hexagon:2611.00884v1

ISOLATED AND SPORADIC POINTS ON $X_1(N)$ AND $X_0(N)$

FILIP NAJMAN

Abstract. We determine all the positive integers N for which the modular curves $X_1(N)$ and $X_0(N)$ have a non-cuspidal isolated point. The curve $X_1(N)$ has such a point if and only if $N = 17$, $N = 19$ or $N \geq 21$, while $X_0(N)$ has such a point if and only if $X_0(N)$ is of genus ≥ 2 or $N \in \{11, 14, 15, 17, 19, 21, 27\}$. We also determine all the N for which $X_1(N)$ has a non-cuspidal sporadic point, with the exception of $N = 83$ and $N = 131$. At these two levels we find isolated points of degree 57 and 143, respectively, and show that the second one is not sporadic. Our main tool for proving that points are sporadic is a lower bound for the minimum density degree of $X_1(N)$ obtained by comparing the Frobenius and diamond operators at the supersingular points.

1. Introduction

A fundamental problem in arithmetic geometry, with many consequences in the theory of elliptic curves, is to understand the low degree points on modular curves. Let C be a curve over $\mathbb{Q}$. If C has genus ≥ 2, then by Faltings' theorem C has only finitely many rational points, while C has infinitely many points of degree d for all d large enough (for example for d equal to the gonality of C). It is natural to single out the points of C which do not belong to an infinite family of points of the same or lower degree. A closed point x of degree d on C is *sporadic* if C has only finitely many closed points of degree $\leq d$. Bourdon, Ejder, Liu, Odumodu and Viray [8] introduced the related notion of an *isolated* point, which, roughly speaking, is a point that does not belong to an infinite family of points of the same degree parametrized either by $\mathbb{P}^1$ or by a positive rank abelian variety (see Definition 2.1 for the precise definition and the survey of Viray and Vogt [52] for more details). Every sporadic point is isolated [8, Theorem 4.2], but the converse is not true.

The non-cuspidal points of degree d on $X_1(N)$ correspond to elliptic curves with a point of order N over number fields of degree d, so sporadic points on $X_1(N)$ correspond to torsion that appears over fields of unusually small degree. Najman [38] found that the elliptic curve 162b1 has a point of order 21 over $\mathbb{Q}(\zeta_9)^+$, the maximal real subfield of $\mathbb{Q}(\zeta_9)$, which gives a sporadic point of degree 3 on $X_1(21)$. Van Hoeij [50] found many points of low degree on $X_1(N)$ using modular units. The classifications of the possible torsion groups of elliptic curves over number fields of degree $d \leq 9$ [36, 30, 28, 17, 18, 39, 40, 41] determine, for small

2020 *Mathematics Subject Classification.* 11G05, 11G18, 14G05, 14H51.

Key words and phrases. modular curves, isolated points, sporadic points, gonality, minimum density degree.

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.

N, the least degree of a non-cuspidal point on $X_1(N)$. Clark, Genao, Pollack and Saia [13] determined the least degree of a CM point on $X_1(N)$ for all N, and proved that $X_1(N)$ has a sporadic CM point for all N outside an explicit finite set, the largest element of which is 720 [13, Theorem 8.2]. For the curves $X_0(N)$, Derickx and Najman [19] recently determined all the N such that $X_0(N)$ has a non-cuspidal sporadic point. The known isolated and sporadic points on the curves $X_1(m,n)$ are collected in the census [43].

The isolated points on modular curves have mostly been studied through their j-invariants. Bourdon, Ejder, Liu, Odumodu and Viray [8] studied the isolated points on $X_1(N)$ with a given j-invariant, and Bourdon, Hashimoto, Keller, Klagsbrun, Lowry-Duda, Morrison, Najman and Shukla [10] gave an algorithm that tests whether a rational non-CM j-invariant is the j-invariant of an isolated point on some $X_1(N)$. Bourdon, Gill, Rouse and Watson [9] characterized the elliptic curves with rational j-invariant that give an isolated point of odd degree on some $X_1(N)$. Bourdon and Ejder [7], completing a partial classification of Ejder [21], determined the rational j-invariants of the isolated points on $X_1(\ell^n)$ and $X_0(\ell^n)$ for ℓ prime, and Bourdon [5] proved finiteness results for the rational j-invariants of the isolated points on $X_1(N)$. Terao [48] classified the isolated points with rational j-invariant on the curves $X_0(N)$, assuming a conjecture on the images of Galois representations of elliptic curves over $\mathbb{Q}$, and Lee [33] gave an algorithm that tests whether a rational non-CM j-invariant is the j-invariant of an isolated point on $X_0(N)$. Calger [12] proved finiteness results for the j-invariants of bounded degree of the isolated points on modular curves of prime power level.

However, it was unknown which of the curves $X_1(N)$ have non-cuspidal sporadic points. The results on isolated points mentioned above concern the points with a given j-invariant, in most cases a rational one, and the question of which of the curves $X_1(N)$ and $X_0(N)$ have a non-cuspidal isolated point at all seems not to have been considered (at least to our knowledge). In this paper we answer these questions, with the exception of two levels. We consider non-cuspidal points of arbitrary degree, including CM points, and in particular we impose no restriction on the field of definition of the j-invariant. Our main results are the following theorems.

Theorem 1.1. *The modular curve $X_1(N)$ has a non-cuspidal isolated point if and only if $N = 17$, $N = 19$ or $N \geq 21$.*

Theorem 1.2. *The modular curve $X_0(N)$ has a non-cuspidal isolated point if and only if*

$$N \notin \{1, \dots, 10, 12, 13, 16, 18, 20, 24, 25, 32, 36, 49\}.$$

In particular $X_0(N)$ has a non-cuspidal isolated point for all N such that $X_0(N)$ is of genus ≥ 2, and the curves $X_0(N)$ of genus 1 with a non-cuspidal isolated point are the ones with $N \in \{11, 14, 15, 17, 19, 21, 27\}$.

Theorem 1.3. *Let*

$$A = \{1, \dots, 20\} \cup \{22, \dots, 27\} \cup \{32\}.$$

For $N \in A$ the curve $X_1(N)$ has no non-cuspidal sporadic points. For $N \notin A \cup \{83, 131\}$ the curve $X_1(N)$ has a non-cuspidal sporadic point.

In particular, $X_1(N)$ has a sporadic point for all $N > 131$ and the question is settled for all composite N. Note that if one allows cusps, then the answer to all three questions is the same: the curve has an isolated (or sporadic) point if and only if it is of positive genus, since both $X_1(N)$ and $X_0(N)$ have a rational cusp, and they have finitely many rational

points when their genus is positive, by Faltings' theorem in genus ≥ 2 and since all the curves $X_1(N)$ and $X_0(N)$ of genus 1 have rank 0 [17, Theorem 3.1].

Unfortunately, we are unable to determine whether $X_1(83)$ and $X_1(131)$ have sporadic points. For $N = 83, 131$ the curve $X_0^+(N) = X_0(N)/w_N$ is an elliptic curve of rank 1, and the composition $X_1(N) \to X_0(N) \to X_0^+(N)$ has degree $N-1$. Hence $\delta(X_1(N)) \leq N-1$, where δ denotes the minimum density degree (see Section 2). The least degree of a CM point on $X_1(N)$ is also $N-1$ [13], so a sporadic point on $X_1(83)$ or $X_1(131)$ would have to be non-CM. We prove that $52 \leq \delta(X_1(83)) \leq 82$ and $111 \leq \delta(X_1(131)) \leq 130$ (see Propositions 9.4 and 9.7). We find two orbits under the diamond operators of isolated points of degree 57 on $X_1(83)$ (Proposition 9.2), which are sporadic if $\delta(X_1(83)) \geq 58$. We also find an isolated point of degree 143 on $X_1(131)$ (Proposition 9.3), which is not sporadic since $\delta(X_1(131)) \leq 130$. We expect that the points of degree 57 on $X_1(83)$ are sporadic and that $X_1(131)$ has no non-cuspidal sporadic points, but we were unable to prove this (see Remark 9.8). Note that $X_1(17)$ also has an isolated point of degree 5 (Proposition 6.2), while it has infinitely many points of degree 4.

We now briefly describe our methods. To prove Theorem 1.2, we use the classification of Derickx and Najman [19], which leaves 34 curves $X_0(N)$ of genus ≥ 2 without sporadic points. For 26 of them the Jacobian $J_0(N)$ has rank 0, and we show that the number of rational divisor classes generated by the cusps is larger than the number of such classes represented by effective cuspidal divisors of degree $\leq g$, which forces the existence of a non-cuspidal point x with $\ell(x) = 1$ (see Corollary 3.3). For the remaining 8 curves, $X_0(N)/w_N$ is an elliptic curve of rank 1, and we use a criterion for isolation of divisors on double covers of elliptic curves (Lemma 3.6), which we apply to CM points, to cubic points found by Box, Gajović and Goodman [11], and to residual divisors of a canonical divisor. The proof of Theorem 1.1 for $N \leq 32$ is similar: we either find an explicit point x with $\ell(x) = 1$ on a curve with $J_1(N)(\mathbb{Q})$ finite, or show that all the rational divisor classes are represented by cuspidal divisors.

The main difficulty in proving Theorem 1.3 is to give good lower bounds for $\delta(X_1(N))$. It is well known that at a prime $p \nmid N$, the p^2-power Frobenius agrees with the diamond operator $\langle p \rangle$ at all the supersingular points of $X_1(N)_{\overline{\mathbb{F}}_p}$, which gives a lower bound for the gonality of $X_1(N)$ (see [44] and Corollary 4.3). Combining this with Frey's inequality $\delta(C) \geq \frac{1}{2}\operatorname{gon}_{\mathbb{Q}}(C)$ gives a lower bound for $\delta(X_1(N))$. Our main tool is Proposition 4.8, which gives

$$\delta(X_1(N)) \geq \frac{(p-1)J_2(N)}{24(p+1)^2},$$

an improvement by a factor of almost 2. It is proved by applying the Hodge index theorem on the product of $X_1(N)_{\overline{\mathbb{F}}_p}$ with the reduction of an abelian variety that parametrizes a hypothetical infinite family of points. When the positive rank part of $J_1(N)$ is known, this can be refined using the Eichler-Shimura relation (Proposition 4.9) and, for elliptic factors, using the degree of the modular parametrization (Section 4.4). On the other hand, we obtain upper bounds for the least degree of a non-cuspidal point from the CM points [13], the census [43], the points of van Hoeij [50] and some new points that we find. For 10 levels we prove the existence of a sporadic point without exhibiting it, by showing that a gonal map of $X_1(N)$ would have a fibre over a rational cusp containing a point of smaller degree (Section 7.4). Finally, for 9 composite levels, listed in Table 2, we need ad hoc arguments. In most of these cases we use the reduction of $X_1(N)$ modulo a prime p dividing N exactly, whose special fibre consists of two components meeting at the supersingular points [16]. A

map of degree d to $\mathbb{P}^1$ in characteristic 0 gives functions on both components whose values at the supersingular points are related by Frobenius (Lemma 8.1), which gives strong lower bounds for the gonality. At level 138 we instead use the tropical Abel-Jacobi map of the special fibre at 2, and at level 121 a ramified quotient of $X_1(121)$.

We introduce conventions and notation in Section 2 and prove some general results about divisors and the minimum density degree in Section 3. The lower bounds for $\delta(X_1(N))$ coming from the supersingular points are proved in Section 4. We prove Theorem 1.2 in Section 5. In Section 6 we deal with the isolated points on $X_1(N)$ for $N \leq 32$, in Section 7 with the sporadic points on $X_1(N)$ for most N, and in Section 8 with the 9 remaining composite levels. The two prime levels 83 and 131 are treated in Section 9, where we also prove Theorem 1.1. We prove Theorem 1.3 in Section 10.

All the code used in the paper can be found at

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

1.1. **Data availability and reproducibility.** We use revision `88bc530` of the repository above, and all the links to code in this paper point to this revision. In the digital form of this article, the words reporting a computation, such as "we compute", are hyperlinks to the script that carries it out. The README of the repository describes how to run each computation. The computations use Magma [4] (version V2.30-1), SageMath [49] (version 10.7) and some programs written in Python and C++. The data of the LMFDB [34] that we use (labels, Hecke eigenvalues, characters and modular degrees of newforms) is stored in the repository, together with the data from the census [43] and from the computations of the least CM degrees [13].

All of our computations were performed on the *Mordell* server at the Department of Mathematics, University of Zagreb with an AMD EPYC 9175F CPU with 16 cores and 384 GB of RAM. Running all the computations linked in this paper takes about 45 minutes on a single core and uses at most 1.1 GB of RAM. Most of this time is spent on the levels 150 (about 20 minutes), 94 (8 minutes), 108 (6 minutes) and 71 (5 minutes).

AI disclosure and comments. I posed the questions considered in this paper, guided the work and reviewed it. OpenAI's GPT-6.2 Astra did the mathematics for the new results, carried out the computations and organized the accompanying code repository, while Anthropic's Claude Opus 5.5 and Claude Fable 5.2 reviewed and rechecked some of the computations and drafted the manuscript. I have not yet fully checked the proofs.

2. Conventions and notation

Throughout the paper all curves are smooth, projective and geometrically integral, and a point of a curve C over $\mathbb{Q}$ is a closed point unless stated otherwise. We identify a point x of degree d with the effective divisor of degree d on C (defined over $\mathbb{Q}$) which is the sum of its d geometric points. For a divisor D on C we write

$$\ell(D) = \dim_{\mathbb{Q}} H^0(C, \mathcal{O}_C(D)).$$

We denote by $J_C = \mathrm{Pic}^0_C$ the Jacobian of C, by $C^{(d)}$ its d-th symmetric power and by $W_d(C) \subseteq \mathrm{Pic}^d_C$ the image of $C^{(d)}$. All the curves that we will consider have a rational point, which we use to identify Pic^d_C with J_C when this is convenient. In particular, every rational divisor class of degree d on such a curve is the class of a divisor defined over $\mathbb{Q}$.

For a field K, the *gonality* $\mathrm{gon}_K C$ of C over K is the least degree of a non-constant morphism $C_K \to \mathbb{P}^1_K$. The *minimum density degree* $\delta(C)$ of C is the least positive integer

d such that C has infinitely many points of degree d. This invariant was studied by Smith and Vogt [45], who call it the arithmetic degree of irrationality, and by Kadets and Vogt [27], whose terminology we use (see also [52]). It is denoted by $\min \delta(C/\mathbb{Q})$ in [27, 19].

Definition 2.1 ([8, Section 4])**.** Let C be a curve over $\mathbb{Q}$ and x a point of degree d on C.

a) The point x is $\mathbb{P}^1$-*isolated* if $\ell(x) = 1$.
b) The point x is *AV-isolated* if there is no abelian subvariety $A \subseteq J_C$ over $\mathbb{Q}$ of positive rank such that $[x] + A \subseteq W_d(C)$.
c) The point x is *isolated* if it is both $\mathbb{P}^1$-isolated and AV-isolated.
d) The point x is *sporadic* if C has only finitely many points of degree $\leq d$.

Note that $\ell(x) \geq 2$ if and only if there is a morphism $C \to \mathbb{P}^1$ of degree d which has x as a fibre. A point x is sporadic if and only if $\deg x < \delta(C)$.

Theorem 2.2 ([8, Theorem 4.2])**.** *A curve C over $\mathbb{Q}$ has infinitely many points of degree d if and only if it has a point of degree d which is not isolated. In particular, every sporadic point is isolated.*

For a positive integer N we denote by $X_1(N)$ and $X_0(N)$ the usual modular curves over $\mathbb{Q}$, by $J_1(N)$ and $J_0(N)$ their Jacobians, and by w_N the Fricke involution of $X_0(N)$. We write $X_0^+(N) = X_0(N)/w_N$. For $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ we denote by $\langle a \rangle$ the diamond operator on $X_1(N)$, which sends a pair (E, P) to (E, aP). Since (E, P) and $(E, -P)$ are isomorphic, $\langle a \rangle$ depends only on the class of a in $(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$, and the map $X_1(N) \to X_0(N)$ is the quotient by the diamond operators. For $N \geq 5$ we put

$$J_2(N) = N^2 \prod_{\ell \mid N} \left(1 - \frac{1}{\ell^2}\right),$$

which is the number of points of exact order N on an elliptic curve over an algebraically closed field of characteristic not dividing N. For a prime $p \nmid N$ we put

$$S_p(N) = \frac{(p-1)J_2(N)}{24}.$$

By Lemma 4.1, $S_p(N)$ is the number of supersingular points on $X_1(N)_{\overline{\mathbb{F}}_p}$.

For a curve C_0 over $\mathbb{F}_p$ we denote by Φ the base change to $\overline{\mathbb{F}}_p$ of the p-power Frobenius endomorphism of C_0. In particular, Φ^2 is the base change of the p^2-power Frobenius endomorphism of $C_{0,\mathbb{F}_{p^2}}$.

For a newform f of weight 2 we denote by ϵ its character, by K_f its coefficient field, by $a_n(f)$ its Fourier coefficients and by A_f the corresponding abelian variety over $\mathbb{Q}$ (a quotient of $J_1(N)$), which has dimension $[K_f : \mathbb{Q}]$. We refer to newforms by their LMFDB labels [34], and to elliptic curves over $\mathbb{Q}$ by their labels in Cremona's tables [14].

For computations we use Magma [4], SageMath [49] and some programs written in Python and C++. Throughout the paper, in places where we used a computer to compute something, we use the phrase "we compute" or something very similar, and the code can be found in the repository mentioned in the introduction.

3. Divisors and the minimum density degree

We first collect some well-known facts about the minimum density degree. The first inequality in a) below is due to Frey [25].

Lemma 3.1. *Let C be a curve over $\mathbb{Q}$ with a rational point.*

a) $\frac{1}{2}\operatorname{gon}_{\mathbb{Q}} C \leq \delta(C) \leq \operatorname{gon}_{\mathbb{Q}} C$.
b) *If $J_C(\mathbb{Q})$ is finite, then $\delta(C) = \operatorname{gon}_{\mathbb{Q}} C$.*
c) *If $C \to C'$ is a non-constant morphism of curves over $\mathbb{Q}$, then $\delta(C) \geq \delta(C')$.*

Proof. By Hilbert's irreducibility theorem, a morphism $C \to \mathbb{P}^1$ of degree $\operatorname{gon}_{\mathbb{Q}} C$ has infinitely many fibres over rational points which are points of degree $\operatorname{gon}_{\mathbb{Q}} C$, so $\delta(C) \leq \operatorname{gon}_{\mathbb{Q}} C$. The images of infinitely many points of degree d on C are infinitely many points of degree $\leq d$ on C', which proves c).

Suppose C has infinitely many points of degree d. If two of them are linearly equivalent, then $\ell(x) \geq 2$ for one of them, so $\operatorname{gon}_{\mathbb{Q}} C \leq d$. If $J_C(\mathbb{Q})$ is finite, then C has only finitely many rational divisor classes of degree d, so this has to happen, which proves b). Suppose now that the points of degree d give infinitely many distinct rational points of $W_d(C)$. By Faltings' theorem [22], $W_d(C)$ contains a translate $a + A$, where $a \in \operatorname{Pic}^d_C(\mathbb{Q})$ and $A \subseteq J_C$ is an abelian subvariety such that $A(\mathbb{Q})$ is infinite. For $t \in A(\mathbb{Q})$ let D_t and D_{-t} be effective divisors over $\mathbb{Q}$ in the classes $a + t$ and $a - t$. The divisors $D_t + D_{-t}$ all lie in the linear system $|2a|$, and there are infinitely many of them, since a fixed effective divisor has only finitely many effective subdivisors. It follows that $\ell(D_t + D_{-t}) \geq 2$, so $\operatorname{gon}_{\mathbb{Q}} C \leq 2d$. □

Lemma 3.2. *Let C be a curve of genus g over $\mathbb{Q}$ and $c \in C(\mathbb{Q})$. Every class $L \in J_C(\mathbb{Q})$ can be written as $L = [D - (\deg D)c]$ for a unique effective divisor D over $\mathbb{Q}$ such that $c \notin \operatorname{supp} D$ and $\ell(D) = 1$. Furthermore, $\deg D \leq g$.*

Proof. Let $m \geq 0$ be the least integer such that $H^0(C, L(mc)) \neq 0$. By Riemann-Roch, $m \leq g$. Since $H^0(C, L((m-1)c)) = 0$, evaluation at c injects $H^0(C, L(mc))$ into a 1-dimensional space, so $H^0(C, L(mc))$ is spanned by a section whose divisor D does not contain c, and $\ell(D) = 1$. Conversely, let D be any effective divisor with $c \notin \operatorname{supp} D$, $\ell(D) = 1$ and $L = [D - (\deg D)c]$. The unique (up to scalars) section of $\mathcal{O}_C(D)$ does not vanish at c, so $H^0(C, \mathcal{O}_C(D - c)) = 0$. It follows that $\deg D$ is the least m as above, and D is the divisor of the unique section of $L(mc)$. □

Corollary 3.3. *Let C be a curve of genus g over $\mathbb{Q}$ such that $J_C(\mathbb{Q})$ is finite, let $c \in C(\mathbb{Q})$, let $\mathcal{C}$ be a finite set of points of C containing c, and let $H \subseteq J_C(\mathbb{Q})$ be the subgroup generated by the classes $[Q - (\deg Q)c]$ for $Q \in \mathcal{C}$. Suppose that fewer than $\#H$ classes in H are of the form $[D - (\deg D)c]$, with D an effective divisor supported on $\mathcal{C}$ of degree $\leq g$. Then C has an isolated point of degree $\leq g$ which is not in $\mathcal{C}$.*

Proof. Take a class in H which is not of this form, and let D be the divisor attached to it in Lemma 3.2. Then D is not supported on $\mathcal{C}$, so $D \geq x$ for some point $x \notin \mathcal{C}$. Since $\ell(D) = 1$ we have $\ell(x) = 1$, and x is AV-isolated since $J_C(\mathbb{Q})$ is finite. □

Lemma 3.4. *Let C be a curve over $\mathbb{Q}$ and let $E \subseteq J_C$ be an elliptic curve over $\mathbb{Q}$ of positive rank such that $(J_C/E)(\mathbb{Q})$ is finite. Then every abelian subvariety $A \subseteq J_C$ over $\mathbb{Q}$ of positive rank contains E.*

Proof. Let $P \in A(\mathbb{Q})$ be a point of infinite order. Since $(J_C/E)(\mathbb{Q})$ is finite, $nP \in E(\mathbb{Q})$ for some $n > 0$. The subgroup generated by nP is infinite, and hence Zariski dense in E, so $E \subseteq A$. □

Lemma 3.5. *Let C be a curve over $\mathbb{Q}$ and $F : C \to E$ a non-constant morphism to an elliptic curve E over $\mathbb{Q}$ with origin O. Suppose that $E(\mathbb{Q})$ is infinite and that $(J_C/F^*E)(\mathbb{Q})$*

is finite, where $F^*E \subseteq J_C$ is the image of $F^* : \mathrm{Pic}^0_E \to J_C$. Let D be an effective divisor on C such that $\ell(D + F^*(O)) = 1$. Then $\ell(D) = 1$, and there is no abelian subvariety $A \subseteq J_C$ over $\mathbb{Q}$ of positive rank such that $[D] + A \subseteq W_{\deg D}(C)$.

Proof. Since $F^*(O) \geq 0$, we have $\ell(D) \leq \ell(D + F^*(O)) = 1$. Suppose $[D] + A \subseteq W_{\deg D}(C)$ for some A as in the statement. By Lemma 3.4, $F^*E \subseteq A$. Hence for every $t \in E(\overline{\mathbb{Q}})$ there is an effective divisor D_t linearly equivalent to $D + F^*((t) - (O))$. Since $(t) + (-t) \sim 2(O)$ on E, it follows that $D_t + F^*(-t) \in |D + F^*(O)|$. A divisor contains only finitely many fibres of F, so these are infinitely many distinct divisors in $|D + F^*(O)|$, which contradicts $\ell(D + F^*(O)) = 1$. □

Lemma 3.6. *Let $\pi : C \to E$ be a morphism of degree 2 from a curve C of genus g to an elliptic curve E, both over $\mathbb{Q}$, and let D be an effective divisor on C of degree $d \leq g - 1$ such that $\pi^*(t) \not\leq D$ for every $t \in E(\overline{\mathbb{Q}})$. Then $[D] + \pi^* \mathrm{Pic}^0_E \not\subseteq W_d(C)$. If $d < g - 1$, then furthermore $\ell(D) = 1$.*

Proof. We work over $\overline{\mathbb{Q}}$. Let $V = \pi_* \mathcal{O}_C(D)$, a vector bundle of rank 2 on E. The section 1 of $\mathcal{O}_C(D)$ gives a section of V which vanishes at $t \in E$ if and only if $\pi^*(t) \leq D$, so by assumption it vanishes nowhere. Hence we have an exact sequence $0 \to \mathcal{O}_E \to V \to M \to 0$ with M a line bundle. By Riemann-Roch, $\deg M = \chi(V) = \chi(\mathcal{O}_C(D)) = d + 1 - g \leq 0$. For $\alpha \in \mathrm{Pic}^0_E$ we have $H^0(C, \mathcal{O}_C(D) \otimes \pi^*\alpha) = H^0(E, V \otimes \alpha)$. If $\alpha \neq \mathcal{O}_E$ and $M \otimes \alpha \neq \mathcal{O}_E$, then neither α nor $M \otimes \alpha$ has a non-zero section, so $H^0(E, V \otimes \alpha) = 0$. This happens for all but at most 2 classes α, so $[D] + \pi^* \mathrm{Pic}^0_E \not\subseteq W_d(C)$. If $d < g - 1$ then $\deg M < 0$, and taking $\alpha = \mathcal{O}_E$ gives $\ell(D) = h^0(V) \leq h^0(\mathcal{O}_E) = 1$. □

4. Supersingular points and lower bounds for the minimum density degree

4.1. Supersingular points on $X_1(N)$.

Lemma 4.1. *Let $N \geq 5$ and let $p \nmid N$ be a prime. The curve $X_1(N)_{\overline{\mathbb{F}}_p}$ has exactly $S_p(N)$ supersingular points, and at each of them $\Phi^2(x) = \langle p \rangle(x)$.*

Proof. Every supersingular elliptic curve over $\overline{\mathbb{F}}_p$ has a model over $\mathbb{F}_{p^2}$ whose p^2-power Frobenius endomorphism is multiplication by $-p$. For such a model, Φ^2 sends the point (E, P) to $(E, -pP) \simeq (E, pP) = \langle p \rangle(E, P)$. Since $N \geq 5$, the group $\mathrm{Aut}(E)$ acts freely on the $J_2(N)$ points of exact order N of E, and $-1 \in \mathrm{Aut}(E)$ identifies P with $-P$. Hence there are $J_2(N)/\#\,\mathrm{Aut}(E)$ points of $X_1(N)_{\overline{\mathbb{F}}_p}$ above $j(E)$, so by the Eichler mass formula $\sum_E 1/\#\,\mathrm{Aut}(E) = (p-1)/24$, the sum running over the isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, there are $S_p(N)$ supersingular points. □

Lemma 4.2. *Let C_0 be a curve over $\mathbb{F}_p$, let $e \geq 1$, let τ be an automorphism of C_0 defined over $\mathbb{F}_p$, and suppose that $\Phi^e(x) = \tau(x)$ for S distinct points $x \in C_0(\overline{\mathbb{F}}_p)$. Then every non-constant morphism $g : C_{0,\overline{\mathbb{F}}_p} \to \mathbb{P}^1$ satisfies $(p^e + 1) \deg g \geq S$.*

Proof. The morphisms $g \circ \Phi^e$ and $g \circ \tau$ have degrees $p^e \deg g$ and $\deg g$, so they are distinct. Hence the pullback of the diagonal of $\mathbb{P}^1 \times \mathbb{P}^1$ along $(g \circ \Phi^e, g \circ \tau)$ is an effective divisor of degree $(p^e + 1) \deg g$, and it contains all the S points. □

Corollary 4.3. *Let $N \geq 5$ and let $p \nmid N$ be a prime. Then*

$$\mathrm{gon}_{\overline{\mathbb{Q}}} X_1(N) \geq \mathrm{gon}_{\overline{\mathbb{F}}_p} X_1(N) \geq \frac{S_p(N)}{p^2 + 1}.$$

Proof. The first inequality holds since $X_1(N)$ has good reduction at p [44, Proposition A.1 (vii)], and the second follows from Lemma 4.1 and Lemma 4.2 with $e = 2$ and $\tau = \langle p \rangle$. □

4.2. **The incidence bound.** Combining Corollary 4.3 with Lemma 3.1 a) gives $\delta(X_1(N)) \geq S_p(N)/(2p^2+2)$. We now prove a bound which is better by a factor of almost 2. We need three lemmas.

