Elliptic Curves

Contents

Introduction

Resources

These are some notes (in progress) on elliptic curves that I've combined from various sources, including the following classes:

1. Andrew Sutherland's course at MIT (18.783) from spring 2012 http://co.mit.edu/18.783 (parts of these notes are from notes scribed by students in the class and edited by Sutherland),

2. a reading course with Sug Woo Shin at MIT on class field theory and complex multiplication, and

3. Tom Fisher's course at the University of Cambridge from autumn 2013 (lecture notes at https://dl.dropboxusercontent.com/u/27883775/math%20notes/part_iii_elliptic.pdf; alternate version at http://www.pancratz.org/notes/Elliptic.pdf).

I will draw heavily on the following books:

1. Silverman, The arithmetic of elliptic cuves **??**.

2. Silverman, Advanced topics in the arithmetic of elliptic curves, by Silverman **??**.

3. Washington, Elliptic curves and cryptography **??**.

4. Cox, Primes of the form $x^2 + ny^2$ **??**.

I would also like to put in material such as from the following:

1. Silverman and Hindry, Diophantine Geometry: An Introduction **??**.

2. Koblitz, Elliptic Curves and Modular Forms **??**.

3. Lang, Elliptic functions **??**.

4. Diamond and Shurman, A First Course in Modular Forms **??**.

Using these notes

I eventually want these to be a complete set of notes, but for the time being, see it more as a "reading guide" or "road map," to be used as a supplement to textbooks or course material.

When you see things like "ADD a discussion on ...", take this as a sign that you should be able to discuss the topic in your studies on elliptic curves.

I would like the prerequisites for these notes to be minimal. However, I will assume familiarity with basic things such as exact sequences and equivalence of categories that make many theorems much more compact to state. Currently, I will have to refer a reader elsewhere for the basics of algebraic geometry.

Philosophy

(I.e., what I'd like to do differently from texts already out there.) In these notes I would like to focus on...

1. intuition. How to talk about the material in a non-rigorous way? A strong way of building intuition is connecting to previous topics, even if the analogies are imperfect. I also hope to add in discussion of big-picture questions such as "why does geometry matter for arithmetic questions?" and "what the heck do elliptic curves have to do with modular forms?" As a result, take everything outside of formal statements of theorems and proofs with a grain of salt.

2. motivations, and connections. How would someone come up with the statements or proofs? How are different subtopics related to one another?

3. summaries and "index-carding." What is the most compact way you can remember the topics? What is the big-picture?

4. road maps. For topics where I do not have notes for yet, what resources are out there? What is the big picture?

5. problem-solving based learning. Have problems before theorems to get the reader thinking, and possibly derive some of the ideas of the theorems on his/her own.

6. fun problems. Stray away from the core material occasionally.

7. algorithms. Elliptic curves is a very computational subject, so it is helpful to learn how to program algorithms involving EC. I'll try to include SAGE code with comments. (For more on SAGE, see **??**.)

Collaboration

Send me any comments or corrections at holdenlee@alum.mit.edu. In particular, let me know if you'd like to collaborate on these notes.

Chapter 1

Conics

Before we study elliptic curves, we gain some geometric experience by studying some more basic curves: conics, which are defined by quadratic equations. We'll see that we can understand all conics, and that they are basically the same geometrically.

First, we'll consider a common equation: the Pythagorean equations.

1 Pythagorean triples

Definition: A **Pythagorean triple** is a triple of integers (a, b, c) that are the side lengths of a right triangle. Here a and b are lengths of the two legs and c is the length of the hypotenuse.

A **primitive Pythagorean triple** is a Pythagorean triple (a, b, c) where the greatest common divisor of a, b, and c is 1.

1.1 Number theoretic solution

Theorem 1.1.1. *Any Pythagorean has the form*

$$a = (m^2 - n^2)k,\ b = 2mnk,\ c = (m^2 + n^2)k$$

$$a = 2mnk,\ b = (m^2 - n^2)k,\ c = (m^2 + n^2)k,$$

where

1. $\gcd(m, n) = 1,\ \gcd(x, y) = k.$
2. *m, n are of different parity.*
3. $m > n > 0,\ k > 0.$

Proof. Idea: Rewrite as $a^2 = c^2 - b^2 = (c-b)(c+b)$. Assume a, b, c have no common factor, so $c-b, c+b$ have no common factor except possibly 2; they must each be a square or 2 times a square. □

1.2 Geometric solution

We now explore a more geometric way of finding all Pythagorean triples.

Problem 1.1.2:

1. We can reduce the problem of finding all primitive Pythagorean triples to finding all right triangles whose hypotenuse is 1 and whose legs are rational numbers. Why?
2. We want to find all rational points on the circle $x^2 + y^2 = 1$. Let's consider a vertical line ℓ going through the origin. Let A be the point $(-1, 0)$, and B be any other rational point on $x^2+y^2 = 1$. What can you say about the intersection of $\overline{AB}$ with ℓ?
3. Now suppose we have a rational point on ℓ, $(0, z)$. Let B be the second intersection of the line going through A and $(0, z)$ with the circle. Find the coordinates of B. What can you say about B?
4. You have now found all rational points on the circle $x^2 + y^2 = 1$. Why? Now use this to find all Pythagorean triples.

1. Given a Pythagorean triple, we can find a right triangle with rational legs and hypotenuse 1 by dividing all lengths by the hypotenuse:

$$(a,\ b,\ c) \mapsto \left(\frac{a}{c},\ \frac{b}{c},\ 1\right)$$

   If we're given a right triangle with rational legs and hypotenuse 1, we can get a primitive Pythagorean triple by multiplying through by the least common denominator. This is the unique primitive triple that's a multiple of the original lengths.

   These two operations are inverse to each other.

   If we place the right triangle with hypotenuse 1 at the origin, its other vertex is on the circle $x^2 + y^2 = 1$. Indeed, this is just the Pythagorean formula.

   So we've reduced the problem of finding all Pythagorean triples to **finding all rational points on** $x^2 + y^2 = 1$. (We just need the points in the first quadrant.)

2. The line going through 2 points with rational coordinates will be of the form $y = mx+b$, with m and b both rational. Indeed, the line going through $(-1, 0)$ and (r, s) is

$$y = \frac{s}{r+1}(x+1) = \frac{s}{r+1}x + \frac{s}{r+1}.$$

   This means its intersection with ℓ is also rational: $(0, b) = \left(0, \frac{s}{r+1}\right)$.

3. Now we're going the other way, drawing the line through a point on ℓ and looking at its intersection with the circle. The line going through $(-1, 0)$ and $(1, z)$ has equation

$$y = z(x + 1).$$

We substitute this into the equation for the circle $x^2 + y^2 = 1$ and get

$$\begin{aligned} x^2 + [z(x+1)]^2 &= 1 \\ x^2 + z^2(x+1)^2 - 1 &= 0 \\ (1+z^2)x^2 + 2z^2x + (z^2 - 1) &= 0. \end{aligned}$$

This looks like a rather nasty quadratic. But before we pull out the quadratic formula to solve for x, note that this equation represents the intersection points of the line with the circle, and we already know one intersection point – it is $(-1, 0)$, when $x = -1$. The sum of the roots is $-\frac{2z^1}{1+z^2}$ so the other solution is

$$-\frac{2z^1}{1+z^2} - (-1) = \frac{1-z^2}{1+z^2}.$$

Then

$$y = z(x+1) = z\left(\frac{1-z^2}{1+z^2} + 1\right) = \frac{2z}{1+z^2}.$$

The second intersection is

$$\left(\frac{1-z^2}{1+z^2}, \frac{2z}{1+z^2}\right).$$

In particular, since z is rational, it is rational!

4. We've established a 1-to-1 correspondence between rational points on ℓ and rational points on the circle (excluding the point $(-1, 0)$).

Now we simply have to go from rational points on the circle back to Pythagorean triples, as we said in step 1. Write $z = \frac{m}{n}$ is lowest terms. We have a right triangle with legs

$$\left(\frac{1 - \left(\frac{m}{n}\right)^2}{1 + z\left(\frac{m}{n}\right)^2}, \frac{\frac{m}{n}}{1 + \left(\frac{m}{n}\right)^2}, 1\right) = \left(\frac{n^2 - m^2}{n^2 + m^2}, \frac{2mn}{m^2 + n^2}, 1\right).$$

Multiplying through by the denominator $m^2 + n^2$, we get

$$\left(\frac{1 - \left(\frac{m}{n}\right)^2}{1 + z\left(\frac{m}{n}\right)^2}, \frac{\frac{m}{n}}{1 + \left(\frac{m}{n}\right)^2}, 1\right) = \left(n^2 - m^2, 2mn, n^2 + m^2\right).$$

Note this is a primitive Pythagorean triple because the greatest common divisor divides $(n^2 + m^2) - (n^2 - m^2) = 2m^2$ and $2mn$.

2 General conics

For general conics, we can do something similar.

3 Group law

See http://www.quora.com/Elliptic-Curves/Why-is-there-a-group-law-on-an-elli

Problem 1.3.1: Suppose you are given two Pythagorean triples (a_1, b_1, c_1) and (a_2, b_2, c_2). Produce (in a nontrivial way) a Pythagorean triple (a, b, c) with $c = c_1 c_2$?

4 Hasse-Minkowski

(It's good to know about how the local-to-global principle works before seeing how it fails in the case of elliptic curves!)

5 Summary

You should now be able to find all solutions to any conic over $\mathbb{Q}$ (or prove that it has no solutions).

Chapter 2

Introduction to algebraic geometry

We introduce some algebraic geometry that we'll need.

We'll cover the following.

1. Varieties (affine and projective), morphisms, and rational maps: Define the basic objects we study in algebraic geometry and maps between them.

