# ON THE LEVEL OF MODULAR CURVES THAT GIVE RISE TO SPORADIC $j$-INVARIANTS

ABBEY BOURDON, ÖZLEM EJDER, YUAN LIU, FRANCES ODUMODU, AND BIANCA VIRAY

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 $\deg(x)$. Motivated by well-known classification problems concerning rational torsion of elliptic curves, we study sporadic points on the modular curves $X_1(N)$. In particular, we show that any non-cuspidal non-CM sporadic point $x \in X_1(N)$ maps down to a sporadic 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 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 points.

## 1. Introduction

Let $E$ be an elliptic curve over a number field $k$. It is well-known that the torsion subgroup $E(k)_{\rm tors}$ of the $k$-rational points is a finite subgroup of $(\mathbb{Q}/\mathbb{Z})^2$. In 1996, Merel [Mer96], building on work of Mazur [Maz77] and Kamienny [Kam92], 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 $E/k$,

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

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 [Fre94] observed that Faltings's theorem implies that an arbitrary curve $C$ over a number field $k$ can have infinitely many degree $d$ points if and only if these infinitely many points are parametrized by $\mathbb{P}^1_k$ or a positive rank subabelian variety of $\mathrm{Jac}(C)$. From this, Frey deduced that if a curve $C/k$ has infinitely many degree $d$-points, then the $k$-gonality of the curve[1] must be at most $2d$. Frey's criterion combined with Abramovich's lower bound on the gonality of modular curves [Abr96] 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[2]. 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 of arbitrary degree, focusing particularly on those corresponding to non-CM elliptic curves. We show that any sporadic point $x \in X_1(n)$ that corresponds to a non-CM elliptic curve $E$ maps down to a sporadic point on $X_1(\gcd(n, M_E))$, where $M_E$ denotes the level of the adelic Galois representation of $E$ (see Theorem 4.1).

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

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

Despite the fact that the level of the adelic Galois representation associated to an elliptic curve can be arbitrarily large, even after fixing the field of definition of the elliptic curve (see Section 2.3 for more details), we are able to use our techniques to show (conditionally) that non-CM non-cuspidal sporadic points $x \in X_1(n)$ map to sporadic points on $X_1(m)$ where $m$ is bounded by a constant that depends only on the degree of the $j$-invariant $j(x) \in \mathbb{P}^1$.

This result is conditional on a folklore conjecture motivated by a question of Serre.

**Conjecture 1.1** (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-$\ell$ Galois representation of $E$ is surjective for all $\ell > C$.*

**Conjecture 1.2** (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-$\ell$ Galois representation of $E$ is surjective for all $\ell > C$.*

**Remark 1.3.** Conjecture 1.1 when $k = \mathbb{Q}$, or equivalently Conjecture 1.2 when $d = 1$, is the case originally considered by Serre [Ser72, §4.3]. In this case, Serre asked whether $C$ could be taken to be 37 [Ser81, p.399]. The choice $C = 37$ has been formally conjectured by Zywina [Zyw, Conj. 1.12] and Sutherland [Sut16, Conj. 1.1].

We use $\operatorname{Spor}(n)$ to denote the set of sporadic points on $X_1(n)$ and use sporadic $j$-invariant to refer to any point in $\mathbb{P}^1_j$ that is the image of a point in $\cup_{n\in\mathbb{N}} \operatorname{Spor}(n)$. With this notation, we may now precisely state our main result.

**Theorem 1.4.** *Assume Conjecture 1.1. Then for any number field $k$, there exists a positive integer $A = A(k)$ such that*

$$j\left(\bigcup_{n\in\mathbb{N}} \operatorname{Spor}(n)\right) \cap \mathbb{P}^1_j(k) \subset j\left(\bigcup_{n\in\mathbb{N}, n|A} \operatorname{Spor}(n)\right).$$

*In particular, the set of $k$-rational sporadic $j$-invariants is finite. Moreover if the stronger Conjecture 1.2 holds, then $A$ depends only on $[k : \mathbb{Q}]$ so the set of sporadic $j$-invariants of bounded degree is finite.*

The bound $A$ in the theorem depends on the constant $C(k)$ or $C(d)$ from Conjecture 1.1 or Conjecture 1.2, respectively, and also depends on a uniform bound for the level of the $\ell$-adic Galois representationfor 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 $A$. This is discussed more in Section 7.

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 $\ell$ [CCS13]. Sutherland has extended this argument to sufficiently large composite integers [Sut].

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 a sporadic point on $X_1(21)$ corresponding to a non-CM elliptic curve with rational $j$-invariant [Naj16]. To date, it is still unknown whether this is the unique degree 3 sporadic point on the modular curves $X_1(n)$. Work of van Hoeij [vH] and Derickx–Sutherland [DS17] show that there are degree 5 sporadic points on $X_1(28)$ and $X_1(30)$ and a degree 6 sporadic point on $X_1(37)$.

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 3.6 is useful for determining the level of an $m$-adic Galois representation from information about the $\ell$-adic representations. In Section 4, we study sporadic points over a fixed non-CM $j$-invariant. Our main result therein shows that any non-CM non-cuspidal sporadic point $x$ can be mapped down to a sporadic point on a modular curve $X_1(n)$, where $n$ divides the level of the Galois representation associated to an elliptic curve with $j$-invariant $j(x)$. These results are used in Section 5 to prove Theorem 1.4.

