ON THE FINITENESS OF ISOLATED j-INVARIANTS FOR $X_1(N)$

ABBEY BOURDON

ABSTRACT. Characterizing isolated points on the modular curve $X_1(N)$ is a key obstruction to classifying all points of a fixed degree. These points do not lie in infinite parameterized families, making them difficult to obtain through geometric constructions. In this paper, we focus on the collection of "isolated j-invariants" for $X_1(N)$, which are the values obtained by mapping isolated points to the j-line. Work of the author in collaboration with Ejder, Liu, Odumodu, and Viray [10] asks whether there are only finitely many isolated j-invariants lying in extensions of bounded degree. Here, we explore how this question relates to other uniformity problems in the field and demonstrate the extent to which current techniques imply finiteness of isolated j-invariants in $\mathbb{Q}$. As an application, we show similar methods give sharpened polynomial bounds on torsion for elliptic curves having rational j-invariant.

1. Introduction

The modular curve $X_1(N)$ is a smooth projective curve over $\mathbb{Q}$ whose (non-cuspidal) points parametrize elliptic curves with a distinguished point of order N. A classical problem is to characterize the K-rational points of $X_1(N)$ for a fixed number field K. For $K = \mathbb{Q}$, this was done by Mazur, confirming a conjecture of Ogg [48]. The classification shows $X_1(N)(\mathbb{Q})$ has a non-cuspidal point if and only if the curve has genus 0. That is, these points are "explained by geometry."

Theorem 1 (Mazur [42])**.** *$X_1(N)$ has a non-cuspidal rational point if and only if $1 \leq N \leq 10$ or $N = 12$.*

By Merel's uniform boundedness theorem [45], we now know that for a fixed degree d there are only finitely many modular curves $X_1(N)$ with a non-cuspidal degree d point. Thus a modern take on the classical classification problem is to determine the N for which $X_1(N)$ admits a non-cuspidal degree d point. This is known for $d \leq 4$ [42, 37, 35, 22, 23]. In degree 2, we again find that a non-cuspidal point exists on $X_1(N)$ only when it belongs to an infinite parameterized family: if it has positive genus, then $X_1(N)$ has a non-cuspidal quadratic point only when it arises from a degree 2 map to $\mathbb{P}^1$. However, for $d > 2$, an essential challenge to classifying degree d points on $X_1(N)$ is the need to control torsion structures that occur for only finitely many elliptic curves. Explicit examples of these exceptional points are known for $d = 3$ and $5 \leq d \leq 13$, as discussed in [23, Appendix A], as well as many other suspected examples of higher degree.

In general, if a closed point does not belong to a infinite parameterized family of points of the same degree, we say it is **isolated**; see Section 2.3 for a more precise definition. The problem of classifying degree d isolated points is the only obstruction to extending the classification of degree d points on $X_1(N)$ for $5 \leq d \leq 9$ by [24, Theorem 3] and [47, Theorem 1.1]. Though any curve has only finitely many isolated points, it can be quite difficult to determine them computationally, especially when the curve's Jacobian has positive rank. Indeed, if the genus of a curve is at least 2, then in particular all rational points are isolated, and this set can be notoriously difficult to compute. However, in the case of modular curves, we can use the moduli interpretation to pose new questions about these mysterious points.

One line of investigation first introduced by the author in collaboration with Ejder, Liu, Odumodu, and Viray [10] is the problem of classifying the elliptic curves which give rise to isolated points. We say $j \in X_1(1)$ is an **isolated j-invariant** if there exists an isolated point $x \in X_1(N)$ with $j(x) = j$ under the natural map $j : X_1(N) \to X_1(1)$.[1] The **degree** of an isolated j-invariant is the degree of its residue field $\mathbb{Q}(j)$. For example, the modular curve $X_1(21)$ has 2 isolated points of degree 3 as discovered by Najman [46], each associated to an elliptic curve with j-invariant $-140625/8$. Thus $-140625/8$ is an isolated j-invariant of degree 1. Since the degree of the residue field of a closed point on $X_1(N)$ is determined by an elliptic curve defined over $\overline{\mathbb{Q}}$, it is enough to consider elliptic curves up to geometric isomorphism.

[1] Note j is not itself an isolated point on $X_1(1) \cong \mathbb{P}^1$, which has no isolated points.

One subset of isolated j-invariants that is relatively well understood are the CM j-invariants, which correspond to elliptic curves with complex multiplication. Any CM j-invariant gives rise to isolated points on $X_1(N)$ for infinitely many integers N by [10, Theorem 7.1], and conversely any $X_1(N)$ for $N \geq 721$ has an isolated CM point [16, Theorem 8.2]. However, many non-CM isolated j-invariants are known. We summarize low degree examples in Table 1, where $r(k)$ indicates there are k closed points of degree r. This is largely based on van Hoeij's table of low degree points [61], and we provide full justification in Section 6. The 4 non-CM isolated j-invariants in $\mathbb{Q}$ are conjectured to be the only ones [12, 60].

d	**# non-CM degree d isolated j-invariants**	**Curves**	**Degrees of associated isolated points**
1	4	$X_1(21), X_1(28), X_1(37)$	3, 9, 6 & 18
2	1	$X_1(34)$	8
3	4	$X_1(25), X_1(31), X_1(39), X_1(42)$	6, 9, 9, 9
4	6	$X_1(33), X_1(34), X_1(35), X_1(39), X_1(40), X_1(42)$	8, 8, 8, 12, 8, 8
5	5	$X_1(28), X_1(29), X_1(30), X_1(40)$	5, 10, 5(2), 10
6	2	$X_1(39)$	12(2)
7	4	$X_1(25), X_1(33), X_1(36)$	7, 7, 7(2)
8	2	$X_1(42)$	8(2)
9	15	$X_1(29), X_1(32), X_1(33), X_1(34), X_1(40)$	9, 9(8), 9, 9(4), 9
10	8	$X_1(29), X_1(35), X_1(38), X_1(39), X_1(40)$	10, 10(2), 10(3), 10, 10

TABLE 1. Known non-CM isolated j-invariants of degree ≤ 10.

As consequence of Merel's uniform boundedness theorem [45], there are only finitely many non-cuspidal isolated points of fixed degree d on $X_1(N)$ as N ranges over all integers. However, this does not imply finiteness of isolated j-invariants of degree d. Thus we can pose a new uniformity problem.

Question 1 (Bourdon, Ejder, Liu, Odumodu, Viray [10])**.** *Are there only finitely many isolated j-invariants of each fixed degree?*

In this article, we will explain how Question 1 relates to other uniformity problems in the literature and provide new results in the case of elliptic curves with rational j-invariant.

1.1. **Relation to Other Uniformity Questions.** There are a number of other hypotheses one can make concerning the uniformity of Galois representations of elliptic curves over number fields of a fixed degree. Recall $X_0(N)$ is the smooth projective curve over $\mathbb{Q}$ whose non-cuspidal points correspond to elliptic curves with a rational cyclic isogeny of degree N.

