# ODD DEGREE ISOLATED POINTS ON $X_1(N)$ WITH RATIONAL $j$-INVARIANT

ABBEY BOURDON, DAVID R. GILL, JEREMY ROUSE, AND LORI D. WATSON

Abstract. Let $C$ be a curve defined over a number field $k$. We say a closed point $x \in C$ of degree $d$ is isolated if it does not belong to an infinite family of degree $d$ points parametrized by the projective line or a positive rank abelian subvariety of the curve's Jacobian. Building on work of [11], we characterize elliptic curves with rational $j$-invariant which give rise to an isolated point of odd degree on $X_1(N)/\mathbb{Q}$ for some positive integer $N$.

## 1. Introduction

Let $C$ be a curve defined over a number field $k$, and let $x \in C$ be a closed point of degree $d$. Following [11], we say $x$ is **isolated** if it does not belong to an infinite family of degree $d$ points parametrized by $\mathbb{P}^1$ or a positive rank abelian subvariety of the curve's Jacobian. (See §2.5 for details.) Motivated by the well-known problem of classifying torsion subgroups of elliptic curves over number fields, we seek to describe isolated points on the modular curve $X_1(N)/\mathbb{Q}$. As a first case, we focus on those isolated points corresponding to elliptic curves with rational $j$-invariant. That is, we consider isolated points $x \in X_1(N)$ such that $j(x) \in \mathbb{Q}$, where $j : X_1(N) \to X_1(1) \cong \mathbb{P}^1$ denotes the $j$-map. Though there are infinitely many isolated points with this condition—indeed, there are infinitely many isolated points above any $j$-invariant associated to an elliptic curve with complex multiplication (CM) by [11, Thm. 7.1]—there is strong evidence that all isolated points $x \in X_1(N)$ with $j(x) \in \mathbb{Q}$ arise from points on one of a *finite* number of elliptic curves, even as $N$ ranges over all positive integers.

**Theorem 1** (Bourdon, Ejder, Liu, Odumodu, Viray [11])**.** *Let $\mathcal{I}$ denote the set of all isolated points on all modular curves $X_1(N)$ for $N \in \mathbb{Z}^+$. Suppose there exists a constant $C = C(\mathbb{Q})$ such that for all non-CM elliptic curves $E/\mathbb{Q}$, the mod $p$ Galois representation associated to $E$ is surjective for primes $p > C$. Then $j(\mathcal{I}) \cap \mathbb{Q}$ is finite.*

The existence of a constant $C$ as in the theorem statement was first suggested in a question of Serre [51], and in [52] he asked whether $C(\mathbb{Q}) = 37$. Significant partial results combined with computational evidence have led to this increasingly standard assumption becoming known as Serre's Uniformity Conjecture. See for example [4], [5], [2], [62], [58], [39], [40].

A natural problem in light of Theorem 1 is to identify the (likely finite) set $j(\mathcal{I}) \cap \mathbb{Q}$. By [11, Thm. 7.1], the set contains all 13 CM $j$-invariants in $\mathbb{Q}$ as well as at least two non-CM $j$-invariants: $-3^2 \cdot 5^6/2^3$, corresponding to two isolated points of degree 3 on $X_1(21)$ identified by Najman [47], and $-7 \cdot 11^3$, corresponding to degree 6 points on $X_1(37)$ lying above one of the two non-cuspidal rational points on $X_0(37)$ as in work of van Hoeij [60]. Here, we give an unconditional version of Theorem 1 by restricting our attention to points of odd degree. Our main result is the following:

**Theorem 2.** *Let $\mathcal{I}_{odd}$ denote the set of all isolated points of odd degree on all modular curves $X_1(N)$ for $N \in \mathbb{Z}^+$. Then $j(\mathcal{I}_{odd}) \cap \mathbb{Q}$ contains at most the $j$-invariants in the following list:*

| *non-CM $j$-invariants* | *CM $j$-invariants* |
|---|---|
| $-3^2 \cdot 5^6/2^3$ | $-2^{18} \cdot 3^3 \cdot 5^3$ |
| $3^3 \cdot 13/2^2$ | $-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$ |
| | $-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$ |

*Conversely, $j(\mathcal{I}_{odd}) \cap \mathbb{Q}$ contains $-3^2 \cdot 5^6/2^3$ and $3^3 \cdot 13/2^2$.*

The $j$-invariant $3^3 \cdot 13/2^2$ corresponds to a degree 9 point on $X_1(28)$. The existence of such a point was noted during an extensive computational search performed by Najman and González-Jiménez (see [29]), and in fact it can be realized by a rational elliptic curve under base extension. However, this is the first instance this point has been identified as isolated. The CM $j$-invariants give points of degree 21 on $X_1(43)$, degree 33 on $X_1(67)$, and degree 81 on $X_1(163)$, respectively. They are in $j(\mathcal{I}_{odd}) \cap \mathbb{Q}$ if and only if these points are isolated. One difficulty in determining whether they are in fact isolated stems from the fact that the Jacobian variety of each of the last three curves has positive rank; see Remark 38.

The first step in the proof of Theorem 2 is to establish a connection between points on $X_1(N)$ of odd degree and rational isogenies. This is analogous to the connection found in the case of odd degree CM points on modular curves [1, Cor. 9.4], and it relies on the classification of rational isogenies of elliptic curves over $\mathbb{Q}$ due to Mazur [46], Kenku [36], and others.

**Theorem 3.** *Let $x \in X_1(n)$ be a point of odd degree with $j(x) \in \mathbb{Q}$. If $j(x) \neq 3^3 \cdot 5 \cdot 7^5/2^7$, then there exists $y \in X_0(p)(\mathbb{Q})$ with $j(x) = j(y)$ for every odd prime $p$ dividing $n$ (of which there might not be any). Moreover:*

*(i) If $j(x) \neq j(z)$ for all $z \in X_0(21)(\mathbb{Q})$, then $n = 2^a p^b$ for $p \in \{3, 5, 7, 11, 13, 19, 43, 67, 163\}$ and nonnegative integers $a, b$ with $a \leq 3$. If $b > 0$, then $a \leq 2$.*

*(ii) If there exists $z \in X_0(21)(\mathbb{Q})$ with $j(x) = j(z)$, then $n = 2^a 3^b 7^c$ for nonnegative integers $a, b, c$ with $a \leq 1$.*

*If $j(x) = 3^3 \cdot 5 \cdot 7^5/2^7$, then $n = 2^a 7^b$ for nonnegative integers $a, b$ with $a \leq 1$.*

*Remark* 4. From work of Zywina [62], it is known that the mod 7 Galois representation of a non-CM elliptic curve over $\mathbb{Q}$ is properly contained in the normalizer of a split Cartan subgroup if and only if $j(E) = 3^3 \cdot 5 \cdot 7^5/2^7$.

*Remark* 5. There are precisely 4 non-cuspidal points in $X_0(21)(\mathbb{Q})$ which correspond to non-CM elliptic curves with $j$-invariants $-3^2 \cdot 5^6/2^3$, $3^3 \cdot 5^3/2$, $-3^2 \cdot 5^3 \cdot 101^3/2^{21}$, $-3^3 \cdot 5^3 \cdot 383^3/2^7$. As mentioned above, the first of these is known to correspond to an isolated point.

Provided $j(x) \neq 3^3 \cdot 5 \cdot 7^5/2^7$, $j(x)$ is not in $j(X_0(21)(\mathbb{Q}))$, and does not correspond to a CM elliptic curve, we can deduce information about the degree of $x \in X_1(2^a p^b)$ using work of Greenberg [31] and Greenberg, Rubin, Silverberg, and Stoll [32] which concerns the image of Galois representations of an elliptic curve over $\mathbb{Q}$ with a rational isogeny. Often, the degree of $x$ is as large as possible given the degree of its image in $X_1(2^a p)$ or $X_1(2^a p^2)$, which means an isolated point would remain isolated under the natural projection map [11]. We must then determine whether isolated points corresponding to elliptic curves with rational $j$-invariant exist on this curve of lower level. If $p = 3$, we rely on the classification of 3-adic images of elliptic curves over $\mathbb{Q}$ due to Rouse, Sutherland, and Zureick-Brown [49]. Our proof involves finding all rational points on an explicit genus 4 curve which characterizes a certain kind of "entanglement" of torsion point fields; see Proposition 29. Other notable cases include elliptic curves with rational cyclic isogenies of degree 21 or 25. In the first case, we show in §4.2 that explicit computations for particular elliptic curves produce bounds on the level of certain Galois representations which improve those of [11, Prop. 6.1]. For elliptic curves with a rational cyclic 25-isogeny, our arguments use intermediate modular curves

lying between $X_1(N)$ and $X_0(N)$ in addition to refined results of Greenberg [31]; see Proposition 21.

The results on CM elliptic curves follow from work of Kwon [37], Aoki [1], and recent work of the first author and Pete L. Clark [8], [9].

Our work involves a number of explicit computations with Magma [7]. Supporting computations can be found at https://users.wfu.edu/rouseja/isolated/. Filenames listed in the paper refer to files found at this repository.


## Acknowledgements

We thank Pete L. Clark for helpful conversations. We also thank Filip Najman, Bianca Viray, and David Zureick-Brown for helpful comments on an earlier draft. We are very grateful for the suggestions and feedback of the anonymous referee which significantly improved the paper.

## Funding

The first author was partially supported by an A. J. Sterge Faculty Fellowship and NSF grant DMS-2137659.


## Data Availability Statement

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

## 2. Background and Notation

2.1. **Galois representations of elliptic curves.** Let $k$ be a number field and let $E/k$ be an elliptic curve. Then for any fixed $N \in \mathbb{Z}^+$ the points of $E(\overline{k})$ with order dividing $N$, denoted $E[N]$, form a free $\mathbb{Z}/N\mathbb{Z}$-module of rank 2. By choosing a basis for $E[N]$, the action of the absolute Galois group of $k$, denoted $\mathrm{Gal}_k$, is recorded in the mod $N$ Galois representation associated to $E$

$$\rho_{E,N} : \mathrm{Gal}_k \to \mathrm{Aut}(E[N]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Taking the inverse limit over all $N$, we obtain the adelic Galois representation associated to $E$, which gives the Galois action on all torsion points of $E$

$$\rho_E : \mathrm{Gal}_k \to \mathrm{Aut}(E(\overline{k})_{\mathrm{tors}}) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

For any positive integer $m$, we may compose $\rho_E$ with projection onto the restricted product

$$\rho_{E,m^\infty} : \mathrm{Gal}_k \xrightarrow{\rho_E} \mathrm{GL}_2(\widehat{\mathbb{Z}}) \cong \prod_{p \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_p) \xrightarrow{\mathrm{proj}} \prod_{p|m} \mathrm{GL}_2(\mathbb{Z}_p),$$

obtaining the $m$-adic representation associated to $E$. More generally, if $m, n$ are relatively prime positive integers, we write $\rho_{E,m\cdot n^\infty}$ for $\rho_E$ composed with the natural projection

$$\mathrm{GL}_2(\widehat{\mathbb{Z}}) \cong \prod_{p \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \times \prod_{p|n} \mathrm{GL}_2(\mathbb{Z}_p).$$

Throughout we use $\pi$ to denote the natural reduction map.

For a fixed non-CM elliptic curve $E/k$, Serre's Open Image Theorem [51] states that $\mathrm{im}\,\rho_E$ is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Thus there exists a positive integer $N$ such that $\mathrm{im}\,\rho_E = \pi^{-1}(\mathrm{im}\,\rho_{E,N})$. The smallest such $N$ is called the level of the adelic Galois representation. Similarly, the smallest positive integer $n$ such that $\mathrm{im}\,\rho_{E,m^\infty} = \pi^{-1}(\mathrm{im}\,\rho_{E,n})$ is called the level of the $m$-adic Galois representation associated to $E$. In fact, for any fixed integer $m$, there exists a bound on the level of $\rho_{E,m^\infty}$ that depends only on the degree of $k$. See [13, Thm. 1.1], [16, Thm 2.3] in the case where $m$ is prime and [11, Prop. 6.1] for the general case.

A consequence of Serre's Open Image Theorem is that, given a non-CM elliptic curve $E/k$, the mod $p$ Galois representation is surjective for all sufficiently large primes. In [51], Serre asked whether there might exist some uniform constant $C$ depending only on $k$ such that $\operatorname{im}\rho_{E,p} = \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ for all primes $p > C$ and *all* non-CM elliptic curves $E/k$. In the case where $k = \mathbb{Q}$, both significant theoretical results and computational evidence make it appear likely that the answer is yes, and this is now often referred to as Serre's Uniformity Conjecture. It is even believed that $C$ can be taken to be 37 in the case of non-CM elliptic curves over $\mathbb{Q}$. See, for example, [62, Conj. 1.12] and [58, Conj. 1.1].

If $\operatorname{im}\rho_{E,p}$ is not all of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, then it is contained in one of its known maximal subgroups. These include the Borel subgroup, the normalizer of a split or non-split Cartan subgroup, or an exceptional subgroup; see [51, Section 2] for details. For primes $p \leq 13$, the groups that arise as $\operatorname{im}\rho_{E,p}$ for a non-CM elliptic curve $E/\mathbb{Q}$ are known. The case of primes $p \leq 11$ was completed by Zywina [62]; see also Sutherland [58]. At the time, the classification for $p = 13$ was complete aside from ruling out the existence of non-CM elliptic curves $E/\mathbb{Q}$ with $\operatorname{im}\rho_{E,p}$ contained in the normalizer of a (split or non-split) Cartan subgroup. Baran [3] showed that such an elliptic curve would correspond to a rational point on an explicit genus 3 curve, and work of Balakrishnan, Dogra, Müller, Tuitman, and Vonk [2] showed that this genus 3 curve had no non-cuspidal, non-CM points. For a list of the groups that arise as $\operatorname{im}\rho_{E,p}$ for primes $p \leq 13$, as well as degrees of fields of definition for points of order $p$, see Tables 1 and 2 in [30]. Throughout, we use the notation of Sutherland [58] to denote subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, which is also the notation used in LMFDB.

More generally, one could seek to classify which groups arise as $\operatorname{im}\rho_{E,p^\infty}$ for a non-CM elliptic curve $E/\mathbb{Q}$.[1] One of the first results in this direction was work of Rouse and Zureick-Brown [50] which gave the complete classification for $p = 2$. The groups which arise infinitely often as $\operatorname{im}\rho_{E,p^\infty}$ were classified by Sutherland and Zywina [59]. For $p = 3$, evidence suggests that the groups identified in [59] are in fact the only groups which arise; see forthcoming work of Rouse, Sutherland, and Zureick-Brown [49].

2.2. **Isogenies of elliptic curves.** Let $E/k$ be an elliptic curve, and let $P \in E(\overline{k})$ be a point of order $N$. If the subgroup generated by $P$ is fixed (as a group) by $\mathrm{Gal}_k$, then we say $E$ possesses a rational cyclic subgroup of order $N$. Alternatively, since such a subgroup is the kernel of a $k$-rational isogeny from $E$ to another elliptic curve defined over $k$, we may say $E$ has a $k$-rational cyclic $N$-isogeny. In the case of elliptic curves $E/\mathbb{Q}$, we have a complete determination of the rational cyclic subgroups that can occur.

**Theorem 6** (Mazur [46], Kenku [36], and others; see Section 9 of [43])**.** *If $E/\mathbb{Q}$ is an elliptic curve possessing a $\mathbb{Q}$-rational cyclic subgroup of order $N$, then $N \leq 19$ or $N \in \{21, 25, 27, 37, 43, 67, 163\}$.*

Let $p \geq 5$ be prime, and let $E/\mathbb{Q}$ be a non-CM elliptic curve with a rational cyclic $p$-isogeny. Work of Greenberg, Rubin, Silverberg, and Stoll [31], [32] shows that $\operatorname{im}\rho_{E,p^\infty}$ is as large as possible given the isogenies over $\mathbb{Q}$ with degree a power of $p$. In particular, their work implies the following theorem which plays a crucial role in the proof of our main results.

**Theorem 7** (Greenberg [31], Greenberg, Rubin, Silverberg, Stoll [32])**.** *Let $E/\mathbb{Q}$ be a non-CM elliptic curve with a $\mathbb{Q}$-rational cyclic isogeny of prime degree $p$.*

*(i) If $p \geq 7$, then for any choice of basis the image of $\rho_{E,p^\infty}$ contains $I_2 + pM_2(\mathbb{Z}_p)$.*
*(ii) Suppose $p = 5$. If $E/\mathbb{Q}$ does not have a rational cyclic 25-isogeny, then for any choice of basis the image of $\rho_{E,5^\infty}$ contains $I_2 + 5M_2(\mathbb{Z}_5)$. Otherwise, the image of $\rho_{E,5^\infty}$ contains $I_2 + 25M_2(\mathbb{Z}_5)$.*

[1] The case of a CM elliptic curve $E$ defined over $\mathbb{Q}(j(E))$ is addressed in recent work of Lozano-Robledo [44].

