Elliptic Curves and Galois Representations

Mentees: Sam Allen and David Kruzel Mentor: Tyler Genao

Department of Mathematics, The Ohio State University

DEPARTMENT OF MATHEMATICS

Primary Goal

The goal of this project was to learn about elliptic curves and their group structure, as well as elliptic curve Galois Representations. This project has expanded to an exploration of their division fields.

Elliptic Curves and Their Group Law

An **elliptic curve** over a field K is a nonsingular, projective, cubic plane curve with a K-rational point. It is written as $E_{/K}$, or just E.

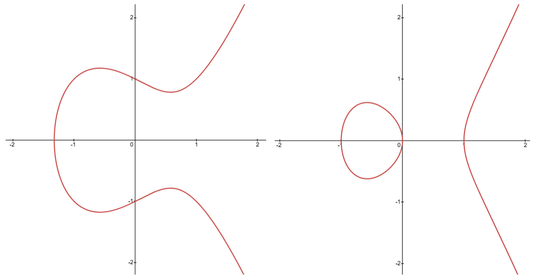

Figure 1. Two common shapes for an elliptic curve in $\mathbb{R}^2$.

Here are what these terms mean. Let $\overline{K}$ be an algebraic closure of K (we will assume that K is a perfect field).

- **Cubic plane curve:** This is the set of points in $\overline{K}^2$ which are solutions to an irreducible cubic polynomial $f(x,y) \in \overline{K}[x,y]$. We often write the curve as
$$C : f(x,y) = 0.$$
If $f \in K[x,y]$, then we say that C is **defined over** K, and write $C_{/K}$. For example, elliptic curves are generally given in *Weierstrass form*,
$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$
Thus, E is defined over K if $a_1, a_2, a_3, a_4, a_6 \in K$. A special case is the "short Weierstrass form"
$$E : y^2 = x^3 + Ax + B,$$
where E is defined over K if $A, B \in K$.
- **Nonsingular:** For a curve $C : f(x,y) = 0$, this means there is no point P on C for which the two partial derivatives $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ are simultaneously zero at P.
- **Projective:** This means that the curve lies in the *projective plane* $\mathbb{P}^2$. This is a bit technical, but important, since elliptic curves have a "point at infinity" that can only be seen in $\mathbb{P}^2$.

Any curve $C_{/K}$ has infinitely many points in $\overline{K}^2$ – however, it is interesting to ask what is known about $C(K)$, the set of points in K^2. Studying K-rational points on curves is a big part of modern number theory.

Group Law: A remarkable fact about elliptic curves $E_{/K}$ is that the set $E(K)$ of their K-rational points is an *abelian group*. The group law is defined using the "chord and tangent" method. We illustrate this with an example.

Example: Consider the elliptic curve $E : y^2 = x^3 - x + 2$, and points $P_1 := (-1, \sqrt{2})$ and $P_2 := (0, \sqrt{2})$ on E. We want to compute the two sums $P_1 \oplus P_2$ and $2P_1 := P_1 \oplus P_1$. We will start with $P_1 \oplus P_2$:

The first step is to find the chord (line segment) between P_1 and P_2. This is given by the line $y = \sqrt{2}$. By geometric considerations, this line will always intersect the elliptic curve three times (possibly with multiplicity). The third intersection point here is $P_1 \star P_2 := (1, \sqrt{2})$.

The next step is to take the chord between $P_1 \star P_2$ and the *point at infinity* $\mathcal{O}$ (which is only seen in the projective plane). The corresponding line is just the vertical line through $P_1 \star P_2$, which in this case is $x = 1$. This line intersects E at a third point, which is our sum, $P_1 \oplus P_2 := (1, -\sqrt{2})$.

To compute $2P_1$, the first step is to compute the tangent line to E at P_1, which is $y = \frac{\sqrt{2}}{2}x + \frac{3\sqrt{2}}{2}$. In this case, we have $P_1 \star P_1 = \left(\frac{5}{2}, \frac{11}{\sqrt{8}}\right)$. For the next step, the vertical line through $P_1 \star P_1$ is $x = \frac{5}{2}$, which implies that $2P_1 = \left(\frac{5}{2}, -\frac{11}{\sqrt{8}}\right)$.

