Elliptic Curves, Torsion Points and Galois Representations

Tyler Genao

The Ohio State University

CTNT 2026 Conference
June 5, 2026

- My goal is to introduce you to the study of torsion points on elliptic curves through their Galois representations, highlighting how elementary group theory can help you prove interesting results.
- Here is an outline of this talk:
  1. Define elliptic curves and torsion points.
  2. Define division fields and Galois representations of elliptic curves.
  3. Share an undergraduate research project I led on studying division fields and Galois representations with elementary group theory.

What is an elliptic curve?

- Elliptic curves are special algebraic curves where you can **add points on the elliptic curve to produce new points on it.**
- An **elliptic curve** E defined over a field F, written E/F, is a nonsingular curve defined by an equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

  where $a_1, a_2, a_3, a_4, a_6 \in F$.
- When the characteristic of F is neither 2 nor 3, an elliptic curve E/F also has an equation

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

  where $A, B \in F$ and $4A^3 + 27B^2 \neq 0$.
- These equations are *Weierstrass equations.*

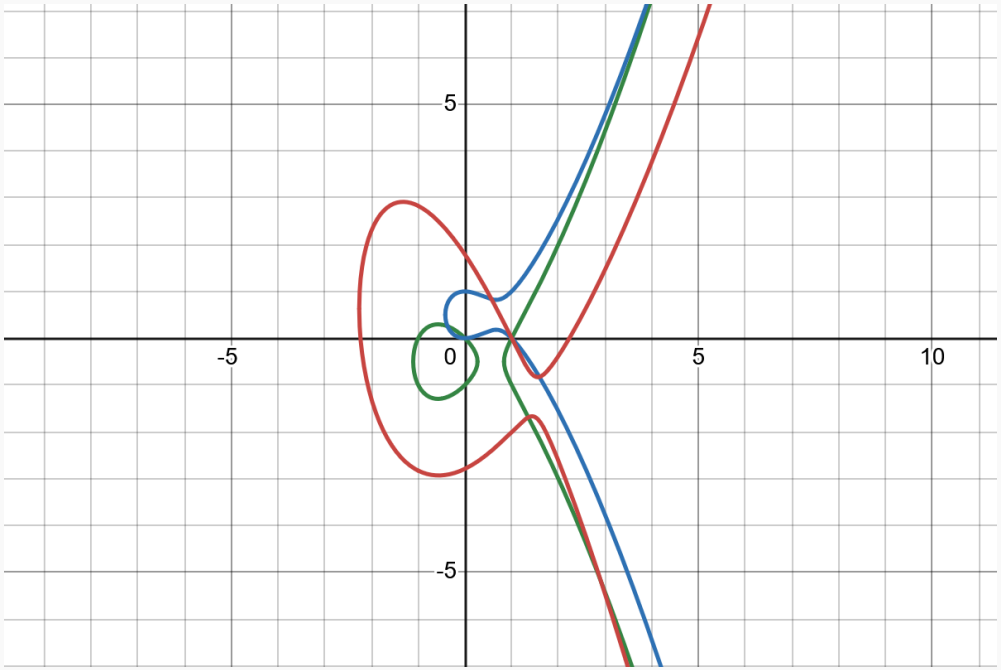
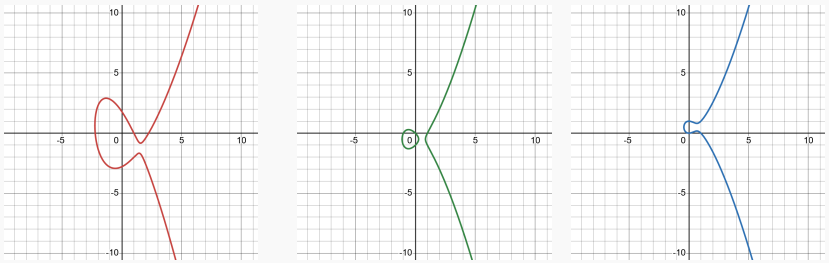
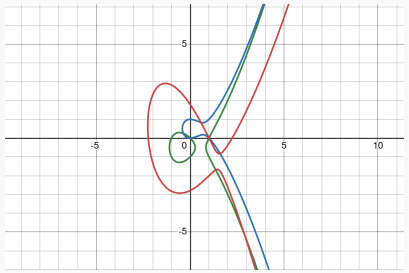
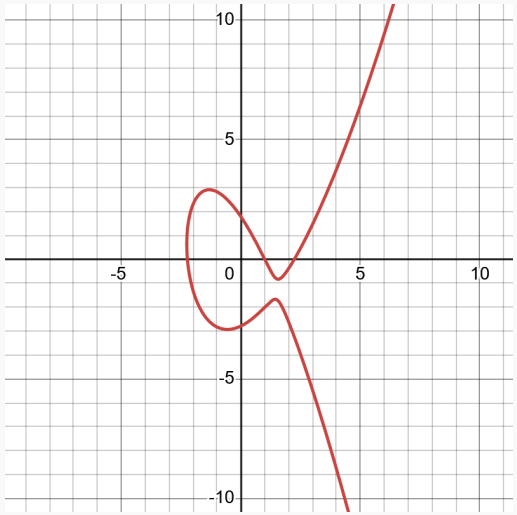


