SPORADIC POINTS OF ODD DEGREE ON $X_1(N)$ COMING FROM $\mathbb{Q}$-CURVES

ABBEY BOURDON AND FILIP NAJMAN

ABSTRACT. We say a closed point x on a curve C is sporadic if there are only finitely many points on C of degree at most $\deg(x)$. In the case where C is the modular curve $X_1(N)$, most known examples of sporadic points come from elliptic curves with complex multiplication (CM). We seek to understand all sporadic points on $X_1(N)$ corresponding to $\mathbb{Q}$-curves, which are elliptic curves isogenous to their Galois conjugates. This class contains not only all CM elliptic curves, but also any elliptic curve $\overline{\mathbb{Q}}$-isogenous to one with a rational j-invariant, among others. In this paper, we show that all non-CM $\mathbb{Q}$-curves giving rise to a sporadic point of odd degree lie in the $\overline{\mathbb{Q}}$-isogeny class of the elliptic curve with j-invariant $-140625/8$. In addition, we show that a stronger version of this finiteness result would imply Serre's Uniformity Conjecture.

1. INTRODUCTION

Let E be an elliptic curve defined over a number field F. By the Mordell-Weil Theorem, the set of points on E with coordinates in F is a finitely generated abelian group. That is, there exists a finite abelian group $E(F)_{\mathrm{tors}}$ and nonnegative integer r such that

$$E(F) \cong E(F)_{\mathrm{tors}} \times \mathbb{Z}^r.$$

A standard classification problem is to describe the groups that arise as $E(F)_{\mathrm{tors}}$ as E ranges over all number fields F of a fixed degree d. In general, there are only finitely many possible torsion subgroups that appear—a consequence of Merel's Uniform Boundedness Theorem [49]—and the list of groups is known explicitly for degrees $1 \le d \le 3$; see [47, 34, 41, 35, 20]. For example, the possible torsion subgroups of elliptic curves over $\mathbb{Q}$ are given by the following theorem:

Theorem 1.1 (Mazur, [47]). *If $E/\mathbb{Q}$ is an elliptic curve, then $E(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to one of the following:*

$$\mathbb{Z}/m\mathbb{Z}, \ \text{with } 1 \le m \le 10 \ \text{or } m = 12,$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, \ \text{with } 1 \le m \le 4.$$

Moreover, for each group T that arises, there are infinitely many non-isomorphic elliptic curves $E/\mathbb{Q}$ such that $E(\mathbb{Q})_{\mathrm{tors}} \cong T$.

The classification of torsion subgroups of elliptic curves over cubic fields presents a new phenomenon. For the first time, there are certain groups which arise for only finitely many isomorphism classes of elliptic curves.

Theorem 1.2 (Najman [51], Derickx, Etropolski, van Hoeij, Morrow, Zureick-Brown [20]). *The elliptic curve 162.c3 over $\mathbb{Q}(\zeta_9)^+$ with j-invariant $-140625/8$ is the unique elliptic curve over a cubic field with a point of order 21.*

Phrased another way, this means the elliptic curve 162.c3 corresponds to a sporadic point of degree 3 on the modular curve $X_1(21)$. Recall $X_1(N)$ is an algebraic curve over $\mathbb{Q}$ whose non-cuspidal points parametrize isomorphism classes of pairs of an elliptic curve together with a distinguished point of order N. We say a point x on a curve defined over a number field is **sporadic** if there are

only finitely many points of degree at most $\deg(x)$. By definition, such points cannot belong to an infinite parameterized family of points of the same degree, making them more difficult to detect using standard tools. Our lack of understanding of sporadic points on the modular curves $X_1(N)$ has made it difficult to extend the classification of torsion subgroups beyond cubic fields.

Inspired by this, we seek to characterize the elliptic curves capable of producing sporadic points on $X_1(N)$, in search of some sort of framework which might explain their existence. Moreover, this problem is inextricably linked to Serre's Uniformity Conjecture on Galois representations of elliptic curves. We say j is a **sporadic j-invariant** if there exists a sporadic point $x \in X_1(N)$ such that $j = j(x)$. So, for example, by Theorem 1.2, we see that $-140625/8$ is a sporadic j-invariant, as is any j-invariant associated to an elliptic curve with complex multiplication (CM) by [8, Theorem 7.1]. Work of the first author in collaboration with Ejder, Liu, Odumodu, Viray [8] shows that there are only finitely many sporadic[1] j-invariants in $\mathbb{Q}$, assuming the following conjecture; such a result is known unconditionally for points of odd degree [9].

Conjecture 1 (Uniformity Conjecture)**.** There exists a constant such that for all non-CM elliptic curves $E/\mathbb{Q}$, the mod p Galois representation of E is surjective for all $p > C$.

Conjecture 1 originated with a question of Serre [55], but has since been formally conjectured by both Zywina [62] and Sutherland [60]. A wealth of computational evidence and partial theoretical progress which supports an affirmative answer. See for example [4, 5, 3, 62, 60, 43, 44].

While Serre's Uniformity Conjecture implies that there are only finitely many sporadic j-invariants in $\mathbb{Q}$, showing that the same holds true for all sporadic j-invariants associated to non-CM $\mathbb{Q}$-curves would actually imply Serre's Uniformity Conjecture. Recall a $\mathbb{Q}$-curve is any elliptic curve isogenous (over $\overline{\mathbb{Q}}$) to its Galois conjugates. This is a property enjoyed by CM elliptic curves and elliptic curves with rational j-invariant, though the collection of all $\mathbb{Q}$-curves properly contains these sets.

Theorem 1.3. *Suppose there exist only finitely many isogeny classes containing non-CM $\mathbb{Q}$-curves (up to isomorphism over $\overline{\mathbb{Q}}$) that give rise to a sporadic point on $X_1(p^2)$ for some prime p. Then Serre's Uniformity Conjecture holds.*

This motivates the study torsion points within isogeny classes of $\mathbb{Q}$-curves, which we initiate in the present work. In particular, we pose the following question, which extends those raised in [8].

Question 1. *Do all non-CM $\mathbb{Q}$-curves giving rise to sporadic points on any modular curve $X_1(N)$ belong to only finitely many $\overline{\mathbb{Q}}$-isogney classes, even as we allow N to range over all positive integers?*

In our main result, we answer Question 1 for sporadic points of odd degree, showing that the elliptic curve 162.c3 actually plays a much larger role in explaining sporadic points on the modular curves $X_1(N)$ than what is apparent from Theorem 1.2. Not only does this elliptic curve give a non-cuspidal sporadic point of least possible degree, but it is also isogenous to any other non-CM $\mathbb{Q}$-curve corresponding to a sporadic point of odd degree on $X_1(N)$ for any positive integer N. Since any sporadic point on $X_1(N)$ must have degree less than its $\mathbb{Q}$-gonality,[2] this is a consequence of the following more general result.

Theorem 1.4. *Let $x \in X_1(N)$ be a point of odd degree corresponding to a non-CM $\mathbb{Q}$-curve E. If $\deg(x) < \mathrm{gon}_{\mathbb{Q}}(X_1(N))$, then E is $\overline{\mathbb{Q}}$-isogenous to an elliptic curve with the j-invariant $-140625/8$. In particular, any non-CM $\mathbb{Q}$-curve giving rise to a sporadic point of odd degree on $X_1(N)$ is isogenous (over $\overline{\mathbb{Q}}$) to the elliptic curve 162.c3.*

---

[1]In fact, [8] shows there are only finitely many *isolated* j-invariants in $\mathbb{Q}$. The set of all isolated points strictly contains the set of all sporadic points, so the claim about sporadic j-invariants is immediate.

[2]Recall the k-gonality of a curve C over a number field k is the least degree of a non-constant rational map $f : C \to \mathbb{P}^1_k$. Hilbert's irreducibility theorem [56, Ch.9] implies $f^{-1}(\mathbb{P}^1(k))$ contains infinitely many degree d points.

The proof builds on recent work of Cremona and the second author [15] (which in turn builds on work of Elkies [24]). A crucial result at the foundation of our approach is that any non-CM $\mathbb{Q}$-curve defined over a number field of odd degree is isogenous to an elliptic curve with rational j-invariant [15, Theorem 2.7], making it possible to use information about the Galois representations of elliptic curves over $\mathbb{Q}$ to deduce results for the original $\mathbb{Q}$-curve. For example, in Theorem 1.1 of [15], this isogeny connection is used to show that there exists a point of odd degree on $X_1(N)$ corresponding to a non-CM $\mathbb{Q}$-curve only if $\text{Supp}(N) \subseteq \{2, 3, 5, 7, 11, 13, 17, 37\}$. Paired with results of [8], we immediately see that there will be only finitely many $\mathbb{Q}$-curves with j-invariant in an extension of *bounded* degree giving rise to a sporadic point of odd degree on any modular curve of the form $X_1(N)$.[3] Thus the strength of Theorem 1.4 is in showing that these sporadic j-invariants lie in finitely many isogeny classes, even if we remove the bound on the degree of $\mathbb{Q}(j)$.

In the case where N is a power of a single prime, bounds on the $\mathbb{Q}$-gonality of $X_1(N)$ due to Derickx and van Hoeij [22] are strong enough to imply that there are no sporadic points of odd degree corresponding to non-CM $\mathbb{Q}$-curves. This is in direct contrast to the CM case.

Theorem 1.5. *Let p be a prime number and k a positive integer. If $x = [E, P] \in X_1(p^k)$ is a point of odd degree corresponding to a $\mathbb{Q}$-curve with $\deg(x) < \text{gon}_{\mathbb{Q}}(X_1(p^k))$, then E has complex multiplication. Moreover, for any prime $p \equiv 3 \pmod 4$ and k sufficiently large, there exist sporadic CM points of odd degree on $X_1(p^k)$.*

Our proof shows that there are infinitely many CM j-invariants producing sporadic points on $X_1(p^k)$ of odd degree, and that they necessarily belong to infinitely many distinct $\overline{\mathbb{Q}}$-isogeny classes; see Remark 5.4. This shows that the "non-CM" assumption in Theorem 1.4 is necessary if one wishes to characterize a set of $\mathbb{Q}$-curves producing sporadic points of odd degree which belong to only finitely many isogeny classes.

Even though we have established that all non-CM $\mathbb{Q}$-curves corresponding to a sporadic point on $X_1(N)$ of odd degree lie in a single $\overline{\mathbb{Q}}$-isogeny class, it remains to determine whether there can be infinitely sporadic j-invariants within that isogeny class. Our final question is the following:

Question 2. *Does there exist a non-CM $\overline{\mathbb{Q}}$-isogeny class containing infinitely many sporadic j-invariants?*

In Proposition 8.1, we show that the answer is yes if there exists a sporadic point of sufficiently low degree associated to a curve in the $\overline{\mathbb{Q}}$-isogeny class. However, as the only known examples of points satisfying this degree condition correspond to CM elliptic curves, it is not clear whether one should expect the existence of such a point.

1.1. **Related Work.** While sporadic points on more general modular curves are certainly of interest as they pertain to the classification of Galois representations of elliptic curves (see, for example [3]) or the modularity of elliptic curves (see, for example, [25, 21, 11]), for this summary we will restrict our attention to modular curves $X_1(N)$ and $X_0(N)$ (which parametrizes elliptic curves with a cyclic N-isogeny). The first examples of sporadic points on modular curves of this form arise as points in $X_0(N)(\mathbb{Q})$ in cases where this curve has genus greater than 0. Key contributions to this classification were made by Mazur [48] and Kenku [36, 38, 37, 39], but see Table 4 in [46] for a more complete list of references. The classification of quadratic and cubic points on modular curves $X_0(N)$ is the topic of several recent works, and many new examples of sporadic points have been discovered; see, for example [52, 12]. For modular curves $X_1(N)$, the least possible degree of a non-cuspidal sporadic point is 3, and, as mentioned above, there is a unique elliptic curve

---

[3]Indeed, there exists a uniform bound on the level of the m-adic Galois representation associated to all non-CM elliptic curves over number fields of fixed degree [8, Prop. 6.1]. Since any curve by definition can have only finitely many sporadic points, the claim follows from Proposition 5.8 and Theorem 4.3 of [8].

producing such a point which was first discovered by the second author [51]. Others can be found in tables associated to work of Derickx and van Hoeij [22]; note that any point in degree less than the $\mathbb{Q}$-gonality of the curve will be sporadic, provided the associated Jacobian has rank 0 over $\mathbb{Q}$. Sporadic points associated to elliptic curves with rational j-invariant were the topic of [8] and [9], and those corresponding to elliptic curves with supersingular reduction were studied in [59].

For a complete summary of what is known concerning sporadic CM points on modular curves, see work of Clark, Genao, Pollack, and Saia [14].

1.2. **Outline.** We summarize relevant background information on Galois representations and isogenies of elliptic curves in §2, along with some basic information concerning modular curves. Section 3 contains the proof of Theorem 1.3. Our approach to Theorem 1.4 relies on first establishing certain divisibility conditions for the existence of a rational torsion point on a non-CM $\mathbb{Q}$-curve defined over a number field of odd degree (see Proposition 4.1) which are obtained by studying torsion points within isogeny classes of elliptic curves. Theorem 1.5 is a relatively quick consequence of these divisibility conditions and is proved in §5. To complete the proof of Theorem 1.4, we first show that there exists a point of odd degree on $X_1(N)$ associated to a non-CM $\mathbb{Q}$-curve only for N of a certain form, as in Proposition 6.1. In Section 7, we show that any odd degree point $x \in X_1(N)$ with $\deg(x) < \mathrm{gon}_{\mathbb{Q}}(X_1(N))$ associated to a non-CM $\mathbb{Q}$-curve would force a low degree point on one of finitely many modular curves; see sections 7.1 or 7.2. In cases where these low degree points would arise on modular curves of the form $X_1(N)$, their existence can generally be ruled out by prior work. However, other cases require an analysis of certain modular curves which parametrize elliptic curves with unusual entanglement between their 2^a- and 3^k-torsion point fields. Explicit computations of the rational points on these entanglement modular curves appear in section 7.3, completing the proof of Theorem 1.4. Partial progress towards Question 2 appears in §8.

We note that all code for Magma computations relevant to sections 7.2 and 7.3 is publicly available at `https://web.math.pmf.unizg.hr/~fnajman/code_QC.zip`.

2. Background and Notation

2.1. **Conventions.** For a number field k and algebraic closure $\overline{k}$, we let $\mathrm{Gal}_k := \mathrm{Gal}(\overline{k}/k)$ denote the absolute Galois group of F. If $n \in \mathbb{Z}^+$, we use $\mathrm{Supp}(n)$ to denote the set of all prime numbers dividing n. If $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ for distinct primes p_i, then $\mathrm{ord}_{p_i}(n) := a_i$.

If C is a curve defined over a number field k and $x \in C$ is a closed point, then $k(x)$ denotes the residue field of x. By the degree of x we mean the degree of $k(x)$ over k.

If E is an elliptic curve defined over a number field k and $P \in E(\overline{k})$, then $k(P)$ denotes the field extension of k generated by the x- and y-coordinates of P. By m-isogeny of elliptic curves, we mean a cyclic isogeny of degree m. Specific elliptic curves are referred to by their LMFDB label.

For subgroups of $\mathrm{GL}_2(\mathbb{Z}_p)$, we generally use the notation of Sutherland and Zywina in [61], though in a few cases for the prime $p = 2$ we use that of Rouse and Zureick-Brown [54] for ease of reference.

2.2. **Galois Representations of Elliptic Curves.** For an elliptic curve E defined over a number field k, the absolute Galois group Gal_k acts naturally on the set of all torsion points of E, denoted $E(\overline{k})_{\mathrm{tors}}$. This action is encoded in the adelic Galois representation associated to E:

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

Through the isomorphism $\mathrm{GL}_2(\hat{\mathbb{Z}}) \cong \prod_{p \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_p)$ and natural projection, we obtain the m-adic representation associated to E for any integer m, denoted

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

This representation describes the action of Gal_k on all points of E of order n with $\mathrm{Supp}(n) \subseteq \mathrm{Supp}(m)$. Via reduction mod n, we recover the mod n Galois representation associated to E

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

which gives the action of Gal_k on $E[n]$, the set of points on E of order dividing n. If m and n are relatively prime, we may combining reduction mod n in some components with projection in others to define

$$\rho_{E,n \cdot m^\infty} : \mathrm{Gal}_k \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}_m).$$

Here, $\mathbb{Z}_m := \prod_{p \in \mathrm{Supp}(m)} \mathbb{Z}_p$.

