TOWARDS A CLASSIFICATION OF ISOLATED j-INVARIANTS

ABBEY BOURDON, SACHI HASHIMOTO, TIMO KELLER, ZEV KLAGSBRUN, DAVID LOWRY-DUDA, TRAVIS MORRISON, FILIP NAJMAN, AND HIMANSHU SHUKLA,
WITH AN APPENDIX BY MAARTEN DERICKX AND MARK VAN HOEIJ

Abstract. We develop an algorithm to test whether a non-CM elliptic curve $E/\mathbf{Q}$ gives rise to an isolated point of any degree on any modular curve of the form $X_1(N)$. This builds on prior work of Zywina which gives a method for computing the image of the adelic Galois representation associated to E. Running this algorithm on all elliptic curves presently in the L-functions and Modular Forms Database and the Stein–Watkins Database gives strong evidence for the conjecture that E gives rise to an isolated point on $X_1(N)$ if and only if $j(E) = -140625/8, -9317, 351/4$, or -162677523113838677.

1. Introduction

The modular curve $X_1(N)$ is an algebraic curve over $\mathbf{Q}$ whose non-cuspidal points parametrize elliptic curves with a distinguished point of order N. We are interested in studying isolated points on $X_1(N)$, which are roughly those not belonging to an infinite family of points parametrized by a geometric object. For example, if $f\colon X_1(N) \to \mathbf{P}^1$ is a rational map of degree d, then $f^{-1}(\mathbf{P}^1(\mathbf{Q}))$ contains infinitely many closed points of degree d by Hilbert's irreducibility theorem [Ser97, Chapter 9]. We say a degree d point *not* arising from such a map is **$\mathbf{P}^1$-isolated**. Other infinite families of degree d points correspond to positive rank abelian subvarieties of the curve's Jacobian; see Section 2 for details. A point which is not thus parametrized is **AV-isolated**. If a closed point $x \in X_1(N)$ is both $\mathbf{P}^1$- and AV-isolated, then we say x is **isolated**. One special class of isolated points is **sporadic** points, which are points $x \in X_1(N)$ such that there are only finitely many points on $X_1(N)$ of degree at most $\deg(x)$. While every sporadic point is isolated [BEL+19, Theorem 4.2], the converse need not hold.

Elliptic curves with complex multiplication (CM) provide many natural examples of isolated points, since the extra endomorphisms of a CM elliptic curve constrain the size of the image of the associated Galois representation. Indeed, as shown in [CGPS22, Theorem 8.2], there exist sporadic CM points on $X_1(N)$ for all $N \geq 721$. Non-CM isolated points on $X_1(N)$ remain much more mysterious, and are tied to open uniformity problems of Balakrishnan and Mazur [BM, Conjecture 17] and Serre [Ser72, §4.3]; see Section 1.2 for details. One recent line of investigation has focused on the class of isolated points associated to non-CM elliptic curves with j-invariant in $\mathbf{Q}$. To date, there are only three known examples of such elliptic curves, up to isomorphism over $\overline{\mathbf{Q}}$:

- The elliptic curve with j-invariant $-140625/8$ corresponds to two sporadic points of degree 3 on $X_1(21)$. This example was first discovered by Najman [Naj16]. In fact, this is the unique elliptic curve giving a sporadic point of degree at most 3 on *any* modular curve $X_1(N)$, as shown in [DEvH+21].
- The elliptic curve with j-invariant -9317 gives three points of degree 6 on $X_1(37)$, as in work of van Hoeij [vH]. Since 6 is less than half the $\mathbf{Q}$-gonality of $X_1(37)$, as computed in [DvH14], the points are necessarily sporadic by work of Frey [Fre94].
- The elliptic curve with j-invariant $351/4$ gives an isolated point of degree 9 on $X_1(28)$; see [BGRW, Theorem 2]. There are infinitely many points on $X_1(28)$ of degree 9, as shown in [DvH14], so this point is isolated but not sporadic.

If $x \in X_1(N)$ is an isolated (resp. sporadic) point, we say $j(x) \in X_1(1) \cong \mathbf{P}^1$ is an **isolated** (resp. **sporadic**) **j-invariant**. Thus the three j-invariants listed above are isolated j-invariants, while only the first two, $-140625/8$ and -9317, are sporadic j-invariants. We have good reason to believe that the set of all isolated j-invariants in $\mathbf{Q}$ is finite. Indeed, in [BEL+19, Corollary 1.7] the authors show that this would follow from an affirmative answer to Serre's Uniformity Question [Ser72], which is now a conjecture of Sutherland [Sut16] and Zywina [Zywc]. Moreover, in [BEL+19, §1.2], the authors pose the following question:

Question 1 (Bourdon, Ejder, Liu, Odumodu, Viray)**.** *Can one explicitly identify the (likely finite) set of isolated j-invariants in $\mathbf{Q}$?*

This question serves as motivation for the present work. To this end, we develop an algorithm which can be used to determine whether a given non-CM j-invariant in $\mathbf{Q}$ is isolated. Starting with the image of the adelic Galois representation associated to $E/\mathbf{Q}$ with $j(E) = j$, as computed by Zywina [Zywa], we apply various filters to determine whether there exists an isolated point $x \in X_1(N)$ with $j(x) = j$ for some N.

Algorithm: Main Algorithm

Input: A non-CM j-invariant $j \in \mathbf{Q}$.

Output: A finite list $\{(a_1, d_1), \ldots, (a_k, d_k)\}$ of (level, degree) pairs such that j is isolated if and only if there exists an isolated point $x \in X_1(a_i)$ of degree d_i with $j(x) = j$ for some (a_i, d_i) in the list.

In particular, if the output of Algorithm 1 is the empty set, then j is not an isolated j-invariant. If the output is nonempty, one can try to use other techniques to determine whether each point of degree d_i on $X_1(a_i)$ associated to E is isolated, from which we can definitively say whether $j(E)$ is an isolated j-invariant.

We ran Algorithm 1 on all elliptic curves currently in the L-functions and Modular Forms Database (LMFDB) [Col] and in the Stein–Watkins Database [SW02], which together contain over 36 million distinct non-CM j-invariants associated to elliptic curves over $\mathbf{Q}$ of conductor at most 10^8. The output shows that all but 6 of the non-CM j-invariants included in these databases are *not* isolated. As noted above, half of these remaining j-invariants are known to be isolated; in Section 9 we perform a case-by-case analysis on the remaining 3 candidates. In particular, these findings imply the following result.

Theorem 2. *Let $x = [E, P] \in X_1(N)$ be a non-CM isolated point with $j(E) \in \mathbf{Q}$. Fix an equation for $E/\mathbf{Q}$ and let N_E denote its conductor. Suppose that one of the following holds:*

- *$N_E \leq 500\,000$,*
- *N_E is only divisible by primes $p \leq 7$, or*
- *$N_E = p \leq 300\,000\,000$ for some prime number p.*

Then $j(E) \in \{-140625/8, -9317, 351/4, -162677523113838677\}$. Moreover, each one of these j-invariants corresponds to a $\mathbf{P}^1$-isolated point on $X_1(21)$, $X_1(37)$, $X_1(28)$, or $X_1(37)$, respectively.

Remark 3. Though we did not find a result in the literature showing the degree 18 point on $X_1(37)$ associated to $j = -162677523113838677$ is $\mathbf{P}^1$-isolated, the point itself was well-known prior to this work. Indeed, this j-invariant corresponds to one of two non-CM elliptic curves over $\mathbf{Q}$ with a rational cyclic 37-isogeny (see, e.g., [LR13, Table 4]), and any elliptic curve with a $\mathbf{Q}$-rational cyclic N-isogeny will give a point on $X_1(N)$ in degree at most $\varphi(N)/2$. The appendix by Maarten Derickx and Mark van Hoeij shows that this point is AV-isolated as well, allowing us to conclude that the 4 j-invariants identified in Theorem 2 are in fact *isolated*.

We conjecture that the four non-CM j-invariants identified above are the *only* j-invariants in $\mathbf{Q}$ associated to non-CM elliptic curves which give rise to isolated points on $X_1(N)$. Such a result has already been established for points of odd degree: by [BGRW] we know that $j = -140625/8$ and $j = 351/4$ are the only non-CM j-invariants in $\mathbf{Q}$ giving an isolated point of odd degree on $X_1(N)$, even as N ranges over all positive integers.

Conjecture 4. *If $x \in X_1(N)$ is an isolated point with $j(x) \in \mathbf{Q}$, then $j(x) = -140625/8$, -9317, $351/4$, -162677523113838677, or one of the 13 CM j-invariants in $\mathbf{Q}$.*

Since any CM elliptic curve is known to produce sporadic points on infinitely many modular curves of the form $X_1(N)$ by [BEL+19, Theorem 7.1], it follows conversely that every j-invariant in this set is $\mathbf{P}^1$-isolated (and in fact isolated — see the appendix).

Remark 5. Let $x \in X_1(N)$ be an isolated point with $j(x) \in \mathbf{Q}$. One expects that the square-free part of the conductor of any E with $j(E) = j(x)$ will be very small. The reason for this is that any such isolated point will generally have small mod ℓ image for some ℓ dividing N. Unless ℓ is small, we expect this to force potentially good reduction on E at all odd primes; see [Maz78, Corollary 4.4] and [BP11, Theorem 5.1] for examples of this phenomenon. Indeed this happens for all the curves appearing in Conjecture 4: their conductors are either a square, or twice a square.

Heuristically one might except to find most or all of the isolated points among elliptic curves with relatively small conductor (and hence in the LMFDB). One can also numerically observe that elliptic curves with small Galois representations are over-represented among curves with small conductor. Only 4 of the first 50 curves ordered by conductor have trivial torsion groups and all of them have non-trivial isogenies, while one expects asymptotically almost all curves to have surjective Galois representations when ordered by height, see [Duk97, Theorem 1].

These observations bolster the computational evidence supporting Conjecture 4.

It is natural to suspect a connection between isolated points on $X_1(N)$ and isolated points on $X_0(N)$, the modular curve parametrizing elliptic curves with a rational cyclic N-isogeny. We say a point $x \in X_0(N)(\mathbf{Q})$ is **exceptional** if $X_0(N)(\mathbf{Q})$ is finite and x corresponds to a non-CM elliptic curve over $\mathbf{Q}$. It is worth noting that the sporadic points on $X_1(21)$ associated to $j = -140625/8$ and the sporadic points on $X_1(37)$ associated to $j = -9317$ lie above exceptional rational points on $X_0(21)$ and $X_0(37)$, respectively. One might wonder whether other sporadic j-invariants can be obtained by a similar construction. Running Algorithm 1 on all 14 j-invariants corresponding to exceptional rational points on $X_0(N)$ for any N (described, for example, in [LR13, Table 4]) shows that there are no additional sporadic j-invariants.

Theorem 6. *Let E be an elliptic curve corresponding to an exceptional rational point on $X_0(N)$ for some positive integer N. If $j(E)$ is sporadic, then $j(E) = -140625/8$ or -9317.*

It is still an open problem to determine all sporadic points $x \in \cup_{N \in \mathbf{Z}^+} X_1(N)$ with $j(x) = -140625/8$ or -9317.

1.1. **Key Components of Algorithm.** The first step of our algorithm applies results of [BEL+19] and [Zywa] to compute the finite set of **primitive points** associated to a non-CM elliptic curve $E/\mathbf{Q}$. The primitive points are characterized by the following theorem.

Theorem 7. *Let $E/\mathbf{Q}$ be a non-CM elliptic curve. There exists a finite set $\mathcal{P} = \mathcal{P}(E)$ of primitive points in $\cup_{n \in \mathbf{Z}^+} X_1(n)$ associated to E which are characterized by the following properties:*

(i) *For each $N \in \mathbf{Z}^+$, a point $x \in X_1(N)$ with $j(x) = j(E)$ corresponds to a unique element $x' \in \mathcal{P}$ under the natural projection map. Moreover, if $x' \in X_1(a)$, then $a \mid N$ and $\deg(x) = \deg(f) \cdot \deg(x')$, where $f \colon X_1(N) \to X_1(a)$ is the natural map.*

(ii) *The rational number $j(E)$ is isolated if and only if there exists an isolated point in $\mathcal{P}$.*

Moreover, the set $\mathcal{P}$ is minimal with respect to condition (i).

