hexagon:2611.00120v1

POINTS OF PRIME ORDER ON ELLIPTIC CURVES OVER NUMBER FIELDS OF DEGREE 9 TO 22

FILIP NAJMAN

Abstract. Let $S(d)$ be the set of primes p for which there exists an elliptic curve over a number field of degree d with a point of order p. The sets $S(d)$ are known for $d \leq 8$. We determine $S(d)$ for all $9 \leq d \leq 22$. For example, the largest prime in $S(22)$ is 67, and $S(16)$ consists of the primes up to 37. To reduce the problem to finitely many primes we prove a version of Oesterlé's bound which uses reduction modulo 2 instead of modulo 3, and which is much smaller for $d \geq 13$. The remaining primes are dealt with using results of Derickx and Stoll and extensive computations with the modular curves $X_1(p)$ over $\mathbb{F}_2$ for $p \leq 139$.

1. Introduction

Let K be a number field and E/K an elliptic curve. By the Mordell-Weil theorem the torsion group $E(K)_{\text{tors}}$ is finite, and Merel [28] proved that its order is bounded by a constant depending only on the degree $d = [K : \mathbb{Q}]$. A key step in all the proofs of such results is to bound the primes that divide $\#E(K)_{\text{tors}}$. Following [10, Definition 1.1] we denote by $S(d)$ the set of primes p for which there exists an elliptic curve over a number field of degree d with a point of order p (in [18] the same notation is used for fields of degree at most d), and by $\text{Primes}(x)$ the set of primes $p \leq x$.

Mazur [24] proved that $S(1) = \text{Primes}(7)$, Kamienny [17] proved that $S(2) = \text{Primes}(13)$ (which, together with the work of Kenku and Momose [21], determined the torsion groups over quadratic fields), and Parent [35, 36] proved that $S(3) = \text{Primes}(13)$. Derickx, Kamienny, Stein and Stoll [10, Theorem 1.2] proved that

$$S(4) = \text{Primes}(17), \quad S(5) = \text{Primes}(19), \quad S(6) = \text{Primes}(19) \cup \{37\}, \quad S(7) = \text{Primes}(23),$$

and Khawaja [22] proved that $S(8) = \text{Primes}(23)$. An important ingredient of [10] is a bound of Oesterlé, which states that $p \leq (3^{d/2} + 1)^2$ for all $p \in S(d)$ [10, Theorem 6.1]. Derickx and Stoll [12] studied the behavior of $S(d)$ as $d \to \infty$. Among other things they gave a criterion [12, Corollary 7.5], in terms of the *strange* characters modulo p, that rules out most primes below Oesterlé's bound, and they determined the strange characters modulo all primes $p < 10^5$ [12, Proposition 5.2 and Table 2]. They have also determined $S(9)$, up to not being able to eliminate 89 from $S(9)$ [13]. The sets $S(d)$ are the starting point of the classifications of the possible torsion groups of elliptic curves over number fields of degree d, which are now known

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

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

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.

for $d \leq 10$ (see [9, 11, 29, 31, 32] and the references therein). In particular, the determinations of $S(9)$ and $S(10)$ in this paper are used in [32] and [31].

In this paper we determine $S(d)$ for $9 \leq d \leq 22$. Our main result is the following theorem.

Theorem 1.1. *We have*

$$\begin{aligned} S(9) = S(11) &= \mathrm{Primes}(31), \\ S(10) = S(13) = S(16) &= \mathrm{Primes}(37), \\ S(12) = S(15) &= \mathrm{Primes}(37) \cup \{43\}, \\ S(14) = S(17) = S(18) = S(19) &= \mathrm{Primes}(43), \\ S(20) &= \mathrm{Primes}(47) \cup \{61\}, \\ S(21) &= \mathrm{Primes}(47), \\ S(22) &= \mathrm{Primes}(53) \cup \{67\}. \end{aligned}$$

Together with the results mentioned above, this determines $S(d)$ for all $d \leq 22$. Note that $S(d') \subseteq S(d)$ if d' divides d, but that $S(d)$ is not increasing in d: for example $37 \in S(10)$, but $37 \notin S(11)$, and $41, 43 \in S(14)$, but $41, 43 \notin S(16)$. The primes $31 \in S(10)$, $29, 43 \in S(14)$, $41, 61 \in S(20)$ and $67 \in S(22)$ are of the form $2d + 1$ or $3d + 1$, and such primes are always in $S(d)$ for even d, because of points with complex multiplication [12, Corollary 7.5]. Derickx and Stoll [12, Corollary 7.8] showed that, assuming a conjecture on the sparsity of strange newforms, $S(d)$ is contained in $\mathrm{Primes}(d+1) \cup \{\frac{3}{2}d+1, 2d+1, 3d+1\}$ for d large enough. Note that the degrees we consider are far from this range, as $S(22)$ contains all the primes up to 53.

We now describe the proof. For a point of order p on an elliptic curve over a number field of degree d, we study the corresponding effective divisor D of degree d on the modular curve $X_1(p)$, and our methods depend on the size of p.

For large p we use Oesterlé's bound together with [12, Corollary 7.5]. Unfortunately, Oesterlé's bound exceeds 10^5, the limit of [12, Table 2], for $d \geq 11$, and it grows like 3^d. For $d \geq 13$ we prove a version of Oesterlé's bound that uses reduction modulo 2 instead of modulo 3 (Proposition 4.5), which gives bounds of size about 2^d. The price we pay for using the prime 2 is that we have to check that $2d$, instead of d, Hecke operators acting on the winding element are linearly independent modulo 2. For $d \in \{11, 12\}$ we use reduction modulo 3, 5 and 7 instead. Above 10^5 at most 1488 primes remain in each degree, and for each of them we show that sufficiently many characters are not strange, by a computation with modular symbols over a finite field (Section 4.3). Below $4 \cdot 10^5$ this agrees with a list of the strange characters that Michael Stoll has sent us, which also gives an independent proof for these primes (see the end of Section 4.3).

For medium-sized p we use [12, Proposition 4.1], which shows that D is invariant under a diamond operator whenever the gonality of $X_1(p)$ is large compared to d (Section 4.4). For a few primes $p > 157$ its hypothesis on rational 2-torsion is not known, and we check it by showing that a Hecke operator restricts to an isogeny of odd degree on a suitable abelian subvariety of $J_1(p)$.

The remaining primes, which satisfy $37 \leq p \leq 139$, require most of the work (Sections 5 and 6). We reduce D modulo 2 and enumerate all the possible reductions, using all the elliptic curves over $\mathbb{F}_{2^f}$ for $f \leq d$. Reductions supported on rational cusps are ruled out by the formal immersion criterion of [10]. For all other reductions we use the Hecke operator $A_3 = T_3 - 1 - 3\langle 3 \rangle$, composed with an element of the group ring of the diamond operators which kills the part of $J_1(p)$ of positive rank: if D exists, a certain divisor of degree 0 on $X_1(p)_{\mathbb{F}_2}$ has to be principal [10, Lemma 8.6]. We show that it is not, by linear algebra in the canonical ring of $X_1(p)_{\mathbb{F}_2}$,

which we compute from q-expansions. This argument rules out all but a short list of reductions. For these we show that D is invariant under a diamond operator, which typically leads to a contradiction by counting, or we use a relative version of the formal immersion criterion, or the formal immersion criterion at the reductions of known points of smaller degree, or quotients of $X_1(p)$.

Our methods are those of [10], [12] and [22], applied to a much larger range of degrees. The main difference is the scale of the computations: for $d = 22$ we have to deal with 155750 primes, the local computations concern 501 types of reductions at 17 primes, and they consist of 129638 new linear algebra certificates on the curves $X_1(p)_{\mathbb{F}_2}$, of genus up to 737. The certificates for $d = 22$ alone occupy about 220 GB.

All the code used in the paper can be found at

https://github.com/F-Najman/Sd

and the complete certificates at Harvard Dataverse [30].

AI disclosure and comments. AI models were extensively used in the work leading to this paper. OpenAI's GPT-Sol 6.1 and GPT-6 Astra models produced almost all of the mathematical content of the first versions of the proofs and carried out the computations. Anthropic's Claude Opus 5.5 reviewed these proofs, without rerunning the computations, wrote the draft of the present manuscript and organized the code repository.

Acknowledgements

I thank Maarten Derickx for helpful discussions and Michael Stoll for sending me his list of the strange characters modulo all primes $p < 4 \cdot 10^5$ (see the end of Section 4.3).

2. Notation and auxiliary results

Throughout the paper $p \geq 5$ is a prime. The modular curve $X_1(p)$ parametrizes pairs (E, P), where E is an elliptic curve and $P \in E$ is a point of order p, and it is a fine moduli space. It has a smooth proper model over $\mathbb{Z}[1/p]$, which we also denote by $X_1(p)$, so in particular it has good reduction at 2. We write $J_1(p)$ for its Jacobian, $X_0(p)$ and $J_0(p)$ for the curve parametrizing pairs (E, C) with $C \subseteq E$ cyclic of order p and for its Jacobian, $X^{(d)}$ for the d-th symmetric power of a curve X, and $\mathrm{gon}_k X$ for the gonality of X over a field k. For an effective divisor D of degree d on a curve X over $\mathbb{Q}$ we write D also for the corresponding point of $X^{(d)}(\mathbb{Q})$, and, when X has good reduction at 2, $\overline{D}$ for its reduction modulo 2, an effective divisor of degree d on $X_{\mathbb{F}_2}$.

2.1. **Diamond and Hecke operators.** For $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ we write $\langle a \rangle$ for the automorphism $(E, P) \mapsto (E, aP)$ of $X_1(p)$. It depends only on the class of a in

$$\Delta(p) := (\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\},$$

which is a cyclic group of order $(p-1)/2$, and for $h \in \Delta(p)$ we denote by $\mathrm{ord}(h)$ its order in $\Delta(p)$. We identify $h \in \Delta(p)$ with the corresponding diamond operator. For a subgroup $H \subseteq \Delta(p)$ we write $X_H = X_1(p)/H$ and J_H for its Jacobian, so that $X_H = X_1(p)$ if H is trivial. If X_H has positive genus, then it has good reduction at every prime $q \neq p$, and the quotient map $X_1(p) \to X_H$ extends to a finite morphism of the smooth models over $\mathbb{Z}_{(q)}$ [23, Corollary 4.10]. For a prime $q \neq p$ we denote by T_q the Hecke correspondence

$$T_q(E, P) = \sum_C (E/C, P \bmod C),$$

the sum running over the $q+1$ subgroups $C \subseteq E$ of order q, and we put

$$A_q = T_q - 1 - q\langle q \rangle, \qquad B_q = T_q - \langle q \rangle - q.$$

Diamond and Hecke operators act on divisors on $X_1(p)$ and X_H, on $J_1(p)$ and J_H, and, by reduction, on divisors on $X_1(p)_{\mathbb{F}_2}$ when q is odd.

The curve $X_1(p)$ has $(p-1)/2$ cusps defined over $\mathbb{Q}$, which we call the *rational cusps*, and $(p-1)/2$ cusps defined over $\mathbb{Q}(\zeta_p)^+$, the maximal real subfield of $\mathbb{Q}(\zeta_p)$. The group $\Delta(p)$ acts simply transitively on each of these two sets. The rational cusps reduce to the $\mathbb{F}_2$-rational cusps of $X_1(p)_{\mathbb{F}_2}$, and the other cusps reduce to closed points of degree ord(2), which we call the *non-rational cusps*. We call the images of the rational cusps on X_H the rational cusps of X_H. We fix a rational cusp c_0 of $X_1(p)$, and we denote its image on X_H also by c_0.

2.2. **The trace divisor.** Let K be a number field of degree d and E/K an elliptic curve with a point $P \in E(K)$ of order p. Then $x = (E, P)$ is a non-cuspidal point of $X_1(p)$ defined over K, and we call

$$D = \sum_{\sigma : K \hookrightarrow \overline{\mathbb{Q}}} \sigma(x)$$

the *trace divisor* of (E, P), or of a point of order p over a number field of degree d. It is an effective divisor of degree d defined over $\mathbb{Q}$, its support contains no cusps, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts transitively on its support, and all the points in its support have the same multiplicity d/n, where $n = [\mathbb{Q}(x) : \mathbb{Q}]$ divides d. In particular $p \in S(d)$ if and only if such a divisor exists. If $p \notin S(d')$ for every proper divisor d' of d, then $n = d$ and D is a closed point of degree d.

For a trace divisor D we write

$$\overline{D} = Z + C',$$

where C' is supported on the $\mathbb{F}_2$-rational cusps of $X_1(p)_{\mathbb{F}_2}$ and Z has none of them in its support (Z may contain non-rational cusps). We denote by C the rational cuspidal divisor lifting C', and put $c = \deg C$. For a subgroup $H \subseteq \Delta(p)$ we say that D *is a pullback from* X_H if $D = \pi^* D'$, where $\pi : X_1(p) \to X_H$ is the quotient map and D' is an effective divisor on X_H, defined over $\mathbb{Q}$, with no cusps in its support.

We will need the following theorem of Silverberg [39], in the sharper form stated in [37, Section 1] and [7, Theorem 1.1].

Lemma 2.1 (Silverberg)**.** *Let F be a number field and E/F an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field k. If $E(F)$ has a point of order p, then $p - 1 \leq \delta \cdot \#\mathcal{O}^\times \cdot [F : \mathbb{Q}]$, where $\delta = 1/2$ if $k \subseteq F$ and $\delta = 1$ otherwise.*

Lemma 2.2. *Let $x = (E, P)$ be a non-cuspidal point of $X_1(p)$ of degree n which is fixed by a non-trivial element of $\Delta(p)$. Then n is even, and either $j(E) = 1728$ and $n \geq (p-1)/2$, or $j(E) = 0$ and $n \geq (p-1)/3$.*

Proof. As $X_1(p)$ is a fine moduli space, we can take E and P to be defined over $F = \mathbb{Q}(x)$. If $\langle a \rangle \neq 1$ fixes x, there is an automorphism $\alpha \neq \pm 1$ of E with $\alpha(P) = aP$. It is unique, as an automorphism $\beta \neq 1$ fixes no point of order p ($\beta - 1$ has degree at most 4), so α is defined over F. Hence $j(E) \in \{0, 1728\}$, and α acts on the invariant differential by a root of unity $\zeta \in F$ of order 3, 4 or 6, so the field $k = \mathbb{Q}(\zeta)$ of complex multiplication of E is contained in F, and n is even. By Lemma 2.1, $p - 1 \leq \frac{1}{2}\mu n$, where $\mu = \#\operatorname{Aut}(E)$ is 4 if $j(E) = 1728$ and 6 if $j(E) = 0$. □

Lemma 2.3. *Let K be a number field of degree d, let E/K be an elliptic curve with a point P of order p, let D be the trace divisor of (E, P), and let $n = [\mathbb{Q}(x) : \mathbb{Q}]$ for $x = (E, P)$. Let $H \subseteq \Delta(p)$ be a subgroup such that $hD = D$ for all $h \in H$.*

a) *The orbits of H on the (geometric) support of D all have the same length m, and m divides n.*
b) *If n is odd or $n < (p-1)/3$, then H acts freely on the support of D, so $m = \#H$, and D is a pullback from X_H.*

Proof. As the elements of H are defined over $\mathbb{Q}$, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ permutes the orbits of H, and as it acts transitively on the n points of the support of D, all the orbits have the same length m, and $m \mid n$. Under the assumption of b), no point of the support of D is fixed by a non-trivial element of H by Lemma 2.2. So each orbit is a fibre of the quotient map $\pi : X_1(p) \to X_H$, which is unramified there, and as all the points of the support of D have the same multiplicity, $D = \pi^* D'$ for the effective divisor $D' = \pi_* D/\#H$ on X_H, which is defined over $\mathbb{Q}$ and has no cusps in its support. □

By the proof of Lemma 2.2, the stabilizer in $\Delta(p)$ of a non-cuspidal point has order dividing 2 or 3, so in general $m \in \{\#H, \#H/2, \#H/3\}$. Note that for $p > 67$ and $n \leq 22$ we always have $n < (p-1)/3$.

2.3. **Finiteness of Mordell-Weil groups.** Recall from [12, Definition 5.1] that a non-trivial even Dirichlet character χ modulo p is *strange* if there is a newform f of weight 2 and level p with character χ such that $L(f,1) = 0$, that p is *strange* if there is a strange character modulo p, and that $\mathrm{str}(p)$ is the order of the group generated by the strange characters modulo p. The strange characters modulo $p < 10^5$ are listed in [12, Proposition 5.2 and Table 2]. The strange primes below 200 are 61, 97, 101, 181 and 193, and their strange characters have orders 6, 12, 10, 6 and 12, respectively.