Theorem 1.4 implies that, assuming Conjecture 1.2, there are finitely many sporadic $j$-invariants of bounded degree. This raises two interesting questions:

(1) Are there finitely many sporadic *points* lying over $j$-invariants of bounded degree, or can there be infinitely many sporadic points over a single $j$-invariant?
(2) In the case of degree 1, when there is strong evidence for Conjecture 1.2, can we come up with a candidate list for the rational sporadic $j$-invariants?

Question 1 is the focus of Section 6, where we show that any CM $j$-invariant has infinitely many sporadic points lying over it. Section 7 focuses on Question 2; there we provide a candidate list of levels from which the rational sporadic $j$-invariants can be found.


## Acknowledgements

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 Clay Mathematics Institute, Microsoft Research, the National Science Foundation, the Number Theory Foundation, and the Pacific Institute for Mathematics Sciences.

We thank Jeremy Rouse, Drew Sutherland, and David Zureick-Brown for helpful conversations. The third author was partially supported by NSF grant 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 $\mathrm{Gal}_k$ denotes the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$.

We use $\ell$ to denote a prime number and $\mathbb{Z}_\ell$ to denote the $\ell$-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 $G_{n^\infty}$, 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

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

By curve we mean a projective nonsingular 1-dimensional scheme over a field. For a curve $C$ over a 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 use $E$ to denote an elliptic curve, i.e., a curve of genus 1 with a specified point $O$. Throughout 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 $k$, we may assume that 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 $E$.

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

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

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 $X_1(n)$. In fact, we may view $X_1(n)$ as an algebraic curve defined over $\mathbb{Q}$ (See [DS05, Section 7.7] or [DR73] 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 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 $c_x = 1$. ∎

We say that a closed point $j \in \mathbb{P}^1_{\mathbb{Q}}$ is a sporadic $j$-invariant if there exists an elliptic curve $E/\mathbf{k}(j)$ with $j(E) = j$ and a torsion point $P \in E$ such that the point $x = [(E,P)] \in X_1(n)$ is sporadic, where $n$ is the order of $P$.

2.2.2. *Maps between modular curves.*

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

$$\deg(\pi) = c_\pi \cdot b^2 \prod_{p|b,\, p\nmid a} \left(1 - \frac{1}{p^2}\right),$$

*where $c_\pi = 1/2$ if $-I \in \Gamma_1(a)$ and $-I \notin \Gamma_1(ab)$ and $c_\pi = 1$ 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 $\Gamma_1(ab)\tau \mapsto \Gamma_1(a)\tau$. On non-cuspidal points, this map has the moduli interpretation $[(E,P)] \mapsto [(E,bP)]$, which shows that it is $\mathbb{Q}$-rational. The degree computation then follows from the formula [DS05, p.66], which states

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

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 $E[n]$, we obtain a Galois representation

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

whose image is uniquely determined up to conjugacy. After choosing compatible generators for each $n$, we obtain a Galois representation

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

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

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

to be the composition of $\rho_E$ with the projection onto the $\ell$-adic factors for $\ell | n$. Note that $\rho_{E,n^\infty}$ depends only on the support of $n$.

If $E/k$ does not have complex multiplication, then Serre's Open Image Theorem [Ser72] states that $\rho_E(\operatorname{Gal}_k)$ is open—and hence of finite index—in $\operatorname{GL}_2(\hat{\mathbb{Z}})$. Since the kernels of the natural projection maps $\operatorname{GL}_2(\hat{\mathbb{Z}}) \to \operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})$ form a fundamental system of open neighborhoods of the identity in $\operatorname{GL}_2(\hat{\mathbb{Z}})$ [RZ10, Lemma 2.1.1], it follows that for any open subgroup $G$ of $\operatorname{GL}_2(\hat{\mathbb{Z}})$ 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 $M_E$. Further, for any finite set of primes $S$, we let $M_E(S)$ be the least positive integer such that $\operatorname{im} \rho_{E,\mathfrak{m}_S^\infty} = \pi^{-1}(\operatorname{im} \rho_{E,M_E(S)})$.

We also define

$$S_E = S_{E/k} := \{2,3\} \cup \{\ell : \rho_{E,\ell^\infty}(\operatorname{Gal}_k) \neq \operatorname{GL}_2(\mathbb{Z}_\ell)\}\,; \tag{2.1}$$

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

For any elliptic curve $E/\mathbb{Q}$ with discriminant $\Delta_E$, Serre observed that the quadratic 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 $\Delta_E$, then $2\ell$ must divide the level $M_E$ (see [Jon09a, Sec. 3] for more details). In particular, the level of an elliptic curve can be arbitrarily large. In contrast, for a fixed prime $\ell$, the level of the $\ell$-adic Galois representation is bounded depending only on the degree of the field of definition.

**Theorem 2.3** ([CT13, Theorem 1.1], see also [CP, Theorem 2.3])**.** *Let $d$ be a positive integer and let $\ell$ be a prime number. There exists a constant $C = C(d)$ 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 $\mathrm{GL}_2(\hat{\mathbb{Z}})$

The proofs in this paper involve a detailed study of the mod-$n$, $\ell$-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 $\ell \geq 5$ is a prime such that $G_\ell = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, then for any integer $n$ relatively prime to $\ell$, 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 $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ only if $\ell | n$. This result is known in the case $\ell > 5$ (see [Coj05, 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 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 $\ell$-adic components.

### 3.1. Goursat's Lemma.

**Lemma 3.1** (Goursat's Lemma, see e.g., [Lan02, pg75] or [Gou89])**.** *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 $N := \ker(\rho)$ and $N' := \ker(\rho')$; one can identify $N$ as a normal subgroup of $G'$ and $N'$ as a normal subgroup of $G$. Then the image of $H$ in $G \times G'$ 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 such that $G_\ell = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. 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 $\ell \nmid n$.*

The proof of this proposition relies on the following classification of subquotients of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. In the case $\ell > 5$, this classification result was proved by Kani [Coj05, Appendix, Corollary 11].

