E with $\alpha(P, Q) = g(P, Q)$. It is unique, as $X_1(m, n)$ is a fine moduli space, so it is defined over the residue field $\mathbb{Q}(x)$, and it is not ± 1, as g is not the identity. This contradicts the first part applied to $E/\mathbb{Q}(x)$. The same applies to every non-trivial power of g, which proves the last assertion. □

We will also need the following special case of a result of Derickx and Stoll.

Lemma 2.13 ([DS25, Proposition 2.2])**.** *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 $L = 0$.*

Here $A_q = h_1(T_q) - h_2(T_q)$ for the polynomials $h_1(x) = x$ and $h_2(x) = 1 + q\langle q \rangle$, in the notation of [DS25].

3. 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 $m \mid n$. For $d \in \{6, 7, 8, 9\}$ let $\mathcal{G}_d$ be the union of $\Phi^\infty(d)$ and the sporadic groups in degree d listed in Theorem 1.1. Each $\mathcal{G}_d$ is closed under passing to subgroups, and by the realizations in Section 13 it is contained in $\Phi(d)$. Recall from Section 1 that $S(6) = \{2, 3, 5, 7, 11, 13, 17, 19, 37\}$, that $S(7)$ and $S(8)$ are the sets of primes up to 23, and that $S(9)$ is the set of primes up to 31 [Naj26c].

Lemma 3.1. *For $d \in \{6, 7, 8, 9\}$ let $\mathcal{M}_d$ be the set of groups $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with $m \mid n$ such that $\varphi(m) \mid d$, every prime dividing n lies in $S(d)$, $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \notin \mathcal{G}_d$, and every proper subgroup of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ lies in $\mathcal{G}_d$. Then $\mathcal{M}_6$ consists of the following 66 groups:*

$$\begin{aligned}
&\mathbb{Z}/n\mathbb{Z} \text{ for } n \in \{32, 33, 34, 35, 36, 38, 39, 40, 42, 44, 45, 48, 49, 50,\\
&\qquad 51, 52, 54, 55, 56, 57, 60, 63, 65, 75, 77, 81, 85, 91, 95,\\
&\qquad 119, 121, 125, 133, 143, 169, 187, 209, 221, 247, 289, 323, 361\},\\
&\mathbb{Z}/37n\mathbb{Z} \text{ for } n \in \{2, 3, 5, 7, 11, 13, 17, 19, 37\},\\
&\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \text{ for } n \in \{11, 13, 14, 15\},\\
&\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z} \text{ for } n \in \{5, 6, 7, 8, 9\},\\
&\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4n\mathbb{Z} \text{ for } n \in \{4, 5, 6\},\\
&\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}, \quad \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}, \quad \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z},
\end{aligned}$$

$\mathcal{M}_7$ consists of the following 58 groups:

$$\begin{aligned}
&\mathbb{Z}/n\mathbb{Z} \text{ for } n \in \{32, 34, 35, 38, 39, 40, 42, 44, 45, 46, 48, 49, 50, 51, 52, 54, 55, 56, 57, 60,\\
&\qquad 63, 65, 66, 69, 72, 75, 77, 81, 85, 91, 95, 99, 115, 119, 121, 125, 133, 143, 161,\\
&\qquad 169, 187, 209, 221, 247, 253, 289, 299, 323, 361, 391, 437, 529\},\\
&\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \text{ for } n \in \{11, 12, 13, 14, 15, 18\},
\end{aligned}$$

$\mathcal{M}_8$ consists of the following 80 groups:

$$\begin{aligned}
&\mathbb{Z}/n\mathbb{Z} \text{ for } n \in \{38, 44, 45, 46, 48, 49, 50, 51, 52, 54, 55, 56, 57, 60, 63,\\
&\quad 64, 65, 66, 68, 69, 70, 72, 75, 77, 78, 80, 81, 84, 85, 91, 95, 99, 105,\\
&\quad 115, 117, 119, 121, 125, 133, 143, 161, 169, 175, 187, 209, 221, 247,\\
&\quad 253, 289, 299, 323, 361, 391, 437, 529\},\\
&\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \text{ for } n \in \{13, 14, 15, 16, 17, 18, 20, 21\},\\
&\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z} \text{ for } n \in \{6, 7, 8, 9, 10, 11, 13\},\\
&\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4n\mathbb{Z} \text{ for } n \in \{4, 5, 6\},\\
&\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5n\mathbb{Z} \text{ for } n \in \{3, 4, 5, 7\},\\
&\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}, \quad \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z},
\end{aligned}$$

and $\mathcal{M}_9$ consists of the following 81 groups:

$$\begin{aligned}
&\mathbb{Z}/n\mathbb{Z} \text{ for } n \in \{35, 38, 44, 45, 46, 48, 49, 50, 51, 52, 54, 55, 56, 57, 58, 60, 62, 63, 64, 65,\\
&\quad 66, 68, 69, 72, 75, 77, 78, 80, 81, 84, 85, 87, 91, 93, 95, 99, 115, 117, 119, 121, 125,\\
&\quad 133, 143, 145, 155, 161, 169, 187, 203, 209, 217, 221, 247, 253, 289, 299, 319, 323,\\
&\quad 341, 361, 377, 391, 403, 437, 493, 527, 529, 551, 589, 667, 713, 841, 899, 961\},\\
&\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \text{ for } n \in \{14, 15, 16, 17, 18, 20, 21\}.
\end{aligned}$$

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

Proof. By the Weil pairing and by the description of $S(d)$ above, every group in $\Phi(d)$ is of the form $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with $\varphi(m) \mid d$ and with all the primes dividing n in $S(d)$. As $\mathcal{G}_d$ is closed under passing to subgroups, a group in $\Phi(d) \setminus \mathcal{G}_d$ contains a subgroup of minimal order which is not in $\mathcal{G}_d$, and this subgroup lies in $\mathcal{M}_d$. If $\mathbb{Z}/n\mathbb{Z} \in \mathcal{M}_d$ then $\mathbb{Z}/(n/p)\mathbb{Z} \in \mathcal{G}_d$ for every prime $p \mid n$, so n is at most the largest element of $S(d)$ times the largest n' with $\mathbb{Z}/n'\mathbb{Z} \in \mathcal{G}_d$, and if $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \in \mathcal{M}_d$ with $m > 1$ then $\mathbb{Z}/n\mathbb{Z} \in \mathcal{G}_d$. It remains to run through these finitely many groups, which we do by computer in each degree (the scripts for $d = 6$, $d = 7$, $d = 8$ and $d = 9$ are linked). The computation for $d = 9$ uses the primes up to 89 instead of $S(9)$, and gives in addition the 13 groups $\mathbb{Z}/p\mathbb{Z}$ with $37 \leq p \leq 89$, which are not in $\mathcal{M}_9$ as $p \notin S(9)$. □

Remark 3.2. No group in $\Phi(1) \cup \Phi(3)$ has a subgroup isomorphic to a group in $\mathcal{M}_9$ [Maz77, DEvH+21], so if E/K has a subgroup isomorphic to a group in $\mathcal{M}_9$ and $[K : \mathbb{Q}] = 9$, the corresponding point x has $\mathbb{Q}(x) = K$, and the trace divisor is a closed point of degree 9. The same holds for the points on $X_1(33)$, $X_1(39)$ and $X_1(2, 26)$ of degree 9 that we consider in Sections 11 and 13.

To rule out a group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \in \mathcal{M}_d$ 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 $[K : \mathbb{Q}] = d$.

Several members of $\mathcal{M}_d$ are reduced to others by a 2-isogeny.

Lemma 3.3. *Let $k \geq 2$. There is a $\mathbb{Q}$-rational morphism $X_1(4k) \to X_1(2, 2k)$, $(E, P) \mapsto \big(E/\langle 2kP\rangle, Q, P \bmod \langle 2kP\rangle\big)$, where Q generates $E[2]/\langle 2kP\rangle$. Hence, if $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field K, then neither is $\mathbb{Z}/4k\mathbb{Z}$.*

Proof. The morphism is the one described in [DN25, §2] (see also [DS17, §2]). It maps non-cuspidal points to non-cuspidal points, and the image of a point defined over K is defined over K, as it only uses the rational 2-isogeny $E \to E/\langle 2kP\rangle$. □

In each degree Lemma 3.3 reduces $\mathbb{Z}/4k\mathbb{Z}$ to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}$ whenever the latter is in $\mathcal{M}_d$. It does not apply to $\mathbb{Z}/48\mathbb{Z}$ for $d = 6, 8, 9$ and to $\mathbb{Z}/52\mathbb{Z}$ for $d = 9$, as $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$, respectively $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$, lies in $\Phi(d)$, and we treat these groups in Propositions 11.14 to 11.16. Section 14 lists where each of the groups in $\mathcal{M}_d$ is excluded.

4. 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] (Section 4.1) and by its version at the prime 2, in which we use several diamond operators at once (Section 4.2). The group $\mathbb{Z}/81\mathbb{Z}$ is excluded in all four degrees in Section 4.3, and the groups $\mathbb{Z}/133\mathbb{Z}$ and $\mathbb{Z}/247\mathbb{Z}$ in degree 9 need further arguments, which we give in Section 4.4.

Throughout the section we use the following consequence of Kato's theorem, as in [Naj26a, §7 and the proof of Proposition 4.1]. The isogeny decomposition

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

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. Hence, for $\psi = \sum_a c_a \langle a \rangle \in \mathbb{Z}[\Delta(n)]$, the group $\psi\big(J_1(n)(\mathbb{Q})\big)$ is finite if $\sum_a c_a \chi_f(a) = 0$ for every newform f of level dividing n with $L(f,1) = 0$. All the analytic ranks that we take from the LMFDB [LMF26] are recorded there as proved. We check them and the character values for the levels that occur in degree 6, and the scripts that check them in the other degrees are linked in the proofs below.

4.1. **The global method.** The main tool is the global method of Derickx [DN25, Proposition 4.3], which we recall for a number field of degree d, as in [Naj26a, Section 4]. Let n 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 moreover 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 $k_q = 2(q+1)$ otherwise. If $dk_q < \operatorname{gon}_{\mathbb{Q}} X_1(n)$, then every effective rational divisor of degree d on $X_1(n)$ whose support contains no cusp is a sum of orbits under $\langle a \rangle$. Using Abramovich's bound, the inequality holds as soon as

$$b(n) := \frac{325}{2^{15}} \cdot \frac{i(n)}{k_q} > d, \qquad \text{where } i(n) = [\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma_1(n)}].$$

For $q = 2$ the proof of [DN25, Proposition 4.3] 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. We use $q = 3$, except for $n = 115$ in degree 9, where we use $q = 2$.

For the levels 115, 161, 253, 299, 391, 437 and 529 we obtain the finiteness of $(\langle a \rangle - 1)J_1(n)(\mathbb{Q})$ from the following lemma, which we also use for $n = 99$ in Proposition 4.4.

Lemma 4.1. *Let $n \in \{99, 115, 161, 253, 299, 391, 437, 529\}$. Then $L(f,1) \neq 0$ for every newform f of weight 2 and level dividing n with non-trivial character. In particular, $(\langle a \rangle - 1)J_1(n)(\mathbb{Q})$ is finite for every $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.*

Proof. For each n and each Galois orbit of non-trivial even Dirichlet characters χ modulo n, we compute, using modular symbols, the plus quotient S_χ of the space of cusp forms of weight 2 and character χ, and its winding submodule W_χ, the Hecke module generated by the projection of the winding element. In every case $W_\chi = S_\chi$. For $n = 529$ and χ of order

253 we verify this instead by computing the projection v of the winding element and the operator T_2, and checking that $v, vT_2, \dots, vT_2^{44}$ have rank $45 = \dim S_\chi$ modulo the prime 2531, which splits completely in the field of values of χ and at which all the denominators are units. As a check that no factor is missed, the sum of $\varphi(\operatorname{ord}\chi)\dim S_\chi$ over all orbits, including the trivial character, equals the genus of $X_1(n)$, which is 281, 441, 925, 2421, 3433, 5985, 7525 and 11265, respectively. It follows that $L(f,1) \neq 0$ for every newform f of level dividing n with non-trivial character. As $\langle a\rangle - 1$ kills the factors of $J_1(n)$ with trivial character, Kato's theorem shows that $(\langle a\rangle - 1)J_1(n)(\mathbb{Q})$ is finite. □

Proposition 4.2. *Let n and d be as in one of the rows of Table 1. 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 d.*

Proof. For each row we take q and a as in Table 1, and we first show that $(\langle a\rangle - 1)J_1(n)(\mathbb{Q})$ is finite, and that it has odd order in the row with $q = 2$.

For the 11 levels of the rows with $d = 6, \dots, 9$ we use the elements a from [Naj26a, Table 2]. For $n \in \{119, 121, 125, 169, 221, 289, 361\}$ every newform of weight 2 and level dividing n with positive analytic rank has trivial character, and for the remaining n the newforms of positive analytic rank and non-trivial character have character orbits 143.h, 187.g, 209.f and 323.k, and a lies in the kernel of each of them. So $(\langle a\rangle - 1)J_1(n)(\mathbb{Q})$ is finite, as is also shown in the proofs of [Naj26a, Propositions 4.1 and 4.2]. For $n = 133$ and $n = 247$ the newforms of positive analytic rank have trivial character or a character in one of the orbits listed in Table 2, and these characters are trivial on a: for $n = 133$ as $64 = 2^6$ and the characters have order 3 or 6, and for $n = 247$ as $144 = 12^2$ and the characters are trivial on 12. We check the entries of Table 1 in the rows with $d = 6, \dots, 9$. An LMFDB search confirms the data above for these 13 levels, and that all the other newforms of these levels have analytic rank 0.

For $n \in \{115, 161, 253, 299, 391, 437, 529\}$ and $a = 3$ the finiteness follows from Lemma 4.1. For the 17 levels that occur only in degree 9 we compute (with `common/winding_probe.m`, and with `large_levels/winding_probe_krylov.m` for the levels 551, 667, 713, 841, 899 and 961) that the winding submodule is the whole space of modular symbols with character χ for every Galois orbit of even characters χ modulo n with $\chi(a) \neq 1$, and we check the character values. For the characters of large order at the levels 841, 899 and 961 (and again at the level 529) we check this modulo a suitable prime, as in the proof of Lemma 4.1.

For $n = 115$ and $d = 9$ we use $q = 2$ and $a = 16$. Then $(\langle 16\rangle - 1)J_1(115)$ is isogenous to the part of $J_1(115)$ with characters of order 11, 22 and 44, which has dimension 400, and it has finitely many rational points by Lemma 4.1. For each of these three character orbits we compute the norm of $\det\big((1 + 3\chi(3)) - T_3\big)$ on the corresponding space of cusp forms, which is a power of the number of $\mathbb{F}_3$-points of the corresponding factor, and we find that all three are odd. Hence $(\langle 16\rangle - 1)J_1(115)(\mathbb{Q})$ has odd order, as it injects into the group of $\mathbb{F}_3$-points.

By Table 1 we have $b(n) > d$ in every row, so the trace divisor D of a point of order n over a number field of degree d is a sum of $\langle a\rangle$-orbits. Its support consists of non-CM points, for $d = 6$ as $d_{\mathrm{CM}}X_1(n) > 6$, and for $d \geq 7$ by Lemma 2.11. So by Lemma 2.8 each of these orbits has length $\operatorname{ord}\langle a\rangle$, the order of $\langle a\rangle$ in $\Delta(n)$, and $\operatorname{ord}\langle a\rangle$ divides d, which contradicts Table 1. □

n	d	q	a	$\mathrm{ord}\langle a\rangle$	k_q	$i(n)$	$b(n)$	$d_{\mathrm{CM}}X_1(n)$
115	7, 8	3	3	44	7	6336	8.97	
115	9	2	16	11	6	6336	10.47	
119	6–9	3	3	48	7	6912	9.79	96
121	6–9	3	2	55	8	7260	9.00	110
125	6–9	3	3	50	7	7500	10.62	50
133	7, 8	3	64	3	8	8640	10.71	
143	6–9	3	67	12	8	10080	12.49	120
145	9	3	3	14	7	10080	14.28	
155	9	3	16	5	8	11520	14.28	
161	7–9	3	3	66	7	12672	17.95	
169	6–9	3	3	39	7	14196	20.11	52
187	6–9	3	122	16	8	17280	21.42	160
203	9	3	6	7	8	20160	24.99	
209	6–9	3	34	18	8	21600	26.77	180
217	9	3	3	15	7	23040	32.64	
221	6–9	3	3	48	7	24192	34.27	96
247	7, 8	3	144	3	8	30240	37.49	
253	7–9	3	3	55	7	31680	44.88	
289	6–9	3	3	136	7	41616	58.96	136
299	7–9	3	3	33	7	44352	62.84	
319	9	3	3	140	7	50400	71.41	
323	6–9	3	101	18	8	51840	64.27	288
341	9	3	32	2	8	57600	71.41	
361	6–9	3	3	171	7	64980	92.06	114
377	9	3	5	28	8	70560	87.47	
391	7–9	3	3	176	7	76032	107.72	
403	9	3	92	2	8	80640	99.97	
437	7–9	3	3	198	7	95040	134.66	
493	9	3	3	112	7	120960	171.38	
527	9	3	3	240	7	138240	195.87	
529	7–9	3	3	253	7	139656	197.87	
551	9	3	12	12	8	151200	187.45	
589	9	3	3	45	7	172800	244.83	
667	9	3	3	308	7	221760	314.20	
713	9	3	2	55	8	253440	314.20	
841	9	3	12	58	8	353220	437.91	
899	9	3	3	420	7	403200	571.28	
961	9	3	3	465	7	461280	653.58	

TABLE 1. The pairs (n, d) of Proposition 4.2, the group $\mathbb{Z}/n\mathbb{Z}$ being excluded in all the degrees d in the second column. The order of $\langle a\rangle$ is its order in $\Delta(n)$, and $b(n)$ is rounded down to two decimal places (for $n = 121$ we have $b(n) = 9.0007\ldots$). The least degree $d_{\mathrm{CM}}X_1(n)$ of a CM point on $X_1(n)$ is given only in the rows with $d = 6, \ldots, 9$, as we use it only for $d = 6$.

4.2. **Several diamond operators.** For the levels $n = 77, 85, 91, 95, 133, 247$ the global method does not apply in degree 6, either because $\mathrm{ord}\langle a\rangle \mid 6$ for every a with $(\langle a\rangle - 1)J_1(n)(\mathbb{Q})$ finite, or because the gonality bound is too weak. In [Naj26a] the levels 91, 95,

133 and 247 were handled by the global method, with $a = 3, 11, 64, 144$, but the orders of these diamond operators, 6, 3, 3 and 3, divide 6. For these levels we work at the prime 2, and we use more general elements of the group ring of the diamond operators, such as $1 + \langle 31\rangle$ and $(\langle 6\rangle - 1)(\langle 3\rangle - 1)$, together with an argument with $X_0(91)$. We use the same method in degree 7 at the levels 77, 85, 91, 95 and 99, in degree 8 at the levels 85, 91 and 95, and in degree 9 at the levels 95 and 99 (Propositions 4.4 and 4.7).

Proposition 4.3. *Let n be odd, let $\psi \in \mathbb{Z}[\Delta(n)]$ be such that $\psi\big(J_1(n)(\mathbb{Q})\big)$ is finite, and write $\|\psi\|$ for the sum of the absolute values of its coefficients. Let $d \in \{6, 7, 8, 9\}$ and assume that $\operatorname{gon}_{\mathbb{C}} X_1(n) > 2d\|\psi\|$. Let K be a number field of degree d, let E/K be an elliptic curve with a point of order n, and suppose that E has bad reduction at every prime of K above 2. Then the trace divisor D satisfies $\psi(D) = 0$.*

Proof. By Lemma 2.4 the reduction of E at every prime of K above 2 is multiplicative, so the reduction of D modulo a prime $\wp$ of $L := \mathbb{Q}(\zeta_n)$ above 2 is cuspidal. As the cuspidal subscheme is finite étale over $\mathbb{Z}[\frac{1}{n}]$ and all cusps are defined over L, it lifts to an effective cuspidal divisor C of degree d on $X_1(n)_L$. The class $\psi[D - C] = \psi[D - dc_0] + \psi[dc_0 - C]$ is torsion, as $\psi\big(J_1(n)(\mathbb{Q})\big)$ is finite and by Manin-Drinfeld, and it reduces to 0 modulo $\wp$, so $2\psi[D - C] = 0$ by Parent's result, as 2 is unramified in L. Writing $\psi = \psi^+ - \psi^-$, where ψ^+ and ψ^- are the positive and negative parts of ψ, the effective divisors $2\psi^+(D) + 2\psi^-(C)$ and $2\psi^-(D) + 2\psi^+(C)$, of degree $2d\|\psi\|$, are linearly equivalent. As $\operatorname{gon}_L X_1(n) \geq \operatorname{gon}_{\mathbb{C}} X_1(n) > 2d\|\psi\|$, they are equal by Lemma 2.7, so $\psi(D) = \psi(C)$. The diamond operators preserve the set of cusps and its complement, and D has no cusps in its support, so $\psi(D) = 0$. □

We will apply Proposition 4.3 with $\psi = \langle a\rangle - 1$, in which case its conclusion is that D is invariant under $\langle a\rangle$, and with a few other elements. Note that the case $\psi = \langle a\rangle - 1$ is the degree d version of [Naj26a, Proposition 7.2], and that it is also the case of Lemma 2.9(c) in which C is the lift of the reduction of D.

n	characters of the newforms of positive analytic rank	$d_{\mathrm{CM}} X_1(n)$	$\frac{325}{2^{15}} i(n)$
77	trivial	60	28.56
85	trivial, 85.j (order 4)	32	34.27
91	trivial, 91.g (order 3), 91.u (order 6)	24	39.99
95	95.l (order 12)	72	42.84
133	trivial, 133.f (order 3), 133.s (order 6)	36	85.69
247	trivial, 247.be (order 12)	72	299.92

TABLE 2. The newforms of weight 2 and level dividing n with positive analytic rank, listed by their character orbits, and the data used in Propositions 4.4 and 4.5, with $i(n)$ as in Table 1. Their Conrey labels are 85.4, 91.9, 91.30, 95.8, 133.39, 133.31 and 247.8.

Proposition 4.4. *The group $\mathbb{Z}/n\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree d for $n \in \{77, 91\}$ and $d \in \{6, 7\}$, for $n = 85$ and $d \in \{6, 7, 8\}$, for $n = 95$ and $d \in \{6, 7, 8, 9\}$, and for $n = 99$ and $d \in \{7, 9\}$.*

Proof. Let E be such an elliptic curve over a number field K of degree d, and let D be the trace divisor of the corresponding point of $X_1(n)$. Its support consists of non-CM points, for

$d = 6$ as $d_{\mathrm{CM}} X_1(n) > 6$ (Table 2) and for $d \geq 7$ by Lemma 2.11. No elliptic curve over $\mathbb{F}_{2^e}$ with $e \leq d$ has a point of order n. For $e \leq 6$ this follows from the Hasse bound, as such a curve has at most 81 points, and for $n = 77$ and $e = 6$ from the discussion after Lemma 2.6. For $e = 7$ the Hasse interval $[107, 151]$ contains no multiple of n, for $e = 8$ and $n = 85$ we compute this, and for $e \in \{8, 9\}$ and $n \in \{95, 99\}$ the Hasse bound leaves only the group order 285 for $e = 8$ and the group orders 475 and 495 for $e = 9$, with traces -28, 38 and 18, which are even and not traces of supersingular curves (see the discussion after Lemma 2.6). So by Lemma 2.6 the curve E has bad reduction at every prime of K above 2.

For $n = 77, 85, 91, 99$ take $\psi = \langle a \rangle - 1$ with $a = 3, 2, 3, 2$, so that $\langle a \rangle$ has order $30, 8, 6, 15$ in $\Delta(n)$, and for $n = 95$ take $\psi = 1 + \langle 31 \rangle$. By Table 2 and an LMFDB search, for $n = 77, 85, 91$ every newform of weight 2 and level dividing n with positive analytic rank has trivial character or a character χ with $\chi(a) = 1$, and for $n = 95$ every such newform has a character χ with $\chi(31) = -1$, as we compute. For $n = 99$ we use Lemma 4.1. So $\psi\big(J_1(n)(\mathbb{Q})\big)$ is finite. As $\|\psi\| = 2$ and $\operatorname{gon}_{\mathbb{C}} X_1(n) > 28.56, 34.27, 39.99, 42.84, 42.84$ for $n = 77, 85, 91, 95, 99$ (Table 2, and $i(99) = 4320$), which is larger than $4d$ in every case, Proposition 4.3 gives $\psi(D) = 0$.

For $n = 95$ this says that $D + \langle 31 \rangle D = 0$, which is impossible for a non-zero effective divisor. Otherwise $\langle a \rangle D = D$, and by Lemma 2.8 the order of $\langle a \rangle$ divides d, a contradiction unless (n, d) is $(91, 6)$ or $(85, 8)$. In these two cases D is a single $\langle a \rangle$-orbit of length d with multiplicity 1, so its image on $X_1(n)/\langle a \rangle$ is a single point, which is rational as D is rational. Hence $X_0(n)$ has a rational non-cuspidal point, which is impossible, as $X_0(91)$ has no rational non-cuspidal points [Ken80] and there are no cyclic 85-isogenies over $\mathbb{Q}$ [Maz78, Ken82]. □

Proposition 4.5. *The groups $\mathbb{Z}/133\mathbb{Z}$ and $\mathbb{Z}/247\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over a sextic field.*

Proof. Let $n \in \{133, 247\}$, and let D be the trace divisor of a point of order n over a sextic field K. By the Hasse bound no elliptic curve over $\mathbb{F}_{2^f}$ with $f \leq 6$ has a point of order n, so by Lemma 2.6 the elliptic curve has bad reduction at every prime of K above 2, and Proposition 4.3 applies to D. As $d_{\mathrm{CM}} X_1(n) > 6$ (Table 2), the support of D consists of non-CM points.

For $n = 133$, let χ_f and χ_s be characters in the orbits 133.f and 133.s. We compute that $\chi_f(6) = 1$ and $\chi_s(3) = 1$, so

$$\psi = (\langle 6 \rangle - 1)(\langle 3 \rangle - 1), \qquad \|\psi\| = 4, \qquad 12\|\psi\| = 48 < 85.69,$$

annihilates every factor of positive analytic rank, and Proposition 4.3 gives $\psi(D) = 0$. Hence the divisor $D_1 := \langle 3 \rangle D - D$ satisfies $\langle 6 \rangle D_1 = D_1$. Its support consists of non-CM points, so by Lemma 2.8 its geometric points form a union of $\langle 6 \rangle$-orbits of length $\operatorname{ord}\langle 6 \rangle = 18$. But these are among the at most 12 geometric points in the supports of D and $\langle 3 \rangle D$, and hence $D_1 = 0$. So $\langle 3 \rangle D = D$, and since $\langle 3 \rangle$ has order 9, we get $9 \mid \deg D = 6$, which is a contradiction.

For $n = 247$, the characters in 247.be are trivial on 12 and on 56, so Proposition 4.3 gives $\langle 12 \rangle D = \langle 56 \rangle D = D$. We compute that $\langle 12 \rangle$ and $\langle 56 \rangle$ generate a subgroup of order 9 of $\Delta(247)$, so by Lemma 2.8, D is a sum of orbits of length 9 of this subgroup, and $9 \mid \deg D = 6$, which is a contradiction. □

Lemma 4.6. *Let s and t be commuting permutations of a set S, of orders 3 and 6, which generate a group isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ acting freely on S. If a finitely supported divisor Z on S satisfies $(s-1)(t-1)Z = 0$, then $3 \mid \deg Z$.*

Proof. Fix a point $z \in S$ and write the coefficient of $s^i t^j z$ in Z as z_{ij}, for $i \in \mathbb{Z}/3\mathbb{Z}$ and $j \in \mathbb{Z}/6\mathbb{Z}$. The condition says that $z_{ij} - z_{i+1,j} - z_{i,j+1} + z_{i+1,j+1} = 0$ for all i, j, so $z_{ij} = r_i + b_j$ for some integers r_i and b_j, and the sum of the coefficients on the orbit of z is $6\sum_i r_i + 3\sum_j b_j$. So 3 divides the sum of the coefficients on each orbit, and hence $3 \mid \deg Z$. □

Proposition 4.7. *The group $\mathbb{Z}/91\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over an octic field.*

Proof. Put $t = \langle 3 \rangle$ and $s = \langle 16 \rangle$, which have orders 6 and 3 in $\Delta(91)$ and generate a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. As in the proof of Proposition 4.4, the group $(t-1)J_1(91)(\mathbb{Q})$ is finite. Let D be the trace divisor of a point of order 91 over an octic field K. Its support consists of non-CM points by Lemma 2.11, so by Lemma 2.8 the group generated by s and t acts freely on it.

We compute that the only $e \leq 8$ such that an elliptic curve over $\mathbb{F}_{2^e}$ has a point of order 91 is $e = 8$. Suppose first that E has bad reduction at every prime of K above 2. Then Proposition 4.3 with $\psi = t - 1$ applies, as $\operatorname{gon}_{\mathbb{C}} X_1(91) > 39.99 > 32$, and gives $tD = D$, which is impossible by Lemma 2.8, as t has order 6.

So E has good reduction at a prime of K above 2 of residue degree 8, which is the unique prime of K above 2, and the reduction $\overline{D}$ of D is a closed point of degree 8 of $X_1(91)_{\mathbb{F}_2}$. We compute that there are exactly two elliptic curves over $\mathbb{F}_{256}$ with a point of order 91, up to isomorphism. Both have $j = 0$ and cyclic group of order 273, and for a point P of order 91 on either of them the points uP, for u running over the automorphisms of the curve, are the points aP with $a \in \{\pm 1, \pm 16, \pm 74\}$. Hence $s\overline{D} = \overline{D}$.

Consider the divisor $Z := (s-1)(t-1)D = stD + D - sD - tD$ of degree 0. Its class $[Z] = (s-1)(t-1)[D - 8c_0] + 8[(s-1)(t-1)c_0]$ is rational and torsion, as $(t-1)J_1(91)(\mathbb{Q})$ is finite and by Manin-Drinfeld, and it reduces to $[(t-1)(s-1)\overline{D}] = 0$. By Parent's result $2[Z] = 0$, so $2Z$ is principal. Its positive part $2stD + 2D$ has degree $32 < \operatorname{gon}_{\mathbb{C}} X_1(91)$, so $2Z = 0$ and $(s-1)(t-1)D = 0$. As the group generated by s and t acts freely on the support of D, Lemma 4.6 gives $3 \mid 8$, which is a contradiction. □

4.3. The group $\mathbb{Z}/81\mathbb{Z}$.

Proposition 4.8. *The group $\mathbb{Z}/81\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree $d \in \{6, 7, 8, 9\}$.*

Proof. By [DEvH+21, Theorem 3.1(2)] the group $J_1(81)(\mathbb{Q})$ is finite. We first show that $J_1(81)(\mathbb{Q})[2] = 0$. For $q = 5, 7$ the operator A_q annihilates $J_1(81)(\mathbb{Q})_{\text{tors}}$ by Proposition 2.2(2), so $J_1(81)(\mathbb{Q})[2]$ is contained in the intersection of the kernels of A_5 and A_7 on $J_1(81)[2] \simeq H_1(X_1(81)(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{F}_2$. We compute the action of the Hecke and diamond operators on the integral homology $H_1(X_1(81)(\mathbb{C}), \mathbb{Z})$, a lattice of rank 380, using modular symbols, and find that the kernel of A_5 on $H_1(X_1(81)(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{F}_2$ has dimension 8, while the intersection of the kernels of A_5 and A_7 is 0. Hence $J_1(81)(\mathbb{Q})[2] = 0$, so reduction modulo 2 is injective on $J_1(81)(\mathbb{Q})$ by Parent's result, and by (5) the operator $A_2 = T_2 - 1 - 2\langle 2 \rangle$ kills $J_1(81)(\mathbb{Q})$. Let D be the trace divisor of a point of order 81 over a number field of degree $d \leq 9$. As $A_2 c_0 = 0$ by Lemma 2.3, applying A_2 to $[D - dc_0]$ we get $T_2 D \sim D + 2\langle 2 \rangle D$. Both sides are effective of degree $3d \leq 27$, while $\operatorname{gon}_{\mathbb{C}} X_1(81) > 28.92$ by Abramovich's bound, as $i(81) = 2916$. So $T_2 D = D + 2\langle 2 \rangle D$ by Lemma 2.7, and the finite non-empty set of j-invariants of the points in the support of D is closed under cyclic 2-isogenies. But for $E_\tau = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ the map $E_\tau \to E_{2\tau}$ is a cyclic 2-isogeny, and $j(2^k\tau) = q^{-2^k} + 744 + O(q^{2^k})$, with $q = e^{2\pi i \tau}$, is unbounded as $k \to \infty$. □

4.4. **The groups $\mathbb{Z}/133\mathbb{Z}$ and $\mathbb{Z}/247\mathbb{Z}$.** In degree 9 we treat the levels 133 and 247 with Lemma 2.13.

Proposition 4.9. *The group $\mathbb{Z}/133\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a nonic field.*

Proof. Let D be the trace divisor of a point of order 133 over a nonic field, and put $h = \langle 64\rangle$, of order 3 in $\Delta(133)$. We compute that the winding submodule is the whole space for every character χ with $\chi(64) \neq 1$, so $(h-1)J_1(133)(\mathbb{Q})$ is finite. Hence $A_3(h-1)[D - 9c_0] = 0$, so $A_3(h-1)D$ is principal. Its positive part $T_3hD + D + 3\langle 3\rangle D$ has degree 72, while $\operatorname{gon}_{\mathbb{C}} X_1(133) \geq \frac{325}{2^{15}} \cdot 8640 > 85$, so $A_3(h-1)D = 0$. By Lemma 2.11 the points in the support of D have no complex multiplication, so $hD = D$ by Lemma 2.13, and D is the pull-back of an effective rational divisor D_Y of degree 3 on $Y = X_1(133)/\langle h\rangle$, by Lemma 2.12.

Write $H_{19} = \{1, 7, 11\} \subseteq (\mathbb{Z}/19\mathbb{Z})^\times$. As $64 \equiv 1 \pmod 7$ and $64 \equiv 7 \pmod{19}$, a non-cuspidal point of Y over $\mathbb{F}_{2^e}$ gives an elliptic curve E over $\mathbb{F}_{2^e}$ with a point of order 7, up to sign (after replacing E by a suitable twist), and a Frobenius stable H_{19}-orbit of points of order 19, on which the Frobenius acts as an element $\lambda \in H_{19}$. We enumerate the elliptic curves over $\mathbb{F}_{2^e}$, $e \leq 3$, with a point of order 7: they have trace $a = -2$ for $e = 2$ and $a = -5$ for $e = 3$, and $\lambda^2 - a\lambda + 2^e \not\equiv 0 \pmod{19}$ for $\lambda \in H_{19}$. Hence $Y_{\mathbb{F}_2}$ has no non-cuspidal closed points of degree at most 3, and the reduction of D_Y modulo 2 is cuspidal.

Let $Z = X_1(133)/\langle 78\rangle$, where $\langle 78\rangle$ has order 18 and contains h. As $78 \equiv 1 \pmod 7$ and 78 generates $(\mathbb{Z}/19\mathbb{Z})^\times$, the curve Z parametrizes triples (E, P_7, C_{19}) consisting of a point of order 7 and a cyclic subgroup of order 19. The group $\langle 78\rangle$ acts freely on $X_1(133)$, also on the cusps and in characteristic 2, as an automorphism of an elliptic curve fixing a point of order 7 is trivial, so Z has genus 35 and good reduction at 2. The push-forward D_Z of D_Y to Z is an effective rational divisor of degree 3 with non-cuspidal support and cuspidal reduction. Let $\delta = \langle 2\rangle$, of order 3 on Z, and put

$$\psi_0 = (1 + \delta + \delta^2)(T_2^4 + 4T_2^3 + T_2^2 - 8T_2 - 3), \qquad \psi_3 = (2 - \delta - \delta^2)(T_2 - 2\delta^2).$$

We compute that the factors of J_Z outside the winding quotient have characters of order 1 and 3, of total dimension 4 and 2 respectively, that the polynomial $X^4 + 4X^3 + X^2 - 8X - 3$ kills T_2 on the former, and that $T_2 = 2\delta^2$ on the latter. Hence $\psi_0(J_Z(\mathbb{Q}))$ and $\psi_3(J_Z(\mathbb{Q}))$ are finite. By (5), modulo 2 we have $\psi_0^* = (1 + \delta^* + \delta^{*2})(M^4 + M^2 + 1)$ and $\psi_3^* = (\delta^* + \delta^{*2})M$, where $M = \mathcal{C}\delta^*$. The space $U = (\mathcal{C} - 1)\big(\psi_0^* H^0(Z_{\mathbb{F}_2}, \Omega^1) + \psi_3^* H^0(Z_{\mathbb{F}_2}, \Omega^1)\big)$ has dimension 22. The closed cusps of $Z_{\mathbb{F}_2}$ have degrees $1^6, 3^2$, and we compute that the restriction of U to each of the $\binom{8}{3} + 2 = 58$ effective cuspidal divisors of degree 3 is surjective. By Proposition 7.3 this is a contradiction. □

Note that $\psi_0\psi_3 = 0$, as $(1 + \delta + \delta^2)(2 - \delta - \delta^2) = 0$, so it is essential that Proposition 7.3 allows several operators ψ_i.

Proposition 4.10. *The group $\mathbb{Z}/247\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a nonic field.*

Proof. Let D be the trace divisor of a point of order 247 over a nonic field and put $h = \langle 144\rangle$, of order 3. We compute that every character modulo 247 whose winding submodule is not the whole space is trivial on 144, so $(h-1)J_1(247)(\mathbb{Q})$ is finite. As in the proof of Proposition 4.9, $A_3(h-1)D$ is principal and its positive part has degree 72, while $\operatorname{gon}_{\mathbb{C}} X_1(247) \geq \frac{325}{2^{15}} \cdot 30240 > 299$, so $A_3(h-1)D = 0$ and $hD = D$ by Lemmas 2.11 and 2.13.

Let $H \subseteq \Delta(247)$ be the subgroup of order 18 generated by 40, which contains 144. As $40 \equiv 1 \pmod{13}$ and 40 generates $(\mathbb{Z}/19\mathbb{Z})^\times$, the curve $Z = X_1(247)/H$ parametrizes triples (E, P_{13}, C_{19}), and as in Proposition 4.9 the action of H is free, so Z has genus 129, $i(n)/18 = 1680$ as index, and good reduction at 2, 3 and 17. As above, D gives an effective rational divisor D_Z of degree 3 on Z whose support consists of points without complex multiplication. Let $t = \langle 2 \rangle$, of order 6 on Z, and put $s = t^2$. We compute the winding submodules for the characters of $\Delta(247)/H$: for the characters of order 1, 2, 3 and 6 the dimensions of the spaces are 21, 20, 22 and 22, and those of the winding submodules 14, 20, 22 and 22. Hence the abelian variety $A = (t-1)J_Z$, of dimension 108, has finitely many rational points. Put $A' = (s-1)J_Z$ and $A'' = (1+s+s^2)A$, of dimensions 88 and 20. We compute from the characteristic polynomials of T_3 and T_{17} that $\#A'(\mathbb{F}_3)$ and $\#A''(\mathbb{F}_{17})$ are odd. If $T \in A(\mathbb{Q})[2]$, then $(s-1)T \in A'(\mathbb{Q})[2] = 0$, so $sT = T$ and $T = 3T = (1+s+s^2)T \in A''(\mathbb{Q})[2] = 0$. Hence $A(\mathbb{Q})$ is finite of odd order.

Let c be the image on Z of a rational cusp of $X_1(247)$, so that $T_2 c = c + 2tc$ by Lemma 2.3. The class $y = (t-1)[D_Z - 3c] \in A(\mathbb{Q})$ has odd order, and $A_2 y = (T_2 - 1 - 2t)y$ reduces to 0 modulo 2 by (5), so $A_2 y = 0$. As $A_2(t-1)c = 0$, we get

$$T_2(tD_Z) + tD_Z + D_Z \sim T_2 D_Z + 2t^2 D_Z.$$

Both sides are effective of degree 15, while $\operatorname{gon}_{\mathbb{C}} Z \geq \frac{325}{2^{15}} \cdot 1680 > 16$, so they are equal, and $A_2(t-1)D_Z = 0$. By Lemma 2.13 with $q = 2$ we get $tD_Z = D_Z$. But an automorphism of an elliptic curve without complex multiplication which preserves a cyclic subgroup of order 19 and maps a point P_{13} of order 13 to $2^k P_{13}$ is ± 1, so $2^k \equiv \pm 1 \pmod{13}$ and $6 \mid k$. Hence the orbits of the group generated by t on the support of D_Z have length 6, which does not divide 3. □

5. The rank zero criterion and cuspidal divisor classes

When the Jacobian has rank 0 we use Proposition 2.5, which shows that the elliptic curve must have good reduction at some prime above a suitable p. At $p = 2$ we replace its gonality condition by a computation (Section 5.2), and we also use computations in the group generated by the cuspidal divisor classes over a finite field (Sections 5.3 and 5.4). Most of the propositions of this section are about sextic fields, while Lemmas 5.1, 5.3 and 5.6 are also used in the other degrees.

5.1. The rank zero criterion.

To apply Proposition 2.5 to $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ we need the following lemma, as these cases are not covered by [DS17, Theorem 4.1].

Lemma 5.1. *For $m = 7$ and $m = 9$ we have* $\operatorname{rk} J_1(m,m)(\mathbb{Q}(\zeta_m)) = 0$.

Proof. Put $F = \mathbb{Q}(\zeta_m)$. We use the argument of the proof of [DS17, Theorem 4.1], where F is quadratic. Over F the curve $X_1(m,m)$ is isomorphic to the quotient X_H of $X_1(m^2)$ by the diamond operators congruent to 1 modulo m [DS17, §2], so it suffices to show that $B(F)$ is finite for the Jacobian B of X_H, which is an abelian variety over $\mathbb{Q}$. The space of cusp forms of weight 2 on X_H is

$$V_m := \bigoplus_{\varepsilon} S_2(\Gamma_0(m^2), \varepsilon),$$

the sum being over the even Dirichlet characters ε modulo m, so after extending scalars to $\overline{\mathbb{Q}}_\ell$ the ℓ-adic representation of B is the sum of the representations ρ_f attached to the newforms f occurring in V_m, with multiplicities. We have $B(F) = R(\mathbb{Q})$ for the restriction

of scalars $R := \mathrm{Res}_{F/\mathbb{Q}} B_F$, whose ℓ-adic representation is induced from the restriction of that of B to $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$. Hence, over $\overline{\mathbb{Q}}_\ell$, it is the sum of the twists $\rho_f \otimes \chi$, where χ runs over the characters of $\mathrm{Gal}(F/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$. The twist of a newform of level dividing m^2 and character ε modulo m by a character χ modulo m is an eigenform of level dividing m^2 and character $\varepsilon\chi^2$, which is again even and defined modulo m, so $\rho_f \otimes \chi \simeq \rho_g$ for a newform g occurring in V_m. The multiset of these newforms g is stable under the action of $\mathrm{Aut}(\mathbb{C})$ on the coefficients, so by Faltings' isogeny theorem [Fal83] the abelian variety R is isogenous over $\mathbb{Q}$ to a product of the abelian varieties $A_{[g]}$ attached to the Galois orbits of the newforms g occurring in V_m. By Kato's theorem it therefore suffices to show that $L(g,1) \neq 0$ for every newform g occurring in V_m. Using modular symbols we compute the dimension of the winding submodule of each Galois orbit of newforms occurring in V_m, and it is equal to the dimension of the orbit in every case. The newforms in question have level 49 for $m = 7$, and levels 27 and 81 for $m = 9$. □

Proposition 5.2. *The groups $\mathbb{Z}/55\mathbb{Z}$, $\mathbb{Z}/75\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}\times\mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over a sextic field.*

Proof. In each case suppose that E is an elliptic curve over a sextic field K containing the group in question, and let $d = d_m = [K : \mathbb{Q}(\zeta_m)]$. We show that the hypotheses of Proposition 2.5 hold for a suitable prime p, and that E cannot have good reduction at any prime of K above p by Lemma 2.6, which is a contradiction.

For $n = 55, 75$ we have $\mathrm{rk}\, J_1(n)(\mathbb{Q}) = 0$ by [DEvH+21, Theorem 3.1(2)], and Abramovich's bound gives $\mathrm{gon}_{\mathbb{Q}} X_1(n) > 14.28, 23.80$, respectively, both larger than 12, so Proposition 2.5(b) applies with $p = 2$ and $d = 6$. No elliptic curve over $\mathbb{F}_{2^f}$ with $f \leq 5$ has a point of order n by the Hasse bound. Over $\mathbb{F}_{64}$ a point of order 55 or 75 would force $\#E(\mathbb{F}_{64}) = 55$ or 75, which is impossible (see the discussion after Lemma 2.6).

For $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$ we have $d = 3$. By [DS17, Theorem 4.1], $\mathrm{rk}\, J_1(4,24)(\mathbb{Q}(i)) = 0$, and $i(4,24) = 768$ gives $\mathrm{gon}_{\mathbb{C}} X_1(4,24) > 7.61 > 3$, so Proposition 2.5(a) applies with $p = 5$. The prime 5 splits in $\mathbb{Q}(i)$, so the residue fields of K at the primes above 5 are $\mathbb{F}_5$, $\mathbb{F}_{25}$ or $\mathbb{F}_{125}$. The Hasse intervals of these fields contain no multiple of 96, since $(\sqrt{25}+1)^2 < 96$ and $96 < (\sqrt{125}-1)^2 < (\sqrt{125}+1)^2 < 192$.

For $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ we have $K = \mathbb{Q}(\zeta_m)$ and $d = 1$. The genera of $X_1(7,7)$ and $X_1(9,9)$ are 3 and 10, so $\mathrm{gon}_{\mathbb{Q}(\zeta_m)} X_1(m,m) > 1$, and Lemma 5.1 gives $\mathrm{rk}\, J_1(m,m)(\mathbb{Q}(\zeta_m)) = 0$. Take $p = 29$ for $m = 7$ and $p = 19$ for $m = 9$. Then $p \equiv 1 \pmod m$, so the residue fields of K at the primes above p are $\mathbb{F}_p$, and since $(\sqrt{p}+1)^2 < m^2$ no elliptic curve over $\mathbb{F}_p$ has full m-torsion. □

5.2. **A criterion using twice a cuspidal divisor.** When $p = 2$, Proposition 2.5 requires $\mathrm{gon}_{\mathbb{Q}(\zeta_m)} X_1(m,n) > 2d$, because the kernel of reduction on the torsion of the Jacobian can contain elements of order 2. For $X_1(3,15)$ and $X_1(3,21)$ the gonality bounds that we have are too weak for this, and we replace the gonality condition by a computation. We use it for $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$ in Proposition 5.5 and for $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z}$ in Proposition 12.2.