Lemma 2.4. *Let $H \subseteq \Delta(p)$ be a subgroup, and let $\alpha \in \mathbb{Z}[\Delta(p)]$ be such that $\chi(\alpha) = 0$ for the trivial character χ and for all the strange characters χ modulo p which are trivial on H. Then $\alpha J_H(\mathbb{Q})$ is finite. The same holds for every endomorphism α of J_H in the Hecke algebra which kills the abelian subvarieties of J_H attached to the newforms of weight 2 and level p with trivial or strange character. In particular, if p is not strange, then $(h-1)J_H(\mathbb{Q})$ is finite for every $h \in \Delta(p)$. If $p \in \{41, 47, 59, 71\}$, then $J_1(p)(\mathbb{Q})$ is finite.*

Proof. Up to isogeny over $\mathbb{Q}$, J_H is the product of the abelian varieties A_f attached to the Galois orbits of newforms f of weight 2 and level p whose character is trivial on H, and $\Delta(p)$ acts on A_f through the character of f. Hence αJ_H is contained in the sum of the A_f for which the character of f is non-trivial and not strange. These have $L(f,1) \neq 0$, so $A_f(\mathbb{Q})$ is finite by Kato's theorem [19, Corollary 14.3]. The last statement is [10, Proposition 3.1]. □

Lemma 2.5. a) *Let $A/\mathbb{Q}$ be an abelian variety with good reduction at a prime ℓ. If ℓ is odd, then reduction modulo ℓ is injective on $A(\mathbb{Q})_{\mathrm{tors}}$. If $\ell = 2$, then the kernel of reduction modulo 2 on $A(\mathbb{Q})_{\mathrm{tors}}$ is killed by 2.*
b) *Let $H \subseteq \Delta(p)$ be a subgroup. For an odd prime $q \neq p$, the operator A_q kills $J_H(\mathbb{Q})_{\mathrm{tors}}$. If $p \leq 157$ and $\#H$ is odd, then A_2 kills $J_H(\mathbb{Q})_{\mathrm{tors}}$ as well.*
c) *Let $H \subseteq \Delta(p)$ be a subgroup and $q \neq p$ a prime. Then $A_q c = 0$ for every rational cusp c of X_H, and $B_q c = 0$ for every other cusp c of X_H, as divisors. In particular $B_q A_q$ kills every cuspidal divisor on X_H.*

Proof. For odd ℓ part a) is [20, Appendix], and for $\ell = 2$ it is [35, Lemme 1.7], applied to the Néron model of A over $\mathbb{Z}_{(2)}$. The modular interpretation used in [10] and [12] differs from ours by the Atkin-Lehner involution, which transforms $T_q - \langle q \rangle - q$ and $T_q - q\langle q \rangle - 1$ into A_q and B_q, up to a diamond operator (see the discussion after [10, Lemma 8.6]). In that interpretation the rational cusps of $X_1(p)$ are killed by $T_q - \langle q \rangle - q$ and the other cusps by $T_q - q\langle q \rangle - 1$

(see the remark after [10, Proposition 2.4] and [35, Sections 1.5 and 2.4]), so in ours we have $T_q c = c + q\langle q\rangle c$ for a rational cusp c and $T_q c = \langle q\rangle c + qc$ for the other cusps. These formulas descend to X_H, which proves c). On X_H modulo q we have $T_q = \mathrm{Frob}_q + q\langle q\rangle \mathrm{Frob}_q^{-1}$ (the Eichler-Shimura relation), so A_q kills $J_H(\mathbb{F}_q)$, and as $J_H(\mathbb{Q})_{\mathrm{tors}}$ injects into $J_H(\mathbb{F}_q)$ for odd q by a), A_q kills $J_H(\mathbb{Q})_{\mathrm{tors}}$. For $q = 2$ the same argument shows that A_2 kills the odd part of $J_H(\mathbb{Q})_{\mathrm{tors}}$. If $p \leq 157$, the 2-primary part of $J_1(p)(\mathbb{Q})_{\mathrm{tors}}$ is contained in the subgroup generated by differences of rational cusps [12, Remark 4.4], so it is killed by A_2 by c). If moreover $\#H$ is odd, then the pullback $J_H \to J_1(p)$ is injective on the 2-primary part of $J_H(\mathbb{Q})_{\mathrm{tors}}$, as its composition with the pushforward is multiplication by $\#H$, and it commutes with A_2, so A_2 kills the 2-primary part of $J_H(\mathbb{Q})_{\mathrm{tors}}$ as well. □

2.4. **Gonality.** If a curve X over $\mathbb{Q}$ has good reduction at a prime ℓ, then $\mathrm{gon}_{\mathbb{Q}} X \geq \mathrm{gon}_{\mathbb{F}_\ell} X$, and an obvious count of points gives $\mathrm{gon}_{\mathbb{F}_\ell} X \geq \#X(\mathbb{F}_{\ell^k})/(\ell^k + 1)$ for all $k \geq 1$. We will use the following lower bounds.

Proposition 2.6. a) *We have* $\mathrm{gon}_{\mathbb{Q}} X_1(p) \geq \frac{325}{2^{16}}(p^2 - 1)$, *and if* $p \leq 880$, *then* $\mathrm{gon}_{\mathbb{Q}} X_1(p) \geq \frac{1}{192}(p^2 - 1)$.
b) *We have* $\mathrm{gon}_{\mathbb{Q}} X_1(37) = 18$, $\mathrm{gon}_{\mathbb{Q}} X_1(43) = 24$ *and* $\mathrm{gon}_{\mathbb{Q}} X_1(53) \geq 20$.

Proof. The first statement of a) is [12, Theorem 3.3]. Its proof uses the bound $\mathrm{gon}_{\mathbb{C}} X_1(p) \geq \frac{\lambda}{24} \cdot \frac{p^2-1}{2}$ from the proof of [2, Theorem 0.1], which holds if $\lambda \leq \frac{1}{4}$ and the Laplacian on $X_1(p)$ has no eigenvalues in $(0, \lambda)$, with $\lambda = \frac{975}{4096}$. Booker, Lee and Strömbergsson [5, Theorem 1.1] proved the Selberg eigenvalue conjecture for $\Gamma_1(N)$ with $N \leq 880$, so for $p \leq 880$ we can take $\lambda = \frac{1}{4}$ (see also [12, Remark 3.4]), which gives the second statement. The first two statements of b) are [14, Table 1] and [44, Theorem D].

The curve $X_1(53)_{\mathbb{F}_2}$ has 26 rational points, the reductions of the rational cusps, and no closed points of degree between 2 and 8. Let f be a function of degree $e \leq 19$ on $X_1(53)_{\mathbb{F}_2}$. One of the fibres of f above the three points of $\mathbb{P}^1(\mathbb{F}_2)$ contains at least 9 rational points, and after composing f with an automorphism of $\mathbb{P}^1$ we can assume that this is the fibre above ∞. Its non-rational part then has degree at most 10, so it is 0, a closed point of degree 9, or a closed point of degree 10. Hence the divisor of poles of f is bounded by $C_{53} + E$, where C_{53} is the sum of all the rational points and E is either an effective divisor of degree 10 supported on the rational points, or the sum of a rational point and a closed point of degree 9, or a closed point of degree 10. Using the action of $\Delta(53)$ we compute that $\ell(C_{53} + E) = 1$ in the first case, and also in the other two, so f does not exist. Hence $\mathrm{gon}_{\mathbb{Q}} X_1(53) \geq \mathrm{gon}_{\mathbb{F}_2} X_1(53) \geq 20$. □

2.5. **Stabilizers.** The following is trivial.

Lemma 2.7. *Let X be a curve over a field F, and let D_1 and D_2 be effective divisors of degree d on X, defined over F, such that $D_1 \sim D_2$. If $\mathrm{gon}_F X > d$, then $D_1 = D_2$.*

We will often use the following lemma, which is a variant of the argument of [12, Proposition 4.1].

Lemma 2.8. *Let X be a curve over $\mathbb{Q}$ with good reduction at 2, let J be its Jacobian, and let s be an automorphism of X defined over $\mathbb{Q}$, of order m, such that $(s-1)J(\mathbb{Q})$ is finite. Let D and C be effective divisors on X, defined over $\mathbb{Q}$, of degrees e and c, such that $s(\overline{D} - \overline{C}) = \overline{D} - \overline{C}$, and put $y = [s(D - C) - (D - C)] \in J(\mathbb{Q})$.*

a) *Then $2y = 0$, and $y = 0$ if one of the following holds:*
   i) *reduction modulo 2 is injective on $J(\mathbb{Q})_{\mathrm{tors}}$, for example if $J(\mathbb{Q})[2] = 0$,*
   ii) *m is odd and s acts trivially on $J(\mathbb{Q})[2]$,*

iii) *m is odd and there is an endomorphism β of J which kills $J(\mathbb{Q})_{\mathrm{tors}}$ and restricts to an isogeny of odd degree on the abelian subvariety $(s-1)J$.*

b) *If $y = 0$ and $\mathrm{gon}_{\mathbb{Q}} X > e + c$, or if $\mathrm{gon}_{\mathbb{Q}} X > 2(e + c)$, then $sD + C = D + sC$.*

Proof. Put $Z_0 = D - C$ and $N = 1 + s + \cdots + s^{m-1}$. Note that Z_0 need not have degree 0, but $mZ_0 - NZ_0$ does, and

$$my = (s-1)[mZ_0 - NZ_0],$$

so y is torsion. The reduction of y is the class of $s(\overline{D}-\overline{C})-(\overline{D}-\overline{C}) = 0$, so $2y = 0$ by Lemma 2.5 a), and in case i) $y = 0$. In case ii) we have $Ny = my$, and $Ny = [NsZ_0 - NZ_0] = 0$, so $my = 0$, and as m is odd, $y = 0$. In case iii), as m is odd and $2y = 0$, we have $y = my = (m - N)y$, and as $m - N$ is divisible by $s - 1$ in $\mathbb{Z}[s]$, y lies in $B = (s-1)J$. Since $\beta(y) = 0$ and β has odd degree on B, it follows that $y = 0$.

If $y = 0$, then $sD + C \sim D + sC$, and if $2y = 0$, then $2sD + 2C \sim 2D + 2sC$. These divisors are effective and defined over $\mathbb{Q}$, so under the assumptions of b) Lemma 2.7 shows that $sD + C = D + sC$. □

For trace divisors we use Lemma 2.8 in the following form.

Lemma 2.9. *Let D be the trace divisor of a point of order p over a number field of degree d. Let $h \in \Delta(p)$ be such that $(h-1)J_1(p)(\mathbb{Q})$ is finite and $hZ = Z$, and put $y = [h(D-C)-(D-C)] \in J_1(p)(\mathbb{Q})$. Then $2y = 0$, and $y = 0$ if one of the conditions i), ii) and iii) of Lemma 2.8 holds for $X = X_1(p)$ and $s = h$. If $y = 0$ and $\mathrm{gon}_{\mathbb{Q}} X_1(p) > d + c$, or if $\mathrm{gon}_{\mathbb{Q}} X_1(p) > 2(d + c)$, then $hD = D$ and $hC = C$. In particular $\mathrm{ord}(h)$ divides c.*

Proof. As $\overline{D} - \overline{C} = Z$ is fixed by h, Lemma 2.8 applies with $X = X_1(p)$, $s = h$ and $e = d$, and under the assumptions on the gonality it gives $hD + C = D + hC$. As D has no cusps in its support, $hD = D$ and $hC = C$. Finally, $\Delta(p)$ acts freely on the rational cusps, so C is a sum of orbits of length $\mathrm{ord}(h)$. □

2.6. **Non-principal divisors.** The following criterion, which we also used in [32], is our main tool for showing that a divisor of degree 0 over a finite field is not principal when the genus is large. For a curve X we write $R_i = H^0(X, iK_X)$, where K_X is a canonical divisor.

Lemma 2.10. *Let X be a smooth projective geometrically integral curve over a field k, and let $B = U - V$, where U, V are effective divisors of the same degree. Let $\mathcal{L}$ and $\mathcal{M}$ be line bundles on X, and choose $0 \neq F \in H^0(X, \mathcal{L}(-U))$ and $H \in H^0(X, \mathcal{M}(-U))$. If the linear map*

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

is injective, then B is not principal. The same holds if several sections H are used.

Proof. Suppose $B = \mathrm{div}(g)$. Then $G = F/g$ is a non-zero section of $\mathcal{L}$ vanishing on V, and $GH = F \cdot (H/g)$ with $H/g \in H^0(X, \mathcal{M})$, so G is in the kernel of the map. □

We apply the lemma with $\mathcal{L} = \mathcal{M} = K_X$ or $2K_X$, where the multiplication maps $R_i \times R_j \to R_{i+j}$ are computed from the q-expansions of a basis of the weight 2 cusp forms, with enough coefficients to determine all the products. To evaluate sections at the points of V we use local parameters at these points, which we obtain by deforming the corresponding elliptic curve and lifting its point of order p by Hensel's lemma, together with the modular units of Sutherland [41] (see [14, Section 2]), whose linear relations with the canonical forms we verify to a precision beyond their degree bounds.

2.7. **Formal immersions.** Let X be $X_1(p)$ or X_H for a subgroup $H \subseteq \Delta(p)$ such that X_H has positive genus, considered as a smooth curve over $\mathbb{Z}_{(2)}$, and let J be its Jacobian. For a tuple $t = (t_1, \dots, t_\nu)$ of endomorphisms of J, viewed as a homomorphism $t : J \to J^\nu$, and for $d \geq 1$ let

$$f_{t,d} : X^{(d)} \to J^\nu, \qquad E \mapsto t[E - dc_0].$$

Let $\overline{x} \in X^{(d)}(\mathbb{F}_2)$. The cotangent map of $f_{t,d}$ at $\overline{x}$ is the restriction of the space $\sum_i t_i^* H^0(J_{\mathbb{F}_2}, \Omega^1) \subseteq H^0(X_{\mathbb{F}_2}, \Omega^1)$ to the divisor $\overline{x}$, and $f_{t,d}$ is a *formal immersion* at $\overline{x}$ if this cotangent map is surjective, i.e. if the restriction map

$$\sum_i t_i^* H^0(J_{\mathbb{F}_2}, \Omega^1) \to H^0(X_{\mathbb{F}_2}, \Omega^1 \otimes \mathcal{O}_{\overline{x}})$$

is surjective. At a sum $\overline{x} = \sum_k d_k c_k$ of rational cusps, with $c_k = h_k c_0$ for elements $h_k \in \Delta(p)$ which are distinct (modulo H if $X = X_H$), this means that the vectors of the first d_k coefficients of the q-expansions of the forms in $\sum_i t_i^* H^0(J_{\mathbb{F}_2}, \Omega^1)$ at the cusps c_k span $\mathbb{F}_2^d$. As in the proof of [10, Proposition 5.3], this holds if the tuples $(t_i h_k T_j)_{1 \leq i \leq \nu}$, $1 \leq j \leq d_k$, are linearly independent modulo 2.

Lemma 2.11. *Let X be $X_1(p)$ or X_H for a subgroup $H \subseteq \Delta(p)$ such that X_H has positive genus, let J be its Jacobian, let t be a tuple of endomorphisms of J, let $d \geq 1$, and suppose that $f = f_{t,d}$ is a formal immersion at $\overline{x} \in X^{(d)}(\mathbb{F}_2)$.*

a) *Let W be the ring of integers of a finite unramified extension of $\mathbb{Q}_2$. If $D_1, D_2 \in X^{(d)}(W)$ both reduce to $\overline{x}$ and $f(D_1) = f(D_2)$, then $D_1 = D_2$.*
b) *Suppose that $t(J(\mathbb{Q}))$ is finite and that reduction modulo 2 is injective on it (for example, $t(J(\mathbb{Q})) = 0$). If $D_1, D_2 \in X^{(d)}(\mathbb{Q})$ both reduce to $\overline{x}$, then $D_1 = D_2$.*

Proof. Part a) is a slight generalization of [10, Lemma 4.2], and the proof carries over verbatim. In b) the points $f(D_1), f(D_2) \in t(J(\mathbb{Q}))$ have the same reduction, so they are equal, and b) follows from a) (see [10, Corollaries 4.3 and 4.4, Lemma 8.2]). □

Typically $t = \alpha A_q$, where $\alpha \in \mathbb{Z}[\Delta(p)]$ has $\alpha J_H(\mathbb{Q})$ finite (Lemma 2.4) and q is an odd prime. Then $t(J_H(\mathbb{Q})) = 0$ by Lemma 2.5 b). If $\overline{x}$ is a sum of rational cusps, D_2 is its rational lift, and Lemma 2.11 b) shows that no trace divisor reduces to $\overline{x}$. If $\overline{x}$ is the reduction of a known effective divisor D_2 which is not a trace divisor (for example the sum of a point of smaller degree and a rational cusp), it again shows that no trace divisor reduces to $\overline{x}$. Note that if f is a formal immersion at $\overline{x}$, then it is a formal immersion at every effective $\overline{x}' \leq \overline{x}$, so a computation in degree d covers all the cuspidal reductions in smaller degrees: pad a divisor of degree $d' < d$ by adding $d - d'$ to one of its multiplicities.

When f is constant on a family of divisors through $\overline{x}$, for example on a family of pullbacks from a quotient of X, it cannot be a formal immersion at $\overline{x}$, and we use the following relative version, which is an integral form of the relative symmetric Chabauty method of Siksek [38, Section 4].

