hexagon:2611.01082v1

LOWER BOUNDS FOR THE GONALITY AND THE MINIMUM DENSITY DEGREE OF MODULAR CURVES

FILIP NAJMAN

ABSTRACT. Let C be a curve over $\mathbb{Q}$ with good reduction C_0 at a prime p, let q be a power of p, and suppose that the q-power Frobenius agrees with an automorphism of C_0 at S points. We prove that C has only finitely many points of degree d for every $d < S/(\sqrt{q}+1)^2$. In particular, the minimum density degree of C is at least $\#C_0(\mathbb{F}_q)/(\sqrt{q}+1)^2$, and this bound can be sharp. Applying this, and the analogous bound $S/(q+1)$ for the gonality of the reduction of C, at the supersingular points of modular curves, we obtain lower bounds for the gonality and the minimum density degree of modular curves which are linear in the index. For every fixed prime p, the bound for the gonality also holds over $\overline{\mathbb{F}}_p$ for all modular curves in characteristic p, including those with Igusa level structure, which gives a lower bound linear in the index of the kind expected by Poonen. For example, $\operatorname{gon}_{\mathbb{C}} X_\Gamma \geq D/60$ for every congruence subgroup Γ of index D in $\mathrm{PSL}_2(\mathbb{Z})$ and level not divisible by 6, and this is sharp. As applications, we show that the non-CM points of degree 6 on $X_1(37)$ have sporadic lifts to $X_1(N)$ for all N divisible by 37 and not divisible by 30, answering a question of Bourdon, Ejder, Liu, Odumodu and Viray, and that the $\overline{\mathbb{Q}}$-isogeny class of the elliptic curve 1225.b2 contains infinitely many j-invariants of sporadic points on the curves $X_1(N)$, answering a question of Bourdon and Najman.

1. INTRODUCTION

Let C be a curve over $\mathbb{Q}$. The *gonality* $\operatorname{gon}_K C$ of C over a field $K \supseteq \mathbb{Q}$ is the least degree of a non-constant morphism $C_K \to \mathbb{P}^1_K$, and the *minimum density degree* $\delta(C)$ of C is the least positive integer d such that C has infinitely many points of degree d. The minimum density degree was studied by Smith and Vogt [25], who call it the arithmetic degree of irrationality, and by Kadets and Vogt [13], whose terminology we use (see also [28]). A point x of C is *sporadic* if C has only finitely many points of degree $\leq \deg x$, i.e. if $\deg x < \delta(C)$. Hilbert's irreducibility theorem and a result of Frey [12, Proposition 2] give (see [28, Corollary 5.2.2 and (5.4.1)])

$$\tfrac{1}{2} \operatorname{gon}_{\mathbb{Q}} C \leq \delta(C) \leq \operatorname{gon}_{\mathbb{Q}} C, \tag{1.1}$$

so lower bounds for the gonality give lower bounds for the minimum density degree, but lose a factor of 2.

2020 *Mathematics Subject Classification.* 11G18, 14G35, 14H51, 11G05.

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

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

For $N \geq 4$, a non-cuspidal point of degree d on the modular curve $X_1(N)$ gives an elliptic curve with a point of order N over its residue field, which has degree d, and an elliptic curve with a point of order N over a number field of degree d gives a point of $X_1(N)$ of degree dividing d. Hence sporadic points on $X_1(N)$ correspond to torsion that appears over fields of unusually small degree (see [3, 5, 6, 9] and the references there). Lower bounds for the gonality of modular curves which are linear in the index go back to Zograf [29, Theorem 5], who proved that $\mathrm{gon}_{\mathbb{C}} X_\Gamma > D_\Gamma/128$ for every congruence subgroup Γ, where D_Γ is the index of the image of Γ in $\mathrm{PSL}_2(\mathbb{Z})$. Abramovich [1, Theorem 0.1], using an argument of Yau, improved this to $\mathrm{gon}_{\mathbb{C}} X_\Gamma \geq 7D_\Gamma/800$. His proof gives $\mathrm{gon}_{\mathbb{C}} X_\Gamma \geq \lambda D_\Gamma/24$ for any lower bound $\lambda \leq 1/4$ for the smallest positive eigenvalue λ_1 of the Laplacian on the congruence quotients of the upper half plane (see [10, Theorem 2]), so the bound $\lambda_1 \geq 975/4096$ of Kim and Sarnak [15, Appendix 2] gives $\mathrm{gon}_{\mathbb{C}} X_\Gamma \geq 325D_\Gamma/32768 \approx D_\Gamma/100.8$, and Selberg's eigenvalue conjecture would give $\mathrm{gon}_{\mathbb{C}} X_\Gamma \geq D_\Gamma/96$ [1, Section 0.1]. Zywina [30, Theorem 5.1], using the known cases of Selberg's conjecture, showed that $\mathrm{gon}_{\mathbb{C}} X_\Gamma > D_\Gamma/96$ if the level of Γ is at most 226. In positive characteristic, Poonen [21, Proposition 3.1] used the supersingular points to show that a twist of the reduction of X_Γ modulo a prime ℓ not dividing the level of Γ has $\mathbb{F}_{\ell^2}$-gonality at least $(\ell-1)D_\Gamma/(12(\ell^2+1))$, from which he deduced a lower bound of order $\sqrt{D_\Gamma}$ for its $\overline{\mathbb{F}}_\ell$-gonality [21, Corollary 3.3]. He expects a lower bound for the $\overline{\mathbb{F}}_p$-gonality of all modular curves in characteristic p (including those whose level is divisible by p, such as the Igusa curves) which is linear in the index, with a constant independent of p, but notes that he is unable to prove a lower bound linear in the index even for fixed p [21, Section 1.2].

In this paper we prove the following general lower bound for the minimum density degree. 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.

Theorem 1.1. *Let C be a curve over $\mathbb{Q}$ with good reduction at a prime p, let C_0 be its reduction, let $e \geq 1$, $q = p^e$, and let τ be an automorphism of $C_{0,\overline{\mathbb{F}}_p}$. Suppose that $\Phi^e(x) = \tau(x)$ for S distinct points $x \in C_0(\overline{\mathbb{F}}_p)$. Then*

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

Taking τ to be the identity, we obtain $\delta(C) \geq \#C_0(\mathbb{F}_q)/(\sqrt{q}+1)^2$, and this bound can be sharp (see Remark 4.4). This is an analogue for the minimum density degree of the classical bound $\mathrm{gon}_{\mathbb{Q}} C \geq \mathrm{gon}_{\mathbb{F}_q} C_0 \geq \#C_0(\mathbb{F}_q)/(q+1)$, which together with (1.1) gives only $\delta(C) \geq \#C_0(\mathbb{F}_q)/(2q+2)$. The proof applies the Hodge index theorem on the product of C_0 with the reduction of an abelian variety that parametrizes a hypothetical infinite family of points of degree $d < S/(\sqrt{q}+1)^2$. A simpler counting argument (Lemma 3.1) shows that the $\overline{\mathbb{F}}_p$-gonality of C_0 is at least $S/(q+1)$. Note that here the map to $\mathbb{P}^1$ need not be defined over $\mathbb{F}_q$, which is what keeps the bounds below linear in the index.

At a prime ℓ not dividing the level, the ℓ^2-power Frobenius agrees with an automorphism of the modular curve at all of its supersingular points (Lemmas 3.2 and 3.4). Applying the bounds above at these points, we obtain the following results. For $N \geq 3$ we write

$$D_N = D_{\Gamma_1(N)} = \frac{N^2}{2} \prod_{q \mid N} \left(1 - \frac{1}{q^2}\right),$$

where q runs through the primes dividing N, for the degree of the map $X_1(N) \to X(1)$.

Theorem 1.2. *Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup of level N and let $\ell \nmid N$ be a prime. Then*

$$\operatorname{gon}_{\mathbb{C}} X_\Gamma \geq \frac{\ell - 1}{12(\ell^2+1)} D_\Gamma,$$

and the same bound holds for the $\overline{\mathbb{F}}_\ell$-gonality of the reduction of X_Γ modulo ℓ. In particular, if $6 \nmid N$, then $\operatorname{gon}_{\mathbb{C}} X_\Gamma \geq D_\Gamma/60$.