*Proof.* Let $E/\mathbb{Q}$ be a non-CM elliptic curve with a rational cyclic $p$-isogeny. Note that any Sylow pro-$p$ subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ contains $I_2 + pM_2(\mathbb{Z}_p)$. Thus if $p > 7$, the theorem statement can be deduced from Theorem 1 in [31] and the discussion which follows [31, p.1186-1187]. For $p = 7$, this is given by Theorem 5.5 in [32]. So suppose $p = 5$. If none of the elliptic curves in the $\mathbb{Q}$-isogeny class of $E$ has 2 independent isogenies of degree 5, then the statement follows from Theorem 2 of [31]. So suppose there exists an elliptic curve $\mathbb{Q}$-isogenous to $E$ with 2 independent isogenies of degree 5. Then either $E$ has a rational cyclic 25-isogeny, and the claim follows from Proposition 5.1.1 of [31], or else $E$ has 2 independent isogenies of degree 5. Suppose the latter holds. Then $\rho_{E,5^\infty} : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_5)$ has level $5^r$ which we identify with a subgroup $G$ of $\mathrm{GL}_2(\mathbb{Z}/5^r\mathbb{Z})$. Let $K \subseteq G$ be the kernel of reduction map modulo 5. Then, $[G : K]$ has order coprime to 5 because $E$ has two independent 5-isogenies (see Table 1 in [30]). It follows that $K$ is a Sylow 5-subgroup of $G$ and Theorem 2 of [31] gives that the index of $K$ in $\mathrm{GL}_2(\mathbb{Z}/5^r\mathbb{Z})$ is divisible by 5 but not 25. If we let $L = \{g \in \mathrm{GL}_2(\mathbb{Z}/5^r\mathbb{Z}) : g \equiv I \pmod 5\}$, then $K \subseteq L$ and $|K| = |L|$. Thus, $K = L$ and the image of $\rho_{E,5^\infty}$ contains all matrices congruent to the identity modulo 5. □

*Remark* 8. This shows that if $E/\mathbb{Q}$ is a non-CM elliptic curve with a rational cyclic $p$-isogeny for some prime $p \geq 5$, then $\operatorname{im}\rho_{E,p^\infty}$ is the complete pre-image of $\operatorname{im}\rho_{E,p^m}$ in $\mathrm{GL}_2(\mathbb{Z}_p)$, where $m$ is the maximum integer such that $E$ possesses a $\mathbb{Q}$-rational cyclic $p^m$-isogeny. This does not hold if $p = 3$. For example, by Sutherland and Zywina [59] there exist non-CM elliptic curves $E/\mathbb{Q}$ such that the associated 3-adic Galois representation has level 27. However, no non-CM elliptic curves over $\mathbb{Q}$ have a rational cyclic 27-isogeny (see Table 4 of [43] for a convenient listing; the model for $X_0(27)$ and its rational points were first worked out by Ligozat in [42, pg. 45, 55]).

2.3. **Modular curves.** Here we briefly recall the constructions of the modular curves $X_1(N)$ and $X_0(N)$, along with some useful formulas regarding maps between modular curves. For more details, see, for example, [25, §7.7], [24], [54, §6.7], [21].

For any $N \in \mathbb{Z}^+$, the curve $Y_1(N)$ parametrizes $\mathbb{C}$-isomorphism classes of elliptic curves with a distinguished point of order $N$. An explicit construction is given by

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

where $\mathbb{H}$ denotes the upper half plane and

$$\Gamma_1(N) \coloneqq \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod N \text{ and } a \equiv d \equiv 1 \pmod N \right\}$$

acts on $\mathbb{H}$ via linear fractional transformations. The resulting Riemann surface is not compact. By adding in a finite number of points—the cusps—we obtain its compactification $X_1(N)$. This can be identified with a smooth projective curve defined over $\mathbb{Q}$.

**Proposition 9.** *For positive integers $a$ and $b$, there is a natural $\mathbb{Q}$-rational map $f : X_1(ab) \to X_1(a)$ defined by sending $[E, P]$ to $[E, bP]$. Moreover*

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

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

*Proof.* The fact that the map is $\mathbb{Q}$-rational follows from the moduli interpretation. The degree calculation can be deduced from [25, p.66]. □

Similarly, the curve $Y_0(N)$ parametrizes $\mathbb{C}$-isomorphism classes of elliptic curves with a cyclic subgroup of order $N$. Specifically,

$$Y_0(N) \coloneqq \mathbb{H}/\Gamma_0(N),$$

where

$$\Gamma_0(N) \coloneqq \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.$$

The compactification $X_0(N)$ can be identified with a smooth projective curve over $\mathbb{Q}$.

**Proposition 10.** *For a positive integer $N$, there is a natural $\mathbb{Q}$-rational map $f : X_1(N) \to X_0(N)$ defined by sending $[E, P]$ to $[E, \langle P \rangle]$. If $N \leq 2$, then $\deg(f) = 1$. Otherwise $\deg(f) = \varphi(N)/2$, where $\varphi$ denotes the Euler phi function.*

*Proof.* As with the previous proposition, the fact that the map is $\mathbb{Q}$-rational follows from the moduli interpretation, and the degree calculation can be deduced from [25, p.66]. □

2.4. **Closed points on curves.** Let $C$ be a curve defined over a number field $k$, i.e., a projective nonsingular geometrically integral 1-dimensional scheme over $k$. Throughout, we consider closed points $x \in C$, which are in bijection with $\mathrm{Gal}_k$-orbits of points in $C(\overline{k})$. By the degree of $x$ we mean the degree of the associated residue field $k(x)$ over $k$. In the case where $C = X_1(N)$ and $k = \mathbb{Q}$, the following lemma gives a way to compute the degree of a closed point $x \in X_1(N)$ associated to a non-CM elliptic curve $E$ and point $P$ of order $N$. Here, $K(P)$ denotes the field extension of $K$ generated by the coordinates of $P$.

**Lemma 11.** [11, 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 $x = [E, P] \in X_1(N)$ denote the associated closed point. 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.*

*Remark* 12. It is important not to confuse the closed point $x \in X_1(N)$ associated to $[E, P]$ with the $K(P)$-valued point of $X_1(N)$ associated to $[E, P]$. Recall a $K(P)$-valued point of $X_1(N)$ is a morphism of $\mathbb{Q}$-schemes $s : \mathrm{Spec}(K(P)) \to X_1(N)$. The closed point $x \in X_1(N)$ associated to $[E, P]$ is the image of $s$.

More generally, it is often useful to construct the residue field of a closed point on $X_1(N)$ using Weber functions. For an elliptic curve $E$ defined over $\mathbb{Q}(j(E))$, let $\mathfrak{h} : E \to E/\mathrm{Aut}(E) \cong \mathbb{P}^1$ be a Weber function; see [54, p.107] or [55, Example 5.5.1 and 5.5.2] for more details. If $E : y^2 = x^3 + Ax + B$ and $P = (x, y) \in E$, then $\mathfrak{h}$ can be taken to be

$$\mathfrak{h}(P) = \begin{cases} x & AB \neq 0 \\ x^2 & B = 0 \\ x^3 & A = 0 \end{cases}.$$

We have $B = 0$ if and only if $j(E) = 1728$ and $A = 0$ if and only if $j(E) = 0$. Then for $x = [E, P] \in X_1(N)$, the residue field $\mathbb{Q}(x)$ is

$$\mathbb{Q}(j(E), \mathfrak{h}(P)).$$

It follows from [21, Proposition VI.3.2] that there is a model of $E$ over $\mathbb{Q}(x)$ such that $P \in E(\mathbb{Q}(x))$.

2.5. **Isolated points.** Let $C/k$ be a curve, and suppose $P_0 \in C(k)$.[2] For any positive integer $d$, we let $C^{(d)}$ denote the $d$th symmetric product of $C$, a variety whose points correspond to effective divisors of degree $d$ on $C$. Any closed point $x \in C$ of degree $d$ gives a $k$-rational point of $C^{(d)}$, and we have a natural map to the Jacobian variety

$$\Phi : C^{(d)} \to \mathrm{Jac}(C)$$

[2]For the case where $C$ does not have a $k$-rational point, see §4 of [11].

defined by sending $x = P_1 + \cdots + P_d$ to the divisor class $[P_1 + \cdots + P_d - dP_0]$, where $P_1, \ldots, P_d$ denote the points in the $\mathrm{Gal}_k$ orbit $x$.

If $C$ has infinitely many closed points of degree $d$, then one of the following must be true:

(i) $\Phi(x) = \Phi(y)$ for distinct closed points $x$ and $y$. As effective degree $d$ divisors, $x$ and $y$ have distinct support, so it follows there is a function $f$ of degree $d$ such that $\mathrm{div}(f) = x - y$. Hence $f : C \to \mathbb{P}^1$ is a dominant morphism of degree $d$, and by Hilbert's irreducibility theorem [53, Ch.9] $f^{-1}(\mathbb{P}^1(k))$ contains infinitely many points of degree $d$. That is, there exists an infinite family of degree $d$ points "parametrized by $\mathbb{P}^1$."

(ii) $\Phi$ is injective on the set of degree $d$ points. Since $\mathrm{im}\,\Phi$ is a closed subscheme of $\mathrm{Jac}(C)$, Faltings's Theorem [27] implies there exist a finite number of $k$-rational abelian subvarieties $A_i \subset \mathrm{Jac}(C)$ and $k$-rational points $x_i \in \mathrm{im}\,\Phi$ such that

$$(\mathrm{im}\,\Phi)(k) = \bigcup_{i=1}^{n} [x_i + A_i(k)].$$

Thus one of the $A_i$ has positive rank, and this gives an infinite family of degree $d$ points "parametrized by $A_i$."

Thus we see that the existence of infinitely many degree $d$ points implies we either have a degree $d$ function $f : C \to \mathbb{P}^1$ or else $\mathrm{im}\,\Phi$ contains the translate of a positive rank abelian subvariety of $\mathrm{Jac}(C)$. In fact, the converse holds as well.[3] Following [11], we say a closed point $x \in C$ of degree $d$ is **isolated** if it does not belong to one of these infinite families of degree $d$ points, that is, if (1) there is no other point $y \in C^{(d)}(k)$ such that $\Phi(x) = \Phi(y)$ and (2) there is no positive rank abelian subvariety $A \subset \mathrm{Jac}(C)$ such that $\Phi(x) + A \subset \mathrm{im}(\Phi)$. Moreover, we say points satisfying condition (1) are $\mathbb{P}^1$-isolated, and points satisfying condition (2) are AV-isolated. The following characterization of isolated points strengthens an observation of Frey [28].

**Theorem 13** (Bourdon, Ejder, Liu, Odumodu, Viray, [11, Theorem 4.2])**.** *Let $C$ be a curve over a number field.*

*(i) 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.*

*(ii) There are only finitely many isolated points on $C$.*

In particular, if there exist only finitely many points of degree $d$, then each degree $d$ point is isolated. However, having infinitely many degree $d$ points does not preclude the existence of additional isolated degree $d$ points. Some places in the literature (such as [26, 22, 15, 56, 12]) use the term **sporadic** to denote a closed point $x \in C$ such that there are only finitely many points of degree at most $\deg(x)$. By Theorem 13, we see that every sporadic point is in fact an isolated point.

One ingredient in the proof of the second part of Theorem 13 is a bound on the degree of an isolated point. We will make frequent use of this bound.

**Lemma 14.** *Let $C$ be a curve over a number field $k$ with genus $g$. If $x \in C(\overline{k})$ is a closed point with degree $\geq g + 1$, then $x$ is not $\mathbb{P}^1$-isolated.*

*Proof.* Let $D$ be the degree $d$ effective divisor corresponding to $x$. Since $\deg(D) \geq g + 1$, the Riemann-Roch theorem implies that $\dim L(D) \geq \deg(D) - g + 1 \geq 2$. In particular, there is a non-constant function $f : C \to \mathbb{P}^1$ with pole divisor $D$. Define $y \coloneqq f^*([0 : 1])$. Then $y - x = \mathrm{div}(f)$, and it follows that $\Phi(y) = \Phi(x)$. Thus $x$ is not $\mathbb{P}^1$-isolated. □

[3] The main challenge in justifying the converse is the case where no degree $d$ map $f : C \to \mathbb{P}^1$ exists, yet $\mathrm{im}\,\Phi$ contains the translate of a positive rank abelian subvariety of $\mathrm{Jac}(C)$. It follows immediately that $C$ has infinitely many points of degree $\leq d$, but the implication that $C$ has infinitely many points of degree *exactly* $d$ takes more work. See [11, Theorem 4.2].

A key tool in studying isolated points is the following criterion for when the image of isolated points remain isolated.

**Theorem 15** (Bourdon, Ejder, Liu, Odumodu, Viray, [11, Theorem 4.3])**.** *Let $f\colon C \to D$ be a finite map of curves and let $x \in C$ be an isolated point. If $\deg(x) = \deg(f(x)) \cdot \deg(f)$, then $f(x)$ is an isolated point of $D$.*

The following proposition from [11] gives a convenient way to check the hypothesis that $\deg(x) = \deg(f(x)) \cdot \deg(f)$.

**Proposition 16** (Bourdon, Ejder, Liu, Odumodu, Viray, [11, 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 $\mathrm{Supp}(ab) \subset S$. 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*

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

2.6. **CM elliptic curves.** Let $E$ be an elliptic curve defined over a number field $F$. We say $E$ has **complex multiplication**, or CM, if $\mathrm{End}_{\overline{F}}(E)$ is strictly larger than $\mathbb{Z}$. In this case, $\mathrm{End}_{\overline{F}}(E) \cong \mathcal{O}$, an order in an imaginary quadratic field $K$. If $\mathcal{O}_K$ denotes the ring of integers in $K$, then $\mathcal{O}$ is a subring of $\mathcal{O}_K$ of index $\mathfrak{f}$, where $\mathfrak{f}$ is called the **conductor** of $\mathcal{O}$, and it is the unique subring of $\mathcal{O}_K$ of this index. Explicitly, we have

$$\mathcal{O} = \mathbb{Z} + \mathfrak{f}\mathcal{O}_K.$$

Thus an order $\mathcal{O}$ in $K$ can be uniquely determined by its **discriminant**

$$\Delta \coloneqq \mathfrak{f}^2 \Delta_K,$$

where $\Delta_K$ denotes the discriminant of $K$. See [18, Lemma 7.2] for details.

If $E/F$ is an $\mathcal{O}$-CM elliptic curve, then elements of $\mathrm{Gal}_{FK}$ commute with elements of $\mathcal{O}$ in their action on $E[N]$, a free $\mathcal{O}/N\mathcal{O}$-module of rank 1 by [48, Lemma 1]. This implies the mod $N$ Galois representation of $E/FK$ can be expressed as

$$\rho_{E,N} : \mathrm{Gal}_{FK} \to \mathrm{Aut}_{\mathcal{O}/N\mathcal{O}}(E[N]) \cong (\mathcal{O}/N\mathcal{O})^\times.$$

Thus we may interpret the action of $\mathrm{Gal}_{FK}$ on $N$-torsion points of an $\mathcal{O}$-CM elliptic curve as the action of $(\mathcal{O}/N\mathcal{O})^\times$ on a free $\mathcal{O}/N\mathcal{O}$-module of rank 1. We denote $(\mathcal{O}/N\mathcal{O})^\times$ by $C_N(\mathcal{O})$ and call it the **mod $N$ Cartan subgroup**.

If we fix a model of $E$ defined over $K(j(E))$, the action of $\mathcal{O}$ on points of $E$ is rationally defined. Denote by $\overline{E[N]}$ the orbits of points in $E[N]$ under the action of $\mathcal{O}^\times$. The action of $\mathcal{O}/N\mathcal{O}$ on $E[N]$ induces an action of the **reduced mod N Cartan subgroup** $\overline{C_N(\mathcal{O})}$ on $\overline{E[N]}$, where

$$\overline{C_N(\mathcal{O})} \coloneqq C_N(\mathcal{O})/q_N(\mathcal{O}^\times)$$

and $q_N : \mathcal{O} \to \mathcal{O}/N\mathcal{O}$ is the natural map. For any point $P \in E$ of order $N$, the degree of $K(j(E))(\mathfrak{h}(P))$ over $K(j(E))$ is equal to the size of the $\overline{C_N(\mathcal{O})}$-orbit of $\overline{P} \in \overline{E[N]}$. From this we can deduce the degree of $[E, P]$ on $X_1(N)$ viewed as a curve over $K$. See Section 7A of [8] for details.

## 3. Points of Odd Degree on $X_1(N)$

In this section we will prove Theorem 3. We begin with preliminary lemmas in §3.1-3.2, and the theorem itself is proved in §3.3. A refinement of Theorem 3 is given in §3.4. A key observation is that aside from one exceptional $j$-invariant, to have a point $x = [E, P] \in X_1(n)$ of odd degree with $j(x) \in \mathbb{Q}$, there must exist a model of $E/\mathbb{Q}$ with a rational cyclic $p$-isogeny for all odd primes $p$ dividing $n$. Thus Theorem 6 significantly restricts the possibilities for $n$. In the case of CM elliptic curves, our results can be deduced from work of Aoki [1]. For non-CM elliptic curves, Theorem 3 follows from classification results for Galois representations of elliptic curves over $\mathbb{Q}$, as outlined in §2.1, along with various computations which address special cases. In particular, many of the fiber product computations we require were originally performed by Daniels and González-Jiménez [19], [20]. We also employ a useful result about lifting rational points due to Najman and González-Jiménez [30, Prop. 4.6].