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

*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 isomorphism when restricted to any subquotient isomorphic to $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

(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 $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ 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 $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ then there is a $p \in T$ such that $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ has a subquotient isomorphic to $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

(3) If $p$ and $\ell$ are primes with $\ell \geq 5$ and $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ has a subquotient isomorphic to $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$, then $p = \ell$.

**Proof of Claim 1:** Let $N \lhd G < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be subgroups and let $\pi$ 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 $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is the trivial group, if $G/N \cong \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$, 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 $G/N \cong \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Let $H$ be the normal subgroup of $G$ containing $N$ such that $H/N \cong \mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Consider the following two maps
$$\pi_S\colon \prod_{p \in T} \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z}) \to \prod_{p \in S} \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z}) \quad \text{and} \quad \pi_{S^c}\colon \prod_{p \in T} \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z}) \to \prod_{p \in T-S} \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z}).$$
Since the only quotient of $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ that contains a subgroup isomorphic to $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ 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 $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Furthermore, since $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ 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
$$\frac{H \cap \ker \pi_S}{N \cap \ker \pi_S} \cong \mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}) \quad \text{and} \quad \frac{H \cap \ker \pi_{S^c}}{N \cap \ker \pi_{S^c}} \cong \mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

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

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

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 $(\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}))^2$ are $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}) \times \{1\}$ or $\{1\} \times \mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ (see [LW, Proof of Lemma 6.1]), 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 $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$. If $p \nmid \#G$, then by [Ser72, 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 isomophic to $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$. 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 [Suz82, 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 $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$, $G \cap \mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ cannot be solvable and hence $G = \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ and $p = \ell$. □

*Proof of Proposition 3.2.* Since $G_{\ell^s n}$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^s n\mathbb{Z}) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell^s\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, 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 $G_{\ell^s}$ 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 $s = 1$. If $\ker \varpi_1$ is contained in the center of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, then the left-hand side of (3.2) has a quotient $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$, which contradicts Lemma 3.3. Hence, by [Art57, Theorem 4.9], $\ker \varpi_1$ must contain $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

For $s > 1$, since $\varpi_s$ 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 [Coj05, Appendix, Lemma 12]. □

### 3.3. **Bounding the level from the index.**

**Proposition 3.4** ([LT76, Part I, §6, Lemmas 2 & 3]). *Let $\ell$ be a prime and let $G$ be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Set $s_0 = 1$ if $\ell$ 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 3.5.** 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 [LT76, 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 $\ell^{th}$ 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 $k$:

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

where the vertical maps are raising to the $(\ell^k)^{th}$ 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 $\ell$-adic components.

**Proposition 3.6.** *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.

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

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 $\ell_i$. Similarly, the order of the kernel of the lower horizontal map is a power of $\ell_i$, while the order of the kernels of the vertical maps are coprime to $\ell_i$. 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 $1 \leq q' \leq q$ and let $\{r_i\}_{i=1}^{q'}$ be a collection of positive integers. Consider the following commutative diagram of natural reduction maps.

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

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. Sporadic 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

$$S_E = S_{E/k} := \{2, 3\} \cup \{\ell : \rho_{E,\ell^\infty}(\mathrm{Gal}_k) \neq \mathrm{GL}_2(\mathbb{Z}_\ell)\} .$$

In this section we show that any non-cuspidal non-CM sporadic point on $x \in X_1(n)$ maps to a sporadic point on $X_1(a)$ for some $a$ dividing $M_{E_x}(S_{E_x})$, where $E_x$ is an elliptic curve over $\mathbb{Q}(j(x))$ with $j$-invariant $j(x)$. More precisely, we prove the following theorem.

**Theorem 4.1.** *Fix a non-CM elliptic curve $E$ over $k := \mathbb{Q}(j(E))$. 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*

$$\operatorname{im} \rho_{E,\mathfrak{m}_S^\infty} = \pi^{-1}(\operatorname{im} \rho_{E,M}). \tag{4.1}$$

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

**Remark 4.2.** Note that if $E$ and $E'$ are quadratic twists of each other, both defined over $\mathbb{Q}(j(E))$, then $S_E = S_{E'}$ (see, e.g., [Sut16, Lemma 5.27]). Furthermore, for any $S$,

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

(see, e.g., [Sut16, 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 (4.1) for all quadratic twists of a fixed elliptic curve.

**Corollary 4.3.** *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 points on $X_1(\ell^s)$ lying over $j(E)$ for any $s \in \mathbb{N}$.*

In Section 4.1 we give a numerical criterion for when a non-cuspidal non-CM sporadic point on $X_1(n)$ maps to a sporadic point on a modular curve of lower level. This numerical criterion is then used in two different ways. First, to shrink the support of $n$ by removing primes $\ell$ for which the corresponding elliptic curve has surjective $\ell$-adic Galois representation (see Section 4.2), and second, to understand sporadic points on $X_1(n')$ for integers $n'$ with bounded support (see Section 4.3). The results of these two sections are brought together in Section 4.4 to prove Theorem 4.1.

**Remark 4.4.** 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 4.3 alone then imply that any sporadic point on $x \in X_1(n)$ with $j(x) = j(E)$ maps to a sporadic point on $X_1(\gcd(n, M_E))$, which yields a slightly weaker version of Theorem 4.1.

