Small Division Fields of Elliptic Curves

Tyler Genao
(coauthor: Sam Allen)
arXiv: 2511.23381

The Ohio State University

JMM 2026
January 6, 2026
AMS Special Session on A Showcase of Research in Number Theory with Undergraduate Contributions, I

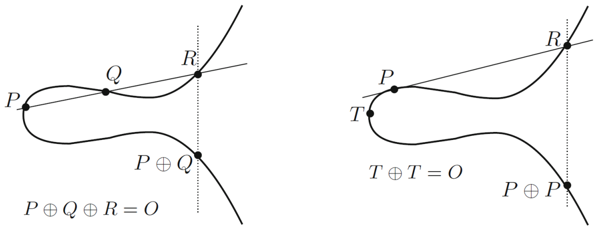
What is... an elliptic curve?

- Concretely, when the base field F has $\mathrm{char}(F) \neq 2$, an **elliptic curve** E/F is a curve defined by

$$E : y^2 = x^3 + Ax + B$$

  where $A, B \in F$, with $-16(4A^3 + 27B^2) \neq 0$.
- An elliptic curve E/F has the unique property that the set $E(F)$ of its F-rational points is an **abelian group.**

- As a planar curve, this group law $\oplus$ is described by a *chord and tangent method.*



Addition of distinct points   Adding a point to itself

Figure 3.3: The composition law.

Figure: The chord and tangent method on an elliptic curve $E/\mathbb{R}$ in Weierstrass form. From Silverman's "The Arithmetic of Elliptic Curves."

Torsion points

- Under the group law, the points in $E(\overline{F})$ of **finite order** are called **torsion points.**
- If $P \in E$ has finite order dividing n, say that P is an n-**torsion point:**

$$nP := \underbrace{P \oplus P \oplus \cdots \oplus P}_{n \text{ times}} = O,$$

  where O is the identity element of E. Such a point is called an n-**torsion point.**
- For each $n \in \mathbb{Z}^+$, we let $E[n]$ denote the n-**torsion subgroup** of $E(\overline{F})$ of points with order dividing n.

Division fields

- x and y-coordinates of torsion points are roots of polynomials, and so they generate finite degree field extensions of F.
- For each integer $n \in \mathbb{Z}^+$, we let $F(E[n]))$ denote the n-**division field of** E**,** obtained by adjoining all coordinates of n-torsion points on E to F. There are finitely many n-torsion points, so this is a finite extension of F.

- An example: consider the elliptic curve

$$E : y^2 = x^3 - 2x.$$

- It has $E[2] = \{O, (0,0), (\pm\sqrt{2}, 0)\}$.
- Thus its 2-division field is $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{2})$.
- With extra work, one can check that

$$E[3] = \left\{ O, (\alpha, \pm\sqrt{\alpha^3 - 2\alpha}) \;\middle|\; \alpha = \pm\sqrt{2 \pm \frac{4}{\sqrt{3}}} \right\}.$$

More work shows that $\mathbb{Q}(E[3])/\mathbb{Q}$ is Galois, of degree 16. This field also contains the primitive cube root of unity $\zeta_3 := \frac{-1+\sqrt{-3}}{2}$.

Galois representations of elliptic curves

- $F(E[n])/F$ naturally arises as the fixed field under a Galois action.
- $G_F := \mathrm{Gal}(\overline{F}/F)$ on $E[n]$ coordinate-wise:

$$\sigma \cdot (x, y) := (\sigma(x), \sigma(y)).$$

- This group action homomorphism is called the **mod-n Galois representation of E/F:**

$$\rho_{E,n} \colon G_F \to \mathrm{Aut}(E[n]).$$

- This action describes "how rational" each n-torsion point is, and where these coordinates live.

- $E[n]$ is a free rank two $\mathbb{Z}/n\mathbb{Z}$-module, so fixing a basis, the representation becomes

$$\rho_{E,n} \colon G_F \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

  i.e., the image can be realized as a subgroup of 2×2 invertible matrices over $\mathbb{Z}/n\mathbb{Z}$.
- We have $\ker \rho_{E,n} = \mathrm{Gal}(\overline{F}/F(E[n]))$. Modding out by the kernel gives a faithful representation

$$\rho_{E,n} \colon \mathrm{Gal}(F(E[n])/F) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

- The image of the mod-n Galois representation of an elliptic curve tells you about its n-torsion points.
- For example, an elliptic curve E/F has up to conjugacy

$$\rho_{E,n}(G_F) \subseteq \left\{ \begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix} \right\}$$

  iff E has an F-rational order n torsion point.
- Similarly, one has up to conjugacy

$$\rho_{E,n}(G_F) \subseteq \left\{ \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \right\}$$

  iff E has a cyclic subgroup of order n fixed by the action of G_F. (Keyword: "rational cyclic isogeny of degree n.")

Cyclotomy in division fields

- Torsion points of elliptic curves E/F are closely connected to **roots of unity** $\zeta \in \overline{F}$ which are elements in $\overline{F}^{\times}$ of finite multiplicative order:

$$\zeta^n = 1$$

  for some $n \in \mathbb{Z}^+$. We will write ζ_n for a primitive n'th root of unity (exact order n).
- By properties of the *n-Weil pairing*, one always has

$$\zeta_n \in F(E[n]).$$

- It's easy (with computers) to come up with explicit examples of n-division fields which *strictly* contain $F(\zeta_n)$. Calculations might suggest this containment is *almost always strict.*
- Guiding question for this talk: **when are these two fields equal,** i.e.,

$$F(\zeta_n) = F(E[n]).$$

- We call such n-division fields above **cyclotomic,** or **small.**

- We have a complete answer for elliptic curves over $\mathbb{Q}$.