For X_Γ hyperelliptic of genus at least 2 or trigonal of genus at least 5, the bound for $\operatorname{gon}_{\mathbb{C}} X_\Gamma$ in Theorem 1.2 was proved by Zywina [30, Theorem 5.4], using Poonen's construction. Taking $\ell \in \{2, 3, 5, 7\}$, we obtain a better bound than $D_\Gamma/100.8$ for all N not divisible by 210, and a better bound than $D_\Gamma/96$ for all N not divisible by 30. The constant $1/60$ cannot be improved: if Γ is contained in $\Gamma(5)$, or in a conjugate of $\Gamma(5)$ by an element of $\mathrm{GL}_2(\mathbb{Q})$ of positive determinant, and $6 \nmid N$, then $\operatorname{gon}_{\mathbb{C}} X_\Gamma = D_\Gamma/60$ (Remark 3.5). In particular, for all $n \geq 1$ with $6 \nmid n$ we obtain

$$\operatorname{gon}_{\mathbb{Q}} X_1(25n) = \operatorname{gon}_{\mathbb{C}} X_1(25n) = \frac{D_{25n}}{60}.$$

For $n = 1$ we recover the value $\operatorname{gon}_{\mathbb{Q}} X_1(25) = 5$, which was determined by Derickx and van Hoeij [10]. For $n \leq 10$ these values are equal to the upper bounds for $\operatorname{gon}_{\mathbb{Q}} X_1(25n)$ in [10, Table 1], so these upper bounds are sharp for $N = 50$, 75, 100, 125, 175, 200, 225 and 250. In the terminology of [10, Section 4], Theorem 1.2 shows that every non-constant function f on X_Γ has *improvement factor* $D_\Gamma / \deg f \leq 60$ if $6 \nmid N$. Derickx and van Hoeij observed that the improvement factors of the modular units they found on $X_1(N)$ for $N \leq 300$ are often 48, and that they are larger for N divisible by p^2 with $p \geq 5$, reaching 60 for $N = 25$ [10, Section 4].

For a fixed prime ℓ, the bound for the $\overline{\mathbb{F}}_\ell$-gonality in Theorem 1.2 is linear in the index. In Section 7 we show that it holds, with the same constant, for all the modular curves in characteristic ℓ considered by Poonen [21, Section 1.2], including those whose level is divisible by ℓ, such as the Igusa curves (Theorem 7.5). For each fixed prime this gives the linear lower bound that Poonen was unable to prove. Let $X(\ell^e; N)$ be the curve parametrizing elliptic curves with full level N structure and Igusa structure of level ℓ^e, where $N \geq 3$ is not divisible by ℓ and $e \geq 1$. The main step is that every non-constant function on $X(\ell^e; N)$ of degree less than $\varphi(\ell^e) D_{\Gamma(N)}/24$ is the pullback of a function on $X(N)$ (Corollary 7.4). Its proof uses the wild ramification of the Igusa tower above the supersingular points. It also gives the equality

$$\operatorname{gon}_{\overline{\mathbb{F}}_\ell} X(\ell^e; N) = \varphi(\ell^e) \operatorname{gon}_{\overline{\mathbb{F}}_\ell} X(N)$$

for $N \geq 4$ (Proposition 7.6). Unfortunately, the constant $(\ell - 1)/(12(\ell^2+1))$ tends to 0 as ℓ grows. By Proposition 7.6, a linear lower bound with a constant independent of the characteristic, as expected by Poonen, would follow from such a bound for the modular curves of level not divisible by the characteristic (Remark 7.7).

For the minimum density degree we obtain the following.

Theorem 1.3. a) *Let $N \geq 5$ and let $\ell \nmid N$ be a prime. Then*

$$\delta(X_1(N)) \geq \frac{(\ell - 1) D_N}{12(\ell+1)^2}.$$

b) *Let $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be a subgroup containing $-I$ such that $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$, and let $\ell \nmid N$ be a prime. Then*

$$\delta(X_G) \geq \frac{(\ell-1)D_G}{12(\ell+1)^2},$$

where $D_G = [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G]$ is the degree of the map $X_G \to X(1)$.

This improves on the bound obtained from Theorem 1.2 and (1.1) by a factor of $2(\ell^2+1)/(\ell+1)^2$, which tends to 2 as ℓ grows. For $\ell = 2, 3, 5, 7$ the constant $(\ell-1)/(12(\ell+1)^2)$ is $1/108$, $1/96$, $1/108$ and $1/128$, respectively, while Abramovich's bound with the eigenvalue bound of Kim and Sarnak and (1.1) give $\delta(X_G) \geq 325D_G/65536 \approx D_G/201.6$ for all levels.

We give two applications to sporadic points. Bourdon, Ejder, Liu, Odumodu and Viray [3, Lemma 7.2] showed, using Abramovich's bound, that if a point $x \in X_1(N)$ satisfies $\deg x < \frac{7}{1600} D_{\Gamma_1(N)}$, then for every $d \geq 1$ every point of $X_1(dN)$ lying over x is sporadic. They used this to show that every CM j-invariant is the j-invariant of infinitely many sporadic points [3, Theorem 7.1], and noted that none of the known non-CM sporadic points satisfies this degree condition. They asked whether there exist non-CM sporadic points with infinitely many sporadic lifts [3, Remark 7.3] (see also [8, Section 10]). We answer this question.

Theorem 1.4. *Let x be a point of degree 6 on $X_1(37)$ with $j(x) = -9317$. For every N divisible by 37 and not divisible by 30, every point of $X_1(N)$ lying over x is sporadic. In particular, x is a non-CM sporadic point with sporadic lifts to infinitely many curves $X_1(N)$.*

Points of degree 6 on $X_1(37)$ were found by van Hoeij [27] (see also [4] and the point 1.37.6.a of the census [18]). Note that $6 \geq \frac{7}{1600} \cdot 684$ and $6 \geq \frac{325}{65536} \cdot 684$, so Abramovich's bound does not suffice here, even with the eigenvalue bound of Kim and Sarnak.

Bourdon and Najman [5] showed that all non-CM $\mathbb{Q}$-curves giving rise to a sporadic point of odd degree on some $X_1(N)$ lie in a single $\overline{\mathbb{Q}}$-isogeny class, and asked [5, Question 2] whether there exists a non-CM $\overline{\mathbb{Q}}$-isogeny class containing infinitely many sporadic j-invariants, i.e. j-invariants of sporadic points on the curves $X_1(N)$. We answer this question.

Theorem 1.5. *The $\overline{\mathbb{Q}}$-isogeny class of the elliptic curve 1225.b2 (which has j-invariant -9317) contains infinitely many elliptic curves with pairwise distinct j-invariants which give sporadic points on the curves $X_1(37 \cdot 2^k)$, $k \geq 1$.*

Finally, Derickx and Stoll [9, Proposition 3.6] showed, using Abramovich's bound, that if there are infinitely many elliptic curves with pairwise distinct j-invariants over number fields of degree d with a point of order p over that field, then $p^2 - 1 \leq C_1' d$ with $C_1' = 2^{17}/325 \approx 403.3$. Theorem 1.3 a) shows that one can take $C_1' = 192$ (Corollary 4.5).

Theorem 1.1 for curves with a rational point and automorphisms τ defined over $\mathbb{F}_p$, Lemma 3.1 for curves and automorphisms defined over $\mathbb{F}_p$, and Theorem 1.3 a) first appeared in the first version of [19], where they are used to determine the integers N for which $X_1(N)$ has a non-cuspidal sporadic point, with the exception of $N = 83$ and $N = 131$. Later versions of [19] will cite the present paper for them.

AI disclosure. AI models were extensively used in the work leading to this paper. Some (but not all) mathematical results were obtained by OpenAI's GPT-6.2 Astra, while Anthropic's Claude Opus 5.5 reviewed and rechecked the mathematics, and drafted the manuscript. I guided the work, and rewrote parts of the manuscript.

Acknowledgements

I thank Abbey Bourdon and Maarten Derickx for helpful discussions and suggestions.