Lemma 5.3. *Let $m \mid n$ with n odd and $mn > 4$, let $\mathfrak{p}$ be a prime of $\mathbb{Q}(\zeta_m)$ above 2 with residue field k, and let $d \geq 1$. Put $X = X_1(m,n)$ and assume that $\mathrm{rk}\, J(\mathbb{Q}(\zeta_m)) = 0$ and that*

$$\dim L(2\overline{C}) = 1$$

for every effective cuspidal divisor $\overline{C}$ of degree d on X_k. Then every elliptic curve E over a degree d extension K of $\mathbb{Q}(\zeta_m)$ with $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \subseteq E(K)$ has good reduction at at least one prime of K above $\mathfrak{p}$.

Proof. Suppose the opposite, and let D be the trace divisor of the corresponding point. By Lemma 2.4 the reduction of E at every prime of K above $\mathfrak{p}$ is multiplicative, so D reduces to an effective cuspidal divisor $\overline{C}$ of degree d on X_k. Let $M = \mathbb{Q}(\zeta_n)$, choose a prime $\mathfrak{P}$ of M above $\mathfrak{p}$, and let $F \subseteq M$ be the fixed field of its decomposition group in $\mathrm{Gal}(M/\mathbb{Q}(\zeta_m))$. The prime $\mathfrak{P} \cap F$ of F has residue field k, and F is unramified at 2 as n is odd. All cusps are defined over M and the cuspidal subscheme is finite étale at 2, so the closed points in the support of $\overline{C}$ lift to orbits of $\mathrm{Gal}(M/F)$ of the same size, and $\overline{C}$ lifts to an effective F-rational cuspidal divisor C of degree d. As in the proof of Proposition 2.5, the class $[D - C] = [D - dc_0] + [dc_0 - C] \in J(F)$ is torsion, by the rank assumption on $J(\mathbb{Q}(\zeta_m))$ and by Manin-Drinfeld, and it reduces to 0 modulo $\mathfrak{P} \cap F$, so $2[D - C] = 0$ by Parent's result, and $2D \sim 2C$. By semicontinuity [Har77, Theorem III.12.8], the dimension of the Riemann-Roch space of $2C$ on X_F satisfies

$$\dim L(2C) \leq \dim L(2\overline{C}) = 1,$$

so $2C$ is the only effective divisor in its class and $2D = 2C$, which is impossible as D is non-cuspidal and C is cuspidal. □

We check the condition of Lemma 5.3 using differentials. Write $\overline{C} = \sum_P m_P P$. The space $\Omega(2\overline{C})$ is cut out in $H^0(X_k, \Omega^1)$ by the vanishing of the first $2m_P$ coefficients of the expansions in a local parameter at each P. These coefficients lie in the residue field of P, so these are $\sum_P 2m_P \deg P = 2d$ linear conditions over k, and by the Riemann-Roch theorem $\dim L(2\overline{C}) = 1 + 2d - \operatorname{codim} \Omega(2\overline{C})$. So $\dim L(2\overline{C}) = 1$ if and only if these conditions are linearly independent. As $\Omega(2\overline{C})$ is the intersection of the subspaces $\Omega(2m_P P)$, and $\Omega(2jP)$ depends only on the closed cusp P and on $j \leq d/\deg P$, each of these subspaces is computed only once, by expanding a basis of $H^0(X_k, \Omega^1)$ at P, and for each $\overline{C}$ it remains to intersect at most d of them.

For $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$ we also need the following lemma, which we use again over octic fields in Proposition 13.23.

Lemma 5.4. *Let $F = \mathbb{Q}(\zeta_3)$ and $X = X_1(3, 15)$ over F, a curve of genus 9 with $\operatorname{rk} J_X(F) = 0$* [DS17, Theorem 4.1]. *Then $\mathrm{Cl}^c_F X \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/96\mathbb{Z} \times \mathbb{Z}/96\mathbb{Z}$ and $3J_X(F) \subseteq \mathrm{Cl}^c_F X$. Reduction modulo the prime of F above 2 is injective on $J_X(F)$.*

Proof. All the cusps are defined over $\mathbb{Q}(\zeta_{15})$, and the Frobenius at a prime above 7 generates $\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/F)$, so the 20 Galois orbits of cusps over F, of degrees $1^{16}, 4^4$, remain irreducible modulo 7. We identify them with their reductions at the primes above 2, 7, 13 and 19 using the valuations of integral modular units, in the normal form $y^2 + a_1xy + a_3y = x^3$ with $P = (0, 0)$ of order 3. We compute that the reductions of $\mathrm{Cl}^c_F X$ at these four primes all have invariants $[3, 3, 24, 96, 96]$, so $\mathrm{Cl}^c_F X$ has these invariants, and that $\#J_X(\mathbb{F}_7) = 149299200$, $\#J_X(\mathbb{F}_{13}) = 12230590464$ and $\#J_X(\mathbb{F}_{19}) = 247669456896$, whose greatest common divisor is $5971968 = 3\#\,\mathrm{Cl}^c_F X$. As reduction at these primes is injective on $J_X(F)$, the order of $J_X(F)$ divides $3\#\,\mathrm{Cl}^c_F X$, so $J_X(F)/\,\mathrm{Cl}^c_F X$ has order dividing 3. In particular $J_X(F)[2^\infty] = (\mathrm{Cl}^c_F X)[2^\infty]$, on which reduction above 2 is injective, and reduction above 2 is injective on the odd part of $J_X(F)$. □

Proposition 5.5. *The group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a sextic field.*

Proof. Let E be an elliptic curve over a sextic field K with $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \subseteq E(K)$, and let F and X be as in Lemma 5.4. Then $K \supseteq F$ and $d = [K : F] = 3$. Let $\mathfrak{p}$ be the prime of F above 2, with residue field $\mathbb{F}_4$. As 2 is inert in F, the residue fields of K at the primes above 2 are $\mathbb{F}_4$, $\mathbb{F}_{16}$ or $\mathbb{F}_{64}$, and the Hasse intervals of these fields contain no multiple of 45. So E has bad reduction at every prime of K above 2 by Lemma 2.6, and it suffices to show that E has good reduction at some prime above 2.

We argue as in the proof of Lemma 5.3, with one extra step. The curve $X_{\mathbb{F}_4}$ has 16 cusps of degree 1 and 8 of degree 2, so there are $\binom{18}{3} + 16 \cdot 8 = 944$ effective cuspidal divisors of degree 3. We compute that $\dim L(2\overline{C}) = 1$ for 912 of them, so the proof of Lemma 5.3 excludes these as reductions of the trace divisor D. The remaining 32 divisors are supported on the cusps of degree 1 and satisfy $\dim L(\overline{C}) = 1$.

The 16 F-rational cusps of X (see the proof of Lemma 5.4) reduce to 16 distinct cusps of degree 1, as the cuspidal subscheme is finite étale at 2, so they are all the cusps of $X_{\mathbb{F}_4}$ of degree 1. It follows that each of the 32 remaining divisors $\overline{C}$ lifts to an F-rational cuspidal divisor C, and if D reduces to $\overline{C}$, then $[D - C] \in J_X(F)$ reduces to 0.

By Lemma 5.4, reduction modulo $\mathfrak{p}$ is injective on $J_X(F)$, so $D \sim C$. By semicontinuity [Har77, Theorem III.12.8] we have $\dim L(C) \leq \dim L(\overline{C}) = 1$, so $D = C$, which is a contradiction. □

5.3. **Arguments with cuspidal divisor classes.** The Hecke sieve (Section 6) uses only the fact that A_q kills $J(\mathbb{Q}(\zeta_m))$. When $J(\mathbb{Q}(\zeta_m))$ is known explicitly, and in particular when it is generated by cuspidal divisor classes, we can instead compare the classes of the possible reductions with the reduction of $J(\mathbb{Q}(\zeta_m))$ itself. This is the method of [DEvH+21, §5.2] and [Naj26a, §8], which we use in the following form.

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*

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

Proof. This is the reduction of the class $[D - dc_*] \in J(F)$. □

So an effective divisor D' of degree e with non-cuspidal support can be the non-cuspidal part of the reduction of D only if $[D' + C' - d\,\overline{c_*}] \in G$ for some effective cuspidal divisor C' of degree $d - e$ on X_k. To check this for many D' at once, we compute for each $j \geq 0$ the set $\mathcal{S}_j \subseteq J(k)/G$ of the classes of $[j\overline{c_*} - C']$, where C' runs over the effective cuspidal divisors of degree j on X_k. The condition then says that the image of $[D' - e\overline{c_*}]$ in $J(k)/G$ lies in $\mathcal{S}_{d-e}$. Note that $\mathcal{S}_j \subseteq \mathcal{S}_{j+1}$, as $[j\overline{c_*} - C'] = [(j+1)\overline{c_*} - (C' + \overline{c_*})]$, so a divisor D' which fails the test in degree $d + 1$ also fails it in degree d.

In practice G is either the image of the reduction map on $J(F)$, when $J(F)$ is known and reduction is injective on it, or the subgroup generated by the classes $[\overline{c} - \deg(\overline{c})\overline{c_*}]$ of all closed cusps $\overline{c}$ of X_k, when $J(F)$ is generated by cuspidal divisor classes. In the latter case G contains the reduction of $J(F)$ without any assumption on which cusps are rational, and it contains the classes of all cuspidal divisors of degree 0 on X_k. So every $\mathcal{S}_j$ is trivial, and the condition is simply $[D' - e\overline{c_*}] \in G$.

Usually we test only one representative D' of each orbit of a group of automorphisms of X over F, such as the diamond operators or the level automorphisms of Section 2.4, and the numbers of divisors D' that we give are then numbers of orbit representatives. This is justified by the identity

$$[gD' - e\,\overline{c_*}] = g[D' - e\,\overline{c_*}] + e[g\overline{c_*} - \overline{c_*}]$$

for such an automorphism g, which maps cusps to cusps. In both cases above G is stable under g and contains $[g\overline{c_*} - \overline{c_*}]$, as gc_* is again an F-rational cusp. Moreover, g permutes the effective cuspidal divisors of each degree, and the sets of cuspidal divisors that we allow in our computations are stable under g as well, so the condition holds for D' if and only if it holds for gD'.

5.4. **The curve $X_1(32)$.** The proof below uses the Hecke sieve and the types of decompositions of Section 6.1.

Proposition 5.7. *The group $\mathbb{Z}/32\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree $d \in \{6, 7\}$.*

Proof. We have $\operatorname{rk} J_1(32)(\mathbb{Q}) = 0$ and $J_1(32)(\mathbb{Q}) = \mathrm{Cl}^c_{\mathbb{Q}} X_1(32) \simeq (\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z} \times \mathbb{Z}/11640\mathbb{Z}$ [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], and $\operatorname{gon}_{\mathbb{Q}} X_1(32) = 8$ [DvH14, Theorem 4 and Table 1]. So for $d = 6, 7$, Proposition 2.5(a) with $p = 3$ excludes the entirely cuspidal reduction of the trace divisor D modulo 3. Let $D' + C'$ be the reduction of D, as in Lemma 5.6, let c_* be a rational cusp, and let G be the subgroup of $J_1(32)(\mathbb{F}_3)$ generated by the reductions of the rational cuspidal divisors of degree 0. We compute that $G \simeq (\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z} \times \mathbb{Z}/11640\mathbb{Z}$, so G is the reduction of $J_1(32)(\mathbb{Q})$, and by Lemma 5.6 we have $[D' + C' - d\,\overline{c_*}] \in G$.

The non-cuspidal closed points of $X_1(32)_{\mathbb{F}_3}$ of degrees $3, \dots, 7$ form $1, 1, 2, 19$ and 39 diamond orbits. The primes $q = 5, 7$ are admissible for cuspidal parts of degree at most 1, and the Hecke sieve at 3 with $q = 5, 7$ leaves, for $d = 7$, 8 possible non-cuspidal parts D' up to the diamond operators, of degrees $3, 4, 5, 5, 6, 6, 6, 6$. For these 8 divisors we compute the classes $[D' + C' - 7\overline{c_*}]$ for all $1688, 412, 82, 82, 12, 12, 12, 12$ effective cuspidal divisors C' of the complementary degree, and none of these 2312 classes lies in G. As G is stable under the diamond operators, this excludes all the possible reductions for $d = 7$, and by the monotonicity of these tests in the degree (Sections 5.3 and 6.1) also for $d = 6$. □

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

The groups of this section are excluded by reducing the trace divisor of a point modulo a small prime p and applying the Hecke sieve of [DN25, Proposition 5.5] to the possible reductions. For some of them we also compare the class of the reduction with the reduction of a known Mordell-Weil group, on the curve itself or after pushing the trace divisor forward to a modular curve of smaller level. In this way we exclude $\mathbb{Z}/n\mathbb{Z}$ for $n \in \{33, 34, 35, 38, 40, 42, 49, 50\}$ over sextic fields, for $n \in \{34, 35, 38, 40, 42, 46, 49\}$ over septic fields, for $n \in \{38, 44, 46, 50\}$ over octic fields and for $n \in \{35, 38, 44, 46, 50, 58, 62\}$ over nonic fields. The sieve computation on $X_1(32)$ is completed with cuspidal divisor classes in Proposition 5.7, and the same sieve over $\mathbb{Q}(\zeta_m)$ is used for the groups $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with $m \geq 3$ in Section 12.

6.1. **The sieve and the push-forwards.** Let $X = X_1(m,n)$ with $\operatorname{rk} J(\mathbb{Q}(\zeta_m)) = 0$, let $\mathfrak{p}$ be a prime of $\mathbb{Q}(\zeta_m)$ above a prime $p \nmid n$, with residue field $k = \mathbb{F}_{p^f}$, let $K \supseteq \mathbb{Q}(\zeta_m)$ be a number field of degree d, and let D be the trace divisor of a point $x \in Y_1(m,n)(K)$, which has degree d_m. 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 $\mathfrak{p}$, so the reductions with $e = 0$ are excluded by Proposition 2.5 whenever its condition on the gonality holds. As in [Naj26a, §6] 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(4) 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, that is, if it comes from a Galois orbit of cusps over $\mathbb{Q}(\zeta_m)$ which stays irreducible modulo $\mathfrak{p}$. As A_q commutes with the diamond operators, it suffices to test one D' in each orbit of the diamond operators, and when D' is a sum of several closed points, it suffices to take one of them up to the diamond operators.

We also use Lemma 5.6, on X itself or after pushing the trace divisor forward to another curve. 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 $\mathbb{Z}_{(p)}$, as all the degeneracy and forgetful maps that we use do, 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 $J_Y(\mathbb{Q})$, as in Section 5.3. If the reduction of D is $D' + C'$ as above, with $\deg D' = e$, then Lemma 5.6, applied to $\pi_* D$, gives

$$[\pi_* D' - e\,\overline{y_0}] \in G + \mathcal{S}_{d-e}, \tag{6}$$

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 $\mathcal{S}_j \subseteq G$, as every class $[j\overline{y_0} - B]$ is then the reduction of a class in $J_Y(\mathbb{Q})$, and (6) reduces to $[\pi_* D' - e\,\overline{y_0}] \in G$.

These tests are monotone in the degree. A prime q which is admissible for all the cuspidal divisors of degree j is also admissible for those of smaller degree, as each of them is contained in one of degree j obtained by adding a multiple of the reduction of c_0, and $\mathcal{S}_j \subseteq \mathcal{S}_{j+1}$ (see Section 5.3). Hence, if a computation excludes all the possible non-cuspidal parts D' for the fields of degree d, then it also excludes them for the fields of every smaller degree. In particular, a computation of all the possible reductions in degree 9 also covers the degrees 6, 7 and 8.

The numbers of non-cuspidal closed points of $X_{\mathbb{F}_p}$ that we use are listed in Table 3, and for $X_1(2,26)$ and $X_1(2,28)$ in Table 4. They are computed from the models (in degree 9 also from the zeta functions), and checked independently by counting the elliptic curves over $\mathbb{F}_{p^f}$ with the required level structure (see Section 15).

X	p	non-cuspidal closed points of degree $1, 2, \dots$
$X_1(29)$	3	$0, 0, 14, 28, 14, 133, 280, 770, 2282$
$X_1(31)$	3	$0, 0, 0, 15, 91, 120, 330, 930, 1980$
$X_1(32)$	3	$0, 0, 8, 8, 16, 140, 312$
$X_1(33)$	5	$0, 10, 60, 230, 602, 2660$
$X_1(34)$	3	$0, 0, 0, 26, 32, 80, 256$
$X_1(35)$	3	$0, 0, 12, 0, 36, 126, 348, 813, 2240$
$X_1(38)$	3	$0, 0, 3, 0, 72, 87, 216, 801, 2127$
$X_1(39)$	2	$0, 0, 0, 0, 0, 12, 0$
$X_1(40)$	3	$0, 0, 0, 32, 72, 80, 408$
$X_1(42)$	5	$0, 0, 4, 183, 648, 2286, 11160$
$X_1(44)$	3	$0, 0, 0, 0, 60, 160, 240, 920, 2260$
$X_1(46)$	3	$0, 0, 0, 55, 44, 55, 264, 781, 1958$
$X_1(49)$	3	$0, 0, 0, 21, 63, 154, 379$
$X_1(50)$	3	$0, 0, 0, 0, 0, 60, 200, 1045, 2040$
$X_1(55)$	2	$0, 0, 0, 0, 0, 0, 20, 0, 40$
$X_1(58)$	3	$0, 0, 0, 0, 0, 140, 224, 756, 2380$
$X_1(62)$	3	$0, 0, 0, 0, 180, 150, 330, 930, 1600$
$X_1(2, 22)$	3	$0, 0, 0, 0, 60, 100, 240$

TABLE 3. Non-cuspidal closed points of $X_{\mathbb{F}_p}$ of small degree. For each curve the list ends at the largest degree in which we use it. For $X_1(2, 26)$ and $X_1(2, 28)$ see Table 4.

6.2. **The curves over $\mathbb{Q}$ in degrees 6 and 7.**

Proposition 6.1. *The group $\mathbb{Z}/33\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a sextic field.*

Proof. We have $\operatorname{rk} J_1(33)(\mathbb{Q}) = 0$ [DEvH+21, Theorem 3.1(2)] and $\operatorname{gon}_{\mathbb{Q}} X_1(33) = 10$ [DvH14, Theorem 4 and Table 1], so Proposition 2.5(a) with $p = 5$ excludes the entirely cuspidal reduction. As $Y_1(33)(\mathbb{F}_5) = \emptyset$ (Table 3), the cuspidal part has degree at most 4. The only Galois orbit of cusps over $\mathbb{Q}$ that splits modulo 5 has degree 10 and splits into 2 places of degree 5, which cannot occur in such a cuspidal part, so every prime $q \nmid 330$ is admissible. The non-cuspidal closed points of $X_1(33)_{\mathbb{F}_5}$ of degrees $2, \dots, 6$ form $1, 6, 24, 61, 269$ diamond orbits, and we compute that $[A_7(D')] \neq 0$ for every possible non-cuspidal part D' of every type of degree at most 6, up to the diamond operators (the computation is split over several scripts, which are listed in the `README` of the sextic repository). □

Proposition 6.2. *The group $\mathbb{Z}/34\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 6 or 7.*

Proof. We have $\operatorname{rk} J_1(34)(\mathbb{Q}) = 0$ [DEvH+21, Theorem 3.1(2)] and $\operatorname{gon}_{\mathbb{Q}} X_1(34) = 10$ [DvH14, Theorem 4 and Table 1], so Proposition 2.5(a) with $p = 3$ excludes the entirely cuspidal reduction. Every closed cusp of $X_1(34)_{\mathbb{F}_3}$ of degree at most 7 is the reduction of a rational cusp, as the other closed cusps have degree 8, so every prime $q \nmid 102$ is admissible. The non-cuspidal closed points of $X_1(34)_{\mathbb{F}_3}$ of degrees 4, 5, 6 and 7 form 5, 4, 11 and 32 diamond orbits, and we compute with the Hecke sieve at $p = 3$ and $q \in \{5, 7, 11\}$ that every possible non-cuspidal part D', of every type of degree at most 7, satisfies $[A_q(D')] \neq 0$ for one of these q. This excludes all the possible reductions for $d = 6$ and for $d = 7$. □

For $X_1(40)$ one possible reduction survives the Hecke sieve with the admissible primes, and it requires a correction by cuspidal divisors which are not reductions of rational ones.

Lemma 6.3. *Let P be the closed point of degree 5 of $X_1(40)_{\mathbb{F}_3}$ which survives the Hecke sieve at 3 with $q = 11$. Then $A_7(P + C)$ is not principal for any effective cuspidal divisor C of degree 2 on $X_1(40)_{\mathbb{F}_3}$.*

Proof. The closed cusps of $X_1(40)_{\mathbb{F}_3}$ which are not reductions of rational cuspidal divisors are 4 cusps of degree 2, of type $k = 5$ in the description of the cusps of $X_1(40)$ as $(\mu_{40/k} \times \mathbb{Z}/k\mathbb{Z})'/\{\pm 1\}$ [DN25, Section 2]. They come from 2 Galois orbits of degree 4 over $\mathbb{Q}$, each of which splits into 2 closed points of degree 2 over $\mathbb{F}_3$. Write a geometric cusp of this type as (ζ_8^a, b) with $a \in (\mathbb{Z}/8\mathbb{Z})^\times$ and $b \in (\mathbb{Z}/5\mathbb{Z})^\times$, modulo $(a, b) \sim (-a, -b)$. The Frobenius at 3 sends (a, b) to $(3a, b)$, the Galois element σ_7 sends it to $(7a, b)$, and the diamond operator $\delta = \langle 7\rangle$ sends it to $(7a, 7b)$. Hence $\sigma = \sigma_7$ interchanges the 2 closed points in each orbit, and $\delta^2 = \sigma$ on these 4 points. As $\sigma^{-1} = \sigma$ on them, Lemma 2.3 gives

$$A_7 c = (\sigma - 1)c + 7\delta(\sigma - 1)c$$

for such a cusp c, while $A_7 C = 0$ for the other 80 effective cuspidal divisors C of degree 2, which are reductions of rational cuspidal divisors. We do not identify the cusps of the model with their labels (a, b), so we test both permutations δ of order 4 of these 4 cusps with $\delta^2 = \sigma$. They are the actions of $\langle 7\rangle$ and of $\langle 7\rangle^{-1} = \langle 23\rangle$, as $23^2 \equiv 7^2 \pmod{40}$, so the two cases also correspond to the two conventions for the diamond operators of Section 2.3. We compute that $A_7 P$ and the 8 divisors $A_7(P + c)$, for the 4 cusps c and both permutations δ, are non-principal. □

Proposition 6.4. *The group $\mathbb{Z}/40\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 6 or 7.*

Proof. Let $d \in \{6, 7\}$. We have $\operatorname{rk} J_1(40)(\mathbb{Q}) = 0$ [DEvH+21, Theorem 3.1(2)] and $\operatorname{gon}_{\mathbb{Q}} X_1(40) = 12$ [DvH14, Theorem 4 and Table 1], so the entirely cuspidal reduction at 3 is excluded by Proposition 2.5(a). By Table 3 the non-cuspidal part D' of the reduction is a single closed point of degree $4, \dots, d$, and there are $4, 9, 10$ and 51 diamond orbits of points of degree $4, 5, 6$ and 7. The prime $q = 11$ is admissible for cuspidal parts of degree at most 3, and $q = 7$ for those of degree 1. For $d = 7$ we compute that the Hecke sieve excludes all the representatives of degree 4 and 6, all but one of degree 5, and all those of degree 7, for which the cuspidal part is empty and every $q \nmid 120$ is admissible, and by the monotonicity in Section 6.1 this also holds for $d = 6$. The remaining point P of degree 5 is excluded by Lemma 6.3: for $d = 7$ its cuspidal part C' has degree 2, and for $d = 6$ it has degree 1 and $A_7(P + C') = A_7(P + C' + \overline{c_0})$, as $A_7\overline{c_0} = 0$, where $C' + \overline{c_0}$ has degree 2. □

Proposition 6.5. *The group $\mathbb{Z}/42\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 6 or 7.*

Proof. We have $\operatorname{rk} J_1(42)(\mathbb{Q}) = 0$ [DEvH+21, Theorem 3.1(2)], and Derickx and van Hoeij proved $\operatorname{gon}_{\mathbb{Q}} X_1(42) > 8$ [DvH14, proof of Proposition 6], so Proposition 2.5(a) with $p = 5$ excludes the entirely cuspidal reduction. The closed cusps of $X_1(42)_{\mathbb{F}_5}$ have degrees $1^{12}, 2^6, 3^4, 6^2$, while the Galois orbits over $\mathbb{Q}$ have degrees $1^{12}, 2^6, 6^4$. A cusp with stabilizer $H \subseteq (\mathbb{Z}/42\mathbb{Z})^\times$ gives a closed cusp which is fixed by σ_q for every q in the subgroup generated by H and 5, so every prime q is admissible for cuspidal parts of degree at most 2, and the primes $q \equiv 5^i \pmod{42}$ for cuspidal parts of degree 3 or 4. For septic fields the

possible types of the non-cuspidal part and the tests are the following:

type	diamond representatives	$\deg C'$	q
[3]	2	4	17
[4]	33	3	17
[5]	108	2	11, 13, 17
[6]	392	1	11
[7]	1860	0	11, 13, 17
[3, 3]	8	1	11, 13, 17
[3, 4]	366	0	11, 13, 17

We compute that every one of these 2769 divisors D' satisfies $[A_q(D')] \neq 0$ for one of the listed primes. The types [3], [5], [6] and [3, 3] were tested in the sextic computation, which is split over several scripts listed in the `README` of the sextic repository, with primes that are admissible here, and the types [4], [3, 4] and [7] anew. We check that the tests cover all 2769 divisors. By the monotonicity in Section 6.1 this also covers sextic fields. □

6.3. **The curve $X_1(35)$.** The octic points of $X_1(35)$ are determined in Proposition 13.9.

Proposition 6.6. *The group $\mathbb{Z}/35\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 6, 7 or 9.*

Proof. Let $d \in \{6, 7, 9\}$. We have $\operatorname{gon}_{\mathbb{Q}} X_1(35) = 12$ [DvH14, Theorem 4 and Table 1], and $J_1(35)(\mathbb{Q}) \simeq \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/109148520\mathbb{Z}$ is finite and generated by rational cuspidal divisors [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2]. So by Proposition 2.5(a) with $p = 3$ the reduction of D modulo 3 is $D' + C'$ with $e = \deg D' \geq 1$. The closed cusps of $X_1(35)_{\mathbb{F}_3}$ have degrees $1^{12}, 4^3, 6^2, 12$, the same as the Galois orbits of cusps over $\mathbb{Q}$, so every closed cusp of $X_1(35)_{\mathbb{F}_3}$ is the reduction of a rational cuspidal divisor of the same degree. Let H be the reduction of $J_1(35)(\mathbb{Q})$. By (6) with $\pi = \mathrm{id}$, $y_0 = c_0$ and $G = H$, as then $\mathcal{S}_{d-e} \subseteq H$, we have $[D' - e\,\overline{c_0}] \in H$. We compute

$$J_1(35)(\mathbb{F}_3) \simeq (\mathbb{Z}/4\mathbb{Z})^2 \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/520\mathbb{Z} \times \mathbb{Z}/218297040\mathbb{Z},$$

in which H has index $2^{11} \cdot 5$. By Table 3 the possible types of D' of degree at most 9 are [3], [5], [6], [7], [8], [9], [3, 3], [5, 3], [6, 3] and [3, 3, 3]. This gives 5961 cases, and we find that exactly 6 of them have class in H, all of type [8]. This excludes the degrees 6 and 7.

So $d = 9$, and D reduces to $P + \overline{c}$ for one of these 6 points P of degree 8 and a rational cusp c. The 6 points are the reductions of the closed points of degree 8 of $X_1(35)$ in the diamond orbit of the octic point of level 35 of Proposition 13.3, as we check. So D reduces to $\overline{B} + \overline{c}$ for such an octic point B, and as reduction modulo 3 is injective on $J_1(35)(\mathbb{Q})$, we get $D \sim B + c$. As $\operatorname{gon}_{\mathbb{Q}} X_1(35) > 9$, Lemma 2.7 gives $D = B + c$, which is a contradiction, as the support of D contains no cusp. □

6.4. **The curves $X_1(38)$, $X_1(46)$ and $X_1(50)$.** Over septic fields, $\mathbb{Z}/50\mathbb{Z}$ is excluded in Proposition 13.6.

Proposition 6.7. *The group $\mathbb{Z}/38\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree $d \in \{6, 7, 8, 9\}$, nor is $\mathbb{Z}/46\mathbb{Z}$ for $d \in \{7, 8, 9\}$, nor $\mathbb{Z}/50\mathbb{Z}$ for $d \in \{6, 8, 9\}$.*

Proof. Let $n \in \{38, 46, 50\}$. We have $\operatorname{rk} J_1(n)(\mathbb{Q}) = 0$ [DEvH+21, Theorem 3.1(2)], $\operatorname{gon}_{\mathbb{Q}} X_1(38) = 12$ [DvH14, Theorem 4 and Table 1] and $\operatorname{gon}_{\mathbb{Q}} X_1(n) \geq 10$ for $n = 46, 50$ [NV26, Table 1], so Proposition 2.5(a) with $p = 3$ excludes the entirely cuspidal reduction.

The closed cusps of $X_1(n)_{\mathbb{F}_3}$ have degrees $1^{18}, 9^2$ for $n = 38$, $1^{22}, 11^2$ for $n = 46$ and $1^{20}, 4^4, 10^2$ for $n = 50$, the same as the Galois orbits of cusps over $\mathbb{Q}$, so every prime $q \nmid 3n$ is admissible for every cuspidal part.

Let $\pi : X_1(n) \to Y = X_1(n/2)$ be the map $(E, P) \mapsto (E, 2P)$. The groups $J_1(19)(\mathbb{Q})$, $J_1(23)(\mathbb{Q})$ and $J_1(25)(\mathbb{Q})$ are cyclic of orders 4383, 408991 and 227555 and generated by rational cuspidal divisors [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2]. Their reductions G have index 2, 23 and 11 in $J_1(19)(\mathbb{F}_3) \simeq \mathbb{Z}/8766\mathbb{Z}$, $J_1(23)(\mathbb{F}_3) \simeq \mathbb{Z}/9406793\mathbb{Z}$ and $J_1(25)(\mathbb{F}_3) \simeq \mathbb{Z}/2503105\mathbb{Z}$, and every effective cuspidal divisor of degree at most 9 on $Y_{\mathbb{F}_3}$ has zero image in $J_Y(\mathbb{F}_3)/G$, so (6) says that $[\pi_* D' - e\,\overline{y_0}] \in G$. In particular neither of the two tests depends on d.

By Table 3 the possible types of D' of degree at most 9 are [3], [5], [6], [3, 3], [7], [8], [5, 3], [9], [6, 3] and [3, 3, 3] for $n = 38$, with 1, 8, 11, 3, 24, 89, 24, 239, 33 and 6 cases up to the diamond operators, [4], [5], [6], [7], [8], [4, 4], [9] and [5, 4] for $n = 46$, with 5, 4, 5, 24, 71, 275, 178 and 220 cases, and [6], [7], [8] and [9] for $n = 50$, with 6, 20, 107 and 204 cases. We compute that each of these cases fails (6) or satisfies $[A_q(D')] \neq 0$ for some prime q: for $n = 38$ with $q \in \{5, 7, 11, 13, 17\}$ for all 438 cases (see the log), for $n = 46$ with $q \in \{5, 7, 11, 13, 17, 19\}$ for all 782 cases (see the log), and for $n = 50$ with $q \in \{7, 11, 13, 17, 19\}$, for the 133 cases of degree at most 8 in the octic computation and for the 204 cases of type [9] in the nonic computation. This excludes all $d \in \{6, 7, 8, 9\}$. □

6.5. **The curve $X_1(44)$.**

Proposition 6.8. *The group $\mathbb{Z}/44\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 8 or 9.*

Proof. Let $d \in \{8, 9\}$. We have $\operatorname{rk} J_1(44)(\mathbb{Q}) = 0$ [DEvH+21, Theorem 3.1(2)] and $\operatorname{gon}_{\mathbb{Q}} X_1(44) \geq 10$ [NV26, Table 1], so Proposition 2.5(a) with $p = 3$ excludes the entirely cuspidal reduction. By Table 3 the non-cuspidal part D' is a single closed point of degree $5, \dots, d$, so C' has degree at most 4. The closed cusps of $X_1(44)_{\mathbb{F}_3}$ have degrees $1^{15}, 2^5, 5^3, 10$, and those of degree at most 4 are reductions of rational cuspidal divisors of the same degree, so every prime $q \nmid 132$ is admissible. There are 6, 16, 24 and 92 diamond orbits of points of degree 5, 6, 7 and 8, and we compute that for a representative D' of each of them one of $[A_q(D')]$, $q \in \{5, 7, 13, 17, 19\}$, is non-zero.

For $d = 9$ it remains to treat $D' = P$ of degree 9, with $C' = 0$. Then $[A_5 P] = 0$ by Proposition 2.2(4), that is, $B = T - U$ is principal, where $T = T_5 P$ and $U = P + 5\langle 5\rangle P$, both of degree 54 and computed directly on the moduli model, and P may be taken among the 226 representatives of the diamond orbits of the 2260 points of degree 9. The genus of $X_1(44)$ is 36, and $\dim R_2 = 105$, $\dim R_4 = 245$. We compute the canonical model over $\mathbb{F}_3$, of degree 70 in $\mathbb{P}^{35}$, as the canonical embedding of a plane model of degree 19, from which we also obtain the local parameters, and the multiplication $R_2 \times R_2 \to R_4$, and we check with Lemma 8.1 (Section 8), with $\mathcal{L} = \mathcal{M} = 2K_X$, that $\ell(B) = 0$ in all 226 cases, which is a contradiction. □

6.6. **The curve $X_1(49)$.** Over octic and nonic fields, $\mathbb{Z}/49\mathbb{Z}$ is excluded by formal immersion at 2 in Proposition 7.7. Over sextic and septic fields we use the Hecke operators A_5 and A_2. The prime $q = 2$ is not covered by Proposition 2.2(2), so we first show the following.

Lemma 6.9. *The operator $A_2 = T_2 - 2\langle 2\rangle - 1$ annihilates $J_1(49)(\mathbb{Q})$.*

Proof. By [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2] the group $J_1(49)(\mathbb{Q})$ is finite with invariant factors $[7, 52367710906884085342]$, so its 2-primary part is $\{0, z\}$

for an element z of order 2. Reduction modulo 2 is injective on the odd part, and on the reduction of a rational point Frobenius acts trivially and Verschiebung acts as multiplication by 2, so A_2 annihilates the odd part by the Eichler-Shimura relation. By Proposition 2.2(2) the element z lies in the kernel of A_5 on $J_1(49)[2]$, and we compute, using the action of the Hecke algebra on $H_1(J_1(49)(\mathbb{C}),\mathbb{Z})/2H_1(J_1(49)(\mathbb{C}),\mathbb{Z}) \simeq J_1(49)[2]$, that this kernel has dimension 2 and meets the kernel of T_2 trivially. As T_2 and $\langle 2\rangle$ preserve $\{0,z\}$, it follows that $T_2 z = \langle 2\rangle z = z$, so $A_2 z = -2z = 0$. □

Proposition 6.10. *The group $\mathbb{Z}/49\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 6 or 7.*

Proof. Let $d \in \{6,7\}$, and let D be the trace divisor of a point of order 49 over a number field of degree d. We have $\operatorname{rk} J_1(49)(\mathbb{Q}) = 0$ by [DEvH+21, Theorem 3.1(2)], and Abramovich's bound gives $\operatorname{gon}_{\mathbb{Q}} X_1(49) > 11.66 > 7$, so Proposition 2.5(a) with $p = 3$ excludes the entirely cuspidal reduction. The Galois orbits of cusps over $\mathbb{Q}$ have degrees $1^{21}, 6^3, 21$, and 3 is a primitive root modulo 49, so each of them stays irreducible modulo 3. So every closed cusp of $X_1(49)_{\mathbb{F}_3}$ is the reduction of a rational cuspidal divisor of the same degree, and $A_5 C' = A_2 C' = 0$ for every cuspidal part C' by Lemma 2.3. By Table 3 the non-cuspidal part D' of the reduction is a single closed point of degree $4 \le \deg D' \le d$. Moreover $[A_5(D)] = 0$ by Proposition 2.2(4), and $[A_2(D)] = 0$ by Lemma 6.9, as $A_2 c_0 = 0$, so $[A_5(D')] = [A_2(D')] = 0$. We compute that $[A_5(D')] \neq 0$ for the representatives of the 1 and 3 diamond orbits of degrees 4 and 5, and also for the representatives of the 8 diamond orbits of degree 6, and we compute that $[A_2(D')] \neq 0$ for the representatives of the 19 diamond orbits of degree 7. □

6.7. The curves $X_1(58)$ and $X_1(62)$.

Proposition 6.11. *The groups $\mathbb{Z}/58\mathbb{Z}$ and $\mathbb{Z}/62\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over a nonic field.*

Proof. Let $n = 58$ or 62, put $N = n/2$, so that $N = 29$ or 31, and let $\pi : X_1(n) \to Y = X_1(N)$, $(E,P) \mapsto (E,2P)$, which over a non-cuspidal point (E,P_N) has fibre $E[2]\setminus\{0\}$. We have $\operatorname{gon}_{\mathbb{Q}} X_1(29) = 11$ and $\operatorname{gon}_{\mathbb{Q}} X_1(31) = 12$ [DvH14, Theorem 4 and Table 1], and

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

[DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], and in both cases $J_1(N)(\mathbb{Q})$ is generated by rational cuspidal divisors. Let $D_Y = \pi_* D$. The closed cusps of $Y_{\mathbb{F}_3}$ have degrees $1^{N'}, N'$ with $N' = (N-1)/2$, as do the orbits of cusps over $\mathbb{Q}$, since 3 has order $N-1$ modulo N. If D_Y reduced to a cuspidal divisor, it would be supported on the rational cusps, and Proposition 2.5(a) would give a contradiction. So D reduces to $D' + C'$ with $D' \neq 0$.

By the Hasse bound a non-cuspidal point of $X_1(n)$ over $\mathbb{F}_{3^e}$ has $e \ge 5$, so D' is a single closed point Q_e of degree $e \in \{5,\dots,9\}$, and C' has degree at most 4, so it is supported on the rational cusps. Write $\pi(Q_e) = P_k$ with $e = fk$ and $f \in \{1,2,3\}$. If $f = 2$, then $(k,e) \in \{(3,6),(4,8)\}$, and an elliptic curve over $\mathbb{F}_{27}$ or $\mathbb{F}_{81}$ with a point of order N has N or $3N$ points, an odd number, so its 2-division polynomial is irreducible and the fibre has no point of degree 2 over P_k. If $f = 3$ then $k = 3$, as Y has no non-cuspidal points over $\mathbb{F}_9$, and for $N = 31$ also no points of degree 3. So $\pi_* Q_e$ is $3P_3$, for $N = 29$, or a point P_k of degree $k \in \{5,\dots,9\}$ at which the elliptic curve has a rational point of order 2, and the

cuspidal part of $\pi_* D$ is supported on the rational cusps. Hence

$$[P_k - k\,\overline{c_0}] \in H \quad \text{or} \quad [3P_3 - 9\,\overline{c_0}] \in H,$$

where $H \subseteq J_Y(\mathbb{F}_3)$ is the reduction of $J_Y(\mathbb{Q})$. We compute

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

so that H has index $2^9 \cdot 3$, respectively $2^2 \cdot 31 \cdot 61$. For $n = 58$ there are 14, 84, 168, 476 and 1582 tests in degrees 3, 6, 7, 8 and 9, and none of the classes lies in H. For $n = 62$ there are 90, 90, 180, 630 and 1200 tests in degrees $5, \dots, 9$, and exactly 5 classes lie in H, all of degree 9.

These 5 points are the reductions of the closed point B of degree 9 of $X_1(31)$, and of its diamond translates, given by the point of order 31 of Proposition 13.5. Indeed, we check that the field of definition of B is inert at 3 and that the reductions of the 15 diamond translates of B are exactly these 5 points. So D_Y and a diamond translate B' of B have the same reduction, and as $[D_Y - B'] \in J_1(31)(\mathbb{Q})$ we get $D_Y \sim B'$, so $D_Y = B'$ by Lemma 2.7. As $X_1(31)$ is a fine moduli space, the elliptic curve of D is then a curve of Proposition 13.5 over its field of definition, and its torsion is $\mathbb{Z}/31\mathbb{Z}$, so it has no point of order 2, which is a contradiction. □

7. Formal immersion at the prime 2

At the levels n of this section the trace divisor can reduce modulo 2 to an entirely cuspidal divisor, and in most cases neither Proposition 2.5(b) nor Proposition 4.3 excludes this: the lower bounds that we have for the gonality of $X_1(n)$ are too weak (for $n = 51$ Abramovich's bound gives only $\mathrm{gon}_{\mathbb{C}}\, X_1(51) > 11.42$, while Proposition 2.5(b) needs a bound larger than 12 already for $d = 6$), or the Jacobian has positive rank. We exclude the entirely cuspidal reduction by a formal immersion argument at 2 (Proposition 7.3). It allows elements of the Hecke algebra with finite image on the Mordell-Weil group, so it applies also when the Jacobian has positive rank. We treat each level once, for all the degrees in which this method is needed, and usually a single computation, in the largest degree, covers all of them (Remark 7.4). The level 75 is included here because its proof uses the same kind of quotient of $X_1(n)$.

Reduction modulo 2 need not be injective on the torsion of the Jacobian (the point -1 of μ_2 over $\mathbb{Z}_2$ reduces to 1). The following lemma shows that a suitable Hecke operator kills such points.

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 $(T - \delta)z = 0$.*

Proof. Choose coordinates $X = (X_1, \dots, X_g)$ of the formal group of A, that is, functions vanishing on the zero section whose differentials at the origin of $A_{\mathbb{F}_2}$ form a basis of the cotangent space. Then the points of $A(\mathbb{Q}_2)$ that reduce to 0 are the points with coordinates in $2\mathbb{Z}_2$ (see the proof of Lemma′ in [Kat81, Appendix]). Write

$$[2](X) = 2X + Q(X) + R(X),$$

where the coordinates of Q are homogeneous of degree 2 and R has only terms of degree at least 3, all with coefficients in $\mathbb{Z}_2$. Let M be a matrix over $\mathbb{Z}_2$ whose reduction $\overline{M}$ is the matrix of the linear part of V. As $[2] = V \circ F$ on $A_{\mathbb{F}_2}$ and F squares the coordinates, the reduction of Q is $\overline{Q}(X) = \overline{M}(X_1^2, \dots, X_g^2)^t$.

Write the coordinates of z as $2u$ with $u \in \mathbb{Z}_2^g$. As $2z = 0$, we have

$$0 = [2](2u) \equiv 4u + 4Q(u) \pmod 8,$$

so $\overline{u} + \overline{M}(\overline{u}_1^2, \dots, \overline{u}_g^2)^t = 0$, and as $a^2 = a$ for $a \in \mathbb{F}_2$, we get $(\overline{M} - 1)\overline{u} = 0$. Put $\alpha = T - \delta$. As the linear part of F is 0, the linear part of α on $A_{\mathbb{F}_2}$ is $\overline{N}(\overline{M} - 1)$, where $\overline{N}$ is the linear part of δ. Hence the linear term of α at $2u$ is divisible by 4, and so are all the other terms, so the coordinates of αz lie in $4\mathbb{Z}_2$.

Finally, a non-zero point v with coordinates in $4\mathbb{Z}_2$ is not killed by 2. Indeed, 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 $2s > s + 1$. As $2\alpha z = \alpha(2z) = 0$, we get $\alpha z = 0$. □

We apply this to quotients of $X_1(n)$. 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 c_0 for the image of the standard cusp, and $\mathcal{C}$ for the Cartier operator on the differentials of $Y_{\mathbb{F}_2}$: if x is a separating variable, every differential can be written uniquely as $(f^2 + g^2 x)\,dx$ with f, g rational functions on $Y_{\mathbb{F}_2}$, and $\mathcal{C}\big((f^2 + g^2 x)\,dx\big) = g\,dx$. Equivalently, in terms of a local parameter t we have $\mathcal{C}\big(\sum_n a_n t^n\,dt\big) = \sum_n a_{2n+1}^{1/2} t^n\,dt$. The operator $\mathcal{C}$ preserves $H^0(Y_{\mathbb{F}_2}, \Omega^1)$ and is $\mathbb{F}_2$-linear on it, and at a cusp at which q is a local parameter it acts on q-expansions by $\sum_n a_n q^n\,dq/q \mapsto \sum_n a_{2n}^{1/2} q^n\,dq/q$. If all a_n lie in $\mathbb{F}_2$, this is Atkin's operator U_2: $\sum_n a_n q^n \mapsto \sum_n a_{2n} q^n$ applied to $\sum_n a_n q^n$. Note that here U_2 is only an operation on q-expansions, as n is odd and the Hecke operators U_q are defined only for $q \mid n$.

We describe the fixed points of the diamond operators with the following lemma.