Lemma 4.4. *Let C be a curve over $\mathbb{Q}$ with a rational point, and let $d < \operatorname{gon}_{\overline{\mathbb{Q}}} C$ be such that C has infinitely many points of degree d. Then $W_d(C)$ contains a translate $a+A$, where $a \in \operatorname{Pic}^d_C(\mathbb{Q})$ and $A \subseteq J_C$ is an abelian subvariety of positive dimension over $\mathbb{Q}$ such that $A(\mathbb{Q})$ is Zariski dense in A. Every class in $(a+A)(\overline{\mathbb{Q}})$ contains a unique effective divisor.*

Proof. Every effective divisor class of degree d on $C_{\overline{\mathbb{Q}}}$ contains a unique effective divisor, as otherwise $\operatorname{gon}_{\overline{\mathbb{Q}}} C \leq d$. Hence the points of degree d give infinitely many distinct points of $W_d(C)(\mathbb{Q})$. By Faltings' theorem [22], the Zariski closure of this set is a finite union of translates of abelian subvarieties of J_C. Its rational points are Zariski dense in it, so a component of positive dimension is defined over $\mathbb{Q}$ and has a dense set of rational points. Translating it by one of its rational points gives $a + A$. □

Lemma 4.5. *Let C be a curve over $\mathbb{Q}$ with a rational point and good reduction at p, and let C_0 be its reduction. Let $a \in \operatorname{Pic}^d_C(\mathbb{Q})$ and let $A \subseteq J_C$ be an abelian subvariety over $\mathbb{Q}$ such that $a + A \subseteq W_d(C)$, and suppose that $d < \operatorname{gon}_{\overline{\mathbb{F}}_p} C_0$. Let A_0 and a_0 be the reductions of A and a. Then $a_0 + A_0 \subseteq W_d(C_0)$, and there is an effective divisor $\mathcal{D}$ on $C_0 \times A_0$, defined over $\mathbb{F}_p$ and finite and flat of degree d over A_0, such that for every $y \in A_0(\overline{\mathbb{F}}_p)$ the fibre $\mathcal{D}_y$ is the unique effective divisor in the class $a_0 + y$.*

Proof. The abelian variety A has good reduction at p, since it is an isogeny factor of J_C, and the inclusion $A \to J_C$ extends to the Néron models over $\mathbb{Z}_{(p)}$. The point a extends by properness, and the relative W_d is closed, being the image of the relative symmetric power. Hence $a_0 + A_0 \subseteq W_d(C_0)$. Since $d < \operatorname{gon}_{\overline{\mathbb{F}}_p} C_0$, every class in $a_0 + A_0$ has a 1-dimensional space of sections. Pull back the Poincaré line bundle, normalized at a rational point of C_0, to $C_0 \times A_0$ along $y \mapsto a_0 + y$. By cohomology and base change, its direct image to A_0 is a line bundle, and the canonical section gives the divisor $\mathcal{D}$. □

In the following lemma we use the following notation. For a curve C_0 and an abelian variety A_0 of dimension r, both over $\mathbb{F}_p$, and an ample divisor H on A_0 defined over $\mathbb{F}_p$, we also write H for its pullback to $C_0 \times A_0$, V for the class of $\{x\} \times A_0$, $M = H^r > 0$ for the top self-intersection of H on A_0, and we use the pairing

$$(D, D') = D \cdot D' \cdot H^{r-1}$$

on numerical classes of divisors on $C_0 \times A_0$. For a divisor Z which is finite over A_0, its degree over A_0 is $(Z, H)/M$, and we put $h(Z) = (Z, V)$, which is the degree of Z_x against H^{r-1} for general $x \in C_0$.

Lemma 4.6. *Let C_0 be a curve and A_0 an abelian variety of dimension $r \geq 1$, both over $\mathbb{F}_p$, let $q = p^e$, let $F_C = \Phi^e$ and F_A be the q-power Frobenius endomorphisms of $C_{0,\overline{\mathbb{F}}_p}$ and $A_{0,\overline{\mathbb{F}}_p}$, and let τ be an automorphism of C_0 defined over $\mathbb{F}_p$. Suppose that $F_C(x) = \tau(x)$ for S distinct points $x \in C_0(\overline{\mathbb{F}}_p)$. Let $Z \subseteq C_0 \times A_0$ be a reduced effective divisor defined over*

$\mathbb{F}_p$ whose geometric components form one orbit under $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$*, such that Z is finite of degree $b > 0$ over A_0 and Z is not of the form $\{x\} \times A_0$. Then*

$$S \leq (\sqrt{q}+1)^2\, b.$$

Proof. Choose a very ample divisor H on A_0 defined over $\mathbb{F}_p$, and use the notation above. Since every component of Z is finite over A_0 and of dimension r, it dominates A_0, and since it is not of the form $\{x\}\times A_0$, it dominates C_0. Hence Z_x is a non-zero effective divisor on A_0 for general x, so $h = h(Z) > 0$. We have $(V,V) = (H,H) = 0$, $(V,H) = M$, $(Z,H) = bM$ and $(Z,V) = h$. The pairing is negative semidefinite on the orthogonal complement of V and H. To see this, restrict to the surface $C_0 \times B$, where B is a general complete intersection of $r-1$ divisors in the linear system of H (for $r = 1$ take $B = A_0$), and apply the Hodge index theorem.

We first show that $(Z,Z) \geq 0$. The stabilizer in A_0 of each geometric component of Z is a proper subgroup, since a divisor stable under all translations which dominates C_0 would be the whole product. Hence a general translate Z' of Z by a point of A_0 has no common component with Z, so $Z \cdot Z'$ is an effective cycle of codimension 2, and its degree against the ample class H^{r-1} is non-negative. Since Z' is algebraically equivalent to Z, it follows that $(Z,Z) \geq 0$.

Write numerically $Z = bV + (h/M)H + U$ with U orthogonal to V and H. Then $(Z,Z) = 2bh + (U,U)$, so $-(U,U) \leq 2bh$. Let $u = \tau \times F_A$, an endomorphism of $(C_0 \times A_0)_{\overline{\mathbb{F}}_p}$ of degree q^r. Numerically we have $u^*V = V$ and $u^*H = qH$, so by the projection formula $(u^*D, u^*D') = q(D,D')$ for all D, D'. In particular u^*U is orthogonal to V and H, and $(u^*U, u^*U) = q(U,U)$. By the Cauchy-Schwarz inequality on the negative semidefinite complement,

$$(Z, u^*Z) = (q+1)bh + (U, u^*U) \leq (q+1)bh + \sqrt{q}\,(-(U,U)) \leq (\sqrt{q}+1)^2 bh.$$

It remains to show that $(Z, u^*Z) \geq Sh$. Since the geometric components Z_i of Z are Galois conjugate, they all have the same pair of degrees $((Z_i,H)/M, (Z_i,V))$, with both entries positive. The morphism u is radicial, so u^*Z_i is a positive multiple of a single irreducible divisor, and its pair of degrees is $((Z_i,H)/M, q(Z_i,V))$. As the ratio of the two degrees changes, Z and u^*Z have no common component. Let x be one of the S points. The simultaneous q-power Frobenius $F_C \times F_A$ pulls Z back to qZ, as Z is defined over $\mathbb{F}_p$, and $\tau(x) = F_C(x)$, so the restrictions of Z and u^*Z to $\{x\} \times A_0$ are Z_x and qZ_x. Let R be the local ring of $C_0 \times A_0$ at the generic point of a component of $\{x\} \times Z_x$, let f, g be local equations of Z and u^*Z, and let t be a local parameter of C_0 at x. Then g is, modulo t, a unit times f^q, so

$$\operatorname{length} R/(f,g) \geq \operatorname{length} R/(f,g,t) = \operatorname{length} R/(f,t).$$

Hence the cycle $Z \cdot u^*Z$ contains $\sum_x \{x\} \times Z_x$, the sum running over the S points, with all multiplicities. Intersecting with the nef class H^{r-1} gives $(Z, u^*Z) \geq Sh$. Combining the two inequalities proves the lemma. □

Proposition 4.7. *Let C be a curve over $\mathbb{Q}$ with a rational point and good reduction at p, let C_0 be its reduction, let $e \geq 1$, $q = p^e$, and let τ be an automorphism of C_0 defined over $\mathbb{F}_p$. Suppose that $\Phi^e(x) = \tau(x)$ for S distinct points $x \in C_0(\overline{\mathbb{F}}_p)$. Then*

$$\delta(C) \geq \frac{S}{(\sqrt{q}+1)^2}.$$

Proof. Suppose the opposite, that C has infinitely many points of degree $d < S/(\sqrt{q}+1)^2$. Then $d < S/(q+1) \leq \mathrm{gon}_{\overline{\mathbb{F}}_p} C_0 \leq \mathrm{gon}_{\overline{\mathbb{Q}}} C$ by Lemma 4.2 and [44, Proposition A.1 (vii)]. Let $a + A \subseteq W_d(C)$ be the translate given by Lemma 4.4, and $\mathcal{D} \subseteq C_0 \times A_0$ the divisor given by Lemma 4.5. The divisors $\mathcal{D}_y$ are not all equal, since their classes $a_0 + y$ are distinct, so $\mathcal{D}$ has a component which is not of the form $\{x\} \times A_0$. Let Z be the reduced union of its Galois orbit. Then Z satisfies the assumptions of Lemma 4.6, with $b \leq d$, so $S \leq (\sqrt{q}+1)^2 d$, which is a contradiction. □

Proposition 4.8. *Let $N \geq 5$ and let $p \nmid N$ be a prime. Then*

$$\delta(X_1(N)) \geq \frac{(p-1)J_2(N)}{24(p+1)^2} = \frac{S_p(N)}{(p+1)^2}.$$

Proof. This follows from Lemma 4.1 and Proposition 4.7 with $e = 2$ and $\tau = \langle p \rangle$. □

4.3. **Newform factors.** When we know which factors of $J_1(N)$ have positive rank, Proposition 4.8 can be improved using the Eichler-Shimura relation. For a newform f and a prime $p \nmid N$ put

$$B_p(f) = \max_{\sigma : K_f \hookrightarrow \mathbb{C}} |\sigma(a_p(f))|^2, \qquad D_p(f) = \max\{p^2+1, (p+1)^2 - B_p(f)\}.$$

Proposition 4.9. *Let $N \geq 5$, let $p \nmid N$ be a prime, and suppose that $X_1(N)$ has infinitely many points of degree $d < \mathrm{gon}_{\overline{\mathbb{Q}}} X_1(N)$. Let $a + A \subseteq W_d(X_1(N))$ be the translate given by Lemma 4.4, and let f be a newform of level dividing N such that there is a non-zero homomorphism $A_f \to A$ over $\mathbb{Q}$. Then $d \geq S_p(N)/D_p(f)$.*

Proof. Let $C = X_1(N)$ and $i : A_f \to A$ a non-zero homomorphism. Suppose the opposite, that $d < S_p(N)/D_p(f)$. Since $D_p(f) \geq p^2 + 1$, we have $d < \mathrm{gon}_{\overline{\mathbb{F}}_p} C_0$ by Corollary 4.3. Replacing A by $i(A_f)$ and pulling the family back along i, we may use A_f as the parameter space of our family. Write $q = p^2$, $S = S_p(N)$ and A_0 for the reduction of A_f modulo p. As in the proof of Proposition 4.7, we obtain an effective divisor Z on $C_0 \times A_0$ which is finite of degree d over A_0, whose fibre over y is the unique effective divisor in the class $a_0 + i(y)$. The reduction $i_0 : A_0 \to J_{C_0}$ of i is non-zero with finite kernel, since a left inverse of i up to multiplication by an integer also reduces.

The inequalities $Sh \leq (Z, u^*Z)$ and $-(U,U) \leq 2dh$ from the proof of Lemma 4.6, with $u = \langle p \rangle \times F_A$ and $Z = dV + (h/M)H + U$, hold for the whole divisor Z, including multiplicities. For the first, decompose Z into Galois orbits of components. A component of the form $\{x\} \times A_0$ is nef and has $h = 0$, each orbit of other components contributes at least S times its value of h by the proof of Lemma 4.6, a multiplicity n contributes $n^2 \geq n$, and the cross terms are non-negative, since after a translation in A_0 the components of different orbits meet properly. The same translation argument gives $(Z, Z) \geq 0$.

We now compute (U, u^*U). Modulo the radical of the pairing, U is determined by the homomorphism i_0, since the class of Z modulo pullbacks of classes from both factors corresponds, by the universal property of the Poincaré bundle, to the homomorphism $y \mapsto [Z_y] - [Z_0]$, which is i_0. A pullback from A_0 orthogonal to V restricts to a numerically trivial class on $C_0 \times B$, while a non-zero homomorphism $A_0 \to J_{C_0}$ gives a non-zero vector in the negative definite quotient (the Jacobian of B maps onto A_0, and a numerically trivial class on $C_0 \times B$ induces the zero homomorphism $J_B \to J_{C_0}$). On these classes, u^* sends i_0 to $\langle p \rangle^* \circ i_0 \circ \pi^2$, where π is the p-power Frobenius endomorphism of A_0. The diamond operator $\langle p \rangle$ acts on the image of A_f as $\epsilon(p)$, and its action by pullback is the

inverse, while the homomorphisms $A_f \to J_1(N)$ commute with $K_f = \mathrm{End}^0_{\mathbb{Q}}(A_f)$. Hence u^* acts on i_0 by composition on the right with $T = \epsilon(p)^{-1}\pi^2$. The Eichler-Shimura relation $\pi + p\epsilon(p)\pi^{-1} = a_p(f)$ gives

$$T + qT^{-1} = \beta - 2p, \qquad \beta = \frac{a_p(f)^2}{\epsilon(p)}.$$

The conjugates of β are real, equal to $|\sigma(a_p(f))|^2$. For the positive definite inner product $\langle\ ,\ \rangle = -(\ ,\ )$ on the negative definite quotient, the adjoint of u^* is $q(u^*)^{-1}$. It follows that on the classes obtained from i_0 by composition on the right with elements of $\mathbb{Q}[\beta]$, the symmetric part $\frac{1}{2}(u^* + q(u^*)^{-1})$ of u^* acts as $(\beta - 2p)/2$.

Finally, we arrange that the largest conjugate of β appears. For $n \geq 0$ precompose the parameter map with the isogeny $(1+\beta)^n$ of A_f (after clearing denominators). The degree of the family over the parameter space is still d, and the new mixed class U_n represents $i_0 \circ (1+\beta)^n$. The cyclic $\mathbb{Q}[\beta]$-module generated by i_0 is faithful, as every non-zero element of the field $\mathbb{Q}[\beta]$ is an isogeny up to a denominator. Since β is self-adjoint on it with non-negative eigenvalues, the Rayleigh quotients $r_n = \langle U_n, \beta U_n\rangle / \langle U_n, U_n\rangle$ tend to $B_p(f)$. Writing h_n for the corresponding value of h, we obtain

$$Sh_n \leq (q+1)dh_n + \tfrac{1}{2}(2p - r_n)\langle U_n, U_n\rangle \leq dh_n \max\{q+1, (p+1)^2 - r_n\},$$

using $\langle U_n, U_n\rangle \leq 2dh_n$. Dividing by h_n and letting $n \to \infty$ gives $S \leq D_p(f)d$, which is a contradiction. □

Corollary 4.10. *Let $N \geq 5$ and let $\mathcal{F}$ be a set of newforms of level dividing N which contains a representative of every Galois orbit of newforms f such that $A_f(\mathbb{Q})$ is infinite. Suppose $\mathcal{F} \neq \emptyset$, and let P be a non-empty finite set of primes not dividing N. Then*

$$\delta(X_1(N)) \geq \min_{f\in\mathcal{F}} \max_{p\in P} \frac{S_p(N)}{D_p(f)}.$$

Proof. Suppose that $X_1(N)$ has infinitely many points of degree d smaller than the right-hand side. Since $D_p(f) \geq p^2 + 1$, we have $d < S_p(N)/(p^2+1) \leq \mathrm{gon}_{\overline{\mathbb{Q}}} X_1(N)$ for some $p \in P$, by Corollary 4.3. Let $a + A$ be the translate given by Lemma 4.4. Since $A(\mathbb{Q})$ is Zariski dense in A, every simple isogeny factor of A over $\mathbb{Q}$ has positive rank, so there is a newform $f \in \mathcal{F}$ and a non-zero homomorphism $A_f \to A$ over $\mathbb{Q}$. By Proposition 4.9, $d \geq \max_{p\in P} S_p(N)/D_p(f)$, which is a contradiction. □

Example 4.11. The only newform of level 53 which can have a positive rank abelian variety is 53.2.a.a, which is attached to an elliptic curve with $a_3 = -3$. Hence $S_3(53) = 234$, $D_3 = 10$, and Corollary 4.10 gives $\delta(X_1(53)) \geq 24$. It follows that the point of degree 22 on $X_1(53)$ found by van Hoeij [50] is sporadic. At level 720, Proposition 4.8 alone suffices: $J_2(720) = 331776$, $S_7(720) = 82944$ and $82944/64 = 1296$, which is larger than the least degree 1152 of a CM point on $X_1(720)$ [13].

The following variant uses the top self-intersection of the incidence divisor. For a newform f, a prime $p \nmid N$ and $t_p = a_p(f)^2/\epsilon(p) - 2p \in K_f$ put

$$c_p(f) = \begin{cases} \Big(\displaystyle\sum_{\sigma: K_f \hookrightarrow \mathbb{C}} \frac{1}{-\sigma(t_p)} \Big)^{-1} & \text{if } \sigma(t_p) < 0 \text{ for all } \sigma, \\ 0 & \text{otherwise.} \end{cases}$$

Note that $c_p(f) \leq 2p/[K_f : \mathbb{Q}]$.

Proposition 4.12. *Let $N \geq 5$, let $p \nmid N$ be a prime and let f be a newform of level dividing N. Suppose that $X_1(N)$ has infinitely many points of degree d, that $S_p(N) > (p^2+1)d$, and that the translate given by Lemma 4.4 contains a translate of the image of a non-zero homomorphism $A_f \to J_1(N)$. Then*

$$S_p(N) \leq (p^2 + 1 + c_p(f))d.$$

Proof. Let $A = A_f$ and $r = [K_f : \mathbb{Q}]$, and use A as the parameter space of the family as in the proof of Proposition 4.9. Since $S_p(N) > (p^2+1)d$, the divisors of the family are unique on both fibres. On $C_0 \times A_0$ remove the components of the form $\{x\} \times A_0$, and write the remaining divisor numerically as $Z = eV + L + U$, where $e \leq d$, L is pulled back from A_0 and U is the mixed class of $i : A \to J_C$. The class L is the restriction of the incidence divisor to a general $\{x\} \times A$. It is defined over $\mathbb{Q}$ in characteristic 0 and specializes to the corresponding class at p, by uniqueness. It is ample, since it is non-zero and effective and A is simple over $\mathbb{Q}$. Let $B = i^*\Theta$ be the pullback of the theta divisor of J_C, which is ample since i has finite kernel.

Any $r+1$ general translates of Z by points of A_0 meet properly, since for fixed (x, a) the allowed translation in each position lies in the proper divisor $a - Z_x$ of A_0, so the incidence variety of all the intersections and translations has dimension at most $1 + r + (r+1)(r-1) = r(r+1)$, the dimension of the space of translations. Hence $Z^{r+1} \geq 0$. The projection to A_0 of U^2 is numerically $-2B$, by the symplectic pairing on $H^1(C)$ and the principal polarization of J_C, and products with three mixed factors vanish numerically by the Künneth decomposition. Expanding gives

$$0 \leq Z^{r+1} = (r+1)\big(eL^r - rBL^{r-1}\big).$$

The element $\lambda = \phi_L^{-1}\phi_B$ belongs to the totally real subfield of $K_f = \mathrm{End}^0_{\mathbb{Q}}(A)$ fixed by the Rosati involution and is totally positive. The degree formula for polarizations (equivalently, differentiating the norm polynomial of $L + sB$) gives $rBL^{r-1}/L^r = \sum_\sigma \sigma(\lambda)$, where each embedding occurs once since $\mathrm{Lie}(A)$ is a 1-dimensional K_f-vector space. Hence $\sum_\sigma \sigma(\lambda) \leq e$.

Now apply the inequality $Sh \leq (Z, u^*Z)$ with an ample class H on A defined over $\mathbb{Q}$. Polarizing the identity above and using $T + T^\dagger = t_p$ as in the proof of Proposition 4.9 gives

$$S_p(N)\, LH^{r-1} \leq (p^2+1)e\, LH^{r-1} - B_{t_p}H^{r-1}, \qquad \phi_{B_{t_p}} = \phi_B t_p.$$

Take $H = \alpha^*L$, where α is a non-zero element of the totally real subfield. By the same degree formula, the ratio $B_{t_p}H^{r-1}/(LH^{r-1})$ is the weighted average of the values $\sigma(\lambda t_p)$ with weights $\sigma(\alpha)^{-2}$. By weak approximation (and clearing denominators) we can make these weights concentrate at any real embedding of the totally real subfield, and the embeddings of K_f above it give the same value. We obtain

$$S_p(N) \leq (p^2+1)e - \sigma(\lambda)\sigma(t_p) \quad \text{for every } \sigma.$$

If $\sigma(t_p) \geq 0$ for some σ, this contradicts $S_p(N) > (p^2+1)d$. Otherwise divide by $-\sigma(t_p)$ and sum over σ, using $\sum_\sigma \sigma(\lambda) \leq e \leq d$, to obtain the claim. □

Note that $c_p(f) = P(0)/P'(0)$, where $P(X) = \prod_\sigma (X - \sigma(t_p))$, when all the roots of P are negative, and that a monic polynomial with only real roots has only negative roots if and only if all its coefficients are positive. This is how we compute $c_p(f)$.

4.4. **Elliptic factors.** When the positive rank part of $J_1(N)$ is an elliptic curve, we can do better by using the degree of the modular parametrization.

Lemma 4.13. *Let $N \geq 5$, let E_0 be the optimal elliptic quotient of $J_0(N)$ attached to a newform of level N with rational coefficients, and let m_0 be its modular degree. Let $F : X_1(N) \to E$ be the optimal parametrization of an elliptic curve in the isogeny class of E_0, sending a fixed rational cusp to the origin, and let $m = \deg F$. Then*

$$\frac{\varphi(N)}{2} m_0 = em,$$

where $e = \#T$ is the order of the image $T \subseteq E(\mathbb{Q})_{\mathrm{tors}}$ of the group of diamond operators. In particular $e \mid \varphi(N)/2$ and $e \mid \#E(\mathbb{Q})_{\mathrm{tors}}$.

Proof. Each diamond operator acts trivially on the differential attached to F, so it changes F by a translation by a rational point of E. The composition $X_1(N) \to X_0(N) \to E_0$ factors as F followed by an isogeny $E \to E_0$, which kills T. The induced map $X_1(N) \to E/T$ is invariant under the diamond operators, so it descends to $X_0(N)$, and the optimality of $J_0(N) \to E_0$ shows that the isogeny $E/T \to E_0$ is an isomorphism. Comparing degrees gives the claim. □

Since $\mathrm{Hom}_{\mathbb{Q}}(E, E_0) \simeq \mathbb{Z}$, the degree of any isogeny $E \to E_0$ is of the form $a^2 b$, where b is the least degree of an isogeny $E \to E_0$. Hence Lemma 4.13 and the LMFDB data leave only finitely many possible values of m, and we treat each of them separately.

We first state the incidence inequality for an elliptic parameter on a curve over a finite field. For a curve B and an elliptic curve E over $\mathbb{F}_p$ and an effective divisor Z on $B \times E$, finite over E, we call the degrees of Z over E and over B its *bidegree*, and we call the morphism $B \to E$ sending x to the sum (in the group law of E) of the points of the divisor Z_x the *sum map* of Z.