2. Curves: Understand the equivalence of categories between curves and certain field extensions. Talk about degree and ramification of maps between curves.

3. Divisors

4. Differentials

5. Genus, and the Riemann-Roch Theorem

We assume the reader can do the following. See Silverman [2][Chapter I-II].

- Define affine variety; understand the relationship between ideals of a polynomial ring and varieties.

- Define projective variety, and how the above relationship is modified in this case. Why do we study projective rather than affine varieties?

- Understand the local ring at a point.

- Define dimension and smoothness. (What are the two definitions of smoothness, and when are they equivalent?)

- Understand "field of definition" and Galois action.

- Define morphism and rational map.

- Optional: understand all the above in terms of schemes.

1 Varieties

1.1 Affine varieties

1.2 Projective varieties

1.3 Morphisms and rational maps

2 Curves

Definition 2.2.1: A **curve** is a projective variety of dimension 1.

2.1 Curves correspond to field extensions

Our main result is the following.

Theorem 2.2.2. *There is an contravariant equivalence of categories between the following.*

1. *Objects: Smooth curves defined over K*

   Maps: Non-constant rational maps defined over K

2. *Extensions L/K of transendence degree 1 and $LK = K$.*

   Maps: field injections fixing K.

The equivalence is given by sending C/K to $K(C)$ and $\phi : C_1 \to C_2$ to $\phi^* : K(C_2) \hookrightarrow K(C_1)$ with $\phi^* f = f \circ \phi$.

$$\begin{array}{ccc} C_1/K & \xrightarrow{\phi} & C_2/K \\ \vdots & & \vdots \\ K(C_1) & \xleftarrow[\phi^*]{} & K(C_2) \end{array}$$

$$f \circ \phi \longleftarrow\!\shortmid f.$$

Why do we consider functions and divisors on curves? There are two good motivations, depending on your background:

1. Algebraic number theory: Let K be a number field. We know the following.

   (a) Primes: K has a set of primes. Call it $\operatorname{Spec} \mathscr{O}_K = \{\mathfrak{p} \text{ prime in } K\}$.

   (b) Unique factorization: Each fractional ideal $\mathfrak{a}$ in K has a unique factorization. In other words, we can think of the elements of K as functions from $\operatorname{Spec} \mathscr{O}_K$ to $\mathbb{Z}$

that are zero almost everywhere; the function gives the orders with respect to various primes.

i. Discrete valuation: When we localize at $\mathfrak{p}$, we get a local field $K_\mathfrak{p}$, which has a **discrete valuation** $\mathrm{ord}_\mathfrak{p}$.

(c) Class group: K has finite **class group** Cl_K. In other words, the factorizations of elements of $K^\times$ is cofinite in the group of all possible factorizations (of ideals),

$$1 \to \mathscr{O}_K^\times \to K^\times \to \mathrm{Id}_K \to \mathrm{Cl}_K \to 0. \tag{2.1}$$

(d) Field extensions: Three kinds of behavior can result. Namely, a prime can split, remain inert, and ramify. We can define **ramification** indices, and find they multiply when we have field extensions K/L and M/K.

2. Riemann manifolds:

(We often say algebraic number theory is "algebraic geometry in dimension 0." For more information, look up Arakelov geometry.) Because each curve has an associated field extension, it makes sense to consider analogues of the above concepts. A curve in has some associated function field $\overline{K}(C)$, and the elements here are *actually* functions; we can define discrete valuations when we localize at a point. (Note we have to be careful with the analogy because we're dealing with *projective* curves; geometry is really necessary here.)

(Todo: make more precise. See chapter 3 of Ravi Vakil's Algebraic geometry [4].)

Here's a partial dictionary.

$$\begin{aligned} \{\text{prime ideals of } K\} &\leftrightarrow \{\text{points of } C\} \\ \mathrm{Id}_K &\leftrightarrow \mathrm{Div}(C) \\ \mathrm{Cl}_K &\leftrightarrow \mathrm{Pic}(C) \\ e_{L/K} &\leftrightarrow e_\phi(C) \end{aligned}$$

Proposition 2.2.3: Let C be a curve and $P \in C$ a smooth point. Then $\overline{K}[C]_P$ is a discrete valuation ring.

Thus for each P, we have a discrete valuation $\mathrm{ord}_P : K(C)^* \twoheadrightarrow \mathbb{Z}$:

1. $\mathrm{ord}_P(f_1 f_2) = \mathrm{ord}_P(f_1)\,\mathrm{ord}_P(f_2)$.

2. $\mathrm{ord}_P(f_1 + f_2) \geq \min(\mathrm{ord}_P(f_1), \mathrm{ord}_P(f_2))$.

Definition 2.2.4: $t \in K(C)$ is a **uniformizer** at P if $\mathrm{ord}_P(t) = 1$.

Because $\overline{K}[C]_P$ is a DVR, once we've found a uniformizer at P, we can then write functions as power series in the uniformizer.

2.2 Divisors and the Picard group

Definition 2.2.5: A **divisor** is a formal sum of points on C,

$$D = \sum_{P \in C} n_P P$$

with $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many P.

1. Define the **degree**
$$\deg D = \sum_{P \in C} n_P.$$
2. D is **effective** (written $D \geq 0$) if $n_P \geq 0$ for all P.
3. If $f \in K(C)^\times$ then define
$$\operatorname{div}(f) := \sum_{P \in C} \operatorname{ord}_P(f) P.$$

You can think of divisors as functions from the points of C to $\mathbb{Z}$, just like fractional ideals in K were functions from the primes of K to $\mathbb{Z}$. With this analogy, effective divisors correspond to proper ideals (as opposed to fractional ideals), and the map div corresponds to the map $K^\times \to \mathrm{Id}_K$.

One important fact is that $\operatorname{div}(f)$ always has degree 0. (We don't have this behavior for K; this nice fact comes from the fact that we're working with projective varieties. Rational functions have the same number of zeros as poles, so have degree 0; this count only works if we think about the point at infinity.)

We will define $\operatorname{Div}(C)$ similar to Cl_K.

Definition 2.2.6: Divisors $D_1, D_2 \in \operatorname{Div}(C)$ are **linearly equivalent** (written $D_1 \sim D_2$) if there exists $f \in \overline{K}(C)^\times$ with $\operatorname{div}(f) = D_1 - D_2$. Write

$$[D] = \{D' \in \operatorname{Div}(C) : D' \sim D\}.$$

Define the **Picard group**

$$\operatorname{Pic}(C) = \frac{\operatorname{Div}(C)}{\sim}$$
$$\operatorname{Pic}^0(C) = \frac{\operatorname{Div}^0(C)}{\sim}.$$

where $\operatorname{Div}^0(C)$ is the group of divisors on E of degree 0.

We summarize the main result similar to (2.1).

Proposition 2.2.7: There is an exact sequence

$$1 \to \overline{K}^\times \to \overline{K}(C)^\times \xrightarrow{\text{div}} \operatorname{Div}^0(C) \to \operatorname{Pic}^0(C) \to 1.$$

Proof. We need to check that

1. $\deg(\mathrm{div}(f)) = 0$. See the proof after Proposition 2.2.11.
2. If $\mathrm{div}(f) = 0$, then $f \in \overline{K}^\times$.

□

Projectivity is essential for both these statements.

2.3 Maps are like field extensions

Using the fact that a morphism of curves corresponds to a field extension (see Theorem 2.2.2), we can take notions that apply to field extensinos (degree, separability, ramification) and apply them to morphisms.

Definition 2.2.8: Let $\phi : C_1 \to C_2$ be a morphism of smooth projective curves. Recall that we defined (Theorem 2.2.2)

$$\begin{aligned} \phi^* : K(C_2) &\to K(C_1) \\ f &\mapsto f \circ \phi \end{aligned}$$

(This is a ring homomorphism and hence an embedding of fields.)

1. Define the **degree** to be
$$\deg \phi := [K(C_1) : \phi^* K(C_2)].$$
2. Define the **separable/inseparable degree** to be the separable/inseparable degree of $K(C_1)/\phi^* K(C_2)$. ϕ is **separable** if $K(C_1)/\phi^* K(C_2)$ is separable.

Note that separability is automatic if $\mathrm{char}(K) = 0$.
Note that ϕ is an isomorphism iff $\deg \phi = 1$ (Proposition 2.2.14).

2.3.1 Degree and ramification

There is another way of thinking of degree (cf. the Riemann manifold viewpoint): Fix a point on C_2; the number of points on C_1 mapping to it, counted with appropriate multiplicity (see below), is always constant and equal to the degree.

Definition 2.2.9: Supoose $P \in C_1, Q \in C_2, \phi(P) = Q$. Let $t \in K(C_2)$ be a uniformizer at Q. Define
$$e_\phi(P) = \mathrm{ord}_P(\phi^* t).$$

This is always at least 1, and independent of the choice of t.

Theorem 2.2.10. *Let $\phi : C_1 \to C_2$ be a nonconstant morphism of smooth projective curves (over algebraically closed K). Then*

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi) \tag{2.2}$$

for all $Q \in C_2$. Moreover if ϕ is separable then $e_\phi(P) = 1$ for all but finitely many P. In particular,

1. *ϕ is surjective*
2. *$|\phi^{-1}(Q)| \leq \deg \phi$, and if ϕ is separable, then we have equality for all but finitely many $Q \in C_2$.*

Compare this to the following theorem from algebraic number theory: Given an extension of number fields L/K and a prime $\mathfrak{p}$ in K, we have

$$\sum_{\mathfrak{P}|\mathfrak{p}} e_{L/K}(\mathfrak{P}) f_{L/K}(\mathfrak{P}) = [L : K].$$

The absence of f is because we are working with smooth curves. Furthermore, only finitely many primes ramify in L, and if L/K is Galois, we have the nice fact that $e_{L/K}(\mathfrak{P})$ are equal for all $\mathfrak{P} \mid \mathfrak{p}$, and this reduces to

$$e_{L/K} f_{L/K} g_{L/K} = [L : K].$$

Later we will see that this formula (2.2) becomes similarly nice for elliptic curves.

