# MINIMAL TORSION CURVES IN GEOMETRIC ISOGENY CLASSES

ABBEY BOURDON, NINA RYALLS, AND LORI D. WATSON

ABSTRACT. Let $E/\mathbb{Q}$ be a non-CM elliptic curve and let $\mathcal{E}$ denote the collection of all elliptic curves geometrically isogenous to $E$. In this paper, we introduce the problem of studying minimal torsion curves in $\mathcal{E}$, which are elliptic curves $E' \in \mathcal{E}$ attaining a point of prime-power order in least possible degree. If $\ell$ is an odd prime and $k$ is an integer larger than 3, we show there exists $E_0/\mathbb{Q} \in \mathcal{E}$ and a cyclic subgroup $C$ in $E_0$ of order $\ell$ such that $E_0/C$ produces a point on $X_1(\ell^k)$ in least odd degree among all odd degree points associated to curves in $\mathcal{E}$. It is somewhat surprising that such a uniform construction exists given the various groups that can arise as the image of the $\ell$-adic Galois representation associated to $E$. Our work concludes with a study of minimal torsion curves within the geometric isogeny class of an elliptic curve with complex multiplication.

## 1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve. In 1922, Mordell [30] proved that the collection of points on $E$ with coordinates in $\mathbb{Q}$ forms a finitely generated abelian group. In particular, the torsion subgroup of $E(\mathbb{Q})$ is a finite abelian group, and the groups which occur as $E(\mathbb{Q})_{\text{tors}}$ are know due to work of Mazur [29] in 1977. The past decade has seen a renewed interest in studying torsion points of rational elliptic curves, from characterizing the groups which arise as torsion subgroups of $E/\mathbb{Q}$ under base extension to number fields of higher degree (see, for example, [28, 31, 20, 22, 13]) to classifying images of $\ell$-adic Galois representations associated to $E/\mathbb{Q}$; see [32, 26, 38, 27]. This prior work can be leveraged to begin to understand a new class of elliptic curves, namely, those geometrically isogenous to an elliptic curve $E/\mathbb{Q}$.

Let $E/\mathbb{Q}$ be an elliptic curve, and let $\mathcal{E}$ denote the collection of all elliptic curves geometrically isogenous to $E$. That is, for any $E' \in \mathcal{E}$, there exists an isogeny $\varphi : E \to E'$ defined over $\overline{\mathbb{Q}}$. This class of elliptic curves has been studied in several prior works [12, 9, 19]. In this paper, our central questions are the following:

(1) What is the least degree of a point on $X_1(\ell^k)$ associated to an elliptic curve in $\mathcal{E}$?
(2) What elliptic curve(s) in $\mathcal{E}$ attain this point on $X_1(\ell^k)$ of least possible degree?

To answer these questions it is necessary to determine whether a point of least-possible degree on $X_1(\ell^k)$ can correspond to an elliptic curve $E' \in \mathcal{E}$ with $j(E') \in \mathbb{Q}$, or whether it is necessary to work with an elliptic curve with $j$-invariant defining an extension of larger degree, but with exceptional arithmetic (such as low-degree prime-power isogenies) which allow it to produce a point on $X_1(\ell^k)$ in *lower* degree than any elliptic curve in $\mathcal{E}$ with rational $j$-invariant. In fact both cases can arise; see Remark 1.4.

One motivation for studying torsion points on elliptic curves in geometric isogeny classes is a connection to Serre's Uniformity Conjecture, which states that there is a constant $C$ such that the mod $\ell$ Galois representation associated to any elliptic curve over $\mathbb{Q}$ without complex multiplication (CM) is surjective for primes $\ell > C$. This originally appeared as a question in a 1972 paper of Serre [33], but it has since been formally conjectured by both Sutherland [37] and Zywina [39]. Recent work of the first author and Najman [9] identifies a connection between this conjecture and sporadic points on modular curves associated to elliptic curves in the geometric isogeny class of an elliptic curve with rational $j$-invariant. We say a point $x \in X_1(\ell^k)$ is **sporadic** if there are only finitely many points of degree at most $\deg(x)$.

**Theorem 1.1** (Bourdon, Najman [9]). *Suppose there exist only finitely many isogeny classes $\mathcal{E}$ containing a non-CM elliptic curve $E/\mathbb{Q}$ that give rise to a sporadic point on $X_1(\ell^2)$ for some prime $\ell$. Then Serre's Uniformity Conjecture holds.*

**Remark 1.2.** Though the statement of [9, Theorem 1.2] concerns isogeny classes of non-CM $\mathbb{Q}$-curves, the proof shows it is enough to have finiteness of isogeny classes which contain a non-CM elliptic curve $E/\mathbb{Q}$. Indeed, we find that for an elliptic curve $E/\mathbb{Q}$ whose mod $\ell$ Galois representation lands in the normalizer of a non-split Cartan subgroup, there is an elliptic curve $E' \in \mathcal{E}$ producing a point on $X_1(\ell^2)$ of degree at most $2\ell(\ell^2-1)$; this point is sporadic for primes sufficiently large by work of Abramovich [1, Theorem 0.1] and Frey [18, Proposition 2]. It is worth pointing out that $E$ itself does not correspond to a sporadic point on $X_1(\ell^2)$, as proved by Ejder [17].

We say an elliptic curve $E' \in \mathcal{E}$ is **minimal for** $X_1(\ell^k)$ if it attains a point on $X_1(\ell^k)$ in least possible degree among all elliptic curves in $\mathcal{E}$. If $E'$ is minimal for $X_1(\ell^k)$ for all $k \in \mathbb{Z}^+$, we say $E'$ is a **minimal torsion curve for the prime** $\ell$, denoted $E_{\min}$. Given an isogeny class and fixed prime $\ell$, there can exist infinitely many elliptic curves which are minimal for some $X_1(\ell^k)$. For example, if the $\ell$-adic Galois representation of a non-CM elliptic curve $E/\mathbb{Q}$ is surjective, then for any cyclic subgroup $C$ of order a power of $\ell$ the elliptic curve $E/C$ is minimal for $X_1(\ell^k)$ for $k$ sufficiently large; see Remark 3.5. However, there can exist at most finitely many minimal torsion curves for $\ell$ since any such curve must in particular be minimal for $X_1(\ell)$, and hence have $j$-invariant in an extension of bounded degree; see Proposition 3.3. Our first result shows that if we consider only points on $X_1(\ell^k)$ of odd degree, where $\ell$ is an odd prime, then minimal torsion curves exist within non-CM isogeny classes unless $\ell = 3$ and $\mathcal{E}$ is one of 4 exceptional classes. Moreover, in each case, there exists a uniform construction for $E' \in \mathcal{E}$ which yields this point of minimal odd degree.

**Theorem 1.3.** *Let $E/\mathbb{Q}$ be a non-CM elliptic curve and let $\mathcal{E}$ denote the corresponding geometric isogeny class. Suppose $\ell$ is an odd prime number and $k \geq 4$ is an integer. There exists $E_1/\mathbb{Q} \in \mathcal{E}$ and a cyclic subgroup $C \leq E_1$ of order $\ell$ such that $E_1/C$ gives a point of least possible odd degree on $X_1(\ell^k)$ among all odd degree points associated to $\mathcal{E}$. We may include the values $1 \leq k \leq 3$ unless $\ell = 3$ and $\mathcal{E}$ contains an elliptic curve over $\mathbb{Q}$ with 3-adic image 9.12.0.2, 9.36.0.2, 9.36.0.7, or 9.36.0.8.*

**Remark 1.4.** Note that $j(E_1/C)$ need not be in $\mathbb{Q}$, and for certain cases, the point of least odd degree associated to $\mathcal{E}$ *cannot* be constructed from an elliptic curve having rational $j$-invariant. In particular, the proof of Theorem 1.3 shows that in order to produce points on $X_1(\ell^k)$ of least odd degree among points associated to $\mathcal{E}$, one cannot use an elliptic curve with $j$-invariant in $\mathbb{Q}$ if $\ell = 7$ and $j(E) = 3^3 \cdot 5 \cdot 7^5/2^7$ or if $\ell = 3$ and $\mathcal{E}$ contains an elliptic curve over $\mathbb{Q}$ with 3-adic image 9.12.0.2, 9.36.0.2, 9.36.0.7, or 9.36.0.8. We may choose $E_1$ and $C$ such that $j(E_1/C) \in \mathbb{Q}$ in all other cases.

In order to prove Theorem 1.3, we analyze each geometric isogeny class and determine the least possible odd degree in which an elliptic curve $E \in \mathcal{E}$ can give a point on $X_1(\ell^k)$. We obtain divisibility conditions which are best-possible for $k$ sufficiently large: see Proposition 4.1 and Proposition 5.1. By comparing across all possible isogeny classes and ruling out certain points of order a power of 2, we attain the following result, which strengthens Proposition 4.1 in [9].

**Theorem 1.5.** *Let $E/\mathbb{Q}$ be a non-CM elliptic curve and let $\mathcal{E}$ denote the corresponding geometric isogeny class. If $E' \in \mathcal{E}$ and $x = [E', P'] \in X_1(\ell^k)$ is a point of odd degree, then $\ell \in \{2, 3, 5, 7, 11, 13\}$ and the following divisibility conditions hold and are best possible without placing restrictions on $\mathcal{E}$:*

*(1) If $\ell = 13$, then $3 \cdot 13^{2k-2} \mid \deg(x)$.*
*(2) If $\ell = 11$, then $5 \cdot 11^{2k-2} \mid \deg(x)$.*
*(3) If $\ell = 7$ and $j(E) \neq 3^3 \cdot 5 \cdot 7^5/2^7$, then $7^{2k-2} \mid \deg(x)$.*

*(4) If $\ell = 7$ and $j(E) = 3^3 \cdot 5 \cdot 7^5/2^7$, then $9 \cdot 7^{\max(0,2k-3)} \mid \deg(x)$.*
*(5) If $\ell = 5$, then $5^{\max(0,2k-3)} \mid \deg(x)$.*
*(6) If $\ell = 3$, then $3^{\max(0,2k-4)} \mid \deg(x)$.*
*(7) If $\ell = 2$, then $k \leq 3$ and $1 \mid \deg(x)$.*

Our investigation begins with a more general divisibility condition for degrees of torsion points on elliptic curves within a fixed geometric isogeny classes, which plays a key role in the proofs of Theorem 1.3 and Theorem 1.5, and strengthens Lemma 4.6 in [9]. Here, $\rho_{E,\ell^\infty}$ denotes the $\ell$-adic Galois representation associated to $E$.

**Proposition 1.6.** *Let $E/\mathbb{Q}$ be a non-CM elliptic curve, and let $\mathcal{E}$ denote the corresponding geometric isogeny class. Suppose $\ell$ is a prime number, and set $d \coloneqq \operatorname{ord}_\ell([\mathrm{GL}_2(\mathbb{Z}_\ell) : \operatorname{im}\rho_{E,\ell^\infty}])$. If $E' \in \mathcal{E}$, then the degree of any point on $X_1(\ell^k)$ associated to $E'$ is divisible by*

$$\begin{cases} \deg(x) \cdot \ell^{\max(0,2k-2-d)} & \text{if } \ell \text{ is odd,} \\ \deg(x) \cdot \ell^{\max(0,2k-3-d)} & \text{if } \ell = 2, \end{cases}$$

*for some $x \in X_1(\ell)$ associated to $E$ or $E/C$ where $C$ is the kernel of a $\mathbb{Q}$-rational cyclic $\ell$-isogeny. In particular, if $E$ has no $\ell$-isogeny over $\mathbb{Q}$, then the latter case cannot occur.*

Since $\deg(X_1(\ell^k) \to X_1(\ell)) = \ell^{2k-2}$ for $\ell$ odd and $\deg(X_1(2^k) \to X_1(2)) = 2^{2k-3}$, these lower bounds are best-possible whenever $\operatorname{ord}_\ell([\mathrm{GL}_2(\mathbb{Z}_\ell) : \operatorname{im}\rho_{E,\ell^\infty}]) = 0$, and in this case a minimal torsion curve with $j$-invariant in $\mathbb{Q}$ exists. This holds in many cases; see, for example, Lemma 4.2. We can also show the divisibility conditions of Proposition 1.6 are best-possible when the $\ell$-adic Galois representation of $E$ has level $\ell$, though the minimal torsion curve need not have $j$-invariant in $\mathbb{Q}$; see Proposition 7.1. However, there are certain isogeny classes for which there does not exist a point on $X_1(\ell^k)$ in least degree allowed by Proposition 1.6. For example, by Proposition 5.1, if $\ell = 3$ and there exists $E_1 \in \mathcal{E}$ with $\operatorname{im}\rho_{E_1,3^\infty} = 9.36.0.6$, then the degree of a point on $X_1(3^k)$ associated to an elliptic curve in $\mathcal{E}$ is divisible by $2 \cdot 3^{\max(0,2k-4)}$ or $3^{\max(0,2k-3)}$ provided $k \geq 2$. Since there exists $x \in X_1(3)$ of degree 1 associated to $E_1$, this strengthens the lower bound in Proposition 1.6 by a factor of 2 or 3, respectively. The isogeny class of $E_1$ also illustrates that, away from points odd degree, we cannot always produce points on $X_1(\ell^k)$ of least degree among those from a fixed isogeny class by taking the quotient of a rational elliptic curve by a cyclic subgroup of order $\ell$. See Remark 5.4 for details.

In the final section of our paper, we consider minimal torsion curves within CM isogeny classes, building on work of the first author and Pete Clark [5]. Whether or not a minimal torsion curve exists for a given prime $\ell$ depends on whether $\ell$ is split, inert, or ramified in the associated CM field.