Lemma 2.12. *Let W be the ring of integers of a finite unramified extension of $\mathbb{Q}_2$, with residue field k. Let S be a smooth scheme of relative dimension d over W, let $\overline{x} \in S(k)$, and let $L \subseteq \widehat{S}_{\overline{x}}$ be a smooth closed formal subscheme of relative dimension r of the formal completion of S at $\overline{x}$. Let $\Phi : S \to A$ be a morphism to a smooth group scheme over W with $\Phi(L) = 0$, and suppose that the kernel of the tangent map of Φ_k at $\overline{x}$ is the tangent space of L_k. Then every $D \in S(W)$ reducing to $\overline{x}$ with $\Phi(D) = 0$ lies on L.*

Proof. Choose formal coordinates $u_1, \dots, u_r, v_1, \dots, v_{d-r}$ at $\overline{x}$ such that L is given by $v = 0$, and functions $g_1, \dots, g_{d-r}$ on A vanishing at 0 such that the differentials of the $\Phi^* g_i$ at $\overline{x}$ are

linearly independent, which is possible by the assumption on the tangent map. As the $\Phi^* g_i$ vanish on L, we can write $\Phi^* g_i = \sum_j m_{ij} v_j$, and the matrix (m_{ij}) is invertible at $\overline{x}$, hence invertible over the completed local ring. So the common zero locus of the $\Phi^* g_i$ is L. □

For divisors on $X_1(p)$ and its quotients we use Lemma 2.12 in the following form.

Lemma 2.13. *Let X be $X_1(p)$ or X_H for a subgroup $H \subseteq \Delta(p)$ such that X_H has positive genus, let J be its Jacobian, let t be a tuple of endomorphisms of J such that $t(J(\mathbb{Q}))$ is finite and reduction modulo 2 is injective on it, let $d \geq 1$, and let $f = f_{t,d}$. Let W be the ring of integers of a finite unramified extension of $\mathbb{Q}_2$, with residue field k, let $\overline{x} \in X^{(d)}(k)$, and let L be a smooth closed formal subscheme of the formal completion of $X_W^{(d)}$ at $\overline{x}$ on which f vanishes. If the kernel of the tangent map of f_k at $\overline{x}$ is the tangent space of L_k (we then say that the rank condition holds), then every $D \in X^{(d)}(\mathbb{Q})$ reducing to $\overline{x}$ lies on L.*

Proof. The point $f(D) \in t(J(\mathbb{Q}))$ reduces to $f(\overline{x}) = 0$, as $\overline{x}$ lies on L. Hence $f(D) = 0$, and Lemma 2.12 applies with $S = X_W^{(d)}$ and $\Phi = f$. □

We apply Lemma 2.13 with $L = R + \pi^* Y^{(r)}$ near $\overline{x}$, where $\pi : X \to Y$ is the quotient by a subgroup H' of $\Delta(p)$ and R is a fixed effective divisor defined over W, typically a non-zero rational cuspidal divisor. Here L is smooth when H' acts freely on the support of $\overline{x} - \overline{R}$, or more generally when the quotient map is tamely ramified there. If t kills $\pi^* J_Y$, then f is constant on L, so it vanishes on L as soon as $t[R + \pi^* E_0 - d c_0] = 0$ for one point E_0 of $Y^{(r)}$. For example, if $t = (h-1)A_q$ with $h \in H'$ and R is a rational cuspidal divisor, then t kills $\pi^* J_Y$, and

$$t[R + \pi^* E_0 - d c_0] = A_q[(h-1)R - d(h-1)c_0] = 0$$

by Lemma 2.5 c). If the rank condition holds, a trace divisor reducing to $\overline{x}$ lies on L, so it contains R, which is impossible if R contains a cusp. In some cases R also contains the unique lifts of the points of $\overline{x}$ that are fixed by a subgroup of order 3 of $\Delta(p)$.

3. Points of prime order over number fields of degree $9 \leq d \leq 22$

In this section we show that the primes listed in Theorem 1.1 belong to $S(d)$.

Lemma 3.1. *If d' divides d, then $S(d') \subseteq S(d)$.*

Proof. Let K' be a number field of degree d' and E/K' an elliptic curve with a point of order p. Let ℓ be a prime which is unramified in K', and α a root of $x^{d/d'} - \ell$. This polynomial is Eisenstein at every prime of K' above ℓ, so $K = K'(\alpha)$ has degree d, and $E(K)$ has a point of order p. □

Lemma 3.2. *If $d \geq 2g(X_1(p))$, then $p \in S(d)$. In particular $11, 13, 17 \in S(d)$ for $d \geq 10$, and $19 \in S(d)$ for $d \geq 14$.*

Proof. Let c be a rational cusp of $X_1(p)$. As $d - 1 \geq 2g - 1$, the Riemann-Roch theorem gives $\ell(dc) = \ell((d-1)c) + 1$, so there is a function f on $X_1(p)$ whose only pole is a pole of order d at c. By Hilbert's irreducibility theorem, the fibre $f^{-1}(t)$ is a closed point of degree d for infinitely many $t \in \mathbb{Q}$, and all but finitely many of these points are not cusps. As $X_1(p)$ is a fine moduli space, each of them gives an elliptic curve with a point of order p over a number field of degree d. The second statement follows as $X_1(11)$, $X_1(13)$, $X_1(17)$ and $X_1(19)$ have genus 1, 2, 5 and 7. □

Most of our explicit examples are of the following form. Let $f \in \mathbb{Q}[t]$ be an irreducible polynomial of degree d, let x be a root of f, put $K = \mathbb{Q}(x)$, and let $y \in K$ be such that (x, y) is a point on Sutherland's model of $X_1(p)$ [40]. Put

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

Then $P = (0, 0)$ is a point of order p on the elliptic curve

$$E(b, c) : \ Y^2 + (1 - c)XY - bY = X^3 - bX^2$$

over K. For each example we check directly that f is irreducible, that $E(b, c)$ is non-singular and that $pP = 0$, so we do not need to know where the examples came from. Most of these examples come from the tables of low degree points on $X_1(p)$ of van Hoeij [43], or from specializations of functions of degree d on $X_1(p)$. For example, for $p = 43$ and $d = 12$ we can take

$$\begin{aligned} f &= t^{12} - t^{11} - 5t^{10} + 6t^9 + 9t^8 - 16t^7 - 3t^6 + 19t^5 - 3t^4 - 12t^3 + t^2 + 4t + 1, \\ 43y &= 35x^{11} - 65x^{10} - 107x^9 + 314x^8 - 34x^7 - 580x^6 + 601x^5 \\ &\quad + 156x^4 - 552x^3 + 219x^2 + 136x - 81, \end{aligned}$$

and for $p = 37$ and $d = 10$ we can take

$$\begin{aligned} f &= t^{10} - 5t^8 + 3t^7 + 10t^6 - 8t^5 - 7t^4 + 9t^3 - 3t + 1, \\ y &= 2x^9 + x^8 - 10x^7 + x^6 + 23x^5 - 6x^4 - 22x^3 + 11x^2 + 9x - 5. \end{aligned}$$

Here $j(E)$ has degree 4 in the first example and degree 10 in the second. The few examples that are not of this form are similar. For instance, for $(d, p) = (22, 67)$ we use a point of order 67 on a twist of $y^2 = x^3 + 1$ over a field of degree 22, which comes from a point with complex multiplication.

Proposition 3.3. *For $9 \leq d \leq 22$, all the primes listed in Theorem 1.1 belong to $S(d)$.*

Proof. By Lemma 3.1, the results for $d \leq 8$ listed in the introduction, [33, Theorem 1.1] for $p \in \{17, 19, 23\}$ and $d = 9$, and Lemma 3.2, it is enough to give an example over a number field of degree d for each of the pairs (d, p) in Table 1. Here we also use Lemma 3.1 for $d \in \{18, 20, 22\}$ with $d' = 9, 10, 11$, respectively. For each of these pairs we give an explicit example as above, and we verify that it has the required properties. □

d	p	d	p
9	29, 31	16	29, 31, 37
10	23, 29, 31, 37	17	23, 29, 31, 37, 41, 43
11	19, 23, 29, 31	18	41, 43
12	23, 29, 31, 43	19	23, 29, 31, 37, 41, 43
13	19, 23, 29, 31, 37	20	41, 43, 47, 61
14	29, 31, 37, 41, 43	21	29, 31, 37, 41, 43, 47
15	23, 29, 31, 37, 43	22	37, 41, 43, 47, 53, 67

TABLE 1. The pairs (d, p) for which we give an explicit point of order p over a number field of degree d.

4. Reduction to finitely many primes

In this section we show that for each $9 \le d \le 22$ it is enough to rule out the primes in Table 4 below. We put $\kappa = 2^{19}/325$, so that Proposition 2.6 a) says that $\operatorname{gon}_{\mathbb{Q}} X_1(p) \ge 8(p^2-1)/\kappa$.

4.1. **Oesterlé's bound and a version at the prime 2.** Let $\mathbb{T} \subseteq \operatorname{End} J_0(p)$ be the Hecke algebra generated over $\mathbb{Z}$ by the Hecke operators T_n, let $e \in H_1(X_0(p), \mathbb{Q})$ be the winding element, i.e. the class of the path from 0 to $i\infty$, let $I = \operatorname{Ann}_{\mathbb{T}}(e)$, and let

$$\pi : J_0(p) \to A = J_0(p)/IJ_0(p)$$

be the winding quotient. The group $A(\mathbb{Q})$ is finite [10, Theorem 2.2]. Following [10, Definition 6.5] we put

$$T'_n = \sum_{m|n} \mu(n/m) T_m, \qquad L_n = T'_{2n} - 2T'_n.$$

For an odd prime M let $\varepsilon_M(a) = 0$ if the representative of $a \in (\mathbb{Z}/M\mathbb{Z})^\times$ in $\{1, \dots, M-1\}$ is less than $M/2$, and $\varepsilon_M(a) = 1$ otherwise.

Lemma 4.1. *Let $m \ge 1$, let ℓ be a prime, let $M > m$ be an odd prime, let $p > 2mM$ be a prime, and let u be such that $pu \equiv 1 \pmod{M}$. If the $m \times (M-1)$ matrix*

$$\big(\varepsilon_M(na) - \varepsilon_M(nu/a)\big)_{1 \le n \le m,\ a \in (\mathbb{Z}/M\mathbb{Z})^\times}$$

has rank m modulo ℓ, then $T_1 e, \dots, T_m e$ are linearly independent in $\mathbb{T}e/\ell\mathbb{T}e$.

Proof. By [10, Lemma 6.7] the entries of the matrix are, up to sign, the intersection numbers of $L_n e \in H_1(X_0(p), \mathbb{Z})$ with the modular symbols $\{0, a/M\}$, so $L_1 e, \dots, L_m e$ are linearly independent in $H_1(X_0(p), \mathbb{F}_\ell)$. The $\mathbb{Z}$-span of $L_1, \dots, L_m$ is the same as that of $(T_2-3)T_1, \dots, (T_2-3)T_m$, and $(T_2-3)\mathbb{T}e \subseteq H_1(X_0(p), \mathbb{Z})$ (see the proofs of [10, Corollaries 6.4 and 6.6]). So if $\sum \lambda_n T_n e \in \ell\mathbb{T}e$ with $\lambda_n \in \mathbb{Z}$, then $\sum \lambda_n (T_2-3) T_n e \in \ell H_1(X_0(p), \mathbb{Z})$, and hence all the λ_n are divisible by ℓ. □

Definition 4.2. Let ℓ be a prime and $d \ge 1$. We say that a prime p is *ℓ-admissible for d* if p divides $\#E(\mathbb{F}_{\ell^f})$ for some elliptic curve E over $\mathbb{F}_{\ell^f}$ with $f \le d$, or if p divides $\ell^f - 1$ or $\ell^f + 1$ for some $f < d$.

Lemma 4.3. *Let $\ell \ne p$ be primes, let K be a number field of degree d, let E/K be an elliptic curve with a point P of order p, and let D_0 be the trace divisor of the point $(E, \langle P \rangle) \in X_0(p)(K)$. If p is not ℓ-admissible for d, then $\overline{D_0}$ (the reduction modulo ℓ) is d times one of the two cusps of $X_0(p)_{\mathbb{F}_\ell}$.*

Proof. Let v be a prime of K above ℓ, with residue field $\mathbb{F}_{\ell^f}$. If E had good reduction at v, then P would reduce to a point of order p, so E has bad reduction at v. The prime to ℓ torsion of $E(K_v)$ injects into the group of components when the reduction is additive, so as this group has order at most 4, the reduction is multiplicative. If P reduces to the identity component, then p divides $\ell^f - 1$ or $\ell^f + 1$, so $f = d$, v is the only prime above ℓ, and over the unramified extension of K_v over which E is a Tate curve, $\langle P \rangle$ is the canonical subgroup μ_p, so $(E, \langle P \rangle)$ reduces to the cusp ∞ at v. Otherwise $\langle P \rangle \ne \mu_p$, and $(E, \langle P \rangle)$ reduces to the cusp 0 at v. Hence either all the points in the support of D_0 reduce to 0, or there is just one prime above ℓ and they all reduce to ∞. □

The following proposition for odd ℓ is the argument of Oesterlé [10, Section 6] (see also [34, Theorem 4.18]). For $\ell = 2$ it is new. The extra factor 2 in $m = 2d$ compensates for the two ways in which reduction modulo 2 behaves worse than reduction modulo an odd prime: the

kernel of reduction on rational torsion is only killed by 2, and the cotangent lattice of the Néron model of A may have index 2^r in its saturation. The second point is dealt with in the following lemma.

Lemma 4.4. *Let $m \geq 1$, and let p be a prime such that $T_1 e, \dots, T_m e$ are linearly independent in $\mathbb{T}e/2\mathbb{T}e$. Let $A_{\mathbb{Z}_2}$ be the Néron model of A over $\mathbb{Z}_2$, let*

$$f_m : X_0(p)^{(m)} \to A, \qquad D \mapsto \pi[D - m\infty],$$

and let $s_1, \dots, s_m$ be the elementary symmetric functions in the q-parameter at ∞, which are formal coordinates on $X_0(p)^{(m)}_{\mathbb{Z}_2}$ at $m\infty$. Then there are formal functions $g_1, \dots, g_m$ on $A_{\mathbb{Z}_2}$ at 0, vanishing at 0, such that

$$f_m^* g_i = 2s_i + Q_i(s_1, \dots, s_m), \qquad Q_i \in (s_1, \dots, s_m)^2.$$

Proof. Let $S = H^0(X_0(p)_{\mathbb{Z}_2}, \Omega^1)$, $M = S[I]$, and $L = \pi^* H^0(A_{\mathbb{Z}_2}, \Omega^1) \subseteq M$. We first show that $2M \subseteq L$. This follows from a theorem of Raynaud [1, Appendix A, Theorem A.1], applied to the exact sequence $0 \to IJ_0(p) \to J_0(p) \to A \to 0$ of abelian varieties with good reduction over $\mathbb{Q}_2$, whose ramification index is $1 = 2 - 1$: the cokernel of the map of tangent spaces of the Néron models over $\mathbb{Z}_2$ is killed by 2 (compare [4, Section 4.4]). Dually, L has index killed by 2 in its saturation, which is M.

The pairing $\mathbb{T} \otimes \mathbb{Z}_2 \times S \to \mathbb{Z}_2$, $(t, \omega) \mapsto a_1(t\omega)$, is perfect (see [1, Lemma 2.1]), so $M \simeq \mathrm{Hom}(\mathbb{T}/I \otimes \mathbb{Z}_2, \mathbb{Z}_2)$. As $\mathbb{T}e \simeq \mathbb{T}/I$, our assumption implies that the map $M \to \mathbb{Z}_2^m$, $\omega \mapsto (a_1(\omega), \dots, a_m(\omega))$, is surjective, where $\omega = \sum a_n(\omega) q^{n-1} dq$ is the q-expansion at ∞.

The cotangent map of f_m at $m\infty$ is $\omega \mapsto (a_1(\pi^*\omega), -a_2(\pi^*\omega), \dots, (-1)^{m-1} a_m(\pi^*\omega))$ [34, Lemma 4.16], so by the two previous paragraphs its image contains $2\mathbb{Z}_2^m$. Hence there are $g_1, \dots, g_m$ as required. □

Proposition 4.5. *Let ℓ be a prime, $d \geq 1$, and put $m = d$ if ℓ is odd and $m = 2d$ if $\ell = 2$. Let $p \neq \ell$ be a prime such that $T_1 e, \dots, T_m e$ are linearly independent in $\mathbb{T}e/\ell\mathbb{T}e$. If $p \in S(d)$, then p is ℓ-admissible for d.*

Proof. Suppose the opposite. By Lemma 4.3, after applying the Atkin-Lehner involution if necessary, there is a non-cuspidal effective divisor D_0 of degree d on $X_0(p)$, defined over $\mathbb{Q}$, with $\overline{D_0} = d\infty$. For $k \geq 1$ let $f_k : X_0(p)^{(k)} \to A$, $D \mapsto \pi[D - k\infty]$. The point $f_d(D_0) \in A(\mathbb{Q})$ is torsion and it reduces to $f_d(d\infty) = 0$.

Suppose first that ℓ is odd. Then $f_d(D_0) = 0$ by Lemma 2.5 a), and f_d is a formal immersion at $d\infty$ modulo ℓ by [34, Theorem 4.18] (see [10, Proposition 6.3]), so $D_0 = d\infty$ by [10, Lemma 4.2], which is a contradiction.