2.3.2 Basic facts on degree

Proposition 2.2.11: Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves. Then for all $D_i \in \mathrm{Div}(C_i)$, $f_i \in \overline{K}(C_i)^\times$

1. $\deg(\phi^* D_2) = \deg(\phi) \deg(D_2)$.
2. $\phi^*(\mathrm{div}\, f_2) = \mathrm{div}(\phi^* f_2)$.
3. $\deg(\phi_* D) = \deg D$.
4. $\phi_*(\mathrm{div}\, f_1) = \mathrm{div}(\phi_* f_1)$.
5. $\phi_* \circ \phi^*$ is multiplication by $\deg \phi$ on $\mathrm{Div}(C_2)$.
6. For $\psi : C_2 \to C_3$, $(\psi \circ \phi)^* = \phi^* \circ \psi^*$ and $(\psi \circ \phi)_* = \psi_* \circ \phi_*$.

Proof. [2][II.3.6] □

A very useful relation is

$$\operatorname{div}(f) = f^*((0) - (\infty)).$$

This holds because noting $t \mapsto t$ is a uniformizer at 0 on $\mathbb{P}^1$ and $t \mapsto \frac{1}{t}$ is a uniformizer at ∞ for $\mathbb{P}^1$,

$$f^*((0)) = \sum_{Q \in f^{-1}(0)} \operatorname{ord}_Q(f^*t) = \sum_{Q \in f^{-1}(0)} \operatorname{ord}_Q(f) = \sum_{P, \operatorname{ord}_P(f) > 0} \operatorname{ord}_P(f) P \tag{2.3}$$

$$f^*((\infty)) = \sum_{Q \in f^{-1}(\infty)} \operatorname{ord}_Q\left(f^* \frac{1}{t}\right) = \sum_{Q \in f^{-1}(\infty)} \operatorname{ord}_Q\left(\frac{1}{f}\right) = -\sum_{P, \operatorname{ord}_P(f) < 0} \operatorname{ord}_P(f) P \tag{2.4}$$

$$\operatorname{div}(f) = f^*((0) - (\infty)).. \tag{2.5}$$

Proof of Proposition 2.2.7. We have

$$\deg(\operatorname{div}(f)) = \deg(f^*((0) - (\infty))) = \deg(f) \underbrace{\deg((0) - (\infty))}_{0} = 0.$$

□

We summarize:

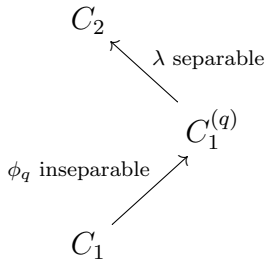
Number fields	Elliptic curves
$\sum_{\mathfrak{P}\mid\mathfrak{p}} e_{L/K}(\mathfrak{P}) f_{L/K}(\mathfrak{P}) = [L : K]$.	$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi)$
FABFM Q, $\lvert\phi^{-1}(Q)\rvert = \deg_s \phi$	Finitely many primes ramify.
$e_{\psi\circ\phi}(P) = e_\phi(P) e_\psi(\phi P)$	$e_{M/L}(\mathfrak{Q}/\mathfrak{P}) e_{L/K}(\mathfrak{P}/\mathfrak{p}) = e_{M/K}(\mathfrak{Q}/\mathfrak{p})$

2.3.3 Separability

Just like we can break up a field extension into a purely inseparable and a separable part, we can do the same for maps between smooth curves.

Proposition 2.2.12: Let $\psi : C_1 \to C_2$ be a rational map of smooth curves. Then we can factor $\psi = \lambda \circ \phi_q$, where

1. ϕ_q is the Frobenius map, which is purely inseparable, with $q = \deg_i(\psi)$.
2. λ is purely separable.



Proof. □

2.4 Rational maps are morphisms

In algebraic geometry there are two kinds of maps: morphisms and rational maps. For curves these are actually the same. (Again, projectivity is essential. If a rational map tries to blow up, that's fine, because a point at infinity exists!)

Theorem 2.2.13. *Let C_1 be a smooth curve and $V \subseteq \mathbb{P}^N$ be a projective variety, and*

$$\phi : C_1 \dashrightarrow V \subseteq \mathbb{P}^N$$

be a rational map. Then ϕ is a morphism.

Proof. Write the map as $f = [f_0 : \cdots : f_n]$. Given a point P, we may have trouble with $f(P)$ if $f_0(P) = \cdots = f_n(P) = 0$. *Because C is smooth at P*, we have a discrete valuation at P (Proposition 2.2.3). Let $v = \min_i \operatorname{ord}_P(f_i)$, let t be a uniformizer for P. Then we can define

$$f(P) = \left[\frac{f_0}{t^v}(P) : \cdots : \frac{f_n}{t^v}(P)\right]$$

because all of the $\frac{f_i}{t^v}$ have positive valuation at P, and at least one of them have valuation 0 so is nonzero. *Because V is projective*, this point is in V. □

Proposition 2.2.14: A rational map of degree 1 between smooth curves C_1, C_2 is an isomorphism.

Proof. □

3 Differentials

Why would we consider differentials in algebra? See http://math.stackexchange.com/questions/307439/appearance-of-formal-derivative-in-algebra. From Silverman [2][II.4], differentials...

1. perform the traditional calculus role of linearization.
2. give a useful criterion for determining when an algebraic map is separable (cf. a field extension is separable iff the minimal polynomial of each element has nonzero derivative).

Let C be a smooth projective curve over $K = \overline{K}$. The space of differentials Ω_C is the $K(C)$-vector space generated by df for $f \in K(C)$ subject to relations

1. $d(f+g) = df + dg$ for all $f, g \in K(C)$.
2. $d(fg) = f\,dg + g\,df$ for all $f, g \in K(C)$.

3. $da = 0$ for all $a \in K$.

Proposition 2.3.1: If C be a curve, Ω_C is a 1-dimensional $K(C)$-vector space.

Hence, if $\omega \in \Omega_C \backslash \{0\}$, $P \in C$, and $t \in K(C)$ is a uniformizer at P, then $\omega = f dt$ for some $f \in K(C)$.

Definition 2.3.2: Keep the notation above. Define

$$\mathrm{ord}_P(\omega) := \mathrm{ord}_P(f).$$

Note this is independent of the choice of t.

Moreover $\mathrm{ord}_P(\omega) = 0$ for all but finitely many $P \in C$. We define $\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega) P$.

4 Riemann-Roch Theorem

See Silverman [2][II.5].

Definition 2.4.1: The **Riemann-Roch space** of $D \in \mathrm{div}(C)$ is

$$\mathscr{L}(D) = \{f \in K(C)^* : \mathrm{div}(f) + D \geq 0\} \cup \{0\}$$

i.e., the K-vector space of rational functions on C with poles no worse than specified by D. Denote its dimension by

$$\ell(D) = \dim_{\overline{K}} \mathscr{L}(D).$$

We have the following basic facts.

Proposition 2.4.2 (Silverman [2][II.5.2)**:** Let $D \in \mathrm{Div}(C)$.

1. (We don't need to worry about negative divisors) If $\deg D < 0$, then
$$\mathscr{L}(D) = \{0\} \text{ and } \ell(D) = 0.$$
2. (Finite-dimensionality) $\mathscr{L}(D)$ is a finite-dimensional $\overline{K}$ vector space.
3. If $D' \sim D$, then
$$\mathscr{L}(D) \cong \mathscr{L}(D') \text{ and } \ell(D) = \ell(D').$$

The Riemann-Roch theorem tells us the dimension of these spaces based on an invariant called the genus.

Theorem 2.4.3 (Riemann-Roch)**.** *Let C be a smooth curve and $K_C = \mathrm{div}(\omega)$ a canonical divisor on C. Then there is an integer $g \geq 0$, called the **genus** of C, such that for every divisor $D \in \mathrm{Div}(C)$,*

$$\ell(D) - \ell(K_C - D) = \deg D - g + 1.$$

The genus is the same as the topological genus if the curve is considered over $\mathbb{C}$.

The left hand side is a difference of ℓ's. To get $\ell(D')$ for some D', we have to make the other term 0. We can do this by noting that $\ell(D) = 0$ for $D < 0$ and $D = 0$.

Corollary 2.4.4 (Computation of $\ell(D)$)**.** *As above, let C be a smooth curve and $K_C = \operatorname{div}(\omega)$ a canonical divisor on C. We have the following.*

1. $\ell(K_C) = g$.
2. $\deg K_C = 2g - 2$.
3. *If* $\deg D > 2g - 2$, *then*
$$\ell(D) = \deg D - g + 1.$$

Proof. 1. Use the Riemann-Roch Theorem 2.4.3 with $D = 0$ and note $\mathscr{L}(0) = \overline{K}$.

2. Use (1) and Riemann-Roch with $D = K_C$.

3. From (2) we get $\deg(K_C - D) < 0$, so by Proposition 2.4.2, $\ell(D) - 0 = \deg D - g + 1$.

□

Corollary 2.4.5 (Riemann-Roch for elliptic curves)**.** *If the genus is 1 (i.e. C is an elliptic curve), then*
$$\dim \mathscr{L}(D) = \begin{cases} \deg(D), & \text{if } \deg D > 0 \\ 0 \text{ or } 1, & \text{if } \deg D = 0 \\ 0, & \text{if } \deg D < 0. \end{cases}$$

Proof. Put in $g = 1$. □

Chapter 3

Introduction and geometry

What are elliptic curves and why are they important? See Andrew Sutherland's slides http://math.mit.edu/classes/18.783/Lecture1.pdf for an introduction.

