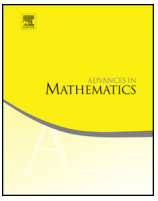
Advances in Mathematics 357 (2019) 106824

Contents lists available at ScienceDirect

Advances in Mathematics

www.elsevier.com/locate/aim



On the level of modular curves that give rise to isolated j-invariants

Abbey Bourdon [a,*], Özlem Ejder [b], Yuan Liu [c], Frances Odumodu [d,e], Bianca Viray [f]

[a] *Wake Forest University, Department of Mathematics and Statistics, Winston-Salem, NC 27109, USA*
[b] *Colorado State University, Department of Mathematics, Fort Collins, CO 80524, USA*
[c] *University of Michigan, Department of Mathematics, Ann Arbor, MI 48109, USA*
[d] *Institut de Mathématiques de Bordeaux, Université de Bordeaux, 351 cours de la Libération, 33405 Talence cedex, France*
[e] *Dipartimento di Matematica Pura ed Applicata, Università degli Studi di Padova, Via Trieste 63, 35121, Padova, Italy*
[f] *University of Washington, Department of Mathematics, Box 354350, Seattle, WA 98195, USA*

ARTICLE INFO

Article history:
Received 15 November 2018
Received in revised form 21 August 2019
Accepted 11 September 2019
Available online 9 October 2019
Communicated by Kartik Prasanna

Keywords:
Isolated points
Sporadic points
Modular curves
Serre's uniformity conjecture
Faltings's theorem

ABSTRACT

We say a closed point x on a curve C is sporadic if C has only finitely many closed points of degree at most $\deg(x)$ and that x is isolated if it is not in a family of effective degree d divisors parametrized by $\mathbb{P}^1$ or a positive rank abelian variety (see Section 4 for more precise definitions and a proof that sporadic points are isolated). Motivated by well-known classification problems concerning rational torsion of elliptic curves, we study sporadic and isolated points on the modular curves $X_1(N)$. In particular, we show that any non-cuspidal non-CM sporadic, respectively isolated, point $x \in X_1(N)$ maps down to a sporadic, respectively isolated, point on a modular curve $X_1(d)$, where d is bounded by a constant depending only on $j(x)$. Conditionally, we show that d is bounded by a constant

* Corresponding author.
E-mail addresses: bourdoam@wfu.edu (A. Bourdon), ejder@math.colostate.edu (Ö. Ejder), yyyliu@umich.edu (Y. Liu), francesodumodu@gmail.com (F. Odumodu), bviray@uw.edu (B. Viray).
URLs: http://users.wfu.edu/bourdoam/ (A. Bourdon), https://sites.google.com/site/ozheidi/Home (Ö. Ejder), https://sites.google.com/view/yuanliu-homepage (Y. Liu), http://math.washington.edu/~bviray (B. Viray).

https://doi.org/10.1016/j.aim.2019.106824

Merel's uniform boundedness theorem

depending only on the degree of $\mathbb{Q}(j(x))$, so in particular there are only finitely many j-invariants of bounded degree that give rise to sporadic or isolated points.

1. Introduction

Let E be an elliptic curve over a number field k. It is well-known that the torsion subgroup $E(k)_{\text{tors}}$ is a finite subgroup of $(\mathbb{Q}/\mathbb{Z})^2$. In 1996, Merel [35], building on work of Mazur [34] and Kamienny [24], proved the landmark uniform boundedness theorem: that for any positive integer d, there exists a constant $B = B(d)$ such that for all number fields k of degree at most d and all elliptic curves E/k,

$$\#E(k)_{\text{tors}} \leq B(d).$$

Merel's theorem can equivalently be phrased as a statement about closed points on modular curves: that for any positive integer d, there exists a constant $B' = B'(d)$ such that for $n > B'$, the modular curve $X_1(n)/\mathbb{Q}$ has no non-cuspidal degree d points.

Around the same time as Merel's work, Frey [19] observed that Faltings's theorem implies that an arbitrary curve C over a number field k can have infinitely many points of degree at most d if and only if these infinitely many points are parametrized by $\mathbb{P}^1_k$ or a positive rank subabelian variety of $\text{Jac}(C)$.[1] From this, Frey deduced that if a curve C/k has infinitely many degree d-points, then the k-gonality of the curve[2] must be at most $2d$. Frey's criterion combined with Abramovich's lower bound on the gonality of modular curves [1] immediately shows that there exists a (computable!) constant $B'' = B''(d)$ such that for $n > B''$, the modular curve $X_1(n)/\mathbb{Q}$ has only finitely many degree d points, or in other words, that for $n > B''$ all degree d points on $X_1(n)$ are sporadic.[3] Thus, the strength of the uniform boundedness theorem is in controlling the existence of sporadic points of bounded degree on $X_1(n)$ as n tends to infinity.

In this paper, we study sporadic points and, more generally, isolated[4] points of arbitrary degree, focusing particularly on such points corresponding to non-CM elliptic curves. We prove that non-CM non-cuspidal sporadic, respectively isolated, points on $X_1(n)$ map to sporadic, respectively isolated, points on $X_1(d)$, for d some bounded divisor of n.

[1] While Frey assumes that C has a k-point, an inspection of the proof reveals that this is needed only to obtain a k-morphism $\text{Sym}^d(C) \to \text{Jac}(C)$. Since the existence of a degree d point also guarantees the existence of a suitable such morphism, the hypothesis on the existence of a rational point can be removed.

[2] The k-gonality of a curve C is the minimal degree of a k-rational map $\phi\colon C \to \mathbb{P}^1_k$.

[3] A closed point x on a curve C is sporadic if C has only finitely many points of degree at most $\deg(x)$.

[4] A closed point x on a curve C is isolated if it is not contained in a family of effective degree d divisors parametrized by $\mathbb{P}^1$ or a positive rank abelian variety. See Definition 4.1 for more details.

Theorem 1.1. *Fix a non-CM elliptic curve E over k, and let m be an integer divisible by $2, 3$ and all primes ℓ where the ℓ-adic Galois representation of E is not surjective. Let $M = M(E, m)$ be the level of the m-adic Galois representation of E and let f denote the natural map $X_1(n) \to X_1(\gcd(n, M))$. If $x \in X_1(n)$ is sporadic, respectively isolated, with $j(x) = j(E)$, then $f(x) \in X_1(\gcd(n, M))$ is sporadic, respectively isolated.*

For many elliptic curves, we may take both m and M to be quite small. For instance, let $\mathcal{E}$ be the set of elliptic curves over $\mathbb{Q}$ where the ℓ-adic Galois representation is surjective for all $\ell > 3$ and where the 6-adic Galois representation has level dividing 24. Note that $\mathcal{E}$ contains all Serre curves [40, Proof of Prop. 22] (that is, elliptic curves over $\mathbb{Q}$ whose adelic image is of index 2 in $\mathrm{GL}_2(\hat{\mathbb{Z}})$, which is as large as possible) and hence contains almost all elliptic curves over $\mathbb{Q}$ when counted according to height [23, Theorem 4]. For $E \in \mathcal{E}$, we may apply Theorem 1.1 with $m = 6$ and $M|24$.

The curve $X_1(24)$ has infinitely many quartic points, but no rational or quadratic points, nor cubic points corresponding to elliptic curves over $\mathbb{Q}$ [34,25,36]. Therefore $X_1(24)$ has no sporadic points with $\mathbb{Q}$-rational j-invariant. For M a proper divisor of 24, the curves $X_1(M)$ have genus 0, and so also have no sporadic points. Hence Theorem 1.1 yields the following corollary.

Corollary 1.2. *For all n, there are no sporadic points on $X_1(n)$ corresponding to elliptic curves in $\mathcal{E}$. In particular, there are no sporadic points corresponding to Serre curves.*

In addition to giving strong control on sporadic points over a fixed j-invariant, we are also able to use Theorem 1.1 to derive a uniform version that is conditional on a folklore conjecture motivated by a question of Serre.

Conjecture 1.3 *(Uniformity conjecture). Fix a number field k. There exists a constant $C = C(k)$ such that for all non-CM elliptic curves E/k, the mod-ℓ Galois representation of E is surjective for all $\ell > C$.*

Conjecture 1.4 *(Strong uniformity conjecture). Fix a positive integer d. There exists a constant $C = C(d)$ such that for all degree d number fields k and all non-CM elliptic curves E/k, the mod-ℓ Galois representation of E is surjective for all $\ell > C$.*

Remark 1.5. Conjecture 1.3 when $k = \mathbb{Q}$, or equivalently Conjecture 1.4 when $d = 1$, is the case originally considered by Serre [40, §4.3]. In this case, Serre asked whether C could be taken to be 37 [41, p. 399]. The choice $C = 37$ has been formally conjectured by Zywina [50, Conj. 1.12] and Sutherland [44, Conj. 1.1].

Theorem 1.6. *Assume Conjecture 1.3. Then for any number field k, there exists a positive integer $M = M(k)$ such that if $x \in X_1(n)$ is a non-cuspidal, non-CM sporadic, respectively isolated, point with $j(x) \in k$, then $\pi(x) \in X_1(\gcd(n, M))$ is a sporadic, respectively*

isolated, point. Moreover, if the stronger Conjecture 1.4 holds, then M depends only on $[k : \mathbb{Q}]$.

We call a point $j \in X_1(1) \cong \mathbb{P}^1$ an isolated j-invariant if it is the image of an isolated point on $X_1(n)$, for some positive integer n. Since any curve only has finitely many isolated points (see Theorem 4.2(2)) and there are only finitely many CM j-invariants of bounded degree, we immediately obtain the following corollary.

Corollary 1.7. *Fix a number field k.*

a) *Assume Conjecture 1.3. There are finitely many k-rational isolated j-invariants.*
b) *Assume Conjecture 1.4. There are finitely many isolated j-invariants of bounded degree.*

The integer M in Theorem 1.6 depends on the constant $C(k)$ or $C(d)$ from Conjecture 1.3 or Conjecture 1.4, respectively, and also depends on a uniform bound for the level of the ℓ-adic Galois representation for all $\ell \leq C(k)$, respectively $C(d)$. The existence of this latter bound depends on Faltings's Theorem and as such is ineffective. However, in the case when $k = \mathbb{Q}$, it is possible to make a reasonable guess for M. This is discussed more in Section 8.

1.1. Prior work

CM elliptic curves provide a natural class of examples of sporadic points due to fundamental constraints on the image of the associated Galois representation. Indeed, Clark, Cook, Rice, and Stankewicz show that there exist sporadic points corresponding to CM elliptic curves on $X_1(\ell)$ for all sufficiently large primes ℓ [8]. Sutherland has extended this argument to include composite integers [46].

In the non-CM case, all known results on sporadic points have arisen from explicit versions of Merel's theorem for low degree. For instance, in studying cubic points on $\cup_{n\in\mathbb{N}} X_1(n)$, Najman identified two degree 3 sporadic points on $X_1(21)$ all corresponding to the same non-CM elliptic curve with rational j-invariant [37]. Derickx, Etropolski, van Hoeij, Morrow, and Zureick-Brown are currently classifying all degree 3 non-cuspidal non-CM sporadic points on $X_1(n)$, and preliminary results suggest that these examples of Najman are the only examples [14]. Work of van Hoeij [49], Derickx–van Hoeij [15], and Derickx–Sutherland [16] show that there are additional sporadic points, e.g., degree 5 points on $X_1(28)$ and $X_1(30)$ and a degree 6 point on $X_1(37)$.

There are also examples of isolated points that are not sporadic. Derickx and van Hoeij [15] have shown $X_1(25)$ has a (nonempty) finite collection of points of degree $d = 6$ and $d = 7$. These points are isolated by Theorem 4.2, but not sporadic since the $\mathbb{Q}$-gonality of $X_1(25)$ is 5. In general, having infinitely points on a curve of degree d does not preclude the existence of isolated points of degree d: see [43,6,21,5] for some examples.

1.2. Outline

We set notation and review relevant background in Section 2. In Section 3 we record results about subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ that will be useful in later proofs; in particular, Proposition 3.7 is useful for determining the level of an m-adic Galois representation from information about the ℓ-adic representations. In Section 4, we prove a general criterion for the images of sporadic or isolated points to remain sporadic or isolated (Theorem 4.3); this result is likely of independent interest. In Section 5, we study isolated points on modular curves over a fixed non-CM j-invariant and prove Theorem 1.1. This is then used in Section 6 to prove Theorem 1.6.

Theorem 1.6 implies that, assuming Conjecture 1.4, there are finitely many isolated j-invariants of bounded degree. This raises two interesting questions:

(1) Are there finitely many isolated *points* lying over j-invariants of bounded degree, or can there be infinitely many isolated points over a single j-invariant?
(2) In the case of degree 1, when there is strong evidence for Conjecture 1.4, can we come up with a candidate list for the rational isolated j-invariants?

Question 1 is the focus of Section 7, where we show that any CM j-invariant has infinitely many isolated (and in fact, sporadic!) points lying over it. Section 8 focuses on Question 2; there we provide a candidate list of levels from which the rational isolated j-invariants can be found.