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 Theorem 4.1, namely Theorem 1.4 (see §5).

### 4.1. **Reducing sporadic points to a lower level.**

**Proposition 4.5.** *Let $a$ and $b$ be positive integers, $E$ a non-CM elliptic curve over $k := \mathbb{Q}(j(E))$, and $P \in E$ a point of order $ab$. Assume that $[k(P) : k(bP)]$ is as large as possible, i.e., that $[k(P) : k(bP)] = \#\{Q \in E : bQ = bP, Q \text{ order } ab\}$. If $x = [(E, P)] \in X_1(ab)$ is a sporadic point, then $\pi(x) \in X_1(a)$ is a sporadic point, where $\pi$ denotes the natural map $X_1(ab) \to X_1(a)$.*

Before proving Proposition 4.5, we first prove the following lemma, which will be used in the proof.

**Lemma 4.6.** *Let $a$ and $b$ be positive integers, $E$ a non-CM elliptic curve over $k := \mathbb{Q}(j(E))$, and $P \in E$ a point of order $ab$. Let $x := [(E, P)] \in X_1(ab)$ and let $\pi(x)$ be the image of $x$ under 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*

$$\deg(x) = \deg(\pi(x)) \deg(X_1(ab) \to X_1(a)).$$

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

$$\#\{Q \in E : bQ = bP, Q \text{ order } ab\} = \begin{cases} 2\deg(X_1(ab) \to X_1(a)) & \text{if } a \leq 2 \text{ and } ab > 2, \\ \deg(X_1(ab) \to X_1(a)) & \text{otherwise.} \end{cases} \tag{4.2}$$

Let us first consider the case that $a \leq 2$ and $ab > 2$. Then $\deg(\pi(x)) = [k(bP) : \mathbb{Q}]$. 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 (4.2) yields the desired result.

Now assume that $ab \leq 2$. Then $\deg(\pi(x)) = [k(bP) : \mathbb{Q}]$ and $\deg(x) = [k(P) : \mathbb{Q}]$, so (4.2) again yields the desired result.

Finally we consider the case when $a > 2$. Note that for any point $y \in X_1(ab)$, $\deg(y) \leq \deg(\pi(y)) \cdot \deg(X_1(ab) \to X_1(a))$. Combining this with (4.2), it remains to prove that

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

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

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

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

*Proof of Proposition 4.5.* For any point $y \in X_1(ab)$,

$$\deg(y) \leq \deg(\pi(y)) \cdot \deg(X_1(ab) \to X_1(a)).$$

If $\pi(x)$ is not sporadic, then there exist infinitely many points $x' \in X_1(ab)$ such that $\deg(\pi(x)) \geq \deg(\pi(x'))$. Lemma 4.6 implies that for each of these infinitely many points $x' \in X_1(ab)$ we have

$$\deg(x) = \deg(\pi(x)) \cdot \deg(X_1(ab) \to X_1(a)) \geq \deg(\pi(x')) \cdot \deg(X_1(ab) \to X_1(a)) \geq \deg(x'),$$

which implies that $x$ is not sporadic. □

## 4.2. Eliminating primes with surjective Galois representation.

**Proposition 4.7.** *Let $E$ be a non-CM elliptic curve over $k := \mathbb{Q}(j(E))$, let $\ell \geq 5$ be a prime such that $\rho_{E,\ell^\infty}$ is surjective, and let $a$ and $s$ be positive integers with $\ell \nmid a$. If $x \in X_1(a\ell^s)$ is a sporadic point with $j(x) = j(E)$, then $\pi(x) \in X_1(a)$ is a sporadic point.*

The following lemma will be useful in the proof of Proposition 4.7.

**Lemma 4.8.** *Let $a$ and $b$ be relatively prime positive integers, $E$ a non-CM elliptic curve over $k := \mathbb{Q}(j(E))$, and $P \in E$ a point of order $ab$. Let $H := \ker(\operatorname{im}\rho_{E,ab} \to \operatorname{im}\rho_{E,a})$ and $B_b^1 \subset \operatorname{Aut}(E[b])$ be the stabilizer of $aP$. If $\#\,(H/H \cap B_b^1) = \#\,(\operatorname{Aut}(E[b])/B_b^1)$, then $x := [(E,P)] \in X_1(ab)$ sporadic implies that $\pi(x) \in X_1(a)$ is sporadic.*

*Proof.* Let $B_{ab}^1 \subset \operatorname{Aut}(E[ab])$ be the stabilizer of $P$. By the definition of $H$, we have the following exact sequence

$$1 \to H \cap B_{ab}^1 \to (\operatorname{im}\rho_{E,ab}) \cap B_{ab}^1 \to (\operatorname{im}\rho_{E,a}) \cap B_a^1. \tag{4.3}$$

Consideration of the towers of fields $k(E[ab]) \supset k(P) \supset k(bP)$ and $k(E[ab]) \supset k(E[a]) \supset k(bP)$ together with (4.3) gives the following inequality, where $B_a^1 \subset \operatorname{Aut}(E[a])$ is the stabilizer of $bP$:

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

On the other hand, we have

$$\#\left(\operatorname{Aut}(E[b])/B_b^1\right) = \#\{Q \in E : bQ = bP,\ Q \text{ order } ab\} \geq [k(P):k(bP)],$$

so by assumption we have $[k(P):k(bP)] = \#\{Q \in E : bQ = bP,\ Q \text{ order } ab\}$. Proposition 4.5 then completes the proof. ☐