In this chapter we'll present an elementary, computational approach side by side with a more theoretical, geometric approach. (The reader may choose to focus on one or the other.)

1 Definition and motivations

An elliptic curve is essentially the "next simplest curve" besides a conic. We give two definitions of an elliptic curve which make this precise.

Definition 3.1.1 (Elementary definition)**:** An **elliptic cuve** E over a field K is the projective closure of a plane affine curve

$$y^2 = f(x)$$

with a specified rational point (typically the point at infinity). Here, $f \in K[x]$ is a monic cubic polynomial with distinct roots in $\overline{K}$.[1]

Definition 3.1.2 (Algebraic geometry definition)**:** An **elliptic curve** E over a field K is a smooth projective curve of genus 1 with a distinguished point in K.

Why is this interesting to study? We give an example of a problem where elliptic curves naturally arise.

1.1 The congruent number problem

As elliptic curves are the "next simplest curves" apart from conics, and there is a lot more freedom for elliptic curves, it is natural that a lot of Diophantine equations reduce to problems about elliptic curves. This is a large part of the motivation for studying them.

[1] When $\mathrm{char}(K) = 2$, we have to allow equations of the form $y^2 + a_1xy + a_3y = f(x)$. More on this when we talk about the Weierstrass form.

One famous still unsolved Diophantine equation is the congruent number problem, which we'll now consider. See Keith Conrad's article at http://www.thehcmr.org/issue2_2/congruent_number.pdf for an in-depth discussion, and [1] for the approach to the problem using modular forms.

Consider a right triangle $\triangle$ with legs a, b, and hypotenuse c. It satisfies the following.

$$a^2 + b^2 = c^2$$
$$\text{Area}(\triangle) = \frac{1}{2}ab.$$

Definition 3.1.3: We say

1. $\triangle$ is **rational** if $a, b, c \in \mathbb{Q}$.
2. $\triangle$ is **primitive** if $a, b, c \in \mathbb{Z}$ and $\gcd(a, b, c) = 1$. (This is the same as saying that a, b, c are pairwise coprime.)

Recall the following parametrization.

Lemma 3.1.4 (Rephrasing Theorem 1.1.1)**.** *Every primitive triangle is of the form* $(u^2 - v^2, 2uv, u^2 + v^2)$ *for* $u, v \in \mathbb{Z}$ *where* $u > v > 0$.

Definition 3.1.5: $D \in \mathbb{Q}^+$ is **congruent** if it is the area of some rational right-angled triangle.

Note that it suffices to consider squarefree integers $D \in \mathbb{N}$ since they form a coset of $\mathbb{Q}^{\times 2}$ in $\mathbb{Q}$.

For example, 5 and 6 are congruent.

Lemma 3.1.6. *$D \in \mathbb{Q}^+$ is congruent iff $Dy^2 = x^3 - x$ for some $x, y \in \mathbb{Q}$ with $y \neq 0$, iff $y^2 = x^3 - D^2x$ for some $y \neq 0$.*

Thus the problem of whether or not a number is congruent is equivalent to whether or not there exists a

Proof. We first show the first two conditions are equivalent. Suppose D is congruent. Then there is w such that Dw^2 is the area of a primitive triangle. By lemma 3.1.4, we can write the sides in the form $u^2 - v^2$, $2uv$, and $u^2 + v^2$ for $u, v, w \in \mathbb{Q}$. Then

$$Dw^2 = \frac{1}{2}(u^2 - v^2)2uv$$
$$D\left(\frac{w}{v^2}\right)^2 = \left(\frac{u}{v}\right)\left(\left(\frac{u}{v}\right)^2 - 1\right).$$

Set $x = \frac{u}{v}$ and $y = \frac{w}{v^2}$. Conversely, given x, y, let u, v be the numerator and denominator of x, and let $w = yv^2$.

To go between $Dy^2 = x^3 - x$ and $y^2 = x^3 - D^2x$, make the substitution $y \mapsto \frac{y}{D^2}$ and $x \mapsto \frac{x}{D}$. □

Fermat showed $D = 1$ is not congruent.

Theorem 3.1.7. *There are no solutions to*

$$w^2 = uv(u - v)(u + v) \tag{3.1}$$

for $u, v, w \in \mathbb{Z}$. Hence 1 is not a congruent number.

Proof. An elementary approach is to use infinite descent. See the notes at https://dl.dropboxusercontent.com/u/27883775/math%20notes/part_iii_elliptic.pdf. □

2 The equation of an elliptic curve

2.1 Every elliptic curve can be put in Weierstrass form

We would like to have some "standard form" for an elliptic curve, that is

1. a form involving as few terms as possible, such that every elliptic curve is isomorphic to an elliptic curve in that form, and
2. an easy way to tell if two elliptic curves in that form are isomorphic.

We'll investigate two natural forms for an elliptic curve: the Weierstrass and Legendre forms.

Definition 3.2.1: A **(long) Weierstrass equation** is an eqution in the following form

$$\begin{array}{rc} \text{affine coordinates} & y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \\ \text{projective coordinates} & Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \end{array}$$

A **(short) Weierstrass equation** is an equation in the following form

$$\begin{array}{rc} \text{affine coordinates} & y^2 = x^3 + Ax + B \\ \text{projective coordinates} & Y^2Z = X^3 + AXZ^2 + BZ^3. \end{array}$$

A note on the numbering in the coefficients: they are the weights for the coefficients that make the equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ homogeneous if y has weight 3 and x has weight 2.

Our main theorem in this section is the following. (The proof may be safely skipped for an elementary course, by using Definition 3.1.1 for an elliptic curve.)

Theorem 3.2.2. *Every elliptic curve E is isomorphic over K to a curve in Weierstrass form, via an isomorphism mapping $O_E \mapsto (0 : 1 : 0)$.*

Fact 3.2.3: Let D be a divisor on E, i.e., a formal sum of $\overline{K}$-points on E. If D is defined over K (i.e., D is fixed by the action of $G(\overline{K}/K)$), then $\mathscr{L}(D)$ has a basis consisting of rational functions defined over K, not just in $\overline{K}(E)$.

Proof of Theorem 3.2.2. Step 1: The idea is that if we pick some functions x, y to be our coordinates, by Riemann-Roch, we will get a linear dependence relations between terms $x^i y^j$ before too long.

1. $\mathscr{L}(2O_E)$ is 2-dimensional by Riemann-Roch 2.4.5. Pick a basis $1, x$.
2. $\mathscr{L}(3O_E)$ is 3-dimensional by Riemann-Roch. Extend to a basis $1, x, y$.
3. Look at the elements $1, x, y, x^2, xy, x^3, y^2$: these are all in $\mathscr{L}(6, O_E)$. But the dimension of the space is 6 and there are 7 elements, so there is a linear dependence relation.

   Leaving out either x^3 or y^2 gives a basis for $\mathscr{L}(6O_E)$ since each term has a different order pole at O_E. Thus the coefficients of x^3 and y^2 are nonzero. Rescaling x and y we get
   $$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
   for some $a_i \in K$.

We obtain a rational map

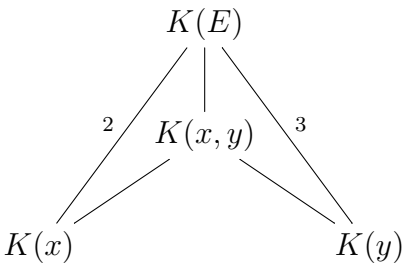
$$\begin{aligned} \phi : E &\to E' \subseteq \mathbb{P}^2 \\ P &\mapsto [x(P) : y(P) : 1]. \end{aligned}$$

A rational map from a smooth curve to a smooth curve is always a morphism (Theorem 2.2.13).

Step 2: We show ϕ is an isomorphism by showing its degree is 1. By Theorem 2.2.10 on the point $\infty \in \mathbb{P}^1$ with inverse O_E under x, y, we have

$$\begin{aligned} [K(E) : K(x)] &= \deg(E \xrightarrow{x} \mathbb{P}^1) = \operatorname{ord}_{O_E}\left(\frac{1}{x}\right) = 2 \\ [K(E) : K(y)] &= \deg(E \xrightarrow{y} \mathbb{P}^1) = \operatorname{ord}_{O_E}\left(\frac{1}{y}\right) = 3. \end{aligned}$$

We write down the fields involved.



The tower law says that $[K(E) : K(x, y)]$ divides 2 and 3 so $K(E) = K(x, y)$ thus $\phi^* K(E') = K(E)$ and $\deg(\phi) = 1$. Thus ϕ is birational.

We know E is projective, and we need E' to be smooth. If E' is singular, we can find a rational parametrization, so E and E' are rational. This is a contradiction because E has genus 1.

Thus E' is smooth and ϕ is an isomorphism.

We check the image of O_E. Since x has a pole of order 2 at O_E and y has a pole of order 3,

$$\begin{aligned} \phi : E &\to E' \\ P &\mapsto \left[\frac{x}{y}(P) : 1 : \frac{1}{y}(P)\right] \\ O_E &\mapsto [0:1:0]. \end{aligned}$$

□

2.2 Transforming an elliptic curve

We can use the proof of Theorem 3.2.2 to find when 2 curves in Weierstrass form are isomorphic.

Proposition 3.2.4: Let K be algebraically closed. Let E, E' be elliptic curves over K in Weierstrass form. Then $E \cong E'$ over K iff the equations are related by substitutions

$$\begin{aligned} x &= u^2 x' + r \\ y &= u^3 y' + u^2 s x' + t \end{aligned}$$

for some $r, s, t, u \in K$ with $u \neq 0$.