If E does not have complex multiplication, then Serre's Open Image Theorem [55] states that the image of ρ_E, denoted $\mathrm{im}\,\rho_E$, is open (and thus of finite index) in $\mathrm{GL}_2(\hat{\mathbb{Z}})$. In particular, the image of the p-adic Galois representation associated to a non-CM elliptic curve E is of finite index in $\mathrm{GL}_2(\mathbb{Z}_p)$. The following proposition summarizes a few of the known constraints on this index in the case of elliptic curves over $\mathbb{Q}$.

Proposition 2.1. *For any non-CM elliptic curve $E/\mathbb{Q}$,*

$$\mathrm{ord}_2([\mathrm{GL}_2(\mathbb{Z}_2) : \mathrm{im}\,\rho_{E/\mathbb{Q},2^\infty}]) \leq 6.$$

If $E/\mathbb{Q}$ is a non-CM elliptic curve with a rational cyclic p-isogeny for some odd prime p, then we have the following:

- *(1) If $p \geq 7$, then $\mathrm{ord}_p([\mathrm{GL}_2(\mathbb{Z}_p) : \mathrm{im}\,\rho_{E/\mathbb{Q},p^\infty}]) = 0$.*
- *(2) If $p = 5$, then $\mathrm{ord}_5([\mathrm{GL}_2(\mathbb{Z}_5) : \mathrm{im}\,\rho_{E/\mathbb{Q},5^\infty}]) = 0$ unless $E/\mathbb{Q}$ has either a rational cyclic 25-isogeny or two independent 5-isogenies. In the latter cases, we have $\mathrm{ord}_5([\mathrm{GL}_2(\mathbb{Z}_5) : \mathrm{im}\,\rho_{E/\mathbb{Q},5^\infty}]) = 1$.*
- *(3) If $p = 3$, then $\mathrm{ord}_3([\mathrm{GL}_2(\mathbb{Z}_3) : \mathrm{im}\,\rho_{E/\mathbb{Q},3^\infty}]) \leq 2$.*

Proof. For $p = 5$ or $p > 7$, this follows from work of Greenberg (see Theorems 1 and 2, along with Remark 4.2.1 in [31]). The case of $p = 7$ is addressed in work of Greenberg, Rubin, Silverberg, Stoll [30]. For $p = 3$, the result follows from Corollary 1.10 in [33]. The case of $p = 2$ is given by Corollary 1.3 in work of Rouse and Zureick-Brown [54]. $\square$

A further implication of Serre's Open Image Theorem is the existence of a positive integer N such that $\mathrm{im}\,\rho_E = \pi^{-1}(\mathrm{im}\,\rho_{E,N})$, where π denotes the natural reduction map. The smallest such N is called the level of the adelic Galois representation. In a similar way, for any positive integer m, we defined the level of the m-adic representation to be the least positive integer N such that $\mathrm{im}\,\rho_{E,m^\infty} = \pi^{-1}(\mathrm{im}\,\rho_{E,N})$.

2.3. **Isogenies of Elliptic Curves.** For an elliptic curve E defined over a number field k, we say the subgroup C of E is k-rational if $\sigma(C) = C$ for all $\sigma \in \mathrm{Gal}_k$. That is, for all $P \in C$, we have $\sigma(P) \in C$ (though σ need not fix P itself). There is a one-to-one correspondence between finite subgroups C of E and isomorphism classes of isogenies $\varphi : E \to E'$ given by associating C with the unique isogeny having $\ker(\varphi) = C$, and φ is defined over k if and only if C is k-rational. See §III.4 of [58] for details. For any two non-CM elliptic curves E, E' isogenous over $\overline{\mathbb{Q}}$, there exists a cyclic isogeny $\varphi : E \to E'$ which is unique up to sign [15, Lemma A.1], so we may generally assume our isogenies are cyclic.

In the case of elliptic curves over $\mathbb{Q}$, we have a complete classification of the possible rational cyclic subgroups that can occur.

Theorem 2.2 (Mazur [48], Kenku [36, 38, 37, 39, 40], and others; see Section 9 of [46]). *If $E/\mathbb{Q}$ is an elliptic curve possessing a $\mathbb{Q}$-rational cyclic subgroup of order N, then $N \leq 19$ or $N \in \{21, 25, 27, 37, 43, 67, 163\}$.*

This classification can also be used to characterize certain rational isogenies for non-CM elliptic curves $E/\mathbb{Q}$ under base extension to number fields of odd degree. If a non-CM elliptic curve E/k has a k-rational cyclic isogeny of degree n, then so will any E'/k with $j(E') = j(E)$. Thus the following result can be used to deduce isogeny information for any non-CM elliptic curve with j-invariant in $\mathbb{Q}$.

Proposition 2.3 (Cremona, Najman [15]). *Let $E/\mathbb{Q}$ be an elliptic curve without CM, and let p be an odd prime such that E has no p-isogenies defined over $\mathbb{Q}$. Then all p-isogenies of E are defined over number fields of even degree, unless $j(E) = 2268945/128$, in which case E acquires 7-isogenies over the cubic field generated by a root of $x^3 - 5x - 5$.*

Finally, we note that any $\mathbb{Q}$-curve defined over a number field k of odd degree is isogenous over k to an elliptic curve with rational j-invariant, as a consequence of the following key result.

Theorem 2.4 (Cremona, Najman [15]). *Let E be a non-CM $\mathbb{Q}$-curve defined over a number field k. If $\mathbb{Q}(j(E))$ has no quadratic subfields, then E is isogenous over k to an elliptic curve with rational j-invariant.*

2.4. **Modular Curves.** Points on the affine curve $Y_1(N)$ correspond to equivalence classes of elliptic curves $E/\mathbb{C}$ with a distinguished point P of order N. We consider two pairs $[E, P]$ and $[E', P']$ to be equivalent if there exists an isomorphism $\varphi : E \to E'$ such that $\varphi(P) = P'$. By adding a finite number of points to $Y_1(N)$—called cusps—we obtain the smooth projective curve $X_1(N)$. In fact, $X_1(N)$ can be given the structure of an algebraic curve over $\mathbb{Q}$, and we view it as such unless otherwise noted. See [23, Section 7.7] or [19] for details.

If $x = [E, P] \in X_1(N)$ is a non-cuspidal point, we say a Weierstrass equation over a number field k is a model for E/k if it has j-invariant equal to $j(E)$, and we use P to denote the image of the point associated to x under the implied isomorphism. For any model of E/k having $P \in E(k)$, the residue field $\mathbb{Q}(x)$ is contained in k. Conversely, there exists a model of $E/\mathbb{Q}(x)$ such that $P \in E(\mathbb{Q}(x))$. See [19, p. 274, Proposition VI.3.2]. It is often useful to have a more concrete way of describing the residue field, as given in the following lemma.

Lemma 2.5. *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 $\mathfrak{h} : E \to E/\mathrm{Aut}(E) \cong \mathbb{P}^1$ is a Weber function for E.

Proof. Since $X_1(N)$ parametrizes elliptic curves up to isomorphism, we may choose a model of E defined over $F := \mathbb{Q}(j(E))$. It is clear that $F(\mathfrak{h}(P))) \subseteq F(P)$, and this field does not depend on

6

the choice of model for E/F: for any other E'/F with $j(E') = j(E)$ and isomorphism $\psi : E \to E'$, we have $F(\mathfrak{h}(P)) = F(\mathfrak{h}(\psi(P)))$ by [57, p. 107]. Thus $F(\mathfrak{h}(P)) \subseteq \mathbb{Q}(x)$.

To show equality holds, it suffices to construct a model of E over $F(\mathfrak{h}(P)))$ such that P becomes rational. Indeed, for any $\sigma \in \mathrm{Gal}_{F(\mathfrak{h}(P))}$,

$$\sigma(P) = \zeta P$$

for some $\zeta \in \mathrm{Aut}(E) = \mu_2, \mu_4$ or μ_6. This defines a character χ, and P is rational on the twist $E^{\chi^{-1}}$ over $F(\mathfrak{h}(P))$. $\qquad \square$

Remark 2.6. If E is given by an equation of the form $y^2 = 4x^3 - c_2 x - c_3$, then for $P = (x, y) \in E$ and $\Delta = c_2^3 - 27c_3^2$ we may take $\mathfrak{h}$ to be

$$\mathfrak{h}(P) = \begin{cases} \frac{c_2 c_3}{\Delta} x & j(E) \neq 0, 1728, \\ \frac{c_2^2}{\Delta} x^2 & j(E) = 1728, \\ \frac{c_3}{\Delta} x^3 & j(E) = 0. \end{cases}$$

If $\psi : E \to E'$ is an isomorphism, then one can check that $\mathfrak{h}_E = \mathfrak{h}_{E'} \circ \psi$; see [57, p. 107]. Thus if E does not have CM, the residue field of $[E, P] \in X_1(N)$ is generated over $\mathbb{Q}(j(E))$ by the x-coordinate of P.

Lemma 2.5 also gives a concrete way of computing the degree of a point on $X_1(N)$ from a particular model of $E/\mathbb{Q}(j(E))$. The following lemma allows us to relate the degree of this point to that of its image on other modular curves.

Proposition 2.7. *For positive integers a and b, there is a natural $\mathbb{Q}$-rational map $f : X_1(ab) \to X_1(a)$ defined by sending $[E, P]$ to $[E, bP]$. Moreover*

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

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

Proof. By the moduli interpretation, the map is $\mathbb{Q}$-rational, and the degree calculation follows from [23, p.66]. $\qquad \square$

In a similar way, the modular curve $X_0(N)$ is a smooth projective curve over $\mathbb{Q}$ whose non-cuspidal points parametrize pairs $[E, C]$ where E is an elliptic curve and $C \subset E$ is a cyclic subgroup of order N. As noted above, the group C defines a unique isogeny $\varphi : E \to E'$ with $\ker(\varphi) = C$, so we may alternatively notate $[E, C]$ with the triple $[E, E', \varphi]$. The following lemma gives a useful description of the residue field of a non-cuspidal point on $X_0(N)$.

Lemma 2.8. *Let $\varphi : E \to E'$ be a cyclic isogeny of non-CM elliptic curves of degree n. Then*

$$\mathbb{Q}(\varphi) = \mathbb{Q}(j(E), j(E'))$$

is the residue field of the induced point $[E, \ker(\varphi)] \in X_0(n)$.

Proof. This follows directly from [15, Corollary A.5]. See also [13, Proposition 3.3]. $\qquad \square$

3. Proof of Theorem 1.3

In this section, we connect the existence of sporadic points $X_1(p^2)$ to Serre's Uniformity Conjecture, as discussed in the introduction. Let $X(p)$ be the compactification of the modular curve which parametrizes isomorphism classes of pairs $(E, (P, Q))$, where E is an elliptic curve and (P, Q) is and $\mathbb{F}_p$-basis of $E[p]$. This is a smooth projective curve defined over $\mathbb{Q}$ whose base change to $\mathbb{Q}(\zeta_p)$ has $p - 1$ connected components.

Theorem 3.1. *Suppose either that there exists finitely many primes p such that $X(p)$ has a sporadic point corresponding to a non-CM elliptic curve with j-invariant in $\mathbb{Q}$ or that all non-CM $\mathbb{Q}$-curves corresponding to sporadic points on $X_1(p^2)$ lie in finitely many isogeny classes, as p varies through all primes. Then there exists a bound C such that for every non-CM elliptic curve $E/\mathbb{Q}$, the mod p representation $\rho_{E,p}$ attached to E is surjective for all $p > C$.*

Proof. We will prove this theorem by showing that for any p large enough, a non-CM elliptic curve $E/\mathbb{Q}$ with non-surjective $\rho_{E,p}$ will induce both a sporadic point on $X(p)$, corresponding to E, and a sporadic point corresponding to a non-CM $\mathbb{Q}$-curve, isogenous to E, on $X_1(p^2)$. Since only finitely many rational j-invariants can lie in a single $\overline{\mathbb{Q}}$-isogeny class,[4] these non-CM $\mathbb{Q}$-curves would necessarily lie in infinitely many geometric isogeny classes. Recall the result of Abramovich [1, Theorem 0.1], which says that the $\mathbb{C}$-gonality $d_{\mathbb{C}}(X_\Gamma)$ of a modular curve X_Γ corresponding to a congruence subgroup Γ satisfies

$$\frac{7}{800} D_\Gamma \leq d_{\mathbb{C}}(X_\Gamma),$$

where D_Γ is the index of Γ in $\mathrm{PSL}_2(\mathbb{Z})$. We have that $D_{\Gamma(p)} = \frac{p(p^2-1)}{2}$ and $D_{\Gamma_1(p^2)} = \frac{p^2(p^2-1)}{2}$. Recall that any point of degree $< d_{\mathbb{C}}(X_\Gamma)/2$ is sporadic on X_Γ (see [26, Proposition 2]).

Suppose now that $E/\mathbb{Q}$ is an elliptic curve without CM, $p > 37$ a prime and that $\rho_{E,p}$ is not surjective. By known results about images of Galois (see e.g. [62, Theorem 1.11]) we know that $\mathrm{im}\,\rho_{E,p}$ is contained in $C_{ns}^+(p)$, the normalizer of the non-split Cartan subgroup. Since $\#C_{ns}^+(p) = 2(p^2-1)$, it follows that $[\mathbb{Q}(E[p]) : \mathbb{Q}] | 2(p^2-1)$, and hence E (together with a basis for $E[p]$) induces a $\mathbb{Q}(E[p])$-rational point on $X(p)$. By Abramovich's bound (see also Remark 7.4. in [14]), it follows that this point is necessarily sporadic for sufficiently large p.

Furthermore, as E has two independent $\mathbb{Q}(E[p])$-rational p-isogenies, it is $\mathbb{Q}(E[p])$-isogenous to an elliptic curve E' which has a $\mathbb{Q}(E[p])$-rational p^2-isogeny f and a point of order p lying in the kernel of f defined over $\mathbb{Q}(E[p])$. In particular, we have

$$\mathrm{im}\,\rho_{E'/\mathbb{Q}(E[p]),p^2} \subseteq \left\{ \begin{pmatrix} 1+pt & * \\ 0 & 1+pk \end{pmatrix} \right\}.$$

Taking the fixed field K' of the subgroup

$$\left\{ \begin{pmatrix} 1 & * \\ 0 & 1+pk \end{pmatrix} \right\},$$

we obtain that K' is of degree $\leq 2p(p^2-1)$ and that E' (which is a $\mathbb{Q}$-curve) has a K'-rational point of order p^2. By Abramovich's bound, we again get that this point is sporadic for sufficiently large p. $\qquad\square$

Remark 3.2. There are infinitely many CM $\mathbb{Q}$-curves (up to isomorphism over $\overline{\mathbb{Q}}$) that give rise to a sporadic point on $X_1(p^2)$ for some prime p, and they lie in infinitely many distinct isogeny classes. To see this, let $E/\overline{\mathbb{Q}}$ be an elliptic curve with complex multiplication by the maximal order in an imaginary quadratic field K. For simplicity, we may assume $j(E) \neq 0, 1728$. Then for any prime $p \geq 5$ that is split in K and $x \in X_1(p^2)$, we have by Theorem 6.2 in [6] that

$$\deg(x) = h_K \cdot \varphi(p^2),$$

where h_K denotes the class number of K. For any prime sufficiently large,

$$h_K < \frac{7}{3200} p(p+1),$$

---

[4]This follows from Lemma 2.8 and the fact that there are only finitely many elliptic curves over $\mathbb{Q}$ in a $\mathbb{Q}$-rational isogeny class. The latter is originally due to Shafarevich; see, for example, Corollary IX.6.2 in [58].

and so
$$\deg(x) < \frac{7}{3200} p(p+1)\varphi(p^2) = \frac{7}{1600} [\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(p^2)] < \frac{1}{2} \mathrm{gon}_{\mathbb{Q}}(X_1(p^2)),$$
where the last inequality follows from by Theorem 0.1 of [1]. Thus x is sporadic by [26, Prop. 2]. Moreover, since the endomorphism algebra $K = \mathrm{End}(E) \otimes \mathbb{Q}$ is an isogeny invariant, it follows that the CM j-invariants corresponding to sporadic points on the curves $X_1(p^2)$ lie in infinitely many distinct $\overline{\mathbb{Q}}$-isogeny classes.