2. Conventions and notation

Throughout the paper all curves are smooth, projective and geometrically integral, and a point of a curve over a field is a closed point unless stated otherwise. We identify a point x of degree d on a curve C over $\mathbb{Q}$ with the effective divisor of degree d on C (defined over $\mathbb{Q}$) which is the sum of its geometric points. We denote by $J_C = \mathrm{Pic}^0_C$ the Jacobian of C and by $W_d(C) \subseteq \mathrm{Pic}^d_C$ the image of the d-th symmetric power of C. The Jacobian J_C acts on Pic^d_C by translation, and for $a \in \mathrm{Pic}^d_C$ and an abelian subvariety $A \subseteq J_C$ we write $a + A$ for the image of A under $y \mapsto a + y$.

Let C be a curve over a number field K with good reduction at a prime $\mathfrak{p}$ of K, with residue field $\mathbb{F}_\mathfrak{p}$. Then $\mathrm{gon}_{\mathbb{F}_\mathfrak{p}} C_{\mathbb{F}_\mathfrak{p}} \leq \mathrm{gon}_K C$ [20, Section 3]. Applying this over a number field K such that $K(C)$ contains a function of degree $\mathrm{gon}_{\overline{\mathbb{Q}}} C$, we obtain, for a curve C over $\mathbb{Q}$ with good reduction at p and reduction C_0,

$$\mathrm{gon}_{\overline{\mathbb{F}}_p} C_{0,\overline{\mathbb{F}}_p} \leq \mathrm{gon}_{\overline{\mathbb{Q}}} C. \tag{2.1}$$

For a positive integer N we denote by $X_1(N)$ the modular curve over $\mathbb{Q}$ whose non-cuspidal points parametrize pairs (E, P), where E is an elliptic curve and $P \in E$ a point of order 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 (E, P) to (E, aP). Since (E, P) and $(E, -P)$ are isomorphic, $\langle a \rangle$ depends only on the class of a in $(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$. For $N \geq 5$ and a prime $p \nmid N$ we put

$$S_p(N) = \frac{(p-1)D_N}{12}.$$

By Lemma 3.2, $S_p(N)$ is the number of supersingular points on $X_1(N)_{\overline{\mathbb{F}}_p}$. Note that $2D_N$ is the number of points of exact order N on an elliptic curve over an algebraically closed field of characteristic not dividing N. Hence for $M \mid N$ with $M \geq 3$, the map $X_1(N) \to X_1(M)$, $(E, P) \mapsto (E, (N/M)P)$, has degree D_N/D_M.

For a congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ we denote by X_Γ the corresponding modular curve over $\mathbb{C}$ and by D_Γ the index of the image of Γ in $\mathrm{PSL}_2(\mathbb{Z})$, which is the degree of the natural map $X_\Gamma \to X(1)$. We write $X(N) = X_{\Gamma(N)}$. For a subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ containing $-I$ with $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$, we denote by X_G the modular curve over $\mathbb{Q}$ whose non-cuspidal points parametrize pairs $(E, [\alpha])$, where $\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \to E[N]$ is an isomorphism and $[\alpha]$ is its orbit under the action of G by $\alpha \mapsto \alpha \circ g$. It is geometrically connected, and the map $X_G \to X(1)$ has degree $D_G = [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G]$. The curve X_G has good reduction at every prime $\ell \nmid N$, and the non-cuspidal points of its reduction over $\overline{\mathbb{F}}_\ell$ have the same moduli interpretation [7].

3. Lower bounds for the gonality

The following lemma is a variant of Ogg's argument. Compare [2, Lemma 3.22], where the points x with $F(x) = \langle -p \rangle x$ are counted in the same way for a map to $\mathbb{P}^1$ that is defined over $\mathbb{F}_p$, and [21, Proposition 3.1], where the supersingular points are used to bound the $\mathbb{F}_{p^2}$-gonality of a twist of a modular curve. Note that in Lemma 3.1 the map to $\mathbb{P}^1$ is not required to be defined over $\mathbb{F}_q$.

Lemma 3.1. *Let X be a curve over a finite field $\mathbb{F}_q$, let $\overline{X}$ be its base change to $\overline{\mathbb{F}}_q$, let $F : \overline{X} \to \overline{X}$ be the base change of the q-power Frobenius morphism of X, and let σ be an automorphism of $\overline{X}$. Then*

$$\#\{x \in \overline{X}(\overline{\mathbb{F}}_q) : F(x) = \sigma(x)\} \leq (q+1)\operatorname{gon}_{\overline{\mathbb{F}}_q} \overline{X}.$$

Proof. Let $f \in \overline{\mathbb{F}}_q(\overline{X})$ be a function of degree $d = \operatorname{gon}_{\overline{\mathbb{F}}_q} \overline{X}$. As F has degree q and σ has degree 1, the functions $f \circ F$ and $f \circ \sigma$ have degrees qd and d, so they are different. Hence the set T of points $x \in \overline{X}(\overline{\mathbb{F}}_q)$ with $f(F(x)) = f(\sigma(x))$ is finite, and it contains every point x with $F(x) = \sigma(x)$. Composing f with an automorphism of $\mathbb{P}^1$, which does not change T, we may assume that $f(\sigma(x)) \neq \infty$ for all $x \in T$. Then the function $g = f \circ F - f \circ \sigma$ is non-zero and vanishes at every point of T. Every pole of g is a pole of $f \circ F$ or of $f \circ \sigma$, so g has at most $qd + d$ poles, counted with multiplicity, and hence at most $(q+1)d$ zeros. It follows that $\#T \leq (q+1)d$. □

Lemma 3.2. *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 $-p$ [2, Lemma 3.21]. 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 $\operatorname{Aut}(E)$ acts freely on the $2D_N$ points of exact order N of E, and $-1 \in \operatorname{Aut}(E)$ identifies P with $-P$. Hence there are $2D_N/\#\operatorname{Aut}(E)$ points of $X_1(N)_{\overline{\mathbb{F}}_p}$ above $j(E)$, so by the Eichler mass formula $\sum_E 1/\#\operatorname{Aut}(E) = (p-1)/24$, the sum running over the isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, there are $S_p(N)$ supersingular points. □

Corollary 3.3. *Let $N \geq 5$ and let $p \nmid N$ be a prime. Then*

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

Proof. The first inequality is (2.1), since $X_1(N)$ has good reduction at p, and the second follows from Lemma 3.2 and Lemma 3.1 with $q = p^2$, $F = \Phi^2$ and $\sigma = \langle p \rangle$. □

For $\Gamma = \Gamma_1(N)$ the bound of Corollary 3.3 is the bound of Theorem 1.2. To prove Theorem 1.2 in general, we apply the same argument to a model of $X(N)$ over $\mathbb{Q}$, using the following lemma, which we will also use in Section 4.

Lemma 3.4. *Let $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be a subgroup containing $-I$ with $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$, let $\ell \nmid N$ be a prime, and let τ be the automorphism of X_G which sends $(E, [\alpha])$ to $(E, [\ell\alpha])$. Then τ is defined over $\mathbb{Q}$, and the reduction of X_G modulo ℓ has at least $(\ell-1)D_G/12$ supersingular points, at each of which $\Phi^2(x) = \tau(x)$.*

Proof. Since $[\ell\alpha] = [\alpha \circ \ell I]$ and ℓI is central in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, the map τ is well defined on G-orbits. It commutes with the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, which acts on α by composition on the left, so τ is defined over $\mathbb{Q}$. Let E be a supersingular elliptic curve over $\overline{\mathbb{F}}_\ell$. The group G acts freely on the isomorphisms $\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \to E[N]$, so there are D_G orbits $[\alpha]$, and the points of the reduction of X_G above $j(E)$ are the orbits of $\operatorname{Aut}(E)$ on this set. Since $-I \in G$, the automorphism -1 fixes every $[\alpha]$, so each of these orbits has at most $\#\operatorname{Aut}(E)/2$ elements, and there are at least $2D_G/\#\operatorname{Aut}(E)$ points above $j(E)$. By the Eichler mass formula, as in the proof of Lemma 3.2, there are at least $(\ell-1)D_G/12$ supersingular points. Every supersingular elliptic curve over $\overline{\mathbb{F}}_\ell$ has a model E over $\mathbb{F}_{\ell^2}$

whose ℓ^2-power Frobenius endomorphism is multiplication by $-\ell$ [2, Lemma 3.21], and for such a model Φ^2 sends $(E,[\alpha])$ to $(E,[-\ell\alpha]) = (E,[\ell\alpha])$, since $-I \in G$. □