### 3.1. **Connection with rational cyclic isogenies.**

**Lemma 17.** *Let $E/\mathbb{Q}$ be an elliptic curve and $P \in E(\overline{\mathbb{Q}})$ a point of order $pn$ where $p \geq 3$ is prime and $n \in \mathbb{Z}^+$. Then one of the following occurs:*

*(i) $p \in \{3, 5, 7, 11, 13, 19, 43, 67, 163\}$ and $E$ has a rational $p$-isogeny,*
*(ii) $p = 7$ and $j(E) = 3^3 \cdot 5 \cdot 7^5/2^7$, or*
*(iii) the residue field of $[E, P] \in X_1(pn)$ has even degree.*

*Proof.* If $E$ has complex multiplication and the residue field of $[E, P] \in X_1(pn)$ has odd degree, then by §2.4 there is a number field $F$ of odd degree and a model of $E/F$ where $P \in E(F)$. By Aoki [1, Cor. 9.4], $E$ has CM by an order in $K = \mathbb{Q}(\sqrt{-p})$. Since $j(E) \in \mathbb{Q}$, the field $K$ has class number 1, and $p \in \{3, 7, 11, 19, 43, 67, 163\}$. Moreover the model of $E$ over $\mathbb{Q}$ has a rational cyclic $p$-isogeny; see for example [10, Prop. 5.7]. From now on we assume $E$ is non-CM and fix a model of $E/\mathbb{Q}$.

If $\rho_{E,p}$ is surjective, then the residue field of $[E, nP] \in X_1(p)$ has even degree by [43, Theorem 5.1] and Lemma 11, and hence the residue field of $[E, P] \in X_1(pn)$ has even degree. Thus we may assume $\rho_{E,p}$ is not surjective.

First, suppose $p \leq 13$. Then as discussed in §2.1, the subgroups that arise as $\operatorname{im} \rho_{E,p}$ are known. By checking each case, see for example [30, Tables 1 & 2] and Lemma 11, we see that we are in case (i) or (iii) except when $p = 7$ and $\operatorname{im} \rho_{E,7}$ is conjugate to 7Ns.2.1 or 7Ns.3.1 (here we use LMFDB labels, also following [58]). By [62, Theorem 1.5], $\operatorname{im} \rho_{E,7}$ is conjugate to one of these groups only if $j(E) = 3^3 \cdot 5 \cdot 7^5/2^7$.

Next, suppose $p \geq 17$. Here, $\rho_{E,p}$ is known to have at least 4 possible images aside from $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, each of which is contained in a Borel subgroup. For each of these, we are in case (iii). (See, e.g., [30, Table 2] and Lemma 11.) If $\operatorname{im} \rho_{E,p}$ is not one of these known groups, then it is conjugate to one of two subgroups of the normalizer of a non-split Cartan subgroup. See for example [30, Theorem 3.2]. The degree of the residue field of $[E, nP]$ is even in either case by [30, Theorem 5.6] and Lemma 11. □

### 3.2. **Elliptic curves with rational cyclic isogenies of degree 15 or 21.**

**Proposition 18.** *Let $E/\mathbb{Q}$ be an elliptic curve, and suppose $[E, P] \in X_1(n)$ has odd degree.*

*(i) If $E$ has a rational cyclic 15-isogeny, then $n = 2^a 3^b$ or $2^a 5^c$ where $a \leq 1$.*
*(ii) If $E$ has a rational cyclic 21-isogeny, then $n = 2^a 3^b 7^c$ where $a \leq 1$.*

*Proof.* If $E$ has a rational cyclic 15-isogeny or 21-isogeny, then $j(E)$ is one of the eight values listed in [43, Table 4]. Since the residue field is model independent as discussed in §2.4, we are free to use any Weierstrass equation over $\mathbb{Q}$ with $j$-invariant $j(E)$ to compute the degree of $\mathbb{Q}(j(E), \mathfrak{h}(P))$.

Note that since $E$ is non-CM, we may take $\mathfrak{h}((x,y)) = x$, so the degree of this extension can be explicitly computed by factoring division polynomials.

Each representative in case $(i)$ has a rational cyclic $p$-isogeny for a prime $p$ if and only if $p = 3$ or 5. Similarly, each representative in case $(ii)$ has a rational cyclic $p$-isogeny if and only if $p = 3$ or 7. By Lemma 17, since $j(E) \neq 3^3 \cdot 5 \cdot 7^5/2^7$, the prime divisors of $n$ are $\{2,3,5\}$ or $\{2,3,7\}$, so we consider numbers of the form $n = 2^a 3^b 5^c$ in case $(i)$ and $n = 2^a 3^b 7^c$ in case $(ii)$. Computing the $15^{th}$ division polynomial for each representative in case $(i)$, we see that the point on $X_1(15)$ corresponding to $E$ has even degree. So $n = 2^a 3^b$ or $2^a 5^c$. Finally, computing the $4^{th}$ division polynomial for all eight representatives shows that the point on $X_1(4)$ corresponding to $E$ has even degree. Thus $a \leq 1$ in both cases. □

*Remark* 19. Computing the $21^{st}$ division polynomial for each representative in case $(ii)$, we see that the point on $X_1(21)$ corresponding to $E$ can have odd degree.

3.3. **Proof of Theorem 3.** Let $x = [E,P] \in X_1(n)$ be a point of odd degree with $j(x) \in \mathbb{Q}$. First suppose $E$ has complex multiplication. Then there is a number field $F$ of odd degree and a model of $E/F$ where $P \in E(F)$. By Aoki [1, Cor. 9.4], $n = 2^a p^b$ for an odd prime $p$ and $a \leq 2$. If $b > 0$, then $a \leq 1$ and $E$ has CM by an order in $K = \mathbb{Q}(\sqrt{-p})$. Since $j(E) \in \mathbb{Q}$, it follows that $K$ has class number 1, and so $p \in \{3,7,11,19,43,67,163\}$. Moreover any model of $E$ over $\mathbb{Q}$ has a rational cyclic $p$-isogeny; see for example [10, Prop. 5.7]. From [43, Table 4], $E$ does not have a cyclic 15-isogeny or 21-isogeny defined over $\mathbb{Q}$.

From now on we will assume $E$ is non-CM. We fix a model of $E/\mathbb{Q}$. First suppose $j(E) \neq 3^3 \cdot 5 \cdot 7^5/2^7$. If $p \mid n$ where $p \geq 3$ is prime, then $E$ has a rational cyclic $p$-isogeny by Lemma 17. Since $E$ is non-CM, $p \in \{3,5,7,11,13\}$ (see, for example, [43, Table 4]). If $p_1$ and $p_2$ divide $n$ where $p_i \geq 3$ are distinct primes, then $E$ has a rational cyclic $p_1 p_2$-isogeny. By Theorem 6, this cannot happen unless $E$ has a rational cyclic isogeny of degree 15 or degree 21. Such elliptic curves are addressed in Proposition 18. It follows that unless $E$ has a rational cyclic isogeny of degree 21, then $n = 2^a p^b$ for $p \in \{3,5,7,11,13\}$ and $E$ has a rational cyclic $p$-isogeny.

We next address the exponent of 2. First suppose $E$ has a rational cyclic 2-isogeny, which means that any point of order 2 defined over an extension of odd degree is in fact defined over $\mathbb{Q}$. By [30, Prop. 4.6], we see that $[\mathbb{Q}(P) : \mathbb{Q}(2P)]$ divides 4, and so $[\mathbb{Q}(\mathfrak{h}(P)) : \mathbb{Q}(\mathfrak{h}(2P))]$ divides 8 by Lemma 11; here $\mathfrak{h}$ denotes a Weber function. Under the assumptions, $\mathbb{Q}(x) = \mathbb{Q}(\mathfrak{h}(P))$ is an extension of odd degree, and so it must be that $\mathbb{Q}(\mathfrak{h}(P)) = \mathbb{Q}(\mathfrak{h}(2P))$. Hence any point on $E$ of order $2^a$ corresponding to a point on $X_1(2^a)$ of odd degree must in fact be a point in $X_1(2^a)(\mathbb{Q})$. By [41], there is no elliptic curve over $\mathbb{Q}$ with a rational point of order 16, so $a \leq 3$. If $E$ does not have a rational cyclic 2-isogeny, then by the classification of 2-adic images of non-CM elliptic curves over $\mathbb{Q}$ due to Rouse and Zureick-Brown [50], a point of order 4 will occur only in even degree unless the 2-adic image has label X20, X20a, or X20b. A Magma computation considering the actions of these groups on $(\mathbb{Z}/8\mathbb{Z})^2$ and using Lemma 11 shows that if $E$ is an elliptic curve whose 2-adic image has label X20, X20a or X20b, then for every point $P$ on $E$ of order 8, $[E,P]$ is a degree 12 point on $X_1(8)$. (See the file X20deg.txt.) This implies $[E,Q]$ has even degree if $Q$ has order $2^a$ and $a \geq 3$. Thus, $a \leq 2$ if $E$ has no 2-isogeny.

It remains to show that if $b > 0$, then $a \leq 2$. By the previous paragraph, we may assume $E$ has a rational 2-isogeny. Since $E$ is non-CM elliptic curve which also has a rational cyclic $p$-isogeny, Theorem 6 and [43, Table 4] imply $p \leq 5$.

- Suppose $p = 5$. Since $E$ gives a rational point on $X_1(2)$ and $\deg(X_1(4) \to X_1(2)) = 2$ by Proposition 9, $E$ gives a point on $X_1(4)$ of degree 1 or 2. If it is of degree 1, then $E$ has a 4-isogeny, which contradicts Theorem 6. Thus any point on $X_1(4)$ corresponding to $E$ has even degree and $a \leq 1$.

- Suppose $p = 3$. As in the previous case, the only way $E$ can give a point of odd degree on $X_1(4)$ is if it gives a rational point on $X_1(4)$. By [30, Prop. 4.6], the only way $E$ can give a point on $X_1(8)$ of odd degree is if it is in degree 1, which cannot happen by Theorem 6. Thus $a \leq 2$.

If $j(E) = 3^3 \cdot 5 \cdot 7^5/2^7$, it suffices to pick a particular elliptic curve $E/\mathbb{Q}$ with this $j$-invariant. Since $E$ has no rational isogenies, $\mathrm{Supp}(n) \subseteq \{2, 7\}$ by Lemma 17. Computing division polynomials shows that any point on $X_1(4)$ corresponding to $E$ has degree 6, so $a \leq 1$.

3.4. **Refined bounds on exponent of 2.** Often we may improve the bound on the exponent of 2 found in Theorem 3.

**Proposition 20.** *Let $x \in X_1(2^a p^b)$ be a point of odd degree where $a, b$ are nonnegative integers and $p \geq 5$ is prime. Suppose*

$$j(x) \in \mathbb{Q} \setminus \{-3^3 \cdot 13 \cdot 479^3/2^{14}, 3^3 \cdot 13/2^2\}.$$

*If $b > 0$, then $a \leq 1$.*

*Proof.* Let $x = [E, P] \in X_1(2^a p^b)$ be as in the theorem statement, where $b > 0$. If $E$ has CM, the claim follows from Aoki [1, Cor. 9.4], so henceforth we assume $E$ is non-CM and fix a model of $E/\mathbb{Q}$. If $j(E) = 3^3 \cdot 5 \cdot 7^5/2^7$, then computing division polynomials shows that any point on $X_1(4)$ corresponding to $E$ has degree 6, so $a \leq 1$. If $j(E) \neq 3^3 \cdot 5 \cdot 7^5/2^7$, then by Lemma 17, $E$ has a rational $p$-isogeny, and so $p \in \{5, 7, 11, 13\}$ by [43, Table 4].

If $p = 5$ and $E$ has a rational 2-isogeny, then $a \leq 1$ by the proof in §3.3. Suppose therefore that $p > 5$. By Theorem 6 and [43, Table 4], it follows that $E$ has no rational 2-isogeny. By the classification of 2-adic images due to Rouse and Zureick-Brown [50], any point on $X_1(4)$ corresponding to $E$ is of even degree unless $E$ corresponds to a rational point on X20. So it suffices to consider the fiber product of X20 and $X_0(p)$. We consider each prime separately:

(i) If $p = 5$, then Daniels and González-Jiménez [19, Proposition 6(k)] show the fiber product of X20 and $X_0(5)$ has only cusps. So $a \leq 1$.

(ii) If $p = 7$, Daniels and González-Jiménez [19, Proposition 6(s)] compute the fiber product of $X_0(7)$ and X20. They show the non-cuspidal rational points on this curve correspond to $j$-invariants $-3^3 \cdot 13 \cdot 479^3/2^{14}$ and $3^3 \cdot 13/2^2$, which appear in the theorem statement. So aside from these two $j$-invariants, $a \leq 1$.

(iii) If $p = 11$, there are only a finite number of elliptic curves over $\mathbb{Q}$ with a rational cyclic 11-isogeny. See [43, Table 4]. Computing division polynomials shows that $a \leq 1$.

(iv) If $p = 13$, it will suffice to show the fiber product of $X_0(13)$ and X3 has no non-cuspidal rational points, since X20 covers X3. By Daniels and González-Jiménez [20, Table 8], this curve only has 2 rational points, and both are cusps. Indeed, there are two rational cusps $0, \infty$ on $X_0(13)$, and X3 $\cong \mathbb{P}^1_{\mathbb{Q}}$. This means there are two cuspidal points $(0, \infty)$, $(\infty, \infty)$ in the fiber product and $a \leq 1$. □

## 4. Non-CM Isolated Points in Odd Degree

Here, we build on the results of Section 3 to prove that the non-CM $j$-invariants in $j(\mathcal{I}_{odd}) \cap \mathbb{Q}$ are $-3^2 \cdot 5^6/2^3$ and $3^3 \cdot 13/2^2$, giving the non-CM part of Theorem 2. In §4.1, we address the case of elliptic curves $E/\mathbb{Q}$ with a rational cyclic 25-isogeny. The argument uses constraints on $\mathrm{im}\, \rho_{E,5^\infty}$ due to Greenberg [31] in addition to work of Jeon, Kim, and Schweizer concerning intermediate modular curves [34], [35]. Following this, in §4.2-4.5, we show that aside from the two exceptional $j$-invariants noted above, any isolated point $x \in X_1(n)$ corresponding to a non-CM elliptic curve with $\deg(x)$ odd and $j(x) \in \mathbb{Q}$ must map to an isolated point on $X_1(54)$ or $X_1(162)$. We use explicit bounds on the level of the $m$-adic Galois representation as computed in [11], which at times

can be improved by accounting for constraints on ramification in torsion point fields (see Lemma 22), in addition to classification results concerning the 2-adic [50] and 3-adic [49] images of Galois representations of non-CM elliptic curves. In §4.6, we show that any isolated point $x$ on $X_1(54)$ or $X_1(162)$ with $\deg(x)$ odd and $j(x) \in \mathbb{Q}$ must map to an isolated point on $X_1(54)$ for which $\mathbb{Q}(E[2])$ is an $S_3$-extension contained in $\mathbb{Q}(E[27])$. In §4.7, we show this occurrence would give a rational point on a genus 4 modular curve of level 54, but in fact all such rational points correspond to cusps. This leaves only points associated to $j$-invariants $-3^2 \cdot 5^6/2^3$ and $3^3 \cdot 13/2^2$. The first corresponds to an isolated point of degree 3 on $X_1(21)$ identified by Najman [47]. In §4.8, we show that there is a point $x \in X_1(28)$ of degree 9 with $j(x) = 3^3 \cdot 13/2^2$ such that the associated Riemann-Roch space is 1-dimensional. Since the Jacobian of $X_1(28)$ has rank 0, this is enough to conclude the point is isolated.

### 4.1. **Elliptic curves with a rational cyclic 25-isogeny.**

**Proposition 21.** *Let $x \in X_1(2^a5^b)$ be a point corresponding to a non-CM elliptic curve with $\deg(x)$ odd and $j(x) \in \mathbb{Q}$. If there exists $y \in X_0(25)(\mathbb{Q})$ with $j(y) = j(x)$, then $x$ is not isolated.*

*Proof.* Suppose by way of contradiction that $x$ is isolated, and fix a model for $E/\mathbb{Q}$. If $b = 0$, then $a \leq 3$ by Theorem 3 and $X_1(2^a)$ has genus 0 (and thus $x$ is not isolated). So we may assume $b > 0$. Then $a \leq 1$ by Proposition 20. Suppose first that $a = 0$. Since $X_1(5)$ has genus 0 (and hence has no isolated points), we may assume $b > 1$. Let $f : X_1(5^b) \to X_1(25)$ be the natural map. By Theorem 7, $\operatorname{im} \rho_{E,5^\infty} = \pi^{-1}(\operatorname{im} \rho_{E,5^2})$ and so $\deg(x) = \deg(f)\deg(f(x))$ by Proposition 16. By Theorem 15, since $x$ is isolated, $f(x) \in X_1(25)$ is also isolated. We claim that $\deg(f(x)) = 5$.

Let $f(x) = [E, P] \in X_1(25)$. Since $f(x)$ has odd degree, the classification of images of mod 5 Galois representations (see, for example, Table 1 in [30]) shows it corresponds to a point of degree 1 or 5 on $X_1(5)$. Let $y \in X_1(5)$ be the point corresponding to $f(x)$ and consider the tower of fields $\mathbb{Q} \subseteq \mathbb{Q}(y) \subseteq \mathbb{Q}(5P) \subseteq \mathbb{Q}(P)$. By Lemma 11, $[\mathbb{Q}(5P) : \mathbb{Q}(y)] \leq 2$. By Proposition 4.6 in [30], $[\mathbb{Q}(P) : \mathbb{Q}(5P)]$ divides either $5^2$ or $4 \cdot 5$. Thus $[\mathbb{Q}(P) : \mathbb{Q}]$ divides $8 \cdot 125$. As $\mathbb{Q}(f(x)) \subseteq \mathbb{Q}(P)$, $\deg(f(x)) = 5^k$ for some $k \leq 3$ (since by assumption $\deg(f(x))$ is odd). By Mazur's result on torsion points over $\mathbb{Q}$ [45], $\deg(f(x)) \neq 1$. If the degree is $5^2$ or $5^3$, then Lemma 14 implies that $f(x)$ is not $\mathbb{P}^1$-isolated, since $X_1(25)$ has genus 12. Thus we must have $\deg(f(x)) = 5$.