Proof. Because x, y and x', y' are Weierstrass coordinates, we must have $x, x' \in \mathscr{L}(2O_E)$ and $y, y' \in \mathscr{L}(3O_E) \backslash \mathscr{L}(2O_E)$.

Again by Riemann-Roch, we have

$$\langle 1, x \rangle = \mathscr{L}(2O_E) = \langle 1, x' \rangle .$$

From this we see $x = \lambda x' + r$ for some $\lambda, r \in K$. Similarly,

$$\langle 1, x, y \rangle = \mathscr{L}(3O_E) = \langle 1, x', y' \rangle$$

and hence $y = \mu y' + \sigma x' + t$ for some $\mu, \sigma, t \in K$ and $\mu \neq 0$. Looking at coefficients of y^2 and x^3 we need $\lambda^3 = \mu^2$, so $\lambda = u^2$ and $\mu = u^3$ for some $u \in K$. Put $s = \frac{\sigma}{u^2}$. □

A Weierstrass equation defines an elliptic curve iff it defines a smooth curve, iff $\Delta(a_1, \ldots, a_6) \neq 0$ where $\Delta \in \mathbb{Z}[a_1, \ldots, a_6]$ is a certain polynomial (see the formula sheet!).

If $\mathrm{char}(K) \neq 2, 3$, we can reduce to the case $y^2 = x^3 + ax + b$, with discriminant

$$\Delta = -16(4a^3 + 27b^2).$$

(this is 16 times the usual formula for the discriminant of a polynomial).

Corollary 3.2.5. *Assume* $\mathrm{char}(K) \neq 2, 3$. *The elliptic curve*

$$E : y^2 = x^3 + ax + b$$
$$E' : y^2 = x^3 + a'x + b'$$

are isomorphic over K iff $a' = u^4 a$ and $b' = u^6 b$ for some $u \in K^*$.

Proof. E and E' are related by a substition as in Proposition 3.2.4 with $r = s = t = 0$. □

2.3 Legendre form

Another useful for an elliptic curve is the **Legendre form**.

Lemma 3.2.6. *Let* $C \subset \mathbb{P}^2$ *be a smooth plane cubic, and* $P \in C$ *a point of inflection. Then we can change coordinates such that*

$$C : Y^2Z = X(X - Z)(X - \lambda Z), \qquad \lambda \neq 0, 1, \qquad P = (0 : 1 : 0).$$

Proof. We change coordinates such that $P = (0 : 1 : 0)$ and $T_pC = \{Z = 0\}$. Then

$$C : \{F(X, Y, Z) = 0\} \subset \mathbb{P}^2.$$

A point of inflection means the line meets the curve with multiplicity 3, so we get a triple root

$$F(t, 1, 0) = ct^3.$$

Thus there are no terms X^2Y, XY^2, Y^3. Thus

$$F \in \left\langle Y^2Z, XYZ, YZ^2, X^3, X^2Z, XZ^2, Z^3 \right\rangle,$$

with the coefficient of Y^2Z nonzero (otherwise $P \in C$ would be singular), otherwise everything is divisible by Z, and C contains $\{Z = 0\}$ (curves are irreducible).

We can rescale X, Y, Z, F, so WLOG

$$C : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \qquad \text{Weierstrass form}$$

Substituting $Y \leftarrow Y - \frac{1}{2}a_1X - \frac{1}{2}a_3Z$ (completing the square) we may assume $a_1 = a_3 = 0$ (we assume $\mathrm{char}(K) \neq 2$), giving

$$C : Y^2Z = Z^3 f\left(\frac{X}{Z}\right).$$

C is smooth, so f has distinct roots, without loss of generality, 0, 1, λ. Thus

$$C : Y^2Z = X(X - Z)(Z - \lambda Z). \qquad \text{Legendre form}$$

□

2.4 Invariants of an elliptic curve

Definition 3.2.7: The j**-invariant** of E is

$$j(E) = \frac{1728(4a^3)}{4a^3 + 27b^3}.$$

Corollary 3.2.8. *$E \cong E'$ implies $j(E) = j(E')$ and the converse holds over $K = \overline{K}$.*

Proof. We have $E \cong E'$ iff $a' = u^4 a$, $b' = u^6 b$ for some $u \in K^*$. This implies $(a^3 : b^2) = ((a')^3 : (b')^2)$, which is true iff $j(E) = j(E')$. The converse holds if the field is algebraically closed (we need to extract roots). □

2.5 Singular cubics

[Weierstrass form, etc.]

3 Group law

There is a natural group law on elliptic curve. There are several ways to think about it.

1. The key point here is that every line intersects an elliptic curve in 3 points, counted with multiplicity. Given two points P and Q on an elliptic curve E, let the third point of intersection be $-(P + Q)$ (and its reflection across the x-axis be $P + Q$). We can obtain explicit expressions for $P + Q$.

2. Every algebraic curve has a group associated with it, the group of divisors. It turns out that the divisor class group of an elliptic curve can be put in direct correspondence to the points on the elliptic curve.

3. For an elliptic curve over $\mathbb{C}$, we can define the group law by finding some analytic map $\mathbb{C} \to E(\mathbb{C})$. Then addition on $\mathbb{C}$ pushed forward gives a group law on E. This is just like the fact that the addition formulas for $\sin, \cos$ give a group law on the circle. We'll see this in the chapter on elliptic curves over $\mathbb{C}$.

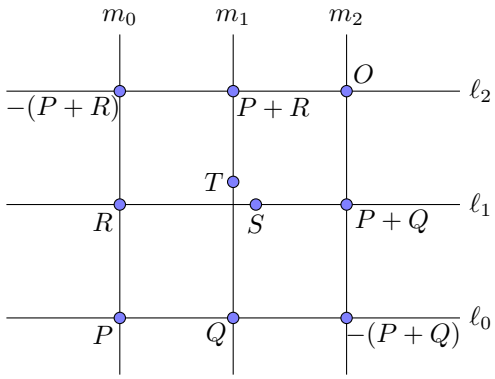
3.1 Elementary approach, I

The following is an adaptation of the proof in [**?**, p. 28]. The proof is nice, but fails to capture all cases, so we will give a more correct, but messier, proof later.

Theorem. *Let P, Q, and R be three points on an elliptic curve $E(K)$ for some field K that we may assume is algebraically closed. Assume that P, Q, R, and the zero point O are all in* general position *(this means that in the diagram below there are no relationships among the points other than those that necessarily exist by construction). Then*

$$(P + Q) + R = P + (Q + R).$$

Proof. The line ℓ_0 through P and Q meets the curve E at a third point, $-(P+Q)$, and the line m_2 through O and $-(P+Q)$ meets E at $P+Q$. Similarly, the line m_0 through P and R meets E at $-(P+R)$, and the line ℓ_2 through O and $-(P+R)$ meets E at $P+R$. Let S be the third point where the line ℓ_1 through $Q+P$ and R meets E, and let T be the third point where the line m_1 through Q and $P+R$ meets E. See the diagram below.



We have $S = -(Q+P)+R$ and $T = -(Q+(P+R))$. It suffices to show $S = T$. Suppose not. Let $g(x,y,z)$ be the cubic polynomial formed by the product of the lines ℓ_0, ℓ_1, ℓ_2 in homogeneous coordinates, and similarly let $h(x,y,z) = m_0 m_1 m_2$. We may assume $g(T) \neq 0$ and $h(S) \neq 0$, since the points are in general position and $S \neq T$. Thus g and h are linearly independent elements of the k-vector space V of homogeneous cubic polynomials in $k[x,y,z]$. The space V has dimension 10, thus the subspace of homogeneous cubic polynomials that vanish at the eight points O, P, Q, R, $\pm(Q+P)$, and $\pm(P+R)$ has dimension 2 and is spanned by g and h. The homogeneous polynomial $f(x,y,z) = x^3 + Axz^2 + Bz^3 - zy^2$ that defines E is a nonzero element of this subspace, so we may write $f = ag + bh$ as a linear combination of g and h. But $f(S) = f(T) = 0$, since S and T are both points on E, which implies that a and b are both zero. This contradicts the linear independence of g and h, since f is not the zero polynomial. □

3.2 Elementary approach, II: The group law in algebraic terms

Let $P = (x_1, y_1, z_1)$ and $Q = (x_2, y_2, z_2)$ be two points on E. We will compute the sum $P + Q = R = (x_3, y_3, z_3)$ by expressing the coordinates of R as rational functions of the coordinates of P and Q. If either P or Q is the point at infinity, then R is simply the other point, so we assume that P and Q are affine points with $z_1 = z_2 = 1$. There are two cases:

Case 1. $x_1 \neq x_2$. The line $\overline{PQ}$ has slope $m = (y_2 - y_1)/(x_2 - x_1)$, which yields the equation $y - y_1 = m(x - x_1)$. The point $-R = (x_3, -y_3, 1)$ is on this line, thus $-y_3 = m(x_3 - x_1) + y_1$. Substituting for y_3 in the Weierstrass equation for E yields

$$(m(x_3 - x_1) + y_1)^2 = x_3^3 + Ax_3 + B.$$

Simplifying, we obtain $0 = x_3^3 - m^2 x_3^2 + \cdots$, where the ellipsis hides lower order terms. The values x_1 and x_2 satisfy the same cubic equation, and the quadratic coefficient

$-m^2$ must be the sum of the roots. Thus $x_3 = m^2 - x_1 - x_2$. To sum up, we have

$$\begin{aligned} m &= \frac{y_2 - y_1}{x_2 - x_1}, \\ x_3 &= m^2 - x_1 - x_2, \\ y_3 &= m(x_1 - x_3) - y_1. \end{aligned}$$

Thus to compute $P + Q = R$, we need one inversion and three multiplications (one of which is a squaring). We'll denote this cost 3M+I.