4. DIVISIBILITY CONDITIONS

In this section, we prove that there are certain divisibility conditions which must be satisfied in order for a $\mathbb{Q}$-curve to possess a point of prime-power order defined over a number field of odd degree. As we have seen, any $\mathbb{Q}$-curve E defined over a number field F of odd degree is isogenous to an elliptic curve E' with rational j-invariant by Theorem 2.4. After establishing some preliminary results concerning the Galois representations of isogenous elliptic curves (§4.1), we prove that the existence of a point of order p^k in $E(F)$ implies $[F : \mathbb{Q}]$ is divisible by a power of p controlled by the index of the image of the p-adic Galois representation of an elliptic curve over $\mathbb{Q}$ with j-invariant $j(E')$ (see Lemma 4.6). In §4.3, these results are taken together to prove the following:

Proposition 4.1. *Let E be a non-CM $\mathbb{Q}$-curve defined over a number field F of odd degree. Then E is F-isogenous to an elliptic curve E' with $j(E') \in \mathbb{Q}$. If $E(F)$ has a point of order p^k for some prime number p and $k \in \mathbb{Z}^+$, then $p \in \{2, 3, 5, 7, 11, 13\}$ and the following divisibility conditions hold:*

(1) If $p = 13$, then $3 \cdot 13^{2k-2} \mid [F : \mathbb{Q}]$.
(2) If $p = 11$, then $5 \cdot 11^{2k-2} \mid [F : \mathbb{Q}]$.
(3) If $p = 7$ and $j(E') \neq 3^3 \cdot 5 \cdot 7^5/2^7$, then $7^{2k-2} \mid [F : \mathbb{Q}]$.
(4) If $p = 7$ and $j(E') = 3^3 \cdot 5 \cdot 7^5/2^7$, then $3 \cdot 7^{\max(0, 2k-3)} \mid [F : \mathbb{Q}]$.
(5) If $p = 5$, then $5^{\max(0, 2k-3)} \mid [F : \mathbb{Q}]$.
(6) If $p = 3$, then $3^{\max(0, 2k-4)} \mid [F : \mathbb{Q}]$.
(7) If $p = 2$, then $k \leq 4$.

4.1. **Torsion in Isogeny Classes.** In this section, we study the implications for rational torsion points on an elliptic curve for the Galois representation of an isogenous curve. Though Lemma 4.2 and its corollary are similar to results already in the literature (see, for example, [53, Proposition 1.4] and [18, Lemma 2.5]), the assumptions are slightly different so we include complete proofs. Note that Proposition 4.4 is not used in the proof of our main result, but we include it here as this more refined result may be of independent interest.

Lemma 4.2. *Let E_1/F be an elliptic curve with a point $P \in E_1(F)$ of prime order p and let $\varphi : E_1 \to E_2$ be an isogeny defined over F. Then either $E_2(F)$ has a point of order p or for some basis of $E_2[p]$*
$$\rho_{E_2, p}(\sigma) = \begin{pmatrix} \chi_p(\sigma) & y \\ 0 & 1 \end{pmatrix}, \ \textit{for all } \sigma \in \mathrm{Gal}_F.$$

Proof. Note we may assume φ is cyclic. With respect to the basis $\{P, Q\}$ for $E_1[p]$,
$$\rho_{E_1, p}(\sigma) = \begin{pmatrix} 1 & b \\ 0 & \chi_p(\sigma) \end{pmatrix} \ \text{for all } \sigma \in \mathrm{Gal}_F.$$

If $\varphi(P)$ has order p, we are done, so suppose not. Then $\varphi(Q)$ must have order p, and we have
$$\sigma(\varphi(Q)) = \varphi(\sigma(Q)) = \varphi(bP + \chi_p(\sigma)Q) = \chi_p(\sigma)\varphi(Q).$$

Thus if $E_2[p] = \{\varphi(Q), R\}$, we see

$$\rho_{E_2,p}(\sigma) = \begin{pmatrix} \chi_p(\sigma) & b \\ 0 & 1 \end{pmatrix} \text{ for all } \sigma \in \mathrm{Gal}_F. \qquad \square$$

Corollary 4.3. *Let E be an elliptic curve defined over a number field F which is isogenous over F to an elliptic curve E'. If $P \in E(F)$ is a point of prime order p, then:*

(1) *E' has a point of order p over $F(\zeta_p)$.*
(2) *E' has a rational point of order p over an extension of F of degree dividing p.*

Proof. Let $\varphi : E \to E'$ be an isogeny, where E, E', and φ are defined over F. By Lemma A.1 in [15], we may assume φ is cyclic. If $E'(F)$ has a point of order p, we are done, so suppose not. Then in particular, $\varphi(P) = O$. By Lemma 4.2 there is a basis of $E'[p]$ such that

$$\mathrm{im}\,\rho_{E',p} = \left\{ \begin{pmatrix} \chi_p(\mathrm{Gal}_F) & * \\ 0 & 1 \end{pmatrix} \right\},$$

where χ_p is the mod p cyclotomic character and $*$ is nonzero. Part (1) follows immediately. As shown in the proof of [15, Proposition 4.1], E' attains a rational point of order p over an extension of degree p, proving part 2. $\qquad \square$

Proposition 4.4. *Suppose E_1/F is an elliptic curve with a point $P \in E_1(F)$ of order N and $\{P, Q\}$ is a basis for $E_1[N]$, and let $\varphi : E_1 \to E_2$ be an m-isogeny with $m \mid N$ and $\ker \varphi = \langle (N/m)P \rangle$. Then with respect to the basis $\{\varphi(Q), R\}$, where $R \in E[N]$ satisfies $mR = \varphi(P)$,*

$$\rho_{E_2,N}(\sigma) = \begin{pmatrix} \chi_N(\sigma) & y \\ z & 1 \end{pmatrix}, \text{ where } y \equiv 0 \pmod{N/m}, z \equiv 0 \pmod{m}.$$

Proof. Let $\sigma \in \mathrm{Gal}_F$. Let P be a point of order N in $E_1(F)$, and fix a basis $\{P, Q\}$ for $E_1[N]$ and $\{\varphi(Q), R\}$ for $E_2[N]$. As $\varphi(P)$ is a point of order N/m independent with $m\varphi(Q)$ in $E_2[N/m]$ we can choose R such that $mR = \varphi(P)$ and which will necessarily be independent to $\varphi(Q)$. With respect to these bases, we have

$$\rho_{E_1,N}(\sigma) = \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \text{ and } \rho_{E_2,N}(\sigma) = \begin{pmatrix} x & y \\ z & w \end{pmatrix}.$$

Since

$$(mR)^\sigma = \varphi(P)^\sigma = \varphi(P^\sigma) = \varphi(P) = mR,$$

we can conclude that $y \equiv 0 \pmod{N/m}$.

We have

$$\varphi(Q)^\sigma = \varphi(Q^\sigma) = \varphi(bP + dQ) = b\varphi(P) + d\varphi(Q) = bmR + d\varphi(Q),$$

so we conclude that $x = d$ and $z \equiv 0 \pmod m$. Since

$$d = \det \rho_{E_1,N}(\sigma) = \chi_N(\sigma) = \det \rho_{E_2,N}(\sigma) = xw - yz = dw - yz,$$

and $yz \equiv 0 \pmod N$, we conclude that $w = 1$. $\qquad \square$

4.2. General Divisibility Conditions.

Lemma 4.5. *Let p be a prime number, and let E/F be a non-CM elliptic curve isogenous over F to an elliptic curve $E'/\mathbb{Q}$. Then*

$$[\mathrm{GL}_2(\mathbb{Z}_p) : \mathrm{im}\,\rho_{E/F,p^\infty}] = [\mathrm{GL}_2(\mathbb{Z}_p) : \mathrm{im}\,\rho_{E'/\mathbb{Q},p^\infty}] \cdot [F \cap \mathbb{Q}(E'[p^\infty]) : \mathbb{Q}].$$

Proof. Over F, the images of ρ_{E,p^∞} and ρ_{E',p^∞} have the same index in $\mathrm{GL}_2(\mathbb{Z}_p)$ since the curves are isogenous, i.e.,

$$[\mathrm{GL}_2(\mathbb{Z}_p) : \mathrm{im}\,\rho_{E/F,p^\infty}] = [\mathrm{GL}_2(\mathbb{Z}_p) : \mathrm{im}\,\rho_{E'/F,p^\infty}].$$

See, for example, §2.1 of [31]. The claim will follow from the fact that

$$[\mathrm{GL}_2(\mathbb{Z}_p) : \mathrm{im}\,\rho_{E'/F,p^\infty}] = [\mathrm{GL}_2(\mathbb{Z}_p) : \mathrm{im}\,\rho_{E'/\mathbb{Q},p^\infty}] \cdot [F \cap \mathbb{Q}(E'[p^\infty]) : \mathbb{Q}].$$

Indeed, by Galois theory (see, for example, Proposition 7.14 in [50]),

$$\mathrm{im}\,\rho_{E'/F,p^\infty} \cong \mathrm{Gal}(F(E'[p^\infty])/F) \cong \mathrm{Gal}(\mathbb{Q}(E'[p^\infty])/F \cap \mathbb{Q}(E'[p^\infty])).$$

Thus we may view $\mathrm{im}\,\rho_{E'/F,p^\infty}$ as a subgroup of $\mathrm{im}\,\rho_{E'/\mathbb{Q},p^\infty}$ of index $[F \cap \mathbb{Q}(E'[p^\infty]) : \mathbb{Q}]$. $\qquad\square$

Lemma 4.6. *Let E/F be a non-CM elliptic curve with a point $P \in E(F)$ of order p^k, where p is a prime number. If E is F-isogenous to an elliptic curve E' with $j(E') \in \mathbb{Q}$, then $[F : \mathbb{Q}]$ is divisible by*

$$\begin{cases} p^{\max(0,2k-2-d)} & \text{if } p \text{ is odd} \\ p^{\max(0,2k-2-d-1)} & \text{if } p = 2, \end{cases}$$

where $d = \mathrm{ord}_p([\mathrm{GL}_2(\mathbb{Z}_p) : \mathrm{im}\,\rho_{E''/\mathbb{Q},p^\infty}])$ for any elliptic curve $E''/\mathbb{Q}$ with $j(E'') = j(E')$.

Proof. Let E/F be a non-CM elliptic curve with $P \in E(F)$ of order p^k, and suppose $\varphi : E \to E'$ is an F-rational isogeny. Replacing F with at worst a quadratic extension L/F, we may view φ as an L-isogeny from E to an elliptic curve $E''/\mathbb{Q}$ with $j(E'') = j(E')$. Since E has a rational point of order p^k over L, we have $\mathrm{Gal}(L(E[p^k])/L)$ is contained in the group of matrices in $\mathrm{GL}_2(\mathbb{Z}/p^k/\mathbb{Z})$ of the form

$$\left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\}.$$

Thus $\#\mathrm{Gal}(L(E[p^k])/L) \mid p^k \cdot \varphi(p^k) = p^{2k-1}(p-1)$, and it follows that

$$\mathrm{ord}_p([\mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z}) : \mathrm{im}\,\rho_{E/L,p^k}]) \geq 2k-2.$$

Thus $p^{2k-2} \mid [\mathrm{GL}_2(\mathbb{Z}_p) : \mathrm{im}\,\rho_{E''/\mathbb{Q},p^\infty}] \cdot [L \cap \mathbb{Q}(E''[p^\infty]) : \mathbb{Q}]$ by Lemma 4.5. If $d = \mathrm{ord}_p([\mathrm{GL}_2(\mathbb{Z}_p) : \mathrm{im}\,\rho_{E''/\mathbb{Q},p^\infty}])$, then since L is at most a quadratic extension of F, it follows that

$$p^{\max(0,2k-2-d)} \mid [F : \mathbb{Q}]$$

if p is odd and

$$p^{\max(0,2k-2-d-1)} \mid [F : \mathbb{Q}]$$

if $p = 2$. $\qquad\square$

4.3. **Proof of Proposition 4.1.** Suppose E/F is a non-CM $\mathbb{Q}$-curve, where $[F : \mathbb{Q}]$ is odd, and suppose $E(F)$ contains a point of order p^k. Then $p \in \{2, 3, 5, 7, 11, 13, 17, 37\}$ by Theorem 1.1 in [15], and by Theorem 2.4, there exists a rational isogeny $\varphi : E \to E'$ such that $j(E') \in \mathbb{Q}$. By Lemma 4.6, we have that $[F : \mathbb{Q}]$ is divisible by

$$\begin{cases} p^{\max(0,2k-2-d)} & \text{if } p \text{ is odd} \\ p^{\max(0,2k-2-d-1)} & \text{if } p = 2, \end{cases}$$

where $d = \mathrm{ord}_p([\mathrm{GL}_2(\mathbb{Z}_p) : \mathrm{im}\,\rho_{E''/\mathbb{Q},p^\infty}])$ for any elliptic curve $E''/\mathbb{Q}$ with $j(E'') = j(E')$. Since E'' and E' are isomorphic over an extension L/F of degree at most 2, we may also view $\varphi : E \to E''$ as an isogeny over L.

Since E has a p-isogeny defined over F, so does E' by Proposition 3.2 of [15]. If p is odd, then since F has odd degree, it follows by Proposition 3.3 in [15] that E'' has a rational cyclic p-isogeny

11

over $\mathbb{Q}$ or else $p = 7$ and $j(E') = 3^3 \cdot 5 \cdot 7^5/2^7$. Thus unless $j(E') = 3^3 \cdot 5 \cdot 7^5/2^7$ and $p = 7$, an upper bound for d is given by Proposition 2.1. In particular, we note that $k \leq 4$ if $p = 2$.

If $j(E') = 3^3 \cdot 5 \cdot 7^5/2^7$, then $\# \operatorname{im} \rho_{E''/\mathbb{Q},7} = 18$ or 36. By [9, Lemma 21], the 7-adic Galois representation of $E''/\mathbb{Q}$ has level 7, and so together these imply

$$\operatorname{ord}_7([\operatorname{GL}_2(\mathbb{Z}_7) : \operatorname{im} \rho_{E''/\mathbb{Q},7^\infty}]) = 1,$$

$$\operatorname{ord}_3([\operatorname{GL}_2(\mathbb{Z}_7) : \operatorname{im} \rho_{E''/\mathbb{Q},7^\infty}]) = 0.$$

Since E has a rational point of order 7^k over L, as in the proof of Lemma 4.6 we have $\# \operatorname{Gal}(L(E[7^k])/L) \mid 7^{2k-1} \cdot 6$, and so

$$\operatorname{ord}_7([\operatorname{GL}_2(\mathbb{Z}/7^k\mathbb{Z}) : \operatorname{im} \rho_{E/L,7^k}]) \geq 2k - 2,$$

$$\operatorname{ord}_3([\operatorname{GL}_2(\mathbb{Z}/7^k\mathbb{Z}) : \operatorname{im} \rho_{E/L,7^k}]) \geq 1.$$

By Lemma 4.5, we have $3 \cdot 7^{2k-2} \mid [\operatorname{GL}_2(\mathbb{Z}_7) : \operatorname{im} \rho_{E''/\mathbb{Q},7^\infty}] \cdot [L \cap \mathbb{Q}(E''[7^\infty]) : \mathbb{Q}]$, and the computations above on the index of $\operatorname{im} \rho_{E''/\mathbb{Q},7^\infty}$ in $\operatorname{GL}_2(\mathbb{Z}_7)$ imply $3 \cdot 7^{\max(0,2k-3)} \mid [L \cap \mathbb{Q}(E''[13^\infty]) : \mathbb{Q}]$. Thus

$$3 \cdot 7^{\max(0,2k-3)} \mid [F : \mathbb{Q}].$$

as desired.

Now, suppose $p \geq 11$. Since $E(L)$ has a point of order p, by Corollary 4.3 the curve E'' gains a point of order p over an extension L'/L of degree dividing p. As $\operatorname{ord}_2([L : \mathbb{Q}]) \leq 1$, the classification of mod p images of elliptic curves over $\mathbb{Q}$ with a rational cyclic p-isogeny (see, for example, Tables 1 and 2 in [28], which is complete for elliptic curves with a p-isogeny by [63]) implies

$$5 \mid [F : \mathbb{Q}] \text{ if } p = 11,$$

$$3 \mid [F : \mathbb{Q}] \text{ if } p = 13,$$

and that we reach a contradiction if $p = 17$ or 37.

5. Proof of Theorem 1.5

In this section, we prove Theorem 1.5. The first part of the theorem, which implies that there are no sporadic points of odd degree on $X_1(p^k)$ corresponding to non-CM $\mathbb{Q}$-curves, is proven in §5.1. We show that the divisibility conditions established in Section 4 are sufficient to prove the degree of such a point is greater than or equal to the $\mathbb{Q}$-gonality of $X_1(p^k)$, using bounds implied by work of Derickx and van Hoeij [22]. On the other hand, it can be deduced from work of Bourdon and Pollack [10] that there are infinitely many CM points of odd degree on these curves; see §5.2.