Suppose now that $\ell = 2$, so $m = 2d$. Then $2f_d(D_0) = f_m(2D_0) = 0$ by Lemma 2.5 a). As $\overline{D_0} = d\infty$, the polynomial $E_{D_0}(t) = \prod_j (1 - q_j t)$, where the q_j are the values of q at the points of D_0, has coefficients in $\mathbb{Z}_2$ and is congruent to 1 modulo 2. Hence $E_{2D_0}(t) = E_{D_0}(t)^2 \equiv 1 \pmod 4$, i.e. all the coordinates $s_i(2D_0)$ are in $4\mathbb{Z}_2$, and as $D_0 \neq d\infty$, not all of them are 0. Let $k \geq 2$ be the minimum of their valuations, attained at s_i, and let g_i be as in Lemma 4.4. Then $2s_i(2D_0)$ has valuation $k+1$, while $Q_i(s(2D_0))$ has valuation at least $2k > k+1$. Hence $g_i(f_m(2D_0)) \neq 0$, which contradicts $f_m(2D_0) = 0$. □

Remark 4.6. In particular, if $p > (2^{d/2} + 1)^2$ and $T_1 e, \dots, T_{2d} e$ are linearly independent in $\mathbb{T}e/2\mathbb{T}e$, then $p \notin S(d)$, which is the analogue of Oesterlé's bound with 3 replaced by 2. Using Parent's estimate [34, Proposition 1.9] instead of Lemma 4.1, the same argument should give $p \leq \max\{(2^{d/2}+1)^2, 65(4d)^6\}$ for all $p \in S(d)$ (see the note `dyadic/asymptotic_prime_bound.pdf`), but we do not need this.

For $d \in \{9, 10\}$ Oesterlé's bound $p \leq (3^{d/2}+1)^2$ [10, Theorem 6.1] is smaller than 10^5, and for the larger d we use Proposition 4.5.

Corollary 4.7. *Let $11 \leq d \leq 22$, let ℓ, M and $B(d)$ be as in Table 2, and let $p \in S(d)$. Then $p \leq B(d)$, and if $p > 10^5$, then p is one of the $N(d)$ primes listed in* `large_primes.md`.

Proof. Let $m = d$ if ℓ is odd and $m = 2d$ if $\ell = 2$. We compute that the matrices of Lemma 4.1 have rank m modulo ℓ for all $u \in (\mathbb{Z}/M\mathbb{Z})^\times$ ($d = 11$, $d = 12$, $d \geq 13$), so by Proposition 4.5 every $p \in S(d)$ with $p > 2mM$ is ℓ-admissible for d, for each ℓ in the table. As $2mM < 10^5$ in all cases, it remains to determine the admissible primes. An elliptic curve over $\mathbb{F}_{\ell^f}$ has at most $(\ell^{f/2}+1)^2$ points, and if its trace of Frobenius is divisible by ℓ, it is supersingular, so $j = 0$ for $\ell \in \{2, 3, 5\}$ and $j = 1728$ for $\ell = 7$, and we can list all the possible group orders. Note that an ordinary elliptic curve over $\mathbb{F}_{2^f}$ has a rational point of order 2, so a prime p dividing its order satisfies $2p \leq (2^{f/2}+1)^2$. For $d \geq 13$ this gives $p \leq B(d)$, and in all cases we compute the admissible primes above 10^5. □

d	ℓ	M	$2mM$	$B(d)$	$N(d)$
11	3, 5	53, 73	1166, 1606	177989	21
12	3, 5, 7	61, 59, 59	1464, 1416, 1416	532900	92
13	2	157	8164	8374	0
14	2	157	8792	16641	0
15	2	157	9420	33131	0
16	2	157	10048	66049	0
17	2	181	12308	66049	0
18	2	181	13032	263169	81
19	2	181	13756	525313	196
20	2	229	18320	525313	444
21	2	229	19236	1050024	850
22	2	229	20152	2099200	1488

TABLE 2. The primes ℓ and moduli M used in Lemma 4.1, the resulting bound $B(d)$ for the primes in $S(d)$, and the number $N(d)$ of admissible primes in $(10^5, B(d)]$. For $d \in \{11, 12\}$, $B(d)$ is Oesterlé's bound.

4.2. **The results of Derickx and Stoll.** We will use the following two results of Derickx and Stoll, which we state in our notation (see Lemma 2.5). For $d \geq 1$, let $S_{new}(d)$ be the set of primes p such that $X_1(p)$ has a non-cuspidal closed point of degree d, so that $S(d) = \bigcup_{d'|d} S_{new}(d')$.

Proposition 4.8 ([12, Corollary 7.5])**.** *Let $d \geq 1$ and $p \in S_{new}(d)$. Then one of the following holds:*

a) $p^2 \leq \kappa d + 1$,
b) *d is even and $p \in \{2d+1, 3d+1\}$,*
c) *$(p-1)/(2\,\mathrm{str}(p))$ divides d, and the image of the point on X_H, where $H \subseteq \Delta(p)$ is the subgroup of order $(p-1)/(2\,\mathrm{str}(p))$, has degree $2\,\mathrm{str}(p)d/(p-1)$.*

Proposition 4.9 ([12, Proposition 4.1])**.** *Let $a \in \Delta(p)$ and $\ell \in \{2, 3\}$, and put $n = 2\ell + 1$ if $a \in \{\ell, \ell^{-1}\}$ and $n = 2\ell + 2$ otherwise. Suppose that $(\langle a \rangle - 1)J_1(p)(\mathbb{Q})$ is finite and, if $\ell = 2$, that its 2-primary part is killed by A_2. Let D be an effective divisor of degree d on $X_1(p)$,*

defined over $\mathbb{Q}$, with no cusps in its support. If $nd < \operatorname{gon}_{\mathbb{Q}} X_1(p)$, then $\langle a \rangle D = D$. The same holds with $X_1(p)$ replaced by X_H for a subgroup $H \subseteq \Delta(p)$ and $a \in \Delta(p)/H$.

By Lemma 2.5 b) the assumption for $\ell = 2$ holds if $p \leq 157$. For larger p we use the following lemma.

Lemma 4.10. *Let $h \in \Delta(p)$ be such that $(h-1)J_1(p)(\mathbb{Q})$ is finite, and suppose that there is an endomorphism β of $J_1(p)$ which kills $J_1(p)(\mathbb{Q})_{\mathrm{tors}}$ and restricts to an isogeny of odd degree on $B = (h-1)J_1(p)$. Then $(h-1)J_1(p)(\mathbb{Q})$ has odd order.*

Proof. The group $(h-1)J_1(p)(\mathbb{Q})$ is contained in $B(\mathbb{Q})$ and is killed by β. □

We will apply this lemma with $\beta = A_3$, or a combination of several A_q with q odd. To show that A_3 has odd degree on B we compute its determinant on the rational homology of B, which is the sum of the components of $H_1(X_1(p), \mathbb{Q})$ belonging to the characters χ with $\chi(h) \neq 1$, and on each of them the determinant is an element of the field of values of χ whose norm is odd.

4.3. **Primes above 10^5.**

Lemma 4.11. *Let p be a prime with $p^2 > \kappa d + 1$ and $p \notin \{2d'+1, 3d'+1\}$ for all $d' \mid d$, let $m = (p-1)/2$, and let r be a prime with $v_r(m) > v_r(d)$. If no even character modulo p whose order n satisfies $v_r(n) \geq v_r(m) - v_r(d)$ is strange, then $p \notin S(d)$.*

Proof. The strange characters generate a cyclic group of order $\operatorname{str}(p)$, and by assumption $v_r(\operatorname{str}(p)) < v_r(m) - v_r(d)$. Hence $v_r(m/\operatorname{str}(p)) > v_r(d)$, so $m/\operatorname{str}(p)$ does not divide any divisor d' of d, and the result follows from Proposition 4.8. □

To show that a character is not strange we use the method of [12, Section 5], made rigorous as follows.

Lemma 4.12. *Let χ be a non-trivial even character modulo p of order n, and let $q \nmid 6p(p-1)$ be a prime with $q \equiv 1 \pmod{n}$, so χ takes values in $\mathbb{F}_q$. Let V be the plus part of the space of modular symbols of weight 2, level p and character χ over $\mathbb{F}_q$, let $V_0 \subseteq V$ be its cuspidal subspace, of dimension k, and let $e' = (T_2 - 1 - 2\chi(2))(T_2 - 2 - \chi(2))\{0, \infty\}$, which lies in V_0. If $e', T_2e', \ldots, T_2^{k-1}e'$ are linearly independent, then χ (and every character of order n) is not strange.*

Proof. The space V and the action of T_2 are the reductions of their analogues over the ring of integers of $\mathbb{Q}(\chi)$ localized at a prime above q, so the corresponding vectors in characteristic 0 are linearly independent as well. Hence e' generates the cuspidal part as a module over the Hecke algebra, so its projection to the eigenspace of every newform f with character χ is non-zero. This projection is a non-zero multiple of $L(f, 1)$, so $L(f, 1) \neq 0$. The characters of order n are Galois conjugate. □

In practice we take a random linear functional λ on V_0 and check that the sequence $\lambda(T_2^i e')$, $0 \leq i < 2k$, has linear complexity k, i.e. that it does not satisfy a linear recurrence of length less than k, which implies the assumption of Lemma 4.12. We certify the linear complexity by a rational function ϕ/ψ with $\psi(0) = 1$, $\deg \psi \leq k$, $\deg \phi < k$, $\max(\deg \psi, \deg \phi + 1) = k$, $\gcd(\phi, \psi) = 1$, and $\psi \cdot \sum_i \lambda(T_2^i e')x^i \equiv \phi \pmod{x^{2k}}$. For p up to $2.1 \cdot 10^6$ the dimension k is close to $p/12$, so these are large sparse computations, for which we wrote our own implementation (see Section 7).

Proposition 4.13. *Let $9 \leq d \leq 22$ and $p > 10^5$. Then $p \notin S(d)$.*

Proof. For $d \leq 10$ this follows from Oesterlé's bound, and for $13 \leq d \leq 17$ from Corollary 4.7. For the other d, let p be one of the $N(d)$ primes of Corollary 4.7. For each of them we choose r as in Lemma 4.11 and show, using Lemma 4.12, that no character of the required orders is strange. This requires 73, 656, 615, 1147, 3020, 5289 and 10065 character orders for $d = 11, 12, 18, 19, 20, 21, 22$, respectively, many of which are shared between the degrees ($d = 11$, $d = 12$, $d = 18$, $d \geq 19$). The result follows from Lemma 4.11. □

Michael Stoll has sent us the list of the strange characters modulo all primes $p < 4 \cdot 10^5$ (private communication), which extends [12, Table 2], and this gives an independent check of Proposition 4.13 for $p < 4 \cdot 10^5$. Using his list, we compute that $(p-1)/(2\,\mathrm{str}(p)) \geq 4787$ for all primes $10^5 < p < 4 \cdot 10^5$, so by Proposition 4.8 none of them is in $S(d)$ for $d \leq 22$. As $B(11)$ and $B(18)$ are smaller than $4 \cdot 10^5$, together with Corollary 4.7 this gives a proof of Proposition 4.13 for $d \in \{11, 18\}$ which does not use Lemma 4.12. Moreover, none of the 5450 pairs (p, n) with $p < 4 \cdot 10^5$ for which we showed in the proof of Proposition 4.13 that the characters of order n modulo p are not strange appears in his list. Note that his list does not cover the primes above $4 \cdot 10^5$, which we need for $d = 12$ and $19 \leq d \leq 22$.

4.4. **Primes below 10^5.** For three primes above 157 we check the 2-primary assumption of Proposition 4.9 as follows.

Lemma 4.14. *Let (p, a) be one of $(163, 8)$, $(167, 2)$ and $(181, 64)$. Then $(\langle a \rangle - 1)J_1(p)(\mathbb{Q})$ is finite and has odd order.*

Proof. The group is finite by Lemma 2.4, as 163 and 167 are not strange, and $\langle 64 \rangle$ is trivial on the characters of order 6 modulo 181, which are the strange ones. For $p \in \{163, 167\}$ we compute ($p = 167$) that A_3 restricts to an isogeny of odd degree on $(\langle a \rangle - 1)J_1(p)$, so Lemma 4.10 applies with $\beta = A_3$. For $p = 181$ the operator A_3 has even degree on some components, and we use instead $\beta = EA_{11} + (45 - E)A_3$, where $u = \langle 2 \rangle^2$ (of order 45) and $E = 5N_{u^5} - N_u$, N_g denoting the sum of the powers of g. On the components of $H_1(X_1(181), \mathbb{Q})$ belonging to characters of order 5 and 10, E acts as 45, and on the other components of $(\langle 64 \rangle - 1)J_1(181)$ it acts as 0. We compute that A_{11}, respectively A_3, has odd determinant on these components, so Lemma 4.10 applies. □

Proposition 4.15. *Let $9 \leq d \leq 22$, and let $p < 10^5$ be a prime which is neither one of the primes listed for d in Theorem 1.1 nor one of the primes listed for d in Table 4, and such that $(d, p) \notin \{(14, 127), (16, 127), (16, 193)\}$. Then $p \notin S(d)$.*

Proof. Let $p \in S_{new}(d')$ for some $d' \mid d$. If $p^2 > \kappa d + 1$, then by Proposition 4.8 and [12, Table 2], and as $(d, p) \neq (16, 193)$, p is one of 181 (for $d = 15$), 409 and 1021 (for $d = 17$). We check this for all $p < 10^5$, using that the possible exceptions b) of Proposition 4.8 are in $S(d)$. For these three primes we have $(p - 1)/(2\,\mathrm{str}(p)) = d$, so Proposition 4.8 c) gives a non-cuspidal rational point on $X_0(p)$, which does not exist by Mazur's theorem [25, Theorem 1].

The remaining primes satisfy $p^2 \leq \kappa d + 1$, and as $(d, p) \notin \{(14, 127), (16, 127)\}$, they are either in Table 4 or in Table 3. For (p, a, ℓ, n) and d as in Table 3, the assumptions of Proposition 4.9 hold: $(\langle a \rangle - 1)J_1(p)(\mathbb{Q})$ is finite by Lemma 2.4 (the only strange p in the table is 181, and $\langle a \rangle$ is trivial on the characters of order 6 modulo 181), the gonality bound holds by Proposition 2.6 a) (for $p \in \{163, 173\}$ and $d = 22$ we need its second bound), and the 2-primary assumption holds by Lemma 2.5 b) for $p \leq 157$ and by Lemma 4.14 for the larger p with $\ell = 2$. Hence the trace divisor D of degree d' is invariant under $\langle a \rangle$. As $p > 67$, Lemma 2.3 shows that the orbits of $\langle a \rangle$ on its support have length $\mathrm{ord}(a)$, which is listed in Table 3 and does not divide d'. This is a contradiction. □

p	a	ℓ	n	d	$\mathrm{ord}(a)$
103	2	2	5	9, 10	51
107	2	2	5	9–11	53
109	2	2	5	9–11	18
113	2	2	5	9–12	14
127	2	2	5	10–13, 15	7
131	2	2	5	11–17	65
137	2	2	5	12–18	34
139	2	2	5	12–19	69
149	2	2	5	14–22	74
151	6	2	6	15	75
151	2	2	5	16–22	15
157	2	2	5	16–22	26
163	3	3	7	17, 18	81
163	8	2	6	19–22	27
167	3	3	7	18, 19	83
167	2	2	5	20–22	83
173	3	3	7	19–22	86
179	3	3	7	20–22	89
181	64	2	6	21, 22	15

TABLE 3. The applications of Proposition 4.9. Here $\mathrm{ord}(a)$ is the order of a in $\Delta(p)$.