For $N \geq 3$ let $G_N \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be the subgroup of the matrices $\pm\left(\begin{smallmatrix}1&0\\0&d\end{smallmatrix}\right)$ with $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, so that $\det(G_N) = (\mathbb{Z}/N\mathbb{Z})^\times$ and $D_{G_N} = \#\,\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/2 = D_{\Gamma(N)}$. Let ζ be a primitive N-th root of unity in $\mathbb{C}$, or in $\overline{\mathbb{F}}_\ell$ for a prime $\ell \nmid N$. If α sends the standard basis to (P,Q), then $[\alpha]$ consists of the isomorphisms sending it to $\pm(P,dQ)$ with $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, so it contains exactly two bases $\pm(P,Q')$ of $E[N]$ with Weil pairing $e_N(P,Q') = \zeta$. Hence X_{G_N} is isomorphic over $\mathbb{C}$ to $X(N)$, and its reduction modulo ℓ is isomorphic over $\overline{\mathbb{F}}_\ell$ to the reduction $X(N)_{\overline{\mathbb{F}}_\ell}$ of $X(N)$, the curve of triples (E,P,Q) with $e_N(P,Q) = \zeta$.

Proof of Theorem 1.2. Let $M \geq 3$ be a multiple of N not divisible by ℓ. By Lemma 3.4, the reduction of X_{G_M} modulo ℓ has at least $(\ell-1)D_{\Gamma(M)}/12$ points x with $\Phi^2(x) = \tau(x)$, so Lemma 3.1 with $q = \ell^2$, $F = \Phi^2$ and $\sigma = \tau$, and (2.1) give

$$\mathrm{gon}_{\mathbb{C}}\, X(M) = \mathrm{gon}_{\overline{\mathbb{Q}}}\, X_{G_M} \geq \mathrm{gon}_{\overline{\mathbb{F}}_\ell}\, X(M)_{\overline{\mathbb{F}}_\ell} \geq \frac{\ell-1}{12(\ell^2+1)} D_{\Gamma(M)},$$

where the equality is [21, Proposition A.1 (ii)]. Since $\Gamma(M) \subseteq \Gamma$, the natural map $X(M) \to X_\Gamma$ has degree $D_{\Gamma(M)}/D_\Gamma$, and so does the quotient map from $X(M)_{\overline{\mathbb{F}}_\ell}$ to the reduction of X_Γ modulo ℓ, which is the quotient of $X(M)_{\overline{\mathbb{F}}_\ell}$ by the image of Γ in $\mathrm{SL}_2(\mathbb{Z}/M\mathbb{Z})$ (see [2, Lemma 3.20] and its proof). Pulling back a function of minimal degree along these maps, we obtain

$$\mathrm{gon}_{\mathbb{C}}\, X(M) \leq \frac{D_{\Gamma(M)}}{D_\Gamma}\, \mathrm{gon}_{\mathbb{C}}\, X_\Gamma,$$

and the same inequality for the $\overline{\mathbb{F}}_\ell$-gonalities of the reductions. This proves the first two statements. The last statement follows by taking $\ell = 2$ if N is odd and $\ell = 3$ if $3 \nmid N$, since $\frac{1}{12\cdot 5} = \frac{2}{12\cdot 10} = \frac{1}{60}$. □

Remark 3.5. The curve $X(5)$ has genus 0 and $D_{\Gamma(5)} = 60$. If $\Gamma' \subseteq \mathrm{SL}_2(\mathbb{Z})$ is conjugate to $\Gamma(5)$ by an element of $\mathrm{GL}_2(\mathbb{Q})$ of positive determinant, then also $X_{\Gamma'} \simeq \mathbb{P}^1$ and $D_{\Gamma'} = 60$ (the index is proportional to the hyperbolic area). Hence for every congruence subgroup $\Gamma \subseteq \Gamma'$ of level not divisible by 6, the map $X_\Gamma \to X_{\Gamma'}$ of degree $D_\Gamma/60$ and Theorem 1.2 give $\mathrm{gon}_{\mathbb{C}}\, X_\Gamma = D_\Gamma/60$.

For $\Gamma = \Gamma_1(25n)$ such a map can be taken to be defined over $\mathbb{Q}$. The quotient Y of $X_1(25)$ by the diamond operators $\langle d\rangle$ with $d \equiv \pm 1 \pmod 5$ is the modular curve of $\Gamma_0(25) \cap \Gamma_1(5)$, which is conjugate to $\Gamma(5)$ by $\left(\begin{smallmatrix}1&0\\0&5\end{smallmatrix}\right)$ (see [10, Section 4]). As Y is defined over $\mathbb{Q}$ and has a rational cusp, $Y \simeq \mathbb{P}^1$ over $\mathbb{Q}$, so composing $X_1(25n) \to X_1(25)$, $(E,P) \mapsto (E,nP)$, with $X_1(25) \to Y$ gives a function on $X_1(25n)$ defined over $\mathbb{Q}$ of degree $D_{\Gamma_1(25n)}/60$.

Remark 3.6. For every prime $N \geq 5$, Corollary 3.3 with $p = 2$ gives $\mathrm{gon}_{\mathbb{Q}}\, X_1(N) \geq D_N/60 = (N^2-1)/120$, so

$$\liminf_{N\to\infty} \frac{\mathrm{gon}_{\mathbb{Q}}\, X_1(N)}{N^2-1} \geq \frac{1}{120} \approx 0.00833,$$

where N runs through the primes. In the discussion of the asymptotic behaviour of $\mathrm{gon}_{\mathbb{Q}}\, X_1(N)/(N^2-1)$ for primes N in [9, p.7], the lower bound $\frac{325}{2^{16}} \approx 0.00496$ (or $\frac{1}{192} \approx 0.00521$ under Selberg's conjecture) coming from Abramovich's bound [9, Theorem 3.3] is used, while the upper bound of van Hoeij and Smith gives $\limsup_{N\to\infty} \mathrm{gon}_{\mathbb{Q}}\, X_1(N)/(N^2-1) \leq \frac{11}{840} \approx 0.01310$ [9, p.7].

4. Lower bounds for the minimum density degree

In this section we prove Theorem 1.1 and Theorem 1.3. We need three lemmas.

Lemma 4.1. *Let C be a curve over $\mathbb{Q}$, 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 $W_d(C)(\mathbb{Q})$. Translation by one of them is an isomorphism $J_C \to \operatorname{Pic}^d_C$ defined over $\mathbb{Q}$, so by Faltings' theorem [11], 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 4.2. *Let C be a curve over $\mathbb{Q}$ with 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, and let $i_0 : A_0 \to J_{C_0}$ be the reduction of the inclusion $A \to J_C$. Then i_0 has finite kernel, $a_0 + i_0(A_0) \subseteq W_d(C_0)$, 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 $a_0 + i_0(y)$.*