Acknowledgments

This project was started at the Women in Numbers 4 conference, which was held at the Banff International Research Station. We thank BIRS for the excellent working conditions and the organizers, Jennifer Balakrishnan, Chantal David, Michelle Manes, and the last author, for their support. We also thank the other funders of the conference: the Association for Women in Mathematics (NSF ADVANCE grant HRD-1500481), the Clay Mathematics Institute, Microsoft Research, the National Science Foundation (NSF grant DMS-1712938), the Number Theory Foundation, and the Pacific Institute for Mathematics Sciences.

We thank Jeremy Rouse, Drew Sutherland, and David Zureick-Brown for helpful conversations. We also thank Nigel Boston, Pete L. Clark, Loïc Merel, Filip Najman, Paul Pollack, and the anonymous referees for comments on an earlier draft. The third author was partially supported by NSF grants DMS-1652116 and DMS-1301690 and the last author was partially supported by NSF CAREER grant DMS-1553459.

2. Background and notation

2.1. Conventions

Throughout, k denotes a number field, $\overline{\mathbb{Q}}$ denotes a fixed algebraic closure of $\mathbb{Q}$, and Gal_k denotes the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$.

We use ℓ to denote a prime number and $\mathbb{Z}_\ell$ to denote the ℓ-adic integers. For any positive integer m, we write $\mathrm{Supp}(m)$ for the set of prime divisors of m and write $\mathbb{Z}_m := \prod_{\ell \in \mathrm{Supp}(m)} \mathbb{Z}_\ell$. We use S to denote a set of primes, typically finite; when S is finite, we write $\mathfrak{m}_S := \prod_{\ell \in S} \ell$.

For any subgroup G of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ and any positive integer n, we write G_n and G_{n^∞}, respectively for the images of G under the projections

$$\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \quad \text{and} \quad \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}_n).$$

In addition, for any positive integer m relatively prime to n we write $G_{n \cdot m^\infty}$ for the image of G under the projection

$$\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}_m).$$

Throughout, we will abuse notation and use π to denote any natural projection map among the groups G, G_{n^∞}, and G_n.

By curve we mean a projective nonsingular geometrically integral 1-dimensional scheme over a field. For a curve C, we write $\mathbf{k}(C)$ for the function field of C and Pic_C for the Picard scheme of C. For any non-negative integer d, we write Pic^d_C for the connected component of Pic_C consisting of divisor classes of degree d and $\mathrm{Sym}^d C$ for the dth symmetric product of C, i.e., C^d/S_d. If C is defined over the field K, we use $\mathrm{gon}_K(C)$ to denote the K-gonality of C, which is the minimum degree of a dominant morphism $C \to \mathbb{P}^1_K$. If x is a closed point of C, we denote the residue field of x by $\mathbf{k}(x)$ and define the degree of x to be the degree of the residue field $\mathbf{k}(x)$ over K. A point x on a curve C/K is sporadic if there are only finitely many points $y \in C$ with $\deg(y) \leq \deg(x)$. We also consider other related properties of a closed point on a curve: isolated, $\mathbb{P}^1$-isolated, and AV-isolated; these terms are defined in Section 4.

We use E to denote an elliptic curve, i.e., a curve of genus 1 with a specified point O. Unless stated otherwise, we will consider only elliptic curves defined over number fields. We say that an elliptic curve E over a field K has complex multiplication, or CM, if the geometric endomorphism ring is strictly larger than $\mathbb{Z}$. Given an elliptic curve E over a number field k, an affine model of E is given by a short Weierstrasss equation $y^2 = x^3 + Ax + B$ for some $A, B \in k$. Then the j-invariant of E is $j(E) := 1728\frac{4A^3}{4A^3+27B^2}$ and uniquely determines the geometric isomorphism class of E. For a positive integer n, we write $E[n]$ for the subgroup of E consisting of points of order at most n.

2.2. Modular curves

For a positive integer n, let

$$\Gamma_1(n) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{n},\ a \equiv d \equiv 1 \pmod{n} \right\}.$$

The group $\Gamma_1(n)$ acts on the upper half plane $\mathbb{H}$ via linear fractional transformations, and the points of the Riemann surface

$$Y_1(n) \coloneqq \mathbb{H}/\Gamma_1(n)$$

correspond to $\mathbb{C}$-isomorphism classes of elliptic curves with a distinguished point of order n. That is, a point in $Y_1(n)$ corresponds to an equivalence class of pairs $[(E, P)]$, where E is an elliptic curve over $\mathbb{C}$ and $P \in E$ is a point of order n, and where $(E, P) \sim (E', P')$ if there exists an isomorphism $\varphi\colon E \to E'$ such that $\varphi(P) = P'$. By adjoining a finite number of cusps to $Y_1(n)$, we obtain the smooth projective curve $X_1(n)$. Concretely, we may define the extended upper half plane $\mathbb{H}^* \coloneqq \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$. Then $X_1(n)$ corresponds to the extended quotient $\mathbb{H}^*/\Gamma_1(n)$. In fact, we may view $X_1(n)$ as an algebraic curve defined over $\mathbb{Q}$ (see [17, Section 7.7] or [13] for more details).

2.2.1. Degrees of non-cuspidal algebraic points

If $x = [(E, P)] \in X_1(n)(\overline{\mathbb{Q}})$ is a non-cuspidal point, then the moduli definition implies that $\deg(x) = [\mathbb{Q}(j(E), \mathfrak{h}(P)) : \mathbb{Q}]$, where $\mathfrak{h} : E \to E/\operatorname{Aut}(E) \cong \mathbb{P}^1$ is a Weber function for E. From this we deduce the following lemma:

Lemma 2.1. *Let E be a non-CM elliptic curve defined over the number field $k = \mathbb{Q}(j(E))$, let $P \in E$ be a point of order n, and let $x = [(E, P)] \in X_1(n)$. Then*

$$\deg(x) = c_x[k(P) : \mathbb{Q}],$$

where $c_x = 1/2$ if $2P \neq O$ and there exists $\sigma \in \mathrm{Gal}_k$ such that $\sigma(P) = -P$ and $c_x = 1$ otherwise.

Proof. Let E be a non-CM elliptic curve defined over $k = \mathbb{Q}(j(E))$ and let $\mathfrak{h}$ be a Weber function for E. If $\sigma \in \mathrm{Gal}_{k(\mathfrak{h}(P))}$, then $\sigma(P) = \xi(P)$ for some $\xi \in \operatorname{Aut}(E)$. Thus in the case where $\operatorname{Aut}(E) = \{\pm 1\}$,

$$[k(P) : k(\mathfrak{h}(P))] = 1 \text{ or } 2.$$

If there exists $\sigma \in \mathrm{Gal}_k$ such that $\sigma(P) = -P$, then $[k(P) : k(\mathfrak{h}(P))] = 2$ and $c_x = 1/2$. Otherwise $k(P) = k(\mathfrak{h}(P))$ and $c_x = 1$. □

2.2.2. Maps between modular curves

Proposition 2.2. *For positive integers a and b, there is a natural $\mathbb{Q}$-rational map $f\colon X_1(ab) \to X_1(a)$ with*

$$\deg(f) = c_f \cdot b^2 \prod_{p \mid b,\, p \nmid a} \left(1 - \frac{1}{p^2}\right),$$

where $c_f = 1/2$ *if* $a \leq 2$ *and* $ab > 2$ *and* $c_f = 1$ *otherwise.*

Proof. Since $\Gamma_1(ab) \subset \Gamma_1(a)$, we have a natural map $X_1(ab) \to X_1(a)$ that complex analytically is induced by $\Gamma_1(ab)\tau \mapsto \Gamma_1(a)\tau$ for $\tau \in \mathbb{H}^*$. On non-cuspidal points, this map has the moduli interpretation $[(E, P)] \mapsto [(E, bP)]$, which shows that it is $\mathbb{Q}$-rational. Since $-I \in \Gamma_1(n)$ if and only if $n|2$, the degree computation then follows from the formula [17, p. 66], which states

$$\deg(f) = \begin{cases} [\Gamma_1(a) : \Gamma_1(ab)]/2 & \text{if } -I \in \Gamma_1(a) \text{ and } -I \notin \Gamma_1(ab) \\ [\Gamma_1(a) : \Gamma_1(ab)] & \text{otherwise.} \end{cases}$$ □

2.3. Galois representations of elliptic curves

Let E be an elliptic curve over a number field k. Let n be a positive integer. After fixing two generators for $E(\overline{k})[n]$, we obtain a Galois representation

$$\rho_{E,n} \colon \mathrm{Gal}_k \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Note that the conjugacy class of the image of $\rho_{E,n}$ is independent of the choice of generators. After choosing compatible generators for each n, we obtain a Galois representation

$$\rho_E \colon \mathrm{Gal}_k \to \mathrm{GL}_2(\hat{\mathbb{Z}}) \cong \prod_{\ell} \mathrm{GL}_2(\mathbb{Z}_\ell),$$

which agrees with $\rho_{E,n}$ after reduction modulo n. For any positive integer n we also define

$$\rho_{E,n^\infty} \colon \mathrm{Gal}_k \to \mathrm{GL}_2(\mathbb{Z}_n)$$

to be the composition of ρ_E with the projection onto the ℓ-adic factors for $\ell|n$. Note that ρ_{E,n^∞} depends only on the support of n. We refer to $\rho_{E,n}$, ρ_{E,n^∞}, and ρ_E as the mod n Galois representation of E, the n-adic Galois representation of E, and the adelic Galois representation of E, respectively.

If E/k does not have complex multiplication, then Serre's Open Image Theorem [40] states that $\rho_E(\mathrm{Gal}_k)$ is open—and hence of finite index—in $\mathrm{GL}_2(\hat{\mathbb{Z}})$. Since the kernels of the natural projection maps $\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ form a fundamental system of open neighborhoods of the identity in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ [38, Lemma 2.1.1], it follows that for any open subgroup G of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ there exists $m \in \mathbb{Z}^+$ such that $G = \pi^{-1}(G \mod m)$. Thus Serre's Open Image Theorem can be rephrased in the following way: for any non-CM elliptic curve E/k, there exists a positive integer M such that

$$\operatorname{im}\rho_E = \pi^{-1}(\operatorname{im}\rho_{E,M}).$$

We call the smallest such M the level and denote it M_E. Similarly, for any finite set of primes S, we let $M_E(S)$ be the least positive integer such that $\operatorname{im}\rho_{E,\mathfrak{m}_S^\infty} = \pi^{-1}(\operatorname{im}\rho_{E,M_E(S)})$ and we say that $M_E(S)$ is the level of the $\mathfrak{m}_S$-adic Galois representation.

We also define

$$S_E = S_{E/k} := \{2,3\} \cup \{\ell : \rho_{E,\ell^\infty}(\mathrm{Gal}_k) \not\supset \mathrm{SL}_2(\mathbb{Z}_\ell)\} \cup \{5, \text{ if } \rho_{E,5^\infty}(\mathrm{Gal}_k) \neq \mathrm{GL}_2(\mathbb{Z}_5)\}; \tag{2.1}$$

by Serre's Open Image Theorem, this is a finite set.

For any elliptic curve $E/\mathbb{Q}$ with discriminant Δ_E,[5] Serre observed that the field $\mathbb{Q}(\sqrt{\Delta_E})$ is contained in the 2-division field $\mathbb{Q}(E[2])$ as well as a cyclotomic field $\mathbb{Q}(\mu_n)$ for some n, which in turn is contained in the n-division field $\mathbb{Q}(E[n])$. Thus if $\ell > 2$ is a prime that divides the squarefree part of Δ_E, then 2ℓ must divide the level M_E (see [40, Proof of Prop. 22] for more details). In particular, the level of an elliptic curve can be arbitrarily large. In contrast, for a fixed prime ℓ, the level of the ℓ-adic Galois representation is bounded depending only on the degree of the field of definition.

Theorem 2.3 *([7, Theorem 1.1], see also [9, Theorem 2.3]). Let d be a positive integer and let ℓ be a prime number. There exists a constant $C = C(d,\ell)$ such that for all number fields k of degree d and all non-CM elliptic curves E/k,*

$$[\mathrm{GL}_2(\mathbb{Z}_\ell) : \operatorname{im}\rho_{E,\ell^\infty}] < C.$$

3. Subgroups of $\mathbf{GL_2}(\hat{\mathbb{Z}})$

The proofs in this paper involve a detailed study of the mod-n, ℓ-adic and adelic Galois representations associated to elliptic curves. As such, we use a number of properties of closed subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ and subgroups of $\mathrm{GL}(\mathbb{Z}/n\mathbb{Z})$ that we record here. Throughout G denotes a subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

In Section 3.1, we state Goursat's lemma. In Section 3.2 we show that if $\ell = 5$ and $G_5 = \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$ or if $\ell > 5$ is a prime such that $G_\ell \supset \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$, then for any integer n relatively prime to ℓ, the kernel of the projection $G_{\ell^s n} \to G_n$ is large, in particular, it contains $\mathrm{SL}_2(\mathbb{Z}/\ell^s\mathbb{Z})$. This proof relies on a classification of subquotients of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$: that $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ can contain a subquotient isomorphic to $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$ or $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for $\ell > 5$ only if $5|n$ or $\ell|n$ respectively. This result is known in the case $\ell > 5$ (see [10, Appendix, Corollary 11]), but we are not aware of a reference in the case $\ell = 5$. In Section 3.3 we review results of Lang and Trotter that show that the level of a finite

[5] While the discriminant depends on a Weierstrass model, the class of $\Delta_E \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ is independent of the choice of model. Since we are concerned only with Δ_E mod squares, we allow ourselves this abuse of notation.

index subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ can be bounded by its index. Finally in Section 3.4 we show how to obtain the m-adic level of a group from information of its ℓ-adic components.