Lemma 4.16. *Let $Y = X_1(127)/\langle 2\rangle$, where $\langle 2\rangle$ has order 7. Then $\mathrm{gon}_{\mathbb{Q}} Y \geq 20$.*

Proof. We compute that $X_1(127)_{\mathbb{F}_2}$ has 48 supersingular closed points of degree 14, each fixed by $\langle 2\rangle$, and that they map to 48 distinct closed points of degree 2 on $Y_{\mathbb{F}_2}$. Hence $\#Y(\mathbb{F}_4) \geq 96$, so $\mathrm{gon}_{\mathbb{F}_4} Y \geq 96/5$, and $\mathrm{gon}_{\mathbb{Q}} Y \geq \mathrm{gon}_{\mathbb{F}_2} Y \geq \mathrm{gon}_{\mathbb{F}_4} Y \geq 20$. □

Proposition 4.17. *We have $127 \notin S(14)$ and $127 \notin S(16)$.*

Proof. Let $d \in \{14, 16\}$, and suppose that $127 \in S(d)$. As $127 \notin S(d')$ for $d' \leq 8$, there is a trace divisor D of a point of order 127 over a number field of degree d which is a closed point of degree d. Note that $\mathrm{ord}(\langle 2\rangle) = 7$, that 127 is not strange, and that $\mathrm{gon}_{\mathbb{Q}} X_1(127) \geq 84 > 5d$ by Proposition 2.6 a). So Proposition 4.9 with $(a, \ell, n) = (2, 2, 5)$ applies (the 2-primary assumption holds by Lemma 2.5 b)), and D is $\langle 2\rangle$-invariant. By Lemma 2.3 its support consists of orbits of length 7, so $d = 14$, and D is a pullback from $Y = X_1(127)/\langle 2\rangle$, of an effective divisor D' of degree 2. The image of $\langle 3\rangle$ in $\Delta(127)/\langle 2\rangle$ has order 9, $(\langle 3\rangle - 1)J_Y(\mathbb{Q})$ is finite by Lemma 2.4, and $\mathrm{gon}_{\mathbb{Q}} Y \geq 20 > 7 \cdot 2$ by Lemma 4.16, so Proposition 4.9 on Y with $(a, \ell, n) = (3, 3, 7)$ shows that D' is a sum of $\langle 3\rangle$-orbits. These have length 9 or 3, which is a contradiction. □

Proposition 4.18. *We have $193 \notin S(16)$.*

Proof. Suppose the opposite. As $193 \notin S(d')$ for $d' \leq 8$, we have $193 \in S_{new}(16)$. As $\mathrm{str}(193) = 12$ [12, Table 2], Proposition 4.8 shows that the image of the point on $Y = X_H$, where $H \subseteq \Delta(193)$ is the subgroup of order 8, is a non-cuspidal point y of degree 2. If y had non-cuspidal reduction modulo 2, then a point above it on $X_1(193)_{\mathbb{F}_2}$ would have degree at most 16 and j-invariant in $\mathbb{F}_4$, and we compute that there are no such points. The non-rational cusps of $Y_{\mathbb{F}_2}$ have degree 6, so the trace divisor of y reduces to a sum of two rational cusps of Y. We compute

an element α of the Hecke algebra of J_Y with $\alpha J_Y(\mathbb{Q})$ finite, and check that $f_{t,2}$ with $t = \alpha A_3$ is a formal immersion at all these divisors. As $t(J_Y(\mathbb{Q})) = 0$ by Lemma 2.5 b), Lemma 2.11 b) shows that the trace divisor of y is a rational cuspidal divisor, which is a contradiction. □

d	primes p treated in Sections 5 and 6
9	$37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101$
10	$41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101$
11	$37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103$
12	$41, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109$
13	$41, 43, 47, 53, \ldots, 113$
14	$47, 53, \ldots, 113$
15	$41, 47, 53, \ldots, 113$
16	$41, 43, 47, 53, \ldots, 113$
17	$47, 53, \ldots, 113, 127$
18	$47, 53, \ldots, 113, 127, 131$
19	$47, 53, \ldots, 113, 127, 131, 137$
20	$53, 59, 67, 71, \ldots, 113, 127, 131, 137, 139$
21	$53, 59, 61, 67, \ldots, 113, 127, 131, 137, 139$
22	$59, 61, 71, 73, \ldots, 113, 127, 131, 137, 139$

TABLE 4. The primes that remain after Propositions 4.13, 4.15, 4.17 and 4.18. Here $53, \ldots, 113$ denotes all the primes from 53 to 113.

5. The local method at the prime 2

For the pairs (d, p) of Table 4 we follow [10, Section 8] and reduce the trace divisor D modulo 2, writing $\overline{D} = Z + C'$ as in Section 2.2.

5.1. **The census.** For each $f \leq d$ we enumerate all elliptic curves E over $\mathbb{F}_{2^f}$ up to isomorphism, and for each of them all the points of order p of $E(\mathbb{F}_{2^f})$ up to the action of $\mathrm{Aut}(E)$ (all the cyclic subgroups of order p when $E[p] \subseteq E(\mathbb{F}_{2^f})$). This gives all the non-cuspidal closed points of $X_1(p)_{\mathbb{F}_2}$ of degree at most d, together with the action of $\Delta(p)$ on them. For $d \geq 20$ we check the number of these points independently, using class numbers for the ordinary points and the description of the supersingular ones by quaternions.

A non-cuspidal closed point of $X_1(p)_{\mathbb{F}_2}$ is *supersingular* if its j-invariant is 0, and *ordinary* otherwise. We write O_k, SS_k and NC_k for an ordinary closed point, a supersingular closed point and a non-rational cusp of degree k, and C_c for an effective divisor of degree c supported on the rational cusps. The *type* of $\overline{D}$ is the corresponding formal sum, e.g. $O_8 + SS_7 + C_7$. The supersingular points and the non-rational cusps of degree at most 22 at the primes we need are listed in Table 5. An ordinary elliptic curve over $\mathbb{F}_{2^f}$ has a rational point of order 2, so if it has a point of order p, then $2p \leq (2^{f/2} + 1)^2$ by the Hasse bound. Hence ordinary closed points have degree at least 6, and at least 7 for $p \geq 41$, so Z contains at most three ordinary points.

p	supersingular points	non-rational cusps
37	SS_9 (1)	
41	SS_5 (2)	NC_{10} (2)
43	SS_7 (3), SS_{14}	NC_7 (3)
53	SS_{13} (1)	
61	SS_{15} (1), SS_{20}	
73	SS_6 (4), SS_{18}	NC_9 (4)
89	SS_{22} (15)	NC_{11} (4)
97	SS_{16} (2)	
109	SS_9 (3), SS_{12} (3)	NC_{18} (3)
113	SS_7 (4)	NC_{14} (4)
127	SS_{14} (48)	NC_7 (9)
137	SS_{17}	

TABLE 5. The supersingular points and non-rational cusps of degree at most 22 on $X_1(p)_{\mathbb{F}_2}$, for the primes p of Table 4 at which there are any, with the number of closed points of each degree in brackets where we use it. Only the degrees that occur in the relevant range of d are listed.

For each (d, p) we enumerate all the possible types of $\overline{D}$, and for each type all the possible Z up to the action of $\Delta(p)$, which we may use as $\Delta(p)$ commutes with reduction and with all the operators we apply. For $d = 22$ there are 501 types at the 17 primes, and we checked the list by a second, independent enumeration.

5.2. **Reductions supported on the rational cusps.** If $Z = 0$, we use Lemma 2.11 b) on $X_1(p)$ or on an intermediate curve X_H, with $t = \alpha A_q$ for an element α of the Hecke algebra with $\alpha J_H(\mathbb{Q})$ finite and an odd prime q, or with a tuple of such maps, and we check the criterion of [10, Proposition 5.3] for all the multiplicity vectors (d_k) of total degree d. Using the action of $\Delta(p)$ we may assume that $d_0 = \max_k d_k$. When the number of vectors is too large, we instead compute all the linear relations modulo 2 between the vectors of q-expansion coefficients and check that each of them involves more than d coefficients in total (see [10, Lemma 5.5]).

Proposition 5.1. *Let (d, p) be a pair in Table 4 other than $p = 53$ with $d \geq 19$, $p = 101$ with $d \geq 20$, $p = 103$ with $d \geq 17$ and $p = 131$ with $d \geq 18$. Then for a suitable subgroup $H \subseteq \Delta(p)$ and a suitable tuple t as above, $f_{t,d}$ is a formal immersion at every sum of rational cusps of degree d on X_H. In particular, if D is the trace divisor of a point of order p over a number field of degree d, then $Z \neq 0$.*

Proof. The subgroups H, the maps t and the numbers of multiplicity vectors are in the files `formal_immersion.json` in the repository. In several cases (for example at $p = 71$ and $p = 127$ for $d \geq 21$) the computation on the intermediate curve we first tried fails, and we work on $X_1(p)$ itself. If $Z = 0$, then the image of D on X_H is equal to the rational cuspidal divisor with the same reduction by Lemma 2.11 b), which is impossible as D has no cusps in its support. □

The four exceptional cases are treated in Proposition 6.14.

5.3. **The Hecke obstruction.** For $Z \neq 0$ we use the following form of [10, Lemma 8.6].

Lemma 5.2. *Let D be the trace divisor of a point of order p over a number field of degree d, let $\alpha \in \mathbb{Z}[\Delta(p)]$ be such that $\alpha J_1(p)(\mathbb{Q})$ is finite, and let $q \neq p$ be an odd prime. Then the divisor $\alpha A_q Z$ on $X_1(p)_{\mathbb{F}_2}$ is principal.*

Proof. The class $\alpha[D - dc_0]$ is torsion, so $A_q\alpha[D - dc_0] = 0$ by Lemma 2.5 b), and hence its reduction $[\alpha A_q(Z + C' - dc_0)]$ is 0. As α maps rational cusps to sums of rational cusps, and A_q kills each rational cusp by Lemma 2.5 c), $\alpha A_q(C' - dc_0) = 0$ as a divisor. □

We use α as in Table 6, which have $\alpha J_1(p)(\mathbb{Q})$ finite by Lemma 2.4, and almost always $q = 3$. To compute A_3Z we use the 3-isogenies of the elliptic curves representing the points of Z, and we show that $\alpha A_3 Z$ is not principal using Lemma 2.10 with $\mathcal{L} = \mathcal{M} = K$, or $2K$ when the degree of the divisor is too large (at $p \leq 53$, and at 61, 67 and 97 for some d). If a part Z_1 of Z is invariant under a subgroup $H \subseteq \Delta(p)$, we replace α by $(h - 1)\alpha$ with $h \in H$, which kills Z_1. For example, at $p = 41$ we use $\alpha = \langle a\rangle^2 - 1$, where $\langle a\rangle$ generates $\Delta(41)$, for $Z = SS_5 + O_k$, as $\langle a\rangle^2$ fixes both closed points of degree 5.

p	α
$41, 47, 59, 71$	1
61	$\sigma^6 - 1$
97	$\sigma^{12} - 1$, $(\sigma - 1)\Phi_{12}(\sigma)$ or $(\sigma - 1)(\sigma^6 + 1)$
101	$(\sigma - 1)(\sigma^5 + 1)$
other p	$\sigma - 1$

TABLE 6. The elements α used in Lemma 5.2, where σ is a generator of $\Delta(p)$ and Φ_{12} is the 12-th cyclotomic polynomial. They kill the trivial character and the strange characters of orders 6, 12 and 10 modulo 61, 97 and 101.

Proposition 5.3. *Let (d, p) be a pair from Table 4, and let D be the trace divisor of a point of order p over a number field of degree d. Then Z is one of the divisors listed for p in Table 7.*

Proof. By Proposition 5.1, $Z \neq 0$, apart from the four exceptional cases of Proposition 6.14, which are listed in the table. For all the other possibilities for Z given by the census, we compute that $\alpha A_3 Z$ (or, in a few cases, $\alpha A_5 Z$ or $\alpha A_7 Z$) is not principal (pairs and triples, mixed supports, mixed supports at 113 for $d = 22$), which contradicts Lemma 5.2. Each of these computations depends only on Z, so a computation made for one d applies to all larger d as well. For example, at $p = 43$, if Z is one of the three non-rational cusps, then up to sign and a diamond operator $(\langle 3\rangle - 1)A_3 Z$ is $2(2\langle 3\rangle Z - \langle 9\rangle Z - Z)$, and we compute that this divisor is not principal, which excludes $Z = NC_7$ in all degrees. □

These computations involve a very large number of divisors, on curves of genus up to 737. For example, for $d = 22$ alone there are 71224 new orbits under $\Delta(p)$ of ordinary closed points of degree 22. Note that the test cannot succeed if Z is the reduction of a divisor D_1 defined over $\mathbb{Q}$, for example of a point of smaller degree on $X_1(p)$ plus some rational cusps. In fact, some of the ordinary points in Table 7 are reductions of points of degree 10, 12 and 14 on $X_1(37)$, $X_1(41)$ and $X_1(43)$, and the others have a large stabilizer in $\Delta(p)$.

p	Z	d
37	O_6, O_9, SS_9	$9, 11$
37	two orbits of O_{10}	11
41	O_{14}	$15, 16$
43	O_{12}	$13, 16$
43	O_{14}, O_{15}, SS_{14}, $2SS_7$, $2NC_7$, $SS_7 + NC_7$	16
53	SS_{13}	13–21
53	0	19–21
61	SS_{15}	15–19, 21, 22
61	SS_{20}, O_{20}	$21, 22$
73	sums of SS_6, NC_9 and SS_{18}	9–22
89	NC_{11}, $2NC_{11}$, SS_{22}	11–22
97	SS_{16}	16–22
101	0	20–22
103	0	17–22
109	SS_9, NC_{18}, $2SS_9$, $SS_9 + SS_{12}$	12–22
113	$2SS_7$, $3SS_7$, NC_{14}, $SS_7 + NC_{14}$	14–22
113	O_8, $2O_8$, $O_8 + SS_7$, $O_8 + NC_{14}$	13–22
127	sums of NC_7 and SS_{14}	17–22
127	O_9, $2O_9$, $O_9 + NC_7$	17–22
131	0	18–22
137	SS_{17}, O_{17}	19–22

TABLE 7. The reductions Z that are not excluded by Propositions 5.1 and 5.3, and the degrees d in which they have to be considered. Here O_k denotes the exceptional ordinary closed points described in Section 6, and $Z = 0$ means that $\overline{D}$ is supported on the rational cusps.

6. The remaining reductions

For the pairs (d, p) of Table 4, Proposition 5.3 shows that the reduction Z of a trace divisor is one of the divisors in Table 7, and the propositions of this section exclude them. Most of the cases are dealt with by Lemma 2.9, in which case we give the element h, the reason why $y = 0$ (if we use it), and the relevant inequality for the gonality, which always comes from Proposition 2.6. All the statements that h fixes a closed point of $X_1(p)_{\mathbb{F}_2}$ are checked on the elliptic curves representing these points.

6.1. The prime 37.

Lemma 6.1. *Let K be a number field of degree 9, and let E/K be an elliptic curve with $j(E) \in \{-7 \cdot 11^3, -7 \cdot 137^3 \cdot 2083^3\}$. Then $E(K)$ has no point of order 37.*

Proof. These are the j-invariants of the curves 1225.b2 and 1225.b1, and as $j(E) \neq 0, 1728$, E is a quadratic twist of one of them over K. Hence the x-coordinate of a point of order 37 of $E(K)$ would be a root in K of the 37-division polynomial of one of these curves. But we compute that the irreducible factors of these division polynomials have degrees $6, 6, 6, 666$ and $18, 222, 222, 222$, none of which divides 9. □

Proposition 6.2. *We have $37 \notin S(9)$ and $37 \notin S(11)$.*

Proof. Let $d \in \{9, 11\}$, and let D be the trace divisor of a point of order 37 over a number field K of degree d. As $37 \notin S(1) \cup S(3)$, D is a closed point of degree d. By Propositions 5.1 and 5.3, Z is one of the orbits considered below. We compute that the common kernel of A_3 and A_5 on $H_1(X_1(37), \mathbb{Z}) \otimes \mathbb{F}_2$, which contains $J_1(37)(\mathbb{Q})[2]$ by Lemma 2.5 b), is 0. So $y = 0$ in Lemma 2.9, and we have $\mathrm{gon}_{\mathbb{Q}} X_1(37) = 18$. As 37 is not strange, $(h-1)J_1(37)(\mathbb{Q})$ is finite for every $h \in \Delta(37)$ by Lemma 2.4.

Suppose first that $Z = O_6$, one of 3 closed points of degree 6 fixed by $h = \langle 8 \rangle$, of order 6. Then $c = d - 6 \in \{3, 5\}$, and $18 > d + c$, so $6 \mid c$ by Lemma 2.9, which is a contradiction.

Suppose now that Z is one of the 2 ordinary closed points of degree 9, or the supersingular closed point of degree 9, all of which are fixed by $h = \langle 4 \rangle$, of order 9. Then $c \in \{0, 2\}$ and $18 > d + c$, so $hD = D$ and $9 \mid c$. Hence $c = 0$, $d = 9$, and by Lemma 2.3 the support of D is a single orbit of $\langle 4 \rangle$, so the image of D on $X_0(37)$ is a non-cuspidal rational point. The j-invariants of these points are $-7 \cdot 11^3$ and $-7 \cdot 137^3 \cdot 2083^3$ [26, Section 5], which contradicts Lemma 6.1.

Suppose finally that $d = 11$ and $Z = O_{10}$, so $c = 1$. For one of the two orbits, Z is fixed by $h = \langle 6 \rangle$, of order 2, and as $18 > 12$, Lemma 2.9 gives $2 \mid 1$. The other orbit consists of the reductions of the closed points of degree 10 in the supports of the trace S of the point of order 37 of Section 3 and of its images under $\Delta(37)$ (we check this). Replacing S by such an image we can assume $\overline{S} = Z$, so D and $S + C$ both reduce to $Z + C'$. We compute that for $t = \langle 2 \rangle - 1$ the map $f_{t,11}$ is a formal immersion at $Z + \overline{c_1}$ for each of the 18 rational cusps c_1. The group $tJ_1(37)(\mathbb{Q})$ is finite, and as $J_1(37)(\mathbb{Q})[2] = 0$, reduction is injective on it, so $D = S + C$ by Lemma 2.11 b), which is a contradiction as D contains no cusps. □

6.2. **The primes** 41 **and** 43.