Proof. The abelian variety A has good reduction at p, since it is an isogeny factor of J_C, and the inclusion $i : A \to J_C$ extends to the Néron models over $\mathbb{Z}_{(p)}$. By Poincaré's complete reducibility theorem there are a homomorphism $\rho : J_C \to A$ and an integer $m \geq 1$ such that $\rho \circ i = [m]$. Reducing, we obtain $\rho_0 \circ i_0 = [m]$, so i_0 has finite kernel. The point a extends by properness, and the relative W_d is closed, being the image of the relative symmetric power. Hence $a_0 + i_0(A_0) \subseteq W_d(C_0)$. We identify the symmetric power $C_0^{(d)}$ with the scheme of effective divisors of degree d on C_0 [16, Remark 3.9]. Since $d < \operatorname{gon}_{\overline{\mathbb{F}}_p} C_0$, and the gonality does not change under extensions of algebraically closed fields [21, Proposition A.1 (ii)], every effective divisor class of degree d on C_0 over an algebraically closed field contains a unique effective divisor. Hence every non-empty geometric fibre of the Abel map $C_0^{(d)} \to \operatorname{Pic}^d_{C_0}$ is a linear system of dimension 0, which is a reduced point [16, Theorem 3.13]. As $C_0^{(d)}$ is proper, the Abel map is therefore a closed immersion [26, Tag 04XV], and it identifies $C_0^{(d)}$ with $W_d(C_0)$. Since A_0 is reduced, the morphism $A_0 \to \operatorname{Pic}^d_{C_0}$, $y \mapsto a_0 + i_0(y)$, which is defined over $\mathbb{F}_p$, factors through $W_d(C_0)$, so it lifts to a morphism $A_0 \to C_0^{(d)}$ over $\mathbb{F}_p$. We take $\mathcal{D}$ to be the pullback along it of the universal divisor on $C_0 \times C_0^{(d)}$, which is finite and flat of degree d over $C_0^{(d)}$. □

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 $C_0 \times A_0$, which is nef, V for the class of $\{x\} \times A_0$ for a point $x \in C_0(\overline{\mathbb{F}}_p)$, $M = H^r > 0$ 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 4.3. *Let C_0 be a curve and A_0 an abelian variety of dimension $r \geq 1$, both over $\mathbb{F}_p$, let $e \geq 1$, $q = p^e$, 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 $C_{0,\overline{\mathbb{F}}_p}$. 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 dominates C_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 the components of Z are Galois conjugate and Z dominates C_0, each of them 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 nef 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. □

Proof of Theorem 1.1. 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 3.1 (applied to $C_{0,\mathbb{F}_q}$ with $F = \Phi^e$ and $\sigma = \tau$) and (2.1). Let $a + A \subseteq W_d(C)$ be the translate given by Lemma 4.1, and $\mathcal{D} \subseteq C_0 \times A_0$ the divisor given by Lemma 4.2. Since i_0 has finite kernel and $\dim A_0 = \dim A > 0$, the classes $a_0 + i_0(y)$, and hence the divisors $\mathcal{D}_y$, are not all equal. Every component of $\mathcal{D}$ is finite over A_0, so it is either of the form $\{x\} \times A_0$ with $x \in C_0(\overline{\mathbb{F}}_p)$ or it dominates C_0, and as the $\mathcal{D}_y$ are not all equal, some component dominates C_0. Let Z be the reduced union of its Galois orbit. Then Z satisfies the assumptions of Lemma 4.3, with $b \leq d$, so $S \leq (\sqrt{q}+1)^2 d$, which is a contradiction. □

Remark 4.4. Taking τ to be the identity in Theorem 1.1, we obtain $\delta(C) \geq \#C_0(\mathbb{F}_q)/(\sqrt{q}+1)^2$ for every curve C over $\mathbb{Q}$ with good reduction at p, and every power q of p. Note that the denominator is the Hasse bound for the number of points of an elliptic curve over $\mathbb{F}_q$. This bound can be sharp. For example, the elliptic curve $E : y^2 + y = x^3 + 2x$ has good reduction at 2, and the point $(0,0) \in E(\mathbb{Q})$ is of infinite order (the curve E is 77.a1, which has trivial torsion [17]), so $\delta(E) = 1$. Its reduction $y^2 + y = x^3$ modulo 2 has 9 points over $\mathbb{F}_4$, so the bound with $q = 4$ is also 1.

Proof of Theorem 1.3. a) The curve $X_1(N)$ has good reduction at ℓ, so this follows from Lemma 3.2 and Theorem 1.1 with $p = \ell$, $e = 2$ and $\tau = \langle \ell \rangle$.

b) This follows in the same way from Lemma 3.4 and Theorem 1.1. □

Corollary 4.5. *Let $d \geq 1$ and let p be a prime such that there are infinitely many elliptic curves E with pairwise distinct j-invariants over number fields K of degree d such that $E(K)$ has a point of order p. Then $p^2 - 1 \leq 192d$. In particular, one can take $C_1' = 192$ in* [9, Proposition 3.6].

Proof. The pairs (E, P) give infinitely many points of degree $\leq d$ on $X_1(p)$, so $\delta(X_1(p)) \leq d$. If $p \leq 3$, then $p^2 - 1 \leq 8 \leq 192d$. If $p \geq 5$, then Theorem 1.3 a) with $\ell = 3$ gives $\delta(X_1(p)) \geq 2(p^2-1)/(24 \cdot 16) = (p^2-1)/192$. □

Using Corollary 3.3 and (1.1) instead of Theorem 1.3 gives the constant 240 in Corollary 4.5.

5. Sporadic lifts

For $M \mid N$ we say that a point $y \in X_1(N)$ *lies over* a point $x \in X_1(M)$ if y maps to x under the map $X_1(N) \to X_1(M)$, $(E, P) \mapsto (E, (N/M)P)$.

Proposition 5.1. *Let $M \geq 5$, let $x \in X_1(M)$ and let ℓ be a prime such that*

$$\deg x < \frac{(\ell-1)D_M}{12(\ell+1)^2}.$$

Then for every N divisible by M and not divisible by ℓ, every point of $X_1(N)$ lying over x is sporadic.

Proof. Let $y \in X_1(N)$ lie over x. As the map $X_1(N) \to X_1(M)$ has degree D_N/D_M, we have

$$\deg y \leq \frac{D_N}{D_M} \deg x < \frac{(\ell-1)D_N}{12(\ell+1)^2} \leq \delta(X_1(N))$$

by Theorem 1.3 a), since $\ell \nmid N$. □

Proof of Theorem 1.4. We have $D_{37} = 684$, so the right-hand side of the inequality in Proposition 5.1 with $M = 37$ is $684/108 = 6.33\ldots$ for $\ell = 2$ and $\ell = 5$, and $684/96 = 7.125$ for $\ell = 3$. As $30 \nmid N$, one of the primes 2, 3 and 5 does not divide N, so the first claim follows from Proposition 5.1. The point x is itself sporadic, by the case $N = 37$, and it is not a CM point, since -9317 is not the j-invariant of an elliptic curve with complex multiplication. The curves $X_1(37^r)$, $r \geq 1$, give infinitely many curves $X_1(N)$ to which the first claim applies. □

Remark 5.2. Unfortunately, our methods do not settle the levels N divisible by $30 \cdot 37 = 1110$. For $N = 1110$ the points lying over x have degree at most $6D_{1110}/D_{37} = 3456$, while the best bound given by Theorem 1.3 a) is $\delta(X_1(1110)) \geq 3078$, obtained with $\ell = 7$.

6. Sporadic j-invariants in an isogeny class

Proof of Theorem 1.5. Let x be a point of degree 6 on $X_1(37)$ with $j(x) = -9317$, let K be its residue field, and let (E_0, P) be the corresponding pair, where E_0 is an elliptic curve over K and $P \in E_0(K)$ is a point of order 37. As $j(E_0) = -9317$, the curve E_0 is isomorphic over $\overline{\mathbb{Q}}$ to the curve 1225.b2, and it does not have complex multiplication.

Choose points $T_k \in E_0(\overline{K})$ of order 2^k for $k \geq 1$ such that $2T_{k+1} = T_k$, and let C_k be the cyclic subgroup generated by T_k, so that $C_1 \subset C_2 \subset \cdots$. Let $\psi_k : E_0 \to E_k = E_0/C_k$ be the quotient isogeny. Since $\#C_k$ is prime to 37, the point $P_k = \psi_k(P)$ has order 37. The kernel of the dual isogeny $\widehat{\psi}_k : E_k \to E_0$ is $\psi_k(E_0[2^k]) \simeq E_0[2^k]/C_k$, which is cyclic of order 2^k. Let Q_k be a generator of it. Then $R_k = P_k + Q_k$ is a point of order $37 \cdot 2^k$ on E_k, and $y_k = (E_k, R_k)$ is a non-cuspidal point of $X_1(37 \cdot 2^k)$.