**Theorem 1.7.** *Let $K$ be an imaginary quadratic field, and suppose $\ell$ is an odd prime. Let $E$ be an elliptic curve with CM by the full ring of integers in $K$, and let $\mathcal{E}$ denote the geometric isogeny class of $E$. Then a minimal torsion curve exists for $\mathcal{E}$ if and only if $\ell$ is split in $K$.*

As in the non-CM case, this theorem is a consequence of attaining sharp divisibility conditions for the degrees of points on $X_1(\ell^k)$ coming from elliptic curves in $\mathcal{E}$. See Propositions 8.1,8.2, and 8.4.


## Acknowledgements

We thank Álvaro Lozano-Robledo, Jeremy Rouse, and Parker Schwartz for helpful conversations. The first author was partially supported by an A. J. Sterge Faculty Fellowship. All authors were supported by NSF grant DMS-2137659.

## 2. Background

2.1. **Galois Representations.** Let $E$ be an elliptic curve defined over a number field $F$, and let $\ell$ be a prime number. The elements of the absolute Galois group of $F$, denoted $\mathrm{Gal}_F$, induce a natural automorphism of points of $E(\overline{F})$ with order dividing $\ell^k$, denoted $E[\ell^k]$. This action is recorded in the **mod $\ell^k$ Galois representation** associated to $E$, which can be made to have image in $\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ by choosing a basis for $E[\ell^k]$:

$$\rho_{E,\ell^k} \mathrm{Gal}_F \to \mathrm{Aut}(E[\ell^k]) \cong \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z}).$$

By choosing compatible bases, the mod $\ell^k$ Galois representations fit together to give the **$\ell$-adic Galois representation** associated to $E$,

$$\rho_{E,\ell^\infty} \mathrm{Gal}_F \to \mathrm{GL}_2(\mathbb{Z}_\ell),$$

which gives the Galois action on all points of order a power of $\ell$.

All known images of the mod $\ell$ Galois representations associated to a non-CM elliptic curve over $\mathbb{Q}$ are given in Tables 1 and 2 of [22]. This list is complete for $\ell \leq 13$ by [39, 37, 3, 2], and it has been conjectured to be complete for all $\ell$; see work of Sutherland [37, Conjecture 1.1] and Zywina [39, Conjecture 1.12]. Unconditionally, we have the following result, where $C_{ns}(\ell)$ denotes a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ with normalizer $C_{ns}^+(\ell)$.

**Proposition 2.1.** *Suppose $E/\mathbb{Q}$ is a non-CM elliptic curve and $\ell$ is prime. If $\mathrm{im}\,\rho_{E,\ell}$ is not equal to $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ or any group appearing in Table 1 and 2 of* [22]*, then $\ell \geq 17$ and:*

*(1) If $\ell \equiv 1 \pmod 3$, then $\mathrm{im}\,\rho_{E,\ell}$ is conjugate to $C_{ns}^+(\ell)$.*
*(2) If $\ell \equiv 2 \pmod 3$, then $\mathrm{im}\,\rho_{E,\ell}$ is conjugate to $C_{ns}^+(\ell)$ or to the subgroup*

$$\{a^3 : a \in C_{ns}(\ell)\} \cup \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \cdot a^3 : a \in C_{ns}(\ell)\}.$$

*Proof.* See [40, Proposition 1.13] and [22, Theorem 3.2]. □

The classification of 2-adic images associated to elliptic curves over $\mathbb{Q}$ is complete due to work of Rouse and Zureick-Brown [32], and there has been significant recent progress towards the classification of $\ell$-adic images for odd primes $\ell$; see [26, 38] for elliptic curves without complex multiplication and [27] for the CM case.

Throughout we use the current LMFDB notation to refer to subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z}_\ell)$, which matches that of [37] and [26].

2.2. **Elliptic Curves with an Isogeny.** Suppose $E/F$ is an elliptic curve with an $F$-rational cyclic $N$-isogeny. That is, there exists $P \in E$ of order $N$ such that for any $\sigma \in \mathrm{Gal}_F$, there is some $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$ for which $\sigma(P) = \alpha P$. This defines a homomorphism called the **isogeny character**:

$$\begin{aligned} \chi : \mathrm{Gal}_F &\to (\mathbb{Z}/N\mathbb{Z})^\times \\ \sigma &\mapsto \alpha. \end{aligned}$$

**Proposition 2.2.** *Let $N \geq 3$ be an integer, and let $E/F$ be an elliptic curve with an $F$-rational cyclic isogeny of degree $N$. There is an extension $L/F$ with $[L : F] \mid \frac{\varphi(N)}{2}$ and a quadratic twist $E'$ of $E/L$ such that $E'(L)$ has a point of order $N$.*

*Proof.* This follows from [6, Theorem 5.5]. □

2.3. **Modular Curves.** In this paper, we are interested in characterizing degrees of points on the modular curve $X_1(N)$, where $N$ is a positive integer. Recall $X_1(N)$ is an algebraic curve over $\mathbb{Q}$ whose non-cuspidal points correspond to isomorphism classes of elliptic curves with a distinguished point of order $N$. See [16, Section 7.7], [15], [34, §6.7], [35, Appendix C, §13], or [14] for more details. If $x \in X_1(N)$ is closed point, we define the **degree** of $x$ to be the degree of the residue field $\mathbb{Q}(x)$. For a non-cuspidal point $x$, we can construct $\mathbb{Q}(x)$ explicitly via the following result.

**Lemma 2.3.** *Let $E$ be an elliptic curve and let $P \in E$ be a point of order $N$. Then the residue field of the closed point $x = [E, P] \in X_1(N)$ is given by*

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

*where $\mathfrak{h} : E \to E/\operatorname{Aut}(E) \cong \mathbb{P}^1$ is a Weber function for $E$. There is Weierstrass equation for $E$ defined over $\mathbb{Q}(x)$ for which $P \in E(\mathbb{Q}(x))$, and $\mathbb{Q}(x)$ is contained in any number field over which both $E$ and $P$ are defined.*

*Proof.* See, for example, [9, Lemma 2.5], and [14, p. 274, Proposition VI.3.2]. □

If $E/\mathbb{Q}(j(E))$ corresponds to an equation of the form $y^2 = x^3 + Ax + B$ and $P = (x_0, y_0) \in E$, then we may take

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

Thus by Lemma 2.3 we can compute the degree of a point on $X_1(N)$ associated to a non-CM elliptic curve by factoring division polynomials. See [34, p. 107] for details.

Many of our results rely on first constructing an explicit point $x \in X_1(\ell^k)$ for some small integer $k$, and then obtaining information on the degree of lifts of $x$ using known results about the degree of maps between modular curves.

**Proposition 2.4.** *For positive integers $a$ and $b$, there is a $\mathbb{Q}$-rational map $f : X_1(ab) \to X_1(a)$ which sends $[E, P]$ 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 moduli interpretation ensures the map is defined over $\mathbb{Q}$, and the degree calculation follows from [16, p.66]. □

## 3. Preliminary Results

In this section, we begin by establishing a brief technical result concerning the field of definition of an isogeny (§3.1), which essential follows from prior work of Cremona and Najman [12, Corollary A.5] or Clark [10, Proposition 3.2]. This is used in the proof of Proposition 1.6 appearing in §3.2, and also to show in §3.3 that only finitely many minimal torsion curves exist within a fixed geometric isogeny class for a given prime $\ell$. In §3.4 we conclude with a lemma relating the image of certain Galois representations attached to elliptic curves connected by a rational cyclic isogeny.

3.1. **Fields of Definition of Isogenies.** Let $E_0/\mathbb{Q}$ be a non-CM elliptic curve and let $E \in \mathcal{E}$. By definition, there exists an isogeny $\varphi : E \to E_0$ defined over $\overline{\mathbb{Q}}$. Since we are only interested in characterizing degrees of closed points on $X_1(N)$, which can be computed using any model of $E$ by Lemma 2.3, we are free to replace $E$ and $E_0$ by quadratic twists in order to achieve a more convenient representation of $\varphi$. The lemma given below essentially follows from the fact that $\mathbb{Q}(j(E), j(E_0)) = \mathbb{Q}(j(E))$ is contained in the residue field of any closed point on $X_1(N)$ associated to $E$, and this is the field of moduli of the isogeny $\varphi$; see [10, §3.3] or [12, Corollary A.5].

**Lemma 3.1.** *Let $\mathcal{E}$ be the geometric isogeny class of a non-CM elliptic curve $E_0/\mathbb{Q}$ and let $E \in \mathcal{E}$. Suppose $x = [E, P] \in X_1(\ell^k)$ for some prime number $\ell$, and let $F \coloneqq \mathbb{Q}(x)$. There is a model of $E/F$ for which $P \in E(F)$ and such that there exists an $F$-rational cyclic isogeny $\varphi : E \to E'$ with $j(E') = j(E_0)$.*

*Proof.* Since $E \in \mathcal{E}$, by definition there exists an isogeny $\varphi : E \to E_0$ defined over $\overline{\mathbb{Q}}$ which we may assume is cyclic of degree $N$; see Lemma A.1 in [12]. Let $C$ denote its kernel. Note that $F = \mathbb{Q}(j(E), \mathfrak{h}(P))$ by Lemma 2.3 and there exists a Weierstrass equation of $E/F$ with $P \in E(F)$. The proof of [10, Proposition 3.2] shows $C$ is $F$-rational, as we will now show. Suppose $\sigma(C) \neq C$ for some $\sigma \in \mathrm{Gal}_F$, and consider the induced isogeny $E^\sigma \to (E/C)^\sigma$. Since $j(E/C) \in \mathbb{Q}$, we see that $j((E/C)^\sigma) = j(E_0)$. Thus composition with an isomorphism to $E_0$ yields a cyclic $N$-isogeny $\psi : E \to E_0$ with kernel $\sigma(C)$. But having two cyclic $N$-isogenies from $E$ to $E_0$ with distinct kernels can happen only if $E$ has complex multiplication (see the proof of [10, Proposition 3.2] for details). We have reached a contradiction. □

3.2. **Proof of Proposition 1.6.** In this section, we prove Proposition 1.6, which we restate as Proposition 3.2 below. This strengthens [9, Lemma 4.6].

**Proposition 3.2.** *Let $E_0/\mathbb{Q}$ be a non-CM elliptic curve, and let $\mathcal{E}$ denote the corresponding geometric isogeny class. Suppose $\ell$ is a prime number, and set $d \coloneqq \mathrm{ord}_\ell([\mathrm{GL}_2(\mathbb{Z}_\ell) : \operatorname{im} \rho_{E_0,\ell^\infty}])$. If $E \in \mathcal{E}$, then the degree of any point on $X_1(\ell^k)$ associated to $E$ is divisible by*

$$\begin{cases} \deg(x) \cdot \ell^{\max(0,2k-2-d)} & \text{if } \ell \text{ is odd,} \\ \deg(x) \cdot \ell^{\max(0,2k-3-d)} & \text{if } \ell = 2, \end{cases}$$

*for some $x \in X_1(\ell)$ associated to $E_0$ or $E_0/C$ where $C$ is the kernel of a $\mathbb{Q}$-rational cyclic $\ell$-isogeny. In particular, if $E_0$ has no $\ell$-isogeny over $\mathbb{Q}$, then the latter case cannot occur.*

*Proof.* Let $E \in \mathcal{E}$, and fix $P \in E$ of order $\ell^k$. Define $F \coloneqq \mathbb{Q}(j(E), \mathfrak{h}(P))$. By Lemma 3.1, there is a model of $E/F$ where $P \in E(F)$ and such that there exists an $F$-rational cyclic isogeny $\varphi : E \to E'$ with $j(E') = j(E_0)$. By [9, Lemma 4.6], we have $[F : \mathbb{Q}]$ is divisible by

$$\begin{cases} \ell^{\max(0,2k-2-d)} & \text{if } \ell \text{ is odd,} \\ \ell^{\max(0,2k-3-d)} & \text{if } \ell = 2. \end{cases}$$

By [9, Corollary 4.3], $E'$ has a point of order $\ell$ over an extension $F'/F$ of degree dividing $\ell$. In particular, there exists $x = [E', P'] \in X_1(\ell)$ such that $\mathbb{Q}(\mathfrak{h}(P')) \subseteq F'$. Hence

$$\deg(x) \mid \ell \cdot [F : \mathbb{Q}].$$

By checking the possible images characterized in Proposition 2.1, we see that if $\operatorname{im} \rho_{E_0,\ell}$ does not land in a Borel or split Cartan subgroup, then $\deg(x)$ is relatively prime to $\ell$. Thus $\deg(x) \mid [F : \mathbb{Q}]$. Combining this with the divisibility conditions obtained above, we find $[F : \mathbb{Q}]$ is divisible by

$$\begin{cases} \deg(x) \cdot \ell^{\max(0,2k-2-d)} & \text{if } \ell \text{ is odd,} \\ \deg(x) \cdot \ell^{\max(0,2k-d-3)} & \text{if } \ell = 2. \end{cases}$$

So suppose $E_0/\mathbb{Q}$ has a rational cyclic $\ell$-isogeny $C$, but $\operatorname{im}\rho_{E_0,\ell}$ is not in a split Cartan subgroup. By Theorem 3.32 and Tables 3 and 4 of [37], by replacing $E_0$ with $E_0/C$ if necessary, we may assume $E_0$ has mod $\ell$ image in Table 1 of the appendix. If $\deg(x)$ is prime to $\ell$, the argument goes as before, so suppose $\deg(x) = \ell \cdot x_0$. As we see in Table 1, in each case there exists $x' \in X_1(\ell)$ associated to $E_0$ such that $\deg(x') \mid x_0$, so the result holds with $x'$ in place of $x$. □

### 3.3. **Minimal Torsion Curves.**

**Proposition 3.3.** *Let $E/\mathbb{Q}$ be an elliptic curve and fix a prime number $\ell$. There exist at most finitely many minimal torsion curves for $\ell$ up to isomorphism over $\overline{\mathbb{Q}}$.*

*Proof.* Let $\mathcal{E}$ denote the geometric isogeny class of $E$, and let $E_{\min} \in \mathcal{E}$ be a minimal torsion curve for $\ell$. Then in particular, $E_{\min}$ corresponds to a point on $X_1(\ell)$ of least possible degree among all curves in $\mathcal{E}$, and so

$$[\mathbb{Q}(j(E_{\min})) : \mathbb{Q}] \leq \frac{\ell^2 - 1}{2},$$

the least possible degree of a point on $X_1(\ell)$ associated to $E$. If $E$ has complex multiplication, then there are only finitely many options for $E_{\min}$ as there are only finitely many CM $j$-invariants in an extension of bounded degree (since there are only finitely many imaginary quadratic fields—and hence imaginary quadratic orders—of a given class number [25]). So suppose $E$ is non-CM.