5.1. **Non-CM Sporadic Points of Odd Degree.**

Theorem 5.1. *Let p be a prime number. If $x = [E, P] \in X_1(p^k)$ is a point of odd degree corresponding to a non-CM $\mathbb{Q}$-curve, then $\deg(x) \geq \operatorname{gon}_{\mathbb{Q}}(X_1(p^k))$. In particular, x is not sporadic.*

Proof. Let $x = [E, P] \in X_1(p^k)$ be a point of odd degree corresponding to a non-CM $\mathbb{Q}$-curve. By Proposition 4.1, we know $p \in \{2, 3, 5, 7, 11, 13\}$. We will consider each case separately. Claims about the $\mathbb{Q}$-gonality of $X_1(N)$ follow from Table 1 in work of Derickx and van Hoeij [22].

- Suppose $p = 13$. Then $3 \cdot 13^{2k-2} \mid [\mathbb{Q}(x) : \mathbb{Q}]$ by Proposition 4.1. Since $\operatorname{gon}_{\mathbb{Q}}(X_1(13)) = 2$, it follows that $\operatorname{gon}_{\mathbb{Q}}(X_1(13^k))$ is at most

$$2 \cdot \deg(X_1(13^k) \to X_1(13)) = 2 \cdot (13^{k-1})^2 = 2 \cdot 13^{2k-2},$$

  and $\deg(x) > \operatorname{gon}_{\mathbb{Q}}(X_1(13^k))$.

- Suppose $p = 11$. Then $5 \cdot 11^{2k-2} \mid [\mathbb{Q}(x) : \mathbb{Q}]$ by Proposition 4.1. Since $\mathrm{gon}_{\mathbb{Q}}(X_1(11)) = 2$, it follows that $\mathrm{gon}_{\mathbb{Q}}(X_1(11^k))$ is at most

$$2 \cdot \deg(X_1(11^k) \to X_1(11)) = 2 \cdot (11^{k-1})^2 = 2 \cdot 11^{2k-2},$$

  and $\deg(x) > \mathrm{gon}_{\mathbb{Q}}(X_1(11^k))$.
- Suppose $p = 7$. Since $X_1(7)$ is genus 0, we may assume $k \geq 2$. Then $7^{2k-2} \mid [\mathbb{Q}(x) : \mathbb{Q}]$ or $3 \cdot 7^{2k-3} \mid [\mathbb{Q}(x) : \mathbb{Q}]$ by Proposition 4.1. Since $\mathrm{gon}_{\mathbb{Q}}(X_1(7^2)) \leq 21$, it follows that $\mathrm{gon}_{\mathbb{Q}}(X_1(7^k))$ is at most

$$21 \cdot \deg(X_1(7^k) \to X_1(7^2)) = 21 \cdot (7^{k-2})^2 = 3 \cdot 7^{2k-3},$$

  and $\deg(x) \geq \mathrm{gon}_{\mathbb{Q}}(X_1(7^k))$.
- Suppose $p = 5$. Since $X_1(5)$ is genus 0, we may assume $k \geq 2$. Then $5^{2k-3} \mid [\mathbb{Q}(x) : \mathbb{Q}]$ by Proposition 4.1. Since $\mathrm{gon}_{\mathbb{Q}}(X_1(25)) = 5$, it follows that $\mathrm{gon}_{\mathbb{Q}}(X_1(5^k))$ is at most

$$5 \cdot \deg(X_1(5^k) \to X_1(25)) = 5 \cdot (5^{k-2})^2 = 5^{2k-3},$$

  and $\deg(x) \geq \mathrm{gon}_{\mathbb{Q}}(X_1(5^k))$.
- Suppose $p = 3$. Since $X_1(3)$ and $X_1(9)$ are genus 0, we will assume $k \geq 3$. Then $3^{2k-4} \mid [\mathbb{Q}(x) : \mathbb{Q}]$ by Proposition 4.1. Since $\mathrm{gon}_{\mathbb{Q}}(X_1(27)) = 6$, it follows that $\mathrm{gon}_{\mathbb{Q}}(X_1(3^k))$ is at most

$$6 \cdot \deg(X_1(3^k) \to X_1(27)) = 6 \cdot (3^{k-3})^2 = 2 \cdot 3^{2k-5} < 3 \cdot 3^{2k-5} = 3^{2k-4},$$

  and $\deg(x) > \mathrm{gon}_{\mathbb{Q}}(X_1(3^k))$.
- Suppose $p = 2$. Then $k \leq 4$ by Proposition 4.1. If $k \leq 3$, then $X_1(2^k)$ is genus 0. As $\mathrm{gon}_{\mathbb{Q}}(X_1(16)) = 2$ and no non-cuspidal rational points by [45], again the claim follows. $\square$

5.2. Existence of Sporadic CM Points of Odd Degree.

Proposition 5.2. *For any $p \equiv 3 \pmod 4$, there exist sporadic CM points of odd degree on $X_1(p^k)$ for k sufficiently large.*

Remark 5.3. We note that by work of Aoki [2, Cor. 9.4], there is no CM point of odd degree on $X_1(p^k)$ if p is a prime with $p \equiv 1 \pmod 4$.

Proof. For a prime $p \equiv 3 \pmod 4$ and $n \in \mathbb{Z}^+$ we define δ as follows:

$$\delta := \begin{cases} \lfloor 3n/2 \rfloor - 1, & p > 3, \\ 0, & p = 3 \text{ and } n = 1, \\ \lfloor 3n/2 \rfloor - 2, & p = 3 \text{ and } n \geq 2. \end{cases}$$

By [10, Thm 2.6] there exists a CM point $x \in X_1(p^n)$ of odd degree

$$\deg(x) = h_{\mathbb{Q}(\sqrt{-p})} \cdot \frac{p-1}{2} p^{\delta},$$

where $h_{\mathbb{Q}(\sqrt{-p})}$ denotes the class number of $\mathbb{Q}(\sqrt{-p})$. For n sufficiently large, we will have

$$h_{\mathbb{Q}(\sqrt{-p})} < \frac{7}{1600} p^{2n - \lfloor 3n/2 \rfloor}.$$

In particular, this forces $n > 1$ if $p = 3$. Thus by Theorem 0.1 of [1],

$$\deg(x) < \frac{7}{1600} [\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(p^n)] \leq \frac{1}{2} \mathrm{gon}_{\mathbb{Q}}(X_1(p^n)),$$

and x is sporadic by [26, Prop. 2]. $\square$

Remark 5.4. Suppose $p \equiv 3 \pmod{4}$ is prime. By [2, Cor. 9.4], a CM elliptic curve with a point of order p^n over an odd degree number field has CM by an order in $\mathbb{Q}(\sqrt{-p})$. Thus for distinct primes $p \equiv 3 \pmod{4}$ the sporadic points of Proposition 5.2 necessarily come from CM elliptic curves that are not isomorphic over $\overline{\mathbb{Q}}$. Said another way, if $\mathcal{I}_{\mathrm{odd}}$ is the set of all sporadic points of odd degree on all curves $X_1(N)$ for $N \in \mathbb{Z}^+$, then $j(\mathcal{I}_{\mathrm{odd}})$ contains infinitely many CM j-invariants. Moreover, since the endomorphism algebra $\mathrm{End}(E) \otimes \mathbb{Q}$ is an isogeny invariant, these CM elliptic curves lie in infinitely many distinct $\overline{\mathbb{Q}}$-isogeny classes.

6. Beyond Powers of a Single Prime

In fact, studying points of odd degree on $X_1(p^k)$ associated to non-CM $\mathbb{Q}$-curves is not far from the case of such points of odd degree on $X_1(n)$. Since any such $\mathbb{Q}$-curve E is isogenous to an elliptic curve E' with rational j-invariant, it follows that E' corresponds to a point of odd degree on $X_0(p)$ for any odd prime p dividing n. As shown in [15, Proposition 3.3], this generally implies that E' must in fact correspond to a point in $X_0(p)(\mathbb{Q})$. Thus the support of n is constrained by the possible rational isogenies of elliptic curves over $\mathbb{Q}$, as in Theorem 2.2. This can be used to prove the following result, which generalizes [9, Theorem 3].

Proposition 6.1. *Let $x = [E, P] \in X_1(N)$ be a point of odd degree, where E is a non-CM $\mathbb{Q}$-curve. Then $N = 2^a p^k$ for $p \in \{3, 5, 7, 11, 13\}$ unless E is in the isogeny class of an elliptic curve over $\mathbb{Q}$ with a rational cyclic 21-isogeny. If $k > 0$, then we obtain the following bounds on a:*

  (1) If $p = 3$, then $a \leq 2$.
  (2) If $p = 5$, then $a \leq 1$.
  (3) If $p = 7$, then $a \leq 2$.
  (4) If $p = 11$, then $a \leq 1$.
  (5) If $p = 13$, then $a \leq 1$.

After establishing a preliminary lemma in §6.1, we prove Proposition 6.1 in §6.2. From the proof of Proposition 6.1, we also deduce the following:

Corollary 6.2. *Let $x \in X_1(4 \cdot p^k)$ be a point of odd degree associated to a non-CM $\mathbb{Q}$-curve E, where $k > 0$. Then:*

  (1) If $p = 3$ and E is not isogenous to E' with $j(E') \in \{3^2 \cdot 23^3/2^6, -3^3 \cdot 11^3/2^2\}$, then E is $\overline{\mathbb{Q}}$-isogenous to an elliptic curve $E''/\mathbb{Q}$ with a rational cyclic 6-isogeny or with a rational cyclic 3-isogeny and full 2-torsion (but no 4-isogeny) in a cubic extension.
  (2) If $p = 7$ and E is not isogenous to E' with $j(E') \in \{-3^3 \cdot 13 \cdot 479^3/2^{14}, 3^3 \cdot 13/2^2\}$, then E is $\overline{\mathbb{Q}}$-isogenous to an elliptic curve $E''/\mathbb{Q}$ with a rational cyclic 7-isogeny and full 2-torsion (but no 4-isogeny) in a cubic extension.

6.1. **A Preliminary Result.**

Lemma 6.3. *Let E and E' be non-CM elliptic curves which are F-isogenous and suppose that E has a p^n-isogeny over F. Then E' has either 2 independent F-isogenies of degrees p^{n-t} and p^t for some t, or E' has a p^a-isogeny over F, where $a \geq \min\{n, 1 + \frac{n}{2}\}$.*

Proof. Let $f : E \to E'$ be a cyclic F-isogeny (which is unique up to sign). If $\deg f$ is coprime to p, then E' has a p^n-isogeny defined over F and we are done. If $\deg f = p^t \cdot b$ where $(b, p) = 1$, then there exists a curve E_0 which is b-isogenous to E' and its p-adic representation will be the same as that of E', so will have the same degrees of p-power isogenies as E'. Hence we can suppose without loss of generality that $\deg f = p^t$, as otherwise we work with E_0 instead of E'.

Let $f_1 : E \to E_1$ be the p^n-isogeny that E has by our assumptions. If $\ker f_1 \cap \ker f = \{O\}$, then $f_1 \circ \hat{f}$ is a p^{t+n}-isogeny over F and we are done. If $\ker f_1 \supseteq \ker f$ then f_1 factors as $f_1 = f_2 \circ f$,

14

where $f_2 : E' \to E_1$ is a p^{n-t}-isogeny over F which is independent with the p^t-isogeny $\hat{f} : E' \to E$. If $\ker f \supseteq \ker f_1$, then we have $t \geq n$ and the isogeny p^t-isogeny $\hat{f} : E' \to E$ again completes this case.

Suppose finally that $\ker f_1 \cap \ker f \neq \{O\}$ and that neither of $\ker f_1$ and $\ker f$ is contained in the other (this implies $n, t \geq 2$). Then there exists an elliptic curve E_2 and a p^m-isogeny $f_2 : E \to E_2$ defined over F such that both f and f_1 factor through f_2; we choose E_2 and m such that m is the largest integer satisfying this condition. Let $f = f_3 \circ f_2$ and $f_1 = f_4 \circ f_2$. Now we see that $\hat{f} : E' \to E$ is a p^t-isogeny over F and $f_4 \circ \hat{f_3} : E' \to E_1$ is an $p^{(t-m)+(n-m)}$-isogeny over F. We have $1 \leq m < t$ and $m < n$, so if $m \geq \frac{n}{2}$, then we have $t = (t-m) + m \geq 1 + \frac{n}{2}$ and if $m < \frac{n}{2}$, then $(t-m) + (n-m) \geq 1 + \frac{n}{2}$. $\qquad\square$

6.2. **Proof of Proposition 6.1.** Let $F \coloneqq \mathbb{Q}(x)$, and fix a model of E/F with $P \in E(F)$. By Proposition 4.1, $\mathrm{Supp}(N) \subseteq \{2, 3, 5, 7, 11, 13\}$. By Theorem 2.4, there exists an F-rational isogeny $\varphi : E \to E'$ such that $j(E') \in \mathbb{Q}$. Let $p \mid N$ be prime. Since E has a p-isogeny defined over F, so does E' by Proposition 3.2 of [15]. If p is odd, then since F has odd degree, it follows by Proposition 3.3 in [15] that any $E''/\mathbb{Q}$ with $j(E'') = j(E')$ has a rational cyclic p-isogeny or else $p = 7$ and $j(E') = 3^3 \cdot 5 \cdot 7^5/2^7$.

For now, suppose $j(E') \neq 3^3 \cdot 5 \cdot 7^5/2^7$. If distinct odd primes p, q divide N, then $E''/\mathbb{Q}$ has a rational cyclic pq-isogeny. By the classification of rational isogenies over $\mathbb{Q}$ (see Theorem 2.2), this cannot happen unless E'' has a rational cyclic 15- or 21-isogeny. By the theorem statement, it suffices to consider the case where E'' has a rational cyclic 15-isogeny. For the sake of contradiction assume $N = 2^a 3^b 5^c$ for $b, c > 0$. By Corollary 4.3, there is an extension F_1/F of degree dividing 3 such that $E'(F_1)$ has a point of order 3. Similarly, there is an extension F_2/F of degree dividing 5 such that $E'(F_2)$ has a point of order 5. It follows that E' has a point of order 15 over $F_1 F_2$, which has odd degree over $\mathbb{Q}$. This contradicts Proposition 15 in [9]. If $j(E') = 3^3 \cdot 5 \cdot 7^5/2^7$, then E'' has no rational isogenies over $\mathbb{Q}$, so it does not gain a p-isogeny, for odd primes $p \neq 7$, over any odd degree number field; the first part of the result follows.

Now, suppose $b > 0$. Suppose first that E'' has a 2-torsion point over $\mathbb{Q}$, which implies by Theorem 2.2 that $p \leq 7$. Then any subgroup of $\rho_{E'', 2^\infty}(\mathrm{Gal}_\mathbb{Q})$ will be of order which is a power of 2, from which we conclude that $\rho_{E'', 2^\infty}(\mathrm{Gal}_\mathbb{Q}) = \rho_{E'', 2^\infty}(\mathrm{Gal}_F)$. Thus all the 2-power isogenies of E'' which are defined over F are already defined over $\mathbb{Q}$. So, by Lemma 6.3 it follows that if $a \geq 3$, E'' has either an 8-isogeny or a 4-isogeny which is independent to a 2-isogeny. But now it is not possible that $b > 0$, as now it would follow that E'' has an $8p$-isogeny over $\mathbb{Q}$, or is isogenous over $\mathbb{Q}$ to an elliptic curve with an $8p$-isogeny over $\mathbb{Q}$. If $a = 2$, then Lemma 6.3 implies $E''/\mathbb{Q}$ has either a 4-isogeny or independent 2-isogenies, and thus E'' is isogenous over $\mathbb{Q}$ to an elliptic curve with a rational cyclic $4p$-isogeny. This cannot happen if $p = 5, 7$.

The case when E'' has no 2-torsion point over $\mathbb{Q}$ remains. Hence E'' gains a point of order 2 over a cubic field K. Since $\rho_{E'', 2^\infty}(\mathrm{Gal}_K) = \rho_{E'', 2^\infty}(\mathrm{Gal}_F)$, if follows that if E'' has a 2^k-isogeny over F then this same isogeny is defined over K. By Lemma 6.3 if $a > 1$, then in particular E'' has either a K-rational 4-isogeny or full 2-torsion over K. If $a \geq 3$, then by Lemma 6.3, E'' has a 4-isogeny over K.