3.1. Goursat's lemma

Lemma 3.1 *(Goursat's lemma, see e.g., [27, p. 75] or [20]). Let G, G' be groups and let H be a subgroup of $G \times G'$ such that the two projection maps*

$$\rho\colon H \to G \quad \text{and} \quad \rho'\colon H \to G'$$

are surjective. Let $N \coloneqq \ker(\rho)$ and $N' \coloneqq \ker(\rho')$; one can identify N as a normal subgroup of G' and N' as a normal subgroup of G. Then the image of H in $G/N' \times G'/N$ is the graph of an isomorphism

$$G/N' \simeq G'/N.$$

3.2. Kernels of reduction maps

Proposition 3.2. *Let $\ell \geq 5$ be a prime. Assume that $G_\ell \supset \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ when $\ell > 5$ and $G_\ell = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ when $\ell = 5$. Then $\mathrm{SL}_2(\mathbb{Z}/\ell^s\mathbb{Z}) \subset \ker(G_{\ell^s n} \to G_n)$ for any positive integer n with $\ell \nmid n$.*

For $\ell > 5$, a key ingredient in the proof is a classification result that implies that $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ cannot appear as a subquotient of G_n [10, Appendix, Corollary 11]. This is false when $\ell = 5$ (for instance, there is a subquotient of $\mathrm{GL}_2(\mathbb{Z}/11\mathbb{Z})$ that is isomorphic to $\mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z})$). However, we prove that $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$ cannot be isomorphic to a subquotient of G_n unless $5|n$.

Lemma 3.3. *Let n be a positive integer. If $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ has a subquotient that is isomorphic to $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$, then $5 \mid n$.*

Remark 3.4. Throughout the proof, we freely use the isomorphism $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z}) \cong S_5$ and $\mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z}) \cong A_5$ to deduce information about subgroups and subquotients contained in these groups.

Proof. The lemma is a straightforward consequence of the following 3 claims (Claim (2) is applied to the set $T = \mathrm{Supp}(n)$).

(1) The projection

$$\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \to \prod_{p \in \mathrm{Supp}(n)} \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$$

is an injection when restricted to any subquotient isomorphic to $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$.

(2) Let $\emptyset \neq S \subsetneq T$ be finite sets of primes. If $\prod_{p\in T} \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ has a subquotient isomorphic to $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$ then so does at least one of

$$\prod_{p\in S} \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z}) \quad \text{or} \quad \prod_{p\in T-S} \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z}).$$

Hence, by induction, if $\prod_{p\in T} \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ has a subquotient isomorphic to $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$ then $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ has a subquotient isomorphic to $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$ for some $p \in T$.

(3) If p is a prime and $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ has a subquotient isomorphic to $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$, then $p = 5$.

Proof of Claim 1: Let $N \lhd G < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be subgroups and let π denote the surjective map

$$\pi\colon \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \to \prod_{p\in \mathrm{Supp}(n)} \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z}).$$

Using the isomorphism theorems, we obtain the following

$$\frac{\pi(G)}{\pi(N)} \cong \frac{G/(G\cap \ker\pi)}{N/(N\cap\ker\pi)} \cong \frac{G}{N\cdot(G\cap\ker\pi)} \cong \frac{G/N}{(G\cap\ker\pi)/(N\cap\ker\pi)}. \tag{3.1}$$

For each prime p, the kernel of $\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is a p-group and the kernel of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \to \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is a cyclic group, so $\ker\pi$ is a direct product of solvable groups. Hence $\ker\pi$ is solvable and so is $(G\cap\ker\pi)/(N\cap\ker\pi)$ for any $N \lhd G < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Since the only solvable normal subgroup of $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$ is the trivial group, if $G/N \cong \mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$, then $\pi(G)/\pi(N) \cong G/N$.

Proof of Claim 2: Let $N \lhd G < \prod_{p\in T} \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ be subgroups such that $G/N \cong \mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$. Let H be the normal subgroup of G containing N such that $H/N \cong \mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z})$. Consider the following two maps

$$\pi_S\colon \prod_{p\in T} \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z}) \to \prod_{p\in S} \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z}) \quad \text{and}$$
$$\pi_{S^c}\colon \prod_{p\in T} \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z}) \to \prod_{p\in T-S} \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z}).$$

Since the only quotient of $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$ that contains a subgroup isomorphic to $\mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z})$ is $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$ itself, by (3.1) it suffices to show that either $\pi_S(H)/\pi_S(N)$ or $\pi_{S^c}(H)/\pi_{S^c}(N)$ is isomorphic to $\mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z})$. Furthermore, since $\mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z})$ is simple, it suffices to rule out the case where $\pi_S(H) = \pi_S(N)$ and $\pi_{S^c}(H) = \pi_{S^c}(N)$, which by the isomorphism theorems are equivalent, respectively, to the conditions that

$$\frac{H\cap\ker\pi_S}{N\cap\ker\pi_S} \cong \mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z}) \quad \text{and} \quad \frac{H\cap\ker\pi_{S^c}}{N\cap\ker\pi_{S^c}} \cong \mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z}).$$

Let

$$H_S := (H \cap \ker \pi_S) \cdot (H \cap \ker \pi_{S^c}) \cong (H \cap \ker \pi_S) \times (H \cap \ker \pi_{S^c}),$$
$$N_S := (N \cap \ker \pi_S) \cdot (N \cap \ker \pi_{S^c}) \cong (N \cap \ker \pi_S) \times (N \cap \ker \pi_{S^c}).$$

Assume by way of contradiction that $H_S/N_S \cong \frac{H\cap\ker \pi_S}{N\cap\ker \pi_S} \times \frac{H\cap\ker \pi_{S^c}}{N\cap\ker \pi_{S^c}} \cong (\mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z}))^2$, and consider the normal subgroup $(H_S \cap N)/N_S$. The isomorphism theorems yield an inclusion

$$\frac{H_S/N_S}{(H_S \cap N)/N_S} \cong H_S/(H_S \cap N) \cong H_S N/N \hookrightarrow H/N \cong \mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z}),$$

so $(H_S \cap N)/N_S$ must be a nontrivial normal subgroup of H_S/N_S. However, the only proper nontrivial normal subgroups of $(\mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z}))^2$ are $\mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z}) \times \{1\}$ or $\{1\} \times \mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z})$, so N_S must contain either $H \cap \ker \pi_S$ or $H \cap \ker \pi_{S^c}$, which results in a contradiction.

Proof of Claim 3: Let $G < \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ be a subgroup that has a quotient isomorphic to $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$. If $p \nmid \#G$, then by [40, Section 2.5], G must be isomorphic to a cyclic group, a dihedral group, A_4, S_4 or $A_5 \cong \mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z})$, so has no quotient isomorphic to $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$. Thus, p must divide $\#G$. Then $G \cap \mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ is also of order divisible by p and so by [48, Theorem 6.25, Chapter 3], $G \cap \mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ is solvable or equal to $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$. Since G has a quotient isomorphic to $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$, $G \cap \mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ cannot be solvable and hence $G = \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ and $p = 5$. □

Proof of Proposition 3.2. Since we have $G_{\ell^s n} < \mathrm{GL}_2(\mathbb{Z}/\ell^s n\mathbb{Z}) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell^s\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, there are natural surjective projection maps

$$\pi_s : G_{\ell^s n} \to G_{\ell^s} \quad \text{and} \quad \varpi_s : G_{\ell^s n} \to G_n.$$

Observe that $\ker \pi_s$ and $\ker \varpi_s$ can be identified as normal subgroups of G_n and G_{ℓ^s} respectively, and by Goursat's Lemma (see Lemma 3.1), we have

$$G_{\ell^s}/\ker \varpi_s \cong G_n/\ker \pi_s. \tag{3.2}$$

We first prove the proposition for the case when $s = 1$. By [2, Theorem 4.9], $\ker \varpi_1$ either contains $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ or is a subgroup of the center $Z(\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}))$ of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. If $\ker \varpi_1 \subseteq Z(\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}))$ and $\ell = 5$, then the left-hand side of (3.2) has a quotient $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$, which contradicts Lemma 3.3 since the right-hand side cannot have such a quotient. Similarly, if $\ker \varpi_1 \subseteq Z(\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}))$ and $\ell > 5$, then the left-hand side of (3.2) has a subquotient $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$, which is impossible by [10, Appendix, Corollary 11]. Therefore, $\ker \varpi_1$ must contain $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

For $s > 1$, since ϖ_s is surjective and factors through

$$G_{\ell^s n} \subset \mathrm{GL}_2(\mathbb{Z}/\ell^s n\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/\ell n\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

$\ker \varpi_s \subset \mathrm{GL}_2(\mathbb{Z}/\ell^s\mathbb{Z})$ maps surjectively onto $\ker \varpi_1 \subset \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Then the proposition follows from [10, Appendix, Lemma 12]. □

3.3. Bounding the level from the index

Proposition 3.5 *([28, Part I, §6, Lemmas 2 & 3]). Let ℓ be a prime and let G be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Set $s_0 = 1$ if ℓ is odd and $s_0 = 2$ otherwise. If*

$$\ker(G \bmod \ell^{s+1} \to G \bmod \ell^s) = I + \mathrm{M}_2(\ell^s\mathbb{Z}/\ell^{s+1}\mathbb{Z})$$

for some $s \geq s_0$, then

$$\ker(G \to G \bmod \ell^s) = I + \ell^s\,\mathrm{M}_2(\mathbb{Z}_\ell).$$

Remark 3.6. This proof follows the one given by Lang and Trotter. We repeat it here for the reader's convenience and to show that the proof does give the lemma as stated, even though the statement of [28, Part I, §6, Lemmas 2 & 3] is slightly weaker.

Proof. For any positive integer n, let $U_n := \ker(G \to G \bmod \ell^n)$ and let $V_n := I + \ell^n\,\mathrm{M}_2(\mathbb{Z}_\ell)$. Note that for all n, $U_n \subset V_n$ and $U_n = U_1 \cap V_n$.

Observe that for $s \geq s_0$, raising to the ℓth power gives the following maps

$$V_s/V_{s+1} \xrightarrow{\sim} V_{s+1}/V_{s+2}, \quad \text{and} \quad U_s/U_{s+1} \hookrightarrow U_{s+1}/U_{s+2}.$$

By assumption, the natural inclusion $U_s/U_{s+1} \subset V_s/V_{s+1}$ is an isomorphism for some $s \geq s_0$. Combining these facts, we get the following commutative diagram for any positive k:

$$\begin{array}{ccc} U_s/U_{s+1} & \xrightarrow{\sim} & V_s/V_{s+1} \\ \downarrow & & \downarrow\sim \\ U_{s+k}/U_{s+k+1} & \hookrightarrow & V_{s+k}/V_{s+k+1}, \end{array}$$

where the vertical maps are raising to the (ℓ^k)th power and the horizontal maps are the natural inclusions. Hence, $U_{s+k}/U_{s+k+1} = V_{s+k}/V_{s+k+1}$ for all $k \geq 0$ and so $U_s = V_s$. □

3.4. Determining m-adic level from level of ℓ-adic components

Proposition 3.7. *Let $\ell_1, \ldots, \ell_q$ be distinct primes and let $\mathfrak{m} := \prod_{i=1}^q \ell_i$. For $i = 1, \ldots, q$, let $t_i \geq 1$ be positive integers and let $\mathfrak{m}_i := \prod_{j \neq i} \ell_j$. If G is a closed subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ such that $G_{\mathfrak{m}_i \cdot \ell_i^\infty} = \pi^{-1}(G_{\mathfrak{m}_i \ell_i^{t_i}})$ for each i, then $G_{\mathfrak{m}^\infty} = \pi^{-1}(G_M)$ for $M = \prod_{i=1}^q \ell_i^{t_i}$.*

Proof. For any $1 \leq i \leq q$ and $r_i \geq 0$, consider the following commutative diagram of natural reduction maps.

$$\begin{array}{ccc} G_{M\ell_i{}^{r_i}} & \twoheadrightarrow & G_M \\ \downarrow & & \downarrow \\ G_{\mathfrak{m}_i\ell_i{}^{r_i+t_i}} & \twoheadrightarrow & G_{\mathfrak{m}_i\ell_i{}^{t_i}} \end{array}$$

The kernel of the top horizontal map is a subgroup of $I+\mathrm{M}_2(M\mathbb{Z}/M\ell_i^{r_i}\mathbb{Z})$, so its order is a power of ℓ_i. Similarly, the order of the kernel of the lower horizontal map is a power of ℓ_i, while the order of the kernels of the vertical maps are coprime to ℓ_i. Since $\#\ker(G_{M_i\ell_i^{r_i}} \to G_M)\cdot\#\ker(G_M \to G_{\mathfrak{m}_i\ell_i^{t_i}})$ is equal to $\#\ker(G_{M_i\ell_i^{r_i}} \to G_{\mathfrak{m}_i\ell_i^{r_i}})\cdot\#\ker(G_{\mathfrak{m}_i\ell_i^{r_i}} \to G_{\mathfrak{m}_i\ell_i^{t_i}})$, the kernels of horizontal maps must be isomorphic, and hence $G_{M\ell_i{}^{r_i}}$ is the full preimage of G_M, by assumption.