*Proof of Proposition 4.7.* Let $H$ denote the kernel of the projection map $\operatorname{im}\rho_{E,a\ell^s} \to \operatorname{im}\rho_{E,a}$, let $P \in E$ be such that $x = [(E,P)]$, and let $B_{\ell^s}^1 \subset \operatorname{Aut}(E[\ell^s])$ be the stabilizer of $aP$. By Proposition 3.2 applied to $\operatorname{im}\rho_E$, $H$ contains $\mathrm{SL}_2(\mathbb{Z}/\ell^s\mathbb{Z})$, thus we have set inclusions

$$\mathrm{SL}_2(\mathbb{Z}/\ell^s\mathbb{Z})/\left(\mathrm{SL}_2(\mathbb{Z}/\ell^s\mathbb{Z})\cap B_{\ell^s}^1\right) \hookrightarrow H/\left(H\cap B_{\ell^s}^1\right) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell^s\mathbb{Z})/(\mathrm{GL}_2(\mathbb{Z}/\ell^s\mathbb{Z})\cap B_{\ell^s}^1).$$

The sets on the right and the left have the same cardinality hence all inclusions are bijections, and so we may apply Lemma 4.8 with $b = \ell^s$. ☐

## 4.3. Sporadic points on $X_1(n)$ where $n$ has specified support.

**Proposition 4.9.** *Let $E$ be a non-CM elliptic curve over $k := \mathbb{Q}(j(E))$, 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 $\operatorname{Supp}(M) \subset S$ such that*

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

*and let $a$ and $b$ be positive integers with $\gcd(ab,M)|a$ and $\operatorname{Supp}(ab) \subset S$. If $x \in X_1(ab)$ is a sporadic point with $j(x) = j(E)$, then $\pi(x) \in X_1(a)$ is a sporadic point, where $\pi$ denotes the natural map $X_1(ab) \to X_1(a)$.*

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

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

where by abuse of notation, we use $\pi$ 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, Proposition 4.5 completes the proof. □

4.4. **Proof of Theorem 4.1.** Let $n$ be a positive integer such that there is a sporadic point $x \in X_1(n)$ with $j(x) = j(E)$ and write $n = n_0 n_1$ where $\operatorname{Supp}(n_0) \subset S$ and $\operatorname{Supp}(n_1)$ is disjoint from $S$. Note that $\gcd(n, M) | n_0$. By inductively applying Proposition 4.7 to powers of primes $\ell \notin S_E$, we see that $\pi(x) \in X_1(n_0)$ is sporadic where $\pi$ denotes the natural map $X_1(n) \to X_1(n_0)$. Then an application of Proposition 4.9 with $a = \gcd(n, M)$, $b = n_0 / \gcd(n, M)$, and $\pi(x) \in X_1(ab)$ completes the proof. □

## 5. Proof of Theorem 1.4

In this section we prove Theorem 1.4. Since there are only finitely many CM $j$-invariants of bounded degree and the map $j$ maps any cusp to $\infty$, it suffices to prove Theorem 1.4 for sporadic points corresponding to non-CM elliptic curves. For a fixed number field $k$, Conjecture 1.1 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 1.2 implies that $S(k)$ can be taken to depend only on $[k : \mathbb{Q}]$. Thus, to deduce Theorem 1.4 from Theorem 4.1, 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 5.1 completes the proof of Theorem 1.4.

**Proposition 5.1.** *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 5.2.** In the proof of Proposition 5.1(2), if $\operatorname{im} \rho_{E,\mathfrak{m}_{S-\{\ell\}}}$ is a Sylow $\ell$-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 $\tau$. 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 5.3.** A weaker version of Proposition 5.1 follows from [Jon09b, 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 $S = \{2,3,5\} \cup \{p : \operatorname{im}\rho_{E,p} \neq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})\} \cup \operatorname{Supp}(\Delta_E)$ as is stated) and shows that $v_\ell(M_d(S,\mathcal{E})) \leq \max(v_\ell(M_d(\{\ell\},\mathcal{E})), v_\ell(2\ell)) + v_\ell(\#\,\mathrm{GL}_2(\mathbb{Z}/\mathfrak{m}_{S-\{\ell\}}\mathbb{Z}))$. The structure of the proof here and the one in [Jon09b] roughly follow the same structure; however, by isolating the purely group-theoretic components (e.g., Proposition 3.6), we are able to obtain a sharper bound in (2).

*Proof.* When $\#S = 1$, part (1) follows from Theorem 2.3 and Proposition 3.4 and part (2) is immediate.

We prove part (1) when $\#S$ is arbitrary by induction using Proposition 3.6. 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 3.6 implies that we may take $M = \prod_i \ell_i^{t_i}$.

Fix $i \in \{1,\ldots,q\}$. 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

$$\begin{array}{ccc} \operatorname{im}\rho_{E,\ell_i^{r+1}}/K^i_{E,r+1} & \twoheadrightarrow & \operatorname{im}\rho_{E,\ell_i^r}/K^i_{E,r} \\ \downarrow \cong & & \downarrow \cong \\ \operatorname{im}\rho_{E,N_i}/L^i_{E,r+1} & = & \operatorname{im}\rho_{E,N_i}/L^i_{E,r} \end{array} \tag{5.1}$$

where the vertical isomorphisms are given by Goursat's Lemma (Lemma 3.1)[3]. 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 (5.1) implies that $K^i_{E,r+1}$ is the full preimage of $K^i_{E,r}$ under the natural reduction map. Then by Proposition 3.4, $K^i_E$ 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.

$$\begin{array}{ccc} \operatorname{im}\rho_{E,\ell_i^s}/K^i_{E,s} & \twoheadrightarrow & \operatorname{im}\rho_{E,\ell^{s_i}}/K^i_{E,s_i} \\ \downarrow \cong & & \downarrow \cong \\ \operatorname{im}\rho_{E,N_i}/L^i_{E,s} & \twoheadrightarrow & \operatorname{im}\rho_{E,N_i}/L^i_{E,s_i} \end{array} \tag{5.2}$$

[3] 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.