We will next show $[E, \langle P \rangle] \in X_0(25)(\mathbb{Q})$. Suppose not. Then since the residue field of this point is a subfield of $\mathbb{Q}(f(x))$, the degree of $[E, \langle P \rangle]$ must be 5. By assumption, $E$ corresponds to a rational point on $X_0(25)$, so there must be a point $Q \in E$ of order 25 such that $[E, \langle Q \rangle] \in X_0(25)(\mathbb{Q})$. As $Q$ and $P$ both have order 25, the group $G \coloneqq \langle Q, P \rangle$ is isomorphic to one of $\mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/5^s\mathbb{Z}$, $s = 0, 1$, or 2. We consider cases according to $\langle Q \rangle \cap \langle P \rangle$. If $\langle Q \rangle$ and $\langle P \rangle$ have nontrivial intersection, then either $\langle Q \rangle \cap \langle P \rangle = \langle Q \rangle$ in which case, $[E, \langle P \rangle]$ is $\mathbb{Q}$-rational, contradicting our assumption, or $|\langle Q \rangle \cap \langle P \rangle| = 5$. As $\langle Q \rangle$ and $\langle P \rangle$ are each cyclic of order 25, they contain a unique subgroup of order 5, and thus $\langle 5Q \rangle = \langle Q \rangle \cap \langle P \rangle = \langle 5P \rangle$. Since $[E, \langle 5Q \rangle] \in X_0(5)(\mathbb{Q})$, the group $\langle 5P \rangle$ is $\mathbb{Q}$-rational. Let $\phi : X_0(25) \to X_0(5)$ be the natural map (note that $\phi$ has degree 5). Then $[E, \langle P \rangle]$ and $[E, \langle Q \rangle]$ are in the support of $\phi^*([E, \langle 5P \rangle])$, which means $\deg(\phi^*([E, \langle 5P \rangle]) \geq 1 + 5$. Since $\deg(\phi^*(y)) = \deg(\phi)\deg(y) = 5 \cdot 1$ for any closed point $y \in X_0(5)(\mathbb{Q})$, we have reached a contradiction.

If $\langle Q \rangle$ and $\langle P \rangle$ have trivial intersection, then $G$ is isomorphic to $\mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$. Since the isogeny character associated to a cyclic subgroup of order $N$ can be trivialized over an extension of degree dividing $\varphi(N)$, we have $[\mathbb{Q}(Q) : \mathbb{Q}] | \varphi(25)$. Moreover, $[\mathbb{Q}(P) : \mathbb{Q}] | 10$ since by assumption, $[E, P]$ has degree 5 and $P$ requires at most a degree 2 extension of this degree 5 extension. Thus $F = \mathbb{Q}(Q, P) = \mathbb{Q}(E[25])$ has degree at most 200. Since $5^4 \nmid [F : \mathbb{Q}]$,

$$[\mathrm{GL}_2(\mathbb{Z}/25\mathbb{Z}) : \operatorname{im} \rho_{E,25}] = \frac{5^5 \cdot 3 \cdot 2^5}{[F : \mathbb{Q}]}$$

is divisible by $5^2$. This contradicts Theorem 2 in [31]. Thus we may assume $[E, \langle P \rangle] \in X_0(25)(\mathbb{Q})$.

Consider the map

$$X_1(25) \to X_{\Delta_2}(25) \to X_0(25),$$

where $X_{\Delta_2}(25)$ denotes the intermediate modular curve associated to $\Delta_2 = \{\pm 1, \pm 4, \pm 6, \pm 9, \pm 11\}$. See [34], [35] for more on intermediate modular curves including the degrees of natural maps and genus information. Since $\deg(X_{\Delta_2}(25) \to X_0(25)) = 2$, $[E, P]$ must correspond to a degree 1 point under the map $X_1(25) \to X_{\Delta_2}(25)$ (otherwise the residue field $M/\mathbb{Q}$ of the image of $[E, P]$ on $X_{\Delta_2}(25)$ is a quadratic extension, but the residue field of $[E, P]$ on $X_1(25)$, which we assumed to have degree 5, contains $M$). Since this map $X_1(25) \to X_{\Delta_2}(25)$ is of degree 5, Theorem 15 implies the image of $f(x)$ is isolated on $X_{\Delta_2}(25)$; as this curve has genus 0, this is impossible.

Next, suppose $a = 1$. So $x = [E, P] \in X_1(2 \cdot 5^b)$ is isolated. Since $X_1(10)$ has genus 0, we may assume $b > 1$. Let $g : X_1(2 \cdot 5^b) \to X_1(50)$ denote the natural map. We will first show that $\deg(x) = \deg(g) \deg(g(x))$. By Theorem 7, $x$ maps to a point $y = [E, 2P] \in X_1(5^b)$ such that $\deg(y) = \deg(f) \deg(f(y))$ where $f$ is the natural map $f : X_1(5^b) \to X_1(25)$. By Proposition 9, we have that $5^{2b-4}$ divides $[\mathbb{Q}(x) : \mathbb{Q}(f(y))] = [\mathbb{Q}(x) : \mathbb{Q}(h(g(x)))]$, where $h : X_1(50) \to X_1(25)$. Since $\deg(h) = 3$ (again, by Proposition 9), it follows that $5^{2b-4}$ divides $[\mathbb{Q}(x) : \mathbb{Q}(g(x))]$, and as $[\mathbb{Q}(x) : \mathbb{Q}(g(x))] \leq \deg(g) = 5^{2b-4}$, it follows that $[\mathbb{Q}(x) : \mathbb{Q}(g(x))] = \deg(g)$ and $\deg(x) = \deg(g) \deg(g(x))$. Thus $g(x) \in X_1(50)$ is isolated by Theorem 15. Next, by the assumption that $\deg(x)$ is odd we have that $\deg(g(x))$ is odd. Then, since $[\mathbb{Q}(g(x)) : \mathbb{Q}(h(g(x)))] \leq \deg(h) = 3$, either $\deg(g(x)) = \deg(h(g(x))$ or $\deg(g(x)) = 3 \cdot \deg(h(g(x)) = \deg(h) \deg(h(g(x)))$. We will show that $\deg(g(x)) = \deg(h) \deg(h(g(x)))$. Suppose by way of contradiction that $\deg(g(x)) = \deg(h(g(x)))$. By the argument given above, $\deg(h(g(x))) = 5^k$ for some $k \in \mathbb{Z}^+$. This implies $E$ corresponds to a point on $X_1(2)$ of degree dividing $5^k$. Since $\deg(X_1(2) \to X_1(1)) = 3$, it follows that $E$ has a 2-isogeny over $\mathbb{Q}$. By assumption $E$ has a 25-isogeny over $\mathbb{Q}$, so this implies $E$ has a 50-isogeny over $\mathbb{Q}$, contradicting Theorem 6. Thus $\deg(g(x)) = \deg(h) \deg(h(g(x)))$. By Theorem 15, $h(g(x))$ is an isolated point on $X_1(25)$, but as shown above, there are no odd degree isolated points on $X_1(5^b)$ for any $b \in \mathbb{Z}^+$. □

4.2. **Elliptic curves with a rational cyclic 21-isogeny.** In Proposition 23, we show that there are no isolated points of odd degree on $X_1(n)$ corresponding to elliptic curves with $j$-invariant $3^3 \cdot 5^3/2$, $-3^2 \cdot 5^3 \cdot 101^3/2^{21}$, or $-3^3 \cdot 5^3 \cdot 383^3/2^7$. This relies on the following lemma, where we give improved bounds on the level of $\rho_{E,14 \cdot 3^\infty}$ using the approach of Prop. 6.1 in [11].

**Lemma 22.** *Let $E/\mathbb{Q}$ be an elliptic curve with LMFDB label 162.c1, 162.c2, or 162.c4. Then* $\operatorname{im} \rho_{E,14 \cdot 3^\infty} = \pi^{-1}(\operatorname{im} \rho_{E,14 \cdot 3^2})$ *and* $\operatorname{im} \rho_{E,7 \cdot 3^\infty} = \pi^{-1}(\operatorname{im} \rho_{E,7 \cdot 3^2})$.

*Proof.* Let $E/\mathbb{Q}$ be one of the curves listed above. Magma confirms $\mathbb{Q}(\zeta_9)^+$ is a subfield of one of the points on $X_1(7)$ associated to $E$, so $\mathbb{Q}(\zeta_9)^+ \subseteq \mathbb{Q}(E[7]) \cap \mathbb{Q}(E[9])$ by the Weil pairing. Following the proof of [11], Prop. 6.1, for all $s \in \mathbb{Z}^+$ we let

$$\begin{aligned} L_s &\coloneqq \ker(\operatorname{im} \rho_{E,14 \cdot 3^s} \to \operatorname{im} \rho_{E,3^s}), \\ K_s &\coloneqq \ker(\operatorname{im} \rho_{E,14 \cdot 3^s} \to \operatorname{im} \rho_{E,14}), \\ K &\coloneqq \ker(\operatorname{im} \rho_{E,14 \cdot 3^\infty} \to \operatorname{im} \rho_{E,14}). \end{aligned}$$

We may view $L_s$ as a subgroup of $\operatorname{im}\rho_{E,14}$ and $K_s$ as a subgroup of $\operatorname{im}\rho_{E,3^s}$. Moreover, we have the following diagram, where the vertical isomorphisms follow from Goursat's Lemma.

$$\begin{array}{ccc} \operatorname{im}\rho_{E,3^s}/K_s & \twoheadrightarrow & \operatorname{im}\rho_{E,3}/K_1 \\ \downarrow\cong & & \downarrow\cong \\ \operatorname{im}\rho_{E,14}/L_s & \twoheadrightarrow & \operatorname{im}\rho_{E,14}/L_1 \end{array}$$

The kernel of the top map is a power of 3, and so the kernel of the bottom map is as well. Thus $[L_1 : L_s]$ is a power of 3, and more generally $[L_{s_1} : L_{s_2}]$ is a power of 3 for all $1 \le s_1 \le s_2$.

We will show the maximal chain of proper containments $L_1 \supsetneq L_2 \supsetneq \cdots \supsetneq L_r$ has length $r = 2$. Magma confirms $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 6$, and moreover that $\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[9]) = \mathbb{Q}$. As above, we let

$$\begin{aligned} L'_s &\coloneqq \ker(\operatorname{im}\rho_{E,2\cdot 3^s} \to \operatorname{im}\rho_{E,3^s}), \\ K'_s &\coloneqq \ker(\operatorname{im}\rho_{E,2\cdot 3^s} \to \operatorname{im}\rho_{E,2}), \\ K' &\coloneqq \ker(\operatorname{im}\rho_{E,2\cdot 3^\infty} \to \operatorname{im}\rho_{E,2}). \end{aligned}$$

As before, $[L'_{s_1} : L'_{s_2}]$ is a power of 3 for all $1 \le s_1 \le s_2$. Since $\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[9]) = \mathbb{Q}$, we have $\#L'_2 = \#L'_1 = 6$. It follows that $L'_1 = L'_2$, which gives the following diagram.

$$\begin{array}{ccc} \operatorname{im}\rho_{E,3^2}/K'_2 & \twoheadrightarrow & \operatorname{im}\rho_{E,3}/K'_1 \\ \downarrow\cong & & \downarrow\cong \\ \operatorname{im}\rho_{E,2}/L'_2 & = & \operatorname{im}\rho_{E,2}/L'_1 \end{array}$$

Since Magma shows $[\mathbb{Q}(E[9]) : \mathbb{Q}(E[3])] = 3^4$, it follows that $\operatorname{im}\rho_{E,3^2} = \pi^{-1}(\operatorname{im}\rho_{E,3})$. Thus the diagram implies

$$\ker(K' \bmod 3^2 \to K' \bmod 3) = I + \mathrm{M}_2(3\mathbb{Z}/3^2\mathbb{Z}).$$

By Prop. 3.5 of [11],

$$\ker(K' \to K' \bmod 3) = I + 3\mathrm{M}_2(\mathbb{Z}_3),$$

and so $\operatorname{im}\rho_{E,2\cdot 3^\infty} = \pi^{-1}(\operatorname{im}\rho_{E,2\cdot 3})$. This means $\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[3^s]) = \mathbb{Q}$ for all $s$.

Let $(\alpha_i, 0)$ for $1 \le i \le 3$ be the points on $E$ of order 2. Magma confirms $\mathbb{Q}(\zeta_7)^+\mathbb{Q}(\alpha_i)$ has degree 9 over $\mathbb{Q}$, and the only subfields of degree 3 are $\mathbb{Q}(\zeta_7)^+$ and $\mathbb{Q}(\alpha_i)$. Neither $\mathbb{Q}(\alpha_i)$ nor $\mathbb{Q}(\zeta_7)^+$ is a subfield of $\mathbb{Q}(E[3^s])$ since $E$ has good reduction at 7, so their compositum is linearly disjoint from $\mathbb{Q}(E[3^s])$. Thus $3^2$ divides the size of $L_s$ for all $s$. Since $\operatorname{ord}_3(\#L_1) \le \operatorname{ord}_3(\#\operatorname{GL}_2(\mathbb{Z}/14\mathbb{Z})) = 3$ and $[L_{s_1} : L_{s_2}]$ is a power of 3 for all $1 \le s_1 \le s_2$, we have $r \le 2$.

Thus the maximal chain of proper containments $L_1 \supsetneq L_2 \supsetneq \cdots \supsetneq L_r$ has length $r = 2$. In particular, we have the following diagram.

$$\begin{array}{ccc} \operatorname{im}\rho_{E,3^3}/K_3 & \twoheadrightarrow & \operatorname{im}\rho_{E,3^2}/K_2 \\ \downarrow\cong & & \downarrow\cong \\ \operatorname{im}\rho_{E,14}/L_3 & = & \operatorname{im}\rho_{E,14}/L_2 \end{array}$$

As above, this implies

$$\ker(K \bmod 3^3 \to K \bmod 3^2) = I + \mathrm{M}_2(3^2\mathbb{Z}/3^3\mathbb{Z}).$$

Prop. 3.5 of [11] now gives that

$$\ker(K \to K \bmod 3^2) = I + 3^2\mathrm{M}_2(\mathbb{Z}_3),$$

and so $\operatorname{im}\rho_{E,14\cdot 3^\infty} = \pi^{-1}(\operatorname{im}\rho_{E,14\cdot 3^2})$. The second claim follows immediately. □

**Proposition 23.** *If $x \in X_1(2^a3^b7^c)$ is a point of odd degree with $b, c > 0$ and $j(x) \in \{3^3 \cdot 5^3/2, -3^2 \cdot 5^3 \cdot 101^3/2^{21}, -3^3 \cdot 5^3 \cdot 383^3/2^7\}$, then $x$ is not isolated.*

*Proof.* Let $x = [E, P] \in X_1(2^a3^b7^c)$ be such an isolated point, and choose the model of $E/\mathbb{Q}$ labeled 162.c1, 162.c2, or 162.c4. Note $E$ has a rational 3-isogeny and a rational 7-isogeny. From the classification in [49], we see that $\rho_{E,3^\infty}$ has level 3, and by Theorem 7, $\rho_{E,7^\infty}$ has level 7. Then by Proposition 6.1 in [11],

$$\operatorname{im} \rho_{E,42^\infty} = \pi^{-1}(\operatorname{im} \rho_{E,2^\alpha 3^\beta 7})$$

where $\beta \leq 4$. Let $g : X_1(2^a3^b7^c) \to X_1(\gcd(2^a3^b7^c, 2^\alpha 3^\beta 7))$ be the natural map. By Proposition 5.8 in [11],

$$\deg(x) = \deg(g) \deg(g(x)),$$

and so $x$ maps to an isolated point on $X_1(\gcd(2^a3^b7^c, 2^\alpha 3^\beta 7))$ by Theorem 15. We have $a \leq 1$ by Proposition 18, and since we have assumed $b, c > 0$, the possibilities for $\gcd(2^a3^b7^c, 2^\alpha 3^\beta 7)$ are $3^d \cdot 7$ or $2 \cdot 3^d \cdot 7$ for $1 \leq d \leq 4$. By Lemma 22 and Theorem 15, we may further assume $d \leq 2$. We consider each $j$-invariant separately:

- Suppose $E = 162.c1$. Factoring division polynomials shows that any odd degree point on $X_1(n')$ for $n' \in \{21, 63, 42, 126\}$ must have degree 63, 567, 189, or 1701, respectively. Since $567 = 9 \cdot 63$ and $1701 = 9 \cdot 189$, by Theorem 15, we need only consider $n' = 3 \cdot 7$ and $n' = 2 \cdot 3 \cdot 7$. However, $X_1(21)$ has genus 5 and $X_1(42)$ has genus 25, so points of degree 63 and 189 (respectively) cannot be isolated by Lemma 14. We have reached a contradiction.
- Suppose $E = 162.c2$. Here, any point of odd degree on $X_1(n')$ must have degree 21, 189, 63, or 567, respectively. As in the previous case, we reach a contradiction.
- Suppose $E = 162.c4$. In this case, an odd degree point on $X_1(n')$ will have degree 9, 81, 27, or 243, respectively. Again, we will reach a contradiction. □

4.3. **On the level of the Galois representations for $E/\mathbb{Q}$ with $j(E) = 3^3 \cdot 5 \cdot 7^5/2^7$.**

**Lemma 24.** *If $E/\mathbb{Q}$ is an elliptic curve with $j(E) = 3^3 \cdot 5 \cdot 7^5/2^7$, then for any choice of basis the image of $\rho_{E,7^\infty}$ contains $I_2 + 7M_2(\mathbb{Z}_7)$.*

*Proof.* Let $E : y^2 + xy = x^3 - x^2 - 107x - 379$ be a particular elliptic curve $E/\mathbb{Q}$ with $j(E) = 3^3 \cdot 5 \cdot 7^5/2^7$. There is a degree 9 extension of $\mathbb{Q}$ which contains the $x$-coordinate of a point of order 7 on $E$. Theorem 1.5 of [62] shows that the mod 7 image of Galois for $E$ is the subgroup $H$ generated by $\begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix}$, $\begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}$, and $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$. By [38, Part I, §6, Lemmas 2 & 3], it will suffice to show that $\operatorname{im} \rho_{E,49}$ is the complete preimage of $\operatorname{im} \rho_{E,7}$.