We first bound the degree of y_k. Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$ be such that $\sigma(C_k) = C_k$ and $\sigma(Q_k) = Q_k$. Then σ fixes E_k and ψ_k, and hence P_k, so it fixes R_k. Let L be the field of definition of C_k, i.e. the fixed field of the stabilizer of C_k in $\mathrm{Gal}(\overline{K}/K)$. As $\mathrm{Gal}(\overline{K}/K)$ permutes the $3 \cdot 2^{k-1}$ cyclic subgroups of order 2^k of $E_0[2^k]$, we have $[L : K] \leq 3 \cdot 2^{k-1}$. The curve E_k and the isogenies ψ_k and $\widehat{\psi}_k$ are defined over L, so $\mathrm{Gal}(\overline{K}/L)$ permutes the 2^{k-1} generators of $\ker \widehat{\psi}_k$, and $[L(Q_k) : L] \leq 2^{k-1}$. The residue field of y_k is contained in $L(Q_k)$, so

$$\deg y_k \leq 6 \cdot 3 \cdot 2^{k-1} \cdot 2^{k-1} = 6 \cdot 3 \cdot 4^{k-1} = 6\,\frac{D_{37 \cdot 2^k}}{D_{37}} = \frac{D_{37 \cdot 2^k}}{114},$$

as $D_{37 \cdot 2^k}/D_{37} = 3 \cdot 4^{k-1}$ and $D_{37} = 684$. On the other hand, Theorem 1.3 a) with $\ell = 3$ gives $\delta(X_1(37 \cdot 2^k)) \geq D_{37 \cdot 2^k}/96$. Hence y_k is sporadic.

It remains to show that the j-invariants $j(E_k)$, $k \geq 0$, are pairwise distinct. Suppose $j(E_i) = j(E_k)$ with $0 \leq i < k$. The isogeny $E_i \to E_k$ induced by ψ_k has kernel C_k/C_i, which is cyclic of order $2^{k-i} > 1$. Composing it with an isomorphism $E_k \to E_i$ we obtain an endomorphism of E_i with cyclic kernel of order 2^{k-i}. As E_i is isogenous to E_0, it does not have complex multiplication, so this endomorphism is multiplication by an integer m, whose kernel $E_i[m]$ is not cyclic for $|m| > 1$. This is a contradiction. □

Remark 6.1. More generally, the proof of [5, Proposition 8.1], with Abramovich's bound replaced by Theorem 1.3 a), shows that the conclusion of [5, Proposition 8.1] holds for every non-CM point $x \in X_1(N)$ with $N \geq 5$ such that

$$\deg x < \frac{(\ell-1)D_N}{12(\ell+1)^2}$$

for some prime $\ell \nmid N$. Indeed, that proof constructs, for a prime $p \mid N$, a point $x' \in X_1(pN)$ with $\deg x' \leq p^2 \deg x = \frac{D_{pN}}{D_N} \deg x$, and $\ell \nmid pN$. Applied to the point x of degree 6 on $X_1(37)$ with $p = 37$, this gives sporadic j-invariants in the isogeny class of 1225.b2 on the curves $X_1(37^k)$.

7. Modular curves with Igusa level structure

In this section p is a prime and all curves are over $\overline{\mathbb{F}}_p$. We use the modular curves in characteristic p defined by Poonen [21, Section 1.2]. For an integer $N \geq 1$ not divisible by p, let $X(N)$ be the smooth projective model of the moduli space of triples (E, P, Q), where (P, Q) is a basis of $E[N]$ with Weil pairing $e_N(P, Q) = \zeta$ for a fixed primitive N-th root of unity ζ. It is the reduction modulo p of $X_{\Gamma(N)}$, and for $N \geq 3$ the map $X(N) \to X(1)$ has degree $D_{\Gamma(N)} = \#\operatorname{SL}_2(\mathbb{Z}/N\mathbb{Z})/2$. For $e \geq 1$, let $X(p^e; N)$ be the smooth projective model of the moduli space of quadruples (E, R, P, Q), where E is ordinary, (P, Q) is as above and R is a generator of the kernel of the Verschiebung $V_{p^e} : E^{(p^e)} \to E$, and put $X(p^0; N) = X(N)$. For $e \geq 1$ we denote by $X(p^e; N) \to X(p^{e-1}; N)$ the map which forgets R if $e = 1$, and which sends R to its image under the Verschiebung $E^{(p^e)} \to E^{(p^{e-1})}$ if $e \geq 2$.

The group $G_{p^eN} = (\mathbb{Z}/p^e\mathbb{Z})^\times \times \operatorname{SL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on $X(p^e; N)$, and the kernel of this action is $\{\pm 1\}$, embedded diagonally. For a subgroup $H \subseteq G_{p^eN}$ containing $\{\pm 1\}$, the map from (the smooth projective model of) $X(p^e; N)/H$ to $X(1)$ has degree $D_H = [G_{p^eN} : H]$. Replacing e and N by $e' \geq e$ and a multiple N' of N not divisible by p, and H by its inverse image in $G_{p^{e'}N'}$, does not change the curve $X(p^e; N)/H$ or D_H. Poonen's modular curves in characteristic p are exactly the curves $X(p^e; N)/H$, and D_H is the index of the corresponding open subgroup of $\mathbb{Z}_p^\times \times \prod_{q \neq p} \operatorname{SL}_2(\mathbb{Z}_q)$ [21, Section 1.2]. The curves with $e = 0$ are the reductions modulo p of the curves X_Γ of level not divisible by p, and those with $N = 1$ are the quotients of the Igusa curves.

Lemma 7.1. *Let $N \geq 3$ be an integer not divisible by p and let $e \geq 1$.*

a) *The subgroup $(\mathbb{Z}/p^e\mathbb{Z})^\times \times \{1\}$ of G_{p^eN} acts faithfully on $X(p^e; N)$, and the map $X(p^e; N) \to X(N)$ forgetting R is the quotient by this subgroup. It is étale above the ordinary points of $X(N)$ and totally ramified above the supersingular points.*

b) *If $e \geq 2$, then the map $X(p^e; N) \to X(p^{e-1}; N)$ is the quotient by the kernel of the reduction map $(\mathbb{Z}/p^e\mathbb{Z})^\times \to (\mathbb{Z}/p^{e-1}\mathbb{Z})^\times$, which has order p, and its different exponent at each point above a supersingular point of $X(N)$ is $(p-1)p^{2e-2}$.*

Proof. Since $N \geq 3$, we have $-I \neq I$ in $\operatorname{SL}_2(\mathbb{Z}/N\mathbb{Z})$, so the subgroup $(\mathbb{Z}/p^e\mathbb{Z})^\times \times \{1\}$ meets the diagonal $\{\pm 1\}$ trivially, and the action is faithful. For an ordinary elliptic curve E the kernel of V_{p^e} is cyclic of order p^e, so $(\mathbb{Z}/p^e\mathbb{Z})^\times$ acts simply transitively on its generators. The Verschiebung $E^{(p^e)} \to E^{(p^{e-1})}$ maps it onto the kernel of $V_{p^{e-1}}$, and its kernel has order p, so two generators R and R' have the same image if and only if $R' = aR$ with $a \equiv 1 \pmod{p^{e-1}}$. This identifies the two maps with the quotient maps. The remaining

statements of a) are [14, Corollary 12.6.2], and the different exponent in b) is [14, Lemma 12.9.3] with $n = e - 1$. □

Lemma 7.2. *Let $N \geq 3$ be an integer not divisible by p. Then $X(N)$ has exactly $(p-1)D_{\Gamma(N)}/12$ supersingular points.*

Proof. Let E be a supersingular elliptic curve over $\overline{\mathbb{F}}_p$. Since $N \geq 3$, the group $\mathrm{Aut}(E)$ acts freely on the $\#\,\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = 2D_{\Gamma(N)}$ bases (P, Q) of $E[N]$ with $e_N(P, Q) = \zeta$, so there are $2D_{\Gamma(N)}/\#\,\mathrm{Aut}(E)$ points of $X(N)$ above $j(E)$. The claim follows from 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 $\overline{\mathbb{F}}_p$. □

The following lemma is where the wild ramification of the Igusa tower enters.

