Elliptic Curves, Torsion Points and Galois Representations

Tyler Genao

The Ohio State University

Carnegie Mellon University
January 30, 2026

- The goal of this talk is to introduce you to the study of elliptic curves and their torsion points via (almost purely) group-theoretic considerations.
- Hopefully I can convince you that you can do elliptic curves research with some experience in abstract algebra!
- Here is an outline:
  1. Describe elliptic curves and torsion points.
  2. Define division fields and Galois representations of elliptic curves.
  3. Illustrate how group theory is used in understanding torsion points, via explicit matrix calculations.
  4. Share some research vistas.

What is an elliptic curve?

- Elliptic curves are special algebraic curves where **points can be added together** to produce more points on the curve.
- An **elliptic curve** E defined over a field F, written E/F, is a nonsingular curve defined by the 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 not 2, elliptic curves E/F also have an equation of the form

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

  where $A, B \in F$.
- These equations are called *Weierstrass forms.*

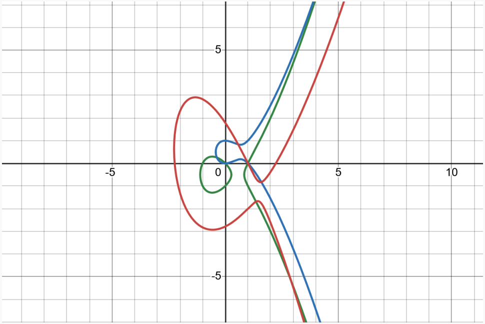
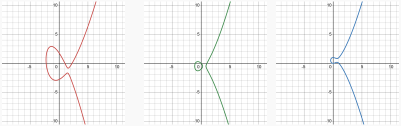
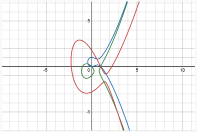
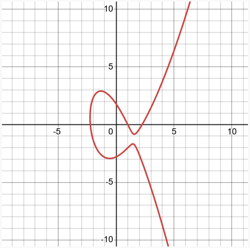


Figure: Three elliptic curves pictured above each other in $\mathbb{R}^2$, also seen below.

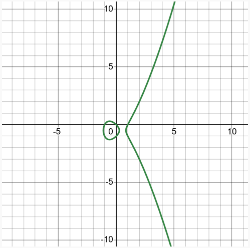


(a) (b) (c)

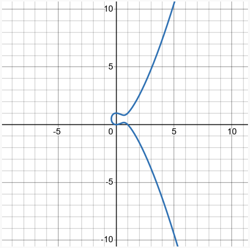




$E_1 : y^2 + xy + y = x^3 - x^2 - 5x + 5$



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



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

- Elliptic curves E/F always have a point that lies beyond the affine plane F^2, called the *point at infinity.* This point O can only be seen in *projective space.*

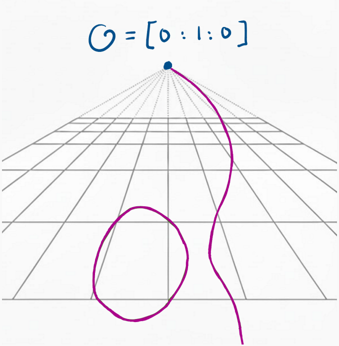


Figure: An elliptic curve pictured in real projective space $\mathbb{RP}^2$, with point at infinity O. "Parallel lines in $\mathbb{R}^2$ converge in $\mathbb{RP}^2$."

- A great video on visualizing the projective space is *Putting Algebraic Curves in Perspective,* by Shillito.

The group law

- For an elliptic curve E/F, let $E(F)$ denote its set of F-rational points on E.
- Then $E(F)$ is a group under a *chord and tangent method.*

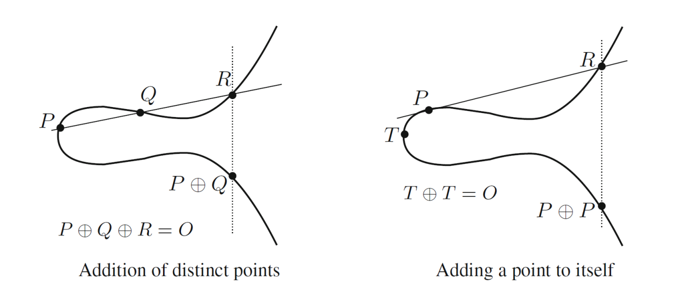


Figure: Example of the chord and tangent method on an elliptic curve $E/\mathbb{R}$. From [1].

- This group law was described geometrically, but its algebraic constructions also hold over fields beyond $\mathbb{R}$:

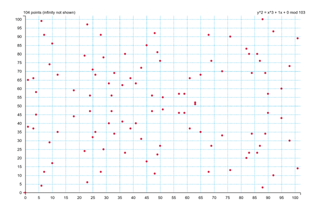


Figure: The elliptic curve $y^2 = x^3 + x$ over the finite field of size 103.