If not, then the mod 49 image is contained in a maximal subgroup of the mod 49 preimage of $H$, which we denote $\tilde{H}$. This subgroup has 8 maximal subgroups. We verify that for $\tilde{H}$, the set $\{(\operatorname{trace}(g), \det(g)) : g \in \tilde{H}\}$ has 483 elements, while for every maximal subgroup $M$, the size of $\{(\operatorname{trace}(g), \det(g)) : g \in M\}$ has at most 357 elements. For any prime $p \neq 7$ of good reduction,

$$\operatorname{trace}(\rho_{E,49}(\operatorname{Frob}_p)) \equiv a_p(E) \pmod{49}$$
$$\det(\rho_{E,49}(\operatorname{Frob}_p)) \equiv p \pmod{49}.$$

We compute $a_p(E)$ and determine a lower bound for the size of the set $\{(\operatorname{trace}(g), \det(g)) : g \in \operatorname{im} \rho_{E,49}\}$. Testing all primes $p \leq 10^5$, we find that the latter set contains 483 entries, and this proves that the image of $\rho_{E,49}$ must be $\tilde{H}$. The Magma code used is in the file `odd7.txt`. □

4.4. **Isolated points on $X_1(2^ap^b)$ for $p > 3$.**

**Theorem 25.** *Let $x \in X_1(n)$ be an isolated point corresponding to a non-CM elliptic curve with $\deg(x)$ odd and $j(x) \in \mathbb{Q}$. Then $n = 2^a3^b$ for nonnegative integers $a, b$ or $j(x) \in \{-3^2 \cdot 5^6/2^3, 3^3 \cdot 13/2^2\}$.*

*Proof.* Let $x = [E, P] \in X_1(n)$ be an isolated point corresponding to a non-CM elliptic curve with $\deg(x)$ odd and $j(x) \in \mathbb{Q}$. We fix a model for $E/\mathbb{Q}$. For now, we assume $j(x) \neq -3^3 \cdot 13 \cdot 479^3/2^{14}$ and that $j(x)$ is not one of the two $j$-invariants in the theorem statement. By Theorem 3, Proposition 23, and [43, Table 4], $n = 2^ap^b$ for $p \in \{3, 5, 7, 11, 13\}$ and nonnegative integers $a, b$. It suffices to consider the case where $b > 0$ and $p \geq 5$. Then $a \leq 1$ by Proposition 20 (since we have assumed for now that $j(x) \neq -3^3 \cdot 13 \cdot 479^3/2^{14}$, and $3^3 \cdot 13/2^2$ appears in the theorem statement), and $j(x) = 3^3 \cdot 5 \cdot 7^5/2^7$ or $E$ corresponds to a rational point on $X_0(p)$ by Theorem 3. For $p = 5$, we may suppose further that $E$ does not have a $\mathbb{Q}$-rational cyclic 25-isogeny by Proposition 21.

First suppose $n = p^b$, and let $f : X_1(p^b) \to X_1(p)$ be the natural map. Theorem 7 and Lemma 24 give that $\operatorname{im} \rho_{E,p^\infty} = \pi^{-1}(\operatorname{im} \rho_{E,p})$, so $\deg(x) = \deg(f) \cdot \deg(f(x))$ by Proposition 16. Thus $f(x) \in X_1(p)$ is isolated by Theorem 15. However, $X_1(p)$ has no isolated points of odd degree if $p \in \{5, 7, 11, 13\}$, as we will now demonstrate. $X_1(5)$ and $X_1(7)$ have genus 0 and thus have no isolated points. Since $X_1(11)$ and $X_1(13)$ have no non-cuspidal rational points by [45], the assumption of odd degree gives $\deg(f(x)) \geq 3$. However, since $X_1(11)$ has genus 1 and $X_1(13)$ has genus 2, by Lemma 14 the point $f(x)$ is not $\mathbb{P}^1$-isolated. We have reached a contradiction.

So suppose $n = 2p^b$. Let $g : X_1(2p^b) \to X_1(2p)$ be the natural map. We will show that $\deg(x) = \deg(g) \cdot \deg(g(x))$. As above, Theorem 7 and Lemma 24 show $x$ maps to a point $x' = [E, 2P] \in X_1(p^b)$ such that $\deg(x') = \deg(f) \cdot \deg(f(x'))$. By Proposition 9, we have

$$p^{2b-2} \mid [\mathbb{Q}(x) : \mathbb{Q}(f(x'))] = [\mathbb{Q}(x) : \mathbb{Q}(h(g(x)))],$$

where $h : X_1(2p) \to X_1(p)$. Since $\deg(h) = 3$ by Proposition 9, it follows that $p^{2b-2} \mid [\mathbb{Q}(x) : \mathbb{Q}(g(x))]$. Since $[\mathbb{Q}(x) : \mathbb{Q}(g(x))] \leq \deg(g) = p^{2b-2}$, it follows that $[\mathbb{Q}(x) : \mathbb{Q}(g(x))] = \deg(g)$, or that $\deg(x) = \deg(g) \cdot \deg(g(x))$. Thus $g(x) \in X_1(2p)$ is isolated by Theorem 15. We will reach a contradiction by considering each prime separately.

(i) Suppose $p = 5$. Then $X_1(10)$ has genus 0 and thus has no isolated points.

(ii) Suppose $p = 7$. Then $X_1(14)$ has genus 1. By Mazur [45], there are no non-cuspidal rational points on $X_1(14)$, so the assumption of odd degree forces $\deg(g(x)) \geq 3$. Thus the Riemann-Roch space $L(g(x))$ has dimension at least 3, and so $g(x)$ is not $\mathbb{P}^1$-isolated.

(iii) Suppose $p = 11$. Since $E$ corresponds to a rational point on $X_0(11)$ and is non-CM, we have $j(E) = -11^2$ or $j(E) = -11 \cdot 131^3$ by [43, Table 4]. By computing division polynomials associated to a fixed model of $E/\mathbb{Q}$ for each $j$-invariant, we find $\deg(g(x)) \geq 15$. Since $X_1(22)$ has genus 6, the Riemann-Roch space $L(g(x))$ has dimension at least 10, and so $g(x)$ is not $\mathbb{P}^1$-isolated.

(iv) Suppose $p = 13$. Since $\deg(g(x))$ is odd, the classification of images of mod 13 Galois representations for elliptic curves over $\mathbb{Q}$ implies $g(x)$ maps to a point of degree 3 or 39 on $X_1(13)$. See for example [30, Tables 1 & 2]. If it is degree 39, then $g(x) \in X_1(26)$ has degree at least 39. But $X_1(26)$ has genus 10, and so by Lemma 14 the point $g(x)$ is not $\mathbb{P}^1$-isolated. So $g(x)$ must map to a point of degree 3 on $X_1(13)$. Since there are no degree 3 points on $X_1(26)$ associated to elliptic curves with rational $j$-invariant by Theorem 1.3 in [33], we have $\deg(g(x)) = 9$. But then if $h : X_1(26) \to X_1(13)$, we have $\deg(g(x)) = \deg(h) \cdot \deg(h(g(x))$, and so $h(g(x)) \in X_1(13)$ is isolated by Theorem 15. As in the second paragraph, no such isolated point exists.

In each case, we arrive at a contradiction.

If $j(x) = -3^3 \cdot 13 \cdot 479^3/2^{14}$, then $E$ corresponds to a rational point on $X_0(p)$ only if $p = 7$. Thus Theorem 3 shows that $n = 2^a$, $7^b$, $2 \cdot 7^b$, or $2^2 \cdot 7^b$ for $b > 0$. The first three cases follow as above, so it remains to consider the case when $n = 2^2 \cdot 7^b$. We will show that $x$ maps to an isolated point on $X_1(28)$. Let $g : X_1(4 \cdot 7^b) \to X_1(4 \cdot 7)$ and $h : X_1(4 \cdot 7) \to X_1(7)$ be the natural maps. Since the $x$-coordinate of a point of order 4 satisfies a polynomial of degree 6, the degree of $\mathbb{Q}(g(x))$ over $\mathbb{Q}(h(g(x))$ is not divisible by 7. Then as in the third paragraph of this proof,

$$[\mathbb{Q}(x) : \mathbb{Q}(g(x))] = 7^{2b-2} = \deg(g).$$

By Theorem 15, $g(x)$ is isolated. Since $X_1(28)$ has genus 10 and factorization of division polynomials shows that $\deg(g(x)) = 63$, $g(x)$ is not $\mathbb{P}^1$-isolated by Lemma 14. □

4.5. **Isolated points on $X_1(2^a3^b)$.** To study isolated points on $X_1(2^a3^b)$ we rely on the results of [49], which give a complete classification of the image of the 3-adic Galois representation for non-CM elliptic curves $E/\mathbb{Q}$ with a rational 3-isogeny. The only cases that arise are parametrized by genus 0 modular curves, and Sutherland and Zywina [59] exhibit all such subgroups containing $-I$. (Note for any $E/\mathbb{Q}$ there exists a twist $E'/\mathbb{Q}$ such that $-I \in \operatorname{im} \rho_{E'}$, and the choice of twist does not affect the degree of a point on $X_1(N)$.) A table giving a list of these images appears in the appendix.

**Proposition 26.** *Let $x \in X_1(2^a3^b)$ be an isolated point corresponding to a non-CM elliptic curve with $\deg(x)$ odd and $j(x) \in \mathbb{Q}$. Then $x$ maps to an isolated point on one of $X_1(54)$ or $X_1(162)$.*

*Proof.* Let $x = [E, P] \in X_1(2^a3^b)$ be an isolated point corresponding to a non-CM elliptic curve with $\deg(x)$ odd and $j(x) \in \mathbb{Q}$. We fix a model of $E/\mathbb{Q}$. If $b = 0$, then $x$ is not isolated as in the proof of Proposition 21. Next, suppose $a = 0$, and let $3^d$ be the level of the 3-adic Galois representation associated to $E$. Then $\deg(x) = \deg(f)\deg(f(x))$, where $f : X_1(3^b) \to X_1(\gcd(3^d, 3^b))$ is the natural map; see Proposition 5.8 in [11]. By Lemma 17, $E$ has a rational 3-isogeny and from the classification in [49] it follows that $d \leq 3$. Thus $f(x) \in X_1(3^{d'})$ is isolated by Theorem 15 for some $d' \leq 3$ by Proposition 16. If $d' \leq 2$, then we have reached a contradiction since $X_1(3^{d'})$ has genus 0, so suppose $d' = 3$. Note this is only possible if the image of the 3-adic Galois representation associated to $E$ has level 27, which implies that it is $27A^0$-$27a$. By looking at orbit sizes of points of order 9 and points of order 27 (see Appendix), we see that in fact $f(x)$ will again map to an isolated point on $X_1(9)$, which is a contradiction.

Thus we may assume $a, b > 0$, and $E$ has a rational 3-isogeny by Lemma 17. By the classification in [49], the 3-adic Galois representation has level $3^d$ for $d \in \{1, 2, 3\}$. Then by Proposition 6.1 in [11],

$$\operatorname{im} \rho_{E,6^\infty} = \pi^{-1}(\operatorname{im} \rho_{E,2^\alpha 3^\beta})$$

where $\beta \leq d + 1$. Let $g : X_1(2^a3^b) \to X_1(\gcd(2^a3^b, 2^\alpha 3^\beta))$ be the natural map. By Proposition 5.8 in [11],

$$\deg(x) = \deg(g)\deg(g(x)),$$

and so $x$ maps to an isolated point on $X_1(\gcd(2^a3^b, 2^\alpha 3^\beta))$ by Theorem 15. Since $a \leq 2$ by Theorem 3, and $\beta \leq 4$, it follows that $x$ maps to an isolated point on $X_1(2^m3^n)$ for $m \leq 2$ and $n \leq 4$. We have already shown we cannot have $m = 0$ or $n = 0$, so after removing curves of genus 0 we are left with

$$X_1(2 \cdot 3^2),\ X_1(2 \cdot 3^3),\ X_1(2 \cdot 3^4)$$
$$X_1(2^2 \cdot 3^2),\ X_1(2^2 \cdot 3^3), \text{ and } X_1(2^2 \cdot 3^4).$$

Now $X_1(18)$ has no non-cuspidal points of degree 1 by [45], so any point of odd degree must have degree at least 3. Since $X_1(18)$ has genus 2, the point $g(x)$ is not $\mathbb{P}^1$-isolated by Lemma 14. It

remains to rule out curves of the form $X_1(2^2 \cdot 3^n)$. Note that if $g(x) \in X_1(2^2 \cdot 3^n)$ is of odd degree, then its image on $X_1(4)$ has odd degree.

First suppose $E$ does not have a rational point of order 2. Then the only way $E$ can correspond to a point on $X_1(4)$ of odd degree is if $E$ gives a rational point on X20 by [50]. However, the fiber product of $X_0(3)$ and X20 has non-cuspidal points corresponding only to $j = 3^2 \cdot 23^3/2^6$ and $j = -3^3 \cdot 11^3/2^2$ [19, Prop. 6]. Using the classification of 3-adic images in [49], we confirm the 3-adic Galois representation associated to an elliptic curve with each of these $j$-invariants has level 3. Thus it suffices to rule out isolated points on $X_1(36)$ corresponding to these $j$-invariants. Note $X_1(36)$ has genus 17. By computing division polynomials, we see that in either case the degree of a point on $X_1(36)$ is at least 27, and so by Lemma 14 the point is not isolated.

Suppose $E$ has a rational point of order 2. Since $\deg(X_1(4) \to X_1(2))$ has degree 2, $x$ corresponds to a point of odd degree on $X_1(4)$ only if it has degree 1. We now consider the possible images of the 3-adic Galois representation associated to $E$ in the case where it has a 4-isogeny and a 3-isogeny. It suffices to consider only those subgroups containing $-I$ (since if $-I$ is not contained in the 3-adic image, a twist of $E$ can be chosen so that it does). Then:

- the 3-adic image cannot be contained in $9B^0$-$9a$, since that would imply $E$ had a rational cyclic 36-isogeny, contradicting Theorem 6.
- the 3-adic image cannot be contained in $3D^0$-$3a$, since that would imply $E$ had a 3-isogeny and an independent 12-isogeny. This cannot occur. See [36, Theorem 2].
- the 3-adic image cannot be contained in $9C^0$-$9a$ because the fiber product of $X_0(4)$ and $X_{9C^0\text{-}9a}$ covers the fiber product of $X_0(2)$ and $X_{9C^0\text{-}9a}$ and that curve has no non-cuspidal, non-CM rational points. It is genus 2 with 5 rational points: 3 cusps, $j = 0$ and $j = 2^4 \cdot 3^3 \cdot 5^3$. Code is available in the file `x02andX9C.txt`.

Thus the image of the 3-adic Galois representation associated to $E$ must be $3B^0$-$3a$. In particular, it has level 3. This is the case where $\beta \leq 2$, so $x$ maps to an isolated point on $X_1(4 \cdot 3^2)$ of degree at least 9. We consider two cases.

(i) Suppose $x$ lies above a point of degree 1 on $X_1(3)$. Since $x$ also lies above a point of degree 1 on $X_1(4)$, then the assumption that $x$ has odd degree means it corresponds to a point of degree 1 on $X_1(12)$. Then $x$ corresponds to a point of degree 9 on $X_1(36)$, and since $\deg(X_1(36) \to X_1(12)) = 9$, by Theorem 15 $x$ maps to an isolated point on $X_1(12)$. This is a contradiction since $X_1(12)$ has genus 0.

(ii) Suppose $x$ lies above a point of degree 3 on $X_1(3)$. Then $x$ corresponds to a point of degree at least 27 on $X_1(36)$. Since $X_1(36)$ has genus 17, by Lemma 14 the point on $X_1(36)$ is not isolated.

In every case, we have reached a contradiction, so we are left with the curves $X_1(2 \cdot 3^3)$ and $X_1(2 \cdot 3^4)$, as in the theorem statement. □

### 4.6. Isolated points on $X_1(54)$ and $X_1(162)$.

**Proposition 27.** *Any odd degree, non-cuspidal, non-CM isolated point on $X_1(162)$ with $j(x) \in \mathbb{Q}$ maps to an isolated point on $X_1(54)$. Moreover, there are no non-cuspidal, non-CM isolated points on $X_1(54)$ for which the corresponding $j(x) \in \mathbb{Q}$ and the elliptic curve $E$ satisfies $[\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[27]) : \mathbb{Q}] \in \{1, 2, 3\}$.*

*Proof.* If $E$ is an elliptic curve and $j(x) \in \mathbb{Q}$, then the degree of $\mathbb{Q}(E[3^k])/\mathbb{Q}(j)$ is a divisor of $|\operatorname{GL}_2(\mathbb{Z}/3^k\mathbb{Z})| = 2^4 \cdot 3^{4k-3}$. This implies that if $x$ is an odd degree point with $j(x) \in \mathbb{Q}$, then the degree of $x$ is a power of 3.