Lemma 4.14. *Let B be a curve and E an elliptic curve, both over $\mathbb{F}_p$, let τ be an automorphism of B defined over $\mathbb{F}_p$, and suppose that $\Phi^2(x) = \tau(x)$ for S distinct points $x \in B(\overline{\mathbb{F}}_p)$. Let Z be an effective divisor on $B \times E$ defined over $\mathbb{F}_p$, finite over E and with no components of the form $\{x\} \times E$, of bidegree (b, k), and let $F : B \to E$ be its sum map. Suppose that $F \circ \tau - F$ is constant, and let $m = \deg F$ ($m = 0$ if F is constant). Then*

$$m \leq bk \qquad \text{and} \qquad Sk \leq (p^2+1)bk - (a_p(E)^2 - 2p)m.$$

Proof. Every component of Z dominates both factors. Let $u = \tau \times F_E$, where F_E is the p^2-power Frobenius endomorphism of E. As in the proofs of Lemma 4.6 and Proposition 4.9 (with $r = 1$, H a point of E and $h = k$), we have $Sk \leq Z \cdot u^* Z$ and $Z^2 \geq 0$. Let f_1 and f_2 be the classes of $\{x\} \times E$ and $B \times \{y\}$. For every x the divisor Z_x is linearly equivalent to $(F(x)) + (k-1)(0)$, so $Z \equiv bf_1 + kf_2 + U$, where U is the mixed part of the class of the graph Γ_F of F (and $U = 0$ if F is constant). Since $\Gamma_F \equiv mf_1 + f_2 + U$ and $\Gamma_F^2 = 0$, we have $U^2 = -2m$, so $0 \leq Z^2 = 2bk - 2m$. Similarly, $u^*\Gamma_F \equiv mf_1 + p^2 f_2 + u^* U$, and $\Gamma_F \cdot u^* \Gamma_F$ is the number of solutions of $F_E(F(x)) = F(\tau x) = F(x) + c$, counted with multiplicity, which is $m \deg(F_E - 1) = m(p^2 + 1 - (a_p(E)^2 - 2p))$. Hence $U \cdot u^* U = -m(a_p(E)^2 - 2p)$, and

$$Sk \leq Z \cdot u^* Z = (p^2+1)bk + U \cdot u^* U = (p^2+1)bk - (a_p(E)^2 - 2p)m.$$

□

Let $C = X_1(N)$ and let $F : C \to E$ be as in Lemma 4.13. Suppose that $W_d(C)$ contains a translate $a + F^*E$ such that every class in it contains a unique effective divisor. The incidence divisor on $C \times E$ of this family, with all the components of the form $\{x\} \times E$ removed, will be called the *moving incidence divisor*. Let $d' \leq d$ be its degree over E and $k > 0$ its degree over C. Its mixed class induces F^*, so its square, computed as for the graph of F, is $2d'k - 2m$. Since its translates by points of E are algebraically equivalent to it and meet it properly, its square is non-negative, so

$$m \leq d'k. \tag{4.1}$$

Proposition 4.15. *Let $N \geq 5$, let $p \nmid N$ be a prime, let $F : X_1(N) \to E$ be as in Lemma 4.13, and suppose that $W_d(X_1(N))$ contains a translate of F^*E, where $d < S_p(N)/(p^2+1)$. Let d' and k be the degrees of its moving incidence divisor over E and over $X_1(N)$. Then*

$$S_p(N)k \leq (p^2+1)d'k - mt, \qquad t = a_p(E)^2 - 2p.$$

Proof. By Corollary 4.3, every class of the translate contains a unique effective divisor, both in characteristic 0 and in characteristic p, so the incidence divisor of the family specializes to the incidence divisor of the reduced family. The moving incidence divisor specializes to a divisor which is finite over E, with the same mixed class (which induces F^*) and bidegree (d', k), and removing its components of the form $\{x\} \times E$ gives a divisor Z of bidegree (b, k) with $b \leq d'$, whose sum map is $\pm F$ up to translation. Since the newform attached to E has trivial character, $F \circ \langle p \rangle - F$ is constant. The claim now follows from Lemma 4.14 applied to $B = X_1(N)_{\mathbb{F}_p}$ and $\tau = \langle p \rangle$, using Lemma 4.1. □

Proposition 4.16. *In the setting of Proposition 4.15, suppose that $m = dk$. Then $k = 1$.*

Proof. By (4.1), $m \leq d'k \leq dk = m$, so $d' = d$ and the moving incidence divisor Z (in characteristic 0) has $Z^2 = 0$. Suppose $k > 1$, and consider the morphism $g : C \times E \to E$, $(x, y) \mapsto F(x) \pm [k]y$, with the sign chosen to agree with the mixed class of Z. The two fibre degrees and the mixed class give the numerical equivalence $g^*(0) \equiv kZ$. All the fibres of g are geometrically irreducible, since they are pullbacks of the finite étale isogeny $[k] : E \to E$ along translates of F. The optimal quotient $F_* : J_1(N) \to E$ is surjective on the integral ℓ-adic Tate modules for $\ell \mid k$, since its kernel is connected, so these covers of C are connected, and since they are smooth they are irreducible. Since $Z^2 = 0$, the effective divisor Z has intersection 0 with $g^*(0)$, so each component of Z is a fibre of g. Hence $Z \equiv rg^*(0)$ for a positive integer r, so $kr = 1$, which is a contradiction. □

For a proposed degree d let $k_0 = \lceil m/d \rceil$, and increase k_0 by 1 if $m = k_0 d$ and $k_0 > 1$. By (4.1) and Proposition 4.16, $k \geq k_0$, so Proposition 4.15 gives the following corollary.

Corollary 4.17. *In the setting of Proposition 4.15,*

$$S_p(N) \leq (p^2+1)d + \frac{\max(0, -t)\, m}{k_0}.$$

We will also use the gonality to bound k.

Lemma 4.18. *In the setting of Proposition 4.15, if $k \geq 2$ then $\operatorname{gon}_{\mathbb{Q}} X_1(N) \leq 2(d'k - m) \leq 2(dk - m)$.*

Proof. We work in characteristic 0. By Proposition 4.16 applied with d' in place of d, we have $Z^2 = 2(d'k - m) > 0$. For a general $t \in E$, intersect Z with its translate by t and push

the intersection cycle forward to C. This gives an effective divisor D_t of degree Z^2, and $t \mapsto D_t$ is a rational map $E \to C^{(Z^2)}$ defined over $\mathbb{Q}$. Since $D_t = D_{-t}$, it factors through $E/\{\pm 1\} \simeq \mathbb{P}^1$, and it is non-constant, since for a fixed $x \in C$ the point x lies in D_t only for t in the finite set $\mathrm{supp}(Z_x) - \mathrm{supp}(Z_x)$. The Abel-Jacobi image of a rational curve is a point, so we obtain infinitely many linearly equivalent effective divisors of degree Z^2 over $\mathbb{Q}$, and hence a rational pencil of degree $\leq Z^2$. □

The degree k is the same at all primes, which allows us to combine several primes. Put $u = m/k$. Then by (4.1) we have $u \leq d$, and we have the following.

Proposition 4.19. *In the setting of Proposition 4.15, for every prime $\ell \nmid N$ we have*

$$S_\ell(N) \leq (\ell^2+1)d - (a_\ell(E)^2 - 2\ell)u.$$

Proof. Let $t_\ell = a_\ell(E)^2 - 2\ell$. If $t_\ell < 0$ and $S_\ell(N) \leq (\ell^2+1)d$, the inequality is automatic. If $t_\ell < 0$ and $S_\ell(N) > (\ell^2+1)d$, this is Proposition 4.15 at ℓ, since $d' \leq d$. Suppose $t_\ell \geq 0$. Take the closure of the characteristic 0 moving incidence divisor in the product of the smooth proper models of $X_1(N)$ and E over $\mathbb{Z}_{(\ell)}$. It is a Cartier divisor, and its special fibre has the same fibre degrees and the same mixed class. Remove the components of the form $C_0 \times \{y\}$ and $\{x\} \times E_0$. The remaining divisor has degrees $k' \leq k$ and $d'' \leq d$ and the same mixed class, so the argument of Proposition 4.15 gives $S_\ell(N) \leq (\ell^2+1)d'' - mt_\ell/k' \leq (\ell^2+1)d - mt_\ell/k$. □

The same comparison works for a simple factor of arbitrary dimension. Fix an ample class H on the parameter abelian variety A over $\mathbb{Q}$, put $u = \langle U, U\rangle/(2h) > 0$ for the mixed class U of the moving incidence divisor, and let t_ℓ be the Rayleigh quotient of $\beta_\ell - 2\ell$ on U, where $\beta_\ell = a_\ell(f)^2/\epsilon(\ell)$. The mixed pairings are preserved under specialization, so the argument above gives

$$\Delta_\ell + t_\ell u \leq 0, \qquad \Delta_\ell = S_\ell(N) - (\ell^2+1)d,$$

for every prime $\ell \nmid N$. For two primes ℓ_1, ℓ_2 with $\Delta_{\ell_1} > 0 \geq \Delta_{\ell_2}$ let $w = -\Delta_{\ell_2}/\Delta_{\ell_1}$ and consider the totally real element $\gamma = w(\beta_{\ell_1} - 2\ell_1) + (\beta_{\ell_2} - 2\ell_2)$ of K_f. Adding the two inequalities with weights w and 1 shows that the Rayleigh quotient of γ is not positive, and this remains true after precomposing the parameter map with any isogeny of A. If γ has a positive conjugate, then precomposing with powers of $c + \gamma$, for an integer c larger than all $|\sigma(\gamma)|$, makes the Rayleigh quotient of γ positive, as in the proof of Proposition 4.9, which is a contradiction. The characteristic polynomial of γ has only real roots, so it has a positive root if and only if one of its coefficients has the wrong sign, which we check in exact rational arithmetic.

4.5. **The equality case.**

Proposition 4.20. *Let $N \geq 5$, let $p \nmid N$ be a prime, and suppose that $X_1(N)$ has infinitely many points of degree $d = S_p(N)/(p+1)^2$. Then every simple abelian subvariety A of positive rank of the translate given by Lemma 4.4 has dimension 1. The same conclusion holds if $d = S_p(N)/((p+1)^2 - v)$, where $v < 2p$ is a rational number such that $a_p(f)^2/\epsilon(p) = v$ for the newform f attached to A.*

Proof. Form the moving incidence divisor Z of the family parametrized by A on the special fibre at p, as in the proof of Proposition 4.9. The map $A_0 \to J_{C_0}$ given by its mixed class has finite kernel. The estimates for the whole moving divisor give

$$Sh \leq (Z, u^*Z) \leq (q+1)bh + \sqrt{q}\,(2bh - (Z,Z)),$$

so $S = (p+1)^2 d$ implies $(Z, Z) = 0$. In the second case the contribution of the mixed class to (Z, u^*Z) is $(2p - v)(bh - (Z, Z)/2)$, and again equality forces $(Z, Z) = 0$.

For a general point $s \in A_0$, the divisors Z and its translate $Z + s$ meet properly, and their intersection is finite over its image in A_0, since $Z \to A_0$ is finite. Every non-empty component of the intersection would have positive degree against $H^{\dim A-1}$, so $(Z, Z) = 0$ implies that Z and $Z + s$ are disjoint. Hence for every x the effective divisor Z_x on A_0 is disjoint from its general translate. These divisors all have the same numerical class L. A non-zero effective divisor on an abelian variety is the pullback of an ample divisor on the quotient by the connected component B of its stabilizer, and on an abelian variety of dimension ≥ 2 two translates of an ample divisor meet. Hence B has codimension 1. It stabilizes every Z_x, so it stabilizes the whole family, and hence lies in the kernel of $A_0 \to J_{C_0}$. This kernel is finite, so $\dim A = 1$. □

5. Isolated points on $X_0(N)$

By [19, Theorems 1.1 and 1.2], the curve $X_0(N)$ has a non-cuspidal sporadic point, and hence a non-cuspidal isolated point by Theorem 2.2, for all N outside a set of 54 levels. Of these 54 levels, 15 are the levels with $X_0(N)$ of genus 0, 5 are the levels $N = 20, 24, 32, 36, 49$, with $X_0(N)$ of genus 1, and the remaining 34 levels are

$$\begin{aligned} &22, 23, 26, 28, 29, 30, 31, 33, 35, 39, 40, 41, 46, \\ &47, 48, 50, 59, 60, 70, 71, 72, 80, 87, 94, 96, 144, \\ &53, 61, 65, 79, 83, 89, 101, 131. \end{aligned} \tag{5.1}$$

Proposition 5.1. *Suppose $X_0(N)$ is of genus ≤ 1. Then $X_0(N)$ has a non-cuspidal isolated point if and only if $N \in \{11, 14, 15, 17, 19, 21, 27\}$.*

Proof. On a curve of genus 0 with a rational point, every point x of degree d satisfies $\ell(x) = d + 1 \geq 2$. On a curve of genus 1 with a rational point, every point x of degree $d \geq 2$ satisfies $\ell(x) = d \geq 2$. Hence only rational points can be isolated on the curves $X_0(N)$ of genus 1, and all of them are isolated since all these curves have rank 0 [17, Theorem 3.1]. The curves $X_0(N)$ of genus 1 are the ones with $N \in \{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}$, and by the results of Mazur and Kenku (see [19]), they have non-cuspidal rational points exactly for $N \in \{11, 14, 15, 17, 19, 21, 27\}$. □

5.1. **The 26 levels with $J_0(N)(\mathbb{Q})$ finite.** For the 26 levels in the first two lines of (5.1), the group $J_0(N)(\mathbb{Q})$ is finite [17, Theorem 3.1]. We apply Corollary 3.3 with $C = X_0(N)$, $c = \infty$ and $\mathcal{C}$ the set of all cusps of $X_0(N)$. Recall (see for example [54]) that the cusps of $X_0(N)$ fall into Galois orbits Q_u indexed by the divisors u of N, where Q_u consists of the cusps a/s with $\gcd(s, N) = u$ and has degree $\varphi(\gcd(u, N/u))$. We compute the group H generated by the classes $[Q_u - (\deg Q_u)\infty]$ as follows. In integral homology coordinates, the class $[Q_u - (\deg Q_u)\infty]$ is the sum over the cusps a/s in Q_u of the cuspidal periods of the modular symbols $\{\infty, a/s\}$, modulo $\mathbb{Z}^{2g}$, which we compute with the integral period map of SageMath [49] on the plus and minus modular symbols. The Smith normal form of the lattice of integral relations between these vectors gives H and the coordinates of each generator. We then enumerate the sums $\sum_u m_u[Q_u - (\deg Q_u)\infty]$ with $m_u \geq 0$ and $\sum_u m_u \deg Q_u \leq g$, and count the distinct classes among them. Note that we use only the subgroup H of $J_0(N)(\mathbb{Q})$, so we do not need to know $J_0(N)(\mathbb{Q})$.

Proposition 5.2. *Let N be one of the 26 levels in the first two lines of (5.1). Then $X_0(N)$ has a non-cuspidal isolated point.*

Proof. We compute the order of H and the number b of classes in H represented by effective cuspidal divisors of degree $\leq g$, which are listed in Table 1. In all the cases $b < \#H$, so the claim follows from Corollary 3.3. □

TABLE 1. The order of the group H generated by the cuspidal divisor classes on $X_0(N)$ and the number b of classes in H represented by effective cuspidal divisors of degree $\leq g$.

N	g	$\#H$	b	N	g	$\#H$	b
22	2	25	9	47	4	23	5
23	2	11	3	48	3	128	112
26	2	21	9	50	2	15	9
28	2	36	19	59	5	29	6
29	2	7	3	60	7	55 296	24 540
30	3	192	96	70	9	41 472	9 400
31	2	5	3	71	6	35	7
33	3	100	16	72	5	1 152	976
35	3	48	16	80	7	6 912	3 896
39	3	56	16	87	9	1 960	220
40	3	144	96	94	11	2 116	244
41	3	10	4	96	9	32 768	22 496
46	5	242	36	144	13	884 736	559 760

5.2. **The 8 levels with $X_0^+(N)$ an elliptic curve of rank 1.** For the 8 levels $N \in \{53, 61, 65, 79, 83, 89, 101, 131\}$ in the last line of (5.1), the curve $E = X_0^+(N)$ is an elliptic curve of rank 1 and $\operatorname{rk} J_0(N)(\mathbb{Q}) = 1$ [11, Section 5.2], [42, Table 1 and Section 9]. Let $\pi : X_0(N) \to E$ be the quotient map. By the isogeny decomposition, $(J_0(N)/\pi^*E)(\mathbb{Q})$ is finite, so by Lemma 3.4 every abelian subvariety of $J_0(N)$ of positive rank contains π^*E. Hence by Lemma 3.6, a point x of degree $d < g - 1$ on $X_0(N)$ such that $\pi^*(t) \not\leq x$ for all $t \in E(\overline{\mathbb{Q}})$ is isolated. Since $\delta(X_0(N)) = 2$, such points are not sporadic.

Lemma 5.3. *Let $p \equiv 3 \pmod 4$ be a prime and let E_{-p} be an elliptic curve over $\overline{\mathbb{Q}}$ with CM by the maximal order of $\mathbb{Q}(\sqrt{-p})$. Then $(E_{-p}, \ker \sqrt{-p})$ defines a point of degree $h(-p)$ on $X_0(p)$, all of whose geometric points are fixed by w_p.*

Proof. The endomorphism $\sqrt{-p}$ has degree p and cyclic kernel. Let $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(j(E_{-p})))$ and choose a model of E_{-p} over $\mathbb{Q}(j(E_{-p}))$. Then $\sigma(\sqrt{-p}) = \pm\sqrt{-p}$, and both have the same kernel, so the point is defined over $\mathbb{Q}(j(E_{-p}))$, which has degree $h(-p)$, and its degree is exactly $h(-p)$ since its image on $X_0(1)$ has this degree. The quotient $E_{-p}/\ker\sqrt{-p}$ is isomorphic to E_{-p} via $\sqrt{-p}$, and the image of $E_{-p}[p]$ is $\ker\sqrt{-p}$, so the point is fixed by w_p, and the same holds for its conjugates. □

Proposition 5.4. *The curves $X_0(83)$ and $X_0(131)$ have isolated CM points of degree 3 and 5, respectively.*

Proof. Let $p \in \{83, 131\}$ and let x be the point given by Lemma 5.3. Its $h(-p)$ geometric points are distinct and all of them are ramification points of π. Hence for $t \in E(\overline{\mathbb{Q}})$ the divisor $\pi^*(t)$ is either twice a geometric point of x or the sum of two distinct points

with the same image, and neither is $\leq x$. Since $h(-83) = 3 < 6 = g(X_0(83)) - 1$ and $h(-131) = 5 < 10 = g(X_0(131)) - 1$, the point x is isolated. □

Proposition 5.5. *The curve $X_0(65)$ has an isolated cubic point.*

Proof. Box, Gajović and Goodman [11, Section 5.2.4] found non-cuspidal cubic points on $X_0(65)$ defined over $\mathbb{Q}(\alpha)$, where $\alpha^3 - \alpha^2 + \alpha - 2 = 0$. Let x be such a point. The degree of x over $\pi(x)$ divides 3 and is at most 2, so it is 1, and the 3 geometric points of x have distinct images on E. Hence $\pi^*(t) \not\leq x$ for all $t \in E(\overline{\mathbb{Q}})$, and since $3 < g(X_0(65)) - 1 = 4$, the point x is isolated. □

For the remaining 5 levels we use the residual divisor of a canonical divisor.

Proposition 5.6. *Let $p \in \{53, 61, 79, 89, 101\}$ and let g be the genus of $X_0(p)$. Then $X_0(p)$ has an isolated point of degree $g - 1$.*

Proof. Let $C = X_0(p)$ and $D = (g-1)\infty$. The Fricke involution interchanges the cusps ∞ and 0, so $\pi^*(t) \not\leq D$ for all $t \in E(\overline{\mathbb{Q}})$, and by Lemma 3.6, $[D] + \pi^* \operatorname{Pic}^0_E \not\subseteq W_{g-1}(C)$. Since $L \mapsto K_C - L$ maps $W_{g-1}(C)$ to itself, the same holds for the class $K_C - D$.

We compute that the echelon basis of $S_2(\Gamma_0(p))$ at ∞ has leading orders $1, \ldots, g$. Hence the last form $f = q^g + \cdots$ spans the space of differentials vanishing on D, and $\operatorname{div}(f\,dq/q) = D + P$, where P is an effective divisor of degree $g - 1$ over $\mathbb{Q}$ with $\infty \notin \operatorname{supp} P$ and $\ell(P) = \ell(K_C - D) = 1$. At prime level we have $w_p = -U_p$ on $S_2(\Gamma_0(p))$, so if the coefficient $a_p(f)$ is non-zero, then the differential $f\,dq/q$ does not vanish at the cusp 0. We compute that

p	53	61	79	89	101
g	4	4	6	7	8
$a_p(f)$	1/3	1/2	1/8	1/9	1/27

so P is supported on non-cuspidal points. Since $P \sim K_C - D$, it is not contained in a translate of π^*E in $W_{g-1}(C)$, so it is not contained in a translate of any positive rank abelian subvariety. Every point $x \leq P$ is then isolated, since a pencil or an abelian translate through x would give one through P after adding $P - x$.

In fact P is a single point. To see this, let $Z = D + P$, let ω_1, ω_2 be the differentials given by the first two echelon forms and $\omega = f\,dq/q$. For $i = 3, 4$, restriction to Z gives an isomorphism

$$H^0(C, iK_C)/\omega H^0(C, (i-1)K_C) \simeq H^0(Z, iK_C|_Z).$$

We compute these spaces by multiplying differentials, checking the dimensions given by Riemann-Roch (expansions modulo $q^{4(2g-2)+1}$ suffice by the degree bound). Multiplication by ω_1 between the two spaces is invertible, and we compute that the characteristic polynomial of the multiplication by ω_2/ω_1 is $T^{g-1}F_p(T)$, where the factor T^{g-1} comes from D and F_p is irreducible over $\mathbb{Q}$ of degree $g - 1$. Hence P is a single point of degree $g - 1$. □

Proof of Theorem 1.2. This follows from [19, Theorems 1.1 and 1.2], Theorem 2.2 and Propositions 5.1, 5.2 and 5.4 to 5.6. □

6. Isolated points on $X_1(N)$ of small level

Proposition 6.1. *Let $N \in \{1, \ldots, 16, 18, 20\}$. Then $X_1(N)$ has no non-cuspidal isolated points.*

Proof. The curve $X_1(N)$ is of genus 0 for $N \in \{1, \dots, 10, 12\}$, and on such a curve every point x satisfies $\ell(x) \geq 2$. It is of genus 1 for $N \in \{11, 14, 15\}$, and then only rational points can satisfy $\ell(x) = 1$, but all the rational points on $X_1(N)$ are cusps by Mazur's theorem [36].

It remains to deal with $N \in \{13, 16, 18, 20\}$. Let g be the genus of $X_1(N)$ and c a rational cusp. By [17, Theorem 3.1], $J_1(N)(\mathbb{Q})$ is finite. We compute all the effective divisors D of degree $\leq g$ supported on the cusps other than c which satisfy $\ell(D) = 1$, and an upper bound for $\#J_1(N)(\mathbb{Q})$, as the greatest common divisor of the orders of $J_1(N)(\mathbb{F}_p)$ for the odd primes $p \leq 73$ not dividing N:

N	g	$\#D$ of degree $0, \dots, g$	total	bound for $\#J_1(N)(\mathbb{Q})$
13	2	$1, 5, 13$	19	19
16	2	$1, 5, 14$	20	20
18	2	$1, 5, 15$	21	21
20	3	$1, 5, 18, 36$	60	60

By the uniqueness in Lemma 3.2, distinct divisors D give distinct classes $[D - (\deg D)c]$, so all the classes in $J_1(N)(\mathbb{Q})$ are of this form. Suppose x is a non-cuspidal point with $\ell(x) = 1$. Then by the uniqueness in Lemma 3.2, x is the divisor attached to the class $[x - (\deg x)c]$, which is a contradiction since this divisor is cuspidal. □

Proposition 6.2. *Let $N \in \{17, 19, 22, 23, 24, 25, 26, 27, 32\}$. Then $X_1(N)$ has a non-cuspidal isolated point of degree d_N, where*

N	17	19	22	23	24	25	26	27	32
d_N	5	7	5	10	5	6	6	6	9

Proof. By [17, Theorem 3.1], $J_1(N)(\mathbb{Q})$ is finite, so it is enough to find a non-cuspidal point x of degree d_N with $\ell(x) = 1$. For example, let a be a root of the irreducible polynomial $t^5 - 3t^3 + 2t + 1$. On the alternative model of $X_1(17)$ from [47], the point

$$(x, y) = (a^4 - a^3 - 2a^2 + 2a + 1,\ a)$$

is a non-cuspidal point of degree 5, and the corresponding point x of $X_1(17)$ satisfies $\ell(x) = 1$.

In general, for each N we give an irreducible polynomial f_N of degree d_N and the coordinates (x, y) of a point on the alternative model of $X_1(N)$ from [47] as polynomials in a root a of f_N. In the coordinates of [47], the parameters

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

$$b = rs(r - 1), \qquad c = s(r - 1)$$

give the elliptic curve $y^2 + (1-c)xy - by = x^3 - bx^2$ with the point $(0, 0)$. We verify that the place of the function field has degree d_N, that the discriminant is non-zero and that $(0, 0)$ has exact order N. We then verify that f_N remains squarefree of the same degree modulo 101, that all the reductions of the points lie in the smooth part of the model and away from the cusps, and that the sum $\overline{x}$ of the corresponding places of the reduction satisfies $\ell(\overline{x}) = 1$. By upper semicontinuity, $\ell(x) = 1$. The same script can also compute $\ell(x)$ directly in characteristic 0. The points at levels 25 and 32 are the points `1.25.6.a` and `1.32.9.a` of the census [43], found by van Hoeij [50]. □

Remark 6.3. One way to find such points is the following. Let T be a divisor of degree g on $X_1(N)$ supported on the rational cusps (not necessarily effective) such that $\ell(T) = 1$. Then the unique effective divisor Z linearly equivalent to T is defined over $\mathbb{Q}$, and every non-cuspidal point $x \leq Z$ satisfies $\ell(x) = 1$. This explains why we find isolated points even at levels where no non-cuspidal point is sporadic.

7. Sporadic points on $X_1(N)$

7.1. **Reduction to finitely many levels.** By [13, Theorem 8.2], the curve $X_1(N)$ has a sporadic CM point for all N outside the union of [13, Tables 4 and 5]. These tables contain 67 and 227 levels, respectively, all of them ≤ 720. For the levels in Table 4 the curve $X_1(N)$ has no sporadic CM points, so we need to find a non-CM sporadic point, while for the levels in Table 5 either a CM or a non-CM sporadic point is needed. Hence it remains to deal with these 294 levels.

For each such N we take as an upper bound $w(N)$ for the least degree of a non-cuspidal point on $X_1(N)$ the smallest of the least degree of a CM point [13], the degrees of the points in the census [43] (after forgetting the first generator), the degrees of the points of van Hoeij [50], and the degrees of the explicit points that we find below. For $m, N \geq 1$ and $h = \gcd(m, N)$, we can map a point of $X_1(m)$ to $X_1(h)$ and take a point in its preimage on $X_1(N)$, which gives

$$w(N) \leq w(m)\,[\overline{\Gamma}_1(h) : \overline{\Gamma}_1(N)],$$

where the bars denote the images in $\mathrm{PSL}_2(\mathbb{Z})$. All these maps preserve the non-cuspidal locus.