Lemma 7.2. *Let n be odd, and let $\langle a \rangle \neq 1$ fix a geometric point x of $X_1(n)$ in characteristic 0 or 2. If x is a cusp, then a is congruent to the same sign ± 1 modulo every prime dividing n, so n is not squarefree. If x is not a cusp, then $a^2 \equiv -1$ or $a^2 \pm a + 1 \equiv 0 \pmod n$, and $a \not\equiv \pm 1 \pmod m$ for every divisor $m \geq 5$ of n.*

Proof. If $x = (E, P)$ is not a cusp, then $u(P) = aP$ for an automorphism u of E, and $u \neq \pm 1$ as $\langle a \rangle \neq 1$. Up to sign, $u^2 = -1$ or $u^2 + u + 1 = 0$, which gives the congruences. If $a \equiv \pm 1 \pmod m$ for a divisor $m \geq 5$ of n, then u or $-u$ fixes the point $(n/m)P$ of order m, which is impossible, as the kernel of $v - 1$ has order at most 4 for every automorphism $v \neq 1$ of E. For a cusp in characteristic 0 this is Section 2.1, and it also holds in characteristic 2, as the cuspidal subscheme is finite étale over $\mathbb{Z}[\frac{1}{n}]$. □

Let $\mathbb{T}_Y$ be 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, all of which descend to Y as they commute with H. By the Néron mapping property every $\psi \in \mathbb{T}_Y$ extends to the Néron model of J_Y over $\mathbb{Z}_2$, which is an abelian scheme, and we write ψ^* for its action on the cotangent space $H^0(Y_{\mathbb{F}_2}, \Omega^1)$ of the special fibre. As ψ commutes with the Verschiebung of the special fibre, ψ^* commutes with $\mathcal{C}$, which is the pull-back by the

Verschiebung [Oda69]. By the Eichler-Shimura relation $T_2 = F + \langle 2\rangle V$ and as the Frobenius F pulls back differentials to 0, we have

$$T_2^* = \mathcal{C}\,\langle 2\rangle^* \quad \text{on } H^0(Y_{\mathbb{F}_2}, \Omega^1), \tag{7}$$

and hence

$$(T_2 - \langle 2\rangle)^* = (\mathcal{C} - 1)\langle 2\rangle^* \quad \text{on } H^0(Y_{\mathbb{F}_2}, \Omega^1). \tag{8}$$

In the following criterion, the elements ψ_i turn the class of the difference of a rational divisor and a cuspidal divisor with the same reduction into a torsion class, Lemma 7.1 shows that $T_2 - \langle 2\rangle$ kills this class, and by (8) the formal immersion condition becomes a condition on the space U below.

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.

Proof. Suppose that D reduces to $\overline{C}$. The cuspidal subscheme of Y is finite étale at 2, so $\overline{C}$ lifts uniquely to a cuspidal divisor C, which is fixed by a Frobenius element at 2, so it is defined over the decomposition field $L \subseteq \mathbb{Q}(\zeta_n)$ of a prime λ above 2, which satisfies $L_\lambda = \mathbb{Q}_2$. For each i the class $\psi_i[D - C] = \psi_i[D - dc_0] - \psi_i[C - dc_0]$ is torsion, by the assumption on ψ_i and by Manin-Drinfeld, and it reduces to 0 modulo λ, as ψ_i commutes with reduction. By Parent's result it is killed by 2, so by Lemma 7.1, applied to the Néron model of $J(Y)$ over $\mathbb{Z}_2$ with $T = T_2$ and $\delta = \langle 2\rangle$, we get $(T_2 - \langle 2\rangle)\psi_i[D - C] = 0$.

Consider the morphism $f : Y^{(d)} \to J(Y)^r$ over $\mathbb{Z}_2$ given by $f(B) = \big((T_2 - \langle 2\rangle)\psi_i[B - dc_0]\big)_i$. Then $f(D) = f(C)$, and D and C have the same reduction $\overline{C}$. By (8), and since $\langle 2\rangle^*$ is invertible and commutes with $\mathcal{C}$ and with the ψ_i^*, the image of the cotangent map of f at $\overline{C}$ is the restriction of U to $\overline{C}$, as the cotangent map of $Y^{(d)} \to J(Y)$, $B \mapsto [B - dc_0]$, at $\overline{C}$ is the restriction map $H^0(Y_{\mathbb{F}_2}, \Omega^1) \to H^0(\overline{C}, \Omega^1|_{\overline{C}})$. By assumption it is surjective, so f is a formal immersion at $\overline{C}$, and by [DKSS23, Lemma 4.2] (which is due to Parent [Par99, Lemme 4.13]) f is injective on the residue class of $\overline{C}$. Hence $D = C$, which is a contradiction since D is non-cuspidal. □

As in Section 5.2, we compute the subspaces $\Omega(jP)$ of $H^0(Y_{\mathbb{F}_2}, \Omega^1)$ once for each closed cusp P of $Y_{\mathbb{F}_2}$ and each j, as spaces of differentials or from local expansions at P, and $\Omega(\overline{C})$ as their intersection. When a group of automorphisms of Y which commute with $\mathcal{C}$ and preserve U acts on the cusps, we compute $\Omega(jP)$ for one cusp in each orbit and transport it to the others. When $J(Y)(\mathbb{Q})$ is finite we take $r = 1$ and $\psi_1 = 1$, and then $U = (\mathcal{C} - 1)H^0(Y_{\mathbb{F}_2}, \Omega^1)$.

Remark 7.4. If the restriction of U to $\overline{C}$ is surjective, then so is its restriction to every effective divisor $\overline{C}' \le \overline{C}$, as the restriction map $H^0(\overline{C}, \Omega^1|_{\overline{C}}) \to H^0(\overline{C}', \Omega^1|_{\overline{C}'})$ is surjective. Every effective cuspidal divisor of degree $d' < d$ is contained in one of degree d, for example in the divisor obtained by adding $d - d'$ times a rational cusp, and in all our applications this preserves the conditions on the cuspidal divisors that can occur. So the computation

for the largest degree in which we use a curve also covers the smaller degrees. The same holds for the condition of Lemma 5.3, as $L(2\overline{C}') \subseteq L(2\overline{C})$.

Remark 7.5. The condition in Proposition 7.3 is the usual formal immersion criterion, written in terms of cotangent spaces. When $\overline{C}$ is a sum of rational cusps it corresponds, by the duality between the Hecke algebra and q-expansions, to the linear independence of suitable Hecke operators modulo 2, as in the criterion of Kamienny [Kam92b] for $X_0(p)$ and its generalization by Parent [Par00, Théorème 1.10 and Proposition 2.7] (see [DKSS23, Proposition 5.3]), and when $\overline{C}$ is a sum of distinct points it is [DKSS23, Lemma 8.3]. Instead of $T_2 - \langle 2\rangle$ one could use Parent's trick [DKSS23, Corollary 5.2], with A_q for an odd prime q congruent modulo n to a power of 2: such a q splits completely in the field L of the proof of Proposition 7.3, so A_q kills the torsion of $J_Y(L)$ by the argument of Proposition 2.2(2). We use $T_2 - \langle 2\rangle$ because its action on differentials modulo 2 is given by the Cartier operator, which is computed directly from a model of $Y_{\mathbb{F}_2}$, whereas A_q requires the Hecke correspondence T_q on Y for a prime q that need not be small (for $n = 63$ the smallest such q is 67), and because the condition is then checked in the same way at every effective cuspidal divisor, including those supported on cusps that are not rational and those with multiplicities.

7.1. The curve $X_1(45)$.

Proposition 7.6. *The group $\mathbb{Z}/45\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree $d \in \{6, 7, 8, 9\}$.*

Proof. Let $X = X_1(45)$, which has genus 41, and let D be the trace divisor of a point of order 45 over a number field of degree d. We have $\operatorname{rk} J_1(45)(\mathbb{Q}) = 0$ [DEvH+21, Theorem 3.1(2)] and $\operatorname{gon}_{\mathbb{Q}} X \geq 10$ [NV26, Table 1]. We compute that the non-cuspidal closed points of $X_{\mathbb{F}_2}$ of degree at most 9 are 60 points of degree 8 and 60 points of degree 9, each forming 5 diamond orbits.

Suppose first that the reduction of D modulo 2 is not entirely cuspidal. Then $d \in \{8, 9\}$, and the reduction is $P + C'$, where P is one of these points, and $C' = 0$ or C' is a cusp of degree 1, which is the reduction of a rational cusp. As $J_1(45)(\mathbb{Q})$ is finite, it follows that $[A_q P] = 0$ for every prime $q \nmid 90$ (Proposition 2.2(4) and Lemma 2.3). We compute that for a representative P of each orbit of points of degree 8 one of $[A_q P]$, $q \in \{7, 11, 13, 17, 19\}$, is non-zero, and we compute that $A_7 P$ is not principal for a representative P of each orbit of points of degree 9.

So the reduction of D is entirely cuspidal. The closed cusps of $X_{\mathbb{F}_2}$ have degrees $1^{12}, 2^4, 4^5, 6^2, 12$, so there are 148945 effective cuspidal divisors of degree 8. We compute that $U = (\mathcal{C} - 1)H^0(X_{\mathbb{F}_2}, \Omega^1)$ has dimension 39 and that its restriction to each of these divisors has rank 8. By Remark 7.4 the restriction of U is also surjective at every effective cuspidal divisor of degree 6 or 7, so for $d \leq 8$ Proposition 7.3 gives a contradiction.

Now let $d = 9$. Using the subspaces $\Omega(m\bar{c})$ with $m \deg \bar{c} \leq 8$ from the computation above, and the subspace $\Omega(9\bar{c})$ at a rational cusp $\bar{c}$, which we compute and transport to the other rational cusps with the diamond operators, we check that the restriction of U to every effective cuspidal divisor of degree 9 is surjective, except for 8 divisors, which are supported on the cusps of degree 1 and 2. The Galois orbits of cusps of X over $\mathbb{Q}$ have degrees $1^{12}, 2^4, 4^3, 6^2, 8, 12$ [DEvH+21, Lemma 2.8], so, comparing with the closed cusps of $X_{\mathbb{F}_2}$, the closed cusps of degree 1 and 2 are reductions of Galois orbits of cusps of the same degree, and the 8 exceptional divisors are reductions of effective rational cuspidal divisors C. If reduction modulo 2 is injective on $J_1(45)(\mathbb{Q})$, then $D \sim C$, and as $\operatorname{gon}_{\mathbb{Q}} X \geq 10 > 9$, Lemma 2.7 gives $D = C$, which is a contradiction.

It remains to show that reduction modulo 2 is injective on $J_1(45)(\mathbb{Q})$. It is injective on the odd part. The 2-primary part of $J_1(45)(\mathbb{Q})$ is $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/32\mathbb{Z}$ [DEvH+21, Theorem 4.13 and Table 2], whose automorphism group is a 2-group, so the subgroup $H = \{1, 16, 31\}$ of $\Delta(45)$ acts trivially on it, and $\pi^*\pi_* = 3$ on it, where $\pi : X \to Y = X/H$. Hence it suffices to show that reduction modulo 2 is injective on $J_Y(\mathbb{Q})[2^\infty]$. Over $F = \mathbb{Q}(\zeta_3)$ the curve Y is isomorphic to $X_1(3, 15)$: the quotient of (E, P) by the subgroup generated by $15P$ gives a point of order 15 together with the kernel of the dual isogeny, with a generator determined by $15P$ and the Weil pairing, and this data is invariant exactly under H. This isomorphism comes from the moduli interpretation, so it is compatible with reduction modulo the prime of F above 2. By Lemma 5.4, reduction modulo this prime is injective on $J_1(3, 15)(F)$, and hence on $J_Y(\mathbb{Q}) \subseteq J_Y(F)$. □

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

Proposition 7.7. *The group $\mathbb{Z}/49\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 8 or 9.*

Proof. Let $X = X_1(49)$ and $J = J_1(49)$, let $d \in \{8, 9\}$, and let D be the trace divisor of a point of order 49 over a number field of degree d. We have

$$J(\mathbb{Q}) \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/52367710906884085342\mathbb{Z}$$

by [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], so $J(\mathbb{Q})[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z}$. We first show that reduction modulo 2 is injective on $J(\mathbb{Q})$. It is injective on the odd part. The diamond group $\Delta(49)$ has order 21, so it acts trivially on $J(\mathbb{Q})[2^\infty]$, and for the forgetful map $\pi : X \to X_0(49)$ we have $\pi^*\pi_* = \sum_{\delta \in \Delta(49)} \delta = 21$ on this group. Hence π_* is injective on $J(\mathbb{Q})[2^\infty]$. The curve $X_0(49)$ is the elliptic curve 49.a4, $y^2 + xy = x^3 - x^2 - 2x - 1$, whose rational point $(2, -1)$ of order 2 reduces to the non-zero point $(0, 1)$ modulo 2. As reduction commutes with π_*, it is injective on $J(\mathbb{Q})[2^\infty]$.

No elliptic curve over $\mathbb{F}_{2^e}$ with $e \leq 8$ has a point of order 49. For $e \leq 5$ this follows from the Hasse bound, for $e = 6$ a point of order 49 forces $E(\mathbb{F}_{64}) = E[7]$ (see the discussion after Lemma 2.6), and for $e = 7, 8$ the only possible group orders are 147 and 245, with traces of Frobenius -18 and 12, which are impossible by [Wat69, Theorem 4.1]. So $X_{\mathbb{F}_2}$ has no non-cuspidal closed points of degree at most 8, and we compute that it has 42 of degree 9, in 2 diamond orbits. For $d = 9$ a non-cuspidal reduction of D modulo 2 is one of these points P, and $[A_3 P] = 0$ as $J(\mathbb{Q})$ is finite, but $A_3 P$ is not principal for a representative P of each orbit. So the reduction $\overline{D}$ of D modulo 2 is entirely cuspidal. The Galois orbits of cusps of X have degrees $1^{21}, 6^3, 21$, and the closed cusps of $X_{\mathbb{F}_2}$ have degrees $1^{21}, 3^6, 21$.

If $\overline{D}$ is supported on the cusps of degree 1, it is the reduction of an effective rational cuspidal divisor C, and $[D - C] \in J(\mathbb{Q})$ reduces to 0, so $D \sim C$. As $\operatorname{gon}_{\mathbb{Q}} X > 11.66 > 9$, this contradicts Lemma 2.7.

So $\overline{D}$ contains a cusp of degree 3, and at most $d - 3 \leq 6$ cusps of degree 1, counted with multiplicity. The 21 cusps of degree 1 lie on the Néron 49-gon, and $\Delta(49)$ acts on them simply transitively, as a diamond operator $\langle a \rangle$ multiplies the label of such a cusp in $(\mathbb{Z}/49\mathbb{Z})^\times/\{\pm 1\}$ by a. Fix a set $\mathcal{A}$ of 18 of these cusps. For each of the at most 6 cusps of degree 1 in the support of $\overline{D}$ and each of the 3 cusps not in $\mathcal{A}$, exactly one diamond operator maps the former to the latter. As $6 \cdot 3 < 21$, there is a $\delta \in \Delta(49)$ such that $\delta\overline{D}$ is supported on $\mathcal{A}$ and the 6 cusps of degree 3, and as δD is again the trace divisor of a point of order 49, we may assume that $\delta = 1$. The space $U = (\mathcal{C} - 1)H^0(X_{\mathbb{F}_2}, \Omega^1)$ has dimension 68, and

we compute that its restriction to each of the

$$6\binom{23}{6} + \binom{7}{2}\binom{20}{3} + \binom{8}{3} = 629678$$

effective divisors of degree 9 supported on these cusps which contain a cusp of degree 3 is surjective. By Remark 7.4, adding a cusp in $\mathcal{A}$, the same holds for the divisors of degree 8 of this form, and Proposition 7.3 with $H = \{1\}$ gives a contradiction. □

7.3. **The curve $X_1(51)$.** The following lemma treats the quotients Y_{51} (used only in Section 15) and Y_{63} (used in Section 7.5).

Lemma 7.8. *Let $Y_{51} := X_1(51)/\langle 16\rangle$ and $Y_{63} := X_1(63)/\langle 8\rangle$. The diamond operators $\langle 16\rangle$ and $\langle 8\rangle$ have order 2 and act freely on $X_1(51)$ and $X_1(63)$, also in characteristic 2, so Y_{51} and Y_{63} have good reduction at 2 and have genus 33 and 49. The function field of Y_{51} is obtained by adjoining to the function field of $X_1(17)$ a root of the 3-division polynomial of the universal elliptic curve, and that of Y_{63} by adjoining to the function field of $X_1(9)$ a root of the 7-division polynomial of the universal elliptic curve. The groups $J(Y_{51})(\mathbb{Q})$ and $J(Y_{63})(\mathbb{Q})$ are finite.*

Proof. Write $(r, s, a) = (17, 3, 16)$ and $(9, 7, 8)$ in the two cases, so that $a \equiv -1 \pmod r$ and $a \equiv 1 \pmod s$. A point of order rs corresponds to a pair of points (P_r, P_s) of orders r and s, and modulo the common sign, $\langle a\rangle$ identifies (P_r, P_s) with $(P_r, -P_s)$. So Y parametrizes pairs (E, P_r) together with the x-coordinate of P_s, which gives the description of the function field. As $a \equiv -1 \pmod r$ with $r \geq 9$ and $a \equiv 1 \pmod s$, Lemma 7.2 shows that $\langle a\rangle$ fixes no geometric point of $X_1(rs)$, in characteristic 0 or 2. So the quotient map is étale, also at 2, and the genera follow from Riemann-Hurwitz, as $X_1(51)$ and $X_1(63)$ have genus 65 and 97.

The Jacobian of $X_1(rs)/\langle a\rangle$ is isogenous to the part of $J_1(rs)$ on which $\langle a\rangle$ acts trivially, whose isogeny factors correspond to the newforms of level dividing rs whose characters χ satisfy $\chi(a) = 1$. For $rs = 51$ we have $\operatorname{rk} J_1(51)(\mathbb{Q}) = 0$ by [DEvH+21, Theorem 3.1(2)]. For $rs = 63$ the only newform of level dividing 63 with positive analytic rank is 63.2.s.a, whose character χ satisfies $\chi(8) = -1$, as we check, so it does not contribute to $J(Y_{63})$, and $J(Y_{63})(\mathbb{Q})$ is finite by Kato's theorem. □

Proposition 7.9. *The group $\mathbb{Z}/51\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree $d \in \{6, 7, 8, 9\}$.*

Proof. Let $X = X_1(51)$, which has genus 65, and let D be the trace divisor of a point of order 51 over a number field of degree d. We have $\operatorname{rk} J_1(51)(\mathbb{Q}) = 0$ [DEvH+21, Theorem 3.1(2)]. No elliptic curve over $\mathbb{F}_{2^e}$ with $e \leq 8$ has a point of order 51. For $e \leq 5$ this follows from the Hasse bound, for $e = 6$ and $e = 8$ the only multiples of 51 in the Hasse intervals are 51 and 255, with traces of Frobenius 14 and 2, which are impossible by [Wat69, Theorem 4.1], and for $e = 7$ the Hasse interval $[107, 151]$ contains no multiple of 51. So $X_{\mathbb{F}_2}$ has no non-cuspidal closed points of degree at most 8, and we compute that it has 80 of degree 9, in 5 diamond orbits. For $d = 9$ a non-cuspidal reduction of D modulo 2 is one of these points P, and $[A_5 P] = 0$ as $J_1(51)(\mathbb{Q})$ is finite, but we compute that $A_5 P$ is not principal for a representative P of each orbit. So the reduction of D is entirely cuspidal.

The closed cusps of $X_{\mathbb{F}_2}$ have degrees $1^{16}, 2^8, 8^4$, and $U = (\mathcal{C} - 1)H^0(X_{\mathbb{F}_2}, \Omega^1)$ has dimension 62. We compute the subspaces $\Omega(m\bar{c})$ with $m \deg \bar{c} \leq 8$, and we compute the subspace

$\Omega(9\bar{c})$ at a rational cusp $\bar{c}$, which we transport to the other rational cusps with the diamond operators. From these we check that the restriction of U to each of the

$$[t^9](1-t)^{-16}(1-t^2)^{-8}(1-t^8)^{-4} = 3333264$$

effective cuspidal divisors of degree 9 is surjective. By Remark 7.4 the same holds in the degrees 6, 7 and 8, and Proposition 7.3 with $H = \{1\}$ gives a contradiction. □

7.4. **The curve $X_1(55)$.** For the levels 55 and 77 the curve Y is a cyclic unramified cover of $X_0(n)$, which we construct over $\mathbb{F}_2$ by class field theory, as we also do for $X_0(57)$ and $X_0(69)$ in Section 9.2. By class field theory, a geometrically connected unramified cyclic cover of degree k of $Z_{\mathbb{F}_2}$, for a curve Z, in which a given rational point splits, corresponds to a surjective homomorphism $\mathrm{Pic}^0(Z_{\mathbb{F}_2}) \to \mathbb{Z}/k\mathbb{Z}$, and it is determined by its values at enough closed points. For $k = 2$ we construct it by an Artin-Schreier equation, and for $k = 4$ by Artin-Schreier-Witt equations of length 2.

Lemma 7.10. *Let $H \subseteq \Delta(55)$ be the subgroup of order 5 generated by $\langle 16\rangle$, and $Y = X_1(55)/H$. Then $Y \to X_0(55)$ is an unramified cyclic cover of degree 4, also over $\mathbb{F}_2$, and Y has genus 17. The closed cusps of $Y_{\mathbb{F}_2}$ have degrees $1^4, 2^2, 4^2$, and the push-forward to $Y_{\mathbb{F}_2}$ of an effective cuspidal divisor of degree at most 9 on $X_1(55)_{\mathbb{F}_2}$ is supported on the four rational cusps above the cusp of width 55 of $X_0(55)$ and the cusp of degree 4 above the cusp of width 11.*

Proof. By Lemma 7.2, $\Delta(n)$ acts freely on $X_1(n)$ for $n \in \{55, 77\}$, in characteristic 0 and in characteristic 2, as n is squarefree, and for $n = 55$ the congruence $a^2 \equiv -1$ is impossible modulo 11 and $a^2 \pm a + 1 \equiv 0$ modulo 5, and for $n = 77$ the first is impossible modulo 7 and the second modulo 11. So $X_1(55) \to Y \to X_0(55)$ are unramified, also over $\mathbb{F}_2$, and Y has genus $1 + (81-1)/5 = 17$. The group $\Delta(55)/H$ is cyclic of order 4, generated by $\langle 2\rangle$. The Frobenius elements at the cusps of $X_0(55)_{\mathbb{F}_2}$ of widths $55, 11, 5, 1$ are $\langle 2\rangle^0, \langle 2\rangle^1, \langle 2\rangle^2, \langle 2\rangle^3$, which gives the degrees of the cusps of $Y_{\mathbb{F}_2}$. The source cusps of $X_1(55)_{\mathbb{F}_2}$ above the remaining cusps of $Y_{\mathbb{F}_2}$ have degrees 10 and 20, which proves the last assertion. □

We construct $Y_{\mathbb{F}_2}$ as follows. We have $\mathrm{Pic}(X_0(55)_{\mathbb{F}_2}) \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}$, and there is exactly one homomorphism to $\mathbb{Z}/4\mathbb{Z}$ with the Frobenius values at the cusps given in the proof of Lemma 7.10. We construct the corresponding Artin-Schreier-Witt cover, and check that it has genus 17, that a rational cusp of width 55 splits in it, and that its Frobenius elements at a set of generators of $\mathrm{Pic}(X_0(55)_{\mathbb{F}_2})/4$ are the right ones. By class field theory this cover is $Y_{\mathbb{F}_2}$.

Proposition 7.11. *The group $\mathbb{Z}/55\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree $d \in \{7, 8, 9\}$.*

Proof. Let D be the trace divisor of a point of order 55 over a number field of degree d. We have $\mathrm{rk}\, J_1(55)(\mathbb{Q}) = 0$ [DEvH+21, Theorem 3.1(2)]. We compute that the non-cuspidal closed points of $X_1(55)_{\mathbb{F}_2}$ of degree at most 9 are 20 points of degree 7, which form a single diamond orbit, and 40 points of degree 9, which form 2 diamond orbits. The closed cusps of $X_1(55)_{\mathbb{F}_2}$ have degrees $1^{20}, 4^5, 10^2, 20$, and those of degree 1 are reductions of rational cusps. So if the reduction of D modulo 2 is not entirely cuspidal, it is $P + C'$ with P of degree 7 and C' supported on the reductions of the rational cusps, or P of degree 9. As $J_1(55)(\mathbb{Q})$ is finite and A_3 annihilates the rational cusps, we get $[A_3 P] = 0$. We compute that $[A_3 P] \neq 0$ for a representative P of the orbit of points of degree 7, and that $A_3 P$ is not principal for a representative P of each orbit of points of degree 9.

So the reduction of D is entirely cuspidal. For $d = 7$ this contradicts Proposition 2.5(b), as Abramovich's bound gives $\mathrm{gon}_{\mathbb{Q}} X_1(55) > 14.28 > 14$. For $d \in \{8, 9\}$ the reduction of the push-forward $\pi_* D$ of D to the curve Y of Lemma 7.10 is entirely cuspidal as well, and by Lemma 7.10 it is supported on the four rational cusps of width 55 and the closed cusp of degree 4 above the cusp of width 11, which gives $[z^d](1-z)^{-4}(1-z^4)^{-1}$ possible divisors, that is, 201 for $d = 8$ and 280 for $d = 9$. As $J_Y(\mathbb{Q})$ is finite, we apply Proposition 7.3 with $r = 1$ and $\psi_1 = 1$. On the model of $Y_{\mathbb{F}_2}$ described above, $U = (\mathcal{C} - 1)H^0(Y_{\mathbb{F}_2}, \Omega^1)$ has dimension 15, and we compute that its restriction to each of the 201 divisors of degree 8 has rank 8, which proves the claim for $d = 8$, and we compute that its restriction to each of the 280 divisors of degree 9 is surjective, except for 8 of them, which are supported on the rational cusps and satisfy $\ell(\overline{C}) = 1$. Such a divisor $\overline{C}$ is the reduction of a rational cuspidal divisor C. If reduction modulo 2 is injective on $J_Y(\mathbb{Q})$, then $\pi_* D \sim C$, and by semicontinuity $\ell(C) \leq \ell(\overline{C}) = 1$, so $\pi_* D = C$, which is a contradiction.

It remains to show that reduction modulo 2 is injective on $J_Y(\mathbb{Q})$. By [DEvH+21, Theorem 4.13 and Table 2], $J_1(55)(\mathbb{Q})[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$, and as $\pi_* \pi^* = 5$, the group $J_Y(\mathbb{Q})[2^\infty]$ has order at most 32. Every closed cusp of $Y_{\mathbb{F}_2}$ is the reduction of a rational cuspidal divisor of the same degree, and we compute 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. Hence reduction is injective on $J_Y(\mathbb{Q})[2^\infty]$, and on the odd torsion it always is. □

7.5. **The curve $X_1(63)$.**

Proposition 7.12. *The group $\mathbb{Z}/63\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree $d \in \{6, 7, 8, 9\}$.*

Proof. Let $Y = Y_{63}$ be the quotient of Lemma 7.8, and let D be the push-forward to Y of the trace divisor of a point of order 63 over a number field of degree d. As $J(Y)(\mathbb{Q})$ is finite by Lemma 7.8, the operator $A_5 = T_5 - 1 - 5\langle 5 \rangle$ annihilates it (Proposition 2.2), and it annihilates the rational cuspidal divisors on Y (Lemma 2.3).

We compute that the non-cuspidal closed points of $X_1(63)_{\mathbb{F}_2}$ of degree at most 9 have degrees 7, 8 and 9, and that there are 54, 54 and 72 of them. They give 27, 27 and 36 closed points of $Y_{\mathbb{F}_2}$ of the same degrees, which form 3, 3 and 4 orbits under the residual diamond operators $\langle 2 \rangle$ and $\langle 5 \rangle$. The closed cusps of $Y_{\mathbb{F}_2}$ have degrees $1^9, 2^3, 3^9, 6$, and we check that those of degree at most 2 are reductions of rational cuspidal divisors of the same degree. So if the reduction of D modulo 2 is not entirely cuspidal, then $d \geq 7$, and the reduction is $P + C'$, where P is one of these closed points and C' is the reduction of an effective rational cuspidal divisor of degree $d - \deg P \leq 2$. As A_5 annihilates $J(Y)(\mathbb{Q})$ and the rational cuspidal divisors, this gives $[A_5 P] = 0$. For a representative P of each of the 10 orbits we compute that $A_5 P = T_5 P - P - 5\langle 5 \rangle P$ is not principal, for the points of degree 7, 8 and 9.

So the reduction of D is entirely cuspidal. The space $U = (\mathcal{C} - 1)H^0(Y_{\mathbb{F}_2}, \Omega^1)$ has dimension 45, and we compute that its restriction to each of the 105040 effective cuspidal divisors of degree 9 on $Y_{\mathbb{F}_2}$ is surjective. By Remark 7.4 the same holds in the degrees 6, 7 and 8, and Proposition 7.3 with $r = 1$ and $\psi_1 = 1$ gives a contradiction. □

7.6. **The curve $X_1(75)$.** We use the following quotient of $X_1(75)$. Let $H \subseteq \Delta(75)$ be the subgroup of order 2 generated by $\langle 26 \rangle$, and $Y = X_1(75)/H$. As $26 \equiv 1 \pmod{25}$ and $26 \equiv -1 \pmod{3}$, Lemma 7.2 shows that H acts freely, also in characteristic 2, so Y has

genus 73 and good reduction at 2. The curve Y parametrizes elliptic curves with a point of order 25 and a cyclic subgroup of order 3. In characteristic 2 an ordinary elliptic curve has a model $y^2+xy=x^3+a_2x^2+1/j$, and the non-zero points of a subgroup of order 3 have a common x-coordinate x_3 with $x_3^4+x_3^3+1/j=0$. So we obtain a model of $Y_{\mathbb{F}_2}$ by adjoining x_3 to the function field of $X_1(25)_{\mathbb{F}_2}$, and we check that this quartic extension is irreducible and has genus 73.

Proposition 7.13. *The group $\mathbb{Z}/75\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 8 or 9.*

Proof. Let $d\in\{8,9\}$ and let D be the trace divisor of a point of order 75 over a number field of degree d. We have $\operatorname{rk} J_1(75)(\mathbb{Q})=0$ [DEvH+21, Theorem 3.1(2)], and Abramovich's bound gives $\operatorname{gon}_{\mathbb{Q}} X_1(75)>23.80>2d$. So by Proposition 2.5(b) the elliptic curve has good reduction at some prime above 2, and the reduction of D modulo 2 is not entirely cuspidal.

We compute that the only non-cuspidal closed points of $X_1(75)_{\mathbb{F}_2}$ of degree at most 9 are 20 points of degree 7, which form a single diamond orbit. So the reduction of D is $P+C'$, where P is one of these points and C' is cuspidal of degree $d-7\le 2$, and we check that C' is the reduction of a rational cuspidal divisor which is fixed by σ_7. The Jacobian of the curve Y above has finitely many rational points, as it is a quotient of $J_1(75)$, so the operator $A_7=T_7-1-7\langle 7\rangle$ annihilates $J_Y(\mathbb{Q})$, and by Lemma 2.3 it annihilates the image of C' on Y. Hence the image P on $Y_{\mathbb{F}_2}$ of the closed point of degree 7 satisfies $[A_7P]=0$. We compute that T_7P consists of four closed points of degree 14, each with multiplicity 1, and that $\ell(A_7P)=0$ for a representative P of the orbit, which is a contradiction. □

7.7. The curve $X_1(77)$.

Lemma 7.14. *The groups $(\langle a\rangle-1)J_1(77)(\mathbb{Q})$, for every a, and $T_2J_1(77)(\mathbb{Q})$ are finite. If D is the trace divisor of a point of order 77 over a number field of degree at most 9, then the reduction of D modulo 2 is entirely cuspidal.*

Proof. We compute the winding submodules for all even characters modulo 77 (see also `C77/winding77.m`). Their dimensions add up to the genus 181 of $X_1(77)$, every non-trivial character has full winding submodule, and the winding submodule of the trivial character, of dimension 7, has codimension 1, and T_2 acts as 0 on the quotient. This proves the first claim. No elliptic curve over $\mathbb{F}_{2^e}$ with $e\le 9$ has a point of order 77. For $e\le 5$ this follows from the Hasse bound, and for $6\le e\le 9$ the only multiples of 77 in the Hasse intervals are 77, 231 and 539, for $e=6,8,9$, with traces of Frobenius -12, 26 and -26, which are even and not traces of supersingular curves (see the discussion after Lemma 2.6). So the elliptic curve has bad reduction at all primes above 2, which is multiplicative by Lemma 2.4, and this proves the second claim. □

Lemma 7.15. *Let $H\subseteq\Delta(77)$ be the subgroup of order 5 generated by $\langle 36\rangle$, and $Y=X_1(77)/H$. Then $Y\to X_0(77)$ is an unramified cyclic cover of degree 6, also over $\mathbb{F}_2$, and Y has genus 37. The closed cusps of $X_1(77)_{\mathbb{F}_2}$ have degrees $1^{30},3^{10},10^3,30$. Those of degree 1 are the reductions of the 30 rational cusps, whose images are the 6 rational cusps of Y above the cusp of width 77, and those of degree 3 map to the 2 closed cusps of degree 3 of $Y_{\mathbb{F}_2}$ above the cusp of width 11.*

Proof. By the proof of Lemma 7.10, $\Delta(77)$ acts freely on $X_1(77)$, also in characteristic 2. So $Y\to X_0(77)$ is unramified, also over $\mathbb{F}_2$, and Y has genus $1+(181-1)/5=37$. The last assertions follow from the description of the cusps, as we check. □

We construct $Y_{\mathbb{F}_2}$ as follows. The curve $X_0(77)_{\mathbb{F}_2}$ is obtained by adjoining to the function field of $X_0(11)_{\mathbb{F}_2}$ a root v of $v^8 + jv^7 + v^4 + 1 = 0$, which gives $X_0(7) \times_{X(1)} X_0(11)$, and we check that its normalization has genus 7 and four rational cusps of widths $1, 7, 11, 77$. The cover $Y \to X_0(77)$ is the composite of a cyclic cubic and a quadratic cover. The cubic one is $X_1(7) \times_{X(1)} X_0(11)$, which we construct using the Tate normal form of $X_1(7)$, with parameter t, and whose automorphisms over $X_0(7)$ are generated by $t \mapsto 1/(t+1)$. For the quadratic one we compute $\mathrm{Pic}(X_0(77)_{\mathbb{F}_2}) \simeq \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}$, and there are six homomorphisms to $\mathbb{Z}/6\mathbb{Z}$ with the Frobenius values $\langle 2\rangle^0, \langle 2\rangle^2, \langle 2\rangle^3, \langle 2\rangle^5$ at the cusps of widths $77, 11, 7, 1$. Exactly one of them is compatible with the splitting in Y of the images on $X_0(77)$ of the points of order 77 over $\mathbb{F}_{1024}$, and we construct its quadratic part by an Artin-Schreier equation, which we check against the Frobenius elements at a set of generators of $\mathrm{Pic}(X_0(77)_{\mathbb{F}_2})/2$. The composite has genus 37 and a split rational cusp, and by class field theory it is $Y_{\mathbb{F}_2}$.

Proposition 7.16. *The group $\mathbb{Z}/77\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 8 or 9.*

Proof. Let $d \in \{8, 9\}$, let D be the trace divisor of a point of order 77 over a number field of degree d, and let Y be as in Lemma 7.15. By Lemma 7.14 the reduction of D modulo 2 is entirely cuspidal, so it is supported on the closed cusps of degree 1 and 3, and by Lemma 7.15 the reduction of the push-forward of D to Y is supported on the 6 rational cusps of width 77 and the 2 closed cusps of degree 3 of $Y_{\mathbb{F}_2}$. The group $T_2 J_Y(\mathbb{Q})$ is finite by Lemma 7.14, as J_Y is a quotient of $J_1(77)$. We apply Proposition 7.3 with $r = 1$ and $\psi_1 = T_2$, for which

$$U = (\mathcal{C} - 1)T_2^* H^0(Y_{\mathbb{F}_2}, \Omega^1) = \langle 2\rangle^* \mathcal{C}(\mathcal{C} - 1)H^0(Y_{\mathbb{F}_2}, \Omega^1)$$

by (7). We compute that $\mathcal{C}(\mathcal{C}-1)H^0(Y_{\mathbb{F}_2}, \Omega^1)$ has dimension 32, and we compute the spaces $\Omega(jP)$ for $j \leq 8$ at one rational cusp P, which we transport to the other five with the automorphisms of Y over $X_0(77)$, as these commute with $\mathcal{C}$. We compute the spaces for $j = 9$ at a rational cusp and for $j \leq 3$ at a cusp of degree 3, which we transport in the same way, and we check that the restriction of U to each of the

$$\binom{14}{5} + 2\binom{11}{5} + 3\binom{8}{3} + 4 = 3098$$

effective divisors of degree 9 supported on these 8 cusps is surjective. By Remark 7.4 the same holds in degree 8, and Proposition 7.3 gives a contradiction. □

8. Riemann-Roch computations in the canonical ring

In this section we treat levels n at which the Hecke sieve has to be applied over nonic fields on curves of large genus. For most of them $J_1(n)$ has positive rank. The groups $\mathbb{Z}/57\mathbb{Z}$ and $\mathbb{Z}/65\mathbb{Z}$ over fields of degree 6, 7 and 8 are treated in Section 9. On such curves our main tool for showing that a divisor class over a finite field is not principal is the following criterion, which replaces Riemann-Roch computations by linear algebra in the canonical ring.

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.

Proof. Let $f \in L(T-U)$. As F and H vanish on T, we have $G := fF \in H^0(X, \mathcal{L}(-U))$ and $fH \in H^0(X, \mathcal{M})$. Hence $GH = F \cdot fH$, so G lies in the kernel of the map, and $G = 0$. As $F \neq 0$ we get $f = 0$. □

We apply the lemma with $\mathcal{L} = iK_X$ and $\mathcal{M} = jK_X$, so that the second component is the multiplication $R_i \times R_j \to R_{i+j}$. For the curves of this section we compute an integral basis of $S_2(\Gamma_1(n))$, or of the cusp forms on the quotient that we use, including the old forms, and its q-expansions beyond the Sturm bound. This gives the canonical model and the products in R_2 (or R_3, R_4), as products of q-expansions are determined by their coefficients up to the Sturm bound, and we check by comparing dimensions that the products of the q-expansions of the basis of $R_1 = H^0(X, \Omega^1)$ span the spaces R_i that we use. To evaluate sections at the support of U we need local parameters there. At non-cuspidal points we obtain them from the deformation $a_6 \mapsto a_6 + t$ of an ordinary curve $y^2 + xy = x^3 + a_2x^2 + a_6$, or $a_1 \mapsto t$ of a supersingular curve $y^2 + a_3y = x^3 + a_4x + a_6$ (these are the normal forms of ordinary and supersingular elliptic curves over a field of characteristic 2), by lifting the point of order n by Hensel's lemma, and then compute the canonical coordinates from the standard modular units of [DvH14, Sections 2 and 2.1], whose linear relations with the canonical forms we verify to an order beyond the degree bound. For $n = 87$ we obtain the local parameters from the canonical quadrics instead. When $\alpha = \langle a \rangle - 1$ has finite image on $J_1(n)(\mathbb{Q})$, the class $[\langle a \rangle D - D]$ is torsion, and for a non-cuspidal closed point P the divisor $A_q(\langle a \rangle P - P)$ has positive and negative parts of the same degree. The divisors T_qP are computed from the $q+1$ isogenies of degree q of an elliptic curve representing P. As the identification of the diamond operators on the canonical model with those on the moduli problem is a matter of convention (see Section 2.3), we test both forms of the annihilator and all the simultaneous diamond translates of the target points, which covers all conventions, unless the divisors are computed directly on the moduli model, as in Step 3 of Proposition 8.3, or the two forms coincide, as for $n = 87$.

Proposition 8.2. *The group $\mathbb{Z}/87\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a nonic field.*

Proof. The group $J_1(87)(\mathbb{Q})$ is finite [DEvH+21, Theorem 3.1(2)], and $i(87) = 3360$, so $\operatorname{gon}_{\mathbb{C}} X_1(87) \geq \frac{325}{2^{15}} \cdot 3360 > 33 > 18$, and Proposition 2.5(b) excludes the entirely cuspidal reduction modulo 2. We compute that no elliptic curve over $\mathbb{F}_{2^e}$ with $e \leq 8$ has a point of order 87, and that over $\mathbb{F}_{2^9}$ exactly 36 curves do, all ordinary with 522 points and cyclic 87-torsion, with j-invariants in 4 Frobenius orbits of length 9. So D reduces to a single closed point of degree 9.

Let H be the subgroup of $\Delta(87)$ generated by $\langle 16 \rangle$, which has order 7, and let $Y = X_1(87)/H$, of genus 33. As $16^2 \equiv -5 \pmod{87}$, the operator $\langle 5 \rangle$ acts trivially on Y, so $A_5 = T_5 - 6$ kills $J_Y(\mathbb{Q})$, and $A_5c_0 = 6c_0 - 6c_0 = 0$. The map $X_1(87) \to Y$ is Galois of degree 7, so the image P of the reduction of D is a closed point of degree 9 of $Y_{\mathbb{F}_2}$, one of 16, and $Q - 6P$ is principal, where $Q = T_5P$. For each of the 4 elliptic curves above, the 6 isogenies of degree 5 have distinct target j-invariants which form one Frobenius orbit of length 54, so Q is a single closed point of degree 54. We compute a canonical model of $Y_{\mathbb{F}_2}$, of degree 64 in $\mathbb{P}^{32}$, and the complete fibres of the j-map above the 4 target j-invariants, which contain 16 closed points of degree 54 each. We check with Lemma 8.1, with $\mathcal{L} = \mathcal{M} = 2K$, that $\ell(Q - 6P) = 0$ for one P in each diamond orbit and all 16 points Q in the corresponding fibre, i.e. in 64 cases. □

Proposition 8.3. *The group $\mathbb{Z}/57\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a nonic field.*

Proof. By Lemma 9.1 and its proof, every diamond difference has finite image on $J_1(57)(\mathbb{Q})$, and so do the operators $T_\ell - a_\ell$ for $\ell \in \{2,5,7,11,13\}$, where $a_2, a_5, a_7, a_{11}, a_{13} = -2, -3, -5, 1, 2$ are the coefficients of 57.2.a.a, as they act as 0 on the corresponding factor. By the Hasse bound $X_1(57)_{\mathbb{F}_2}$ has no non-cuspidal points of degree at most 5.

Step 1: a quotient of genus 9. Let $Y_{57} = X_1(57)/H$ be the curve of genus 9 of Lemma 9.4, where H, the subgroup of $\Delta(57)$ of odd order, is generated by $\langle 4\rangle$ and has order 9, and let $\sigma = \langle 5\rangle$, which generates $\Delta(57)/H$. The Jacobian $J_{Y_{57}}$ is isogenous to the product of $J_0(57)$ and an abelian fourfold A with $L(A,1) \neq 0$, on which σ acts as -1, so $\alpha J_{Y_{57}}(\mathbb{Q})$ is finite for $\alpha = \sigma - 1$. We compute that $J_{Y_{57}}(\mathbb{F}_2) \simeq \mathbb{Z}/105\mathbb{Z} \times \mathbb{Z}/210\mathbb{Z}$ and that the α-images of the classes of the cuspidal divisors generate a subgroup $V \simeq (\mathbb{Z}/7\mathbb{Z})^2$, which is the whole α-image as $\#A(\mathbb{F}_2) = 49$. On V the annihilator A_5, computed from the action of T_5 on the cusps, has kernel $V_0 \simeq \mathbb{Z}/7\mathbb{Z}$, so the reduction of $\alpha J_{Y_{57}}(\mathbb{Q})$ lies in V_0. The closed cusps of $X_1(57)$ of degree at most 3 are reductions of rational cuspidal divisors, so if D reduces to $P + C'$ with P non-cuspidal, of degree $e \geq 6$, then the class of the image of P in $J_{Y_{57}}(\mathbb{F}_2)$, normalized at a rational cusp, satisfies $\alpha[\pi_* P - e\,\overline{c_0}] \in V_0$. We enumerate the closed points of $(Y_{57})_{\mathbb{F}_2}$ of degree at most 9 above the j-invariants of the elliptic curves over $\mathbb{F}_{2^e}$ with a point of order 57, and this condition leaves only 3 possibilities for $\pi_* P$: $3P_2$ with P_2 of degree 2 above $j = 0$, and 2 points of degree 8. Similarly, the only closed cusps of $X_1(57)_{\mathbb{F}_2}$ of degree at most 9 which are not reductions of rational cuspidal divisors of the same degree are 2 cusps of degree 9 splitting an orbit of degree 18, and for both the condition fails. So either the reduction of D is $P + C'$ with P of degree 6 or 8 above one of the 3 points above and C' the reduction of a rational cuspidal divisor C, or it is the reduction of a rational cuspidal divisor C.

Step 2: the cuspidal case. For $r \in \{2,5,7,11,13\}$ and $\ell \in \{5,7,11,13\}$ put $\Phi_{r,\ell} = (T_r - a_r)(T_\ell - \langle \ell\rangle - \ell)$ on the q-expansion model. Each of them kills $J_1(57)(\mathbb{Q})$, so $\Phi_{r,\ell}[D - C] = 0$, and we use the map $X_1(57)^{(9)} \to J_1(57)^{20}$ given by all of them, whose cotangent space modulo 2 we compute from the integral canonical lattice. The pull-backs of the differentials span a space of dimension 82. The cuspidal divisors of degree 9 in question are supported on the 18 rational cusps and the 9 closed cusps of degree 2, and we check that the map is a formal immersion at all of them, which after moving a rational cusp of maximal multiplicity to c_0 by a diamond operator gives 796111 configurations, using local parameters at the cusps of degree 2 obtained from the Tate curve $E(q^{19})$ with the point $\zeta_3 q$. As D and C have the same reduction and the same image, $D = C$ by [DKSS23, Lemma 4.2], which is a contradiction.

Step 3: the non-cuspidal case. The elliptic curves over $\mathbb{F}_{2^6}$ with a point of order 57 are 2 supersingular curves with 57 points, and those over $\mathbb{F}_{2^8}$ are ordinary with 228 points, with j-invariants in one Frobenius orbit. Put $\sigma = \langle 5\rangle$ and $A_5 = T_5 - 1 - 5\sigma$ on the moduli model. As $[\sigma D - D]$ and $[\sigma C - C]$ are torsion and killed by A_5, the divisor

$$B = A_5(\sigma P - P) = \sigma T - T + P + 4\sigma P - 5\sigma^2 P, \qquad T = T_5 P,$$

is principal. We compute T from the isogenies of degree 5: it consists of closed points of degrees 18 and 9, with multiplicities 1 and 2, for the 2 points of degree 6, and of 2 closed points of degree 24 for the point of degree 8. We check with Lemma 8.1, with $\mathcal{L} = \mathcal{M} = 2K$ on $X_1(57)$, of genus 85, that $\ell(B) = 0$ in these 3 cases, and the other convention as well. □

Proposition 8.4. *The group $\mathbb{Z}/65\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a nonic field.*

Proof. By Lemma 9.1 and its proof, every diamond difference has finite image on $J_1(65)(\mathbb{Q})$, and so do the operators $T_\ell - a_\ell$ for $\ell \in \{2,3,7,11,17\}$, where $a_2, a_3, a_7, a_{11}, a_{17} = -1, -2, -4, 2, 2$ are the coefficients of 65.2.a.a, as they act as 0 on the corresponding factor. By the Hasse bound $X_1(65)_{\mathbb{F}_2}$ has no non-cuspidal points of degree at most 5. The elliptic curves over $\mathbb{F}_{2^6}$ with a point of order 65 are supersingular with 65 points, and those over $\mathbb{F}_{2^7}$, $\mathbb{F}_{2^8}$, $\mathbb{F}_{2^9}$ are ordinary, with 130, 260 and 520 points, and give 48, 48 and 72 closed points of degree 7, 8 and 9 of $X_1(65)_{\mathbb{F}_2}$, in 2, 2 and 3 diamond orbits. The degrees of the Galois orbits of cusps and of the closed cusps of $X_1(65)_{\mathbb{F}_2}$ are given in Section 9.1.