Hypothesis 1. *For each $d \in \mathbb{Z}^+$, there exists $C = C(d)$ such that for all non-CM elliptic curves E defined over number fields of degree d and $p > C$, the p-adic Galois representation of E contains $\mathrm{SL}_2(\mathbb{Z}_p)$.*

Hypothesis 2. *For each $d \in \mathbb{Z}^+$, there are only finitely many isolated j-invariants of degree d.*

Hypothesis 3. *For each $d \in \mathbb{Z}^+$, there exists an $C = C(d)$ such that for all $N > C$, the modular curve $X_0(N)$ has no non-cuspidal, non-CM points of degree d.*

Hypothesis 4. *For each $d \in \mathbb{Z}^+$, there exists $C = C(d)$ such that for all non-CM elliptic curves E defined over a number field F with $[\mathbb{Q}(j(E)) : \mathbb{Q}] = d$ we have $\exp E(F)_{\mathrm{tors}} \leq C \cdot [F : \mathbb{Q}]^{1/2}$ and $\#E(F)_{\mathrm{tors}} \leq C \cdot [F : \mathbb{Q}]$.*

When $d = 1$, these hypotheses are all established conjectures or theorems. In this case, Hypothesis 1 is often referred to as "Serre's Uniformity Conjecture", though it was a question of Serre [52, §4.3] which has since been conjectured by both Sutherland [59] and Zywina [63]. Hypothesis 3 for $d = 1$ is a theorem of

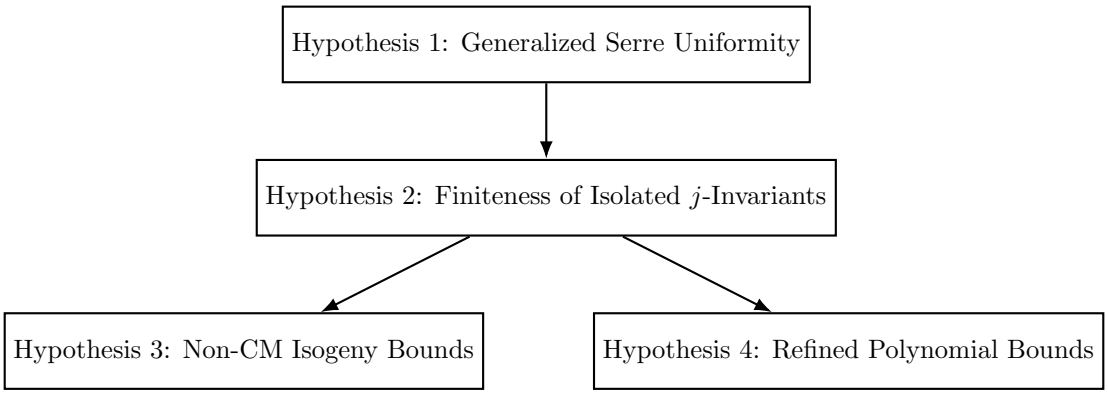

FIGURE 1. Implications Among Hypotheses (Theorem 9)

Mazur [44] and Kenku [36], and we can take $C = 37$. Variants of Hypothesis 4 originate with Clark and Pollack [17, Conjecture 1.4], though the exponent is not specified. It refines various "folklore" polynomial bounds conjectures appearing in the literature (e.g., [15, Conjecture 1]). Prior work of the author and Genao [11] shows $\exp E(F)_{\text{tors}} \leq C_\epsilon \cdot [F : \mathbb{Q}]^{1+\epsilon}$ when $d = 1$.

For $d > 1$, less has been formally conjectured, aside from Hypothesis 4 in [17, Conjecture 1.4], and Hypothesis 3 in the case where $d = 2$ as in [2, Conjecture 1.1] and [6, Conjecture 18]. We note that the statement of Hypothesis 1 was suggested as a possible generalization of Serre's Uniformity Conjecture by Derickx [21], and Hypothesis 3 would imply an affirmative answer to a question of Mazur [43, Question C]; see also Hypothesis SI(d) in [17]. However, in this paper we establish general implications between these hypotheses, as illustrated in Figure 1. This is proven in Theorem 9, with the implication from Hypothesis 1 to Hypothesis 2 coming from [10]. Thus we can view Question 1 as a refinement of Hypotheses 3 and 4 which lacks the full strength of generalized Serre uniformity.

Remark 2. If C is taken to be an absolute constant in Hypothesis 4, this would actually imply Hypothesis 1, as shown in §7. Also, [17, Theorem 1.7] states Hypothesis 3 implies a weaker version of Hypothesis 4. However, this proof relies on [41, Theorem 1.2], which contains an error. See [57, §1] for details.

1.2. **Unconditional Progress for Rational j-invariants.** Though Serre's Uniformity Conjecture is still open, we have partial classification results concerning the image of p-adic Galois representations associated to non-CM elliptic curve over $\mathbb{Q}$. As shown by Ejder [26], these are strong enough to imply there are no non-CM isolated points $x \in X_1(p^a)$ with $j(x) \in \mathbb{Q}$ and $p > 37$. Thus extending unconditional results requires controlling possible "entanglement" of torsion point fields associated to distinct primes. Of key importance are criteria which imply for $x \in X_1(N)$ with large prime $p \mid N$ that the residue field contribution at p is nearly as large as it can be. We establish a new result of this form in Corollary 1, which improves [11, Proposition 5]. When combined with work of Lemos [38, 39], this is sufficient to obtain our next result.

Theorem 3. *There are only finitely many rational isolated j-invariants associated to $X_1(p^a q^b)$ for primes p, q and non-negative integers a, b.*

The same ingredients bring us closer to establishing Hypothesis 4 for elliptic curves with rational j-invariants. Our final main result improves bounds of the first author and Genao [11, Theorem 2] by a square root factor of the degree as well as earlier bounds of Clark and Pollack [17, Theorem 1.3].

Theorem 4. *For any $\epsilon > 0$, there exists a constant C_ϵ such that for all non-CM elliptic curves E/F with $j(E) \in \mathbb{Q}$ we have $\exp E(F)_{\text{tors}} \leq C_\epsilon \cdot [F : \mathbb{Q}]^{1/2+\epsilon}$ and $\#E(F)_{\text{tors}} \leq C_\epsilon \cdot [F : \mathbb{Q}]^{1+\epsilon}$.*

The exponent bound is nearly optimal, in that the $1/2$ cannot be replaced by anything smaller. This follows, for example, from the fact that any elliptic curve over $\mathbb{Q}$ attains a point of prime order p in as extension of degree at most $p^2 - 1$. Moreover, this is the first bound on the exponent which is too small to permit the inclusion of CM elliptic curves. As shown in the proof of [15, Theorem 6], if $E/\mathbb{Q}$ is an elliptic curve with CM by $\mathbb{Q}(\sqrt{-3})$, then there exists a sequence of fields F_n of degree d_n such that $\exp(E(F_n)_{\text{tors}}) \gg d_n \sqrt{\log \log d_n}$.

1.3. **Future Work.** Though our control on entanglement is not sufficient to prove Hypothesis 2 unconditionally for rational j-invariants, experimental data suggests the problem may be accessible to certain formal immersion techniques. Indeed, a primary obstruction to proving Serre's Uniformity Conjecture is that the associated modular curves lack a nontrivial rank 0 quotient. However, the "entanglement modular curves" relevant to strengthening Corollary 1 often possess a such a quotient. See Remark 11.

Acknowledgments

The author is grateful to Pete Clark, Sachi Hashimoto, Filip Najman, and Paul Pollack for providing many helpful comments on an earlier draft of this work. In particular, Clark's suggestion to use upper bounds on $\omega(N)$ greatly streamlined the original proof of Theorem 4.

The author was partially supported by NSF grant DMS-2145270.

2. Background

2.1. **Galois Representations of Elliptic Curves.** If an elliptic curve E is defined over a number field k, then the absolute Galois group of k acts naturally on $E(\overline{k})$. For points of finite order, this action is encoded in the **adelic Galois representation** associated to E. After choosing compatible bases, this can be represented as

$$\rho_E : \mathrm{Gal}_k \to \mathrm{GL}_2(\widehat{\mathbb{Z}}) \cong \prod_p \mathrm{GL}_2(\mathbb{Z}_p).$$

For any positive integer m, we can compose ρ_E with projection onto the p-adic factors for $p \mid m$, giving the the m**-adic representation**,

$$\rho_{E,m^\infty} : \mathrm{Gal}_k \to \prod_{p \mid m} \mathrm{GL}_2(\mathbb{Z}_p).$$

Alternatively, we can reduce ρ_E modulo m to obtain the **mod** m **Galois representation**. This gives the Galois action on points of E with order dividing m:

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

Serre's Open Image Theorem [52] implies that for a fixed non-CM elliptic curve E/k, there exists a constant $C = C(E)$ depending on E such that the mod p Galois representation is surjective for primes $p > C$. It is interesting to determine the proper subgroups that can occur as mod p images of Galois as E ranges over all elliptic curves defined over k. If $k = \mathbb{Q}$ and $p \leq 17$, the groups that can occur as $\operatorname{im} \rho_{E,p}$ are known; this is work of Zywina [63] for $p \leq 11$ and Balakrishnan, Dogra, Müller, Tuitman, and Vonk [3, 5] for $p = 13, 17$. In this paper, we use the labels of Sutherland [59] to refer these subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ that arise as $\operatorname{im} \rho_{E,p}$. For larger primes, we have the following result. Here, $C_{ns}^+(p)$ denotes the normalizer of a non-split Cartan subgroup.