By Theorem 7 (i), one can think of $\mathcal{P}(E)$ as the minimal set needed to reproduce the degrees of all points $x \in \cup_{n\in\mathbf{Z}^+} X_1(n)$ with $j(x) = j(E)$. Moreover, any isolated point $x \in X_1(n)$ with $j(x) = j(E)$ will correspond to a unique primitive point of minimal level. See Section 5 for details.

The second part of Algorithm 1 works to show the primitive points corresponding to E are *not* isolated. For example, if the Riemann–Roch space associated to $x \in X_1(N)$ has dimension at least 2, then x is not $\mathbf{P}^1$-isolated (and therefore not isolated). In other cases, we can show $x \in X_1(N)$ is not isolated by applying the following result.

Theorem 8. *Let $E/\mathbf{Q}$ be an elliptic curve, and let $H \leq \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ be the image of the mod N Galois representation of E, after some choice of basis. If the modular curve X_H has genus 0, then there are no isolated points on $X_1(N)$ associated to E.*

In particular, any elliptic curve with adelic image of genus 0 does not give rise to any isolated points on $X_1(N)$, even as N ranges over all positive integers. However, Theorem 8 is more broadly applicable. Even when the adelic image of E has positive genus, it can still be that for all *primitive* points $x \in X_1(a)$ associated to E, the mod a Galois representation of E gives a genus 0 modular curve. This occurs more often than one might expect: our preliminary computations identified at least 89 distinct such non-CM elliptic curves (up to $\overline{\mathbf{Q}}$-isomorphism) just within those currently in the LMFDB. See Example 40 for one such curve.

1.2. **Connection to Open Uniformity Problems.** Several well-known uniformity problems can be tied to isolated points on $X_1(N)$. One of the most longstanding examples is Serre's Uniformity Problem [Ser72, § 4.3], which in modern formulations [Sut16, Zywc] asks whether the mod ℓ Galois representation for any non-CM elliptic curve over $\mathbf{Q}$ is surjective for all $\ell > 37$. In the proof of [BN, Theorem 1.3], the authors show that a non-CM elliptic curve $E/\mathbf{Q}$ with non-surjective mod ℓ Galois representation can be used to construct sporadic points on $X_1(\ell^2)$ for all ℓ sufficiently large. This approach allows one to phrase Serre's Uniformity Problem to be about controlling isolated points on $X_1(\ell^2)$ within certain families of non-CM $\mathbf{Q}$-curves.

A more recent example is [BM, Conjecture 17], where Balakrishnan and Mazur conjecture that for sufficiently large N, any elliptic curve giving a quadratic point on $X_0(N)$ must have complex multiplication. Since a quadratic point on $X_0(N)$ will give a sporadic point on $X_1(N)$ for N sufficiently large, we can connect this conjecture to one about non-CM isolated points $x \in X_1(N)$ with $j(x)$ generating at most a quadratic extension.

1.3. **Outline.** After providing relevant background material in Section 2, we give an overview of the main algorithm in Section 3. The sub-algorithms used to compute primitive points and related mathematical results are discussed in Sections 4–6, with the proof of Theorem 7 appearing in Section 5. Results on genus 0 adelic images, including the proof of Theorem 8, are in Section 7. We address the validity of Algorithm 1 in Section 8. The output the main algorithm obtained after running it on elliptic curves in the LMFDB and the Stein–Watkins database is discussed in Section 9, along with its final analysis.

1.4. **Code.** We have implemented our algorithm in Magma [BCP97]. Code is available in the GitHub repository at `https://github.com/davidlowryduda/isolated_points`.

Acknowledgments

We thank Pete Clark, Maarten Derickx, Jeremy Rouse, Andrew Sutherland, and David Zureick-Brown for helpful conversations. We also thank David Zywina for making his code to compute Galois images available, and David Roe for further making Zywina's code and implementation more readily available for other mathematicians to use; this project would not have been possible

without their work. This project began at the *COmputations and their Uses in Number Theory* conference at CIRM in March 2023; we thank the organizers as well as CIRM for providing the opportunity for collaboration.

AB was supported by NSF Grants DMS-2145270 and DMS-1928930. Part of the work was completed while this author was in residence at the Simons Laufer Mathematical Science Institute in Berkeley, CA, during the semester of Diophantine Geometry. TK was partially supported by the 2021 MSCA Postdoctoral Fellowship 01064790 – ExplicitRatPoints. DLD was supported by the Simons Collaboration in Arithmetic Geometry, Number Theory, and Computation via the Simons Foundation grant 546235. TM was partially supported by the Commonwealth Cyber Initiative. FN is supported by the QuantiXLie Centre of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004). HS is supported by the DFG-grant STO 299/17-1.

2. Background

2.1. **Isolated Points on Curves.** Let C be a curve, by which we will mean a smooth projective geometrically integral 1-dimensional scheme defined over a number field k; we suppose all curves satisfy these assumptions throughout the paper. To streamline our exposition, we assume there exists a point $P_0 \in C(k)$, but this is not required; see [BEL+19, §4]. Throughout, we consider closed points of the curve C, which correspond to Gal_k-orbits of points in $C(\overline{k})$. The degree of x is defined to be the degree of the residue field $k(x)$ over k, or alternatively, to be the length of the Gal_k-orbit of points in $C(\overline{k})$ corresponding to x.

To any closed point $x \in C$ of degree d we associate the k-rational effective divisor

$$P_1 + \cdots + P_d,$$

where $P_1, \ldots, P_d$ are the points in the Gal_k-orbit associated to x. With this identification, we can study the image of x under the natural map from the dth symmetric power of C to the curve's Jacobian

$$\Phi_d \colon C^{(d)} \to \mathrm{Jac}(C)$$

which sends an effective divisor D of degree d to the class $[D - dP_0]$. If $\Phi_d(x) = \Phi_d(y)$ for some other point $y \in C^{(d)}(k)$, then there exists a non-constant function $f \in k(C)^\times$ with $\mathrm{div}(f) = x - y$. Since x is a degree d point and $x \neq y$, the divisors associated to x and y have distinct support so $f \colon C \to \mathbf{P}^1_k$ is a dominant morphism of degree d.[1] By Hilbert's irreducibility theorem [Ser97, Chapter 9], $f^{-1}(\mathbf{P}^1(k))$ will contain infinitely many closed points of degree d. On the other hand, if Φ_d is injective on closed points of degree d, then Faltings's Theorem [Fal94] implies that all but finitely many such points are parametrized by translates of positive rank abelian subvarieties of $\mathrm{Jac}(C)$. This inspires the following:

Definition 9. Let C be a curve defined over a number field k. Let Φ_d be the map in (2.1).

(i) A closed point $x \in C$ of degree d is **$\mathbf{P}^1$-parametrized** if there exists a point $x' \in C^{(d)}(k)$ with $x' \neq x$ such that $\Phi_d(x) = \Phi_d(x')$. Otherwise, we say x is **$\mathbf{P}^1$-isolated**.

(ii) A closed point $x \in C$ of degree d is **AV-parametrized** if there exists a positive rank abelian subvariety A/k with $A \subset \mathrm{Jac}(C)$ such that $\Phi_d(x) + A \subset \mathrm{im}\,(\Phi_d)$. Otherwise, we say x is **AV-isolated**.

(iii) A closed point $x \in C$ of degree d is **isolated** if it is both $\mathbf{P}^1$-isolated and AV-isolated.

[1] In particular, this shows Φ_d is injective if d is less than the k-gonality of C, which is the least degree of a non-constant rational map to $\mathbf{P}^1$.

(iv) A closed point $x \in C$ of degree d is **sporadic** if there are only finitely many closed points of C of degree at most $\deg(x)$.

If C has genus $g \geq 2$, then the collection of all points on C with coordinates in k is finite by Faltings's theorem [Fal83]. In general, the set $C(k)$ sits inside a larger finite set of points, namely, the set of all isolated points of C.

Theorem 10 (Bourdon, Ejder, Liu, Odumodu, Viray, [BEL+19, Theorem 4.2])**.** *Let C be a curve over a number field.*

(i) *There are infinitely many degree d points on C if and only if there is a degree d point on C that is* not *isolated.*
(ii) *There are only finitely many isolated points on C.*

It follows from Theorem 10 that every sporadic point is isolated, but the converse need not hold.

2.2. **Modular Curves.** For any subgroup $H \leq \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$, we define the modular curve X_H to be the coarse space of the stack $\mathcal{M}_H$, as defined in Deligne–Rapoport [DR73]. The curve X_H is a scheme over $\operatorname{Spec} \mathbf{Z}[1/N]$ and parametrizes generalized elliptic curves with H-level structure. In particular, its k-rational points roughly classify elliptic curves over k whose mod N image is contained in H; see, for example, [RSZB22, §2.3] for details. If we take

$$B_1(N) = \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\} \leq \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z}),$$

then $X_{B_1(N)} = X_1(N)$, the modular curve whose noncuspidal points parametrize elliptic curves with a distinguished point of order N. There is an analytic isomorphism between $X_1(N)(\mathbf{C})$ and the Riemann surface constructed as a quotient of the extended upper-half plane by the congruence subgroup

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

with matrices acting via linear fractional transformations. If $N \geq 4$, then $\mathcal{M}_{B_1(N)}$ is its own coarse moduli space, and so noncuspidal k-rational points of $X_1(N)$ classify pairs (E, P), where E/k is an elliptic curve and $P \in E(k)$, up to k-isomorphism.

We may also define a modular curve associated to an open subgroup G of $\mathrm{GL}_2(\widehat{\mathbf{Z}})$. For any $N \in \mathbf{Z}^+$, let $\pi \colon \mathrm{GL}_2(\widehat{\mathbf{Z}}) \to \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ be the natural projection map, and define $G(N) \coloneqq \pi(G)$. We say G has **level** N if $G = \pi^{-1}(G(N))$ and N is minimal with respect to this property. If $\det(G) = \widehat{\mathbf{Z}}^\times$, we define the modular curve $X_G \coloneqq X_{G(N)}$ where N is the level of G. If $G = \mathrm{GL}_2(\widehat{\mathbf{Z}})$, then we identify $X_G \cong \mathbf{P}^1$ with the j-line.

2.3. **Closed Points on Modular Curves.** To discuss isolated points on modular curves, we must consider closed points on $X_1(N)$, viewed always as a scheme over $\mathbf{Q}$. Let k be a field with an embedding of k into $\overline{\mathbf{Q}}$. Given an elliptic curve E/k with $P \in E(k)$ of order N, the pair (E, P) induces a k-valued point on $X_1(N)$ via the moduli interpretation described above. We denote this k-valued point by $(E, P)_k$, and by definition it corresponds to a morphism of $\mathbf{Q}$-schemes $f \colon \operatorname{Spec} k \to X_1(N)$. The map f sends the unique point of $\operatorname{Spec} k$ to a point $x \in X_1(N)$, and we call x the **closed point** associated to (E, P).[2] We define the **degree** of x to be the degree of the residue field $\mathbf{Q}(x)$ over $\mathbf{Q}$. Since there are many scheme-valued points which induce the same closed point, it is sometimes preferable to consider Galois orbits of points in $X_1(N)(\overline{\mathbf{Q}})$, which are in bijection with the set of closed points. Thus one could alternatively define the closed point associated to (E, P) as the $\mathrm{Gal}_{\mathbf{Q}}$-orbit of $(E, P)_{\overline{\mathbf{Q}}}$.

[2]Note x is indeed closed since $\mathbf{Q}(x)/\mathbf{Q}$ is finite; see, for example, [Liu02, Exercise 5.9, p. 76].