To complete the proof, it remains to show that for any collection of positive integers $\{r_i\}_{i=1}^q$, $G_{M\prod_{i=1}^q \ell_i^{r_i}}$ is the full preimage of G_M. We do so with an inductive argument. Let $1 \le q' \le q$ and let $\{r_i\}_{i=1}^{q'}$ be a collection of positive integers. Consider the following commutative diagram of natural reduction maps.

$$\begin{array}{ccc} G_{M\prod_{i=1}^{q'} \ell_i{}^{r_i}} & \twoheadrightarrow & G_{M\prod_{i=1}^{q'-1} \ell_i{}^{r_i}} \\ \downarrow & & \downarrow \\ G_{M\ell_{q'}{}^{r_{q'}}} & \twoheadrightarrow & G_M \end{array}$$

Again the kernels of the horizontal maps and the kernels of the vertical maps have coprime orders and so, by the induction hypothesis, the kernels of all maps are as large as possible. □

4. Images of isolated points

Let C be a curve over a number field F and consider the morphism

$$\phi_d\colon \mathrm{Sym}^d C \to \mathrm{Pic}^d_C$$

that sends an unordered tuple of points to the sum of their divisor classes. Let W^d be the image of $\mathrm{Sym}^d C$ in Pic^d_C. Note that if there is a degree d point on C then $\mathrm{Pic}^d_C \cong \mathrm{Pic}^0_C$ and in particular is an abelian variety.

Definition 4.1.

(1) A degree d point $x \in C$ is $\mathbb{P}^1$-isolated if there is no other point $x' \in (\mathrm{Sym}^d C)(F)$ such that $\phi_d(x) = \phi_d(x')$.
(2) A degree d point $x \in C$ is AV-isolated if there is no positive rank subabelian variety $A \subset \mathrm{Pic}^0_C$ such that $\phi_d(x) + A \subset W^d$.

(3) A degree d point $x \in C$ is isolated if it is $\mathbb{P}^1$-isolated and AV-isolated.
(4) A degree d point $x \in C$ is sporadic if there are only finitely many closed points $y \in C$ with $\deg(y) \leq \deg(x)$.

Faltings's theorem [18] on rational points on subvarieties of abelian varieties implies the following two results on isolated and sporadic points.

Theorem 4.2. *Let C be a curve over a number field.*

(1) *There are infinitely many degree d points on C if and only if there is a degree d point on C that is* not *isolated. In particular, sporadic points are isolated.*
(2) *There are only finitely many isolated points on C.*

We provide the details of the proof in Section 4.1.

In this section, we consider an arbitrary morphism of curves, and give a criterion for when images of isolated points remain isolated. Our main result is the following.

Theorem 4.3. *Let $f\colon C \to D$ be a finite map of curves, let $x \in C$ be a closed point, and let $y = f(x) \in D$. Assume that $\deg(x) = \deg(y) \cdot \deg(f)$.*

(1) *If x is* $\mathbb{P}^1$-isolated, *then y is* $\mathbb{P}^1$-isolated.
(2) *If x is* AV-isolated, *then y is* AV-isolated.
(3) *If x is sporadic, then y is sporadic.*

Proof. Let $d = \deg(y)$ and let $e = \deg(f)$. Then by assumption $de = \deg(x)$.

(1) Assume that y is not $\mathbb{P}^1$-isolated, so there exists a point $y' \in (\mathrm{Sym}^d C)(F)$, different from y, such that $\phi_d(y) = \phi_d(y')$, or, in other words such that there exists a function $g \in \mathbf{k}(D)^\times$ such that $\mathrm{div}(g) = y - y'$. Since y is a degree d point (and not just an effective degree d divisor), the assumption that $y \neq y'$ implies that y and y' have distinct support. Therefore the map $g\colon D \to \mathbb{P}^1$ has degree d, and hence $g \circ f$ gives a degree de map. Then for any $z \in \mathbb{P}^1(F)$ different from $g(f(x))$, the fiber $(g \circ f)^{-1}(z)$ gives a point of $(\mathrm{Sym}^{de} C)(F)$, distinct from x, such that $\phi_{de}(x) = \phi_{de}((g \circ f)^{-1}(z))$. In particular, x is not $\mathbb{P}^1$-isolated.

(2) Assume that y is not AV-isolated, so there exists a subabelian variety $A \subset \mathrm{Pic}^0_D$ such that $\phi_d(y) + A \subset W^d$. The morphism f induces a commutative diagram

$$\begin{array}{ccc} \mathrm{Sym}^d D & \xrightarrow{\phi_d} & \mathrm{Pic}^d_D \\ \downarrow & & \downarrow{\scriptstyle f^*} \\ \mathrm{Sym}^{de} C & \xrightarrow{\phi_{de}} & \mathrm{Pic}^{de}_C, \end{array}$$

where the left vertical arrow sends y to x. Therefore, $\phi_{de}(x) + f^*A \subset W^{de}$. Since f^*A is a positive rank subabelian variety of $\mathrm{Pic}^0 C$, the point x is not AV-isolated.

(3) Assume that y is not sporadic, i.e., that there are infinitely many closed points $y' \in D$ with $\deg(y') \leq \deg(y) = d$. For each of these points y', there is a closed point $x' \in f^{-1}(y')$ such that

$$\deg(x') \leq \deg(y')e \leq \deg(y)e = de = \deg(x).$$

Hence, the point x is not sporadic. □

4.1. Proof of Theorem 4.2

(1) The forward direction is a straightforward consequence of Faltings's theorem [18]; we include the details for the readers' convenience. Assume that there are infinitely many degree d points. Then either there are two degree d points $x, x' \in C$ such that $\phi_d(x) = \phi_d(x')$ and so in particular x and x' are not $\mathbb{P}^1$-isolated, or ϕ_d is injective on the set of degree d points. In the latter case, $W^d \subset \mathrm{Pic}^d_C$ contains infinitely many rational points. Faltings's theorem states that the rational points on W^d are a finite union of translates of subabelian varieties, so in particular, there must be a positive rank abelian variety $A \subset \mathrm{Pic}^0_C$ and a degree d point $x \in C$ such that $x + A \subset W^d$, i.e., the degree d point x is not AV-isolated.

Now we prove the backwards direction, which requires a more detailed study of Faltings's theorem. Let $x \in C$ be a degree d point that is not isolated. If x is not $\mathbb{P}^1$-isolated, then there exists an $x' \in (\mathrm{Sym}^d C)(F), x \neq x'$, such that $\phi_d(x) = \phi_d(x')$, or equivalently, there exists a rational function $g \in \mathbf{k}(C)^\times$ such that $\mathrm{div}(g) = x - x'$. Since x is a closed point and $x' \in (\mathrm{Sym}^d C)(F)$, $x \neq x'$ implies that x and x' have disjoint support. Thus the function g gives a degree d morphism $g\colon C \to \mathbb{P}^1$. By Hilbert's irreducibility theorem [42, Chap. 9], there are infinitely many degree 1 points $z \in \mathbb{P}^1$ such that $g^{-1}(z)$ has degree d, which gives the desired result.

Now assume that x is $\mathbb{P}^1$-isolated but not AV-isolated, i.e., that x is not equivalent to any other effective divisors and that there is a positive rank subabelian variety $A \subset \mathrm{Pic}^0 C$ such that $x + T \subset W^d$. Since the cokernel of $\mathrm{Pic}\, C \to \left(\mathrm{Pic}\, \overline{C}\right)^{\mathrm{Gal}(\overline{F}/F)}$ is torsion, there is a finite index subgroup $H \subset A(F)$ such that every divisor class in H (and therefore every divisor class in $x + H$) is represented by an F-rational divisor, and every divisor class in $A(F) \setminus H$ is *not* represented by an F-rational divisor. In other words, $\phi_d\left((\mathrm{Sym}^d C)(F)\right) \cap (x + A(F)) = x + H$.

Since H has positive rank, taking the preimage of $x + H$ under ϕ_d yields infinitely many rational points on $\mathrm{Sym}^d C$, or, equivalently, infinitely many effective degree d 0-cycles on C. It remains to prove that infinitely many of these 0-cycles are irreducible, i.e., are not in the image of $\cup_i \left((\mathrm{Sym}^{d-i} C)(F) \times (\mathrm{Sym}^i C)(F)\right)$.

Consider the following commutative diagram

$$\begin{array}{ccc} (\mathrm{Sym}^{d-i} C)(F) \times (\mathrm{Sym}^{i} C)(F) & \xrightarrow{\phi_{d-i} \times \phi_i} & W^{d-i} \times W^{i} \\ \downarrow & & \downarrow \\ (\mathrm{Sym}^{d} C)(F) & \xrightarrow{\phi_d} & W^{d}, \end{array}$$

where the vertical maps are induced by concatenation and summation, respectively. If there are only finitely many degree d points on C, then all but finitely many of the points in $x + H$ are contained in the union $\cup_i (W^{d-i}(F) + W^i(F))$. Faltings's theorem on rational points on subvarieties of abelian varieties implies that

$$\bigcup_{i=1}^{\lfloor d/2 \rfloor} (W^{d-i}(F) + W^i(F)) = \bigcup_{j=1}^{n} y_j + A_j(F), \tag{4.1}$$

where n is some nonnegative integer, the A_j's are some subabelian varieties of Pic^0_C and the y_j's are degree d divisors on C, which can be taken to be reducible and effective.

We are concerned with the intersection

$$\begin{aligned} (x + H) \cap \left(\bigcup_{j=1}^{n} y_j + A_j(F) \right) &= x + \left(H \cap \left(\bigcup_{j=1}^{n} y_j - x + A_j(F) \right) \right) \\ &= x + \bigcup_{j=1}^{n} (H \cap (y_j - x + A_j(F))) \end{aligned}$$

If the intersection $H \cap (y_j - x + A_j(F))$ is nonempty, then it is a coset of $H \cap A_j(F)$. In addition, since x is a $\mathbb{P}^1$-isolated degree d point on C, x cannot be written as the sum of two nonzero effective divisors, so by definition of (4.1), $H \cap (y_j - x + A_j(F))$ does not include the identity. Thus,

$$(x + H) \cap \left(\bigcup_{j=1}^{n} y_j + A_j(F) \right) = x + \bigcup_{j \in J} (z_j + H \cap A_j(F)),$$

where $J \subset \{1, \ldots, n\}$ and $z_j \in H \setminus H \cap A_j(F)$.

For each $j \in J$, let G_j be a subgroup of H of finite index that contains $H \cap A_j(F)$ and that does not contain z_j. Then we have

$$(x + H) \cap \left(\bigcup_{j=1}^{n} y_j + A_j(F) \right) = x + \bigcup_{j \in J} (z_j + H \cap A_j(F))$$

$$\subset x + \bigcup_{j\in J} (z_j + G_j)$$
$$\subset (x + H) \setminus (x + \cap_{j\in J} G_j) \subsetneq x + H.$$

Since each G_j is finite index in H, so is the intersection $\cap_{j\in J} G_j$. Hence, the image of $\cup_i (W^{d-i}(F) + W^i(F))$ misses infinitely many rational points of $x + H$, and so there are infinitely many degree d points on C.

(2) Let P be a point of degree d. If $d \geq g + 1$, then, by the Riemann-Roch theorem, $\ell(P) \geq d - g + 1 \geq 2$ and so P is not $\mathbb{P}^1$-isolated. Therefore, any isolated point on C must have bounded degree, and so it suffices to prove that there are only finitely many isolated points of a fixed degree d.

Recall that degree d points on C give rise to rational points on $\mathrm{Sym}^d C$ that in turn map, via ϕ_d, injectively to rational points on W^d. By Faltings's theorem, $W^d(F)$ is the finite union of translates of subabelian varieties of $\mathrm{Pic}^0 C$. By definition, any degree d point on C that lands in a translate of a positive rank subabelian variety is not AV-isolated. Therefore, the set of degree d isolated points of C must inject (under ϕ_d) into a finite union of translates of rank 0 subabelian varieties, so in particular must be finite. □

5. Isolated points above a fixed non-CM j-invariant

For any non-CM elliptic curve E over a number field k, recall from §2.3 that

$$S_E = S_{E/k} := \{2, 3\} \cup \{\ell : \rho_{E,\ell^\infty}(\mathrm{Gal}_k) \not\supset \mathrm{SL}_2(\mathbb{Z}_\ell)\} \cup \{5, \text{if } \rho_{E,5^\infty}(\mathrm{Gal}_k) \neq \mathrm{GL}_2(\mathbb{Z}_5)\}.$$

In this section we show that the degree of a non-cuspidal non-CM point $x \in X_1(n)$ is as large as possible given the degree of its image in $X_1(a)$ for $a = \gcd(n, M_{E_x}(S_{E_x}))$, where E_x is an elliptic curve over $\mathbb{Q}(j(x))$ with j-invariant $j(x)$.