Since $E_{\min} \in \mathcal{E}$, by definition there exists an isogeny $\varphi : E \to E_{\min}$ defined over $\overline{\mathbb{Q}}$ which we may assume is cyclic of degree $N$ by [12, Lemma A.1]. By replacing $E, E_{\min}$ with quadratic twists if necessary, we may assume $\varphi$, $E$, and $E_{\min}$ are all defined over $\mathbb{Q}(j(E_{\min}))$ by [10, §3.3] or [12, Corollary A.5]. In other words,

$$E_{\min} \cong E/C$$

for some order $N$ cyclic subgroup $C$ of $E$ which is rational over $\mathbb{Q}(j(E_{\min}))$. We will show that $N$ is bounded by a constant that depends only on $\ell$. This will imply there are only finitely many points on $E$ which can serve as a generator for $\ker(\varphi)$ and hence only finitely many possible candidates for $E_{\min}$

By Serre's Open Image Theorem [33], the mod $p$ Galois representation of an elliptic curve $E'/\mathbb{Q}$ with $j(E') = j(E)$ is surjective for sufficiently large primes $p$. In particular, for these primes the degree of a point on $X_0(p)$ associated to $E'$ (or, alternatively, associated to $E$) is $p+1$. Since $p + 1 > (\ell^2 - 1)/2$ for large enough $p$, we see that only finitely many primes divide $N$:

$$\operatorname{Supp}(N) = \{p_1, p_2, \ldots, p_r\}.$$

Note that for each odd $p \in \operatorname{Supp}(N)$, the image of the mod $p$ Galois representation of $E'/\mathbb{Q}$ is of finite index in $\mathrm{GL}_2(\mathbb{Z}_p)$, again as a consequence of Serre's Open Image Theorem [33]. Thus there exists $k \in \mathbb{Z}^+$ such that for any point $x \in X_0(p^d)$ associated to $E'$ with $d \geq k$ we have

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

where $f : X_0(p^d) \to X_0(p^k)$ is the natural map. For $d$ large enough, we have $\deg(f) > (\ell^2 - 1)/2$, so there is an upper bound on the power of $p$ which can divide $N$. Since $\operatorname{Supp}(N)$ is finite and there is an upper bound on the power of each prime which divides $N$, we see that $N$ is bounded by a constant which depends on $\ell$, as desired. □

**Remark 3.4.** The minimal torsion curve within a fixed geometric isogeny class may or may not be unique (up to isomorphism over $\overline{\mathbb{Q}}$). For example, let $E_0/\mathbb{Q}$ be the elliptic curve with LMFBD label 38.b2 and let $\mathcal{E}$ denote its geometric isogeny class. Then the 5-adic Galois representation associated to $E_0$ is 5.24.0.1, and $E_0$ gives a rational point on $X_1(5)$ of degree 1. Since $\operatorname{ord}_5([\mathrm{GL}_2(\mathbb{Z}_5) : \operatorname{im}\rho_{E_0,5^\infty}]) = 0$ and $\deg(X_1(5^k) \to X_1(5)) = 5^{2k-2}$, the elliptic curve $E_0$ is a minimal torsion curve for 5 by Proposition 3.2. Moreover, any minimal torsion curve for 5 must in particular give a point

of minimal degree for $X_1(5)$, which means it must have $j$-invariant in $\mathbb{Q}$. The only other elliptic curve in $\mathcal{E}$ with $j$-invariant in $\mathbb{Q}$ is the elliptic curve $E'$ with LMFDB label 38.b1. However, $E'$ gives points on $X_1(5)$ of degree 2 and 5, so it is not a minimal torsion curve. It follows that there is a unique minimal torsion curve for the geometric isogeny class.

On the other hand, let $E_0/\mathbb{Q}$ be the elliptic curve with LMFDB label 50.b1 and let $\mathcal{E}$ denote its geometric isogeny class. The image of the 3-adic Galois representation associated to $E_0$ is 3.4.0.1. There is a point on $X_1(3)$ associated to $E_0$ if degree 1, and as in the previous example we see that $E_0$ is a minimal torsion curve for 3 by Proposition 3.2. However, one can check that *any* elliptic curve $\mathbb{Q}$-isogenous to $E_0$ is a minimal torsion curve, as they each have 3-adic image 3.4.0.1. This gives 4 distinct minimal torsion curves for the class $\mathcal{E}$ with respect to the prime 3.

**Remark 3.5.** We note there may be infinitely many elliptic curves (up to isomorphism over $\overline{\mathbb{Q}}$) within a fixed geometric isogeny class which are minimal for $X_1(\ell^k)$ for some $k$. For example, suppose the $\ell$-adic Galois representation of a non-CM elliptic curve $E/\mathbb{Q}$ is surjective, and let $C$ be a cyclic subgroup of $E$ of order $\ell^r$ for $r \in \mathbb{Z}^+$. The elliptic curve $E/C$ is defined over the extension $\mathbb{Q}(C)$ of degree $\ell^{r-1}(\ell+1)$ and possesses a $\mathbb{Q}(C)$-rational cyclic $\ell^r$ isogeny. By Proposition 2.2, $E/C$ gives a point on $X_1(\ell^r)$ of degree $\ell^{2r-2}(\ell^2-1)/2$. This is of minimal degree for the geometric isogeny class associated to $E$ by Proposition 3.2.

### 3.4. **Image of Galois Representations Under Isogeny.**

**Lemma 3.6.** *Suppose $E_1/F$ is a non-CM elliptic curve, and fix a prime number $\ell$. If $\varphi : E_1 \to E_2$ is an $F$-rational cyclic $\ell^r$-isogeny of elliptic curves over $F$, then* $\operatorname{im}\rho_{E_2,\ell^k}$ *is completely determined by* $\operatorname{im}\rho_{E_1,\ell^{r+k}}$*. In particular,* $\operatorname{im}\rho_{E_1,\ell^\infty}$ *completely determines* $\operatorname{im}\rho_{E_2,\ell^\infty}$*.*

*Proof.* Let $\{P,Q\}$ be a basis for $E_1[\ell^{r+k}]$, where $\ker(\varphi) = \langle \ell^k P\rangle$. Then with respect to this basis, for any $\sigma \in \mathrm{Gal}_F$, we have

$$\rho_{E_1,\ell^{r+k}}(\sigma) = \begin{pmatrix} a & b \\ \ell^r c & d \end{pmatrix},$$

for $a,b,c,d \in \mathbb{Z}/\ell^{r+k}\mathbb{Z}$, since the matrix must be upper triangular mod $\ell^r$. One can check that $\{\varphi(P), \ell^r\varphi(Q)\}$ gives a basis for $E_2[\ell^k]$. Moreover, for $\sigma \in \mathrm{Gal}_F$, we have

$$\sigma(\varphi(P)) = \varphi(\sigma(P)) = \varphi(aP + \ell^r cQ) = a\varphi(P) + c\ell^r\varphi(Q),$$
$$\sigma(\ell^r\varphi(Q)) = \ell^r\varphi(\sigma(Q)) = \ell^r\varphi(bP+dQ) = \ell^r b\varphi(P) + d\ell^r\varphi(Q).$$

Thus

$$\rho_{E_2,\ell^k}(\sigma) = \begin{pmatrix} a & \ell^r b \\ c & d \end{pmatrix}. \qquad \square$$

## 4. Proof of Theorems 1.5 and 1.3 for $\ell \geq 5$

In this section, we will prove the following, which improves upon the divisibility conditions of [9, Proposition 4.1], and also specifies when minimal torsion curves exists for points of odd degree.

**Proposition 4.1.** *Let $E_0/\mathbb{Q}$ be a non-CM elliptic curve and let $\mathcal{E}$ denote the corresponding geometric isogeny class. Suppose $\ell \geq 5$ is prime. If $E \in \mathcal{E}$ and $x = [E,P] \in X_1(\ell^k)$ is a point of odd degree for $k \geq 2$, then $\ell \in \{5,7,11,13\}$ and the following divisibility conditions hold and are best possible, where $d = \mathrm{ord}_\ell([\mathrm{GL}_2(\mathbb{Z}_\ell) : \operatorname{im}\rho_{E_0,\ell^\infty}])$:*

*(1) If $\ell = 13$, then $3\cdot 13^{2k-2} \mid \deg(x)$.*
*(2) If $\ell = 11$, then $5\cdot 11^{2k-2} \mid \deg(x)$.*
*(3) If $\ell = 7$ and $j(E') \neq 3^3\cdot 5\cdot 7^5/2^7$, then $7^{2k-2} \mid \deg(x)$.*
*(4) If $\ell = 7$ and $j(E') = 3^3\cdot 5\cdot 7^5/2^7$, then $9\cdot 7^{\max(0,2k-3)} \mid \deg(x)$.*

*(5) If $\ell = 5$, then $5^{\max(0,2k-3)} \mid \deg(x)$.*

*Moreover, for each $\mathcal{E}$, a minimal torsion curve exists for points of odd degree and has $j$-invariant in $\mathbb{Q}$ unless $j(E_0) = 3^3 \cdot 5 \cdot 7^5/2^7$ and $\ell = 7$, in which case the $j$-invariant generates an extension of degree 3. By replacing $E_0$ with another elliptic curve over $\mathbb{Q}$ in $\mathcal{E}$ if necessary, we may take $E_{min}$ to be of the form $E_0/C$ where $C$ is a cyclic subgroup of order $\ell$.*

4.1. **A Preliminary Result.** We begin with a preliminary result concerning minimal torsion curves within geometric isogeny classes of elliptic curves with a $\mathbb{Q}$-rational cyclic isogeny. In this case, the result largely follows from Proposition 1.6 and prior work of Greenberg [24] and Greenberg, Rubin, Silverberg, Stoll [23].

**Lemma 4.2.** *Suppose $\ell \geq 5$ is prime. Let $E_0/\mathbb{Q}$ be a non-CM elliptic curve which admits a rational cyclic $\ell$-isogeny, and let $\mathcal{E}$ denote the corresponding geometric isogeny class. Then the divisibility conditions of Proposition 1.6 are best-possible. Moreover, there exists $E'/\mathbb{Q} \in \mathcal{E}$ and a $\mathbb{Q}$-rational cyclic subgroup $C \leq E'$ of order $\ell$ such that $E'/C$ is a minimal torsion curve.*

*Proof.* Suppose first that $\ell > 5$ or that $\ell = 5$ and $E_0$ is not $\mathbb{Q}$-isogenous to an elliptic curve with a rational cyclic 25-isogeny. It follows from Greenberg [24, Theorems 1 and 2, Remark 4.2.1] and Greenberg, Rubin, Silverberg, Stoll [23] that $\mathrm{ord}_\ell([\mathrm{GL}_2(\mathbb{Z}_\ell) : \mathrm{im}\,\rho_{E_0,\ell^\infty}]) = 0$. Since $\deg(X_1(\ell^k) \to X_1(\ell)) = \ell^{2k-2}$, the result follows from Proposition 1.6.

Now, suppose $\ell = 5$ and $E_0$ has a rational cyclic 25-isogeny or two independent 5-isogenies. Then by work of Greenberg [24, Theorem 2], we have $\mathrm{ord}_5([\mathrm{GL}_2(\mathbb{Z}_5) : \mathrm{im}\,\rho_{E_0,5^\infty}]) = 1$. By replacing $E_0$ with a curve $\mathbb{Q}$-isogenous if necessary, we may assume $E_0$ has two independent 5-isogenies. Then $\mathrm{im}\,\rho_{E_0,5}$ is one of the following, and we consider each case separately:

- 5Cs.1.1: $E_0$ has a subgroup $C_1$ generated by a rational point $P$ of order 5 and an additional rational cyclic subgroup $C_2$ of order 5. Then $E_1 \coloneqq E_0/C_2$ has a rational cyclic 25-isogeny, and the image of $P$ is a point of order 5 in $E_1(\mathbb{Q})$ lying in the kernel of this isogeny. Thus the image of the isogeny character $\chi : \mathrm{Gal}_\mathbb{Q} \to (\mathbb{Z}/25\mathbb{Z})^\times$ lands in the subgroup $\{a : a \equiv 1 \pmod 5\}$ and so has order dividing 5. It follows that $E_1$ attains a rational point of order 25 in an extension of order dividing 5. The degree must be exactly 5 by Proposition 1.6 , and moreover lifts of this point show the divisibility condition is best-possible for all $k$.
- 5Cs.1.3 or 5Cs.4.1: A quadratic twist of $E_0$ will have a rational point of order 5 and an independent 5-isogeny, so the conclusion follows as in the last case.
- 5Cs: $E_0$ has two independent 5-isogenies with kernels $C_1$ and $C_2$. Then $E_1 \coloneqq E_0/C_2$ has a rational cyclic 25-isogeny and attains a point of order 5 in degree dividing 2 and a point of order 25 in degree dividing 10. Since 2 divides $\deg(x)$ for all $x \in X_1(5)$ associated to $E_0$ or $E_0/C$ where $C$ is the kernel of a $\mathbb{Q}$-rational cyclic $\ell$-isogeny, this is best possible by Proposition 1.6. □

4.2. **Proof of Proposition 4.1.** Let $F = \mathbb{Q}(x)$. By Lemma 3.1, there is a model of $E/F$ where $P \in E(F)$ and such that there exists an $F$-rational cyclic isogeny $\varphi : E \to E'$ with $j(E') = j(E_0)$. Since $E$ has an $\ell$-isogeny over $F$, so does $E'$ by [12, Proposition 3.2]. It follows from [12, Proposition 3.3] that $E_0/\mathbb{Q}$ has a $\mathbb{Q}$-rational cyclic $\ell$-isogeny, unless $\ell = 7$ and $j(E_0) = 3^3 \cdot 5 \cdot 7^5/2^7$. By Lemma 4.2, Proposition 1.6, and checking the possible images in Tables 1 and 2 of [22] which may yield points of odd degree points, it suffices to assume $\ell = 7$ and $j(E_0) = 3^3 \cdot 5 \cdot 7^5/2^7$.

