Fall 2024 FLT Seminar: Torsion and Isogenies of Elliptic Curves

Zachary Lihn

October 14, 2024

Let (E, O) be an elliptic curve over a field k, and let Ω be a field containing k. Here O is a choice of origin or base point on E. As we saw last time, we can endow $E(k)$ with a group structure: given $A, B \in E(k)$, we consider the third point of intersection C of the line $\overline{AB}$ with E. Then, we define $A \oplus B$ to be the third point of intersection of the line $\overline{OC}$ with E. From the construction, this group is clearly abelian.

In the special case where $k = \mathbb{C}$, we saw before that we can use elliptic functions to define an isomorphism $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, where Λ is a lattice in $\mathbb{C}$. In this case the group structure on $E(\mathbb{C})$ is isomorphic to that on the torus $\mathbb{C}/\Lambda$.

With more machinery, one way to see this is to just prove that the map $P \mapsto P - O$ is an isomorphism from $E(\mathbb{C}) \to \mathrm{Pic}^0(E)$, the group of degree 0 divisors (or line bundles) on E, and then identify $\mathrm{Pic}^0(E)$ with $\mathbb{C}/\Lambda$ using cohomology. This could be seen as one of the starting points of Hodge theory, or abelian varieties.

In this talk, we will attempt to study more of the structure of elliptic curves and their groups. At the risk of giving away the punchline, let's state Mordell's theorem.

Theorem 0.1 (Mordell 1922)**.** *Let E be an elliptic group over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is finitely generated.*

This theorem was subsequently generalized to algebraic number fields by Weil in 1930.

Since we also knew that $E(\mathbb{Q})$ was abelian, this theorem, combined with the classification of finitely-generated abelian groups, tells us that

$$E(\mathbb{Q}) \cong \mathbb{Z}^{\oplus r} \oplus \bigoplus_{i=1}^{n} \mathbb{Z}/p_i\mathbb{Z}^{r_i}.$$

However, the doesn't tell us anything about the rank r, or anything about the torsion subgroups. These turn out to be very interesting questions: interpreting the rank is the content

of the Birch and Swinnerton-Dyer conjecture (a Millenium prize problem). Meanwhile, descriptions of the torsion part of $E(\mathbb{Q})$ or even $E(\mathbb{C})$ will occupy the first part of the talk.

We can also interpret Mordell's theorem as telling us about the number of $\mathbb{Q}$-rational points of E; for example, if the rank $r = 0$, then E has only finitely many rational points. Similar questions about the number of rational points will be in the second part of the talk where we will discuss *Hasse's theorem*, which gives sharp bounds for the number of $\mathbb{F}_q$-rational points of an elliptic curve.

1 Torsion in Elliptic Curves over $\mathbb{Q}$

Let E be an elliptic curve defined over k, and let Ω be a field extension of k.

Definition 1.1. A point $P \in E(\Omega)$ is an *n-division point* of E if $nP = P \oplus \cdots \oplus P = 0$, where $\oplus$ is repeated n times.

Given $P \in E(\Omega)$, the least n for which P is an n-division point is its *order*.

Note that the set of n-division points forms a subgroup of $E(\Omega)$. When $k = \Omega = \mathbb{Q}$, the n-division points are precisely the corresponding n-torsion part of $E(\mathbb{Q})$.

Using Weierstrass forms and calculations, the book classifies the order 2 and 3 points for arbitrary fields $\bar{k}$ and shows that they are isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, respectively, if k is not characteristic 2, or characteristic 2 or 3.

Let us for now restrict to the case $k = \mathbb{Q}$ and $\Omega = \mathbb{C}$; we'll try to figure out which ones are $\mathbb{Q}$-rational later. Let $E[n](\mathbb{C})$ be the set of n-division points in $E(\mathbb{C})$. Then we can write $E(\mathbb{C}) = \mathbb{C}/\Lambda$, with Λ a lattice in $\mathbb{C}$. The n-division points of $E(\mathbb{C})$ are precisely those equivalence classes of $P \in \mathbb{C}$ such that $nP \in \Lambda$; in other words, the group $\frac{1}{n}\Lambda/\Lambda$. If we let ω_1, ω_2 be the generators of Λ, then

$$\frac{1}{n}\Lambda = \left\{ \frac{a_1}{n}\omega_1 + \frac{a_2}{n}\omega_2 \mid a_1, a_2 \in \mathbb{Z} \right\}$$

so

$$\frac{1}{n}\Lambda/\Lambda = \left\{ \frac{a_1}{n}\omega_1 + \frac{a_2}{n}\omega_2 \mid a_1, a_2 \in \mathbb{Z}/n\mathbb{Z} \right\}.$$

Thus, $E[n](\mathbb{C}) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Let us try to understand the number-theoretic properties of points in $E[n](\mathbb{C})$. Let $(x_1, y_1), \ldots, (x_m, y_m)$ denote the coordinates of the points in $E[n](\mathbb{C})$, and consider the field extension

$$K_n = \mathbb{Q}(x_1, y_1, \ldots, x_m, y_m)$$

over $\mathbb{Q}$.