Figure: Three elliptic curves pictured above each other in $\mathbb{R}^2$, also seen below.

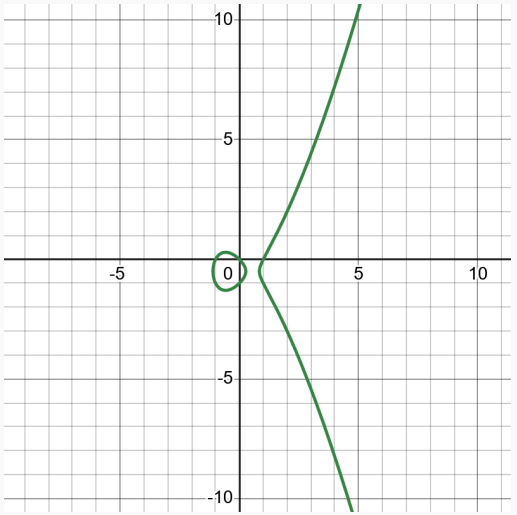


(a) (b) (c)

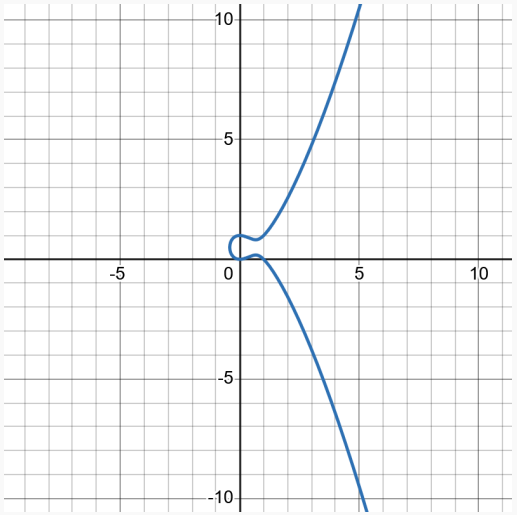




$E_1 : y^2 + xy + y = x^3 - x^2 - 5x + 5$



$E_2 : y^2 + y = x^3 - x$



$E_3 : y^2 - y = x^3 - x^2$

The group law

- For an elliptic curve E/F, let $E(F)$ denote the set of *F-rational points* of E, which are points with coordinates in F.
- Then $E(F)$ is an abelian group under a *chord and tangent method.*