Let $P \in E(F)$ be a point of order $7^k$. Notice that $7^{k-1}P$ is a point of order 7 on $E$ and is also defined over $F$ on $E$. By part [9, Corollary 4.3], for any $E'$ that is $F$-isogenous to $E$, the curve $E'$ has a rational point of order 7 over an extension $F'/F$ of degree 1 or 7. As $j(E') = 3^3 \cdot 5 \cdot 7^5/2^7$, a computation with division polynomials shows $F'$ is divisible by 6 or 9. Since $[F' : F]$ divides 7, it follows that 6 or 9 must divide $[F : \mathbb{Q}]$. Since $F$ is an extension of odd degree, we must have

$9 \mid [F : \mathbb{Q}]$. Moreover, in [9, Proposition 4.1], it is proven that $3 \cdot 7^{\max(0,2k-3)}$ divides $[F : \mathbb{Q}]$. Therefore, $9 \cdot 7^{\max(0,2k-3)}$ divides $[F : \mathbb{Q}]$.

We will now show there is a number field $F$ of degree $9 \cdot 7^{\max(0,2k-3)}$ and an elliptic curve $E/F$ isogenous to $E'$ with $j(E') = 3^3 \cdot 5 \cdot 7^5/2^7$ where $E$ has a point of order $7^k$ defined over $F$. By replacing $E_0$ with a quadratic twist if necessary, we may assume $E_0$ has LMFDB label 2450.y1. A computation with division polynomials confirms that $E_0$ gives a point on $X_1(7)$ of degree 9. Notice that this point fulfills the $k = 0$ case. In addition, the mod 7 image of $E_0$ is 7Ns.2.1, which is generated by the following matrices:

$$\begin{pmatrix} 0 & 5 \\ 5 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 5 \\ 3 & 0 \end{pmatrix}$$

A Magma computation shows that 7NS.2.1 contains an index 3 subgroup conjugate to the group generated by

$$\begin{pmatrix} 2 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}.$$

Thus over a cubic extension $F$, $E_0$ attains two independent 7 isogenies, and is $F$-isogenous to an elliptic curve $E_1/F$ with a rational cyclic 49-isogeny. The curve $E_1$ gives a point on $X_1(49)$ of degree dividing $9 \cdot 7$. The previous paragraph shows it must have degree exactly $9 \cdot 7$, and since $\deg(X_1(7^k) \to X_1(7^2))$ has degree $7^{2k-4}$, the divisibility conditions of Proposition 1.6 are best-possible. Moreover, $E_1$ is a minimal torsion curve for points on $X_1(7^k)$ of odd degree.

## 5. Proof of Theorems 1.5 and 1.3 for $\ell = 3$

In this section, we will prove the following result, which includes instances where the divisibility conditions of Proposition 1.6 can be improved.

**Proposition 5.1.** *Let $E_0/\mathbb{Q}$ be a non-CM elliptic curve and let $\mathcal{E}$ denote the corresponding geometric isogeny class. If $E \in \mathcal{E}$ and $x = [E, P] \in X_1(3^k)$ is a point of odd degree for $k \geq 2$, then the following divisibility conditions hold and are best possible for $k$ sufficiently large, where $d = \operatorname{ord}_3([\mathrm{GL}_2(\mathbb{Z}_3) : \operatorname{im} \rho_{E_0,3^\infty}])$:*

*(1) $3^{\max(0,2k-1-d)} \mid \deg(x)$ if there is $E_1/\mathbb{Q} \in \mathcal{E}$ with $\operatorname{im} \rho_{E_1,3^\infty} \in \{9.36.0.6, 9.36.0.8\}$,*

*(2) $3^{\max(0,2k-2-d)} \mid \deg(x)$ otherwise.*

*Moreover, a minimal torsion curve exists for points of odd degree (and has $j$-invariant in $\mathbb{Q}$) unless there is $E_1/\mathbb{Q} \in \mathcal{E}$ with 3-adic image 9.12.0.2, 9.36.0.2, 9.36.0.7, or 9.36.0.8.*

From the proof, we immediately deduce the following corollaries.

**Corollary 5.2.** *Moreover, in each case, there exists $E_0/\mathbb{Q}$ in $\mathcal{E}$ and a cyclic subgroup $C \leq E$ of order 3 such that $E_0/C$ produces a point on $X_1(3^k)$ in least possible odd degree for all $k$ sufficiently large. In general, there is not a unique choice for such a $C$.*

**Corollary 5.3.** *Let $E/\mathbb{Q}$ be a non-CM elliptic curve and let $\mathcal{E}$ denote the corresponding geometric isogeny class. If $E' \in \mathcal{E}$ and $x = [E', P'] \in X_1(3^k)$ is a point of odd degree, then $3^{\max(0,2k-4)} \mid \deg(x)$, and this is best possible without placing restrictions on $\mathcal{E}$.*

**Remark 5.4.** By Proposition 5.1, if $\ell = 3$ and there exists $E_1 \in \mathcal{E}$ with $\operatorname{im} \rho_{E_1,3^\infty} = 9.36.0.6$, then any odd degree point on $X_1(3^k)$ associated to an elliptic curve in $\mathcal{E}$ is divisible by $3^{\max(0,2k-3)}$. By Proposition 1.6, any point of even degree must be divisible by $2 \cdot 3^{\max(0,2k-4)}$. Since there exists $x \in X_1(3)$ of degree 1 associated to $E_1$, this strengthens the lower bound in Proposition 1.6 by a factor of 2 or 3, respectively. Moreover, both conditions are sharp. This follows from Proposition 5.1 for points of odd degree. To verify the condition for points of even degree, choose $E_0 \in \mathcal{E}$ with $\operatorname{im} \rho_{E_1,3^\infty} = 9.36.0.3$. A Magma computation shows that, over a field extension $F/\mathbb{Q}$ of degree 6,

the elliptic curve $E_0$ attains two independent $F$-rational cyclic 9-isogenies. Thus, $E_0$ is $F$-isogenous to an elliptic curve with an $F$-rational cyclic 81 isogeny which produces a point of degree $2 \cdot 3^4$ by Proposition 2.2. Since $\deg(X_1(3^k) \to X_1(3^4)) = 3^{2k-8}$, we attain a point on $X_1(3^k)$ associated to $\mathcal{E}$ of degree $2 \cdot 3^{2k-4}$ for any $k \geq 4$. Note this construction is formed by taking the quotient of $E_0$ by a cyclic subgroup $C$ of order 9, and Magma computations suggest that no elliptic curve in $\mathcal{E}$ which is the quotient of a rational elliptic curve by a cyclic subgroup of order $\ell$ will achieve a point on $X_1(3^k)$ in degree $2 \cdot 3^{\max(0,2k-4)}$.

5.1. **Preliminary Results.** In this section we prove several lemmas which are necessary in the case where $\mathcal{E}$ contains $E_0/\mathbb{Q}$ with $\operatorname{im}\rho_{E_0,3^\infty} = 9.36.0.6$ or $9.36.0.8$.

**Lemma 5.5.** *Suppose $F$ is a number field of odd degree and $E/F$ is a non-CM elliptic curve with $P \in E(F)$ of order $3^k$, $k \geq 2$. Let $\varphi : E \to E'$ be an $F$-rational isogeny, where there exists $E_0/\mathbb{Q}$ of with $j(E_0) = j(E')$ and $d \coloneqq \operatorname{ord}_3([\mathrm{GL}_2(\mathbb{Z}_3) : \operatorname{im}\rho_{E_0,3^\infty}])$. If $3^{2k-1-d} \nmid [F : \mathbb{Q}]$, then there exists a basis $\{P, Q\}$ of $E[3^k]$ so that*

$$\operatorname{im}\rho_{E/F,3^k} = \left\{ \begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} \mid x \in \mathbb{Z}/3^k\mathbb{Z}, y \in (\mathbb{Z}/3^k\mathbb{Z})^\times \right\}$$

*and* $\operatorname{im}\rho_{E/F,3^\infty} = \pi^{-1}(\operatorname{im}\rho_{E/F,3^k})$.

*Proof.* Suppose $3^{2k-1-d} \nmid [F : \mathbb{Q}]$, and let $\{P, Q\}$ be a basis of $E[3^k]$. Replacing $F$ with at worst a quadratic extension $L/F$, we may view $\varphi$ as an $L$-isogeny from $E$ to our original model for $E_0/\mathbb{Q}$, under base extension to $L$. Then $\operatorname{im}\rho_{E/L,3^k}$ is contained in

$$H \coloneqq \left\{ \begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} \mid x \in \mathbb{Z}/3^k\mathbb{Z}, y \in (\mathbb{Z}/3^k\mathbb{Z})^\times \right\},$$

which has order $3^k \cdot \varphi(3^k) = 3^{2k-1} \cdot 2$. If $\operatorname{ord}_3(\#\operatorname{im}\rho_{E/L,3^k}) < 2k-1$, then the index of the mod $3^k$ Galois representation of $E/L$ is divisible by $3^{2k-1}$. Thus

$$3^{2k-1} \mid [\mathrm{GL}_2(\mathbb{Z}_3) : \operatorname{im}\rho_{E/L,3^\infty}].$$

By Lemma 4.5 of [9], we have $3^{2k-1} \mid [\mathrm{GL}_2(\mathbb{Z}_3) : \operatorname{im}\rho_{E_0/\mathbb{Q},3^\infty}] \cdot [L \cap \mathbb{Q}(E_0[3^\infty]) : \mathbb{Q}]$. Since

$$\operatorname{ord}_3([\mathrm{GL}_2(\mathbb{Z}_3) : \operatorname{im}\rho_{E_0/\mathbb{Q},3^\infty}]) = d,$$

it follows that $3^{2k-1-d} \mid [L \cap \mathbb{Q}(E_0[3^\infty]) : \mathbb{Q}]$. Since $L$ is at most a quadratic extension of $F$, then $3^{2k-1-d} \mid [F : \mathbb{Q}]$, contradicting our assumption. So we may assume $\operatorname{ord}_3(\#\operatorname{im}\rho_{E/L,3^k}) = 2k-1$.

Note $\operatorname{im}\rho_{E/F,3^k}$ contained in $H$ as well, and since $L/F$ is at worst a quadratic extension, we have $\operatorname{ord}_3(\#\operatorname{im}\rho_{E/F,3^k}) = 2k-1$. If $\operatorname{im}\rho_{E/F,3^k}$ is properly contained in $H$, then $\#\operatorname{im}\rho_{E/F,3^k} = 3^{2k-1}$. In particular, it is a Sylow 3-subgroup of $H$ of index 2. By the Sylow Theorems, this index 2 subgroup is unique, so it must be equal to

$$\operatorname{im}\rho_{E/F,3^k} = \left\{ \begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} \mid x \in \mathbb{Z}/3^k\mathbb{Z}, y \in K \leq (\mathbb{Z}/3^k\mathbb{Z})^\times \right\},$$

where $K$ is the subgroup of $(\mathbb{Z}/3^k\mathbb{Z})^\times$ of order $3^{k-1}$. However, since the image of the determinant map is not surjective and has size $3^{k-1}$, we find that $\mathbb{Q}(\zeta_{3^k}) \cap F$ is a quadratic extension. This contradicts $F$ having odd degree. Hence $\operatorname{im}\rho_{E/F,3^k} = H$.