Recall that an extension $L/\mathbb{Q}$ is Galois if L is algebraic and, and if for every $\sigma \in \mathrm{Aut}(\mathbb{C})$ we have $\sigma(L) \subset L$.

Theorem 1.2. *The extension K_n/Q is Galois.*

Proof. Let $\sigma \in \mathrm{Aut}(\mathbb{C})$. Since $\sigma|_{\mathbb{Q}} = \mathrm{Id}_{\mathbb{Q}}$ and E is defined over $\mathbb{Q}$, the automorphism σ respects the group law in $E(\mathbb{C})$ and so $n\sigma(P) = 0$ if $nP = 0$, i.e. $\sigma(E[n]) \subset E[n]$. From here, we know K_n is algebraic since then each $P \in E[n]$ can only have a finite number of conjugates under the action of $\mathrm{Aut}(\mathbb{C})$ (since $E[n]$ is finite), hence are algebraic. Also K_n is Galois since $\sigma(K_n) \subset K_n$. □

Now, consider the absolute Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Since all points of $E[n](\mathbb{C})$ are defined over $\overline{\mathbb{Q}}$, any $\sigma \in G_{\mathbb{Q}}$ permutes the points in $E[n](\mathbb{C}) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. This is a "free $\mathbb{Z}/n\mathbb{Z}$-module," or equivalently when n is prime a rank two vector space over $\mathbb{F}_p$. One can verify that the action of σ preserves the linear structure of $E[n]$ and the group structure of $G_{\mathbb{Q}}$. Therefore, we obtain a homomorphism

$$G_{\mathbb{Q}} \xrightarrow{\rho_n} GL_2(\mathbb{Z}/n\mathbb{Z}),$$

i.e. a representation of $E[n]$. We can also show that $\mathrm{Im}\,\rho_n \cong \mathrm{Gal}(K_n/\mathbb{Q})$, essentially by noting that ρ_n factors through $\mathrm{Gal}(K_n/\mathbb{Q})$ and unwrapping the definitions. Thus, we obtain a representation of the absolute Galois group, and in particular a representation of the Galois group $\mathrm{Gal}(K_n/\mathbb{Q})$!.

But when is ρ_n surjective, i.e. when $\mathrm{Gal}(K_n/\mathbb{Q})$ is isomorphic to $GL_2(\mathbb{Z}/n\mathbb{Z})$? It turns out this is quite rare.

Theorem 1.3 (Serre '72)**.** *Suppose additionally E is not isomorphic over $\overline{\mathbb{Q}}$ to any curve having complex multiplications. Then there exists an integer $N \geq 1$, depending only on E, such that for every integer n prime to N, the representation ρ_n is surjective.*

We'll define complex multiplications later on. For now, it suffices to say that most (almost all) elliptic curves do not have complex multiplications.

We end this section by mentioning the following (hard) theorem, telling us which of the points in $E[n](\mathbb{C})$ are actually rational.

Theorem 1.4 (Mazur)**.** *Let E be an elliptic curve over $\mathbb{Q}$.*

1. *If $E(\mathbb{Q})$ contains a point of order n, then $1 \leq n \leq 10$ or $n = 12$.*
2. *Equivalently, the torsion subgroup of $E(\mathbb{Q})$ is $\mathbb{Z}/m\mathbb{Z}$ with $1 \leq m \leq 10$, $m = 12$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ with $1 \leq m \leq 4$.*

In more specific cases, we can also use p-adic methods and the Weirstrass equation for an elliptic curve E to obtain restrictions on the torsion points.

2 Isogenies and Hasse's Theorem

We now turn to the problem of determining the number of rational points for an elliptic curve defined over $\mathbb{F}_q$, where $q = p^h$. Somewhat unsurprisingly, this can be done using the Frobenius automorphism $z \mapsto z^q$. To place this automorphism in a more general, useful framework, we define isogenies.