As lower bounds for $\delta(X_1(N))$ we use Lemma 3.1, the list of all N with $J_1(N)(\mathbb{Q})$ finite [17, Theorem 3.1], the bounds for the gonality of $X_1(N)$ from [20] and [51, Theorem D], Abramovich's bound [1] with the eigenvalue bound of Kim and Sarnak [31], which gives

$$\mathrm{gon}_{\mathbb{C}}\, X_1(N) \geq \frac{975}{98304}[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma}_1(N)]$$

(see also [19]), the results of Section 4, and the inequality $\delta(X_1(N)) \geq \delta(X_1(h))$ for $h \mid N$ from Lemma 3.1 c). Note also that a known sporadic point of degree e on $X_1(N)$ gives $\delta(X_1(N)) \geq e + 1$.

7.2. **The levels without sporadic points.**

Proposition 7.1. *Let $N \in A = \{1, \ldots, 20\} \cup \{22, \ldots, 27\} \cup \{32\}$. Then $X_1(N)$ has no non-cuspidal sporadic points.*

Proof. The gonality of $X_1(N)$ over $\mathbb{Q}$ [20, Table 1] is given by the following table.

$\mathrm{gon}_{\mathbb{Q}}\, X_1(N)$	N
1	$1, \ldots, 10, 12$
2	$11, 13, 14, 15, 16, 18$
3	20
4	$17, 22, 24$
5	$19, 25$
6	$26, 27$
7	23
8	32

By Lemma 3.1 a), $\delta(X_1(N)) \leq \operatorname{gon}_{\mathbb{Q}} X_1(N)$, so it is enough to show that $X_1(N)$ has no non-cuspidal points of degree $< \operatorname{gon}_{\mathbb{Q}} X_1(N)$. By the classifications of the possible torsion groups of elliptic curves over number fields of degree $d \leq 7$ [36, 30, 28, 17, 18, 39, 40, 41], no elliptic curve over a number field of degree $d < \operatorname{gon}_{\mathbb{Q}} X_1(N)$ has a point of order N. For $N = 32$ we need the fact that there is no point of order 32 over number fields of degree 7, which is [41, Proposition 5.7]. We have rerun this computation (see the README of our repository). □

7.3. **The levels settled by the general bounds.** For each $N \leq 720$, we compute the best upper bound $w(N)$ and the best lower bound for $\delta(X_1(N))$ given by the results of this paper, and record them, together with their sources, in the table of levels in the repository. For the newform comparisons, the script checks that the sum of the dimensions of the coefficient fields, with oldform multiplicities, equals the genus, and for each non-rational newform it isolates the roots of the characteristic polynomial of $a_p(f)^2/\epsilon(p)$ over $\mathbb{Q}$ (a lower bound for the largest root suffices in Proposition 4.9). We use the primes $2, 3, 5, 7, 11, 13, 17, 19$ not dividing N. For most of the levels the inequality $w(N) < \delta(X_1(N))$ follows from Proposition 4.8 or Proposition 4.9, but a few levels need the refinements of Section 4.4. We give the details for these levels.

Proposition 7.2. *We have $\delta(X_1(255)) \geq 257$.*

Proof. We have $S_2(255) = 2304$ and $2304/9 = 256$, so $\delta(X_1(255)) \geq 256$ by Proposition 4.8. Suppose $X_1(255)$ has infinitely many points of degree 256. By Proposition 4.20, the translate given by Lemma 4.4 contains a translate of an elliptic curve of positive rank in $J_1(255)$. By modularity, such an elliptic curve would be isogenous to an elliptic curve over $\mathbb{Q}$ of conductor dividing 255. The only such isogeny classes are 15a, 17a, 51a and 85a, and all of them have rank 0, which is a contradiction. □

Proposition 7.3. *We have $\delta(X_1(105)) > 64$ and $\delta(X_1(252)) > 216$.*

Proof. At level 105, Proposition 4.9 gives $\delta(X_1(105)) \geq 64$, and the only newform which does not give a better bound is 105.2.s.a, for which $a_2(f)^2/\epsilon(2) = 3$. Since $S_2(105) = 384 = ((2+1)^2 - 3) \cdot 64$, the second part of Proposition 4.20 shows that infinitely many points of degree 64 would force A_f to have dimension 1, which is not the case. Similarly, at level 252 the only newform left at degree 216 is 252.2.i.a, with $a_5(f)^2/\epsilon(5) = 4$ and $S_5(252) = 6912 = ((5+1)^2 - 4) \cdot 216$, and A_f is not of dimension 1. □

Proposition 7.4. *We have $\delta(X_1(192)) > 128$.*

Proof. Proposition 4.9 leaves only the elliptic curves in the isogeny class 192a, which has rank 1. The optimal parametrization $X_0(192) \to E_0$ has degree 8. In the normalized integral period map of the 2-dimensional modular symbol space attached to 192a, the paths $\{\infty, 1153/1344\}$ and $\{\infty, 385/1728\}$ have period vectors $(0, -1)$ and $(-1, -3)$. These paths lift to closed paths on $X_1(192)$, since

$$\begin{pmatrix} 1153 & 495 \\ 1344 & 577 \end{pmatrix}, \begin{pmatrix} 385 & 43 \\ 1728 & 193 \end{pmatrix} \in \Gamma_1(192).$$

The two period vectors have determinant -1, so the image of the period lattice of $X_1(192)$ is the full period lattice of $X_0(192)$. Hence in Lemma 4.13 we have $e = 1$ and $m = (\varphi(192)/2) \cdot 8 = 256$. Suppose $X_1(192)$ has infinitely many points of degree $d = 128$. Then

$k_0 = 3$ in Corollary 4.17, and with $p = 5$ we have $S_5(192) = 4096$, $a_5(E) = -2$, $t = -6$, and

$$4096 > 26 \cdot 128 + \frac{6 \cdot 256}{3} = 3840,$$

which is a contradiction. The exact computation of the two periods can be found in `x1-sporadic/certificates/periods192.sage`. □

Proposition 7.5. *We have $\delta(X_1(208)) \geq 193$.*

Proof. The only newform which Proposition 4.9 does not exclude at degree 192 is 208.2.a.b, attached to an elliptic curve E with $a_3(E) = -1$ and $a_7(E) = -5$. Suppose $X_1(208)$ has infinitely many points of degree $d \leq 192$. Since $J_2(208) = 32256$, we have $S_3(208) = 2688$ and $S_7(208) = 8064$, and the traces $a_p(E)^2 - 2p$ are -5 and 11. Proposition 4.19 gives

$$u \geq \frac{2688 - 10 \cdot 192}{5} = \frac{768}{5}, \qquad u \leq \frac{50 \cdot 192 - 8064}{11} = \frac{1536}{11},$$

which is a contradiction. □

Proposition 7.6. *We have $\delta(X_1(141)) > 92$.*

Proof. The only newform left by Proposition 4.9 is 141.2.a.d, attached to the elliptic curve $E =$141d1. The isogeny class of E contains only one curve, the modular degree of E is 4, and $E(\mathbb{Q})_{\mathrm{tors}}$ is trivial, so by Lemma 4.13 the optimal map $F : X_1(141) \to E$ has degree $m = (\varphi(141)/2) \cdot 4 = 184$. Suppose $X_1(141)$ has infinitely many points of degree 92. Since $m = 2 \cdot 92$, Proposition 4.16 and (4.1) give $k \geq 3$. On the other hand, at $p = 2$ we have $S_2(141) = 736$ and $t = -4$, so Proposition 4.15 gives $736 \leq 5 \cdot 92 + 736/k$, so $k \leq 2$, which is a contradiction. □

7.4. **Cuspidal fibres.** For 10 levels we prove the existence of a sporadic point without exhibiting it.

Lemma 7.7. *Let N be such that $J_1(N)(\mathbb{Q})$ is finite, and suppose that $X_1(N)$ has a non-cuspidal point of degree $\leq d$, but no non-cuspidal sporadic points. Then one of the following holds:*

a) *there is a non-constant modular unit on $X_1(N)$, defined over $\mathbb{Q}$, of degree $\leq d$,*
b) *there is an effective cuspidal divisor $D = S + E$ of degree $\leq d$ with $\ell(D) \geq 2$, where S is the sum of all the rational cusps and $E \geq 0$.*

Proof. Let d_0 be the least degree of a non-cuspidal point on $X_1(N)$. By assumption $d_0 \geq \delta(X_1(N))$, and since there are only finitely many cusps, $d_0 \leq \delta(X_1(N))$. By Lemma 3.1 b), $\delta(X_1(N)) = \mathrm{gon}_{\mathbb{Q}} X_1(N)$, so there is a morphism $f : X_1(N) \to \mathbb{P}^1$ of degree $d_0 \leq d$. Let c be a rational cusp. A non-cuspidal point in the fibre of f over $f(c)$ would have degree $\leq d_0 - 1$, so this fibre consists of cusps. If two rational cusps have distinct images under f, then composing f with a fractional linear transformation sending these images to 0 and ∞ gives a modular unit of degree d_0, and a) holds. Otherwise all the rational cusps lie in one fibre, which is a cuspidal divisor $D \geq S$ with $\ell(D) \geq 2$, and b) holds. □

To rule out a) we use the full lattice of rational modular units modulo constants [46, 20]. Multiplying the valuation of a unit at each Galois orbit of cusps by the degree of the orbit, we obtain a vector v whose coordinates sum to 0 and whose ℓ^1-norm is twice the degree of the unit. Let i and j be the indices of a largest and a smallest coordinate of v. Bounding

the positive summands v_a^2 by $v_i v_a$ and the negative ones by $v_j v_a$ gives $\sum_a v_a^2 \le d(v_i - v_j)$, so

$$\|2v - d(e_i - e_j)\|^2 \le 2d^2.$$

Hence it is enough to enumerate the vectors of the lattice in finitely many balls, which we do with Magma's proof flag (by negating v we may assume $i < j$).

To rule out b), note that by Riemann-Roch $\ell(S+E) = 1$ if and only if the $\deg(S+E)$ conditions imposed by $S+E$ on the regular differentials (the coefficients of their expansions, which we call *jets*, at the cusps in the support, up to the multiplicities) are linearly independent. To compute jets of differentials at the cusps we use the following explicit forms of weight 2 on $\Gamma_1(N)$: the products $E^{(1)}_{(0,i)} E^{(1)}_{(0,j)}$ of Eisenstein series of weight 1, whose transformation law and Fourier coefficients are given in [55, Lemma 4.7], and the sums of $(2\pi i)^{-2}\wp((u\tau+v)/N; \mathbb{Z}+\tau\mathbb{Z})$ over the $\Gamma_1(N)$-orbits of non-zero pairs (u,v) modulo N. For $q = e^{2\pi i\tau}$ and $z = \zeta_N^v q^{u/N}$, the normalized Weierstrass function has the expansion

$$\frac{1}{12} + \frac{z}{(1-z)^2} + \sum_{m\ge 1}\left(\frac{q^m z}{(1-q^m z)^2} + \frac{q^m/z}{(1-q^m/z)^2} - \frac{2q^m}{(1-q^m)^2}\right).$$

At the cusp represented by a matrix with bottom row (c,b) the local parameter is $q^{\gcd(c,N)/N}$, and we expand these forms after applying a lift of this row to $\mathrm{SL}_2(\mathbb{Z})$ (see `x1-sporadic/certificates/eisenjets.py` and `x1-sporadic/certificates/extra_eis.py`). A form of weight 2 gives a differential with at most simple poles at the cusps, whose residues are non-zero multiples of its constant terms, so by the residue theorem the matrix of constant terms has rank at most the number of geometric cusps minus 1. We work modulo a prime $\mathfrak{p}$ of $\mathbb{Q}(\zeta_N)$ of degree 1. If the constant term matrix modulo $\mathfrak{p}$ attains this bound, then an invertible maximal minor lifts the kernel, so the kernel modulo $\mathfrak{p}$ (the cusp forms) is the reduction of the kernel in characteristic 0, and the linear independence of jets of cusp forms modulo $\mathfrak{p}$ implies their independence in characteristic 0.

Proposition 7.8. *For $N \in \{54, 59, 60, 71\}$ the curve $X_1(N)$ has a non-cuspidal sporadic point of degree $\le d$, where $d = 13, 31, 13, 44$, respectively.*

Proof. For these N the group $J_1(N)(\mathbb{Q})$ is finite [17, Theorem 3.1], and $X_1(N)$ has a non-cuspidal point of degree d: the points `1.54.13.a`, `1.59.31.a` and `1.60.13.a` of the census [43] and the point of degree 44 on $X_1(71)$ found by van Hoeij [50]. Suppose $X_1(N)$ has no non-cuspidal sporadic points. We compute (and similarly with `x1-sporadic/certificates/ex59.m`, `x1-sporadic/certificates/ex60.m` and `x1-sporadic/certificates/ex71.m`) that there are no non-constant modular units over $\mathbb{Q}$ of degree $\le d$, so we are in case b) of Lemma 7.7. The numbers of rational cusps are $r = 18, 29, 12, 35$, respectively. For $N = 54$ case b) is impossible since $r > d$. For $N = 59$ and $N = 71$ all the other cusps have degree $(N-1)/2 > d - r$, and for $N = 60$ the degree $d - r$ of E is 1. Hence E is supported on the rational cusps, and it remains to show that the jets imposed by $S + E$ are independent, with $\deg E \le 2, 9, 1$, respectively.

For $N = 59, 71$, the Fricke involution maps the orbit of rational cusps to the orbit of the cusp ∞ under the diamond operators. In the transported local parameters, the jets are, up to invertible constants, the coefficient functionals a_i at ∞ and their translates by the diamond operators, which correspond to the Hecke operators $T_i\langle u\rangle$ under the duality between cusp forms and the Hecke algebra. Their linear independence follows from the independence of their actions on a single modular symbol, which we verify on the cuspidal

modular symbols of sign -1 modulo 1009. At level 59 we test the first two jets at all the rational cusps and a third jet at one cusp, which by the diamond symmetry covers all E of degree ≤ 2. At level 71 we test the first three jets at all the rational cusps, and the jets up to order 10 at every triple of cusps up to simultaneous diamond translation. A divisor E of degree ≤ 9 can require more than three jets at no more than three cusps, and independence of a collection implies the independence of all its subcollections.

For $N = 60$ we use the pullback of a nowhere vanishing differential on $X_0(15)$. In the indexing of the cusps of [20], its valuation at the cusp i is $4\gcd(i, 15)/\gcd(i, 60) - 1$, by the ratio of cusp widths, and it has no non-cuspidal zeros since $X_0(15)$ has no elliptic points. Multiplying it by rational modular units, we find, for a representative of each of the two orbits of rational cusps under the diamond operators, regular differentials with valuation 0 and 1 at that representative and positive valuation at all the other rational cusps. Translating by the diamond operators gives the independence of the required jets.

In all cases we obtain a contradiction with Lemma 7.7. □

For the remaining 6 levels in this subsection, the points come from lower levels. The map $X_1(N) \to X_1(N/2)$ has degree 3 for $N = 90, 94$, and the maps $X_1(96) \to X_1(48)$, $X_1(108) \to X_1(54)$ and $X_1(120) \to X_1(60)$ have degree 4, while $X_1(150) \to X_1(75)$ has degree 3. In all six cases $J_1(N)(\mathbb{Q})$ is finite [17, Theorem 3.1]. The test for case b) of Lemma 7.7 is now larger, as the divisor E can contain non-rational cusps, and we organize it as follows. We partition the cuspidal points into buckets. For a bucket width s and an allocation (b_i) of non-negative integers to the buckets, we allow at each cuspidal point of bucket i every multiplicity consistent with an excess degree (the degree of its part in E) of at most $s(b_i + 1) - 1$, truncated at the total budget $d - \deg S$. Every divisor E of degree $\leq d - \deg S$ is covered by the system of jet conditions of an allocation with $\sum_i b_i = \lfloor (d - \deg S)/s \rfloor$. When the rows of such a system are dependent, we compute the space of relations. The support of a non-zero relation forces the multiplicity of each cuspidal point to be at least the largest jet index used at any of its geometric points, and subtracting the contribution of S gives a lower bound for the degree of E. We select coordinates on which one relation is non-zero and which together force $\deg E > d - \deg S$. A relation of allowable degree has to vanish at one of these coordinates, and intersecting the relation space with each of these coordinate hyperplanes reduces its dimension. Repeating this, we exclude all the non-zero relations of allowable degree.

Proposition 7.9. *The curve $X_1(90)$ has a non-cuspidal sporadic point of degree ≤ 30.*

Proof. The point `1.45.10.a` of the census [43] gives a non-cuspidal point of degree ≤ 30. Suppose $X_1(90)$ has no non-cuspidal sporadic points. We compute that there are no non-constant modular units over $\mathbb{Q}$ of degree ≤ 30, so we are in case b) of Lemma 7.7, where S is the sum of the 24 rational cusps and E is a rational effective cuspidal divisor of degree ≤ 6. There are 8, 6 and 4 cuspidal points of degrees 2, 4 and 6, respectively, and all the other non-rational cusps have degree > 6. Modulo the prime above 181 given by the chosen primitive 90-th root of unity in $\mathbb{F}_{181}$, the constant term matrix has rank 127, one less than the number of geometric cusps. We verify that the first three jets at all the rational cusps and the first two jets at every geometric point of the cusps of degree 2, together with the jets up to order 7 at any two rational cusps, the third jet at any cusp of degree 2 and the first jet at any cusp of degree 4 or 6, are linearly independent. There are $\binom{24}{2} \cdot 8 \cdot 10 = 22080$ such collections. Every $S + E$ requires a subcollection of one of them, since each rational

cusp of multiplicity at least 4 uses at least 3 of the 6 available degrees. Hence $\ell(S+E)=1$, which is a contradiction. □

Proposition 7.10. *The curve $X_1(96)$ has a non-cuspidal sporadic point of degree ≤ 44.*

Proof. The point `1.48.11.a` of the census gives a non-cuspidal point of degree ≤ 44. Suppose $X_1(96)$ has no non-cuspidal sporadic points. We compute that there are no non-constant modular units over $\mathbb{Q}$ of degree ≤ 44, so we are in case b) of Lemma 7.7, with $\deg E \leq 20$. The 49 cuspidal points consist of 24, 16, 4, 3 and 2 points of degrees 1, 2, 4, 8 and 16, respectively. Modulo a prime above 193, the constant term matrix has rank 127 and the jets of the cusp forms span a space of dimension 193, the genus. We partition the 49 cuspidal points into 10 buckets of at most 5 points and take $s=2$. This gives $\binom{19}{9} = 92378$ systems of jet conditions, and the relation space test described above excludes all non-zero relations of allowable degree in each of them. Hence $\ell(S+E)=1$, which is a contradiction. □

Proposition 7.11. *For $N=108$ and $N=120$ the curve $X_1(N)$ has a non-cuspidal sporadic point of degree ≤ 52.*

Proof. In both cases the curve at level $N/2$ has a non-cuspidal point of degree 13 (the points `1.54.13.a` and `1.60.13.a` of the census), giving a non-cuspidal point of degree ≤ 52 on $X_1(N)$. Suppose $X_1(N)$ has no non-cuspidal sporadic points. We compute (`x1-sporadic/certificates/ex108fast.m` and `x1-sporadic/certificates/ex120fast.m`) that there are no non-constant modular units over $\mathbb{Q}$ of degree ≤ 52, so we are in case b) of Lemma 7.7. The following table gives the number of rational cusps, the prime used, the ranks of the constant term matrix and of the jets of cusp forms, the bucket width s, the maximal size of a bucket and the number of allocations, which we test.

N	$\deg S$	p	rank of constants	rank of jets	s	size	allocations
108	27	433	149	250	3	5	43758
120	24	241	191	289	3	6	92378

In both cases all the admissible jets are independent, so $\ell(S+E)=1$, which is a contradiction. □

Proposition 7.12. *The curve $X_1(94)$ has a non-cuspidal sporadic point of degree ≤ 60.*

Proof. The point of degree 20 on $X_1(47)$ from the census gives a non-cuspidal point of degree ≤ 60. Suppose $X_1(94)$ has no non-cuspidal sporadic points. The weighted valuation lattice of the modular units has rank 47 in $\mathbb{Z}^{48}$. If v is the vector of a unit of degree at most d whose largest and smallest coordinates are at i and j, then as above

$$\|v - \tfrac{d}{2}(e_i - e_j)\|^2 \leq d^2/2.$$

Up to sign and multiplication of the cusp indices by units modulo 94 there are 50 pairs (i,j) to test. We check the invariance of the lattice, orthogonalize a reduced integral basis over $\mathbb{Q}$ and round the resulting data (`x1-sporadic/certificates/spheredata94.py`). The program `x1-sporadic/certificates/sphere94.cpp` uses lower bounds for the squared lengths of the orthogonalized vectors and rounds each projected coordinate towards zero by at least its total possible rounding error before pruning, so all the vectors in the balls are tested. For $d=60$ we find no non-zero vector of ℓ^1-norm at most 120, so we are in case b) of Lemma 7.7. There are 46 rational cusps and 2 further cuspidal points of degree 23, so $\deg E \leq 14$. Modulo a prime above 283 the ranks of the constant term matrix and of the

jets are 91 and 231. Buckets of width 3 and size at most 4 give 1365 systems, all of which pass the relation space test. Hence $\ell(S+E)=1$, which is a contradiction. □

Proposition 7.13. *The curve $X_1(150)$ has a non-cuspidal sporadic point of degree ≤ 75.*

Proof. The point of degree 25 on $X_1(75)$ found by van Hoeij [50] gives a non-cuspidal point of degree ≤ 75. Suppose $X_1(150)$ has no non-cuspidal sporadic points. We compute that there are no non-constant modular units over $\mathbb{Q}$ of degree ≤ 75, so we are in case b) of Lemma 7.7. There are 40 rational cusps, so $\deg E \leq 35$. Modulo a prime above 601 the ranks of the constant term matrix and of the jets of cusp forms are 223 and 489. Partitioning the 76 cuspidal points into 10 buckets of at most 8 points and taking $s=4$ gives $\binom{17}{9}=24310$ systems, all of which pass the relation space test. Hence $\ell(S+E)=1$, which is a contradiction. □

Remark 7.14. Note that in Propositions 7.8 to 7.13 we prove the existence of a sporadic point of degree at most the given bound, but we do not identify a specific sporadic point.

7.5. **Explicit points.**

Proposition 7.15. *The curves $X_1(81)$ and $X_1(87)$ have non-cuspidal sporadic points of degree 48 and 45, respectively.*

Proof. On the earlier model of $X_1(81)$ from [47], intersect with the line $y=-x$, and on the model of $X_1(87)$ intersect with the curve $y=-1/(x^3+x^2)$. We obtain irreducible factors of degrees 48 and 45, and we verify (and verify) directly over the two number fields that the corresponding Weierstrass equations are non-singular and the marked points have exact order 81 and 87. In both cases the j-invariant generates the field, so these are the degrees of the points. Both $J_1(81)(\mathbb{Q})$ and $J_1(87)(\mathbb{Q})$ are finite [17, Theorem 3.1], so by Lemma 3.1 b) and Corollary 4.3 with $p=2$,

$$\delta(X_1(81)) \geq \left\lceil \frac{5832}{120} \right\rceil = 49, \qquad \delta(X_1(87)) \geq \left\lceil \frac{6720}{120} \right\rceil = 56.$$

Hence both points are sporadic. □

Proposition 7.16. *The curve $X_1(95)$ has a non-cuspidal sporadic point of degree 54.*

Proof. The fibre over $u=1$ on the newer optimized model of $X_1(95)$ from [47] has an irreducible factor of degree 54. We reconstruct the marked elliptic curve in Tate normal form and verify that the marked point has exact order 95. Its j-invariant has degree 27, and the parameter b/c of the Tate normal form has degree 54, so the point has degree 54. By Proposition 4.9 we have $\delta(X_1(95)) \geq 72$ (the limiting form is 95.2.l.a, with $p=3$). □

For the next two levels we use modular units given as products of Siegel functions and of Yang's generalized Dedekind eta functions. We first recall the formulas that we use to compute their divisors and their values at the cusps.

Let $g_i = g_{(0,i/N)}$ be the Siegel function in the normalization of Kubert and Lang [32], and let $u=\prod_i g_i^{e_i}$. Put $S_j=\sum_i i^j e_i$. If $12 \mid S_0$ and $N\gcd(N,2) \mid S_2$, then u is a modular unit on $X_1(N)$ defined over $\mathbb{Q}$ (see [46, Lemma 2.13], whose normalization of the Siegel functions differs by a common fourth root of unity), and its expansion in $q^{1/N}$ at the cusp with scaling matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ has rational coefficients. For $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$ with $c=NC$ and $d=1+ND$ the multiplier of u is $(-1)^{CDS_2+(C+D)S_1-CS_2/N}$. For even N this is 1 since the congruences

give $2 \mid S_1$ and $2N \mid S_2$, and for odd N the exponent is congruent to $D(C+1)S_1$ modulo 2, and D odd forces C odd by the determinant condition.

The geometric cusps of $X_1(N)$ are represented by the bottom rows (c,d) of scaling matrices, with c taken modulo N and d modulo $h = \gcd(c,N)$, $\gcd(d,h) = 1$, up to $(c,d) \sim (-c,-d)$, and for $N \geq 5$ the width of such a cusp is N/h. Choose primitive lifts of the bottom rows and write $ci = k_i N + s_i$ with $0 \leq s_i < N$. In the local parameter $q^{h/N}$ the order of u at this cusp is

$$\sum_i e_i \frac{6s_i^2 - 6Ns_i + N^2}{12Nh},$$

and its leading coefficient, obtained by shifting the first coordinate of $g_{(ci/N,di/N)}$ into $[0,1)$, is

$$\zeta_{2N}^{cdS_2/N + \sum_i e_i((k_i+1)N - di(1+2k_i))} \prod_{s_i=0} (1-\zeta_N^{di})^{e_i}.$$

At a cusp where u has order 0 and value ν, the order of the zero of $u-\nu$ is the least integer $a > 0$ for which the cyclotomic integer

$$\sum_{r \mid ah} r \sum_i e_i \big(\mathbf{1}_{r \equiv s_i \bmod N} \zeta_N^{di\,ah/r} + \mathbf{1}_{r \equiv -s_i \bmod N} \zeta_N^{-di\,ah/r} \big)$$

is non-zero, as follows by expanding the logarithms of the factors $1 - \zeta_N^{\pm di} q^{r/N}$ of the product formula for u/ν.