If $\operatorname{im}\rho_{E/F,3^\infty} \neq \pi^{-1}(\operatorname{im}\rho_{E/F,3^k})$, then $[F(E[3^{k+1}]) : F(E[3^k])]$ divides $3^3$; see, for example, [7, Proposition 3.5]. Since $\#\operatorname{Gal}(F(E[3^k])/F) = 3^{2k-1} \cdot 2$, we have

$$\#\operatorname{Gal}(F(E[3^{k+1}])/F) \mid 3^3 \cdot 3^{2k-1} \cdot 2 = 3^{2k+2} \cdot 2.$$

It follows that $\#\operatorname{Gal}(L(E[3^{k+1}])/F) \mid 3^{2k+2}\cdot 2$, and so the index of the 3-adic Galois representation of $E/L$ is divisible by at least $3^{2k-1}\cdot 8$. By Lemma 4.5 of [9], we have $3^{2k-1}\cdot 8 \mid [\mathrm{GL}_2(\mathbb{Z}_3) : \operatorname{im}\rho_{E_0/\mathbb{Q},3^\infty}]\cdot[L\cap\mathbb{Q}(E_0[3^\infty]) : \mathbb{Q}]$. It follows that $3^{2k-1-d} \mid [L\cap\mathbb{Q}(E_0[3^\infty]) : \mathbb{Q}]$. Since $L$ is at worst a quadratic extension of $F$, then $3^{2k-1-d} \mid [F : \mathbb{Q}]$, contradicting our assumption. Thus $\operatorname{im}\rho_{E/F,3^\infty} = \pi^{-1}(\operatorname{im}\rho_{E/F,3^k})$ □

**Lemma 5.6.** *Suppose $F$ is a number field of odd degree and $E/F$ is a non-CM elliptic curve with $P\in E(F)$ of order $3^k$, $k\geq 2$. Let $\varphi : E\to E'$ be an $F$-rational isogeny of degree $3^r$ for $r\in\mathbb{Z}^+$, where there exists $E_0/\mathbb{Q}$ of with $j(E_0)=j(E')$ and $d \coloneqq \operatorname{ord}_3([\mathrm{GL}_2(\mathbb{Z}_3) : \operatorname{im}\rho_{E_0,3^\infty}])$. If $3^{2k-1-d}\nmid[F:\mathbb{Q}]$, then $r\leq k$ and $\ker(\varphi)\subseteq\langle P\rangle$.*

*Proof.* Suppose $3^{2k-1-d}\nmid[F:\mathbb{Q}]$. First, suppose for the sake of contradiction that $r>k$. Then

$$\operatorname{im}\rho_{E,3^r} \neq \pi^{-1}(\operatorname{im}\rho_{E,3^k}),$$

and by Lemma 5.5 we have $3^{2k-1-d}\mid[F:\mathbb{Q}]$. We have reached a contradiction.

So suppose $r\leq k$ and, for the sake of contradiction, suppose that $\ker(\varphi)\not\subseteq\langle P\rangle$. Then there exists $R\in E$ of order $3^r$ such that $\ker(\varphi)=\langle R\rangle$. With respect to the basis $\{3^{k-r}P, Q_1\}$, by Lemma 5.5 we may assume

$$\operatorname{im}\rho_{E/F,3^r} = \left\{\begin{pmatrix}1 & x\\ 0 & y\end{pmatrix} \mid x\in\mathbb{Z}/3^r\mathbb{Z}, y\in(\mathbb{Z}/3^r\mathbb{Z})^\times\right\} = \mathcal{I}_1.$$

With respect to the basis $\{R, Q_2\}$, the image also consists of upper triangular matrices, say $\mathcal{I}_2$. Thus there exists a matrix $M\in\mathrm{GL}_2(\mathbb{Z}/3^r\mathbb{Z})$ such that $M\mathcal{I}_1M^{-1}=\mathcal{I}_2$. Let

$$M=\begin{pmatrix}a & b\\ c & d\end{pmatrix}.$$

We note $M\begin{pmatrix}1 & x\\ 0 & y\end{pmatrix}M^{-1}$ is upper-triangular iff $dc-c^2x-dcy\equiv 0 \pmod{3^r}$. If $c\not\equiv 0\pmod{3^r}$, then $x=y=1$ implies $c^2\equiv 0\pmod{3^r}$. This cannot be if $r=1$, so assume $r>1$. Moreover, when $y=2$, then this implies $dc\equiv 0\pmod{3^r}$. However, under our assumptions, we have $3^r\mid c^2$ and $3^r\mid dc$, but $3^r\nmid c$. Thus $3\mid c$ and $3\mid d$, which means $\det(M)=ad-bc$ is not a unit in $\mathbb{Z}/3^r\mathbb{Z}$, contradicting the fact that $M$ is invertible. So $c\equiv 0\pmod{3^r}$. But then

$$M\begin{pmatrix}1 & x\\ 0 & y\end{pmatrix}M^{-1} = \begin{pmatrix}1 & x'\\ 0 & y'\end{pmatrix},$$

and $R\in E(F)$.

Since we have assumed $R\notin\langle P\rangle$, then $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\subseteq\langle R,P\rangle$ and

$$\operatorname{im}\rho_{E/F,3^k} = \left\{\begin{pmatrix}1 & x\\ 0 & y\end{pmatrix} \mid x\equiv 0 \pmod 3, y\equiv 1 \pmod 3\right\}.$$

This contradicts Lemma 5.5. □

**Proposition 5.7.** *Suppose $F$ is a number field of odd degree and $E/F$ is an elliptic curve with $P\in E(F)$ of order $3^k$, $k\geq 2$. Let $\varphi : E\to E'$ be an $F$-rational isogeny of degree $3^r$ for $r\in\mathbb{Z}^+$, where there exists $E_0/\mathbb{Q}$ of with $j(E_0)=j(E')$ and $\operatorname{im}\rho_{E_0,3^\infty}$ = 9.36.0.6 or 9.36.0.8. Then $3^{2k-3}\mid[F:\mathbb{Q}]$.*

*Proof.* If $\operatorname{im}\rho_{E_0,3^\infty}$ = 9.36.0.6 or 9.36.0.8, then $\operatorname{ord}_3([\mathrm{GL}_2(\mathbb{Z}_3) : \operatorname{im}\rho_{E_0,3^\infty}]) = 2$. Suppose for the sake of contradiction that $3^{2k-3}\nmid[F:\mathbb{Q}]$. Then by Lemma 5.5, with respect to a basis $\{P,Q\}$,

$$\operatorname{im}\rho_{E/F,3^k} = \left\{\begin{pmatrix}1 & x\\ 0 & y\end{pmatrix} \mid x\in\mathbb{Z}/3^k\mathbb{Z}, y\in(\mathbb{Z}/3^k\mathbb{Z})^\times\right\}$$

and $\operatorname{im}\rho_{E/F,3^\infty} = \pi^{-1}(\operatorname{im}\rho_{E/F,3^k})$. Moreover, by Lemma 5.6, we have $r \le k$ and $\ker(\varphi) \subseteq \langle P\rangle$.

First, suppose $r = k-1$ or $k$. Set $d = r+2$, and let $\{R, S\}$ be a basis of $E[3^d]$ such that $3^{d-k}R = P$ and $3^{d-k}S = Q$. Then we will show $\{\varphi(R), 3^{k-2}\varphi(Q)\}$ is a basis of $E'[9]$. Suppose not. Then there exist integers $\alpha, \beta$ such that $\alpha\varphi(R) = \beta 3^{k-2}\varphi(Q)$ is nontrivial. This implies $\alpha R - \beta 3^{k-2}Q \in \ker(\varphi) \subseteq \langle P\rangle = \langle 3^{d-k}R\rangle$. Thus a nonzero multiple of $S$ is in the cyclic subgroup generated by $R$, which contradicts the fact that $\{R, S\}$ is a basis of $E[3^d]$.

As noted at the start of the proof, there exists $\sigma \in \mathrm{Gal}_F$ such that

$$\rho_{E/F,3^k}(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}.$$

Since $\operatorname{im}\rho_{E/F,3^\infty} = \pi^{-1}(\operatorname{im}\rho_{E/F,3^k})$, with respect to the basis $\{R, S\}$ of $E[3^d]$, we know there exists $\sigma' \in \mathrm{Gal}_F$ such that

$$\rho_{E/F,3^d}(\sigma') = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}.$$

Under the basis $\{\varphi(R), 3^{k-2}\varphi(Q)\}$ of $E'[9]$,

$$\begin{aligned} \sigma'(\varphi(R)) &= \varphi(\sigma'(R)) \\ &= \varphi(R) \end{aligned}$$

$$\begin{aligned} \sigma'(3^{k-2}\varphi(Q)) &= 3^{k-2}\varphi(\sigma'(Q)) \\ &= 3^{k-2}\varphi(4Q) \\ &= 4\cdot 3^{k-2}\varphi(Q) \end{aligned}$$

So

$$\rho_{E'/F,9}(\sigma') = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}.$$

After at worst a quadratic extension $L/F$, we have $E'/L \cong_L E_0/L$. Since the matrix above has order 3,

$$\rho_{E_0/L,9}(\sigma') = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}.$$

This means that the group generated by $\rho_{E_0/L,9}(\sigma')$ is conjugate to an order 3 subgroup of 9.36.0.6 or 9.36.0.8 mod 9, and a Magma computation shows no such subgroup exists.

Now, suppose $r \le k-2$. Then $\{3^{k-r-2}\varphi(P), 3^{k-2}\varphi(Q)\}$ is a basis of $E'[9]$ since $\ker(\varphi) \subseteq \langle P\rangle$. Since $P \in E(F)$, we have $3^{k-r-2}\varphi(P) \in E'(F)$. Moreover,

$$\begin{aligned} \sigma(3^{k-2}\varphi(Q)) &= 3^{k-2}\varphi(\sigma(Q)) \\ &= 3^{k-2}\varphi(xP + yQ) \\ &= x\varphi(3^{k-2}P) + y3^{k-2}\varphi(Q) \\ &= x3^r 3^{k-r-2}\varphi(P) + y3^{k-2}\varphi(Q), \end{aligned}$$

so

$$\operatorname{im}\rho_{E'/F,9} = \left\{ \begin{pmatrix} 1 & 3^r x \\ 0 & y \end{pmatrix} \mid x \in \mathbb{Z}/9\mathbb{Z},\, y \in (\mathbb{Z}/9\mathbb{Z})^\times \right\}.$$

After at worst a quadratic extension $L/F$, we have $E'/L \cong_L E_0/L$, so we may assume $\operatorname{im}\rho_{E_0/L,9}$ contains

$$\begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}.$$

We reach a contradiction as before. □

5.2. **Proof of Proposition 5.1.** Let $F = \mathbb{Q}(x)$. By Lemma 3.1, there is a model of $E/F$ where $P \in E(F)$ and such that there exists an $F$-rational cyclic isogeny $\varphi : E \to E'$ with $j(E') = j(E_0)$. Since $E$ has a 3-isogeny over $F$, so does $E'$ by [12, Proposition 3.2]. It follows from [12, Proposition 3.3] that $E_0/\mathbb{Q}$ has a $\mathbb{Q}$-rational cyclic 3-isogeny. By [26, Corollary 1.3.1], the 3-adic image is one of the following groups, and we will consider each separately. Note that since we are interested in characterizing points on modular curves, we may restrict to cases where $-I$ is contained in the 3-adic image. Also, since $E_0$ gives a point of degree 1 on $X_1(3)$, any minimal torsion curve must have $j$-invariant in $\mathbb{Q}$.

(1) $\operatorname{im}\rho_{E_0,3^\infty}$ = 3.4.0.1: Here, $E_0$ gives a point of degree 1 on $X_1(3)$. Since $d = 0$ and $\deg(X_1(3^k) \to X_1(3)) = 3^{2k-2}$, the divisibility condition of Proposition 1.6 is best possible, and $E_0$ is a minimal torsion curve. Any elliptic curve $\mathbb{Q}$-isogenous to $E_0$ is also a minimal torsion curve.

(2) $\operatorname{im}\rho_{E_0,3^\infty}$ = 3.12.0.1 or 9.12.0.1: By Lemma 3.6, these represent images of elliptic curves in the same $\mathbb{Q}$-isogeny class (consider, for example, isogeny class 98.a in the LMFDB), so we are free to assume $E_0$ has image 9.12.0.1. Thus $E_0$ corresponds to points on $X_1(3)$ and $X_1(9)$ of degree 1 and 3, respectively. Since $d = 1$ and $\deg(X_1(3^k) \to X_1(3)) = 3^{2k-2}$ for $k \geq 2$, the divisibility condition of Proposition 1.6 is best-possible and $E_0$ is a minimal torsion curve. Any elliptic curve $\mathbb{Q}$-isogenous to $E_0$ with 3-adic image 9.12.0.1 is a minimal torsion curve. If the 3-adic image is 3.12.0.1, then it is *not* a minimal torsion curve.

(3) $\operatorname{im}\rho_{E_0,3^\infty}$ = 9.12.0.2: A Magma computation shows that for $E_0/\mathbb{Q}$ with this image, there exists a cubic extension $F$ such that $E_0/F$ has an $F$-rational 9-isogeny and an independent 3-isogeny. Thus over $F$, the curve $E_0$ is isogenous to $E_1/F$ with a rational cyclic 27-isogeny. Thus $E_1$ gives a point on $X_1(27)$ of degree at most 27 by Proposition 2.2. Since $d = 1$ and $\deg(X_1(3^k) \to X_1(27)) = 3^{2k-6}$, the divisibility conditions of Proposition 1.6 are best-possible for all $k \geq 3$. No elliptic curve in $\mathcal{E}$ with $j \in \mathbb{Q}$ has a point of order 27 in this degree or lower, so no minimal torsion curve exists.

(4) $\operatorname{im}\rho_{E_0,3^\infty}$ = 9.36.0.2 or 27.36.0.1: By Lemma 3.6, these represent images of elliptic curves in the same $\mathbb{Q}$-isogeny class (consider, for example, isogeny class 304.c in the LMFBD), so we are free to assume $E_0$ has image 27.36.0.1. A Magma computation shows that for $E_0/\mathbb{Q}$ with this image, there exists a cubic extension $F$ such that $E_0/F$ has an $F$-rational 27-isogeny and an independent 3-isogeny. Thus over $F$, the curve $E_0$ is isogenous to $E_1/F$ with a rational cyclic 81-isogeny. Thus $E_1$ gives a point on $X_1(81)$ of degree at most 81 by Proposition 2.2. Since $d = 2$ and $\deg(X_1(3^k) \to X_1(81)) = 3^{2k-8}$, the divisibility conditions of Proposition 1.6 are best-possible for all $k \geq 4$. No elliptic curve in $\mathcal{E}$ with $j$-invariant in $\mathbb{Q}$ has a point of order 81 in this degree or lower, so there is no minimal torsion curve.