Case 2. $x_1 = x_2$. If $y_1 \neq y_2$, then they must be opposite points and $R = 0$. Otherwise $P = Q$, and we compute the slope of the tangent line by implicitly differentiating the Weierstrass equation for E. This yields $2y\,dy = 3x^2\,dx + A\,dx$, so

$$m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}.$$

The formulas for x_3 and y_3 are then the same as the previous case. Note that we require an extra multiplication here, so computing $R = 2P$ has a cost of 4M+I.

With these equations in hand, we can now prove associativity as a formal identity, treating $x_1, y_1, z_1, x_2, y_2, z_2, x_3, y_3, z_3, A, B$ as indeterminants subject to the three relations implied by the fact that P, Q, and R all lie on the curve E. See the Sage worksheet

https://hensel.mit.edu:8002/home/pub/1/

for details, which includes checking all the special cases.

The equations above can be converted to projective coordinates by replacing x_1, y_1, x_2, and y_2 with x_1/z_1, y_1/z_1, x_2/z_2, and y_2/z_2 respectively, and then writing the resulting expressions for x_3/z_3 and y_3/z_3 with a common denominator. This has the advantage of avoiding inversions, which are more costly than multiplications (in a finite field of cryptographic size inversions may be 50 or even 100 times more expensive). This increases the number of multiplications to 12M in case 1 (addition), and 14M in case 2 (doubling).

3.2.1 Edwards curves*

There are many alternative representations of elliptic curves that have been proposed. We give just one example here, Edwards curves [**?**, **?**], which have two significant advantages over Weierstrass equations. Let d be a non-square element of a field k (assumed to have characteristic not equal to 2, as usual). Then the equation

$$x^2 + y^2 = 1 + dx^2y^2$$

defines an elliptic curve with distinguished point $(0, 1)$.[2] The group operation is given by

$$(x_3, y_3) = \left(\frac{x_1y_2 + y_2x_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$$

[2]Technical point: there are two points at infinity, both of which are singular, violating our requirement that an elliptic curve be smooth. However, this plane curve can be desingularized by embedding it in $\mathbb{P}^3(k)$. The points at infinity are then no longer rational, and do not play a role in the group operation on $E(k)$.

As written, this involves five multiplications and two inversions (ignoring the multiplication by d, which we can choose to be small), which is greater than the cost of the group operation in Weierstrass form. However, in projective coordinates we have

$$\frac{x_3}{z_3} = \frac{z_1 z_2 (x_1 y_2 + x_2 y_1)}{z_1^2 + z_2^2 + d x_1 x_2 y_1 y_2}, \qquad \frac{y_3}{z_3} = \frac{z_1 z_2 (y_1 y_2 - x_1 x_2)}{z_1^2 + z_2^2 + d x_1 x_2 y_1 y_2}.$$

There are a bunch of common subexpressions here, and in order to compute z_3, we need a common denominator. Let $r = z_1 z_2$, let $s = x_1 y_2 + x_2 y_1$, let $t = d x_1 y_2 x_2 y_1$, and let $u = y_1 y_2 - x_1 x_2$. We then have

$$x_3 = rs(r^2 - t), \qquad y_3 = ru(r^2 + t), \qquad z_3 = (r^2 + t)(r^2 - t).$$

This yields a cost of 12M, and, if you are clever, you can reduce it to 11M.

The remarkable thing about these formulas is that they handle every case; there are not separate formulas for addition and doubling, and adding opposite points or the identity element works the same as the general case. Such formulas are called *complete*, and they have two distinct advantages. First, they can be implemented very efficiently because there is no branching. Second, they protect against what is known as a *side-channel* attack. If an adversary can distinguish whether you are doubling or adding points, e.g. by monitoring the CPU and noticing the difference in the time required by each operation, they can break a cryptosystem that performs scalar multiplication by an integer that is meant to be secret.

Having said that, if you know you are going to be doubling and are not concerned about a side-channel attack, there are several optimizations that can be made (these include replacing $1 + dx^2y^2$ with $x^2 + y^2$). This reduces the cost of doubling a point on an Edwards curves to 7M, which is a huge improvement over the 14M cost of doubling a point in Weierstrass coordinates.

The explicit formulas database at `http://hyperelliptic.org/EFD/` contains optimized formulas for Edwards curves and various generalizations, as well as many other forms of elliptic curves. Operation counts and verification scripts are provided with each set of formulas.

We should note that, unlike Weierstrass equations, not every elliptic curve can be put into Edwards form. In particular, an Edwards curve always has a rational point of order 4, the point $(1, 0)$, but this is not true of many elliptic curves.

3.3 Group law via divisors

Recall the definition of the Picard group 2.2.6. We define

$$\begin{aligned} \phi : E &\to \mathrm{Pic}^0(E) \\ P &\mapsto [P - O_E]. \end{aligned}$$

For clarity, we temporarily write the group law on E with $\oplus$.

Proposition 3.3.1: 1. We have $\phi(O_E) = 0$ and $\phi(P \oplus Q) = \phi(P) + \phi(Q)$.

2. ϕ is a bijection.

This shows that addition on the elliptic curve is the pullback under ϕ of addition on $\mathrm{Pic}^0(E)$. Since $\mathrm{Pic}^0(E)$ is an abelian group, we get E is an abelian group under addition. (In particular, $\oplus$ is associative.)

Proof. 1. Let $\ell = 0$ be the line through P, S, Q and $m = 0$ be the line through the point $O_E, S, R = P \oplus Q$. We have

$$\begin{aligned} \mathrm{div}(\ell/m) &= (P) + (S) + (Q) - (O_E) - (S) - (R) \\ &= (P) + (Q) - (P \oplus Q) - (O_E) \\ \implies (P) + (Q) &\sim (P \oplus Q) + (O_E) \\ \implies (P \oplus Q) - (O_E) &\sim (P) - (O_E) + (Q) - (O_E) \\ \implies \phi(P \oplus Q) &= \phi(P) + \phi(Q). \end{aligned}$$

2. Injectivity: Suppose $\phi(P) = \phi(Q)$ and $P \neq Q$. Then there exists $f \in \overline{K}(E)^*$ such that $\mathrm{div}(f) = P - Q$. Then there is a rational map $f : E \to \mathbb{P}^1$ which is automatically a morphism. What is its degree? Only 1 point, P, maps to 0 with ramification index 1, so the degree is 1:

$$\deg(f) = \sum_{P \in f^{-1}(0)} e_f(P) = \sum_{P \in f^{-1}(0)} \mathrm{ord}_P(f) = \sum_{P, \mathrm{ord}_P(f) > 0} \mathrm{ord}_P(f) = 1.$$

A morphism of degree 1 is an isomorphism so $E \cong \mathbb{P}^1$ (Proposition 2.2.14), contradiction.

Surjectivity: Let $D \in \mathrm{Div}^0(E)$. Then $D + (O_E)$ has degree 1. Riemann-Roch **??** tells us that $\dim(\mathscr{L}(D + (O_E))) = 1$ so there exists $f \in \overline{K}(E)^\times$ such that

$$\mathrm{div}(f) + D + (O_E) \geq 0.$$

where the LHS has degree 1. Thus

$$\mathrm{div}(f) + D + (O_E) = (P)$$

for some $P \in E$. We see $D \sim (P) - (O_E)$; taking the divisor class,

$$[D] = \phi(P).$$

□

3.4 Elliptic curves are group varieties

Theorem 3.3.2. *Elliptic curves are group varieties, i.e.,*

$$\begin{aligned} [-1] : E \to E; \qquad & P \mapsto \ominus P \\ \oplus : E \times E \to E; \qquad & (P, Q) \mapsto P \oplus Q. \end{aligned}$$

Being a group variety is more than just being a group and being a variety. The group laws are actually morphisms.

Proof. This requires no further calculation, but there is some subtlety.

1. The above formulas says $[-1] : E \to E$ is a *rational* map. Thus $[-1]$ is a morphism, since E is a smooth projective curve.

2. The above formula say $\oplus : E \times E \to E$ is a rational map regular on $U = \{(P, Q) \in E \times E : P, Q, P \oplus Q$ The result we quoted above only works on a smooth projective curve, not a surface, so we need another trick here.

   For $P \in E$, let

   $$\begin{aligned} \tau_P : E &\to E \\ X &\mapsto X \oplus P \end{aligned}$$

   be translation by P. We have τ_P is a rational map, therefore a morphism. We factor $\oplus : E \times E \to E$ as

   $$E \times E \xrightarrow{\tau_{\ominus A} \times \tau_{\ominus B}} E \times E \xrightarrow{\oplus} E \xrightarrow{\tau_{A \oplus B}} E.$$

   Thus $\oplus$ is regular on $(\tau_A \times \tau_B)(U)$ for all $A, B \in E$. Clearly they agree on overlaps.

   Here's an informal map: we want to avoid the diagonals; U is anything not on those lines.

   Thus $\oplus$ is regular on $E \times E$ and $\oplus$ is a morphism.

□

3.5 The group $E(K)$ for different K

What is the group $E(K)$? We will prove the following later on.

1. For $K = \mathbb{C}$, $E(\mathbb{C}) \cong \mathbb{C}/\Lambda \cong \mathbb{R}/\mathbb{Z} \cong \mathbb{R}/\mathbb{Z}$ for Λ a lattice. (It's a torus.)

2. $K = \mathbb{R}$:

   $$E(\mathbb{R}) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{R}/\mathbb{Z} \text{ if } \Delta > 0 \\ \mathbb{R}/\mathbb{Z} \text{ if } \Delta < 0. \end{cases}$$

3. For $K = \mathbb{F}_q$,

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

   This is Hasse's Theorem.

4. When $[K : \mathbb{Q}_p] < \infty$, $E(K)$ is a contains a subgroup of finite index isomorphic to $(\mathscr{O}_K, +)$.

