Modular Curves and Galois Representations

Abbey Bourdon

June 1, 2025

These notes are based on a series of lectures given at the workshop *Arithmetic Geometry at UNT*, which took place at the University of North Texas from May 5-9, 2025 under the leadership of Lea Beneish. The goal is to provide a kind of "starter pack" for graduate students who have had a yearlong sequence in graduate algebra and want to begin research in the area. These notes are complimented by a list of exercises, written in collaboration with Santiago Arango-Piñeros.

In addition to standard results in modern algebra concerning groups, rings, modules, and fields, these notes assume familiarity with the following definitions:

- The p-adic integers $\mathbb{Z}_p$ and the profinite completion of the integers $\widehat{\mathbb{Z}}$.
- The function field $k(C)$ of a curve C over a number field k.
- Divisors on a curve, the divisor of a function, and the Riemann-Roch space associated to a divisor.
- The genus of a curve.

Comfort with 2-dimensional projective space $\mathbb{P}^2$ and the notion of projective closure will be helpful. I hope to include an introduction to some of these topics in future versions of these notes.

If you find typos or other errors/omissions, please let me know by email: bourdoam@wfu.edu. Thank you to Enrique González Jiménez for feedback on an earlier draft of these notes.

Contents

Chapter 1. Galois Representations of Elliptic Curves

1.1 Introduction

An **elliptic curve** E is a smooth projective curve of genus 1 with a specified base point, $\mathcal{O}$. We may assume that E lies in $\mathbb{P}^2$ and corresponds to the equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

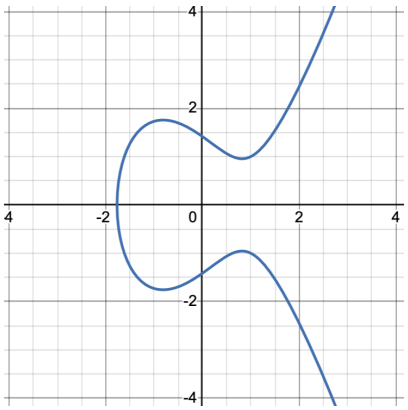
Here, $\mathcal{O} = [0 : 1 : 0]$, and this is the only point on E with $Z = 0$. If $a_i \in k$ with $\mathrm{char}(k) \neq 2, 3$, then after a change of variables the equation can be simplified to

$$Y^2 = X^3 + AXZ^2 + BZ^3.$$

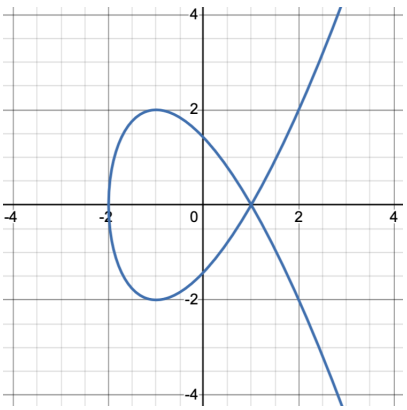
As above, if $Z = 0$, we have only the point $\mathcal{O} = [0 : 1 : 0]$. Otherwise we may scale $Z = 1$ to obtain the affine equation

$$y^2 = x^3 + Ax + B.$$

An equation of this form corresponds to a **smooth** curve if and only if $\Delta = -16(4A^3 + 27B^2) \neq 0$, and it is an elliptic curve whenever this holds. See [64, III. Prop. 1.4].



(a) The real points of the elliptic curve $y^2 = x^3 - 2x + 2$ with $\Delta = -1216$.



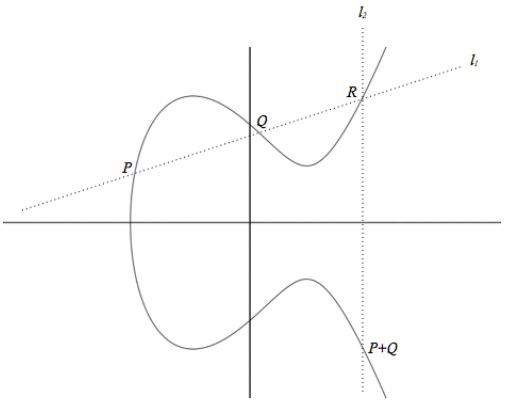
(b) The real points of $y^2 = x^3 - 3x + 2$ with $\Delta = 0$. This is *not* an elliptic curve.

Adding Points

Suppose we want to add points P and Q on an elliptic curve E. By Bézout's Theorem:

1. The line $\overleftrightarrow{PQ}$ intersects E in a third point, R.
2. The line $\overleftrightarrow{RO}$ intersects E in a third point, $P+Q$.

If $P = Q$, we take $\overleftrightarrow{PQ}$ to be the tangent line to E at P.



With this operation, the points of E form an abelian group with identity $\mathcal{O}$; see [64, III. Prop. 2.2].

1.2 Rational points of elliptic curves

Theorem 1 (Mordell [52], Weil [71])**.** *Let E be an elliptic curve over a number field k. Then $E(k)$ is a finitely generated abelian group. That is, $E(k) \cong E(k)_{tors} \times \mathbb{Z}^r$.*

Here, $E(k)_{\text{tors}}$ is a finite abelian group called the **torsion subgroup** and r is a nonnegative integer called the **rank** of E/k. In these notes, we'll be focusing on the torsion subgroup. We have the complete classification of torsion subgroups for elliptic curves over $\mathbb{Q}$.

Theorem 2 (Mazur [47])**.** *If $E/\mathbb{Q}$ is an elliptic curve, then $E(\mathbb{Q})_{tors}$ is isomorphic to one of*

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

Moreover, each occurs as the torsion subgroup for infinitely many non-isomorphic $E/\mathbb{Q}$.

In fact, there are only finitely many groups that occur as torsion subgroups for all elliptic curves defined over all number fields of a fixed degree. This is a consequence of Merel's uniform boundedness theorem:

Theorem 3 (Merel [50])**.** *For all elliptic curves E/k with k of degree d,*

$$\#E(k)_{tors} \leq B(d),$$

where $B(d)$ is some constant depending only on d.

The list of torsion subgroups is known for $d \leq 4$; see [47, 35, 38, 36, 24, 25]. For some $d > 2$, there are examples of torsion subgroups which arise for only *finitely* many isomorphism classes of elliptic curves. These correspond to **isolated** points on modular curves, which we'll discuss in Chapter 3. Our lack of understanding of isolated points is the main obstruction to extending the classification to $d > 4$. In fact, Derickx and Najman [25] ask whether there exist torsion subgroups associated to isolated points for all number fields of degree $d > 4$. As they explain, such groups are known to occur for $d = 3$ and also for each $5 \leq d \leq 13$.

1.3 The mod N Galois representation

Let E/k be the elliptic curve defined by $y^2 = x^3 + Ax + B$ and let $\mathrm{Gal}_k := \mathrm{Gal}(\overline{k}/k)$. Elements of Gal_k act naturally on the points of E. Indeed, suppose $\sigma \in \mathrm{Gal}_k$ and $P = (x_0, y_0) \in E$. Then

$$\sigma(y_0^2) = \sigma(x_0^3 + Ax_0 + B)$$
$$[\sigma(y_0)]^2 = [\sigma(x_0)]^3 + A\sigma(x_0) + B,$$

and so $\sigma(P) := (\sigma(x_0), \sigma(y_0)) \in E$. In fact this action is compatible with our group law: if $P \in E$ is of order N, then $\sigma(P) \in E$ is of order N. Any element of Gal_k acts as an automorphism of the group of N-torsion points,

$$E[N] := \{P \in E \mid N \cdot P = \mathcal{O}\} \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z},$$

where the isomorphism is [64, III. Cor. 6.4]. The **mod N Galois representation** associated to E/k is given by this action:

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

The kernel of $\rho_{E,N}$ is $\mathrm{Gal}(\overline{k}/k(E[N]))$, so we have an injection

$$\rho_{E,N} : \mathrm{Gal}(k(E[N])/k) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

In particular, $\operatorname{im} \rho_{E,N} \cong \mathrm{Gal}(k(E[N])/k)$.

Example 1. Let $E : y^2 = x^3 + 1$. Then $P_1 = (-1, 0), P_2 = \left(\frac{1+\sqrt{-3}}{2}, 0\right), P_3 = \left(\frac{1-\sqrt{-3}}{2}, 0\right)$ are the nontrivial points of $E[2]$. Note $P_1 + P_2 = P_3$, so we may take $\{P_1, P_2\}$ to be a basis for $E[2]$. If $\sigma' \in \mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$ is complex conjugation, $\sigma'(P_1) = P_1$ and $\sigma'(P_2) = P_3$. Thus

$$\rho_{E,2}(\sigma') = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

The mod N Galois representation generally has "large" image, provided E does not have **complex multiplication** (CM). Recall E/k has CM if $\mathrm{End}_{\overline{k}}(E)$ is strictly larger than $\mathbb{Z}$.[1] For example:

Theorem 4 (Serre [59])**.** *Let E/k be a non-CM elliptic curve. Then $\rho_{E,\ell}$ is surjective for all sufficiently large primes ℓ.*

It has been conjectured by both Zywina [73, Conj. 1.12] and Sutherland [67, Conj. 1.1] that for all non-CM elliptic curves over $\mathbb{Q}$, the mod ℓ Galois representation is surjective for primes $\ell > 37$; whether such a uniform constant might exist was first posed as a question by Serre [59]. This is generally referred to "Serre's Uniformity Problem" or "Serre's Uniformity Conjecture."