Lemma 7.3. *Let $N \geq 3$ be an integer not divisible by p, let $r \geq 1$, and let h be a function on $X(p^r; N)$ which is not the pullback of a function on $X(p^{r-1}; N)$. Then*

$$\deg h \geq \frac{(p-1)p^{2r-2}}{24} D_{\Gamma(N)}.$$

Proof. Put $s = (p-1)D_{\Gamma(N)}/12$. By Lemma 7.1 a) and Lemma 7.2, there are exactly s points $y_1, \ldots, y_s$ of $X(p^r; N)$ above the supersingular points of $X(N)$. By Lemma 7.1, the map $X(p^r; N) \to X(p^{r-1}; N)$ is the quotient by a subgroup A of $(\mathbb{Z}/p^r\mathbb{Z})^\times$, which fixes every y_j. Since h is not the pullback of a function on $X(p^{r-1}; N)$, there is $\sigma \in A$ with $h \circ \sigma \neq h$. Put $i = 1$ if $r = 1$ and $i = p^{2r-2}$ if $r \geq 2$.

We claim that $v_{y_j}(t \circ \sigma - t) \geq i$ for every j, where t is a uniformizer at y_j. For $r = 1$ this holds since $\sigma(y_j) = y_j$. Suppose $r \geq 2$. Then A has order p and is the inertia group at y_j. Its ramification groups are subgroups of A, so each of them is either A or trivial, and hence $v_{y_j}(t \circ \tau - t)$ takes the same value for all $\tau \in A$ with $\tau \neq 1$. By Hilbert's formula [23, Chapter IV, Proposition 4], the different exponent at y_j is $p-1$ times this value, so the value is p^{2r-2} by Lemma 7.1 b).

Composing h with an automorphism of $\mathbb{P}^1$, which changes neither its degree nor the fact that $h \circ \sigma \neq h$, we may assume that $h(y_j) \neq \infty$ for all j. Then $h = \sum_{n \geq 0} a_n t^n$ in the completed local ring $\overline{\mathbb{F}}_p[[t]]$ at y_j, and $h \circ \sigma = \sum_{n \geq 0} a_n (t \circ \sigma)^n$. Since $(t \circ \sigma)^n - t^n$ is divisible by $t \circ \sigma - t$, the non-zero function $h \circ \sigma - h$ vanishes to order at least i at every y_j. Every pole of $h \circ \sigma - h$ is a pole of $h \circ \sigma$ or of h, so it has at most $2 \deg h$ poles, counted with multiplicity, and hence at most $2 \deg h$ zeros. It follows that $si \leq 2 \deg h$, which is the claim. □

Corollary 7.4. *Let $N \geq 3$ be an integer not divisible by p and let $e \geq 1$. Then every non-constant function on $X(p^e; N)$ of degree less than $\varphi(p^e)D_{\Gamma(N)}/24$, where φ is Euler's function, is the pullback of a function on $X(N)$.*

Proof. Let f be a non-constant function on $X(p^e; N)$ which is not the pullback of a function on $X(N)$, and let $r \geq 1$ be the least integer such that f is the pullback of a function h on $X(p^r; N)$. Then h is not the pullback of a function on $X(p^{r-1}; N)$, and the map $X(p^e; N) \to X(p^r; N)$ has degree $\varphi(p^e)/\varphi(p^r) = p^{e-r}$, so by Lemma 7.3

$$\deg f = p^{e-r} \deg h \geq p^{e-r} \frac{(p-1)p^{2r-2}}{24} D_{\Gamma(N)} = \varphi(p^e)\, p^{r-1} \frac{D_{\Gamma(N)}}{24} \geq \varphi(p^e) \frac{D_{\Gamma(N)}}{24}.$$

□

Theorem 7.5. *Let $e \geq 0$, let $N \geq 1$ be an integer not divisible by p, and let $H \subseteq G_{p^e N}$ be a subgroup containing $\{\pm 1\}$. Then*

$$\operatorname{gon}_{\overline{\mathbb{F}}_p}\big(X(p^e;N)/H\big) \geq \frac{p-1}{12(p^2+1)} D_H.$$

Proof. We may replace N by a multiple $N' \geq 3$ not divisible by p and H by its inverse image in $G_{p^e N'}$, so we may assume that $N \geq 3$. Put $D = D_{\Gamma(N)}$ and $c = (p-1)/(12(p^2+1))$, and note that $c \leq 1/60$. By Theorem 1.2 with $\Gamma = \Gamma(N)$ and $\ell = p$, we have $\operatorname{gon}_{\overline{\mathbb{F}}_p} X(N) \geq cD$. We claim that $\operatorname{gon}_{\overline{\mathbb{F}}_p} X(p^e;N) \geq c\varphi(p^e)D$. For $e = 0$ this is the previous inequality. Suppose $e \geq 1$. A non-constant function on $X(p^e;N)$ which is the pullback of a function on $X(N)$ has degree at least $\varphi(p^e)\operatorname{gon}_{\overline{\mathbb{F}}_p} X(N) \geq c\varphi(p^e)D$, and any other non-constant function has degree at least $\varphi(p^e)D/24 > c\varphi(p^e)D$ by Corollary 7.4, which proves the claim.

The group $G_{p^e N}$ has order $2\varphi(p^e)D$, and H contains the kernel $\{\pm 1\}$ of its action, so the map $X(p^e;N) \to X(p^e;N)/H$ has degree $\#H/2 = \varphi(p^e)D/D_H$. Pulling back a function of degree $\operatorname{gon}_{\overline{\mathbb{F}}_p}(X(p^e;N)/H)$ along this map, we obtain

$$\operatorname{gon}_{\overline{\mathbb{F}}_p} X(p^e;N) \leq \frac{\varphi(p^e)D}{D_H} \operatorname{gon}_{\overline{\mathbb{F}}_p}\big(X(p^e;N)/H\big), \tag{7.1}$$

and the theorem follows from the claim. □

Using the upper bound for the gonality of $X(N)$ coming from its genus, we obtain an exact formula.

Proposition 7.6. *Let $N \geq 4$ be an integer not divisible by p.*

a) *For every $e \geq 1$ we have*

$$\operatorname{gon}_{\overline{\mathbb{F}}_p} X(p^e;N) = \varphi(p^e)\operatorname{gon}_{\overline{\mathbb{F}}_p} X(N).$$

If $N \geq 5$, then every function of degree $\operatorname{gon}_{\overline{\mathbb{F}}_p} X(p^e;N)$ on $X(p^e;N)$ is the pullback of a function on $X(N)$.

b) *For every $e \geq 0$ and every subgroup $H \subseteq G_{p^e N}$ containing $\{\pm 1\}$ we have*

$$\frac{\operatorname{gon}_{\overline{\mathbb{F}}_p}\big(X(p^e;N)/H\big)}{D_H} \geq \frac{\operatorname{gon}_{\overline{\mathbb{F}}_p} X(N)}{D_{\Gamma(N)}}.$$

Proof. Put $D = D_{\Gamma(N)}$. We first show that $\operatorname{gon}_{\overline{\mathbb{F}}_p} X(N) \leq D/24$, with strict inequality if $N \geq 5$. The image of $\Gamma(N)$ in $\mathrm{PSL}_2(\mathbb{Z})$ has no elliptic elements, and it has $u = D/N$ cusps, all of width N. Since $X_{\Gamma(N)}$ has good reduction at p [7], the genus of $X(N)$ is $g = 1 + D/12 - u/2$ [24, Proposition 1.40]. Hence $(g+3)/2 \leq D/24$ if and only if $u \geq 8$, with equality if and only if $u = 8$. If $N = 4$, then $D = 24$ and $g = 0$, so $\operatorname{gon}_{\overline{\mathbb{F}}_p} X(N) = 1 = D/24$. If $N = 5$, then $u = 12$, and if $N \geq 6$, then

$$u = \frac{N^2}{2}\prod_{q \mid N}\left(1 - \frac{1}{q^2}\right) > \frac{N^2}{2} \cdot \frac{6}{\pi^2} > 8.$$