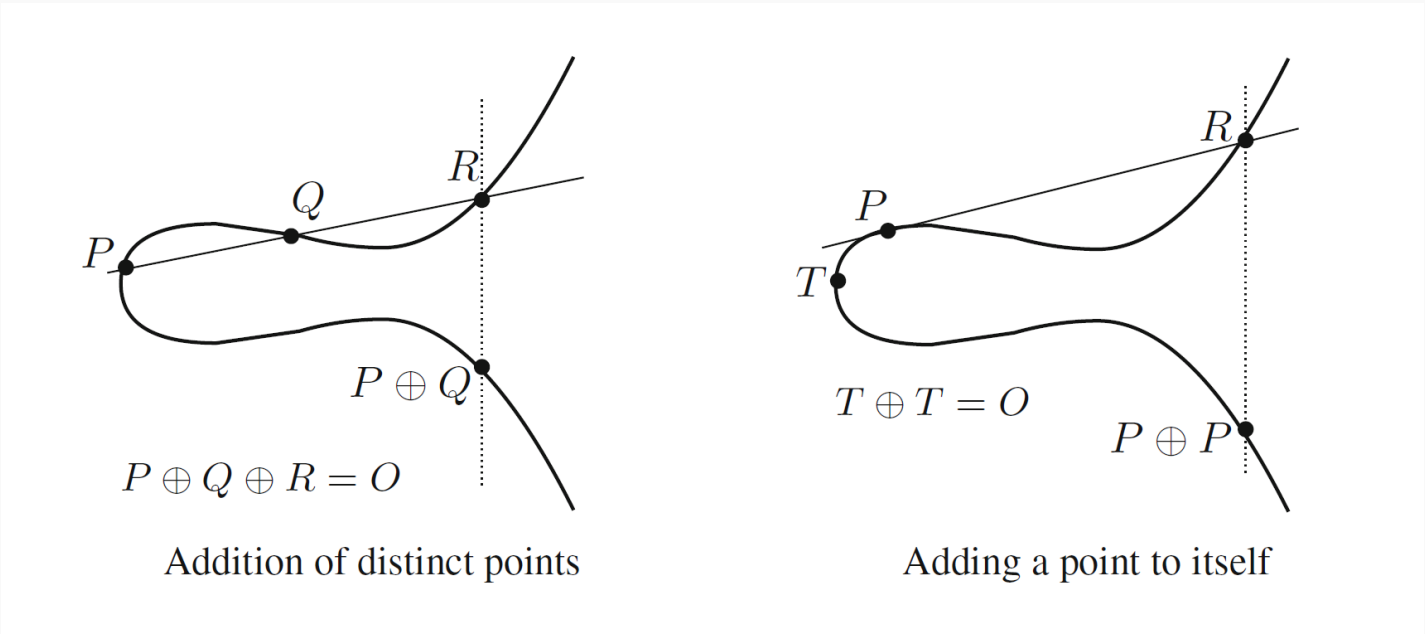


Figure: Example of the chord and tangent method on an elliptic curve $E/\mathbb{R}$. From Silverman [1].

- The identity of this group law is the *point at infinity.* This point O can only be seen on E in *projective space.*
- A great video on visualizing the projective space is *Putting Algebraic Curves in Perspective*, by Shillito.

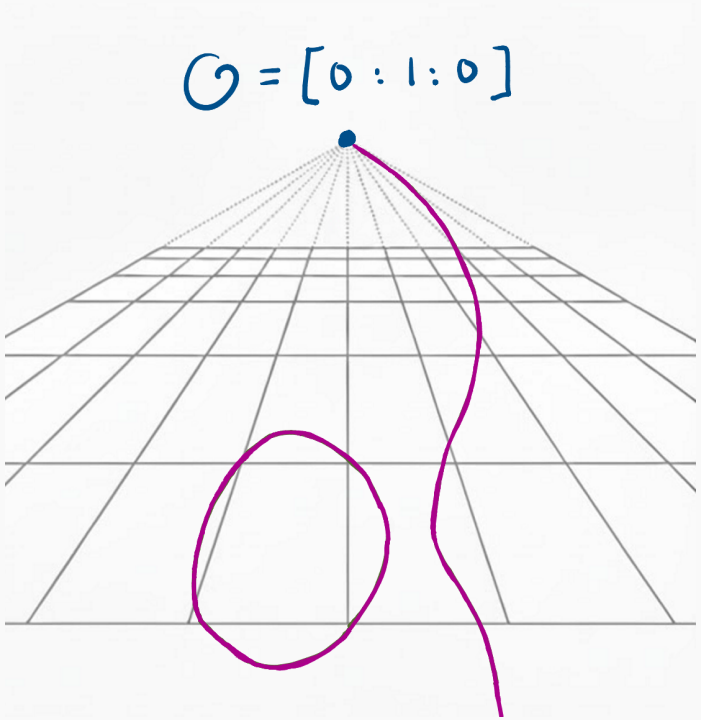


Figure: An elliptic curve pictured in the real projective plane $\mathbb{RP}^2$, along with the point at infinity O. "Parallel lines in $\mathbb{R}^2$ converge in $\mathbb{RP}^2$."

Torsion points

- To make things easier, let us assume our fields F are *number fields* (finite degree extensions of $\mathbb{Q}$).
- The group law on an elliptic curve E/F extends from $E(F)$ to $E(\mathbb{C})$.
- Points $P \in E(\mathbb{C})$ with finite order are called **torsion points:** there exists $n \in \mathbb{Z}^+$ with

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

  Such a point is also called an n-**torsion point.**
- The subgroup of n-torsion points on E is called the n-**torsion subgroup of** E**,** and is written as $E[n]$.
- General theory shows that $\#E[n] = n^2$.