If $\rho_{E,\ell}$ is not surjective, its image is contained in a maximal subgroup: exceptional, Borel, or normalizer of a (split or nonsplit) Cartan subgroup. See [59, §2]. We know the specific subgroups that can occur for $\operatorname{im} \rho_{E,\ell}$, up to conjugacy, if $\ell \leq 13$; this is work of Zywina [73] for $\ell \leq 11$ and Balakrishnan, Dogra, Müller, Tuitman, and Vonk [3] for $\ell = 13$. These are listed on the next page.

[1] We follow [59] and [64] in our CM definition. Other sources distinguish between CM and *potential* CM, with the latter occurring when the "extra" automorphisms are not defined over k.

group	index	generators
2Cs	6	
2B	3	$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
2Cn	2	$\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)$
3Cs.1.1	24	$\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)$
3Cs	12	$\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)$
3B.1.1	8	$\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
3B.1.2	8	$\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
3Ns	6	$\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}0&2\\1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)$
3B	4	$\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
3Nn	3	$\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}2&1\\2&2\end{smallmatrix}\right)$
5Cs.1.1	120	$\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)$
5Cs.1.3	120	$\left(\begin{smallmatrix}3&0\\0&4\end{smallmatrix}\right)$
5Cs.4.1	60	$\left(\begin{smallmatrix}4&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)$
5Ns.2.1	30	$\left(\begin{smallmatrix}2&0\\0&3\end{smallmatrix}\right),\left(\begin{smallmatrix}0&1\\3&0\end{smallmatrix}\right)$
5Cs	30	$\left(\begin{smallmatrix}2&0\\0&3\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)$
5B.1.1	24	$\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
5B.1.2	24	$\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
5B.1.4	24	$\left(\begin{smallmatrix}4&0\\0&3\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
5B.1.3	24	$\left(\begin{smallmatrix}3&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
5Ns	15	$\left(\begin{smallmatrix}0&4\\1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}2&0\\0&3\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)$
5B.4.1	12	$\left(\begin{smallmatrix}4&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
5B.4.2	12	$\left(\begin{smallmatrix}4&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
5Nn	10	$\left(\begin{smallmatrix}1&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}2&3\\4&2\end{smallmatrix}\right)$
5B	6	$\left(\begin{smallmatrix}2&0\\0&3\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
5S4	5	$\left(\begin{smallmatrix}0&3\\3&4\end{smallmatrix}\right),\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}3&0\\4&4\end{smallmatrix}\right)$
7Ns.2.1	112	$\left(\begin{smallmatrix}2&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}0&1\\4&0\end{smallmatrix}\right)$
7Ns.3.1	56	$\left(\begin{smallmatrix}3&0\\0&5\end{smallmatrix}\right),\left(\begin{smallmatrix}0&1\\4&0\end{smallmatrix}\right)$
7B.1.1	48	$\left(\begin{smallmatrix}1&0\\0&3\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
7B.1.3	48	$\left(\begin{smallmatrix}3&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
7B.1.2	48	$\left(\begin{smallmatrix}2&0\\0&5\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
7B.1.5	48	$\left(\begin{smallmatrix}5&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
7B.1.6	48	$\left(\begin{smallmatrix}6&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
7B.1.4	48	$\left(\begin{smallmatrix}4&0\\0&6\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
7Ns	28	$\left(\begin{smallmatrix}0&6\\1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}3&0\\0&5\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&3\end{smallmatrix}\right)$
7B.6.1	24	$\left(\begin{smallmatrix}6&0\\0&6\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&3\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
7B.6.3	24	$\left(\begin{smallmatrix}6&0\\0&6\end{smallmatrix}\right),\left(\begin{smallmatrix}3&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
7B.6.2	24	$\left(\begin{smallmatrix}6&0\\0&6\end{smallmatrix}\right),\left(\begin{smallmatrix}2&0\\0&5\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
7Nn	21	$\left(\begin{smallmatrix}1&0\\0&6\end{smallmatrix}\right),\left(\begin{smallmatrix}2&5\\4&2\end{smallmatrix}\right)$
7B.2.1	16	$\left(\begin{smallmatrix}2&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&3\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
7B.2.3	16	$\left(\begin{smallmatrix}2&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}3&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
7B	8	$\left(\begin{smallmatrix}3&0\\0&5\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&3\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
11B.1.4	120	$\left(\begin{smallmatrix}4&0\\0&6\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
11B.1.6	120	$\left(\begin{smallmatrix}6&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
11B.1.5	120	$\left(\begin{smallmatrix}5&0\\0&7\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
11B.1.7	120	$\left(\begin{smallmatrix}7&0\\0&5\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
11B.10.4	60	$\left(\begin{smallmatrix}10&0\\0&10\end{smallmatrix}\right),\left(\begin{smallmatrix}4&0\\0&6\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
11B.10.5	60	$\left(\begin{smallmatrix}10&0\\0&10\end{smallmatrix}\right),\left(\begin{smallmatrix}5&0\\0&7\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
11Nn	55	$\left(\begin{smallmatrix}1&0\\0&10\end{smallmatrix}\right),\left(\begin{smallmatrix}3&5\\8&3\end{smallmatrix}\right)$
13S4	91	$\left(\begin{smallmatrix}3&0\\12&9\end{smallmatrix}\right),\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}9&5\\0&6\end{smallmatrix}\right)$
13B.3.1	56	$\left(\begin{smallmatrix}3&0\\0&9\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
13B.3.2	56	$\left(\begin{smallmatrix}3&0\\0&9\end{smallmatrix}\right),\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
13B.3.4	56	$\left(\begin{smallmatrix}3&0\\0&9\end{smallmatrix}\right),\left(\begin{smallmatrix}4&0\\0&7\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
13B.3.7	56	$\left(\begin{smallmatrix}3&0\\0&9\end{smallmatrix}\right),\left(\begin{smallmatrix}7&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
13B.5.1	42	$\left(\begin{smallmatrix}5&0\\0&8\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
13B.5.2	42	$\left(\begin{smallmatrix}5&0\\0&8\end{smallmatrix}\right),\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
13B.5.4	42	$\left(\begin{smallmatrix}5&0\\0&8\end{smallmatrix}\right),\left(\begin{smallmatrix}4&0\\0&7\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
13B.4.1	28	$\left(\begin{smallmatrix}4&0\\0&10\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
13B.4.2	28	$\left(\begin{smallmatrix}4&0\\0&10\end{smallmatrix}\right),\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
13B	14	$\left(\begin{smallmatrix}2&0\\0&7\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
17B.4.2	72	$\left(\begin{smallmatrix}4&0\\0&13\end{smallmatrix}\right),\left(\begin{smallmatrix}2&0\\0&10\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
17B.4.6	72	$\left(\begin{smallmatrix}4&0\\0&13\end{smallmatrix}\right),\left(\begin{smallmatrix}6&0\\0&9\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
37B.8.1	114	$\left(\begin{smallmatrix}8&0\\0&14\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
37B.8.2	114	$\left(\begin{smallmatrix}8&0\\0&14\end{smallmatrix}\right),\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$

Table 1: All proper subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ that occur as $\operatorname{im}\rho_{E,\ell}$ for $E/\mathbb{Q}$ with $\ell \leq 13$ and all known examples for $\ell > 13$; taken from [67, Tables 3 & 4].

The following theorem summarizes what is currently known for larger primes.

Theorem 5 (Mazur [48], Serre [60], Bilu, Parent, and Rebolledo [7], Furio, Lombardo [32]). *Suppose $E/\mathbb{Q}$ is a non-CM elliptic curve and $\ell \geq 17$ is prime. If $\operatorname{im}\rho_{E,\ell}$ is not equal to $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and not conjugate to a group in Table 1, then $\operatorname{im}\rho_{E,\ell}$ is conjugate to $C_{ns}^+(\ell)$, the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.*

1.4 Other Galois representations

Let E/k be an elliptic curve, and let ℓ be a prime number. Choose the following:

- $\{P_1, Q_1\}$: basis for $E[\ell]$
- $\{P_2, Q_2\}$: basis for $E[\ell^2]$ with $\ell P_2 = P_1$ and $\ell Q_2 = Q_1$
- $\{P_3, Q_3\}$: basis for $E[\ell^3]$ with $\ell P_3 = P_2$ and $\ell Q_3 = Q_2$
- $\{P_4, Q_4\}$: basis for $E[\ell^4]$ with $\ell P_4 = P_3$ and $\ell Q_4 = Q_3$
- etc.