The kernel of the top horizontal map is an $\ell_i$-primary subgroup, so the index of $L^i_{E,s}$ in $L^i_{E,s_i}$ is a power of $\ell_i$. 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. 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 6.2), 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 6.1.** *Let $E$ be an elliptic curve with CM by an order in an imaginary quadratic field $K$. Then for all sufficiently large primes $\ell$ 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 $\pi$ denotes the natural map $X_1(d\ell) \to X_1(\ell)$.*

The key to the proof of Theorem 6.1 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 [Abr96] and the result of Frey [Fre94] 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 6.2.** *Suppose there is a sporadic point $x \in X_1(N)$ with*

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

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

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

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

By [Abr96, Thm. 0.1], $\deg(y) < \frac{1}{2}\operatorname{gon}_{\mathbb{Q}}(X_1(dN))$. Thus $y$ is sporadic by [Fre94, Prop. 2]. ☐

*Proof of Theorem 6.1.* 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 [Cox13, Thms. 7.24 and 11.1] for details.) Let $\ell$ 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 [BC, Thm. 6.2], there is a point $P \in E$ of order $\ell$ with

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

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

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

The result now follows from Lemma 6.2. □

**Remark 6.3.** Note that none of the known non-cuspidal non-CM sporadic points satisfy the degree condition given in Lemma 6.2. 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 1.4 there would be only finitely many non-CM sporadic points corresponding to $j$-invariants of bounded degree, assuming Conjecture 1.2.

## 7. Sporadic points with rational $j$-invariant

In this section, we study non-CM sporadic points with rational $j$-invariant. Our main result of this section (Theorem 7.1) gives a classification of the non-cuspidal non-CM sporadic 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 sporadic 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 7.3), is a power of 2 (Proposition 7.4), or, conditionally on Sutherland [Sut16, Conj. 1.1] and Zywina [Zyw, Conj. 1.12]), has $\min(\mathrm{Supp}(n)) \ge 17$ (Proposition 7.5), then any non-CM, non-cuspidal sporadic point with rational $j$-invariant has $j(x) = -7 \cdot 11^3$.

### 7.1. Classification of non-CM sporadic points with rational $j$-invariant.

**Theorem 7.1.** *Let $x \in X_1(n)$ be a non-CM non-cuspidal sporadic 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 $\rho_{E,\ell_1}$ and $\rho_{E,\ell_2}$ are not surjective.*
3. *There is an elliptic curve $E/\mathbb{Q}$ with $j(E) = j(x)$ and a prime $2 < \ell \le 37$ in $\mathrm{Supp}(n)$ such that the $\ell$-adic Galois representation of $E$ has level greater than $169$.*

(4) *There is a divisor of $n$ of the form $2^a3^bp^c$ such that the image of $x$ in $X_1(2^a3^bp^c)$ is sporadic 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 7.2.** 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 [Sut16, Conj. 1.1] and Zywina [Zyw, Conj. 1.12].

Elliptic curves as in (2) correspond to points on finitely many modular curves of genus at least 2, so there are at worst finitely many $j$-invariants in this case [CLM+]. Additionally, there are no elliptic curves in the LMFDB database [LMFDB] 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 [Sut16].)

Sutherland and Zywina's classification of modular curves of prime-power level with infinitely many points [SZ17] 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 7.1 gives, for each prime $\ell$, the maximal prime-power level for which there exists a modular curve of that level with infinitely many rational points. Therefore, for $3 \leq \ell \leq 37$,

| $\ell$ | 3 | 5 | 7 | 11 | 13 | 17 | 37 |
|---|---|---|---|---|---|---|---|
| max level | 27 | 25 | 7 | 11 | 13 | 1 | 1 |

TABLE 7.1. Maximal prime-power level for which there exists a modular curve with infinitely many rational points

respectively, there are already only finitely many $j$-invariants of elliptic curves with an $\ell$-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 $\ell$-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 $\ell$-adic Galois representation: $-17 \cdot 373^3/2^{17}$, $-17^2 \cdot 101^3/2$, $-7 \cdot 11^3$, and $-7 \cdot 137^3 \cdot 2083^3$ [Zyw, Conj. 1.12]. For each of these $j$-invariants, Sutherland computed that the $\ell$-adic Galois representation is the full preimage of the mod $\ell$ representation, so the representations are indeed of level $\ell$ and not level $\ell^2$ [Sut17].[4]

*Proof.* Let $x \in X_1(n)$ be a non-cuspidal non-CM sporadic 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 $\ell$ representation for every $\ell > 17$ and $\ell \neq 37$. Thus Proposition 4.7 implies that $x$ maps to a sporadic 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.

[4]Sutherland used a generalization of the algorithm in [Sut16] to prove in each case the index of the mod-$\ell^2$ image is no smaller than that of the mod-$\ell$ image. It then follows from [SZ17, Lemma 3.7] that the $\ell$-adic image is the full preimage of the mod-$\ell$ image.