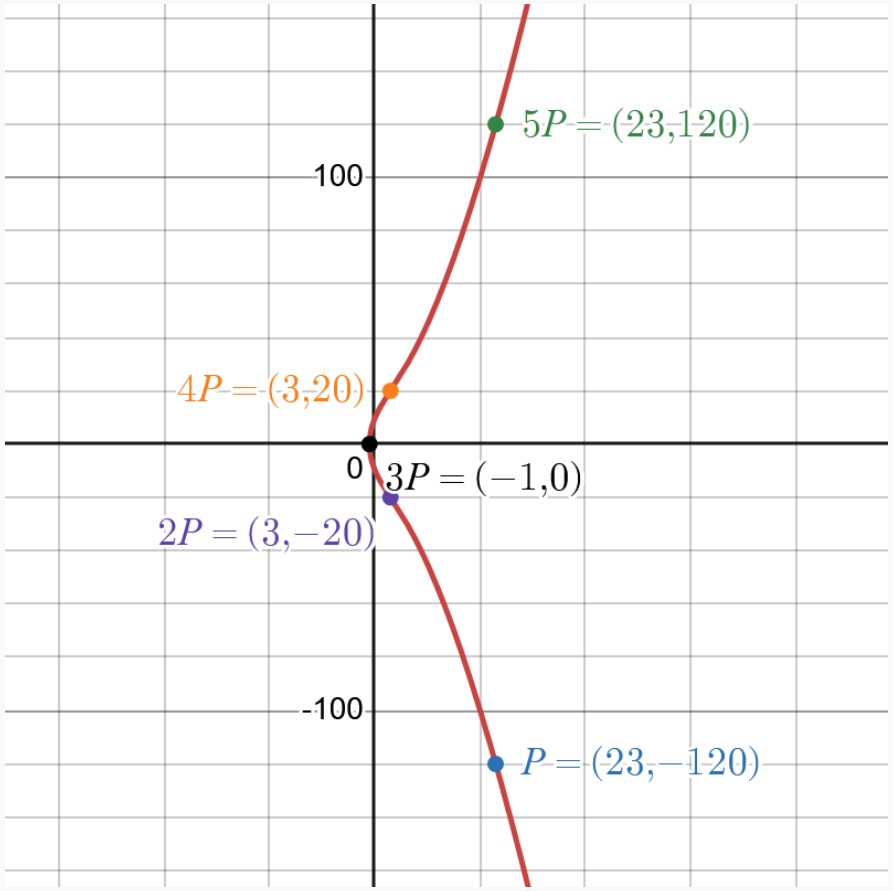


Figure: The elliptic curve $E : y^2 = x^3 + 93x + 94$ pictured in $\mathbb{R}^2$, with an order 6 torsion point $P := (23, -120)$ and its multiples.

Division fields and Galois representations

- For an elliptic curve E/F, an n-torsion point $P \in E(\mathbb{C})$ satisfies
$$nP = O.$$
Similar to algebraic numbers, this equation implies that the x and y-coordinates of P are roots of polynomials over F. (key term: *division polynomials.*)
- What types of number fields do these torsion points generate?
- One can understand these fields/coordinates by studying **division fields** and **Galois representations** of elliptic curves.

Division fields

- Given an elliptic curve E/F, for each integer $n > 0$ we let $F(E[n])$ denote the n-**division field of** E/F**,** obtained by adjoining all x and y-coordinates of n-torsion points from E onto F.
- Since coordinates of torsion points are algebraic numbers, the n-division field is always a finite extension of F.