Continuing in this way, we obtain a basis for the **ℓ-adic Tate module** of E,

$$T_\ell(E) \coloneqq \varprojlim E[\ell^n].$$

This is a free $\mathbb{Z}_\ell$-module of rank 2, and it comes equipped with a natural action of Gal_k. This is recorded in the **ℓ-adic Galois representation** associated to E/k,

$$\rho_{E,\ell^\infty} : \mathrm{Gal}_k \to \mathrm{Aut}(T_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Theorem 6 (Serre [59]). *Suppose E/k is non-CM. Then $\operatorname{im}\rho_{E,\ell^\infty}$ is open in $\mathrm{GL}_2(\mathbb{Z}_\ell)$.*

In other words, Theorem 6 implies $[\mathrm{GL}_2(\mathbb{Z}_\ell) : \operatorname{im}\rho_{E,\ell^\infty}]$ is finite. A useful consequence of this result is that there exists $d \in \mathbb{Z}^{\geq 0}$ such that

$$\operatorname{im}\rho_{E,\ell^\infty} = \pi^{-1}(\operatorname{im}\rho_{E,\ell^d})$$

where

$$\pi : \mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

is the natural reduction map. The smallest ℓ^d for which this holds is called the **level**.

A version of uniformity: If we fix the degree of k, there is a uniform bound on the level of the ℓ-adic Galois representation associated to all non-CM elliptic curves over k.

- Arai [2]: Proved the existence of a uniform bound depending on k.
- Cadoret/Tamagawa [18]: Proved the existence of a uniform bound depending on $[k : \mathbb{Q}]$.

Unfortunately this bound is not explicit. See [21] for a more detailed discussion.

The groups which occur as $\operatorname{im}\rho_{E,\ell^\infty}$ for non-CM elliptic curves over $\mathbb{Q}$ are known for $\ell = 2, 3$; see [58, 57, 4]. (The CM case is treated in [46].) For larger primes, we know the groups which arise infinitely often, among others. See [57] for details.

More generally, we can define the **adelic Galois representation** associated to E/k:

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

If E is non-CM, then Serre [59] proves $\operatorname{im}\rho_E$ is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ if E is non-CM. (By [61, Main Lemma, IV-19], this is roughly a consequence of Theorems 4 and 6.) Thus for non-CM elliptic curves we may define the **level** of $\operatorname{im}\rho_E$ to be the smallest integer M such that

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

where π denotes the natural reduction map. Recently, Zywina [72] has developed a efficient algorithm to compute $\operatorname{im}\rho_E$ for a non-CM elliptic curve $E/\mathbb{Q}$.

1.5 L-functions and modular forms database (LMFDB)

The L-functions and modular forms database (LMFDB) [22] contains complete information on $\rho_{E,N}$, ρ_{E,ℓ^∞}, and ρ_E for over 3.8 million elliptic curves over $\mathbb{Q}$. Check out https://www.lmfdb.org/. You can search the database for specific elliptic curves or for specific Galois images, among many other options. Note that when you are on the homepage for a particular elliptic curve, you can select the options to show commands for Magma, Oscar, PariGP, or SageMath. This provides a convenient way to explore relevant data in your program of choice.

Galois representations

The ℓ-adic Galois representation has maximal image for all primes ℓ except those listed in the table below.

prime ℓ	mod-ℓ image	ℓ-adic image
5	5Cs.1.1	5.120.0.1

The image $H := \rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ of the adelic Galois representation has level $550 = 2 \cdot 5^2 \cdot 11$, index 1200, genus 37, and generators

$$\left(\begin{smallmatrix} 1 & 0 \\ 50 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 50 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 501 & 50 \\ 500 & 51 \end{smallmatrix}\right), \left(\begin{smallmatrix} 16 & 35 \\ 115 & 11 \end{smallmatrix}\right), \left(\begin{smallmatrix} 101 & 50 \\ 204 & 277 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 50 \\ 10 & 501 \end{smallmatrix}\right), \left(\begin{smallmatrix} 381 & 50 \\ 235 & 21 \end{smallmatrix}\right).$$

Input positive integer m to see the generators of the reduction of H to $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$: [ ] submit

The torsion field $K := \mathbb{Q}(E[550])$ is a degree-19800000 Galois extension of $\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q})$ isomorphic to the projection of H to $\mathrm{GL}_2(\mathbb{Z}/550\mathbb{Z})$.

The table below list all primes ℓ for which the Serre invariants associated to the mod-ℓ Galois representation are exceptional.

ℓ	Reduction type	Serre weight	Serre conductor
5	good	2	1
11	split multiplicative	12	1

The LMFDB Galois representation data for the elliptic curve 11.a2.

Chapter 2. Modular Curves

2.1 Introduction

In Chapter 1, we saw the following theorem:

Theorem 7 (Mazur [47]). *If $E/\mathbb{Q}$ be an elliptic curve, then $E(\mathbb{Q})_{tors}$ is isomorphic to one of:*

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

Moreover, each occurs as the torsion subgroup for infinitely many non-isomorphic $E/\mathbb{Q}$.

This is proven by studying modular curves. For example, there exists an elliptic curve $E/\mathbb{Q}$ with $P \in E(\mathbb{Q})$ of order N if and only if the modular curve $X_1(N)$ has a non-cuspidal rational point. This tie to geometry gives a nice explanation for the values of N appearing in the first line of the classification: $X_1(N)$ has genus 0 if and only if $1 \leq N \leq 10$ or $N = 12$. The curve $X_1(11)$ has genus 1, but the only rational points are cusps (which do not correspond to elliptic curves).

2.2 The modular curve $X_1(N)$

Theorem 8 (Uniformization Theorem). *Let $E/\mathbb{C}$ be an elliptic curve. There exists a lattice $\Lambda \subset \mathbb{C}$ and a complex analytic isomorphism*

$$\mathbb{C}/\Lambda \to E(\mathbb{C})$$

that induces an isomorphism of abelian groups $\mathbb{C}/\Lambda \cong E(\mathbb{C})$.

Proof. See, for example, [64, VI. Cor. 5.1.1]. □

With this, we can construct $X_1(N)$ as a Riemann surface. Define

$$\mathbb{H} \coloneqq \{\tau \in \mathbb{C} : \operatorname{Im}(\tau) > 0\},$$
$$\Gamma_1(n) \coloneqq \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{n},\ a \equiv d \equiv 1 \pmod{n} \right\}.$$

The group $\Gamma_1(n)$ acts on $\mathbb{H}$ via linear fractional transformations.

$$\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : \mathbb{H} \to \mathbb{H}$$
$$\tau \mapsto \tfrac{a\tau + b}{c\tau + d}$$

The points of the Riemann surface $\mathbb{H}/\Gamma_1(n)$ correspond to $\mathbb{C}$-isomorphism classes of elliptic curves with a distinguished point of order n; see [64, Appendix C.13]. This correspondence is given by

$$\tau \in \mathbb{H}/\Gamma_1(n) \longleftrightarrow E \coloneqq \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau), P \coloneqq \frac{1}{N} \in E.$$

By adding finitely many points to $\mathbb{H}/\Gamma_1(n)$ called **cusps** we obtain a compact Riemann surface. Concretely:

$$\mathbb{H}^*/\Gamma_1(n) \text{ where } \mathbb{H}^* \coloneqq \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}).$$

Here, $\gamma \in \Gamma_1(n)$ acts on $\mathbb{P}^1(\mathbb{Q})$ by $\gamma([x:y]) = [ax+by : cx+dy]$.

Theorem 9. *There exists a smooth projective curve $X_1(N)/\mathbb{Q}$ and a complex analytic isomorphism*

$$\mathbb{H}^*/\Gamma_1(n) \to X_1(N)(\mathbb{C}).$$

Proof. See [63, §6.7]. □

If E/k is an elliptic curve and $P \in E(k)$ has order N, then $(E,P)_k$ induces a point in $X_1(N)(k)$. If $N \geq 4$, a stronger statement is true: non-cuspidal points in $X_1(N)(k)$ correspond to pairs $(E,P)_k$ where E/k is an elliptic curve and $P \in E(k)$ of order N, up to k-isomorphism. That is, $(E_1,P_1)/k$ and $(E_2,P_2)/k$ give the same point in $X_1(N)(k)$ if and only if there exists an isomorphism $\varphi : E_1 \to E_2$ defined over k with $\varphi(P_1) = P_2$. We say $X_1(N)$ is a **fine moduli space** for $N \geq 4$; this is [26, Theorem 8.2.1], which includes a streamlined exposition on the relevant objects as well as references to the proofs elsewhere in the literature.