Theorem 5.1. *Fix a non-CM elliptic curve E over a number field k. Let S be a finite set of places containing S_E and let $\mathfrak{m}_S := \prod_{\ell\in S} \ell$. Let M be a positive integer with* $\mathrm{Supp}(M) \subset S$ *satisfying*

$$\mathrm{im}\, \rho_{E,\mathfrak{m}_S^\infty} = \pi^{-1}(\mathrm{im}\, \rho_{E,M}). \tag{5.1}$$

If $x \in X_1(n)$ is a closed point with $j(x) = j(E)$, then $\deg(x) = \deg(f)\deg(f(x))$, *where f denotes the natural map $X_1(n) \to X_1(\gcd(n, M))$.*

Remark 5.2. Note that if E and E' are quadratic twists of each other, both defined over a number field k, then $S_E = S_{E'}$ (see, e.g., [44, Lemma 5.27]). Furthermore, for any S,

$$\pm(\mathrm{im}\, \rho_{E,\mathfrak{m}_S^\infty}) = \pm(\mathrm{im}\, \rho_{E',\mathfrak{m}_S^\infty}) \tag{5.2}$$

(see, e.g., [44, Lemma 5.17]). Since any open subgroup of $\mathrm{GL}_2(\mathbb{Z}_{\mathfrak{m}_S})$ has only finitely many subgroups of index 2, there is an integer M that will satisfy (5.1) for all quadratic twists of a fixed elliptic curve.

This theorem combined with Theorem 4.3 yields the following corollary, of which Theorem 1.1 is a special case.

Corollary 5.3. *Fix a non-CM elliptic curve E over a number field k. Let S be a finite set of places containing S_E and let M be a positive integer with* $\mathrm{Supp}(M) \subset S$ *satisfying*

$$\operatorname{im} \rho_{E,\mathfrak{m}_S^\infty} = \pi^{-1}(\operatorname{im} \rho_{E,M}).$$

Let $x \in X_1(n)$ be a point with $j(x) = j(E)$, and let f denote the natural map $X_1(n) \to X_1(\gcd(n, M))$.

(1) *If x is* $\mathbb{P}^1$-isolated, *then $f(x)$ is* $\mathbb{P}^1$-isolated.
(2) *If x is* AV-isolated, *then $f(x)$ is* AV-isolated.
(3) *If x is sporadic, then $f(x)$ is sporadic.*

From this, we deduce the following.

Corollary 5.4. *Let E be a non-CM elliptic curve defined over $k := \mathbb{Q}(j(E))$. If $\ell \notin S_E$, then there are no sporadic or isolated points on $X_1(\ell^s)$ lying over $j(E)$ for any $s \in \mathbb{N}$.*

In Section 5.1, specifically Lemma 5.6, we show that the desired maximal degree growth condition (i.e., the conclusion of Theorem 5.1) is implied by a condition on the degree of field extensions $k(P)/k(bP)$ where P is a point of order ab on a non-CM elliptic curve E. We then show that the assumed growth of the Galois representation (5.1) implies the hypothesis of Lemma 5.6 in two different cases. First, for maps $X_1(n) \to X_1(n\ell^{-1})$ for prime divisors ℓ of n outside of S_E (see Section 5.2), and second, for maps $X_1(ab) \to X_1(a)$ for integers a, b with bounded support (see Section 5.3). The results of these two sections are brought together in Section 5.4 to prove Theorem 5.1.

Remark 5.5. As discussed in Section 2.3, the full strength of Serre's Open Image Theorem implies that for any non-CM elliptic curve E/k, there exists a positive integer M_E such that

$$\operatorname{im} \rho_E = \pi^{-1}(\operatorname{im} \rho_{E,M_E}).$$

The arguments in Section 5.3 alone then imply that $\deg(x) = \deg(f)\deg(f(x))$, where f denotes the natural map $X_1(n) \to X_1(\gcd(n, M_E))$, which yields a weaker version of Theorem 5.1.

While there is not a dramatic difference in the strength of these results for a fixed elliptic curve, the difference is substantial when applied to a family of elliptic curves. It is well-known that M_E can be arbitrarily large for a non-CM elliptic curve E over a fixed number field k (see Section 2.3). However, for a fixed finite set of places S, we prove that $M_E(S)$ can be bounded depending only on $[k : \mathbb{Q}]$. This allows us to obtain the uniform version of Corollary 5.3, namely Theorem 1.6 (see §6).

5.1. Field-theoretic condition for maximal degree growth

Lemma 5.6. *Let a and b be positive integers, E a non-CM elliptic curve over a number field k, and $P \in E$ a point of order ab. Let $x := [(E, P)] \in X_1(ab)$ and let f denote the map $X_1(ab) \to X_1(a)$. If $[k(P) : k(bP)]$ is as large as possible, i.e., if $[k(P) : k(bP)] = \#\{Q \in E : bQ = bP, Q \text{ order } ab\}$, then*

$$\deg(x) = \deg(f)\deg(f(x)).$$

Proof. From the definition of $X_1(n)$, we have that

$$\#\{Q \in E : bQ = bP, Q \text{ order } ab\} = \begin{cases} 2\deg(X_1(ab) \to X_1(a)) & \text{if } a \leq 2 \text{ and } ab > 2, \\ \deg(X_1(ab) \to X_1(a)) & \text{otherwise.} \end{cases} \tag{5.3}$$

Let us first consider the case that $a \leq 2$ and $ab > 2$. Then $\deg(f(x)) = [k(bP) : \mathbb{Q}]$. Since $[k(P) : k(bP)]$ is as large as possible and $a \leq 2$, there must be a $\sigma \in \mathrm{Gal}_k$ such that $\sigma(P) = -P$. Hence $\deg(x) = \frac{1}{2}[k(P) : \mathbb{Q}]$ by Lemma 2.1, so (5.3) yields the desired result.

Now assume that $ab \leq 2$. Then $\deg(f(x)) = [k(bP) : \mathbb{Q}]$ and $\deg(x) = [k(P) : \mathbb{Q}]$, so (5.3) again yields the desired result.

Finally we consider the case when $a > 2$. Note that for any point $y \in X_1(ab)$, $\deg(y) \leq \deg(f(y)) \cdot \deg(X_1(ab) \to X_1(a))$. Combining this with (5.3), it remains to prove that

$$\frac{\deg(x)}{\deg(f(x))} \geq \#\{Q \in E : bQ = bP, Q \text{ order } ab\}.$$

By Lemma 2.1, $\deg(x) = c_x \cdot [k(P) : \mathbb{Q}]$ and $\deg(f(x)) = c_{f(x)} \cdot [k(bP) : \mathbb{Q}]$ where $c_x, c_{f(x)} \in \{1, 1/2\}$. Since any $\sigma \in \mathrm{Gal}_k$ that sends P to $-P$ also sends bP to $-bP$, $c_x \geq c_{f(x)}$ and so these arguments together show that

$$\frac{\deg(x)}{\deg(f(x))} = \frac{c_x[k(P) : \mathbb{Q}]}{c_{f(x)}[k(bP) : \mathbb{Q}]} = \frac{c_x}{c_{f(x)}}[k(P) : k(bP)] \geq [k(P) : k(bP)].$$

By assumption, $[k(P) : k(bP)] = \#\{Q \in E : bQ = bP, Q \text{ order } ab\}$, yielding the desired inequality. □

5.2. Eliminating primes with large Galois representation

Proposition 5.7. *Let E be a non-CM elliptic curve over a number field k, let ℓ be a prime not contained in S_E, and let a and s be positive integers. Let $x \in X_1(a\ell^s)$ be a closed point with $j(x) = j(E)$ and let $f\colon X_1(a\ell^s) \to X_1(a)$ be the natural map. Then*

$$\deg(x) = \deg(f)\deg(f(x)).$$

Proof. Write $a = b\ell^t$ where $\ell \nmid b$, let g denote the map $X_1(a) \to X_1(b)$ and let $h\colon X_1(a\ell^s) \to X_1(b)$ be the composition $g \circ f$. Since $\deg(h) = \deg(f)\deg(g)$, the general case follows from the case when $\ell \nmid a$. We work with this assumption for the remainder of the proof.

Let $P \in E$ be a point of order $a\ell^s$ such that $x = [(E, P)]$ and for any $c|a\ell^s$, let $B_c^1 \subset \mathrm{Aut}(E[c])$ be the stabilizer of $\frac{a\ell^s}{c}P$. Let H denote the kernel of the projection map $\operatorname{im}\rho_{E,a\ell^s} \to \operatorname{im}\rho_{E,a}$.

We wish to prove $[k(P) : k(\ell^s P)] = \#\{Q \in E : \ell^s Q = \ell^s P,\ Q \text{ order } a\ell^s\}$, so that we can apply Lemma 5.6. Note that we always have the following upper bound

$$\#\left(\mathrm{Aut}(E[\ell^s])/B_{\ell^s}^1\right) = \#\{Q \in E : \ell^s Q = \ell^s P,\ Q \text{ order } a\ell^s\} \geq [k(P) : k(\ell^s P)].$$

We may also apply Galois theory to the towers of fields $k(E[a\ell^s]) \supset k(P) \supset k(\ell^s P)$ and $k(E[a\ell^s]) \supset k(E[a]) \supset k(\ell^s P)$ to obtain the following lower bound.

$$\begin{aligned}[k(P) : k(\ell^s P)] &= \frac{[k(E[a\ell^s]) : k(E[a])] \cdot [k(E[a]) : k(\ell^s P)]}{[k(E[a\ell^s]) : k(P)]} = \frac{\#H \cdot \#\left(\operatorname{im}\rho_{E,a} \cap B_a^1\right)}{\#\left(\operatorname{im}\rho_{E,a\ell^s} \cap B_{a\ell^s}^1\right)} \\ &\geq \frac{\#H \cdot \#\left(\operatorname{im}\rho_{E,a} \cap B_a^1\right)}{\#(H \cap B_{a\ell^s}^1) \cdot \#\left(\operatorname{im}\rho_{E,a} \cap B_a^1\right)} = \frac{\#H}{\#(H \cap B_{a\ell^s}^1)} = \frac{\#H}{\#(H \cap B_{\ell^s}^1)}.\end{aligned}$$

Since $\ell \notin S_E$, we may use Proposition 3.2 to conclude that H must contain $\mathrm{SL}_2(\mathbb{Z}/\ell^s\mathbb{Z})$. Therefore we have set inclusions

$$\mathrm{SL}_2(\mathbb{Z}/\ell^s\mathbb{Z})/\left(\mathrm{SL}_2(\mathbb{Z}/\ell^s\mathbb{Z}) \cap B_{\ell^s}^1\right) \hookrightarrow H/\left(H \cap B_{\ell^s}^1\right) \hookrightarrow \mathrm{Aut}(E[\ell^s])/B_{\ell^s}^1. \tag{5.4}$$

Since the sets on the right and the left of (5.4) have the same cardinality, all inclusions in (5.4) must be bijections. Hence, the upper and lower bounds obtained above agree, and, in particular, $[k(P) : k(\ell^s P)] = \#\{Q \in E : \ell^s Q = \ell^s P,\ Q \text{ order } a\ell^s\}$ as desired. □

5.3. Maps between $\{X_1(n)\}$ where n has specified support

Proposition 5.8. *Let E be a non-CM elliptic curve over a number field k, let S be a finite set of primes, and let $\mathfrak{m}_S := \prod_{\ell \in S} \ell$. Let $M = M_E(S)$ be a positive integer with $\mathrm{Supp}(M) \subset S$ such that*

$$\operatorname{im}\rho_{E,\mathfrak{m}_S^\infty} = \pi^{-1}(\operatorname{im}\rho_{E,M})$$

and let a and b be positive integers with $\gcd(ab, M)|a$ and $\operatorname{Supp}(ab) \subset S$. Let $x \in X_1(ab)$ be a closed point with $j(x) = j(E)$ and let f denote the natural map $X_1(ab) \to X_1(a)$. Then

$$\deg(x) = \deg(f)\deg(f(x)).$$

Proof. Let $M' := \operatorname{lcm}(a, M)$ and let $n = ab$. By definition, $\operatorname{im}\rho_{E,n}$ is the mod n reduction of $\operatorname{im}\rho_{E,\mathfrak{m}_S^\infty}$ and $\operatorname{im}\rho_{E,a}$ is the mod a reduction of $\operatorname{im}\rho_{E,M'}$. Since $\operatorname{im}\rho_{E,\mathfrak{m}_S^\infty} = \pi^{-1}(\operatorname{im}\rho_{E,M})$, this implies that

$$\operatorname{im}\rho_{E,\mathfrak{m}_S^\infty} = \pi^{-1}(\operatorname{im}\rho_{E,M'}) \quad \text{and that} \quad \operatorname{im}\rho_{E,n} = \pi^{-1}(\operatorname{im}\rho_{E,a}),$$

where by abuse of notation, we use π to denote both natural projections. In other words, the mod n Galois representation is as large as possible given the mod a Galois representation. Hence, for any $P \in E$ of order n, the extension $[k(P) : k(bP)]$ is as large as possible, i.e., $[k(P) : k(bP)] = \#\{Q \in E : bQ = bP, Q \text{ order } n\}$. In particular this applies to a point $P \in E$ such that $x = [(E, P)] \in X_1(n)$. Therefore, Lemma 5.6 completes the proof. □