Theorem 5 (Mazur [44], Serre [53], Bilu, Parent, Rebolledo [7], Furio, Lombardo [31])**.** *Let $E/\mathbb{Q}$ be a non-CM elliptic curve with $j(E) \notin \{-9317, -162677523113838677\}$. If $p \geq 19$ is prime, then $\operatorname{im} \rho_{E,p} = \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ or $C_{ns}^+(p)$.*

The exceptional j-invariants are associated to elliptic curves with a rational cyclic 37-isogeny. For any elliptic curve $E/\mathbb{Q}$ with $j(E) \in \{-9317, -162677523113838677\}$ and $p > 37$, the associated mod p Galois representation is surjective.

Serre's Uniformity Conjecture states that there exists a single constant C such that $\rho_{E,p}$ is surjective for all non-CM $E/\mathbb{Q}$ and primes $p > C$. This is still an open problem, with Theorem 5 summarizing the progress to date. By contrast, for any fixed positive integer m, there exist strong uniformity results for the level of the m-adic Galois representations of non-CM elliptic curves defined over number fields of a fixed degree. Here, the **level** of the m-adic Galois representation is defined to be the smallest positive integer M such that $\operatorname{im} \rho_{E,m^\infty} = \pi^{-1}(\operatorname{im} \rho_{E,M})$, where $\pi : \mathrm{GL}_2(\mathbb{Z}_m) \to \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ is the natural reduction map.

Theorem 6 ([14, 10])**.** *Let d be a positive integer and $\mathcal{E}$ a set of non-CM elliptic curves over number fields of degree at most d. Then for any positive integer m, there exists a positive integer M with $\mathrm{Supp}(M) \subset \mathrm{Supp}(m)$ such that for all $E/k \in \mathcal{E}$ we have*

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

Proof. If m is a power of a single prime, this is [14, Theorem 1.1]. The proof of the general statement is given in [10, Proposition 6.1]. □

In particular, for a fixed prime p, there are only finitely many groups that can occur as $\operatorname{im}\rho_{E,p^\infty}$ for all non-CM elliptic curves defined over number fields of a fixed degree. In the case of non-CM elliptic curves over $\mathbb{Q}$, the classification of p-adic images is complete for $p = 2, 3, 13$ and 17 by [51, 50, 4]. Throughout, we use the labels introduced by Rouse, Sutherland, and Zureick-Brown [50] to refer subgroups of $\mathrm{GL}_2(\mathbb{Z}_p)$ which can arise as $\operatorname{im}\rho_{E,p^\infty}$ for non-CM elliptic curves $E/\mathbb{Q}$. These labels are of the form `N.i.g.n`, where N denotes the level, i denotes group index in $\mathrm{GL}_2(\mathbb{Z}_p)$, g denotes the genus of the associated modular curve, and n distinguishes groups with the same values for N, g, i.

2.2. **Modular Curves.** The modular curve $Y_1(N)$ is an affine curve over $\mathbb{Q}$ whose k-rational points correspond to elliptic curves E/k with a point $P \in E(k)$ of order N. If $N \geq 4$, then $Y_1(N)(k)$ is in bijection with k-isomorphism classes of such pairs, $(E, P)_k$. Taking the projective closure of $Y_1(N)$ adds a finite number of cusps, which do not correspond to elliptic curves, resulting in the smooth projective curve $X_1(N)$. Throughout we view $X_1(N)$ as a curve defined over $\mathbb{Q}$.

If $x \in X_1(N)$ is a closed point, then its **degree** is defined to be the degree of its residue field, denoted $\mathbb{Q}(x)$. It is also the length of the Galois orbit of the point in $X_1(N)(\overline{\mathbb{Q}})$ corresponding to x. Note that if E/k is an elliptic curve with $P \in E(k)$ of order N, then the degree of the associated closed point $x = [E, P] \in X_1(N)$ may be less than the degree of k. However, there is always E' with $j(E') = j(E)$ which is defined over $\mathbb{Q}(x)$ and has a $\mathbb{Q}(x)$-rational point of order N. For more details, see [40, §3.2.3] and [20, p. 274, Proposition VI.3.2]. Explicit examples illustrating the distinction between closed points, k-rational points, and geometric points of $X_1(N)$ can be found in [12, §2.3].

We define the modular curve $X_0(N)$ in an analogous way. There is an affine curve $Y_0(N)$ over $\mathbb{Q}$ whose k-rational points correspond to elliptic curves E/k with a k-rational isogeny $\varphi : E \to E'$ which is cyclic of degree N. Since k-rational cyclic N-isogenies from E/k are in bijection with k-rational cyclic subgroups of E of order N, this provides an alternate moduli interpretation for the points of $Y_0(N)$. Taking the projective closure of $Y_0(N)$ gives the modular curve $X_0(N)$. Unlike $X_1(N)$ for $N \geq 4$, the curve $X_0(N)$ is not a fine moduli space.

We often make use of the following well-known degree formulas for maps between modular curves.

Proposition 1. *For positive integers a and b, there is a natural $\mathbb{Q}$-rational map $f\colon X_1(ab) \to X_1(a)$ sending $[E, P]$ to $[E, bP]$ with*

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

Here, $c_f = 1/2$ if $a \leq 2$ and $ab > 2$ and $c_f = 1$ otherwise. Similarly, there is a natural $\mathbb{Q}$-rational map $g : X_0(ab) \to X_0(a)$ sending $[E, \langle P\rangle]$ to $[E, \langle bP\rangle]$ with

$$\deg(g) = b \prod_{p \mid b, p \nmid a} \left(1 + \frac{1}{p}\right).$$

Proof. The degree computations follow from [25, p.66]. □

2.3. **Isolated Points.** Let C/k be a nice curve over a number field, i.e., that is smooth, projective, and geometrically integral. Assume for simplicity that $P_0 \in C(k)$; for a more general setup, see [10, §4] or [62]. Then there is a natural map from from the dth symmetric product of C to the curve's Jacobian,

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

defined by sending an effective degree d divisor D to the class $[D - dP_0]$. By identifying a degree d closed point $x \in C$ with the sum of its associated Galois conjugates, we may view x as an element of $\mathrm{Sym}^d(C)(k)$.

Let $x \in \mathrm{Sym}^d(C)(k)$ be a degree d closed point. Then:

- We say x is **$\mathbb{P}^1$-parameterized** if $\Phi(x) = \Phi(y)$ for some $y \in \mathrm{Sym}^d(C)(k)$ with $y \neq x$. In this case, there exists a degree d map $f : C \to \mathbb{P}^1$ with $x \in f^{-1}(\mathbb{P}^1(k))$.
- We say x is **AV-parameterized** if there exists a positive rank abelian subvariety A/k of $\mathrm{Jac}(C)$ with $\Phi(x) + A \subseteq \mathrm{im}(\Phi)$.

- If x is neither $\mathbb{P}^1$-parameterized nor AV-parameterized, then it is **isolated**.
- If there are only finitely many points of degree at most $\deg(x)$, then x is **sporadic**.

By the Riemann-Roch Theorem, any isolated point has degree at most the genus of C. Since degree d points that are *not* $\mathbb{P}^1$-parameterized map injectively into $\mathrm{Jac}(C)(k)$, it is a consequence of a theorem of Faltings [27] that there are only finitely many isolated points of any fixed degree. Taken together, these imply C has only finitely many isolated points of any degree. Moreover, any parameterized point gives an infinite family of points of the same degree. For $\mathbb{P}^1$-parameterized points, this is Hilbert's Irreducibility Theorem [54, Chapter 9]. For AV-parameterized which are $\mathbb{P}^1$-isolated, this is proven in [10, Theorem 4.2], but see [62, Proposition 4.3.5] for a more self-contained reference. We summarize this in the theorem below.