Example 2. The curve $X_1(11)$ can be defined by $y^2 + (x^2+1)y + x = 0$. Let

$$r \coloneqq xy + 1,$$
$$s \coloneqq -x + 1.$$

Then for $(x_0, y_0) \in X_1(11)$, we can construct

$$E \coloneqq [s - rx + 1, rs - r^2 s, rs - r^2 s, 0, 0] \text{ with } P = (0,0).$$

Here, the notation $E \coloneqq [a_1, a_2, a_3, a_4, a_6]$ means E is given by the Weierstrass equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Provided E defines an elliptic curve (i.e., has nonzero discriminant), the point $P \in E$ has order 11. For example, the point $(3, -5\sqrt{22}) \in X_1(11)$ gives

$$E : y^2 + (-29 + 6\sqrt{22})xy + (816 - 174\sqrt{22})y = x^3 + (816 - 174\sqrt{22})x^2,$$

and one can check $P = (0,0)$ has order 11.[a]

[a] This particular example was taken from the master's thesis of Hailey Maxwell.

We can find defining equations for $X_1(N)/\mathbb{Q}$ using the **Kubert-Tate normal form**.

Theorem 10 (Kubert [41]). *Let E/k be an elliptic curve and $P \in E(k)$ of order $N \geq 4$. Then E has an equation of the form*

$$y^2 + (1-c)xy - by = x^3 - bx^2$$

for some $b, b \in k$ and $P = (0,0)$.

For E in this form and $P = (0,0)$, we see

$$NP = \mathcal{O} \iff x(\lceil \tfrac{N+1}{2} \rceil P) = x(\lfloor \tfrac{N-1}{2} \rfloor P).$$

This follows from the fact that if $m + n = N$, then $mP = -nP$. If $m \neq n$, this implies $x(mP) = x(nP)$. This equality gives $f_N(b,c) \in \mathbb{Q}[b,c]$, and a defining equation for $X_1(N)$ appears as an irreducible factor. Sutherland has computed optimized equations for $X_1(N)$ for $N \leq 100$; these are available at https://math.mit.edu/~drew/X1_optcurves.html.

Example 3. We will illustrate how to find an equation for $X_1(6)$. Suppose E is an elliptic curve given by $y^2 + (1-c)xy - by = x^3 - bx^2$ and $P = (0,0)$ on E. The discriminant of E is

$$b^3(16b^2 - 8bc^2 - 20bc + b + c(c-1)^3),$$

so E nonsingular implies $b \neq 0$. Recall $6P = \mathcal{O}$ if and only if $x(4P) = x(2P)$. Thus

$$f_6(b,c) = x(2P) - x(4P) = b - \frac{b(b-c)}{c^2},$$

where the latter equality comes from applying the group law to P. The point $(0,0)$ never has order less than 4, so P has order 6 if and only if $f_6(b,c) = 0$. We may remove the factor of b since $b \neq 0$. Clearing denominators then shows $X_1(6)$ can be defined by

$$c^2 - (b-c) = 0.$$

This is referred to as the "raw form" for $X_1(6)$. An *optimized equation* would define a birationally equivalent curve, but with a goal of minimizing the degree of the variables, the number of terms, and the size of the coefficients. See work of Sutherland [66] for details.

2.3 Degrees of points on $X_1(N)$

Consider $E : y^2 = x^3 - 43x - 166$ with $P = (5, 16\sqrt{-1}) \in E(\overline{\mathbb{Q}})$ of order 7. Then (E, P) gives a point on $X_1(7)$. What is its degree? Most people would guess 2. However, the Kubert-Tate normal form of E is

$$y^2 - xy - 4y = x^3 - 4x^2,$$

and P corresponds to $(0,0)$. In particular, both the Kubert-Tate normal form and $(0,0)$ are defined over $\mathbb{Q}$. Since the defining equation for $X_1(7)$ can be obtained from the general Kubert-Tate normal form, should the degree be 1?

Really, the curve $X \coloneqq X_1(N)$ is a scheme over $\mathbb{Q}$. The point $x \in X$ is **closed** if it is a scheme-theoretic point whose Zariski closure is itself, and we define the **degree** of x to be the degree of its residue field, $\mathbb{Q}(x)$. The closed points on X are precisely the points with $[\mathbb{Q}(x) : \mathbb{Q}]$ finite [55,

Proposition 2.4.3], so it really only makes sense to talk about the degree of closed points. Closed points can be identified with $\mathrm{Gal}_{\mathbb{Q}}$-orbits of points in $X(\overline{\mathbb{Q}})$, and the degree is the size of this Galois orbit. See [55, Proposition 2.4.6].

Example 4. Let $C : x^2 + y^2 = 6$, viewed as a curve over $\mathbb{Q}$. Then

$$\{(1+\sqrt{2}, 1-\sqrt{2}), (1-\sqrt{2}, 1+\sqrt{2})\}$$

corresponds to a closed point on Spec $\mathbb{Q}[x,y]/(x^2+y^2-6)$ of degree 2.

When we say the **degree of the point associated to** (E,P) in $X_1(N)$, we always mean the degree of residue field of the associated closed point. We will denote the closed point by $[E,P]$. Returning to the example $E : y^2 = x^3 - 43x - 166$ with $P = (5, 16\sqrt{-1}) \in E$ of order 7, we have $(E,P) \in X_1(7)(\overline{\mathbb{Q}})$ by the moduli interpretation. An element of $\mathrm{Gal}_{\mathbb{Q}}$ could sent (E,P) to $(E,-P)$, but these correspond to the *same* point on $X_1(7)(\overline{\mathbb{Q}})$ since $-1 \in \mathrm{Aut}(E)$ gives the necessary isomorphism. Thus the $\mathrm{Gal}_{\mathbb{Q}}$-orbit has length 1, and $[E,P] \in X_1(7)$ has degree 1.

A remark on k-valued points of a scheme. It is true that $E : y^2 = x^3 - 43x - 166$ with the point $P = (5, 16\sqrt{-1}) \in E$ induces a $\mathbb{Q}(\sqrt{-1})$-valued point on $X_1(7)$, i.e., a point in $X_1(7)(\mathbb{Q}(\sqrt{-1}))$. But in general k-valued points of a scheme X over $\mathbb{Q}$ correspond to morphisms of $\mathbb{Q}$-schemes,

$$f : \mathrm{Spec}\ k \to X.$$

Spec k consists of a single point, and its image in X is the associated closed point. See [44, §3.2.3] for details.

Luckily, we have a concrete way of describing the residue field of closed points on $X_1(N)$. Recall that given any elliptic curve E/k, there exists $E'/\mathbb{Q}(j(E))$ with $j(E') = j(E)$; see [64, Prop. III. 1.4]. Since E is isomorphic to E' over $\overline{\mathbb{Q}}$ by [64, Prop. III. 1.4] and closed points are $\mathrm{Gal}_{\mathbb{Q}}$-orbits of points in $X_1(N)(\overline{\mathbb{Q}})$, it suffices to describe the residue field for elliptic curves defined over $\mathbb{Q}(j(E))$.

Proposition 11. *Let $E/\mathbb{Q}(j(E))$ be a non-CM elliptic curve, and let $P = (x_0, y_0) \in E$ be a point of order N. Then the residue field of the closed point $[E,P] \in X_1(N)$ is*

$$\mathbb{Q}(x) \cong \mathbb{Q}(j(E), x_0).$$

Proof. See, for example, [14, Lemma 2.5]. □

So if $E/\mathbb{Q}$ is non-CM with $P = (x_0, y_0)$ of order N, we can compute the degree of $[E,P] \in X_1(N)$ by determining $[\mathbb{Q}(x_0) : \mathbb{Q}]$. This can be obtained by factoring **n-division polynomials**; see [64, Exercise III.3.6].

Facts: Let $x = [E,P] \in X_1(N)$ be a closed point.

1. If $(E',P') \in X_1(N)(k)$ induces the same closed point x, then there exists a $\mathbb{Q}$-algebra homomorphism $\mathbb{Q}(x) \to k$. See [44, §3.2.3].

2. There exists $E_0/\mathbb{Q}(x)$ with $P_0 \in E_0(\mathbb{Q}(x))$ such that $\varphi : E \to E_0$ is an isomorphism sending P to P_0. Roughly, given
$$\sigma \in \mathrm{Gal}_{\mathbb{Q}(x_0)},$$
we have $\sigma(P) = \zeta P$ for some $\zeta \in \mathrm{Aut}(E) = \{\pm 1\}$. This defines a quadratic character χ, and we can take E_0 to be the twist $E^{\chi^{-1}}$.

2.4 The modular curve $X_0(N)$

Let E be an elliptic curve over a number field k and let $C \subset E(\overline{\mathbb{Q}})$ be a subgroup. Then C uniquely defines an **isogeny** to another elliptic curve, which is a map locally defined by polynomials that's also a group homomorphism.[1] Precisely, there exists an isogeny $\varphi : E \to E'$ to another elliptic curve E' with $\ker(\varphi) = C$; see [64, Prop. III.4.12]. We say C is **k-rational** if it is Gal_k-invariant, meaning $\sigma(P) \in C$ for all $P \in C$ and $\sigma \in \mathrm{Gal}_k$. The map φ is defined over k if and only if C is k-rational [64, Remark 4.13.2].