Proposition 6.3. *Let $d \in \{15, 16\}$, and let D be the trace divisor of a point of order* 41 *over a number field of degree d. Then $Z \neq O_{14}$.*

Proof. Here O_{14} is one of the 10 closed points of degree 14 which are the reductions of the closed points of degree 14 in the supports of the trace S of an explicit point of degree 14 on $X_1(41)$ and of its images under $\Delta(41)$, as we check. Suppose that $Z = O_{14}$. Replacing S by one of these images we can assume $\overline{S} = Z$, so D and $S + C$ both reduce to $Z + C'$, where $c = d - 14 \in \{1, 2\}$. As $J_1(41)(\mathbb{Q})$ is finite (Lemma 2.4), the tuple $t = (A_3, A_5, A_7)$ kills $J_1(41)(\mathbb{Q})$ by Lemma 2.5 b), and we compute that $f_{t,d}$ is a formal immersion at $Z + C'$ for all the 20 (for $d = 15$) and 210 (for $d = 16$, code) possible C'. So $D = S + C$ by Lemma 2.11 b), which is impossible as D contains no cusps and $C \neq 0$. □

For $p = 43$ and $d = 16$ we need the following lemma.

Lemma 6.4. *Reduction modulo* 2 *is injective on $J_1(43)(\mathbb{Q})_{\mathrm{tors}}$.*

Proof. Let $Y = X_1(43)/\langle 2 \rangle$, where $\langle 2 \rangle$ has order 7, and let $f : X_1(43) \to Y$ be the quotient map. The curve Y has genus 9, and we compute that J_Y contains an elliptic curve A isogenous to 43.a1, whose isogeny class consists of one curve with trivial rational torsion, so $A(\mathbb{Q})[2] = 0$, that $B = J_Y/A$ has rank 0, and that the numbers of points of B over $\mathbb{F}_3$, $\mathbb{F}_5$ and $\mathbb{F}_{23}$ have greatest common divisor $532 = 4 \cdot 133$. Hence $J_Y(\mathbb{Q})[2]$ injects into $B(\mathbb{Q})_{\mathrm{tors}}$, which injects into $B(\mathbb{F}_3)$, $B(\mathbb{F}_5)$ and $B(\mathbb{F}_{23})$, so $\#J_Y(\mathbb{Q})[2] \leq 4$. Let c_1, c_2, c_3 be the rational cusps of Y. The divisors $38(c_2 - c_1)$ and $38(c_3 - c_1)$ are principal, and we compute that the reductions of $x_1 = 19[c_2 - c_1]$, $x_2 = 19[c_3 - c_1]$ and $x_1 + x_2$ are non-zero. So $J_Y(\mathbb{Q})[2] = \{0, x_1, x_2, x_1 + x_2\}$, and reduction is injective on it.

Now let $x \in J_1(43)(\mathbb{Q})_{\mathrm{tors}}$ with $\overline{x} = 0$. Then $2x = 0$, so $f_*x \in J_Y(\mathbb{Q})[2]$ has reduction 0, and hence $f_*x = 0$. We compute that $\langle 2 \rangle$ acts trivially on the common kernel of A_3, A_5 and A_7 on $H_1(X_1(43), \mathbb{Z}) \otimes \mathbb{F}_2$, which contains x. Hence $0 = f^*f_*x = \sum_{i=0}^{6} \langle 2 \rangle^i x = 7x = x$. □

Proposition 6.5. *Let $d \in \{13, 16\}$, and let D be the trace divisor of a point of order 43 over a number field of degree d. Then Z is not one of the divisors listed for 43 in Table 7.*

Proof. As 43 is not strange, $(h-1)J_1(43)(\mathbb{Q})$ is finite for every $h \in \Delta(43)$ by Lemma 2.4. The 7 closed points O_{12} are the reductions of the closed points of degree 12 in the supports of the trace S of the point of order 43 of Section 3 and its images under $\Delta(43)$, as we check, and the 21 closed points O_{14} are, in the same way, the reductions of the trace S of an explicit point of degree 14 on $X_1(43)$ from the tables of [43] and its images (check). If $d = 13$ and $Z = O_{12}$, or $d = 16$ and $Z = O_{14}$, then replacing S by one of its images we can assume $\overline{S} = Z$, so D and $S + C$ both reduce to $Z + C'$, where $c = d - \deg Z \geq 1$. For $d = 13$ and $Z = O_{12}$ we compute that $f_{t,13}$ is a formal immersion at $Z + \overline{c_1}$ for all the 21 rational cusps c_1, with $t = (\langle 3 \rangle^{-1} - 1)\langle 11 \rangle^{-1} A_{11}$, which kills $J_1(43)(\mathbb{Q})$, and for $d = 16$ and $Z = O_{14}$ we compute that $f_{t,16}$ is a formal immersion at all the 231 divisors $Z + C'$, with t combining several maps αA_q, $q \in \{3, 5, 7\}$, with $\alpha J_1(43)(\mathbb{Q})$ finite. In both cases Lemma 2.11 b) gives $D = S + C$, which is impossible as D contains no cusps.

The remaining cases are for $d = 16$. By Lemma 6.4, $y = 0$ in Lemma 2.9, and $\mathrm{gon}_{\mathbb{Q}} X_1(43) = 24$. If $Z = O_{12}$ or Z is one of the two orbits O_{15}, then Z is fixed by $h = \langle 37 \rangle$, of order 3, and $c \in \{4, 1\}$, so as $24 > 16 + c$, Lemma 2.9 gives $3 \mid c$, which is a contradiction. If $Z \in \{SS_{14}, 2SS_7, 2NC_7, SS_7 + NC_7\}$, then Z is fixed by $h = \langle 2 \rangle$, of order 7, and $c = 2$, so as $24 > 18$ we get $7 \mid 2$, which is again a contradiction. □

6.3. **The primes 53 and 61.**

Proposition 6.6. *Let $13 \leq d \leq 21$, and let D be the trace divisor of a point of order 53 over a number field of degree d. Then $Z \neq SS_{13}$.*

Proof. There is a unique supersingular closed point SS_{13} of degree 13, and $h = \langle 4 \rangle$, of order 13, acts simply transitively on its geometric points. As 53 is not strange, $(h-1)J_1(53)(\mathbb{Q})$ is finite, and we compute that $J_1(53)(\mathbb{Q})[2] = 0$, so $y = 0$ in Lemma 2.9.

Suppose that $Z = SS_{13}$, so $c = d - 13$. If $d = 13$, then as $\mathrm{gon}_{\mathbb{Q}} X_1(53) > 13$, Lemma 2.9 gives $hD = D$, and by Lemma 2.3 D is a single orbit of $\langle 4 \rangle$, so its image on $X_0(53)$ is a non-cuspidal rational point, which does not exist [25, Theorem 1]. If $14 \leq d \leq 16$, then $d + c \leq 19 < 20 \leq \mathrm{gon}_{\mathbb{Q}} X_1(53)$, and Lemma 2.9 gives $13 \mid c$, which is a contradiction. For $17 \leq d \leq 21$ we use Lemma 2.13 with $L = C + \pi^*Y$, where $\pi : X_1(53) \to Y = X_1(53)/\langle 4 \rangle$ is the quotient map, and $t = ((h-1)A_3, (h-1)A_5)$. Here t kills $J_1(53)(\mathbb{Q})$ and π^*J_Y, and $t[C + \pi^*E_0 - dc_0] = 0$ for every point E_0 of Y, as $h - 1$ kills π^*E_0 and A_q kills rational cuspidal divisors. We compute that the rank condition holds for all the possible C', so D lies on L and contains $C \neq 0$, which is a contradiction. □

Lemma 6.7. a) *We have $J_1(61)(\mathbb{Q})[2] = 0$.*

b) *Let $W = X_1(61)/\langle 4 \rangle$, where $\langle 4 \rangle$ has order 15, and let s be the automorphism of W induced by $\langle 2 \rangle$. Then W has genus 8, s is an involution with $W/\langle s \rangle = X_0(61)$, $(s-1)J_W(\mathbb{Q})$ is finite, $J_W(\mathbb{Q})[2] = 0$, and W has no map of degree 2 or 3 to $\mathbb{P}^1$ defined over $\mathbb{Q}$.*

Proof. We compute a), and that W has genus 8. The group $\Delta(61)/\langle 4 \rangle$ has order 2 and is generated by the image of $\langle 2 \rangle$, so s is an involution and $W/\langle s \rangle = X_1(61)/\Delta(61) = X_0(61)$. The characters trivial on $\langle 4 \rangle$ have order at most 2, and the strange characters modulo 61 have

order 6, so $(s-1)J_W(\mathbb{Q})$ is finite by Lemma 2.4. The pullback $J_W \to J_1(61)$ is injective on 2-torsion, as its composition with the pushforward is multiplication by 15, so $J_W(\mathbb{Q})[2] = 0$ by a).

The curve $X_0(61)$ has genus 4 and no map of degree at most 3 to $\mathbb{P}^1$ over $\mathbb{Q}$: its canonical model is a complete intersection of a quadric and a cubic in $\mathbb{P}^3$, and the discriminant of the quadric is not a square, so the two g^1_3's are conjugate over $\mathbb{Q}(i)$ (see [15, 16] and our check). Suppose that $u : W \to \mathbb{P}^1$ has degree $e \in \{2, 3\}$. As $g(W) = 8 > (e-1)^2$, the Castelnuovo-Severi inequality implies that u is the unique map of degree e to $\mathbb{P}^1$ up to automorphisms of $\mathbb{P}^1$, so $u \circ s = \beta \circ u$ for some $\beta \in \mathrm{PGL}_2(\mathbb{Q})$ with $\beta^2 = 1$. If $\beta = 1$, then u factors through $W \to X_0(61)$, which is impossible as $e \leq 3$. Otherwise u induces a map $X_0(61) \to \mathbb{P}^1/\langle\beta\rangle \simeq \mathbb{P}^1$ of degree e, which is again impossible. □

Proposition 6.8. *Let $d \in \{15, \ldots, 19, 21, 22\}$, and let D be the trace divisor of a point of order 61 over a number field of degree d. Then $Z \notin \{SS_{15}, SS_{20}, O_{20}\}$.*

Proof. There is a unique supersingular closed point SS_{15} of degree 15, and it is fixed by all of $\Delta(61)$. Let $h = \langle 3\rangle = \langle 2\rangle^6$, of order 5. As the strange characters modulo 61 have order 6, $(h-1)J_1(61)(\mathbb{Q})$ is finite by Lemma 2.4, and $J_1(61)(\mathbb{Q})[2] = 0$ by Lemma 6.7 a), so $y = 0$ in Lemma 2.9. Note that $\mathrm{gon}_{\mathbb{Q}} X_1(61) > 18$ by Proposition 2.6 a).

Suppose that $Z = SS_{15}$. If $d = 16$, then $c = 1$, and Lemma 2.9 gives $5 \mid 1$. If $d \in \{17, 18, 19, 21, 22\}$, we use Lemma 2.13 with $L = C + \pi^* Y^{(3)}$, where $\pi : X_1(61) \to Y = X_1(61)/\langle h\rangle$ is the quotient map, and $t = ((h-1)A_3, (h-1)A_5)$. Here t kills $J_1(61)(\mathbb{Q})$ and $\pi^* J_Y$, and $t[C + \pi^* E_0 - dc_0] = 0$ for every point E_0 of $Y^{(3)}$, as $h - 1$ kills $\pi^* E_0$ and A_q kills rational cuspidal divisors. We compute that the rank condition holds for all possible C', so D contains $C \neq 0$, which is impossible. In the same way, for $d \in \{21, 22\}$ and $Z \in \{SS_{20}, O_{20}\}$, where O_{20} is an orbit of 6 closed points which are pullbacks from Y, we use $L = C + \pi^* Y^{(4)}$ (SS_{20}, O_{20}).

It remains to deal with $d = 15$ and $Z = SS_{15}$, so $c = 0$. By Lemma 2.9 $hD = D$, so by Lemma 2.3 D is a pullback from Y, $D = \pi^* D_Y$, and D_Y is a closed point of degree 3. Let W and s be as in Lemma 6.7. The image D_W of D_Y on W is a closed point of degree 3, as a rational point would map to a non-cuspidal rational point on $X_0(61)$. Its reduction is fixed by s, as $\overline{D} = SS_{15}$ is fixed by $\Delta(61)$. By Lemma 6.7 b) and Lemma 2.8 (with $C = 0$ and condition i)), $sD_W \sim D_W$, and as $\mathrm{gon}_{\mathbb{Q}} W \geq 4$, $sD_W = D_W$. As 2 and 3 are coprime, s fixes each of the three geometric points of D_W. If w is one of them and x is a point of D above it, then $\langle 2\rangle x = gx$ for some $g \in \langle 4\rangle$, so x is fixed by $\langle 2\rangle g^{-1} \neq 1$. This contradicts Lemma 2.2, as x has degree $15 < 20$. □

6.4. **The prime 73.**

Lemma 6.9. *Let $Y = X_1(73)/\langle 2\rangle$, where $\langle 2\rangle$ has order 9. Then every non-cuspidal point of Y has degree at least 3.*

Proof. A non-cuspidal point of Y of degree at most 2 maps to a non-cuspidal point of degree at most 2 on $X_0(73)$. There are no non-cuspidal rational points on $X_0(73)$ [25, Theorem 1], and the quadratic points were determined by Box [8, Section 4.7]. They have 11 different j-invariants (3 of them quadratic and not CM, and 8 rational CM j-invariants). For each of them we check, using the action of Frobenius on $E[73]$ at a prime which splits in the corresponding quadratic field, that no point of Y of degree at most 2 lies above it. □

Proposition 6.10. *Let $9 \leq d \leq 22$, and let D be the trace divisor of a point of order 73 over a number field of degree d. Then Z is not a non-zero sum of points SS_6, NC_9 and SS_{18}.*

Proof. Let $h = \langle 2 \rangle$, of order 9. It fixes each of the 4 supersingular closed points of degree 6 and the 4 non-rational cusps (of degree 9), and the points of degree 18, and the subgroup $\langle 8 \rangle$ of order 3 fixes the geometric points of degree 6. As 73 is not strange, $(h-1)J_1(73)(\mathbb{Q})$ is finite. We compute that h acts trivially on the common kernel of A_3 and A_5 on $H_1(X_1(73), \mathbb{Z}) \otimes \mathbb{F}_2$, which contains $J_1(73)(\mathbb{Q})[2]$, so $y = 0$ in Lemma 2.9 (condition ii) of Lemma 2.8), and $\operatorname{gon}_{\mathbb{Q}} X_1(73) > 26$. As $d < 24 = (73-1)/3$, the orbits of $\langle 2 \rangle$ on the support of D have length 9 (Lemma 2.3).

Suppose that Z is a non-zero sum of points SS_6, NC_9 and SS_{18}, and let $e = \deg Z$, so $c = d - e$ and $e \in \{6, 9, 12, 15, 18, 21\}$. Suppose first that $d + c = 2d - e \leq 26$. Then Lemma 2.9 gives $hD = D$ and $9 \mid c$, and as the orbits of h have length 9, 9 divides d. Hence $d \in \{9, 18\}$, and by Lemma 2.3 D is a pullback from $Y = X_1(73)/\langle 2 \rangle$, of an effective divisor of degree $d/9 \leq 2$ with no cusps in its support. This contradicts Lemma 6.9.

Suppose now that $2d - e > 26$. Then $d \geq 17$, and Z and d are as in Table 8. In these cases we use Lemma 2.13 with $t = ((h-1)A_3, (h-1)A_5)$ and

$$L = Z_0 + R + \pi^* Y^{(r)},$$

where $\pi : X_1(73) \to Y$ is the quotient map, Z_0 is the divisor of degree $6k$ whose points are the unique lifts of the geometric points of SS_6 in Z that are fixed by $\langle 8 \rangle$ (here k is the number of points SS_6 in Z), $C' = \overline{R} + \pi^* E'$ with E' a sum of r' cusps of Y, R has no full orbit of $\langle 2 \rangle$ in its support, and $r = r'$ plus the number of points NC_9 in Z (which are pullbacks of cusps of Y). As h commutes with $\langle 8 \rangle$ and permutes the geometric points of each point SS_6, it fixes Z_0. So t kills $J_1(73)(\mathbb{Q})$ and $\pi^* J_Y$, and $t[Z_0 + R + \pi^* E_0 - dc_0] = 0$ for every point E_0 of $Y^{(r)}$, as $h - 1$ kills Z_0 and $\pi^* E_0$ and A_q kills the rational cuspidal divisor $(h-1)(R - dc_0)$. We compute (NC_9, two or three non-ordinary points) that the rank condition holds in all cases, so D lies on L. If $R \neq 0$, then D contains a cusp, which is impossible. If $R = 0$ and $k > 0$, then D contains a point fixed by $\langle 8 \rangle$, which contradicts Lemma 2.2. If $R = 0$ and $k = 0$, then $Z = NC_9$, $d = 18$, and D is a pullback from Y of an effective divisor of degree 2 with no cusps in its support, which contradicts Lemma 6.9. □

d	Z
17	SS_6
18	SS_6, NC_9
19	SS_6, NC_9
20	SS_6, NC_9, $2SS_6$
21	SS_6, NC_9, $2SS_6$, $SS_6 + NC_9$
22	SS_6, NC_9, $2SS_6$, $SS_6 + NC_9$

TABLE 8. The reductions at 73 for which we use Lemma 2.13.