(5) $\operatorname{im}\rho_{E_0,3^\infty}$ = 9.36.0.3 or 9.36.0.6: By Lemma 3.6, these represent images of elliptic curves in the same $\mathbb{Q}$-isogeny class (consider, for example, isogeny class 22491.u in the LMFBD), so we are free to assume $E_0$ has image 9.36.0.6. If $\varphi : E \to E'$ has degree $3^r \cdot d$ for $3 \nmid d$, then there exists an elliptic curve $d$-isogenous to $E$ with an $F$-rational point of order $3^k$. Replacing $E$ with this curve if necessary, we may assume $\varphi$ has degree $3^r$. Then $3^{2k-3} \mid [F : \mathbb{Q}]$ by Proposition 5.7. Since $d = 2$, the conclusion follows, as $E_0$ is a minimal torsion curve. Note an elliptic curve over $\mathbb{Q}$ with 3-adic image 9.36.0.3 is *not* a minimal torsion curve.

(6) $\operatorname{im}\rho_{E_0,3^\infty}$ = 9.36.0.1, 9.36.0.4, or 9.36.0.5: By Lemma 3.6, these represent images of elliptic curves in the same $\mathbb{Q}$-isogeny class (consider, for example, isogeny class 432.b in the LMFBD), so we are free to assume $E_0$ has image 9.36.0.4. A twist of $E_0$ has a rational point of order 9 and $d = 2$, so divisibility conditions of Proposition 1.6 are best possible and $E_0$ is a minimal torsion curve. Note an elliptic curve over $\mathbb{Q}$ with 3-adic image 9.36.0.1 or 9.36.0.5 is *not* a minimal torsion curve.

(7) $\operatorname{im}\rho_{E_0,3^\infty} = 9.36.0.7$ or $9.36.0.9$: We are free to assume $E_0$ has image $9.36.0.7$ (consider, for example, isogeny class 1734.k in the LMFDB). A Magma computation shows that for $E_0/\mathbb{Q}$ with this image, there exists a cubic extension $F$ such that a twist $E_0^t$ of $E_0/F$ has an $F$-rational point of order 9 (say $Q$) and an independent 3-isogeny (say, with kernel generated by $R$). Then $\psi : E_0^t \to E_1 = E_0^t/\langle R\rangle$ is a degree 3 isogeny, where $E_1$ has an $F$-rational cyclic 27-isogeny and $\psi(Q) \in E_1(F)$ is a point of order 9. Moreover, $\psi(Q)$ is in the kernel of $E_1$'s rational 27-isogeny. Thus the image of the 27-isogeny character $\chi$ associated to $E_1/F$ lands in $\{1, 10, 19\}$ and $E_1$ attains a point of order 27 in $\overline{F}^{\ker(\chi)}$, an extension of $F$ of degree dividing 3. Hence $E_1$ corresponds to a point on $X_1(27)$ of degree dividing 9. Since $d = 2$, the divisibility conditions of Proposition 1.6 are best-possible for $k \geq 3$. No minimal torsion curve exists, as all elliptic curves in $\mathcal{E}$ with $j$-invariant in $\mathbb{Q}$ give a point of order $3^k$ in degree at least $3^{\max(0,2k-3)}$.

(8) $\operatorname{im}\rho_{E_0,3^\infty} = 9.36.0.8$: As in case 5, we may assume $\varphi : E \to E'$ has degree $3^r$. Then $3^{2k-3} \mid [F : \mathbb{Q}]$ by Proposition 5.7. A Magma computation shows that for $E_0/\mathbb{Q}$ with this image, there exists a cubic extension $F$ such that $E_0/F$ has an $F$-rational 9-isogeny and an independent 3-isogeny. Thus over $F$, the curve $E_0$ is isogenous to $E_1/F$ with a rational cyclic 27-isogeny. Thus by Proposition 2.2, the curve $E_1$ gives a point on $X_1(27)$ of degree at most 27, and since $d = 2$, the divisibility conditions of Proposition 5.7 are best-possible for $k \geq 3$. Note $E_0$ gives a point on $X_1(3^k)$ in degree at least $3^{2k-2}$ for all $k$, so no minimal torsion curve exists.

## 6. Proof of Theorem 1.5 for $\ell = 2$

By Proposition 4.1 in [9], if a $\mathbb{Q}$-curve has a point of order $2^k$ defined over a field of odd degree then $k \leq 4$. As any elliptic curve geometrically isogenous to an elliptic curve with rational $j$-invariant is a $\mathbb{Q}$-curve, it suffices to show that $k \neq 4$. By work of [29], there exists a non-CM elliptic curve defined over $\mathbb{Q}$ with a point of order $2^3$, so this is the best possible bound.

**Proposition 6.1.** *There is no elliptic curve $E$ defined over a field $F$ of odd degree such that*
*(i) $E(F)$ contains a point of order $2^4$ and*
*(ii) $E$ is $F$-isogenous to an elliptic curve $E'$ with $j(E') \in \mathbb{Q}$.*

*Proof.* Suppose for the sake of contradiction that $E$ has a point $Q$ such that $Q \in E(F)$ and the order of $Q$ is 16. Then by Theorem 2.7 and Lemma A.1 in [12] there exists a cyclic $F$-rational isogeny $\phi : E \to E'$ where $j(E') \in \mathbb{Q}$. The degree of $\phi$ can be taken to be a power of 2; indeed, if it is not a power of 2, then it can be written as $2^k \cdot n$ for some integers $k$ and odd $n > 1$. Then, as it is cyclic, there is a generator of the kernel $S$, and $2^k S$ is a point of order $n$. Then $E/\langle 2^k S\rangle$ can replace $E$ in the proof going forward, since the image of $Q$ on $E/\langle 2^k S\rangle$ has order 16 and $E/\langle 2^k S\rangle \to E/\langle S\rangle$ has degree $2^k$.

Then $\hat{\phi} : E' \to E$ the dual isogeny of $\phi$ exists and is also cyclic and of the same degree as $\phi$; therefore there exists $P \in E'$ of order $2^k$ such that $\ker(\hat{\phi}) = \langle P\rangle$ and $\langle P\rangle$ is $F$-rational. As $\langle 2^{k-1}P\rangle$ is $F$-rational, but $2^{k-1}P$ is a point of order 2, the point $2^{k-1}P$ is $F$-rational. This is because if $\sigma \in \operatorname{Gal}(\overline{K}/K)$ fixes $\langle 2^{k-1}P\rangle$, which consists only of $\mathcal{O}$ and $2^{k-1}P$, but cannot send $2^{k-1}P$ to $\mathcal{O}$ because it is a nonzero isogeny, it must fix $2^{k-1}P$. As the only points of order 2 on an elliptic curve defined by $y^2 = x^3 + Ax + B$ are of the form $(x_0, 0)$ where $x_0$ is a root of $x^3 + Ax + B$, $[\mathbb{Q}(2^{k-1}P) : \mathbb{Q}] \leq 3$. There is an immediate contradiction if $[\mathbb{Q}(2^{k-1}P) : \mathbb{Q}] = 2$, as $\mathbb{Q}(2^{k-1}P) \subseteq F$ which has odd degree.

If $[\mathbb{Q}(2^{k-1}P) : \mathbb{Q}] = 1$, then $[\mathbb{Q}\langle P\rangle : \mathbb{Q}] = 1$. But $\mathbb{Q}(\langle P\rangle) = \mathbb{Q}(\langle 2^{k-1}P\rangle)$ by Proposition 3.6 of [12]. Therefore $P$ is defined over $\mathbb{Q}$, and $E$ (replaced by a twist if necessary) is defined over $\mathbb{Q}$. In particular, $j(E) \in \mathbb{Q}$, which contradicts Theorem 3 of [8] as it has a point of order 16.

Therefore, the only possibility is that $[\mathbb{Q}(2^{k-1}P):\mathbb{Q}]=3$, and so $[\mathbb{Q}(\langle P\rangle):\mathbb{Q}]=3$. Suppose for sake of contradiction that $k>1$, and consider the point $2^{k-2}P$ of order 4. Because $\langle 2^{k-2}P\rangle$ is defined over the field $\mathbb{Q}(\langle P\rangle)$, there exists a $\mathbb{Q}(\langle P\rangle)$-isogeny character $\chi$ associated to it. Let $\chi:\mathrm{Gal}(\overline{\mathbb{Q}(\langle P\rangle)}/\mathbb{Q}(\langle P\rangle)\to(\mathbb{Z}/4\mathbb{Z})^\times$, which has only two elements. Therefore, $|\operatorname{im}(\chi)|\leq|\{1,3\}|=2$, which implies that $[\mathbb{Q}(\langle P\rangle)(2^{k-2}P):\mathbb{Q}(\langle P\rangle])\leq 2$. Therefore, $[\mathbb{Q}(2^{k-2}P):\mathbb{Q}]\leq 6$.

The field over which a point of order 2 is defined and the field over which an isogeny is defined do not depend upon the equation of the elliptic curve, and so the case of $E'$ defined over a number field $F$ and the case of $E'$ defined over $\mathbb{Q}$ itself are equivalent. However, if $E'$ is defined over $\mathbb{Q}$, then because it has a point of order 2 in degree 3 and a point of order 4 in degree less than or equal to 6, then by the data for Corollaries 3.4 and 3.5 of [21] it has index $16, 8$, or 4. However, this implies the degree of $F$ is even by Proposition 3.2. Therefore $k=1$ and so $P$ has order 2.

However, that implies that the degree of $\hat{\phi}$ is 2, and so the degree of $\phi$ is 2. Therefore the order of $\phi(Q)$ is at least 8, and $\phi(Q)$ is defined over $F$ as both $Q$ and $\phi$ are. Thus $E'$ has a point of order 8 defined over a field of odd degree. Moreover, the point of order 2 generated by $\phi(Q)$ must be defined over a field of degree 3 as in the argument above. We've proven $[\mathbb{Q}(P):\mathbb{Q}]=3$. and so all points of order 2 generate an extension of degree 3. Therefore any $E''/\mathbb{Q}$ with $j(E'')=j(E')$, which must be isomorphic over a degree 2 extension of $F$, must have a point $R$ of order 4 defined over a field of degree dividing $2\cdot[F:\mathbb{Q}]$ and a point $2R$ of order 2 in degree 3. However, $\mathbb{Q}(2R)\subset\mathbb{Q}(R)$ and so note $[\mathbb{Q}(R):\mathbb{Q}(2R)]=1,2,$ or 4 by Proposition 4.6 of [22]. However, as it is contained in a field of degree $2\cdot$ odd, it must be 1 or 2. Therefore, $E''$ has a point of order 4 in degree dividing 6 and a point of order 2 in degree dividing 3, which is a contradiction as before. □

## 7. $\ell$-adic images of level $\ell$

**Proposition 7.1.** *Suppose $\ell$ is an odd prime. Let $E_0/\mathbb{Q}$ be a non-CM elliptic curve whose $\ell$-adic Galois representation has level $\ell$. Let $\mathcal{E}$ denote the corresponding geometric isogeny class. Then there exists $E'/\mathbb{Q}\in\mathcal{E}$ and a cyclic subgroup $C\leq E'$ of order $\ell$ such that $E'/C$ is a minimal torsion curve.*

*Proof.* If $\operatorname{im}\rho_{E_0,\ell}$ is surjective, this follows from Proposition 1.6 and the fact that $\deg(X_1(\ell^k)\to X_1(\ell))=\ell^{2k-2}$. If $E_0/\mathbb{Q}$ has a rational $\ell$-isogeny, then the result follow from Lemma 4.2 if $\ell\geq 5$ and the proof of Proposition 5.1 if $\ell=3$; see, specifically, cases 1 and 2.

If $E_0/\mathbb{Q}$ has no rational $\ell$-isogeny and $\operatorname{im}\rho_{E_0,\ell}$ is not surjective, then $\operatorname{im}\rho_{E_0,\ell^\infty}$ is the complete preimage of one of the following groups by Proposition 2.1 and one may check that $\operatorname{ord}_\ell([\mathrm{GL}_2(\mathbb{Z}_\ell):\operatorname{im}\rho_{E_0,\ell^\infty}])=1$. We will consider each case separately. We note that in each of these cases, no $E'\in\mathcal{E}$ with $j(E')\in\mathbb{Q}$ is a minimal torsion curve.

- $C_{ns}^+(\ell)$: This is a subgroup of size $2(\ell^2-1)$, and up to a choice of basis it contains all matrices
$$\begin{pmatrix}a&0\\0&a\end{pmatrix}, a\not\equiv 0 \pmod{\ell},$$
$$\begin{pmatrix}a&0\\0&-a\end{pmatrix}, a\not\equiv 0 \pmod{\ell}.$$
Since $\ell$ is odd, these matrices form a group of order $2(\ell-1)$. Its fixed field has size $\ell+1$, so over an extension of degree $\ell+1$, the curve $E_0$ attains two independent $\ell$-isogenies with kernels $C_1$ and $C_2$. Then by Proposition 2.2, the curve $E_0/C_1$ attains a point on $X_1(\ell)$ in degree dividing $(\ell+1)\cdot\varphi(\ell)/2=(\ell^2-1)/2$ and a point on $X_1(\ell^2)$ in degree dividing $(\ell+1)\cdot\varphi(\ell^2)/2=(\ell^2-1)\cdot\ell/2$. Since all points on $X_1(\ell)$ associated to $E_0$ have degree $(\ell^2-1)/2$, Proposition 1.6 shows $E_0/C_1$ is a minimal torsion curve.