The smooth projective curve $X_0(N)/\mathbb{Q}$ has non-cuspidal points which parameterize pairs (E, C) where E is an elliptic curve and $C \subset E$ is cyclic of order N. Define
$$\Gamma_0(n) \coloneqq \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{n} \right\}.$$
Then $X_0(N)(\overline{\mathbb{C}})$ corresponds to $\mathbb{H}^*/\Gamma_0(N)$, and
$$\tau \in \mathbb{H}/\Gamma_0(n) \longleftrightarrow E \coloneqq \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau), C \coloneqq \left\langle \frac{1}{N} \right\rangle \in E.$$
See [63, §6.7] for details. If E/k is an elliptic curve and $C \subset E$ is k-rational, then (E, P) gives a point on $X_0(N)(k)$. However, $X_0(N)$ is *not* a fine moduli space: $(E_1, C_1)_k$ and $(E_2, C_2)_k$ may give the same k-rational point without being isomorphic over k (though they will be isomorphic over $\overline{k}$); see [26, §8.1] for additional discussion on this.

Proposition 12. *Let $E/\mathbb{Q}(j(E))$ be a non-CM elliptic curve, and let $C \subset E$ be cyclic of order N. Then the residue field of the closed point $[E, C] \in X_1(N)$ is*
$$\mathbb{Q}(x) \cong \mathbb{Q}(j(E), C).$$

Proof. This is implied by results in [19, §3.3], along with standard results on isogenies [64, Prop. III.4.12 & Remark 4.13.2]. □

2.5 L-functions and modular forms database (LMFDB)

The beta version of the LMFDB [22] has a database of modular curves; see https://beta.lmfdb.org. It contains over 16 million modular curves, including many of the form $X_0(N)$ and $X_1(N)$.

[1] Some authors require isogenies to be nonconstant, but we will follow [64] in allowing the zero isogeny.

Modular curve $X_1(21)$

The modular curve $X_1(21)$ has a sporadic degree 3 point, the lowest possible degree of a sporadic point on a modular curve $X_1(N)$, as found by Najman [10.4310/MRL.2016.v23.n1.a12, MR:3512885, arXiv:1211.2188].

Invariants

Level:	21	SL_2-level:	21	Newform level:	21
Index:	384	PSL_2-index:	192		
Genus:	$5 = 1 + \frac{192}{12} - \frac{0}{4} - \frac{0}{3} - \frac{24}{2}$				
Cusps:	24 (of which 6 are rational)	Cusp widths	$1^6 \cdot 3^6 \cdot 7^6 \cdot 21^6$	Cusp orbits	$1^6 \cdot 2^3 \cdot 6^2$
Elliptic points:	0 of order 2 and 0 of order 3				
Analytic rank:	0				
$\mathbb{Q}$-gonality:	4				
$\overline{\mathbb{Q}}$-gonality:	4				
Rational cusps:	6				
Rational CM points:	none				

Models

Canonical model in $\mathbb{P}^4$ defined by 3 equations

$$\begin{aligned} 0 &= x^2 - xw + xt - yw + yt \\ &= xz + yz + yw - yt + z^2 - wt \\ &= xw + yt + zw + zt + wt \end{aligned}$$

Singular plane model

$$0 = x^5y + 3x^4y^2 + x^4z^2 + 3x^3y^3 - x^3y^2z + 2x^3yz^2 + \cdots - y^3z^3$$

Rational points

This modular curve has 6 rational cusps but no known non-cuspidal rational points. The following are the coordinates of the rational cusps on this modular curve.

Canonical model
$(0:-1:1:0:0)$, $(0:1:0:0:0)$, $(0:0:0:0:1)$, $(0:0:0:1:0)$, $(-1:0:0:0:1)$, $(1:0:-1:1:0)$

Some LMFDB data for the modular curve $X_1(21)$.

Chapter 3. Isolated Points

3.1 Isolated and parameterized points

Let k be a number field, and let C/k be a nice curve (i.e., smooth, projective, and geometrically integral).[1] We say a closed point $x \in C$ has **degree** d if its residue field, $k(x)$, is a degree d extension of k. If we identify x with a Gal_k-orbit of points in $C(\overline{k})$, then the degree of x is the size of this Galois orbit [55, Proposition 2.4.6]. Closed points of degree 1 correspond to points in $C(k)$.

Question: When does C/k have infinitely many degree 1 closed points?

- Genus$(C) = 0$: If $C(k) \neq \emptyset$, then $C \cong \mathbb{P}^1_k$ and $C(k)$ is infinite.
- Genus$(C) = 1$: If $C(k) \neq \emptyset$, then C is an elliptic curve and $C(k)$ is a finitely generated abelian group by the Mordell-Weil Theorem [52, 71].
- Genus$(C) \geq 2$: The set $C(k)$ is finite by Faltings' Theorem [29].

Question: When does C/k have infinitely many degree d closed points?

- We will show there exist infinitely many closed points of degree d if and only if there exists an infinitely family of degree d points parameterized by $\mathbb{P}^1$ or a positive rank abelian subvariety of the Jacobian of C.

What to know about Jac(C)

Let C/k be a curve of genus g with $C(k) \neq \emptyset$. There exists an abelian variety $\mathrm{Jac}(C)$ of dimension g called the **Jacobian** of C that has the following key property: $\mathrm{Jac}(C)(k)$ is in bijection with $\mathrm{Pic}^0(C)$; see [51]. Recall $\mathrm{Pic}^0(C)$ consists of the degree 0 elements of

$$\mathrm{Pic}(C) = \mathrm{Div}(C)/\{\text{principal divisors}\}.$$

There are several ways to define maps from C to $\mathrm{Jac}(C)$. A common one in the study of degree d points is actually from the d-th symmetric power of C, denoted $C^{(d)}$, which is the quotient of the cartesian product C^d by the natural action of the symmetric group S_d. Points of $C^{(d)}$ correspond

[1] If you'd like, you can take $C = X_1(N)$ or $X_0(N)$ and $k = \mathbb{Q}$.

to effective divisors of degree d. For simplicity, assume there exists $P_0 \in C(k)$. Then we define

$$\begin{aligned} \Phi_d : C^{(d)} &\to \mathrm{Jac}(C) \\ D &\mapsto [D - dP_0]. \end{aligned}$$

This map is useful because a degree d point x will give a k-rational point on $C^{(d)}$, and hence $\Phi_d(x) \in \mathrm{Jac}(C)(k)$.

Suppose C has infinitely many closed points of degree d. Then we are in one of two cases:

Case 1: There exists distinct x, y of degree d such that $\Phi_d(x) = \Phi_d(y)$. Since x and y have distinct support, this implies there exists $f \in k(C)^\times$ such that $\mathrm{div}(f) = x - y$. Then $f : C \to \mathbb{P}^1$ is a dominant morphism of degree d, and $f^{-1}(\mathbb{P}^1(k))$ contains infinitely many degree d points by Hilbert's irreducibility theorem [62, Ch.9]. This gives an infinite family of degree d points "parameterized by $\mathbb{P}^1$."

Case 2: The map Φ_d is injective on the set of degree d points. By Faltings' Theorem [30], there exist a finite number of k-rational points $x_i \in \mathrm{im}\,\Phi_d$ such that

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

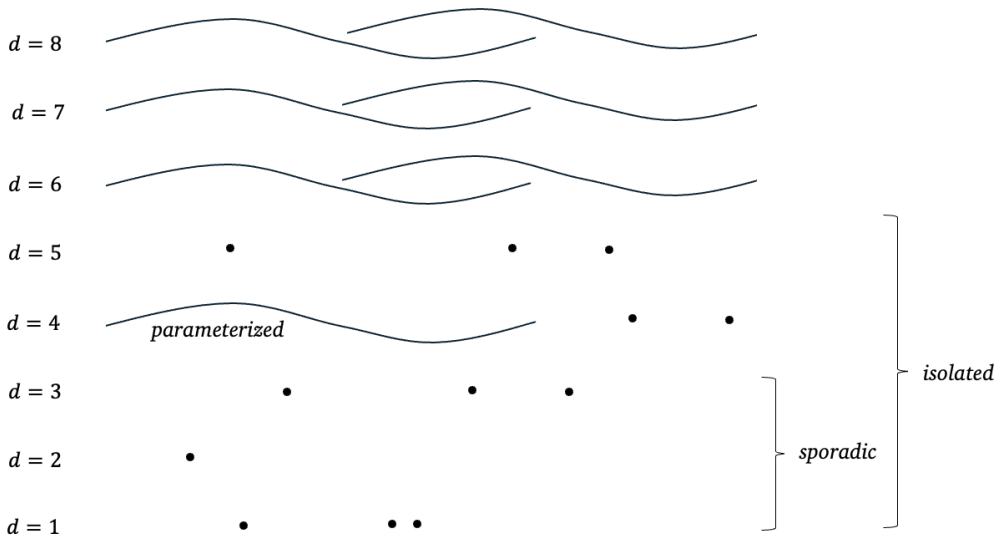
where $A_i \subset \mathrm{Jac}(C)$ are abelian subvarieties. Thus one of the A_i has positive rank, and this gives an infinite family of degree d points "parameterized by A_i."