6.5. The primes 89 and 97.

Proposition 6.11. *Let $11 \leq d \leq 22$, and let D be the trace divisor of a point of order 89 over a number field of degree d. Then $Z \notin \{NC_{11}, 2NC_{11}, SS_{22}\}$.*

Proof. Let $h = \langle 2 \rangle$, of order 11, which fixes the 4 non-rational cusps. As 89 is not strange, $(g-1)J_1(89)(\mathbb{Q})$ is finite for every $g \in \Delta(89)$. We compute that A_3 has odd degree on $(h-1)J_1(89)$, so $y = 0$ in Lemma 2.9 (condition iii) of Lemma 2.8), and $\operatorname{gon}_{\mathbb{Q}} X_1(89) > 39$. If $Z = NC_{11}$, then $c = d - 11$ and $d + c \leq 33$, so Lemma 2.9 gives $hD = D$ and $11 \mid c$. If $c = 0$,

then $d = 11$, D is a single orbit of $\langle 2\rangle$ by Lemma 2.3, and its image on $X_0(89)$ is a non-cuspidal rational point, which does not exist [25, Theorem 1]. So $c = 11$ and $d = 22$.

It remains to deal with $d = 22$ and $Z \in \{NC_{11}, 2NC_{11}, SS_{22}\}$. The supersingular closed points of degree 22 form 5 orbits under $\Delta(89)$, of lengths $4, 4, 4, 2, 1$. For the first three, $\alpha A_3 Z$ or $\alpha A_5 Z$ is not principal (Proposition 5.3), and the other two are fixed by h. Hence, by Lemma 2.9 and Lemma 2.3, in all the remaining cases D is a pullback from $Y = X_1(89)/\langle 2\rangle$, of a divisor D' of degree 2. The curve Y has genus 27, and we compute that $\#Y(\mathbb{F}_2) = 8$ and $\#Y(\mathbb{F}_4) = 38$, so $\operatorname{gon}_{\mathbb{Q}} Y \geq \operatorname{gon}_{\mathbb{F}_4} Y \geq 8$.

If Z contains a non-rational cusp, then $\overline{D'}$ is a sum of two cusps of $Y_{\mathbb{F}_2}$, which are defined over $\mathbb{F}_2$. Let h' be a generator of $\Delta(89)/\langle 2\rangle$. We compute that $f_{t,2}$ on $Y^{(2)}$, with t combining the maps $(h'-1)B_q A_q$ for several primes q, is a formal immersion at all the 36 sums of two such cusps. By Lemma 2.4 and Lemma 2.5 (note that $\langle 2\rangle$ has odd order 11), t kills $J_Y(\mathbb{Q})$ and all the cuspidal divisors on Y. So $f_{t,2}$ maps D' and the cuspidal divisor lifting $\overline{D'}$ (which is defined over an unramified extension of $\mathbb{Q}_2$) to 0, and they are equal by Lemma 2.11 a), which is a contradiction.

If $Z = SS_{22}$, let ι be the element of order 2 of $\Delta(89)/\langle 2\rangle$, which is cyclic of order 4. It fixes $\overline{D'}$, and $(\iota - 1)J_Y(\mathbb{Q})$ is finite, so by Lemma 2.8 (with $C = 0$), $2\iota D' \sim 2D'$. As $\operatorname{gon}_{\mathbb{Q}} Y > 4$, it follows that $\iota D' = D'$. A point of Y fixed by ι lies below a point of $X_1(89)$ fixed by a non-trivial element of $\Delta(89)$, which has degree at least 30 by Lemma 2.2, so it has degree at least 3. Hence ι has no fixed points in the support of D', so $D' = y + \iota(y)$ for a point y of degree at most 2, and the image of D' on $Y/\langle\iota\rangle$ is twice a rational point. Its image on $X_0(89)$ is a non-cuspidal rational point, which does not exist. □

At $p \in \{97, 101\}$ we also need operators that kill the part of $J_1(p)$ belonging to the strange characters. We compute that for these p the newforms with a strange character form a single Galois orbit, and that their coefficients lie in the field of values of their characters. Hence each T_n acts on the corresponding abelian subvariety $B_p \subseteq J_1(p)$ through $\mathbb{Z}[\Delta(p)]$, and we put $\beta_n = T_n - a_n$, where $a_n \in \mathbb{Z}[\Delta(p)]$ is such that β_n kills B_p. For every $h \in \Delta(p)$, the endomorphism $(h-1)\beta_n$ kills B_p and the part of $J_1(p)$ with trivial character, so $(h-1)\beta_n J_1(p)(\mathbb{Q})$ is finite by Lemma 2.4.

Lemma 6.12. *Let $H_8 \subseteq \Delta(97)$ be the subgroup of order 8, let $W = X_1(97)/H_8$, and let h' be an element of order 3 of $\Delta(97)/H_8$. Then W has genus 41, $(h'-1)J_W(\mathbb{Q})$ is finite, A_3 restricts to an isogeny of odd degree on $(h'-1)J_W$, and $\operatorname{gon}_{\mathbb{Q}} W \geq 7$.*

Proof. The Jacobian J_W corresponds to the characters modulo 97 which are trivial on H_8, i.e. of order dividing 6, and the strange characters have order 12, so $(h'-1)J_W(\mathbb{Q})$ is finite by Lemma 2.4. We compute that W has genus 41 and that A_3 has odd degree on $(h'-1)J_W$. A map $W \to \mathbb{P}^1$ of degree k gives a map $X_1(97) \to \mathbb{P}^1$ of degree $8k$, and $\operatorname{gon}_{\mathbb{Q}} X_1(97) \geq 49$ by Proposition 2.6 a), so $\operatorname{gon}_{\mathbb{Q}} W \geq 49/8$. □

Proposition 6.13. *Let $16 \leq d \leq 22$, and let D be the trace divisor of a point of order 97 over a number field of degree d. Then $Z \neq SS_{16}$.*

Proof. The two supersingular closed points of degree 16 are fixed by the subgroup $H_4 \subseteq \Delta(97)$ of order 4, and their geometric points are fixed by the subgroup H_3 of order 3. As the strange characters modulo 97 have order 12, they are trivial on H_4, so $(h-1)J_1(97)(\mathbb{Q})$ is finite for $h \in H_4$ by Lemma 2.4, and Proposition 2.6 a) gives $\operatorname{gon}_{\mathbb{Q}} X_1(97) \geq 49$.

Suppose that $Z = SS_{16}$, and let h be a generator of H_4. If $16 \leq d \leq 19$, then $c = d - 16 \leq 3$ and $2(d + c) \leq 44 < 49$, so Lemma 2.9 gives $hD = D$ and $4 \mid c$, so $c = 0$ and $d = 16$. As $16 < (97 - 1)/3$, D is a pullback from $X_1(97)/H_4$ (Lemma 2.3). Let W and h' be as

in Lemma 6.12. The image D_W of D on W is a closed point of degree $m \in \{2,4\}$, and its reduction is fixed by h', as the geometric points of SS_{16} are fixed by H_3, whose image in $\Delta(97)/H_8$ is generated by h'. By Lemma 6.12 and Lemma 2.5 b), condition iii) of Lemma 2.8 holds for $X = W$, $s = h'$ and $\beta = A_3$, so Lemma 2.8 (with $C = 0$) gives $h'D_W \sim D_W$, and as $\mathrm{gon}_{\mathbb{Q}} W \geq 7 > m$, $h'D_W = D_W$. As $3 \nmid m$, h' fixes each geometric point of D_W, so the points of D are fixed by non-trivial elements of $\Delta(97)$, which contradicts Lemma 2.2.

If $20 \leq d \leq 22$, we use Lemma 2.13 with

$$L = Z_0 + R + \pi^* Y^{(r)},$$

where $\pi : X_1(97) \to Y = X_1(97)/H_3$ is the quotient map, Z_0 is the divisor of degree 16 whose points are the lifts of the geometric points of SS_{16} fixed by H_3, $C' = \overline{R} + \pi^* E'$ with E' a sum of r cusps of Y, and R has no full orbit of H_3 in its support. Here we use $t = (h_3 - 1)\beta_n A_q$, where h_3 generates H_3 and q is odd. As $(h_3 - 1)\beta_n J_1(97)(\mathbb{Q})$ is finite, t kills $J_1(97)(\mathbb{Q})$ by Lemma 2.5 b). It also kills $\pi^* J_Y$, and $t[Z_0 + R + \pi^* E_0 - dc_0] = 0$ for every point E_0 of $Y^{(r)}$, as $h_3 - 1$ kills Z_0 and $\pi^* E_0$ and A_q kills rational cuspidal divisors. We compute that the rank condition holds. So D contains R, which is impossible if $R \neq 0$, or Z_0, which contradicts Lemma 2.2. □

6.6. **Reductions supported on the rational cusps at 53, 101, 103 and 131.**

Proposition 6.14. *Let (d,p) be one of $(19,53)$, $(20,53)$, $(21,53)$, $(20,101)$, $(21,101)$ and $(22,101)$, or let $p = 103$ and $17 \leq d \leq 22$, or $p = 131$ and $18 \leq d \leq 22$. Let D be the trace divisor of a point of order p over a number field of degree d. Then $Z \neq 0$.*

Proof. Suppose that $Z = 0$, i.e. that $\overline{D} = C'$ is supported on the rational cusps.

Let $p = 53$, $h = \langle 4 \rangle$, of order 13, and $\pi : X_1(53) \to Y = X_1(53)/\langle 4 \rangle$. For $d = 19$ the criterion of Proposition 5.1 on X_H with H of order 2 fails at only 7 multiplicity vectors, and at all the 20444 divisors on $X_1(53)$ lying above them we compute that $f_{t,19}$ is a formal immersion, with $t = ((\langle 10 \rangle - 1)A_3, (\langle 10 \rangle - 1)A_5)$, which kills $J_1(53)(\mathbb{Q})$. For $d \in \{20, 21\}$ we work on $X_1(53)$ with $t = ((h-1)A_3, (h-1)A_5)$, and we compute that $f_{t,d}$ is a formal immersion at every sum of rational cusps of degree d that does not contain a full orbit of $\langle 4 \rangle$, while at the others the rank condition of Lemma 2.13 holds with $L = R + \pi^* Y$, where $R \neq 0$ is the rest of the divisor. Here $f_{t,d}$ vanishes on L, as $h - 1$ kills $\pi^* J_Y$ and the pullbacks $\pi^* E_0$, and A_q kills rational cuspidal divisors. In both cases Lemma 2.11 b) or Lemma 2.13 shows that D contains a cusp, which is a contradiction.

For $p = 101$ we use $t = (h-1)\beta_n A_q$ with h a generator of $\Delta(101)$, β_n as above, $n \in \{2,3,5,7\}$, and q odd. As $(h-1)\beta_n J_1(101)(\mathbb{Q})$ is finite, t kills $J_1(101)(\mathbb{Q})$ by Lemma 2.5 b), and we compute that $f_{t,d}$ is a formal immersion at all sums of rational cusps of degree d that do not contain all the 50 rational cusps, which is all of them. So D contains a cusp by Lemma 2.11 b), which is a contradiction.

Let $p = 103$ (resp. $p = 131$), let $H \subseteq \Delta(p)$ be the subgroup of order 3 (resp. 5), $Y = X_H$, and $\pi : X_1(p) \to Y$ the quotient map. Then $\rho : Y \to X_0(p)$ has degree 17 (resp. 13), and the rational cusps of Y form one fibre F of ρ. On Y, the criterion of Proposition 5.1 holds at all sums of rational cusps of degree d that do not contain F, so by Lemma 2.11 b) we can assume that $\overline{\pi_* D}$ contains F, and we write $\overline{\pi_* D} = F + \overline{R}$ for a rational cuspidal divisor R on Y. We use Lemma 2.13 on $Y^{(d)}$ with $L = R + \rho^* X_0(p)$ and $t = (\langle a \rangle - 1)A_3$, where $\langle a \rangle$ generates $\Delta(p)/H$. As p is not strange, $(\langle a \rangle - 1)J_Y(\mathbb{Q})$ is finite by Lemma 2.4, so t kills $J_Y(\mathbb{Q})$ by Lemma 2.5 b). It also kills $\rho^* J_0(p)$, on which $\langle a \rangle$ acts trivially, and $t[R + F - dc_0] = 0$, as A_3 kills rational cuspidal divisors, so $f_{t,d}$ vanishes on L. We compute that the rank condition holds. Hence $\pi_* D$ lies on L. If $R \neq 0$, then $\pi_* D$ contains a cusp, which is impossible. If $R = 0$, then $p = 103$,

$d = 17$, and $\pi_* D$ is the pullback of a non-cuspidal rational point on $X_0(103)$, which does not exist. □

6.7. **The primes** 109, 113, 127 **and** 137.

Proposition 6.15. *Let $12 \leq d \leq 22$, and let D be the trace divisor of a point of order 109 over a number field of degree d. Then $Z \notin \{SS_9, NC_{18}, 2SS_9, SS_9 + SS_{12}\}$.*

Proof. All of these divisors are fixed by $h = \langle 23 \rangle$, of order 18, $(h-1)J_1(109)(\mathbb{Q})$ is finite as 109 is not strange, and $\mathrm{gon}_{\mathbb{Q}} X_1(109) > 58$. We only use $2y = 0$ in Lemma 2.9. If $Z = SS_9$ and $d \leq 19$, or if Z is one of the others, then $2(d+c) \leq 58$, so $hD = D$ and $18 \mid c$. As $c \leq 13$, this gives $c = 0$, so $Z = NC_{18}$ or $2SS_9$ with $d = 18$, or $Z = SS_9 + SS_{12}$ with $d = 21$. As $d < (109-1)/3$, the orbits of h on the support of D have length 18 by Lemma 2.3. So the last case is impossible, and in the first two D is a single orbit of $\langle 23 \rangle$, whose image on $X_0(109)$ is a non-cuspidal rational point, which does not exist. If $Z = SS_9$ and $d \geq 20$, we use Lemma 2.13 with $L = C + \pi^* Y$ or $L = R + \pi^* Y^{(2)}$, where $\pi : X_1(109) \to Y = X_1(109)/\langle h^2 \rangle$, $\langle h^2 \rangle$, of order 9, acts freely on the geometric points of SS_9, and R is a rational cuspidal divisor, and $t = (h^2-1)A_q$ (code). Here t kills $J_1(109)(\mathbb{Q})$ and $\pi^* J_Y$, and $f_{t,d}$ vanishes on L as $h^2 - 1$ kills the pullbacks from Y and A_q kills rational cuspidal divisors. As the rank condition holds, D contains a cusp, which is a contradiction. □

Proposition 6.16. *Let $13 \leq d \leq 22$, and let D be the trace divisor of a point of order 113 over a number field of degree d. Then Z is not one of the divisors listed for 113 in Table 7.*

Proof. Here O_8 denotes one of the 7 ordinary closed points of degree 8 which are fixed by $h_8 = \langle 40 \rangle$, of order 8 (the other 28 ordinary closed points of degree 8, alone or together with non-ordinary points, are excluded by Proposition 5.3), and $\mathrm{gon}_{\mathbb{Q}} X_1(113) > 63$. The element $h_2 = \langle 2 \rangle$, of order 14, fixes the closed points SS_7 and NC_{14}, and the involution $\iota = \langle 98 \rangle$ fixes the points SS_7 and O_8. As 113 is not strange, $(g-1)J_1(113)(\mathbb{Q})$ is finite for every $g \in \Delta(113)$. We only use $2y = 0$ in Lemma 2.9, and as $d < (113-1)/3$, Lemma 2.3 b) applies to every subgroup of $\Delta(113)$ that fixes D.

If $Z \in \{2SS_7, 3SS_7, NC_{14}, SS_7 + NC_{14}\}$, then $2(d+c) \leq 60$, so $h_2 D = D$ and $14 \mid c$, so $c = 0$. Then $d \in \{14, 21\}$, and as $14 \nmid 21$, $d = 14$ and D is a single orbit of h_2, whose image on $X_0(113)$ is a non-cuspidal rational point, which is impossible.

If $Z = O_8$ and $d \leq 19$, or $Z = 2O_8$, then $2(d+c) \leq 62$, so $h_8 D = D$ and $8 \mid c$. Hence $d = 16$ and $c = 0$ or $c = 8$, and D is a pullback of a divisor of degree 2 from $X_1(113)/\langle h_8 \rangle$. Its image on $X_0(113)$ is a non-cuspidal point of degree at most 2, which has complex multiplication, as all the quadratic points on $X_0(113)$ are CM points [3, Table 14] and there are no non-cuspidal rational points [25, Theorem 1]. But then by Lemma 2.1 a point of order 113 on E is defined over a field of degree at least $112/6 > 16$, which is a contradiction. If $Z = O_8$ and $d \geq 20$, we use Lemma 2.13 with $L = R + \pi^* Y^{(r)}$, where π is the quotient by $\langle h_8 \rangle$, which is étale near Z, R is a rational cuspidal divisor, and $t = ((h_8-1)A_2, (h_8-1)A_3)$ (code). Here t kills $J_1(113)(\mathbb{Q})$ by Lemma 2.5 b), and $f_{t,d}$ vanishes on L as $h_8 - 1$ kills the pullbacks and A_q kills rational cuspidal divisors.