- $\{a^3 : a \in C_{ns}(\ell)\} \cup \{\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right) \cdot a^3 : a \in C_{ns}(\ell)\}$: In this case, $\ell \equiv 2 \pmod 3$ and the image has size $2(\ell^2-1)/3$. Moreover, the image contains

$$\begin{pmatrix} a^3 & 0 \\ 0 & a^3 \end{pmatrix}, a \not\equiv 0 \pmod{\ell},$$

$$\begin{pmatrix} a^3 & 0 \\ 0 & -a^3 \end{pmatrix}, a \not\equiv 0 \pmod{\ell}.$$

  Note $a \mapsto a^3$ defines a homomorphism from $(\mathbb{Z}/\ell\mathbb{Z})^\times$ to itself, and the kernel has size 1 since no element of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ has order 3. (Indeed, $\ell - 1 \equiv 1 \pmod 3$, so 3 does not divide $\#(\mathbb{Z}/\ell\mathbb{Z})^\times$.) Thus this map is surjective, and every element of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ is of the form $a^3$. The fixed field of this group of matrices has degree $(\ell+1)/3$, and over this extension $E_0$ has two independent $\ell$-isogenies with kernels $C_1$ and $C_2$. By Proposition 2.2, the curve $E_0/C_1$ attains a point on $X_1(\ell)$ in degree dividing $\frac{(\ell+1)}{3} \cdot \frac{\varphi(\ell)}{2} = \frac{\ell^2-1}{6}$ and a point on $X_1(\ell^2)$ in degree dividing $\frac{(\ell+1)}{3} \cdot \frac{\varphi(\ell^2)}{2} = \frac{(\ell^2-1)\cdot\ell}{6}$. Since all points on $X_1(\ell)$ associated to $E_0$ have degree at least $(\ell^2-1)/6$, Proposition 1.6 shows $E_0/C_1$ is a minimal torsion curve.
- 13S4, 5S4: The curve $E_0$ attains two independent $\ell$-isogenies in degree 6 with kernels $C_1$ and $C_2$. By Proposition 2.2, the curve $E_0/C_1$ attains a point on $X_1(\ell)$ in degree dividing $6 \cdot \frac{\varphi(\ell)}{2} = 3(\ell-1)$ and a point on $X_1(\ell^2)$ in degree dividing $6 \cdot \frac{\varphi(\ell^2)}{2} = 3\ell(\ell-1)$. By Table 1 and 2 in [22] and Proposition 1.6, the elliptic curve $E_0/C_1$ is a minimal torsion curve.
- 7Ns, 7Ns.2.1, 7Ns.3.1, 5Ns, 5Ns.2.1, 3Ns: The curve $E_0$ picks up 2 independent $\ell$-isogenies in degree 2 with kernels $C_1$ and $C_2$. By Proposition 2.2, the curve $E_0/C_1$ attains a point on $X_1(\ell)$ in degree dividing $2 \cdot \frac{\varphi(\ell)}{2} = \ell - 1$ and a point on $X_1(\ell^2)$ in degree dividing $2 \cdot \frac{\varphi(\ell^2)}{2} = \ell(\ell-1)$. By Table 1 and 2 in [22] and Proposition 1.6, the elliptic curve $E_0/C_1$ is a minimal torsion curve. □

**Corollary 7.2.** *Suppose $\ell$ is an odd prime. Let $E_0/\mathbb{Q}$ be a non-CM elliptic curve, and let $\mathcal{E}$ denote the corresponding geometric isogeny class. If $\operatorname{ord}_\ell([\mathrm{GL}_2(\mathbb{Z}_\ell) : \operatorname{im}\rho_{E_0,\ell^\infty}]) \le 1$, then the least degree of any point on $X_1(\ell^k)$ associated to $E \in \mathcal{E}$ is*

$$\deg(x) \cdot \ell^{\max(0,2k-2-d)}$$

*for $x \in X_1(\ell)$ of least degree associated to $E_0$ or $E_0/C$ where $C$ is the kernel of a $\mathbb{Q}$-rational cyclic $\ell$-isogeny. In particular, if $E_0$ has no $\ell$-isogeny over $\mathbb{Q}$, then the latter case cannot occur and $x$ is associated to $E_0$.*

**Remark 7.3.** The expression for the least degree does not necessarily divide all degrees. For example, the proof of Proposition 7.1 shows that the least degree of a point on $X_1(7^k)$ associated to $E_0$ with $\operatorname{im}\rho_{E_0,7^\infty} = \pi^{-1}(7\mathrm{Ns})$ is $7^{\max(0,2k-3)} \cdot 6$. However, there is a point on $X_1(7)$ associated to $E_0$ of degree 9, and points on $X_1(7^k)$ lying above this point will not have degree divisible by $7^{\max(0,2k-3)} \cdot 6$.

## 8. CM Elliptic Curves

Let $K$ be an imaginary quadratic field, let $w = \#\mathcal{O}_K^\times$, and suppose $\ell$ is an odd prime. Let $E$ be an elliptic curve with CM by $\mathcal{O}_K$, and let $\mathcal{E}$ denote the set of all elliptic curves geometrically isogenous to $E$. In this section, we show that a minimal torsion curve exists for $\mathcal{E}$ if and only if $\ell$ is split in $K$. This builds on work of Bourdon and Clark [4, 5]. We consider separately the cases where $\ell$ is split, inert, or ramified in $K$. A key first step of the proof is to establish the best-possible divisibility conditions for degrees of points on $X_1(\ell^n)$ associated to elliptic curves in $\mathcal{E}$. These appear as Propositions 8.1, 8.2, and 8.4.

8.1. $\ell$ **split in** $K$**.**

**Proposition 8.1.** *Let $E$ be an $\mathcal{O}_K$-CM elliptic curve, where $\ell$ is an odd prime split in $K$. Then the least degree of a point on $X_1(\ell^n)$ associated to $E' \in \mathcal{E}$ is*

$$2 \cdot h_K \cdot \frac{\ell^{n-1}(\ell-1)}{w_K},$$

*and this is attained by $E$ itself. In other words, $E$ is a minimal torsion curve.*

*Proof.* That $E$ gives a point on $X_1(\ell^n)$ in this degree follows from [5, Theorem 6.2]; note that $\ell \neq 3$ if $\Delta = -3, -4$ by the assumption that $\ell$ is split in $K$. It remains to show this is the least possible degree among all $E' \in \mathcal{E}$. Since the endomorphism algebra is an isogeny invariant, any $E' \in \mathcal{E}$ has CM by an order in $K$. Since we already have the least degree for a point with CM by the maximal order, we will henceforth assume $E'$ has CM by an order in $K$ of conductor $\mathfrak{f} > 1$. For any point $x = [E', P'] \in X_1(\ell^n)$, by [4, Theorem 6.2] and [5, Theorem 4.1] we have

$$h_K \cdot \frac{\ell^{n-1}(\ell-1)}{2} \mid \deg(x).$$

If $\deg(x) = h_K \cdot \frac{\ell^{n-1}(\ell-1)}{2} \cdot d < 2 \cdot h_K \cdot \frac{\ell^{n-1}(\ell-1)}{w_K}$ for some $d \in \mathbb{Z}^+$, it must be that $d = 1$, $w_K = 2$, and

$$h_K \cdot \frac{\ell^{n-1}(\ell-1)}{2} = \deg(x).$$

This implies $[\mathbb{Q}(j(E')) : \mathbb{Q}] = h_K$. The degree of this extension is equal to the class number of the order $\mathcal{O}$, which in turn is equal to the following expression by [11, Corollary 7.24]

$$h(\mathcal{O}) = [\mathbb{Q}(j(E')) : \mathbb{Q}] = h_K \frac{2}{w_K} \mathfrak{f} \prod_{p \mid \mathfrak{f}} \left(1 - \left(\frac{\Delta_K}{p}\right) \frac{1}{p}\right). \tag{1}$$

Since $w_K = 2$, then $[\mathbb{Q}(j(E')) : \mathbb{Q}] = h_K$ implies $E'$ has CM by an order in K of conductor dividing 2. Since we have assumed $E'$ has CM by an order of conductor $\mathfrak{f} > 1$, we will suppose $E'$ has CM by the order in $K$ of conductor 2. By Equation 1, this can happen only if 2 is split in $K$. In particular, since we have assumed $\ell$ is odd, then $\mathfrak{f}$ is prime to $\ell$, and so we have a contradiction by [4, Theorem 6.2]. □

8.2. $\ell$ **inert in** $K$**.**

**Proposition 8.2.** *Let $E$ be an $\mathcal{O}_K$-CM elliptic curve, where $\ell$ is an odd prime inert in $K$. Then the least degree of a point on $X_1(\ell^n)$ associated to $E' \in \mathcal{E}$ is*

$$h_K \cdot \frac{\ell^{\lfloor 3(n-1)/2 \rfloor}(\ell^2-1)}{w_K}.$$

*This is attained by $E'$ with CM by an order in $K$ of conductor $\mathfrak{f} = \ell^{\lfloor n/2 \rfloor}$.*

*Proof.* Suppose $E'$ has CM by the order in $K$ of conductor $\mathfrak{f} = \ell^{\lfloor n/2 \rfloor}$. Note we can find such an $E'$ in $\mathcal{E}$, for, by example [36, §2.10]. Then by [5, Theorem 6.1,6.6], the point $x' \in X_1(\ell^n)$ of least degree associated to $E'$ has

$$\deg(x') = T(\mathcal{O}, \ell^n) \cdot h(\mathcal{O}),$$

where $T(\mathcal{O}, \ell^n)$ is as defined in [5, Theorem 4.1]. Evaluating $T(\mathcal{O}, \ell^n)$ via [5, Theorem 4.1] and replacing $h(\mathcal{O})$ with the formula in Equation 1 shows $\deg(x')$ is as in the theorem statement.

Now we will justify that this is the least possible degree of a point on $X_1(\ell^n)$ associated to any $E' \in \mathcal{E}$. Suppose $E' \in \mathcal{E}$ has CM by the order of conductor $\ell^d \mathfrak{f}'$ in $\mathcal{O}_K$ where $\ell \nmid \mathfrak{f}'$. If $d = 0$, then by [5, Theorem 4.1, Theorem 6.1] we have the least degree of a point on $X_1(\ell^n)$ associated to $E'$ is

$$h(\mathcal{O}) \cdot T(\mathcal{O}, \ell^n) \geq h_K \cdot \frac{\ell^{2n-2}(\ell^2-1)}{w_K} \geq h_K \cdot \frac{\ell^{\lfloor 3(n-1)/2 \rfloor}(\ell^2-1)}{w_K},$$

so we may henceforth assume $d > 0$. Then by [5, Theorem 4.1, Theorem 6.6] the least degree of a point on $X_1(\ell^n)$ associated to $E'$ is

$$\begin{aligned} h(\mathcal{O}) \cdot T(\mathcal{O}, \ell^n) &= h_K \frac{2}{w_K} \mathfrak{f} \prod_{p \mid \mathfrak{f}} \left(1 - \left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right) \frac{\tilde{T}(\mathcal{O}, \ell^n)}{2} \\ &\geq h_K \frac{1}{w_K} \ell^{d-1}\,(\ell+1)\,\varphi(\ell^n) \\ &= h_K \frac{1}{w_K} \ell^{n+d-2}(\ell^2-1). \end{aligned}$$

If $d > \lfloor n/2 \rfloor$, then this is greater than or equal to the degree given in the theorem statement. If $d = \lfloor n/2 \rfloor$, then if $\mathcal{O}'$ is the order of conductor $\ell^d$, [5, Theorem 4.1, Theorem 6.6] show the least degree is

$$h(\mathcal{O}) \cdot T(\mathcal{O}, \ell^n) \geq h(\mathcal{O}') \cdot T(\mathcal{O}', \ell^n),$$

and the same conclusion holds.

Finally, suppose $0 < d < \lfloor n/2 \rfloor$. Then $n > 2d$ and by [5, Theorem 4.1, Theorem 6.6] the least degree is

$$\begin{aligned} h(\mathcal{O}) \cdot T(\mathcal{O}, \ell^n) &= h_K \frac{2}{w_K} \mathfrak{f} \prod_{p \mid \mathfrak{f}} \left(1 - \left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right) \frac{\tilde{T}(\mathcal{O}, \ell^n)}{2} \\ &\geq h_K \frac{1}{w_K} \ell^{d-1}\,(\ell+1)\,\ell^{2n-2d-1}(\ell-1) \\ &= h_K \frac{1}{w_K} \ell^{2n-d-2}(\ell^2-1) \\ &\geq h_K \cdot \frac{\ell^{\lfloor 3(n-1)/2 \rfloor}(\ell^2-1)}{w_K}. \end{aligned}$$

□

**Corollary 8.3.** *Let $E$ be an $\mathcal{O}_K$-CM elliptic curve, where $\ell$ is an odd prime inert in $K$, and let $\mathcal{E}$ denote the geometric isogeny class of $E$. Then no minimal torsion curve exists.*

*Proof.* Suppose for the sake of contradiction that there exists a minimal torsion curve $E_{\min} \in \mathcal{E}$, with CM by the order $\mathcal{O}$ of conductor $f$ in $\mathcal{O}_K$. Then $j(E_{\min})$ generates an extension of degree at most $h_K \cdot \frac{\ell^2-1}{w_K}$, the least degree of a point on $X_1(\ell)$ for an elliptic curve in $\mathcal{E}$. Since $[\mathbb{Q}(j(E_{\min})) : \mathbb{Q}] = h(\mathcal{O})$ and by [11, Corollary 7.24]

$$h(\mathcal{O}) = h_K \frac{2}{w_K} f \prod_{p \mid f} \left(1 - \left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right),$$

we see that $\mathrm{ord}_\ell(f) \leq 1$. Then by [5, Theorem 6.1,6.6], the point $x \in X_1(\ell^4)$ of least degree associated to $E_{\min}$ has

$$\deg(x) = T(\mathcal{O}, \ell^n) \cdot h(\mathcal{O}) \geq h_K \cdot \frac{\ell^5(\ell^2-1)}{w_K},$$

where $T(\mathcal{O}, \ell^n)$ is as defined in [5, Theorem 4.1]. But this is greater than the least degree given in Proposition 8.2. □

8.3. $\ell$ **ramified in** $K$**.**

**Proposition 8.4.** *Let $E$ be an $\mathcal{O}_K$-CM elliptic curve, where $\ell$ is an odd prime ramified in $K$. Then the least degree of a point on $X_1(\ell^n)$ associated to $E' \in \mathcal{E}$ is*

$$h_K \cdot \frac{\ell^{\lfloor 3n/2 \rfloor - 1}(\ell - 1)}{w_K},$$

*unless $\ell^n = 3$ and $\Delta_K = -3$ in which case the least degree is 1. The least degree is attained by $E'$ with CM by an order in $K$ of conductor $\mathfrak{f} = \ell^{\lfloor n/2 \rfloor}$.*

*Proof.* Suppose $E'$ has CM by an order in $K$ of conductor $\mathfrak{f} = \ell^{\lfloor n/2 \rfloor}$. Note we can find such an $E'$ in $\mathcal{E}$, for, by example [36, §2.10]. Then by [5, Theorem 6.6] the least degree $x' \in X_1(\ell^n)$ associated to $E'$ is

$$\deg(x') = T(\mathcal{O}, \ell^n) \cdot h(\mathcal{O}),$$

where $T(\mathcal{O}, \ell^n)$ is as defined in [5, Theorem 4.1]. Evaluating $T(\mathcal{O}, \ell^n)$ via [5, Theorem 4.1] and replacing $h(\mathcal{O})$ with the formula in Equation 1 shows $\deg(x')$ is as in the theorem statement.