An example

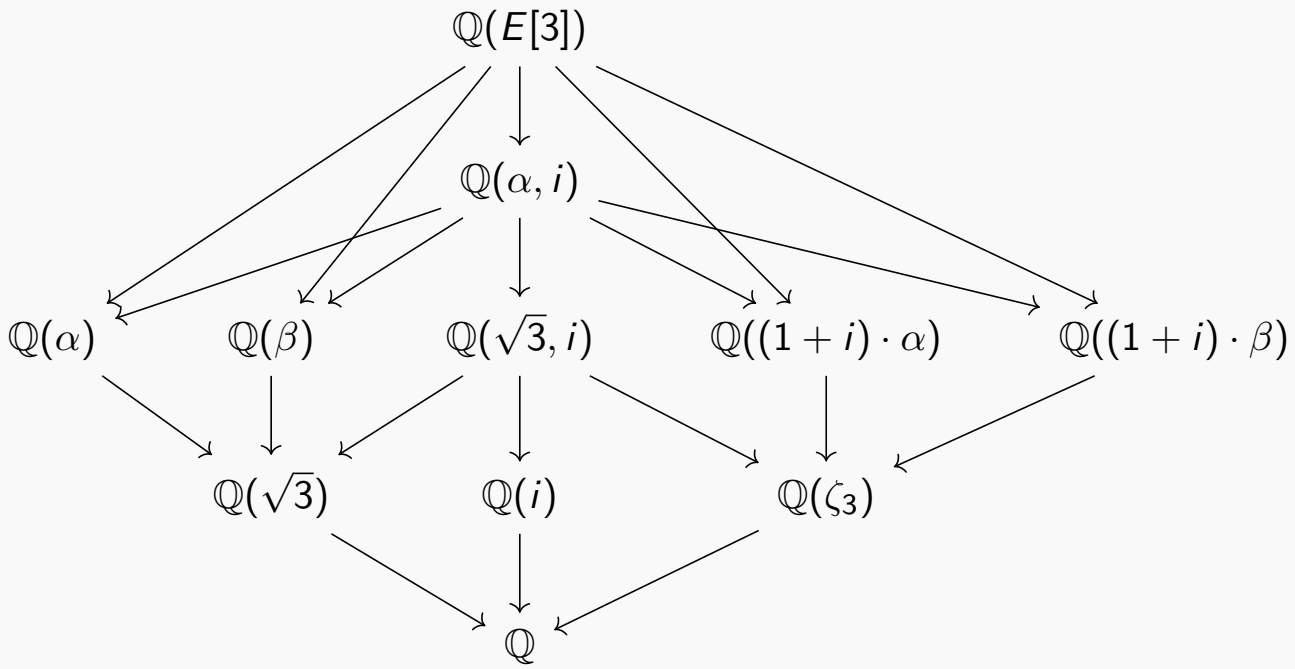
- Consider the elliptic curve

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

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

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

  $\mathbb{Q}(E[3])/\mathbb{Q}$ is Galois, with degree 16.
- Since $i, 3^{1/4} \in \mathbb{Q}(E[3])$, this field also contains the primitive cube root of unity $\zeta_3 := \frac{-1+\sqrt{-3}}{2}$, where $\zeta_3^3 = 1$.



- In the above, we let $\alpha := \sqrt{2 + \frac{4}{\sqrt{3}}}$ and $\beta := \sqrt{2 - \frac{4}{\sqrt{3}}}$.
- Then $\mathbb{Q}(\alpha, i)$ is the splitting field of the 3-division polynomial $\psi_{E,3}(x) := 3x^4 - 12x^2 - 4$, whose roots are $\pm\alpha$ and $\pm\beta$, the x-coordinates of the order 3 points on E.
- $\mathrm{Gal}(\mathbb{Q}(\alpha, i)/\mathbb{Q}) \cong D_4$, the dihedral group of order 8 (which is the symmetry group of the square).
- $\mathbb{Q}(E[3])/\mathbb{Q}(\alpha, i)$ is a quadratic extension. Can you find a generator?

The Galois action on torsion

- As it turns out, for any elliptic curve E/F, the n-division field $F(E[n])$ is always *Galois* over F.
  - $F(E[n])$ contains the splitting field of the n-division polynomial, along with additional square-roots from solving for n-torsion y-coordinates via the Weierstrass equation.
- Furthermore, $G_n := \mathrm{Gal}(F(E[n])/F)$ acts on $E[n]$ coordinate-wise:

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

(Important to note: $n(\sigma \cdot P) = \sigma \cdot (nP) = O$.)

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

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

In fact, it is a faithful (injective) group action.

$$\rho_{E,n} \colon G_n \hookrightarrow \mathrm{Aut}(E[n])$$

- $E[n]$ is a $\mathbb{Z}/n\mathbb{Z}$-module, and the Galois action respects this structure.
- In fact, $E[n]$ is a **free rank two** $\mathbb{Z}/n\mathbb{Z}$-module, i.e., $E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.
- Fixing a basis for $E[n]$, our representation can be written as

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

  where $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is the **general linear group** of 2×2 invertible matrices over $\mathbb{Z}/n\mathbb{Z}$.
- Changing the basis conjugates these matrices.

Explicit Galois representations

- If $\{P, Q\}$ is a basis for $E[n]$, then the image $\rho_{E,n}(G_n)$ can be described concretely: for $\sigma \in G_n$, one has

$$\rho_{E,n}(\sigma) = \begin{array}{c} \\ P \\ Q \end{array} \begin{array}{c} \begin{array}{cc} P & Q \end{array} \\ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \end{array}$$

  if and only if

$$\sigma(P) = aP + cQ,$$
$$\sigma(Q) = bP + dQ.$$

- We can describe rationality of n-torsion points via the "shape" of the Galois representation.
- For an elliptic curve E/F, a point $P \in E[n]$ of order n is F-rational if and only if with respect to a basis $\{P, Q\}$, one has

$$\rho_{E,n}(G_n) \subseteq B_1(n) := \left\{ \begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix} \right\} :$$

$$\rho_{E,n}(\sigma) = \begin{array}{c} \\ P \\ Q \end{array} \begin{array}{c} \begin{array}{cc} P & Q \end{array} \\ \begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix} \end{array} \iff \sigma(P) = P.$$

- In general, E has an F-rational point of order n iff $\rho_{E,n}(G_n)$ is contained in $B_1(n)$ up to conjugacy.