If $E''/\mathbb{Q}$ has a cyclic 4-isogeny over K, it follows that E'' has a point of order 4 over K or over a quadratic extension of K. By the classification of 2-adic images due to Rouse and Zureick-Brown [54] (see, in particular, the data file 2primary_Ss.txt associated to [27]), this means E'' corresponds to a rational point on the modular curve $X20$. Recall that if $j(E'') \neq 3^3 \cdot 5 \cdot 7^5/2^7$, then E'' also has a rational cyclic p-isogeny.

(1) If E'' corresponds to a rational point on the fiber product of $X20$ and $X_0(3)$, then $j(E'') = 3^2 \cdot 23^3/2^6$ or $-3^3 \cdot 11^3/2^2$ by [16, Prop. 6]. An elliptic curve with either j-invariant gives points on $X_0(8)$ of even degree only, so $\mathrm{ord}_2(\deg(\varphi)) \leq 2$. Suppose for the sake of

contradiction that $E(F)$ has a point of order 8. Then some elliptic curve 2-isogenous to E'' must correspond to a point of odd degree on $X_1(4)$. A Magma computation shows no such curve exists; see the research website of either author.

(2) The fiber product of $X20$ and $X_0(5)$ has only cusps by [16, Prop. 6k].

(3) If E'' corresponds to a rational point on the fiber product of $X20$ and $X_0(7)$, then $j(E'') = -3^3 \cdot 13 \cdot 479^3/2^{14}$ or $3^3 \cdot 13/2^2$ by [16, Prop. 6s]. As in the fiber product of $X20$ and $X_0(3)$, these two elliptic curves give no points of odd degree on $X_0(8)$, and no elliptic curve 2-isogenous to E'' gives a point on $X_1(4)$ of odd degree. Thus $a \leq 2$. In this case, it is possible that $E''/\mathbb{Q}$ does not have a rational cyclic 7-isogeny, but then $j(E'') = 3^3 \cdot 5 \cdot 7^5/2^7$. Suppose E'' is an elliptic curve with $j(E'') = 3^3 \cdot 5 \cdot 7^5/2^7$ and let $\psi_{E''}(n)$ be its n-th division polynomial. We check that $\psi_{E''}(4)/\psi_{E''}(2)$, the polynomial whose roots are x-coordinates of points of order 4 on E'' and hence generate the fields over which E'' has a 4-isogeny, is an irreducible degree 6 polynomial, so we conclude that E'' has no 4-isogenies over any odd degree number field.

(4) If E'' corresponds to a rational point on $X_0(11)$, then $j(E'') = -11 \cdot 131^3$ or -11^2 (see, for example, [46, Table 4]). As before, we may choose a specific elliptic curve over $\mathbb{Q}$ with each j-invariant and use division polynomials to show E'' does not have a 4-isogeny over any odd degree number field.

(5) The fiber product of $X3$ and $X_0(13)$ has only cuspidal rational points by [17, Table 8], and thus so does the fiber product of $X20$ and $X_0(13)$ since $X20$ covers $X3$.

Suppose now E'' has full 2-torsion over K but no 4-isogeny; in particular, as noted above, this can happen only if $a \leq 2$. Then $\rho_{E'',2}(\mathrm{Gal}_\mathbb{Q})$ is cyclic and we see that $p \neq 5, 13$ by [17, Tables 8 & 11] and $p \neq 11$ by checking that the curves with 11-isogenies over $\mathbb{Q}$ (i.e $j(E'') \in \{-11 \cdot 131^3, -11^2\}$) have surjective mod 2 representations. Hence the only remaining possibilities are $p = 3, 7$. We see that $j(E'') = 3^3 \cdot 5 \cdot 7^5/2^7$ does not appear in this case as for E with this j-invariant $\mathrm{im}\,\rho_{E,2} \simeq S_3$.

7. Proof of Theorem 1.4

In this section, we prove our main result: If $x \in X_1(N)$ is a point of odd degree corresponding to a non-CM $\mathbb{Q}$-curve E and $\deg(x) < \mathrm{gon}_\mathbb{Q}(X_1(N))$, then E belongs to the $\overline{\mathbb{Q}}$-isogeny class of an elliptic curve with j-invariant $-140625/8$. By Proposition 6.1 and Theorem 1.5, it suffices to address the case where $N = 2p^b$ or $4p^b$ for an odd prime p. If $p > 3$, the general strategy is to show that the existence of such a low degree point would force a point on $X_1(2p)$ or $X_1(4p)$ which is known not to exist. (See §7.1.) This is inspired by the approach of [8] and [9], with the distinction being that the point on $X_1(2p)$ or $X_1(4p)$ is associated to an elliptic curve in the $\overline{\mathbb{Q}}$-isogeny class of E rather than E itself. The prime $p = 3$, addressed in §7.2, requires a different approach. There, we show such a low degree point on $X_1(2 \cdot 3^k)$ or $X_1(4 \cdot 3^k)$ would force the existence of an elliptic curve over $\mathbb{Q}$ with unexpected entanglement between its 2- and 27-torsion point fields. These elliptic curves correspond to rational points on one of 10 possible curves, all of which have genus at least 2. In §7.3, we determine the elliptic curves which correspond to rational points on each of these 10 curves and show that none are $\overline{\mathbb{Q}}$-isogenous to a non-CM elliptic curve producing a point of odd degree on $X_1(N)$ with $\deg(x) < \mathrm{gon}_\mathbb{Q}(X_1(N))$.

7.1. **Points on $X_1(2^a p^k)$ for $p > 3$.** In this section, we show if $p > 3$ is prime, there are no sporadic points of odd degree on $X_1(2p^k)$ associated to non-CM $\mathbb{Q}$-curves. We also show that there are no sporadic points of odd degree $X_1(4 \cdot 7^k)$ associated to a non-CM $\mathbb{Q}$-curve E.

Lemma 7.1. *Let p be prime. Suppose E/F is a non-CM elliptic curve with $[E, C] \in X_0(p)(\mathbb{Q}(j(E)))$. If $Q \in E(F)$ is a point of order p, then there is a subfield of F of degree dividing $\frac{p-1}{2} \cdot [\mathbb{Q}(j(E)) : \mathbb{Q}]$ that is the residue field of a point on $X_1(p)$ associated to either E or E/C.*

Proof. If $\langle Q \rangle = C$, the result follows by [7, Thm. 5.5], so suppose not. Let $\varphi : E \to E' := E/C$, viewed as an isogeny of elliptic curves over F. Then $\varphi(Q) \in E'(F)$ is a point of order p, and since $\hat{\varphi}(\varphi(Q)) = [p]Q = O$ this point generates $\ker(\hat{\varphi})$. Since $[E', \ker(\hat{\varphi})] \in X_0(p)(\mathbb{Q}(j(E))$, the residue field of $[E', \varphi(Q)] \in X_1(p)$ has degree dividing $\frac{p-1}{2} \cdot [\mathbb{Q}(j(E)) : \mathbb{Q}]$ by [7, Thm. 5.5] and is contained in F, as desired. $\qquad\square$

Proposition 7.2. *Suppose $x \in X_1(2p^k)$ is a point of odd degree corresponding to a non-CM $\mathbb{Q}$-curve, where $p \geq 5$ is prime. Then $\deg(x) \geq \mathrm{gon}_{\mathbb{Q}}(X_1(2p^k))$. In particular, x is not sporadic.*

Proof. Let $F := \mathbb{Q}(x)$, and let E/F be the non-CM $\mathbb{Q}$-curve associated to x with an F-rational point of order $2p^k$. Suppose $\deg(x) < \mathrm{gon}_{\mathbb{Q}}(X_1(2p^k))$. Since $X_1(2)$ and $X_1(10)$ have genus 0, we may always assume $k \geq 1$ and that $k \geq 2$ if $p = 5$. By Theorem 2.4, there exists an F-rational isogeny $\varphi : E \to E'$ such that $j(E') \in \mathbb{Q}$. In this case, it follows from Proposition 2.3 that there exists a cyclic subgroup C of E' such that $[E', C] \in X_0(p)(\mathbb{Q})$ or else $p = 7$ and $j(E') = 3^3 \cdot 5 \cdot 7^5/2^7$.

For now, suppose that if $p = 7$ then $j(E') \neq 3^3 \cdot 5 \cdot 7^5/2^7$. From Proposition 4.1, we have $p \in \{5, 7, 11, 13\}$ and $d_0 \mid [F : \mathbb{Q}]$ where

$$d_0 = \begin{cases} 5^{2k-3} & \text{if } p = 5, \\ 7^{2k-2} & \text{if } p = 7, \\ 5 \cdot 11^{2k-2} & \text{if } p = 11, \\ 3 \cdot 13^{2k-2} & \text{if } p = 13. \end{cases}$$

Since we have assumed $\deg(x) < \mathrm{gon}_{\mathbb{Q}}(X_1(2p^k))$ and $\deg(x)$ is odd, it must be that $[F : \mathbb{Q}] = d_0$. Indeed, by Proposition 2.7 and the $\mathbb{Q}$-gonality bounds on $X_1(14)$, $X_1(22)$, $X_1(26)$ and $X_1(50)$ from Table 1 in [22], we see that $\mathrm{gon}_{\mathbb{Q}}(X_1(2p^k)) \leq 3d_0$. In fact, if $p = 11$, it follows that $\mathrm{gon}_{\mathbb{Q}}(X_1(2 \cdot 11^k)) \leq 4 \cdot 11^{2k-2} < d_0$, so the claim follows already in this case.

Suppose for the sake of contradiction that $[F : \mathbb{Q}] = d_0$, and let $\varphi : E \to E'$ be the F-rational isogeny defined above. It follows from Corollary 4.3 that E' has a point Q of order p over a field extension F'/F of degree dividing p. By composing φ with the F-rational isogeny $E' \to E'/C$ induced by $[E', C] \in X_0(p)(\mathbb{Q})$ and replacing E' with E'/C if necessary, we may assume by Lemma 7.1 that the residue field of $[E', Q] \in X_1(p)$ has degree dividing $(p-1)/2$ and is contained in F'.

Since E' also has a 2-isogeny over F (because E does), together these imply E' has a point P of order $2p$ over F', a field of degree dividing pd_0. Let $y := [E', P] \in X_1(2p)$, and let $y_1 := [E', 2P] = [E', Q] \in X_1(p)$ and $y_2 := [E', pP] \in X_1(2)$ be the induced points. Since Proposition 4.1 applies in particular to any non-CM elliptic curve with rational j-invariant, we see that $3 \nmid [F' : \mathbb{Q}(y_1)]$. Thus $\mathbb{Q}(y) = \mathbb{Q}(y_1)\mathbb{Q}(y_2) = \mathbb{Q}(y_1)$. Since y_1 has odd degree dividing both pd_0 and $(p-1)/2$, then Proposition 4.1 shows

$$\deg(y_1) = \begin{cases} 1 & \text{if } p = 5, 7 \\ 3 & \text{if } p = 13. \end{cases}$$

Since $\mathbb{Q}(y) = \mathbb{Q}(y_1)$, we have an elliptic curve with rational j-invariant possessing a point of order $2p$ over a field of the degree indicated above. If $p = 13$, this contradicts Gužvić [32]. If $p = 7$, this contradicts Mazur [47]. If $p = 5$, then in particular this implies any elliptic curve $E''/\mathbb{Q}$ with $j(E'') = j(E')$ has a rational cyclic 2-isogeny. Thus E'' cannot have a rational cyclic 25-isogeny or two independent 5-isogenies, and Proposition 2.1 shows that $\mathrm{ord}_5([\mathrm{GL}_2(\mathbb{Z}_5) : \mathrm{im}\, \rho_{E''/\mathbb{Q}, 5^\infty}]) = 0$. Then Lemma 4.6 shows in fact $5^{2k-2} \mid [F : \mathbb{Q}]$, and we have reached a contradiction.

Finally, suppose $j(E') = 3^3 \cdot 5 \cdot 7^5/2^7$ and $p = 7$. Then by Proposition 4.1, we have $3 \cdot 7^{\max(0, 2k-3)} \mid [F : \mathbb{Q}]$. As above, E' attains a point of order $2 \cdot 7$ in an extension F'/F of degree dividing 7. For a fixed elliptic curve $E''/\mathbb{Q}$ with $j(E'') = 3^3 \cdot 5 \cdot 7^5/2^7$, we may compute the 14-division polynomials to see that 3^3 divides the degree of the residue field of any point of odd degree on $X_1(14)$ associated

17

to E''. Thus $3^3 \mid [F' : \mathbb{Q}]$, and together these imply $3^3 \cdot 7^{\max(0,2k-3)} \mid [F : \mathbb{Q}]$. As above, we see $\mathrm{gon}_{\mathbb{Q}}(X_1(2 \cdot 7^k)) \leq 2 \cdot 7^{2k-2} < [F : \mathbb{Q}]$, as desired. $\qquad\square$

Proposition 7.3. *Let $x \in X_1(4 \cdot 7^k)$ be a point of odd degree corresponding to a non-CM $\mathbb{Q}$-curve E. Then $\deg(x) \geq \mathrm{gon}_{\mathbb{Q}}(X_1(4 \cdot 7^k))$. In particular, x is not sporadic.*

Proof. Let $x \in X_1(4 \cdot 7^k)$ be a point of odd degree corresponding to a non-CM $\mathbb{Q}$-curve E. Since $X_1(4)$ has genus 0, we may assume $k > 0$. Let $F := \mathbb{Q}(x)$, and fix a model of E/F with an F-rational point of order $4 \cdot 7^k$. By Theorem 2.4, there is an F-rational cyclic isogeny $\varphi : E \to E'$ such that $j(E') \in \mathbb{Q}$. Let $E''/\mathbb{Q}$ be an elliptic curve with $j(E'') = j(E')$. For now, suppose $j(E'') \notin \{-3^3 \cdot 13 \cdot 479^3/2^{14}, 3^3 \cdot 13/2^2\}$. By Corollary 6.2, we may assume E'' has a rational cyclic 7-isogeny and full 2-torsion (but no 4-isogeny) over a cubic extension K. In particular, this means $j(E') \neq 3^3 \cdot 5 \cdot 7^5/2^7$.

Suppose for the sake of contradiction that $\deg(x) < \mathrm{gon}_{\mathbb{Q}}(X_1(4 \cdot 7^k))$. By Proposition 4.1, we know that $7^{2k-2} \mid [F : \mathbb{Q}]$. Since E'' corresponds to a degree 3 point on $X_1(2)$ and $E'(F)$ has a point of order 2 (since $E(F)$ does), it follows that $3 \mid [F : \mathbb{Q}]$. Together, this gives

$$3 \cdot 7^{2k-2} \mid [F : \mathbb{Q}].$$

Since $X_1(28)$ has $\mathbb{Q}$-gonality 6 by [22], it follows that $\mathrm{gon}_{\mathbb{Q}}(X_1(4 \cdot 7^k) \leq 6 \cdot 7^{2k-2}$. Thus our assumption that $\deg(x) < \mathrm{gon}_{\mathbb{Q}}(X_1(4 \cdot 7^k))$ and is of odd degree implies

$$\deg(x) = [F : \mathbb{Q}] = 3 \cdot 7^{2k-2}.$$

As in the proof of Proposition 6.1, we have $\rho_{E'',2^\infty}(\mathrm{Gal}_K) = \rho_{E'',2^\infty}(\mathrm{Gal}_F)$, and in particular E'' has no 4-isogeny over F. Thus E'/F has no 4-isogeny. It follows that $\mathrm{ord}_2(\deg(\varphi)) = 1$. If $\ker(\varphi) = \langle P \rangle$, we see that φ factors over F as

$$E \xrightarrow{\varphi_1} E_0 := E/\langle 2P \rangle \xrightarrow{\varphi_2} E'.$$

Since $2 \nmid \deg(\varphi_1)$, there is a point of order 4 in $E_0(F)$, since $E(F)$ has such a point. By Corollary 4.3, the curve E' has a rational point of order 7 in an extension of F'/F of degree dividing 7. Since E'/F' has a point of order 7 and $\deg(\hat{\varphi}_2) = 2$, it follows that E_0 has a point of order 7—and hence a point of order 28—over F'. That is, there exists $a := [E_0, Q] \in X_1(28)$ of odd degree dividing $3 \cdot 7^{2k-1}$.