This inspires the following definitions. Here, C denotes a curve defined over a number field k and $x \in C$ is a closed point of degree d.

1. The point x is **$\mathbb{P}^1$-parameterized** if there exists $x' \in C^{(d)}(k)$ with $x' \neq x$ such that $\Phi_d(x) = \Phi_d(x')$. Otherwise, we say x is **$\mathbb{P}^1$-isolated**.
2. The point x is **AV-parameterized** 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**.
3. The point $x \in C$ is **isolated** if it is both $\mathbb{P}^1$-isolated and AV-isolated.

Example 5. The modular curve $X_0(48)$ can be defined by the equation $y^2 = x^8 + 14x^4 + 1$. We can define a map $f : X_0(48) \to \mathbb{P}^1$ which sends $(x, y) \mapsto x$. For any $x \in \mathbb{Q}$, we obtain a point on $X_0(48)$ of degree at most 2. This gives a $\mathbb{P}^1$-parameterized family of degree 2 points. However, there are other *isolated* points of degree 2 which are not explained by this map: $(\pm\sqrt{-1}, 4), (\pm\sqrt{-1}, -4)$. This is the complete set of isolated points of degree 2 by Bruin and Najman [17].

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



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

Example 6. If $n \geq 7$, the Fermat curves

$$F_n : X^n + Y^n = Z^n$$

viewed as curves over $\mathbb{Q}$ have only finitely many points of degree $\leq n-2$ by work of Debarre and Klassen [23], and thus any point of degree $\leq n-2$ is sporadic (and hence isolated).

For any closed point $x \in C$ of degree d with $d > g := \text{genus}(C)$, the Riemann-Roch space associated x has dimension at least 2 and the point is $\mathbb{P}^1$-parameterized; see, for example, [12, Lemma 14]. Thus any isolated point on C has degree at most g. We can then use Faltings' Theorem [30] to obtain the following result:

Theorem 13 (B./Ejder/Liu/Odumodu/Viray [11])**.** *The curve C/k has only finitely many isolated points of any degree.*

If C/k has $\text{genus}(C) \geq 2$, we have

$$\{C(k)\} \subset \{\text{sporadic points of } C\} \subset \{\text{isolated points of } C\},$$

and all sets are finite. Thus one can view the study of isolated points as a natural generalization of the study of rational points.

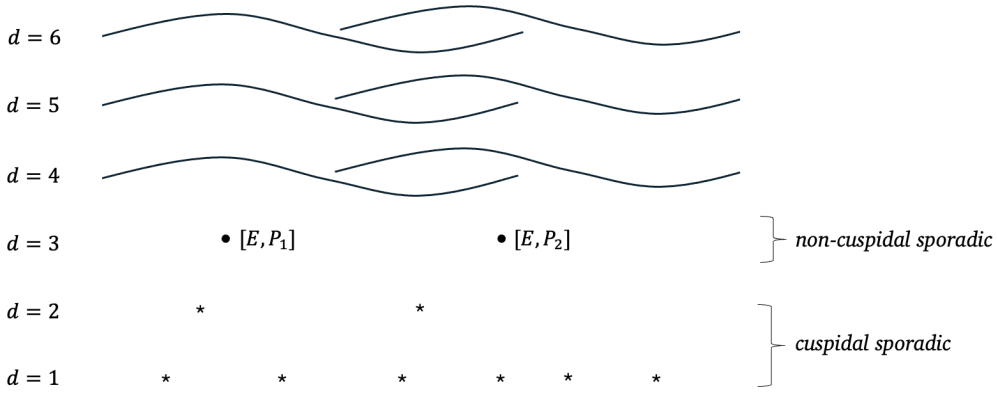
Question: (Viray, Vogt [70]) Is the number of isolated points on C/k bounded by a constant depending only on the genus of C?

See [70, §6] for a discussion and partial progress (and much more on isolated points!).

3.2 Isolated points on modular curves

Our failure to understand isolated points on modular curves is the essential obstruction to extending the classification of torsion subgroups of elliptic curves beyond number fields of degree 4; see Section 3.4 for further discussion other other applications. This motivates the need for a more systematic study of isolated points on modular curves. Here, we will focus on the modular curve $X_1(N)$, but see for example [49, 68] for analogous work on isolated points on more general classes of modular curves. We say $j \in X_1(1) \cong \mathbb{P}^1_j$ is **isolated** if it is the image of an isolated point on $X_1(N)$ for some $n \in \mathbb{Z}^+$ under the natural map $j : X_1(N) \to X_1(1)$ sending $[E, P] \mapsto j(E)$.

> **Warning:** We are *not* saying j is an isolated point of the curve $\mathbb{P}^1_j$ — this curve itself has no isolated points — but only that it is the j-invariant of an elliptic curve giving rise to an isolated point $x \in X_1(N)$ for some $n \in \mathbb{Z}^+$.



Degree d points on $X_1(21)/\mathbb{Q}$. Here, $j(E) = -140625/8$ is an isolated j-invariant.

Known isolated j-invariants in $\mathbb{Q}$:

- $-140625/8$: Comes from two sporadic points of degree 3 on $X_1(21)$; see Najman [53].
- -9317: Comes from three sporadic points of degree 6 on $X_1(37)$; see van Hoeij [69].
- $351/4$: Comes from a degree 9 isolated point on $X_1(28)$; see [12, Theorem 2].
- -162677523113838677: Comes from a degree 18 isolated point on $X_1(37)$; see [13, Appendix].
- Any of the 13 CM j-invariants in $\mathbb{Q}$; see [11, Theorem 7.1].

Question: How many isolated j-invariants exist in $\mathbb{Q}$? It's conjectured to be a finite set!

Theorem 14 (B., Ejder, Liu, Odumodu, Viray [11])**.** *Suppose Serre's Uniformity Conjecture holds. Then there are only finitely many isolated j-invariants in $\mathbb{Q}$. More precisely, if $\mathcal{I}$ is the set of all isolated points on $X_1(N)$ for all $N \in \mathbb{Z}^+$, then $j(\mathcal{I}) \cap \mathbb{Q}$ is finite.*

This is saying that, up to $\overline{\mathbb{Q}}$-isomorphism, there are only finitely many elliptic curves E with $j(E) \in \mathbb{Q}$ that give rise to an isolated point of any degree on $X_1(N)$, even as N ranges over all positive integers. The list of 17 j-invariants given above has been conjectured to be complete in [13], where they show these are the only isolated j-invariants among all elliptic curves in the LMFDB [22] or the Stein-Watkins Database [65]. Together, these databases contain over 36 million distinct non-CM j-invariants in $\mathbb{Q}$. See also [13, Remark 5] for further motivation for this conjecture.

Progress: We have finiteness of isolated j-invariants in $\mathbb{Q}$ in the following cases:

- Isolated points of odd degree: In [12], the authors show the only non-CM j-invariants in $\mathbb{Q}$ which correspond to isolated points $x \in X_1(N)$ of odd degree are $-140625/8$ and $351/4$.
- Curves of the form $X_1(\ell^n)$ for prime ℓ: This is [27] and [15].
- Restrictions on the mod ℓ image: Serre's Uniformity Conjecture holds for the class of non-CM elliptic curves $E/\mathbb{Q}$ admitting a rational cyclic isogeny or with $\operatorname{im} \rho_{E,\ell}$ contained in the normalizer of a split Cartan subgroup [42, 43]. Thus finiteness follows from [11].

Question: Can we extend the list of unconditional results?

3.3 Proof sketch of Theorem 14

Suppose $x \in X_1(n)$ is isolated with $j(x) \in \mathbb{Q}$. Since there are only 13 CM j-invariants in $\mathbb{Q}$, we may assume $j(x)$ is non-CM. Fix $E/\mathbb{Q}$ with $j(E) = j(x)$ and let

$$n = \prod_{\ell_i \leq 37} \ell_i^{a_i} \cdot \prod_{\ell_j > 37} \ell_j^{a_j} = n_1 \cdot n_2.$$

Suppose Serre's Uniformity Conjecture holds. That is, suppose that for all $\ell_j > 37$ we have $\operatorname{im} \rho_{E,\ell_j} = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Then:

1. Let $f : X_1(n) \to X_1(n_1)$ be the natural map sending $[E, P] \mapsto [E, n_2 P]$. Then $\deg(x) = \deg(f) \cdot \deg(f(x))$ by [11, Proposition 5.7].
2. By [11, Theorem 4.3], it follows that $f(x) \in X_1(n_1)$ is isolated.
3. Let $m := \prod_{\ell \leq 37} \ell$. Then by [11, Proposition 6.1] there exists $M \in \mathbb{Z}^+$ such that for all non-CM elliptic curves $E/\mathbb{Q}$, we have
$$\operatorname{im} \rho_{E,m^\infty} = \pi^{-1}(\operatorname{im} \rho_{E,M}),$$
where $\pi : \mathrm{GL}_2(\mathbb{Z}_m) \to \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ denotes the natural reduction map.
4. Let $g : X_1(n_1) \to X_1(\gcd(n_1, M))$ be the natural map. Applying [11, Corollary 5.3], we have that $g(f(x)) \in X_1(\gcd(n_1, M))$ is isolated.
5. Since M does not depend on $j(x) \in \mathbb{Q}$, we see that all isolated points in $\cup_{n=1}^{\infty} X_1(n)$ associated to elliptic curves with rational j-invariant map (under natural projection) to isolated points on a *finite number* of modular curves. Namely, those of the form $X_1(d)$ for $d \mid M$. Since any one of these curves has only finitely many isolated points [11, Theorem 4.2], there are only finitely many isolated j-invariants in $\mathbb{Q}$.