Non-cuspidal reduction. Suppose that D reduces to $P + C'$ with P a non-cuspidal closed point. Then C' has degree at most 3, so it is the reduction of a rational cuspidal divisor. Put $\sigma = \langle 3\rangle^{-1}$, $\tau = \langle 3\rangle$ and $A_3 = T_3 - 1 - 3\tau$. As in Proposition 8.3, with $T = T_3 P$ the divisor $A_3(\sigma P - P) = \sigma T - T - \sigma P - 2P + 3\tau P$ is principal. We compute $X_1(65)$, of genus 121, through its canonical forms and the units $x = f_7/f_8$, $y = f_8/f_9$ of [DvH14, Sections 2 and 2.1], and we check with Lemma 8.1, with $\mathcal{L} = \mathcal{M} = K$, that this divisor and its analogue for the other convention are not principal, for every diamond translate of T: these are 336 tests for the points of degree 7, 8, 9. For the supersingular point of degree 6, T consists of 2 closed points of degree 12 and is computed on the moduli model, and we check that $A_3(\tau P - P)$, which equals $-\tau A_3(\sigma P - P)$ as $\tau = \sigma^{-1}$, and its analogue for the other form of the annihilator are not principal.

Cuspidal reduction at a non-rational cusp. The 4 closed cusps of degree 6 split an orbit of degree 24. Suppose that D reduces to such a cusp c plus the reduction of a rational cuspidal divisor C of degree 3. Let $\pi : X_1(65) \to Y$ be the quotient by the kernel of the character $u \mapsto \left(\frac{65}{u}\right)$ of $\Delta(65)$, a curve of genus 9. By Lemma 2.1, Y has good reduction at 2 and π extends to the smooth models. We compute $J_Y(\mathbb{F}_2) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/336\mathbb{Z}$, and that the images under $\alpha = \langle 3\rangle - 1$ of the classes of the cuspidal divisors generate a subgroup $V \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, on which $T_3 - \langle 3\rangle - 3$, the annihilator of the q-expansion model, has kernel isomorphic to $\mathbb{Z}/8\mathbb{Z}$. Each cusp c maps to a rational cusp c_Y of Y of width 65 with multiplicity 6, and we check that $6\alpha[c_Y - \overline{c_0}] \notin \ker\big((T_3 - \langle 3\rangle - 3)|_V\big)$. But this class is the reduction of $\alpha[\pi_* D - 9c_0] - \alpha[\pi_* C - 3c_0]$, and both terms lie in the finite group $\alpha J_Y(\mathbb{Q})$ by Lemma 9.1, so they are killed by $T_3 - \langle 3\rangle - 3$, which is a contradiction.

Other cuspidal reductions. They are reductions of rational cuspidal divisors C supported on the 24 rational cusps and the 6 cusps of degree 4. As in Proposition 8.3, we use $\Phi_{r,\ell} = (T_r - a_r)(T_\ell - \langle \ell\rangle - \ell)$ for $r \in \{2,3,7,11,17\}$ and $\ell \in \{3,7,11,17\}$, whose pull-backs span a space of dimension 106 modulo 2, and we check that the corresponding map is a formal immersion at all such divisors, which gives 2250325 configurations after moving a rational cusp of maximal multiplicity to c_0. As D and C have the same reduction and the same image, $D = C$ by [DKSS23, Lemma 4.2], which is a contradiction. □

Proposition 8.5. *The groups $\mathbb{Z}/85\mathbb{Z}$, $\mathbb{Z}/91\mathbb{Z}$ and $\mathbb{Z}/93\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over a nonic field.*

Proof. Let $n \in \{85, 91, 93\}$. By Remark 3.2, the trace divisor D is a closed point of degree 9. Put $h = \langle 16\rangle$, $\langle 27\rangle$ and $\langle 4\rangle$ respectively, of order 2, 2 and 5 in $\Delta(n)$. We compute that the characters of the factors outside the winding quotient are trivial on $\langle 2\rangle$ and $\langle 16\rangle$ for $n = 85$ (2 factors of dimension 2), on $\langle 3\rangle$ and hence on $\langle 27\rangle$ for $n = 91$, and that for $n = 93$ there is

a single such factor, of dimension 2 and trivial character. So $(h-1)J_1(n)(\mathbb{Q})$ is finite, and so are $(\langle 2\rangle - 1)J_1(85)(\mathbb{Q})$ and $(\langle 3\rangle - 1)J_1(91)(\mathbb{Q})$.

Cuspidal reduction at 2. We have $i(n) = 3456$, 4032, 3840, and $\operatorname{gon}_{\mathbb{C}} X_1(n) \geq \frac{325}{2^{15}} i(n) > 34, > 39, > 38$. Suppose that D reduces to a cuspidal divisor, and let C be a lift over an unramified extension of $\mathbb{Q}_2$. For $n = 91$ and $n = 93$, Lemma 2.9(c) gives $hD = D$, as $2(9+9) = 36$, which contradicts Lemma 2.12, as h has order 2, respectively 5. For $n = 85$ the closed cusps of $X_1(85)_{\mathbb{F}_2}$ have degrees $1^{32}, 4^8, 8^8$, and h acts freely on the rational cusps and fixes every non-rational closed cusp. If the reduction contains a non-rational cusp, write it as $Z + \overline{R}$ with Z supported on the non-rational cusps and R a rational cuspidal divisor of odd degree $r \in \{1, 5\}$. Then Lemma 2.9(c), with $C = R$ and $2(9+r) \leq 28$, gives $hR = R$, which is impossible as h acts freely on the rational cusps and r is odd.

If the reduction is supported on the rational cusps, it is the reduction of a rational cuspidal divisor C. We use the polynomial $k(X) = (X^2 + 4X + 2)(X^2 + 2X + 2)$, the product of the characteristic polynomials of T_3 on the 2 factors outside the winding quotient, so that $k(T_3)J_1(85)(\mathbb{Q})$ is finite, and the operator $t = (T_3 - \langle 3\rangle - 3)k(T_3)$ on the q-expansion model, which kills $J_1(85)(\mathbb{Q})$. So $t[D - 9c_0] = t[C - 9c_0]$, and by [DKSS23, Lemma 4.2] it suffices to show that the map $X_1(85)^{(9)} \to J_1(85)$, $x \mapsto t[x - 9c_0]$, is a formal immersion modulo 2 at every rational cuspidal divisor of degree 9. By the criterion of [DEvH+21, Lemma 5.9 and Proposition 5.10], applied as in [DKSS23, Corollary 4.4 and Proposition 5.3], whose proof works for any level, this holds at $\sum_c m_c c$ if the rows $t\langle g_c\rangle T_j$ with $1 \leq j \leq m_c$ are linearly independent modulo 2, where $\langle g_c\rangle$ is the diamond operator which maps c_0 to c. At most one cusp has $m_c \geq 5$, and we may move it to c_0 by a diamond operator. We compute the 133×225 matrix of the rows tT_j, $j \leq 9$, at c_0 and $t\langle g_c\rangle T_j$, $j \leq 4$, at the other 31 rational cusps c, and we check that its rank is 122 and that for every linear relation between its rows, the sum over the cusps c of the largest j for which a row at c occurs in the relation is at least 32. As $\sum_c m_c = 9 < 32$, no relation involves only rows with $j \leq m_c$, so the criterion holds, and $D = C$, which is a contradiction.

Non-cuspidal reduction. By the Hasse bound and an enumeration of the elliptic curves over $\mathbb{F}_{2^e}$, $e \leq 9$, the non-cuspidal closed points of $X_1(n)_{\mathbb{F}_2}$ of degree at most 9 are as follows. For $n = 85$, there are 160 points of degree 9 from curves with 510 points, in 5 diamond orbits. For $n = 91$ there are 3 points of degree 8, with $j = 0$, from 2 twists with 273 points, all fixed by h, and 144 points of degree 9 from curves with 546 points, in 4 orbits. For $n = 93$ there are 10 points of degree 9 from curves with 558 points, in one orbit. For $n = 91$, if D reduces to $P_8 + c$ with P_8 of degree 8 and c a rational cusp, Lemma 2.9(c) gives $hc = c$, which is impossible as h acts freely on the rational cusps. In the remaining cases D reduces to a single point P of degree 9, and with $\sigma = \langle 2\rangle^{-1}$, $\langle 3\rangle^{-1}$, $\langle 2\rangle^{-1}$ respectively, the divisor $A_q(\sigma P - P)$, with $q = 3, 3, 5$, is principal. We check with Lemma 8.1, with $\mathcal{L} = \mathcal{M} = K$, on $X_1(n)$ of genus 225, 265 and 261, that these divisors are not principal, in 320, 288 and 120 tests respectively, which include both conventions and all the simultaneous diamond translates of the targets. □

9. The groups $\mathbb{Z}/57\mathbb{Z}$, $\mathbb{Z}/65\mathbb{Z}$ and $\mathbb{Z}/69\mathbb{Z}$

The groups $\mathbb{Z}/57\mathbb{Z}$ and $\mathbb{Z}/65\mathbb{Z}$ over fields of degree 6, 7 and 8 require several arguments each. For both levels the Jacobian $J_1(n)$ has positive rank, and over finite fields of characteristic 2 there are elliptic curves with a point of order n. We first restrict the possible reductions of the trace divisor modulo 2 (Section 9.1). The remaining reductions are excluded on $X_1(n)$ and on its quotients by subgroups of $\Delta(n)$, using elements of the Hecke

algebra whose image on the Mordell-Weil group is finite, and for $n = 57$ some of these quotients are unramified covers of $X_0(57)$ which we construct over $\mathbb{F}_2$ by class field theory (Section 9.2). Most entirely cuspidal reductions are excluded with the Cartier operator (Proposition 7.3). The level 69 uses the same kind of double cover as 57, so we treat it here as well, in degrees 7, 8 and 9 (Section 9.5). The group $\mathbb{Z}/63\mathbb{Z}$ is treated in Proposition 7.12, and the groups $\mathbb{Z}/57\mathbb{Z}$ and $\mathbb{Z}/65\mathbb{Z}$ over nonic fields in Section 8.

9.1. **Reduction modulo 2.** We first collect the facts about the Mordell-Weil groups that we use.

Lemma 9.1. *Let $n \in \{57, 65\}$. The only newform f of level dividing n with $L(f,1) = 0$ is 57.2.a.a for $n = 57$ and 65.2.a.a for $n = 65$. It has trivial character, and its Fourier coefficients satisfy $a_2 = -2$ and $a_3 = -1$ for $n = 57$, and $a_2 = -1$ for $n = 65$. Hence $(\langle a\rangle - 1)J_1(n)(\mathbb{Q})$ is finite for every a, and so are $(T_2 + 2)J_1(57)(\mathbb{Q})$, $(U_3 + 1)J_1(57)(\mathbb{Q})$, $(T_2 + 1)J_1(65)(\mathbb{Q})$ and $(T_2^6 - 1)J_1(65)(\mathbb{Q})$. The same holds on all the quotients of $X_1(n)$ by subgroups of $\Delta(n)$.*

Proof. By the LMFDB, these are the only newforms of level dividing n with positive analytic rank. We verify this by computing the winding submodules of all the even characters modulo n, whose dimensions add up to the genus of $X_1(n)$: every non-trivial character has full winding submodule, and the winding submodule of the trivial character has codimension 1, with $T_2 = -2$ and $U_3 = -1$ on the quotient for $n = 57$, and $T_2 = -1$ for $n = 65$ (see also `C57/winding57_hecke3_certificate.m` and `C65/winding65_hecke2_certificate.m`). By Kato's theorem, all the factors of $J_1(n)$ except the one corresponding to f have finitely many rational points, and the operators above act as 0 on this factor. The Jacobians of the quotients of $X_1(n)$ by subgroups of $\Delta(n)$ are quotients of $J_1(n)$. □

Over sextic fields we first show that for $n = 57$ the reduction to a supersingular curve over $\mathbb{F}_{64}$ cannot occur.

Proposition 9.2. *Let E be an elliptic curve over a sextic field K with a point of order 57. Then E has bad reduction at every prime of K above 2.*

Proof. There are no points of order 57 over number fields of degree at most 3 [DEvH+21], so the point $x \in Y_1(57)(K)$ has degree 6 and its trace divisor D is a closed point of degree 6. Suppose that E has good reduction at a prime $\wp$ of K above 2. By the Hasse bound $\mathbb{F}_\wp = \mathbb{F}_{64}$, so $\wp$ is the only prime of K above 2, and it is unramified. The reduction $\widetilde{E}$ has a point of order 57 over $\mathbb{F}_{64}$, so $\#\widetilde{E}(\mathbb{F}_{64}) = 57$, and the trace of Frobenius is 8. Thus $\widetilde{E}$ is supersingular and $j(\widetilde{E}) = 0$. As $\widetilde{E}$ is supersingular, [2] is purely inseparable [Sil09, Theorem V.3.1], so [8] and the Frobenius endomorphism π of $\widetilde{E}$ are purely inseparable isogenies of degree 64. By [Sil09, Corollary II.2.12] both are the 64-th power Frobenius morphism followed by an isomorphism, so $\pi = \zeta \circ [8]$ for an automorphism ζ of $\widetilde{E}$. As π acts trivially on $\widetilde{E}(\mathbb{F}_{64})$, which has odd order 57, the automorphism ζ acts on it as multiplication by 8^{-1}. In particular ζ maps $8\widetilde{P}$ to $\widetilde{P}$, where $\widetilde{P}$ is the reduction of the point of order 57, so $(\widetilde{E}, 8\widetilde{P}) \simeq (\widetilde{E}, \widetilde{P})$ and $\langle 8\rangle$ fixes the reduction of x. As $\langle 8\rangle$ is defined over $\mathbb{Q}$, it also fixes the conjugates of this point, so the reduction of D is fixed by $\langle 8\rangle$.

By Lemma 9.1 the group $(\langle 8\rangle - 1)J_1(57)(\mathbb{Q})$ is finite, and Abramovich's bound gives $\mathrm{gon}_{\mathbb{C}} X_1(57) > 14.28 > 2 \cdot 6$. So Lemma 2.9(c), applied with $g = \langle 8\rangle$ and $C = 0$, gives $\langle 8\rangle D = D$. The least degree of a CM point on $X_1(57)$ is 12, so the support of D is non-CM and, by Lemma 2.8, $\langle 8\rangle$ acts freely on its geometric points.

The operator $\langle 8\rangle$ has order 3 in $\Delta(57)$, so the image of x on $X_1(57)/\langle 8\rangle$ has degree 2, and the image of x on $X_0(57)$ has degree 1 or 2. The curve $X_0(57)$ has no rational non-cuspidal points, and its quadratic points were determined by Box [Box21, §4.4]. The non-CM ones are defined over $\mathbb{Q}(\sqrt{-23})$ or $\mathbb{Q}(\sqrt{13})$, and the corresponding quadratic field is contained in K. The prime 2 splits in $\mathbb{Q}(\sqrt{-23})$, which contradicts the uniqueness of the prime of K above 2. The two j-invariants over $\mathbb{Q}(\sqrt{13})$ are

$$\frac{3387888351672962316333\sqrt{13} - 12215205167504087643323}{2} \quad \text{and} \quad \frac{-17787\sqrt{13} - 61763}{2},$$

and writing them in the basis $1, t$ of the ring of integers, with $t = (1+\sqrt{13})/2$, they are congruent to t modulo the prime above 2, which is inert. As $t^2 + t + 1 \equiv 0$ modulo this prime, these j-invariants are non-zero modulo 2, contradicting $j(\widetilde{E}) = 0$. □

Lemma 9.3. *The diamond operator $\langle 2\rangle$ acts trivially on $J_1(57)(\mathbb{Q})[2]$.*

Proof. Let $J = J_1(57)$. By Proposition 2.2(2), $J(\mathbb{Q})[2]$ is contained in the kernel of A_5 on $J[2]$. We compute the action of the Hecke operators on $H_1(J(\mathbb{C}),\mathbb{Z})/2H_1(J(\mathbb{C}),\mathbb{Z}) \simeq J[2]$, a space of dimension 170 over $\mathbb{F}_2$, and find that the kernel of A_5 has dimension 2 and that $\langle 2\rangle - 1$ vanishes on it. Here we obtain the diamond operators over $\mathbb{Z}$ from the relation $q\langle q\rangle = T_q^2 - T_{q^2}$, with $q = 2$ and $q = 5$. □

We compute that the numbers of non-cuspidal closed points of $X_1(n)_{\mathbb{F}_2}$ of degrees $1, \dots, 8$ are $0, 0, 0, 0, 0, 2, 36, 18$ for $n = 57$ and $0, 0, 0, 0, 0, 2, 48, 48$ for $n = 65$. The Galois orbits of cusps of $X_1(57)$ and $X_1(65)$ have degrees $1^{18}, 2^9, 18^2$ and $1^{24}, 4^6, 12^2, 24$, and the closed cusps of $X_1(57)_{\mathbb{F}_2}$ and $X_1(65)_{\mathbb{F}_2}$ have degrees $1^{18}, 2^9, 9^2, 18$ and $1^{24}, 4^6, 6^4, 12^2$, so the closed cusps of degree at most 2 are reductions of Galois orbits of cusps of the same degree. So over a number field of degree $d \leq 8$ the reduction of the trace divisor modulo 2 is entirely cuspidal, or it is $G + \overline{C}$, where G is a single non-cuspidal closed point of degree $e \in \{6, 7, 8\}$ and $\overline{C}$ is the reduction of an effective rational cuspidal divisor C of degree $d - e$.

9.2. **Unramified covers of $X_0(57)$ and $X_0(69)$.** For $n = 57$ and $n = 69$ we use the following quotient of $X_1(n)$.

Lemma 9.4. *Let $n = 3\ell$ with $\ell \in \{19, 23\}$, let H be the subgroup of odd order of $\Delta(n)$, which has index 2, and put $Y_n = X_1(n)/H$ and $Z_n = X_0(n)$. The natural map $Y_n \to Z_n$ is an unramified double cover, also over $\mathbb{F}_2$. The curves Z_n and Y_n have genus 5 and 9 for $n = 57$, and 7 and 13 for $n = 69$.*

Proof. As H has odd order, Y_n has good reduction at 2. The elements $\langle a\rangle$ of $\Delta(n)$ outside H have even order, so they are not solutions of $a^2 \pm a + 1 \equiv 0 \pmod{n}$, whose order in $\Delta(n)$ divides 3, and $a^2 \equiv -1$ is impossible modulo 3. As n is squarefree, Lemma 7.2 shows that they fix no geometric point of $X_1(n)$, in characteristic 0 or 2, so the non-trivial element of $\Delta(n)/H$ fixes no geometric point of Y_n. Hence $Y_n \to Z_n$ is unramified, and the genera follow from $g(X_0(57)) = 5$, $g(X_0(69)) = 7$ and the Riemann-Hurwitz formula. □

As in Section 7.4, a geometrically connected unramified double cover of $Z_{n,\mathbb{F}_2}$ is given by a character of $\mathrm{Pic}(Z_{n,\mathbb{F}_2})$ that does not factor through the degree, whose values are the Frobenius elements in $\Delta(n)/H \simeq \mathbb{F}_2$, and it is determined by these at enough closed points. The four cusps of $Z_{n,\mathbb{F}_2}$ are rational and are distinguished by their widths $1, 3, \ell, n$. From the description of the cusps of $X_1(n)$ and the action of 2 on their cyclotomic coordinates,

their Frobenius elements in $\Delta(n)/H$ are $(0,1,1,0)$ for $n=57$ and $(1,0,1,0)$ for $n=69$, in the order of the widths.

We obtain a model of $Z_{n,\mathbb{F}_2}$ by adjoining to the function field of $X_0(\ell)_{\mathbb{F}_2}$ a root t of $t^4+t^3+1/j=0$, which gives the function field of $X_0(3)$ over the j-line, and we compute, for $n=57$ and $n=69$,

$$\mathrm{Pic}(Z_{57,\mathbb{F}_2}) \simeq \mathbb{Z}/15\mathbb{Z}\times\mathbb{Z}/30\mathbb{Z}\times\mathbb{Z}, \qquad \mathrm{Pic}(Z_{69,\mathbb{F}_2}) \simeq \mathbb{Z}/22\mathbb{Z}\times\mathbb{Z}/44\mathbb{Z}\times\mathbb{Z}.$$

For $n=57$ the values at the cusps determine a unique character. For $n=69$ two characters have these values, and we use the condition that the images on Z_{69} of the points of order 69 over $\mathbb{F}_{128}$ (which come from points of Y_{69}) must split in Y_{69}. This determines the character uniquely, and we construct $Y_{n,\mathbb{F}_2}$ as the corresponding class field, which has the required genus, a rational split cusp of width n, and the required Frobenius element at every generator of $\mathrm{Pic}(Z_{n,\mathbb{F}_2})$.

To exclude the entirely cuspidal reduction for $\mathbb{Z}/57\mathbb{Z}$ over octic fields we use the quotient $W_{57}=X_1(57)/\langle 7\rangle$, where $\langle 7\rangle$ has order 3. It has good reduction at 2. By Lemma 7.2, as 57 is squarefree and $a^2\equiv -1$ is impossible modulo 3, the only non-trivial elements of $\Delta(57)$ which can fix a geometric point of $X_1(57)$, in characteristic 0 or 2, are $\langle 7\rangle$ and $\langle 49\rangle=\langle 7\rangle^2$, the solutions of $a^2\pm a+1\equiv 0 \pmod{57}$. So $W_{57}\to X_0(57)$ is an unramified cyclic cover of degree 6, also over $\mathbb{F}_2$, and W_{57} has genus $6\cdot 4+1=25$. We construct $W_{57,\mathbb{F}_2}$ as follows. The curve $X_0(19)_{\mathbb{F}_2}$ is an elliptic curve E_{19} with $\#E_{19}(\mathbb{F}_2)=3$. By class field theory, as $\mathrm{Pic}^0(E_{19})\simeq E_{19}(\mathbb{F}_2)\simeq\mathbb{Z}/3\mathbb{Z}$, there is a unique geometrically connected unramified cyclic cubic cover of E_{19} in which the cusp c_{19} of width 19 splits, namely $P\mapsto \mathrm{Frob}_2(P)-P+c_{19}$. The quotient of $X_1(19)_{\mathbb{F}_2}$ by the subgroup of order 3 of $\Delta(19)$ is such a cover, as this subgroup contains the stabilizers of the elliptic points of order 3, so it is this cover. Pulling back this cubic cover to $Z_{57,\mathbb{F}_2}$ gives a curve of genus 13, and its composite with the double cover $Y_{57,\mathbb{F}_2}$ above, which we construct again by an Artin-Schreier equation checked at a set of generators of $\mathrm{Pic}(Z_{57,\mathbb{F}_2})/2$, has genus 25 and a split rational cusp, so by class field theory it is $W_{57,\mathbb{F}_2}$. Its closed cusps have degrees $1^6,2^3,3^2,6$.

In the case $d=8$ of Proposition 9.6 we also use the operator U_3 on W_{57}. To compute U_3 on the differentials of $W_{57,\mathbb{F}_2}$ we use q-expansions. Let P be a closed cusp of degree 3 of $W_{57,\mathbb{F}_2}$ above the cusp of width 1 of $X_0(57)$, and let q be the corresponding parameter of the Tate curve. We identify the q-expansion of a differential $\omega=f(q)\,dq/q$ at a geometric point above P with the Fourier expansion of f at ∞.

Lemma 9.5. *In this identification, $U_3^*\bigl(\sum_n a_n q^n\,dq/q\bigr)=\sum_n a_{3n}q^n\,dq/q$. An $\mathbb{F}_2$-linear endomorphism of $H^0(W_{57,\mathbb{F}_2},\Omega^1)$ is determined by the first 17 coefficients of the q-expansions at P of the images of a basis.*

Proof. The first assertion is the action of U_3 on Fourier expansions at ∞. For the second, if a holomorphic differential defined over $\mathbb{F}_2$ vanishes to order at least 17 at a geometric point above P, it vanishes to order at least 17 at all three of them, and as $3\cdot 17>48=2g(W_{57})-2$ it is 0. □

In practice, at such a cusp we use the parameter $r=t_3+1$, where t_3 is the parameter of $X_0(3)$ with $j^{-1}=t_3^3(t_3+1)$, and then $j^{-1}=r(1+r)^3$. As $E_4\equiv 1 \pmod 2$, we have $j^{-1}\equiv\Delta=q\prod_{n\geq 1}(1-q^n)^{24} \pmod 2$, and r is obtained as a power series in q by reversion. We compute the matrix of U_3^* in this way, and we check that it has coefficients in $\mathbb{F}_2$ and commutes with $\mathcal{C}$. Depending on the normalization of the action of the Hecke algebra on differentials, the operator computed in this way is U_3 or its conjugate $w_{57}U_3w_{57}^{-1}$ by the

Atkin-Lehner involution w_{57}. This does not matter, as both are endomorphisms of $J_1(57)$ which act on the newform 57.2.a.a by $a_3 = -1$, so for both of them the image of $J(W_{57})(\mathbb{Q})$ under the operator plus 1 is finite by Lemma 9.1.

9.3. **The group $\mathbb{Z}/57\mathbb{Z}$.**

Proposition 9.6. *The group $\mathbb{Z}/57\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree $d \in \{6, 7, 8\}$.*

Proof. Let D be the trace divisor of a point of order 57 over a number field of degree d. Put $g = \langle 2 \rangle$, which has order 9 in $\Delta(57)$, and $h = g^3 = \langle 8 \rangle$. By Lemma 9.1 the groups $(g-1)J_1(57)(\mathbb{Q})$ and $(h-1)J_1(57)(\mathbb{Q})$ are finite, by Lemma 9.3 g and h act trivially on $J_1(57)(\mathbb{Q})[2]$, and the support of D is non-CM, as the least degree of a CM point on $X_1(57)$ is 12. By Section 9.1, the reduction of D modulo 2 is entirely cuspidal, or it is $G + \overline{C}$, where G is a non-cuspidal closed point of degree $e \in \{6, 7, 8\}$ and $\overline{C}$ is the reduction of an effective rational cuspidal divisor C of degree $d - e$. For $d = 6$ only the first case occurs, by Proposition 9.2 and Lemma 2.4.

Suppose first that $e = 6$. Then $d \in \{7, 8\}$, and, as in Proposition 9.2, every elliptic curve over $\mathbb{F}_{64}$ with a point of order 57 is supersingular with $j = 0$ (as we check), and h acts on its points of order 57 through an automorphism of the curve, so $hG = G$, and h fixes the reduction of $D - C$. As $d + (d-6) \leq 10 < 14.28 < \mathrm{gon}_{\mathbb{C}} X_1(57)$, Lemma 2.9(d) gives $hD = D$, so $3 \mid d$ by Lemma 2.8, which is a contradiction.

Suppose next that $e = 7$, and let s be the non-trivial automorphism of Y_{57} over Z_{57} (Lemma 9.4), which is the non-trivial element of $\Delta(57)/H$. As $\langle 5 \rangle \notin H$ we have $\langle 5 \rangle = s$ on Y_{57}, and $(s-1)J(Y_{57})(\mathbb{Q})$ is finite by Lemma 9.1. The operator $A_5 = T_5 - 1 - 5s$ annihilates this group by the Eichler-Shimura relation and the injectivity of reduction at 5, and it annihilates the images on Y_{57} of the rational cuspidal divisors of $X_1(57)$, such as C, as divisors (Lemma 2.3). So the image P of G on $Y_{57,\mathbb{F}_2}$ satisfies

$$[(s-1)(T_5P - P - 5sP)] = [sT_5P - T_5P + 4(sP - P)] = 0.$$

We compute that the elliptic curves over $\mathbb{F}_{128}$ with a point of order 57 form 14 isomorphism classes, with cyclic group of order 114, and give exactly two closed points of degree 7 on $Z_{57,\mathbb{F}_2}$, both of which split in Y_{57}. For each of them, the image under T_5 consists of three closed points of $Z_{57,\mathbb{F}_2}$ of degree 14 and multiplicity 1, and each of them splits in Y_{57}. So T_5P is one of $2^3 = 8$ divisors on Y_{57}, and replacing P by sP applies s to all of them. We compute that $\mathrm{Pic}(Y_{57,\mathbb{F}_2}) \simeq \mathbb{Z}/105\mathbb{Z} \times \mathbb{Z}/210\mathbb{Z} \times \mathbb{Z}$ and that for both points P and all 8 choices the class $[sT_5P - T_5P + 4(sP - P)]$ is non-zero, which is a contradiction.

Suppose next that $e = 8$. Then $d = 8$ and the reduction of D is a single closed point P of degree 8. Put $\delta = \langle 5 \rangle$, which generates $\Delta(57)$. As $(\delta - 1)J_1(57)(\mathbb{Q})$ is finite by Lemma 9.1, $A_5(\delta - 1)$ annihilates it, and $A_5 c_0 = 0$, so $[(\delta - 1)A_5 P] = 0$ in $J_1(57)(\mathbb{F}_2)$. The 18 points of degree 8 form a single diamond orbit, so we may take P to be a fixed one of them. We compute $(\delta - 1)A_5P$ on a model of $X_1(57)_{\mathbb{F}_2}$ of genus 85. Let F_{19} be the function field of $X_1(19)_{\mathbb{F}_2}$, write the universal elliptic curve over it as $y^2 + xy = x^3 + a_2x^2 + 1/j$, and put $w = y/x + x$ for a point (x, y) of order 3. Then $x^4 + x^3 + 1/j = 0$ and $w^2 + w = x + a_2$, so the function field of $X_1(57)_{\mathbb{F}_2}$ is

$$F_{19}(w), \qquad (w^2 + w + a_2)^4 + (w^2 + w + a_2)^3 + 1/j = 0,$$

where the involution $w \mapsto w + 1$ corresponds to negating the point of order 3. We compute that $T_5P = Q_1 + Q_2$ with Q_1, Q_2 closed points of degree 24, by computing the six 5-isogenies

of the corresponding elliptic curve and carrying both level structures through them, and that the divisor

$$(\delta-1)A_5P = \delta Q_1 + \delta Q_2 - Q_1 - Q_2 + 4\delta P + P - 5\delta^2 P$$

satisfies $\ell\big((\delta-1)A_5P\big) = 0$, so it is not principal, which is a contradiction.

Suppose finally that the reduction of D is entirely cuspidal. As the closed cusps of $X_1(57)_{\mathbb{F}_2}$ of degree at most 8 have degree 1 or 2 (Section 9.1), it is the reduction of a rational cuspidal divisor C. If $d \le 7$, then Lemma 2.9(d), applied with g and C, gives $gD = D$, as $2d \le 14 < 14.28 < \operatorname{gon}_{\mathbb{C}} X_1(57)$, which contradicts Lemma 2.8, as $9 \nmid d$. If $d = 8$, the reduction of the push-forward of D to W_{57} is supported on the 6 rational and the 3 quadratic cusps of $W_{57,\mathbb{F}_2}$, which gives $[x^8](1-x)^{-6}(1-x^2)^{-3} = 3654$ possible divisors. We apply Proposition 7.3 with $\psi_1 = T_2 + 2$ and $\psi_2 = U_3 + 1$ (Lemma 9.1), for which, by (7) and with U_3^* as in Lemma 9.5,

$$U = \mathcal{C}(\mathcal{C}-1)H^0(W_{57,\mathbb{F}_2}, \Omega^1) + (U_3^* + 1)(\mathcal{C}-1)H^0(W_{57,\mathbb{F}_2}, \Omega^1).$$

We compute that U has dimension 23 and that its restriction to each of the 3654 divisors has rank 8, which is a contradiction. □

9.4. **The group $\mathbb{Z}/65\mathbb{Z}$.** For $n = 65$ we use the quotients $Y'_{65} = X_1(65)/\langle 4, 51\rangle$ and $W_{65} = X_1(65)/\langle 51\rangle$. We use the coordinate t on $X_1(5)$ for which the universal curve in Tate normal form has $b = c = t$, and a coordinate z on the genus 0 curve $X_1(13)/\langle 3\rangle$. Over $\mathbb{F}_2$ the j-maps are

$$j_5(t) = \frac{t^{12} + t^8 + t^4 + 1}{t^7 + t^6 + t^5}, \qquad j_{13}(z) = \frac{z^{16} + z^4 + 1}{z^{28} + z^{25} + z^{24} + z^{21} + z^{20} + z^{17} + z^{16} + z^{13}},$$

and we compute the coordinate z and the map j_{13} from a model of $X_1(13)$ over $\mathbb{F}_2$.

Lemma 9.7. *The subgroup of $\Delta(65)$ generated by $\langle 4\rangle$ and $\langle 51\rangle$ has order 6 and acts freely on $X_1(65)$, also in characteristic 2, so Y'_{65} and W_{65} have good reduction at 2 and genus 21 and 61. The function field of $Y'_{65,\mathbb{F}_2}$ is generated by t and z with $j_5(t) = j_{13}(z)$, and the diamond operators $\langle 3\rangle$ and $\langle 6\rangle$ act on it by $\tau_T(t,z) = (1/t, z)$ and $\tau_U(t,z) = (t, z+1)$. The curve W_{65} is the normalization of $X_1(5) \times_{X(1)} X_1(13)$.*

Proof. Every element $\langle a\rangle$ of this subgroup has $a \equiv \pm 1 \pmod 5$ (the residues are $\pm 1, \pm 4, \pm 9, \pm 16, \pm 36, \pm 51$ modulo 65), so, as 65 is squarefree, Lemma 7.2 shows that the subgroup acts freely, in characteristic 0 and 2, and the genera follow from Riemann-Hurwitz, as $X_1(65)$ has genus 121. As $51 \equiv 1 \pmod 5$ and $51 \equiv -1 \pmod{13}$, the curve Y'_{65} parametrizes elliptic curves with a point of order 5 up to sign and a $\langle 3\rangle$-orbit of points of order 13 up to sign, so it is the normalization of the fibre product of $X_1(5)$ and $X_1(13)/\langle 3\rangle$ over the j-line, which we verify to be irreducible, and in the same way W_{65} parametrizes elliptic curves with points of order 5 and 13, each up to sign. The maps from Y'_{65} to $X_1(5)$ and to $X_1(13)/\langle 3\rangle$ commute with the diamond operators, so $\langle a\rangle$ acts on t through $a \bmod 5$ and on z through $a \bmod 13$. On $X_1(5)$ the operators $\langle 2\rangle = \langle 3\rangle$ act by $t \mapsto -1/t$, hence by $t \mapsto 1/t$ over $\mathbb{F}_2$, as we compute, and on $X_1(13)/\langle 3\rangle$ over $\mathbb{F}_2$ the operator $\langle 2\rangle$ acts by $z \mapsto z+1$, as we compute from the moduli interpretation. As $3 \equiv -2 \pmod 5$ and $\langle 3\rangle$ acts trivially on $X_1(13)/\langle 3\rangle$, while $6 \equiv 1 \pmod 5$ and $\langle 6\rangle = \langle 2\rangle\langle 3\rangle$ on $X_1(13)$, the operators $\langle 3\rangle$ and $\langle 6\rangle$ act on Y'_{65} by $(t,z) \mapsto (1/t, z)$ and $(t,z) \mapsto (t, z+1)$. □

Proposition 9.8. *The group $\mathbb{Z}/65\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree $d \in \{6, 7, 8\}$.*

Proof. Let D be the trace divisor of a point of order 65 over a number field of degree d. By Section 9.1, its reduction modulo 2 is entirely cuspidal, or it is $G + \overline{C}$, where G is a non-cuspidal closed point of degree $e \in \{6, 7, 8\}$ and $\overline{C}$ is the reduction of an effective rational cuspidal divisor of degree $d - e$.

Suppose first that the reduction is $G + \overline{C}$. On Y'_{65} we have $\langle 3 \rangle = \tau_T$, so $A_3 = T_3 - 1 - 3\tau_T$. For $\psi \in \{\tau_T - 1, \tau_U - 1, T_2 + 1\}$ the group $\psi J(Y'_{65})(\mathbb{Q})$ is finite by Lemma 9.1, so $A_3\psi$ annihilates $J(Y'_{65})(\mathbb{Q})$, and A_3 annihilates the images of the rational cuspidal divisors as divisors (Lemma 2.3). Hence the push-forward P of G to Y'_{65} satisfies $[\psi A_3 P] = 0$ for these three ψ, and none of the following tests depends on $\overline{C}$. For $e = 7$ we compute that all the elliptic curves over $\mathbb{F}_{128}$ with a point of order 65 have cyclic group of order 130, and that their points of order 65 give 56 points of $Y'_{65}(\mathbb{F}_{128})$, that is, 8 closed points of degree 7. For $e \in \{7, 8\}$ the push-forwards of the points of degree e form two orbits under the residual diamond operators, and for a representative P of each of them we compute that the divisor

$$(\tau_T - 1)A_3 P = \tau_T T_3 P - T_3 P + 2(\tau_T P - P)$$

is not principal, for $e = 7$, where $T_3 P$ is a single closed point of degree 28, and for $e = 8$. For $e = 6$, the only elliptic curve over $\mathbb{F}_{64}$ with a point of order 65, up to isomorphism, is supersingular with cyclic group of order 65. We compute the images on Y'_{65} of its 48 points of order 65 and of their images under the four 3-isogenies. This gives 3 possibilities for the divisor P and 10 possibilities for $T_3 P$ for each of them, and for each of the 30 possibilities one of $[(\tau_T - 1)A_3 P]$, $[(\tau_U - 1)A_3 P]$ and $[(T_2 + 1)A_3 P]$ is non-zero.

Suppose finally that the reduction of D is entirely cuspidal. Then so is that of its push-forward to W_{65}. The closed cusps of $W_{65,\mathbb{F}_2}$, with their degrees and widths, are 12 of degree 1 and width 65, 6 of degree 2 and width 13, and 2 each of degree 6 and widths 1 and 5. Those of width 5 lie below cusps of $X_1(65)_{\mathbb{F}_2}$ of degree 12, so they cannot occur, and those of degree 2 lie below cusps of degree 4, so they occur with even multiplicity. For $d = 8$ this leaves $[t^8](1-t)^{-12}(1-t^4)^{-6}(1-t^6)^{-2} = 83949$ possible divisors, which we check using the description of the cusps. The residual diamond group $\Delta(65)/\langle 51 \rangle$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, generated by $\langle 27 \rangle$ and $\langle 41 \rangle$, and $\langle 2 \rangle^6 = 1$ on W_{65}. We apply Proposition 7.3 with $\psi_1 = \langle 27 \rangle - 1$, $\psi_2 = \langle 41 \rangle - 1$ and $\psi_3 = T_2^6 - 1$ (Lemma 9.1), for which $\psi_3^* = \mathcal{C}^6 - 1$ by (7), so

$$U = (\mathcal{C} - 1)\big((\langle 27 \rangle^* - 1)\Omega + (\langle 41 \rangle^* - 1)\Omega + (\mathcal{C}^6 - 1)\Omega\big), \qquad \Omega = H^0(W_{65,\mathbb{F}_2}, \Omega^1).$$

We compute that U has dimension 48, and, computing the spaces $\Omega(jP)$ at one cusp in each orbit of the residual diamond operators and transporting them, that the restriction of U to each of the 83949 divisors has rank 8. Adding $8 - d$ times a cusp of degree 1 to a possible divisor of degree $d \in \{6, 7\}$ gives one of these, so by Remark 7.4 the restriction of U is also surjective at the possible divisors of degree 6 and 7, and Proposition 7.3 gives a contradiction. □

9.5. The group $\mathbb{Z}/69\mathbb{Z}$.

Proposition 9.9. *The group $\mathbb{Z}/69\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree $d \in \{7, 8, 9\}$.*

Proof. Let D be the trace divisor of a point of order 69 over a number field of degree d. We have $\operatorname{rk} J_1(69)(\mathbb{Q}) = 0$ [DEvH+21, Theorem 3.1(2)], and Abramovich's bound gives $\operatorname{gon}_{\mathbb{Q}} X_1(69) > 20.94 > 2d$, so by Proposition 2.5(b) the reduction of D modulo 2 is not entirely cuspidal. We compute that the non-cuspidal closed points of $X_1(69)_{\mathbb{F}_2}$ of degree

at most 9 have degrees 7, 8 and 9, and that there are 66, 44 and 44 of them. 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 $1^{22}, 2^{11}, 11^2, 22$, so the closed cusps of degree 1 and 2 are reductions of Galois orbits of cusps of the same degree. So the reduction of D is $G + \overline{C}$, where G is one of these non-cuspidal points and $\overline{C}$ is the reduction of an effective rational cuspidal divisor of degree $d - \deg G \leq 2$.

Let $Y_{69} \to Z_{69} = X_0(69)$ be the unramified double cover of Lemma 9.4, where H is the subgroup of order 11 of $\Delta(69)$, with the model of $Y_{69,\mathbb{F}_2}$ of Section 9.2. The Jacobians of Y_{69} and Z_{69} are quotients of $J_1(69)$, so their groups of rational points are finite. As $\langle 5 \rangle \in H$, the operator $A_5 = T_5 - 6$ annihilates these groups (Proposition 2.2(2)), and it annihilates the images of the rational cuspidal divisors as divisors (Lemma 2.3). So the image P of G on $Z_{69,\mathbb{F}_2}$ satisfies $[T_5P - 6P] = 0$, and so does its image P_Y on $Y_{69,\mathbb{F}_2}$. 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, and we compute that $T_5P - 6P$ is not principal on $Z_{69,\mathbb{F}_2}$ for two of those of degree 7, for both of degree 8 and for one of degree 9. For the remaining point P of degree 7 and the remaining one of degree 9, the non-trivial automorphism of Y_{69} over Z_{69}, which commutes with T_5, 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, and for all the possible lifts T of T_5P to Y_{69}, eight for degree 7 and two for degree 9, we compute that $T - 6P_Y$ is not principal. □

10. The group $\mathbb{Z}/54\mathbb{Z}$

Let $X = X_1(54)$ and $Y = X_1(27)$, and let $\pi : X \to Y$ be the map $(E, P) \mapsto (E, 2P)$. In degree 6 a class test on Y at the prime 5 leaves only elliptic curves whose reductions modulo 5 have j-invariant 2, and a 2-isogeny excludes them. In degrees 7, 8 and 9 we combine the possible reductions at 2 and at 5 of the push-forward to Y of the trace divisor, which is a form of the Mordell-Weil sieve of Bruin and Stoll [BS10]. As $2 \mid 54$, at the prime 2 we use a semistable model of X over $\mathbb{Z}_2$.

We first collect the facts at 5 which the three proofs share. Let E be an elliptic curve over a number field K of degree $d \in \{6, 7, 8, 9\}$ with a point P of order 54, and let D be the trace divisor of $(E, 2P)$ on Y. It is the push-forward under π of the trace divisor of (E, P) on X, and an effective rational divisor of degree d on Y with non-cuspidal support. We have $\operatorname{rk} J_1(54)(\mathbb{Q}) = 0$ [DEvH+21, Theorem 3.1(2)], and as $i(54) = 972$, we have $\operatorname{gon}_{\mathbb{Q}} X \geq \operatorname{gon}_{\mathbb{C}} X > 9.64 > d$. So Proposition 2.5(a) with $p = 5$ shows that the reduction modulo 5 of the trace divisor of (E, P) is not entirely cuspidal, and neither is that of D.

By [DEvH+21, Theorem 3.1(2), Theorem 4.13, Corollary 4.14 and Table 2], $J_Y(\mathbb{Q}) = \mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}} Y \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/52497\mathbb{Z}$. As 5 is a primitive root modulo 27, every Galois orbit of cusps of Y over $\mathbb{Q}$ reduces to a single closed cusp of $Y_{\mathbb{F}_5}$ of the same degree. We fix a rational cusp c_* of Y and take all the classes relative to it. We compute

$$J_Y(\mathbb{F}_5) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/342175446\mathbb{Z},$$

and that the reduction H_5 of $J_Y(\mathbb{Q})$, which is generated by the classes of the closed cusps of $Y_{\mathbb{F}_5}$, has invariants $[3, 3, 52497]$ and index 6518. So H_5 contains the classes of all cuspidal divisors of degree 0 on $Y_{\mathbb{F}_5}$. If we write the reduction of D modulo 5 as $D' + C'$, as in Lemma 5.6, with D' of degree $e > 0$, then Lemma 5.6 gives $[D' + C' - d\,\overline{c_*}] \in H_5$, and hence $[D' - e\,\overline{c_*}] \in H_5$.

The map π, of degree 3, is the scheme of non-zero 2-torsion points of the universal elliptic curve. Above a non-cuspidal closed point y of $Y_{\mathbb{F}_5}$ of degree k there is one closed point of

$X_{\mathbb{F}_5}$ of degree $3k$, a point of degree k and a point of degree $2k$, or three points of degree k, according to whether the 2-division cubic has 0, 1 or 3 roots over the residue field of y, and their push-forwards are $3y$, y and $2y$, and y, respectively. We also compute that the numbers of non-cuspidal closed points of $Y_{\mathbb{F}_5}$ of degrees $1, \dots, 6$ are $0, 9, 57, 171, 612, 2700$, and that the elliptic curves of $0, 0, 30, 171, 396, 1890$ of them have a point of order 2 over the residue field.

Finally, let $\phi : E \to \widetilde{E} = E/\langle 27P \rangle$ be the quotient isogeny. The point $\phi(P)$ has order 27, and $\ker \hat{\phi} = \phi(E[2])$ is generated by a K-rational point R of order 2, so $\widetilde{P} = \phi(P) + R$ is a point of order 54 of $\widetilde{E}$ over K, with $2\widetilde{P} = \phi(2P)$. So all of the above also holds for the trace divisor $\widetilde{D}$ of $(\widetilde{E}, \phi(2P))$ on Y. As E and $\widetilde{E}$ are isogenous, they have good reduction at the same primes.

Proposition 10.1. *The group $\mathbb{Z}/54\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a sextic field.*

Proof. Let E, P and D be as above, with $d = 6$, and write the reduction of D modulo 5 as $D' + C'$, with D' of degree $e > 0$. As $e \leq 6$, it follows from the description of the fibres of π and the numbers of points above that D' is $3y$ for a closed point y of degree 2, a single closed point of degree 3, 4, 5 or 6, or a sum of two closed points of degree 3 (possibly equal), where in the last two cases the elliptic curve of each point has a point of order 2 over its residue field. We compute that $[D' - e\,\overline{c_*}] \in H_5$ for only six of the $9 + 30 + 171 + 396 + 1890 + 465$ divisors of these types, namely $z_i + z_j$ with $1 \leq i \leq j \leq 3$, where z_1, z_2, z_3 are the closed points of degree 3 of $Y_{\mathbb{F}_5}$ whose elliptic curves have j-invariant 2.