Now we will justify that this is the least possible degree of a point on $X_1(\ell^n)$ associated to any $E' \in \mathcal{E}$. Suppose $E' \in \mathcal{E}$ has CM by the order of conductor $\ell^d \mathfrak{f}'$ in $\mathcal{O}_K$ where $\ell \nmid \mathfrak{f}'$. If $d = 0$, then by [5, Theorem 4.1, Theorem 6.6] we have the least degree of a point on $X_1(\ell^n)$ associated to $E'$ is

$$h(\mathcal{O}) \cdot T(\mathcal{O}, \ell^n) \geq h_K \cdot \frac{\ell^{\lfloor 3n/2 \rfloor - 1}(\ell - 1)}{w_K},$$

so we may henceforth assume $d > 0$.

By [5, Theorem 4.1, Theorem 6.6] the least degree of a point on $X_1(\ell^n)$ associated to $E'$ is

$$\begin{aligned} h(\mathcal{O}) \cdot T(\mathcal{O}, \ell^n) &= h_K \frac{2}{w_K} \mathfrak{f} \prod_{p \mid \mathfrak{f}} \left(1 - \left(\frac{\Delta_K}{p}\right) \frac{1}{p}\right) \frac{\tilde{T}(\mathcal{O}, \ell^n)}{2} \\ &\geq h_K \frac{1}{w_K} \ell^d \varphi(\ell^n) \\ &= h_K \frac{1}{w_K} \ell^{n+d-1}(\ell - 1). \end{aligned}$$

For the sake of contradiction, suppose the least degree associated to $E'$ is less than value given in the theorem statement. Then in particular

$$h_K \frac{1}{w_K} \ell^{n+d-1}(\ell - 1) < h_K \cdot \frac{\ell^{\lfloor 3n/2 \rfloor - 1}(\ell - 1)}{w_K}.$$

This forces $d < \lfloor n/2 \rfloor$ and thus $n > 2d + 1$. But then by [5, Theorem 4.1, Theorem 6.6], the least degree of a point on $X_1(\ell^n)$ associated to $E'$ is

$$\begin{aligned} h(\mathcal{O}) \cdot T(\mathcal{O}, \ell^n) &= h_K \frac{1}{w_K} \mathfrak{f} \prod_{p \mid \mathfrak{f}} \left(1 - \left(\frac{\Delta_K}{p}\right) \frac{1}{p}\right) \tilde{T}(\mathcal{O}, \ell^n) \\ &\geq h_K \frac{1}{w_K} \ell^d \cdot \ell^{2n-2d-2}(\ell - 1) \\ &= h_K \frac{1}{w_K} \ell^{2n-d-2}(\ell - 1) \\ &\geq h_K \cdot \frac{\ell^{\lfloor 3n/2 \rfloor - 1}(\ell - 1)}{w_K}. \end{aligned}$$

□

**Corollary 8.5.** *Let $E$ be an $\mathcal{O}_K$-CM elliptic curve, where $\ell$ is an odd prime ramified in $K$, and let $\mathcal{E}$ denote the geometric isogeny class of $E$. Then no minimal torsion curve exists.*

*Proof.* Suppose for the sake of contradiction that there exists a minimal torsion curve $E_{\min} \in \mathcal{E}$, with CM by the order $\mathcal{O}$ of conductor $f$ in $\mathcal{O}_K$. Then $j(E_{\min})$ generates an extension of degree at most $h_K \cdot \frac{\ell-1}{w_K}$, the least degree of a point on $X_1(\ell)$ for an elliptic curve in $\mathcal{E}$. Since $[\mathbb{Q}(j(E_{\min})) : \mathbb{Q}] = h(\mathcal{O})$ and by [11, Corollary 7.24]

$$h(\mathcal{O}) = h_K \frac{2}{w_K} f \prod_{p|f} \left(1 - \left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right),$$

we see that $\mathrm{ord}_\ell(f) = 0$. Then by [5, Theorem 6.1,6.6], the point $x \in X_1(\ell^3)$ of least degree associated to $E_{\min}$ has

$$\deg(x) = T(\mathcal{O}, \ell^n) \cdot h(\mathcal{O}) \geq h_K \cdot \frac{\ell^4(\ell-1)}{w_K},$$

where $T(\mathcal{O}, \ell^n)$ is as defined in [5, Theorem 4.1]. But this is greater than the least degree given in Proposition 8.2. □

## 9. Appendix

Let $E_0/\mathbb{Q}$ have a rational cyclic $\ell$-isogeny $C$. By Theorem 3.32 and Tables 3 and 4 of [37], by replacing $E_0$ with $E_0/C$ if necessary, we may assume $E_0$ has mod $\ell$ image in the following list.

Table 1

| Image | degrees of points on $X_1(\ell)$ |
|---|---|
| 2B | 1,2 |
| 3B.1.1 | 1,3 |
| 3B | 1,3 |
| 5B.1.1 | 1,1, $10 = 5 \cdot 2$ |
| 5B.1.4 | 1,1, $10 = 5 \cdot 2$ |
| 5B.4.1 | 1,1, $10 = 5 \cdot 2$ |
| 5B | 2, $10 = 5 \cdot 2$ |
| 7B.1.1 | 1, 1, 1, $21 = 7 \cdot 3$ |
| 7B.1.2 | 3, $21 = 7 \cdot 3$ |
| 7B.1.6 | 1, 1, 1, $21 = 7 \cdot 3$ |
| 7B.6.1 | 1, 1, 1, $21 = 7 \cdot 3$ |
| 7B.6.2 | 3, $21 = 7 \cdot 3$ |
| 7B.2.1 | 3, $21 = 7 \cdot 3$ |
| 7B | 3, $21 = 7 \cdot 3$ |
| 11B.1.4 | 5, $55 = 11 \cdot 5$ |
| 11B.1.5 | 5, $55 = 11 \cdot 5$ |
| 11B.10.4 | 5, $55 = 11 \cdot 5$ |
| 13B.3.1 | 3, 3, $78 = 13 \cdot 6$ |
| 13B.3.4 | 3, 3, $78 = 13 \cdot 6$ |
| 13B.5.1 | 2, 2, 2, $78 = 13 \cdot 6$ |
| 13B.5.4 | 6, $78 = 13 \cdot 6$ |
| 13B.4.1 | 3, 3, $78 = 13 \cdot 6$ |
| 13B | 6, $78 = 13 \cdot 6$ |
| 17B.4.2 | 4, 4, $136 = 17 \cdot 8$ |
| 37B.8.1 | 6, 6, 6, $666 = 37 \cdot 18$ |

## References


1. Dan Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices (1996), no. 20, 1005–1011. 1.2
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 2.1
3. Burcu Baran, *An exceptional isomorphism between modular curves of level 13*, J. Number Theory **145** (2014), 273–300. MR 3253304 2.1
4. Abbey Bourdon and Pete L. Clark, *Torsion points and Galois representations on CM elliptic curves*, Pacific J. Math. **305** (2020), no. 1, 43–88. 8, 8.1, 8.1
5. ———, *Torsion points and isogenies on CM elliptic curves*, J. Lond. Math. Soc. (2) **102** (2020), no. 2, 580–622. 1, 8, 8.1, 8.2, 8.2, 8.3, 8.3
6. 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. 2.2
7. 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. 5.1
8. Abbey Bourdon, David Gill, Jeremy Rouse, and Lori D. Watson, *Odd degree isolated points on $x_1(n)$ with rational j-invariant*, preprint, available at arxiv.org:2006.14966. 6
9. Abbey Bourdon and Filip Najman, *Sporadic points of odd degree on $X_1(N)$ coming from $\mathbb{Q}$-curves*, preprint, available at arxiv.org:2107.10909. 1, 1, 1.1, 1.2, 1, 1, 2.3, 3.2, 3.2, 4, 4.2, 5.1, 6
10. Pete L. Clark, *CM elliptic curves: volcanoes, reality, and applications*, preprint, available at `http://alpha.math.uga.edu/~pete/Isogenies.pdf`. 3, 3.1, 3.1, 3.3
11. 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. 8.1, 8.2, 8.3
12. J. E. Cremona and Filip Najman, *$\mathbb{Q}$-curves over odd degree number fields*, Res. Number Theory **7** (2021), no. 4, Paper No. 62, 30. MR 4314224 1, 3, 3.1, 3.1, 3.3, 4.2, 5.2, 6
13. 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 1
14. P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973, pp. 143–316. MR 0337993 2.3, 2.3
15. 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 2.3
16. Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005. 2.3, 2.3
17. Özlem Ejder, *Isolated points on $X_1(\ell^n)$ with rational j-invariant*, Res. Number Theory **8** (2022), no. 1, Paper No. 16, 7. MR 4392066 1.2
18. Gerhard Frey, *Curves with infinitely many points of fixed degree*, Israel J. Math. **85** (1994), no. 1-3, 79–83. 1.2
19. Tyler Genao, *Typically bounding torsion on elliptic curves isogenous to rational j-invariant*, preprint, available at arxiv.org:2112.11566. 1
20. Enrique González-Jiménez, *Complete classification of the torsion structures of rational elliptic curves over quintic number fields*, J. Algebra **478** (2017), 484–505. MR 3621686 1
21. Enrique González-Jiménez and Álvaro Lozano-Robledo, *On the minimal degree of definition of p-primary torsion subgroups of elliptic curves*, Math. Res. Lett. **24** (2017), no. 4, 1067–1096. 6
22. Enrique González-Jiménez and Filip Najman, *Growth of torsion groups of elliptic curves upon base change*, Math. Comp. **89** (2020), no. 323, 1457–1485. MR 4063324 1, 2.1, 2.1, 2.1, 4.2, 6, 7
23. R. Greenberg, K. Rubin, A. Silverberg, and M. Stoll, *On elliptic curves with an isogeny of degree 7*, Amer. J. Math. **136** (2014), no. 1, 77–109. 4.1, 4.1
24. Ralph Greenberg, *The image of Galois representations attached to elliptic curves with an isogeny*, Amer. J. Math. **134** (2012), no. 5, 1167–1196. 4.1, 4.1
25. Hans Heilbronn, *On the class-number in imaginary quadratic fields*, The Quarterly Journal of Mathematics **os-5** (1934), no. 1, 150–160. 3.3
26. Andrew V. Sutherland Jeremy Rouse and David Zureick-Brown, *$\ell$-adic images of Galois for elliptic curves over $\mathbb{Q}$*, to appear in Forum Math. Sigma, available at arXiv:2106.11141. 1, 2.1, 5.2
27. Álvaro Lozano-Robledo, *Galois representations attached to elliptic curves with complex multiplication*, preprint, available at arXiv:1809.02584. 1, 2.1

28. ———, *On the field of definition of p-torsion points on elliptic curves over the rationals*, Math. Ann. **357** (2013), no. 1, 279–305. 1
29. B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978). 1, 6
30. L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees.*, Proc. Camb. Philos. Soc. **21** (1922), 179–192. 1
31. F. 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. 1
32. 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. 1, 2.1
33. Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. 1, 3.3
34. 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. 2.3, 2.3
35. Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. 2.3
36. Andrew V. Sutherland, *Isogeny volcanoes*, ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 1, Math. Sci. Publ., Berkeley, CA, 2013, pp. 507–530. MR 3207429 8.2, 8.3
37. ———, *Computing images of Galois representations attached to elliptic curves*, Forum Math. Sigma **4** (2016), e4, 79. 1, 2.1, 2.1, 3.2, 9
38. 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. 1, 2.1
39. David Zywina, *On the possible image of the mod* $\ell$ *representations associated to elliptic curves over* $\mathbb{Q}$, available at arxiv.org:1508.07660. 1, 2.1
40. ———, *On the possible images of the mod* $\ell$ *representations associated to elliptic curves over* $\mathbb{Q}$, preprint, submitted (https://arxiv.org/abs/1508.07660). 2.1

Wake Forest University, Winston-Salem, NC 27109, USA
*Email address*: bourdoam@wfu.edu
*URL*: http://users.wfu.edu/bourdoam/

University of Georgia, Athens, GA 30602 USA
*Email address*: Nina.Ryalls@uga.edu

Trinity College, Hartford, CT 06106 USA
*Email address*: lori.watson@trincoll.edu
*URL*: https://loridwatson.com