5.4. Proof of Theorem 5.1

Let $x \in X_1(n)$ be a closed point with $j(x) = j(E)$ and write $n = n_0n_1$ where $\operatorname{Supp}(n_0) \subset S$ and $\operatorname{Supp}(n_1)$ is disjoint from S. Note that $\gcd(n, M)|n_0$. We factor the map f as

$$X_1(n) \xrightarrow{f_1} X_1(n_0) \xrightarrow{f_2} X_1(\gcd(n, M)).$$

By inductively applying Proposition 5.7 to powers of primes $\ell \notin S_E$, we see that $\deg(x) = \deg(f_1)\deg(f_1(x))$. Then we apply Proposition 5.8 with $a = \gcd(n, M)$, $b = n_0/\gcd(n, M)$ to show that

$$\deg(f_1(x)) = \deg(f_2)\deg(f_2(f_1(x))).$$

6. Proof of Theorem 1.6

In this section we prove Theorem 1.6. For a fixed number field k, Conjecture 1.3 implies that there is a finite set of primes $S = S(k)$ such that for all non-CM elliptic curves E/k, $S \supset S_{E/k}$ (see (2.1)). Furthermore, Conjecture 1.4 implies that $S(k)$ can be taken to depend only on $[k : \mathbb{Q}]$. Thus, to deduce Theorem 1.6 from Corollary 5.3, it suffices to show that for any positive integer d and any finite set of primes S, there is an

integer $M = M_d(S)$ such that for all number fields k of degree d and all non-CM elliptic curves E/k, we have

$$\operatorname{im} \rho_{E,\mathfrak{m}_S^\infty} = \pi^{-1}(\operatorname{im} \rho_{E,M}).$$

Hence Proposition 6.1 completes the proof of Theorem 1.6.

Proposition 6.1. *Let d be a positive integer, S a finite set of primes, and $\mathcal{E}$ a set of non-CM elliptic curves over number fields of degree at most d.*

(1) *There exists a positive integer M with $\operatorname{Supp}(M) \subset S$ such that for all $E/k \in \mathcal{E}$*

$$\operatorname{im} \rho_{E,\mathfrak{m}_S^\infty} = \pi^{-1}(\operatorname{im} \rho_{E,M}).$$

(2) *Let $M_d(S, \mathcal{E})$ be the smallest such M as in (1) and for all $\ell \in S$, define*

$$\tau = \tau_{S,\mathcal{E},\ell} := \max_{E/k \in \mathcal{E}} \left(v_\ell \left(\# \operatorname{im} \rho_{E,\mathfrak{m}_{S-\{\ell\}}} \right) \right) \leq v_\ell(\# \operatorname{GL}_2(\mathbb{Z}/\mathfrak{m}_{S-\{\ell\}}\mathbb{Z})).$$

Then $v_\ell(M_d(S, \mathcal{E})) \leq \max(v_\ell(M_d(\{\ell\}, \mathcal{E})), v_\ell(2\ell)) + \tau$.

Remark 6.2. In the proof of Proposition 6.1(2), if $\operatorname{im} \rho_{E,\mathfrak{m}_{S-\{\ell\}}}$ is a Sylow ℓ-subgroup of $\operatorname{GL}_2(\mathbb{Z}/\mathfrak{m}_{S-\{\ell\}}\mathbb{Z})$, then a chief series (a maximal normal series) of $\operatorname{im} \rho_{E,\mathfrak{m}_{S-\{\ell\}}}$ does have length τ. So the bound in (2) is sharp if the group structure of $\operatorname{im} \rho_{E,\ell^\infty}$ allows. However, given set values for d, S, and $\mathcal{E}$, information about the group structure of possible Galois representations (rather than just bounds on the cardinality) could give sharper bounds.

Remark 6.3. A weaker version of Proposition 6.1 follows from [22, Proof of Lemma 8]. Indeed, Jones's proof goes through over a number field and for *any* finite set of primes S (rather than only $S = \{2, 3, 5\} \cup \{p : \operatorname{im} \rho_{E,p} \neq \operatorname{GL}_2(\mathbb{Z}/p\mathbb{Z})\} \cup \operatorname{Supp}(\Delta_E)$, which is the case under consideration in [22, Lemma 8]) and shows that

$$v_\ell(M_d(S, \mathcal{E})) \leq \max(v_\ell(M_d(\{\ell\}, \mathcal{E})), v_\ell(2\ell)) + v_\ell(\# \operatorname{GL}_2(\mathbb{Z}/\mathfrak{m}_{S-\{\ell\}}\mathbb{Z})).$$

The proof here and the one in [22] roughly follow the same structure; however, by isolating the purely group-theoretic components (e.g., Proposition 3.7), we are able to obtain a sharper bound in (2).

Proof. When $\#S = 1$, part (1) follows from Theorem 2.3 and Proposition 3.5 and part (2) is immediate.

We prove part (1) when $\#S$ is arbitrary by induction using Proposition 3.7. Let $S = \{\ell_1, \ldots, \ell_q\}$, let $M_i = M_d(\{\ell_i\}, \mathcal{E})$, let $s_i = \max(v_{\ell_i}(M_i), v_{\ell_i}(2\ell_i))$, and let $N_i = \prod_{j \neq i} \ell_j^{s_j}$. It suffices to show that for all $1 \leq i \leq q$ there exists a $t_i \geq s_i$ such that for all $E/k \in \mathcal{E}$

$$\operatorname{im}\rho_{E,N_i\cdot\ell_i^\infty} = \pi^{-1}(\operatorname{im}\rho_{E,N_i\ell_i^{t_i}});$$

then Proposition 3.7 implies that we may take $M = \prod_i \ell_i^{t_i}$.

Fix $i \in \{1,\dots,q\}$. For any $E/k \in \mathcal{E}$ and any $s \geq s_i$, define

$$K^i_{E,s} := \ker(\operatorname{im}\rho_{E,N_i\cdot\ell_i^s} \to \operatorname{im}\rho_{E,N_i}), \quad \text{and} \quad L^i_{E,s} := \ker(\operatorname{im}\rho_{E,N_i\cdot\ell_i^s} \to \operatorname{im}\rho_{E,\ell_i^s}).$$

By definition, $K^i_{E,s'}$ maps surjectively onto $K^i_{E,s}$ for any $s' \geq s$, so $K^i_{E,s}$ is the mod $N_i\ell_i^s$ reduction of $K^i_E := \ker(\operatorname{im}\rho_{E,N_i\cdot\ell_i^\infty} \to \operatorname{im}\rho_{E,N_i})$. Let us now consider $L^i_{E,s}$. Since $\ell_i \nmid N_i$, $L^i_{E,s}$ can be viewed as a subgroup of $\operatorname{im}\rho_{E,N_i}$ and we have $L^i_{E,s'} \subset L^i_{E,s}$ for all $s' \geq s$. Let $r \geq s_i$ be an integer such that $L^i_{E,r} = L^i_{E,r+1}$. Then we have the following diagram

$$\begin{array}{ccc} \operatorname{im}\rho_{E,\ell_i^{r+1}}/K^i_{E,r+1} & \twoheadrightarrow & \operatorname{im}\rho_{E,\ell_i^r}/K^i_{E,r} \\ \downarrow\cong & & \downarrow\cong \\ \operatorname{im}\rho_{E,N_i}/L^i_{E,r+1} & = & \operatorname{im}\rho_{E,N_i}/L^i_{E,r} \end{array} \tag{6.1}$$

where the vertical isomorphisms are given by Goursat's Lemma (Lemma 3.1).[6] Since $r \geq s_i$, $\operatorname{im}\rho_{E,\ell_i^{r+1}}$ is the full preimage of $\operatorname{im}\rho_{E,\ell_i^r}$ under the natural reduction map. So (6.1) implies that $K^i_{E,r+1}$ is the full preimage of $K^i_{E,r}$ under the natural reduction map. Then by Proposition 3.5, K^i_E is the full preimage of $K^i_{E,r}$ under the map $\mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})$ and therefore $\operatorname{im}\rho_{E,N_i\cdot\ell_i^\infty} = \pi^{-1}(\operatorname{im}\rho_{E,N_i\ell_i^r})$. Hence we may take $t_{E,i}$ to be the minimal $r \geq s_i$ such that $L^i_{E,r} = L^i_{E,r+1}$. Since $L^i_{E,s}$ is a subgroup of $\operatorname{im}\rho_{E,N_i} \subset \mathrm{GL}_2(\mathbb{Z}/N_i\mathbb{Z})$, $t_{E,i}$ may be bounded independent of E/k, depending only on N_i. This completes the proof of (1).

It remains to prove (2). Let $s \geq s_i$ and consider the following diagram, where again the vertical isomorphisms follow from Goursat's Lemma.

$$\begin{array}{ccc} \operatorname{im}\rho_{E,\ell_i^s}/K^i_{E,s} & \twoheadrightarrow & \operatorname{im}\rho_{E,\ell^{s_i}}/K^i_{E,s_i} \\ \downarrow\cong & & \downarrow\cong \\ \operatorname{im}\rho_{E,N_i}/L^i_{E,s} & \twoheadrightarrow & \operatorname{im}\rho_{E,N_i}/L^i_{E,s_i} \end{array} \tag{6.2}$$

The kernel of the top horizontal map is an ℓ_i-primary subgroup, so the index of $L^i_{E,s}$ in L^i_{E,s_i} is a power of ℓ_i. Thus, the maximal chain of proper containments $L^i_{E,s_i} \supsetneq L^i_{E,s_i+1} \supsetneq \cdots \supsetneq L^i_{E,t_i}$ is bounded by $v_{\ell_i}(\#\operatorname{im}\rho_{E,N_i}) = v_{\ell_i}(\#\operatorname{im}\rho_{E,\mathfrak{m}_{S-\{\ell_i\}}})$, which yields (2). □

[6] By tracing through the isomorphism given by Goursat's lemma, one can prove that this diagram is commutative. We do not do so here, since the claims that follow can also be deduced from cardinality arguments.

7. Lifting sporadic points

In this section we study when a sporadic point on $X_1(n)$ lifts to a sporadic point on a modular curve of higher level. We give a numerical criterion that is sufficient for lifting sporadic points (see Lemma 7.2), and use this to prove that there exist sporadic points such that *every* lift is sporadic. The examples we have identified correspond to CM elliptic curves.

Theorem 7.1. *Let E be an elliptic curve with CM by an order in an imaginary quadratic field K. Then for all sufficiently large primes ℓ which split in K, there exists a sporadic point $x = [(E, P)] \in X_1(\ell)$ with only sporadic lifts. Specifically, for any positive integer d and any point $y \in X_1(d\ell)$ with $\pi(y) = x$, the point y is sporadic, where π denotes the natural map $X_1(d\ell) \to X_1(\ell)$.*

The key to the proof of Theorem 7.1 is producing a sporadic point of sufficiently low degree so we may apply the following lemma. It is a consequence of Abramovich's lower bound on gonality in [1] and the result of Frey [19] which states that a curve $C_{/K}$ has infinitely many points of degree at most d only if $\operatorname{gon}_K(C) \leq 2d$.

Lemma 7.2. *Suppose there is a point $x \in X_1(N)$ with*

$$\deg(x) < \frac{7}{1600}[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(N)].$$

Then x is sporadic and for any positive integer d and any point $y \in X_1(dN)$ with $\pi(y) = x$, the point y is sporadic, where π denotes the natural map $X_1(dN) \to X_1(N)$.

Proof. We claim that the assumption on the degree of x implies that $\deg(y) < \frac{7}{1600}[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(dN)]$. Then [1, Thm. 0.1], shows that

$$\deg(y) < \frac{1}{2}\operatorname{gon}_{\mathbb{Q}}(X_1(dN)) \quad \text{and} \quad \deg(x) < \frac{1}{2}\operatorname{gon}_{\mathbb{Q}}(X_1(N)).$$

Thus x and y are sporadic by [19, Prop. 2].