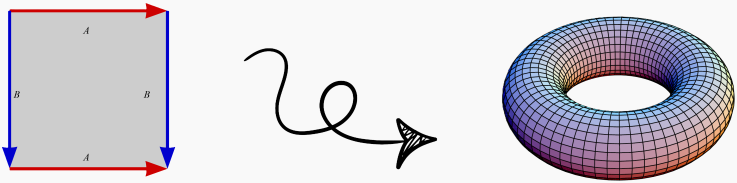


Figure: An elliptic curve as a complex torus $\mathbb{C}/\Lambda$. Right picture from [2].

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 denoted by $E[n]$. General theory shows that $\#E[n] = n^2$.

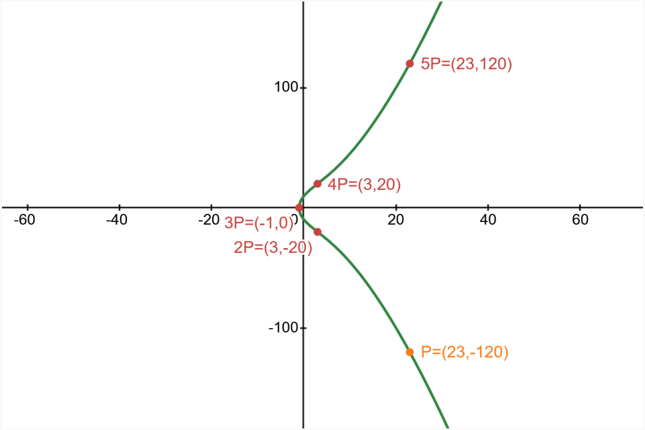


Figure: The elliptic curve $E : y^2 = x^3 + 93x + 94$, with its order 6 torsion point $P = (23, -120)$ and its multiples.

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 implies that the x and y-coordinates of P are roots of polynomials over F. (keyword: *division polynomials.*)
- A portion of arithmetic geometry research is dedicated to understanding the *rationality* of torsion points, i.e., understanding over which fields torsion points live.
- One way to understand rationality of torsion points is through studying **division fields** and **Galois representations** of elliptic curves.

Division fields

- Given 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.

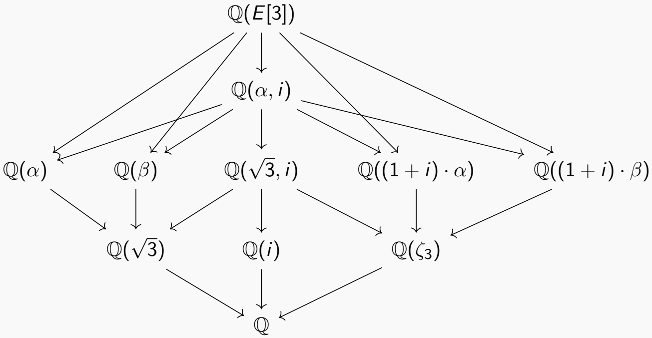
- An example: consider the elliptic curve

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

- 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 $\zeta_3 := e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2}$, 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 $\psi_{E,3}(x) := 3x^4 + 12x^2 - 4$, 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 (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

- For an elliptic curve E/F, one important interpretation of its n-division field $F(E[n])/F$ is as the *fixed field* under the Galois action on $E[n]$.
- Let $\overline{F}$ denote an *algebraic closure* of F. This is e.g. the subfield of $\mathbb{C}$ of all elements which are algebraic over F, i.e., are roots of polynomials over F.
- Consider the *absolute Galois group* of F:

$$G_F := \mathrm{Gal}(\overline{F}/F).$$

- G_F consists of F-automorphisms $\sigma\colon \overline{F} \xrightarrow{\sim} \overline{F}$; these describe where to send *every single algebraic number over F.*

- For any elliptic curve E/F and integer $n > 0$, the absolute Galois group G_F acts 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:**

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

- It is the case that $E[n]$ is a free rank two $\mathbb{Z}/n\mathbb{Z}$-module. Fixing a basis for $E[n]$, our representation can be written as

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

  where $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is the group of 2×2 invertible matrices over $\mathbb{Z}/n\mathbb{Z}$.
- We have $\ker \rho_{E,n} = \mathrm{Gal}(\overline{F}/F(E[n]))$, so that $F(E[n])/F$ is Galois. Modding out by the kernel gives a faithful representation

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

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

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

  if and only if

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

- Sometimes we write $\rho_{E,n,P,Q}$ instead of $\rho_{E,n}$ to specify the basis.

Common shapes

- 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 for $Q \in E[n]$ with $\{P, Q\}$ a basis, one has

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

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

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

- Say the *subgroup* $\langle P \rangle \subseteq E[n]$ is F*-rational* if $\langle P \rangle$ is fixed by the action of G_F on $E[n]$, i.e., for all $\sigma \in G_F$ one has

$$\sigma(P) \in \langle P \rangle.$$

- One has that a cyclic order n subgroup $\langle P \rangle$ is F-rational iff one has

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

  for some $Q \in E[n]$ where $\{P, Q\}$ is a basis.
- (This is related to understanding *rational cyclic isogenies of elliptic curves.*)
- One has $\rho_{E,n}(G_F) = 1$ iff $F(E[n]) = F$.