First suppose that $x = [E, P]$ is a non-cuspidal, non-CM isolated point on $X_1(162)$, and fix a model of $E/\mathbb{Q}$. We will show that the image of $x$ on $X_1(54)$ is isolated. As in the proof of Proposition 26, if the level of the 3-adic Galois representation associated to $E$ is $3^d$ for $d \leq 3$, the

level of the 6-adic Galois representation is $2^\alpha 3^\beta$, where $\beta \leq d+1$. Thus $x$ maps to an isolated point on $X_1(\gcd(2^a 3^b, 2^\alpha 3^\beta))$. Proposition 26 shows $d \neq 1$, and if $d = 2$, then $x$ would map to an isolated point on $X_1(54)$, as desired. Thus we may assume $d = 3$. This implies the 3-adic image is equal to $27A^0$-$27a$ (up to $\pm I$). The fiber product $X_{27A^0\text{-}27a} \times_{X_0(1)} X_0(2)$ is the genus 2 curve $y^2 = x^6 + 10x^3 + 1$ whose Jacobian has rank zero and has exactly four rational points (all of them cusps). For details, see the file `x02andX27A.txt` It follows that $E$ does not have a rational 2-isogeny. Let $G$ be the image of the mod 162 Galois representation attached to $E$. Let $\pi_1 : G \to \mathrm{GL}_2(\mathbb{Z}/81\mathbb{Z})$ and $\pi_2 : G \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ be the natural reduction maps. From the classification of the 3-adic representation, the image of $\pi_1$ contains all matrices $\equiv I \pmod{27}$. Let $H$ be the preimage under $\pi_2$ of a subgroup of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ of index 3. Then $H$ has index 3 in $G$ and so $\pi_1(H)$ is either equal to the mod 81 image of Galois or an index 3 subgroup thereof. However, every maximal subgroup of $27A^0$-$27a$ has level 27 and this means that $\pi_1(H)$ contains all matrices congruent to the identity mod 27. If $g \in H$ is congruent to the identity modulo 27 then $g^2$ is congruent to the identity modulo 54 and from this we see that $G$ contains all matrices congruent to the identity modulo 54. This implies that the degree of $x$ on $X_1(162)$ is $\deg(X_1(162) \to X_1(54))$ times the degree of the image of $x$ on $X_1(54)$ and so the image of $x$ on $X_1(54)$ is isolated by Theorem 15.

For the remainder of the proof, we will assume that $x$ is an odd degree, non-cuspidal, non-CM isolated point on $X_1(54)$ with $j(x) \in \mathbb{Q}$. We fix a model of $E/\mathbb{Q}$.

Suppose that $E$ has a rational point of order 2. The fact that $X_1(18)$ has no odd degree isolated points with rational $j$-invariant implies that the level of the 3-adic Galois representation must be 27 but as mentioned above, the fiber product $X_{27A^0\text{-}27a} \times_{X_0(1)} X_0(2)$ has no non-cuspidal rational points, which is a contradiction.

Next, suppose that the elliptic curve $E$ has no rational point of order 2 and that $\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[27])$ is either $\mathbb{Q}$ or a quadratic extension of $\mathbb{Q}$. This implies that the residue field of $[E, 2P]$ on $X_1(27)$ does not contain the $x$-coordinate of a 2-torsion point, and so the residue field of $[E, P]$ on $X_1(54)$ is a cubic extension of that for $[E, 2P]$ on $X_1(27)$, and by Theorem 15, the image of $x$ on $X_1(27)$ must be isolated. From the 3-adic classification, this does not occur.

Next, suppose that $\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[27])$ is a cyclic cubic extension of $\mathbb{Q}$. This implies that $E$ has square discriminant $\Delta(E)$. A straightforward computation shows that $(j(E) - 1728)\Delta(E)$ is a square, from which it follows that $j(E) = 1728 + t^2$ for some $t \in \mathbb{Q}$. There are infinitely many elliptic curves with square discriminant and with 3-adic image contained in $9C^0$-$9a$, but the modular curves parametrizing elliptic curves with square discriminant and a 9-isogeny, or square discriminant and a pair of two independent 3-isogenies both have genus 1 and are isomorphic to $y^2 = x^3 - 27$. This elliptic curve has two rational points and in both cases, these rational points are cusps. (See the files X9B0squaredisc.txt and X3D0squaredisc.txt.) It remains to consider subgroups of $9C^0$-$9a$, and these are $9J^0$-$9a$, $9J^0$-$9b$ and $9J^0$-$9c$. The latter two would give rise to points on $X_1(54)$ of degree 81 or higher, so it suffices to consider the fiber product of $X_{9J^0\text{-}9a}$ and the curve $j = 1728 + t^2$. This curve has genus 2 and is isomorphic to $y^2 = x^5 + 4x^4 + 3x^3 - x^2 - x$. The Jacobian has rank zero and the curve has precisely three rational points, all of which are cusps. (See the file `X9J09asquaredisc.txt` for details.) Therefore, this case does not occur. □

4.7. **A certain entanglement related to odd degree isolated points on $X_1(54)$.** We must handle the final case not covered by Proposition 27. Before we begin the proof, we provide an overview. If $E/\mathbb{Q}$ is an elliptic curve with a cyclic 9-isogeny, then $E$ gives rise to a point of degree $\leq 81$ on $X_1(54)$. In particular, since $\deg(X_0(27) \to X_0(9)) = 3$, there is a cubic extension $K_1/\mathbb{Q}$ over which $E$ acquires a cyclic 27-isogeny. Since $\deg(X_1(27) \to X_0(27)) = 9$, there is a degree $\leq 9$ extension $K_2/K_1$ over which $E$ acquires a point of order 27. Finally, there is an extension $K_3/K_2$ of degree $\leq 3$ over which $E$ acquires a point of order 2. If this point has degree 81, then it is not

isolated (by Lemma 14) since the genus of $X_1(54)$ is 52. However, we must rule out the possibility that this degree is 27 or less.

We will show that *the only way* the degree of this point is $\leq 27$ is if the cubic extension of $\mathbb{Q}$ over which $E$ acquires a cyclic 27-isogeny is *the same* as the cubic extension over which $E$ acquires a 2-torsion point. Elliptic curves with this property are parametrized by a modular curve $X_K$ of genus 4, where $K$ is a particular subgroup of $\mathrm{GL}_2(\mathbb{Z}/54\mathbb{Z})$. In the course of the proof of the proposition below, we will write down an equation for $X_K$ and show that its only rational points are cusps. This leads to a contradiction.

To start, we give a general criterion that determines the values of a parameter $x$ for which two cubic extensions of $\mathbb{Q}(x)$ have isomorphic specializations.

**Lemma 28.** *Suppose that $p_1(t,x) = t^3 + A_2t + A_3$ and $p_2(t,x) = t^3 + B_2t + B_3$ are two irreducible cubic polynomials in $\mathbb{Q}(x)[t]$. For $x_0 \in \mathbb{Q}$ for which $p_1(t,x_0)$ and $p_2(t,x_0)$ remain irreducible, the number fields defined by $p_1(t,x_0)$ and $p_2(t,x_0)$ are isomorphic if and only if*

$$f(t,x_0) = t^6 - 6A_2B_2t^4 - 27A_3B_3t^3 + 9A_2^2B_2^2t^2 + 81A_2A_3B_2B_3t - 4A_2^3B_2^3 - 27A_2^3B_3^2 - 27A_3^2B_2^3$$

*has a rational root.*

*Proof.* Let $L/\mathbb{Q}$ be the degree three extension containing a root of both $p_1(t,x_0)$ and $p_2(t,x_0)$ and let $M/\mathbb{Q}$ be its Galois closure. Let $t_1$, $t_2$ and $t_3$ be the roots of $p_1(t,x_0)$ in $M$ and $t_4$, $t_5$, and $t_6$ be the roots of $p_2(t,x_0)$ in $M$ and view $\mathrm{Gal}(M/\mathbb{Q}) \subseteq S_3 \times S_3 \subseteq S_6$. Order these roots so that there is some $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$ so that $\sigma(t_1) = t_2$, $\sigma(t_2) = t_3$, $\sigma(t_4) = t_5$ and $\sigma(t_5) = t_6$. It follows that $\theta_1 = t_1t_4 + t_2t_5 + t_3t_6 = \mathrm{tr}_{L/\mathbb{Q}}(t_1t_4) \in \mathbb{Q}$. Let $\theta_2$, $\theta_3$, $\theta_4$, $\theta_5$ and $\theta_6$ be the other elements in the orbit of $\theta_1$ under the action of $S_3 \times S_3$; these are the polynomials $t_1t_{\pi(4)} + t_2t_{\pi(5)} + t_3t_{\pi(6)}$ for $\pi$ a non-identity permutation of $\{4,5,6\}$. It follows that $\prod_{i=1}^6 (t - \theta_i) \in \mathbb{Q}[t]$ and has a rational root and a linear algebra calculation carried out in Magma (see the file `deg3iso.txt` for details) shows that $\prod_{i=1}^6 (t - \theta_i) = f(t,x_0)$.

Conversely, if $f(t,x_0)$ has a rational root and the roots of $f(t,x_0)$ are distinct, then $t_1t_{\pi(4)} + t_2t_{\pi(5)} + t_3t_{\pi(6)} \in \mathbb{Q}$ for some permutation $\pi$ of $\{4,5,6\}$. This element must be fixed by $\mathrm{Gal}(M/\mathbb{Q})$ and the set of permutations in $S_3 \times S_3$ that fix $t_1t_{\pi(4)} + t_2t_{\pi(5)} + t_3t_{\pi(6)}$ form a subgroup isomorphic to $S_3$. Therefore $\mathrm{Gal}(M/\mathbb{Q})$ is isomorphic to a subgroup of $S_3$ and in particular contains a unique subgroup of index 3. Hence the number fields defined by $p_1(t,x_0)$ and $p_2(t,x_0)$ are isomorphic. If $f(t,x_0)$ has a repeated root, then its discriminant is zero. Computing the discriminant of $f(t,x_0)$ shows that either $p_1(t,x_0)$ has a repeated root, $p_2(t,x_0)$ has a repeated root, or that $\frac{A_2^3}{A_3^2} = \frac{B_2^3}{B_3^2}$ which implies that the number fields defined by $p_1(t,x_0)$ and $p_2(t,x_0)$ are isomorphic in this case as well. □

**Proposition 29.** *There are no odd degree, non-cuspidal, non-CM isolated points $x$ on $X_1(54)$ for which $j(x) \in \mathbb{Q}$ and the corresponding elliptic curve $E$ has $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 6$ and $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[27])$.*

*Proof.* Since $x$ must give rise to a point of degree $\leq 27$ on $X_1(54)$, it follows that $E$ must have a point of order 9 in degree 1 or 3. This forces the 3-adic image to equal (up to $\pm I$) 9$B^0$-9$a$, 9$H^0$-9$b$, 9$I^0$-9$a$, 9$I^0$-9$b$, 9$I^0$-9$c$, 9$J^0$-9$a$, or 27$A^0$-27$a$. We next consider the possibilities $K$ for the image of the mod 54 Galois representation attached to $E$. If $\pi_1 : K \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and $\pi_2 : K \to \mathrm{GL}_2(\mathbb{Z}/27\mathbb{Z})$ are the reductions modulo 2 and 27, respectively, then the assumption that $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[27])$ implies that $\ker \pi_2 \subseteq \ker \pi_1$. For each option for the 3-adic image above, we enumerate subgroups $K$ with this property. We rule out any which would force $x$ yields a degree 27 point on $X_1(54)$ and a degree 3 point on $X_1(18)$ since in that case, the image on $X_1(18)$ must be isolated. The genus of $X_1(18)$ is 2 and so this contradicts Lemma 14. Every subgroup $K$ we find is conjugate in $\mathrm{GL}_2(\mathbb{Z}/54\mathbb{Z})$ to a subgroup of one particular subgroup of index 72 that corresponds to the 3-adic

image of Galois equalling $9B^0$-$9a$, which corresponds to $E$ having a cyclic 9-isogeny. (See the file `S3entanglement.txt` for details.) For the rest of the proof, $K$ will denote this particular subgroup of $\mathrm{GL}_2(\mathbb{Z}/54\mathbb{Z})$. The corresponding modular curve $X_K$ has genus 4. There is an element $\vec{v}$ of order 2 in $(\mathbb{Z}/54\mathbb{Z})^2$ whose stabilizer in $K$ is contained in $\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/54\mathbb{Z}) : c \equiv 0 \pmod{54}\right\}$. In particular, if $E/\mathbb{Q}$ is an elliptic curve with $\operatorname{im}\rho_{E,54} \subseteq K$, then $E$ has a rational 9-isogeny and the cubic field over which $E$ acquires a rational point of order 2, and the cubic field over which $E$ acquires a cyclic 27-isogeny are isomorphic. To write down an equation for the modular curve $X_K$, we wish to apply Lemma 28. Since $E$ has a cyclic 9-isogeny, we choose a parameter $x_9$ for which $\mathbb{Q}(X_0(9)) = \mathbb{Q}(x_9)$ consistent with Magma's small modular curves database. We represent these two (a priori different) cubic extensions as degree 3 extensions of $\mathbb{Q}(x_9)$.

Magma's small modular curves database gives the map to the $j$-line $j : X_0(9) \to X_0(1)$ as

$$j = \frac{(x_9+9)^3(x_9^3+243x_9^2+2187x_9+6561)^3}{x_9^9(x_9^2+9x_9+27)}.$$

The curve $X_0(27)$ has equation $y^2+y = x^3-7$. Define $\phi : X_0(27) \to X_0(9)$ by $\phi(x,y) = -3+(y+5)/x$. Then $j\circ\phi$ is the map from $X_0(27)$ to the $j$-line. We wish to represent $X_0(27)$ as a degree 3 cover of $X_0(9)$ via this map, and a Gröbner basis computation shows that if $x_9 \in \mathbb{Q}$, the $x$-coordinate of a preimage of $x_9$ under $\phi$ satisfies

$$x^3-(x_9^2+6x_9+9)x^2+(9x_9+27)x-27 = 0.$$

We make a change of variables, setting $t = 3x-(x_9+3)^2$ and obtain

$$p_1(t,x_9) = t^3-(3x_9^4+36x_9^3+162x_9^2+243x_9)t-(2x_9^6+36x_9^5+270x_9^4+999x_9^3+1701x_9^2+729x_9) = 0.$$

This makes the coefficient of $t^2$ equal to 0. Using an equation for $X_0(2)$, one finds that the degree 3 subfield of $\mathbb{Q}(E[2])$ is given by $p_2(t,x_9) = t^3-jt-16j = 0$. We can now apply Lemma 28. This gives rise to an equation involving $t$ and $x_9$ which has degree 41 in $x_9$ and degree 6 in $t$. We wish to find all of the rational points on the curve defined by this equation. Using the methods in van Hoeij and Novocin's preprint [61], we are able to find a much simpler polynomial that defines the same function field. We find the polynomial

$$X_K : t^6+(-2x_9^3-18x_9^2-54x_9)t^3+x_9^6+18x_9^5+135x_9^4+513x_9^3+972x_9^2+729x_9 = 0.$$

The map $(t,x_9) \mapsto (t^3,x_9)$ is clearly a map to the curve

$$Y : y^2+(-2x_9^3-18x_9^2-54x_9)y+x_9^6+18x_9^5+135x_9^4+513x_9^3+972x_9^2+729x_9 = 0$$

This curve $Y$ has genus 1 and is isomorphic to $y^2 = x^3+1$. This elliptic curve has rank zero and Mordell-Weil group $\mathbb{Z}/6\mathbb{Z}$. The six rational points on $Y$ are $(-324:-9:1)$, $(0:0:1)$, $(1:0:0)$, $(-162:-9:1)$, $(0:-3:1)$, and $(-54:-3:1)$. Of these six points, two are rational cusps, two have image $j = 0$, and two have image $j = -2^{15}\cdot 3\cdot 5^3$. Only two of the rational points on $Y$ lift to rational points on $X_K$, and those are the rational cusps. In particular, the only rational points on $X_K$ are cusps, and there are no non-CM elliptic curves $E$ with $j(E) \in \mathbb{Q}$ that give rise to an odd degree isolated point on $X_1(54)$ and for which $\mathbb{Q}(E[2])/\mathbb{Q}$ is an $S_3$ extension contained in $\mathbb{Q}(E[27])$. A script documenting this computation is in the file `genus4.txt`. □

Although the curve $X_K$ has no non-cuspidal rational points, points on $X_K$ over a number field $k$ do give rise to points on $X_1(54)$ that have degree $\leq 27$ over $k$. For example, there is a cubic point on $X_K$ with $x_9 = \frac{-3\sqrt[3]{105}-21}{7}$. This corresponds to the elliptic curve

$$y^2+xy+ky = x^3, \quad k = -\left(\frac{3\sqrt[3]{105}^2+42\sqrt[3]{105}+211}{1131}\right)^3$$

and it can be verified that this elliptic curve has a point of order 54 over a degree 27 extension of $\mathbb{Q}(\sqrt[3]{105})$.