Now we prove the claim. Let $x \in X_1(N)$ be a $\deg(x) \leq \frac{7}{1600}[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(N)]$. In particular, this implies $N > 2$. Thus for any point $y \in X_1(dN)$ with $\pi(y) = x$ we have

$$\begin{aligned}
\deg(y) &\leq \deg(x) \cdot \deg(X_1(dN) \to X_1(N)) \\
&< \frac{7}{1600}[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(N)] \cdot d^2 \prod_{p \mid d,\, p \nmid N} \left(1 - \frac{1}{p^2}\right) \quad \text{(see Proposition 2.2)} \\
&= \frac{7}{1600} \cdot \frac{1}{2}(dN) \prod_{p \mid dN} \left(1 + \frac{1}{p}\right) \varphi(dN)
\end{aligned}$$

$$= \frac{7}{1600}[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(dN)]. \quad \square$$

Proof of Theorem 7.1. Let E be an elliptic curve with CM by an order $\mathcal{O}$ in an imaginary quadratic field K. Then $L := K(j(E))$ is the ring class field of $\mathcal{O}$ and $[L : K] = h(\mathcal{O})$, the class number of $\mathcal{O}$. (See [11, Thms. 7.24 and 11.1] for details.) Let ℓ be a prime that splits in K and satisfies

$$\ell > \left(\frac{6400}{7} \cdot \frac{h(\mathcal{O})}{\#\mathcal{O}^\times}\right) - 1.$$

By [4, Thm. 6.2], there is a point $P \in E$ of order ℓ with

$$[L(\mathfrak{h}(P)) : L] = \frac{\ell - 1}{\#\mathcal{O}^\times}.$$

Then for $x = [(E, P)] \in X_1(\ell)$,

$$\begin{aligned}\deg(x) = [\mathbb{Q}(j(E), \mathfrak{h}(P)) : \mathbb{Q}] \leq [K(j(E), \mathfrak{h}(P)) : \mathbb{Q}] = [L(\mathfrak{h}(P)) : \mathbb{Q}] &= \frac{\ell - 1}{\#\mathcal{O}^\times} \cdot h(\mathcal{O}) \cdot 2 \\ &< (\ell - 1) \cdot \frac{7}{6400}(\ell + 1) \cdot 2 = \frac{7}{1600}[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(\ell)].\end{aligned}$$

The result now follows from Lemma 7.2. $\square$

Remark 7.3. Note that none of the known non-cuspidal non-CM sporadic points satisfy the degree condition given in Lemma 7.2. Thus it is an interesting open question to determine whether there exist non-CM sporadic points with infinitely many sporadic lifts. If no such examples exist, then by Theorem 1.6 there would be only finitely many non-CM sporadic points corresponding to j-invariants of bounded degree, assuming Conjecture 1.4.

8. Isolated points with rational j-invariant

In this section, we study non-CM isolated points with rational j-invariant. Our main result of this section (Theorem 8.1) gives a classification of the non-cuspidal non-CM isolated points on $X_1(n)$ with rational j-invariant. We prove that they either arise from elliptic curves whose Galois representations are very special (and may not even exist), or they can be mapped to isolated points on $X_1(m)$ for an explicit set of integers m.

Later, we focus on sporadic points with rational j-invariant on $X_1(n)$ for particular values of n. We show that if n is prime (Proposition 8.4), is a power of 2 (Proposition 8.5), or, conditionally on Sutherland [44, Conj. 1.1] and Zywina [50, Conj. 1.12], has $\min(\mathrm{Supp}(n)) \geq 17$ (Proposition 8.6), then any non-CM, non-cuspidal sporadic point with rational j-invariant has $j(x) = -7 \cdot 11^3$.

8.1. Classification of non-CM isolated points with rational j-invariant

Theorem 8.1. *Let $x \in X_1(n)$ be a non-CM non-cuspidal isolated point with $j(x) \in \mathbb{Q}$. Then one of the following holds:*

(1) *There is an elliptic curve $E/\mathbb{Q}$ with $j(E) = j(x)$ and a prime $\ell \in \mathrm{Supp}(n)$ such that either $\ell > 17, \ell \neq 37$ and $\rho_{E,\ell}$ is not surjective or $\ell = 17$ or 37 and $\rho_{E,\ell}$ is a subgroup of the normalizer of a non-split Cartan subgroup.*
(2) *There is an elliptic curve $E/\mathbb{Q}$ with $j(E) = j(x)$ and two distinct primes $\ell_1 > \ell_2 > 3$ in $\mathrm{Supp}(n)$ such that both ρ_{E,ℓ_1} and ρ_{E,ℓ_2} are not surjective.*
(3) *There is an elliptic curve $E/\mathbb{Q}$ with $j(E) = j(x)$ and a prime $2 < \ell \leq 37$ in $\mathrm{Supp}(n)$ such that the ℓ-adic Galois representation of E has level greater than 169.*
(4) *There is a divisor of n of the form $2^a 3^b p^c$ such that the image of x in $X_1(2^a 3^b p^c)$ is isolated and such that $a \leq a_p$, $b \leq b_p$, $p^c \leq 169$ for one of the following values of p, a_p, b_p.*

p	1	5	7	11	13	17	37
a_p	9	14	14	13	14	15	13
b_p	5	6	7	6	7	5	8

Remark 8.2. This theorem also holds for x a $\mathbb{P}^1$-isolated, AV-isolated, or sporadic point, respectively, at the expense of (4) giving the statement that the image of x is $\mathbb{P}^1$-isolated, AV-isolated, or sporadic, respectively.

Remark 8.3. Each of cases (1), (2), and (3) should be rare situations, if they occur at all. Indeed, the question of whether elliptic curves as in (1) exist is related to a question originally raised by Serre in 1972, and their non-existence has since been conjectured by Sutherland [44, Conj. 1.1] and Zywina [50, Conj. 1.12].

Assuming (1) does not hold, elliptic curves as in (2) correspond to points on finitely many modular curves of genus greater than 2, so there are at worst finitely many j-invariants in this case [12, Tables 6–14, Theorem 16A]. Additionally, there are no elliptic curves in the LMFDB database [26] as in (2), so in particular, any elliptic curve as in (2) must have conductor larger than $400,000$. (The Galois representation computations in LMFDB were carried out using the algorithm from [44].) If we do not assume (1) does not hold, then we must consider the case where $\ell_1 > 37$. In this case the elliptic curves of interest no longer correspond to points on finitely many modular curves, but nevertheless, Lemos has shown that such elliptic curves do not exist, assuming that $\operatorname{im} \rho_{E,\ell_2}$ is contained in the normalizer of a split Cartan subgroup or in a Borel subgroup [29,30].

Sutherland and Zywina's classification of modular curves of prime-power level with infinitely many points [47] shows that there are only finitely many rational j-invariants corresponding to elliptic curves as in (3), and suggests that in fact they do not exist. Table 8.1 gives, for each prime ℓ, the maximal prime-power level for which there exists a

Table 8.1
Maximal prime-power level for which there exists a modular curve with infinitely many rational points.

ℓ	3	5	7	11	13	17	37
max level	27	25	7	11	13	1	1

modular curve of that level with infinitely many rational points. Therefore, for $3 \leq \ell \leq 37$, respectively, there are already only finitely many j-invariants of elliptic curves with an ℓ-adic Galois representation of level at least 81, 125, 49, 121, 169, 17, or 37. Since such j-invariants are already rare, it seems reasonable to expect any such correspond to elliptic curves of ℓ-adic level *exactly* 81, 125, 49, 121, 169, 17 and 37, respectively.

This has been (conditionally) verified by Drew Sutherland in the cases $\ell = 17$ and $\ell = 37$. For these primes, there are conjecturally only 4 j-invariants corresponding to elliptic curves with non-surjective ℓ-adic Galois representation: $-17 \cdot 373^3/2^{17}, -17^2 \cdot 101^3/2, -7 \cdot 11^3$, and $-7 \cdot 137^3 \cdot 2083^3$ [50, Conj. 1.12]. For each of these j-invariants, Sutherland computed that the ℓ-adic Galois representation is the full preimage of the mod ℓ representation, so the representations are indeed of level ℓ and not level ℓ^2 [45].[7]

Proof. Let $x \in X_1(n)$ be a non-cuspidal non-CM isolated point with $j(x) \in \mathbb{Q}$. Let E be an elliptic curve over $\mathbb{Q}$ with $j(E) = j(x)$. Assume that (1) does not hold, so in particular E has surjective mod ℓ representation for every $\ell > 17$ and $\ell \neq 37$. Thus Proposition 5.7 and Theorem 4.3 together imply that x maps to an isolated point on $X_1(n')$ where n' is the largest divisor of n that is not divisible by any primes greater than 17 except possibly 37.

Now assume further that (2) does not hold, so there is at most one prime $p > 3$ for which the p-adic Galois representation is not surjective. If the p-adic Galois representation of E is surjective for all primes larger than 3, then we will abuse notation and set $p = 1$. Under these assumptions, additional applications of Proposition 5.7 and Theorem 4.3 show that x maps to an isolated point on $X_1(n'')$ where n'' is a divisor of n' with $\mathrm{Supp}(n'') \subset S := \{2, 3, p\}$[8] and $p \in \{1, 5, 7, 11, 13, 17, 37\}$. Furthermore, Corollary 5.3 shows that x maps to an isolated point on $X_1(\gcd(n'', M))$, where M is the level of the $\mathfrak{m}_S^\infty$ Galois representation of E.

Now we will further assume that (3) does not hold. Let $\mathcal{E}$ denote the set of all non-CM elliptic curves over $\mathbb{Q}$. Proposition 6.1 states that there is an integer $M_1(S, \mathcal{E})$ such that the level of the $\mathfrak{m}_S^\infty$ Galois representation of E divides $M_1(S, \mathcal{E})$ for all $E \in \mathcal{E}$. We will show that $M_1(\{2, 3, p\}, \mathcal{E})$ divides $2^{a_p} 3^{b_p} p^c$ for p, a_p, b_p, c as in (4).

By the assumption that (3) does not hold and [39, Corollary 1.3], we have the following values for the constant $M_1(\{\ell\}, \mathcal{E})$ from Proposition 6.1.

[7] Sutherland used a generalization of the algorithm in [44] to prove in each case the index of the mod-ℓ^2 image is no smaller than that of the mod-ℓ image. It then follows from [47, Lemma 3.7] that the ℓ-adic image is the full preimage of the mod-ℓ image.

[8] When $p = 1$, we conflate the set $\{2, 3, p\}$ with the set $\{2, 3\}$.

Table 8.2
Cardinality of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

ℓ	2	3	5	7	11	13	17	37
$\#\,\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$	$2\cdot 3$	$2^4 3$	$2^5 3^1 5$	$2^5 3^2 7$	$2^4 3^1 5^2 11$	$2^5 3^2 7^1 13$	$2^9 3^2 17$	$2^5 3^4 19^1 37$

ℓ	2	3	5	7	11	13	17	37
$M_1(\{\ell\},\mathcal{E})$	2^5	3^4	5^3	7^2	11^2	13^2	17	37

By Proposition 6.1(2),

$$v_\ell(M_1(S,\mathcal{E})) \le \max(v_\ell(M_1(\{\ell\},\mathcal{E})), v_\ell(2\ell)) + \sum_{\ell'\in S-\{\ell\}} v_\ell(\#\,\mathrm{GL}_2(\mathbb{Z}/\ell'\mathbb{Z})).$$

This upper bound combined with Table 8.2 yields the desired divisibility except for the case where $p = 17$ or $p = 37$.

Let us consider the case that $p = 17$, so $\rho_{E,17}$ is not surjective. Since we are not in case (1), we know $\mathrm{im}\,\rho_{E,17}$ is not contained in the normalizer of the non-split Cartan. Thus [50, Thms. 1.10 and 1.11] show that $\#\,\mathrm{im}\,\rho_{E,17} = 2^6 17$, so Proposition 6.1(2) implies that the level of the $\mathfrak{m}_S^\infty$ Galois representation divides $2^{15}3^5 17$.

The case when $p = 37$ proceeds similarly. In this case [50, Thms. 1.10 and 1.11] show that $\#\,\mathrm{im}\,\rho_{E,37} = 2^4 3^3 37$ and so Proposition 6.1(2) implies that the level of the $\mathfrak{m}_S^\infty$ Galois representation divides $2^{13}3^8 37$. □

8.2. Rational j-invariants of non-CM non-cuspidal sporadic points on $X_1(n)$ for particular values of n

Proposition 8.4. *Fix a prime ℓ. If $x \in X_1(\ell)$ is a non-CM non-cuspidal sporadic point with $j(x) \in \mathbb{Q}$ then $\ell = 37$ and $j(x) = -7\cdot 11^3$.*

Proof. Let $x = [(E,P)]$ be a non-CM sporadic point on $X_1(\ell)$ with $j(E) \in \mathbb{Q}$. We may assume E is defined over $\mathbb{Q}$. Note that $X_1(\ell)$ has infinitely many rational points for $\ell \le 10$. Further, $X_1(\ell)$ has gonality 2 for $\ell = 11, 13$, and no non-cuspidal rational points [34]. Hence if $x \in X_1(\ell)$ is a non-cuspidal non-CM sporadic point, $\ell > 13$.

If the mod ℓ Galois representation of E is surjective, then x cannot be a sporadic point on $X_1(\ell)$ by Corollary 5.4, so assume that $\rho_{E,\ell}$ is not surjective. Then the im $\rho_{E,\ell}$ is contained in a maximal subgroup, which can be an exceptional subgroup, a Borel subgroup or the normalizer of a (split or non-split) Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ [40, Section 2]. We will analyze each case separately.

In the case where im $\rho_{E,\ell}$ is contained in the normalizer of the non-split Cartan subgroup, Lozano-Robledo [32, Theorem 7.3] shows that the degree of a field of definition of a point of order ℓ is greater than or equal to $(\ell^2-1)/6$. Since $\ell > 13$ we have

$$\mathrm{gon}_{\mathbb{Q}}(X_1(\ell)) \le \mathrm{genus}(X_1(\ell)) \le \frac{1}{24}(\ell^2-1).$$

Therefore x cannot be sporadic in this case.