Proposition 7.17. *The curve $X_1(99)$ has a non-cuspidal sporadic point of degree ≤ 54.*

Proof. Let $u = g_{12}g_{27}/(g_6 g_{21})$. Then $S_0 = 0$ and $S_2 = 396 = 4 \cdot 99$, so u is a modular unit on $X_1(99)$ defined over $\mathbb{Q}$, and we compute with the formulas above that it has degree 114, and that the fibre $u = 1$ contains 10 geometric cusps with multiplicity 3, 2 with multiplicity 6 and 2 with multiplicity 9. Subtracting these cusps leaves a non-cuspidal effective divisor of degree 54 over $\mathbb{Q}$, so $X_1(99)$ has a non-cuspidal point of degree ≤ 54. By Proposition 4.9 and the refinements of Section 4.4, we compute that $\delta(X_1(99)) \geq 60$, so this point is sporadic. □

At a prime level p, we use the model of $X_1(p)$ given by the modular curve classifying elliptic curves with an embedding of μ_p. On this model the $(p-1)/2$ cusps above ∞ are rational and the other cusps form one Galois orbit of degree $(p-1)/2$. Quotienting by the marked subgroup and taking the dual isogeny identifies this curve with $X_1(p)$ over $\mathbb{Q}$.

Lemma 7.18. *Let $p \geq 5$ be a prime, let E_i, $1 \leq i \leq (p-1)/2$, be Yang's generalized Dedekind eta functions* [53, Propositions 1–3]*, and let e_i be integers such that $\sum_i e_i = 0$ and $\sum_i i^2 e_i \equiv 0 \pmod p$. Then $u = \prod_i E_i^{e_i}$ is a modular unit on $X_1(p)$ defined over $\mathbb{Q}$ whose divisor is supported on the rational cusps. For an odd integer a representing a class in $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$, put $r_i = ai \bmod p$ with $1 \leq r_i < p$. At the rational cusp attached to a, the order of u is*

$$v_a = \frac{1}{2p} \sum_i e_i r_i (r_i - p),$$

and its leading coefficient is $s_a = (-1)^{\sum_i e_i \lfloor ai/p \rfloor}$. If $v_a = 0$, then $u - s_a$ has a zero of order exactly $\min_{e_i \neq 0} \min(r_i, p-r_i)$ at this cusp.

Proof. The function u is defined over $\mathbb{Q}$ since its q-expansion is rational. The formula for v_a is the usual order formula for the E_i [53]. For $\gamma = \left(\begin{smallmatrix} a & b \\ p & d \end{smallmatrix}\right)$, the transformation formula for the E_i gives the leading coefficient s_a times the phase $(-1)^{b(a\sum_i i^2 e_i/p - \sum_i i e_i)}$, which is 1 since a and p are odd. The last claim follows from the product expansion, since distinct indices in the range $1 \leq i \leq (p-1)/2$ have distinct values of $\min(r_i, p-r_i)$ at a fixed cusp. □

Proposition 7.19. *The curve $X_1(107)$ has a non-cuspidal sporadic point of degree ≤ 93.*

Proof. Let $u = E_{10}E_{52}/(E_3E_{21})$. Then $\sum_i i^2 e_i = 2354 = 22 \cdot 107$, and using Lemma 7.18 we compute that u has degree 153 and that the zeros of $u+1$ at the rational cusps have total degree 60. The remaining effective divisor has degree 93, which is not divisible by 53, the degree of the orbit of non-rational cusps. Hence it contains a non-cuspidal point of degree ≤ 93. By Proposition 4.9 (with the newform 107.2.a.a and $p = 3$) we have $\delta(X_1(107)) \geq \lceil 954/10 \rceil = 96$, so this point is sporadic. □

8. The remaining composite levels

For the 9 levels in Table 2, the results of Sections 4 and 7 do not suffice. In this section we prove, for each of them, that $X_1(N)$ has a non-cuspidal point of degree smaller than $\delta(X_1(N))$.

Table 2. The degree of a non-cuspidal point and a lower bound for the minimum density degree for the levels treated in Section 8.

N	117	121	123	138	180	210	231	303	420
degree of a point	72	110	48	82	117	96	240	400	384
bound for $\delta(X_1(N))$	73	121	56	88	140	116	266	462	404

8.1. **Reduction at a prime dividing the level.** For several levels we use the reduction of $X_1(N)$ modulo a prime p which divides N exactly. By the results of Deligne and Rapoport [16, V, Theorem 2.12 and Section 2.13, and VI, Theorem 6.9] (see also [26, Propositions 5.2 and 7.1]), the special fibre of a suitable model of $X_1(N)$ over $\mathbb{Z}_p[\zeta_p]$ consists of two Igusa curves I_1, I_2, which are covers of degree $p-1$ of $X_1(N/p)_{\mathbb{F}_p}$, totally ramified over the supersingular points, and which meet at the points above the supersingular points. We will use the following lemma to bound the degrees of maps from $X_1(N)$ to $\mathbb{P}^1$ (or to a symmetric power of an elliptic curve) using the two components.

Lemma 8.1. *Let K be a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}$ and residue field $\mathbb{F}$, and let $\mathcal{X}$ be a normal proper flat model over $\mathcal{O}$ of a curve X over K. Suppose that the special fibre $\mathcal{X}_{\overline{\mathbb{F}}}$ consists of two smooth components I_1 and I_2 of multiplicity 1, which meet in s points, and that $\mathcal{X}$ is smooth over $\mathcal{O}$ away from these s points. Let $\mathcal{P}$ be a smooth projective scheme over $\mathcal{O}$ with an ample line bundle $\mathcal{L}$, let L/K be a finite extension and $f : X_L \to \mathcal{P}_L$ a morphism, and let $d = \deg f^*\mathcal{L}$. Let $f_i : I_i \to \mathcal{P}_{\overline{\mathbb{F}}}$ be the restriction of f to I_i, let $e_i = \deg f_i^*\mathcal{L}$, and let M be the number of the s points x at which $f_1(x) = f_2(x)$. Then*

$$e_1 + e_2 + s - M \leq d.$$

If $\mathcal{P} = \mathbb{P}^1_{\mathcal{O}}$ and f is non-constant, then after composing f with an automorphism of $\mathbb{P}^1_L$ we may assume that f_1 is non-constant. If $L = K$, then the maps f_i are defined over $\mathbb{F}$.

Proof. Since I_1 and I_2 have multiplicity 1, the model $\mathcal{X}$ is smooth over $\mathcal{O}$ at their generic points, so the same holds for $\mathcal{X}_{\mathcal{O}_L}$, whose local rings at these points are discrete valuation rings. As $\mathcal{P}$ is proper, f extends to these points, so the maps f_i are well defined. After base change to $\mathcal{O}_L$, normalization, and blowing up points of the special fibre, we obtain a regular model $\mathcal{X}'$ with a morphism $\mathcal{X}' \to \mathcal{P}_{\mathcal{O}_L}$ extending f. The degree of the pullback of $\mathcal{L}$ to the special fibre of $\mathcal{X}'$, counted with the multiplicities of the components, is d. The strict transforms of I_1 and I_2 have multiplicity 1 and contribute e_1 and e_2. Above each of the s points the fibre of $\mathcal{X}' \to \mathcal{X}_{\mathcal{O}_L}$ is connected and meets both strict transforms, so if $f_1(x) \neq f_2(x)$, then some component above x maps non-constantly to $\mathcal{P}_{\overline{\mathbb{F}}}$ and contributes at least 1 to the degree. The fibres above distinct points are disjoint, which proves the inequality.

Suppose $\mathcal{P} = \mathbb{P}^1_{\mathcal{O}}$, and view f as a rational function. Using the valuation v at the generic point of I_1, which takes the value 1 on a uniformizer of L, we first divide f by a power of the uniformizer to obtain $v(f) = 0$. If the residue of f on I_1 is a constant c, we subtract a lift of c from f and divide again by a power of the uniformizer. Since I_1 is geometrically integral of multiplicity 1, the residue field at its generic point has constant field $\overline{\mathbb{F}}$ (after base change), so this is possible. If this procedure did not terminate, the successive constant approximations would converge in the complete field L to f, which would then be constant. The last claim is clear. □

8.2. **The case $X_1(117)$.**

Lemma 8.2. *Let $C = X_1(117)$, let E be the elliptic curve 117a1, and let $F : C \to X_0(117) \to E$ be the composition of the forgetful map with the optimal parametrization of E. Then $\operatorname{gon}_{\overline{\mathbb{Q}}} C \geq 101$. Suppose that C has infinitely many points of degree $d \leq 72$. Then the translate $a + A$ given by Lemma 4.4 is a translate of F^*E.*

Proof. We have $S_2(117) = 504$, so $\operatorname{gon}_{\overline{\mathbb{Q}}} C \geq \lceil 504/5 \rceil = 101$ by Corollary 4.3. The newforms of level dividing 117 whose abelian varieties can have positive rank are 117.2.e.a, 117.2.r.a, 117.2.t.a, 117.2.z.a and the newform attached to E, which occurs with multiplicity one. For the first four, Proposition 4.9 with $p = 2, 2, 5, 2$ gives the lower bounds 504/5, 84, 1008/13 and 504/5 for d, which we verify. All of them are larger than 72. Since $A(\mathbb{Q})$ is Zariski dense in A, every simple isogeny factor of A has positive rank, so by Proposition 4.9 (note that $d < 101 \leq \operatorname{gon}_{\overline{\mathbb{Q}}} C$) every simple isogeny factor of A is isogenous to E. As E occurs with multiplicity one in $J_1(117)$, it follows that $A = F^*E$. □

Lemma 8.3. *Let E and F be as in Lemma 8.2, and let ω be a non-zero regular differential on $E_{\overline{\mathbb{F}}_2}$. Then the differential $F^*\omega$ on $X_1(117)_{\overline{\mathbb{F}}_2}$ vanishes at 216 distinct supersingular points.*

Proof. The eta quotients $u = (\eta(9z)/\eta(z))^3$ and $v = (\eta(13z)/\eta(z))^2$ are Hauptmoduln on $X_0(9)$ and $X_0(13)$, since by the cusp order formula for eta quotients they have a simple zero at ∞ and a single simple pole at 0, and both start with q at ∞. In characteristic 2 they satisfy

$$j = \frac{u^{12} + u^8 + u^4 + 1}{u^3 + u^2 + u} = \frac{v^{14} + v^{12} + v^2 + 1}{v},$$

which can be verified by comparing q-expansions, as the difference between two rational functions of degree $\leq r$ has a zero divisor of degree at most $2r$ unless it is 0. The normalization of the fibre product of these two maps to the j-line is $X_0(117)_{\mathbb{F}_2}$, since a cyclic subgroup of order 9 and one of order 13 determine a cyclic subgroup of order 117. On $X_0(117)$ the

pullback of ω is, up to a non-zero scalar, the reduction of the differential $f(q)\,dq/q$ of the newform f attached to E, since the Manin constant of E is 1 [15, Theorem 1(a)]. We compute a basis of the regular differentials of this model (checking that it is irreducible of genus 11), identify $f(q)\,dq/q$ by its first 70 coefficients at a rational cusp (the coefficient matrix has rank 11), and find that its divisor is

$$2P_1 + 2P_2 + 6P_3,$$

where P_1, P_2, P_3 are distinct places of degree 2 with $j = 0$. In characteristic 2, $j = 0$ is the only supersingular j-invariant.

The map $X_1(117) \to X_0(117)$ is the quotient by the diamond operators, which form a group of order $\varphi(117)/2 = 36$. An automorphism of a supersingular elliptic curve, other than ± 1, preserving a cyclic subgroup of order 117 would give an automorphism of order 3 or 4 preserving a cyclic subgroup of order 9, and hence a root modulo 9 of $X^2 + X + 1$ or $X^2 + 1$, neither of which exists. Hence $X_1(117) \to X_0(117)$ is unramified above the 6 geometric points of P_1, P_2, P_3, each of which has 36 distinct preimages, so $F^*\omega$ vanishes at 216 distinct supersingular points. □

Proposition 8.4. *We have $\delta(X_1(117)) \geq 73$. In particular the CM points of degree 72 on $X_1(117)$ are sporadic.*

Proof. The least degree of a CM point on $X_1(117)$ is 72 [13], so the second claim follows from the first. Let $C = X_1(117)$, and suppose that C has infinitely many points of degree $d \leq 72$. By Lemma 8.2, $W_d(C)$ contains a translate of F^*E. Since $d < 101 \leq \operatorname{gon}_{\overline{\mathbb{F}}_2} C_{\mathbb{F}_2}$, Lemma 4.5 gives a family of effective divisors D_t of degree d on $C_{\overline{\mathbb{F}}_2}$, parametrized by $t \in E(\overline{\mathbb{F}}_2)$, such that D_t is the unique effective divisor in the class $a_0 + F^*((t) - (0))$.

Since $a_2(E) = -1$, the curve $E_{\mathbb{F}_2}$ is ordinary. Let T be its non-zero point of order 2 and let g be a function on E with $\operatorname{div}(g) = 2(T) - 2(0)$. The differential dg/g is regular, since all the orders of g are even, and it is non-zero, since a square root of g would have divisor $(T) - (0)$. We take $\omega = dg/g$. For every t, the divisor $D_{t+T} - D_t - F^*((T) - (0))$ is principal, so there is a function f_t on C with

$$\operatorname{div}(f_t) = 2D_{t+T} - 2D_t, \qquad \frac{df_t}{f_t} = F^*\omega, \qquad \deg f_t \leq 2d,$$

namely $g \circ F$ times a square. In particular f_t is non-constant.

Let $\tau = \langle 2 \rangle$. By Lemma 4.1, $\Phi^2(x) = \tau(x)$ at the 504 supersingular points of $C_{\overline{\mathbb{F}}_2}$. The coincidence divisor of $f_t \circ \Phi^2$ and $f_t \circ \tau$ has degree $5 \deg f_t \leq 10d \leq 720$. Let x be a supersingular point, $R = \tau(x) = \Phi^2(x)$ and $e = e_R(f_t)$ the ramification index of f_t at R. The pullbacks of a local parameter at $f_t(R)$ along the two maps have orders $4e$ and e at x, so the coincidence multiplicity at x is exactly e (also when $f_t(R) = \infty$). At each of the 216 supersingular zeros of $F^*\omega$ from Lemma 8.3 we have $e_R(f_t) \geq 2$: at a zero or a pole of f_t since all the orders of f_t are even, and at the other points since $df_t(R) = 0$. Since τ permutes the supersingular points, the total contribution of the supersingular points to the coincidence divisor is at least $504 + 216 = 720$. Hence, for every t, we have $d = 72$ and $\deg f_t = 144$, so D_t and D_{t+T} have disjoint supports.

Now choose a supersingular point R which is not one of the 216 zeros of $F^*\omega$. The incidence divisor of the family on $C \times E$ has a component dominating C (otherwise all the divisors D_t would be supported on a fixed finite set, and the family would be constant), so $R \in \operatorname{supp} D_t$ for some t. Since D_t and D_{t+T} are disjoint, f_t has a pole of even order at R,

so $e_R(f_t) \geq 2$. This adds 1 to the lower bound above, so the coincidence divisor of $f_t \circ \Phi^2$ and $f_t \circ \tau$ has degree at least 721, which is a contradiction. □

8.3. **The case $X_1(123)$.**

Proposition 8.5. *The curve $X_1(123)$ has a non-CM sporadic point of degree 48.*

Proof. Write $g_i = g_{(0,i/123)}$ for the Siegel functions and $g_I = \prod_{i\in I} g_i$ for a set I. Let

$$u_1 = \frac{g_{\{4,5,26,29,37,46,53,56\}}}{g_{\{2,13,23,28,35,43,47,59\}}}, \qquad u_2 = \frac{g_{\{8,10,11,17,31,49,52,58\}}\, g^2_{\{6,18,39,54\}}}{g_{\{2,13,23,28,35,43,47,59\}}\, g^2_{\{24,30,33,51\}}}.$$

For both, the exponents sum to 0 and $\sum_i i^2 e_i$ is divisible by 123, so they are modular units on $X_1(123)$ defined over $\mathbb{Q}$. The set $G_8 = \{1, 14, 32, 38, 40, 44, 50, 55\}$ is a subgroup of order 8 of $(\mathbb{Z}/123\mathbb{Z})^\times/\{\pm 1\}$, and both units are invariant under the corresponding diamond operators: for each odd lift a of an element of G_8, replacing i by the representative of $\pm ai$ in $[1, 61]$ preserves the exponent vectors, and the sign $(-1)^{\sum_i e_i \lfloor ai/123 \rfloor}$ in the transformation formula is 1.

We compute, using the formulas of Section 7, that u_1 has degree 256 and that the fibre $u_1 = 1$ contains 80 geometric cusps with multiplicity 1 and 16 with multiplicity 2. Let D be its non-cuspidal part, which has degree 144. Since the units descend to $X_1(123)/G_8$, the divisor D is the pullback of a divisor D' of degree 18 on $X_1(123)/G_8$. For $1 \leq k \leq 18$ we compute, by the residue theorem,

$$\sum_{z\in \operatorname{supp} D'(\overline{\mathbb{Q}})} \operatorname{mult}_z(D')\, u_2(z)^k = -\frac{1}{8} \sum_{x \text{ cusp}} \operatorname{res}_x \left(u_2^k \frac{d(u_1 - 1)}{u_1 - 1} \right),$$

and obtain from Newton's identities the characteristic polynomial of u_2 on D'. It factors over $\mathbb{Q}$ into two distinct irreducible factors of degrees 6 and 12, the first of which is

$$T^6 - 399T^5 + 426T^4 - 911T^3 + 300T^2 - 66T + 1.$$

Hence D' has a subdivisor of degree 6 over $\mathbb{Q}$, whose pullback is an effective divisor of degree 48 on $X_1(123)$. This pullback is a single point. To see this, note that the unit $u_3 = g_{16}/g_{25}$ is defined over $\mathbb{Q}$ since $16^2 - 25^2 = -3 \cdot 123$, and its characteristic polynomial on D, computed in the same way, has two distinct irreducible factors of degrees 48 and 96, each with multiplicity one. Hence D is the sum of a point of degree 48 and a point of degree 96.

The point of degree 48 is sporadic. Indeed, we have $S_2(123) = 560$, so $\operatorname{gon}_{\mathbb{Q}} X_1(123) \geq 112$ by Corollary 4.3, and $\delta(X_1(123)) \geq 56$ by Lemma 3.1 a). It is non-CM since the least degree of a CM point on $X_1(123)$ is 80 [13]. □

Remark 8.6. We also verify the point of degree 48 directly. For a polynomial M of degree 48 and elements b, c of $K = \mathbb{Q}[z]/(M)$, the point $P = (0, 0)$ on $y^2 + (1-c)xy - by = x^3 - bx^2$ satisfies $123P = 0$, $41P \neq 0$ and $3P \neq 0$. The parameter b/c has degree 48, which is the degree of the point since the Tate normal form of a point of order 123 is unique. Its j-invariant has degree 6. As a further check that it is non-CM, the minimal polynomial of j has simple roots 1 modulo 19 and 12 modulo 23, and the corresponding elliptic curves are ordinary with squared Frobenius traces 4 and 9. Their endomorphism algebras are $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-83})$, while a CM field would embed into both.

8.4. **The case $X_1(121)$.** Factor the forgetful map $X_1(121) \to X_0(121)$ as

$$X_1(121) \xrightarrow{\pi_{11}} Y \xrightarrow{\pi_5} X_0(121),$$

where π_{11}, of degree 11, is the quotient by the group generated by the diamond operator $\langle 12\rangle$, and π_5 has degree 5. Let E be the elliptic curve 121b1, which has rank 1, and let $F_0 : X_0(121) \to E$ be its optimal parametrization, sending a cusp to the origin.

Lemma 8.7. *Let A be the elliptic curve $y^2+xy = x^3-x^2-2x-1$, and let P be a generator of $\ker((2+\sqrt{-7})^2)$. Then (A, P) defines a point of degree 110 on $X_1(121)$.*

Proof. We have $j(A) = -3375$, so $\mathrm{End}(A_{\overline{\mathbb{Q}}})$ is the maximal order of $K = \mathbb{Q}(\sqrt{-7})$, and all the endomorphisms are defined over K. The element $2+\sqrt{-7}$ has norm 11, so it generates one of the two primes above 11, and $\ker((2+\sqrt{-7})^2)$ is cyclic of order 121. Its generators give at most $\varphi(121)/2 = 55$ geometric points of $X_1(121)$, and this set is stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Hence the point defined by (A, P) has degree at most 110, and since the least degree of a CM point on $X_1(121)$ is 110 [13], its degree is 110. □

Lemma 8.8. *The image of $(F_0\pi_5\pi_{11})^* : E \to J_1(121)$ is, up to isogeny, the only simple abelian subvariety of $J_1(121)$ of positive rank, and it occurs with multiplicity one. In particular $(J_1(121)/(F_0\pi_5\pi_{11})^*E)(\mathbb{Q})$ is finite.*

Proof. The newform of level 11 occurs twice in $J_1(121)$ and has rank 0. At level 121 the four newforms with trivial character are attached to elliptic curves, and only 121.2.a.b, attached to E, has positive rank. The Galois orbits of newforms with non-trivial character have dimensions $4, 4, 4, 4, 4, 100, 400$, and all of them have non-vanishing central L-value, so their abelian varieties have rank 0 by Kato's theorem [29, Corollary 14.3] (see also [35]). To check the non-vanishing exactly, we compute, for one character of each non-trivial even order 5, 11 and 55, that the plus cuspidal modular symbol spaces have dimensions $5, 10, 10$ over the character fields, and that the cuspidal periods of $T_n\{0,\infty\}$ for $1 \le n \le 6, 10, 10$, respectively, span spaces of the same dimensions. If a normalized eigenform f had $L(f, 1) = 0$, its period functional would vanish on the winding element and all its Hecke translates, which is impossible by the full rank. Galois conjugation covers all the characters. Together with the 6 dimensions coming from trivial character, this accounts for $6+4\cdot5+10\cdot10+40\cdot10 = 526$, the genus of $X_1(121)$. □

Lemma 8.9. *The curve Y is isomorphic over $\mathbb{Q}$ to the modular curve $X(11)$ attached to the symplectic module $\mu_{11} \oplus \mathbb{Z}/11\mathbb{Z}$. The curves $X_1(121)$, Y and $X_0(121)$ have genus 526, 26 and 6, and π_{11} has exactly 50 geometric ramification points, each with ramification index 11.*

Proof. Send a pair (A_0, P_0), with P_0 of order 121, to $A' = A_0/\langle 11P_0\rangle$ with the image of P_0 and the kernel of the dual isogeny. The image of P_0 has order 11 and is complementary to this kernel, since the dual isogeny sends it to $11P_0$, and the Weil pairing identifies the kernel with μ_{11}. The eleven lifts of such a marking differ by the multiples of $11P_0$, so this identifies Y with $X_{\mu_{11}\oplus\mathbb{Z}/11\mathbb{Z}}(11)$, and the remaining diamond operators act by diagonal changes of the marking, which in Klein's coordinates is the cyclic permutation of the five coordinates [23, 24]. By the Riemann-Hurwitz formula, $(2\cdot526-2)-11(2\cdot26-2) = 500$, and since π_{11} is a cyclic cover of prime degree 11, every ramification point has index 11 and contributes 10, so there are 50 of them. □

Lemma 8.10. *Let $\iota = \pi_5^* F_0^* : E \to J_Y$ and $M_t = \iota(t)$ for $t \in E = \mathrm{Pic}^0_E$. Let L be a line bundle on $X_1(121)$ of degree $d \le 120$, defined over $\mathbb{Q}$, such that $L \otimes \pi_{11}^* M_t$ has a non-zero section for every $t \in E(\overline{\mathbb{Q}})$. Then $W_{19}(Y)$ contains a translate of $\iota(E)$ by a class in $\mathrm{Pic}^{19}_Y(\mathbb{Q})$.*

Proof. Let $V = \pi_{11*} L$, a vector bundle of rank 11 on Y. By the projection formula, for each $t \in E(\mathbb{Q})$ there is a non-zero homomorphism $M_t^{-1} \to V$ over $\mathbb{Q}$. Let $S \subseteq V$ be the saturated subbundle spanned at the generic point by the images of these homomorphisms, and let r and s be its rank and degree. We first show that $\det S + \iota(E) \subseteq W_s(Y)$. Choose r of these homomorphisms whose images form a basis at the generic point. Among the r hyperplanes obtained by omitting one of the basis vectors, one does not contain the image of M_t^{-1} for infinitely many $t \in E(\mathbb{Q})$. Wedging the corresponding $r-1$ homomorphisms with each of these gives non-zero sections of $\det S \otimes M_{t+t_0}$ for a fixed $t_0 \in E(\mathbb{Q})$ and infinitely many t. The effective locus is closed and an infinite subset of E is dense, which proves the claim. In particular $s \ge 0$.

Let G be the group of automorphisms of $X_1(121)$ over Y. The map $\pi_{11}^* V \to \bigoplus_{\gamma \in G} \gamma^* L$ is an isomorphism at the generic point, so some r of its components restrict to a homomorphism $\det \pi_{11}^* S \to \bigotimes \gamma^* L$ with non-zero determinant. The zero divisor of this determinant has degree $rd - 11s$. It vanishes to order at least $\binom{r}{2}$ at each of the 50 ramification points. To see this, over $\overline{\mathbb{Q}}$ choose a local parameter w at a ramification point on which G acts by eleventh roots of unity ζ, and a local trivialization of L. A local basis of S gives an evaluation matrix with entries $f_j(\zeta^i w)$, and in the expansion of its determinant the terms with repeated exponents of w cancel, while a sum of r distinct non-negative exponents is at least $0 + 1 + \cdots + (r-1)$. Hence

$$11s \le rd - 50\binom{r}{2} \le \max_{1 \le r \le 11} \left(120r - 50\binom{r}{2}\right) = 210,$$

so $s \le 19$. Adding $19 - s$ times a rational cusp gives the claim. □

Lemma 8.11. *The curve Y and the elliptic curve E have good reduction at 2. Let ι_2 be the reduction of ι. There is no class $a \in \mathrm{Pic}^{19}_{Y_{\mathbb{F}_2}}(\mathbb{F}_2)$ such that $a + \iota_2(E_{\overline{\mathbb{F}}_2}) \subseteq W_{19}(Y_{\mathbb{F}_2})$.*

Proof. We use Fisher's affine model [23]

$$y^2 + y = x^3 - x^2, \qquad t^{11} = xy^2(x-1)(x-y-1)^3$$

of Y and take its smooth projective normalization in characteristic 2. The orders of the radicand at the points $O, (0,0), (0,-1), (1,0), (1,-1)$ of the elliptic curve $y^2 + y = x^3 - x^2$ are $-19, 5, 4, 9, 1$. These five sections are disjoint and totally ramified in the Kummer cover, which is tame, so the normalization has good reduction at 2. Let R be the sum of the five rational points above them. Pulling back a regular differential on the elliptic curve gives $K_{Y_2} \sim 10R$. The five points form one orbit under the order 5 rotation of the coordinates, so R is the pullback of a rational point of $X_0(121)_{\mathbb{F}_2}$.