Theorem 7 (Faltings [27], Bourdon, Ejder, Liu, Odumodu, Viray [10])**.**

(1) There are only finitely many isolated points on C.

(2) There are infinitely many degree d points if and only if there is a degree d parameterized point.

In particular, every sporadic point is isolated, but the converse need not hold.

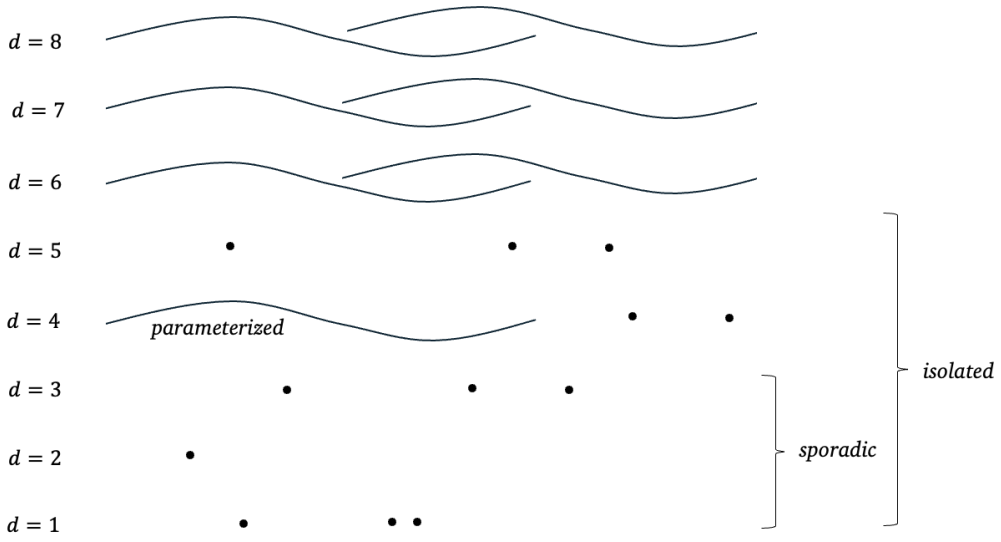

FIGURE 2. A hypothetical curve of genus 7 with points of degree d.

We will often make use of the following result which allows one to show the image of an isolated point is isolated under certain conditions.

Theorem 8 (Bourdon, Ejder, Liu, Odumodu, Viray [10])**.** *Let $f : C \to D$ be a finite map of curves, and let $x \in C$ be an isolated point. If*

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

then $f(x) \in D$ is isolated.

3. Implications Among Hypotheses

In this section, we prove the following implications among Hypotheses 1-4, as summarized in Figure 1.

Theorem 9. *Let Hypotheses 1-4 as in* §1.1*. Then:*

- [10, Corollary 1.7] *Hypothesis 1 implies Hypothesis 2.*
- *Hypothesis 2 implies Hypothesis 3 and Hypothesis 4.*

We note that [10, Corollary 1.7] as stated relies on a stronger conjecture than Hypothesis 1. As pointed out by Derickx [21], the statement of [10, Corollary 1.4] actually fails to hold over general number fields. However, the proof that Hypothesis 1 implies Hypothesis 2 still follows directly from the arguments found in [10]. Indeed, suppose Hypothesis 1 holds for $d \in \mathbb{Z}^+$. Let m be the product of 2, 3, 5, and all primes p

with $p \leq C(d)$, and fix M as in Theorem 6 for $\mathcal{E}$ the set of all non-CM elliptic curves over number fields of degree d. Let $x \in X_1(N)$ be a non-cuspidal isolated point with $j(x)$ of degree d. Since there are only finitely many CM j-invariants of degree d, we may assume $j(x)$ is non-CM. Let $E/\mathbb{Q}(j(E))$ be an elliptic curve with $j(x) = j(E)$. Then by [10, Theorem 5.1], we have

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

where $f : X_1(N) \to X_1(\gcd(N, M))$ is the natural map. By Theorem 8, the point $f(x)$ is isolated, and each modular curve $X_1(a)$ for $a \mid M$ has only finitely many isolated points by Theorem 7. The result follows.

It remains to prove Hypothesis 2 implies Hypotheses 3 and 4, which we do in §3.1 and §3.3, respectively.

3.1. **Implication for Hypothesis 3.** Here we prove that Hypothesis 2 implies Hypothesis 3.

Proposition 2. *Suppose there are only finitely many isolated j-invariants of degree d for each $d \in \mathbb{Z}^+$. Then for each d there exists a $C = C(d)$ such that for all $N > C$, the modular curve $X_0(N)$ has no non-cuspidal, non-CM points of degree d.*

Proof. Let $x \in X_0(N)$ be a non-cuspidal, non-CM point of degree d. If $N \geq 3$, then x lifts to a point $x' \in X_1(N)$ with $\deg(x') \leq d \cdot \varphi(N)/2$, where φ denotes the Euler φ-function. For sufficiently large N, lower bounds on gonality due to Abramovich [1, Theorem 0.1] imply $\deg(x') < \frac{1}{2}\operatorname{gon}_{\mathbb{Q}}(X_1(N))$. Thus x' is sporadic — and hence isolated – by work of Frey [29, Proposition 2]. By assumption, there are only finitely many isolated j-invariants of each degree and $\deg(j(x')) \leq d$, so $j(x')$ belongs to a finite set. By Serre's Open Image Theorem [52], each $j(x')$ gives a degree d point on $X_0(N)$ for at most finitely many integers N. The result follows. □

Remark 10. In fact, it is enough to assume Hypothesis 2 for modular curves of prime level. Indeed, suppose there are only finitely many isolated j-invariants of degree d associated to modular curves $X_1(p)$ as p ranges over all prime numbers. Then the proof of Proposition 2 shows the modular curve $X_0(p)$ has no non-cuspidal, non-CM points of degree d for sufficiently large primes p. Hypothesis 3 now follows from Theorem 6.

3.2. **Preliminary Lower Bounds.** We record the following technical lemma in more generality than is needed here so it can be applied later in the proof of Theorem 4.

Lemma 1. *Fix $d \in \mathbb{Z}^+$, and let $\mathcal{E}$ be a collection of non-CM elliptic curves such that each $E \in \mathcal{E}$ is defined over $\mathbb{Q}(j(E))$ with $[\mathbb{Q}(j(E)) : \mathbb{Q}] = d$. Let S be a finite list of primes. Then there exists a constant $C = C(d)$ such that for any $x \in X_1(N)$ associated to $E \in \mathcal{E}$ with*

$$\operatorname{Supp}(N) \subseteq S \cup \{p : \operatorname{im} \rho_{E,p^\infty} = \mathrm{GL}_2(\mathbb{Z}_p)\}$$

one has

$$\deg(x) \geq \frac{d}{C} \cdot \deg(X_1(N) \to X_1(1)).$$

Proof. We enlarge S to include 2 and 3, if necessary. Let $\mathfrak{m} = \prod_{p \in S} p$. Then by Theorem 6, there exists a positive integer M with $\operatorname{Supp}(M) \subseteq S$ such that for each $E_i/\mathbb{Q}(j(E_i))$ we have

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

where π is the natural projection map.

