ELLIPTIC CURVES

Contents

These notes are from a course taught by Professor Bao Le Hung at Nortwestern University during the winter quarter of the 20/21 academic year. The note taker is responsible for any mistakes or inaccuracies that occur.

1. Lecture 1 (Monday 1/11)

This is a topics class about **elliptic curves**. The goal of today is to give an overview.

A quick and concrete definition:

Definition 1. Let k be a field. An *elliptic curve* E/k is a smooth projective plane cubic determined by an affine equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

where $a_i \in k$, i. e. E is the closure of this affine curve in $\mathbb{P}^2$, *and* the data of a rational point $0 \in E(k)$.

In other words, if $\mathbb{P}^2$ has homogeneous coordinates $[X : Y : Z]$, then E is the curve in $\mathbb{P}^2$ determined by the equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

For this to be *smooth*, there is a condition $\Delta(a_1, a_2, \dots) \neq 0$, where Δ is a polynomial in the a_i. (The precise formula can be found in Silverman.) In the case where the equation is

$$y^2 = x^3 + ax + b, \tag{2}$$

we have $\Delta(a, b) = -4a^3 - 27b^2$. By the way, Equation 1 is called the *Weierstrass equation*, and Equation 2 is called the *short Weierstrass equation*.

1.1. Why study elliptic curves?

Firstly, the plane cubics in $\mathbb{P}^2$ are exactly the smooth projective genus 1 curves. Being genus 1 is between being genus 0, i. e. $\mathbb{P}^1$, and of genus > 1, of "general type". In the theory of curves, there is a trichotomy where the geometry behaves very differently based on whether the genus is 0, 1, or higher than 1.

Secondly, an elliptic curve is exactly a proper group variety of dimension 1. There is a multiplication map $m\colon E \times E \to E$, and inversion map $\mathrm{inv}\colon E \to E$, and an identity map $0\colon \operatorname{Spec} k \to E$, satisfying a bunch of commutative diagrams. The point is that these maps are algebraic maps.

Being a proper group variety means that we have direct access to cohomological invariants of E. For example the *Tate module*. The interaction between the group structure and algebraic variety structure implies many things.

Themes:

(1) Study nature of the abelian group $E(k)$. (We will see later on that *abelian* is a formal consequence of being proper.)
(2) See how cohomological invariant control $E(k)$. More or less everything you want to know about $E(k)$ will be controlled by cohomological invariants, namely the Tate module.

1.2. **Examples.**

(1) $k = \mathbb{C}$. In this case, $E/\mathbb{C}$ is a compact Riemann surface of genus 1. By the uniformization, a genus 1 Riemann surface has universal cover $\mathbb{C}$, hence $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, where $\Lambda \subseteq \mathbb{C}^2$ is a lattice. These are all complex tori. It turns out that the isomorphism $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ can be made to respect the group structure.

More canonically, $\Lambda \cong \pi_1(E(\mathbb{C}), 0) = H_1(E(\mathbb{C}), \mathbb{Z})$. We can understand $\mathbb{C}$ as the Lie algebra of E, and the exponential map $\mathrm{Lie}(E) \to E(\mathbb{C})$ corresponds to the quotient map $\mathbb{C} \to \mathbb{C}/\Lambda$. We have $\mathrm{Lie}(E) = T_0E(\mathbb{C}) = \{\text{invariant global vector fields on } E(\mathbb{C}\} = H^0\left(E(\mathbb{C}), \Omega^1\right)^*$.

Note that the isomorphism $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ is complex analytic, and the x, y that show up in the Weierstrass equation correspond to some doubly periodic meromorphic functions on $\mathbb{C}$. These are so-called *elliptic functions*.

The n-torsion $E[n](\mathbb{C}) \cong \frac{1}{n}\Lambda/\Lambda \cong \mathbb{Z}/n \times \mathbb{Z}/n$. For a prime p, *Tate module* T_pE is defined as

$$T_p(E) = \varprojlim_{\times p} E[p^k](\mathbb{C}) = \varprojlim \left(E[p] \leftarrow E[p^2] \leftarrow \cdots\right).$$

Canonically, in this case

$$T_pE = \varprojlim \frac{1}{p^k}\Lambda/\Lambda = \varprojlim_{\text{projection}} \Lambda/p^k\Lambda = \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_p = H_1(E(\mathbb{C}), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p,$$

the p-adic completion of $\Lambda = H_1(E(\mathbb{C}), \mathbb{Z})$.