Remark 11. Given a k-valued point $(E,P)_k$, we note that the degree of the associated closed point x may be strictly less than the degree of k. However, there always exists $E'/\mathbf{Q}(x)$ with $j(E')=j(E)$ and $P'\in E'(\mathbf{Q}(x))$, where the point $P'\in E'$ maps to $P\in E$ under a $\overline{\mathbf{Q}}$-isomorphism sending E' to E. See [DR73, p. 274, Proposition VI.3.2]. The pair (E',P') gives a $\mathbf{Q}(x)$-valued point, and it is the unique $\mathbf{Q}(x)$-valued point such that $(E,P)_k=(E',P')_k$.

Let E/k be an elliptic curve and let $P\in E(k)$ a point of order N. For any $\xi\in\mathrm{Aut}(E)$, the pair $(E,\xi P)$ induces the same closed point $x\in X_1(N)$, since ξ provides the necessary isomorphism. This can be used to obtain a more explicit description of the residue field $\mathbf{Q}(x)$.

Lemma 12. *Let E be an elliptic curve defined over $\mathbf{Q}(j(E))$, and let $P\in E$ be a point of order N. Then the residue field of the closed point $x\in X_1(N)$ associated to (E,P) is given by*

$$\mathbf{Q}(x)\cong\mathbf{Q}(j(E),\mathfrak{h}(P)),$$

where $\mathfrak{h}\to E/\mathrm{Aut}(E)\cong\mathbf{P}^1$ is a Weber function for E.

Proof. See, for example, [BN, Lemma 2.5]. □

Remark 13. At times, it can be useful to work with an explicit model-independent formulation of a Weber function. For example, if $E: y^2=4x^3-c_2x-c_3$ and $j(E)\neq 0,1728$, we can define

$$\mathfrak{h}((x,y))=\frac{c_2c_3}{\Delta}x,$$

where $\Delta=c_2^3-27c_3^2$. One can verify:

(i) We have $\mathfrak{h}(P)=\mathfrak{h}(P')$ if and only if $P=\xi P'$ for some $\xi\in\mathrm{Aut}(E)$.
(ii) If $\eta\colon E\to E'$ is an isomorphism, then $\mathfrak{h}_E=\mathfrak{h}_{E'}\circ\eta$.

See [Shi71, p. 107]. In particular, if $E/\mathbf{Q}(j(E))$ does not have complex multiplication and $P=(x_0,y_0)$, then one can take $\mathbf{Q}(x)\cong\mathbf{Q}(j(E),x_0)$.

Example 14 (Closed points versus geometric points I)**.** Let $E_1\colon y^2+xy+y=x^3-x^2-3x+3$ and $P_1=(-1,-2)$ a point of order 7. Then (E_1,P_1) gives a $\mathbf{Q}$-valued point on $X_1(7)/\mathbf{Q}$ and also a closed point $x\in X_1(7)$ of degree 1. On the other hand, let $E_2\colon y^2=x^3-43x-166$ and $P_2=(5,\sqrt{-256})$ a point of order 7. Then (E_2,P_2) gives a $\mathbf{Q}(\sqrt{-256})$-valued point on $X_1(7)/\mathbf{Q}$ and also a closed point $x\in X_1(7)$ of degree 1 by Remark 13. In fact, both (E_1,P_1) and (E_2,P_2) induce the same geometric point on $X_1(7)$ since $(E_1,P_1)_{\overline{\mathbf{Q}}}=(E_2,P_2)_{\overline{\mathbf{Q}}}$.

One could alternatively compute the Kubert–Tate normal form associated to $E_2/\mathbf{Q}(\sqrt{-256})$, with $P_2=(5,\sqrt{-256})$:

$$E_3\colon y^2-xy-4y=x^3-4x^2,\ P_3=(0,0).$$

We can check that $(E_1,P_1)_{\mathbf{Q}}=(E_3,P_3)_{\mathbf{Q}}$ and $(E_2,P_2)_{\mathbf{Q}(\sqrt{-256})}=(E_3,P_3)_{\mathbf{Q}(\sqrt{-256})}$. Thus it is fair to say that (E_2,P_2) induces a $\mathbf{Q}$-valued point, even though it is not itself a $\mathbf{Q}$-valued point.

Example 15 (Closed points versus geometric points II)**.** The distinction between closed points and geometric points can be seen when counting the number of points of a particular degree. For example, let E be the elliptic curve with LMFDB label 162.c3. Then E possesses a unique $\mathbf{Q}$-rational subgroup of order 21 with generator P. For each $a\in(\mathbf{Z}/21\mathbf{Z})^\times$, we consider the geometric point on $X_1(21)$ associated to (E,aP). Since $(E,aP)_{\overline{\mathbf{Q}}}=(E,-aP)_{\overline{\mathbf{Q}}}$, we find that there are six distinct geometric points corresponding to (E,aP) for $a\in(\mathbf{Z}/21\mathbf{Z})^\times$. However, these six $\overline{\mathbf{Q}}$-points lie in two Galois orbits, each of size 3. Thus there are two closed points of degree 3, and the cardinality of the Galois orbit equals the degree.

2.4. **Maps Between Modular Curves.**

Proposition 16. *If $G \subseteq G' \subseteq \mathrm{GL}_2(\widehat{\mathbf{Z}})$ are two open subgroups with surjective determinant, then there is a natural $\mathbf{Q}$-rational morphism $X_G \to X_{G'}$ of degree $[\pm G' : \pm G]$. Here, $\pm G$ denotes the subgroup generated by G and $-I_2$.*

Proof. Let N be the level of G. For any subgroup H of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$, we have $\mathbf{Q}(X_H) = \mathbf{Q}(X(N))^H$. Now by Galois theory it follows that $\mathbf{Q}(X_G) \supseteq \mathbf{Q}(X_{G'})$, so we conclude that there exists a $\mathbf{Q}$-rational morphism $f\colon X_G \to X_{G'}$.

To determine its degree, let Γ and Γ' be the intersection with $\mathrm{SL}_2(\mathbf{Z})$ of the inverse image of G and G' in $\mathrm{GL}_2(\mathbf{Z})$. Over $\mathbf{C}$, the morphism f is the quotient map $\Gamma\backslash\mathcal{H}^* \to \Gamma'\backslash\mathcal{H}^*$. Here, $\mathcal{H}^*$ is the extended complex upper half plane. Since the kernel of the action of $\mathrm{SL}_2(\mathbf{Z})$ on $\mathcal{H}$ is $\pm I$, the degree of f is as claimed. □

Let a and b be positive integers. Taking $G = \pi^{-1}(B_1(ab))$ and $G' = \pi^{-1}(B_1(a))$ gives the following corollary, which under the moduli interpretation corresponds to sending (E, P) to (E, bP).

Corollary 17. *For positive integers a and b, the natural $\mathbf{Q}$-rational map $f\colon X_1(ab) \to X_1(a)$ has*

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

where $c_f = \frac{1}{2}$ if $a \leq 2$ and $ab > 2$ and $c_f = 1$ otherwise.

2.5. **Galois Representations.** If E is an elliptic curve defined over a number field k, then Gal_k acts naturally on the $\overline{k}$-points of E. On torsion points, this action is described by the **adelic Galois representation** associated to E/k,

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

From this we can obtain two other Galois representations. On the one hand, fixing a positive integer m, we can choose to record the action of Gal_k on points whose order is divisible only by those primes dividing m. This is the **m-adic Galois representation** associated to E:

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

In particular, if $m = \ell$ is a prime number, we recover the standard ℓ-adic representation associated to E. Alternatively, we may wish to record the Galois action only on points of order dividing m. We use $E[m]$ to denote the finite subgroup of such points. This gives the **mod m Galois representation** associated to E,

$$\rho_{E,m}\colon \mathrm{Gal}_k \to \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbf{Z}/m\mathbf{Z}).$$

Note that $\rho_{E,m}$ agrees with the reduction of ρ_E mod m.

If E/k is a non-CM elliptic curve, we define the **level** of ρ_E to be the smallest positive integer N such that $\mathrm{im}\,\rho_E = \pi^{-1}(\mathrm{im}\,\rho_{E,N})$, where $\pi\colon \mathrm{GL}_2(\widehat{\mathbf{Z}}) \to \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ is the natural reduction map; that such an N exists is a consequence of Serre's Open Image Theorem [Ser72]. The level of ρ_{E,m^∞} may be defined in an analogous way. We take the convention that $\mathrm{GL}_2(\mathbf{Z}/1\mathbf{Z})$ denotes the trivial group, so level 1 corresponds to the associated Galois representation being surjective. Though ρ_E is never surjective when $k = \mathbf{Q}$, this can occur for elliptic curves defined over number fields of higher degree [Gre10, Theorem 1.2].

3. Overview of the Main Algorithm

The following algorithm is the main procedure for determining whether a given non-CM j-invariant in $\mathbf{Q}$ is the image of an isolated point on $X_1(N)$ under the map to the j-line, based on results in [BEL+19, Zywa]. We note that for any CM j-invariant j, there exists infinitely many $N \in \mathbf{Z}^+$ for which there is a sporadic point $x \in X_1(N)$ with $j(x) = j$ by [BEL+19, Theorem 7.1], so it is not necessary to consider them in this algorithm. The outline below gives an overview of the structure, while the algorithms to perform particular steps are described in detail in Sections 4, 6, and 7. We will prove a theorem on the validity of Algorithm 1 in Section 8.

Algorithm 1: Main Algorithm

Input: A non-CM j-invariant $j \in \mathbf{Q}$.

Output: A finite list $\{(a_1, d_1), \ldots, (a_k, d_k)\}$ of (level, degree) pairs such that j is isolated if and only if there exists an isolated point $x \in X_1(a_i)$ of degree d_i with $j(x) = j$ for some (a_i, d_i) in the list.

1 Construct an elliptic curve $E/\mathbf{Q}$ with $j(E) = j$.

2 Compute the adelic image G of $E/\mathbf{Q}$ as a subgroup of $\mathrm{GL}_2(\hat{\mathbf{Z}})$ using Zywina's algorithm [Zywa]. Represent the output as the level N and the subgroup $G(N)$ of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$.

3 Apply Algorithm 2 to $G(N)$ to obtain the level m_0 of the m-adic Galois representation associated to E, where m is the product of 2, 3, and all non-surjective primes.

4 Apply Algorithm 3 to $\operatorname{im} \rho_{E,m_0}$. For each positive divisor n of m_0 and each closed point $x \in X_1(n)$ with $j(x) = j$, this gives the primitive point associated to x, say $x' \in X_1(a)$ of degree d. Return a multiset D with entries $\langle n, (a, d)\rangle$.

5 Construct the multiset $D' \subseteq D$ containing only those elements $\langle n, (a, d)\rangle$ for which $d \leq \mathrm{genus}(X_1(a))$.

6 Create the multiset M consisting of all pairs (a, d) with $\langle n, (a, d)\rangle$ appearing in D'. We include (a, d) with multiplicity μ if and only if $X_1(a)$ has μ distinct closed points of degree d associated to E.

7 Remove from M any pair (a_i, d_i) where the mod a_i Galois representation of $E/\mathbf{Q}$ corresponds to a modular curve of genus 0.

8 **return** M

In particular, note that if Algorithm 1 outputs $\{\}$, then j is not the image of any isolated point on $X_1(N)$, even as N ranges over all positive integers. See Corollary 44.

Example 18. If $j = -9317$, then Algorithm 1 returns $\{(37, 6)^3\}$. This means that any isolated point $x \in X_1(N)$ with $j(x) = j$ and $N \in \mathbf{Z}^+$ maps down under the natural projection map to one of the 3 closed points of degree 6 on $X_1(37)$. In fact, these points are all sporadic by [Fre94, Proposition 2], since $6 < \frac{1}{2}\operatorname{gon}_{\mathbf{Q}}(X_1(37)) = 18$. Here, the gonality computation is a result of [DvH14]. Thus j is a sporadic — and hence isolated — j-invariant.

Example 19. If $j = -121$, then Algorithm 1 returns $\{\}$. This means that there are no isolated points on $X_1(N)$ associated to this j-invariant.

Example 20. If $j = -882216989/131072$, then Algorithm 1 returns $\{(17, 4)^2\}$. This means that j is associated to an isolated point on a modular curve of the form $X_1(N)$ if and only if there exists a degree 4 isolated point $x \in X_1(17)$ with $j(x) = j$. In Section 9, we will see that no such isolated point exists, from which we can conclude that j is not an isolated j-invariant.