Let $N \in \mathbb{Z}^+$, and $x \in X_1(N)$ associated to E_i. Suppose

$$\operatorname{Supp}(N) \subseteq S \cup \{p : \operatorname{im} \rho_{E_i,p^\infty} = \mathrm{GL}_2(\mathbb{Z}_p)\}.$$

Write $N = ab$, where $\operatorname{Supp}(a) \subseteq S$ and $\operatorname{Supp}(b) \cap S = \varnothing$. Since b is the product of primes for which the p-adic Galois representation associated to E_i is surjective, by [10, Proposition 5.7] we have

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

where $f : X_1(N) \to X_1(a)$ is the natural map. By [10, Proposition 5.8], we have

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

where $g : X_1(a) \to X_1(\gcd(a, M))$ is the natural map. Since $\deg(g(f(x))) \geq d$, the claim follows with

$$C = \deg(X_1(M) \to X_1(1)).$$

□

Proposition 3. *Let $d \in \mathbb{Z}^+$. Suppose there are only finitely many isolated j-invariants of degree d. Then there exists a constant $C = C(d)$ such that for any non-CM elliptic curve E with $[\mathbb{Q}(j(E)) : \mathbb{Q}] = d$ and $x \in X_1(N)$ with $j(x) = j(E)$ we have*

$$\deg(x) > C \cdot N^2.$$

Proof. Let $j_1, j_2, \ldots, j_k$ be the non-CM isolated j-invariants of degree d. For each $1 \leq i \leq k$, fix $E_i/\mathbb{Q}(j(E_i))$ with $j(E_i) = j_i$. By Serre's Open Image Theorem [52], there exists a prime $p_0 > 3$ such that the p-adic Galois representation of $E_i/\mathbb{Q}(j(E_i))$ is surjective for $p > p_0$. Taking $S = \{\text{primes} \leq p_0\}$ in Lemma 1, there exists a constant $C_1 = C_1(d)$ such that for any $N \in \mathbb{Z}^+$ and any $x = [E_i, P_i] \in X_1(N)$ we have

$$\begin{aligned}
\deg(x) &\geq \frac{d}{C_1} \cdot \deg(X_1(N) \to X_1(1)) \\
&\geq \frac{d}{2C_1} \cdot N^2 \prod_{p|N} \left(1 - \frac{1}{p^2}\right) \\
&> \frac{d}{2C_1} \cdot N^2 \prod_{p \text{ prime}} \left(1 - \frac{1}{p^2}\right) \\
&= \frac{d}{2C_1} \cdot \frac{1}{\zeta(2)} \cdot N^2.
\end{aligned}$$

Here ζ denotes the Riemann zeta function. Our lower bound argument is modeled after [58, Proposition 5].

So now assume j is not isolated, with $[\mathbb{Q}(j) : \mathbb{Q}] = d$. Then in particular there is no sporadic point on $X_1(N)$ with $j(x) = j$. Thus by lower bounds on gonality due to Abramovich [1], any point on $X_1(N)$ has degree at least

$$\frac{1}{2}\operatorname{gon}_{\mathbb{Q}}(X_1(N)) \geq \frac{7}{1600}[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(N)] = \frac{7}{3200}N^2 \prod_{p|N}\left(1 - \frac{1}{p^2}\right) \cdot > \frac{7}{3200} \cdot \frac{1}{\zeta(2)} \cdot N^2.$$

The statement holds with $C = \min\left\{\frac{d}{2C_1 \cdot \zeta(2)}, \frac{7}{3200 \cdot \zeta(2)}\right\}$. □

3.3. **Implication for Hypothesis 4.** Let $d \in \mathbb{Z}^+$. Suppose there are only finitely many isolated j-invariants of degree d. Suppose E/F is a non-CM elliptic curve with $[\mathbb{Q}(j(E)) : \mathbb{Q}] = d$ and $E(F)$ contains a point P of order N. Then $\mathbb{Q}(x) \hookrightarrow F$, where $x = [E, P] \in X_1(N)$. By Proposition 3, there is a constant $C = C(d)$ depending on d such that

$$C \cdot N^2 < \deg(x) \leq [F : \mathbb{Q}].$$

Since $\#E(F)_{\text{tors}} \mid (\exp E(F)_{\text{tors}})^2$, the bound on the full torsion subgroup follows. Taking the square root of both sides gives the desired bound on N.

4. Rational Isolated j-invariants for $X_1(p^aq^b)$

Here, we prove Theorem 3, which states that there are only finitely many rational isolated j-invariants associated to $X_1(p^aq^b)$, where p, q are primes. Section 4.1 includes preliminary results which rely on work of Lemos [38, 39], whereas Section 4.2 identifies the contribution from ramification results of Smith [57]. These are applied to prove Theorem 3 in Section 4.3.

4.1. Consequences of Work of Lemos.

Lemma 2. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve, and let $p < q$ be primes with $q > 37$. If $\operatorname{im}\rho_{E,q} = C_{ns}^+(q)$, then one of the following holds:*

(1) There is a single closed point point on $X_1(p^a)$ associated to E, and it is of maximal degree.
(2) $p = 2$ and the 2-adic image has RSZB label 4.8.0.2, 4.16.0.2, or 8.16.0.3.

Proof. By work of Lemos [38, 39], the mod p image is not contained in a Borel subgroup, or in the normalizer of a split Cartan subgroup. Thus by classification results in Section 2.1, we can assume the mod p Galois representation is surjective, has image equal to $C_{ns}^+(p)$, or is one of the following exceptional cases: $p = 2$ and the image is 2Cn or $p = 5, 13$ and the image is pS4. We consider each case separately.

- If the mod p image is surjective and $p \geq 5$, the result follows (e.g., [33, Corollary 2.13]).

- Suppose $p = 3$ and mod 3 image is surjective. Then by the classification of 3-adic images [50, 4], we know $\operatorname{im}\rho_{E,3^\infty} = \mathrm{GL}_2(\mathbb{Z}_3)$ or 9.27.0.1. In either case, we apply [12, Proposition 34] to compute the degree of a closed point from this 3-adic image data to confirm that the result follows.
- Suppose $p = 2$ and the mod 2 image is surjective. The classification of 2-adic images [51] shows the claim holds unless the 2-adic image is 4.8.0.2, 4.16.0.2, or 8.16.0.3, as disired.
- Suppose the mod p image is equal to $C_{ns}^+(p)$. We may assume p is odd, and let G be the p-adic image of Galois. By [30, Theorem 6.5] and [30, Proposition 2.2], we are in one of the following cases:
  (1) G has level p^n and $G \pmod{p^n} = C_{ns}^+(p^n)$. Then the first bullet point of the proof of [9, Theorem 6] shows there is a single closed point on $X_1(p^n)$ associated to E of maximal degree, and the claim now follows from [10, Theorem 5.1].
  (2) G has level p^2 and

$$G \pmod{p^2} \cong C_{\mathrm{ns}}^+(p) \ltimes \left\{ I + p \begin{bmatrix} a & \epsilon b \\ -b & c \end{bmatrix} \right\}$$

  where ϵ is a fixed integer which is not a quadratic residue modulo p. Let $F = \mathbb{Q}(E[p])$. In this case, there is a choice of basis $\{P, Q\}$ for $E[p^2]$ such that the image of $\rho_{E/F,p^2}$ is $\left\{ I + p \begin{pmatrix} a & \epsilon b \\ -b & c \end{pmatrix} \right\} \leq \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$. An element of this form fixes the first basis element if and only if it is one of the p matrices of the form

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 + pc \end{pmatrix}.$$

  Thus $F(P)/F$ has degree p^2, which means $\mathbb{Q}(P)/\mathbb{Q}(pP)$ has degree p^2. Since $[\mathbb{Q}(pP) : \mathbb{Q}]$ has degree $p^2 - 1$, it follows that $\mathbb{Q}(P)$ has largest possible degree and all elements of order p^2 are in a single Galois orbit. The claim now follows from [10, Theorem 5.1].
- Suppose $p = 2$ and the image is 2Cn. By [51], it follows that $\operatorname{im}\rho_{E,2^\infty}$ is 2.2.0.1, 4.4.0.2, or 8.4.0.1. In each case, there is a single closed point on $X_1(2^a)$ of maximal degree.
- If $p = 5$ and the image is 5S4, then [50] shows the 5-adic image is 5.5.0.1. The claim follows.
- If $p = 13$ and the image is 13S4, then $j(E)$ is one of 3 known exceptional j-invariants by [5, §5.1]. A computation shows that the mod q Galois image is surjective, and so in fact this case does not occur. See for example [28, Lemma 17]. □

4.2. **Consequence of Work of Smith.** We model the proof of [30, Theorem 7.3], which uses ramification results of Smith [57]. This improvement upon [11, Proposition 5] is crucial for the proof of Theorem 3.

Lemma 3. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve, and let $q > 17$ be prime with $\operatorname{im}\rho_{E,q} = C_{ns}^+(q)$. Let $F = \mathbb{Q}(E[N])$ for some N with $\gcd(N, q) = 1$. Then if P is a point of order q^b, we have*

$$\frac{q^{2b} - q^{2b-2}}{d} \leq [F(P) : F],$$

where $d \in \{1, 2, 3, 4, 6\}$.