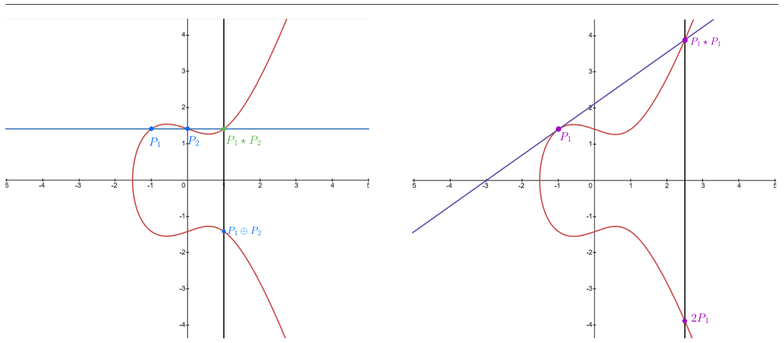

Figure 2. The group law for computing $P_1 \oplus P_2$ and $2P_1$, respectively.

Torsion Points

Torsion Points: A point P on an elliptic curve E is called a **torsion point** if $\exists n \in \mathbb{Z}^+$ such that $nP = \mathcal{O}$. In this case, we also call P an **n-torsion point.**

Torsion Groups: For an elliptic curve $E_{/K}$, we can look at the subgroup of all points in $E(K)$ whose order is finite; this is the **torsion group of E over K,** and is denoted by $E(K)[\text{tors}]$. For an integer $n \in \mathbb{Z}^+$, we also have the n-torsion subgroup $E(K)[n]$, which is the subgroup of points whose order divides n. More generally, we set $E[\text{tors}] := E(\overline{K})[\text{tors}]$ and $E[n] := E(\overline{K})[n]$.

Example: The following image shows how the chord and tangent method can be used to show that on the elliptic curve $E : y^2 = x^3 + 93x + 94$, the point $P_1 := (23, -120) \in E$ has order 6:

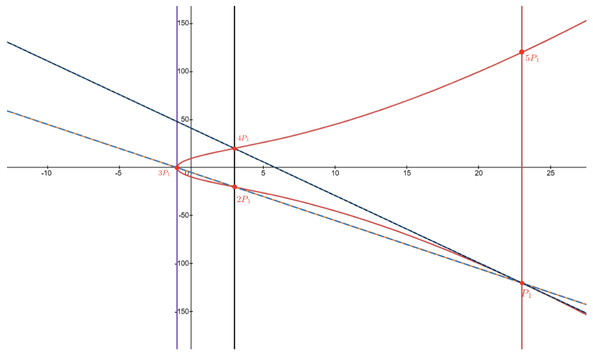

Figure 3. The chord and tangent method applied repeatedly to compute the order of $P_1 := (23, -120)$ on $E : y^2 = x^3 + 93x + 94$.

One of the most important results for elliptic curves is the **Mordell-Weil Theorem**, which further describes the group structure of $E(K)$ when K is a *number field*, i.e., a finite degree extension of $\mathbb{Q}$.

Mordell-Weil Theorem:
Let F be a number field. Then for any elliptic curve $E_{/F}$, its Mordell-Weil group is a finitely generated abelian group: that is, there exist points $P_1, P_2, \ldots, P_n \in E(F)$ such that for any point $P \in E(F)$, one has
$$P = a_1P_1 \oplus a_2P_2 \oplus \cdots \oplus a_nP_n$$
for some $a_1, a_2, \ldots, a_n \in \mathbb{Z}$.

The Mordell-Weil theorem and the fundamental theorem of finitely generated abelian groups together imply the following.

Corollary:
Let F be a number field. Then for any elliptic curve $E_{/F}$, one has
$$E(F) \cong \mathbb{Z}^r \times E(F)[\text{tors}]$$
for some integer $r \geq 0$.

Galois Representations

Given a number field F and an elliptic curve $E_{/F}$, we know that $E(F)[\text{tors}]$ is a finite abelian group. What can we say about $E[\text{tors}]$, the group of torsion points in $\overline{F}^2$? For any integer $n \geq 1$, we always have n^2 points of order dividing n in $E(\overline{F})$ – however, these points do not necessarily live F^2.