5. When $[K : \mathbb{Q}] < \infty$, $E(K)$ is a finitely generated abelian group (Mordell-Weil Theorem).

4 Isogenies

We give two approaches to isogenies.

- We'll give a hands-on approach that shows us how to compute with isogenies (by writing out the rational functions), and lets us understand the degree of an isogeny.
- We'll also see what we can do with a more theoretical approach that avoids calculations.

Definition 3.4.1: Let E_1 and E_2 be elliptic curves defined over k. An **isogeny** is a morphism $\alpha\colon E_1 \to E_2$ that preserves the distinguished point (i.e. $\alpha(0) = 0$).

- We denote the set of isogenies by $\mathrm{Hom}(E_1, E_2)$. It is an abelian group, where addition is defined by addition in $E_2(\overline{k})$:

$$(\alpha + \beta)(P) = \alpha(P) + \beta(P).$$

  When $E_1 = E_2$, we say that α is an **endomorphism**
- We write $\mathrm{Hom}(E, E) = \mathrm{End}(E)$. This is a ring where multiplication is given by composition.

and we write $\mathrm{Hom}(E, E) = \mathrm{End}(E)$.

We have a group structure on an elliptic curve, so it's natural to restrict to isogenies that are group homomorphisms. In fact, we don't need to, because all isogenies are group homomorphisms!

Theorem 3.4.2 (Silverman [2], Theorem III.4.8)**.** *Let E_1 and E_2 be elliptic curves defined over K. A regular rational map $\alpha\colon E_1 \to E_2$ is an isogeny if and only if $\alpha\colon E_1(\overline{K}) \to E_2(\overline{K})$ is a group homomorphism.*

We will prove this fact in Section 4.1 using some algebraic geometry. Alternatively, we can use Theorem 3.4.2 as our definition, since for all the isogenies we will be interested in it is easy (and useful) to show that they are group homomorphisms.

4.1 Isogenies are group homomorphisms

Proof of Theorem 3.4.2. □

4.2 Isogenies: explicit approach

When working with isogenies it is often more convenient to work with affine coordinates and we will do so for the next two lectures. But it is important to remember that whenever refer to the point (x, y) in affine space, we are actually referring to the point $(x : y : 1)$ of projective space, and 0 refers to $(0 : 1 : 0)$, since, as usual, we assume elliptic curves are specified in Weierstrass form $y^2 = x^3 + Ax + B$. We begin by showing that without loss of generality we can assume that isogenies are specified in a standard form.

Lemma 3.4.3. *Suppose E_1, E_2 are elliptic curves in Weierstrass form.*

Any isogeny $\alpha : E_1 \to E_2$ can be written as

$$\alpha(x, y) = \left[\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right]$$

where $u, v, s, t \in \overline{k}[x]$ are polynomials in x.

Proof. Write $\alpha(x, y) = (R_1(x, y), R_2(x, y))$, where $R_1, R_2 \in \overline{K}(x, y)$ are rational functions in x and y.

Let's begin with R_1. We can always write $R_1(x, y) = \frac{p_1(x)+p_2(x)y}{p_3(x)+p_4(x)y}$ because for any power of y greater than one, we can substitute $y^2 = x^3 + Ax + B$. Multiply the top and the bottom by $p_3(x) - p_4(x)y$ to get

$$R_1(x, y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}.$$

Recall that a point (x, y) on an elliptic curve in Weierstrass form has inverse $(x, -y)$, so the x-coordinate does not change under inversion. Since α is a group homomorphism, we must have $R_1(x, -y) = R_1(x, y)$. Therefore, $q_2(x) = 0$.

The argument for R_2 is similar: We have $R_2(x, y) = -R_2(x, -y)$, so for $R_2(x, y) = \frac{r_1(x)+r_2(x)y}{r_3(x)}$, we must have $r_1(x) = 0$. □

We may assume that the polynomials u and v of Lemma 3.4.3 are relatively prime, equivalently, that they have no common root in $\overline{k}$, and we write $u \perp v$ to denote this constraint. Similarly we assume $s \perp t$. We now give a more precise definition of an isogeny that is particularly convenient to work with.

Definition 3.4.4 (cf. Definition 3.4.1)**:** Let E_1 and E_2 be elliptic curves over a field k with characteristic not 2. Let $u, v, s, t \in \overline{k}[x]$ and let α be a map $E_1 \to E_2$ be given by

$$\alpha(x, y) = \begin{cases} \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right) & \text{if } v(x)t(x) \neq 0, \\ 0, & \text{otherwise,} \end{cases}$$

such that $\alpha\colon E_1(\overline{k}) \to E_2(\overline{k})$ is a group homomorphism. Then α is an *isogeny* from E_1 to E_2.

With α in this form, we make the following definitions:

Definition 3.4.5: The *degree* of a nonzero isogeny α is $\deg \alpha = \max\{\deg u, \deg v\}$. By convention, the zero isogeny has degree 0.

Definition 3.4.6: A nonzero isogeny α is *separable* if $\left(\frac{u}{v}\right)' \neq 0$ (as functions) and is *inseparable* otherwise. The zero isogeny is separable.

We can check that this agrees with the definitions of the degree and separability of a rational map.

Proposition 3.4.7: Definitions 3.4.5 and 3.4.6 agree with Definition 2.2.8.

Proof. □

4.3 Examples of isogenies

Our first example of an isogeny is a simple endomorphism, the multiplication by 2 map, which doubles points on an elliptic curve. This is obviously a group homomorphism, and we can easily show that it is defined by rational maps.

Example 3.4.8 (Doubling)**:** Let $\alpha(P) = 2P$ on the elliptic curve $y^2 = f(x) = x^3 + Ax + B$. Recall that the formula for doubling a point is

$$\alpha(x, y) = (m^2 - 2x,\ m(x - (m^2 - 2x)) - y), \qquad \text{where } m = \frac{3x^2 + A}{2y}.$$

We compute

$$\begin{aligned}
\frac{u(x)}{v(x)} &= \frac{(3x^2 + A)^2}{4y^2} - 2x \\
&= \frac{(3x^2 + A^2) - 8xf(x)}{4f(x)}, \\
\frac{s(x)}{t(x)} &= \frac{3x^2 + A}{2y}\left(3x - \frac{(3x^2 + A)^2}{4y^2}\right) - y \\
&= \frac{(3x^2 + A)(12xy^2 - (3x^2 + A)^2) - 8y^4}{8y^3} \\
&= \frac{(3x^2 + A)(12xf(x) - (3x^2 + A)^2) - 8f(x)^2}{8f(x)^2}y \\
&= \frac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2}{8f(x)^2}y.
\end{aligned}$$

Even in this simple example, we see that it is already non-trivial to write down u, v, s, and t for the multiplication by 2 map. In the next section we will introduce *division polynomials* to tackle the general multiplication by m case.

Our second example is the Frobenius endomorphism.

Example 3.4.9 (Frobenius endomorphism)**:** Let $E/\mathbb{F}_p$ be an elliptic curve and let $\pi\colon E \to E$ be the map

$$\pi(x, y) = (x^p, y^p) = (x^p, f(x)^{\frac{p-1}{2}}y).$$

In this case it is easy to see that $\pi(x, y)$ is specified by rational functions, in fact polynomials: $u(x) = x^p$, $v(x) = 1$, $s(x) = f(x)^{\frac{p-1}{2}}$, and $t(x) = 1$.

We now show that π is a group endomorphism of $E(\overline{k})$.[3] We first recall several facts about the Frobenius map over a finite field, which we also denote by π, given by $\pi\colon \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$, $\pi(x) = x^p$. The map π is a field automorphism of $\mathbb{F}_p$, as we may check by noting that

1. $0^p = 0$ and $1^p = 1$.
2. $(ab)^p = a^p b^p$, $(a^{-1})^p = (a^p)^{-1}$ for all $a \in \overline{\mathbb{F}}_p$.
3. $(a+b)^p = \sum \binom{p}{i} a^i b^{p-i} = a^p + b^p$ for all $a, b \in \overline{\mathbb{F}}_p$.
4. $(-a)^p = -a^p$ for all $a \in \overline{\mathbb{F}}_p$.

(Note: these properties also hold hold for the map $\pi(x) = x^q$ over $\mathbb{F}_q$, where $q = p^n$.)

This implies that for any $g \in \mathbb{F}_p[x_1, \ldots, x_k]$, and hence any rational function $g \in \mathbb{F}_p(x_1, \ldots, x_k)$, we have

$$g(x_1, \ldots, x_k)^p = g(x_1^p, \ldots, x_k^p).$$

Applying this to the expressions for adding, doubling, and negating points, and noting that $\pi(0) = 0$, we see that the Frobenius map is an endomorphism on elliptic curves.

Note that if (x, y) is a point in $E(\mathbb{F}_p)$, then $\pi(x, y) = (x^p, y^p) = (x, y)$, so the Frobenius endomorphism acts trivially on $E(\mathbb{F}_p)$. However it is important remember that when we are talking about endomorphisms on elliptic curves, we should be thinking about the group of points over $\overline{k} = \overline{\mathbb{F}}_p$. The Frobenius endomorphism does not act trivially on $E(\overline{\mathbb{F}_p})$. In fact, $\mathbb{F}_p$ is precisely the subset of $\overline{\mathbb{F}_p}$ fixed by π, and it follows that $E(\mathbb{F}_p)$ is precisely the subgroup of $E(\overline{\mathbb{F}_p})$ fixed by π.

We now discuss endomorphisms that multiply points on an elliptic curve by an integer m, which we denote $[m]$. These are clearly group homomorphisms from $E(\overline{k})$ to $E(\overline{k})$, but we need to express them as rational maps. To represent these maps generically, we will define what are known as "division polynomials." We've already seen these polynomials in the case $m = 2$ (Example 3.4.8). To compute polynomials for the general case, rather than using affine or standard projective coordinates, it is more convenient to use weighted projective coordinates, also known as *Jacobian coordinates* (which we may then transform back to our standard affine format).