4. Computing the level of the m-adic representation

Given a non-CM elliptic curve $E/\mathbf{Q}$, we define the set

$$S_E \coloneqq \{2,3\} \cup \{\ell : \rho_{E,\ell^\infty}(\mathrm{Gal}_{\mathbf{Q}}) \neq \mathrm{GL}_2(\mathbf{Z}_\ell)\}.$$

Here, we include 2 and 3 in S_E to allow us to apply results of [BEL+19] in later steps of the algorithm; see Section 5.2 for details. For $m \coloneqq \prod_{\ell \in S_E} \ell$, we want an algorithm to obtain the level of the m-adic Galois representation associated to E from the image of the adelic representation of E, where the latter can be computed by Zywina's algorithm [Zywa]. If $\operatorname{im}\rho_E$ has level N, define $n = \prod_{\ell \in S_E} \ell^{v_\ell(N)}$ and let m_0 denote the level of ρ_{E,m^∞}. We will show in Proposition 22 that $m_0 | n$ and $n | N$. Each of these divisibilities can be proper, as the following examples illustrates.

Example 21. If $E = 75072.bc2$, we see that ρ_E has level $N = 4682 = 2^2 \cdot 3 \cdot 17 \cdot 23$. Since 2 is the only non-surjective prime, $n = 2^2 \cdot 3$. However, the level of the m-adic Galois representation associated to E is 2. On the other hand, it can also happen that $N = m_0$. For example, if $E = 54.b2$, we see that ρ_E has level 72, and this is also the level of the m-adic Galois representation associated to E.

Algorithm 2: Compute Reduced level

Input: $G(N) \leq \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ where $\operatorname{im}\rho_E = G$ and N is the level.
Output: $m_0 \in \mathbf{Z}^+$, the level of ρ_{E,m^∞} for $m = \prod_{\ell \in S_E} \ell$.

1 Let $n = \prod_{\ell \in S_E} \ell^{v_\ell(N)}$.
2 Compute the smallest m_0 dividing n such that

$$\#G(n) = \#G(m_0) \cdot \#\ker\left(\mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z}) \to \mathrm{GL}_2(\mathbf{Z}/m_0\mathbf{Z})\right).$$

3 **return** m_0

The validity of this algorithm is a consequence of the following proposition.

Proposition 22. *Let $E/\mathbf{Q}$ be a non-CM elliptic curve, and let $\operatorname{im}\rho_E = G \leq \mathrm{GL}_2(\widehat{\mathbf{Z}})$ be a subgroup of level N. Define $n \coloneqq \prod_{\ell \in S_E} \ell^{v_\ell(N)}$ and $m \coloneqq \prod_{\ell \in S_E} \ell$. If m_0 is the smallest positive integer dividing n such that*

$$\#G(n) = \#G(m_0) \cdot \#\ker\left(\mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z}) \to \mathrm{GL}_2(\mathbf{Z}/m_0\mathbf{Z})\right),$$

then m_0 is the level of the m-adic Galois representation associated to E.

Proof. First we will show that $\operatorname{im}\rho_{E,m^\infty} = \pi_1^{-1}(G(n))$, where $\pi_1 \colon \prod_{\ell \in S_E} \mathrm{GL}_2(\mathbf{Z}_\ell) \to \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$ is the natural reduction map. It suffices to show that $\ker\pi_1 \subseteq \operatorname{im}\rho_{E,m^\infty}$. We write $N = n \cdot n'$ with $\gcd(n,n') = 1$, and so we may identify $G(N)$ as a subgroup of $\mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z}) \times \mathrm{GL}_2(\mathbf{Z}/n'\mathbf{Z})$. Under this identification, let H be the intersection of $G(N)$ with the subgroup $\{I\} \times \mathrm{GL}_2(\mathbf{Z}/n'\mathbf{Z})$. Then since G has level N,

$$\pi^{-1}(H) \subseteq \operatorname{im}\rho_E,$$

where $\pi \colon \mathrm{GL}_2(\widehat{\mathbf{Z}}) \to \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ is the natural reduction map. The image of this subset relation under the natural projection map $\mathrm{GL}_2(\widehat{\mathbf{Z}}) \cong \prod_\ell \mathrm{GL}_2(\mathbf{Z}_\ell) \to \prod_{\ell \in S_E} \mathrm{GL}_2(\mathbf{Z}_\ell)$ gives

$$\ker(\pi_1) \subseteq \operatorname{im}\rho_{E,m^\infty},$$

as desired.

Let $\pi_2 \colon \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z}) \to \mathrm{GL}_2(\mathbf{Z}/m_0\mathbf{Z})$ be the natural reduction map. The assumption on m_0 implies that $\ker(\pi_2) \subseteq G(n)$, so it follows that $G(n) = \pi_2^{-1}(G(m_0))$. Thus if $\pi_3 \colon \prod_{\ell \in S_E} \mathrm{GL}_2(\mathbf{Z}_\ell) \to$

$\mathrm{GL}_2(\mathbf{Z}/m_0\mathbf{Z})$ denotes the reduction map, we have

$$\begin{aligned}\pi_3^{-1}(G(m_0)) &= \pi_1^{-1}(\pi_2^{-1}(G(m_0))) \\ &= \pi_1^{-1}(G(n)) \\ &= \operatorname{im} \rho_{E,m^\infty}.\end{aligned}$$

By construction m_0 is the smallest positive integer with this property. □

Corollary 23. *Algorithm 2 is correct.*

5. Primitive Points on Modular Curves

Let E be a non-CM elliptic curve. In this section, we will reduce the question of determining whether $j(E)$ is isolated to the analysis of an associated finite set of *primitive points* on modular curves. The primitive points are characterized by the following theorem.

Theorem 24. *Let $E/\mathbf{Q}$ be a non-CM elliptic curve. There exists a finite set $\mathcal{P} = \mathcal{P}(E)$ of primitive points in $\cup_{n\in\mathbf{Z}^+} X_1(n)$ associated to E which are characterized by the following properties:*

(i) *For each $N \in \mathbf{Z}^+$, a point $x \in X_1(N)$ with $j(x) = j(E)$ corresponds to a unique element $x' \in \mathcal{P}$ under the natural projection map. Moreover, if $x' \in X_1(a)$, then $a \mid N$ and $\deg(x) = \deg(f) \cdot \deg(x')$, where $f\colon X_1(N) \to X_1(a)$ is the natural map.*

(ii) *The rational number $j(E)$ is isolated if and only if there exists an isolated point in $\mathcal{P}$.*

Moreover, the set $\mathcal{P}$ is minimal with respect to conditions (i) and (ii).

Though in many ways this can be viewed as a refinement of results in [BEL+19], the uniqueness of Theorem 24 (i) is new. In Section 6, we give an algorithm for enumerating $\mathcal{P}(E)$ given a non-CM elliptic curve $E/\mathbf{Q}$.

5.1. Construction of $\mathcal{P}(E)$ and minimality.

Let $E/\mathbf{Q}$ be a non-CM elliptic curve, and let $m \geq 1$ be an integer. We begin by defining a directed graph $G(E, m)$ on the points of $X_1(n)$ corresponding to E for all $n|m$. The vertices of $G(E, m)$ are tuples (x, n, d) where:

(i) $n|m$,
(ii) x is a closed point on $X_1(n)$ of degree d, and
(iii) $j(x) = j(E)$.

We connect (x, n, d) with a directed edge to (x', n', d') if:

(i) n' is a proper divisor of n,
(ii) $x' = f(x)$ where $f\colon X_1(n) \to X_1(n')$ is the natural map, and
(iii) $d = d' \cdot \deg f$.

This is a directed acyclic graph. A **sink** in a directed acyclic graph is a vertex with no outgoing edges, and a **source** is a vertex with no incoming edges.

Definition 25. Let E be a non-CM elliptic curve over $\mathbf{Q}$ and let $m \geq 1$ be an integer. The **m-primitive points** of E are the sinks of $G(E, m)$. The **m-primitive degrees** are the tuples (n, d), where (x, n, d) is m-primitive for E. The union of all m-primitive points as m ranges over all positive integers is the set of **primitive points** associated to E, denoted $\mathcal{P}(E)$. The union of all m-primitive degrees is the set of **primitive degrees** associated to E.

By construction, for any $(x, n, d) \in \mathcal{P}(E)$, there does *not* exist a proper divisor $n' \mid n$ with $d = \deg(f) \cdot \deg(f(x))$, where $f\colon X_1(n) \to X_1(n')$ is the natural map. Thus $\mathcal{P}(E)$ is the minimal set which can satisfy Theorem 24(i).

Remark 26. Suppose $n''|n'|n|m$ and that $(x,n,d),(x',n',d'),(x'',n'',d'')$ are vertices in $G(E,m)$. This graph is **transitive**, meaning that if there is an edge from (x,n,d) to (x',n',d') and from (x',n',d') to (x'',n'',d''), then there is also an edge from (x,n,d) to (x'',n'',d''). Moreover, if there is an edge from (x,n,d) to (x'',n'',d''), then we claim there is an edge from (x,n,d) to (x',n',d'), where x' is the image of x on $X_1(n')$ and n' is any multiple of n'' which properly divides n. Intuitively, if the degree grows as much as possible from level n'' to level n then it also grows as much as possible from level n' to level n. Indeed, let $f_1\colon X_1(n)\to X_1(n')$ and $f_2\colon X_1(n')\to X_1(n'')$. Suppose for the sake of contradiction that $d<d'\cdot\deg f_1$. Since $d'\le d''\cdot\deg f_2$, this would imply $d<d''\cdot\deg f_1\cdot\deg f_2$. This contradicts our assumption that there is an edge from (x,n,d) to (x'',n'',d'').

Definition 27. Let $E/\mathbf{Q}$ be a non-CM elliptic curve and $m\in\mathbf{Z}^+$. For a fixed vertex (x,n,d) in $G(E,m)$, consider the directed graph induced by (x,n,d) and its **descendants**, i.e., all vertices (x',n',d') reachable by a path from (x,n,d). This is a directed acyclic graph with a single source, (x,n,d).

In Corollary 32 below, we will show the induced graph on the descendants of (x,n,d) has a single sink as well; this is $x'\in\mathcal{P}(\mathcal{E})$ associated to x, as in Theorem 24 (i).

5.2. **Finiteness of $\mathcal{P}(E)$.** Let $E/\mathbf{Q}$ be a non-CM elliptic curve, and let m be the product of 2, 3, and any primes ℓ such that the mod ℓ Galois representation of E is non-surjective. It is a consequence of Serre's Open Image Theorem [Ser72] that $m\in\mathbf{Z}^+$, and there exists $m_0\in\mathbf{Z}^+$ which is the level of the m-adic Galois representation of E. Suppose $v=(x,n,d)\in\mathcal{P}(E)$. Then v is a sink of $G(E,N)$ for some $N\in\mathbf{Z}^+$. By [BEL+19, Theorem 5.1], we have

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

where $f\colon X_1(n)\to X_1(\gcd(n,m_0))$ is the natural map. In particular, we are using the fact that $\{2,3\}\subseteq S_E$ here. If $\gcd(n,m_0)$ properly divides n, this contradicts the fact that v is a sink. Thus $\gcd(n,m_0)=n$ and $n\mid m_0$. In particular, v is a sink of $G(E,m_0)$. It follows that $\mathcal{P}(E)$ is the set of sinks of $G(E,m_0)$, and $\mathcal{P}(E)$ is finite since m_0 is a fixed positive integer depending only on E. We note in particular that the level of any primitive point will divide m_0, which in turn divides the level of the adelic Galois representation associated to E (see §4). We record this observation in the following proposition.

Proposition 28. *Let $E/\mathbf{Q}$ be a non-CM elliptic curve, and let $\mathcal{P}(E)$ denote the set of associated primitive points in $\cup_{n\in\mathbf{Z}^+}X_1(n)$. If $x\in X_1(a)$ is in $\mathcal{P}(E)$, then a divides m_0.*

5.3. **Preliminary Results.** In this section, we establish two results concerning the residue fields of points on modular curves.