Proof. By [26, Proposition 3.1] and [30, Theorem 4.5], the curve E has potentially good supersingular reduction at q and no canonical subgroup of order q. Let $L/\mathbb{Q}_q^{nr}$ be the minimal extension over which E attains good reduction. Since $q > 17$, we know $d = [L : \mathbb{Q}_q^{nr}] \in \{1, 2, 3, 4, 6\}$; see [52, §5.6]. By the Néron-Ogg-Shafarevich criterion [55, Theorem 1], the extension $L(E[N])/L$ is unramified, so $L(E[N]) = L$. In particular $\mathbb{Q}_q(E[N]) \subseteq L$. Work of Smith [57, Theorem 4.6] implies $L(P)$ contains an element with valuation $1/(q^{2b} - q^{2b-2})$, and so

$$[L(P) : L] \geq \frac{q^{2b} - q^{2b-2}}{d}.$$

Since $\mathbb{Q}_q(E[N]) \subseteq L$, we may conclude

$$[\mathbb{Q}_q(E[N])(P) : \mathbb{Q}_q(E[N])] \geq \frac{q^{2b} - q^{2b-2}}{d}.$$

The result follows. □

Corollary 1. *Let $x \in X_1(N)$ be a non-CM point with $j(x) \in \mathbb{Q}$. Suppose $q \mid N$ for some prime $q > 37$, and set $\mathrm{ord}_q(N) = b$. Then*

$$\deg(x) \geq \frac{1}{6} \deg(f(x)) \deg(f),$$

where $f : X_1(N) \to X_1(N/q^b)$ is the natural map.

Proof. Let $E/\mathbb{Q}$ be a non-CM elliptic curve with $j(E) = j(x)$. Since the degrees of closed points associated to E are not effected by quadratic twist, we may assume $-I \in \mathrm{im}\, \rho_{E,N}$. By Theorem 5, the image of $\rho_{E,q}$ is $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$ or $C_{ns}^+(q)$. In the first case, the result follows from [10, Proposition 5.7]. The second case is a consequence of Lemma 3. Indeed, let $x = [E, P] \in X_1(N)$ and $f(x) = [E, P'] \in X_1(N/q^b)$. By Lemma 3, we have $[\mathbb{Q}(P) : \mathbb{Q}(P')] \geq \frac{1}{6} \deg(f)$. If $N \notin \{q^b, 2q^b\}$, the result is now a consequence of [12, Proposition 34]. If $N \in \{q^b, 2q^b\}$, this follows from [9, Proposition 4] and Lemma 2. □

4.3. **Proof of Theorem 3.** Let $x = [E, P] \in X_1(p^a q^b)$ be isolated with $j(x) \in \mathbb{Q}$, and fix an equation for $E/\mathbb{Q}$. Since there are only 13 CM j-invariants in $\mathbb{Q}$, we may assume $j(x)$ is non-CM, and by [9] we may assume $a, b > 0$.

- Suppose $p, q \leq 37$. Let $S = \{\text{primes} \leq 37\}$, and let $m = \prod_{p \in S} p$. Then by Theorem 6, there is an absolute bound M on the level of the m-adic Galois representation for all non-CM elliptic curves over $\mathbb{Q}$. By [10, Proposition 5.8],

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

  where $f : X_1(p^a q^b) \to X_1(\gcd(p^a q^b, M))$ is the natural map. By Theorem 8, we see $f(x)$ is an isolated point on one of finitely many target curves. Each of these has only finitely many isolated points by Theorem 7, and hence there are only finitely many isolated j-invariants from this case.
- Assume $q > 37$ with $\mathrm{im}\, \rho_{E,q} = \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$. Then by [10, Proposition 5.7],

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

  where $f = X_1(p^a q^b) \to X_1(p^a)$. Thus it follows from Theorem 8 that $f(x) \in X_1(p^a)$ is isolated. Thus $j(x)$ is on the finite list of isolated j-invariants coming from [9].
- Assume $q > 37$ with $\mathrm{im}\, \rho_{E,q} \neq \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$. Then by Theorem 5, we have $\mathrm{im}\, \rho_{E,q} = C_{ns}^+(q)$. Suppose first that $p \neq 2$, or the 2-adic image is not 4.8.0.2, 4.16.0.2, or 8.16.0.3. By Lemma 2, we may assume the associated point on $X_1(p^a)$ is of maximal degree. Then by Corollary 1,

  $$\deg(x) \geq \frac{p^{2a-2}(p^2-1) \cdot q^{2b-2}(q^2-1)}{12}.$$

  This is strictly larger than the genus of $X_1(p^a q^b)$ by [56, Proposition 1.40], so the point is not isolated.

  So suppose $p = 2$ and the 2-adic image is 4.8.0.2, 4.16.0.2, or 8.16.0.3. Thus this means the point on $X_1(2^a)$ has degree $2^{\max(2a-4,0)}(2^2-1)$. As before, an application of Corollary 1 shows

  $$\deg(x) \geq \frac{2^{2a-2}(2^2-1) \cdot q^{2b-2}(q^2-1)}{24},$$

  which is strictly larger than the genus by [56, Proposition 1.40]. Thus x is not isolated.

Remark 11. An analogous argument cannot be used for products of more than 2 distinct primes, as the bounds of Corollary 1 are not sufficient to prove the degree of $x \in X_1(N)$ is larger than the genus. Thus to obtain more general results, one must show the factor of $1/6$ appearing in Corollary 1 can be removed. By the proof, it suffices to consider the case where the associated elliptic curve $E/\mathbb{Q}$ has $\mathrm{im}\, \rho_{E,q} = C_{ns}^+(q)$. If $\mathrm{im}\, \rho_{E,N} \cong \mathrm{im}\, \rho_{E,N/q^b} \times \mathrm{im}\, \rho_{E,q^b}$, then the factor $1/6$ is not needed, so this motivates the study of certain "entanglement" modular curves.

When $\mathbb{Q}(E[p^a]) \cap \mathbb{Q}(E[q^b]) \neq \mathbb{Q}$ for distinct primes p and q, then we say there is (horizontal) Galois entanglement. This means that $\mathrm{im}\, \rho_{E,p^a q^b}$ is properly contained in $\mathrm{im}\, \rho_{E,p^a} \times \mathrm{im}\, \rho_{E,q^b}$. Several recent papers propose a systematic study of entanglement; see for example [19, 18]. However, for applications to Hypothesis 2, we are only interested in entanglement which impacts the degrees of points on modular curves. For example, if $E/\mathbb{Q}$ has $\mathrm{im}\, \rho_{E,q} = C_{ns}^+(q)$ for $q > 37$, then work of Lemos [38, 39] shows the other non-surjective prime divisors $p \mid N$ typically have $\mathrm{im}\, \rho_{E,p} = C_{ns}^+(p)$. We have identified modular curves currently found in the LMFDB database which correspond to possible mod pq images with $\mathrm{im}\, \rho_{E,p} = C_{ns}^+(p)$, $\mathrm{im}\, \rho_{E,q} = C_{ns}^+(q)$,

and for which the factor of 1/6 in Corollary 1 cannot be removed. For example: 15.60.3.f.1, 21.126.4.a.1, 33.330.17.a.1, 35.420.29.f.1, 55.1100.81.d.1. In each case, the modular curve possesses a nontrivial rank 0 quotient. This is interesting since the modular curve associated with the fiber product $C_{ns}^+(p) \times C_{ns}^+(q)$ does *not* possess such a quotient. This leaves open the possibility that one could prove there are only finitely many isolated j-invariants in $\mathbb{Q}$ using formal immersion arguments, as in other uniformity results.

5. Improved Polynomial Bounds for Rational j-invariant

This section proves Theorem 4. First, we show how results from Sections 3 and 4 can be applied to obtain preliminary lower bounds on the degree of a point on $X_1(N)$ associated to a non-CM elliptic curve with rational j-invariant. The proof of the main result follows in Section 5.2.