Definition 2.1 (Isogeny)**.** Let (E_1, O_1) and (E_2, O_2) be two elliptic curves over k. An *isogeny* $\varphi : E_1 \to E_2$ *over* k is a rational map from E_1 to E_2, defined over k, such that $\varphi(O_1) = O_2$.

Isogenies are the right notion of "morphism of elliptic curve." We clearly need to preserve the marked points to preserve the group structure.

Only requiring that isogenies be rational is not really significant, since rational maps between smooth curves are automatically morphisms over $\overline{k}$ (i.e. they are defined at every point). In fact, some algebraic geometry tells us that every morphism between curves is either constant or surjective. In fact, we have the following quite general correspondence:

Given a curve C over k, write $k(C)$ to be its *function field*, defined as the fraction field of the ring of regular functions on C. Then there is an equivalence

$$\{\text{Nonconstant rational maps between smooth curves } \varphi : C_1 \to C_2 \text{ over } \overline{k}\}$$
$$\updownarrow$$
$$\{\text{Field extensions } \varphi^*\overline{k}(C_2) \subset \overline{k}(C_1)\}$$

and we can think of these as ramified finite coverings of curves:

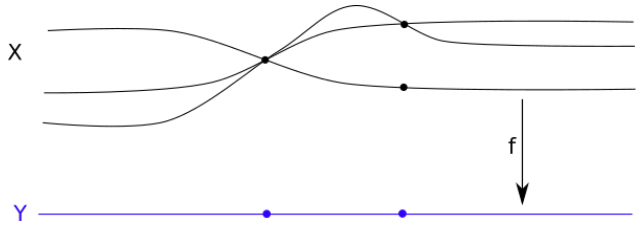

Figure 1: Picture of a morphism of curves from `https://en.wikipedia.org/wiki/Ramification_(mathematics)`

We'll use this correspondence of morphisms as field extensions below. Mainly, if C is an elliptic curve, then it can be written as $y^2 = f(x)$ where f is a cubic in x. So $k[C] = k[x, y]/(y^2 - f(x))$, and the function field $k(C)$ is $k(x, y)$ with these relations on x, y.

Isogenies induce homomorphisms of $E_1(\Omega) \to E_2(\Omega)$ for any extension Ω of k. Also note that two isogenies $\varphi, \psi : E_1 \to E_2$ can be added pointwise:

$$(\varphi + \psi)(P) := \varphi(P) \oplus \psi(P).$$

Example 2.2. Let $n \geq 0$ be an integer. We have the multiplication by n isogeny

$$[n] : P \mapsto nP.$$

Its kernel $E[n]$ consists of the n-torsion points studied before.

Example 2.3. Let E be defined over $\mathbb{F}_q$. Then the Frobenius endomorphism $\mathrm{Frob}_q : z \mapsto z^q$ on $\mathbb{F}_q$ induces an isogeny of E to itself. If Ω is an extension of k, then one can show that Frob_q preserves lines in $\mathbb{P}_2(\Omega)$, and hence Frob_q preserves the group law of $E(\Omega)$ when O is the origin, $O \in E(\mathbb{F}_q)$.

Example 2.4. Assume $\mathrm{char}\, k \neq 2$, and let

$$E_1 : y^2 - (x^3 + ax^2 + bx)$$
$$E_2 : y^2 - (x^3 - 2ax^2 + (a^2 2 - 4b)x)$$

with $2b(a^2 - 4b) \neq 0$. Then the map

$$\varphi : (x, y) \mapsto (\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2})$$

is an isogeny when we choose $(0, 1)$ as the basepoints on both curves. Indeed, one can verify its image is contained in E_2, and after homogenizing and multiplying by X^3 we can write φ as

$$[X : Y : Z] \mapsto [Y^2X : Y(Y^2 - aX^2 - 2bXZ) : (Y^2 - aX^2 - bXZ)Z].$$

to see that $\varphi[0 : 1 : 0] = [0 : 1 : 0]$. We can also write φ as

$$[X : Y : Z] \mapsto [Y(X^2 + aXZ + bZ^2) : (X^2 - bZ^2)(X^2 + aXZ + bZ^2) : XZ^2]$$

by homogenizing and multiplying by XY. This shows that the point $[0 : 0 : 1]$ also gets mapped to $O = [0 : 1 : 0]$, so $\ker \varphi$ has size at least two. Note that this gives an example of a map that is a priori not defined on all of E_1, but turns out to be a morphism!