We note that $[\mathbb{Q}(j(E_0)) : \mathbb{Q}] = 3$, since $\hat{\varphi}_2$ has degree 2 and any point on $X_0(2)$ associated to E' has degree 3. In fact, $\mathbb{Q}(\hat{\varphi}_2) = \mathbb{Q}(j(E_0)) = K$ for the cubic extension K defined above. Moreover, any E_1/K with $j(E_1) = j(E_0)$ will have a rational cyclic 7-isogeny and rational point of order 2, since E'' does. Thus E_0 corresponds to a point of degree 3 on $X_1(2)$, and this is the only possible degree of a point on $X_1(2)$ associated to E_0 having odd degree. It follows that $a_1 := [E_0, 7Q] \in X_1(4)$ has degree 3 as well since it has odd degree and its degree over $[E_0, 14Q] \in X_1(2)$ divides 2^2 by Proposition 4.6 in [28]. Since there exists $[E_0, C] \in X_0(7)(\mathbb{Q}(j(E_0)))$, by replacing E_0 with E_0/C if necessary we may assume by Lemma 7.1 that $a_2 := [E_0, 4Q] \in X_1(7)$ has degree dividing $3 \cdot \frac{7-1}{2} = 9$. Thus it must have degree 3. Since $\mathbb{Q}(a_1)\mathbb{Q}(a_2)$ is contained in $\mathbb{Q}(a)$, it must be that $\mathbb{Q}(a_1)\mathbb{Q}(a_2)$ has degree 3. As $\mathbb{Q}(a)$ is at most a quadratic extension of this field, it follows that $\mathbb{Q}(a)$ has degree 3. But this contradicts Theorem A in [20].

Finally, assume $j(E'') \in \{-3^3 \cdot 13 \cdot 479^3/2^{14}, 3^3 \cdot 13/2^2\}$, and let K_0 denote the residue field of the degree 3 point on $X_1(2)$ associated to E''. As noted above, $K_0 \subseteq F$, and by Corollary 4.3, E' must have a point of order 7 over $F(\zeta_7)$. A computation in Magma shows the 7-division polynomial of E'' over $K_0(\zeta_7)$ factors as a product of irreducible polynomials of degree 3 and 21, which shows that any F over which E' is isogenous to an elliptic curve with a point of order 28 is divisible by 9. Thus by Proposition 4.1, F is divisible by $9 \cdot 7^{2k-2}$ and the claim follows. $\qquad\square$

7.2. Points on $X_1(2^a \cdot 3^k)$. Let $x \in X_1(2^a 3^k)$ be a point of odd degree associated to a non-CM $\mathbb{Q}$-curve E. In this section, we show that $\deg(x) < \mathrm{gon}_{\mathbb{Q}}(X_1(2^a 3^k))$ would imply E is $\overline{\mathbb{Q}}$-isogenous to an elliptic curve corresponding to a rational point on one of 10 curves of genus at least 2.

Lemma 7.4. *Let E be an elliptic curve over $\mathbb{Q}$, and let p be an odd prime. If $p > 3$ and E has no point of order 2 over $\mathbb{Q}(E[p])$, then E has no point of order 2 over $\mathbb{Q}(E[p^k])$ for any $k \in \mathbb{Z}^+$. If $p = 3$ and E has no point of order 2 over $\mathbb{Q}(E[3^{d+1}])$, where 3^d is the level of $\rho_{E,3^\infty}$, then E has no point of order 2 over $\mathbb{Q}(E[3^k])$ for any $k \in \mathbb{Z}^+$.*

Proof. We follow the approach of Proposition 6.1 in [8] and Lemma 19 in [9]. For $s \in \mathbb{Z}^+$, let

$$L_s := \ker(\mathrm{im}\,\rho_{E,2 \cdot p^s} \to \mathrm{im}\,\rho_{E,p^s}),$$
$$K_s := \ker(\mathrm{im}\,\rho_{E,2 \cdot p^s} \to \mathrm{im}\,\rho_{E,2}),$$
$$K := \ker(\mathrm{im}\,\rho_{E,2 \cdot p^\infty} \to \mathrm{im}\,\rho_{E,2}).$$

We may view L_s as a subgroup of $\mathrm{im}\,\rho_{E,2}$ and K_s as a subgroup of $\mathrm{im}\,\rho_{E,p^s}$. Moreover, by Goursat's Lemma (see e.g., [42, pg75] or [29]) we have the following diagram:

$$
\begin{array}{ccc}
\mathrm{im}\,\rho_{E,p^s}/K_s & \longtwoheadrightarrow & \mathrm{im}\,\rho_{E,p}/K_1 \\
\Big\downarrow{\scriptstyle\cong} & & \Big\downarrow{\scriptstyle\cong} \\
\mathrm{im}\,\rho_{E,2}/L_s & \longtwoheadrightarrow & \mathrm{im}\,\rho_{E,2}/L_1
\end{array}
$$

The order of the kernel of the top map is a power of p, and so the order of the kernel of the bottom map is as well. Thus $[L_1 : L_s]$ is a power of p, and more generally $[L_{s_1} : L_{s_2}]$ is a power of p for all $1 \le s_1 \le s_2$. If $p > 3$, it follows that for all $s \in \mathbb{Z}^+$ we have $L_1 = L_s$ and

$$\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[p^s]) = \mathbb{Q}(E[2]) \cap \mathbb{Q}(E[p]).$$

In particular, if E has no point of order 2 over $\mathbb{Q}(E[p])$, then E has no point of order 2 over $\mathbb{Q}(E[p^k])$ for any k, as desired. Thus we may henceforth assume $p = 3$.

Suppose E has no point of order 2 over $\mathbb{Q}(E[3^{d+1}])$. The x-coordinate of any 2-torsion point generates a degree 3 extension of $\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[3^{d+1}])$ contained in $\mathbb{Q}(E[2])$, from which is follows that $3 \mid \#L_{d+1}$. Similarly, $3 \mid \#L_d$. Since $\#L_i \mid 6$ for all i and $[L_d : L_{d+1}]$ is a power of 3, it follows that $L_d = L_{d+1}$. Again by Goursat's Lemma

$$
\begin{array}{ccc}
\mathrm{im}\,\rho_{E,3^{d+1}}/K_{d+1} & \longrightarrow & \mathrm{im}\,\rho_{E,3^d}/K_d \\
\Big\downarrow{\scriptstyle\cong} & & \Big\downarrow{\scriptstyle\cong} \\
\mathrm{im}\,\rho_{E,2}/L_{d+1} & =\!\!=\!\!= & \mathrm{im}\,\rho_{E,2}/L_d
\end{array}
$$

By assumption, $\mathrm{im}\,\rho_{E,3^{d+1}} = \pi^{-1}(\mathrm{im}\,\rho_{E,3^d})$, and so this diagram implies

$$\ker(K \bmod 3^{d+1} \to K \bmod 3^d) = I + \mathrm{M}_2(3^d \mathbb{Z}/3^{d+1}\mathbb{Z}).$$

By Proposition 3.5 of [8],

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

and so $\mathrm{im}\,\rho_{E,2 \cdot 3^\infty} = \pi^{-1}(\mathrm{im}\,\rho_{E,2 \cdot 3^d})$. This means E has no point of order 2 over $\mathbb{Q}(E[3^k])$ for any $k \in \mathbb{Z}^+$. $\qquad\square$

Lemma 7.5. *Let p be prime and let F be a number field of odd degree. Suppose E/F is a non-CM elliptic curve with $P \in E(F)$ of order p^k, and let $\varphi : E \to E'$ be an F-rational isogeny with $\deg(\varphi) = p^a$ and $j(E') \in \mathbb{Q}$. If $x = [E, P] \in X_1(p^k)$, then for any $E''/\mathbb{Q}$ with $j(E'') = j(E')$, we have*

$$\mathbb{Q}(x) \subseteq \mathbb{Q}(E''[p^\infty]).$$

Proof. Let $\varphi : E \to E'$ be the F-rational isogeny as in the lemma statement. By considering the dual isogeny $\hat{\varphi} : E' \to E$, we may view E as the quotient of E' by some cyclic subgroup C of order p^a. By Lemma 2.8,

$$F' := \mathbb{Q}(j(E), j(E')) = \mathbb{Q}(j(E))$$

is the residue field of $[E', C] \in X_0(p^a)$. Thus, by replacing E, E' with elliptic curves over F' having the same j-invariant if necessary (which is permissible since $\mathbb{Q}(x)$ is model-independent), we may view $\hat{\varphi} : E' \to E$ as a cyclic isogeny of elliptic curves over F'. It follows that

$$F'(E'[p^\infty]) = F'(E[p^\infty]).$$

Since $\mathbb{Q}(x)$ is an extension of F' contained in $F'(E[p^\infty])$, we have that $\mathbb{Q}(x) \subseteq F'(E'[p^\infty])$. Now, let E'' be an elliptic curve over $\mathbb{Q}$ with $j(E'') = j(E')$. Then there exists a quadratic extension L/F' over which E' and E'' become isomorphic. Thus

$$\mathbb{Q}(x) \subseteq L(E''[p^\infty]) = L(E'[p^\infty]).$$

But since $F' \subseteq \mathbb{Q}(E''[p^\infty])$, it follows that $L(E''[p^\infty])$ is at most a degree 2 extension of $\mathbb{Q}(E''[p^\infty])$. Since $\mathbb{Q}(E''[p^\infty])$ is a Galois extension and $[\mathbb{Q}(x) : \mathbb{Q}]$ is odd, it must be that $\mathbb{Q}(x) \subseteq \mathbb{Q}(E''[p^\infty])$. $\square$

Lemma 7.6. *Suppose $E/\mathbb{Q}$ is an elliptic curve with $\operatorname{im} \rho_{E,3^\infty}$ contained in one of the following groups:*

$$9H^0\text{-}9a, \ 9H^0\text{-}9b, \ 9H^0\text{-}9c$$

$$9J^0\text{-}9a, \ 9J^0\text{-}9b, \ 9J^0\text{-}9c$$

Then the mod 2 Galois representation associated to E is surjective.

Proof. First, note that E cannot have a rational point of order 2. The fiber product of $9C^0\text{-}9a$ with $X_0(2)$ has no non-CM, non-cuspidal points by [9, proof of Prop. 23], so it remains to check the fiber product of $X_0(2)$ with each of the first 3 groups listed (since the latter 3 all cover $9C^0\text{-}9a$).

Suppose $\mathbb{Q}(E[2])$ is a cyclic cubic extension of $\mathbb{Q}$. Then $\operatorname{im} \rho_{E,3^\infty}$ cannot be contained in $3D^0\text{-}3a$ as an elliptic curve cannot have simultaneously this mod 3 image and a cyclic mod 2 image of order 3 by [17, Tables 8 & 11]. Thus since the first 3 groups cover $3D^0\text{-}3a$, we may assume $\operatorname{im} \rho_{E,3^\infty}$ is contained in

$$9J^0\text{-}9a, \ 9J^0\text{-}9b, \ 9J^0\text{-}9c.$$

For each group we compute the fiber product (over $X_0(1)$) of the modular curve parameterizing elliptic curves E with cyclic $\operatorname{im} \rho_{E,2}$ with the modular curve parameterizing elliptic curves with mod 9 image contained in the respective groups. In all the cases we get genus 2 curves with Jacobian of rank 0 over $\mathbb{Q}$ and an easy computation shows that none of the modular curves have any non-cuspidal rational points. See the research website of either author for the code used. $\square$

Proposition 7.7. *Let $x = [E, P] \in X_1(2 \cdot 3^k)$ be a point of odd degree, where E is a non-CM $\mathbb{Q}$-curve. If $\deg(x) < \operatorname{gon}_{\mathbb{Q}}(X_1(2 \cdot 3^k))$, then E is $\overline{\mathbb{Q}}$-isogenous to an elliptic curve corresponding to a rational point on X_{H_i} for $1 \le i \le 6$, where H_i is as defined in the appendix. In particular, since all curves X_{H_i} have genus at least 2, x is not sporadic unless E is $\overline{\mathbb{Q}}$-isogenous to one of a finite number of elliptic curves over $\mathbb{Q}$.*

Proof. Let $F := \mathbb{Q}(x)$, and fix a model of E/F with $P \in E(F)$. We may assume $k \ge 2$ since $X_1(6)$ has genus 0. Since $X_1(18)$ has $\mathbb{Q}$-gonality 2 by [22], it follows that $\operatorname{gon}_{\mathbb{Q}}(X_1(2 \cdot 3^k))$ is at most

$$\deg(X_1(2 \cdot 3^k) \to X_1(18)) \cdot 2 = 3^{2k-4} \cdot 2.$$

Since we have assumed $\deg(x) < \operatorname{gon}_{\mathbb{Q}}(X_1(2 \cdot 3^k))$ and $3^{2k-4} \mid [F : \mathbb{Q}]$ by Proposition 4.1, it must be that $[F : \mathbb{Q}] = 3^{2k-4}$. Note in this case Proposition 4.1 also implies $F = \mathbb{Q}(f(x))$, where $f : X_1(2 \cdot 3^k) \to X_1(3^k)$.

By Theorem 2.4, there exists an F-rational isogeny $\varphi : E \to E'$ such that $j(E') \in \mathbb{Q}$. We may assume φ is cyclic and generated by a point Q of order $3^a \cdot n$ where $3 \nmid n$. If $n > 1$, then we replace E with the quotient $E/\langle 3^a Q \rangle$. This new curve has a point of order 3^k, and also a rational cyclic 2-isogeny (since E has one). Thus, by replacing E by this quotient if necessary, we may assume φ has degree 3^a.

Now, let E'' be an elliptic curve over $\mathbb{Q}$ with $j(E'') = j(E')$. By Lemma 7.5, we have $F \subseteq \mathbb{Q}(E''[3^\infty])$. Also, since E has a rational 2-isogeny over F, so does E''. That is, there exists a point $P_0 \in E''$ of order 2 such that the residue field of $[E'', P_0] \in X_1(2)$ is contained in $\mathbb{Q}(E''[3^\infty])$.

It follows from Lemma 4.6 that

$$3^{\max(0, 2k-2-d)} \mid [F : \mathbb{Q}]$$

where $d = \mathrm{ord}_3([\mathrm{GL}_2(\mathbb{Z}_3) : \mathrm{im}\, \rho_{E''/\mathbb{Q},3^\infty}])$. Since $[F : \mathbb{Q}] = 3^{2k-4}$, it must be that $d \geq 2$. Thus $d = 2$ by Proposition 2.1, and E'' must have a rational cyclic 3-isogeny over $\mathbb{Q}$ by Proposition 3.3 in [15]. Thus $\mathrm{im}\, \rho_{E'',3^\infty}$ is contained in one of the following by Appendix A of [9] (see also index data in Table 1 of [61]):

$$9H^0\text{-}9a, \; 9H^0\text{-}9b, \; 9H^0\text{-}9c$$
$$9I^0\text{-}9a, \; 9I^0\text{-}9b, \; 9I^0\text{-}9c$$
$$9J^0\text{-}9a, \; 9J^0\text{-}9b, \; 9J^0\text{-}9c$$
$$27A^0\text{-}27a$$

Since it suffices to identify a single elliptic curve over $\mathbb{Q}$ in the $\overline{\mathbb{Q}}$-isogeny class of E, we are free to replace E'' with a different elliptic curve in its $\mathbb{Q}$-isogeny class. In particular, since any elliptic curve with a rational cyclic isogeny of degree 9 is isogenous to an elliptic curve with two independent 3-isogenies, we may assume E'' does *not* have a rational cyclic 9-isogeny. That is, we may assume $\mathrm{im}\, \rho_{E'',3^\infty}$ is contained in one of the following:

$$9H^0\text{-}9a, \; 9H^0\text{-}9b, \; 9H^0\text{-}9c$$
$$9J^0\text{-}9a, \; 9J^0\text{-}9b, \; 9J^0\text{-}9c$$

Note that it is still the case that E'' has a point P_0 of order 2 defined over $\mathbb{Q}(E''[3^\infty])$.