If im $\rho_{E,\ell}$ is contained in the normalizer of the split Cartan subgroup, then by [3], ℓ has to be less than or equal to 13. Similarly, if im $\rho_{E,\ell}$ is one of the exceptional subgroups, then by [32, Theorem 8.1], $\ell \leq 13$.

If im $\rho_{E,\ell}$ is contained in a Borel subgroup, then E has a rational isogeny of degree ℓ. By [33], ℓ is one of the following primes: $2, 3, 5, 7, 11, 13, 17, 37$. Thus we need only consider $\ell = 17$ and 37. For $\ell = 17$, [32, Table 5] shows that $\deg(x) \geq 4$. Since the gonality of $X_1(17)$ is also 4, x cannot be sporadic.

Finally when $\ell = 37$, there are exactly two non-cuspidal points in $X_0(37)(\mathbb{Q})$ [32, Table 5]. The one corresponding to an elliptic curve with j-invariant $-7 \cdot 11^3$ gives a degree 6 point on $X_1(37)$, which is sporadic since $\operatorname{gon}_{\mathbb{Q}} X_1(37) = 18$. The other gives a point on $X_1(37)$ of degree 18, which is not sporadic. □

Proposition 8.5. *Let $s \geq 1$. If $x \in X_1(2^s)$ is a non-cuspidal non-CM sporadic point, then $j(x) \notin \mathbb{Q}$.*

Proof. By [39, Cor. 1.3], the 2-adic Galois representation of any non-CM elliptic curve over $\mathbb{Q}$ has level at most 32. Thus, by Proposition 5.8 it suffices to show that $X_1(2^s)$ has no non-cuspidal non-CM sporadic points with rational j-invariant for $s \leq 5$.

If $s = 1, 2$ or 3, then modular curve $X_1(2^a)$ is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$ and so has no sporadic points. When $s = 4$, the modular curve $X_1(16)$ has genus 2 and hence gonality 2 which implies that it has infinitely many points of degree 2. Additionally, as first established by Levi [31], $X_1(16)$ has no non-cuspidal points over $\mathbb{Q}$ and so has no non-cuspidal sporadic points.

Now we consider $X_1(32)$, which has gonality 8 (see [15, Table 1]). Let $x = [(E, P)]$ be a non-CM sporadic point on $X_1(32)$ with $j = j(E) \in \mathbb{Q}$. We may assume that E is defined over $\mathbb{Q}$. Since x is a sporadic point, there are only finitely many points $y \in X_1(32)$ with $\deg(y) \leq \deg(x)$. Since the degree of a point $y \in X_1(32)$ can be calculated from the mod 32 Galois representation of an elliptic curve with j-invariant $j(y)$, this implies that there are only finitely many j-invariants whose mod 32 Galois representation is contained in a conjugate of im $\rho_{E,32}$. By [39, Table 1], there are only eight non-CM j-invariants with this property:

$$2^{11},\ 2^4 17^3,\ \frac{4097^3}{2^4},\ \frac{257^3}{2^8},\ -\frac{857985^3}{62^8},\ \frac{919425^3}{496^4},$$
$$-\frac{3 \cdot 18249920^3}{171^6},\ \text{and}\ -\frac{7 \cdot 1723187806080^3}{79^{16}}.$$

Using `Magma`, we compute the degree of each irreducible factor of 32nd division polynomial for each of these j-invariants and we find that the least degree of a field where a point of order 32 is defined is 32, hence there are no non-CM sporadic points on $X_1(32)$ with a rational j-invariant. □

Proposition 8.6. *Let n be a positive integer with $\min(\mathrm{Supp}(n)) \geq 17$. Assume [44, Conj. 1.1] or [50, Conj. 1.12]. If $x \in X_1(n)$ is a non-cuspidal non-CM sporadic point with $j(x) \in \mathbb{Q}$, then $37|n$ and $j(x) = -7 \cdot 11^3$.*

Proof. Let E be an elliptic curve over $\mathbb{Q}$ with $j(E) = j(x)$. We apply Theorem 8.1. By assumption and Remark 8.3, cases (1) and (3) of Theorem 8.1 do not occur. Further, case (2) only occurs if $17 \cdot 37|n$ and $\mathrm{im}\,\rho_{E,17}$ and $\mathrm{im}\,\rho_{E,37}$ are both contained in Borel subgroups (see proof of Proposition 8.4), which is impossible (see, e.g., [32, Table 4]).

Hence, we must be in case (4) of Theorem 8.1. Since $\min(\mathrm{Supp}(n)) \geq 17$, the only possible divisors of n of the form $2^a 3^b p^c$ (with a, b, c, p as in Theorem 8.1(4)) are 17 or 37. Thus, for one of $\ell = 17$ or 37 we must have $\ell|n$ and x maps to a sporadic point on $X_1(\ell)$. Proposition 8.4 then completes the proof. □

References

[1] D. Abramovich, A linear lower bound on the gonality of modular curves, Int. Math. Res. Not. (20) (1996) 1005–1011, MR1422373.

[2] E. Artin, Geometric Algebra, Interscience Publishers, Inc., New York–London, 1957, MR0082463.

[3] Y. Bilu, P. Parent, M. Rebolledo, Rational points on $X_0^+(p^r)$, Ann. Inst. Fourier (Grenoble) 63 (3) (2013) 957–984, MR3137477.

[4] A. Bourdon, P.L. Clark, Torsion points and Galois representations on CM elliptic curves, preprint, arXiv:1612.03229.

[5] J. Box, Quadratic points on modular curves with infinite Mordell–Weil group, preprint, arXiv:1906.05206.

[6] P. Bruin, F. Najman, Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields, LMS J. Comput. Math. 18 (1) (2015) 578–602, https://doi.org/10.1112/S1461157015000157, MR3389884.

[7] A. Cadoret, A. Tamagawa, A uniform open image theorem for ℓ-adic representations, II, Duke Math. J. 162 (12) (2013) 2301–2344, MR3102481.

[8] P.L. Clark, B. Cook, J. Stankewicz, Torsion points on elliptic curves with complex multiplication (with an appendix by Alex Rice), Int. J. Number Theory 9 (2) (2013) 447–479, MR3005559.

[9] P.L. Clark, P. Pollack, Pursuing polynomial bounds on torsion, Israel J. Math. 227 (2) (2018) 889–909, https://doi.org/10.1007/s11856-018-1751-8, MR3846346.

[10] A.C. Cojocaru, On the surjectivity of the Galois representations associated to non-CM elliptic curves, with an appendix by Ernst Kani, Canad. Math. Bull. 48 (1) (2005) 16–31, https://doi.org/10.4153/CMB-2005-002-x, MR2118760.

[11] D.A. Cox, Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication, 2nd ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013, MR3236783.

[12] H. Daniels, E. González-Jiménez, Serre's constant of elliptic curves over the rationals, preprint, arXiv:1812.04133.

[13] P. Deligne, M. Rapoport, Les schémas de modules de courbes elliptiques, in: Modular Functions of One Variable, II, Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972, in: Lecture Notes in Math., vol. 349, Springer, Berlin, 1973, pp. 143–316, MR0337993.

[14] M. Derickx, A. Etropolski, M. van Hoeij, J.S. Morrow, D. Zureick-Brown, Sporadic cubic torsion, in preparation.

[15] M. Derickx, M. van Hoeij, Gonality of the modular curve $X_1(N)$, J. Algebra 417 (2014) 52–71, MR3244637.

[16] M. Derickx, A.V. Sutherland, Torsion subgroups of elliptic curves over quintic and sextic number fields, Proc. Amer. Math. Soc. 145 (10) (2017) 4233–4245, MR3690609.

[17] F. Diamond, J. Shurman, A First Course in Modular Forms, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005, MR2112196.

[18] G. Faltings, The general case of S. Lang's conjecture, in: Barsotti Symposium in Algebraic Geometry, Abano Terme, 1991, in: Perspect. Math., vol. 15, Academic Press, San Diego, CA, 1994, pp. 175–182, MR1307396.
[19] G. Frey, Curves with infinitely many points of fixed degree, Israel J. Math. 85 (1–3) (1994) 79–83, MR1264340.
[20] E. Goursat, Sur les substitutions orthogonales et les divisions régulières de l'espace, Ann. Sci. Éc. Norm. Supér. (3) 6 (1889) 9–102, MR1508819.
[21] J. Gunther, J.S. Morrow, Irrational points on random hyperelliptic curves, preprint, arXiv:1709.02041.
[22] N. Jones, A bound for the torsion conductor of a non-CM elliptic curve, Proc. Amer. Math. Soc. 137 (1) (2009) 37–43, MR2439422.
[23] N. Jones, Almost all elliptic curves are Serre curves, Trans. Amer. Math. Soc. 362 (3) (2010) 1547–1570, MR2563740.
[24] S. Kamienny, Torsion points on elliptic curves and q-coefficients of modular forms, Invent. Math. 109 (2) (1992) 221–229, MR1172689.
[25] M.A. Kenku, F. Momose, Torsion points on elliptic curves defined over quadratic fields, Nagoya Math. J. 109 (1988) 125–149, https://doi.org/10.1017/S0027763000002816, MR931956.
[26] The LMFDB Collaboration, The L-functions and modular forms database, 2013, http://www.lmfdb.org.
[27] S. Lang, Algebra, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002, MR1878556.
[28] S. Lang, H. Trotter, Frobenius Distributions in GL_2-Extensions: Distribution of Frobenius Automorphisms in GL_2-Extensions of the Rational Numbers, Lecture Notes in Mathematics, vol. 504, Springer-Verlag, Berlin–New York, 1976, MR0568299.
[29] P. Lemos, Serre's uniformity conjecture for elliptic curves with rational cyclic isogenies, Trans. Amer. Math. Soc. 371 (1) (2019) 137–146, https://doi.org/10.1090/tran/7198, MR3885140.
[30] P. Lemos, Some cases of Serre's uniformity problem, Math. Z. 292 (1–2) (2019) 739–762, https://doi.org/10.1007/s00209-018-2189-8, MR3968924.
[31] B. Levi, Saggio per una teoria aritmetica delle forme cubiche ternarie, Atti Reale Accad. Sci. Torino 43 (1908), 99–120, 413–434, 672–681.
[32] Á. Lozano-Robledo, On the field of definition of p-torsion points on elliptic curves over the rationals, Math. Ann. 357 (1) (2013) 279–305, MR3084348.
[33] B. Mazur, Rational isogenies of prime degree (with an appendix by D. Goldfeld), Invent. Math. 44 (2) (1978) 129–162, MR482230.
[34] B. Mazur, Modular curves and the Eisenstein ideal, Publ. Math. Inst. Hautes Études Sci. 47 (1977) 33–186, 1978, MR488287.
[35] L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, Invent. Math. 124 (1–3) (1996) 437–449, MR1369424.
[36] J.S. Morrow, Composite images of Galois for elliptic curves over $\mathbb{Q}$ and entanglement fields, Math. Comp. 88 (319) (2019) 2389–2421, MR3957898.
[37] F. Najman, Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$, Math. Res. Lett. 23 (1) (2016) 245–272, MR3512885.
[38] L. Ribes, P. Zalesskii, Profinite Groups, 2nd ed., Ergebnisse der Mathematik und Ihrer Grenzgebiete. 3. Folge (Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics), vol. 40, Springer-Verlag, Berlin, 2010, MR2599132.
[39] J. Rouse, D. Zureick-Brown, Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois, Res. Number Theory 1 (2015), Art. 12, 34, MR3500996.
[40] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (4) (1972) 259–331, MR0387283.
[41] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, Publ. Math. Inst. Hautes Études Sci. (54) (1981) 323–401, MR644559.
[42] J.-P. Serre, Lectures on the Mordell-Weil Theorem, 3rd ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997, translated from the French and edited by Martin Brown from notes by Michel Waldschmidt; with a foreword by Brown and Serre, MR1757192.
[43] S. Siksek, Chabauty for symmetric powers of curves, Algebra Number Theory 3 (2) (2009) 209–236, https://doi.org/10.2140/ant.2009.3.209, MR2491943.
[44] A.V. Sutherland, Computing images of Galois representations attached to elliptic curves, Forum Math. Sigma 4 (2016), e4, 79, MR3482279.
[45] A.V. Sutherland, 2017, personal communication.

[46] A.V. Sutherland, Torsion subgroups of elliptic curves over number fields, preprint, available at https://math.mit.edu/~drew/MazursTheoremSubsequentResults.pdf.
[47] A.V. Sutherland, D. Zywina, Modular curves of prime-power level with infinitely many rational points, Algebra Number Theory 11 (5) (2017) 1199–1229, https://doi.org/10.2140/ant.2017.11.1199, MR3671434.
[48] M. Suzuki, Group Theory. I., Grundlehren der Mathematischen Wissenschaften (Fundamental Principles of Mathematical Sciences), vol. 247, Springer-Verlag, Berlin–New York, 1982, MR0648772.
[49] M. van Hoeij, Low degree places on the modular curve $X_1(N)$, preprint, arXiv:1202.4355.
[50] D. Zywina, On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$, preprint, arXiv:1508.07660.