Lemma 29. *Let $n_1,n_2\in\mathbf{Z}^+$ and $n=\operatorname{lcm}(n_1,n_2)$. For $g=\gcd(n_1,n_2)$, we define $n_1'\coloneqq n_1/g$ and $n_2'\coloneqq n_2/g$. Suppose E/F is an elliptic curve, and $P\in E(\overline{F})$ is a point of order n. If $n_2'P\in E(F)$ and $n_1'P\in E(F)$, then $P\in E(F)$.*

Proof. Note $n_2'P\in E(F)$ is a point of order n_1, and $n_1'P\in E(F)$ is a point of order n_2. Thus there is an element Q of order n in

$$\langle n_2'P,n_1'P\rangle\subseteq E(F).$$

Since $\langle n_2'P,n_1'P\rangle\subseteq\langle P\rangle$, it follows that the F-rational point Q is a generator of $\langle P\rangle$. In particular, $P\in\langle Q\rangle$, and so $P\in E(F)$, as desired. □

Lemma 30. *Let $n_1,n_2\in\mathbf{Z}^+$ and $n=\operatorname{lcm}(n_1,n_2)$. For $g=\gcd(n_1,n_2)$, we define $n_1'\coloneqq n_1/g$ and $n_2'\coloneqq n_2/g$. Let $x=[E,P]\in X_1(n)$ for an elliptic curve E with $j(E)\neq 0,1728$, and define $x_1=[E,n_2'P]\in X_1(n_1)$ and $x_2=[E,n_1'P]\in X_1(n_2)$. The residue field $\mathbf{Q}(x)$ is at most a quadratic extension of the compositum $\mathbf{Q}(x_1)\mathbf{Q}(x_2)$. Moreover:*

(i) *If $g > 2$, then $\mathbf{Q}(x_1)\mathbf{Q}(x_2) = \mathbf{Q}(x)$.*
(ii) *If $n_1 = 2$ or if $n_2 = 2$, then $\mathbf{Q}(x_1)\mathbf{Q}(x_2) = \mathbf{Q}(x)$.*

Proof. Since $F_1 = \mathbf{Q}(x_1)$ and $F_2 = \mathbf{Q}(x_2)$ are both subfields of $F = \mathbf{Q}(x)$, it follows that F_1F_2 is as well. We will show the degree of F/F_1F_2 is at most 2. If $n_1 = 2$ or $n_2 = 2$, we may assume without loss of generality that $n_2 = 2$. Fix a Weierstrass equation for $E/\mathbf{Q}(j(E))$ so we may identify $F_1 = \mathbf{Q}(j(E), \mathfrak{h}(n_2'P))$, $F_2 = \mathbf{Q}(j(E), \mathfrak{h}(n_1'P))$, and $F = \mathbf{Q}(j(E), \mathfrak{h}(P))$ by Lemma 12.

There exists E'/F_1 such that $\varphi\colon E \to E'$ is an isomorphism and $\varphi(n_2'P) \in E'(F_1)$; see, for example, [DR73, p. 274, Proposition VI.3.2]. Moreover, we have

$$F_2 = \mathbf{Q}(j(E), \mathfrak{h}(n_1'P)) = \mathbf{Q}(j(E), \mathfrak{h}(\varphi(n_1'P)))$$

by Remark 13, and the same remark shows that the x-coordinate of $\varphi(n_1'P)$ is rational over F_1F_2. The y-coordinate of $\varphi(n_1'P)$ is defined over at worst a quadratic extension L/F_1F_2, and $L = F_1F_2$ if $n_2 = 2$. Then $\varphi(P) \in E'(L)$ by Lemma 29. Since $\mathfrak{h}(\varphi(P)) = \mathfrak{h}(P)$, it follows that $F \subseteq L$.

Suppose that F/F_1F_2 is a quadratic extension. In particular, this means $n_1 \neq 2$ and $n_2 \neq 2$. Then consider E'/F_1F_2, and let $\{\varphi(P), Q\}$ be a basis for $E'[n]$. Recall that if $\rho_{E',n}(\sigma) = M \in \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$ with respect to this basis, then $M \pmod{n_1}$ gives $\rho_{E',n_1}(\sigma)$ with respect to the basis $\{n_2'\varphi(P), n_2'Q\}$. Similarly, $M \pmod{n_2}$ gives $\rho_{E',n_2}(\sigma)$ with respect to the basis $\{n_1'\varphi(P), n_1'Q\}$. Since $n_2'(\varphi(P))$ is F_1F_2-rational and only the x-coordinate of $n_1'\varphi(P)$ is defined over F_1F_2, there is $\sigma \in \mathrm{Gal}_{F_1F_2}$ such that $\sigma(n_1'\varphi(P)) = -n_1'\varphi(P)$ and $\sigma(n_2'(\varphi(P)) = n_2'\varphi(P)$. Thus $\sigma(\varphi(P)) = \alpha\varphi(P) + \beta Q$ where $\alpha \equiv 1 \pmod{n_1}$ and $\alpha \equiv -1 \pmod{n_2}$. Therefore g divides $2 = (\alpha + 1) - (\alpha - 1)$, so $g \leq 2$. □

5.4. **Proof of Theorem 24 (i).** Theorem 24 (i) is a consequence of a corollary to the following result.

Proposition 31. *Let $m \geq 1$ be an integer and let $E/\mathbf{Q}$ be a non-CM elliptic curve. In the graph $G(E, m)$, suppose (x, n, d) is connected by a path to both (x_1, n_1, d_1) and (x_2, n_2, d_2), where $n = \mathrm{lcm}(n_1, n_2)$. Then if $\gcd(n_1, n_2) \neq n_1, n_2$, it follows that both (x_1, n_1, d_1) and (x_2, n_2, d_2) connect to $(x_3, \gcd(n_1, n_2), d_3)$, where x_3 is the image of x on $X_1(\gcd(n_1, n_2))$ under the natural projection map.*

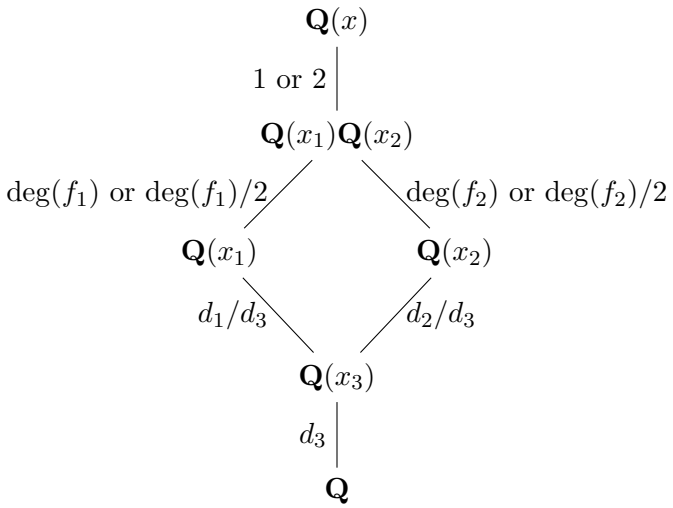


FIGURE 1. Degrees of Residue Fields

Proof. By assumption, the integer $g = \gcd(n_1, n_2)$ is a proper divisor of both $n_1 = gn_1'$ and $n_2 = gn_2'$. Let $f_1 \colon X_1(n) \to X_1(n_1)$ and let $f_2 \colon X_1(n) \to X_1(n_2)$. We consider two cases.

(i) Suppose $g > 2$, or if $g = 1$, that there exists $n_i \leq 2$. In the latter case, our assumptions imply that exactly one of n_1 or n_2 is equal to 2 and the other is greater than 2. So if $g = 1$, without loss of generality we may assume $n_1 > 2$ and $n_2 = 2$. In either case, we have $\mathbf{Q}(x_1)\mathbf{Q}(x_2) = \mathbf{Q}(x)$ by Lemma 30, and so by assumption

$$[\mathbf{Q}(x_1)\mathbf{Q}(x_2) : \mathbf{Q}(x_1)] = \deg(f_1),$$
$$[\mathbf{Q}(x_1)\mathbf{Q}(x_2) : \mathbf{Q}(x_2)] = \deg(f_2).$$

It follows from properties of composite fields that $\deg(f_1) \leq \frac{d_2}{d_3}$ and $\deg(f_2) \leq \frac{d_1}{d_3}$; see Figure 1. Note that for a prime $p \mid n_1'$, we have $p \nmid g$ if and only if $p \nmid n_2$. Similarly, for a prime $p \mid n_2'$, we have $p \nmid g$ if and only if $p \nmid n_1$. Thus by Corollary 17, we have

$$\frac{d_1}{d_3} \leq \deg(X_1(n_1) \to X_1(g)) = \deg(f_2),$$
$$\frac{d_2}{d_3} \leq \deg(X_1(n_2) \to X_1(g)) = \deg(f_1).$$

Thus $d_1 = d_3 \cdot \deg(X_1(n_1) \to X_1(g))$ and $d_2 = d_3 \cdot \deg(X_1(n_2) \to X_1(g))$, so the conclusion holds.

(ii) Suppose $g = 2$ or, if $g = 1$, that $n_1, n_2 > 2$. It follows from Lemma 30 and the same argument as above that $\frac{\deg(f_2)}{2} \leq \frac{d_1}{d_3}$ and $\frac{\deg(f_1)}{2} \leq \frac{d_2}{d_3}$; see Figure 1. However, since $n_1, n_2 > 2$ by assumption, we have

$$\frac{d_1}{d_3} \leq \deg(X_1(n_1) \to X_1(g)) = \frac{1}{2}(\deg(f_2)),$$
$$\frac{d_2}{d_3} \leq \deg(X_1(n_2) \to X_1(g)) = \frac{1}{2}(\deg(f_1)).$$

Thus $d_1 = d_3 \cdot \deg(X_1(n_1) \to X_1(g))$ and $d_2 = d_3 \cdot \deg(X_1(n_2) \to X_1(g))$, so the conclusion follows. □

Corollary 32. *Let $m \geq 1$ be an integer and let $E/\mathbf{Q}$ be a non-CM elliptic curve. For any fixed vertex $v = (x, n, d)$ in $G(E, m)$, the induced subgraph on its descendants has a single sink.*

Proof. Suppose the induced subgraph has two sinks, $v_1 = (x_1, n_1, d_1)$ and $v_2 = (x_2, n_2, d_2)$. We will show that $n_1 = n_2$, which implies $v_1 = v_2$ since both v_1 and v_2 are descendants of the same vertex (x, n, d). Let $g = \gcd(n_1, n_2)$. Since v_1, v_2 are sinks, we must have $g = n_1$ or $g = n_2$, by Proposition 31, so let $g = n_1 | n_2$. Remark 26 implies n_1 does not properly divide n_2 since v_2 is a sink. Therefore $n_1 = n_2$ and $v_1 = v_2$. □

5.5. **Proof of Theorem 24 (ii).** Let $E/\mathbf{Q}$ be a non-CM elliptic curve. If there exists an isolated point in $\mathcal{P}(E)$, then $j(E)$ is isolated by definition. To establish the other direction, suppose $j(E)$ is isolated. Then there exists an isolated point $x \in X_1(n)$ with $j(x) = j(E)$. By Theorem 24 (i), we see that x corresponds to a unique element $(x', n', d') \in \mathcal{P}(E)$ under the natural projection map. By the definition of $\mathcal{P}(E)$,

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

where $f \colon X_1(n) \to X_1(n')$ is the natural projection map. By [BEL+19, Theorem 4.3], the point x' is isolated.

6. Computing Primitive Degrees

Let E be a non-CM elliptic curve over $\mathbf{Q}$ and let $m \geq 1$ be an integer. In this section, we discuss an algorithm for computing the list of m-primitive degrees. At a high level, we are simply traversing the graph $G(E, m)$, always beginning at a source, until finding a sink. The sinks are the m-primitive points, and we record the associated m-primitive degree. We only retain the level n and degree d of a m-primitive point (x, n, d) since, in our main algorithm, we will often try to show that $X_1(n)$ has no isolated points of degree d at all. The input to the algorithm is $G = \operatorname{im} \rho_{E,m} \leq \mathrm{GL}_2(\mathbf{Z}/m\mathbf{Z})$. We represent m-primitive degrees as tuples (a, d) where a is the level of the point $x \in X_1(a)$ and $d = \deg x$.