If $Z = O_8 + SS_7$, then $2(d+c) \leq 58$, so $\iota D = D$ and $2 \mid c = d - 15$. So d is odd, and the orbits of ι on the support of D have length 2 by Lemma 2.3, which is a contradiction. Finally, if $Z = O_8 + NC_{14}$ and $d = 22$, we use Lemma 2.13 with $t = ((h_8-1)B_q A_q)_{q \in \{2,3\}}$ and $L = Z_1 + \pi^* Y$, where Z_1 is the lift of NC_{14} to a cuspidal divisor (code). Here t kills $J_1(113)(\mathbb{Q})$ by Lemma 2.5 b), and as $h_8 - 1$ kills the pullbacks and $B_q A_q$ kills all cuspidal divisors by Lemma 2.5 c), $f_{t,22}$ vanishes on L. Hence D contains a cusp, which is a contradiction. □

Proposition 6.17. *Let $17 \leq d \leq 22$, and let D be the trace divisor of a point of order 127 over a number field of degree d. Then Z is not one of the divisors listed for 127 in Table 7.*

Proof. The element $h_7 = \langle 2 \rangle$, of order 7, fixes the 9 non-rational cusps and the 48 supersingular closed points of degree 14, and the ordinary closed points O_9 are fixed by the subgroup H_9 of order 9. As 127 is not strange, $(g-1)J_1(127)(\mathbb{Q})$ is finite for every $g \in \Delta(127)$. We have $\operatorname{gon}_{\mathbb{Q}} X_1(127) > 79$, and A_2 kills $J_1(127)(\mathbb{Q})_{\mathrm{tors}}$ by Lemma 2.5 b). We only use $2y = 0$ in Lemma 2.9.

Suppose that Z is a sum of points NC_7 and SS_{14}. Then $2(d+c) \leq 74$, so $h_7 D = D$ and $7 \mid c$. This is impossible unless $d = 21$, in which case D is a pullback from $Y = X_1(127)/\langle 2 \rangle$ (Lemma 2.3), of a divisor D' of degree 3. The curve Y has genus 88, and its points over $\mathbb{F}_2$ which are images of cusps are the 9 rational cusps and the 9 images of the non-rational cusps. Let h' be a generator of $\Delta(127)/\langle 2 \rangle$. By Lemma 2.4 and Lemma 2.5 (note that $\langle 2 \rangle$ has odd order), the maps $(h'-1)B_q A_q$ with $q \in \{2,3\}$ kill $J_Y(\mathbb{Q})$ and all the cuspidal divisors on Y.

If Z consists of non-rational cusps, then $\overline{D'}$ is a sum of three of these 18 points, and we compute that $f_{t,3}$ on $Y^{(3)}$, with $t = ((h'-1)B_q A_q)_{q \in \{2,3\}}$, is a formal immersion at all the 1140 such sums. So $f_{t,3}$ maps D' and the cuspidal divisor lifting $\overline{D'}$ (which is defined over an unramified extension of $\mathbb{Q}_2$) to 0, and they are equal by Lemma 2.11 a), which is a contradiction. If $Z = SS_{14}$, so that $c = 7$, then for 5 of the 6 orbits of points SS_{14}, $\alpha A_q Z$ is not principal for some $q \in \{3,5,7\}$, which contradicts Lemma 5.2. For the remaining orbit (of length 3), $\overline{D'} = S + \overline{c_1}$, where c_1 is a rational cusp of Y and S is a supersingular point of degree 2 fixed by the element h_3' of order 3 of $\Delta(127)/\langle 2 \rangle$. We use Lemma 2.13 on $Y^{(3)}$ with $L = S_0 + c_1$, where S_0 is the unique lift of S fixed by h_3', and with t combining the maps $(h_3'-1)A_q$ for several primes $q \in \{2,3,5\}$ (code). Here t kills $J_Y(\mathbb{Q})$ by Lemma 2.4 and Lemma 2.5 b), and $t[S_0 + c_1 - 3c_0] = 0$, as h_3' fixes S_0 and A_q kills rational cuspidal divisors. As the rank condition holds, $D' = S_0 + c_1$ contains a cusp, which is a contradiction. The case $Z = SS_{14} + NC_7$ is excluded by Proposition 5.3.

If $Z = O_9$ or $Z = 2O_9$, then $2(d+c) \leq 72$, so D is H_9-invariant and $9 \mid c$. Hence $d = 18$ and D is a pullback of a divisor of degree 2 from $X_1(127)/H_9$. Its image on $X_0(127)$ is a non-cuspidal point of degree at most 2, which has complex multiplication, as all the quadratic points on $X_0(127)$ are CM points [3, Table 16] and there are no non-cuspidal rational points [25, Theorem 1]. By Lemma 2.1 a point of order 127 on E is then defined over a field of degree at least $126/6 = 21 > 18$, which is a contradiction.

Finally, if $Z = O_9 + NC_7$, we use Lemma 2.13 with $L = C + \pi_9^*(X_1(127)/H_9) + \pi_7^*(X_1(127)/\langle 2 \rangle)$, where π_9 and π_7 are the quotient maps, which is smooth of dimension 2 as H_9 and $\langle 2 \rangle$ act freely on the supports of O_9 and NC_7, and $t = (h_9 - 1)(h_7 - 1)A_q$, $q \in \{2,3\}$, where h_9 generates H_9 (code). Here t kills $J_1(127)(\mathbb{Q})$ and the pullbacks of the Jacobians of both quotients, and $f_{t,d}$ vanishes on L as A_q kills rational cuspidal divisors. So D contains $C \neq 0$, which is a contradiction. □

Proposition 6.18. *Let $19 \leq d \leq 22$, and let D be the trace divisor of a point of order 137 over a number field of degree d. Then $Z \notin \{SS_{17}, O_{17}\}$.*

Proof. The point SS_{17} is fixed by $\langle 2 \rangle$, of order 34, and O_{17} is fixed by $\langle 81 \rangle$, of order 17. As 137 is not strange, $(g-1)J_1(137)(\mathbb{Q})$ is finite for every $g \in \Delta(137)$. In both cases $c = d - 17 \in \{2,3,4,5\}$ and $2(d+c) \leq 54 < \operatorname{gon}_{\mathbb{Q}} X_1(137)$, so Lemma 2.9 gives $34 \mid c$ or $17 \mid c$, which is a contradiction. □

6.8. **Proof of Theorem 1.1.** By Proposition 3.3 all the primes listed in Theorem 1.1 are in $S(d)$. Conversely, let $9 \leq d \leq 22$ and let $p \in S(d)$ be a prime which is not listed. By

Propositions 4.13, 4.15, 4.17 and 4.18, p is one of the primes of Table 4. Let D be the trace divisor of a point of order p over a number field of degree d. By Proposition 5.3, Z is one of the divisors listed in Table 7, and these are excluded by Propositions 6.2, 6.3, 6.5, 6.6, 6.8, 6.10, 6.11 and 6.13 to 6.18.

7. The computations

Most of the computations were done in `Magma` [6], version V2.30-1, using the package `mdmagma` of Derickx and Sutherland [27] and the models of $X_1(N)$ of Sutherland [41, 40], and the independent checks were done in SageMath [42]. For the computations with modular symbols of large level in Lemma 4.12 we exported the sparse matrices of T_2 from `Magma` and computed the sequences in our own exact `C++` code, checking the first 64 terms against `Magma` in every case, and the certificates of linear complexity were checked independently with FLINT. In the code the diamond operators act on q-expansions, and the matrix of $\langle a\rangle$ there is the matrix of $\langle a\rangle^{-1}$ in our notation (this is checked when the models are built), so the operators written $T_q - \langle q\rangle - q$ and $T_q - 1 - q\langle q\rangle$ in the code are A_q and B_q up to a diamond operator, which does not change the rank conditions. All the computations were performed on the *Mordell* server at the Department of Mathematics, University of Zagreb, with an AMD EPYC 9175F CPU (16 cores, 32 threads) and 384 GB of RAM, between 28 October and 3 November 2026. In total they took about 1400 CPU hours. The case $d = 22$ alone took about 900 of them, and the computations of Lemma 4.12 for all the degrees together about 1100. These numbers are the sums of the running times of the individual jobs, which we read off from their log files (see `notes/cpu_time.md`), and they include some exploratory computations that are not used in the proofs. The main obstacle to determining $S(23)$ in the same way would be disk space. The data for $d = 20$, 21 and 22 take about 30, 85 and 220 GB, and since $B(d)$ doubles with each degree, we estimate that $d = 23$ would need about 600 GB (and several thousand CPU hours), mostly for Lemma 4.12.

Data availability and reproducibility. All the code for the computations in this paper, the logs, the machine-readable ledgers and the certificates that fit in a repository are available at

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

All the links to the repository point to its revision `0f661c1`. In the digital version of this paper, the words reporting a computation, such as "we compute", are links to the corresponding script. The repository is organized by degree: the folder `audit11` contains the computations for $d \leq 11$ (and `audit10` the transfer to $d = 10$), and the folders `degree12`, ..., `degree22` those for the larger degrees. Each computation for degree d reuses the certificates for the smaller degrees, after checking that the closed points used there are the same, so the certificates for a given prime are spread over the folders of the degrees in which they were first needed. For each degree, the file `final_coverage.json` records for every prime up to the bound of Table 2 the reason it is excluded or the example showing that it occurs, `support_coverage.json` records the argument used for every possible type of reduction at every prime of Table 4, and the scripts `verify_coverage.py` (for $d = 22$, `degree22/verify_final.py`) check these ledgers against the certificates. The folder `proofs` contains the detailed accounts of the computations for each degree, with the numbers of divisors checked in each case, and the `README.md` file explains how to rerun everything. The complete certificates (about 360 GB, mostly the matrices of the principal divisor tests and the modular symbol computations) are too large for the repository, and they are available at Harvard Dataverse [30]. The repository contains their SHA256 hashes.

The computations were checked in the following ways. The ranks of all the matrices certifying that divisors are not principal (Lemma 2.10), that maps are formal immersions (Lemmas 2.11 and 2.12) and the intersection matrices of Lemma 4.1 were recomputed independently in SageMath from the stored matrices, and the relation spaces used in the formal immersion computations were checked to span the full spaces of relations. For $d \geq 20$ the census of Section 5.1 was checked against independent point counts, and the list of types of reductions was produced twice, independently. The certificates of linear complexity were checked independently of the code that produced them. The computations for $d \leq 11$, which are also the basis of the computations for the larger degrees, were redone from scratch after a first version, and then checked in an independent review (see `proofs/S10_S11_independent_audit.txt`). Finally, Theorem 1.1 for $d = 9$ was also proved, during the work on [32], by an independent set of computations, which partly use quotients of $X_1(p)$ instead of $X_1(p)$. These are in `degree09`.

The local computations at $p = 163$ for $d = 22$ (13 types of reductions on $X_1(163)$, of genus 1027, with 5124 certificates, in `degree22/full163`) and the computation of `degree22/anti173.m` at $p = 173$ were made before we noticed that the second bound of Proposition 2.6 a) excludes these primes for $d = 22$ directly (Proposition 4.15), so they are not needed for the proof.

We should mention that in the first version of the computations for $d \in \{15, 16\}$ the element α at $p = 97$ was the polynomial $(\sigma^2 - 1)(\sigma^4 - 1)$ in a generator σ of $\Delta(97)$, which does not kill the strange characters of order 12, so Lemma 5.2 does not apply. We replaced it by $\sigma^{12} - 1$ and $(\sigma - 1)\Phi_{12}(\sigma)$ and redid all the affected computations (see `proofs/S97_correction.txt`). The computations for the other degrees were not affected.

References

[1] A. Abbes and E. Ullmo, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires*, Compositio Math., 103 (1996), pp. 269–286.

[2] D. Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices, no. 20 (1996), pp. 1005–1011.

[3] N. Adžaga, T. Keller, P. Michaud-Jacobs, F. Najman, E. Ozman, and B. Vukorepa, *Computing quadratic points on modular curves $X_0(N)$*, Math. Comp., 93 (2024), pp. 1371–1397.

[4] A. Agashe, K. Ribet, and W. A. Stein, *The Manin constant*, Pure Appl. Math. Q., 2 (2006), pp. 617–636.

[5] A. R. Booker, M. Lee, and A. Strömbergsson, *Twist-minimal trace formulas and the Selberg eigenvalue conjecture*, J. Lond. Math. Soc. (2), 102 (2020), pp. 1067–1134.

[6] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), pp. 235–265. Computational algebra and number theory (London, 1993).

[7] A. Bourdon and P. L. Clark, *Torsion points and Galois representations on CM elliptic curves*, Pacific J. Math., 305 (2020), pp. 43–88.

[8] J. Box, *Quadratic points on modular curves with infinite Mordell–Weil group*, Math. Comp., 90 (2021), pp. 321–343.

[9] M. Derickx, A. Etropolski, M. van Hoeij, J. S. Morrow, and D. Zureick-Brown, *Sporadic cubic torsion*, Algebra Number Theory, 15 (2021), pp. 1837–1864.

[10] M. Derickx, S. Kamienny, W. Stein, and M. Stoll, *Torsion points on elliptic curves over number fields of small degree*, Algebra Number Theory, 17 (2023), pp. 267–308.

[11] M. Derickx and F. Najman, *Classification of torsion of elliptic curves over quartic fields*, J. Reine Angew. Math., 829 (2025), pp. 123–156.

[12] M. Derickx and M. Stoll, *Prime order torsion on elliptic curves over number fields. Part I: Asymptotics*. Preprint, `https://arxiv.org/abs/2505.14109v1`, 2025.

[13] ———, *Personal communication*, 2026.

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

[15] Y. Hasegawa and M. Shimura, *Trigonal modular curves*, Acta Arith., 88 (1999), pp. 129–140.

[16] D. Jeon, *Modular curves with infinitely many cubic points*, J. Number Theory, 219 (2021), pp. 344–355.

[17] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math., 109 (1992), pp. 221–229.
[18] S. Kamienny and B. Mazur, *Rational torsion of prime order in elliptic curves over number fields*, Astérisque, 228 (1995), pp. 81–100. With an appendix by A. Granville.
[19] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque, 295 (2004), pp. 117–290. Cohomologies p-adiques et applications arithmétiques. III.
[20] N. M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math., 62 (1981), pp. 481–502.
[21] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J., 109 (1988), pp. 125–149.
[22] M. Khawaja, *Torsion primes for elliptic curves over degree* 8 *number fields*, Res. Number Theory, 10 (2024). Paper No. 48.
[23] Q. Liu and D. Lorenzini, *Models of curves and finite covers*, Compositio Math., 118 (1999), pp. 61–102.
[24] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math., 47 (1977), pp. 33–186 (1978). With an appendix by Mazur and M. Rapoport.
[25] B. Mazur, *Rational isogenies of prime degree*, Invent. Math., 44 (1978), pp. 129–162. With an appendix by D. Goldfeld.
[26] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math., 25 (1974), pp. 1–61.
[27] *mdmagma*. https://github.com/nt-lib/mdmagma. M. Derickx and A. V. Sutherland, `Magma` package, revision `d1c019c`.
[28] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math., 124 (1996), pp. 437–449.
[29] F. Najman, *Classification of torsion of elliptic curves over quintic fields*. Preprint, https://arxiv.org/abs/2609.12846, 2026.
[30] ———, *Computational certificates for prime torsion in degrees* 9–22. Harvard Dataverse, 2026. https://doi.org/10.7910/DVN/5HHEY4.
[31] ———, *Torsion of elliptic curves over number fields of degree* 10. Preprint, 2026.
[32] ———, *Torsion of elliptic curves over number fields of degree* 6*,* 7*,* 8 *and* 9. Preprint, https://hexagonmath.org/2611.00073, 2026.
[33] F. Najman and M. Varivoda, *Torsion groups of elliptic curves that appear infinitely often over septic, octic and nonic fields*. Preprint, https://arxiv.org/abs/2602.03513, 2026.
[34] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math., 506 (1999), pp. 85–116.
[35] ———, *Torsion des courbes elliptiques sur les corps cubiques*, Ann. Inst. Fourier (Grenoble), 50 (2000), pp. 723–749.
[36] ———, *No* 17*-torsion on elliptic curves over cubic number fields*, J. Théor. Nombres Bordeaux, 15 (2003), pp. 831–838.
[37] D. Prasad and C. S. Yogananda, *Bounding the torsion in CM elliptic curves*, C. R. Math. Acad. Sci. Soc. R. Can., 23 (2001), pp. 1–5. Preprint version https://arxiv.org/abs/math/9810208.
[38] S. Siksek, *Chabauty for symmetric powers of curves*, Algebra Number Theory, 3 (2009), pp. 209–236.
[39] A. Silverberg, *Torsion points on abelian varieties of CM-type*, Compositio Math., 68 (1988), pp. 241–249.
[40] A. V. Sutherland, *Defining equations for* $X_1(N)$. https://math.mit.edu/~drew/X1_altcurves.html.
[41] ———, *Constructing elliptic curves over finite fields with prescribed torsion*, Math. Comp., 81 (2012), pp. 1131–1147.
[42] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 10.7)*. https://www.sagemath.org, 2025.
[43] M. 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.
[44] M. Varivoda, *Gonality and quintic points on intermediate modular curves*. Preprint, https://hexagonmath.org/2610.00219v1, 2026.

University of Zagreb Faculty of Science, Department of Mathematics, Bijenička cesta 30, 10000 Zagreb, Croatia
Email address: `fnajman@math.hr`