An *endomorphism* of E over $\bar{k}$ is just an isogeny $E \to E$ over $\bar{k}$. We can compose endomorphisms as usual, and also add them using the addition of isogenies. Therefore, we obtain a *ring of endomorphisms* $\mathrm{End}_{\bar{k}}(E)$ of E over $\bar{k}$. One can verify that this is indeed a ring. The harder part is the distributivity of multiplication. While it is clear that

$$(\varphi + \psi) \circ \theta = \varphi \circ \theta + \psi \circ \theta,$$

the other direction

$$\theta \circ (\varphi + \psi) = \psi \circ \varphi + \theta \circ \psi$$

boils down to showing

$$\theta(\varphi(P) \oplus \psi(P)) = \theta \circ \varphi(P) \oplus \theta \circ \varphi(P)$$

for all $P \in E(\overline{k})$. This is follows from the fact that θ is a group homomorphism.

Fact. The ring $\mathrm{End}_{\overline{k}}(E)$ is an integral domain with unit Id_E, not necessarily commutative but of characteristic zero.

Example 2.5. We have a copy of $\mathbb{Z}$ in $\mathrm{End}_{\overline{k}}(E)$ given by multiplication by n, denoted $[n]$. Over $\mathbb{Q}$, we have in general (i.e. for almost all E) that $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \cong \mathbb{Z}$ generated by these $[n]$. However, there are 9 equivalence classes (over $\overline{\mathbb{Q}}$) of elliptic curves over $\mathbb{Q}$ such that $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ is larger than $\mathbb{Z}$; these extra endomorphisms are called *complex multiplications*. These special curves have lots of special properties, and their endomorphism rings are the rings of integers of the 9 principal quadratic imaginary fields.

The most useful properties of $\mathrm{End}_{\overline{k}}(E)$ (at least this talk) will be from defining the degree.

Definition 2.6. Let $\varphi : E_1 \to E_2$ be a isogeny over $\bar{k}$. The *degree* $\deg \varphi$ of φ is the degree of the corresponding field extension $\varphi^* \bar{k}(E_2) \subset \bar{k}(E_1)$. (It is 0 if φ is constant).

Key facts about the degree, which all essentially follow from the corresponding Galois theory for curves and their function fields, are below.

- If $\psi : E_2 \to E_3$ is another isogeny, then

$$\deg(\psi \circ \varphi) = \deg \psi \cdot \deg \varphi.$$

- If the field extension $\overline{k}(E_1)/\overline{k}(E_2)$ is separable, then

$$\deg(\varphi) = \#\operatorname{Ker} \varphi.$$

  Think of an n-sheeted cover. The group property actually lets us prove that φ doesn't have ramification, so the number of points in the preimage is constant.

Example 2.7. By the first part of the talk, we know that $\#\operatorname{Ker}[n] = n^2$.

Example 2.8. Let $E = y^2 - (x^3 + x)$ and $\varphi : (x, y) \mapsto (-x, iy)$. Let's see that φ is a complex multiplication for E. We know $\varphi \in \mathrm{End}_{\mathbb{Q}(i)}(E) \subset \mathrm{End}_{\overline{\mathbb{Q}}}(E)$ and clearly $\varphi \neq \pm\mathrm{Id}$. If φ was in the image of $\mathbb{Z}$, then we would have $\varphi = [n]$ for some n and so $\#\operatorname{Ker} \varphi = n^2$. However, clearly $\#\operatorname{Ker} \varphi = 1$ so $n = \pm 1$. We know this is impossible, so φ is a complex multiplication. Since $\varphi^2 = -\mathrm{Id}$, we have $\varphi = \pm i$ and one can show that $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \cong \mathbb{Z}[i]$.

The big fact that will let us prove Hasse's theorem is the following.

Fact. The map $\deg : \mathrm{End}_{\bar{k}}(E) \to \mathbb{Z}$ is positive-semidefinite quadratic form. In particular, the inequality

$$|\deg(\psi - \varphi) - \deg \varphi - \deg \psi| \leq 2\sqrt{\deg \psi \deg \varphi} \qquad (*)$$

holds. This is proven by minimizing a quadratic equation, similar to proofs of Cauchy-Schwartz.

We can now prove Hasse's theorem.

Theorem 2.9 (Hasse 1941)**.** *Let E be an elliptic curve over $\mathbb{F}_q$. Then*

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

Note that $q + 1 = \#\mathbb{P}_1(\mathbb{F}_q)$.