Algorithm 3: Compute Primitive Degrees

Input: $G \leq \mathrm{GL}_2(\mathbf{Z}/m\mathbf{Z})$ such that $\operatorname{im} \rho_{E,m} = G$.

Output: The multiset of m-primitive degrees for E.

1 Let $H := \langle G, -I_2 \rangle \leq \mathrm{GL}_2(\mathbf{Z}/m\mathbf{Z})$.

2 Compute the orbits O of H acting on $(\mathbf{Z}/m\mathbf{Z})^2$. If $v \in (\mathbf{Z}/m\mathbf{Z})^2 \cong E[m]$ has order n, then v corresponds to $x \in X_1(n)$ with $j(x) = j(E)$. If $n > 2$, then $\deg(x) = \#(Hv)/2$, and $\deg(x) = \#(Hv)$ otherwise.

3 Let $D = \{\}$.

4 For each orbit $Hv \in O$ with v of order n, let $x \in X_1(n)$ be the associated point. Find the largest divisor $d \mid n$ such that $H(dv)$ associated to $x' \in X_1(n/d)$ satisfies $\deg(x) = \deg(x') \cdot \deg(X_1(n) \to X_1(n/d))$. Append $\langle n, (n/d, \deg(x')) \rangle$ to D.

5 **return** D

Example 33. Let $E/\mathbf{Q}$ be the non-CM elliptic curve 147.b1, and let m be the product of 2, 3, and all primes ℓ for which the mod ℓ Galois representation associated to E is not surjective. Zywina's algorithm [Zywa] gives the image of the adelic Galois representation as the complete preimage of $G \leq \mathrm{GL}_2(\mathbf{Z}/546\mathbf{Z})$, and applying Algorithm 2 to G shows the m-adic Galois representation has level 78. By Proposition 28, the level of any primitive point in $\mathcal{P}(E)$ divides 78. Applying Algorithm 3 to $\operatorname{im} \rho_{E,78}$ shows $\mathcal{P}(E)$ consists of 4 points: one point on $X_1(13)$ of degree 6, two points on $X_1(13)$ of degree 39, and one point on $X_1(1)$ of degree 1. The points on $X_1(13)$ are expected, since the mod 13 Galois representation of E is not surjective.

However, it is not necessarily the case that non-surjective primes must divide the level of some primitive point. For example, let $E/\mathbf{Q}$ be the non-CM elliptic curve 232544.f1. Then the adelic Galois representation of E has level 1892 and the m-adic level is 44. In particular, the mod 11 Galois representation associated to E is non-surjective. However, in this case $\mathcal{P}(E)$ consists of a single point, namely, the degree one point on $X_1(1)$ associated to E.

We briefly discuss Algorithm 3. Conceptually, to compute the m-primitive degrees of E, we compute for each closed point $x \in X_1(n)$ above E with $n \mid m$ the unique (by Corollary 32) m-primitive point induced by x and record its level a and degree d. In practice, instead of working with points on $X_1(m)$ above E, we compute with the matrix group $G = \operatorname{im} \rho_{E,m}$ and the orbits of points in $(\mathbf{Z}/m\mathbf{Z})^2$ under the left-action of G. The following proposition allows us to calculate the degrees of points on modular curves from their associated orbit data.

Proposition 34. *Let $E/\mathbf{Q}$ be a non-CM elliptic curve and $m \in \mathbf{Z}^+$. Let $\operatorname{im} \rho_{E,m} \cong G \leq \mathrm{GL}_2(\mathbf{Z}/m\mathbf{Z})$ and let $H = \langle G, -I \rangle$. Let $v \in (\mathbf{Z}/m\mathbf{Z})^2$ have order $n|m$ and let (E, P) be a representative of the point x of $X_1(n)$ corresponding to Gv. If $n > 2$, the degree of x is $\#Hv/2$. If $n \leq 2$, the degree of x is $\#Hv = \#Gv$.*

Proof. We begin by noting that (E, P) and $(E, -P)$ induce the same closed point x on $X_1(n)$. Therefore, since E is defined over $\mathbf{Q}$, the degree of x depends only on $x(P)$ and is equal to $[\mathbf{Q}(x(P)) :$

$\mathbf{Q}]$; see Remark 13. We next observe that $[\mathbf{Q}(P):\mathbf{Q}] = \#Gv$. Assume that $n > 2$. When $-I \in G$, the points P and $-P$ are distinct and in the same Galois orbit so $[\mathbf{Q}(x(P)):\mathbf{Q}] = \frac{1}{2}[\mathbf{Q}(P):\mathbf{Q}]$ and $\#Hv = \#Gv$. We conclude that

$$\deg x = [\mathbf{Q}(x(P)):\mathbf{Q}] = \frac{1}{2}[\mathbf{Q}(P):\mathbf{Q}] = \frac{1}{2}\#Gv = \frac{1}{2}\#Hv.$$

If $-I \notin G$, then there exists a twist E' of $E/\mathbf{Q}$ such that $\operatorname{im}\rho_{E',n} = \langle G, -I\rangle$ by [Sut16, Corollary 5.25]. The point (E,P) is also represented by (E',P') for some $P' \in E'[n]$, and the same argument from above implies

$$\#Hv = [\mathbf{Q}(P'):\mathbf{Q}] = 2[\mathbf{Q}(x(P')):\mathbf{Q}] = 2[\mathbf{Q}(x(P)):\mathbf{Q}],$$

so we again have that the degree of the point represented by (E,P) is $\frac{1}{2}\#Hv$.

Now assume $n \leq 2$. Then $-I = I$ in $\mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$ so $G = H$, and $\mathbf{Q}(x(P)) = \mathbf{Q}(P)$. We conclude

$$\deg x = [\mathbf{Q}(x(P)):\mathbf{Q}] = [\mathbf{Q}(P):\mathbf{Q}] = \#Gv = \#Hv. \qquad \square$$

7. Genus 0 adelic images do not produce isolated points

Let $E/\mathbf{Q}$ be an elliptic curve and $G \leq \mathrm{GL}_2(\hat{\mathbf{Z}})$ its adelic image. Let $G(N)$ denote the image of its mod N representation. Denote by $B_1(N)$ the subgroup of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ consisting of the upper triangular matrices with a 1 in the upper left entry. Note that $X_{B_1(N)} = X_1(N)$. We say that a congruence group Γ is of genus g if X_Γ is of genus g. We say that a point x corresponds to an elliptic curve E if $j(x) = j(E)$. In this section, we show that elliptic curves with genus 0 mod N image do not correspond to $\mathbf{P}^1$-isolated points on $X_1(N)$.

Lemma 35. *Let $f\colon X \to Y$ be a finite morphism of curves of degree d. Then f induces a non-constant morphism $f^*\colon Y \to X^{(d)}$.*

Proof. The point is to show that the natural map $y \mapsto f^{-1}(y)$ is a morphism of schemes. Note that the composition of $\Gamma_f\colon X \to X \times Y$ sending X to the graph of f with $X \times Y \to Y$ is just f, which is flat as a finite morphism of irreducible curves [Liu02, Proposition 4.3.9]. So the graph of f defines a relative effective Cartier divisor in the sense of [Mil86b, Definition 3.4] on $X \times Y/Y$ of degree d. Since all our schemes are regular, we can identify Cartier with Weil divisors. In the hypothesis of the statement of [Mil86b, Theorem 3.13], we can thus take the effective divisor to be the graph of f. This allows us to conclude that, as a map of sets, f^* maps $y \in Y$ to the degree-d divisor $f^{-1}(y) := [\{y\} \times_Y X]$ with the multiplicities of the reduced subscheme of the points in the fiber product equal to the ramification indices (see [Ful98, § 1.5, § 1.7]).

The morphism f^* is non-constant since fibers above different points are mapped to different points by f^*. $\square$

The following lemma rephrases the definition of a point being $\mathbf{P}^1$-parametrized of degree d.

Lemma 36 (Characterization of $\mathbf{P}^1$-parametrized points)**.** *Let X/k be a curve. Let $x \in X^{(d)}(k)$ be an irreducible degree d divisor. The following are equivalent:*

(i) *The point x is $\mathbf{P}^1$-parametrized.*
(ii) *There is a non-constant rational map $\mathbf{P}^1 \dashrightarrow X^{(d)}$ containing x in its image.*

Proof. (i) $\implies$ (ii): If x is $\mathbf{P}^1$-parametrized, then there is an $x' \in X^{(d)}(k)$ different from x such that $x - x' = \operatorname{div}(f)$ for a non-constant function $f \in k(X)$. Here we treat x and x' as effective divisors of degree d on X. This gives a degree d map $f\colon X \to \mathbf{P}^1$, which gives the copy of $\mathbf{P}^1$ inside $X^{(d)}$ as the image under pullback of f as in Lemma 35.

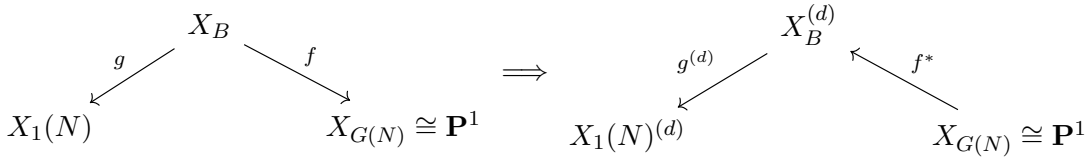
(ii) $\implies$ (i): Since every rational map from a unirational variety to an abelian variety is constant [Mil86a, Corollary 3.9], the $\mathbf{P}^1$ is contracted to a point under $\Phi_d\colon X^{(d)} \to \mathrm{Jac}(X)$. $\square$

Lemma 37. *Let $f\colon X \to Y$ be a finite morphism of curves and x a closed point on X, and assume $\deg x = \deg f(x)$. If x is $\mathbf{P}^1$-parametrized, then so is $f(x)$.*

Proof. Let $d = \deg(x)$. The proof is diagram chasing using $\mathbf{P}^1 \to X^{(d)} \xrightarrow{f^{(d)}} Y^{(d)}$, where $f^{(d)}$ is the natural map from $X^{(d)}$ to $Y^{(d)}$ induced by f. If $x \in X$ is not $\mathbf{P}^1$-isolated (i.e., x is $\mathbf{P}^1$-parametrized), then by Lemma 36, x can be viewed as a point on $X^{(d)}$ lying on the image of a non-constant map from $\mathbf{P}^1$ to $X^{(d)}$. Furthermore, $f(x)$ lies on the image of this $\mathbf{P}^1$ (which is again a $\mathbf{P}^1$ by Lemma 35 or because the induced morphism on the d-th symmetric power is again finite) inside of $Y^{(d)}$. Now the conclusion follows by Lemma 36. □

Theorem 38. *Let $E/\mathbf{Q}$ be an elliptic curve with mod N image $G(N)$ of genus 0 and N a positive integer. Then every $x \in X_1(N)$ with $j(x) = j(E)$ is $\mathbf{P}^1$-parametrized.*

Proof. Let $x = [E, P] \in X_1(N)$. Replacing $G(N)$ with an appropriate choice of conjugation if necessary, we may assume $G(N)$ is with respect to a basis having P as its first element. Let y be a $\mathbf{Q}$-rational point on $X_{G(N)}$ corresponding to E. Let $B := B_1(N) \cap G(N)$ in $G(N)$, and let $d := [\pm G(N) : \pm B]$. The proof is diagram chasing in the following two diagrams while keeping track of the degree of the point. The situation is as follows:



Let $f\colon X_B \to X_{G(N)} \cong \mathbf{P}^1$ be the corresponding degree d map of modular curves. Lemma 35 yields a non-constant morphism $f^*\colon X_{G(N)} \to X_B^{(d)}$ such that $f^*(y)$ lies on a $\mathbf{P}^1 \cong X_{G(N)}$. Hence any point in the support of the divisor represented by $f^*(y)$ in X_B is $\mathbf{P}^1$-parametrized by Lemma 36. Consider the morphism $g\colon X_B \to X_1(N)$ corresponding to $B \leq B_1(N)$. Let $x' \in X_B$ be such that $g(x') = x$ and $f(x') = y$. We want to show that $g(x')$ has the same degree as x'. Note that $\deg(x')$ is d and of $\deg(x) = [\pm G(N) : \pm B]$ as $\pm B$ is the stabilizer of x. Hence it satisfies $\deg(g(x')) = \deg(x')$, so x is $\mathbf{P}^1$-parametrized by Lemma 37. □

Corollary 39. *Let $E/\mathbf{Q}$ be an elliptic curve with adelic image G of genus 0 and n a positive integer. Then every $x \in X_1(n)$ with $j(x) = j(E)$ is $\mathbf{P}^1$-parametrized.*

Proof. Since G is by assumption of genus 0, it follows that so is $G(n)$. The result then follows from Theorem 38. □

Example 40. Consider the elliptic curve E with LMFDB label 15.a7, which has adelic image of genus 13. We can show E has the following primitive points:

- $X_1(1)$ of degree 1,
- $X_1(2)$ of degrees 1 and 2,
- $X_1(4)$ of degree 1,
- $X_1(8)$ of degree 2,
- $X_1(16)$ of degree 4, and
- $X_1(32)$ of degree 8.