4.8. **Non-CM isolated points of odd degree.**

**Theorem 30.** *Let $\mathcal{I}_{odd}$ denote the set of all isolated points of odd degree on all modular curves $X_1(N)$ for $N \in \mathbb{Z}^+$. Then the non-CM $j$-invariants in $j(\mathcal{I}_{odd}) \cap \mathbb{Q}$ are $-3^2 \cdot 5^6/2^3$ and $3^3 \cdot 13/2^2$.*

*Proof.* The fact that $j(\mathcal{I}_{odd}) \cap \mathbb{Q} \subseteq \{-3^2 \cdot 5^6/2^3, 3^3 \cdot 13/2^2\}$ follows from Theorem 25, Proposition 26, Proposition 27, and Proposition 29. It remains to show that these two $j$-invariants correspond to isolated points of odd degree. By work of Najman [47], there is an isolated (in fact, sporadic) point $x \in X_1(21)$ with $\deg(x) = 3$ and $j(x) = -3^2 \cdot 5^6/2^3$. We have also identified a degree 9 point $x \in X_1(28)$ corresponding to the elliptic curve $E$ with LMFDB label 338.e2. Since the Jacobian of $X_1(28)$ has rank 0 [23, Lemma 1], it suffices to show $x$ is $\mathbb{P}^1$-isolated. We use the model of $X_1(28)$ computed by Sutherland [57] (see Table 6). The universal elliptic curve has the form $E_u : y^2 + xy + uy = x^3 + ux^2$ for some $u \in \mathbb{Q}(X_1(28))$. We first find the choices of $u$ in the degree 9 number field $\mathbb{Q}(x)$ for which $j(E_u) = 3^3 \cdot 13/2^2$. There are two such, but only one gives points in the desired degree 9 number field. In the end, we find 6 points on $X_1(28)$ over the desired number field that are interchanged by diamond automorphisms and choose one of them to create a degree 9 divisor $D$ over $\mathbb{Q}$ on $X_1(28)$. Since the natural reduction of a principal divisor is principal over any prime of good reduction [6, Thm. 9.5.1], it suffices to show that the Riemann-Roch space $L(\check{D})$ over $\mathbb{F}_{11}$ is one-dimensional. This can be verified in Magma; see the file `X128.txt` for details. Thus there are no non-constant functions $f : X_1(28) \to \mathbb{P}^1$ over $\mathbb{Q}$ with poles only at $D$ and so the degree 9 point on $X_1(28)$ is isolated. □

## 5. The CM Case

In this section we show that any CM $j$-invariant in $j(\mathcal{I}_{odd}) \cap \mathbb{Q}$ belongs to the set

$$\{-2^{18}3^35^3,\ -2^{15}3^35^311^3,\ -2^{18}3^35^323^329^3\},$$

completing the proof of Theorem 2. These are the elliptic curves with CM by the orders of discriminant $-43, -67, -163$, respectively. Our results follow from work of the first author and Clark [8], [9].

5.1. **Preliminaries on Cartan orbits.** We first recall the necessary ingredients from [8, §7]. Let $\mathcal{O}$ be an order in an imaginary quadratic field and let $N$ be a positive integer. If $P \in \mathcal{O}/N\mathcal{O}$ is a point of order $N$ (which by §2.6 corresponds to a point of order $N$ on an $\mathcal{O}$-CM elliptic curve), then define $M_P := \{xP \mid x \in \mathcal{O}\}$ to be the $\mathcal{O}$-submodule of $\mathcal{O}/N\mathcal{O}$ generated by $P$ and $I_P := \{x \in \mathcal{O} \mid xP = 0\}$. There is a canonical $\mathcal{O}$-module isomorphism

$$M_P \cong \mathcal{O}/I_P$$

defined by $P \mapsto 1 + I_P$. We may use this isomorphism to determine the size of the $(\mathcal{O}/N\mathcal{O})^\times$-orbit on $P$. Recall we denote $(\mathcal{O}/N\mathcal{O})^\times$ by $C_N(\mathcal{O})$.

**Lemma 31.** *Let $p$ be an odd prime, and let $\mathcal{O}$ be an imaginary quadratic order of discriminant $\Delta$ such that $\left(\frac{\Delta}{p}\right) = 0$. Let $P \in \mathcal{O}/p^a\mathcal{O}$ be a point of order $p^a$. Then as abelian groups, $M_P \cong \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}/p^b\mathbb{Z}$ for some integers $0 \le b \le a$, and the $C_{p^a}(\mathcal{O})$-orbit on $P$ has size $p^{a+b-1}(p-1)$.*

*Proof.* The fact that $M_P \cong_{\mathbb{Z}} \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}/p^b\mathbb{Z}$ for some $0 \le b \le a$ is Lemma 7.5 in [8]. Since $\left(\frac{\Delta}{p}\right) = 0$, $\mathcal{O}/I_P$ is local with residue field $\mathbb{Z}/p\mathbb{Z}$. Thus

$$\#(\mathcal{O}/I_P)^\times = \#\mathcal{O}/I_P - \frac{\#\mathcal{O}/I_P}{p} = p^{a+b-1}(p-1).$$

By [8, Lemma 7.4], the size of the $C_N(\mathcal{O})$-orbit on $P$ is equal to the size of $(\mathcal{O}/I_P)^\times$. □

**Lemma 32.** *Let $p$ be an odd prime, and let $\mathcal{O}$ be an imaginary quadratic order of discriminant $\Delta$ such that $\left(\frac{\Delta}{p}\right) \neq 1$. Let $P \in \mathcal{O}/p^a\mathcal{O}$ be a point of order $p^a$ for $a \in \mathbb{Z}^+$. Suppose for some integer $0 \leq m \leq a$ the $C_{p^m}(\mathcal{O})$-orbit on $p^{a-m}P \in \mathcal{O}/p^m\mathcal{O}$ has size greater than $\varphi(p^m)$. Then the size of the $C_{p^a}(\mathcal{O})$-orbit on $P$ is equal to $p^{2(a-m)}$ times the size of the $C_{p^m}(\mathcal{O})$-orbit on $p^{a-m}P$.*

*Proof.* If $\left(\frac{\Delta}{p}\right) = -1$, this follows from [8, Theorem 7.8], so henceforth we may assume $\left(\frac{\Delta}{p}\right) = 0$. Following [8, §7D], we observe that $x \mapsto p^{a-m}x$ gives an $\mathcal{O}$-module isomorphism

$$\mathcal{O}/p^m\mathcal{O} \to p^{a-m}\mathcal{O}/p^a\mathcal{O}.$$

This allows us to view $\mathcal{O}/p^m\mathcal{O}$ as an $\mathcal{O}$-submodule of $\mathcal{O}/p^a\mathcal{O}$. Since we have assumed the $C_{p^m}(\mathcal{O})$-orbit on $p^{a-m}P \in \mathcal{O}/p^m\mathcal{O}$ has size greater than $\varphi(p^m)$, Lemma 31 shows

$$M_P \cong_{\mathbb{Z}} \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}/p^b\mathbb{Z},$$
$$M_{p^{a-m}P} \cong_{\mathbb{Z}} \mathbb{Z}/p^m\mathbb{Z} \times \mathbb{Z}/p^{b'}\mathbb{Z}$$

for some $0 \leq b \leq a$ and $1 \leq b' \leq m$. Since $p^{a-m}M_P = M_{p^{a-m}P}$, we see that $b = b' + a - m$. Another application of Lemma 31 shows that $P$ lies in a $C_{p^a}(\mathcal{O})$-orbit of size $p^{2(a-m)}$ times the size of the $C_{p^m}(\mathcal{O})$-orbit on $p^{a-m}P$. □

5.2. **CM version of Theorem 7.** The following theorem shows that, as in the case of non-CM elliptic curves over $\mathbb{Q}$, points on $X_1(p^a)$ corresponding to a CM elliptic curve $E$ with a rational cyclic $p$-isogeny over $\mathbb{Q}(j(E))$ often arise in largest possible degree allowed by the isogenies. For relevant background information on CM elliptic curves, see Section 2.6.

**Proposition 33.** *Let $p$ be an odd prime and let $E$ be a $K$-CM elliptic curve. Define $m$ to be the maximum integer such that there exists $y \in X_0(p^m)(\mathbb{Q}(j(E))$ with $j(y) = j(E)$.[4] If $m \geq 1$ and $\left(\frac{\Delta_K}{p}\right) \neq 1$, then for any integer $a > m$ and any point $x \in X_1(p^a)$ with $j(x) = j(E)$, we have*

$$\deg(x) = \deg(f(x)) \cdot \deg(f),$$

*where $f : X_1(p^a) \to X_1(p^m)$ is the natural map.*

*Proof.* Let $x = [E, P] \in X_1(p^a)$. The assumption that $m \geq 1$ means there exists a model of $E/\mathbb{Q}(j(E))$ with a rational cyclic $p$-isogeny. Since $p$ is odd, $\left(\frac{\Delta}{p}\right) = 0$ by Proposition 6.8 of [9]. Furthermore, if $\Delta = -3$, then $m = 2$; see, for example, [9, Corollary 5.11].

As in the proof of Lemma 32, we may identify $P$ with an element of $\mathcal{O}/p^a\mathcal{O}$ of order $p^a$ and $p^{a-m}P$ with an element of $\mathcal{O}/p^m\mathcal{O}$ of order $p^m$. Suppose first that the $C_{p^m}(\mathcal{O})$-orbit on $p^{a-m}P$ has size greater than $\varphi(p^m)$. Thus by [8, Lemma 7.6] and Lemma 32 we have the lower bound

$$[K(\mathfrak{h}(P)) : K(\mathfrak{h}(p^{a-m}P))] = p^{2(a-m)} \leq [\mathbb{Q}(\mathfrak{h}(P)) : \mathbb{Q}(\mathfrak{h}(p^{a-m}P))].$$

Since $p^{2(a-m)} = \deg(X_1(p^a) \to X_1(p^m))$, we also have the upper bound

$$[\mathbb{Q}(\mathfrak{h}(P)) : \mathbb{Q}(\mathfrak{h}(p^{a-m}P))] \leq p^{2(a-m)}$$

Thus equality holds, and $\deg(x) = \deg(f(x)) \cdot \deg(f)$.

So suppose the $C_{p^m}(\mathcal{O})$-orbit of $p^{a-m}P$ has size less than or equal to $\varphi(p^m)$.[5] Suppose for the sake of contradiction that the size of the $C_{p^a}(\mathcal{O})$-orbit on $P$ is strictly smaller than $p^{2(a-m)}$ times the size of the $C_{p^m}(\mathcal{O})$-orbit on $p^{a-m}P$. Then the $C_{p^a}(\mathcal{O})$-orbit on $P$ has size less than

$$p^{2(a-m)} \cdot \varphi(p^m) = p^{2a-m-1}(p-1).$$

[4] For the explicit values of $m$, see Propositions 6.4 and 6.8 in [9]. These can mostly be deduced from [37].

[5] In fact, this implies the orbit size must be exactly $\varphi(p^m)$ since $C_{p^m}(\mathcal{O})$ contains all scalar matrices.

With the values of $m$ given in [9, Proposition 6.4], we find this contradicts [8, Theorem 7.2] since we have also assumed $\left(\frac{\Delta_K}{p}\right) \neq 1$. Thus the $C_{p^a}(\mathcal{O})$-orbit on $P$ is equal to $p^{2(a-m)}$ times the size of the $C_{p^m}(\mathcal{O})$-orbit on $p^{a-m}P$, and the argument follows as before. □

*Remark* 34. The statement of Proposition 33 does not hold if $\left(\frac{\Delta_K}{p}\right) = 1$. In this case, for such a $K$-CM elliptic curve $E$, there exists $y' \in X_1(p^M)(K(j(E))$ with $j(y) = j(E)$ for all $M \in \mathbb{Z}^+$. See Proposition 6.4 in [9]. These extra isogenies picked up over $K(j(E))$ prevent the degree condition of Proposition 33 from being satisfied, and they may be used to produce sporadic points associated to any CM $j$-invariant. See Theorem 7.1 in [11].

5.3. **Isolated CM points of odd degree.** There are 13 CM $j$-invariants in $\mathbb{Q}$ corresponding to imaginary quadratic orders of discriminant

$$\Delta \in \{-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\}.$$

For most of these, we can show there is no corresponding isolated point in odd degree using the following theorem.

**Theorem 35.** *Let $x \in X_1(N)$ be an isolated point of odd degree corresponding to an elliptic curve $E$ with CM by the order in $K$ of discriminant $\Delta$. Then $K = \mathbb{Q}(\sqrt{-p})$ for a prime $p \equiv 3 \pmod 4$ and $N = p^r$ or $2p^r$. Moreover, if $m$ is the maximum integer such that there exists $y \in X_0(p^m)(\mathbb{Q}(j(E))$ with $j(y) = j(E)$, then:*

- *(i) If $\left(\frac{\Delta}{2}\right) = -1$, then $f(x) \in X_1(\gcd(N, p^m))$ is isolated where $f : X_1(N) \to X_1(\gcd(N, p^m))$ is the natural map.*
- *(ii) If $\left(\frac{\Delta}{2}\right) \neq -1$, then $f(x) \in X_1(\gcd(N, 2p^m))$ is isolated where $f : X_1(N) \to X_1(\gcd(N, 2p^m))$ is the natural map.*

*Remark* 36. As noted above, for explicit values of $m$, see Propositions 6.4 and 6.8 in [9]; also [37].

*Proof.* Let $x = [E, P] \in X_1(N)$ be an isolated point of odd degree associated to an elliptic curve with CM by the order in $K$ of discriminant $\Delta$. Note there are no isolated points on $X_1(2)$ or $X_1(4)$ as they have genus 0. Thus by [1, Cor. 9.4], the assumption of odd degree implies $N = p^r$ or $2p^r$ where $K = \mathbb{Q}(\sqrt{-p})$ and $p \equiv 3 \pmod 4$ is prime. If $N = p^r$, we may assume $m < r$, for otherwise the statement is clearly true. Since $\left(\frac{\Delta_K}{p}\right) = 0$, we have $m \geq 1$ (see for example [9, Prop. 6.4]), so we may apply Proposition 33. Then by Theorem 15, $x$ maps to an isolated point on $X_1(p^m)$, and the statement holds.

Next, suppose $N = 2p^r$. Note we may assume $r \geq 1$, and if $p = 3$, we may assume $r > 1$ since $X_1(6)$ has genus 0. If $\left(\frac{\Delta}{2}\right) = -1$, then by [8, Lemma 7.1, Proposition 7.7], the size of the $C_N(\mathcal{O})$-orbit of $P$ is equal to 3 times the size of the $C_{p^r}(\mathcal{O})$-orbit of $2P$. Lemma 7.6 of [8] shows that

$$[K(j(E))(\mathfrak{h}(P)) : K(j(E))] = 3 \cdot [K(j(E))(\mathfrak{h}(2P)) : K(j(E))].$$

Since we have assumed $[\mathbb{Q}(j(E))(\mathfrak{h}(P)) : \mathbb{Q}]$ has odd degree, it follows that

$$\deg(x) = \deg(g) \cdot \deg(g(x))$$

where $g : X_1(2p^r) \to X_1(p^r)$ is the natural map. By Theorem 15, $g(x) \in X_1(p^r)$ is isolated. If $m \geq r$, we are done. Otherwise the argument follows as before.

If $\left(\frac{\Delta}{2}\right) \neq -1$, we may assume $m < r$. Then [9, Theorem 6.2, 6.6] shows there is a point in $X_1(2)(\mathbb{Q}(j(E))$ corresponding to $E$, and the assumption that $x$ has odd degree forces $[E, p^r P] \in X_1(2)$ to have degree $[\mathbb{Q}(j(E) : \mathbb{Q}]$. Thus by Proposition 33, we have $\deg(x) = \deg(g(x)) \cdot \deg(g)$ where $g : X_1(2p^r) \to X_1(2p^m)$ is the natural map. By Theorem 15, $g(x) \in X_1(2p^m)$ is isolated, as desired. □

| $\Delta$ | $p$ | $m$ | genus of $X_1(p^m)$ | $d_\Delta$ | genus of $X_1(2p^m)$ if $\left(\frac{\Delta}{2}\right) \neq -1$ |
|---|---|---|---|---|---|
| -3 | 3 | 2 | 0 | 3 | – |
| -7 | 7 | 1 | 0 | 3 | 1 |
| -11 | 11 | 1 | 1 | 5 | – |
| -12 | 3 | 1 | 0 | 1 | 0 |
| -19 | 19 | 1 | 7 | 9 | – |
| -27 | 3 | 3 | 13 | 9 | – |
| -28 | 7 | 1 | 0 | 3 | 1 |
| -43 | 43 | 1 | 57 | 21 | – |
| -67 | 67 | 1 | 155 | 33 | – |
| -163 | 163 | 1 | 1027 | 81 | – |

TABLE 1. Let $m$ be as in Theorem 35 and let $d_\Delta$ be the least degree of a $\Delta$-CM point on $X_1(p^m)$. For values of $m$, see [37] and [9, Proposition 6.4]. The value $d_\Delta$ is given in [9, Theorem 7.1].