For the first theme, we have seen that $E(\mathbb{C})$ is an divisible uncountable abelian group. For the second, E is completely determined by the pair $(\mathrm{Lie}\, E, H_1(E, \mathbb{Z})) = \left(H^0\left(E, \Omega^1\right)^*, H_1(E, \mathbb{Z})\right)$. Here, $H_1(E, \mathbb{Z})$ is a free $\mathbb{Z}$-module, and $H^0\left(E, \Omega^1\right)^*$ is a line in $H_1(E, \mathbb{Z})^* \otimes_{\mathbb{Z}} \mathbb{C}$. This is the data of a *Hodge structure* of weight -1. The interesting fact here is that a nonlinear thing like E is determined by just linear algebrac data that can be extracted from E by cohomological data.

(2) $k = \mathbb{F}_q$ a finite field. Now $E(\mathbb{F}_q)$ is a finite abelian group. A basic fact is that if $a = q+1-\#E(\mathbb{F}_q)$, then $|a| \leq 2\sqrt{q}$. This is known as the *Hasse bound*. We have a double cover

$$E \to \mathbb{P}^1$$
$$(x, y) \mapsto x$$

which should mean that the number of rational points of E is roughly the same as the number of points of $\mathbb{P}^1$, which is $q + 1$. The discrepancy is of order $\sqrt{q}$, and the heuristic is that the Hasse bound is as if $\#E(\mathbb{F}_q)$ is "random" (subject to some natural constraints).

How do the cohomological invariants come into play? We don't have singular cohomology, but we do have the Tate module $T_l(E)$, where $l \neq p = \mathrm{char}\, q$. It is defined as

$$T_lE = \varprojlim E[l^n](\overline{\mathbb{F}_q}).$$

There are two important facts about this Tate module. The first is that $E[l^n]\left(\overline{\mathbb{F}_q}\right) \cong \mathbb{Z}/l^n \times \mathbb{Z}/l^n$ as in the complex case, and consequently $T_lE \cong \mathbb{Z}_l^2$. The second is that T_lE has a natural action of $\mathrm{Gal}\left(\overline{\mathbb{F}_q}/\mathbb{F}_q\right)$. This Galois group is simple, namely procyclic $\cong \hat{\mathbb{Z}}$, as topologically it is generated by the Frobenius Frob_q. In sum, T_lE is a free $\mathbb{Z}_l$-module of rank two with an action of Frob_q. The meaning of a from before is that $a = \mathrm{tr}\,\mathrm{Frob}_q$. (Note that this does not hold for $l = p$.)

In the general context, for algebraic varieties over finite fields you don't have singular cohomology, but you do have l-adic or étale cohomology. Secretly, $T_lE \cong H_1\left(E/\overline{\mathbb{F}_q}, \mathbb{Z}_l\right)$, the l-adic homology of E. One advantage of working with the Tate module is that it is elementaryto define, whereas defining l-adic cohomology is rather complicated.

In the finite field case, E is almost recovered from the action of Frob_q on T_lE. The problem is the choice of l: If you know this action for all l, even $l = p$, then you can indeed recover E. Compared to the complex case, we only work with homology and we have no Hodge structure. However, we do have an action of the Galois group as a substitute for the Hodge structure. This is a recurring theme.

(3) k a local field, i. e. a finite extension of $\mathbb{Q}_p$. Let's stick with $k = \mathbb{Q}_p$ for simplicity, but this will not impact the results. Now $E(\mathbb{Q}_p)$ is a p-adic manifold, i. e. has charts that are isomorphic to p-adic balls $\mathbb{Z}_p$, and in fact a p-adic Lie groups. One feature of $\mathbb{Q}_p$ is the existence of a good integral structure: There is a maximal compact subring $\mathbb{Z}_p \subseteq \mathbb{Q}_p$, and one can comtemplate if there are integral models $\mathcal{E}/\mathbb{Z}_p$ for $E/\mathbb{Q}_p$. We can obtain one such integral model cheaply by clearing denominators in a Weierstrass equation, but it is a subtle question to get the "optimal" one, and this is given by the Néron model. The source of the subtlety is that if $\mathcal{E}$ is proper, then $\mathcal{E}(\mathbb{Z}_p) = E(\mathbb{Q}_p)$, but $\mathcal{E}$ may not have a group structure. It may be impossible for $\mathcal{E}$ to be proper and have a group structure at the same time, but the Néron model $\mathcal{E}$ has a group structure and still satisfies $\mathcal{E}(\mathbb{Z}_p) = E(\mathbb{Q}_p)$. If E has *good reduction* we can take $\mathcal{E}$ to be proper and have a group structure. This implies that we have an exact sequence

$$0 \to \underbrace{\hat{\mathcal{E}}(\mathbb{Z}_p)}_{\text{formal group}} \to E(\mathbb{Q}_p) = \mathcal{E}(\mathbb{Z}_p) \to \underbrace{\mathcal{E}(\mathbb{F}_p)}_{\text{finite group}} \to 0.$$

The formal group on the left, whatever it is, is a pro-p-group.