First, note that the mod 2 Galois representation associated to E'' is surjective by Lemma 7.6. Thus $\mathbb{Q}(P_0)$ is a cubic extension contained in $\mathbb{Q}(E''[3^\infty])$. Since the latter extension is Galois, it follows that $\mathbb{Q}(E''[2]) \subseteq \mathbb{Q}(E''[3^\infty])$. By Lemma 7.4, we have $\mathbb{Q}(E''[2]) \subseteq \mathbb{Q}(E''[3^3])$. We use Magma to search for subgroups of $\mathrm{GL}_2(\mathbb{Z}/54\mathbb{Z})$ which could be the image of the mod 54 Galois representation associated to E'', following the method of [9, Prop. 24]. This results in a list of 30 possible subgroups (up to conjugacy), but for each the mod 18 reduction is (conjugate to) a subgroup of one of the groups H_i for $1 \leq i \leq 6$; see the appendix for a list of generators for each H_i. See the research website of either author for the code used. In each case, the genus of X_{H_i} is at least 2. $\qquad \square$

Proposition 7.8. *Let $x \in X_1(4 \cdot 3^k)$ be a point of odd degree corresponding to a non-CM $\mathbb{Q}$-curve E. If $\deg(x) < \mathrm{gon}_{\mathbb{Q}}(X_1(2 \cdot 3^k))$, then E is $\overline{\mathbb{Q}}$-isogenous to an elliptic curve corresponding to a rational point on X_{H_i} for $7 \leq i \leq 10$, where H_i is as defined in the appendix. In particular, since all curves X_{H_i} have genus at least 2, x is not sporadic unless E is $\overline{\mathbb{Q}}$-isogenous to one of a finite number of elliptic curves over $\mathbb{Q}$.*

Proof. Let $x \in X_1(4 \cdot 3^k)$ be a point of odd degree corresponding to a non-CM $\mathbb{Q}$-curve E, and suppose $\deg(x) < \mathrm{gon}_{\mathbb{Q}}(X_1(2 \cdot 3^k))$. Since $X_1(4)$ and $X_1(12)$ have genus 0, we may assume $k > 1$. Let $F := \mathbb{Q}(x)$, and fix a model of E/F with an F-rational point of order $4 \cdot 3^k$. By Theorem 2.4, there is an F-rational cyclic isogeny $\varphi : E \to E'$ such that $j(E') \in \mathbb{Q}$. Suppose first

that $j(E') \in \{3^2 \cdot 23^3/2^6, \, -3^3 \cdot 11^3/2^2\}$. Since these elliptic curves lie in the same isogeny class, it suffices to consider only one of them, so suppose $j(E') = -3^3 \cdot 11^3/2^2$. Let $E''/\mathbb{Q}$ be an elliptic curve with $j(E'') = j(E') = -3^3 \cdot 11^3/2^2$. We check that 3-adic image (with $\pm I$ added) is $3B^0$-$3A$; we do this by showing that $j_G(t) = j(E'')$ has no roots for all minimal subgroups G of $3B^0$-$3A$. Hence

$$\mathrm{ord}_3([\mathrm{GL}_2(\mathbb{Z}_3) : \mathrm{im}\, \rho_{E''/\mathbb{Q},3^\infty}]) = \mathrm{ord}_3([\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) : \mathrm{im}\, \rho_{E''/\mathbb{Q},3}]) = 0.$$

Thus by Lemma 4.6,

$$3^{2k-2} \mid [F : \mathbb{Q}].$$

Since $X_1(36)$ has $\mathbb{Q}$-gonality 8 by [22], it follows that $\mathrm{gon}_\mathbb{Q}(X_1(4\cdot 3^k)) \leq 8 \cdot 3^{2k-4} < 9 \cdot 3^{2k-4} = 3^{2k-2}$, and we have a contradiction.

Henceforth we may assume $j(E') \notin \{3^2 \cdot 23^3/2^6, \, -3^3 \cdot 11^3/2^2\}$, and so by Corollary 6.2, any $E''/\mathbb{Q}$ with $j(E'') = j(E')$ has a rational cyclic 3-isogeny and either (a) a rational point of order 2 or (b) full 2-torsion over a cubic extension but no 4-isogeny over this extension.

First, suppose E'' has a rational point of order 2. Then as in the third paragraph of the proof of Proposition 6.1, E'' has either a rational cyclic 4-isogeny or independent 2-isogenies. In particular, this means that E'' cannot correspond to a rational point on $X_{3D^0\text{-}3a} = X_0(3,3)$, $X_{9B^0\text{-}9a} = X_0(9)$ by Kenku [40]. In addition, E'' cannot correspond to a rational point on $X_{9C^0\text{-}9a}$ since the fiber product of this curve with $X_0(2)$ has no non-cuspidal, non-CM rational points, as in the proof of Proposition 23 in [9]. Thus we may assume E'' has 3-adic image $3B^0$-$3a$, and we reach a contradiction as before.

Now we suppose E'' has full 2-torsion over a cubic extension but no 4-isogeny over this cubic field. Recall that if E'' has full 2-torsion over a cubic extension, then its discriminant is a square and it corresponds to a rational point on $X_{2A^0\text{-}2a}$. As shown in Proposition 24 of [9], this implies E'' cannot have a 9-isogeny or two independent 3-isogenies. We have already shown E'' cannot have 3-adic image $3B^0$-$3a$, so it must be that E'' corresponds to a rational point on the modular curve $X_{9C^0\text{-}9a}$. By Lemma 7.6, we may assume the 3-adic image of E'' is $9C^0$-$9a$.

Since $\mathrm{ord}_3([\mathrm{GL}_2(\mathbb{Z}_3) : \mathrm{im}\, \rho_{E''/\mathbb{Q},3^\infty}]) = 1$, by Lemma 4.6, we know that $3^{2k-3} \mid [F : \mathbb{Q}]$. Since, as we have already noted, $\mathrm{gon}_\mathbb{Q}(X_1(4\cdot 3^k)) \leq 8 \cdot 3^{2k-4}$, it must be that $[F : \mathbb{Q}] = 3^{2k-3}$. Let $\varphi : E \to E'$ as defined above. We may assume φ is cyclic and generated by a point Q of order $3^a \cdot n$ where $3 \nmid n$. The isogeny φ factors over F as

$$E \xrightarrow{\varphi_1} E_0 \coloneqq E/\langle 3^a Q \rangle \xrightarrow{\varphi_2} E'.$$

The curve E_0 has an F-rational point of order 3^k, and also a rational cyclic 2-isogeny (since E has one). That is, it has an F-rational point P_0 of order $2 \cdot 3^k$. Moreover, by Lemma 4.6, 3^{2k-3} divides the residue field of $x'' \coloneqq [E_0, P_0] \in X_1(2 \cdot 3^k)$. Since $[F : \mathbb{Q}] = 3^{2k-3}$, we may conclude $\mathbb{Q}(x'')$ has degree exactly 3^{2k-3} and $\mathbb{Q}(x'') = F$. In addition, $F = \mathbb{Q}(f(x''))$, where $f : X_1(2 \cdot 3^k) \to X_1(3^k)$.

By applying Lemma 7.5 to $\varphi_2 : E_0 \to E'$, we see that $F \subseteq \mathbb{Q}(E''[3^\infty])$. Also, since E' has a rational 2-isogeny over F, so does E''. That is, there exists a point $P'' \in E''$ of order 2 such that the residue field of $[E'', P''] \in X_1(2)$ is contained in $\mathbb{Q}(E''[3^\infty])$. Since the 3-adic image of E'' is $9C^0$-$9a$, by Lemma 7.4 we have $\mathbb{Q}(E''[2]) \subseteq \mathbb{Q}(E''[3^3])$. A Magma computation following the method of [9, Prop. 24] shows that there are 4 possible subgroups of $\mathrm{GL}_2(\mathbb{Z}/18\mathbb{Z})$—up to conjugacy—that could be the image of the mod 18 Galois representation associated to E''. These correspond to the groups H_7, H_8, H_9, or H_{10} as defined in the appendix. In each case, X_{H_i} has genus at least 2. See the research website of the either author for the code used. $\qquad\square$

7.3. Points on modular curves.

In this section, we find the rational points on the curves X_{H_i}, as in Propositions 7.7 and 7.8. Recall each H_i is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/18\mathbb{Z})$, as defined in the appendix. There are two non-CM j-invariants associated to rational points on these curves (see Lemma 7.12), and the corresponding elliptic curves lie in a single isogeny class. In Proposition

7.13, we show there are no points of odd degree on $X_1(4 \cdot 3^k)$ associated to curves in this isogeny class, completing the proof of Theorem 1.4.

Lemma 7.9. *All the non-cuspidal rational points on the modular curves X_{H_i} for $i = 1, 2$ and 3 correspond to elliptic curves with $j = 0$.*

Proof. Let E be an elliptic curve corresponding to a point on one of the modular curves X_{H_i}. There exists a modular group H of level 6 and genus 1 in which all H_i are of index 3. We compute that H modulo 3 is $3D^0$-$3a$ so $j(E) = f_3(t)$, and using Table 1 in [61] we compute that

$$f_3(t) = \frac{(t(t+6)(t^2 - 6t + 36))^3}{((t-3)(t^2 + 3t + 9))^3}.$$

Furthermore, $H \cap \mathrm{SL}(2, \mathbb{Z}/6\mathbb{Z})$ modulo 2 is cyclic of order 3, which means that $\Delta(E)$ is a square in $\mathbb{Q}(\sqrt{-3})$. Let $E_{f_3(t)}$ be an elliptic curve with j-invariant $f_3(t)$. We compute that $\Delta(E_{f_3(t)})$ is a square if and only if $(t-3)(t^2 + 3t + 9)$ is a square. Hence, we need to compute all the $\mathbb{Q}(\sqrt{-3})$-rational points on the elliptic curve

$$X : y^2 = (t-3)(t^2 + 3t + 9).$$

We get

$$t \in \left\{ 0, 3, -6, 3 \pm 3\sqrt{-3}, \frac{-3 \pm 3\sqrt{-3}}{2} \right\},$$

from which we get 4 cusps and 8 points for which $j(E_{f_3(t)}) = 0$. See the research website of either author for the code used. □

Lemma 7.10. *All the rational points on X_{H_i} for $i = 4, 5$ and 6 are cusps.*

Proof. First we notice that the intersection of the groups H_i for $i = 4, 5$ and 6 with $\{A \in \mathrm{GL}_2(\mathbb{Z}/18\mathbb{Z}) : \det A = \pm 1\}$ are conjugate, which implies that the corresponding modular curves are isomorphic over $\mathbb{Q}(\zeta_9)^+$. Hence it is enough to find all the $\mathbb{Q}(\zeta_9)^+$-rational points on one of the curves and show that all of them are cusps.

Using Zywina's algorithm we compute a model of $X := X_{H_4}$ to be

$$X : y^2 = x^5 + 9x^4 + 29x^3 + 42x^2 + 27x + 6.$$

Let w be a root of $x^3 - 6x^2 + 9x - 3$; it generates the extension $\mathbb{Q}(\zeta_9)^+$. To compute $X(\mathbb{Q}(\zeta_9)^+)$ we note that $\mathrm{Aut}_{\mathbb{Q}(\zeta_9)^+} X \simeq D_6$, and find an automorphism a such that $X/a \simeq E$, where

$$E : y^2 = x^3 + (8w^2 - 37w + 33)x^2 + (22w^2 - 126w + 155)x + (44w^2 - 248w + 300).$$

We have $E(\mathbb{Q}(\zeta_9)^+) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and compute $\#X(\mathbb{Q}(\zeta_9)^+) = 6$. The curve X has 6 cusps, of which 3 are rational. Since all the cusps of X are necessarily defined over some subfield of $\mathbb{Q}(\zeta_9)$, it follows that the non-rational cusps form one orbit of $\mathbb{Q}(\zeta_9)^+$-rational cusps. Hence all 6 $\mathbb{Q}(\zeta_9)^+$-rational points of X are cusps. See the research website of either author for the code used. □

Lemma 7.11. *The modular curves X_{H_7} has no rational points.*

Proof. Using Zywina's algorithm we find that the non-hyperelliptic genus 4 modular $X := X_{H_7}$ is given by the equations

$$-yz + xw = 0 \text{ and } x^3 - 6x^2y + 3xy^2 + y^3 - 9z^3 + 27zw^2 - 9w^3 = 0$$

in $\mathbb{P}^3$. We find that X has 6 automorphisms over $\mathbb{Q}$, and the quotient by one of them is the genus 2 hyperelliptic curve

$$C : y^2 + (x^3 + x^2 + 1)y = 8x^6 - 23x^5 + 47x^4 - 65x^3 + 58x^2 - 27x + 8,$$

with Jacobian of rank 0 over $\mathbb{Q}$. Standard techniques easily show that C and hence also X has no $\mathbb{Q}$-rational points. See the research website of either author for the code used. $\qquad\square$

Lemma 7.12. *The only rational points on the modular curves X_{H_i} for $i = 8, 9$ and 10 correspond to elliptic curves with $j = 1792$ and 406749952*

Proof. First we notice that the intersection of the groups H_i for $i = 8, 9$ and 10 with $\{A \in \mathrm{GL}_2(\mathbb{Z}/18\mathbb{Z}) : \det A = \pm 1\}$ are conjugate, which implies that the corresponding modular curves are isomorphic over $\mathbb{Q}(\zeta_9)^+$. Hence it is enough to find all the $\mathbb{Q}(\zeta_9)^+$-rational points on one of the curves X and the j-invariants to which these points correspond. Using Box's modification of Zywina's algorithm we obtain a model for $X := X_{H_8}$

$$X : y^2 = x^6 - 8x^5 + 30x^4 - 70x^3 + 105x^2 - 90x + 33.$$

Since the groups H_i are of index 72, the j-map is of degree 72, which is too large to compute directly. Hence we compute it by using the fact that H_i modulo 9 is $9C^0$-$9a$, and the j-map f' (of degree 12) from the modular curve X' corresponding to $9C^0$-$9a$ of genus 0 to $X_0(1)$ is known by [61]. We compute the Hauptmodul h of the function field of X' and compute the map $f : X \to X'$ such that $f(x, y) = h(q)$, which implies that $g = f' \circ f$ is the j-map $g : X \to X_0(1)$.

Let w be a root of $x^3 - 6x^2 + 9x - 3$; it generates the extension $\mathbb{Q}(\zeta_9)^+$. To compute $X(\mathbb{Q}(\zeta_9)^+)$ we note that $\mathrm{Aut}_{\mathbb{Q}(\zeta_9)^+} X \simeq D_6$, and find an automorphism a such that $X/a \simeq E$, where

$$E : y^2 = x^3 + (5w^2 - 25w + 30)x^2 + (20w^2 - 108w + 124)/3.$$

We have $E(\mathbb{Q}(\zeta_9)^+) \simeq \mathbb{Z}/21\mathbb{Z}$ and compute $\#X(\mathbb{Q}(\zeta_9)^+) = 12$. We get that 6 of the points are cusps, and there are 3 points corresponding to each of the j-invariants 1792 and 406749952. See the research website of either author for the code used. $\qquad\square$

Proposition 7.13. *There does not exist a $\mathbb{Q}$-curve E corresponding to a point of odd degree on $X_1(4 \cdot 3^k)$ for $k \geq 1$ which is isogenous to an elliptic curve E' with $j(E') \in \{1792, 406749952\}$.*

Proof. We will prove the result by showing that there does not exist a number field F of odd degree and a $\mathbb{Q}$-curve E which is F-isogenous to an elliptic curve E' with $j(E') \in \{1792, 406749952\}$ and such that $E(F)$ has a point of order 12. Since these elliptic curves are in the same isogeny class, it suffices to consider only one of them.

Suppose E is a $\mathbb{Q}$-curve defined over a number field F of odd degree with a point $P \in E(F)$ of order 12. Then by Theorem 2.4, there exists a F-rational isogeny $\varphi : E \to E'$ with $j(E') \in \mathbb{Q}$, and we may assume φ is cyclic with $\ker(\varphi) = \langle Q \rangle$. Suppose for the sake of contradiction that $j(E') = 1792$. Since any point on $X_0(4)$ associated to E' has even degree, it must be that $\deg(\varphi) = 2 \cdot d$ for some odd integer d. Thus the image of $3P$ on $E_0 := E/\langle 2Q \rangle$ has order 4, and by Corollary 4.3 there exists an extension F'/F of degree dividing 3 such that $E_0(F')$ has a point of order 3. In particular, E_0 has a point of order 12 defined over a number field of odd degree, where E_0 is an elliptic curve 2-isogenous to E'. However, a computation in Magma shows that each elliptic curve 2-isogenous to E' corresponds to points on $X_1(12)$ of even degree, contradiction. $\qquad\square$

8. Sporadic j-invariants in a fixed isogeny class

Since non-CM $\mathbb{Q}$-curves giving rise to sporadic points of odd degree on $X_1(N)$ belong to finitely many isogeny classes, it is natural to wonder whether there can be infinitely many distinct sporadic j-invariants within a fixed isogeny class. The following result shows that the answer is yes, provided the degree of the sporadic point is low enough. It is worth pointing out that no known examples of non-CM sporadic points satisfy this bound, so a new idea is needed to provide a definitive answer.

Proposition 8.1. *Suppose that there is a non-CM point $x = [E, P] \in X_1(N)$ with*

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

Then there exists infinitely many sporadic points $x' = [E', P']$ on the curves $X_1(dN)$ (with d varying), such that E' is isogenous to E and that all the $j(E')$ are pairwise distinct. Moreover, if $\deg(x)$ is odd, we can obtain infinitely many sporadic points $x' = [E', P']$ on the curves $X_1(dN)$ such that $\deg(x')$ is odd and such that E' is isogenous to E and that all the $j(E')$ are pairwise distinct.