Let Φ be the 2-power Frobenius acting on points and divisor classes. The elliptic factors of $J_0(121)$ other than E are the curves 121a1, 121c1, 121d1 and two copies of 11a1, with traces $-1, 1, 2$ and -2 at 2, while E has trace 0. Hence

$$H_0(X) = \prod_{b \in \{-2,-1,1,2\}} (X^2 - bX + 2) = X^8 + 3X^6 + 8X^4 + 12X^2 + 16$$

annihilates the reductions of all the other factors and acts as [16] on $E_{\mathbb{F}_2}$, so $H_0(\Phi)J_{X_0(121)_{\mathbb{F}_2}} \subseteq F_0^* E_{\mathbb{F}_2}$.

Identify $\mathbb{F}_{128} = \mathbb{F}_2[z]/(z^7+z+1)$, and encode $\sum a_i z^i$ by the integer $\sum a_i 2^i$. For each of the first three of the triples (x, y, t)

$$(2, 100, 10), \quad (2, 101, 91), \quad (3, 102, 37), \quad (3, 103, 16),$$

let G_i be the sum of the five rotations of the corresponding point. Both G_i and R are pullbacks from $X_0(121)_{\mathbb{F}_2}$, so

$$T_i = H_0(\Phi)(G_i - R) \in \iota_2(E)(\mathbb{F}_{128}).$$

Since $\Phi^7 G_i = G_i$ and $\Phi R = R$, we have $T_i = [U_i - 40R]$, where

$$U_i = 16G_i + \Phi G_i + 12\Phi^2 G_i + 8\Phi^4 G_i + 3\Phi^6 G_i.$$

Suppose $a + \iota_2(E) \subseteq W_{19}(Y_2)$. Since Y_2 has a rational point, a is the class of an effective divisor D of degree 19 over $\mathbb{F}_2$, and $h^0(D + T_i) > 0$ for $i = 1, 2, 3$. By Riemann-Roch,

$$h^0(D + T_i) = 19 - \operatorname{rank}\left(H^0(K_{Y_2} - T_i) \to (K_{Y_2} - T_i)|_D\right),$$

where the target is the space of sections over the finite scheme D, after extending scalars to $\mathbb{F}_{128}$. We compute $H^0(K_{Y_2} - T_i)$ as $L(50R - U_i)$. We compute that each of these spaces has dimension 25 (the 200 conditions imposed by U_i on $L(50R)$, of dimension 225, are independent), and that for every effective divisor D of degree 19 over $\mathbb{F}_2$ the map above has rank 19 for some $i \in \{1, 2, 3\}$. Evaluating the sections of $L(50R)$ along D gives a rank which is at most the rank of the map above, even when D meets U_i, so full rank of this evaluation suffices. The numbers of divisors remaining after testing T_1, then T_2, then T_3 are

$$2\,557\,560 \to 98\,950 \to 3\,875 \to 0.$$

The enumeration allows all the multiplicities of all the places. The numbers of places of Y_2 of degrees $1, \ldots, 19$ are

$$5, 0, 0, 5, 4, 10, 20, 25, 60, 75,$$
$$180, 345, 620, 1160, 2200, 4050, 7740, 14530, 27540,$$

and the coefficient of u^{19} in the zeta function of Y_2, which we compute independently using T_2 and $\langle 2 \rangle$ on modular symbols, is $2\,557\,560$. This proves the claim.

For the computation, a basis of $L(50R)$ is given by 225 monomials in $x, y, x-1, x-y-1, t$, with negative exponents allowed, whose poles are among the five points of R. The script checks the five pole bounds, and distinct orders at the first point of R prove independence. At an affine point we use $x - x(P)$ as a local parameter and solve the equations in truncated power series. At a branch point we write the radicand as $w_0^v b(w_0)$ for a parameter w_0 on the elliptic curve, with $\gcd(v, 11) = 1$ and $b(0) = 1$. Since b has an eleventh root in $\mathbb{F}_2[[w_0]]$, Bézout's identity gives a local parameter w with $w^{11} = w_0$. At a place of degree k each coefficient is expanded in a power basis of $\mathbb{F}_{2^k}$ over $\mathbb{F}_2$ before extending scalars to $\mathbb{F}_{128}$, so all the conjugates are included, also when $7 \mid k$. □

Proposition 8.12. *We have $\delta(X_1(121)) \geq 121$. In particular the CM point of degree 110 from Lemma 8.7 is sporadic.*

Proof. Let $C = X_1(121)$. We have $J_2(121) = 14520$ and $S_2(121) = 605$, so $\operatorname{gon}_{\overline{\mathbb{Q}}} C \geq 121$ by Corollary 4.3. Suppose that C has infinitely many points of degree $d \leq 120$. Then their divisor classes are distinct. By Lemma 8.8, the quotient of J_C by $(F_0\pi_5\pi_{11})^* E$ has finitely

many rational points, so infinitely many of these classes lie on one translate of $(F_0\pi_5\pi_{11})^*E$, and since they are dense in it, $W_d(C)$ contains this translate. It passes through a rational class L, so $L \otimes \pi_{11}^* M_t$ has a section for every $t \in E$. By Lemma 8.10, $W_{19}(Y)$ contains a translate of $\iota(E)$ by a rational class. As in the proof of Lemma 4.5, this translate specializes to a translate $a + \iota_2(E) \subseteq W_{19}(Y_{\mathbb{F}_2})$ with a rational over $\mathbb{F}_2$, and ι_2 still has an elliptic image, since its composition with the pushforward to E is multiplication by $\deg(F_0\pi_5)$. This contradicts Lemma 8.11. □

8.5. **The case $X_1(138)$.**

Lemma 8.13. *The curve $X_1(138)$ has a model over $\mathbb{Z}_2$ whose special fibre over $\overline{\mathbb{F}}_2$ consists of two components, both isomorphic to $D = X_1(69)_{\overline{\mathbb{F}}_2}$, which meet transversally in 176 points. If both components are identified with D, the intersection points are the pairs $(x, \Phi x)$, for x a supersingular point of D. On the supersingular locus of D we have $\Phi^2 = \langle 2 \rangle$.*

Proof. Over $\mathbb{Q}$, a point of order 138 is equivalent to a point of order 69 together with a cyclic subgroup of order 2, and we use the Deligne-Rapoport model for this moduli problem [16, VI, Theorem 6.9]. Its special fibre has two components isomorphic to D. On the component where the kernel of the 2-isogeny is connected we take the source of the isogeny with its point of order 69, and on the other one its target with the image of this point. At a supersingular point the isogeny is the relative Frobenius, so the components meet at the pairs $(x, \Phi x)$. The curve $y^2 + y = x^3$ represents the unique supersingular isomorphism class in characteristic 2. Its 2-power Frobenius has trace 0, so its square is $[-2]$, and hence $\Phi^2 x = \langle 2 \rangle x$ for supersingular x. There are $(3^2 - 1)(23^2 - 1) = 4224$ points of order 69 on this curve, and its automorphism group, of order 24, acts freely on them, so there are 176 intersection points. □

Lemma 8.14. *We have $\operatorname{gon}_{\overline{\mathbb{Q}}} X_1(138) \geq 108$.*

Proof. Let f be a non-constant morphism from $X_1(138)_{\overline{\mathbb{Q}}}$ to $\mathbb{P}^1$ of degree d. By Lemma 8.1 and Lemma 8.13 we may assume that f restricts to a non-constant function f_1 on the first component, and we let f_2 be its restriction to the second component, both viewed as functions on D, of degrees e_1 and e_2 (with $e_2 = 0$ if f_2 is constant). Let $\Psi = \langle 2 \rangle^{-1}\Phi$, which induces the inverse permutation of Φ on the supersingular locus. The intersection point $(x, \Phi x)$ is a point where f_1 and f_2 agree if and only if $f_1(x) = f_2(\Phi x)$, or equivalently $f_2(y) = f_1(\Psi y)$ for $y = \Phi x$.

If $f_1 \neq f_2 \circ \Phi$, then pulling back the diagonal along $(f_1, f_2 \circ \Phi)$ shows that the number M of agreeing intersection points satisfies $M \leq e_1 + 2e_2$, so Lemma 8.1 gives $176 \leq d + e_2$. Similarly, if $f_2 \neq f_1 \circ \Psi$, then $176 \leq d + e_1$. If both inequalities hold, then $176 \leq d + \min(e_1, e_2) \leq 3d/2$, so $d \geq 118$. If $f_1 = f_2 \circ \Phi$ or $f_2 = f_1 \circ \Psi$, then $\{e_1, e_2\} = \{b, 2b\}$ for some $b > 0$, and $d \geq 3b$. By Lemma 4.1 and Lemma 4.2, every non-constant function on D has degree b with $176 \leq 5b$, so $b \geq 36$ and $d \geq 108$. □

Lemma 8.15. *Up to isogeny, the only simple abelian subvariety of $J_1(138)$ of positive rank is the elliptic curve E with Cremona label 138a1, which occurs with multiplicity one. It has rank 1, $a_5(E) = -2$, and multiplicative reduction at 2.*

Proof. The group of even characters modulo 138 is cyclic of order 22. For one character of each order, the following table gives the dimension of the cuspidal plus modular symbol

space, the rank of the cuspidal periods of $T_n\{0,\infty\}$ for $1 \leq n \leq m$, and m.

order of the character	1	2	11	22
dimension	21	20	20	20
rank of the periods	20	20	20	20
m	20	29	20	20

Together with the conjugate characters, the dimensions sum to 441, the genus of $X_1(138)$. If a newform f had $L(f,1) = 0$, its period functional would vanish on all these elements, so all the newforms with non-trivial character, and all but a 1-dimensional part of those with trivial character, have non-vanishing central value, and hence their abelian varieties have rank 0 by Kato's theorem [29, Corollary 14.3]. The missing dimension is accounted for by E, whose root number is -1 and whose conductor is 138. We compute all this and also that E has rank 1. □

Let $E_C \subseteq J_1(138)$ be the elliptic curve obtained by pulling back the dual of the optimal quotient $J_0(138) \to E$ along the forgetful map. It is isogenous to E.

Lemma 8.16. *The model of $X_0(138)$ over $\mathbb{Z}_2$ analogous to the one in Lemma 8.13 has two components, both isomorphic to $X_0(69)_{\overline{\mathbb{F}}_2}$, meeting in 8 points, and the map $X_1(138) \to X_0(138)$ is unramified at the intersection points, each of which has 22 preimages. With a suitable ordering of the 8 intersection points, the Hecke operator T_5 acts on the degree 0 divisors supported on them by the matrix*

$$T_5 = \begin{pmatrix} 2 & 0 & 1 & 0 & 1 & 0 & 0 & 2 \\ 0 & 2 & 0 & 2 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 3 & 0 & 0 \\ 0 & 2 & 1 & 2 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 3 & 0 \\ 0 & 1 & 3 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 3 & 0 & 1 & 1 \\ 2 & 0 & 0 & 0 & 0 & 1 & 1 & 2 \end{pmatrix},$$

whose -2 eigenspace is spanned by $(0,0,1,0,-1,-1,1,0)$.

Proof. There are $(3+1)(23+1) = 96$ cyclic subgroups of order 69 on the supersingular curve $A : y^2 + y = x^3$. Their stabilizers in $\mathrm{Aut}(A)$ are $\{\pm 1\}$, since every other automorphism has order 3, 4 or 6, its characteristic polynomial is irreducible modulo 23, and hence it fixes no line in $A[23]$. Hence there are $96/12 = 8$ intersection points. The forgetful map has degree $\varphi(69)/2 = 22$, and the diamond operators act freely on the preimages of the intersection points, so the map is unramified there and maps the two branches to the corresponding branches.

The Hecke action on these divisors is the Brandt action for the quaternion algebra of discriminant 2 and Eichler level 69 [37]. We identify $\mathrm{End}(A)$ with the Hurwitz order, with quaternion units i, j, k. Then the intersection points correspond to the orbits of its units on $\mathbb{P}^1(\mathbb{F}_3) \times \mathbb{P}^1(\mathbb{F}_{23})$. We represent i by $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and j by $\left(\begin{smallmatrix} a & b \\ b & -a \end{smallmatrix}\right)$, with $(a,b) = (1,1)$ at 3 and $(2,8)$ at 23, and write u for the line through $(u,1)$. The pairs $(0,u)$ for $u = 0,1,2,3,5,6,7,14$ represent the 8 orbits, in this order. The elements $1 \pm 2i$, $1 \pm 2j$, $1 \pm 2k$ have norm 5 and give the 6 kernels of order 5, and counting the orbits of the 6 images of each representative gives the matrix. We compute it, and independently verify the eigenspace in the basis of

ideal classes. The matrix is symmetric with row sums 6, so the eigenvector also gives the unique -2 direction in $\mathbb{R}^8/\mathbb{R}(1,\dots,1)$. □

Proposition 8.17. *We have $\delta(X_1(138)) \geq 88$.*

Proof. Let $C = X_1(138)$. We use the tropical Abel-Jacobi map of C over $\mathbb{C}_2$, whose skeleton is, by Lemma 8.13, the graph with two vertices joined by $s = 176$ edges. Orient every edge from the first vertex to the second. The character group of the torus of the special fibre of J_C is the group of integral cycles $\{(a_i) \in \mathbb{Z}^s : \sum a_i = 0\}$, so the tangent space of the tropical Jacobian is $V_s = \mathbb{R}^s/\mathbb{R}(1,\dots,1)$, and the Abel-Jacobi image of the interior of the i-th edge has direction $[e_i]$, since integration along this edge evaluates a harmonic form on its i-th coordinate. The retraction of the algebraic Abel-Jacobi map to the skeleton is the Abel-Jacobi map of the graph [3, Proposition 6.1 and Corollary 6.6] (see also [2]).

The tropicalization of E in $J_0(138)$ is a circle, since E has multiplicative reduction at 2, and since the inclusion of E into $J_0(138)$ has a left inverse up to multiplication by an integer, the tropicalization of its image is non-zero. By Hecke equivariance, its direction lies in the -2 eigenspace of T_5, since $a_5(E) = -2$, and by Lemma 8.16 it is spanned by $(0,0,1,0,-1,-1,1,0)$. The torus of the special fibre is obtained by gluing scalars at the intersection points modulo a simultaneous rescaling on one component, and a gluing scalar on $X_0(138)$ pulls back to the same scalar at all its 22 preimages. Hence the direction $[v]$ of the tropicalization of E_C has a representative $v \in \mathbb{R}^{176}$ with

$$\#\{i : v_i = 0\} = 88, \qquad \#\{i : v_i = 1\} = \#\{i : v_i = -1\} = 44.$$

The tropicalization of the image of d points of C is contained in a finite union of polytopes, obtained by choosing an edge or a vertex for each point and adding their Abel-Jacobi images, each of which has tangent directions in the span of at most d of the vectors $[e_i]$. By compatibility of the Abel-Jacobi map with the retraction, the tropicalization of $W_d(C)$ is contained in the same union (which is compact, so this persists on taking closures). If $W_d(C)$ contains a translate of E_C, then these polytopes contain a segment in direction $[v]$, so $[v]$ lies in the span of $[e_i]$, $i \in I$, for a set I of at most d indices. Then $v_i = c$ for all $i \notin I$ and some constant c, so

$$d \geq s - \max_c \#\{i : v_i = c\} = 176 - 88 = 88.$$

Now suppose C has infinitely many points of degree $d < 88$. By Lemma 8.14, distinct effective divisors of degree d have distinct classes. By Lemma 8.15, $(J_C/E_C)(\mathbb{Q})$ is finite, so infinitely many of these classes lie on one translate of E_C, which is a curve, so $W_d(C)$ contains this translate, which is a contradiction. □

Proposition 8.18. *The curve $X_1(138)$ has non-CM sporadic points of degrees 82 and 86.*

Proof. Write $g_i = g_{(0,i/138)}$ for the Siegel functions and let

$$u_1 = \frac{g_1 g_3 g_{36}}{g_2 g_9 g_{51}}, \qquad u_2 = \frac{g_1 g_2 g_{56}}{g_4 g_8 g_{41}}, \qquad u_3 = \frac{g_{14} g_{37}}{g_{32} g_{55}}.$$

For each of them $\sum_i e_i = 0$ and $276 \mid \sum_i i^2 e_i$, so they are modular units on $X_1(138)$ defined over $\mathbb{Q}$. For $j = 1, 2$ let D_j be the divisor obtained from the fibre $u_j = 1$ by removing all the cusps with their multiplicities. Using the formulas of Section 7 we compute the following.

j	$\deg u_j$	degree of the cuspidal part	$\deg D_j$
1	185	103	82
2	203	117	86

To show that D_1 and D_2 are single points, let $H_j(T)$ be the monic polynomial whose roots are the values of u_3 at the geometric points of D_j, counted with multiplicity. Since u_3 has poles only at the cusps, the residue theorem gives its k-th power sum as

$$-\sum_{x \text{ cusp}} \operatorname{res}_x \left(u_3^k \frac{d(u_j - 1)}{u_j - 1} \right).$$

At the cusps whose bottom row (c, d) satisfies $\gcd(c, 138) > 1$, the order of u_3 is 0 and only its leading value is needed. At the other cusps we take the bottom row $(c, 276)$, for which the expansions in $q^{1/138}$ have integral coefficients. The first four power sums are $(14, 450, 3053, 37546)$ and $(-1, 605, 1082, 58797)$, respectively, and Newton's identities give $H_1, H_2 \in \mathbb{Z}[T]$. The reductions of H_1 modulo 43 and of H_2 modulo 71 are irreducible, so D_1 and D_2 are single points of degrees 82 and 86, with multiplicity one. They are sporadic by Proposition 8.17, and they are non-CM since the least degree of a CM point on $X_1(138)$ is 88 [13, Table 5]. □

Note that $\operatorname{gon}_{\mathbb{Q}} X_1(138) \leq 132$ [20, Table 1], so $88 \leq \delta(X_1(138)) \leq 132$.

8.6. **The case $X_1(180)$.**

Lemma 8.19. *Let $D = X_1(36)_{\mathbb{F}_5}$, and let $\mathcal{S} \subseteq D(\overline{\mathbb{F}}_5)$ be the set of supersingular points. Then $\#\mathcal{S} = 144$, and $\Phi^2(x) = \langle 5 \rangle(x)$ for $x \in \mathcal{S}$. The curve $X_1(180)$ has a model over $\mathbb{Z}_5[\zeta_5]$ whose special fibre consists of two Igusa curves I_1, I_2 defined over $\mathbb{F}_5$, with cyclic covers $\pi_i : I_i \to D$ of degree 4, defined over $\mathbb{F}_5$, which are totally ramified over $\mathcal{S}$. The two components meet transversally at 144 points, and the point above $x \in \mathcal{S}$ on I_1 is joined to the point above $\Phi(x)$ on I_2.*

Proof. This follows from [16, V, Theorem 2.12 and Section 2.13, and VI, Theorem 6.9] and [26, Propositions 5.2 and 7.1]. Forgetting the generator of the subgroup of order 5 gives a model with $\Gamma_0(5)$-structure and auxiliary $\Gamma_1(36)$-structure. We label one component by the source of the 5-isogeny with its marked point and the other by its target with the image of the marked point. Over the ordinary locus the Igusa structure is an embedding of μ_5 into the source on the connected branch, and dualizing the generator of the étale kernel gives the Igusa structure on the target on the other branch, so both quotients are the marked-point model of D over $\mathbb{F}_5$. At a supersingular point the isogeny is the relative Frobenius, which gives the gluing. The supersingular curve $y^2 = x^3 + 1$ has 6 automorphisms, acting freely on the points of order 36, so $\#\mathcal{S} = (2^4 - 2^2)(3^4 - 3^2)/6 = 144$. It has trace 0 over $\mathbb{F}_5$, so its 25-power Frobenius is $[-5]$, which gives $\Phi^2(x) = \langle 5 \rangle(x)$. □

Lemma 8.20. *Every non-constant function on $D_{\overline{\mathbb{F}}_5}$ has degree ≥ 6, and $\operatorname{gon}_{\mathbb{F}_5} D = 8$.*

Proof. The first claim follows from Lemma 8.19 and Lemma 4.2, since $144 \leq 26b$ implies $b \geq 6$. For the second claim we use the optimized model of $X_1(36)$ from [47]. We check that the generic marked point has exact order 36 and that the pole divisor of its j-invariant has degree 432, the degree of $X_1(36) \to X_0(1)$, which identifies the function field with that of D. The model has genus 17, and D has $15, 5, 49, 144$ places of degree $1, 2, 3, 4$, respectively. A function over $\mathbb{F}_5$ of degree at most 7 maps the 15 rational places to the 6 points of $\mathbb{P}^1(\mathbb{F}_5)$, so one of its fibres contains at least 3 distinct rational places. Adding copies of a rational place to this fibre gives an effective divisor B of degree 7 with $\ell(B) \geq 2$, which contains 3 distinct rational places. For all such divisors (there are 115635, 55965, 133770 and 72345 of them with non-rational part of degree $0, 2, 3, 4$, respectively) we compute that the 7 conditions

imposed by B on the regular differentials are independent, so $\ell(B) = 1$ by Riemann-Roch. The coordinate u of the model has degree 8. This agrees with [20, Table 1 and Remark 1]. □

Lemma 8.21. *Let I be one of the components in Lemma 8.19. A function on $I_{\overline{\mathbb{F}}_5}$ which is not the pullback of a function on D has degree at least* 108*. A non-constant pullback $g \circ \pi$ of a function g on D has degree $4 \deg g$, and if $g \circ \pi$ is defined over $\mathbb{F}_5$, then so is g.*

Proof. A generator of the Galois group $G \simeq (\mathbb{Z}/5\mathbb{Z})^\times$ of π acts on a local parameter at each of the 144 points above $\mathcal{S}$ by the same primitive fourth root of unity. This holds since the canonical Igusa form has fourth power equal to the pullback of the Hasse invariant, has a simple zero at each of these points, and transforms by a fixed faithful character [26, Proposition 5.2], and dividing it by a local trivialization of the Hodge bundle pulled back from D gives such a parameter.

Let f be a function on I which is not a pullback from D, of degree e, let $H \subseteq G$ be its stabilizer, $h = \#H \in \{1, 2\}$ and $r = 4/h$. Let u be the function on I/H induced by f, which has degree e/h. A generator σ of G/H acts on a local parameter at each of the 144 points by the same primitive r-th root of unity η, since the h-th power of a parameter on I is a parameter on I/H. For an indeterminate T consider

$$R_T = \sum_{j=0}^{r-1} \frac{\eta^{-j(r-1)}}{T - (\sigma^j)^* u}$$

on $(I/H)_{\overline{\mathbb{F}}_5(T)}$. The conjugates of u are distinct, so the summands have distinct poles as functions of T and $R_T \neq 0$. Each summand has a pole divisor of degree e/h, and all the summands are regular at the 144 fixed points (also at the poles of u). Since $\sigma^* R_T = \eta^{r-1} R_T$, the expansion of R_T at a fixed point has only exponents congruent to $r - 1$ modulo r, so R_T vanishes to order at least $r - 1$ there. It follows that $re/h \geq 144(r - 1)$, so $e \geq 108$ for $h = 1$ and $e \geq 144$ for $h = 2$. The last two claims are clear, since π and G are defined over $\mathbb{F}_5$. □

Proposition 8.22. *We have $\operatorname{gon}_{\overline{\mathbb{Q}}} X_1(180) \geq 132$ and $140 \leq \delta(X_1(180)) = \operatorname{gon}_{\mathbb{Q}} X_1(180) \leq 192$. The curve $X_1(180)$ has non-CM sporadic points of degrees* 117*,* 120 *and* 135*.*

Proof. Let f be a non-constant morphism from $X_1(180)$ to $\mathbb{P}^1$ of degree d, defined over a finite extension L of $\mathbb{Q}_5(\zeta_5)$, and if f is defined over $\mathbb{Q}$ let $L = \mathbb{Q}_5(\zeta_5)$, whose residue field is $\mathbb{F}_5$. By Lemma 8.1 and Lemma 8.19 we may assume that its restriction f_1 to I_1 is non-constant, and we let f_2 be its restriction to I_2, and e_1, e_2 their degrees. Let M be the number of intersection points at which f_1 and f_2 agree. Then $144 - M \leq d - e_1 - e_2$ by Lemma 8.1. Put $m = 6$ in general and $m = 8$ if f is defined over $\mathbb{Q}$, so that every non-constant function on D arising below has degree $\geq m$ by Lemmas 8.20 and 8.21.

If f_2 is constant, then at most e_1 intersection points agree, so $d \geq 144$. Suppose f_2 is non-constant. If one of f_1, f_2 is not a pullback from D, then by Lemma 8.21 its degree is at least 108, while the degree of the other is at least $\min(108, 4m) = 4m$, so $d \geq 108 + 4m$. It remains to treat the case $f_i = g_i \circ \pi_i$ with $\deg g_i = b_i > 0$. Let $\Psi = \langle 5 \rangle^{-1} \Phi$, which induces the inverse permutation of Φ on $\mathcal{S}$. If $g_1 = g_2 \circ \Phi$ or $g_2 = g_1 \circ \Psi$, then one of the b_i is 5 times the other, so $d \geq 4(b_1 + b_2) \geq 24m$. Otherwise, pulling back the diagonal along $(g_1, g_2 \circ \Phi)$ and $(g_2, g_1 \circ \Psi)$ gives

$$M \leq \min(b_1 + 5b_2, 5b_1 + b_2) \leq 3(b_1 + b_2),$$

and since $e_1 + e_2 = 4(b_1 + b_2)$, we obtain $d \geq 144 + b_1 + b_2 \geq 144 + 2m$. In all cases $d \geq 108 + 4m$, which proves $\operatorname{gon}_{\overline{\mathbb{Q}}} X_1(180) \geq 132$ and $\operatorname{gon}_{\mathbb{Q}} X_1(180) \geq 140$.