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 4.7 show that $x$ maps to a sporadic point on $X_1(n'')$ where $n''$ is a divisor of $n'$ with $\operatorname{Supp}(n'') \subset S := \{2, 3, p\}$[5] and $p \in \{1, 5, 7, 11, 13, 17, 37\}$. Furthermore, Theorem 4.1 shows that $x$ maps to a sporadic 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 5.1 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 [RZB15, Corollary 1.3], we have the following values for the constant $M_1(\{\ell\}, \mathcal{E})$ from Proposition 5.1.

| $\ell$ | 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 5.1(2),

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

This upper bound combined with Table 7.2 yields the desired divisibility except for the case where $p = 17$ or $p = 37$.

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

TABLE 7.2. Cardinality of $\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$

Let us consider the case that $p = 17$, so $\rho_{E,17}$ is not surjective. Since we are not in case (1), we know $\operatorname{im} \rho_{E,17}$ is not contained in the normalizer of the non-split Cartan. Thus [Zyw, Thms. 1.10 and 1.11] show that $\# \operatorname{im} \rho_{E,17} = 2^6 17$, so Proposition 5.1(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 [Zyw, Thms. 1.10 and 1.11] show that $\# \operatorname{im} \rho_{E,37} = 2^4 3^3 37$ and so Proposition 5.1(2) implies that the level of the $\mathfrak{m}_S^\infty$ Galois representation divides $2^{13} 3^8 37$. ☐

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

**Proposition 7.3.** *Fix a prime $\ell$. 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 $\ell \leq 10$. Further, $X_1(\ell)$ has gonality 2 for $\ell = 11, 13$, and no non-cuspidal rational points [Maz77]. Hence if $x \in X_1(\ell)$ is a non-cuspidal non-CM sporadic point, $\ell > 13$.

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

If the mod $\ell$ Galois representation of $E$ is surjective, then $x$ cannot be a sporadic point on $X_1(\ell)$ by Corollary 4.3, 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 $\mathrm{GL}_2(\mathbb{F}_\ell)$ [Ser72, 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 [LR13, Theorem 7.3] shows that the degree of a field of definition of a point of order $\ell$ is greater than or equal to $(\ell^2-1)/6$. Since $\ell > 13$ we have

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

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 [BPR13], $\ell$ has to be less than or equal to 13. Similarly, if im $\rho_{E,\ell}$ is one of the exceptional subgroups, then by [LR13, 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 $\ell$. By [Maz78], $\ell$ is one of the following primes: $2, 3, 5, 7, 11, 13, 17, 37$. Thus we need only consider $\ell = 17$ and 37. For $\ell = 17$, [LR13, Table 5] shows that $\deg(x) \geq 4$. Since the gonality of $X_1(17)$ is also 4, $x$ cannot be sporadic.

Finally when $\ell = 37$, $X_0(37)$ has a point over $\mathbb{Q}$ which corresponds to a degree 6 point on $X_1(37)$, and this is sporadic since $\mathrm{gon}_{\mathbb{Q}} X_1(37) = 18$. The $j$-invariant of the corresponding point on $X_1(37)$ is given as $-7 \cdot 11^3$ in [LR13, Table 5]. The only other point on $X_1(37)$ that has rational $j$-invariant and whose Galois representation is contained in a Borel subgroup is a point of degree 18, so is not sporadic. ☐

**Proposition 7.4.** *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 [RZB15, 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 4.9 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 by [Maz78, Theorem 2], $X_1(16)$ 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 [DvH14, 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 [RZB15, 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 $32^{\text{nd}}$ 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 7.5.** *Let $n$ be a positive integer with $\min(\mathrm{Supp}(n)) \geq 17$. Assume* [Sut16, Conj. 1.1] *or* [Zyw, 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 7.1. By assumption and Remark 7.2, cases (1) and (3) of Theorem 7.1 do not occur. Further, case (2) only occurs if $17 \cdot 37|n$ and $\operatorname{im} \rho_{E,17}$ and $\operatorname{im} \rho_{E,37}$ are both contained in Borel subgroups (see proof of Proposition 7.3), which is impossible (see, e.g., [LR13, Table 4]).

Hence, we must be in case (4) of Theorem 7.1. 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 7.1(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 7.3 then completes the proof. □

## References


[Abr96] Dan Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices **20** (1996), 1005–1011. MR1422373

[Art57] E. Artin, *Geometric algebra*, Interscience Publishers, Inc., New York-London, 1957. MR0082463

[BPR13] Yuri Bilu, Pierre Parent, and Marusia Rebolledo, *Rational points on $X_0^+(p^r)$*, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 3, 957–984 (English, with English and French summaries). MR3137477

[BC] Abbey Bourdon and Pete L. Clark, *Torsion points and Galois representations on CM elliptic curves*. preprint, `arXiv:1612.03229`.

[CT13] Anna Cadoret and Akio Tamagawa, *A uniform open image theorem for $\ell$-adic representations, II*, Duke Math. J. **162** (2013), no. 12, 2301–2344. MR3102481

[CLM+] Catalina Camacho, Wanlin Li, Jackson S. Morrow, Jack Petok, and David Zureick-Brown, *Composite level images of Galois and hyperelliptic modular curves*. preprint.

[CCS13] Pete L. Clark, Brian Cook, and James Stankewicz, *Torsion points on elliptic curves with complex multiplication (with an appendix by Alex Rice)*, Int. J. Number Theory **9** (2013), no. 2, 447–479. MR3005559

[CP] Pete L. Clark and Paul Pollack, *Pursuing polynomial bounds on torsion*. preprint, `arXiv:1705.10401`.