Research in elliptic curves: cyclotomic division fields

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

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

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

- We call these division fields **cyclotomic,** or **small.**
- Our previous example of an for 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

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

- 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';
load 'Qsqrtn1_EC.m'; //74037 elliptic curves defined over Q(i) from the LMFDB
load 'subgroups.m'; //code of computing mod-p images from 'Computing Galois images...' by Sutherland
SmallLevels:=[];
SmallSubgroups:=[];
Amt := 0; //number of small mod-p images
for d in data do
    if #d[5] gt 0 then
        for HString in d[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 if;
end for;
"Approximately",RealField(5)!((#data - Amt)/#data) *100,"% of elliptic curves over Q(i) have a small division field.";
SmallLevels;
SmallSubgroups;
```

(a)

```
Approximately 92.434 % of elliptic curves over Q(i) have a small division field.
> SmallLevels;
[ 5, 2, 3 ]
> SmallSubgroups;
[ 5Cs.1.1, 2Cs, 3Cs.1.1, 5Cs.1.3 ]
```

(b)

Figure: An example of preliminary `Magma` code searching for cyclotomic division fields, along with its output. Our code uses functions from [3], and follows its subgroup labeling scheme.

- A complete answer is known for elliptic curves over $\mathbb{Q}$.

Theorem (González-Jiménez and Lozano-Robledo, 2016 (4)).

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 $\mathbb{Q}$, 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 $\mathbb{Q}$.

- 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 1 (Allen, G., 2025).

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.

Theorem 1 (Allen, G., 2025).

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 p is bounded super-exponentially in terms of $[F : \mathbb{Q}]$.
- If $F(E[p])/F(\zeta_p)$ is abelian, then p is similarly bounded in terms of $[F : \mathbb{Q}]!$.
- Our explicit bounds depend on bounds for orders of torsion points over number fields in terms of the degree of the field (which are conjectured to be polynomial in $[F : \mathbb{Q}]$.)

Ideas behind the proof:

- 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., 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.

Theorem 1 (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.

- Unlike the result over $\mathbb{Q}$, the impetus of our proof is the fact that $F(E[n]) = F(\zeta_n)$ if and only if

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

  where $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ are the matrices in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ with determinant 1.
- This puts constraints on what the image $\rho_{E,n}(G_F)$ 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 on Serre for understanding the mod-p images of inertia. ("arithmetic")
- Together, the algebra and arithmetic lets us put constraints "above and below" the image $\rho_{E,p}(G_F)$, 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 $\rho_{E,p}(G_F)$.

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.*

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 $\rho_{E,p}(G_F)$.

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 in fact diagonalizable.*

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.*~~

Arithmetic

- 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 prove the following almost purely group-theoretic result (essentially due to Serre).

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 $e := e(\mathfrak{P} \mid p)$ denote the ramification index of $\mathfrak{P}$ over p, and set $G := \rho_{E,p}(G_F)$. Assume that $p \nmid \#G$, and that E has semistable reduction at $\mathfrak{P}$. The following is true up to conjugacy:

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

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

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

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

- The work involved in this theorem can be summarized as follows:
  1. Assume $\rho_{E,p}(G_F) \cap \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) = 1$.
  2. Describe the "shape" of $\rho_{E,p}(G_F)$ 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 $\rho_{E,p}(G_F)$.
  4. Use the three items above to drastically reduce which options can appear for $\rho_{E,p}(G_F)$; determine what these options say about rationality of p-torsion on E/F.
  5. Cite results on uniformly bounding order of prime torsion points of elliptic curves over number fields.
- The majority of this project is elementary group theory calculations, and working with Galois theory conceptually.
- Our paper can be found at this arXiv identifier: 2511.23381

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

Future projects:

- Are there uniform bounds on levels of division fields over number fields with a property besides ‘cyclotomic’ or ’abelian’?
- For example, **nilpotent** division fields have uniform bounds connected to *Mersenne primes.* This has been studied over $\mathbb{Q}$ by Daniels and Rouse: 2409.00881
- Finally, our preliminary searches for small division fields suggested that uniform bounds of $p \leq 7$ worked over all number fields that we checked from the LMFDB. Can we push the algebra/arithmetic further to prove a sharper uniform bound?

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. L. Washington, *Elliptic curves. Number theory and cryptography,* 2nd Ed., Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL (2008).
3. A. Sutherland, *Computing images of Galois representations attached to elliptic curves,* Forum Math. Sigma 4 (2016), Paper No. e4, 79 pp.
4. E. González-Jiménez and Á. Lozano-Robledo, *Elliptic curves with abelian division fields,* Math. Z. 283 (2016), no. 3-4, 835–859.
5. S. Allen and T. Genao, *Uniform bounds on the level of cyclotomic division fields of elliptic curves,* preprint, https://arxiv.org/abs/2511.23381.
6. H. Daniels and J. Rouse, *Near coincidences and nilpotent division fields,* preprint, https://arxiv.org/abs/2409.00881.