By Theorem 24, it follows that $j(E) = -1/15$ is isolated if and only if one of these points is isolated. Any point $x \in X_1(n)$ with $\deg(x) > \text{genus}(X_1(n))$ has Riemann–Roch space of dimension at least 2 and thus is $\mathbf{P}^1$-parametrized. It remains only to address the point on $X_1(32)$ of degree 8. However, the mod 32 Galois representation of E has genus 0, so this point is $\mathbf{P}^1$-parametrized by Theorem 38. We may conclude that $j(E) = -1/15$ is not an isolated j-invariant.

8. Validity of Main Algorithm

In this section, we will prove that our Main Algorithm as stated in Section 3 is valid. The section concludes with an additional example.

Theorem 41. *Let $j \in \mathbf{Q}$ be a non-CM j-invariant. If Algorithm 1 returns $\{(a_1, d_1), \ldots, (a_k, d_k)\}$, then any isolated point $x \in X_1(N)$ for $N \in \mathbf{Z}^+$ with $j(x) = j$ maps under the natural projection map to an isolated point of degree d_i on $X_1(a_i)$ for some $1 \leq i \leq k$.*

Remark 42. Since our algorithm builds on that of Zywina [Zywa], it is possible that our algorithm will give an error if the adelic image cannot be computed. See Zywina [Zywb] for details. In particular, he notes that "errors will always occur if E gives rise to an unknown exceptional rational point on certain high genus modular curves." We are not aware of any instances when this error occurs.

Remark 43. The range of the moduli to which `PrimitiveDegreesOfPoints` is applicable is restricted by the amount of memory Magma can use. The input of very large matrix groups may result in a runtime error. Because we take preliminary steps to reduce the modulus of the matrix group (i.e., Section 4), this error did not occur when running our full algorithm on all elliptic curves currently in the LMFDB.

Proof. Let $E/\mathbf{Q}$ be a non-CM elliptic curve with $j(E) = j$. We note that the choice of E will not impact our result; see Section 2.3. We may compute $\operatorname{im} \rho_E = G$ via Zywina's algorithm [Zywa], and represent the output as $G(N) \leq \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ where N is the level. By Algorithm 2, we may use $G(N)$ to compute the level m_0 of the m-adic Galois representation associated to E, where m is the product of 2, 3, and all non-surjective primes. By Proposition 28, the level of any primitive point in $\mathcal{P}(E)$ will divide m_0, so applying Algorithm 3 to $\operatorname{im} \rho_{E,m_0}$ results in the complete set of primitive degrees for E. In particular, for each closed point $x \in X_1(n)$ with $j(x) = j$ and $n \mid m_0$, we have x mapping to the primitive point $x' \in X_1(a)$ of degree d. We record the entry $\langle n, (a, d)\rangle$ in the multiset D. By Theorem 24, we have $\deg(x) = \deg(x') \cdot \deg(X_1(n) \to X_1(a))$, and j is isolated if and only if there is an isolated point on $X_1(a_i)$ of degree d_i for some $\langle n_i, (a_i, d_i)\rangle$ in D.

Next, we will rule out pairs (a, d) which cannot correspond to isolated points. If $d > \operatorname{genus}(X_1(a))$, then the point is not $\mathbf{P}^1$-isolated since its associated Riemann–Roch space has dimension at least 2. Thus we need only consider the multiset $D' \subseteq D$ containing those elements $\langle n, (a, d)\rangle$ for which $d \leq \operatorname{genus}(X_1(a))$. The integer n is not relevant for our purposes, so we create a new multiset M containing (a, d) from D'. We record (a, d) with multiplicity μ if and only if $X_1(a)$ has μ distinct closed points of degree d which are associated to E.

Finally, by Theorem 38, we may remove from M any pair (a, d) where $\operatorname{im} \rho_{E,a}$ corresponds to a modular curve of genus 0. Since Algorithm 1 returns M, we are done. □

Corollary 44. *If Algorithm 1 outputs an empty set on some non-CM j-invariant $j \in \mathbf{Q}$, then j is not the image of an isolated point on $X_1(N)$ for any positive integer N.*

Example 45. We end this section with an extended example to illustrate the impact of each step in Algorithm 1. Let $E = 1225.b1$, a non-CM elliptic curve over $\mathbf{Q}$, and let m denote the product of 2, 3, and all non-surjective primes. Here, one can check that $m = 162$.

(i) Zywina's algorithm shows the adelic image of E is of level $N = 5180$. Let $G(N) \coloneqq \operatorname{im} \rho_{E,N}$.
(ii) Algorithm 2 shows that the level of the m-adic Galois representation of E is 148.
(iii) Algorithm 3 shows that it suffices to consider points on $X_1(n)$ where $n \mid 37$. In particular, it is not necessary to consider points on $X_1(74)$ or $X_1(148)$ since any will map under the natural projection map to a modular curve of lower level. There is a single point of degree 1 on $X_1(1)$ and 4 points on $X_1(37)$ — one of degree 18 and 3 of degree 222.

(iv) We compute that $\mathrm{genus}(X_1(37)) = 40$ and $\mathrm{genus}(X_1(1)) = 0$. Thus no point of degree 222 on $X_1(37)$ can be isolated, and neither is the rational point on $X_1(1)$.
(v) Since the modular curve associated to $\mathrm{im}\,\rho_{E,37}$ has genus 4, the algorithm returns $\{(37, 18)\}$.

9. Remaining Filters and Computational Results

Suppose $E/\mathbf{Q}$ is non-CM elliptic curve such that one of the following holds:

- $N_E \leq 500\,000$,
- N_E is only divisible by primes $p \leq 7$, or
- $N_E = p \leq 300\,000\,000$ for some prime number p.

Then running Algorithm 1 on E results in the empty set, aside from the j-invariants listed in Table 1; the output from elliptic curves in the Stein–Watkins database yields no additional j-invariants. The final step in the main algorithm filters out curves with mod N genus 0; we also list in the table the mod N genus. This genus is computed using code associated to the paper [RSZB22].

j	(N, d)	genus mod N
$-140625/8$	$\{(21, 3)^2\}$	1
-162677523113838677	$\{(37, 18)\}$	4
$-882216989/131072$	$\{(17, 4)^2\}$	1
-9317	$\{(37, 6)^3\}$	4
$16778985534208729/81000$	$\{(24, 4)^2\}$	1
$351/4$	$\{(28, 9)^2\}$	5

Table 1. Output of main algorithm

In this section we describe additional computations that prove that the only $\mathbf{P}^1$-isolated points on $X_1(N)$ for a fixed N correspond to the four j-invariants $j = -140625/8, -9317, 351/4$, and -16267752311383867, proving Theorem 2. Since $j = -140625/8, -9317$, and $351/4$ are known to be isolated (see Section 1), it suffices to consider only the remaining 3 j-invariants.

9.0.1. *Degree* 18 *point on* $X_1(37)$ *corresponding to* $j = -162677523113838677$. We show that the point $x \in X_1(37)(K)$, where K is a degree 18 number field, and $j(x) = -162677523113838677$ is $\mathbf{P}^1$-isolated. We explicitly compute the coordinates of x on a model of $X_1(37)$ and define σ_i, for $i = 1, \ldots, 18$ to be the automorphisms of K and $D = \sum_{i=1}^{18} \sigma_i(x)$. Reducing everything modulo 3 and denoting the reduction of D modulo 3 by $\overline{D}$, we obtain $\ell(\overline{D}) = 1$, which shows that the reduction $\overline{x}$ of x modulo 3 is $\mathbf{P}^1$-isolated. Hence it follows that x is $\mathbf{P}^1$-isolated.

9.0.2. *Degree* 4 *point on* $X_1(17)$ *corresponding to* $j = -882216989/131072$ *and degree* 4 *point on* $X_1(24)$ *corresponding to* $j = 16778985534208729/81000$. To show that these points are not isolated we compute the coordinates of a degree 4 point x corresponding to our curve on a model of $X_1(17)$ and $X_1(24)$. Such a point x is defined over a cyclic quartic field. Let σ_i, for $i = 1, \ldots, 4$ be the automorphisms of K and $D = \sum_{i=1}^{4} \sigma_i(x)$. In each case, we compute $\ell(D) = 2$, which implies that x is not $\mathbf{P}^1$-isolated.

The fact that the degree 4 point on $X_1(17)$ is not $\mathbf{P}^1$-isolated also follows from the results of [DMK18, Proposition 6.7], where it is shown that there are no $\mathbf{P}^1$-isolated quartic points on $X_1(17)$.

9.1. **Computations.** We give some details on the implementation and runtime of the algorithm in this section. We ran Algorithm 1 on two databases of j-invariants of elliptic curves over $\mathbf{Q}$:

- The LMFDB [Col] contains all elliptic curves over $\mathbf{Q}$ of conductor up to 500 000 and includes roughly 2 million j-invariants.
- The Stein–Watkins database [SW02] contains roughly 36 million unique j-invariants of elliptic curves over $\mathbf{Q}$ of absolute discriminant at most 10^{12} that have conductor at most 10^8 or prime conductor at most 10^{10}. However, it has been filtered to include just one representative from each isogeny class and each class of quadratic twists.

All computations were run on a server with an AMD EPYC 7713 2GHz CPU and Magma V2.28-3 [BCP97]. For every elliptic curve $E/\mathbf{Q}$ in the LMFDB, the database contains the genus of X_G where G is the image of the adelic Galois represenation of E. Applying Corollary 39, we filtered the roughly 2 million j-invariants of non-CM elliptic curves $E/\mathbf{Q}$ in the LMFDB to a set of 30 141, such that the image of the adelic Galois representation of E is greater than 0. On this set, the computation took 2 CPU hours and 1714 MB of memory. The Stein–Watkins database contains 35 788 699 unique j-invariants of non-CM elliptic curves over $\mathbf{Q}$, with no information about the image of the adelic Galois representation. Running Algorithm 1 on this database took 442 CPU hours.

10. Appendix: by Maarten Derickx and Mark van Hoeij

Let $X = X_1(37)$ and D be the divisor for the degree 18 closed point in Section 9.0.1. Through the maps $X \to X_0(37) \to X_0(37)^+$, we can view the Jacobian of the latter, $A := J_0(37)^+$, as a abelian subvariety of $J_1(37)$. The question of whether D is AV isolated is equivalent to $\Phi_d(D) + A$ not being contained in $W_{18}(X)$, where $W_d(X) := \Phi_d(X^{(d)})$ with Φ_d as in Section 2.1.