[Coj05] Alina Carmen Cojocaru, *On the surjectivity of the Galois representations associated to non-CM elliptic curves*, Canad. Math. Bull. **48** (2005), no. 1, 16–31, DOI 10.4153/CMB-2005-002-x. With an appendix by Ernst Kani. MR2118760

[Cox13] David A. Cox, *Primes of the form $x^2 + ny^2$*, 2nd ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013. Fermat, class field theory, and complex multiplication. MR3236783

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349 (French). MR0337993

[DvH14] Maarten Derickx and Mark van Hoeij, *Gonality of the modular curve $X_1(N)$*, J. Algebra **417** (2014), 52–71. MR3244637

[DS17] Maarten Derickx and Andrew V. Sutherland, *Torsion subgroups of elliptic curves over quintic and sextic number fields*, Proc. Amer. Math. Soc. **145** (2017), no. 10, 4233–4245. MR3690609

[DS05] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005. MR2112196

[Fre94] Gerhard Frey, *Curves with infinitely many points of fixed degree*, Israel J. Math. **85** (1994), no. 1-3, 79–83. MR1264340

[Gou89] Edouard Goursat, *Sur les substitutions orthogonales et les divisions régulières de l'espace*, Ann. Sci. École Norm. Sup. (3) **6** (1889), 9–102 (French). MR1508819

[Jon09a] Nathan Jones, *Averages of elliptic curve constants*, Math. Ann. **345** (2009), no. 3, 685–710. MR2534114

[Jon09b] ———, *A bound for the torsion conductor of a non-CM elliptic curve*, Proc. Amer. Math. Soc. **137** (2009), no. 1, 37–43. MR2439422

[Kam92] S. Kamienny, *Torsion points on elliptic curves and $q$-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229. MR1172689

[LMFDB] The LMFDB Collaboration, *The L-functions and Modular Forms Database* (2013). `http://www.lmfdb.org`.

[Lan02] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR1878556

[LT76] Serge Lang and Hale Trotter, *Frobenius distributions in $\mathrm{GL}_2$-extensions*, Lecture Notes in Mathematics, Vol. 504, Springer-Verlag, Berlin-New York, 1976. Distribution of Frobenius automorphisms in $\mathrm{GL}_2$-extensions of the rational numbers. MR0568299

[LW] Yuan Liu and Melanie Metchatt Wood, *The free group on $n$ generators modulo $n + u$ random relations as $n$ goes to infinity*. preprint, `arXiv:1708.08509`.

[LR13] Álvaro Lozano-Robledo, *On the field of definition of $p$-torsion points on elliptic curves over the rationals*, Math. Ann. **357** (2013), no. 1, 279–305. MR3084348

[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162. MR482230

[Maz77] ———, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). MR488287

[Mer96] Loïc Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1-3, 437–449 (French). MR1369424

[Naj16] Filip Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$*, Math. Res. Lett. **23** (2016), no. 1, 245–272. MR3512885

[RZ10] Luis Ribes and Pavel Zalesskii, *Profinite groups*, 2nd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 40, Springer-Verlag, Berlin, 2010. MR2599132

[RZB15] Jeremy Rouse and David Zureick-Brown, *Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois*, Res. Number Theory **1** (2015), Art. 12, 34. MR3500996

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331 (French). MR0387283

[Ser81] ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401 (French). MR644559

[Ser98] ———, *Abelian $l$-adic representations and elliptic curves*, Research Notes in Mathematics, vol. 7, A K Peters, Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute; Revised reprint of the 1968 original. MR1484415

[Sut16] Andrew V. Sutherland, *Computing images of Galois representations attached to elliptic curves*, Forum Math. Sigma **4** (2016), e4, 79. MR3482279

[Sut17] ———, 2017. Personal communication.

[Sut] ———, *Torsion subgroups of elliptic curves over number fields*. preprint, available at `https://math.mit.edu/~drew/MazursTheoremSubsequentResults.pdf`.

[SZ17] Andrew V. Sutherland and David Zywina, *Modular curves of prime-power level with infinitely many rational points*, Algebra Number Theory **11** (2017), no. 5, 1199–1229, DOI 10.2140/ant.2017.11.1199. MR3671434

[Suz82] Michio Suzuki, *Group Theory. I.*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 247, Springer-Verlag, Berlin-New York, 1982. MR0648772

[vH] Mark van Hoeij, *Low degree places on the modular curve $X_1(N)$*. preprint, `arXiv:1202.4355`.

[Zyw] D. Zywina, *On the possible images of the mod $\ell$ representations associated to elliptic curves over $\mathbb{Q}$*. preprint, `arXiv:1508.07660`.

Wake Forest University, Department of Mathematics and Statistics, Winston-Salem, NC 27109, USA
*E-mail address*: bourdoam@wfu.edu
*URL*: http://users.wfu.edu/bourdoam/

Colorado State University, Department of Mathematics, Fort Collins, CO 80524, USA
*E-mail address*: ejder@math.colostate.edu
*URL*: https://sites.google.com/site/ozheidi/Home

University of Wisconsin-Madison, Department of Mathematics, 480 Lincoln Drive, Madison, WI 53705, USA
*E-mail address*: yliu@math.wisc.edu
*URL*: http://www.math.wisc.edu/~yliu/

Institut de Matheématiques de Bordeaux Universiteé Bordeaux 1 351, cours de la Libeération 33405 Talence cedex France; and
Dipartimento di Matematica Pura ed Applicata, Università degli Studi di Padova, Via Trieste 63, 35121, Padova, Italy
*E-mail address*: francesodumodu@gmail.com

University of Washington, Department of Mathematics, Box 354350, Seattle, WA 98195, USA
*E-mail address*: bviray@math.washington.edu
*URL*: http://math.washington.edu/~bviray