**Corollary 37.** *There are no isolated points $x \in X_1(N)$ of odd degree corresponding to an elliptic curve with CM by the order of discriminant $\Delta \in \{-3, -4, -7, -8, -11, -12, -16, -19, -27, -28\}$.*

*Proof.* Let $x \in X_1(N)$ be an isolated point of odd degree corresponding to an elliptic curve with CM by the order of discriminant $\Delta \in \{-3, -4, -7, -8, -11, -12, -16, -19, -28\}$. Since $X_1(2)$ and $X_1(3)$ have genus 0, we may assume $N > 3$. By Theorem 35, we may assume $\Delta \notin \{-4, -8, -16\}$, and $x$ maps to an isolated point $f(x)$ in $X_1(\gcd(N, p^m))$ if $\left(\frac{\Delta}{2}\right) = -1$ or in $X_1(\gcd(N, 2p^m))$ if $\left(\frac{\Delta}{2}\right) \neq -1$ for $m, p$ as in the theorem statement. By Table 1, we see that the degree of $f(x)$ is larger than the genus of the curve, which means the dimension of the associated Riemann-Roch space is at least 2. Thus $f(x)$ is not $\mathbb{P}^1$-isolated and we have reached a contradiction.

Now, let $x \in X_1(N)$ be an isolated point of odd degree corresponding to an elliptic curve with CM by the order of discriminant $\Delta = -27$. Then $j(x) = -2^{15} \cdot 3 \cdot 5^3$, and by Theorem 35 and Table 1, $f(x) \in X_1(\gcd(N, 3^3))$ is isolated where $f : X_1(N) \to X_1(\gcd(N, 3^3))$ is the natural map. $X_1(3)$ and $X_1(9)$ are genus 0 and thus have no isolated points, so it suffices to show there are no isolated points of odd degree on $X_1(27)$ associated to this $j$-invariant. By computing division polynomials, we see that any point $x' \in X_1(27)$ of odd degree with $j(x') = -2^{15} \cdot 3 \cdot 5^3$ has degree 9 or 243. Since $X_1(27)$ has genus 13, Lemma 14 implies that points of degree 243 are not isolated, so we need only consider the point on $X_1(27)$ of degree 9.

Since the Jacobian of $X_1(27)$ has rank 0 [23, Lemma 1], it suffices to show $x'$ is not $\mathbb{P}^1$-isolated. We do this by forming the associated divisor and computing its Riemann-Roch space. First we find the Tate normal form of an elliptic curve $E(b, c)$ with $(0, 0)$ of order 27. This is done by constructing a polynomial $f_{27} \in \mathbb{Q}[b, c]$ that vanishes when $(0, 0)$ has order 27 on $E(b, c)$, as in [14, Lemma 2.4]. Using $E(b, c)$, we find the associated point on a model of $X_1(27)$ computed by Sutherland [57]. This allows us to create a degree 9 divisor $D$ over $\mathbb{Q}$ on $X_1(27)$, and a Magma computation shows that the Riemann-Roch space $L(D)$ over $\mathbb{Q}$ has dimension 3. Hence there is a function $f : X_1(27) \to \mathbb{P}^1$ of degree 9 with poles at the points in the support of $D$ and this implies that $D$ is not $\mathbb{P}^1$-isolated. See the file `X127.txt` for details. □

*Remark* 38. Suppose $x \in X_1(N)$ is an isolated point of odd degree corresponding to an elliptic curve with CM by the order of discriminant $\Delta \in \{-43, -67, -163\}$. These discriminants correspond to elliptic curves with $j$-invariants $-2^{18}3^35^3$, $-2^{15}3^35^311^3$, and $-2^{18}3^35^323^329^3$, respectively. By Theorem 35, $N = p^r$ or $2p^r$ where $p = 43, 67$, or 163, respectively. Moreover, since $m = 1$ in each case [37], Theorem 35 shows $f(x) \in X_1(\gcd(N, p))$ is isolated, where $f : X_1(N) \to X_1(\gcd(N, p))$

is the natural map. Thus $-2^{18}3^35^3$, $-2^{15}3^35^311^3$, and $-2^{18}3^35^323^329^3$ are in $j(\mathcal{I}_{odd}) \cap \mathbb{Q}$ if and only if they correspond to an isolated point of odd degree on $X_1(p)$. In each case, the Jacobian of $X_1(p)$ has positive rank; see Proposition 6.2.1 in [17]. Thus to find $j(\mathcal{I}_{odd}) \cap \mathbb{Q}$, one must determine whether these points belong to an infinite family parametrized by a positive rank abelian subvariety of $\mathrm{Jac}(X_1(p))$.

## Appendix A. 3-adic images of Galois

In [49, Corollary 1.10], the authors determine the 3-adic image of Galois for every non-CM elliptic curve $E/\mathbb{Q}$ that has a rational 3-isogeny. Every case that occurs arises from a genus 0 modular curve with infinitely many rational points. The prime power level modular curves with infinitely many rational points for subgroups that contain $-I$ were determined by Sutherland and Zywina [59]. The following table contains information from page 2 of the online supplement to [59] that specifies a label, the index, the level, generators, and a map to a covering modular curve. We also give the labels of the corresponding groups given in [49], which have the form $N.i.g.n$, where $N$ is the level, $i$ is the index, $g$ is the genus of the corresponding modular curve and $n$ is a tiebreak. (For more detail see Subsection 2.6 of [49].)

The labels $3B^0$-$3a$, $3D^0$-$3a$, $9B^0$-$9a$, and $9I^0$-$9c$ denote the curves $X_0(3), X_0(3,3), X_0(9)$, and $X_1(9)$, respectively. For each 3-adic image with level $3^k$, we also give the degrees on $X_1(3^k)$ of each Galois orbit of points order $3^k$.

| SZ label | RSZB label | covering | covering group | Orbit sizes |
|---|---|---|---|---|
| $3B^0$-$3a$ | 3.4.0.1 | $(t+3)^3(t+27)/t$ | $j$-line | $[1,3]$ |
| $3D^0$-$3a$ | 3.12.0.1 | $729/(t^3-27)$ | $3B^0$-$3a$ | $[1,1,2]$ |
| $9B^0$-$9a$ | 9.12.0.1 | $t(t^2+9t+27)$ | $3B^0$-$3a$ | $[3,6,27]$ |
| $9C^0$-$9a$ | 9.12.0.2 | $t^3$ | $3B^0$-$3a$ | $[9,27]$ |
| $9H^0$-$9a$ | 9.36.0.2 | $3(t^3+9)/t^3$ | $3D^0$-$3a$ | $[9,9,18]$ |
| $9H^0$-$9b$ | 9.36.0.1 | $3(t^3+9t^2-9t-9)/(t^3-9t^2-9t+9)$ | $3D^0$-$3a$ | $[3,3,3,6,18]$ |
| $9H^0$-$9c$ | 9.36.0.3 | $-6(t^3-9t)/(t^3+9t^2-9t-9)$ | $3D^0$-$3a$ | $[9,9,18]$ |
| $9I^0$-$9a$ | 9.36.0.5 | $-6(t^3-9t)/(t^3-3t^2-9t+3)$ | $9B^0$-$9a$ | $[3,6,9,9,9]$ |
| $9I^0$-$9b$ | 9.36.0.6 | $-3(t^3+9t^2-9t-9)/(t^3+3t^2-9t-3)$ | $9B^0$-$9a$ | $[3,6,27]$ |
| $9I^0$-$9c$ | 9.36.0.4 | $(t^3-6t^2+3t+1)/(t^2-t)$ | $9B^0$-$9a$ | $[1,1,1,6,27]$ |
| $9J^0$-$9a$ | 9.36.0.7 | $(t^3-3t+1)/(t^2-t)$ | $9C^0$-$9a$ | $[3,3,3,27]$ |
| $9J^0$-$9b$ | 9.36.0.9 | $-18(t^2-1)/(t^3-3t^2-9t+3)$ | $9C^0$-$9a$ | $[9,9,9,9]$ |
| $9J^0$-$9c$ | 9.36.0.8 | $3(t^3+3t^2-9t-3)/(t^3-3t^2-9t+3)$ | $9C^0$-$9a$ | $[9,27]$ |
| $27A^0$-$27a$ | 27.36.0.1 | $t^3$ | $9B^0$-$9a$ | $[27,54,243]$ |

## References


1. Noboru Aoki, *Torsion points on abelian varieties with complex multiplication*, Algebraic cycles and related topics (Kitasakado, 1994), World Sci. Publ., River Edge, NJ, 1995, pp. 1–22.
2. Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*, Ann. of Math. (2) **189** (2019), no. 3, 885–944. MR 3961086
3. Burcu Baran, *An exceptional isomorphism between modular curves of level 13*, J. Number Theory **145** (2014), 273–300. MR 3253304
4. Yuri Bilu and Pierre Parent, *Serre's uniformity problem in the split Cartan case*, Ann. of Math. (2) **173** (2011), no. 1, 569–584. MR 2753610
5. Yuri Bilu, Pierre Parent, and Marusia Rebolledo, *Rational points on $X_0^+(p^r)$*, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 3, 957–984. MR 3137477
6. Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR 1045822

7. Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, vol. 24, 1997, Computational algebra and number theory (London, 1993), pp. 235–265. MR 1484478
8. Abbey Bourdon and Pete L. Clark, *Torsion points and Galois representations on CM elliptic curves*, Pacific J. Math. **305** (2020), no. 1, 43–88. MR 4077686
9. ———, *Torsion points and isogenies on CM elliptic curves*, J. Lond. Math. Soc. (2) **102** (2020), no. 2, 580–622. MR 4171427
10. Abbey Bourdon, Pete L. Clark, and James Stankewicz, *Torsion points on CM elliptic curves over real number fields*, Trans. Amer. Math. Soc. **369** (2017), no. 12, 8457–8496.
11. Abbey Bourdon, Özlem Ejder, Yuan Liu, Frances Odumodu, and Bianca Viray, *On the level of modular curves that give rise to isolated $j$-invariants*, Adv. Math. **357** (2019), 106824, 33. MR 4016915
12. Abbey Bourdon and Filip Najman, *Sporadic points of odd degree on $X_1(N)$ from $\mathbb{Q}$-curves*, preprint, available at arXiv:2107.10909.
13. Anna Cadoret and Akio Tamagawa, *A uniform open image theorem for $\ell$-adic representations, II*, Duke Math. J. **162** (2013), no. 12, 2301–2344. MR 3102481
14. Pete L. Clark, Patrick Corn, Alex Rice, and James Stankewicz, *Computation on elliptic curves with complex multiplication*, LMS J. Comput. Math. **17** (2014), no. 1, 509–535. MR 3356044
15. Pete L. Clark, Tyler Genao, Paul Pollack, and Frederick Saia, *The least degree of a CM point on a modular curve*, J. Lond. Math. Soc. (2) **105** (2022), no. 2, 825–883. MR 4400938
16. Pete L. Clark and Paul Pollack, *Pursuing polynomial bounds on torsion*, Israel J. Math. **227** (2018), no. 2, 889–909. MR 3846346
17. Brian Conrad, Bas Edixhoven, and William Stein, *$J_1(p)$ has connected fibers*, Doc. Math. **8** (2003), 331–408. MR 2029169
18. David A. Cox, *Primes of the form $x^2 + ny^2$*, A Wiley-Interscience Publication, John Wiley & Sons Inc., New York, 1989, Fermat, class field theory and complex multiplication.
19. Harris B. Daniels and Enrique González-Jiménez, *On the torsion of rational elliptic curves over sextic fields*, Math. Comp. **89** (2020), no. 321, 411–435. MR 4011550
20. ———, *Serre's constant of elliptic curves over the rationals*, Exp. Math. **31** (2022), no. 2, 518–536. MR 4458130
21. Pierre Deligne and Michael Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 1973, pp. 143–316. Lecture Notes in Math., Vol. 349. MR 0337993
22. Maarten Derickx, Anastassia Etropolski, Mark van Hoeij, Jackson S. Morrow, and David Zureick-Brown, *Sporadic cubic torsion*, Algebra Number Theory **15** (2021), no. 7, 1837–1864. MR 4333666
23. Maarten Derickx and Mark van Hoeij, *Gonality of the modular curve $X_1(N)$*, J. Algebra **417** (2014), 52–71. MR 3244637
24. Fred Diamond and John Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), CMS Conf. Proc., vol. 17, Amer. Math. Soc., Providence, RI, 1995, pp. 39–133. MR 1357209
25. Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005.
26. Sutherland Drew, *Torsion subgroups of elliptic curves over number fields*, `https://math.mit.edu/~drew/MazursTheoremSubsequentResults.pdf`.
27. Gerd Faltings, *The general case of S. Lang's conjecture*, Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), Perspect. Math., vol. 15, Academic Press, San Diego, CA, 1994, pp. 175–182.
28. Gerhard Frey, *Curves with infinitely many points of fixed degree*, Israel J. Math. **85** (1994), no. 1-3, 79–83.
29. Enrique González-Jiménez and Filip Najman, *An algorithm for determining torsion growth of elliptic curves*, available at `https://arxiv.org/abs/1904.07071`.
30. ———, *Growth of torsion groups of elliptic curves upon base change*, Math. Comp. **89** (2020), no. 323, 1457–1485. MR 4063324
31. Ralph Greenberg, *The image of Galois representations attached to elliptic curves with an isogeny*, Amer. J. Math. **134** (2012), no. 5, 1167–1196.
32. Ralph Greenberg, Karl Rubin, Alice Silverberg, and Michael Stoll, *On elliptic curves with an isogeny of degree 7*, Amer. J. Math. **136** (2014), no. 1, 77–109.
33. Tomislav Gužvić, *Torsion of elliptic curves with rational $j$-invariant defined over number fields of prime degree*, Proc. Amer. Math. Soc. **149** (2021), no. 8, 3261–3275. MR 4273133
34. Daeyeol Jeon and Chang Heon Kim, *On the arithmetic of certain modular curves*, Acta Arith. **130** (2007), no. 2, 181–193. MR 2357655
35. Daeyeol Jeon, Chang Heon Kim, and Andreas Schweizer, *Bielliptic intermediate modular curves*, J. Pure Appl. Algebra **224** (2020), no. 1, 272–299. MR 3986422

36. Monsur A. Kenku, *On the number of* $\mathbf{Q}$*-isomorphism classes of elliptic curves in each* $\mathbf{Q}$*-isogeny class*, J. Number Theory **15** (1982), no. 2, 199–202. MR 675184
37. Soonhak Kwon, *Degree of isogenies of elliptic curves with complex multiplication*, J. Korean Math. Soc. **36** (1999), no. 5, 945–958.
38. 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 $GL_2$-extensions of the rational numbers. MR 0568299
39. Pedro Lemos, *Serre's uniformity conjecture for elliptic curves with rational cyclic isogenies*, Trans. Amer. Math. Soc. **371** (2019), no. 1, 137–146. MR 3885140
40. ———, *Some cases of Serre's uniformity problem*, Math. Z. **292** (2019), no. 1-2, 739–762. MR 3968924
41. Beppo Levi, *Saggio per una teoria aritmetica delle forme cubiche ternarie*, Atti della Reale Acc. Sci. di Torino **43** (1908), 99–120, 413–434, 672–681.
42. Gérard Ligozat, *Courbes modulaires de genre* 1, Supplément au Bull. Soc. Math. France, Tome 103, no. 3, Société Mathématique de France, Paris, 1975, Bull. Soc. Math. France, Mém. 43. MR 0417060
43. 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. MR 3084348
44. Álvaro Lozano-Robledo, *Galois representations attached to elliptic curves with complex multiplication*, Algebra Number Theory **16** (2022), no. 4, 777–837. MR 4467123
45. Barry Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978), With an appendix by Mazur and M. Rapoport. MR 488287
46. ———, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162. MR 482230
47. 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.
48. James L. Parish, *Rational torsion in complex-multiplication elliptic curves*, J. Number Theory **33** (1989), no. 2, 257–265.
49. Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown, *$\ell$-adic images of Galois for elliptic curves over $\mathbb{Q}$ (and an appendix with John Voight)*, Forum Math. Sigma **10** (2022), Paper No. e62, 63, With an appendix with John Voight. MR 4468989
50. 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.
51. Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.
52. ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 54, 323–401. MR 644559
53. ———, *Lectures on the Mordell-Weil theorem*, third 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. MR 1757192
54. Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971, Kanô Memorial Lectures, No. 1.
55. Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.
56. Hanson Smith, *Ramification in division fields and sporadic points on modular curves*, Res. Number Theory **9** (2023), no. 1, Paper No. 17. MR 4546874
57. Andrew V. Sutherland, *Constructing elliptic curves over finite fields with prescribed torsion*, Math. Comp. **81** (2012), no. 278, 1131–1147. MR 2869053
58. ———, *Computing images of Galois representations attached to elliptic curves*, Forum Math. Sigma **4** (2016), e4, 79.
59. 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. MR 3671434
60. Mark van Hoeij, *Low degree places on the modular curve* $X_1(N)$, preprint, available at arXiv:1202.4355.
61. Mark van Hoeij and Andrew Novocin, *A reduction algorithm for algebraic function fields*, `https://math.fsu.edu/~hoeij/papers/HoeijNovocin.pdf`.
62. David Zywina, *On the possible image of the mod $\ell$ representations associated to elliptic curves over $\mathbb{Q}$*, `https://arxiv.org/abs/1508.07660`.

Wake Forest University, Department of Mathematics and Statistics, Winston-Salem, NC 27109, USA

*Email address*: bourdoam@wfu.edu
*URL*: http://users.wfu.edu/bourdoam/

*Email address*: davidgill139@gmail.com

*Email address*: rouseja@wfu.edu
*URL*: http://users.wfu.edu/rouseja/

*Email address*: watsonl@wfu.edu
*URL*: https://loridwatson.com