Theorem (González-Jiménez and Lozano-Robledo, 2016).

Let $E/\mathbb{Q}$ be an elliptic curve. If one has $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$, then $n \leq 5$.

- They prove this with a close analysis of mod-n Galois representations over $\mathbb{Q}$, with careful group-theoretic calculations and explicit calculations with *modular curves* over $\mathbb{Q}$, which are a sort of moduli space for elliptic curves with specific torsion group structure.
- They are able to use the wealth of progress towards understanding rational points on modular curves, and Galois representations over $\mathbb{Q}$.

- What about a similar result over general number fields? Considerably less is known about Galois representations and modular curves over number fields larger than $\mathbb{Q}$.
- However, we are able to prove the following uniformity result for prime levels.

Theorem (Allen, G., 2025).

Let F be a number field. Let E/F be an elliptic curve and $p \in \mathbb{Z}^+$ a prime. If $F(E[p]) = F(\zeta_p)$, then p is uniformly bounded in F.

- With our work, we can bound p super-exponentially in terms of $[F : \mathbb{Q}]$ (conjecturally polynomially).

Ideas behind the proof:

- The main idea for our proof uses the fact that $F(E[n]) = F(\zeta_n)$ is equivalent to

$$\rho_{E,n}(G_F) \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) = 1,$$

  where $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ are the matrices in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ with determinant 1.
- We prove this for prime levels p since we can utilize a known classification of subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. ("algebra")
- We also apply work of Serre on computing mod-p images of inertia. ("arithmetic")
- The algebra and arithmetic lets us put constraints "above and below" the image $\rho_{E,p}(G_F)$, which lets us uniformly bound p. (We will describe one case of this in a moment.)

Upper bounds

- We have a classification of subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ by work of Dickson/Serre, which give us our "upper bounds" on $\rho_{E,p}(G_F)$.

Theorem.

Let $G \subseteq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ be any subgroup. Then one of the following holds (up to conjugacy):

a. *G contains $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.*
b. *G is upper triangular.*
c. *G is contained in the normalizer of a split or nonsplit Cartan subgroup.*
d. *The quotient $G/G \cap (\mathbb{Z}/p\mathbb{Z})^\times I$ is isomorphic to A_4, S_4 or A_5.*

Upper bounds

- We have a classification of subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ by work of Dickson/Serre, which give us our "upper bounds" on $\rho_{E,p}(G_F)$.

Theorem.

Let $G \subseteq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ be any subgroup. Then one of the following holds (up to conjugacy). Assuming that $G \cap \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) = 1$:

a. ~~*G contains $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.*~~
b. *G is upper triangular and is generated by $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $G \cap (\mathbb{Z}/p\mathbb{Z})^\times I$.*
c. *G is contained in the normalizer of a split or nonsplit Cartan subgroup and is generated by any non-Cartan element in G, along with the subgroup $G \cap (\mathbb{Z}/p\mathbb{Z})^\times I$.*
d. ~~*The quotient $G/G \cap (\mathbb{Z}/p\mathbb{Z})^\times I$ is isomorphic to A_4, S_4 or A_5.*~~

Lower bounds

- On the other hand, Serre has provided a description for the action of the *inertia subgroup* of G_K on an elliptic curve's p-torsion subgroup $E[p]$, when K is a local field.
- We can use this to give an explicit image of inertia in our mod-p representation. This result is essentially due to Serre; we will give an abridged version here.

Theorem.

(Abridged) Let E/F be an elliptic curve, $p \in \mathbb{Z}^+$ a prime and $\mathfrak{P}$ a prime in F over p. Let $e_0 := e(\mathfrak{P} \mid p)$ denote the ramification index of $\mathfrak{P}$ over p, and set $G := \rho_{E,p}(G_F)$. Assume that both $p \nmid \#G$ and E has semistable reduction at $\mathfrak{P}$. Then the following is true up to conjugacy:

a. *If E has good ordinary or bad multiplicative reduction at $\mathfrak{P}$, then*

$$\left\{ \begin{bmatrix} * & 0 \\ 0 & 1 \end{bmatrix}^{e_0} \right\} \subseteq G.$$

b. *If E has good supersingular reduction at $\mathfrak{P}$, then G contains the e_0'th power of the non-split Cartan subgroup (which has size $(p^2 - 1)/\gcd(p^2 - 1, e)$).*

- This gives us our "lower bounds" on $\rho_{E,p}(G_F)$.
- Combining these two results lets us create bounds on p in terms of e_0, and thus in terms of $[F : \mathbb{Q}]$, thereby giving us **uniform bounds.**

The Cycle program

The Cycle program

- This project was started through Ohio State's **Cycle** program, which was created in 2021.
- Cycle is an accredited program in the math department, which is largely run by graduate students.
- Undergraduates can enroll to receive 1 credit hour for each semester they participate (though this is not required to participate).
- Undergraduate participants are paired up with project mentors (which include faculty and graduate students), and are expected to work on a reading/research project with their mentors for two semesters. This culminates in presenting a posterboard at a project fair at the end of the Spring semester.

- Beyond helping students experience and transition into active research, the other two principal goals of Cycle are:

1. Fostering a community of students within the department.
2. Offering professional development opportunities to students.

- We do this through organizing weekly meetings with all of our students, often offering pizza and inviting faculty speakers to talk about the mathematics profession.

- The Cycle program is steadily growing:
- In Spring 2022, Cycle had 15 projects, with 18 mentors and 16 mentees.
- In Fall 2024 - Spring 2025, it had 26 projects, with 27 mentors and 41 mentees.
- This Fall 2025 - Spring 2026 year currently has 32 projects, 33 mentors and 66 mentees!

Thank you for listening!

Figure: From the 2025 Cycle Fair. Sam, David and me.