Lemma 46. *Let A be an abelian subvariety of $\mathrm{Jac}(X)$ and let $\pi : X^{(d)} \to J(X)/A$ be the composition of Φ_d with the quotient map. Let $D \in X^{(d)}$ and suppose that $\Phi_d(D) + A \subseteq W_d(X)$, then π, restricted to the tangent space at D, is not injective.*

Proof. Assume that Φ_d is injective on the tangent space at D, otherwise there is nothing to prove as π factors through Φ_d. Then Φ_d induces an isomorphism between the tangent spaces of $X^{(d)}$ at D, and W_d at $\Phi_d(D)$. The positive dimensional variety $\Phi_d(D) + A$ is contracted to a point under the quotient map $J(X) \to J(X)/A$, in particular the entire tangent space of $\Phi_d(D) + A$ at $\Phi_d(D)$ is sent to zero under the quotient map, and the result follows. □

Corollary 47. *If the corresponding map $\pi^* : \mathrm{Cot}_0 J(X)/A \to \mathrm{Cot}_D X^{(d)}$ on cotangent spaces is surjective then there is no translate of A contained in $W_d(X)$ passing through $\Phi_d(D)$.*

Proof. This is because a map on tangent spaces is injective if and only if the corresponding map on cotangent spaces is surjective. □

In other words, if π is a *formal immersion* [DKSS] at D then D is AV-isolated. To prove that π is a formal immersion at D, can use Proposition 3.7 in [DKSS] if we have a basis of the cotangent space of A viewed as a subspace of $J(X)$.

Write $D = y_1 + \cdots + y_{18}$ where the y_i form the Galois orbit corresponding to the degree 18 closed point. These y_i also form one orbit under the diamond operators (they map to the same point in $X_0(37)$). We order them in such a way that $y_i = \langle 2^i \rangle y_1$. Let q_1 be a uniformizer at y_1, and let $q_i := q_1 \circ \langle 2^{-i} \rangle$ be the corresponding uniformizer at y_i. Note that since A is inside $J_0(37)$ we have $(\langle 2 \rangle - 1)(A) = 0$, so $\langle 2 \rangle - 1$ factors via $J(X)/A$. In particular all one-forms of the form $\langle 2^i \rangle(\langle 2 \rangle - 1)w$ inside $\mathrm{Cot}_0 J(X)$ come from $\mathrm{Cot}_0 J(X)/A$.

Next we show that there is a one-form w such that $a(w, q_1, 1) = 1$ and $a(w, q_i, 1) = 0$ for all $i > 1$, with $a(\ldots)$ as in Proposition 3.7 in [DKSS]. By Riemann Roch,

$$\dim H^0(O_X(y_1 + \ldots + y_{18})) - \dim H^0(\Omega^1(-y_1 - \ldots - y_{18})) = 18 + 1 - 40$$

and

$$\dim H^0(O_X(y_2 + \ldots + y_{18})) - \dim H^0(\Omega^1(-y_2 - \ldots - y_{18})) = 17 + 1 - 40.$$

Now $\dim H^0(O_X(y_1 + \ldots + y_{18})) = 1$ (equivalent to the degree 18 point being $\mathbf{P}^1$-isolated) and thus equal to $\dim H^0(O_X(y_2 + \ldots + y_{18}))$. Then by Riemann Roch,

$$\dim H^0(\Omega^1(-y_2 - \ldots - y_{18})) > \dim H^0(\Omega^1(-y_1 - \ldots - y_{18})).$$

So the wanted one-form w can be found by picking an element of $H^0(\Omega^1(-y_2 - \ldots - y_{18}))$ that is not in $H^0(\Omega^1(-y_1 - \ldots - y_{18}))$ and scaling it to make $a(w, q_1, 1) = 1$.

Now let $w_i = \langle 2^i \rangle (\langle 2 \rangle - 1)w$. These one-forms all come from $\mathrm{Cot}_0 J(X)/A$ as mentioned before. The matrix in Proposition 3.7 in [DKSS] now has the following form:

$$\begin{pmatrix} 1 & -1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & -1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & -1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & -1 \end{pmatrix}$$

This matrix has rank 17, but for Proposition 3.7, we need rank 18. An additional one-form w' with $a(w', q_1, 1) = \ldots = a(w', q_{18}, 1) = 1$ would increase the rank to 18. We can take w' to be the pullback of a one-form on $J_0(37)^-$ to $J(X)$. Indeed, $J_0(37)^-$ is a quotient of $J_0(37)/A$ and thus of $J(X)/A$. Such w' is invariant under the diamond operators so $a(w', q_1, 1) = \ldots = a(w', q_{18}, 1)$ automatically holds. It remains to show that it does not vanish at y_1. Since $J_0(37)^-$ is an elliptic curve, w' does not vanish anywhere, and in particular not at the image of y_1 in $J_0(37)^-$. The only possibility for w' to vanish at y_1 is then for $X_1(37) \to J_0(37)^-$ to be ramified at y_1, however, this is not the case since the map is only ramified at CM points, and y_1 does not have CM. Indeed, $X_1(37) \to X_0(37)$ only ramifies at $j = 0$ and $j = 1728$, while $X_0(37) \to J_0(37)^-$ only ramifies at fixed points of the Atkin-Lehner involution, which have CM as well (by an order in $\mathbb{Q}(\sqrt{-37})$).

References

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. volume 24, pages 235–265. 1997. Computational algebra and number theory (London, 1993). ↑4, 20.

[BEL+19] 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.*, 357:106824, 33, 2019. ↑1, 2, 3, 5, 6, 9, 10, 11, 12, 14.

[BGRW] 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, 3.

[BM] Jennifer S. Balakrishnan and Barry Mazur. Ogg's torsion conjecture: Fifty years later. Available at arxiv.org:2307.04752. ↑1, 4.

[BN] Abbey Bourdon and Filip Najman. Sporadic points of odd degree on $X_1(N)$ coming from $\mathbb{Q}$-curves. Preprint available at arxiv.org:2107.10909. ↑4, 7.

[BP11] Yuri Bilu and Pierre Parent. Serre's uniformity problem in the split Cartan case. *Ann. Math. (2)*, 173(1):569–584, 2011. ↑3.

[CGPS22] Pete L. Clark, Tyler Genao, Paul Pollack, and Frederick Saia. The least degree of a CM point on a modular curve. *J. Lond. Math. Soc. (2)*, 105(2):825–883, 2022. ↑1.

[Col] The LMFDB Collaboration. The L-functions and modular forms database, (2023). Available at `lmfdb.org`. ↑2, 20.

[DEvH+21] Maarten Derickx, Anastassia Etropolski, Mark van Hoeij, Jackson S. Morrow, and David Zureick-Brown. Sporadic cubic torsion. *Algebra Number Theory*, 15(7):1837–1864, 2021. ↑1.

[DKSS] Maarten Derickx, Sheldon Kamienny, William Stein, and Michael Stoll. Torsion points on elliptic curves over number fields of small degree. Preprint available at arxiv.org/pdf/1707.00364v1.pdf. ↑20, 21.

[DMK18] Maarten Derickx, Barry Mazur, and Sheldon Kamienny. Rational families of 17-torsion points of elliptic curves over number fields. In *Number theory related to modular curves: Momose memorial volume. Proceedings of the Barcelona-Boston-Tokyo Number Theory Seminar in memory of Fumiyuki Momose, Barcelona, Spain, May 21–23, 2012*, pages 81–104. Providence, RI: American Mathematical Society (AMS), 2018. ↑19.

[DR73] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349, 1973. ↑6, 7, 13.

[Duk97] William Duke. Elliptic curves with no exceptional primes. *C. R. Acad. Sci., Paris, Sér. I, Math.*, 325(8):813–818, 1997. ↑3.

[DvH14] Maarten Derickx and Mark van Hoeij. Gonality of the modular curve $X_1(N)$. *J. Algebra*, 417:52–71, 2014. ↑1, 9.

[Fal83] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983. ↑6.

[Fal94] Gerd Faltings. The general case of S. Lang's conjecture. In *Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991)*, volume 15 of *Perspect. Math.*, pages 175–182. Academic Press, San Diego, CA, 1994. ↑5.

[Fre94] Gerhard Frey. Curves with infinitely many points of fixed degree. *Israel J. Math.*, 85(1-3):79–83, 1994. ↑1, 9.

[Ful98] William Fulton. *Intersection theory*, volume 2 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 1998. ↑16.

[Gre10] Aaron Greicius. Elliptic curves with surjective adelic Galois representations. *Experiment. Math.*, 19(4):495–507, 2010. ↑8.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications. ↑6, 16.

[LR13] Álvaro Lozano-Robledo. On the field of definition of p-torsion points on elliptic curves over the rationals. *Math. Ann.*, 357(1):279–305, 2013. ↑2, 3.

[Maz78] B. Mazur. Rational isogenies of prime degree. (With an appendix by D. Goldfeld). *Invent. Math.*, 44:129–162, 1978. ↑3.

[Mil86a] J. S. Milne. Abelian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986. ↑16.

[Mil86b] J. S. Milne. Jacobian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 167–212. Springer, New York, 1986. ↑16.

[Naj16] F. Najman. Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$. *Math. Res. Lett.*, 23(1):245–272, 2016. ↑1.

[RSZB22] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown. ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$ (and an appendix with John Voight). *Forum Math. Sigma*, 10:Paper No. e62, 63, 2022. With an appendix with John Voight. ↑6, 19.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972. ↑1, 2, 4, 8, 12.

[Ser97] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre. ↑1, 5.

[Shi71] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971. Kanô Memorial Lectures, No. 1. ↑7.

[Sut16] Andrew V. Sutherland. Computing images of Galois representations attached to elliptic curves. *Forum Math. Sigma*, 4:e4, 79, 2016. ↑2, 4, 16.

[SW02] William A. Stein and Mark Watkins. A database of elliptic curves—first report. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 267–275. Springer, Berlin, 2002. ↑2, 20.

[vH] Mark van Hoeij. Low degree places on the modular curve $X_1(n)$. Preprint available at arxiv.org:1202.4355. ↑1.

[Zywa] David Zywina. Explicit open images for elliptic curves over $\mathbb{Q}$. Preprint available at arxiv.org:2206.14959. ↑2, 3, 9, 10, 15, 18.

[Zywb] David Zywina. Github repository related to *Explicit open images for elliptic curves over* $\mathbb{Q}$. Available at `https://github.com/davidzywina/OpenImage`. ↑18.

[Zywc] David Zywina. On the possible image of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$. Available at arxiv.org:1508.07660. ↑2, 4.

Abbey Bourdon, Wake Forest University, Department of Mathematics, 127 Manchester Hall, PO Box 7388, Winston-Salem, NC 27109
Email address: bourdoam@wfu.edu

Sachi Hashimoto, Department of Mathematics, Brown University, Box 1917, 151 Thayer Street, Providence, RI, 02912
Email address: sachi_hashimoto@brown.edu
URL: https://sachihashimoto.github.io/

Timo Keller, Rijksuniveriteit Groningen, Bernoulli Institute, Bernoulliborg, Nijenborgh 9, 9747 AG Groningen, The Netherlands (previously: Leibniz Universität Hannover, Institut für Algebra, Zahlentheorie und Diskrete Mathematik, Welfengarten 1, 30167 Hannover, Germany)
Email address: t.keller@rug.nl
URL: https://www.timo-keller.de

Zev Klagsbrun, Center for Communications Research - La Jolla, 4320 Westerra Court, San Diego, CA, 92121
Email address: zdklags@ccr-lajolla.org

David Lowry-Duda, ICERM, 121 South Main Street, Box E, 11th Floor, Providence, RI, 02903
Email address: david@lowryduda.com
URL: https://davidlowryduda.com

Travis Morrison, Virginia Tech Department of Mathematics, 226 Stanger Street, 24061 Blacksburg, VA USA
Email address: tmo@vt.edu
URL: https://travismo.github.io/

Filip Najman, University of Zagreb, Bijenička Cesta 30, 10000 Zagreb, Croatia
Email address: fnajman@math.hr
URL: https://web.math.pmf.unizg.hr/~fnajman/

Himanshu Shukla, Mathematisches Institut, Uiversität Bayreuth, Universitätstrasse 30, 95444 Bayreuth, Germany
Email address: Himanshu.Shukla@uni-bayreuth.de
URL: https://www.mathe2.uni-bayreuth.de/hishukla/