We can use *Galois representations* to study rationality of torsion points. Fix an $n \geq 1$. Then there is an action of the absolute Galois group $G_F := \text{Gal}(\overline{F}/F)$ on $E[n]$:
$$\forall \sigma \in G_F,\ \forall P = (x,y) \in E[n], \qquad \sigma(P) := (\sigma(x), \sigma(y)).$$
The associated group action homomorphism
$$\rho_{E,n} \colon G_F \to \text{Aut}(E[n])$$
is called the **mod-n Galois representation of E.**

Fact: Each n-torsion subgroup $E[n]$ is free $\mathbb{Z}/n\mathbb{Z}$-module of rank 2. Thus, choosing a basis $\{P, Q\}$ of $E[n]$ gives an isomorphism $\text{Aut}(E[n]) \cong \text{GL}_2(\mathbb{Z}/n\mathbb{Z})$, and so our representation becomes
$$\rho_{E,n,P,Q} \colon G_F \to \text{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$
In particular, fixing a basis of $E[n]$ means that the image $\rho_{E,n}(G_F)$ can be realized as a subgroup of invertible 2×2 matrices over $\mathbb{Z}/n\mathbb{Z}$. Picking a different basis will conjugate this image.

For an elliptic curve $E_{/F}$, its mod-n image $\rho_{E,n}(G_F)$ encodes explicit information about the rationality of its n-torsion points.

Example: We have
$$\rho_{E,n,P,Q}(G_F) \subseteq \left\{ \begin{bmatrix} 1 & b \\ 0 & d \end{bmatrix} \in \text{GL}_2(\mathbb{Z}/n\mathbb{Z}) \right\} \iff P \in E(F) \quad .$$
Additionally,
$$\rho_{E,n,P,Q}(G_F) \subseteq \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in \text{GL}_2(\mathbb{Z}/n\mathbb{Z}) \right\} \iff \langle P \rangle := \{aP : 0 \leq a < n\} \text{ is } G_F\text{-stable}$$
$$\iff \forall \sigma \in G_F,\ \sigma(P) \in \langle P \rangle.$$
Without specifying a basis $\{P, Q\}$ of $E[n]$, these properties will hold up to conjugation of the image $\rho_{E,n}(G_F)$.

Current Directions

In studying the rationality of n-torsion points on an elliptic curve, it is natural to consider its *n-division field*.

Division Fields: Given an elliptic curve $E_{/F}$ and an integer $n \in \mathbb{Z}^+$, the **n-division field** of E, denoted by $F(E[n])$, is the minimal extension of F over which all n-torsion points of E are rational. Explicitly, the field $F(E[n])$ is generated over F by the coordinates of n-torsion points:
$$F(E[n]) = F(\{x(P), y(P) : P \in E[n]\}).$$

The n-division field is also connected to the mod-n Galois representation. For an elliptic curve $E_{/F}$ and an integer $n \in \mathbb{Z}^+$, one has $\ker \rho_{E,n} = \text{Gal}(\overline{F}/F(E[n]))$. Thus $F(E[n])/F$ is Galois, with Galois group isomorphic to a subgroup of $\text{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

For $n \in \mathbb{Z}^+$, let $\zeta_n := e^{2\pi i/n}$ denote a primitive n'th root of unity. For a number field $F/\mathbb{Q}$, let $F(\zeta_n)$ denote the minimal extension of F containing ζ_n. For any elliptic curve $E_{/F}$, algebraic considerations imply that $\zeta_n \in F(E[n])$, and hence $F(\zeta_n) \subseteq F(E[n])$. When is it possible that $F(\zeta_n) = F(E[n])$? A *uniform* answer to this question is known in the case $F = \mathbb{Q}$:

[GL16, Theorem 1.1]:
For any elliptic curve $E_{/\mathbb{Q}}$, if there is $n \in \mathbb{Z}^+$ such that $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$, then $n = 2, 3, 4, 5$.

We are currently exploring a generalization of this result to other number fields:

Question:
Fix a number field F. Does there exist an integer $c := c(F) \in \mathbb{Z}^+$ such that for any elliptic curve $E_{/F}$, if there is $n \in \mathbb{Z}^+$ such that $F(E[n]) = F(\zeta_n)$, then $n \leq c$?

References

[GL16] Enrique González-Jiménez and Álvaro Lozano-Robledo. "Elliptic curves with abelian division fields". In: Math. Z. 283.3-4 (2016), pp. 835–859. ISSN: 0025-5874,1432-1823. DOI: 10.1007/s00209-016-1623-z. URL: https://doi.org/10.1007/s00209-016-1623-z.

allen.2767@osu.edu kruzel.7@osu.edu genao.5@osu.edu