As $\operatorname{gon}_{\overline{\mathbb{F}}_p} X(N) \leq \lfloor (g+3)/2 \rfloor$ [21, Proposition A.1 (v)], this proves the claim.

a) Pulling back a function of degree $\operatorname{gon}_{\overline{\mathbb{F}}_p} X(N)$, we see that $\operatorname{gon}_{\overline{\mathbb{F}}_p} X(p^e;N) \leq \varphi(p^e)\operatorname{gon}_{\overline{\mathbb{F}}_p} X(N)$. A non-constant function on $X(p^e;N)$ which is the pullback of a function on $X(N)$ has degree at least $\varphi(p^e)\operatorname{gon}_{\overline{\mathbb{F}}_p} X(N)$, and any other non-constant

function has degree at least $\varphi(p^e)D/24$ by Corollary 7.4. By the claim, this is at least $\varphi(p^e)\operatorname{gon}_{\overline{\mathbb{F}}_p} X(N)$, with strict inequality if $N \geq 5$, which proves a).

b) The inequality (7.1) from the proof of Theorem 7.5 is b) for $e = 0$, and together with a) it gives b) for $e \geq 1$. □

Remark 7.7. a) For $p \neq 5$ the curve $X(5)$ has genus 0 and $D_{\Gamma(5)} = 60$, so $\operatorname{gon}_{\overline{\mathbb{F}}_p} X(p^e;5) \leq \varphi(p^e)$, while $D_{\{\pm 1\}} = 60\varphi(p^e)$ for $H = \{\pm 1\}$. For $p \in \{2,3\}$ the constant in Theorem 7.5 is $1/60$, so $\operatorname{gon}_{\overline{\mathbb{F}}_p} X(p^e;5) = \varphi(p^e)$, and the bound of Theorem 7.5 is sharp for $p \in \{2,3\}$ at every Igusa level p^e.

b) By Proposition 7.6 b), applied after replacing N by a multiple $N' \geq 4$ not divisible by p, for each prime p the infimum of $\operatorname{gon}_{\overline{\mathbb{F}}_p}(X(p^e;N)/H)/D_H$ over all e, N and H is equal to the infimum over the curves with $e = 0$, i.e. the modular curves of level not divisible by p. Hence a linear lower bound with a constant independent of p, as expected by Poonen [21, Section 1.2], would follow from such a bound for the modular curves of level not divisible by the characteristic.

c) Poonen proved a function field analogue of the uniform boundedness of torsion of elliptic curves [21, Theorem 1.4]: there is a constant $N_{p,d}$ such that for every field k of characteristic p, every field K of degree at most d over $k(t)$ and every elliptic curve E over K with $j(E)$ not algebraic over k, the group $\rho_E(\operatorname{Gal}(K^s/K)) \cap S$ has index at most $N_{p,d}$ in $S = \mathbb{Z}_p^\times \times \prod_{q \neq p} \operatorname{SL}_2(\mathbb{Z}_q)$. Here K^s is a separable closure of K, and ρ_E describes the action of $\operatorname{Gal}(K^s/K)$ on $\varprojlim \ker V_{p^e}$ and on the q-adic Tate modules of E (with GL_2 in place of SL_2 the index can be infinite [21, Remark 1.6]). His proof requires only that $N_{p,d} \geq 2D_H$ for all the curves $X(p^e;N)/H$ of gonality at most d [21, Section 7], so by Theorem 7.5 one can take

$$N_{p,d} = \left\lfloor \frac{24(p^2+1)}{p-1} d \right\rfloor.$$

d) For the curves with $N = 1$, Poonen deduced the better bound $\operatorname{gon}_{\overline{\mathbb{F}}_p}(X(p^e;1)/H) > D_H/12$ [21, Corollary 4.2] from results of Schweizer [22, Lemma 1.5], among them the equality $\operatorname{gon}_{\overline{\mathbb{F}}_p} \operatorname{Ig}(p^e) = p \operatorname{gon}_{\overline{\mathbb{F}}_p} \operatorname{Ig}(p^{e-1})$ for the Igusa curves $\operatorname{Ig}(p^e)$, where $e \geq 2$ and $p^e \notin \{4, 8, 9, 25\}$ (see [21, Theorem 4.1]). Proposition 7.6 a) is an analogue of this equality for the curves $X(p^e;N)$ with $N \geq 4$.

References

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

[2] M. H. Baker, E. González-Jiménez, J. González, and B. Poonen, *Finiteness results for modular curves of genus at least 2*, Amer. J. Math., 127 (2005), pp. 1325–1387. 3, 3, 3

[3] 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, 1

[4] 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

[5] A. Bourdon and F. Najman, *Sporadic points of odd degree on $X_1(N)$ coming from $\mathbb{Q}$-curves*, Algebra Number Theory, 20 (2026), pp. 1901–1936. 1, 1, 6.1

[6] 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

[7] 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. 2, 7
[8] M. Derickx, S. Hashimoto, F. Najman, and A. Shnidman, *Rational points on modular curves: parameterization and geometric explanations*. Preprint, https://arxiv.org/abs/2602.20964v2, 2026. 1
[9] M. Derickx and M. Stoll, *Prime order torsion on elliptic curves over number fields. Part I: asymptotics*, 2026. preprint, https://arxiv.org/abs/2505.14109v2. 1, 1, 3.6, 4.5
[10] M. Derickx and M. van Hoeij, *Gonality of the modular curve $X_1(N)$*, J. Algebra, 417 (2014), pp. 52–71. 1, 1, 3.5
[11] 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. 4
[12] G. Frey, *Curves with infinitely many points of fixed degree*, Israel J. Math., 85 (1994), pp. 79–83. 1
[13] B. Kadets and I. Vogt, *Subspace configurations and low degree points on curves*, Adv. Math., 460 (2025), p. 110021. 1
[14] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, vol. 108 of Annals of Mathematics Studies, Princeton University Press, Princeton, NJ, 1985. 7
[15] 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. 1
[16] S. L. Kleiman, *The Picard scheme*. In: Fundamental algebraic geometry, Math. Surveys Monogr. 123, Amer. Math. Soc., 2005; we use the numbering of https://arxiv.org/abs/math/0504020v1, 2005. 4
[17] LMFDB Collaboration, *The L-functions and modular forms database*. https://www.lmfdb.org. 4.4
[18] F. 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
[19] ———, *Isolated and sporadic points on $X_1(N)$ and $X_0(N)$*, 2026. preprint, https://hexagonmath.org/2611.00884v1. 1
[20] F. Najman and P. Orlić, *Gonality of the modular curve $X_0(N)$*, Math. Comp., 93 (2024), pp. 863–886. 2
[21] B. Poonen, *Gonality of modular curves in characteristic p*, Math. Res. Lett., 14 (2007), pp. 691–701. 1, 1, 3, 3, 4, 7, 7, 7.7
[22] A. Schweizer, *On the p^e-torsion of elliptic curves and elliptic surfaces in characteristic p*, Trans. Amer. Math. Soc., 357 (2005), pp. 1047–1059. 7.7
[23] J.-P. Serre, *Local fields*, vol. 67 of Graduate Texts in Mathematics, Springer-Verlag, New York-Berlin, 1979. 7
[24] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, vol. 11 of Publications of the Mathematical Society of Japan, Princeton University Press, Princeton, NJ, 1971. 7
[25] G. Smith and I. Vogt, *Low degree points on curves*, Int. Math. Res. Not. IMRN, (2022), pp. 422–445. 1
[26] The Stacks project authors, *The Stacks project*. https://stacks.math.columbia.edu, 2026. 4
[27] 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
[28] B. Viray and I. Vogt, *Isolated and parameterized points on curves*, Essent. Number Theory, 5 (2026), pp. 1–47. 1
[29] P. G. Zograf, *Small eigenvalues of automorphic Laplacians in spaces of parabolic forms*, J. Soviet Math., 36 (1987), pp. 106–114. 1
[30] D. Zywina, *Classification of modular curves with low gonality*. Preprint, https://davidzywina.github.io/papers/lowgonality.pdf, 2025. 1, 1

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