Research in elliptic curves: cyclotomic division fields

(In collaboration with S. Allen)

Cyclotomy in division fields

- Torsion points of elliptic curves E/F are closely connected to **roots of unity** $\zeta \in \mathbb{C}$, which are elements in $\mathbb{C}^\times$ 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 multiplicative order n).
- By properties of the *n-Weil pairing*, one always has

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

- A natural question is **when are these two fields equal,** i.e.,

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

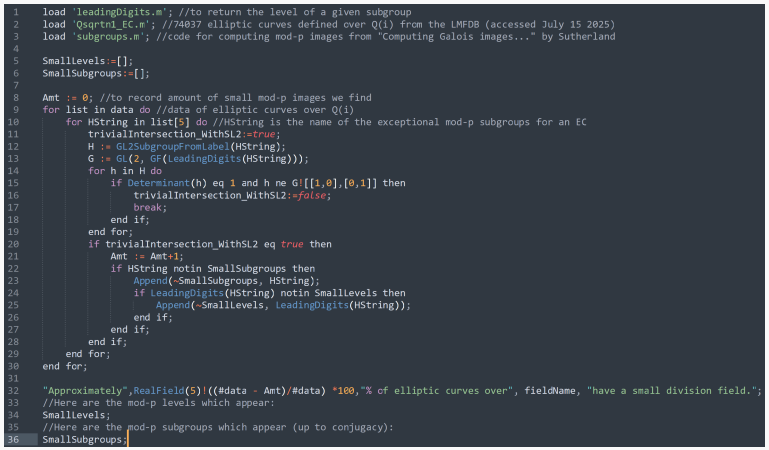
- We call these n-division fields **cyclotomic,** or **small.**
- Our previous example with the 3-division field of

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

had $\zeta_3 \in \mathbb{Q}(E[3])$, as well as $[\mathbb{Q}(E[3]) : \mathbb{Q}] = 16$. Since $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$, we conclude that

$$\mathbb{Q}(\zeta_3) \neq \mathbb{Q}(E[3]).$$

- One can use computers to try and look for explicit examples of cyclotomic division fields. Calculations would suggest this is uncommon, *and only happens for small n.*



```
load 'leadingDigits.m'; //to return the level of a given subgroup
load 'Qsqrtn1_EC.m'; //74037 elliptic curves defined over Q(i) from the LMFDB (accessed July 15 2025)
load 'subgroups.m'; //code for computing mod-p images from "Computing Galois images..." by Sutherland

SmallLevels:=[];
SmallSubgroups:=[];

Amt := 0; //to record amount of small mod-p images we find
for list in data do //data of elliptic curves over Q(i)
    for HString in list[5] do //HString is the name of the exceptional mod-p subgroups for an EC
        trivialIntersection_WithSL2:=true;
        H := GL2SubgroupFromLabel(HString);
        G := GL(2, GF(LeadingDigits(HString)));
        for h in H do
            if Determinant(h) eq 1 and h ne G![[1,0],[0,1]] then
                trivialIntersection_WithSL2:=false;
                break;
            end if;
        end for;
        if trivialIntersection_WithSL2 eq true then
            Amt := Amt+1;
            if HString notin SmallSubgroups then
                Append(~SmallSubgroups, HString);
                if LeadingDigits(HString) notin SmallLevels then
                    Append(~SmallLevels, LeadingDigits(HString));
                end if;
            end if;
        end if;
    end for;
end for;

"Approximately",RealField(5)!((#data - Amt)/#data) *100,"% of elliptic curves over", fieldName, "have a small division field.";
//Here are the mod-p levels which appear:
SmallLevels;
//Here are the mod-p subgroups which appear (up to conjugacy):
SmallSubgroups;
```

(a)

```
Approximately 92.434 % of elliptic curves over Q(i) have a small division field.
> //Here are the mod-p levels which appear:
> SmallLevels;
[ 5, 2, 3 ]
> //Here are the mod-p subgroups which appear (up to conjugacy):
> SmallSubgroups;
[ 5Cs.1.1, 2Cs, 3Cs.1.1, 5Cs.1.3 ]
Approximately 92.851 % of elliptic curves over Q(sqrt(-3)) have a small division field.
> //Here are the mod-p levels which appear:
> SmallLevels;
[ 7, 2, 3, 5 ]
> //Here are the mod-p subgroups which appear (up to conjugacy):
> SmallSubgroups;
[ 7Cs.1.1, 2Cs, 3Cs.1.1[2], 5Cs.1.1, 7Cs.1.2, 7Cs.1.4, 5Cs.1.3 ]
Approximately 91.132 % of elliptic curves over Q(zeta_21)^+ have a small division field.
> //Here are the mod-p levels which appear:
> SmallLevels;
[ 7, 2, 3 ]
> //Here are the mod-p subgroups which appear (up to conjugacy):
> SmallSubgroups;
[ 7Cs.1.1[3], 2Cs, 3Cs.1.1 ]
```