Proof. Note in particular that N must be greater than 2, and let p be a prime divisor of N. Starting with a sporadic point $x = [E, P] \in X_1(N)$, we will construct a sporadic point $x' = [E', P'] \in X_1(pN)$ such that

$$\deg(x') \leq p^2 \deg(x) = \deg(X_1(pN) \to X_1(N)) \deg(x) < \frac{7}{1600}[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(pN)],$$

which will show that x' is sporadic. Let F be the residue field of x, let $k = v_p(N)$ and $P_0 = (N/p^k)P$. We have

$$\mathrm{im}\, \rho_{E/F,p} \subseteq \left\{ \begin{pmatrix} 1 & * \\ 0 & \chi_p(\mathrm{Gal}_F) \end{pmatrix} \right\}.$$

Let S be the set of subgroups of $E[p]$ of order p that are distinct from $\langle p^{k-1}P_0 \rangle$. We have $\#S = p$ and Gal_F (and hence $\mathrm{im}\, \rho_{E/F,p}$) acts on S. The group $\mathrm{im}\, \rho_{E/F,p}$ is isomorphic to a subgroup of $\mathrm{AGL}_1(\mathbb{F}_p)$ and by [15, Lemma 3.5] it acts on S either transitively or with a fixed point. If this action has a fixed point, E has an isogeny of degree p with kernel different from $\langle p^{k-1}P_0 \rangle$ over F. If the action is transitive, the stabilizer of a group is of index p in Gal_F and hence E has an isogeny of degree p with kernel different from $\langle p^{k-1}P_0 \rangle$ over F', an extension of F of degree p. To conclude, there exists an isogeny $\psi : E \to E'$ defined over F' where F' is either F or a degree p extension, such that $(\ker \psi) \cap \langle P_0 \rangle = \{O\}$. Note that $j(E) \neq j(E')$ by the assumption that E does not have CM. Hence $\psi(P_0) \in E'(F')$ is a point of order p^k. Furthermore $\psi(P_0)$ is in the kernel of the cyclic isogeny $\varphi \circ \hat{\psi}$ of order p^{k+1} where φ is the isogeny of E such that $\ker \varphi$ is generated by P_0. It follows that

$$\mathrm{im}\, \rho_{E'/F',p^{k+1}} \subseteq \left\{ \begin{pmatrix} 1 + p^k t & * \\ 0 & * \end{pmatrix} \right\}.$$

The fixed field of the associated isogeny character is an extension F''/F' of degree 1 or p, and $\mathrm{Gal}_{F''}$ fixes a point P'' of order p^{k+1}. As $E'(F'')$ has at least the same prime-to-p torsion as $E(F)$, we conclude that $E'(F'')$ has a point of order pN and hence corresponds to a point x' on $X_1(pN)$ of degree dividing $p^2 \deg(x)$, as desired. Note that if $\deg(x)$ is odd, we may take p to be odd by Theorem 1.5 and then $\deg(x')$ is also odd.

It remains to show that repeating this procedure will give in each step a j-invariant that hasn't been already obtained previously. Denote by E_i the elliptic curve that has been obtained in the ith step corresponding to a sporadic point on $X_1(p^i N)$. The graph whose vertex set consists of non-CM j-invariants of elliptic curves connected by an isogeny of degree a power of p and whose edges are between p-isogenous j-invariants is a tree, as the existence of a cycle would imply an endomorphism with nontrivial cyclic kernel and hence complex multiplication on some (and thus all) curves in the isogeny class. So all that one needs to show is that $j(E_{i-1}) \neq j(E_{i+1})$. To see this, note that in our construction a multiple of the point of order p^k on E_i that we obtained will generate the kernel of the isogeny to E_{i-1}, but not to E_{i+1}, from which the claim follows. $\square$

Appendix

We define the following subgroups of $\mathrm{GL}_2(\mathbb{Z}/18\mathbb{Z})$:

$$H_1 := \left\langle \left(\begin{smallmatrix} 2 & 7 \\ 15 & 16 \end{smallmatrix} \right), \left(\begin{smallmatrix} 7 & 11 \\ 12 & 11 \end{smallmatrix} \right), \left(\begin{smallmatrix} 13 & 2 \\ 9 & 17 \end{smallmatrix} \right), \left(\begin{smallmatrix} 1 & 8 \\ 15 & 5 \end{smallmatrix} \right) \right\rangle$$

$$H_2 := \left\langle \left(\begin{smallmatrix} 2 & 9 \\ 7 & 10 \end{smallmatrix} \right), \left(\begin{smallmatrix} 14 & 3 \\ 7 & 10 \end{smallmatrix} \right), \left(\begin{smallmatrix} 17 & 15 \\ 3 & 14 \end{smallmatrix} \right) \right\rangle$$

$$H_3 := \left\langle \left(\begin{smallmatrix} 7 & 2 \\ 15 & 11 \end{smallmatrix} \right), \left(\begin{smallmatrix} 1 & 6 \\ 6 & 13 \end{smallmatrix} \right), \left(\begin{smallmatrix} 13 & 3 \\ 9 & 4 \end{smallmatrix} \right), \left(\begin{smallmatrix} 2 & 3 \\ 15 & 5 \end{smallmatrix} \right) \right\rangle$$

$$H_4 := \left\langle \left(\begin{smallmatrix} 17 & 7 \\ 0 & 1 \end{smallmatrix} \right), \left(\begin{smallmatrix} 7 & 7 \\ 15 & 16 \end{smallmatrix} \right), \left(\begin{smallmatrix} 1 & 9 \\ 12 & 17 \end{smallmatrix} \right) \right\rangle$$

$$H_5 := \left\langle \left(\begin{smallmatrix} 17 & 9 \\ 9 & 8 \end{smallmatrix} \right), \left(\begin{smallmatrix} 1 & 1 \\ 15 & 10 \end{smallmatrix} \right), \left(\begin{smallmatrix} 5 & 5 \\ 12 & 7 \end{smallmatrix} \right) \right\rangle$$

$$H_6 := \left\langle \left(\begin{smallmatrix} 14 & 17 \\ 3 & 5 \end{smallmatrix} \right), \left(\begin{smallmatrix} 13 & 1 \\ 12 & 5 \end{smallmatrix} \right), \left(\begin{smallmatrix} 11 & 8 \\ 15 & 7 \end{smallmatrix} \right), \left(\begin{smallmatrix} 17 & 1 \\ 12 & 1 \end{smallmatrix} \right) \right\rangle$$

$$H_7 := \left\langle \left(\begin{smallmatrix} 11 & 16 \\ 6 & 17 \end{smallmatrix} \right), \left(\begin{smallmatrix} 13 & 3 \\ 9 & 14 \end{smallmatrix} \right) \right\rangle$$

$$H_8 := \left\langle \left(\begin{smallmatrix} 5 & 2 \\ 12 & 11 \end{smallmatrix} \right), \left(\begin{smallmatrix} 17 & 5 \\ 15 & 16 \end{smallmatrix} \right) \right\rangle$$

$$H_9 := \left\langle \left(\begin{smallmatrix} 11 & 1 \\ 3 & 4 \end{smallmatrix} \right), \left(\begin{smallmatrix} 7 & 15 \\ 9 & 14 \end{smallmatrix} \right) \right\rangle$$

$$H_{10} := \left\langle \left(\begin{smallmatrix} 16 & 1 \\ 3 & 11 \end{smallmatrix} \right), \left(\begin{smallmatrix} 5 & 15 \\ 9 & 16 \end{smallmatrix} \right) \right\rangle$$

References

1. Dan Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices (1996), no. 20, 1005–1011. 3, 3.2, 5.2

2. Noboru Aoki, *Torsion points on abelian varieties with complex multiplication*, Algebraic cycles and related topics (Kitasakado, 1994), World Sci. Publ., River Edge, NJ, 1995, pp. 1–22. 5.3, 5.4

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. MR 3961086 1, 1.1

4. Yuri Bilu and Pierre Parent, *Serre's uniformity problem in the split Cartan case*, Ann. of Math. (2) **173** (2011), no. 1, 569–584. MR 2753610 1

5. Yuri Bilu, Pierre Parent, and Marusia Rebolledo, *Rational points on $X_0^+(p^r)$*, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 3, 957–984. MR 3137477 1

6. Abbey Bourdon and Pete L. Clark, *Torsion points and isogenies on CM elliptic curves*, J. Lond. Math. Soc. (2) **102** (2020), no. 2, 580–622. MR 4171427 3.2

7. 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. 7.1

8. Abbey Bourdon, Özlem Ejder, Yuan Liu, Frances Odumodu, and Bianca Viray, *On the level of modular curves that give rise to isolated j-invariants*, Adv. Math. **357** (2019), 106824, 33. MR 4016915 1, 1, 1, 1, 3, 1.1, 7, 7.2

9. 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. 1, 1.1, 4.3, 6, 6.2, 7, 7.2, 7.2, 7.2, 7.2

10. Abbey Bourdon and Paul Pollack, *Torsion subgroups of CM elliptic curves over odd degree number fields*, Int. Math. Res. Not. IMRN (2017), no. 16, 4923–4961. 5, 5.2

11. Josha Box, *Elliptic curves over totally real quartic fields not containing $\sqrt{5}$ are modular*, available at: https://arxiv.org/abs/2103.13975. 1.1

12. Josha Box, *Quadratic points on modular curves with infinite Mordell-Weil group*, Math. Comput. **90** (2021), no. 327, 321–343 (English). 1.1

13. Pete L. Clark, *CM elliptic curves: volcanoes, reality, and applications*, preprint, available at `http://alpha.math.uga.edu/~pete/Isogenies.pdf`. 2.4

14. Pete L. Clark, Tyler Genao, Paul Pollack, and Frederick Saia, *The least degree of a CM point on a modular curve*, to appear in J. London. Math. Soc, available at: http://alpha.math.uga.edu/~pete/least_CM_degree-1226.pdf. 1.1, 3

15. John Cremona and Filip Najman, *Q-curves over odd degree number fields*, to appear in Res. Number Theory, available at arxiv.org:2004.10054. 1, 2.3, 2.3, 2.4, 2.4, 4.1, 4.3, 6, 6.2, 7.2, 8

16. 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, 2, 3

17. Harris B. Daniels and Enrique González-Jiménez, *Serre's constant of elliptic curves over the rationals*, Exp. Math. (2019), 1–19. 5, 6.2, 7.2

18. Harris B. Daniels and Jackon S. Morrow, *A group theoretic perspective on entanglements of division fields*, available at: arXiv:2008.09886. 4.1

19. 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. MR 0337993 2.4

20. Maarten Derickx, Anastassia Etropolski, Mark van Hoeij, Jackson S. Morrow, and David Zureick-Brown, *Sporadic cubic torsion*, to appera in Algebra Number Theory, available at arxiv.org:2007.13929. 1, 1.2, 7.1

21. Maarten Derickx, Filip Najman, and Samir Siksek, *Elliptic curves over totally real cubic fields are modular*, Algebra Number Theory **14** (2020), no. 7, 1791–1800 (English). 1.1

22. Maarten Derickx and Mark van Hoeij, *Gonality of the modular curve $X_1(N)$*, J. Algebra **417** (2014), 52–71. 1, 1.1, 5, 5.1, 7.1, 7.1, 7.2, 7.2

23. Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005. 2.4, 2.4

24. Noam D. Elkies, *On elliptic K-curves*, Modular curves and Abelian varieties. Based on lectures of the conference, Bellaterra, Barcelona, July 15–18, 2002, Basel: Birkhäuser, 2004, pp. 81–91 (English). 1

25. Nuno Freitas, Bao V. Le Hung, and Samir Siksek, *Elliptic curves over real quadratic fields are modular*, Invent. Math. **201** (2015), no. 1, 159–206 (English). 1.1

26. Gerhard Frey, *Curves with infinitely many points of fixed degree*, Israel J. Math. **85** (1994), no. 1-3, 79–83. 3, 3.2, 5.2

27. 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. 6.2

28. Enrique González-Jiménez and Filip Najman, *Growth of torsion groups of elliptic curves upon base change*, Math. Comput. **89** (2020), no. 323, 1457–1485. 4.3, 7.1

29. Edouard Goursat, *Sur les substitutions orthogonales et les divisions régulières de l'espace*, Ann. Sci. École Norm. Sup. (3) **6** (1889), 9–102 (French). 7.2

30. 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. 2.2

31. Ralph Greenberg, *The image of Galois representations attached to elliptic curves with an isogeny*, Amer. J. Math. **134** (2012), no. 5, 1167–1196. 2.2, 4.2

32. Tomislav Gužvić, *Torsion of elliptic curves with rational j-invariant defined over number fields of prime degree*, Proc. Am. Math. Soc. **149** (2021), no. 8, 3261–3275 (English). 7.1

33. Andrew V. Sutherland Jeremy Rouse and David Zureick-Brown, *ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$*, preprint, available at arXiv:2106.11141. 2.2

34. S. Kamienny, *Torsion points on elliptic curves over all quadratic fields*, Duke Math. J. **53** (1986), no. 1, 157–162. 1

35. _____, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229. 1

36. M. A. Kenku, *The modular curve $X_0(39)$ and rational isogeny*, Math. Proc. Camb. Philos. Soc. **85** (1979), 21–23 (English). 1.1, 2.2

37. _____, *The modular curve $X_0(169)$ and rational isogeny*, J. Lond. Math. Soc., II. Ser. **22** (1980), 239–244 (English). 1.1, 2.2

38. _____, *The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny*, Math. Proc. Camb. Philos. Soc. **87** (1980), 15–20 (English). 1.1, 2.2

39. _____, *On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$*, J. Lond. Math. Soc., II. Ser. **23** (1981), 415–427 (English). 1.1, 2.2

40. 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. MR 675184 2.2, 7.2

41. M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149. 1

42. Serge Lang, *Algebra*, 3 ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. 7.2

43. Pedro Lemos, *Serre's uniformity conjecture for elliptic curves with rational cyclic isogenies*, Trans. Amer. Math. Soc. **371** (2019), no. 1, 137–146. MR 3885140 1

44. _____, *Some cases of Serre's uniformity problem*, Math. Z. **292** (2019), no. 1-2, 739–762. MR 3968924 1

45. Beppo Levi, *Saggio per una teoria aritmetica delle forme cubiche ternarie*, Atti della Reale Acc. Sci. di Torino **43** (1908), 99–120, 413–434, 672–681. 5.1

46. Álvaro Lozano-Robledo, *On the field of definition of p-torsion points on elliptic curves over the rationals*, Math. Ann. **357** (2013), no. 1, 279–305. 1.1, 2.2, 4

47. B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978). 1, 1.1, 7.1

48. ———, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162. 1.1, 2.2

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

50. J.S. Milne, *Fields and galois theory*, available at: https://www.jmilne.org/math/CourseNotes/FT.pdf. 4.2

51. 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. 1.2, 1.1

52. Ekin Ozman and Samir Siksek, *Quadratic points on modular curves*, Math. Comp. **88** (2019), no. 319, 2461–2484. MR 3957901 1.1

53. Amadeu Reverter and Núria Vila, *Images of mod p Galois representations associated to elliptic curves*, Canad. Math. Bull. **44** (2001), no. 3, 313–322. MR 1847493 4.1

54. 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. 2.1, 2.2, 6.2

55. Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. 1, 2.2

56. ———, *Lectures on the Mordell-Weil theorem*, third ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997, Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre. MR 1757192 2

57. Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kanô Memorial Lectures, 1. MR 1291394 2.4, 2.6

58. Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. 2.3, 4

59. Hanson Smith, *Ramification in division fields and sporadic points on modular curves*, available at: https://arxiv.org/abs/1810.04809. 1.1

60. Andrew V. Sutherland, *Computing images of Galois representations attached to elliptic curves*, Forum Math. Sigma **4** (2016), e4, 79. 1

61. 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. 2.1, 7.2, 7.3, 7.3

62. David Zywina, *On the possible image of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$*, available at arxiv.org:1508.07660. 1, 3

63. ———, *On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$*, preprint, submitted (https://arxiv.org/abs/1508.07660). 4.3

WAKE FOREST UNIVERSITY, WINSTON-SALEM, NC 27109, USA
Email address: bourdoam@wfu.edu
URL: http://users.wfu.edu/bourdoam/

UNIVERSITY OF ZAGREB, BIJENIČKA CESTA 30, 10000 ZAGREB, CROATIA
Email address: fnajman@math.hr
URL: http://web.math.pmf.unizg.hr/~fnajman/