For a prime $\wp$ of K above 5, the reduction of $(E, 2P)$ modulo $\wp$ is a point of Y with values in the residue field of $\wp$, so it lies on a closed point of $Y_{\mathbb{F}_5}$, which is non-cuspidal if and only if E has good reduction at $\wp$. The reduction of D modulo 5 is a sum of positive multiples of these closed points, so the support of D' consists of those for the primes $\wp$ at which E has good reduction, and as $e > 0$ there is at least one such prime. As each of them is one of z_1, z_2, z_3, the reduction of E modulo each such $\wp$ has j-invariant 2.

Let $\wp$ be such a prime. The above also applies to $\widetilde{E}$, which has good reduction at $\wp$, so the reduction of $\widetilde{E}$ modulo $\wp$ also has j-invariant 2. But this reduction is the quotient of the reduction of E by a subgroup of order 2. The curve $y^2 = x^3 + x + 1$ has j-invariant $1728 \cdot 4/31 = 2$, so over $\overline{\mathbb{F}}_5$ the reduction of E is isomorphic to it. Its points of order 2 are $(r, 0)$ with $r^3 + r + 1 = 0$, and as $x^3 + x + 1$ has no root in $\mathbb{F}_5$, r has degree 3 over $\mathbb{F}_5$. Moving $(r, 0)$ to $(0, 0)$ gives the model $y^2 = x(x^2 + 3rx + 3r^2 + 1)$, and the quotient of a curve $y^2 = x(x^2 + ax + b)$ by $\langle (0, 0) \rangle$ is $y^2 = x(x^2 - 2ax + a^2 - 4b)$. So the quotient by $\langle (r, 0) \rangle$ is $y^2 = x(x^2 + 4rx + 2r^2 + 1)$, whose j-invariant is

$$\frac{1}{r^2 + r + 1} = 2r^2 + r + 4 \notin \mathbb{F}_5,$$

which is a contradiction. □

In degrees 7, 8 and 9 we also use the prime 2.

Lemma 10.2. *Let E be an elliptic curve over a number field K of degree $d \in \{7, 8, 9\}$ with a point P of order 54. Then E has good reduction at some prime of K above 2. Moreover, every prime of K above 2 at which E has good reduction is unramified and has residue degree at least 6, and the reduction of E at it is ordinary.*

Proof. We have seen that $J_1(54)(\mathbb{Q})$ is finite and that $\mathrm{gon}_{\mathbb{Q}} X > d$. The rational cuspidal subgroup $(\mathbb{Z}/3\mathbb{Z})^3 \times (\mathbb{Z}/9\mathbb{Z})^2 \times \mathbb{Z}/1102437\mathbb{Z} \times \mathbb{Z}/1529080119\mathbb{Z}$ of $J_1(54)(\mathbb{Q})$ has index dividing 3 in it [DEvH+21, Theorem 4.13 and Table 2], so $J_1(54)(\mathbb{Q})$ has odd order.

As $\Gamma_1(54) = \Gamma_1(27) \cap \Gamma_0(2)$ and the $\Gamma_1(27)$-structure is rigid, Deligne and Rapoport [DR73, Chapter VI, Theorem 6.9] give a regular semistable model of X over $\mathbb{Z}_2$. Its special fibre consists of two copies of $Y_{\mathbb{F}_2}$ glued at the supersingular points, and the cusps reduce to smooth points. All the cusps are defined over subfields of $\mathbb{Q}(\zeta_{27})$, and 2 is a primitive root modulo 27, so every Galois orbit of cusps over $\mathbb{Q}$ reduces to a single closed point of the same degree.

Suppose that E has bad reduction at every prime of K above 2, and let D_X be the trace divisor of (E, P) on X. By Lemma 2.4, applied to the point $2P$ of order 27, the elliptic curve E has multiplicative reduction at every prime of K above 2, so D_X reduces to a sum of cusps. By the above, this is also the reduction of a $\mathbb{Q}$-rational cuspidal divisor C. As D_X and C have the same reduction on a regular model, the class $[D_X - C] \in J_1(54)(\mathbb{Q})$ maps to 0 in the special fibre of the Néron model of $J_1(54)$. Every torsion point in the kernel of reduction modulo 2 has order a power of 2, and $J_1(54)(\mathbb{Q})$ has odd order, so $[D_X - C] = 0$. As $\mathrm{gon}_{\mathbb{Q}} X > d$, this forces $D_X = C$, which is impossible as D_X is not cuspidal.

Now let $\mathfrak{p}$ be a prime of K above 2 at which E has good reduction. Reduction modulo $\mathfrak{p}$ is injective on the points of odd order, so the reduction of $(E, 2P)$ is a non-cuspidal point of Y over the residue field of $\mathfrak{p}$. As we compute that $Y_{\mathbb{F}_2}$ has no non-cuspidal closed points of degree at most 5, the residue degree f of $\mathfrak{p}$ is at least 6, and as its ramification index e satisfies $ef \leq d \leq 9$, we have $e = 1$. If the reduction were supersingular, its j-invariant would be 0, so E would have a Weierstrass equation over the completion $K_{\mathfrak{p}}$ with integral coefficients and $a_1 \in 2\mathcal{O}_{K_{\mathfrak{p}}}$, and as the reduction has no point of order 2, the point $27P$ of order 2 would lie in the formal group. But then $[2](T) = 2T - a_1T^2 + O(T^3)$, where the terms of degree at least 3 have integral coefficients, and for $v_2(T) \geq 1$ the valuation of $2T$ is smaller than that of all the other terms. So, as $K_{\mathfrak{p}}$ is unramified over $\mathbb{Q}_2$, the formal group has no non-zero point of order 2 over $K_{\mathfrak{p}}$, which is a contradiction. □

As $J_Y(\mathbb{Q})$ has odd order, reduction at 2 is injective on it, and we compute that its reduction is the whole group $J_Y(\mathbb{F}_2) \simeq (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/52497\mathbb{Z}$ (see also `N54_via27_final.m` and `C54/C54_lower_reproduce.m`). As 2 is a primitive root modulo 27, the Galois orbits of cusps of Y over $\mathbb{Q}$ also stay irreducible modulo 2. We match the closed cusps modulo 2 and modulo 5 using the orders of vanishing of the functions b^4/Δ and b, where $y^2+(1-c)xy-by = x^3 - bx^2$ is the universal elliptic curve in Tate normal form and Δ is its discriminant. These functions are units on $Y_1(27)_{\mathbb{Z}[1/27]}$, so their orders of vanishing along the cusps do not change under reduction. This gives a map $\kappa : H_5 \to J_Y(\mathbb{F}_2)$, sending the reduction modulo 5 of a class in $J_Y(\mathbb{Q})$ to its reduction modulo 2, and κ is an isomorphism.

Proposition 10.3. *The group $\mathbb{Z}/54\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 7 or 8.*

Proof. Let D be as above, and suppose first that $d = 8$. At 2, the reduction is not entirely cuspidal by Lemma 10.2. We compute that the non-cuspidal closed points of $Y_{\mathbb{F}_2}$ of degrees $1, \ldots, 8$ number $0, 0, 0, 0, 0, 9, 9, 18$, so the reduction $\overline{D}$ is a closed point of degree 6 plus a cuspidal divisor of degree 2, a closed point of degree 7 plus one of the 9 rational cusps, or a closed point of degree 8. The effective cuspidal divisors of degree 2 give 48 distinct classes, so we obtain a set $S_2 \subseteq J_Y(\mathbb{F}_2)$ of $9 \cdot 48 + 9 \cdot 9 + 18 = 531$ classes $[\overline{D} - 8\overline{c_*}]$, and the class

$a = [\overline{D} - 8\overline{c_*}]$ of the reduction at 5 must satisfy

$$a \in H_5 \quad \text{and} \quad \kappa(a) \in S_2. \tag{9}$$

By the description of the fibres of π and the numbers of points above, the non-cuspidal part of $\overline{D}$ is P_k for a closed point P_k of degree $k \in \{3, \dots, 8\}$ with a rational 2-torsion point, $3P_2$ for a closed point P_2 of degree 2, or $P_3 + P_3'$, $P_3 + P_4$, $P_3 + P_5$ or $P_4 + P_4'$, where the points may coincide. Reducing the first point by the diamond operators, which preserve condition (9), and allowing all the classes of cuspidal divisors of the complementary degree, we obtain the following tests:

non-cuspidal part	supports	cuspidal classes	tests
P_3	4	1836	7344
P_4	19	636	12084
P_5	44	192	8448
P_6	212	48	10176
P_7	828	9	7452
P_8	3579	1	3579
$3P_2$	1	48	48
$P_3 + P_3'$	120	48	5760
$P_3 + P_4$	684	9	6156
$P_3 + P_5$	1584	1	1584
$P_4 + P_4'$	3249	1	3249

For the 828 points of degree 7 we compute the elliptic curves over $\mathbb{F}_{5^7}$ with a point of order 27 and a rational 2-torsion point directly, and check the completeness of this list against an independent count of the points of $X_1(54)$ over $\mathbb{F}_{5^7}$. For the points of degree 8 we compute the elliptic curves over $\mathbb{F}_{5^8}$ with a point of order 27 and a rational point of order 2, by running through all the j-invariants and their twists. We do not assume that the 3-primary part of the group is cyclic: if it is $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3^k\mathbb{Z}$, we take all the cyclic subgroups of order 27. This gives 3579 diamond orbits of closed points of $Y_{\mathbb{F}_5}$ of degree 8, 2704 with one and 875 with three rational points of order 2, which we verify separately. They account for $9(2704 + 3 \cdot 875) = 47961$ closed points of degree 8 of $X_1(54)_{\mathbb{F}_5}$, and the remaining 126 lie above points of degree 4 with one rational 2-torsion point, whose push-forward is $2P_4$. Their sum 48087 is the number of closed points of degree 8 of $X_1(54)_{\mathbb{F}_5}$, which we compute independently.

Of the 65880 tests, we compute (`C54/C54_lower_reproduce.m` for the 62301 with a non-cuspidal part of degree at most 7, `C54/C54_good8_class_shard.m` for the others) that 153 give a class in H_5, and none of their images under κ lies in S_2. This contradicts (9).

Suppose now that $d = 7$. By Lemma 10.2 the reduction of D at 2 is not entirely cuspidal, so, by the numbers of non-cuspidal closed points of $Y_{\mathbb{F}_2}$ above, it is a closed point of degree 6 plus one of the 9 rational cusps, or a closed point of degree 7. The reduction of D at 5 is $D' + C'$, where D' is of one of the types of degree at most 7 in the table above, which lists all the possible non-cuspidal parts of degree at most 8, and C' is cuspidal of the complementary degree. Adding $\overline{c_*}$ to the reductions of D at 2 and at 5 does not change their classes relative to c_*, and gives possibilities considered above for $d = 8$ (see the discussion after Lemma 5.6). So the class $[D' + C' - 7\overline{c_*}]$ satisfies (9), which the computation above excludes. □

Proposition 10.4. *The group $\mathbb{Z}/54\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a nonic field.*

Proof. Let E, P, D, $\widetilde{E}$ and $\widetilde{D}$ be as above, with $d = 9$. Neither D nor $\widetilde{D}$ reduces modulo 5 to a cuspidal divisor. Modulo 2, by Lemma 10.2, D reduces to an ordinary non-cuspidal closed point of degree 6, 7, 8 or 9 of $Y_{\mathbb{F}_2}$ plus a cuspidal divisor of the complementary degree, and as the closed cusps of $Y_{\mathbb{F}_2}$ are reductions of rational cuspidal divisors, the classes of these reductions, taken relative to c_*, form a set S_2 of 2412 classes. Hence the class $a = [\overline{D} - 9\overline{c_*}]$ of the reduction of D modulo 5 satisfies $a \in H_5$ and $\kappa(a) \in S_2$, and the same holds for $\widetilde{D}$.

Using the description of the fibres of π and the numbers of points above, we run through all the possible reductions of D modulo 5, which are single points of degree $3, \dots, 9$, the multiples $3P_2$, $3P_3$, $2P_3$, $2P_4$, the sums $P_3 + P_3'$, $P_3 + P_4$, $P_3 + P_5$, $P_3 + P_6$, $P_4 + P_4'$, $P_4 + P_5$, $P_3 + P_3' + P_3''$ and $3P_2 + P_3$, where the points in the sums may coincide, each completed by every cuspidal divisor of the remaining degree, and we find (for $3P_2 + P_3$ in a separate computation) that apart from single points of degree 8 and 9 only 3 possibilities satisfy both conditions, of the forms $P_3 + P_6$, $P_4 + P_5$ and $P_4 + P_5$. For the points of degree 8, none of the 3579 representatives up to the diamond operators has class in H_5. For the points of degree 9 there are 16135 representatives, and we first use Lemma 2.10: a function f on $Y_{\mathbb{F}_5}$ with $\operatorname{div} f = 2A$ defines a homomorphism $\chi_f : J_Y(\mathbb{F}_5) \to \mathbb{F}_5^\times/\mathbb{F}_5^{\times 2}$, which is trivial on H_5, as H_5 has odd order. It excludes 8087 of them, and of the remaining 8048 exactly 4 satisfy both conditions.

Finally, for these 7 possibilities we compute the reductions of $\widetilde{D}$ for all the possible choices of the reduction of $\langle 27P \rangle$, which are 1, 3, 3 and 3, 1, 1, 1 choices respectively, using the isogenies of degree 2 of the elliptic curves over finite fields, and we find that none of the 13 resulting classes lies in H_5, which is a contradiction. □

11. 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 $2n \in \{22, 28, 30\}$ for $d = 6$, $2n \in \{22, 24, 28, 30\}$ for $d = 7$, $2n \in \{28, 30, 32, 36, 42\}$ for $d = 8$ and $2n \in \{28, 30, 32, 34, 36, 40, 42\}$ for $d = 9$, and we show that none of them is a subgroup of the torsion of an elliptic curve over a number field of degree d. In the last two subsections we treat the groups $\mathbb{Z}/48\mathbb{Z}$ for $d \in \{6, 8, 9\}$ and $\mathbb{Z}/52\mathbb{Z}$ for $d = 9$, using the morphisms $X_1(4k) \to X_1(2, 2k)$ of Lemma 3.3 with $k = 12$ and $k = 13$. The group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$ for $d \in \{6, 7, 8\}$, the points of degree 9 on $X_1(2, 26)$ and the points of degree 6 on $X_1(2, 24)$ are treated in Section 13.

The method is the same in all degrees. In all these cases the Jacobian of $X_1(2, 2n)$ has rank 0 over $\mathbb{Q}$, and we exclude the entirely cuspidal reduction of the trace divisor at an odd prime p. We test only one representative of each orbit of a group of level automorphisms of $X_1(2, 2n)$ (see Section 5.3), and we push the possible reductions of the trace divisor forward to $X_1(2n)$, to curves $X_1(2, m)$ and $X_1(m)$ with m a proper divisor of $2n$, and to quotients of $X_1(2, 2n)$ by groups of level automorphisms. On each of these curves the class of the push-forward is constrained by the reduction of the Mordell-Weil group of its Jacobian (Lemma 5.6 and (6)). The few cases that survive these tests are excluded by the Hecke sieve, by Riemann-Roch computations, or by showing that a level automorphism which fixes the reduction of the trace divisor would fix the trace divisor itself.

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 $P \notin \langle Q \rangle$, i.e. $P \neq nQ$. If n is even, the maps

$$(E, P, Q) \longmapsto \big(E, P + n\beta Q,\ \gamma P + aQ\big), \qquad \beta, \gamma \in \{0, 1\},\ a \in (\mathbb{Z}/2n\mathbb{Z})^\times, \tag{10}$$

are level automorphisms, and taken modulo -1 they form a group of $2\varphi(N)$ automorphisms of X: as $n(\gamma P+aQ)=nQ$, the new point of order 2 is not in the subgroup generated by the new point of order N. If n is odd, the level automorphisms permute the three points of order 2 and act by $\Delta(n)$ on the point of order n, and they form a group isomorphic to $S_3\times\Delta(n)$. These automorphisms, and the other ones that we use, commute with the Hecke operators T_q for odd primes $q\nmid N$, as these are defined by isogenies of odd degree. We identify the Galois orbits of cusps of X over $\mathbb{Q}$ and their reductions using the valuations of integral modular units. In the normalization $y^2=x^3+cx^2+b(1-b-c)x$, $P=(0,0)$, $Q=(b,b)$, of (13), the functions b, $b(1-b-c)$, $c^2-4b(1-b-c)$ and $x(kQ)$, $1\le k\le N/2$, are units on $Y_1(2,N)$ over $\mathbb{Z}[\frac{1}{2N}]$, so their valuations at the cusps do not change under reduction modulo an odd prime $p\nmid N$. We also use the four maps $X\to X_1(2n)$ 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 $2n$ in all cases.

By [DEvH+21, Theorem 3.1(3)] (see also [DS17, Theorem 4.1]), $\operatorname{rk} J_1(2,N)(\mathbb{Q})=0$ for all the $N=2n$ above. By [NV26, Table 1] we have $\operatorname{gon}_{\mathbb{Q}} X\ge 8,8,12,12,10,10,10$ for $N=22,24,26,28,30,32,36$ and $\operatorname{gon}_{\mathbb{Q}} X_1(2,34)>9$, and for $N=40,42$ we have $i(2,N)=1152$, so $\operatorname{gon}_{\mathbb{C}} X\ge \frac{325}{2^{15}}\cdot 1152>11.42$, hence $\operatorname{gon}_{\mathbb{C}} X\ge 12$. So $\operatorname{gon}_{\mathbb{Q}} X>d$ in every degree d in which we use X, and by Proposition 2.5(a) the reduction of the trace divisor modulo an odd prime $p\nmid N$ is not entirely cuspidal. By Lemma 3.3, excluding $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z}$ also excludes $\mathbb{Z}/4n\mathbb{Z}$. The numbers of non-cuspidal closed points of $X_{\mathbb{F}_p}$ that we use are listed in Table 4, except those of $X_1(2,22)$, which are in Table 3, and those of $X_1(2,24)$, which are in the proof of Proposition 11.2.

X	p	non-cuspidal closed points of degree $1,\dots,9$
$X_1(2,26)$	3	$0,0,0,0,36,122,288,936,2328$
$X_1(2,28)$	3	$0,0,0,0,48,64,312,606,2112$
$X_1(2,32)$	3	$0,0,0,0,0,192,320,960,1824$
$X_1(2,34)$	3	$0,0,0,36,48,48,144,738,2160$
$X_1(2,36)$	5	$0,0,48,120,720,2904,10416,50334,218080$
$X_1(2,40)$	3	$0,0,0,32,96,64,480,504,2048$
$X_1(2,42)$	5	$0,0,0,126,648,2080,11376,48816,211776$

TABLE 4. Non-cuspidal closed points of $X_1(2,2n)_{\mathbb{F}_p}$ of small degree, checked against the zeta functions.

11.1. **The curves $X_1(2,22)$ and $X_1(2,24)$.** The curve $X_1(2,24)$ is also used for $\mathbb{Z}/48\mathbb{Z}$ in Section 11.7.

Proposition 11.1. *The group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/22\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 6 or 7.*

Proof. Let $X=X_1(2,22)$, a curve of genus 16, and let $d\in\{6,7\}$. By Table 3 the reduction of the trace divisor modulo 3 is $x+C$, with x a single non-cuspidal closed point of degree $e\in\{5,\dots,d\}$ and C cuspidal of degree $d-e\le 2$. The closed cusps have degrees $1^{15},5^3$, and the cusps of degree 1 are reductions of rational cusps, so $A_5C=0$ and $[A_5x]=0$. We compute that A_5x is not principal for the representatives of all $12,20,48$ diamond orbits of points of degree $5,6,7$, which covers both degrees. □

Proposition 11.2. *The group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/24\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a septic field.*

Proof. Let $X = X_1(2,24)$, a curve of genus 13, and work at $p = 5$. Using the valuations of integral modular units, we find 19 classes of closed cusps of $X_{\mathbb{F}_5}$ which are reductions of rational cuspidal divisors, of degrees $1^8, 2^6, 4^5$, and we fix one of the 8 rational cusps as c_*. We compute

$$J(\mathbb{F}_5) \simeq (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/4\mathbb{Z})^2 \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \times (\mathbb{Z}/480\mathbb{Z})^2,$$

and that the classes of these divisors generate a subgroup $G \simeq \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^2 \times \mathbb{Z}/120\mathbb{Z} \times \mathbb{Z}/240\mathbb{Z}$ of order 921600, which is the order of $J(\mathbb{Q})$ [DEvH+21, Proposition 4.16 and Table 3], so G is the reduction of $J(\mathbb{Q})$ and reduction is injective on $J(\mathbb{Q})$.

By Proposition 13.20(2), X has 8 non-cuspidal closed points of degree 6. Adding any of the 8 rational cusps to them gives a set $\mathcal{R}$ of 64 reducible effective rational divisors of degree 7, with 64 distinct reduction classes, and $\mathcal{R}$ is stable under the diamond operators. The non-cuspidal closed points of $X_{\mathbb{F}_5}$ of degrees $1, \dots, 7$ number $0, 0, 16, 96, 672, 2712, 11184$, so the non-cuspidal part of the reduction of the trace divisor D is a single closed point of degree $3, \dots, 7$, a sum of two cubic points, or a sum of a cubic and a quartic point. Taking the first point up to the diamond operators, there are $4, 32, 168, 684, 2796$ cases of the first kind and 64 and 384 of the other two. For each of these 4132 cases we compute the classes of all the possible reductions $\overline{D}$, with all the cuspidal parts of the complementary degree, and find that only 16 of them lie in G, all coming from 2 closed points of degree 6. These 16 classes are exactly the reduction classes of 16 divisors in $\mathcal{R}$, as we verify using the two sextic points. Hence $[D - 7c_*] = [R - 7c_*]$ for some $R \in \mathcal{R}$, so $D \sim R$, and $D = R$ by Lemma 2.7, which is impossible since D is irreducible. □

11.2. **The curve $X_1(2,28)$.** Let $X = X_1(2,28)$, a curve of genus 25, with $\operatorname{gon}_{\mathbb{Q}} X \geq 12$ [NV26, Table 1], and work at $p = 3$. The closed cusps of $X_{\mathbb{F}_3}$ have degrees $1^{12}, 2^6, 3^4, 6^2$, and those of degree 1 and 2 are reductions of rational cuspidal divisors of the same degree, so $q = 5$ and $q = 11$ are admissible for every cuspidal divisor supported on them. All the cusps are defined over $\mathbb{Q}(\zeta_{28})$, and the Frobenius at 3 has order 6 in $\operatorname{Gal}(\mathbb{Q}(\zeta_{28})/\mathbb{Q})$, so σ_5 either fixes a cusp c of degree 3 or maps it to the other cusp of degree 3 with the same valuations of the unit functions above. Hence $A_5 c = (\sigma_5 c - c) + 5\langle 5\rangle(\sigma_5 c - c)$ is 0 or of the form $v + 5w$, where v and w are differences of two such cusps, which gives 17 possible values of $A_5 c$. Let $Y = X_1(28)$. By [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], $J_Y(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/936\mathbb{Z}$ is generated by rational cuspidal divisor classes, and we compute that its reduction G has index 4 in $J_Y(\mathbb{F}_3) \simeq (\mathbb{Z}/4\mathbb{Z})^2 \times \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/936\mathbb{Z}$.

Proposition 11.3. *The group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree $d \in \{6, 7, 8, 9\}$.*

Proof. By Table 4 the reduction of the trace divisor D is $x + C$, with x a single non-cuspidal closed point of degree $e \in \{5, \dots, d\}$ and C cuspidal of degree $d - e$.

Suppose first that $d \leq 8$. If $d - e \leq 2$, then $[A_q x] = 0$ for $q = 5, 11$. If $d = 8$ and $e = 5$, then C may contain a cusp of degree 3, and $A_5 x + A_5 C$ is principal, where $A_5 C$ is one of the 17 values above, which include 0. Up to the group (10) there are $2, 5, 13, 29$ possible points x of degree $5, 6, 7, 8$, which we enumerate. For the 2 points of degree 5 we compute that $A_5 x + A_5 C$ is not principal for all 17 values, and for the points of degree 6, 7 and 8 we compute that $A_5 x$ or $A_{11} x$ is not principal, except for 2 points of degree 8, which we call x_1 and x_2. As $d - e \leq 2$ for $d \leq 7$, this proves the claim for $d \in \{6, 7\}$.

To exclude x_1 and x_2 for $d = 8$ we use the forgetful map $\pi : X \to Y$, $(E, P, Q) \mapsto (E, Q)$. For a rational cusp c_* of Y, the class $[\pi_* x_2 - 8\overline{c_*}]$ is not in G, which excludes x_2. The

class $[\pi_* x_1 - 8\overline{c_*}]$ is the reduction of $[L - 8c_*]$ for an explicit rational cuspidal divisor L of degree 8 on Y, so if D reduces to x_1 (after applying an automorphism of X, which maps trace divisors to trace divisors), then $\pi_* D \sim L$ by injectivity of reduction. We compute that $\ell(L) = 1$ on Y over $\mathbb{Q}$ and that the unique effective divisor y in its class is a closed point of degree 8, with residue field $K = \mathbb{Q}(t)$, where

$$16t^8 - 78t^7 + 149t^6 - 118t^5 - 22t^4 + 132t^3 - 120t^2 + 48t - 8 = 0.$$

Hence $\pi_* D = y$, and D is a closed point of degree 8 with the same residue field K. But the 2-division polynomial of the elliptic curve corresponding to y factors over K into factors of degrees 1 and 2, so this curve has only one point of order 2 over K, and y does not lift to a point of X over K. This is a contradiction.

Suppose now that $d = 9$. Up to the 24 automorphisms (10) there are 2, 5, 13, 29 and 88 cases. We use the four maps to Y, and we compute that only 10 cases satisfy (6) for all four maps. For these we use A_5, with the 17 possible values of $A_5 c$ if the complement of a sextic point is a cusp c of degree 3. We compute that A_5 of the non-cuspidal part, with any of these corrections, is not principal, except for one case, a point x of degree 8 with a cuspidal complement c of degree 1, which is the reduction of a rational cusp. The level automorphism $h(P, Q) = (P + 14Q, 13Q)$, of order 2, fixes x and none of the rational cusps. If D reduced to $x + c$, then Lemma 2.9(a), with $d = 9$, $e = 1$ and $\operatorname{gon}_{\mathbb{Q}} X \geq 12 > 10$, would give $hc = c$, which is a contradiction. □

11.3. **The curve $X_1(2, 30)$.** Let $X = X_1(2, 30)$, a curve of genus 25. In all four degrees we push the divisors forward to quotient curves. Let $Y = X_1(30)$ and consider the three morphisms

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

from X to Y. They are defined over $\mathbb{Q}$, they map cusps to cusps and they commute with the diamond operators. This is because $15Q$, P and $P + 15Q$ are the non-zero points of $E[2]$, and adding $16Q$, which has order 15, to them gives points of order 30. These three maps do not suffice, and we also use the quotient W of X by the automorphism $(E, P, Q) \mapsto (E, 15Q, P + Q)$ of order 3, which permutes the three non-zero points of $E[2]$ cyclically. We denote the quotient map by $\alpha : X \to W$. The curve W sees a part of J_X that is invisible on Y (see Remark 11.4). Recall that $X_1(15)$ is an elliptic curve. The curve W is the double cover $f : W \to X_1(15)$ 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 it, and it has genus 9, as we compute.

Remark 11.4. The covering $X \to X_1(15)$, $(E, P, Q) \mapsto (E, 2Q)$, is Galois with group $\mathrm{SL}_2(\mathbb{F}_2) \simeq S_3$, acting on the ordered bases $(P, 15Q)$ of $E[2]$, and W is its quotient by the subgroup A_3 of order 3. The space $H^0(X, \Omega^1)$ decomposes into 1 copy of the trivial representation of S_3, 8 copies of the sign representation and 8 copies of the 2-dimensional one, as the genera 1, 9, 9 and 25 of $X_1(15)$, W, Y and X show. Each π_i is invariant under a subgroup of order 2 of S_3, so the differentials pulled back from Y involve only the trivial and the 2-dimensional representations, while those on W are the invariants of A_3, which are the trivial and the sign representations. So the test on W detects the part of J_X, of dimension 8, on which S_3 acts by the sign character and which is invisible on Y.

The map α is unramified, also over $\mathbb{F}_7$: a non-trivial element of A_3 fixing a non-cuspidal point (E, P, Q) would be induced by an automorphism of E fixing the point $2Q$ of order 15,

which is the identity, and the identity does not permute the points of order 2 non-trivially. The stabilizers of the cusps in S_3 have order 2, so A_3 acts freely on the cusps as well.

Above a non-cuspidal closed point y of $W_{\mathbb{F}_7}$ of degree k, the 2-division cubic of the corresponding elliptic curve has square discriminant, so it either splits, and then α has three points of degree k above y, or it is irreducible, and then there is one point of degree $3k$ above y, whose push-forward is $3y$. The Galois orbits of cusps of W have degrees $1, 1, 4, 2, 4, 1, 2, 1$, and we denote them by $C_1, \dots, C_8$ in this order. Let $c_W = \alpha(c_0)$, a rational cusp of W.

By [DEvH+21, Proposition 4.16 and Table 3], $J_X(\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^5 \times \mathbb{Z}/24\mathbb{Z} \times (\mathbb{Z}/8160\mathbb{Z})^2$ is generated by rational cuspidal divisor classes, and push-forward maps rational cuspidal divisors of degree 0 on X to rational cuspidal divisors of degree 0 on W. So for every effective rational divisor D of degree d on X, the class $[\alpha_* D - d\, c_W] = \alpha_*[D - d\, c_0]$ lies in the subgroup H of $J_W(\mathbb{Q})$ generated by the classes $[C_i - (\deg C_i) c_W]$. The group $J_W(\mathbb{Q})$ is finite, as α^* maps it to $J_X(\mathbb{Q})$ with finite kernel, so reduction modulo 7 is injective on it, and we identify H with its reduction. We compute

$$J_W(\mathbb{F}_7) \simeq (\mathbb{Z}/2\mathbb{Z})^6 \times \mathbb{Z}/102\mathbb{Z} \times \mathbb{Z}/10608\mathbb{Z}, \qquad H \simeq (\mathbb{Z}/2\mathbb{Z})^5 \times \mathbb{Z}/8\mathbb{Z}.$$

Similarly, by [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], $J_Y(\mathbb{Q}) = \mathrm{Cl}^c_{\mathbb{Q}}\, Y \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8160\mathbb{Z}$, and we compute that $J_Y(\mathbb{F}_7) \simeq (\mathbb{Z}/4\mathbb{Z})^3 \times \mathbb{Z}/136\mathbb{Z} \times \mathbb{Z}/16320\mathbb{Z}$, in which the reduction G of $J_Y(\mathbb{Q})$ has index 4352. We apply (6) to the three maps π_i with $p = 7$ and this G, and the images in $J_Y(\mathbb{F}_7)/G$ of the sets $\mathcal{S}_0, \dots, \mathcal{S}_5$ of (6) have $1, 9, 41, 67, 68, 68$ elements.

Proposition 11.5. *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 $d \in \{6, 7, 8, 9\}$.*

Proof. Let D be the trace divisor and work at $p = 7$. The entirely cuspidal reduction is excluded as explained at the beginning of the section.

Suppose first that $d \leq 7$. We determine all the possible reductions on W, and then test their lifts with the map π_2. If $d = 6$ we replace D by $D + c_0$, whose reduction has the same non-cuspidal part, as the argument below uses only that D is an effective rational divisor of degree 7 whose reduction is not entirely cuspidal (the condition on H holds for every effective rational divisor, and the test with π_2 is Lemma 5.6 applied to $\pi_{2*}D$). The divisor $T := \alpha_* \overline{D}$ is effective of degree 7, and its class $[T - 7\overline{c_W}]$ lies in H. For each of the 256 classes $h \in H$ we compute the Riemann-Roch space of a divisor of degree 7 in the class $h + [7\overline{c_W}]$, which gives all the effective divisors in that class. This gives 1404 effective divisors T, of which 816 are not entirely cuspidal. For these 816 divisors T we run through all the divisors $\overline{D}$ with $\alpha_* \overline{D} = T$, using the description of the fibres of α above. For 448 of them no such $\overline{D}$ exists, as the multiplicities are not divisible by 3. For the remaining 368 we obtain 1440 possibilities for the non-cuspidal part D' of $\overline{D}$, of degree e say. By (6) for π_2, the class $[\pi_{2*} D' - e\, \overline{y_0}]$ lies in $G + \mathcal{S}_{7-e}$, and we compute that this fails for all 1440 possibilities.

Suppose now that $d = 8$, and let x be the corresponding point of X. No elliptic curve over a number field of degree 1, 2 or 4 has a point of order 30 [Maz77, KM88, Kam92a], [DN25, Theorem 1.1], so x has degree 8 and D is a closed point of degree 8. As α is a cyclic cover of degree 3, the push-forward $D_W := \alpha_* D$ is also a closed point of degree 8, and $[D_W - 8c_W] \in H$.

For each of the 256 classes $h \in H$ we choose a rational cuspidal divisor $L = \sum_i v_i C_i$ of degree 8 with $[L - 8c_W] = h$, and we compute $\ell(\overline{L})$ on $W_{\mathbb{F}_7}$. As $\ell(L) \leq \ell(\overline{L})$, and as the

members of $|L|$ reduce to members of $|\overline{L}|$, this determines the possible divisors D_W. Write $B = \sum_i \lfloor v_i/2 \rfloor f(C_i)$ and $C = \sum_i (v_i \bmod 2) C_i$. Then $L = f^*B + C$, as f is totally ramified at the cusps, and the pull-backs of the sections of $L(B)$ on $X_1(15)$ give lower bounds for $\ell(L)$. We find the following:

a) for 35 classes, $\ell(\overline{L}) = 0$,
b) for 116 classes, $\ell(\overline{L}) = 1$ and L is effective and cuspidal,
c) for 96 classes, $C \neq 0$ and $\ell(L) = \ell(\overline{L}) = \ell(B)$, so every divisor in $|L|$ is of the form $f^*B' + C$,
d) for 4 classes, $L = f^*B$ with $\deg B = 4$ and $\ell(L) = \ell(\overline{L}) = 4$, so every divisor in $|L|$ is the pull-back of a divisor in $|B|$,
e) for the remaining 5 classes, $\ell(\overline{L}) = 2$.

By injectivity of reduction, $[D_W - 8c_W]$ is one of these 256 classes, and $D_W \in |L|$ for the corresponding L. This is impossible in cases a), b) and c), as D_W is non-cuspidal. In case d), $D_W = f^*B'$ for an effective divisor B' of degree 4, which is a closed point as D_W is closed. Let F be its residue field, of degree 4. The universal elliptic curve and the point of order 15 are defined over F, and the residue field K of D, of degree 2 over F, contains all the 2-torsion. So the Galois group of the 2-division polynomial over F has order at most 2, and the curve has a point of order 2 over F, hence a point of order 30 over a field of degree 4, which is impossible.

In case e), D_W reduces to one of the 8 divisors in the pencil $|\overline{L}|$ over $\mathbb{F}_7$. For each of the 5 pencils we compute these 8 divisors and their lifts to $X_{\mathbb{F}_7}$, using the description of the fibres of α above. Only one pencil has members that lift to a non-cuspidal divisor on $X_{\mathbb{F}_7}$, namely 6 closed points of degree 8, each with three lifts, so $\overline{D}$, which is not entirely cuspidal, is one of 18 divisors. Finally, (6) for the three maps π_i, with $e = 8$, says that $[\pi_{i*}\overline{D} - 8\overline{y_0}] \in G$ for $i = 1, 2, 3$. We compute that for each of the 18 divisors at least one of the three classes does not lie in G. This is a contradiction.

Suppose finally that $d = 9$. The class $[\alpha_* D - 9c_W]$ lies in H, and we compute that the 956 effective cuspidal divisors of degree 9 on W represent all 256 classes of H. For each class we choose such a divisor $L = \sum_i v_i C_i$, and write $L = f^*B + C$ with $B = \sum_i \lfloor v_i/2 \rfloor f(C_i)$ and $C = \sum_i (v_i \bmod 2) C_i$. Note that $C \neq 0$, as $\deg L = 9$ is odd and $\deg f^*B$ is even. Riemann-Roch computations over $\mathbb{F}_7$ give $\ell(\overline{L}) = 1$ for 84 of these classes, $\ell(\overline{L}) = \ell_{X_1(15)}(\overline{B})$ for 144 others, and $\ell(\overline{L}) = 2$ for the remaining 28. As $\ell(L) \geq 1$, and $\ell(L) \geq \ell_{X_1(15)}(B)$ as $f^*L(B) \subseteq L(L)$, semicontinuity shows that the first two equalities also hold over $\mathbb{Q}$. Hence for these 228 classes every effective divisor in $|L|$ over $\mathbb{Q}$ contains a cusp: it is L itself in the first case, and $f^*B' + C$ in the second. As $\alpha_* D$ is effective with non-cuspidal support, its class is one of the 28 pencil classes, and its reduction is one of the $8 \cdot 28 = 224$ members of these pencils over $\mathbb{F}_7$. We lift them to $X_{\mathbb{F}_7}$, using the description of the fibres of α above, and we find 42 possible reductions of D that are not entirely cuspidal, 24 closed points of degree 9 and 18 of degree 8 together with a cusp. Finally we compute that each of the 42 cases fails (6) for one of the three maps π_i. □

11.4. **The curves $X_1(2,32)$, $X_1(2,34)$ and $X_1(2,40)$.** Over octic fields the groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/34\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/40\mathbb{Z}$ are excluded in Propositions 13.8 and 13.18, where we determine the octic points on $X_1(34)$ and $X_1(40)$.

Proposition 11.6. *The group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/32\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 8 or 9, and the groups $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/34\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/40\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over a nonic field.*

Proof. We work modulo 3. For $X_1(2,32)$, by Table 4 the reduction of D is a closed point of degree $6,\dots,d$ plus a cuspidal divisor, and there are 8, 10, 32 and 57 cases of degree $6,\dots,9$ up to the 32 automorphisms (10). We use the four maps to $X_1(32)$, whose Mordell-Weil group $(\mathbb{Z}/2\mathbb{Z})^3\times\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/120\mathbb{Z}\times\mathbb{Z}/11640\mathbb{Z}$ is generated by rational cuspidal divisors [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2] and has index 68 in $J_1(32)(\mathbb{F}_3)$, allowing all the cuspidal complements over $\mathbb{F}_3$, and we compute that each of the 107 cases fails (6) with $d=9$ for one of them. As $\mathcal{S}_{8-e}\subseteq\mathcal{S}_{9-e}$, this also excludes $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/32\mathbb{Z}$ over octic fields.

For $X_1(2,34)$ the possible types of the non-cuspidal part are $[4],\dots,[9]$, $[4,4]$ and $[4,5]$, which gives 239 cases up to the 48 level automorphisms, where in the types with two points we normalize only the first one. We use the two maps to $X_1(34)$ which keep Q and $P+Q$. The group $J_1(34)(\mathbb{Q})\simeq\mathbb{Z}/8760\mathbb{Z}\times\mathbb{Z}/595680\mathbb{Z}$ is generated by rational cuspidal divisors [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], its reduction has index 128 in $J_1(34)(\mathbb{F}_3)$ and contains the classes of all the cuspidal divisors, and we compute that each of the 239 cases fails (6) for one of the two maps.

For $X_1(2,40)$ the possible types are $[4],\dots,[9]$, $[4,4]$ and $[4,5]$, which gives 234 cases up to the 32 automorphisms (10). We use the map $X_1(2,40)\to X_1(2,20)$, $(E,P,Q)\mapsto(E,P,2Q)$, and the map which divides E by $\langle 20Q\rangle$ and keeps the images of P and Q, which are independent of orders 2 and 20. 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 divisors [DEvH+21, Proposition 4.16 and Table 3], its reduction has index 4 in $J_1(2,20)(\mathbb{F}_3)$, and it contains the classes of all the cuspidal divisors. These two maps leave 27 cases, all with non-cuspidal part of degree 8 or 9. For them we use the map to $X_1(40)$, with $J_1(40)(\mathbb{Q})\simeq(\mathbb{Z}/2\mathbb{Z})^3\times\mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/120\mathbb{Z}\times\mathbb{Z}/895440\mathbb{Z}$ of index 4592 in $J_1(40)(\mathbb{F}_3)$, and we compute that all 27 cases fail (6). □

11.5. **The curve $X_1(2,36)$.** Over septic fields the group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/36\mathbb{Z}$ is excluded in Proposition 13.10, where we determine the septic points on $X_1(36)$.

Let $X=X_1(2,36)$, a curve of genus 41, and work at $p=5$. The closed cusps of $X_{\mathbb{F}_5}$ have degrees $1^{24},2^8,6^4$, and we use the group of 24 automorphisms of the form (10). We use the map $X\to X_1(2,18)$, $(E,P,Q)\mapsto(E,P,2Q)$, and the four maps to $X_1(36)$ described at the beginning of the section. By [DEvH+21, Theorem 3.1(3), Proposition 4.16 and Table 3], $J_1(2,18)(\mathbb{Q})\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/42\mathbb{Z}\times\mathbb{Z}/126\mathbb{Z}$, and by [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], $J_1(36)(\mathbb{Q})\simeq\mathbb{Z}/12\mathbb{Z}\times\mathbb{Z}/252\mathbb{Z}\times\mathbb{Z}/7812\mathbb{Z}$, both generated by rational cuspidal divisor classes. As 5 generates $(\mathbb{Z}/18\mathbb{Z})^\times$, every closed cusp of $X_1(2,18)_{\mathbb{F}_5}$ is the reduction of a Galois orbit of cusps of the same degree, so the reduction of $J_1(2,18)(\mathbb{Q})$ contains the classes of all the cuspidal divisors, and (6) says that the push-forward to $X_1(2,18)$ of the non-cuspidal part of the reduction of the trace divisor has class in it.

Let $g(E,P,Q)=(E,P+18Q,P+Q)$, an automorphism of X of order 4, with $g^2(E,P,Q)=(E,P,19Q)$. Every power of g fixes the point $4Q$ of order 9, and a non-trivial automorphism of an elliptic curve does not fix a point of order 9, so the group generated by g acts freely on the non-cuspidal points of X, and we check that it acts on the cusps with orbits of length 4. So the quotient $W=X/\langle g\rangle$ is a curve of genus 11, and $X\to W$ is unramified. Let t be the parameter of $X_1(9)$ in Tate normal form,

$$r=t^2-t+1,\quad c=t(r-1),\quad b=rc,\quad E_9:\ y^2+(1-c)xy-by=x^3-bx^2,$$

and $j_9(t) = j(E_9)$. Writing $R = 18Q$, $S = 9Q$, $U = P$ and $V = P + R$, the functions t of $(E, 4Q)$ and $w = 4(x(S) - x(R))/(x(U) - x(V))$ are invariant under g, and we check that

$$\mathbb{Q}(W) = \mathbb{Q}(t, w), \qquad 16(w^2 + 16)^3 = j_9(t)\, w^4.$$

To see this, after moving R to $(0, 0)$ and writing $E : y^2 = x(x^2 + \alpha x + \beta)$, we have $(x(S) - x(R))^2 = \beta$ and $(x(U) - x(V))^2 = \alpha^2 - 4\beta$, so $w^2 = 16\beta/(\alpha^2 - 4\beta)$, which gives the equation, and the degrees match.

Over nonic fields we also need the following two lemmas, and a quotient Z of X of genus 9, defined in Lemma 11.8.

Lemma 11.7. *Let X be $X_1(m, n)$, with good reduction at an odd prime p and $J_X(\mathbb{Q})$ finite, let h be a level automorphism of X, and let D be an effective rational divisor whose support contains no cusp. Suppose that D reduces to $x + \overline{c}$, where $hx = x$ and c is a cusp defined over a number field unramified at p, with the same residue field as $\overline{c}$, and suppose that the h-orbit of c consists of r cusps $c_i = h^{i-1}c$, $1 \le i \le r$, with distinct reductions. Then $\ell\big(x + \sum_i \overline{c_i}\big) \ge r$.*

Proof. As in Lemma 2.9, the class $[hD - D - hc + c]$ is torsion and reduces to 0, so it is 0, and the class of $L = D - c$ is h-invariant. Put $M = L + \sum_i c_i$. For each i we have $M \sim h^{i-1}D + \sum_{j \ne i} c_j$, which is effective, and the corresponding sections vanish at all c_j with $j \ne i$ but not at c_i, as $h^{i-1}D$ contains no cusp. So these r sections are linearly independent, and the claim follows by semicontinuity, as M reduces to $x + \sum_i \overline{c_i}$. □

Lemma 11.8. *Let $X = X_1(2, 36)$, $h(P, Q) = (P, 13Q)$, which has order 3, and $Z = X/\langle h\rangle$, of genus 9. The reduction of $J_Z(\mathbb{Q})$ modulo 5 is contained in a subgroup $H \simeq (\mathbb{Z}/3\mathbb{Z})^3 \times (\mathbb{Z}/24\mathbb{Z})^3$ of index 8 of $J_Z(\mathbb{F}_5) \simeq (\mathbb{Z}/3\mathbb{Z})^3 \times (\mathbb{Z}/24\mathbb{Z})^2 \times \mathbb{Z}/192\mathbb{Z}$.*

Proof. The curve Z is the cover of $X_1(2, 12)$ obtained by adjoining a root of the cubic factor of the 3-division polynomial of $E/\langle 4Q_{12}\rangle$ which corresponds to the three cyclic subgroups of order 3 other than the kernel of the dual isogeny. Its Jacobian has rank 0, as a quotient of J_X, so $A_7 J_Z(\mathbb{Q}) = 0$. We compute that the classes of the cuspidal divisors of $Z_{\mathbb{F}_5}$ generate the subgroup H, that $A_7 H = 0$ by Proposition 2.2, and that for a cubic point z the class $a = [z - 3\overline{c_0}]$ generates $J_Z(\mathbb{F}_5)/H$ and $A_7 a$ has order 8, so $\ker(A_7) = H$. □

Proposition 11.9. *The group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 8 or 9.*

Proof. Let D be the trace divisor.