Insert picture

Spec $\mathbb{Z}_p$ has two points, namely the generic point Spec $\mathbb{Q}_p$ and Spec $\mathbb{F}_p$. The elliptic curve E lives over Spec $\mathbb{Q}_p$, and the integral model $\mathcal{E}$ is a way too expand E over the other point Spec $\mathbb{F}_p$. Any point of $E(\mathbb{Q}_p)$ then corresponds to a "section" Spec $\mathbb{Z}_p \to \mathcal{E}$, which specializes to a point $\mathcal{E}(\mathbb{F}_p)$. We can interpret the exact sequence as decomposing $E(\mathbb{Q}_p)$ into p-adic balls.

The Tate module $T_l E$, which is defined as before, has an action of Gal $\left(\overline{\mathbb{Q}_p}/\mathbb{Q}_p\right)$, a much more complicated Galois group than in the case of finite fields. The Tate module with the Galois action does not quite determine E as strongly as in the case of finite fields, however it does determine many things about $\mathcal{E}$. In particular, it can recognize when E has good reduction. This is the criterion of *Néron-Ogg-Shafarevich.*

(4) k is a number field, i. e. a finite extension of $\mathbb{Q}$, and let us for simplicity consider the case $k = \mathbb{Q}$.

Theorem 2 (Mordell-Weil)**.** *$E(\mathbb{Q})$ is a finitely generated abelian group.*

In other words, $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$. The number r is the *rank* of E.

Remark 3. Let $C/\mathbb{Q}$ be a smooth projective curve of genus g. If $g = 0$, then $C(\mathbb{Q})$ is either ∞ or $\emptyset$. If $g > 1$, then $C(\mathbb{Q})$ is finite by Faltings' Theorem. If $g = 1$, then $C(\mathbb{Q})$ can be $\emptyset$, finite, or infinite.

Computing $E(\mathbb{Q})$ is interesting from an arithmetic point of view. As an example, take the *congruent number problem*: An integer $n \in \mathbb{Z}$ that is square-free is a *congruent number* if there is a triple $a, b, c \in \mathbb{Q}$ with $a^2 + b^2 = c^2$ and $n = \frac{1}{2}ab$, or in geometric terms a right-angled triangle with rational sides a, b, c and area n. Equivalently, we can ask about an arithmetic progression α^2, $\beta^2 = \alpha^2 + n$, $\gamma^2 = \beta^2 + n$. For example, $n = 1$ is not congruent, as shown by Fermat. On the other hand $n = 5$ is congruent, because we can take $a = \frac{20}{3}$, $b = \frac{3}{2}$.

Proposition 4. *Let E_n be the elliptic curve given by $y^2 = x^3 - n^2 x$. Then n is a congruent number if and only if* rank $E_n(\mathbb{Q}) > 0$*, i. e. if and only if $E_n(\mathbb{Q})$ is infinite.*

Explanation. If (x, y) is a rational point on E, then $a = \frac{x^2 - n^2}{y}$, $b = 2n\frac{x}{y}$, $c = \frac{x^2 + n^2}{y}$ realizes n as a congruent number. This gives a bijection between triples (a, b, c) realizing n as a congruent number and $(x, y) \in E(\mathbb{Q})$ such that $y \neq 0$. To prove the proposition, we check that $E_n(\mathbb{Q})_{\text{tors}} \subseteq \{y = 0\}$, which strongly uses the exact sequence from before.

How does $T_l E$ control $E(\mathbb{Q})$? The function

$$L(E, s) = \prod_{p \text{ prime of good reduction}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \prod_{p \text{ prime of bad reduction}} (\cdots),$$

where $a_p = p + 1 - \#E(\mathbb{F}_p)$. assembles all possible point counts of E modulo p.

Conjecture 5 (Birch-Swinnerton-Dyer)**.** *$L(E, s)$ has holomorphic continuation to all $s \in \mathbb{C}$, and* $\operatorname{ord}_{s=1} L(E, s) = \operatorname{rank} E$.

For the congruent number problem, $L(E, s)$ is "easy" and there exists an explicit formula for $L(E, 1)$ involving some ternary quadratic forms.