5.1. Preliminary Bounds.

This sharpens [11, Proposition 5] for large non-surjective prime divisors.

Proposition 4. *There exists an absolute constant C such that for any non-CM elliptic curve $E/\mathbb{Q}$ and any $x = [E, P] \in X_1(N)$ we have*

$$\deg(x) \geq C \cdot N^2 \cdot \prod_{p \mid N} \frac{1}{6}\left(1 - \frac{1}{p^2}\right)$$

Proof. Let $E/\mathbb{Q}$ be a non-CM elliptic curve. Replacing E by a twist if necessary, we may assume $-I \in \operatorname{im} \rho_{E,N}$. Set $S \coloneqq \{\text{primes} \leq 37\}$. Let $N = n_1 \cdot n_2$, where $\operatorname{Supp}(n_1) \subseteq S$ and $\operatorname{Supp}(n_2) \cap S = \varnothing$. By repeatedly apply Corollary 1, we see

$$[\mathbb{Q}(P) : \mathbb{Q}(n_2 P)] \geq n_2^2 \prod_{p \mid n_2} \frac{1}{6}\left(1 - \frac{1}{p^2}\right).$$

By Lemma 1, there is a constant C_0 which does not depend on E such that

$$[\mathbb{Q}(n_2 P) : \mathbb{Q}] \geq \frac{1}{C_0} \deg(X_1(n_1) \to X_1(1)) \geq \frac{1}{C_0} \cdot \frac{1}{2} \cdot n_1^2 \cdot \prod_{p \mid n_1} \frac{1}{6}\left(1 - \frac{1}{p^2}\right).$$

Since $\deg(x)$ is at least $\frac{1}{2} \cdot [\mathbb{Q}(P) : \mathbb{Q}] = \frac{1}{2} \cdot [\mathbb{Q}(P) : \mathbb{Q}(n_2 P)] \cdot [\mathbb{Q}(n_2 P) : \mathbb{Q}]$, the result follows. □

5.2. Proof of Theorem 4.

Suppose E/F is a non-CM elliptic curve with $j(E) \in \mathbb{Q}$, and let $P \in E(F)$ of order N. Let $d = [F : \mathbb{Q}]$. By Proposition 4 we have

$$\begin{aligned} d &\geq C \cdot N^2 \cdot \prod_{p \mid N} \frac{1}{6} \cdot \left(1 - \frac{1}{p^2}\right) \\ &> C \cdot N^2 \cdot \prod_{p \text{ prime}} \left(1 - \frac{1}{p^2}\right) \cdot \prod_{p \mid N} \frac{1}{6} \\ &= \frac{C}{\zeta(2)} \cdot N^2 \left(\frac{1}{6}\right)^{\omega(N)}, \end{aligned}$$

where ζ denotes the Riemann zeta function and $\omega(N)$ counts the number of primes dividing N.

Suppose $N \geq 3$ and fix $0 < \epsilon < \frac{1}{4}$. We proceed as suggested by Pete Clark. By [49, Theorem 11] we have $\omega(N) \leq 1.3841 \log(N)/\log(\log(N))$, and it follows that

$$6^{\omega(N)} \leq 6^{c_1 \log_6(N)/\log(\log(N))} = N^{c_1/\log(\log(N))}.$$

Thus for N sufficiently large, we have $6^{\omega(N)} < N^{\epsilon}$, and so there exists a constant $c_{\epsilon,1}$ depending on ϵ such that $6^{\omega(N)} \leq c_{\epsilon,1} N^{\epsilon}$. Combining this with our initial inequality gives

$$d > \frac{C}{\zeta(2)} \cdot \frac{1}{c_{\epsilon,1}} \cdot N^{2-\epsilon}.$$

Solving for N shows $N < c_{\epsilon,2} \cdot d^{1/(2-\epsilon)} < c_{\epsilon,2} \cdot d^{1/2+\epsilon}$, as desired. Since $\#E(F)_{\text{tors}} \mid (\exp E(F)_{\text{tors}})^2$, the bound on the full torsion subgroup follows.

6. Examples of Isolated j-invariants

Here, we justify the examples of non-CM isolated j-invariants appearing in Table 1. Each point appears in van Hoeij's table of low degree points [61]. The degree 1 isolated j-invariants are described in detail in [12], so it suffices to provide justification for isolated j-invariants of degree $2 \leq d \leq 10$.

6.1. **Justifying Isolated.** If a curve's Jacobian has rank 0 over $\mathbb{Q}$, then any point in degree less than the $\mathbb{Q}$-gonality is isolated. The $\mathbb{Q}$-gonality of $X_1(N)$ is known for $1 \leq N \leq 40$ by work of Derickx and van Hoeij [24], and the gonality of $X_1(42)$ is at least 10 by recent work of Najman and Varivoda [47]. For isolated j-invariants in Table 1 having degree $d \geq 2$, the modular curves have rank 0 by [22, Theorem 3.1]. This justifies the listed points are isolated except for $X_1(25)$ and $X_1(32)$. For those, we apply Theorem 7 combined with [24, Theorem 3] for $X_1(25)$ and [47, Theorem 1.1] for $X_1(32)$.

6.2. **Justifying Non-CM.** If $x \in X_1(N)$ is a CM point with $j(x)$ of degree $d > 1$, then by [8, Theorem 6.2]

$$\deg(x) \geq d \cdot \varphi(N)/2.$$

Thus all points in the table associated to j-invariants of degree greater than 1 are non-CM.

7. On Stronger Polynomial Bounds

Hindry and Silverman [34, §3] ask whether there exists a constant c such that for any non-CM elliptic curve E defined over F of degree at least 3, one has $\#E(F)_{\text{tors}} \leq c\sqrt{[F:\mathbb{Q}]\log\log[F:\mathbb{Q}]}$. This improves Hypothesis 4 by assuming the existence of a single, absolute constant c, in addition to giving a better bound for $\#E(F)_{\text{tors}}$ as a function of $[F:\mathbb{Q}]$. Here, we show an affirmative answer to even the exponent bound suggested by Hindry and Silverman would imply Hypothesis 1.

Theorem 12. *Suppose there exists an absolute constant c such that for any non-CM elliptic curve E defined over a number field F of degree at least 3, one has $\exp E(F)_{\text{tors}} \leq c\sqrt{[F:\mathbb{Q}]\log\log[F:\mathbb{Q}]}$. Then Hypothesis 1 holds.*

Proof. Suppose Hypothesis 1 fails for some $d \in \mathbb{Z}^+$. Then for arbitrarily large primes p, there exists a non-CM elliptic curve E defined over a degree d number field for which $\operatorname{im}\rho_{E,p^\infty}$ does not contain $\mathrm{SL}_2(\mathbb{Z}_p)$. In particular, provided $p \geq 5$, this means the mod p image does not contain $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ for arbitrarily large primes p; see [33, Lemma 2.12]. By [32, Remark 2.1], $\operatorname{im}\rho_{E,p}$ cannot have image in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ isomorphic to A_4, S_4, or A_5 once $p > 60d+1$. Thus by [52, §2], one of the following cases must occur for infinitely many primes p:

(1) $\operatorname{im}\rho_{E,p}$ is contained in a Borel subgroup. In this case, E attains a point of order p in an extension of degree dividing $p-1$. Thus, there is a number field F of degree dividing $d(p-1)$ such that $E(F)$ contains a point of order p.
(2) $\operatorname{im}\rho_{E,p}$ is contained in the normalizer of a split Cartan subgroup. Here, E attains a p isogeny over a quadratic extension, and so as above there is a number field F of degree dividing $2d \cdot (p-1)$ such that $E(F)$ contains a point of order p.
(3) $\operatorname{im}\rho_{E,p}$ is contained in the normalizer of a non-split Cartan subgroup. Here, E attains full p-torsion over an extension of degree at most $2(p^2-1)$. As shown in [13, Theorem 3.1], there is an elliptic curve E' (geometrically isogenous to E) defined over a number field F of degree at most $d \cdot 2p(p^2-1)$ which has an F-rational point of order p^2.