Suppose first that $d = 8$. By Table 4 the non-cuspidal part of the reduction of D is a closed point of degree $3, \dots, 8$, or a sum of two closed points, of type $[3, 3]$, $[3, 4]$, $[3, 5]$ or $[4, 4]$. We find $2, 5, 30, 126, 434, 2115$ representatives of the closed points of degrees $3, \dots, 8$ under the group of automorphisms, and for the sums of two points we reduce only the first point. We compute that only 461 of the 2712 single points and 2376 pairs pass the test with the map to $X_1(2, 18)$. For these we use three of the maps to $X_1(36)$, given by $(E, P, Q) \mapsto (E', Q')$, where E' is E, $E/\langle P\rangle$ or $E/\langle P + 18Q\rangle$ and Q' is the image of Q, and we apply (6) with all the cuspidal divisors over $\mathbb{F}_5$. We compute that only one divisor passes all three tests, a single closed point $\overline{x}$ of degree 8 with multiplicity 1. We check that $g\overline{x} = \overline{x}$. If D reduces to $\overline{x}$, then Lemma 2.9(a), with $C = 0$ and $\operatorname{gon}_{\mathbb{Q}} X \ge 10 > 8$, gives $gD = D$, so D is the pull-back of a rational divisor D_W of degree 2 on W. The Jacobian of W has rank 0, as it is a quotient of J_X, so for an odd prime $q \nmid 36$ the operator $A_q = T_q - 1 - q\langle q\rangle$, which descends

to W, annihilates $J_W(\mathbb{Q})$ and the image of the rational cusp c_0. So $[A_q\overline{x}_W] = 0$ for the image $\overline{x}_W$ of $\overline{x}$ on $W_{\mathbb{F}_5}$, which is a closed point of degree 2. We compute that $\ell(A_7\overline{x}_W) = 0$, which is a contradiction.

Suppose now that $d = 9$. By Table 4 the possible types of the non-cuspidal part of the reduction of D are $[3], \dots, [9]$, $[3,3]$, $[3,4]$, $[3,5]$, $[3,6]$, $[4,4]$, $[4,5]$ and $[3,3,3]$. Normalizing the first point by the 24 automorphisms gives 25936 cases. The map to $X_1(2,18)$, where the reduction of $J_1(2,18)(\mathbb{Q})$ has index 12 in $J_1(2,18)(\mathbb{F}_5)$, leaves 2064 cases. Lemma 11.8, applied to the image of D on Z, leaves 267 cases, and the four maps to $X_1(36)$, where the reduction of $J_1(36)(\mathbb{Q})$ has index 214272 in $J_1(36)(\mathbb{F}_5)$, leave a single case, which is a closed point x of degree 8 plus a rational cusp c. We compute all of this.

The automorphism g fixes x, and the 24 rational cusps of $X_{\mathbb{F}_5}$ form 6 orbits of length 4 under g, so by Lemma 11.7 it suffices to show that $\ell(x + \sum_{j=0}^{3} g^j c) < 4$ for every rational cusp c. We construct $W_{\mathbb{F}_5}$ explicitly from the model above, as the extension $\mathbb{F}_5(t,w)$ of the function field of $X_1(9)$, and $X_{\mathbb{F}_5} \to W_{\mathbb{F}_5}$ as the unramified cyclic cover of degree 4 given by $\zeta^4 = f$, where $\operatorname{div}(f) = 4D_0$ with D_0 of order 4, which we check. Then $\ell_X(\pi^*A) = \sum_{j=0}^{3} \ell_W(A + jD_0)$ for every divisor A on $W_{\mathbb{F}_5}$, where $\pi : X \to W$ is the quotient map. The point x is the pull-back of a closed point x_W of degree 2 of $W_{\mathbb{F}_5}$, and each orbit $\{g^j c\}$ is the pull-back of a rational cusp c_W. We compute $\ell_W(x_W + c_W + jD_0) = 1, 0, 0, 0$ for $j = 0, 1, 2, 3$, so $\ell_X(x + \sum_j g^j c) = 1 < 4$, which is a contradiction. □

11.6. **The curve $X_1(2,42)$.** Let $X = X_1(2,42)$, a curve of genus 61, and work at $p = 5$. The cusps of X have degrees $1^{18}, 2^9, 6^6$ over $\mathbb{Q}$, and the closed cusps of $X_{\mathbb{F}_5}$ have degrees $1^{18}, 2^9, 3^6, 6^3$. Put $S_1 = P$, $S_2 = 21Q$ and $S_3 = P + 21Q$. The 36 automorphisms $(E, P, Q) \mapsto (E, S_i, S_j + 2uQ)$, with $i \neq j$ and $u \in \{1, 2, 4, 5, 8, 10\}$, form a group isomorphic to $(\mathrm{SL}_2(\mathbb{F}_2) \times (\mathbb{Z}/21\mathbb{Z})^\times)/\{\pm 1\}$. We push the trace divisor forward to $X_1(2,14)$ and to $X_1(21)$, whose Jacobians have finite Mordell-Weil groups generated by rational cuspidal divisor classes, namely $J_1(2,14)(\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ [DEvH+21, Theorem 3.1(3), Proposition 4.16 and Table 3] and $J_1(21)(\mathbb{Q}) \simeq \mathbb{Z}/364\mathbb{Z}$ [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2]. For $d = 8$ we also use a quotient of X of genus 31.

Lemma 11.10. *Let $X = X_1(2,42)$ and let ι be the automorphism $(E, P, Q) \mapsto (E, P, 29Q)$, which negates the 3-primary part of Q and fixes P and $3Q$. Then $Z = X/\langle\iota\rangle$ has genus 31 and good reduction at every prime $p \nmid 42$, and $J_Z(\mathbb{Q})$ is finite. Over the function field of $X_1(2,14)$, with the universal elliptic curve $y^2 = x^3 + cx^2 + b(1-b-c)x$, $P = (0,0)$, $3Q = (b,b)$, the function field of Z is obtained by adjoining a root x_3 of the 3-division polynomial $3x_3^4 + 4cx_3^3 + 6b(1-b-c)x_3^2 - b^2(1-b-c)^2$. For a rational effective divisor of degree 8 on X whose reduction modulo 5 is $N + C$, with N non-cuspidal and C cuspidal of degree at most 1 (resp. 4), the divisor $A_{11}\pi_*N$ (resp. $A_{17}\pi_*N$) is principal on $Z_{\mathbb{F}_5}$, where $\pi : X \to Z$ is the quotient map.*

Proof. A fixed point of ι would be induced by an automorphism of an elliptic curve fixing a point of order 14, which is the identity, and the identity does not negate a point of order 3. We check that ι acts freely on the 72 cusps as well, so π is unramified, also modulo every prime $p \nmid 42$, and $g(Z) = 31$ as $g(X) = 61$. A point of order 3 is determined up to sign by its x-coordinate, which gives the function field. The Jacobian of Z is a quotient of J_X, which has rank 0. For a prime $q \nmid 42$ the isogenies of degree q commute with ι, so T_q descends to Z, and A_q annihilates $J_Z(\mathbb{Q})$ and the image of the rational cusp c_0. We check that σ_{11} fixes

every closed cusp of $X_{\mathbb{F}_5}$ of degree 1, while σ_{17} fixes every closed cusp as $17 \equiv 5^5 \pmod{42}$, so $A_q C = 0$ in the respective cases by Lemma 2.3. □

Lemma 11.11. *Let $X = X_1(2,42)$ and $h(E,P,Q) = (E, P+21Q, Q)$. Let x be a non-cuspidal closed point of X of degree $d \mid 8$, and $D = (8/d)x$. Then the reduction of D modulo 5 is not fixed by h.*

Proof. Suppose $h\overline{D} = \overline{D}$. Then $[hD - D] \in J_X(\mathbb{Q})$ reduces to 0, so $hD \sim D$, and $hD = D$ by Lemma 2.7, as $\operatorname{gon}_{\mathbb{Q}} X \geq 12$. So $hx = x$. The map $X \to X_1(42)$, $(E,P,Q) \mapsto (E,Q)$, has degree 2, and h is its non-trivial automorphism over $X_1(42)$. The map is unramified on the non-cuspidal locus, as an automorphism of an elliptic curve fixing a point of order 42 is the identity. As $hx = x$, the image of x is a non-cuspidal point of $X_1(42)$ of degree $d/2$, which divides 4. This is impossible, as no elliptic curve over a number field of degree 1, 2 or 4 has a point of order 42 [Maz77, KM88, Kam92a], [DN25, Theorem 1.1]. □

For $d = 9$ let G_9 be the group of level automorphisms generated by $a(P,Q) = (21Q, P+Q)$, which permutes the three points of order 2 cyclically, and $b(P,Q) = (P, 25Q)$, which multiplies the point of order 7 by 4, and let $Y = X/G_9$, which has genus 5, with quotient map $\pi_Y : X \to Y$.

Lemma 11.12. *The reduction of $J_Y(\mathbb{Q})$ modulo 5, taken relative to a rational cusp c_*, is contained in a subgroup $K \simeq (\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/24\mathbb{Z}$ of index 18 of $J_Y(\mathbb{F}_5) \simeq \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/6\mathbb{Z})^2 \times \mathbb{Z}/48\mathbb{Z}$.*

Proof. The function field of Y is obtained from the Tate normal form of $X_1(7)$, with parameter v, by putting $t = (v^3 - 3v + 1)/(v(v-1)) - 8$, adjoining u with $u^2 = t$, and the coordinates of a point of order 3 on the elliptic curve

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

where $f_1 = t^2+13t+49$, $f_2 = t^2+5t+1$ and $f_3 = t^4+14t^3+63t^2+70t-7$. This field has degree 8 over $\mathbb{Q}(u)$, and $j = f_1 f_2^3/t$ has degree 16 as a function of u, so it has degree $128 = 1152/9$ over $\mathbb{Q}(j)$ and is the full invariant field of G_9. We compute its reduction modulo 5, which has genus 5. The Jacobian J_Y has rank 0, as a quotient of J_X, so $A_{11} = T_{11} - 1 - 11\langle 11 \rangle$ kills $J_Y(\mathbb{Q})$. We compute A_{11} on $J_Y(\mathbb{F}_5)$, on the cusps by Proposition 2.2 and on three ordinary cubic places from the isogenies of degree 11, and find that its kernel is K. □

Proposition 11.13. *The group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/42\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 8 or 9.*

Proof. Let D be the trace divisor.

Suppose first that $d = 8$. By Table 4 the non-cuspidal part of the reduction of D is a single closed point of degree $4, \dots, 8$ or a sum of two closed points of degree 4. We find $5, 18, 64, 316, 1372$ representatives of the closed points of degrees $4, \dots, 8$ under the group of 36 automorphisms. For the sums of two quartic points we reduce only the first point and take all 126 choices of the second, which gives 1775 single points and 630 pairs to test.

We first use the maps $X \to X_1(2,14)$, $(E,P,Q) \mapsto (E,P,3Q)$, and $X \to X_1(21)$, $(E,P,Q) \mapsto (E,2Q)$, and we apply (6), with all the cuspidal divisors over $\mathbb{F}_5$. We compute that only 288 of the 2405 cases pass. Next we use the three maps $X \to X_1(21)$ given by $(E,P,Q) \mapsto (E/G, 2Q \bmod G)$ for $G = \langle P \rangle, \langle 21Q \rangle, \langle P + 21Q \rangle$, and find that 41 cases pass: 2 quartic points with a cuspidal part of degree 4, a septic point with a cusp of degree

1, 4 octic points and 34 pairs of quartic points. Up to the full group of automorphisms these are 30 cases.

For these we use the curve Z of Lemma 11.10. We compute that $A_{17}\pi_*N$ is not principal for both quartic points, and that $A_{11}\pi_*N$ is not principal for the septic point, all 4 octic points and 21 of the 23 remaining pairs. For one of the two remaining pairs $A_{17}\pi_*N$ is not principal, as we compute, and the other pair is fixed by the automorphism h of Lemma 11.11, so it is excluded by that lemma.

Suppose now that $d = 9$. By Table 4 the possible types of the non-cuspidal part of the reduction of D are $[4], \dots, [9]$, $[4, 4]$ and $[4, 5]$, and up to the 36 level automorphisms there are 11533 cases. We compute the following sequence of necessary conditions.

a) The two maps to $X_1(2, 14)$, keeping $(P, 3Q)$ or dividing by $\langle 14Q\rangle$, where the reduction of $J_1(2, 14)(\mathbb{Q})$ has index 4 in $J_1(2, 14)(\mathbb{F}_5)$, leave 919 cases.
b) Lemma 11.12, applied to the image of D on Y with all the cuspidal complements allowed, leaves 119 cases.
c) The four maps to $X_1(21)$, keeping $2Q$ on E and on its three quotients by points of order 2, where the reduction of $J_1(21)(\mathbb{Q})$ has index 6 in $J_1(21)(\mathbb{F}_5)$, leave 44 cases.
d) If the non-cuspidal part has degree 8 and is fixed by a level automorphism g of even order, then Lemma 2.9(b), with a cuspidal complement of degree 1 and $9 + 1 < \operatorname{gon}_{\mathbb{C}} X$, gives $gD = D$, which contradicts Lemma 2.12. This leaves 18 cases.

Exactly 3 of the remaining cases are single closed points P_9 of degree 9, and each is fixed by an element $h \in G_9$ of order 3. As $J_X(\mathbb{Q})$ is finite, Lemma 2.9(a) gives $hD = D$, and by Lemma 2.12 D is the pull-back of a closed point of degree 3 of $X/\langle h\rangle$, so $\pi_{Y*}D/3$ is a rational effective divisor of degree 3 on Y, and the class of its reduction, taken relative to c_*, must lie in K. This excludes 2 of these 3 cases. For the third, $h = ab^2$, the image of D on $V = X/\langle h\rangle$ is a rational effective divisor of degree 3 whose reduction is a cubic point P_3 of $V_{\mathbb{F}_5}$. As $J_V(\mathbb{Q})$ is finite, $B = T_{11}P_3 - P_3 - 11\langle 11\rangle P_3$ is principal. We compute $T_{11}P_3$ from the 12 isogenies of degree 11, a sum of 4 closed points of degree 9, and we check by a Riemann-Roch computation on $V_{\mathbb{F}_5}$ that $\ell(B) = 0$. Here V has genus 17. Indeed, h fixes no cusp, as it permutes the points of order 2 cyclically, while at a cusp a point of order 2 is distinguished. A non-cuspidal fixed point of h needs an automorphism of order 3 of E, so $j = 0$, and counting the compatible level structures for the two automorphisms of order 3 gives 6 fixed points for each. So h has 12 fixed points, and $120 = 3(2g(V) - 2) + 24$ by the Riemann-Hurwitz formula.

Among the 15 remaining cases, 8 are closed points of degree 6 with $j = 0$, which are fixed by b. The image of such a point on Y is three times a point of degree 2, and a cuspidal complement which is not the reduction of a rational cuspidal divisor is a closed cusp c of degree 3, which is fixed by b and maps to $3c_Y$ with c_Y one of the two cusps of Y defined over $\mathbb{Q}(\sqrt{21})$, which are $\mathbb{F}_5$-rational as 5 splits in $\mathbb{Q}(\sqrt{21})$. Both of these contribute the same non-zero class of order 2 modulo K, and for 4 of these 8 points the condition of Lemma 11.12 forces this contribution. For them the whole reduction is fixed by b. The cuspidal lift C of c satisfies $bC = C$, so $[bD - D] = [bD - D - bC + C]$ is torsion and reduces to 0, hence it is 0, and $bD = D$ by Lemma 2.7, as $\operatorname{gon}_{\mathbb{Q}} X > 9$. So $\pi_{Y*}D/3$ is a rational divisor of degree 3 on Y reducing to $P_2 + c_Y$, and we compute that $[P_2 + c_Y - 3\overline{c_*}] \notin K$. For the remaining 11 cases, 4 of degree 6 with $j = 0$ and 7 others, the same argument shows that the cuspidal complement is the reduction of a rational cuspidal divisor C. Then $A_{11}N$ is principal, where N is the non-cuspidal part of the image on $X_1(42)$ under $(E, P, Q) \mapsto (E, Q)$, as A_{11} kills $J_1(42)(\mathbb{Q}) \simeq \mathbb{Z}/182\mathbb{Z} \times \mathbb{Z}/1092\mathbb{Z} \times \mathbb{Z}/131040\mathbb{Z}$ [DEvH+21, Theorem 3.1(2), Corollary 4.14

and Table 2] and the rational cuspidal divisors. We compute that $\ell(A_{11}N) = 0$ in 10 cases, and in the last one for the map $(E, P, Q) \mapsto (E, P + Q)$. □

11.7. **The group $\mathbb{Z}/48\mathbb{Z}$.** Over septic fields the group $\mathbb{Z}/48\mathbb{Z}$ is excluded by Lemma 3.3 and Proposition 11.2. In the other degrees we need a separate argument.

Proposition 11.14. *The group $\mathbb{Z}/48\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a sextic field.*

Proof. Suppose E_1 is an elliptic curve over a sextic field K with a point P_1 of order 48. By Lemma 3.3, the curve $E' = E_1/\langle 24P_1\rangle$ has $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \subseteq E'(K)$, so by Proposition 13.20(3) we may assume that $K = K_{2,24}$ and $E' = E_{2,24}$. Let $\phi : E_1 \to E'$ be the quotient isogeny. Its kernel has order 2, and $\ker \hat{\phi} = \phi(E_1[2])$ is generated by a K-rational point of order 2, so E_1 is isomorphic to one of the three curves 2-isogenous to $E_{2,24}$ over K. We compute that their torsion groups over K are $\mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/24\mathbb{Z}$, which is a contradiction. □

For octic and nonic fields we use the Hecke sieve and the push-forwards of Section 6.

Proposition 11.15. *The group $\mathbb{Z}/48\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 8 or 9.*

Proof. We have $\operatorname{rk} J_1(48)(\mathbb{Q}) = 0$ [DEvH+21, Theorem 3.1(2)] and $\operatorname{gon}_{\mathbb{Q}} X_1(48) \geq \operatorname{gon}_{\mathbb{F}_5} X_1(48) \geq 10$ [NV26, Table 1], so the entirely cuspidal reduction modulo 5 is excluded by Proposition 2.5. The numbers of non-cuspidal closed points of $X_1(48)_{\mathbb{F}_5}$ of degrees $1, \ldots, 9$ are 0, 0, 16, 64, 656, 2712, 10784, 48992 and 217520, so for $d = 9$ the possible types of D' are $[k]$ for $3 \leq k \leq 9$, $[3,3]$, $[3,4]$, $[3,5]$, $[3,6]$, $[4,4]$, $[4,5]$ and $[3,3,3]$.

We use the map $\pi : X_1(48) \to Y = X_1(2,24)$, $(E, P) \mapsto (E/\langle 24P\rangle, T, \overline{P})$, where T is the non-zero point of the kernel of the dual isogeny and $\overline{P}$ the image of P, which has order 24. It has degree 2, as P and $25P$ have the same image, and it commutes with the diamond operators. The group $J_Y(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^2 \times \mathbb{Z}/120\mathbb{Z} \times \mathbb{Z}/240\mathbb{Z}$ is generated by rational cuspidal divisors [DEvH+21, Proposition 4.16 and Table 3], and we compute that its reduction G has index 4608 in $J_Y(\mathbb{F}_5)$ (the group $J_Y(\mathbb{F}_5)$ and the order 921600 of G are given in the proof of Proposition 11.2). We apply (6) with $d = 9$, allowing all the effective cuspidal divisors of degree $9-e$ on $Y_{\mathbb{F}_5}$. For the types other than [9] there are 20882 cases, and 48 of them satisfy (6). For the type [9] we enumerate the 216208 closed points of degree 9 of $Y_{\mathbb{F}_5}$, in 13513 orbits under the 16 level automorphisms of Y which preserve G and the sets $\mathcal{S}_j$. Of these orbits, 1644 do not lift to $X_1(48)$. Before computing the classes of the others, we evaluate four characters χ_f as in Lemma 2.10, for functions f on $Y_{\mathbb{F}_5}$ with $\operatorname{div}(f) = 2A$, which we check to be trivial on G. They exclude 11173 orbits, and of the remaining 696 only 11 satisfy (6), which gives 24 cases on $X_1(48)$. We compute all of this.

For the remaining 72 cases we use the Hecke sieve on $X_1(48)_{\mathbb{F}_5}$. The cusps of $X_1(48)$ are defined over $\mathbb{Q}(\zeta_{48})$ and the orbits of closed cusps of $X_1(48)_{\mathbb{F}_5}$ have degrees $1^{16}, 2^{12}, 4^4$. As $29 \equiv 5^3 \pmod{48}$, the automorphism σ_{29} fixes every closed cusp, so 29 is admissible for every C'. As the closed cusps of degree 1 are defined over $\mathbb{Q}$ or $\mathbb{Q}(i)$, the prime 13 is admissible if C' is 0 or a single closed cusp of degree 1. So we use A_{29} if D' has degree 6 or 7, A_{13} if D' has degree 8 and A_7 if D' has degree 9, and we compute that $A_q D'$ is not principal in all 72 cases. This also covers $d = 8$: as $\mathcal{S}_{8-e} \subseteq \mathcal{S}_{9-e}$, every D' that satisfies (6) for $d = 8$ also satisfies it for $d = 9$, so it is, up to the diamond operators, one of the 48 cases above, and the prime that we use for it is admissible for its cuspidal part of degree

$8-e$: 29 is admissible for every C', and 13 is used only if D' has degree 8, when $C'=0$ (see Section 6.1). □

11.8. **The group $\mathbb{Z}/52\mathbb{Z}$.** Over sextic, septic and octic fields the group $\mathbb{Z}/52\mathbb{Z}$ is excluded in Proposition 13.22. Over nonic fields we use the uniqueness of the elliptic curve with a subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/26\mathbb{Z}$, which follows from the same proposition.

Proposition 11.16. *The group $\mathbb{Z}/52\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a nonic field.*

Proof. Let F/K have a point U of order 52, and let $\phi: F\to E=F/\langle 26U\rangle$. The point $\phi(U)$ has order 26 and is independent of the generator of the kernel of the dual isogeny, as the dual isogeny maps $13\phi(U)$ to $26U\neq 0$. So E has a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/26\mathbb{Z}$, and by Proposition 13.22 and Remark 3.2 the pair (K,E) is isomorphic to the pair $(K_{2,26},E_{2,26})$ of Proposition 13.5. Hence F is the quotient of $E_{2,26}$ by one of its three subgroups of order 2. If F has full 2-torsion over K, then $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/26\mathbb{Z}\subseteq F(K)$, and the same reductions as for $E_{2,26}$ show that $\#F(K)_{\mathrm{tors}}$ divides 52, so F has no point of order 4. Otherwise the point of order 4 would be a half of the generator of the kernel of the dual isogeny. Writing $E_{2,26}: y^2=x^3+cx^2+b(1-b-c)x$ with 2-torsion points $(r_i,0)$, the quotient by $(r_i,0)$ is $y^2=x^3-2Ax^2+\delta^2x$ with $A=c+3r_i$ and $\delta=r_j-r_k$, and a half of $(0,0)$ on it has $x=\pm\delta$ and $y^2=2x(\delta^2-Ax)$. We check, by reducing modulo primes above 3 and 7, that all 6 of these values are non-squares in $K_{2,26}$. □

12. The groups $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ with $m\geq 3$

Let E be an elliptic curve over a number field K with $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\subseteq E(K)$ for some $m\geq 3$. By the Weil pairing $\varphi(m)$ divides $[K:\mathbb{Q}]$, and $\varphi(m)$ is even, so K is a sextic or an octic field (see Section 2.2). Over sextic fields we treat here the groups $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/18\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/21\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/27\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/20\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$. The groups $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}\times\mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}$ are ruled out in Proposition 5.2, and $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/15\mathbb{Z}$ in Proposition 5.5. Over octic fields we treat here the groups $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3n\mathbb{Z}$ for $n=6,7,8,9$, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4n\mathbb{Z}$ for $n=4,5,6$, $\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/5n\mathbb{Z}$ for $n=3,4,5$, $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/10\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$. For most groups that we treat in both degrees, the computation for octic fields also covers sextic fields. The groups $\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/15\mathbb{Z}$ do occur over octic fields (Propositions 13.4 and 13.23), and the uniqueness in Proposition 13.23 also rules out $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/30\mathbb{Z}$. The groups $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/33\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/39\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/35\mathbb{Z}$ are ruled out in Propositions 13.7, 13.9 and 13.14.

In this section $F=\mathbb{Q}(\zeta_m)$ with $m\geq 3$, and the trace divisor of a point over K has degree $d_m=[K:F]$ over F. For $m\in\{3,4,6\}$ we have $d_m=3$ over sextic fields and $d_m=4$ over octic fields, and for $m\in\{5,10\}$ we have $d_m=2$. By [DS17, Theorem 4.1], $\operatorname{rk} J_1(m,n)(F)=0$ for

$$(m,n)\in\{(3,15),(3,18),(3,21),(3,24),(3,27),(4,16),(4,20),(4,24),(5,15),(5,20),(6,12)\}.$$

In [DS17] the case $m=5$ is listed without a written proof, so we also checked it: by the argument recalled before Lemma 12.8 below, it suffices that all the twists $f\otimes\chi$ of the newforms f occurring in $J_1(5,15)$ and $J_1(5,20)$ by characters χ modulo 5 have non-zero L-value at 1. These twists have levels dividing 75 and 100, and there are no newforms of positive analytic rank at these levels [LMF26]. For a prime $q\nmid n$ with $q\equiv 1 \pmod m$, the operator A_q annihilates $J_1(m,n)(F)$ when this group is finite, and it annihilates the F-rational cusps as divisors (Proposition 2.2). In each case over an octic field we also use an

explicit group of automorphisms of $X_1(m,n)$ over F, given by replacing the level structure (P,Q) by integral linear combinations of P and Q which preserve the orders and the Weil pairing, taken modulo ± 1. They commute with T_q for $q \equiv 1 \pmod m$. By Lemma 2.11, an elliptic curve over an octic field with one of the groups that we exclude in this section has no complex multiplication, so Lemma 2.8 applies to its trace divisor. As the cusps of $X_1(m,n)$ are defined over $\mathbb{Q}(\zeta_n)$, they are finite étale at every prime $p \nmid n$, and if $\operatorname{gon}_F X_1(m,n) > d_m$ and p is odd, the reduction of the trace divisor modulo a prime of F above p is not entirely cuspidal by Proposition 2.5(a).

12.1. The groups $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$.

Proposition 12.1. *There is no elliptic curve over a number field of degree 6 or 8 with a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$, and there is no elliptic curve over an octic field with a subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$ or $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$.*

Proof. In each case we show that the assumptions of Proposition 2.5 hold for a suitable prime p, and that the elliptic curve cannot have good reduction at a prime above p by Lemma 2.6. For $(m,n) = (5,15), (5,20)$ we have $d_m = 2$, and $i(5,15) = 480$ and $i(5,20) = 720$ give $\operatorname{gon}_{\mathbb{C}} X_1(m,n) > 4.76$ and > 7.14. We take $p = 11$, which splits completely in F, so the residue fields are $\mathbb{F}_{11}$ and $\mathbb{F}_{121}$. Their Hasse intervals $[6,18]$ and $[100,144]$ contain no multiple of 75, and the only multiple of 100 is 100 itself, over $\mathbb{F}_{121}$. Then the trace of Frobenius is 22, so the Frobenius is the scalar 11 and the group is $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, which has no point of order 20. For $(m,n) = (3,27)$ we take $p = 2$. We have $d_m = 3$ or 4, and $i(3,27) = 972$ gives $\operatorname{gon}_{\mathbb{C}} X_1(3,27) > 9.64 > 2d_m$. The prime 2 is inert in F, so the residue fields of K above 2 are $\mathbb{F}_4$, $\mathbb{F}_{16}$ and $\mathbb{F}_{64}$, and also $\mathbb{F}_{256}$ when K is an octic field. We check that no elliptic curve over these fields has a subgroup $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$. For the first two this follows from the Hasse bound. Over $\mathbb{F}_{64}$ it would force $E(\mathbb{F}_{64}) = E[9] \simeq (\mathbb{Z}/9\mathbb{Z})^2$ (see the discussion after Lemma 2.6), which has no point of order 27. Over $\mathbb{F}_{256}$ the only multiple of 81 in the Hasse interval is 243, which would require the trace of Frobenius 14, and this is impossible by [Wat69, Theorem 4.1]. □

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

Proposition 12.2. *There is no elliptic curve over a number field of degree 6 or 8 with a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z}$.*

Proof. Let E be an elliptic curve over a number field K of degree 6 or 8 with $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z} \subseteq E(K)$, so that $d_m = [K:F]$ is 3 or 4. Let $X = X_1(3,21)$ over $F = \mathbb{Q}(\zeta_3)$, of genus 25, and let $\mathfrak{p}$ be the prime of F above 2, with residue field $\mathbb{F}_4$. The closed cusps of $X_{\mathbb{F}_4}$ have degrees $1^{24}, 3^8$, so there are $\binom{27}{4} + 24 \cdot 8 = 17742$ effective cuspidal divisors $\overline{C}$ of degree 4 on $X_{\mathbb{F}_4}$, and we compute that $\ell(2\overline{C}) = 1$ for each of them (see also `C3x21/double_cusp_3_21_D4.m`), using the spaces $\Omega(2jP)$ as in Section 5.2. Every effective cuspidal divisor of degree 3 on $X_{\mathbb{F}_4}$ is contained in one of degree 4, so by Remark 7.4 the same holds for the divisors of degree 3. As $\operatorname{rk} J_X(F) = 0$, Lemma 5.3 with $d = d_m$ shows that E has good reduction at some prime of K above $\mathfrak{p}$.

If K is a sextic field, then the residue fields of K above $\mathfrak{p}$ are $\mathbb{F}_4$, $\mathbb{F}_{16}$ and $\mathbb{F}_{64}$. No elliptic curve over $\mathbb{F}_{64}$ has exactly 63 points (see the discussion after Lemma 2.6), and the Hasse intervals of these fields contain no other multiple of 63, so E has bad reduction at every prime of K above 2 by Lemma 2.6, which is a contradiction.

If K is an octic field, we compute that the non-cuspidal closed points of $X_{\mathbb{F}_4}$ of degrees $1,\dots,4$ number $0,0,0,144$, so the trace divisor reduces to one of the 144 non-cuspidal closed points of degree 4. Write $Q_3 = 7Q$ and $Q_7 = 3Q$. The 72 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, have 2 orbits on these points, and we compute that $A_{13}x$ is not principal for a representative x of each orbit. This is a contradiction. □

12.3. **The groups $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/24\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/24\mathbb{Z}$.** Over sextic fields the group $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/24\mathbb{Z}$ is ruled out in Proposition 5.2.

Proposition 12.3. *There is no elliptic curve over a number field of degree 6 or 8 with a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/24\mathbb{Z}$, and there is no elliptic curve over an octic field with a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/24\mathbb{Z}$.*

Proof. For $(m,n) = (3,24)$ let $X = X_1(3,24)$ over $F = \mathbb{Q}(\zeta_3)$, of genus 25, and work at a prime $\mathfrak{p}$ above 7. The closed cusps of $X_{\mathbb{F}_7}$ have degrees $1^{24}, 2^{12}$, the 24 cusps of degree 1 are reductions of F-rational cusps, and the non-cuspidal closed points of degrees $1,\dots,4$ number $0,0,48,456$. As $i(3,24) = 576$ gives $\mathrm{gon}_{\mathbb{C}} X > 5.71 > d_m$, the reduction of the trace divisor at $\mathfrak{p}$ is not entirely cuspidal by Proposition 2.5(a), so it is a point of degree 3, plus the reduction of an F-rational cusp if $d_m = 4$, or a point of degree 4. Writing $R_3 = 8Q$ and $R_8 = 3Q$, the 48 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 orbit on the points of degree 3 and 13 on those of degree 4, and we compute that $A_{13}x$ is not principal for all 14 representatives x, which excludes all these reductions.

For $(m,n) = (4,24)$ let $X = X_1(4,24)$ over $F = \mathbb{Q}(i)$, of genus 33, and work at a prime above 5. As $i(4,24) = 768$, we have $\mathrm{gon}_{\mathbb{C}} X > 7.61 > 4$. The closed cusps of $X_{\mathbb{F}_5}$ have degrees $1^{16}, 2^{24}$, and the non-cuspidal closed points of degrees $1,\dots,4$ number $0,0,0,96$. So the reduction is a single point of degree 4. The 64 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 these points, and we compute that $A_{13}x$ is not principal for a representative x of each of them. □

12.4. **The group $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/18\mathbb{Z}$.** For $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/18\mathbb{Z}$ the Hecke sieve at a single prime does not suffice, and we do not know $J_1(3,18)(\mathbb{Q}(\zeta_3))$ explicitly. Instead we compare the reductions at two primes, using the following lemma, which does not require the Mordell-Weil group to be generated by cuspidal divisor classes. We use the same comparison for $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/16\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ over octic fields below.

Lemma 12.4. *Let X be a curve over a number field F with $J(F)$ 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 $J(F)$, let $H_i \subseteq J(k_i)$ 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 $J(k_1)/H_1$ 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*

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

Proof. Let $y = [D - dc_*] \in J(F)$. The reduction of ey modulo $\mathfrak{p}_1$ lies in H_1, so it is the reduction of some $c \in \mathrm{Cl}^c_F X$. Then $ey - c$ has trivial reduction modulo $\mathfrak{p}_1$, so $ey = c$. Reducing modulo $\mathfrak{p}_2$ gives the claim. □

Let $F = \mathbb{Q}(\zeta_3)$ and let $X = X_1(3,18)$ over F, a curve of genus 10 with $\operatorname{rk} J_X(F) = 0$ [DS17, Theorem 4.1]. We work at primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of F above 7 and 13, with residue fields $\mathbb{F}_7$ and $\mathbb{F}_{13}$. As 7 and 13 both generate $\mathrm{Gal}(\mathbb{Q}(\zeta_{18})/F)$, the Galois orbits of cusps over F stay irreducible modulo $\mathfrak{p}_1$ and $\mathfrak{p}_2$, so at both primes the closed cusps have degrees $1^{18}, 3^6$, and every closed cusp is the reduction of an F-rational cuspidal divisor of the same degree.

To compare the two primes we need to identify the reductions of the cuspidal divisor classes. We use the model of X of [DS16], as implemented in [mdm], 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. A point of this curve with $x = 0$ is $\pm P$, and one with $y = 0$ is P, so $x(Q)$ and $y(Q)$ have no zeros or poles on $Y_1(3,18)$, and the normalization makes a_1 and a_3 regular functions on $Y_1(3,18)$ over $\mathbb{Z}[\zeta_3, \frac{1}{6}]$. The functions

$$a_3, \quad a_1^3 - 27a_3, \quad x(kQ + jP),\ y(kQ + jP) \ \ (1 \le k \le 9,\ 0 \le j \le 2),$$
$$x(kQ) - x(kQ + P) \ \ (1 \le k \le 9), \qquad x(kQ + P) - x(kQ + 2P) \ \ (1 \le k \le 8)$$

are units on $Y_1(3,18)$ over $\mathbb{Z}[\zeta_3, \frac{1}{6}]$. Indeed, the discriminant of the curve is $a_3^3(a_1^3 - 27a_3)$, the points $kQ + jP$ are never equal to O or $\pm P$, and in every fibre $kQ + P \neq \pm kQ$ and $kQ + 2P \neq \pm(kQ + P)$ for these k. So grouping the cusps by their orders of vanishing at these functions gives the same 24 blocks, of degrees $1^{18}, 3^6$, at both primes, each of them the reduction of a Galois orbit of cusps over F. Let H_1 and H_2 be the reductions of $\mathrm{Cl}^c_F X$ modulo $\mathfrak{p}_1$ and $\mathfrak{p}_2$. We compute that H_1 and H_2 both have invariant factors $[3,3,3,3,63,63,63]$ and that $J_X(\mathbb{F}_7)/H_1 \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$. As 7 is odd, unramified in F and a prime of good reduction for X, reduction modulo $\mathfrak{p}_1$ is injective on $J_X(F) = J_X(F)_{\mathrm{tors}}$, so the map ψ of Lemma 12.4 is defined, and the blocks determine it. Fix an F-rational cusp c_*. By Lemma 12.4 with $e = 9$, the reductions $\overline{D}_1$ and $\overline{D}_2$ of an effective F-rational divisor D of degree d satisfy

$$\psi\big(9[\overline{D}_1 - d\overline{c_{*,1}}]\big) = 9[\overline{D}_2 - d\overline{c_{*,2}}]. \tag{11}$$

Proposition 12.5. *The group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 6 or 8.*

Proof. Let D be the trace divisor, of degree $d_m \in \{3,4\}$. As $\mathrm{gon}_F X \ge 6$ [NV26, Table 1], Proposition 2.5(a) excludes the entirely cuspidal reduction at $\mathfrak{p}_1$ and at $\mathfrak{p}_2$. The non-cuspidal closed points of degrees $1, \dots, 4$ number $0, 27, 144, 513$ over $\mathbb{F}_7$ and $0, 54, 846, 7506$ over $\mathbb{F}_{13}$.

Suppose first that $d_m = 3$. Then the non-cuspidal part of the reduction of D modulo $\mathfrak{p}_i$ is either a single point of degree 3 or a point of degree 2, in which case the cuspidal complement is a cusp of degree 1, which is the reduction of an F-rational cusp. The diamond operators act on these points with orbits of length 3. At $\mathfrak{p}_1$ we compute that A_{13} excludes all 9 orbits of points of degree 2 and 36 of the 48 orbits of points of degree 3, and at $\mathfrak{p}_2$ that A_7 excludes all 18 orbits of points of degree 2 and 270 of the 282 orbits of points of degree 3. This leaves 36 possible reductions at each prime, and we compute that none of the $36 \cdot 36$ pairs $(\overline{D}_1, \overline{D}_2)$ satisfies (11) with $d = 3$.

Suppose now that $d_m = 4$, and write $Q' = 6Q$, of order 3. The 27 automorphisms $(P,Q) \mapsto (aP + bQ',\ cP + dQ)$, with $b, c \in \mathbb{Z}/3\mathbb{Z}$, $d \in \{1,5,7\}$ and $a \equiv d^{-1} \pmod 3$, preserve the Weil pairing. At 7 they have 1, 8 and 19 orbits on the points of degrees $2, 3, 4$. We compute that A_{13} or A_{19} excludes the quadratic orbit (with all the possible cuspidal

parts, and also all the sums of two quadratic points), 4 of the cubic orbits and 11 of the quartic orbits. The remaining 4 cubic orbits have length 9, so a point x in them is fixed by an automorphism g of order 3. Its cuspidal complement is the reduction of a single F-rational cusp, and as $\operatorname{gon}_F X \geq 6 > 5$, Lemma 2.9(a) gives $gD = D$, and Lemma 2.8 gives $3 \mid \deg D = 4$, which is impossible. So the reduction of D at 7 is one of the 216 quartic points in the remaining 8 orbits.

These 216 quartic points give 135 distinct classes $9[x - 4\overline{c_*}]$. At 13 we test all the possible reductions against (11) with $d = 4$: 9234 quadratic points with a cuspidal part, 15228 cubic points with a cusp, 1485 pairs of quadratic points and 278 representatives of the quartic points, 26225 cases in all. Only 270 cases of a cubic point with a cusp, involving 54 cubic points in 6 orbits of length 9, and 9 quartic representatives pass. The former are excluded by Lemma 2.9(a) and Lemma 2.8 as at 7, and for the latter we compute that $A_7 x$ is not principal. □

12.5. **The group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$.**

Proposition 12.6. *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 6 or 8.*

Proof. Let $X = X_1(4, 16)$ over $F = \mathbb{Q}(i)$, of genus 13, and let D be the trace divisor, of degree $d_m \in \{3, 4\}$. We have $\operatorname{gon}_F X \geq 8$ by [NV26, Table 1]. We use the primes of F above 5, 3 and 13, with residue fields $\mathbb{F}_5$, $\mathbb{F}_9$ and $\mathbb{F}_{13}$. The cusps are defined over $\mathbb{Q}(\zeta_{16})$, and both 5 and 13 generate $\operatorname{Gal}(\mathbb{Q}(\zeta_{16})/F)$, so the 24 Galois orbits of cusps over F, of degrees $1^{16}, 2^4, 4^4$, stay irreducible modulo the primes above 5 and 13. The prime 3 is inert in F, and its Frobenius σ_9 has order 2 in $\operatorname{Gal}(\mathbb{Q}(\zeta_{16})/F)$, so modulo 3 the 4 quadratic orbits split, and $X_{\mathbb{F}_9}$ has 24 cusps of degree 1. We identify the orbits at all these 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 non-cuspidal closed points of degrees $1, \dots, 4$ number $0, 0, 64, 160$ over $\mathbb{F}_5$ and $0, 0, 320, 1808$ over $\mathbb{F}_9$.

Suppose first that $d_m = 3$. By Proposition 2.5(a), as $\operatorname{gon}_F X > 3$, and by these numbers, the trace divisor reduces modulo the prime above 3 to one of the 320 non-cuspidal closed points x of degree 3 of $X_{\mathbb{F}_9}$, which form 80 diamond orbits. The prime $q = 5$ splits in F, so A_5 annihilates $J_X(F)$, and the standard cusp c_0 satisfies $A_5(c_0) = 0$ by Proposition 2.2(3). Hence $[A_5(x)] = 0$, while we compute that $[A_5(x)] \neq 0$ for one representative x of each diamond orbit, which is a contradiction.

Suppose now that $d_m = 4$. We compute

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

so $J_X(F)/\operatorname{Cl}_F^{\mathrm{c}} X$ is killed by 2, as reduction at 5 is injective on $J_X(F)$. At 5 the reduction of D is a cubic point plus one of the 16 rational cusps, or a quartic point, which gives 1184 possibilities. At 3 it is a cubic point plus one of the 24 cusps of $X_{\mathbb{F}_9}$ of degree 1, or a quartic point. The 64 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, have 5 orbits on the cubic points and 33 on the quartic points at 3, which gives 153 cases. Fix an F-rational cusp c_*. Comparing the classes $2[\overline{D} - 4\overline{c_*}]$ at the two primes by Lemma 12.4 with $e = 2$, only 17 cases at 3 pass, all of them a cubic point x plus a cusp.

The cusps of degree 1 of $X_{\mathbb{F}_9}$ are the 16 reductions of F-rational cusps and the 8 points of the 4 pairs $\{c, c'\}$ into which the quadratic orbits over F split, and σ_5 interchanges the two

points in each pair. By Lemma 2.3, $A_5 c = 0$ for the former, and $A_5 c = (c' - c) + 5\langle 5\rangle (c' - c)$ for the latter. The operator $\langle 5\rangle$ maps each pair to a pair, which we determine from the valuations of the unit functions at Q and at $5Q$, but this leaves open the order of its two cusps. So there are $1 + 8 \cdot 2 = 17$ possible values of A_5 on the cuspidal part, and we compute that in 16 of the 17 cases above, A_5 of the reduction is not principal for any of these values. In the remaining case the class $2[D - 4c_*]$ is the class of $L - 8c_*$ for an explicit F-rational cuspidal divisor L of degree 8, so $2D \sim L$. At a prime above 13 we compute that $\ell(\overline{L}) = 1$ and that the unique effective divisor in $|\overline{L}|$ is a sum of two distinct quartic points. This is a contradiction, as the reduction of $2D$ is an effective divisor in $|\overline{L}|$ with even coefficients. □

12.6. **The group $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.**

Proposition 12.7. *There is no elliptic curve over a number field of degree 6 or 8 with a subgroup isomorphic to $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.*

Proof. Let $X = X_1(6, 12)$ over $F = \mathbb{Q}(\zeta_3)$, of genus 9, with $\operatorname{gon}_F X \geq 6$ [NV26, Table 1], and let D be the trace divisor, of degree 3 or 4. At a prime above 7 the closed cusps have degrees $1^{16}, 2^8$ and are reductions of F-rational cuspidal divisors of the same degree, and the non-cuspidal closed points of degrees $1, \dots, 4$ number $0, 0, 96, 468$. As $\operatorname{gon}_F X > 4$, the entirely cuspidal reduction is excluded by Proposition 2.5(a), so the reduction of D is a cubic point, plus a cusp if $\deg D = 4$, or a quartic point. As $\langle 13\rangle = 1$ on X, we have $A_{13} = T_{13} - 14$, and it annihilates $J_X(F)$ and the F-rational cuspidal divisors. So $[A_{13}x] = 0$ for the cubic point x, and we compute that $A_{13}x$ is not principal for the 48 representatives under the diamond involution. This proves the claim for sextic fields. Over an octic field it follows that the reduction of D at 7 is a single quartic point, with multiplicity 1, and in particular D is a closed point of degree 4.

Fix an F-rational cusp c_*. The cuspidal divisors of degree 0 over F are combinations of the 24 Galois orbits of cusps over F, and we compute

$$J_X(\mathbb{F}_7) \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times (\mathbb{Z}/24\mathbb{Z})^2 \times (\mathbb{Z}/48\mathbb{Z})^2, \qquad \mathrm{Cl}^c_F X \simeq \mathbb{Z}/6\mathbb{Z} \times (\mathbb{Z}/12\mathbb{Z})^3 \times (\mathbb{Z}/24\mathbb{Z})^2,$$

so $J_X(\mathbb{F}_7)$ modulo the reduction of $\mathrm{Cl}^c_F X$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. For a quartic point x at 7 let $r \in \{2, 4\}$ be the order of $[x - 4\overline{c_*}]$ modulo this reduction. Then $r[D - 4c_*] \in \mathrm{Cl}^c_F X$, as in the proof of Lemma 12.4. We compare with the reductions at a prime above 13, where all the 32 cusps are rational and the non-cuspidal closed points of degrees $1, \dots, 4$ number $0, 144, 576, 7116$, testing all the 112020 possible reductions with all the cuspidal parts. Only 12 quartic points at 7 remain, all with $r = 2$. For each of them $2D \sim L$ for an F-rational cuspidal divisor L of degree 8, which we identify using the valuations of 141 integral modular units, and after adding principal divisors of such units we obtain six distinct effective cuspidal divisors $L_1, \dots, L_6$ of degree 8. We compute that $\ell(L_i) = 2$, that $|L_i|$ is a base point free pencil, and that its ramification divisor is a sum of four closed points of degree 8, for each i. If $2D \sim L_i$, then $2D$ is a fibre of the corresponding map $X \to \mathbb{P}^1$, so every point of D is a ramification point. This is impossible, as D is a closed point of degree 4 and the ramification divisor is a sum of closed points of degree 8. □

12.7. **The group $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.** For $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ we need the rank over $\mathbb{Q}(\zeta_5)$ of Jacobians which are not covered by [DS17, Theorem 4.1]. By the argument of the proof of Lemma 5.1, if B is a quotient of $J_1(N)$ over $\mathbb{Q}$ and F is an abelian field, then $B(F)$ is finite if, for every newform f occurring in B and every character χ of $\mathrm{Gal}(F/\mathbb{Q})$, the twist $\rho_f \otimes \chi$ is the representation of a newform g with $L(g, 1) \neq 0$.