(b)

Figure: An example of `Magma` code which searches for cyclotomic division fields over number fields, including some output. Our code uses functions from Sutherland [2], and follows his subgroup labeling scheme.

- A complete answer is known 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 $n \leq 5$. More generally, if $\mathbb{Q}(E[n])/\mathbb{Q}$ is abelian then $n \leq 8$.

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

- Considerably less is known about Galois representations and modular curves over number fields beyond $\mathbb{Q}$.
- However, we are able to prove the following *uniformity* result for prime levels: these bounds depend only on F, rather than both E and F.

Theorem 1 (Allen, G., 2026).

Let F be a number field. Let E/F be an elliptic curve and $p \in \mathbb{Z}^+$ a prime.

a. *If $F(E[p]) = F(\zeta_p)$, then p is uniformly bounded in F.*
b. *If $F(E[p])/F$ is abelian, then p is uniformly bounded in F.**

*Under these two technical hypotheses: that the Generalized Riemann Hypothesis (GRH) is true, and that F does not contain the Hilbert class field of an imaginary quadratic number field. Together, these rule out the existence of an F-rational isogeny of arbitrarily large prime degree.

Theorem 1 (Allen, G., 2026).

Let F be a number field. Let E/F be an elliptic curve and $p \in \mathbb{Z}^+$ a prime.

a. *If $F(E[p]) = F(\zeta_p)$, then p is uniformly bounded in F.*
b. *If $F(E[p])/F$ is abelian, then p is uniformly bounded in F.**

- If $F(E[p]) = F(\zeta_p)$, then for $p > 12[F : \mathbb{Q}] + 1$, E must have an order p point over an extension K/F with $[K : F] \leq 6[F : \mathbb{Q}]$. By famous results of Merel/Parent, this gives a *strong* uniform bound on p, which depends only on $[F : \mathbb{Q}]$.
- If $F(E[p])/F$ is abelian, then for $p > 12[F : \mathbb{Q}] + 1$,* the image $\rho_{E,p}(G_p)$ is contained in a "Cartan subgroup" of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. This gives uniform bounds under our previous two technical hypotheses.

Proof techniques

- We will focus on the how we can prove uniform bounds on primes p which appear for small p-division fields over F.

Theorem 1 (Allen, G., 2026).

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.

- Unlike the result over $\mathbb{Q}$, we utilize the fact that $F(E[n]) = F(\zeta_n)$ if and only if

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

  where $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ are the matrices in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ with determinant 1.
- This puts strong constraints on what the image $\rho_{E,n}(G_n)$ can be.

- Why is our result for prime levels p? Two reasons:
  1. There exists a classification of subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. ("algebra")
  2. There exists work of Serre for understanding the action of the inertia group on $E[p]$. ("arithmetic")
- Together, the algebra and arithmetic impose constraints "above and below" the image $\rho_{E,p}(G_p)$, which lets us uniformly bound p.

Algebra

- 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 $\rho_{E,p}(G_p)$.

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.*

Algebra

- 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 $\rho_{E,p}(G_p)$.

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 in fact diagonalizable.*

c. *G is contained in the normalizer of a split or nonsplit Cartan subgroup, and if not contained in the Cartan subgroup, then is generated by any non-Cartan element in G with $G \cap (\mathbb{Z}/p\mathbb{Z})^\times I$.*

d. ~~*The quotient $G/G \cap (\mathbb{Z}/p\mathbb{Z})^\times I$ is isomorphic to A_4, S_4 or A_5.*~~

- The Cartan groups and their normalizers can be made explicit:
- The *split Cartan subgroup of* $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is

$$C_s(p) := \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} : ad \neq 0 \right\}.$$

  Its normalizer is

$$N_s(p) = \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}, \begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix} : ad \neq 0 \right\}.$$

- Let ϵ be the least positive generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. Then the *nonsplit Cartan subgroup of* $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is

$$C_{ns}(p) := \left\{ \begin{bmatrix} a & b\epsilon \\ b & a \end{bmatrix} : (a,b) \neq (0,0) \right\}.$$

  (This is the regular representation of the quadratic extension of $\mathbb{Z}/p\mathbb{Z}$ acting on itself via multiplication, under the basis $\{1, \sqrt{\epsilon}\}$.)