Proof of Hasse's Theorem. Let $\overline{\mathbb{F}}_q(E) = \overline{\mathbb{F}}_q(x, y)$ be the funcion field of E, where x, y are coordinate functions satisfying $y^2 = f(x)$, where f a cubic polynomial. Let φ be the Frobenius endomorphism

$$(x, y) \mapsto (x^q, y^q)$$

which sends $O \mapsto O$ and hence is an isogeny. The field $\mathbb{F}_q$ is precisely the fixed points of φ on $\overline{\mathbb{F}}_q$, i.e. the $z \in \mathbb{F}_q$ with $z^q = z$. Equivalently, this is the kernel of $\mathrm{Frob}_q - \mathrm{Id}$. Assuming that $\varphi - \mathrm{Id}$ is separable, we then have

$$E(\mathbb{F}_q) = \#\operatorname{Ker}(\varphi - \mathrm{Id}) = \deg(\varphi - \mathrm{Id}).$$

Now $\deg \mathrm{Id} = 1$. In view of the inequality $(*)$, to prove Hasse's theorem it suffices to prove that $\deg \varphi = q$.

For simplicity we assume the characteristic $p > 2$ (but the proof can be extended to $p = 2$). Then by definition of the degree,

$$\deg \varphi = [\overline{\mathbb{F}}_q(x, y) : \overline{\mathbb{F}}_q(x^q, y^q)] = [\overline{\mathbb{F}}_q(x, y) : \overline{\mathbb{F}}_q(x, y^q)][\overline{\mathbb{F}}_q(x, y^q) : \overline{\mathbb{F}}_q(x^q, y^q)].$$

The first term on the left hand side equals 1, since y satisfies the quadratic equation $y^2 = f(x)$ and so the degree of y over $\overline{\mathbb{F}}_q(x, y^q)$ must divide both 2 and q, hence equals 1 since $p > 2$. The second factor then must equal q, since x satisfies no lower-order relations. This concludes the proof. □

Theorem 2.10. *If two elliptic curves E_1, E_2 over $\mathbb{F}_q$ have a non-constant isogeny $\theta : E_1 \to E_2$ between them, then $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.*

The crucial point is that θ is defined over $\mathbb{F}_q$, hence "commutes" with Frobenius (since it's constant on $\mathbb{F}_q$).

Proof. Let φ_1, φ_2 be the corresponding Frobenius endomorphisms. Then $\#\mathbb{E}_i(\mathbb{F}_q) = \deg(\varphi_i - \mathrm{Id})$. Since θ is defined over $\mathbb{F}_q$, we have the commutative diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{\varphi_1} & E_1 \\ \downarrow{\scriptstyle\theta} & & \downarrow{\scriptstyle\theta} \\ E_2 & \xrightarrow[\varphi_2]{} & E_2 \end{array}$$

and so also the commutative diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{\varphi_1 - \mathrm{Id}} & E_1 \\ \Big\downarrow{\scriptstyle \theta} & & \Big\downarrow{\scriptstyle \theta} \\ E_2 & \xrightarrow[\varphi_2 - \mathrm{Id}]{} & E_2 \end{array}$$

Since the degree is multiplicative,

$$\deg\theta \cdot \deg(\varphi_1 - \mathrm{Id}) = \deg(\varphi_2 - \mathrm{Id}) \cdot \deg\theta$$

and since $\deg\theta \neq 0$ we see that

$$\deg(\varphi_1 - \mathrm{Id}) = \deg(\varphi_2 - \mathrm{Id}).$$

□

Example 2.11. Recall that we had constructed an isogeny between the curves

$$E_1 : y^2 - (x^3 + ax^2 + bx)$$
$$E_2 : y^2 - (x^3 - 2ax^2 + (a^2 2 - 4b)x)$$

with $a, b \in \mathbb{F}_q$ and $2b(a^2 - 4b) \neq 0$ (when $\mathrm{char}\, neq 2$). By the theorem $E_1(\mathbb{F}_q) = E_2(\mathbb{F}_q)$.

Example 2.12. Consider the curves over $\mathbb{F}_3$

$$E_1 : y^2 - (x^3 - x + 1) \tag{1}$$
$$E_2 : y^2 - (x^3 - x - 1). \tag{2}$$

These are isomorphic over $\mathbb{F}_9$, but $\#E_1(\mathbb{F}_3) = 7$ and $\#E_2(\mathbb{F}_3) = 1$, so they are not isomorphic over $\mathbb{F}_3$.