See [11] for additional details.

3.4 Connection with other open problems

Here we discuss how isolated points on modular curves relate to other open problems in the field.

3.4.1 Classifying torsion subgroups

As we saw in Chapter 1, the list of groups that occur as $E(k)_{\text{tors}}$ for all elliptic curves E defined over all number fields k of degree d is known for $d \leq 4$; see [47, 35, 38, 36, 24, 25]. A key obstruction to extending this classification for $d > 4$ is our lack of understanding of isolated points on $X_1(N)$. For example, in the $d = 3$ classification, there is *exactly one* elliptic curve over a cubic field with a 21-torsion point; see [24, Theorem A]. This corresponds to the degree 3 sporadic points on $X_1(21)$ mentioned above. In fact, Derickx and Najman [25] ask whether there is a degree d sporadic point on $X_1(N)$ for all $d > 4$. Such points are known to occur for $5 \leq d \leq 13$, as a consequence of van Hoeij's results [69].

3.4.2 Serre Uniformity

As we've mentioned, the following is a conjecture of Zywina [73, Conj. 1.12] and Sutherland [67, Conj. 1.1], but it was originally a question of Serre [59].

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

Though this is a uniformity question about non-CM rational points on a more general family of modular curves, we will show this conjecture can be reframed as one about isolated points on $X_1(N)$, following [14, §3].

1. Suppose $E/\mathbb{Q}$ with $\operatorname{im}\rho_{E,\ell} = C_{ns}^{+}(\ell)$, the normalizer of a nonsplit Cartan subgroup. As we saw in Chapter 1, showing this does not occur for any prime $\ell > 37$ would prove Serre's Uniformity Conjecture.

2. There exists an extension $F/\mathbb{Q}$ of degree $\ell + 1$ for which $\rho_{E,\ell}(\mathrm{Gal}_F)$ consists of diagonal matrices. That is, the curve E/F has two independent F-rational cyclic ℓ-isogenies.

$$E_1 \xleftarrow{\varphi_1} E \xrightarrow{\varphi_2} E_2.$$

3. The curve E_1/F has an F-rational cyclic ℓ^2-isogeny: $\varphi_2 \circ \hat{\varphi}_1$, where $\hat{\varphi}_1$ denotes the dual isogeny [64, §III.6].

4. A twist of E_1 gives a point on $X_1(\ell^2)$ of degree at most $\frac{\ell(\ell^2-1)}{2}$; see, for example, [10, Theorem 5.5]. This will be sporadic for ℓ sufficiently large. Indeed,

$$\frac{\ell(\ell^2-1)}{2} < \frac{1}{2}\mathrm{gon}_{\mathbb{Q}}X_1(\ell^2)$$

for sufficiently large primes using gonality bounds of Abramovich [1]. Here, $\mathrm{gon}_{\mathbb{Q}}X_1(\ell^2)$ denotes the **$\mathbb{Q}$-gonality** of $X_1(\ell^2)$, which is the least degree of a nonconstant rational map $f : X_1(\ell^2) \to \mathbb{P}^1$. Such a point is sporadic by work of Frey [31].

In this argument, E_1 is a **$\mathbb{Q}$-curve**, which means it is isogenous (over $\overline{\mathbb{Q}}$) to its Galois conjugates.[2] Thus we obtain the following result.

Theorem 15 (B./Najman [14])**.** *Suppose there are only finitely many isolated j-invariants associated to non-CM $\mathbb{Q}$-curves. Then Serre's Uniformity Conjecture holds.*

We've seen in Theorem 14 that Serre's Uniformity Conjecture implies the set of isolated j-invariants in $\mathbb{Q}$ is finite. Theorem 15 provides a kind of converse, provided we expand the class of j-invariants under consideration.

3.4.3 Uniformity of degree d points on $X_0(N)$

Recall Merel [50] showed that for all elliptic curves E/k with $[k:\mathbb{Q}] = d$, we have

$$\#E(k)_{\text{tors}} \leq C(d),$$

where $C(d)$ is a constant depending only on d. This means that for N sufficiently large, $X_1(N)$ has no non-cuspidal degree d points.

Question: Can we obtain an analogous result for $X_0(N)$?

For $d = 1$, the answer is yes: $X_0(N)$ has no non-cuspidal rational points for $n > 163$.

Theorem 16 (Mazur [48], Kenku [37], and others; see Section 9 of [45])**.** *If $E/\mathbb{Q}$ is an elliptic curve possessing a $\mathbb{Q}$-rational cyclic subgroup of order N, then $N \leq 19$ or $N \in \{21, 25, 27, 37, 43, 67, 163\}$.*

However, we run into problems when trying to extend our classification to $d = 2$. For example, suppose E is a CM elliptic curve with geometric endomorphism ring isomorphic to the full ring of integers in K, an imaginary quadratic field of class number 1. Then for any prime ℓ which is split in K and any $n \in \mathbb{Z}^+$, we have a degree 2 point $x \in X_1(\ell^n)$ with $j(x) = j(E)$. This is a consequence of classical CM theory; see, for example [8]. In particular, there is *no* upper bound on the size of a k-rational cyclic subgroup as we range over all quadratic fields. That such a bound might exist if we omit these CM points is a recent conjecture of Balakrishnan and Mazur.

Conjecture (Balakrishnan, Mazur [5])**.** *For N sufficiently large, there are no quadratic points on $X_0(N)$ corresponding to non-CM elliptic curves.*

For $N > 131$, any quadratic point is sporadic by work of Harris and Silverman [34], Ogg [54], and Bars [6]. So this is a conjecture which seeks to control non-CM sporadic points on $X_0(N)$. Some sporadic quadratic points on $X_0(\ell)$ arise from unexpected rational points on $X_0^+(\ell)$, which is the quotient of $X_0(\ell)$ by the Atkin-Lehner involution sending an isogeny $\varphi : E \to E'$ of degree ℓ to its dual $\widehat{\varphi} : E' \to E$. Elkies [28] had conjectured that unexpected (i.e., non-cuspidal, non-CM) rational points on $X_0^+(\ell)$ could arise only in the case where $X_0^+(\ell)$ is hyperelliptic. In this case, the hyperelliptic involution can send rational cusps or rational CM points to new unexpected points. (This type of construction explains the unexpected rational points on $X_0(37)$, for example. See [16, §5] for more details.) However, the conjecture of Elkies was disproven by Galbraith [33], who found exceptional rational points on $X_0^+(137)$ and $X_0^+(311)$.

Question: Why do these exceptional rational points on $X_0^+(137)$ and $X_0^+(311)$ exist?

[2] Example of $\mathbb{Q}$-curves include CM elliptic curves, elliptic curves E with $j(E) \in \mathbb{Q}$, and elliptic curves isogenous to E with $j(E) \in \mathbb{Q}$. These are precisely the elliptic curves over number fields that are modular [56, 39, 40].

3.4.4 Existence of sporadic points

There are several additional lines of investigation which focus on the existence of certain sporadic points. For example, in [25, Appendix A], we find a kind of compliment to the conjecture of Balakrishnan and Mazur discussed in Section 3.4.3.

Conjecture (Derickx, Najman [25])**.** *For every positive integer d there exists an n such that there exists a sporadic point of degree d on $X_0(N)$.*

Other lines of inquiry focus on CM sporadic points. In [20, Theorem 8.2], Clark, Genao, Pollack, and Saia show that for $N \geq 721$, the modular curves $X_0(N)$ and $X_1(N)$ have sporadic points associated to CM elliptic curves. However, there are 106 values of N for which it is unknown whether $X_0(N)$ has a sporadic CM point, and there are 67 values of N for which is unknown whether $X_1(N)$ has a sporadic CM point. See [20, Tables 3 & 4]. In each case, complete information about the degree d and the residue field is known (see [9, 20, 19]).

Question: Can one determine whether there exist sporadic CM points on $X_0(N)$ or $X_1(N)$ for the remaining values of N?