- Its normalizer is

$$N_{ns}(p) = \left\{ \begin{bmatrix} a & b\epsilon \\ b & a \end{bmatrix}, \begin{bmatrix} a & b\epsilon \\ -b & -a \end{bmatrix} : (a,b) \neq (0,0) \right\}.$$

Arithmetic

- On the other hand, Serre has provided a description for the action of the *inertia group* of a local field K of residue characteristic p, on the p-torsion group of an elliptic curve E/K.
- We can use this to prove the following almost purely group-theoretic result (essentially concluded from Serre's paper). This gives "lower bounds" on $\rho_{E,p}(G_p)$.

Theorem (A black-box result for students).

(Abridged) Let E/F be an elliptic curve, $p \in \mathbb{Z}^+$ a prime and $\mathfrak{P}$ a prime in F over p. Let $e := e(\mathfrak{P} \mid p)$ denote the ramification index of $\mathfrak{P}$ over p. Assume that $p \nmid \#\rho_{E,p}(G_p)$, and that 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*

$$\left\{ \begin{bmatrix} * & 0 \\ 0 & 1 \end{bmatrix}^e \right\} \subseteq \rho_{E,p}(G_p).$$

b. *If E has good supersingular reduction at $\mathfrak{P}$, then $\rho_{E,p}(G_p)$ contains the e'th power of the non-split Cartan subgroup.*

Theorem (A black-box result for students).

(Abridged) Let E/F be an elliptic curve, $p \in \mathbb{Z}^+$ a prime and $\mathfrak{P}$ a prime in F over p. Let $e := e(\mathfrak{P} \mid p)$ denote the ramification index of $\mathfrak{P}$ over p. Assume that $p \nmid \#\rho_{E,p}(G_p)$, and that 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*

$$\left\{ \begin{bmatrix} * & 0 \\ 0 & 1 \end{bmatrix}^e \right\} \subseteq \rho_{E,p}(G_p).$$

This then involves a case-by-case analysis using group and matrix theory.

b. *If E has good supersingular reduction at $\mathfrak{P}$, then $\rho_{E,p}(G_p)$ contains the e'th power of the non-split Cartan subgroup. The size of this power is $(p^2-1)/\gcd(p^2-1, e)$, and since $\#\rho_{E,p}(G_p) \mid (p-1)$, this forces $p \leq e+1$.*

- The cases to analyze are where $\rho_{E,p}(G_p)$ is upper triangular, or in the normalizer of the split/nonsplit Cartan subgroup, each of which can be done on the level of matrices.
- Analyzing these shows we can bound p in terms of e. Since $e \leq [F : \mathbb{Q}]$, this gives us **strong uniform bounds.**
- The abelian case is more involved!

- The work in this theorem can be summarized as follows:
  1. Assume that $\rho_{E,p}(G_p) \cap \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) = 1$.
  2. Describe the "shape" of $\rho_{E,p}(G_p)$ via the classification of subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.
  3. **Black-box** work of Serre to analyze which groups must appear in $\rho_{E,p}(G_p)$.
  4. Use the three items above to drastically reduce which options can appear for $\rho_{E,p}(G_p)$.
  5. For the remaining cases, use the structure of $\rho_{E,p}(G_p)$ to uniformly bound the order of prime torsion points of elliptic curves over number fields via more conceptual results.
- A good chunk of this paper involves elementary group theory calculations, and working with Galois theory conceptually.
- Our preprint can be found at this arXiv identifier: 2511.23381

- This paper also provides a framework for future projects:
- Given another group-theoretic ingredient of a division field (such as nilpotent, solvable, etc.), can you "sandwich" this property between the algebra and arithmetic of mod-p images of Galois to prove uniform bounds?

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

Thank you!

References (in order of appearance):

1. J. Silverman, *The arithmetic of elliptic curves,* 2nd Ed., Graduate Texts in Mathematics, vol. 106, Springer (2009).
2. A. Sutherland, *Computing images of Galois representations attached to elliptic curves,* Forum Math. Sigma 4 (2016), Paper No. e4, 79 pp.
3. E. González-Jiménez and Á. Lozano-Robledo, *Elliptic curves with abelian division fields,* Math. Z. 283 (2016), no. 3-4, 835–859.
4. S. Allen and T. Genao, *Uniform bounds on the level of cyclotomic division fields of elliptic curves,* preprint, https://arxiv.org/abs/2511.23381.
5. L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. 124 (1996), 437–449.
6. P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math. 506 (1999), 85–116.