By [17, Theorem 3.1], $J_1(180)(\mathbb{Q})$ is finite, so $\delta(X_1(180)) = \operatorname{gon}_{\mathbb{Q}} X_1(180)$ by Lemma 3.1 b), and $\operatorname{gon}_{\mathbb{Q}} X_1(180) \leq 192$ by [20, Table 1]. For the points, we use the following three points (E, P) of the census [43], of level $n \in \{45, 60\}$, and the map $X_1(180) \to X_1(n)$ sending a point Q of order 180 to $[180/n]Q$.

point	$[\mathbb{Q}(P) : \mathbb{Q}]$	$[\mathbb{Q}(Q) : \mathbb{Q}(P)]$	$[\mathbb{Q}(Q) : \mathbb{Q}]$
`1.60.13.a`	13	9	117
`1.45.10.a`	10	12	120
`1.60.15.a`	15	9	135

We verify the order of P and that one of j, b, c generates the field of definition of P. At level 60, $x(P) = 0$ and the numerator of $x([3]Q)$ is irreducible of degree 9 over each of the two fields. Each root gives a unique solution of $[3]Q = P$, since the two points with this x-coordinate have opposite images and $P \neq -P$, and every such Q has order 180. At level 45, the 6 values of x at the points of exact order 4 form one Galois orbit, and the quadratic polynomial giving their y-coordinates is irreducible over the sextic field, so the 12 points T of exact order 4 form one Galois orbit. The points $Q = 34P + T$ are exactly the solutions of $[4]Q = P$ of order 180. A marked point of order 45 or 60 has no non-trivial automorphisms, so the sizes of these orbits are the degrees over $\mathbb{Q}(P)$. All three degrees are smaller than 140, so the points are sporadic, and they are non-CM since the least degree of a CM point on $X_1(180)$ is 144 [13, Table 5]. □

8.7. **The cases $X_1(210)$ and $X_1(420)$.**

Lemma 8.23. *Let $(N, p) \in \{(210, 2), (420, 3)\}$, let $D = X_1(N/p)_{\mathbb{F}_p}$ and let $\mathcal{S} \subseteq D(\overline{\mathbb{F}}_p)$ be the set of supersingular points. Then $\#\mathcal{S} = 384$ if $N = 210$ and $\#\mathcal{S} = 1152$ if $N = 420$, and $\Phi^2(x) = \langle p \rangle(x)$ for $x \in \mathcal{S}$. The curve $X_1(N)$ has a model over $\mathbb{Z}_p[\zeta_p]$ whose special fibre consists of two components I_1, I_2 with maps $\pi_i : I_i \to D$ of degree $p - 1$, totally ramified over $\mathcal{S}$, meeting transversally at $\#\mathcal{S}$ points, such that the point above $x \in \mathcal{S}$ on I_1 is joined to the point above $\Phi(x)$ on I_2. Every non-constant function on $D_{\overline{\mathbb{F}}_p}$ has degree at least 77 if $N = 210$ and at least 116 if $N = 420$.*

Proof. The description of the special fibre follows from [16, V, Theorem 2.12 and Section 2.13, and VI, Theorem 6.9] exactly as in the proof of Lemma 8.19. For $p = 2$ the maps π_i are isomorphisms, since a subgroup of order 2 is equivalent to its non-zero point, and for $p = 3$ they are Igusa double covers. The unique supersingular isomorphism class is represented by $y^2 + y = x^3$, with 24 automorphisms, in characteristic 2, and by $y^2 = x^3 - x$, with 12 automorphisms, in characteristic 3. These automorphism groups act freely on the points of exact order N/p, so there are

$$\frac{(3^2 - 1)(5^2 - 1)(7^2 - 1)}{24} = 384 \quad \text{and} \quad \frac{(4^2 - 2^2)(5^2 - 1)(7^2 - 1)}{12} = 1152$$

supersingular points, respectively. Both curves have trace 0 over $\mathbb{F}_p$, so their p^2-power Frobenius is $[-p]$, which gives $\Phi^2(x) = \langle p \rangle(x)$. The last claim follows from Lemma 4.2, since $384/5 > 76$ and $1152/10 > 115$. □

Lemma 8.24. *Let $s = \sqrt{-6}$, $\mathcal{O} = \mathbb{Z}[s]$, $E = \mathbb{C}/\mathcal{O}$ and $P_N = (s - 48)/N \bmod \mathcal{O}$. Then (E, P_{210}) and (E, P_{420}) define points of degree 96 on $X_1(210)$ and of degree 384 on $X_1(420)$.*

Proof. The coefficient of s shows that P_N has exact order N. The reduced binary quadratic forms of discriminant -24 are $[1,0,6]$ and $[2,0,3]$, so $[\mathbb{Q}(j(E)):\mathbb{Q}]=2$. Over the Hilbert class field $\mathbb{Q}(s,j(E))$, by CM reciprocity, the Galois orbit of the marked point is the orbit of $s-48$ under $(\mathcal{O}/N\mathcal{O})^\times$, modulo the common sign [6, Theorem 1.4]. Modulo 2 or 3 the numerator is s, with $s^2=0$, so its orbit has size 1 or 2. Modulo 4 the products of s with the units $a+bs$ (a odd) are $2b+as$, which gives 4 elements. Both 5 and 7 split in $\mathbb{Q}(s)$, and since $48^2+6=11\cdot 210$, the element $s-48$ is zero in exactly one of the two residue fields at each of these primes, so its orbits there have sizes 4 and 6. By the Chinese remainder theorem, the orbits of $s-48$ have sizes $1\cdot 2\cdot 4\cdot 6=48$ modulo 210 and $4\cdot 2\cdot 4\cdot 6=192$ modulo 420, and passing to the marked isomorphism classes divides these by 2. The lattice $\mathcal{O}$ is stable under complex conjugation, so $j(E)$ is real, and complex conjugation exchanges the two residue fields at 5, so it gives a disjoint orbit over $\mathbb{Q}(s,j(E))$. Hence the degree over $\mathbb{Q}(j(E))$ is 48, respectively 192, and the degree over $\mathbb{Q}$ is 96, respectively 384. We also verify these orbit computations. □

Proposition 8.25. *We have* $\operatorname{gon}_{\overline{\mathbb{Q}}} X_1(210)\geq 231$ *and* $\operatorname{gon}_{\overline{\mathbb{Q}}} X_1(420)\geq 808$*, so* $\delta(X_1(210))\geq 116$ *and* $\delta(X_1(420))\geq 404$*. In particular, the CM points from Lemma 8.24 are sporadic.*

Proof. The bounds for δ follow from the bounds for the gonality by Lemma 3.1 a). Let f be a non-constant morphism from $X_1(N)_{\overline{\mathbb{Q}}}$ to $\mathbb{P}^1$ of degree d. By Lemma 8.1 and Lemma 8.23 we may assume that f restricts to a non-constant function f_1 on I_1, and we let f_2 be its restriction to I_2, e_i their degrees, and M the number of intersection points at which they agree, so that

$$d\geq e_1+e_2+\#\mathcal{S}-M.$$

If f_2 is constant, then $M\leq e_1$, so $d\geq\#\mathcal{S}$. Suppose f_2 is non-constant, and let $\Psi=\langle p\rangle^{-1}\Phi$.

Suppose $N=210$, so that I_1 and I_2 are identified with D. If $f_1=f_2\circ\Phi$ or $f_2=f_1\circ\Psi$, then the degrees are b and $2b$ with $b\geq 77$, so $d\geq 231$. Otherwise, pulling back the diagonal along $(f_1,f_2\circ\Phi)$ and $(f_2,f_1\circ\Psi)$ gives $M\leq\min(e_1+2e_2,2e_1+e_2)=e_1+e_2+\min(e_1,e_2)$, so $384\leq d+\min(e_1,e_2)\leq 3d/2$ and $d\geq 256$.

Suppose $N=420$. Each I_i has an involution ι over D fixing the 1152 points above $\mathcal{S}$. If $f_i\neq f_i\circ\iota$, then these two functions of degree e_i agree at the 1152 fixed points, so $e_i\geq 576$. If $f_i=f_i\circ\iota$ is non-constant, it is the pullback of a function g_i on D, and $e_i=2\deg g_i\geq 232$. Hence if one of the f_i is not invariant, then $d\geq 576+232=808$. Suppose $f_i=g_i\circ\pi_i$ for $i=1,2$, and let $b_i=\deg g_i$. If $g_1=g_2\circ\Phi$ or $g_2=g_1\circ\Psi$, then the b_i are b and $3b$ with $b\geq 116$, so $d\geq 2(b+3b)\geq 928$. Otherwise

$$M\leq\min(b_1+3b_2,3b_1+b_2)\leq 2(b_1+b_2)=e_1+e_2,$$

so $d\geq 1152$. In all cases $d\geq 808$. The degrees 96 and 384 of the CM points are smaller than 116 and 404, which are the least degrees of CM points on $X_1(210)$ and $X_1(420)$ [13, Table 5]. □

8.8. **The cases $X_1(231)$ and $X_1(303)$.**

Lemma 8.26. *Let* $s=\sqrt{-6}$*,* $\mathcal{O}=\mathbb{Z}[s]$*,* $E=\mathbb{C}/\mathcal{O}$ *and* $P_N=(s-216)/N \bmod \mathcal{O}$*. Then* (E,P_{231}) *and* (E,P_{303}) *define points of degree* 240 *on* $X_1(231)$ *and of degree* 400 *on* $X_1(303)$*.*

Proof. We argue as in the proof of Lemma 8.24. The coefficient of s shows that P_N has exact order N. We have $216^2+6=2\cdot 3\cdot 7\cdot 11\cdot 101$. Modulo 3 the numerator is a non-zero nilpotent, whose orbit under the units has size 2, and modulo each of 7, 11 and 101, which

split in $\mathbb{Q}(s)$, it is zero in exactly one of the two residue fields, so its orbit has size $\ell - 1$. Hence its orbit under $(\mathcal{O}/N\mathcal{O})^\times$ has size $\varphi(N)$, and by CM reciprocity [6, Theorem 1.4] the orbit of the marked point over the Hilbert class field has size $\varphi(N)/2$. Complex conjugation exchanges the two residue fields and gives a disjoint orbit, and $[\mathbb{Q}(j(E)) : \mathbb{Q}] = 2$, so the degrees are $2\varphi(N) = 240$ and 400. We also verify these computations. □

Lemma 8.27. *Let (N, d_N, E) be $(231, 265, 77\text{a}1)$ or $(303, 461, 101\text{a}1)$, let $C = X_1(N)$, and suppose that C has infinitely many points of degree $d \le d_N$. Then the translate $a + A$ given by Lemma 4.4 is a translate of an elliptic curve isogenous to E.*

Proof. We have $S_2(231) = 1920$ and $S_2(303) = 3400$, so $d < S_2(N)/5 \le \operatorname{gon}_{\overline{\mathbb{Q}}} C$ by Corollary 4.3. Since $A(\mathbb{Q})$ is Zariski dense in A, every simple isogeny factor of A is isogenous to some A_f with $A_f(\mathbb{Q})$ infinite. If $\dim A_f = r \ge 2$, then Proposition 4.12 and $c_2(f) \le 4/r \le 2$ give $S_2(N) \le 7d$, which is false since $1920 > 7 \cdot 265$ and $3400 > 7 \cdot 461$. Hence A_f is an elliptic curve, attached to a newform with trivial character of level dividing N. By Cremona's tables [14], the isogeny classes of positive rank among these are 77a for $N = 231$, and 101a, 303a and 303b for $N = 303$, with the following traces.

E	a_2	a_3	a_5
77a	0	−3	−1
101a	0	−2	−1
303a	0	1	−3
303b	−2	1	−1

Proposition 4.9 excludes 303a with $p = 5$, since $S_5(303) = 13600 > 27 \cdot 461$, and 303b with $p = 2$, since $3400 > 5 \cdot 461$. □

Lemma 8.28. *Let $M \in \{77, 101\}$, $N = 3M$, $D = X_1(M)_{\mathbb{F}_3}$, and let $\mathcal{S} \subseteq D(\overline{\mathbb{F}}_3)$ be the set of supersingular points and $s = \#\mathcal{S}$. Then $s = 480$ if $M = 77$ and $s = 850$ if $M = 101$, and $\Phi^2(x) = \langle 3 \rangle(x)$ for $x \in \mathcal{S}$. The curve $X_1(N)$ has a model over $\mathbb{Z}_3[\zeta_3]$ whose special fibre consists of two components I_1, I_2, with double covers $\rho_i : I_i \to D$ defined over $\mathbb{F}_3$, with involutions ι_i, totally ramified above $\mathcal{S}$. The two components meet transversally at s points, and the point above $x \in \mathcal{S}$ on I_1 is joined to the point above $\Phi(x)$ on I_2.*

Proof. This is proved exactly as Lemmas 8.19 and 8.23. The supersingular curve $y^2 = x^3 - x$ has 12 automorphisms, acting freely on the points of order M, so $s = (7^2 - 1)(11^2 - 1)/12 = 480$ and $s = (101^2 - 1)/12 = 850$. □

We will need the following two facts about maps to symmetric powers of an elliptic curve. For a curve B and an elliptic curve E, both over a field, and a morphism $g : B \to E^{(k)}$, we write $H_t \subseteq E^{(k)}$ for the divisor of the effective divisors containing a fixed point $t \in E$, and $\deg g$ for $\deg g^* H_t$ (which does not depend on t). The divisor H_t is ample, since its pullback to E^k is the sum of the pullbacks of t along the k projections. We write $a : E^{(k)} \to E$ for the addition map.

Lemma 8.29. *Let B be a curve and E an elliptic curve over an algebraically closed field, and let $g, h : B \to E^{(k)}$ be distinct morphisms.*

a) *If $a \circ g = a \circ h$, then g and h agree at at most $\deg g + \deg h$ points.*
b) *In general, g and h agree at at most $2(\deg g + \deg h)$ points.*

Proof. a) The incidence line bundles of g and h on $B \times E$ have isomorphic restrictions to every $\{x\} \times E$, since $a \circ g = a \circ h$, so by the see-saw principle they differ by a line bundle

pulled back from B. Let s_g and s_h be their defining sections. For $t, u \in E$ the section $s_g(t)s_h(u) - s_h(t)s_g(u)$ is then a section of a line bundle on B of degree $\deg g + \deg h$, which vanishes wherever the two divisors coincide. Choosing a point where the divisors $g(x)$ and $h(x)$ differ, and then t, u such that the corresponding sections are independent, shows that it is non-zero.

b) For $c \in E$ let $p_c : E \to \mathbb{P}^1$ be the quotient by $y \mapsto c - y$, which induces $p_c^{(k)} : E^{(k)} \to (\mathbb{P}^1)^{(k)} = \mathbb{P}^k$, and the pullback of a hyperplane is $H_0 + H_c$. Choose a point x where $g(x) \neq h(x)$, and c different from all the sums of two distinct points in the supports of $g(x)$ and $h(x)$. Then $p_c^{(k)} \circ g$ and $p_c^{(k)} \circ h$ differ. These maps have degree $2 \deg g$ and $2 \deg h$, so a non-zero 2×2 minor of their coordinates gives the claim. □

Proposition 8.30. *We have $\delta(X_1(231)) \geq 266$ and $\delta(X_1(303)) \geq 462$. In particular, the CM points from Lemma 8.26 are sporadic.*

Proof. Let (N, M, d_N, E) be $(231, 77, 265, 77\text{a}1)$ or $(303, 101, 461, 101\text{a}1)$, let $C = X_1(N)$, and suppose that C has infinitely many points of degree $d \leq d_N$. By Lemma 8.27, after pulling back along an isogeny, we may use E as the parameter space of the translate $a + A$. Taking the moving incidence divisor in the other direction gives a morphism $v : C \to E^{(k)}$ over $\mathbb{Q}$, where k is its degree over C, with $\deg v \leq d$, and $F = a \circ v$ is non-constant, since up to sign it induces the dual of the non-zero homomorphism $E \to J_C$.

Let s, D, I_1, I_2, ρ_i and ι_i be as in Lemma 8.28. By Lemma 8.1 (with $\mathcal{P}$ the relative symmetric power of E over $\mathbb{Z}_3$ and $\mathcal{L} = \mathcal{O}(H_t)$), the restrictions $v_i : I_i \to E^{(k)}$ of v are defined over $\mathbb{F}_3$, and if ν denotes the number of intersection points where they agree and $e_i = \deg v_i$, then

$$e_1 + e_2 + s - \nu \leq d. \tag{8.1}$$

We first show that $a \circ v_i$ is non-constant and invariant under ι_i. Let $f : X_0(M) \to E$ be a modular parametrization and let f_M be its reduction composed with $D \to X_0(M)_{\mathbb{F}_3}$, which is non-constant. The two degeneracy maps $X_1(N) \to X_0(M)$ span the E-isotypic part of J_C up to isogeny, since E occurs with multiplicity 2 and $\mathrm{End}_{\mathbb{Q}}(E) = \mathbb{Z}$. On the first component the target of the 3-isogeny is the Frobenius twist of the source, and on the second the dual isogeny gives the reverse description, while multiplication by 3 preserves the tame cyclic subgroup. Hence, after multiplying F by an integer, and up to constants, the restrictions of F to the two components are

$$(u + w\pi) f_M \rho_1 \qquad \text{and} \qquad (u\pi + w) f_M \rho_2,$$

where π is the Frobenius endomorphism of $E_{\mathbb{F}_3}$ and u, w are integers, not both 0. Since $\deg \pi = 3$, the endomorphism π is not in $\mathbb{Q}$, so both maps are non-constant. The difference $a \circ v_i \circ \iota_i - a \circ v_i$ takes values in a finite group scheme, so it is constant, and it vanishes at a ramification point of ρ_i.

If $v_i \neq v_i \circ \iota_i$, then by Lemma 8.29 a), applied at the s fixed points of ι_i, we have $2e_i \geq s$. If $v_i = v_i \circ \iota_i$, then $v_i = g_i \circ \rho_i$ for a morphism $g_i : D \to E^{(k)}$ over $\mathbb{F}_3$, and we write $b_i = \deg g_i$, so $e_i = 2b_i$. By the same computation on $X_0(M)$, the sum map $a \circ g_i$ is non-constant and invariant under $\langle 3 \rangle$ up to translation. Apply Lemma 4.14 to the incidence divisor of g_i on $D \times E$, with the components of the form $D \times \{y\}$ removed, with $\tau = \langle 3 \rangle$ and $S = s$. Since $a_3(77\text{a}1)^2 - 6 = 3$ and $a_3(101\text{a}1)^2 - 6 = -2$, it gives $480 < 10b_i$ if $N = 231$ and $850 \leq 10b_i + 2b_i$ if $N = 303$ (using $m \leq bk$). Hence an invariant component has $b_i \geq 49$, respectively $b_i \geq 71$.

It follows that both v_i are invariant. Indeed, otherwise (8.1) would give $d \geq s/2+2\cdot 49 = 338$, respectively $d \geq s/2 + 2 \cdot 71 = 567$. Put $B_* = b_1 + b_2$. Then $2B_* \leq d$ by (8.1). Let $\Psi = \langle 3 \rangle^{-1}\Phi$, which induces the inverse permutation of Φ on $\mathcal{S}$, and consider the pairs

$$(g, h) = (g_1, g_2 \circ \Phi) \qquad \text{and} \qquad (g, h) = (g_2, g_1 \circ \Psi).$$

An intersection point above $x \in \mathcal{S}$ on I_1 and above $\Phi(x)$ on I_2 is a point where v_1 and v_2 agree if and only if $g_1(x) = g_2(\Phi x)$, or equivalently $g_2(y) = g_1(\Psi y)$ for $y = \Phi(x)$. If $g = h$ for one of the pairs, then the b_i are b and $3b$, so $d \geq 2(b + 3b) = 8b$, which is impossible as $b \geq 49$, respectively $b \geq 71$. Hence $g \neq h$ for both pairs.

Fix one of the two pairs, and let T be the reduced divisor of the ν points of $\mathcal{S}$ at which g and h agree, which is defined over $\mathbb{F}_3$. Let $G = a \circ g + a \circ h : D \to E$. After the same integer multiplication as above, and up to constants, the two possible maps G are

$$\big(-2u + (a_3u + 2w)\pi\big) f_M \qquad \text{and} \qquad \big(-2w + (2u + a_3w)\pi\big) f_M,$$

where $a_3 = a_3(E)$, since $\pi^2 - a_3\pi + 3 = 0$, $f_M \circ \Phi = \pi f_M$ and $f_M \circ \langle 3 \rangle = f_M$. Since 1 and π are linearly independent over $\mathbb{Q}$, these maps are non-constant unless $u = w = 0$, and they are invariant under $\langle 3 \rangle$ up to translation. For $c \in E(\overline{\mathbb{F}}_3)$ let $p_c : E \to \mathbb{P}^1$ be given by the linear system $|(0) + (c)|$. Then the induced map on symmetric powers pulls back a hyperplane to $H_0 + H_c$. For general c the maps $p_c^{(k)} \circ g$ and $p_c^{(k)} \circ h$ to $\mathbb{P}^k$ differ (as in the proof of Lemma 8.29 b)), and a non-zero 2×2 minor of their coordinates vanishes on T. Hence the line bundle

$$L_c = g^*\mathcal{O}(H_0 + H_c) \otimes h^*\mathcal{O}(H_0 + H_c) \otimes \mathcal{O}_D(-T)$$

is effective, of degree $R = 2(\deg g + \deg h) - \nu$. Since $\mathcal{O}(H_c - H_0) = a^*\mathcal{O}_E((c) - (0))$ (which can be checked on the restriction to $x \mapsto (x) + (k-1)(t)$ for a fixed general t), as c varies these classes fill the translate $[L_0] + G^* \operatorname{Pic}^0_E$, which is therefore contained in $W_R(D)$, as $W_R(D)$ is closed.

We claim that $R \geq 49$ if $N = 231$ and $R \geq 71$ if $N = 303$. If the generic line bundle in this translate has two or more sections, subtract a fixed rational cusp of D, and repeat until the generic class has exactly one section, which gives a translate of $G^* \operatorname{Pic}^0_E$ in $W_{R'}(D)$ with $R' \leq R$. Its unique divisors give a rational map from E to $D^{(R')}$, which extends to E since E is a smooth curve. Its incidence divisor on $D \times E$ has degree R' over E, and its mixed class induces G^*, so its sum map is $\pm G$ up to translation, of degree $m' > 0$. Remove the components of the form $\{x\} \times E$, and let $k' > 0$ be the degree over D. Then Lemma 4.14 gives $480 \leq 10R - 3m'/k' < 10R$ if $N = 231$, and $850 \leq 10R + 2m'/k' \leq 12R$ if $N = 303$, which proves the claim.

Let $r = 49$ if $N = 231$ and $r = 71$ if $N = 303$. Since $\deg(g_2 \circ \Phi) = 3b_2$ and $\deg(g_1 \circ \Psi) = 3b_1$, the two pairs give

$$\nu + r \leq 2\min(b_1 + 3b_2, 3b_1 + b_2) \leq 4B_*,$$

and combining this with (8.1), in the form $s - \nu \leq d - 2B_*$, we obtain

$$s + r \leq d + 2B_* \leq d + 2\lfloor d/2 \rfloor.$$

The left-hand side is 529, respectively 921, so $d \leq 264$, respectively $d \leq 460$, is impossible. For $d = 265$, respectively $d = 461$, all these inequalities are equalities, so $B_* = (d-1)/2$ and $s - \nu = 1$. The one intersection point at which v_1 and v_2 do not agree then lies above an $\mathbb{F}_3$-rational supersingular point of $X_1(M)$, since T is defined over $\mathbb{F}_3$. For $M = 77, 101$ such a point would give an elliptic curve over $\mathbb{F}_3$ with an $\mathbb{F}_3$-rational point of order M, which is

impossible by the Hasse bound. This proves the bounds for δ. The degrees 240 and 400 of the CM points in Lemma 8.26 are smaller than 266 and 462, and they are the least degrees of CM points on $X_1(231)$ and $X_1(303)$ [13, Table 5]. □

9. The prime levels 83 and 131

For $p \in \{83, 131\}$ let $E_p = X_0^+(p)$, which is the elliptic curve 83a1 with model $y^2+xy+y = x^3 + x^2 + x$, respectively the elliptic curve 131a1. Both have rank 1. Let $F_p : X_1(p) \to X_0(p) \to E_p$ be the composition of the forgetful map and the quotient map, which has degree $p-1$, and take the common image of the two cusps of $X_0(p)$ as the origin O of E_p.

Lemma 9.1. *Let $p \in \{83, 131\}$.*

a) *The map $X_1(p) \to X_0(p)$ is unramified, and $F_p^*(O)$ is the sum of the $p-1$ geometric cusps of $X_1(p)$, each with multiplicity 1.*
b) *Up to isogeny, $F_p^*E_p$ is the only simple abelian subvariety of $J_1(p)$ of positive rank, and it occurs with multiplicity one. In particular $(J_1(p)/F_p^*E_p)(\mathbb{Q})$ is finite.*
c) *We have $\operatorname{gon}_{\overline{\mathbb{Q}}} X_1(83) \geq 58$ and $\operatorname{gon}_{\overline{\mathbb{Q}}} X_1(131) \geq 143$.*

Proof. a) Since $p \equiv -1 \pmod{12}$, the curve $X_0(p)$ has no elliptic points, and the cusps of $X_1(p)$ have the same widths as the cusps of $X_0(p)$ below them, so the forgetful map is unramified. The Fricke involution exchanges the two cusps of $X_0(p)$, so they are not ramification points of $X_0(p) \to E_p$.

b) The newform factors of $J_1(83)$ have dimensions 1, 6 and 240 and occur with multiplicity one. The last two, 83.2.a.b and 83.2.c.a, have non-vanishing central L-values [34], so their abelian varieties have rank 0 by Kato's theorem [29, Corollary 14.3]. At level 131, we compute that on the plus modular symbol spaces for characters of orders 1, 5, 13 and 65 (one for each order) the winding elements generate submodules of ranks $10, 10, 10, 10$, in spaces of dimensions $11, 10, 10, 10$ over the respective character fields. The missing dimension is accounted for by E_{131}, and the rest has rank 0 by Kato's theorem.

c) We have $S_2(83) = 287$ and $S_3(131) = 1430$, so this follows from Corollary 4.3. □

9.1. Isolated points on $X_1(83)$ and $X_1(131)$.

Proposition 9.2. *The curve $X_1(83)$ has isolated points x_1 and x_2 of degree 57 with non-isomorphic residue fields. Their orbits under the diamond operators consist of 82 distinct isolated points.*

Proof. Let $C = X_1(83)$, $F = F_{83}$ and $E = E_{83}$. We use the functions E_i of Lemma 7.18, and index the rational cusps c_i by $i \in (\mathbb{Z}/83\mathbb{Z})^\times/\{\pm 1\}$ as there. Consider the modular units

$$v = \frac{E_{35}E_{40}}{E_3E_{34}}, \qquad u = \frac{E_2E_9}{E_{18}E_{33}},$$

and let x_1 and x_2 be the non-cuspidal parts of the fibres $v = 1$ and $u = -1$. By Lemma 7.18, v has degree 95 and the cuspidal part of the fibre $v = 1$ is $8c_{10} + 27c_{18} + 3c_{26}$, while u has degree 97 and the cuspidal part of the fibre $u = -1$ is $H = 19c_{12} + 21c_{31}$. Hence x_1 and x_2 are effective divisors of degree 57 over $\mathbb{Q}$, and $x_2 \sim T - H$, where T is the pole divisor of u.