Lemma 12.8. *Let $F = \mathbb{Q}(\zeta_5)$. The Jacobian of the modular curve $X(10)$ over F, parametrizing elliptic curves with a basis of the 10-torsion with fixed Weil pairing, has rank 0 over F.*

Proof. Let $H = \langle 11 \rangle \subseteq (\mathbb{Z}/100\mathbb{Z})^\times$, of order 10. By the description of [DS17, Section 2], $X(10)$ is isomorphic over F to $X_1(100)/H$, which is defined over $\mathbb{Q}$. The non-trivial even characters modulo 100 that are trivial on H factor through $(\mathbb{Z}/10\mathbb{Z})^\times$, so the newforms occurring in the Jacobian of $X_1(100)/H$ have level dividing 100 and character trivial or quadratic of conductor 5. Their local representations at 5 have conductor exponent at most 2 and tame determinant, so they are tamely ramified, as a wildly ramified two-dimensional representation with conductor exponent at most 2 has a wildly ramified determinant. So their twists by characters χ modulo 5 again have level dividing 100 and even character modulo 10. We compute that for each of the six Galois orbits of even characters modulo 100, of orders $1, 20, 10, 5, 4, 2$, the winding submodule is the full space of cusp forms, of relative dimensions $7, 13, 12, 12, 9, 6$, which add up to the genus 231 of $X_1(100)$ when counted with the degrees $1, 8, 4, 4, 2, 1$ of the fields of values. So every newform of level dividing 100 has non-zero L-value at 1, and the lemma follows from the argument above. □

Proposition 12.9. *There is no elliptic curve over an octic field with a subgroup isomorphic to $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.*

Proof. Let $F = \mathbb{Q}(\zeta_5)$ and $X = X(10)_F$, a curve of genus 13 with 36 cusps, all defined over F, and $\operatorname{gon}_{\mathbb{C}} X \geq \lceil \frac{325}{2^{15}} \cdot 360 \rceil = 4$. A trace divisor D has degree 2 over F. We use the following model. Let

$$\begin{aligned} a(t) &= t^{20} - 228t^{15} + 494t^{10} + 228t^5 + 1, \\ b(t) &= t^{30} + 522t^{25} - 10005t^{20} - 10005t^{10} - 522t^5 + 1, \\ h(t) &= t^5(t^{10} + 11t^5 - 1)^5, \end{aligned}$$

so that $b^2 - a^3 = 1728h$. The elliptic curve $y^2 = x^3 - 27a(t)x + 54b(t)$ over $F(t)$ has j-invariant $-a^3/h$, of degree 60, and its 5-torsion representation is ± 1, so a quadratic twist of it has full 5-torsion, and $F(t)$ is the function field of $X(5)_F$. Adjoining the 2-torsion, we obtain the function field $F(t)(r, s)$, $r^3 - 27a(t)r + 54b(t) = 0$, $s^2 = -3r^2 + 108a(t)$, of X, and check that it has genus 13.

Let $C \subseteq J_X(F)$ be generated by the classes of the differences of the cusps, and fix a cusp c_*. We work at primes above 11 and 31, which split completely in F, at which reduction is injective on $J_X(F)$ by Lemma 12.8. We compute

$$J_X(\mathbb{F}_{11}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times (\mathbb{Z}/30\mathbb{Z})^4 \times (\mathbb{Z}/90\mathbb{Z})^4,$$

in which the reduction of C is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times (\mathbb{Z}/30\mathbb{Z})^8$, so $3J_X(F) \subseteq C$. We identify the cusps at the two primes using the valuations of the units t, $t - u$ for the ten roots u of $u^{10} + 11u^5 - 1$, and the differences of the roots of the cubic, which are units on the integral model away from 2 and 5. There are no non-cuspidal points of X over $\mathbb{F}_{11}$ and $\mathbb{F}_{31}$. By Proposition 2.5(a), as $\operatorname{gon}_F X \geq 4 > 2$, the reduction of D at 11 is not entirely cuspidal. So D reduces to one of the 150 non-cuspidal closed points P of degree 2 of $X_{\mathbb{F}_{11}}$, and similarly to one of the 810 such points Q of $X_{\mathbb{F}_{31}}$, and $3[P - 2\overline{c_*}]$ and $3[Q - 2\overline{c_*}]$ are the reductions of the same element of C. We compute that this holds for none of the $150 \cdot 810$ pairs. □

12.8. **The group $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$.**

Lemma 12.10. *Let $F = \mathbb{Q}(\zeta_5)$. Then $J_1(25)(F)$ is finite of odd order.*

Proof. The non-zero spaces of cusp forms of weight 2 on $\Gamma_1(25)$ have characters of order 5 or 10. Let f be a newform in them with character ε and let χ be a character modulo 5. The local representation of f at 5 has conductor exponent 2, which is the codimension of the inertia invariants plus the Swan conductor. If the Swan conductor were 2, the inertia invariants would be the whole space, which is impossible, as an unramified representation has Swan conductor 0. So the Swan conductor is at most 1. Twisting by the tame character χ does not change the Swan conductor, which depends only on the action of the wild inertia group, so $f \otimes \chi$ has conductor exponent at most 3 at 5, and it is unramified elsewhere. So $f \otimes \chi$ has level dividing 125, and its character $\varepsilon\chi^2$ is trivial on 26, as $26 \equiv 1 \pmod{25}$. We compute that the spaces of cusp forms of level 125 with characters of orders 5 and 10 trivial on 26 are generated by their winding elements. So $L(f \otimes \chi, 1) \neq 0$ for all f and χ, and $J_1(25)(F)$ is finite by the argument above. The prime 11 splits completely in F, and we compute that $\#J_1(25)(\mathbb{F}_{11}) = 5014032203125$, which is odd. As reduction at 11 is injective on the torsion, $J_1(25)(F)$ has odd order. □

Proposition 12.11. *There is no elliptic curve over an octic field with a subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$.*

Proof. Let $F = \mathbb{Q}(\zeta_5)$, so $[K : F] = 2$, and let D be the trace divisor on $X = X_1(25)_F$ of the point of order 25, obtained by forgetting the point of order 5. It is an effective F-rational divisor of degree 2. The prime above 2 in F has residue field $\mathbb{F}_{16}$, and we compute $\#X(\mathbb{F}_{16}) = 18$, all of these points being cusps. These 18 cusps are reductions of F-rational cusps: the 10 cusps on the Néron 25-gon are rational, the 8 cusps on the Néron 5-gon with 5-torsion in μ_5 are defined over F, and the other 10 cusps form two orbits of length 5 under the Frobenius 16, which generates $\mathrm{Gal}(\mathbb{Q}(\zeta_{25})/F)$.

If D reduces to a sum of cusps, let C be its lift. Then $[D - C] \in J_1(25)(F)$ reduces to 0, so $D \sim C$ by Lemma 12.10, as reduction is injective on the odd torsion. We compute that $\dim \Omega(\overline{C}) = 10$ for all the 171 effective divisors $\overline{C}$ of degree 2 supported on the 18 cusps, so $\ell(\overline{C}) = 1$, and $\ell(C) = 1$ by semicontinuity. So $D = C$, which is a contradiction.

So the reduction of D is a closed point P of degree 2, corresponding to an elliptic curve over $\mathbb{F}_{256}$ with a subgroup $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$. By the Hasse bound its order is 250, and its group is $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$. We find 4 such curves, giving 100 closed points of degree 2 of X over $\mathbb{F}_{16}$, in 12 diamond orbits. At the prime 11, A_{11} annihilates $J_1(25)(F)$ and the rational cusp c_0, so $[A_{11}P] = 0$, and hence also $[(\langle 6\rangle - 1)A_{11}P] = 0$. It suffices to test this consequence, and we compute that $(\langle 6\rangle - 1)A_{11}P$ is not principal for the representatives P of all 12 orbits, which is a contradiction. □

12.9. **The group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$.** For $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$ over octic fields we use the following elliptic curve.

Lemma 12.12. *Let $F = \mathbb{Q}(i)$ and let Z be the normalization of the curve*

$$\frac{16(w^2 + 16)^3}{w^4} = \frac{(t^2 + 10t + 5)^3}{t}.$$

Then Z has genus 1, and $Z(F)$ consists of 4 points with $t \in \{0, \infty\}$ or $w \in \{0, \infty\}$ and 4 points at which both sides are equal to 1728.

Proof. We check that the maps

$$t = \frac{(x-3)^2(x+2)}{(x+1)^2}, \qquad w = \frac{y(x+1)^2}{4(x+2)}$$

define a birational map from $E' : y^2 = (x-3)(x+1)(x+2)$ to Z. The curves E' and its quadratic twist by -1 have rank 0 over $\mathbb{Q}$, by 2-descent, so $E'(F)$ is finite. Reduction modulo the prime 3, which is inert in F, injects $E'(F)_{\mathrm{tors}}$ into $E'(\mathbb{F}_9) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, and of the three points of order 2 only $(-1,0)$ is divisible by 2 over F, so $E'(F) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, consisting of O, $(-2,0)$, $(-1,0)$, $(3,0)$ and $(-1 \pm 2i, \pm(4 \mp 2i))$. The first four map to the points where t or w is 0 or ∞, and the last four to $t = -11 \pm 2i$, $w = \pm 2i$, where both sides equal 1728. □

Proposition 12.13. *There is no elliptic curve over a number field of degree* 6 *or* 8 *with a subgroup isomorphic to* $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$.

Proof. Let $F = \mathbb{Q}(i)$ and $X = X_1(4,20)$ over F, of genus 25, with $\operatorname{gon}_{\mathbb{C}} X > \frac{325}{2^{15}} \cdot 576 > 5$. Let D be the trace divisor, of degree 3 or 4. We work at the prime 3, which is inert in F, with residue field $\mathbb{F}_9$. The closed cusps of $X_{\mathbb{F}_9}$ have degrees $1^{24}, 2^{12}$, the 24 cusps of degree 1 are reductions of F-rational cusps, and the non-cuspidal closed points of degrees $1, \dots, 4$ number $0, 96, 320, 888$. The entirely cuspidal reduction is excluded by Proposition 2.5(a), as $\operatorname{gon}_{\mathbb{C}} X > 5$, so the non-cuspidal part of the reduction of D is a point of degree 2, 3 or 4, or a sum of two points of degree 2. Let G be the group of 96 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 $(-I,-1)$. It has $2,4,12$ orbits on the points of degrees $2,3,4$. For $q \equiv 1 \pmod 4$, $q \nmid 60$, the operator A_q annihilates $J_X(F)$, and $q = 13, 17$ are admissible for cuspidal parts of degree at most 1, and $q = 29 \equiv 9 \pmod{20}$ for those of degree at most 2. We compute that $A_q x$ is not principal for one of these q for all the representatives of the points of degree 2 and 3 and for 10 of the 12 quartic representatives, and that for the sums $x + x'$ of two quadratic points, with x one of the 2 representatives and x' any of the 96 quadratic points, $A_q(x + x')$ is not principal except in 2 cases. This proves the claim for sextic fields.

In the remaining cases over an octic field the reduction $\overline{D}$ has no cuspidal part. If $g \in G$ fixes $\overline{D}$, then $gD = D$ by Lemma 2.9(a) with $C = 0$, as $\operatorname{gon}_F X > 4$. So D is invariant under the stabilizer of $\overline{D}$ in G, and by Lemma 2.8 the order of this stabilizer divides $\deg D = 4$. The 2 remaining quartic points lie in orbits of length 12, so their stabilizers have order 8, which is impossible. The 2 remaining sums of two quadratic points have stabilizers of order 4, which are conjugate in G to the subgroup H_1 generated by the automorphisms with parameters $\left(\begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}, 1\right)$ and $\left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, 2\right)$. Replacing D by its image under an element of G, which is again a trace divisor, we may assume that D is H_1-invariant. Then D is a single H_1-orbit of a non-CM point, so its image on X/H_1 is an F-rational point. We check that there is a non-constant map $X/H_1 \to Z$ to the curve of Lemma 12.12, preserving the j-invariant. Here $t = b - 11 - 1/b$, where $y^2 + (1-b)xy - by = x^3 - bx^2$ is the Tate normal form of (E, Q_5). As t does not change when Q_5 is replaced by a multiple, it is a parameter on $X_0(5)$, and $j = (t^2 + 10t + 5)^3/t$. Further, $w = 4(x(U) - x(T))/(x(P_2) - x(P_2 + T))$, where $U = P - Q_4$, $T = 2U$ and $P_2 = -2Q_4$, with $j = 16(w^2 + 16)^3/w^4$. So the image of D on Z is an F-rational point which is not a cusp, hence it has $j = 1728$ by Lemma 12.12, and the elliptic curve has complex multiplication, contradicting Lemma 2.11. □

12.10. **The group $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.**

Proposition 12.14. *There is no elliptic curve over an octic field with a subgroup isomorphic to $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.*

Proof. By the Weil pairing $K \supseteq \mathbb{Q}(\zeta_8)$, and a basis of $E[8]$ with fixed Weil pairing gives a non-cuspidal point of $X(8)$ of degree at most 2 over $\mathbb{Q}(\zeta_8)$. But Bars, Kontogeorgis and Xarles [BKX13, Remark 5.3] showed that the only points of degree at most 2 over $\mathbb{Q}(\zeta_8)$ on $X(8)$ are the 24 cusps. □

13. The sporadic points

We now describe the sporadic torsion groups in degree $d \in \{6, 7, 8, 9\}$, that is, the groups in $\Phi(d) \setminus \Phi^\infty(d)$. Table 5 lists the elliptic curves with these torsion groups that we give explicitly, and the results in which they are given. Each subsection after Section 13.1 treats one modular curve in degrees in which the corresponding group is sporadic, and three of them also treat degrees in which it does not occur: $X_1(36)$ in degree 6, $X_1(39)$ in degrees 6 and 7, and $X_1(2, 26)$ in degrees 6, 7 and 8. In most cases we determine all the points of degree d on the curve, which shows that the curves we give are the only ones with the given torsion group and excludes the groups properly containing it.

For the curves $X_1(N)$ we argue as follows in degree d. We work at a prime p at which reduction is injective on $J_1(N)(\mathbb{Q})$, which is finite and generated by rational cuspidal divisor classes [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], and, except for $X_1(25)$, the fact that $\operatorname{gon}_{\mathbb{Q}} X_1(N) > d$, so by Lemma 2.7 distinct effective rational divisors of degree d have distinct classes. As in Section 10, we identify the Galois orbits of cusps over $\mathbb{Q}$ with their reductions using the valuations of the modular units b and b^4/Δ of the Tate normal form, which are units on $Y_1(N)$ over $\mathbb{Z}[\frac{1}{N}]$. We write $H \subseteq J_1(N)(\mathbb{F}_p)$ for the subgroup generated by the reductions of the rational cuspidal divisors of degree 0, which is the reduction of $J_1(N)(\mathbb{Q})$. Let D be an effective rational divisor of degree d on $X_1(N)$ whose support contains no cusp. Then $[\overline{D} - d\overline{c_0}] \in H$, and if this is also the class of the reduction of a known effective rational divisor A of degree d, then $D = A$. In particular, $\overline{D}$ is not the reduction of an effective rational cuspidal divisor. Finally, the diamond operators change neither the elliptic curve nor the residue field of a closed point. So if every such D is a diamond translate of one of the known closed points of degree d, then, as $X_1(N)$ is a fine moduli space, every elliptic curve over a number field of degree d with a point of order N is, together with its field, isomorphic to a pair given by one of these points, and its torsion group is the one given in Section 13.1. In the proofs for the curves $X_1(N)$ below, D and H always have this meaning.

13.1. **Realizations.** Recall that for b, c in a field, the curve

$$E(b, c): \quad y^2 + (1 - c)xy - by = x^3 - bx^2 \tag{12}$$

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 $Y_1(N)$, and that the curve

$$E'(b, c): \quad y^2 = x^3 + cx^2 + (1 - b - c)bx \tag{13}$$

has the point $P = (0, 0)$ of order 2 and the point $Q = (b, b)$.

The curve $E_{25}^{(6)}$ of Proposition 13.1, the curves of Propositions 13.2 and 13.3 and the first eight curves of Proposition 13.5 come from the lists of low degree points of van Hoeij [vH14].

For a point (x, y) on the model of $X_1(N)$ of [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 elliptic curve (12), on which the point $(0, 0)$ has order N.

In the proofs of Propositions 13.2, 13.3 and 13.5 we bound $E(K)_{\mathrm{tors}}$ by reduction at primes $\wp$ of K above odd primes p unramified in K at which E has good reduction. Table 6 lists them as $(p, f_\wp, \#\widetilde{E}(\mathbb{F}_\wp))$, with $f_\wp$ the residue degree of $\wp$. As $E(K)_{\mathrm{tors}}$ injects into $\widetilde{E}(\mathbb{F}_\wp)$, its order divides the gcd of these numbers, which in each case is N.

d	G	K	E	
6	$\mathbb{Z}/25\mathbb{Z}$	6.2.28037.1	$E_{25}^{(6)}$	Proposition 13.1
	$\mathbb{Z}/37\mathbb{Z}$	6.6.300125.1	E_{37}, $j = -9317$	Proposition 13.11
	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$	6.0.419904.2	$E_{4,12}$, base change of 162.d2	Proposition 13.1
	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$	6.2.231852.1	$E_{2,24}$	Proposition 13.20
7	$\mathbb{Z}/25\mathbb{Z}$	7.1.184607.1	E_{25}	Proposition 13.2
	$\mathbb{Z}/33\mathbb{Z}$	7.3.792873.1	E_{33}	
	$\mathbb{Z}/36\mathbb{Z}$	7.1.1609956.1	E_{36}	
	$\mathbb{Z}/36\mathbb{Z}$	7.3.3192732.1	E'_{36}	
8	$\mathbb{Z}/33\mathbb{Z}$	8.2.7486875.1		Proposition 13.3
	$\mathbb{Z}/34\mathbb{Z}$	8.0.1257728.1	$j = 1728$	
	$\mathbb{Z}/34\mathbb{Z}$	8.0.1265625.1	j of degree 2	
	$\mathbb{Z}/34\mathbb{Z}$	8.4.19360000.1	j of degree 4	
	$\mathbb{Z}/35\mathbb{Z}$	8.4.31878125.1		
	$\mathbb{Z}/39\mathbb{Z}$	8.0.1601613.1	$j = 0$	
	$\mathbb{Z}/40\mathbb{Z}$	8.2.31500500.1		
	$\mathbb{Z}/42\mathbb{Z}$	8.4.23040000.1		
	$\mathbb{Z}/42\mathbb{Z}$	8.2.7993287.1	two curves, 2-isogenous	
	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$	$\mathbb{Q}(\zeta_{20})$	$j = 1728$	Proposition 13.4
	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$	8.0.2313441.1	$j = 1331/8$	Proposition 13.23
9	$\mathbb{Z}/29\mathbb{Z}$	9.5.507490937.1		Proposition 13.5
	$\mathbb{Z}/31\mathbb{Z}$	9.3.114479303.1	base change from a cubic subfield	
	$\mathbb{Z}/32\mathbb{Z}$	9.1.32344469.1		
	$\mathbb{Z}/33\mathbb{Z}$	9.3.393718863.1		
	$\mathbb{Z}/34\mathbb{Z}$	9.3.131123051.1		
	$\mathbb{Z}/39\mathbb{Z}$	9.3.195458751.1	base change from a cubic subfield	
	$\mathbb{Z}/40\mathbb{Z}$	9.1.30626693.1		
	$\mathbb{Z}/42\mathbb{Z}$	9.3.272097792.1	base change of 162.c3	
	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$	9.3.157505216.1	$E_{2,26}$, base change from a cubic subfield	

TABLE 5. The elliptic curves E over number fields K of degree d with $E(K)_{\mathrm{tors}} \simeq G$ given in this section, for the sporadic torsion groups G in degree d. The curves with $j = 0$ and $j = 1728$ have complex multiplication, in accordance with [CCRS14].

Proposition 13.1. (1) *Let* $K_{25}^{(6)} = \mathbb{Q}(x,y)$ *with* $x^3 - x^2 + 1 = 0$ *and* $y^2 + (x^2 - 2x - 1)y + x = 0$, *which is the field 6.2.28037.1, and let* $E_{25}^{(6)} = E(b,c)$, *with* b *and* c *given by the formulas above. Then* $(0,0)$ *has order* 25 *and* $E_{25}^{(6)}(K_{25}^{(6)})_{\mathrm{tors}} \simeq \mathbb{Z}/25\mathbb{Z}$.

(2) *Let* $K_{4,12} = \mathbb{Q}(\alpha, i)$ *with* $\alpha^3 - 3\alpha - 4 = 0$, *which is the field 6.0.419904.2, and let* $E_{4,12}$ *be the base change of 162.d2:* $y^2 + xy + y = x^3 - x^2 + 4x - 1$ *to* $K_{4,12}$. *Then* $E_{4,12}(K_{4,12})_{\mathrm{tors}} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.

Proof. The curve in (2) was found by González-Jiménez and Najman [GJN23]. We verify both claims directly in Magma [BCP97]. □

Proposition 13.2. *Let* N, f *and* y *be one of the following:*

$$\begin{aligned}
N = 25: &\quad f = x^7 + x^6 - x^5 - x^4 + x^2 + x - 1, \qquad y = x^2 + x,\\
N = 33: &\quad f = x^7 - 6x^6 + 9x^5 - 5x^3 - x + 1,\\
&\quad y = \tfrac{1}{3}\big(-3x^6 + 16x^5 - 17x^4 - 9x^3 + 11x^2 + 3x + 4\big),\\
N = 36: &\quad f = x^7 - x^6 + 2x^5 - 4x^4 + 3x^3 + 2x^2 - 2x + 1,\\
&\quad y = \tfrac{1}{6}\big(-2x^6 + 3x^5 - 5x^4 + 11x^3 - 9x^2 + 4x + 7\big),\\
N = 36: &\quad f = x^7 - 2x^6 + 4x^5 - x^4 - 8x^3 + 2x^2 + 5x + 1,\\
&\quad y = \tfrac{1}{2}\big(-13x^6 + 36x^5 - 79x^4 + 73x^3 + 51x^2 - 65x - 16\big),
\end{aligned}$$

where x *is a root of* f, *and put* $K = \mathbb{Q}(x)$ *and* $E = E(b,c)$. *Then* $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/N\mathbb{Z}$. *The fields* K *are listed, in the same order, in Table 5, and we denote the four pairs* (K,E) *by* (K_{25}, E_{25}), (K_{33}, E_{33}), (K_{36}, E_{36}) *and* (K'_{36}, E'_{36}).

Proof. We compute that $(0,0)$ has order N and that E has good reduction at the primes listed in Table 6, with the numbers of points given there. □

Proposition 13.3. *Let N, f and g be one of the following, let x be a root of f and y the corresponding root of g, and put $K = \mathbb{Q}(x, y)$ and $E = E(b, c)$.*

N	f *and* g
33	$x^4 - 3x^3 + 3x^2 - 3x + 1$
	$y^2 + (x^3 - 3x^2 + x - 3)y + 2x^2 - x + 2$
34	$x^8 - 6x^7 + 16x^6 - 28x^5 + 42x^4 - 44x^3 + 27x^2 - 8x + 1$
	$157y + 3x^7 + 53x^6 - 320x^5 + 716x^4 - 1036x^3 + 1516x^2 - 1197x + 64$
34	$x^8 + x^7 - x^5 - x^4 - x^3 + x + 1$
	$y + x^7 - x^5 - x^4 - x^3 + 1$
34	$x^8 - 2x^6 + 8x^4 - 7x^2 + 1$
	$3y + 3x^7 - 5x^5 + 23x^3 - 16x$
35	$x^8 - 10x^7 + 36x^6 - 55x^5 + 19x^4 + 35x^3 - 25x^2 - 5x + 5$
	$y + 6x^7 - 65x^6 + 268x^5 - 531x^4 + 473x^3 - 49x^2 - 177x + 74$
39	$x^8 - 4x^7 + 10x^6 - 25x^5 + 37x^4 - 25x^3 + 10x^2 - 4x + 1$
	$3y - 2x^7 + 6x^6 - 13x^5 + 34x^4 - 33x^3 - x^2 - 3x$
40	$5x^8 - 15x^7 + 15x^6 - 10x^5 + 13x^4 - 8x^3 - 7x^2 + 10x - 2$
	$6653y - 5455x^7 + 25010x^6 - 27370x^5 + 10105x^4 - 24648x^3$
	$+ 20135x^2 + 10773x - 14311$
42	$x^8 - 4x^7 + 6x^5 - 3x^2 - 2x + 1$
	$7y + 3x^7 - 11x^6 - 3x^5 + 16x^4 - x^3 + 7x^2 - 12x - 6$

Then $[K : \mathbb{Q}] = 8$ and $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/N\mathbb{Z}$. The fields K are listed, in the same order, in Table 5.

Proof. For $N = 33$ the element $x + y$ generates K, with minimal polynomial $t^8 - 15t^7 + 95t^6 - 331t^5 + 741t^4 - 1100t^3 + 1009t^2 - 688t + 359$. We compute that $(0, 0)$ has order N on E and that E has good reduction at the primes listed in Table 6, with the numbers of points given there. □

Van Hoeij's list contains two more octic points on $X_1(42)$, for which the same holds. They are defined over the same field 8.2.7993287.1, and the two elliptic curves are 2-isogenous but not isomorphic.

Proposition 13.4. *Let $z = \zeta_{20}$, $i = z^5$ and $K = \mathbb{Q}(z)$. The elliptic curve $E : y^2 + (1 - i)xy - iy = x^3 - ix^2$ over K has $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.*

Proof. The curve has j-invariant 1728, and this example is contained in [CCRS14, Section 4.8]. The points $P = (-1 + z^2 + z^3 - z^4, -1 + z^4 - z^7)$ and $Q = (1 + z^5, -2)$ have orders 5 and 10, and the Weil pairing of P and $2Q$ is the primitive fifth root of unity $-z^6$, as we compute, so they generate a subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$. The reductions of E modulo the primes $(41, z - 2)$ and $(61, z - 8)$ of K are good, with 50 points each, so $\#E(K)_{\mathrm{tors}}$ divides 50. □

Proposition 13.5. *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	$x^9-8x^8+23x^7-26x^6+2x^5+17x^4-11x^3+2x^2+1$
	$y-x^8+6x^7-11x^6+4x^5+6x^4-6x^3+3x^2$
31	$x^9-2x^8+x^6-x^5+14x^4-28x^3+19x^2-2x-1$
	$119y-9x^8+28x^7-16x^6-46x^5+11x^4-125x^3+440x^2-386x-150$
32	$x^9-x^7-x^6+2x^5+2x^4-x^3-2x^2+1$
	$y-x^7-x^6+x^5+x^4-x^3-3x^2-x+1$
33	$x^9-5x^8-3x^7+25x^6+20x^5-19x^4-15x^3+4x^2+2x-1$
	$543y-113x^8+638x^7+71x^6-3534x^5-544x^4+5545x^3+1342x^2-2083x-197$
34	$x^9-2x^8-x^7+3x^6+2x^5+x^3-2x-1$
	$y+40x^8-108x^7+36x^6+94x^5+14x^4-9x^3+47x^2-33x-57$
39	$x^9-5x^8+8x^7-10x^5+4x^4+4x^2-4x+1$
	$3y+7x^8-33x^7+46x^6+15x^5-67x^4+7x^3+2x^2+29x-18$
40	$x^9-6x^8+14x^7-17x^6+12x^5-4x^4-x^3+3x^2-2x+1$
	$y+x^2-2x$
42	$x^9+7x^6-3x^4+4x^3-3x^2+3x-1$
	$4y-x^8-x^7+x^6-10x^5-4x^4+5x^3-13x^2+2x-7$

Then $[K:\mathbb{Q}]=9$ and $E(K)_{\mathrm{tors}}\simeq\mathbb{Z}/N\mathbb{Z}$. The fields K are listed, in the same order, in Table 5. We denote the points of $X_1(31)$, $X_1(33)$ and $X_1(39)$ given by the second, fourth and sixth entry by x_{31}, x_{33} and x_{39}.

Moreover, let $K_{2,26}=\mathbb{Q}(z)$, where $z^9+5z^8+15z^7+14z^6-14z^5-25z^4-7z^3+5z^2+4z+1=0$, which is the field 9.3.157505216.1, and put

$$\begin{aligned}907b &= 62z^8+1386z^7+6639z^6+18950z^5+20738z^4-6786z^3\\ &\quad -25017z^2-14822z-2411,\\ 907c &= -3864z^8-22538z^7-75946z^6-112918z^5-25630z^4+94470z^3\\ &\quad +104296z^2+46530z+8797.\end{aligned}$$

Then the elliptic curve $E_{2,26}=E'(b,c)$ over $K_{2,26}$, as in (13), satisfies $E_{2,26}(K_{2,26})_{\mathrm{tors}}\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/26\mathbb{Z}$, generated by $(0,0)$ and (b,b). We denote by $x_{2,26}$ the corresponding point of $X_1(2,26)$.

Proof. The list of [vH14] contains 19 points of degree 9 on the curves $X_1(N)$ with $N\geq 29$, all of which we check. For the first eight entries above we compute that f is irreducible, that $(0,0)$ has order N on E, and that E has good reduction at the primes listed in Table 6, with the numbers of points given there. For $E_{2,26}$ we check that $(0,0)$ and (b,b) have orders 2 and 26 and that $(0,0)\neq 13(b,b)$. The polynomial defining $K_{2,26}$ is irreducible modulo 3, and $E_{2,26}$ has good reduction at the prime above 3, with 19604 points over $\mathbb{F}_{3^9}$. Modulo 7 the polynomial factors into irreducible factors of degrees $2,2,2,3$, and $E_{2,26}$ has good reduction at the four primes above 7, with 52, 52, 52 and 364 points. Hence $\#E_{2,26}(K_{2,26})_{\mathrm{tors}}$ divides $\gcd(19604,52,364)=52$. □

d	N	$(p, f_\wp, \#\widetilde{E}(\mathbb{F}_\wp))$
7	25	$(3,7,2175)$, $(5,2,25)$
	33	$(5,3,132)$, $(13,7,62752635)$
	36	$(29,1,36)$
	36	$(5,3,108)$, $(19,2,360)$
8	33	$(7,8,5760579)$, $(13,8,815675619)$
	34	$(5,2,34)$
	34	$(7,4,2448)$, $(11,2,102)$, $(13,4,28900)$
	34	$(7,4,2482)$, $(13,4,28424)$
	35	$(7,8,5763520)$, $(11,2,105)$
	39	$(7,2,39)$
	40	$(3,4,80)$, $(31,3,29560)$
	42	$(41,1,42)$
9	29	$(3,3,29)$
	31	$(53,1,62)$, $(83,1,93)$
	32	$(3,3,32)$
	33	$(5,2,33)$
	34	$(11,3,1292)$, $(13,4,28594)$
	39	$(13,2,156)$, $(19,3,6981)$
	40	$(3,4,80)$, $(5,3,120)$
	42	$(37,1,42)$

TABLE 6. Primes $\wp$ of good reduction of the elliptic curves E over the fields K of degree d of Propositions 13.2, 13.3 and 13.5, in the order of these propositions, above odd primes p unramified in K, with the residue degree $f_\wp$ and $\#\widetilde{E}(\mathbb{F}_\wp)$.

We also check that the curves with $N = 31$ and $N = 39$, and $E_{2,26}$, are base changes of elliptic curves over the cubic subfields of their fields of definition of discriminants -23, -31 and -44, and that the curve with $N = 42$ is the base change of 162.c3, which has torsion $\mathbb{Z}/21\mathbb{Z}$ over the cubic field of discriminant 81 [Naj16]. A second elliptic curve with a point of order 42 over the same field is the base change of a curve over its cubic subfield of discriminant -648.

13.2. **The curve $X_1(25)$.**

Proposition 13.6. *Every closed point of degree 7 on $X_1(25)$ is in the orbit under $\Delta(25)$ of the point (x, y) of Proposition 13.2. Hence, if E is an elliptic curve over a septic field K with a point of order 25, then $(K, E) \simeq (K_{25}, E_{25})$ and $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/25\mathbb{Z}$. In particular, $\mathbb{Z}/50\mathbb{Z}$, $\mathbb{Z}/75\mathbb{Z}$, $\mathbb{Z}/125\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over a septic field.*

Proof. Let $X = X_1(25)$ and $J = J_1(25)$. As $\mathrm{gon}_{\mathbb{Q}} X = 5 < 7$ [DvH14, Theorem 4 and Table 1], we use part (2) of Lemma 2.7. By [DvH14, Theorem 3], X has only finitely many closed points of degree 7, so by Hilbert's irreducibility theorem there is no rational function of degree 7 on X. By [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], $J(\mathbb{Q})$ is cyclic of order 227555 and generated by rational cuspidal divisor classes. As this order is odd, reduction at 2 is injective on $J(\mathbb{Q})$, and we compute $J(\mathbb{F}_2) \simeq \mathbb{Z}/227555\mathbb{Z}$, so reduction

is an isomorphism $J(\mathbb{Q}) \simeq J(\mathbb{F}_2)$. The cusps are defined over $\mathbb{Q}(\zeta_{25})$ and 2 is a primitive root modulo 25, so every closed cusp of $X_{\mathbb{F}_2}$ is the reduction of a Galois orbit of cusps of the same degree. The closed cusps of $X_{\mathbb{F}_2}$ have degrees $1^{10}, 4^2, 10$.

Let D be a closed point of degree 7 on X. If $\overline{D}$ is the reduction of an effective rational divisor A of degree 7, then $D \sim A$, so $D = A$ by Lemma 2.7. If $\overline{D}$ is cuspidal, it is the reduction of a rational cuspidal divisor A, which is impossible as D is not cuspidal. The non-cuspidal closed points of $X_{\mathbb{F}_2}$ of degrees $1, \dots, 7$ number $0, 0, 0, 0, 1, 5, 10$, so the non-cuspidal part of $\overline{D}$ is a single closed point of degree 5, 6 or 7. If it has degree 5, the cuspidal part has degree 2, and we compute that for all 55 effective cuspidal divisors C of degree 2 the class of $P_5 + C - 7\overline{c_0}$ is also the class of an effective cuspidal divisor of degree 7, so this case is impossible as before.

The sextic point of Proposition 13.1(1) reduces modulo 2 to a closed point of degree 6, and we compute that the reductions of its translates by $\Delta(25)$ are all the 5 closed points of degree 6 of $X_{\mathbb{F}_2}$. So if $\overline{D}$ is a closed point of degree 6 plus a rational cusp, it is the reduction of a reducible effective rational divisor of degree 7, which is impossible. Similarly, the reductions of the translates of the septic point of Proposition 13.2 are all the 10 closed points of degree 7 of $X_{\mathbb{F}_2}$, so if $\overline{D}$ is a closed point of degree 7, then D is one of these translates. The rest of the proof is as explained at the beginning of the section. □

13.3. **The curve $X_1(33)$.**

Proposition 13.7. *Let $d \in \{7, 8, 9\}$. Every effective rational divisor of degree d on $X_1(33)$ whose support contains no cusp is one of the 10, 5, respectively 10 closed points of degree d in the $\Delta(33)$-orbit of the point of level 33 of Proposition 13.2, Proposition 13.3, respectively Proposition 13.5 (the point x_{33}). Hence, if E is an elliptic curve over a number field K of degree d with a point of order 33, then (K, E) is isomorphic to the pair with $N = 33$ of the same proposition, and $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/33\mathbb{Z}$. In particular, $\mathbb{Z}/66\mathbb{Z}$, $\mathbb{Z}/99\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/33\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over a number field of degree d.*

Proof. Let $X = X_1(33)$. We have $\mathrm{gon}_{\mathbb{Q}} X = 10$ [DvH14, Theorem 4 and Table 1], and $J_X(\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/42373650\mathbb{Z}$ [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2]. We work at $p = 2$. The Galois orbits of cusps over $\mathbb{Q}$ have degrees $1^{10}, 2^5, 10^2$, and modulo 2 one of the orbits of degree 10 splits into two closed points of degree 5, so the closed cusps of $X_{\mathbb{F}_2}$ have degrees $1^{10}, 2^5, 5^2, 10$, and a cuspidal divisor on $X_{\mathbb{F}_2}$ need not be the reduction of a rational one. We compute that $J_X(\mathbb{F}_2) \simeq \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/42373650\mathbb{Z}$ and that H has invariant factors $[5, 42373650]$, so reduction modulo 2 is injective on $J_X(\mathbb{Q})$, including its 2-primary part. The non-cuspidal closed points of $X_{\mathbb{F}_2}$ of degrees $1, \dots, 9$ number $0, 0, 0, 0, 2, 20, 30, 25, 50$, so the reduction of an effective divisor of degree 9 contains at most one of them.

We run through all the 155770 effective divisors of degree 9 on $X_{\mathbb{F}_2}$ with at most one non-cuspidal point, and compute which of them have class, normalized at a rational cusp, in H. These are the 144250 reductions of effective rational cuspidal divisors, the 600 divisors $\overline{S} + \overline{C'}$ with S one of the ten closed points of degree 7 of the statement and C' an effective rational cuspidal divisor of degree 2, the 50 divisors $\overline{O} + \overline{c}$ with O one of the five closed points of degree 8 of the statement and c a rational cusp, the reductions of the ten closed points of degree 9 of the statement, and ten further closed points of degree 9, whose classes are the reductions of $[C_i - 9c_0]$ for explicit $\mathbb{Z}$-linear combinations $C_1, \dots, C_{10}$ of degree 9 of rational cuspidal divisors.

Let D be as in the statement, let c_* be a rational cusp, and put $D_9 = D + (9-d)c_*$. The reduction of D_9 is one of these divisors, so by the injectivity D_9 is linearly equivalent to an effective rational cuspidal divisor, to a divisor $S + C'$ or $O + c$ as above, to one of the ten closed points of degree 9 of the statement, or to one of the C_i. In the first four cases Lemma 2.7 shows that D_9 is equal to this divisor. As the support of D contains no cusp, the first case is impossible, and comparing the parts of the supports outside the cusps in the next three cases gives $D = S$ (so $d = 7$), $D = O$ (so $d = 8$), respectively that D is one of the ten closed points of degree 9 (so $d = 9$). It remains to show that no effective rational divisor is linearly equivalent to one of the C_i, and for this it suffices that $\ell(\overline{C_i}) = 0$ on $X_{\mathbb{F}_5}$, by semicontinuity. Let $A = \sum_c \max_i\{0, v_c(C_i)\}c$, of degree 48, so that $B_i = A - C_i$ is effective of degree 39. By Riemann-Roch $\ell(A) = 48 + 1 - 21 = 28$, and we compute a basis of $L(\overline{A})$ over $\mathbb{F}_5$ and check that the 28×39 matrix of its restrictions to $\overline{B_i}$ has rank 28 for every i, so $L(\overline{C_i}) = L(\overline{A} - \overline{B_i}) = 0$. The rest of the proof is as explained at the beginning of the section. □

13.4. **The curve $X_1(34)$.**

Proposition 13.8. *Every effective rational divisor of degree 8 on $X_1(34)$ with non-cuspidal support is one of the 7 closed points in the $\Delta(34)$-orbits of the three octic points of level 34 of Proposition 13.3, which have lengths 1, 2 and 4. Hence, if E is an elliptic curve over an octic field K with a point of order 34, then (K, E) is isomorphic to one of the three pairs of Proposition 13.3 with $N = 34$, and $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/34\mathbb{Z}$. In particular, $\mathbb{Z}/68\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/34\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over an octic field.*

Proof. We work at $p = 3$. By [DEvH+21, Table 2], $J_1(34)(\mathbb{Q}) \simeq \mathbb{Z}/8760\mathbb{Z} \times \mathbb{Z}/595680\mathbb{Z}$, and we compute $J_1(34)(\mathbb{F}_3) \simeq (\mathbb{Z}/4\mathbb{Z})^3 \times \mathbb{Z}/8760\mathbb{Z} \times \mathbb{Z}/1191360\mathbb{Z}$, in which H has invariants $[8760, 595680]$, so reduction is injective on $J_1(34)(\mathbb{Q})$. We have $\mathrm{gon}_{\mathbb{Q}} X_1(34) = 10$ [DvH14, Theorem 4 and Table 1]. The Galois orbits of cusps over $\mathbb{Q}$ and the closed cusps over $\mathbb{F}_3$ both have degrees $1^{16}, 8^2$, so the entirely cuspidal reduction is excluded. The non-cuspidal closed points of degrees $1, \dots, 8$ number $0, 0, 0, 26, 32, 80, 256, 734$, so the non-cuspidal part of $\overline{D}$ is a single closed point of degree $4, \dots, 8$, or a sum of two quartic points. All the cuspidal parts have class in H. Of these single points and the 351 sums of two quartic points, exactly one octic point and 6 sums of two quartic points have class in H. The three octic points of level 34 of Proposition 13.3 reduce to an octic point, to twice a quartic point and to a sum of two distinct quartic points, respectively, and their diamond translates give exactly these 7 classes. The rest of the proof is as explained at the beginning of the section, and the three pairs are not isomorphic, as their j-invariants have degrees 1, 2 and 4. □

13.5. **The curve $X_1(35)$.**

Proposition 13.9. *Every effective rational divisor of degree 8 on $X_1(35)$ with non-cuspidal support is one of the 6 translates under $\Delta(35)$ of the octic point of Proposition 13.3. Hence, if E is an elliptic curve over an octic field K with a point of order 35, then (K, E) is isomorphic to the pair of Proposition 13.3, and $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/35\mathbb{Z}$. In particular, $\mathbb{Z}/70\mathbb{Z}$, $\mathbb{Z}/105\mathbb{Z}$, $\mathbb{Z}/175\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/35\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over an octic field.*

Proof. The argument in the proof of Proposition 6.6 applies to $d = 8$, as $\mathrm{gon}_{\mathbb{Q}} X_1(35) = 12 > 8$. Let D be an effective rational divisor of degree 8 on $X_1(35)$ whose support contains no cusp. Its reduction modulo 3 is not cuspidal, its non-cuspidal part is one of the 5961

divisors of degree at most 9 tested there, and the only ones of these with class in the reduction of $J_1(35)(\mathbb{Q})$ are the reductions of the 6 translates under $\Delta(35)$ of the octic point B of Proposition 13.3. So D and a translate δB have the same reduction, hence $D \sim \delta B$, as reduction modulo 3 is injective on $J_1(35)(\mathbb{Q})$, and $D = \delta B$ by Lemma 2.7. The rest of the proof is as explained at the beginning of the section. □

13.6. **The curve $X_1(36)$.**

Proposition 13.10. *The group $\mathbb{Z}/36\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a sextic field. The non-cuspidal closed points of degree 7 on $X_1(36)$ are the points in the two $\Delta(36)$-orbits of the septic points of Proposition 13.2. Hence, if E is an elliptic curve over a septic field K with a point of order 36, then (K, E) is isomorphic to (K_{36}, E_{36}) or (K'_{36}, E'_{36}), and $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/36\mathbb{Z}$. In particular, $\mathbb{Z}/72\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over a septic field.*

Proof. Let $X = X_1(36)$ and $J = J_1(36)$, and work at $p = 5$. We have $\mathrm{gon}_{\mathbb{Q}} X = 8$ [DvH14, Theorem 4 and Table 1], and $J(\mathbb{Q})$ has invariant factors $[12, 252, 7812]$ and is generated by rational cuspidal divisor classes [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2]. The Galois orbits of cusps over $\mathbb{Q}$ have degrees $1^9, 2^6, 3, 4, 6^2$, and the closed cusps of $X_{\mathbb{F}_5}$ have degrees $1^{15}, 2^5, 3, 6^2$. The computations in this proof were done in one interactive Magma session, whose log of the class computations and exported certificate are kept in the repository. We compute

$$J(\mathbb{F}_5) \simeq (\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/12\mathbb{Z})^2 \times \mathbb{Z}/36\mathbb{Z} \times (\mathbb{Z}/7812\mathbb{Z})^2,$$

and that the reductions of the rational cuspidal divisors of degree 0 generate a subgroup H with invariant factors $[12, 252, 7812]$, so H is the injective image of $J(\mathbb{Q})$.

Let D be a non-cuspidal closed point of degree 7 on X. As explained at the beginning of the section, it suffices to show that the class of $\overline{D} - 7\overline{c_0}$, which lies in H, is the class of the reduction of an effective rational cuspidal divisor or of a translate of one of the two septic points. There are 19159 effective rational cuspidal divisors of degree 7, with distinct classes, and among the 188865 effective cuspidal divisors of degree 7 on $X_{\mathbb{F}_5}$, those with class in H are exactly these. So $\overline{D}$ is not cuspidal. The non-cuspidal closed points of $X_{\mathbb{F}_5}$ of degrees $1, \dots, 7$ number $0, 0, 48, 144, 660, 2856, 10728$, so the non-cuspidal part of $\overline{D}$ is a single closed point of degree $3, \dots, 7$, a sum of two cubic points (possibly equal) or a sum of a cubic and a quartic point. We take the first point up to $\Delta(36)$ and allow all the cuspidal parts of the complementary degree.

To speed up the cases of degree 6 and 7 we first use the map $\pi : X_1(36) \to X_1(2, 18)$ given by the 2-isogeny $E \to E/\langle 18P \rangle$, as in the proof of Lemma 3.3. By [DEvH+21, Proposition 4.16 and Table 3], $J_1(2, 18)(\mathbb{Q})$ has invariant factors $[2, 42, 126]$ and is generated by rational cuspidal divisor classes. We compute $J_1(2, 18)(\mathbb{F}_5) \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z} \times \mathbb{Z}/252\mathbb{Z}$. As 5 generates $(\mathbb{Z}/18\mathbb{Z})^\times$, the closed cusps of $X_1(2, 18)_{\mathbb{F}_5}$ are reductions of Galois orbits of the same degree, and their classes generate the reduction H' of $J_1(2, 18)(\mathbb{Q})$. Every cusp class lies in H', so the class of the push-forward of the non-cuspidal part of $\overline{D}$ (minus the appropriate multiple of a rational cusp) must lie in H'. The cases that pass this test are then tested in $J(\mathbb{F}_5)$. The results are the following, and we replay the class computations of

the certificate independently with integer arithmetic (see the log):

type of the non-cuspidal part	cases	passing the test on $X_1(2,18)$	remaining
[3]	8	–	0
[4]	24	–	0
[5]	110	–	0
[3, 3]	384	–	0
[3, 4]	1152	–	1
[6]	480	54	0
[7]	1788	150	1

Here "remaining" counts the cases with a cuspidal part such that the class of $\overline{D} - 7\overline{c_0}$ lies in H and is not the class of the reduction of an effective rational cuspidal divisor. The two septic points of Proposition 13.2 reduce to a closed point of degree 7 and to the sum of a cubic and a quartic point, respectively, and each of their $\Delta(36)$-orbits gives 6 distinct classes. The two remaining cases are among these 12 classes. So D is a translate of one of the two septic points, and the rest of the proof for septic fields is as explained at the beginning of the section.