In each case, this would contradict the assumption that for any F of degree at most 3,

$$\exp E(F)_{\text{tors}} \leq c\sqrt{[F:\mathbb{Q}]\log\log[F:\mathbb{Q}]}.$$

□

References

1. Dan Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices (1996), no. 20, 1005–1011.
2. Nikola Adžaga, Timo Keller, Philippe Michaud-Jacobs, Filip Najman, Ekin Ozman, and Borna Vukorepa, *Computing quadratic points on modular curves $X_0(N)$*, Math. Comp. **93** (2024), no. 347, 1371–1397.
3. 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.

4. Jennifer S. Balakrishnan, L. Alexander Betts, Daniel Raynor Hast, Aashraya Jha, and J. Steffen Müller, *Rational points on the non-split cartan modular curve of level 27 and quadratic chabauty over number fields*, preprint, available at arxiv.org:2501.07833.
5. Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk, *Quadratic Chabauty for modular curves: algorithms and examples*, Compos. Math. **159** (2023), no. 6, 1111–1152.
6. Jennifer S. Balakrishnan and Barry Mazur, *Ogg's torsion conjecture: fifty years later*, Bull. Amer. Math. Soc. (N.S.) **62** (2025), no. 2, 235–268, With an appendix by Netan Dogra.
7. Yuri Bilu, Pierre Parent, and Marusia Rebolledo, *Rational points on $X_0^+(p^r)$*, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 3, 957–984.
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.
9. Abbey Bourdon and Özlem Ejder, *Rational isolated j-invariants from $X_1(\ell^n)$ and $X_0(\ell^n)$*, Res. Number Theory **12** (2026), no. 2, Paper No. 47, 13.
10. 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.
11. Abbey Bourdon and Tyler Genao, *Uniform polynomial bounds on torsion from rational geometric isogeny classes*, to appear in Math. Res. Lett. Available at arxiv.org:2409.08214.
12. Abbey Bourdon, Sachi Hashimoto, Timo Keller, Zev Klagsbrun, David Lowry-Duda, Travis Morrison, Filip Najman, and Himanshu Shukla, *Towards a classification of isolated j-invariants*, Math. Comp. **94** (2025), no. 351, 447–473, With an appendix by Maarten Derickx and Mark van Hoeij.
13. 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.
14. Anna Cadoret and Akio Tamagawa, *A uniform open image theorem for ℓ-adic representations, II*, Duke Math. J. **162** (2013), no. 12, 2301–2344.
15. Pete L. Clark, Brian Cook, and James Stankewicz, *Torsion points on elliptic curves with complex multiplication (with an appendix by Alex Rice)*, Int. J. Number Theory **9** (2013), no. 2, 447–479.
16. 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.
17. Pete L. Clark and Paul Pollack, *Pursuing polynomial bounds on torsion*, Israel J. Math. **227** (2018), no. 2, 889–909.
18. Harris B. Daniels, Álvaro Lozano-Robledo, and Jackson S. Morrow, *Towards a classification of entanglements of Galois representations attached to elliptic curves*, Rev. Mat. Iberoam. **39** (2023), no. 3, 803–844. MR 4605883
19. Harris B. Daniels and Jackson S. Morrow, *A group theoretic perspective on entanglements of division fields*, Trans. Amer. Math. Soc. Ser. B **9** (2022), 827–858. MR 4496973
20. 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), 1973, pp. 143–316. Lecture Notes in Math., Vol. 349.
21. Maarten Derickx, *What are the strongest conjectured uniform versions of Serre's Open Image Theorem?*, available at http://mathoverflow.net/q/203837.
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.
23. Maarten Derickx and Filip Najman, *Classification of torsion of elliptic curves over quartic fields*, preprint, available at arxiv.org:2412.16016.
24. Maarten Derickx and Mark van Hoeij, *Gonality of the modular curve $X_1(N)$*, J. Algebra **417** (2014), 52–71.
25. Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005.
26. Özlem Ejder, *Isolated points on $X_1(\ell^n)$ with rational j-invariant*, Res. Number Theory **8** (2022), no. 1, Paper No. 16, 7.
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. Kate Finnerty, Tyler Genao, Jacob Mayle, and Rakvi, *The possible adelic indices for elliptic curves admitting a rational cyclic isogeny*, available at arxiv.org:2512.00652.
29. Gerhard Frey, *Curves with infinitely many points of fixed degree*, Israel J. Math. **85** (1994), no. 1-3, 79–83.
30. Lorenzo Furio, *Effective bounds for adelic galois representations attached to elliptic curves over the rationals*, preprint, available at arxiv.org:2412.10340.
31. Lorenzo Furio and Davide Lombardo, *Serre's uniformity question and proper subgroups of $C_{ns}^+(p)$*, preprint, available at arxiv.org:2305.17780.
32. E. Ghate and P. Parent, *On uniform large Galois images for modular abelian varieties*, Bull. Lond. Math. Soc. **44** (2012), no. 6, 1169–1181. MR 3007649
33. Aaron Greicius, *Elliptic curves with surjective adelic Galois representations*, Experiment. Math. **19** (2010), no. 4, 495–507.
34. Marc Hindry and Joseph Silverman, *Sur le nombre de points de torsion rationnels sur une courbe elliptique*, C. R. Acad. Sci. Paris Sér. I Math. **329** (1999), no. 2, 97–100. MR 1710502
35. S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229.
36. M. 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.

37. M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.
38. Pedro Lemos, *Serre's uniformity conjecture for elliptic curves with rational cyclic isogenies*, Trans. Amer. Math. Soc. **371** (2019), no. 1, 137–146.
39. ———, *Some cases of Serre's uniformity problem*, Math. Z. **292** (2019), no. 1-2, 739–762.
40. Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, Translated from the French by Reinie Erné, Oxford Science Publications.
41. Álvaro Lozano-Robledo, *Ramification in the division fields of elliptic curves with potential supersingular reduction*, Res. Number Theory **2** (2016), Paper No. 8, 25.
42. B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186, With an appendix by Mazur and M. Rapoport.
43. ———, *Rational points on modular curves*, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), Lecture Notes in Math., vol. Vol. 601, Springer, Berlin-New York, 1977, pp. 107–148.
44. ———, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.
45. Loïc Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1-3, 437–449.
46. 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.
47. Filip Najman and Marin Varivoda, *Torsion groups of elliptic curves that appear infinitely often over septic, octic and nonic fields*, preprint, available at arxiv.org:2602.03513.
48. A. P. Ogg, *Diophantine equations and modular forms*, Bull. Amer. Math. Soc. **81** (1975), 14–27.
49. Guy Robin, *Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n*, Acta Arith. **42** (1983), no. 4, 367–389. MR 736719
50. Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown, *ℓ-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.
51. Jeremy Rouse and David Zureick-Brown, *Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois*, Res. Number Theory **1** (2015), Paper No. 12, 34.
52. Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.
53. ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 54, 323–401.
54. ———, *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.
55. Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517.
56. Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Kanô Memorial Lectures, vol. No. 1, Iwanami Shoten Publishers, Tokyo; Princeton University Press, Princeton, NJ, 1971, Publications of the Mathematical Society of Japan, No. 11.
57. Hanson Smith, *Ramification in division fields and sporadic points on modular curves*, Res. Number Theory **9** (2023), no. 1, Paper No. 17, 19.
58. Patrick Solé and Michel Planat, *Extreme values of the Dedekind Ψ function*, J. Comb. Number Theory **3** (2011), no. 1, 33–38. MR 2908180
59. Andrew V. Sutherland, *Computing images of Galois representations attached to elliptic curves*, Forum Math. Sigma **4** (2016), e4, 79.
60. Kenji Terao, *Degrees of points with rational j-invariant on $X_0(n)$ and $X_1(n)$*, available at arxiv.org:2507.13199, 2022.
61. Mark van Hoeij, *Low degree places on the modular curve $X_1(n)$*, preprint, available at arxiv.org:1202.4355.
62. Bianca Viray and Isabel Vogt, *Isolated and parameterized points on curves*, preprint, available at arxiv.org:2406.14353.
63. David Zywina, *On the possible image of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$*, available at arxiv.org:1508.07660.