We now show that x_1 and x_2 are points. Let x be the Weierstrass coordinate on E. For each of the two divisors we compute the primitive integral polynomial whose roots are the 57 values of $x \circ F$ on the divisor, counted with multiplicity. We do this by taking the norm of the function defining the fibre along the tower $C \to X_0(83) \to E \to \mathbb{P}^1_x$. On $X_0(83)$ the first norm L_1 has divisor $\pi_* x_j - 57c_0$, where $\pi : C \to X_0(83)$ and c_0 is the cusp below the rational

cusps, and its expansion at c_0 is, up to a constant, the product of the 41 expansions at the cusps above it. Let w be the Fricke involution. The function $z = f_E/(\eta(\tau)^2\eta(83\tau)^2)$, where f_E is the newform attached to E, is anti-invariant under w and has a pole of order 6 at each cusp, and z^2 is a polynomial in x, y determined by its principal part and constant term at O. The second norm is $(T_1^2 - z^2W_1^2)/4$, where $T_1 = L_1 + wL_1$ and $W_1 = (L_1 - wL_1)/z$, and we recover W_1 and T_1 in the Riemann-Roch spaces $L(51O)$ and $L(57O)$ on E by successively cancelling the leading terms in the bases of monomials in x, y. Finally, for a function $A(x) + B(x)y$ on E the last norm is $A(A - (x+1)B) - (x^3 + x^2 + x)B^2$. We compute the cusp expansions with `level-83/series.py`, the norms with `level-83/exact.py`, and the two polynomials are stored in `level-83/records/minima-all.json`. Their leading coefficients, the coefficients of X^{56}, a prime modulo which they are irreducible, and the degrees of their irreducible factors modulo 2 are

	$[X^{57}]$	$[X^{56}]$	irreducible mod	factors mod 2
x_1	3319^2	-1101379019	11	$9, 48$
x_2	167^2	-95955529	29	$9, 15, 33$

and modulo 2 all the factors have multiplicity one. Each polynomial is irreducible of degree 57, so each divisor is a single point, and $x \circ F$ generates its residue field. At 2 both leading coefficients are units and both reductions are squarefree, so the factorizations modulo 2 give the splitting of 2 in the two residue fields, which is different, so the residue fields are not isomorphic.

We now prove that x_2 is isolated. Let $S = F^*(O)$, which is the sum of the 82 geometric cusps by Lemma 9.1 a), and let $B = (T - H + S)_+$, which has degree 177. Modulo a prime above 167, the canonical cusp jets imposed by B have rank 176. Here we use differentials obtained from the weight 2 forms of Section 7.4, whose constant term matrix has rank 81, which is the upper bound given by the residue theorem, and hence the cusp forms modulo the prime are the reductions of cusp forms in characteristic 0. Hence $\ell(B) \leq 2$ in characteristic 0. The functions 1 and u lie in $L(B)$, so they span it. The coefficient of $T - H + S$ at c_{12} is -18, so $1 \notin L(T - H + S)$, while $u + 1 \in L(T - H + S)$. Hence $\ell(x_2 + S) = \ell(T - H + S) = 1$, and x_2 is isolated by Lemma 9.1 b) and Lemma 3.5. For x_1 the corresponding divisor B has degree 174, its canonical jets have rank 173, and the same argument with the function $v - 1$ gives $\ell(x_1 + S) = 1$.

The diamond operators act on C over $\mathbb{Q}$, so they map isolated points to isolated points with the same residue field. Their group has order 41 and acts freely on the geometric points of C, by Lemma 9.1 a). A non-trivial diamond operator fixing a point of degree 57 would partition its 57 geometric points into sets of size 41, which is impossible. Hence the orbits of x_1 and x_2 have 41 elements each, and they are disjoint since the residue fields are different. □

Proposition 9.3. *The curve $X_1(131)$ has an isolated point of degree 143, which is not sporadic.*

Proof. Let $C = X_1(131)$, $F = F_{131}$ and $S = F^*(O)$, which is the sum of the 130 geometric cusps by Lemma 9.1 a). Let

$$u = \frac{E_{19}E_{54}}{E_{27}E_{37}},$$

let T be its pole divisor and x the non-cuspidal part of the fibre $u = 1$. By Lemma 7.18, $\deg T = 231$ and the cuspidal part of this fibre is $H = 19c_1 + 39c_{16} + 29c_{31} + c_{46}$, so x is an effective divisor of degree 143 over $\mathbb{Q}$ with $x \sim T - H$. To show that x is a point,

we compute the characteristic polynomial of the unit $E_{10}E_{65}/(E_{11}E_{55})$ on x. The sets of possible degrees of its proper factors given by the factorizations modulo the primes 2153, 2161, 2179, 2203 and 2213 have empty intersection, so the polynomial is irreducible and x is a single point.

Let $B = (T - H + S)_+$, which has degree 357. We compute, modulo 263, that the evaluation of regular differentials at the jets prescribed by B has rank at least 356. For this we use the forms of weight 2 of Section 7.4, namely products of two Eisenstein series of weight 1 and orbit sums of the normalized Weierstrass function. Their constant term matrix has rank at most 129 by the residue theorem, and its reduction has rank 129, so its kernel modulo 263 lifts to characteristic 0. The regular differentials obtained in this way span a space of dimension at least 650 (the genus is 651), and they give the minor of rank 356. By Riemann-Roch, $\ell(B) \le 1+357-356 = 2$. Both 1 and u lie in $L(B)$, so they span it. The coefficient of $T-H+S$ at c_1 is -18, so $1 \notin L(T-H+S)$, while $u-1 \in L(T-H+S)$. Hence $\ell(x+S) = \ell(T-H+S) = 1$, so x is isolated by Lemma 9.1 b) and Lemma 3.5. Since F has degree 130 and $E_{131}(\mathbb{Q})$ is infinite, we have $\delta(C) \le 130 < 143$, so x is not sporadic. □

9.2. **Lower bounds for $\delta(X_1(83))$ and $\delta(X_1(131))$.**

Proposition 9.4. *We have $111 \le \delta(X_1(131)) \le 130$.*

Proof. The upper bound follows from Lemma 3.1 c), since F_{131} has degree 130 and $E_{131}(\mathbb{Q})$ is infinite. Suppose $X_1(131)$ has infinitely many points of degree $d \le 110$. By Lemma 9.1 c), $d < \operatorname{gon}_{\overline{\mathbb{Q}}} X_1(131)$, and by Lemma 4.4 and Lemma 9.1 b), $W_d(X_1(131))$ contains a translate of $F_{131}^* E_{131}$. The isogeny class of E_{131} contains only one curve [34], so a factorization of F_{131} through an isogeny would be through multiplication by an integer n with $n^2 \mid 130$, and hence F_{131} is optimal, of degree $m = 130$. By (4.1), $130 \le d'k \le 110k$, so $k \ge 2$. Since $a_3(E_{131}) = -1$, Proposition 4.15 with $p = 3$ gives

$$1430 \le 10d + \frac{130\,(6 - a_3(E_{131})^2)}{k} \le 1100 + 325 = 1425,$$

which is a contradiction. □

The bound at 83 uses an étale double cover in characteristic 2. In the rest of this section let $C = X_1(83)$, $E = E_{83}$ and $F = F_{83}$, and denote by the same letters their reductions over $\overline{\mathbb{F}}_2$. The curve $E : y^2 + xy + y = x^3 + x^2 + x$ is ordinary at 2, with $\#E(\mathbb{F}_2) = 4$ and $\#E(\mathbb{F}_4) = 8$. Let Φ be the base change of the 2-power Frobenius of each of the curves, and $V : E \to E$ the Verschiebung, which is separable of degree 2, with kernel generated by a point $\kappa \in E(\mathbb{F}_2)$ of order 2.

Lemma 9.5. *The curve $\widetilde{C} = C \times_{F,E,V} E$ is connected, and $\rho : \widetilde{C} \to C$ is an étale double cover. Let ι be its non-trivial automorphism over C. The trace sequence*

$$0 \longrightarrow \mathcal{O}_C \longrightarrow \rho_* \mathcal{O}_{\widetilde{C}} \xrightarrow{\mathrm{Tr}} \mathcal{O}_C \longrightarrow 0$$

has a non-zero extension class $\eta \in H^1(C, \mathcal{O}_C)$, and η spans the tangent direction of $F^*E \subseteq J_C$.

Proof. The map $X_0(83) \to E$ has degree 2 and is separable, since the Fricke involution exchanges the two cusps, and it is ramified by the Riemann-Hurwitz formula, as $X_0(83)$ has genus 7. Hence it does not factor through V, so the quadratic extension of the function

field of $X_0(83)$ given by V is non-trivial, and it stays non-trivial in the function field of C, which has odd degree 41 over it. So $\widetilde{C}$ is connected, and ρ is étale since V is. The extension class η is non-zero, since every global function on $\widetilde{C}$ is constant and has trace 0 (we are in characteristic 2), so the connecting map $H^0(C, \mathcal{O}_C) \to H^1(C, \mathcal{O}_C)$ is injective. By base change $\eta = F^*\eta_E$, where η_E is the class of the trace sequence of V, which is non-zero and hence spans $H^1(E, \mathcal{O}_E)$. Hence η is the image of the tangent space of E under F^*. □

Lemma 9.6. *Let $\tau = \langle 2 \rangle$, and lift it to $\widetilde{\tau}(P, Q) = (\tau P, Q)$ on $\widetilde{C}$. There are exactly* 205 *supersingular points P of C such that both points of $\widetilde{C}$ above P satisfy $\Phi^2 = \widetilde{\tau}$.*

Proof. The lift $\widetilde{\tau}$ is well defined since $F \circ \tau = F$. Let P be supersingular, so $\Phi^2(P) = \tau(P)$ by Lemma 4.1, and let $(P, Q) \in \widetilde{C}$. Then $\Phi^2(P, Q) = (\tau P, \Phi^2 Q)$ and $\widetilde{\tau}(P, Q) = (\tau P, Q)$, so they agree if and only if $Q \in E(\mathbb{F}_4)$. Since κ is rational, this holds for both points above P or for neither, and it holds if and only if $F(P) \in V(E(\mathbb{F}_4))$. The group $E(\mathbb{F}_4)$ is cyclic of order 8, as $E[2](\overline{\mathbb{F}}_2)$ has order 2, so its subgroup $V(E(\mathbb{F}_4))$ of order 4 is $E(\mathbb{F}_2)$.

On $E_{\mathbb{F}_2}$ we have the identity

$$\mathrm{Norm}_{X_0(83)/E}(j) = \big(x(x+1)y\big)^{12}.$$

Both sides have poles only at O, of order 84, and comparing the coefficients of $q^{-84}, \dots, q^0$ of $j(q)j(q^{83})$ with the expansions of the right-hand side proves the identity, which we check. The only supersingular j-invariant is $j = 0$, and the automorphism group of the corresponding curve modulo ± 1, of order 12, acts freely on its 84 cyclic subgroups of order 83, since $83 \equiv -1 \pmod{12}$ and no automorphism of order 3 or 4 preserves such a subgroup. Hence there are 7 supersingular points on $X_0(83)$, each of multiplicity 12 in the divisor of zeros of j, and the divisor of zeros of $x(x+1)y$ records their images on E. With $\alpha^2 + \alpha + 1 = 0$, these images and the number of supersingular points above them are

	$(0,0)$	$(0,1)$	$(1,1)$	$(\alpha,0)$	$(\alpha^2,0)$
number	2	1	2	1	1

so 5 of the 7 supersingular points map to $E(\mathbb{F}_2)$, and each of them has 41 preimages on C. □

Proposition 9.7. *We have $52 \le \delta(X_1(83)) \le 82$.*

Proof. The upper bound follows from Lemma 3.1 c). Suppose $X_1(83)$ has infinitely many points of degree $d \le 51$. By Lemma 9.1, $d < 58 \le \mathrm{gon}_{\overline{\mathbb{Q}}} X_1(83)$, and $W_d(X_1(83))$ contains a translate of F^*E by Lemma 4.4. As in the proof of Lemma 4.5, this translate specializes to a translate of F^*E in $W_d(C)$ over $\overline{\mathbb{F}}_2$. Let $b \le d$ be minimal such that $W_b(C)$ contains a translate of F^*E, and write the line bundles of such a translate as $L_t = L \otimes F^*t$, $t \in \mathrm{Pic}^0_E$. Since $b < 58$, every L_t has a unique section up to scalars, with divisor D_t, and by cohomology and base change these sections form a line bundle on the parameter curve. Hence the section s_t deforms in the direction η of Lemma 9.5, so $s_t \cup \eta = 0$ in $H^1(C, L_t)$, since this cup product is the obstruction to lifting a section along the first order deformation of the line bundle. This cup product is also the connecting map of the trace sequence tensored with L_t, so s_t lifts by the trace to a section of ρ^*L_t, and dividing it by ρ^*s_t gives a rational function h_t on $\widetilde{C}$ with

$$\iota^* h_t = h_t + 1, \qquad (h_t)_\infty \le \rho^* D_t.$$

Both Φ and $\widetilde{\tau}$ commute with ι, since κ is rational. Hence the function $h_t \circ \Phi^2 - h_t \circ \widetilde{\tau}$ is invariant under ι, so it is $\rho^* u_t$ for a rational function u_t on C. The two terms have degrees

$4 \deg h_t$ and $\deg h_t$, and h_t is non-constant, so u_t is non-constant. Its poles are bounded by $(\Phi^2)^* D_t + \tau^* D_t$, which has degree $5b$.

By the minimality of b, the divisors D_t have no point in common (otherwise removing it would give a translate in $W_{b-1}(C)$), so for general t the divisor D_t avoids the finite supersingular locus. Let Z be the reduced divisor of the 205 supersingular points of Lemma 9.6. At every $P \in Z$ both evaluations defining $u_t(P)$ are regular, and they are equal, so u_t vanishes on Z. It follows that

$$(\Phi^2)^* L_t \otimes \tau^* L_t \otimes \mathcal{O}_C(-Z) \in W_{5b-205}(C).$$

As t varies, these classes form a translate of F^*E. Indeed, on the parameter the two pullbacks act as V^2 and 1, and $V^2 + 1 \neq 0$ since $\deg V^2 = 4$, and the image of $W_{5b-205}(C)$ is closed. By the minimality of b, $b \leq 5b - 205$, so $b \geq 52$, which contradicts $b \leq d \leq 51$. □

Proof of Theorem 1.1. For $N \notin A \cup \{83, 131\}$ the curve $X_1(N)$ has a non-cuspidal sporadic point by Theorem 1.3, which is isolated by Theorem 2.2. The levels in A are covered by Propositions 6.1 and 6.2 (note that $A = \{1, \ldots, 16, 18, 20\} \cup \{17, 19, 22, \ldots, 27, 32\}$), and the levels 83 and 131 by Propositions 9.2 and 9.3. □

Remark 9.8. Unfortunately, our methods do not determine whether $X_1(83)$ and $X_1(131)$ have sporadic points. We summarize what we know in the following table, which lists the least degree of a CM point, the bounds for the minimum density degree, and the degree of the isolated points that we found.

N	least CM degree	bounds for $\delta(X_1(N))$	isolated point
83	82	$52 \leq \delta \leq 82$	57
131	130	$111 \leq \delta \leq 130$	143

In particular $\delta(X_1(83)) \geq 58$ would imply that the points of Proposition 9.2 are sporadic. A sporadic point on either curve would have to be non-CM. We expect that $\delta(X_1(83)) \geq 58$, so that the points of degree 57 of Proposition 9.2 are sporadic, and that $X_1(131)$ has no non-cuspidal sporadic points, but we were unable to prove either of these statements.

10. Proof of Theorem 1.3

For $N \in A$ this is Proposition 7.1. For $N > 720$ the curve $X_1(N)$ has a sporadic CM point by [13, Theorem 8.2]. For $N \leq 720$, the table of levels, computed with levels.py from the results of Sections 4, 7 and 8, gives an upper bound $w(N)$ for the least degree of a non-cuspidal point which is strictly smaller than the lower bound for $\delta(X_1(N))$ for 681 levels. For the 10 levels $54, 59, 60, 71, 90, 94, 96, 108, 120, 150$, Propositions 7.8 to 7.13 give a sporadic point. This accounts for 691 levels, which are all the $N \leq 720$ outside $A \cup \{83, 131\}$. Among the 294 levels in [13, Tables 4 and 5] the resulting counts are as follows.

	has a sporadic point	has none	open
Table 4	40	27	0
Table 5	225	0	2

The two open levels are 83 and 131.

References

[1] D. Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices, (1996), pp. 1005–1011. 7.1

[2] M. Baker and X. Faber, *Metric properties of the tropical Abel-Jacobi map*, J. Algebraic Combin., 33 (2011), pp. 349–381. https://arxiv.org/abs/0905.1679. 8.5
[3] M. Baker and J. Rabinoff, *The skeleton of the Jacobian, the Jacobian of the skeleton, and lifting meromorphic functions from tropical to algebraic curves*, Int. Math. Res. Not. IMRN, (2015), pp. 7436–7472. https://arxiv.org/abs/1308.3864. 8.5
[4] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), pp. 235–265. 1.1, 2
[5] A. Bourdon, *On the finiteness of isolated j-invariants for $X_1(N)$*. Preprint, https://arxiv.org/abs/2608.19354, 2026. 1
[6] A. Bourdon and P. L. Clark, *Torsion points and Galois representations on CM elliptic curves*, Pacific J. Math., 305 (2020), pp. 43–88. 8.7, 8.8
[7] A. Bourdon and Ö. Ejder, *Rational isolated j-invariants from $X_1(\ell^n)$ and $X_0(\ell^n)$*, Res. Number Theory, 12 (2026). Paper No. 47. 1
[8] A. Bourdon, Ö. Ejder, Y. Liu, F. Odumodu, and B. Viray, *On the level of modular curves that give rise to isolated j-invariants*, Adv. Math., 357 (2019), pp. 106824, 33. 1, 2.1, 2.2
[9] A. Bourdon, D. R. Gill, J. Rouse, and L. D. Watson, *Odd degree isolated points on $X_1(N)$ with rational j-invariant*, Res. Number Theory, 10 (2024). Paper No. 5. 1
[10] A. Bourdon, S. Hashimoto, T. Keller, Z. Klagsbrun, D. Lowry-Duda, T. Morrison, F. Najman, and H. Shukla, *Towards a classification of isolated j-invariants*, Math. Comp., 94 (2025), pp. 447–473. 1
[11] J. Box, S. Gajović, and P. Goodman, *Cubic and quartic points on modular curves using generalised symmetric Chabauty*, Int. Math. Res. Not. IMRN, (2023), pp. 5604–5659. 1, 5.2, 5.2
[12] C. Calger, *Isolated points on modular curves of prime-power level*. Preprint, https://arxiv.org/abs/2512.11996, 2025. 1
[13] P. L. Clark, T. Genao, P. Pollack, and F. Saia, *The least degree of a CM point on a modular curve*, J. Lond. Math. Soc. (2), 105 (2022), pp. 825–883. 1, 1, 1.1, 4.11, 7.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 10
[14] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, second ed., 1997. 2, 8.8
[15] ———, *The elliptic curve database for conductors to 130000*, in Algorithmic number theory (ANTS VII), vol. 4076 of Lecture Notes in Comput. Sci., Springer, Berlin, 2006, pp. 11–29. https://johncremona.github.io/papers/ecdb_ants.pdf. 8.2
[16] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, in Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), vol. 349 of Lecture Notes in Math., Springer, Berlin, 1973, pp. 143–316. 1, 8.1, 8.5, 8.6, 8.7
[17] 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. 1, 1, 5, 5.1, 6, 6, 7.1, 7.2, 7.4, 7.5, 8.6
[18] M. Derickx and F. Najman, *Classification of torsion of elliptic curves over quartic fields*, J. Reine Angew. Math., 829 (2025), pp. 123–156. 1, 7.2
[19] ———, *Sporadic points on $X_0(N)$*. Preprint, https://arxiv.org/abs/2511.09015v2, 2025. 1, 1, 2, 5, 5, 5.2, 7.1
[20] M. Derickx and M. van Hoeij, *Gonality of the modular curve $X_1(N)$*, J. Algebra, 417 (2014), pp. 52–71. 7.1, 7.2, 7.4, 7.4, 8.5, 8.6, 8.6
[21] Ö. Ejder, *Isolated points on $X_1(\ell^n)$ with rational j-invariant*, Res. Number Theory, 8 (2022). Paper No. 16. 1
[22] G. Faltings, *The general case of S. Lang's conjecture*, in Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), vol. 15 of Perspect. Math., Academic Press, San Diego, CA, 1994, pp. 175–182. 3, 4.2
[23] T. Fisher, *Rational points on $X(11)$ over $\mathbb{Q}(\mu_{11})$ via Galois equivariance of the Cassels-Tate pairing*. Preprint, https://www.dpmms.cam.ac.uk/~taf1000/papers/galoiseq.pdf. 8.4, 8.4
[24] ———, *On families of n-congruent elliptic curves*. Preprint, https://arxiv.org/abs/1105.1706, 2011. 8.4
[25] G. Frey, *Curves with infinitely many points of fixed degree*, Israel J. Math., 85 (1994), pp. 79–83. 3
[26] B. H. Gross, *A tameness criterion for Galois representations associated to modular forms (mod p)*, Duke Math. J., 61 (1990), pp. 445–517. 8.1, 8.6, 8.6

[27] B. Kadets and I. Vogt, *Subspace configurations and low degree points on curves*, Adv. Math., 460 (2025), p. 110021. 2
[28] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math., 109 (1992), pp. 221–229. 1, 7.2
[29] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque, (2004), pp. 117–290. 8.4, 8.5, 9
[30] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J., 109 (1988), pp. 125–149. 1, 7.2
[31] H. H. Kim, *Functoriality for the exterior square of* GL_4 *and the symmetric fourth of* GL_2. *With appendix 1 by Dinakar Ramakrishnan and appendix 2 by Kim and Peter Sarnak*, J. Amer. Math. Soc., 16 (2003), pp. 139–183. 7.1
[32] D. S. Kubert and S. Lang, *Modular units*, vol. 244 of Grundlehren Math. Wiss., Springer, New York-Berlin, 1981. 7.5
[33] M. Lee, *Isolated j-invariants arising from the modular curve* $X_0(n)$, Res. Number Theory, 12 (2026). Paper No. 104. 1
[34] LMFDB Collaboration, *The L-functions and modular forms database*. `https://www.lmfdb.org`. 1.1, 2, 9, 9.2
[35] Y. Matsuda, *Determination of the modular Jacobian varieties* $J_1(M, MN)$ *with the Mordell-Weil rank zero*, Res. Number Theory, 9 (2023). `https://doi.org/10.1007/s40993-023-00430-4`. 8.4
[36] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math., (1977), pp. 33–186. 1, 6, 7.2
[37] J.-F. Mestre, *La méthode des graphes. Exemples et applications*, in Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986), Nagoya Univ., Nagoya, 1986, pp. 217–242. 8.5
[38] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on* $X_1(n)$, Math. Res. Lett., 23 (2016), pp. 245–272. 1
[39] ———, *Classification of torsion of elliptic curves over quintic fields*. Preprint, `https://arxiv.org/abs/2609.12846`, 2026. 1, 7.2
[40] ———, *Classification of torsion of elliptic curves over sextic fields*. Preprint, `https://arxiv.org/abs/2611.03933`, 2026. 1, 7.2
[41] ———, *Torsion of elliptic curves over number fields of degree* 6, 7, 8 *and* 9. Preprint, `https://hexagonmath.org/2611.00073v2`, 2026. 1, 7.2
[42] F. Najman and B. Vukorepa, *Quadratic points on bielliptic modular curves*, Math. Comp., 92 (2023), pp. 1791–1816. 5.2
[43] F. m. Najman, *Isolated and sporadic points on* $X_1(m, n)$, *a census*. `https://x1mn-sporadic.github.io/`; we use the revision `https://github.com/x1mn-sporadic/x1mn-sporadic.github.io/tree/dca0c196ae2bc3ffc09319b03171bba7323c1d16`. 1, 1, 1.1, 6, 7.1, 7.4, 7.4, 8.6
[44] B. Poonen, *Gonality of modular curves in characteristic p*, Math. Res. Lett., 14 (2007), pp. 691–701. 1, 4.1, 4.2
[45] G. Smith and I. Vogt, *Low degree points on curves*, Int. Math. Res. Not. IMRN, (2022), pp. 422–445. 2
[46] M. Streng, *Generators of the group of modular units for* $\Gamma^1(N)$ *over the rationals*. Preprint, `https://arxiv.org/abs/1503.08127`. 7.4, 7.5
[47] A. V. Sutherland, *Optimized equations for* $X_1(N)$. `https://math.mit.edu/~drew/X1_optcurves.html` and `https://math.mit.edu/~drew/X1_altcurves.html`. 6, 7.5, 7.5, 8.6
[48] K. Terao, *Isolated points on modular curves*, Adv. Math., 494 (2026), p. 110930. 1
[49] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 10.7)*. `https://www.sagemath.org`. 1.1, 2, 5.1
[50] 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/`. 1, 1, 4.11, 6, 7.1, 7.4, 7.4
[51] M. Varivoda, *Gonality and quintic points on intermediate modular curves*. Preprint, `https://hexagonmath.org/2610.00219v1`. 7.1
[52] B. Viray and I. Vogt, *Isolated and parameterized points on curves*, Essent. Number Theory, 5 (2026), pp. 1–47. 1, 2

[53] Y. Yang, *Modular units and cuspidal divisor class groups of $X_1(N)$*, J. Algebra, 322 (2009), pp. 514–553. 7.18, 7.5
[54] H. Yoo, *The rational cuspidal divisor class group of $X_0(N)$*. Preprint, `https://arxiv.org/abs/1908.06411`. 5.1
[55] D. Zywina, *Explicit open images for elliptic curves over $\mathbb{Q}$*. Preprint, `https://arxiv.org/abs/2206.14959`. 7.4

University of Zagreb, Bijenička Cesta 30, 10000 Zagreb, Croatia
Email address: `fnajman@math.hr`