Finally, let D be the trace divisor of a point of order 36 over a sextic field, and let c_* be a rational cusp. The computations above apply to the effective rational divisor $D + c_*$ of degree 7, as they allow all the cuspidal parts, and by the point counts the reduction of $D + c_*$ is cuspidal or its non-cuspidal part has one of the types [3], [4], [5], [3, 3] and [6]. So by the computations above $[\overline{D} + \overline{c_*} - 7\overline{c_0}]$ is the class of the reduction of an effective rational cuspidal divisor A of degree 7. Then $D + c_* \sim A$, and $D + c_* = A$ by Lemma 2.7, as $\operatorname{gon}_{\mathbb{Q}} X = 8 > 7$, which is impossible, as the support of D contains no cusp. □

13.7. **The curve $X_1(37)$.**

Proposition 13.11. *Let $E_{1225} : y^2 = g(x) = x^3 - 10395x + 444150$, which is a model of 1225.b2, let w be a root of*

$$f_{37} = x^6 - 3150x^5 + 796635x^4 - 75770100x^3 + 3111596775x^2 - 44606598750x - 85333003875,$$

put $K_{37} := \mathbb{Q}(w)$ and $\delta := g(w)$, and let

$$E_{37} : \quad y^2 = x^3 - 10395\delta^2 x + 444150\delta^3.$$

Then K_{37} is the cyclic totally real sextic field 6.6.300125.1, the point $(\delta w, \delta^2)$ of E_{37} has order 37 and $E_{37}(K_{37})_{\mathrm{tors}} \simeq \mathbb{Z}/37\mathbb{Z}$. If K is a sextic field and E/K is an elliptic curve with a point of order 37, then the pair (K, E) is isomorphic to (K_{37}, E_{37}). In particular, no group properly containing $\mathbb{Z}/37\mathbb{Z}$ is a sextic torsion group.

Proof. The map $(x, y) \mapsto (\delta x, \delta^2 y)$ is an isomorphism from $E^* : \delta y^2 = g(x)$ to E_{37}, which sends $P = (w, 1)$ to $(\delta w, \delta^2)$. We compute that K_{37} is the cyclic totally real field 6.6.300125.1, and we compute that P has order 37 and that the irreducible factors over $\mathbb{Q}$ of the 37-division polynomial of E_{1225} have degrees $6, 6, 6, 666$.

As E^* is a quadratic twist of E_{1225}, the x-coordinates x_r of the points rP, for $1 \le r \le 18$, are 18 distinct roots of this division polynomial. They lie in K_{37}, so they have degree at most 6, and hence they are exactly the 18 roots of the three sextic factors. In particular $\mathbb{Q}(x_r) = K_{37}$ for every r. Writing $rP = (x_r, y_r)$, we have $\delta y_r^2 = g(x_r)$ with $y_r \neq 0$, as rP does not have order 2.

Now let (K, E) be as in the statement. By [DKSS23, Proposition 1.4] we have $j(E) = -9317 = j(E_{1225})$, so E is isomorphic to $E_d : dy^2 = g(x)$ for some $d \in K^\times$. A point of order 37 on E_d has x-coordinate $x' \in K$, which is a root of the 37-division polynomial of E_{1225} of degree at most 6, hence a root of one of the sextic factors. So $K = \mathbb{Q}(x')$, and there is an isomorphism $\tau : K \to K_{37}$ with $\tau(x') = x_r$ for some r. As d and $g(x')$ differ by a non-zero square in K, the elements $\tau(d)$ and $g(x_r) = \delta y_r^2$ differ by a square in K_{37}, so $E_d^\tau \simeq E^* \simeq E_{37}$ over K_{37}. Thus $(K, E) \simeq (K_{37}, E_{37})$.

Finally, we compute that f_{37} has roots modulo 29 and modulo 41, and that at the corresponding primes of degree 1 of K_{37}, which are of good reduction, the reduction of E_{37} has exactly 37 points. As reduction is injective on the torsion of order prime to the residue characteristic, $\#E_{37}(K_{37})_{\mathrm{tors}}$ divides 37. □

13.8. **The curve $X_1(39)$.** Let $X = X_1(39)$. By [DEvH+21, Theorem 3.1(2), Corollary 4.14 and Table 2], the group $J_X(\mathbb{Q}) \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/31122\mathbb{Z} \times \mathbb{Z}/3236688\mathbb{Z}$ is generated by rational cuspidal divisor classes, and $\mathrm{gon}_{\mathbb{Q}} X = 14$ [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. We compute that the non-cuspidal closed points of $X_{\mathbb{F}_2}$ of degrees $1, \dots, 8$ number $0, 0, 0, 0, 0, 12, 0, 49$, that the 12 points of degree 6 form one diamond orbit, and that the 49 points of degree 8 form 5 diamond orbits.

Lemma 13.12. *Reduction modulo 2 is injective on $J_1(39)(\mathbb{Q})$.*

Proof. As $J_1(39)(\mathbb{Q})$ is generated by rational cuspidal divisor classes, it suffices that the reductions of these classes generate a subgroup of $J_1(39)(\mathbb{F}_2)$ of order $\#J_1(39)(\mathbb{Q})$, and we compute that this is the case. □

Hence no effective rational divisor D of degree $d < 14$ on X whose support contains no cusp reduces to a cuspidal divisor modulo 2: otherwise D and an effective rational cuspidal divisor C have the same reduction, so $D \sim C$ by Lemma 13.12, and $D = C$ by Lemma 2.7, as $\mathrm{gon}_{\mathbb{Q}} X = 14 > d$. For $d \geq 7$ we cannot use Proposition 2.5(b) instead, as it would require $\mathrm{gon}_{\mathbb{Q}} X > 2d$.

Proposition 13.13. *The group $\mathbb{Z}/39\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree 6 or 7.*

Proof. Let D be the trace divisor on X of a point of order 39 over a number field of degree $d \in \{6, 7\}$. By the above and the point counts, the reduction of D modulo 2 is $D' + C'$, where D' is one of the 12 points of degree 6, and $C' = 0$ if $d = 6$ and C' is the reduction of a rational cusp if $d = 7$. So every prime $q \nmid 78$ is admissible for C', and as the 12 points form one diamond orbit, it suffices to take one of them as D'. We compute that $[A_q(D')] \neq 0$ for $q = 5$ or $q = 7$, so the Hecke sieve at 2 excludes this reduction. □

Proposition 13.14. *The octic point of level 39 of Proposition 13.3 is the only effective rational divisor of degree 8 on $X_1(39)$ with non-cuspidal support. Hence, if E is an elliptic curve over an octic field K with a point of order 39, then (K, E) is isomorphic to the pair of Proposition 13.3, and $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/39\mathbb{Z}$. In particular, $\mathbb{Z}/78\mathbb{Z}$, $\mathbb{Z}/117\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/39\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over an octic field.*

Proof. We work at $p = 2$, where reduction is injective on $J_X(\mathbb{Q})$ by Lemma 13.12. By the above, $\overline{D}$ is not cuspidal, so by the point counts it is a sextic point plus the reduction of

a rational cuspidal divisor of degree 2, or an octic point. As A_5 annihilates $J_X(\mathbb{Q})$ and the rational cuspidal divisors, $[A_5P] = 0$ for the non-cuspidal part P. We compute that A_5P is not principal for the representatives of the sextic orbit and of 4 of the octic orbits. The fifth octic orbit consists of a single point, which is the reduction of the octic point of Proposition 13.3. The rest of the proof is as explained at the beginning of the section. □

Lemma 13.15. *Let E be an elliptic curve over a nonic field K with a point P of order 39, and let D be the trace divisor of (E, P). Then K has a unique prime above 2, it is unramified of residue degree 9, E has good ordinary reduction there, and D reduces to a closed point of degree 9 of $X_1(39)_{\mathbb{F}_2}$.*

Proof. By the above, D does not reduce to a cuspidal divisor, so by the point counts the non-cuspidal part of its reduction is a point of degree 6, 8 or 9, and its cuspidal part is the reduction of a rational cuspidal divisor. The computations of Proposition 13.14, with the operator A_5, which kills the rational cuspidal complements, exclude the orbit of degree 6 and four of the five orbits of degree 8. The fifth consists of the reduction of the octic point O of Proposition 13.14, and if D reduced to $\overline{O} + \overline{c}$ with c a rational cusp, then $D \sim O + c$ by Lemma 13.12, so $D = O + c$ by Lemma 2.7, which is impossible. So D reduces to a single closed point of degree 9, which implies the other assertions, as the prime-to-2 part of the torsion reduces injectively. The supersingular curves over $\mathbb{F}_{2^9}$ have 481, 513 or 545 points, none divisible by 39, so the reduction is ordinary. □

Proposition 13.16. *The group $\mathbb{Z}/117\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a nonic field.*

Proof. Let E have a point of order 117 over K, and apply Lemma 13.15 to P three times this point. Then 117 divides $\#E(\mathbb{F}_{2^9})$, which lies in the Hasse interval $[468, 558]$, so $\#E(\mathbb{F}_{2^9}) = 468$. We compute that the elliptic curves over $\mathbb{F}_{2^9}$ with 468 points are three curves with j-invariants in $\mathbb{F}_8$, whose points of order 39 give 36 points of $X_1(39)$ over $\mathbb{F}_{2^9}$, in four Frobenius orbits. These are exactly the reductions of the four closed points of degree 9 in the diamond orbit of x_{39}. So the trace divisor D of the point of order 39 of Lemma 13.15 and a diamond translate of x_{39} have the same reduction, hence are linearly equivalent by Lemma 13.12, and equal by Lemma 2.7. Thus E is isomorphic over K to the curve of Proposition 13.5, whose torsion is $\mathbb{Z}/39\mathbb{Z}$, which is a contradiction. □

Proposition 13.17. *The group $\mathbb{Z}/78\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a nonic field.*

Proof. Let E/K have a point Q of order 78, put $P = 2Q$ and $R = 39Q$, and let $\phi : E \to E' = E/\langle R\rangle$, which is defined over K, and $P' = \phi(P)$, of order 39. Let D and D' be the trace divisors of (E, P) and (E', P'). As the curve of Proposition 13.5 with a point of order 39 has torsion $\mathbb{Z}/39\mathbb{Z}$, neither D nor D' is a diamond translate of x_{39}, so by Lemma 13.15 the prime $\mathfrak{p}$ of K above 2 is unique and unramified with residue field $\mathbb{F}_{2^9}$, E and E' have good ordinary reduction at $\mathfrak{p}$, and D and D' reduce to closed points of degree 9. 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, 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 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 $\langle 2\rangle D$. By Lemma 13.12 and Lemma 2.7 we get $D' = D$ or $D' = \langle 2\rangle D$.

Hence the K-points (E', P') and (E, P), respectively $(E, 2P)$, of $X_1(39)$ lie above the same closed point with residue field K, so they differ by an automorphism σ of K. As $X_1(39)$ is a fine moduli space, $E' \simeq E^\sigma$ over K, and ϕ gives a K-rational isogeny $\psi : E \to E^\sigma$ of degree 2. The order r of σ divides $\#\operatorname{Aut}(K)$, which divides $[K : \mathbb{Q}] = 9$, so r is odd. The composition $\psi^{\sigma^{r-1}} \circ \cdots \circ \psi^\sigma \circ \psi$ is an endomorphism of E defined over K of degree 2^r, so by Lemma 2.12 it is multiplication by an integer, and 2^r is a square, which is impossible as r is odd. □

13.9. **The curve $X_1(40)$.**

Proposition 13.18. *Every effective rational divisor of degree 8 on $X_1(40)$ with non-cuspidal support is a translate under $\Delta(40)$ of the octic point of Proposition 13.3. Hence, if E is an elliptic curve over an octic field K with a point of order 40, then (K, E) is isomorphic to the pair of Proposition 13.3, and $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/40\mathbb{Z}$. In particular, $\mathbb{Z}/80\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/40\mathbb{Z}$ are not subgroups of the torsion of an elliptic curve over an octic field.*

Proof. We work at $p = 3$. By [DEvH+21, Table 2], $J_1(40)(\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z} \times \mathbb{Z}/895440\mathbb{Z}$, and $\operatorname{gon}_{\mathbb{Q}} X_1(40) = 12$ [DvH14, Theorem 4 and Table 1]. We compute $\#J_1(40)(\mathbb{F}_3) = 31579088486400$, and that H has order $6876979200 = \#J_1(40)(\mathbb{Q})$, so reduction is injective on $J_1(40)(\mathbb{Q})$. The 21 Galois orbits of cusps over $\mathbb{Q}$ have degrees $1^{12}, 2^2, 4^6, 8$, and the closed cusps of $X_1(40)_{\mathbb{F}_3}$ have degrees $1^{12}, 2^6, 4^6$. The effective cuspidal divisors of degree 8 over $\mathbb{F}_3$ give 194142 classes, of which 113912 are reductions of effective rational cuspidal divisors, and exactly these lie in H. So $\overline{D}$ is not cuspidal. The non-cuspidal closed points of degrees $1, \ldots, 8$ number $0, 0, 0, 32, 72, 80, 408, 708$, with $4, 9, 10, 51, 96$ diamond orbits in degrees $4, \ldots, 8$, so the non-cuspidal part of $\overline{D}$ is a single closed point of degree $4, \ldots, 8$ or a sum of two quartic points. Allowing all the cuspidal parts, none of the single points gives a class in H, and of the 128 sums of a representative quartic point and any quartic point, exactly one does. The octic point of Proposition 13.3 reduces to a sum of two distinct quartic points, and its translates give 4 distinct classes, which contain this one. The rest of the proof is as explained at the beginning of the section. □

13.10. **The curve $X_1(2, 24)$.** Proposition 13.19 shows that the non-cuspidal sextic points on $X_1(2, 24)$ form at most two diamond orbits, and Proposition 13.20 shows that both occur.

Proposition 13.19. *Let $X = X_1(2, 24)$. There are $\mathbb{Q}$-rational cuspidal divisors L_1, L_2 of degree 6 on X with the following property. If D is an effective $\mathbb{Q}$-rational divisor of degree 6 on X with non-cuspidal support, then $\delta D \sim L_i$ for some $\delta \in \Delta(24)$ and some $i \in \{1, 2\}$. Each of the linear systems $|L_1|$ and $|L_2|$ contains at most one effective divisor.*

Proof. The curve X has genus 13, its Jacobian has rank 0 and $J(\mathbb{Q}) = \mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}} X \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z} \times \mathbb{Z}/240\mathbb{Z}$ [DEvH+21, Theorem 3.1(3), Proposition 4.16 and Table 3], and $\operatorname{gon}_{\mathbb{F}_5} X > 6$ [DS17, proof of Proposition 5.5], so $\operatorname{gon}_{\mathbb{Q}} X > 6$. We work at $p = 5$.

Let D be an effective $\mathbb{Q}$-rational divisor of degree 6 on X with non-cuspidal support. If D were not a single closed point of degree 6, its support would contain a closed point of degree at most 3, which would give an elliptic curve over a number field of degree at most 3 with a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$, which is impossible [Maz77, Kam92a, DEvH+21]. So D is a closed point of degree 6, and hence the trace divisor of a point of $Y_1(2, 24)(K)$, where K is its residue field. In particular the totally cuspidal reduction of D is excluded by Proposition 2.5.

As in Section 11, the orders of vanishing at the cusps of the units b, $b(1-b-c)$, $c^2-4b(1-b-c)$ and $x(jQ)$, $1 \le j \le 12$, do not change under reduction modulo 5, and grouping the cusps by them gives 19 blocks $B_1, \dots, B_{19}$, each of which is a sum of Galois orbits of cusps over $\mathbb{Q}$, of degrees $1^8, 2^6, 4^5$. Let c_* be a rational cusp that forms a block by itself, and let $G \subseteq J(\mathbb{F}_5)$ be the subgroup generated by the classes $[\overline{B_j} - \deg(B_j)\overline{c_*}]$. We compute that G has invariant factors $[2, 4, 4, 120, 240]$, so G is the reduction of $J(\mathbb{Q})$, and that $J(\mathbb{F}_5)/G \simeq (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z}$. The sets $\mathcal{S}_j$ defined after Lemma 5.6 have $1, 5, 23, 75$ elements for $j = 0, 1, 2, 3$.

Over $\mathbb{F}_5$ the numbers of non-cuspidal closed points of degrees $1, \dots, 6$ are 0, 0, 16, 96, 672, 2712, so the non-cuspidal part Z of the reduction of D has type [3], [4], [5], [6] or [3, 3]. Up to the diamond operators there are 4, 32, 168, 684 and 64 such Z, respectively, and we compute that the condition $[Z - (\deg Z)\overline{c_*}] \bmod G \in \mathcal{S}_{6-\deg Z}$ holds for exactly two of them, both of type [6]. As G is the reduction of $J(\mathbb{Q}) = \mathrm{Cl}^c_{\mathbb{Q}} X$, their classes $[Z - 6\overline{c_*}]$ are the reductions of the classes $[L_1 - 6c_*]$ and $[L_2 - 6c_*]$ of rational cuspidal divisors L_1 and L_2 of degree 6.

So, after applying a diamond operator, D reduces to one of these two points, and then $[D - L_i]$ is a rational torsion class with trivial reduction, so $D \sim L_i$. As $\mathrm{gon}_{\mathbb{Q}} X > 6$, each of the linear systems $|L_1|$ and $|L_2|$ contains at most one effective divisor. □

Proposition 13.20. *Let $K_{2,24} = \mathbb{Q}(w)$ with $w^6 - 2w^4 + 2w^2 - 3 = 0$, which is the field 6.2.231852.1, and let $E_{2,24} = E'(b, c)$ as in (13) with*

$$b = \tfrac{1}{32}\big(3w^5+7w^4-24w^3-15w^2+21w+18\big), \qquad c = \tfrac{1}{16}\big(-7w^5+5w^4+24w^3-5w^2-17w-2\big).$$

(1) *The point $Q = (b, b)$ has order 24, and $E_{2,24}(K_{2,24})_{\mathrm{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$.*
(2) *The curve $X_1(2, 24)$ has exactly 8 non-cuspidal closed points of degree 6. They form two orbits of length 4 under $\Delta(24)$, and they all come from $E_{2,24}$.*
(3) *If K is a sextic field and E/K is an elliptic curve with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \subseteq E(K)$, then $(K, E) \simeq (K_{2,24}, E_{2,24})$.*

The curve $E_{2,24}$ has no complex multiplication, its j-invariant generates the cubic subfield of $K_{2,24}$, which has discriminant -139, and its conductor has norm 6.

Proof. Write $K = K_{2,24}$ and $E = E_{2,24}$. We compute (1) and the last sentence. Moreover $\#\operatorname{Aut}(K) = 2$: as $h(t) = t^3 - 2t^2 + 2t - 3$ is strictly increasing (its derivative $3t^2 - 4t + 2$ has no real roots) and $h(0) < 0$, it has exactly one real root, which is positive, so the defining polynomial $h(x^2)$ of w has exactly two real roots $\pm w_0$. Hence, in a real embedding of K, every automorphism of K sends w to $\pm w$, and $w \mapsto -w$ is one.

We prove (2). There are 32 pairs (P', Q') generating $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$ (16 choices of Q' and 2 of $P' \notin \langle Q' \rangle$), and two of them give the same point of $Y_1(2, 24)$ if and only if they differ by an automorphism of E. As $\operatorname{Aut}(E) = \{\pm 1\}$ and $(-P', -Q') = (P', -Q')$, they give 16 distinct K-points of $Y_1(2, 24)$. Each of them lies on a closed point of degree 6, as $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \notin \Phi(d)$ for $d \in \{1, 2, 3\}$, whose residue field is isomorphic to K, and such a closed point has exactly $\#\operatorname{Aut}(K) = 2$ points with values in K. Hence E gives at least 8 closed points of degree 6. On the other hand, by Proposition 13.19, for every non-cuspidal closed point D of degree 6 there are $\delta \in \Delta(24)$ and i with $\delta D \sim L_i$, and $|L_i|$ contains at most one effective divisor, so there are at most $2 \cdot \#\Delta(24) = 8$ such points. Hence there are exactly 8, they form two orbits of length 4, and they all come from E, and the 16 points above are all the K-points on these 8 closed points.

For (3), let (K', E') be as in (3). It gives a non-cuspidal closed point of degree 6 on $X_1(2,24)$, which is one of the 8 points of (2), so its residue field is isomorphic to K. Choosing such an isomorphism, we obtain a K-point on one of these closed points, which is one of the 16 points above, all of which come from E. As $X_1(2,24)$ is a fine moduli space, $(K', E') \simeq (K, E)$. □

Remark 13.21. The sextic points on $X_1(37)$ and $X_1(2,24)$ are sporadic, since both curves have only finitely many points of degree at most 6: for $X_1(37)$ this follows from $\operatorname{gon}_{\mathbb{Q}} X_1(37) = 18$ [DvH14, Theorem 1] and Frey's theorem [Fre94], and for $X_1(2,24)$ it follows from $\operatorname{rk} J_1(2,24)(\mathbb{Q}) = 0$ and $\operatorname{gon}_{\mathbb{Q}} X_1(2,24) > 6$ (see the proof of Proposition 13.19) by [DS17, Proposition 2.3]. The conductor of $E_{2,24}$ is very small, as for the curve with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ over a quintic field in [Naj26a]. The points of degree 6 that give the four sporadic groups in degree 6 are listed in [Naj26b], as the points 1.25.6.a, 1.37.6.a, 4.12.6.a and 2.24.6.a.

13.11. **The curve $X_1(2,26)$.**

Proposition 13.22. *The group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$ is not a subgroup of the torsion of an elliptic curve over a number field of degree $d \in \{6,7,8\}$, and hence, by Lemma 3.3, neither is $\mathbb{Z}/52\mathbb{Z}$. Every closed point of degree 9 of $Y_1(2,26)$ lies in the orbit of the point $x_{2,26}$ of Proposition 13.5 under the level automorphisms. This orbit has 12 elements.*

Proof. Let $X = X_1(2,26)$, and let D be the trace divisor of a point of $Y_1(2,26)$ over a number field of degree $d \in \{6,7,8\}$, or a closed point of degree $d = 9$ of $Y_1(2,26)$. The group $J_X(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/266\mathbb{Z} \times \mathbb{Z}/3990\mathbb{Z} \times \mathbb{Z}/11970\mathbb{Z}$ is finite and generated by rational cuspidal divisors [DEvH+21, Theorem 3.1(3), Proposition 4.16 and Table 3], and $\operatorname{gon}_{\mathbb{Q}} X \geq 12$ [NV26, Table 1]. The closed cusps of $X_{\mathbb{F}_3}$ have degrees $1^{18}, 3^6$, and the 18 cusps of degree 1 are reductions of rational cusps. We compute that their differences generate a subgroup of $J_X(\mathbb{F}_3) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/70\mathbb{Z} \times \mathbb{Z}/1330\mathbb{Z} \times \mathbb{Z}/3990\mathbb{Z} \times \mathbb{Z}/11970\mathbb{Z}$ with the invariant factors of $J_X(\mathbb{Q})$, which is therefore the reduction of $J_X(\mathbb{Q})$, of index 350. By Table 4 and Proposition 2.5(a), the reduction of D is $x + C$, with x a non-cuspidal closed point of degree $e \in \{5, \dots, d\}$ and C cuspidal of degree $d - e$. For $e = 5, \dots, 8$ there are 6, 26, 48 and 159 diamond orbit representatives x, and none of them, completed by any effective cuspidal divisor of degree at most $9 - e$, has class, normalized at a rational cusp, in the reduction of $J_X(\mathbb{Q})$. This proves the first assertion, and for $d = 9$ it shows that $e = 9$. The 2328 closed points of degree 9 form 66 orbits under the 36 level automorphisms, and the three maps to $X_1(26)$ which keep Q, $P + Q$ and $P + 14Q$ leave two of them, of which one has class outside the reduction of $J_X(\mathbb{Q})$. The other is the orbit of the reduction of $x_{2,26}$, which has degree 9 as the field of definition of $x_{2,26}$ is inert at 3. So after applying a level automorphism, D and $x_{2,26}$ have the same reduction, and $D = x_{2,26}$ by injectivity and Lemma 2.7. The stabilizer of the reduction has order 3, and every element of it fixes $x_{2,26}$ by Lemma 2.9, so the orbit of $x_{2,26}$ has $36/3 = 12$ elements. □

13.12. **The curve $X_1(3,15)$.**

Proposition 13.23. *Let $z^2 + z + 1 = 0$, $F = \mathbb{Q}(z)$ and $K = F(w)$ with $w^4 - 5w^3 + 8w^2 - 6w + 3 = 0$, which is the octic field 8.0.2313441.1. Let*

$$a_1 = \tfrac{1}{6}\big((-7z-8)w^3 + (23z+34)w^2 + (-8z-43)w\big) + \tfrac{1}{2}(-3z+10),$$
$$a_3 = \tfrac{1}{12}\big((17z+13)w^3 + (-82z-71)w^2 + (106z+119)w\big) - 2z - 5,$$

and let $E : y^2+a_1xy+a_3y = x^3$*, which has* $j(E) = 1331/8$*. Then* $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/15\mathbb{Z}$*. If* E' *is an elliptic curve over an octic field* K' *with* $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/15\mathbb{Z} \subseteq E'(K')$*, then* $(K', E') \simeq (K, E)$ *and* $E'(K')_{\mathrm{tors}} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$*. In particular,* $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ *is not a subgroup of the torsion of an elliptic curve over an octic field.*

Proof. The point $P = (0, 0)$ has order 3, and the point $Q = (x_Q, y_Q)$ with

$$x_Q = \tfrac{1}{6}\big((-z+1)w^3 + (8z-2)w^2 + (-17z-1)w\big) + \tfrac{3z}{2},$$
$$y_Q = \tfrac{1}{4}\big((z+2)w^3 + (-4z-8)w^2 + (3z+6)w + 2z + 3\big)$$

has order 15, with $e_3(P, 5Q) = z^2$, as we compute. The discriminant of $w^4-5w^3+8w^2-6w+3$ is $-507 = -3 \cdot 13^2$, so 43 is unramified in K. At the prime of K given by $z \mapsto 6$, $w \mapsto 4$, of residue field $\mathbb{F}_{43}$, the curve has good reduction with group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$. So $E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$.

Let $X = X_1(3, 15)$ over F, and let D_0 be the trace divisor on X of the point (E, P, Q). The invariant $-y_Q^2/x_Q^3$ of the triple has degree 4 over F, so D_0 is a closed point of degree 4 with residue field K. Now let D be the trace divisor of any point of X over an octic field. We compute all the possible reductions of D at the primes above 2 and 7: 5000 effective cuspidal divisors and 102 quartic points over $\mathbb{F}_4$, and over $\mathbb{F}_7$, where the entirely cuspidal reduction is excluded by Proposition 2.5(a) as $\operatorname{gon}_F X \geq 6$ [NV26, Table 1], 3264 quadratic points with a cuspidal part, 2304 cubic points with a cusp, 396 quartic points and 300 sums of two quadratic points. Fix an F-rational cusp c_*. By Lemma 5.4, $3[D-4c_*] \in \mathrm{Cl}_F^c X$, and comparing the two reductions inside $\mathrm{Cl}_F^c X$ leaves 60 pairs, all of whose classes over $\mathbb{F}_4$ lie in the reduction of $\mathrm{Cl}_F^c X$. As reduction above 2 is injective on $J_X(F)$ by Lemma 5.4, it follows that $[D - 4c_*] \in \mathrm{Cl}_F^c X$, and comparing the classes $[D - 4c_*]$ themselves leaves 12 elements of $\mathrm{Cl}_F^c X$. We check that these 12 classes form one orbit under the 48 automorphisms $(P, Q) \mapsto \big(aP + bQ_3,\ 2(cP + dQ_3) + 2uQ_5\big)$ of X over F, where $Q_3 = 5Q$, $Q_5 = 3Q$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_3)$ and $u \in \{1, 2\}$. So $[D - 4c_*] = [gD_0 - 4c_*]$ for an automorphism g, and as $\operatorname{gon}_F X > 4$, $D = gD_0$ by Lemma 2.7. The automorphisms only change the level structure, so the elliptic curve corresponding to D is E, over a field isomorphic to K. □

14. Proof of the main theorems

Tables 7 to 10 list, for each degree d and each of the groups of $\mathcal{M}_d$, where it is shown that it is not a subgroup of the torsion of an elliptic curve over a number field of degree d.

$G \in \mathcal{M}_6$	treated in
$\mathbb{Z}/37n\mathbb{Z}$, $n = 2, 3, 5, 7, 11, 13, 17, 19, 37$	Proposition 13.11
$\mathbb{Z}/n\mathbb{Z}$ for the 11 levels n of Table 1 with $d = 6$	Proposition 4.2 (global method)
$\mathbb{Z}/n\mathbb{Z}$, $n = 77, 85, 91, 95, 133, 247$	Propositions 4.4 and 4.5 (diamond operators)
$\mathbb{Z}/n\mathbb{Z}$, $n = 55, 75$, and $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$	Proposition 5.2
$\mathbb{Z}/81\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$	Propositions 4.8 and 12.1
$\mathbb{Z}/45\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z}$	Propositions 5.5, 7.6 and 12.2
$\mathbb{Z}/54\mathbb{Z}$	Proposition 10.1
$\mathbb{Z}/n\mathbb{Z}$, $n = 33, 34, 40, 42$	Propositions 6.1, 6.2, 6.4 and 6.5 (Hecke sieve)
$\mathbb{Z}/n\mathbb{Z}$, $n = 35, 38, 49, 50$	Propositions 6.6, 6.7 and 6.10
$\mathbb{Z}/39\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$, $n = 11, 13, 14$	Propositions 11.1, 11.3, 13.13 and 13.22
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$	Propositions 12.3 and 12.6, Propositions 12.7 and 12.13
$\mathbb{Z}/32\mathbb{Z}$, $\mathbb{Z}/36\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$	Propositions 5.7 and 13.10, Propositions 11.5 and 12.5
$\mathbb{Z}/51\mathbb{Z}$, $\mathbb{Z}/63\mathbb{Z}$	Propositions 7.9 and 7.12 (formal immersion at 2)
$\mathbb{Z}/57\mathbb{Z}$, $\mathbb{Z}/65\mathbb{Z}$	Propositions 9.6 and 9.8
$\mathbb{Z}/n\mathbb{Z}$, $n = 44, 52, 56, 60$	Lemma 3.3
$\mathbb{Z}/48\mathbb{Z}$	Proposition 11.14

TABLE 7. Treatment of the 66 groups of $\mathcal{M}_6$.

$G \in \mathcal{M}_7$	treated in
$\mathbb{Z}/n\mathbb{Z}$ for the 20 levels n of Table 1 with $d = 7$	Proposition 4.2 (global method)
$\mathbb{Z}/n\mathbb{Z}$, $n = 77, 85, 91, 95, 99$	Proposition 4.4 (diamond operators at 2)
$\mathbb{Z}/81\mathbb{Z}$	Proposition 4.8
$\mathbb{Z}/n\mathbb{Z}$, $n = 32, 34, 35, 38, 40, 42, 46, 49$	Propositions 5.7, 6.2, 6.6 and 6.7, Propositions 6.4, 6.5 and 6.10 (Hecke sieve)
$\mathbb{Z}/n\mathbb{Z}$, $n = 39, 45, 51, 55$	Propositions 7.6, 7.9, 7.11 and 13.13
$\mathbb{Z}/n\mathbb{Z}$, $n = 57, 63, 65, 69$	Propositions 7.12, 9.6, 9.8 and 9.9
$\mathbb{Z}/54\mathbb{Z}$	Proposition 10.3
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$, $n = 11, 12, 13, 14, 15$	Propositions 11.1, 11.2 and 13.22 and Propositions 11.3 and 11.5
$\mathbb{Z}/n\mathbb{Z}$, $n = 44, 48, 52, 56, 60$	Lemma 3.3
$\mathbb{Z}/50\mathbb{Z}$, $\mathbb{Z}/75\mathbb{Z}$	Proposition 13.6
$\mathbb{Z}/66\mathbb{Z}$	Proposition 13.7
$\mathbb{Z}/72\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$	Proposition 13.10

TABLE 8. Treatment of the 58 groups of $\mathcal{M}_7$.

$G \in \mathcal{M}_8$	treated in
$\mathbb{Z}/n\mathbb{Z}$ for the 20 levels n of Table 1 with $d = 8$	Proposition 4.2 (global method)
$\mathbb{Z}/n\mathbb{Z}$, $n = 81, 85, 91, 95$	Propositions 4.4, 4.7 and 4.8
$\mathbb{Z}/n\mathbb{Z}$, $n = 38, 44, 46, 50$	Propositions 6.7 and 6.8
$\mathbb{Z}/n\mathbb{Z}$, $n = 45, 49, 51, 55, 63, 75, 77$	Propositions 7.6, 7.7 and 7.9, Propositions 7.11 to 7.13 and 7.16
$\mathbb{Z}/n\mathbb{Z}$, $n = 57, 65, 69$	Propositions 9.6, 9.8 and 9.9
$\mathbb{Z}/54\mathbb{Z}$	Proposition 10.3
$\mathbb{Z}/48\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$, $n = 13, 14, 15, 16, 18, 21$	Propositions 11.3, 11.15 and 13.22, Propositions 11.5, 11.6, 11.9 and 11.13
$\mathbb{Z}/n\mathbb{Z}$, $n = 52, 56, 60, 64, 72, 84$	Lemma 3.3
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z}$, $n = 6, 7, 8, 9$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4n\mathbb{Z}$, $n = 4, 5, 6$, $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5n\mathbb{Z}$, $n = 3, 4, 5$, $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$	Propositions 12.1 to 12.3, Propositions 12.5 to 12.7 and 12.9, Propositions 12.11, 12.13 and 12.14
$\mathbb{Z}/66\mathbb{Z}$, $\mathbb{Z}/99\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/33\mathbb{Z}$	Proposition 13.7
$\mathbb{Z}/68\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/34\mathbb{Z}$	Proposition 13.8
$\mathbb{Z}/70\mathbb{Z}$, $\mathbb{Z}/105\mathbb{Z}$, $\mathbb{Z}/175\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/35\mathbb{Z}$	Proposition 13.9
$\mathbb{Z}/78\mathbb{Z}$, $\mathbb{Z}/117\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/39\mathbb{Z}$	Proposition 13.14
$\mathbb{Z}/80\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/40\mathbb{Z}$	Proposition 13.18
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$	Proposition 13.23

TABLE 9. Treatment of the 80 groups of $\mathcal{M}_8$. The groups in the last six rows contain $\mathbb{Z}/33\mathbb{Z}$, $\mathbb{Z}/34\mathbb{Z}$, $\mathbb{Z}/35\mathbb{Z}$, $\mathbb{Z}/39\mathbb{Z}$, $\mathbb{Z}/40\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$, and they are ruled out by the determination of all the elliptic curves over octic fields containing these groups.

$G \in \mathcal{M}_9$	treated in
$\mathbb{Z}/n\mathbb{Z}$ for the 35 levels n of Table 1 with $d = 9$	Proposition 4.2 (global method)
$\mathbb{Z}/n\mathbb{Z}$, $n \in \{81, 95, 99, 133, 247\}$	Propositions 4.4 and 4.8 to 4.10
$\mathbb{Z}/n\mathbb{Z}$, $n \in \{35, 38, 44, 46, 50, 58, 62\}$	Propositions 6.6 to 6.8 and 6.11
$\mathbb{Z}/48\mathbb{Z}$	Proposition 11.15
$\mathbb{Z}/n\mathbb{Z}$, $n \in \{45, 49, 51, 55, 63, 69, 75, 77\}$	Propositions 7.6, 7.7, 7.9 and 7.11, Propositions 7.12, 7.13, 7.16 and 9.9
$\mathbb{Z}/n\mathbb{Z}$, $n \in \{57, 65, 85, 87, 91, 93\}$	Propositions 8.2 to 8.5
$\mathbb{Z}/54\mathbb{Z}$	Proposition 10.4
$\mathbb{Z}/66\mathbb{Z}$, $\mathbb{Z}/78\mathbb{Z}$, $\mathbb{Z}/117\mathbb{Z}$	Propositions 13.7, 13.16 and 13.17
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$, $n \in \{14, 15, 16, 17, 18, 20, 21\}$, and $\mathbb{Z}/52\mathbb{Z}$	Propositions 11.3, 11.5 and 11.6, Propositions 11.9, 11.13 and 11.16
$\mathbb{Z}/4n\mathbb{Z}$, $n \in \{14, 15, 16, 17, 18, 20, 21\}$	Lemma 3.3

TABLE 10. Treatment of the 81 groups of $\mathcal{M}_9$.

Proof of Theorem 1.1. Let $d \in \{6, 7, 8, 9\}$. Every group in $\mathcal{G}_d$ occurs over a number field of degree d: the groups in $\Phi^\infty(d)$ by definition, and the sporadic groups by Propositions 13.1, 13.11 and 13.20 for $d = 6$, by Proposition 13.2 for $d = 7$, by Propositions 13.3, 13.4 and 13.23 for $d = 8$, and by Proposition 13.5 for $d = 9$. Conversely, by Lemma 3.1 every group in $\Phi(d) \setminus \mathcal{G}_d$ contains one of the groups of $\mathcal{M}_d$, and these are not subgroups of the torsion of an elliptic curve over a number field of degree d by the results listed in Tables 7 to 10. Hence $\Phi(d) = \mathcal{G}_d$. □

Proof of Theorem 1.2. For $d = 6$ the theorem follows from Propositions 13.11 and 13.20, for $d = 7$ from Propositions 13.6, 13.7 and 13.10, and for $d = 8$ from Propositions 13.7 to 13.9, 13.14, 13.18 and 13.23, with the curves of Propositions 13.2 and 13.3. For $d = 9$ and $G = \mathbb{Z}/33\mathbb{Z}$ it is Proposition 13.7. Finally, let $d = 9$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z} \subseteq E(K)$. By Remark 3.2 the corresponding point of $X_1(2, 26)$ has degree 9, so by Proposition 13.22 it lies in the orbit of $x_{2,26}$ under the level automorphisms, which do not change the elliptic curve. As $X_1(2, 26)$ is a fine moduli space, (K, E) is isomorphic to $(K_{2,26}, E_{2,26})$, and $E(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$ by Proposition 13.5. □

15. The computations

Our computations were performed in Magma V2.30-1 [BCP97], apart from some auxiliary ones in Python in all four degrees (such as the lists of groups, the values of Abramovich's bound, the queries to the LMFDB and the replay of data exported from Magma), in PARI/GP in degrees 8 and 9, and in Sage in degree 9. 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. 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], Sutherland's package [Sut] for independent counts of points on modular curves over finite fields, and the LMFDB [LMF26] for the analytic ranks of newforms. The Hecke operators on closed points of $X_1(m, n)_{\mathbb{F}_p}$ were computed with the routines of [Naj26a, §10], extended to $m \geq 3$ by carrying both level points through the isogenies. In degree 6 these extensions were tested against the full computation of the isogenies on sample points. In degree 9 the divisors $T_q P$ were computed both by our own routines and by Magma's isogeny functions. The computations took about 11, 19, 39 and 38 hours of CPU time in total for the degrees 6, 7, 8 and 9. For degree 7 this is the time of the computations recorded in the repository. These figures do not include the reruns made for the repositories, which took about 15 hours in degree 8 and 3 hours in degree 9, nor the independent recomputations described below. The figure for degree 9 includes the computations for the prime orders, which this paper does not use.

The completeness of the enumeration of closed points of small degree, which every sieve computation assumes, was checked independently of the models by counting the isomorphism classes of elliptic curves with the required level structure over $\mathbb{F}_{p^e}$, using $\#Y_1(m, n)(\mathbb{F}_{p^e}) = \sum_{k|e} k \cdot n_k$, where n_k is the number of non-cuspidal closed points of degree k (see `independent_counts.m`, `independent_counts_fast.m`, the octic and the nonic code, and the other scripts listed in the `README` files). For $X_1(10, 10)$ in Proposition 12.9 we count the elliptic curves with full level 10 structure. In the sieve computations on the curves $X_1(n)$ the degrees of the closed cusps over $\mathbb{F}_p$, on which the admissibility of the primes q depends, are computed from the models and checked against the prediction of [DEvH+21, Lemma 2.8].

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` files of the septic, octic and nonic repositories, and for degree 6 in the `README` of the sextic repository. Most of them are the original computations in the smaller degrees, which are covered by the computation in the largest degree (see Section 6.1 and Remark 7.4), for instance the Hecke sieve in degree 6 on $X_1(32)$, $X_1(34)$, $X_1(39)$, $X_1(40)$, $X_1(2, 22)$ and $X_1(2, 28)$, the computations on the quotient Y_{51} of Lemma 7.8 in degrees 6 and 7, and those for $\mathbb{Z}/65\mathbb{Z}$ in degree 6 on a quotient of $X_1(65)$ of genus 41. Most of the computations of ranks

of restriction maps, of ranks of the matrices in Lemma 8.1 and of classes in finite groups in degrees 8 and 9 were done, or replayed, by independent programs, using integer and binary linear algebra, from the data exported by the Magma computations. Other results were checked by a second method, such as the finiteness of $J_1(69)(\mathbb{Q})$ and $J_1(81)(\mathbb{Q})$ by winding computations, independently of [DEvH+21], the spaces $\Omega(jP)$ used for Propositions 7.16 and 12.2, and $\ell(B) = 0$ in the proof of Proposition 11.13, by lattice reduction.

We checked the computations on which the proofs depend most heavily a second time, with code written independently of the first implementation and, where models of the curves are involved, with different models. In all four degrees these are the list of Lemma 3.1, the explicit examples of Section 13 and the analytic ranks and character values taken from the LMFDB (in degree 9 those at the levels up to 99 and at 115, 133 and 247, and those for the curves $X_1(2, 2n)$). In degree 6 they also include the 2-torsion computations of Lemma 6.9 and Lemma 9.3, the doubled cuspidal computations for $X_1(45)$ and $X_1(3, 21)$, and the Cartier operator computations on the quotients of Lemma 7.8 and on the quotient of $X_1(65)$ mentioned above. In degree 7 they include the numbers of non-cuspidal closed points over $\mathbb{F}_2$ and $\mathbb{F}_3$ and the septic points on $X_1(25)$ and $X_1(33)$. In degree 8 they include all the numbers of non-cuspidal closed points and their orbits, the orders of the groups $J(\mathbb{F}_p)$, the octic points on $X_1(33)$, $X_1(34)$, $X_1(35)$, $X_1(39)$ and $X_1(40)$, the quartic points on $X_1(3, 15)$ over $\mathbb{Q}(\zeta_3)$, and the formal immersion criteria in Propositions 7.6, 7.7, 7.12, 12.2 and 12.11 (for $X_1(51)$ our models were too large for this). In degree 9 they include 47 of the lists of numbers of non-cuspidal closed points that we use, by an enumeration of all elliptic curves over $\mathbb{F}_{p^e}$ for $p \leq 5$ and $e \leq 9$, and the list in Lemma 2.11(3), which we also derived from the results of Bourdon and Pollack [BP17]. In all cases the results agree. These computations are in the folders `independent`, `independent`, `independent` and `independent` of the four repositories.

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).

[BKX13] Francesc Bars, Aristides Kontogeorgis, and Xavier Xarles, *Bielliptic and hyperelliptic modular curves $X(N)$ and the group* $\mathrm{Aut}(X(N))$, Acta Arith. **161** (2013), no. 3, 283–299.

[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.

[Box21] Josha Box, *Quadratic points on modular curves with infinite Mordell–Weil group*, Math. Comp. **90** (2021), no. 327, 321–343.

[BP17] Abbey Bourdon and Paul Pollack, *Torsion subgroups of CM elliptic curves over odd degree number fields*, Int. Math. Res. Not. IMRN (2017), no. 16, 4923–4961.

[BS10] Nils Bruin and Michael Stoll, *The Mordell–Weil sieve: proving non-existence of rational points on curves*, LMS J. Comput. Math. **13** (2010), 272–306.

[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.

[CGPS22] Pete L. Clark, Tyler Genao, Paul Pollack, and Frederick Saia, *The least degree of a CM point on a modular curve*, J. Lond. Math. Soc. (2) **105** (2022), no. 2, 825–883.

[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.

[DGJ20] Harris B. Daniels and Enrique González-Jiménez, *On the torsion of rational elliptic curves over sextic fields*, Math. Comp. **89** (2020), no. 321, 411–435.

[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.

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math., vol. 349, Springer, Berlin, 1973, pp. 143–316.

[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.

[DS26] ———, Personal communication, 2026.

[DvH14] Maarten Derickx and Mark van Hoeij, *Gonality of the modular curve* $X_1(N)$, J. Algebra **417** (2014), 52–71.

[Fal83] Gerd Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366.

[Fre94] Gerhard Frey, *Curves with infinitely many points of fixed degree*, Israel J. Math. **85** (1994), no. 1-3, 79–83.

[GJN23] Enrique González-Jiménez and Filip Najman, *An algorithm for determining torsion growth of elliptic curves*, Exp. Math. **32** (2023), no. 1, 70–81.

[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.

[Kam92a] Sheldon Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229.

[Kam92b] ———, *Torsion points on elliptic curves over fields of higher degree*, Internat. Math. Res. Notices (1992), no. 6, 129–133.

[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.

[Ken80] M. A. Kenku, *The modular curves* $X_0(65)$ *and* $X_0(91)$ *and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **87** (1980), no. 1, 15–20.

[Ken82] ———, *On the number of* $\mathbf{Q}$*-isomorphism classes of elliptic curves in each* $\mathbf{Q}$*-isogeny class*, J. Number Theory **15** (1982), no. 2, 199–202.

[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.

[Maz78] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), no. 2, 129–162.

[mdm] *mdmagma*, https://github.com/nt-lib/mdmagma, M. Derickx and A. V. Sutherland, `Magma` 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://github.com/F-Najman/Sd, 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.

[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.

[Sut] Andrew V. Sutherland, *Magma intrinsics for subgroups of* $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ *and modular curves*, https://github.com/AndrewVSutherland/Magma, `Magma` package; point counting in `gl2points.m`.

[Sut12a] ———, *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.

[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`