Bibliography

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

[2] Keisuke Arai, *On uniform lower bound of the Galois images associated to elliptic curves*, J. Théor. Nombres Bordeaux **20** (2008), no. 1, 23–43. MR 2434156

[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

[4] Jennifer S. Balakrishnan, L. Alexander Betts, Daniel Raynor Hast, Aashraya Jha, and J. Steffen Müller, *Rational points on the non-split cartan modular curve of level 27 and quadratic chabauty over number fields*, preprint, available at arxiv.org:2501.07833.

[5] Jennifer S. Balakrishnan and Barry Mazur, *Ogg's torsion conjecture: Fifty years later*, 2024.

[6] Francesc Bars, *Bielliptic modular curves*, J. Number Theory **76** (1999), no. 1, 154–165. MR 1688168

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

[8] Abbey Bourdon and Pete L. Clark, *Torsion points and Galois representations on CM elliptic curves*, Pacific J. Math. **305** (2020), no. 1, 43–88.

[9] ———, *Torsion points and isogenies on CM elliptic curves*, J. Lond. Math. Soc. (2) **102** (2020), no. 2, 580–622.

[10] Abbey Bourdon, Pete L. Clark, and James Stankewicz, *Torsion points on CM elliptic curves over real number fields*, Trans. Amer. Math. Soc. **369** (2017), no. 12, 8457–8496. MR 3710632

[11] Abbey Bourdon, Özlem Ejder, Yuan Liu, Frances Odumodu, and Bianca Viray, *On the level of modular curves that give rise to isolated j-invariants*, Adv. Math. **357** (2019), 106824, 33.

[12] Abbey Bourdon, David R. Gill, Jeremy Rouse, and Lori D. Watson, *Odd degree isolated points on $X_1(N)$ with rational j-invariant*, Res. Number Theory **10** (2024), no. 1, Paper No. 5, 32. MR 4678892

[13] Abbey Bourdon, Sachi Hashimoto, Timo Keller, Zev Klagsbrun, David Lowry-Duda, Travis Morrison, Filip Najman, and Himanshu Shukla, *Towards a classification of isolated j-invariants*, Math. Comp. **94** (2025), no. 351, 447–473, With an appendix by Maarten Derickx and Mark van Hoeij. MR 4807817

[14] 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.

[15] Abbey Bourdon and Özlem Edjer, *Rational isolated j-invariants from $X_1(\ell^n)$ and $X_0(\ell^n)$*, in progress.

[16] Josha Box, *Quadratic points on modular curves with infinite Mordell-Weil group*, Math. Comp. **90** (2021), no. 327, 321–343. MR 4166463

[17] Peter Bruin and Filip Najman, *Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields*, LMS J. Comput. Math. **18** (2015), no. 1, 578–602. MR 3389884

[18] Anna Cadoret and Akio Tamagawa, *A uniform open image theorem for ℓ-adic representations, II*, Duke Math. J. **162** (2013), no. 12, 2301–2344. MR 3102481

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

[20] Pete L. Clark, Tyler Genao, Paul Pollack, and Frederick Saia, *The least degree of a CM point on a modular curve*, J. Lond. Math. Soc. (2) **105** (2022), no. 2, 825–883. MR 4400938

[21] Pete L. Clark and Paul Pollack, *Pursuing polynomial bounds on torsion*, Israel J. Math. **227** (2018), no. 2, 889–909.

[22] The LMFDB Collaboration, *The L-functions and modular forms database, (2023)*, Available at lmfdb.org.

[23] Olivier Debarre and Matthew J. Klassen, *Points of low degree on smooth plane curves*, J. Reine Angew. Math. **446** (1994), 81–87.

[24] Maarten Derickx, Anastassia Etropolski, Mark van Hoeij, Jackson S. Morrow, and David Zureick-Brown, *Sporadic cubic torsion*, Algebra Number Theory **15** (2021), no. 7, 1837–1864. MR 4333666

[25] Maarten Derickx and Filip Najman, *Classification of torsion of elliptic curves over quartic fields*, preprint, available at arxiv.org:2412.16016.

[26] Fred Diamond and John Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), CMS Conf. Proc., vol. 17, Amer. Math. Soc., Providence, RI, 1995, pp. 39–133. MR 1357209

[27] Özlem Ejder, *Isolated points on $X_1(\ell^n)$ with rational j-invariant*, Res. Number Theory **8** (2022), no. 1, Paper No. 16, 7.

[28] Noam D. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, Computational perspectives on number theory (Chicago, IL, 1995), AMS/IP Stud. Adv. Math., vol. 7, Amer. Math. Soc., Providence, RI, 1998, pp. 21–76. MR 1486831

[29] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366. MR 718935

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

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

[32] Lorenzo Furio and Davide Lombardo, *Serre's uniformity question and proper subgroups of* $c_{ns}^{+}(p)$, Available at arxiv.org:2305.17780.

[33] Steven D. Galbraith, *Rational points on* $X_0^+(p)$, Experiment. Math. **8** (1999), no. 4, 311–318.

[34] Joe Harris and Joe Silverman, *Bielliptic curves and symmetric products*, Proc. Amer. Math. Soc. **112** (1991), no. 2, 347–356. MR 1055774

[35] S. Kamienny, *Torsion points on elliptic curves over all quadratic fields*, Duke Math. J. **53** (1986), no. 1, 157–162. MR 835802

[36] ———, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229. MR 1172689

[37] 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

[38] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149. MR 931956

[39] Chandrashekhar Khare and Jean-Pierre Wintenberger, *Serre's modularity conjecture. I*, Invent. Math. **178** (2009), no. 3, 485–504. MR 2551763

[40] ———, *Serre's modularity conjecture. II*, Invent. Math. **178** (2009), no. 3, 505–586. MR 2551764

[41] Daniel Sion Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) **33** (1976), no. 2, 193–237. MR 434947

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

[43] ———, *Some cases of Serre's uniformity problem*, Math. Z. **292** (2019), no. 1-2, 739–762.

[44] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, Translated from the French by Reinie Erné, Oxford Science Publications. MR 1917232

[45] Álvaro Lozano-Robledo, *On the field of definition of p-torsion points on elliptic curves over the rationals*, Math. Ann. **357** (2013), no. 1, 279–305. MR 3084348

[46] ———, *Galois representations attached to elliptic curves with complex multiplication*, Algebra Number Theory **16** (2022), no. 4, 777–837. MR 4467123

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

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

[49] Zonia Menendez, *Images of sporadic points on the family of modular curves* $X_0(n)$, Available at https://zmenendez.wixsite.com/zkm78, 2022.

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

[51] J. S. Milne, *Jacobian varieties*, (1986), 167–212. MR 861976

[52] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees.*, Proc. Camb. Philos. Soc. **21** (1922), 179–192.

[53] 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.

[54] Andrew P. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France **102** (1974), 449–462. MR 364259

[55] Bjorn Poonen, *Rational points on varieties*, Graduate Studies in Mathematics, vol. 186, American Mathematical Society, Providence, RI, 2017. MR 3729254

[56] Kenneth A. Ribet, *Abelian varieties over* $\mathbf{Q}$ *and modular forms*, Modular curves and abelian varieties, Progr. Math., vol. 224, Birkhäuser, Basel, 2004, pp. 241–261. MR 2058653

[57] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown, *ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$ (and an appendix with John Voight)*, Forum Math. Sigma **10** (2022), Paper No. e62, 63, With an appendix with John Voight. MR 4468989

[58] Jeremy Rouse and David Zureick-Brown, *Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois*, Res. Number Theory **1** (2015), Paper No. 12, 34. MR 3500996

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

[60] ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 54, 323–401. MR 644559

[61] ———, *Abelian l-adic representations and elliptic curves*, second ed., Advanced Book Classics, Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989, With the collaboration of Willem Kuyk and John Labute. MR 1043865

[62] ———, *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

[63] 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.

[64] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094

[65] William A. Stein and Mark Watkins, *A database of elliptic curves—first report*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 267–275. MR 2041090

[66] Andrew V. Sutherland, *Constructing elliptic curves over finite fields with prescribed torsion*, Math. Comp. **81** (2012), no. 278, 1131–1147. MR 2869053

[67] ———, *Computing images of Galois representations attached to elliptic curves*, Forum Math. Sigma **4** (2016), e4, 79.

[68] Kenji Terao, *Maps between isolated points on modular curves*, (2024).

[69] Mark van Hoeij, *Low degree places on the modular curve* $X_1(n)$, preprint, available at arxiv.org:1202.4355.

[70] Bianca Viray and Isabel Vogt, *Isolated and parameterized points on curves*, preprint, available at arxiv.org:2406.14353.

[71] André Weil, *L'arithmétique sur les courbes algébriques*, Acta Math. **52** (1929), no. 1, 281–315.

[72] David Zywina, *Explicit open images for elliptic curves over* $\mathbb{Q}$, preprint, available at arxiv.org:2206.14959.

[73] ———, *On the possible image of the mod* ℓ *representations associated to elliptic curves over* $\mathbb{Q}$, available at arxiv.org:1508.07660.