In weighted project coordinates our standard Weierstrass curve equation becomes

$$y^2 = x^3 + Axz^4 + Bz^6,$$

where we think of x as having weight 2 and y having weight 3; this makes the equation homogeneous of degree 6. In weighted projected coordinates, our equivalence relation on triples changes: now $(x, y, z) \sim (\lambda^2 x, \lambda^3 y, \lambda z)$ for any scalar $\lambda \in \overline{k}^*$. The triple $(x : y : z)$ corresponds to the affine point $\left(\frac{x}{z^2}, \frac{y}{z^3}\right)$.

[3] Note that π is *not* the multiplication by p map, which is another endomorphism that we will see soon.

In order to use these weighted projective coordinates, we need to write down the group law for them. We can do this using the corresponding affine points. For example, to double the point $(x_1 : y_1 : z_1)$ we compute

$$m = \frac{3(x_1/z_1^2) + A}{2(y_1/z_1^3)} = \frac{3x_1^2 + Az_1^4}{2y_1z_1}$$
$$\frac{x_3}{z_3^2} = m^2 - 2\frac{x_1}{z_1^2} = \frac{(3x_1^2 + Az_1^4)^2 - 8x_1y_1^2}{z_3^2} \quad \text{where } z_3 = 2y_1z_1$$
$$\frac{y_3}{z_3^3} = m\left(\frac{x_1}{z_1^2} - \frac{x_3}{z_3^2}\right) - \frac{y_1}{z_1^3} = \frac{(3x_1^2 + Az_1^4)(4x_1y_1^2 - x_3) - 8y_1^4}{z_3^3}.$$

The addition law may be computed similarly.

If we start with a generic point $P = (x : y : 1)$, and apply the group law to compute $2P$, $3P$, $4P$, ... we obtain generic formulas for the multiplication-by-m maps as triples of polynomials $(\phi_m : \omega_m : \psi_m)$ in $\mathbb{Z}[x, y, A, B]$. Here we treat A and B as variables in order to get generic formulas, but in practical applications these will be instantiated with the coefficients of a particular curve equation. To put these formulas in standard form we use the curve equation $y^2 = x^3 + Ax + B$ to reduce powers of y, and then put the maps in affine form $(\phi_m/\psi_m^2, \omega_m/\psi_m^3)$, eliminating any common factors from the numerator and denominator of each coordinate. See the Sage worksheet for details:

https://hensel.mit.edu:8002/home/pub/4/

In principal this approach can be used to generate rational maps for $[m]$ for any m. However, it turns out that the computation can be simplified dramatically by focusing just on the polynomial ψ_m for the z-coordinate, which satisfies a set of recurrences that allow us to compute ψ_m much more efficiently, and can also be used to define the polynomials ϕ_m and ω_m. Thus the polynomials ψ_m are traditionally known as "the" division polynomials, although we may use term more generically to refer to any of the polynomials associated with the multiplication-by-m maps.

Note that the points where ψ_m vanishes are precisely the non-trivial points in the kernel of the endomorphism $[m]$, correspond to the m-torsion subgroup of $E(\overline{k})$. We will see in later lectures that any finite subgroup of $E(\overline{k})$ uniquely determines an isogeny (in this case, an endomorphism), which explains why ψ_m effectively determines $[m]$.

4.4 Division Polynomials

Let $\psi_0 = 0$, and let $\psi_1, \psi_2, \psi_3, \psi_4$ be as computed in Sage:

$$\psi_1 = 1$$
$$\psi_2 = 2y$$
$$\psi_3 = 3x^4 + 6x^2A - A^2 + 12xB$$
$$\psi_4 = 4x^6y + 20x^4yA - 20x^2yA^2 + 80x^3yB - 4yA^3 - 16xyAB - 32yB^2$$

To compute ψ_m for $m > 4$, we may apply the following recurrences:

$$\begin{aligned} \psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, && m \geq 2 \\ \psi_{2m} &= \frac{1}{2y}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2), && m \geq 3 \end{aligned}$$

It is not difficult to show that $\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$ is always divisible by $2y$, so that ψ_{2m} is in fact a polynomial.

We next define the polynomials ϕ_m and ω_m for the x and y coordinates in terms of ψ_m.

$$\begin{aligned} \phi_m &:= x\psi_m^2 - \psi_{m+1}\psi_{m-1} && m \geq 1 \\ \omega_m &:= \frac{1}{4y}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) && m \geq 1,\ \psi_{-1} = -1 \end{aligned}$$

We now record some key properties of these polynomials.

Lemma 3.4.10. *Let $f(x) = x^3 + Ax + B$. Then*

$$\begin{aligned} \psi_n \bmod (y^2 - f(x)) \text{ lies in } &\begin{cases} \mathbb{Z}[x, A, B] & n \text{ odd} \\ 2y\mathbb{Z}[x, A, B] & n \text{ even,} \end{cases} \\ \phi_n \bmod (y^2 - f(x)) \text{ lies in } &\ \mathbb{Z}[x, A, B] \quad \text{for all } n, \\ \omega_n \bmod (y^2 - f(x)) \text{ lies in } &\begin{cases} \mathbb{Z}[x, A, B] & n \text{ even} \\ y\mathbb{Z}[x, A, B] & n \text{ odd.} \end{cases} \end{aligned}$$

Proof. See Lemmas 3.3 and 3.4 in Washington [5]. □

Theorem 3.4.11. *Let $P = (x, y)$ be a point on an elliptic curve $E : y^2 + x^3 + Ax + B$ over a a field of characteristic different from 2. Then*

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x, y)}{\psi_n^3(x, y)}\right) \qquad \text{for all } n > 0.$$

Proof. The standard proof uses complex analysis and the Weierstrass $\wp$-function (as in Chapter 9 of Washington [5]). However, it can be given a purely computational proof using the group law, as we did earlier in Sage. See Exercise 3.7 in Silverman [2]. □

Theorem 3.4.12. *The polynomials ϕ_n and ψ_n are in the form*

$$\begin{aligned} \phi_n(x) &= x^{n^2} + (\text{lower degree terms}), \\ \psi_n(x) &= \begin{cases} nx^{\frac{n^2-1}{2}} + (\text{lower degree terms}), & n \text{ odd} \\ y(nx^{\frac{n^2-4}{2}} + (\text{lower degree terms})), & n \text{ even.} \end{cases} \end{aligned}$$

Proof. We'll just do the case where $n = 2m + 1$ and m is odd, we'll leave the rest as an exercise. In this case the leading term of $\psi_n = \psi_{2m+1}$ is

$$\begin{aligned}
&(m+2)x^{\frac{(m+2)^2-1}{2}}m^3x^{3\cdot\frac{m^2-1}{2}} - (m-1)x^{\frac{(m-1)^2-4}{2}}(m+1)^3x^{3\cdot\frac{(m+1)^2-4}{2}}y^2 \\
&= -(m^4+2m^3)x^{\frac{4m^2+4m}{2}} + (m^4+2m^3+2m+1)x^{\frac{4m^2+4m}{2}} \\
&= (2m+1)x^{\frac{(2m+1)^2-1}{2}} \\
&= nx^{\frac{n^2-1}{2}}.
\end{aligned}$$

□

4.4.1 The degree and separability of the multiplication-by-n map

In several of our later proofs we use the fact that multiplication by n is a separable isogeny whenever $p \nmid n$, and has degree n^2. To prove this, we begin with some easy lemmas.

Lemma 3.4.13. *If $u \perp v$, then $\left(\frac{u}{v}\right)' = 0$ if and only if $u' = v' = 0$.*

Proof. The proof is a simple computation:

$$\left(\frac{u}{v}\right)' = \frac{u'v - uv'}{v^2}$$

If $u' = v' = 0$, then clearly $\left(\frac{u}{v}\right)' = 0$. Conversely, if $\left(\frac{u}{v}\right)' = 0$, then we have $u'v = v'u$. Consider the roots of the left hand side, with multiplicity. Since $u \perp v$, every root of v must be a root of v'. Thus v' has at least $\deg v$ roots. But this is impossible unless $v' = 0$, since otherwise $\deg v' < \deg v$. The same argument shows $u' = 0$. □

In characteristic zero the only polynomials with zero derivatives are the constant functions. But u and v cannot both be constants: if they were then α would have trivial kernel (since $v \neq 0$) and finite image (at most two points have x-coordinate u/v), which is impossible, since its domain $E_1(\overline{k})$ is infinite. Thus in characteristic zero every isogeny is separable. But in positive characteristic things get more interesting.

Lemma 3.4.14. *In any field k, a polynomial $f \in k[x]$ has $f' = 0$ if and only if $f(x) = g(x^p)$ for some $g \in k[x]$, where $p = \operatorname{char} k$.*

Proof. Let $f(x) = \sum_i a_i x^i$. Then $f'(x) = \sum i a_i x^{i-1} = 0$ if and only if $ia_i = 0$ for all i. This holds if and only if $p|i$ for every i with $a_i \neq 0$, equivalently $f(x) = g(x^p)$, where $g(x) = \sum_j a_{pj} x^j$. □

Example 3.4.15: For $k = \mathbb{F}_p$, the Frobenius endomorphism, $\pi(x, y) = (x^p, y^p)$ has degree p and is inseparable, since $(x^p)' = px^{p-1} = 0$ in characteristic p.

Theorem 3.4.16. *The multiplication-by-n map $[n] = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)}\right)$ has degree n^2, and is separable if p does not divide n.*

Proof. We use a shortcut here that simplifies in the proof in Washington [5, Corollary 3.7].

If $\phi_n \perp \psi_n^2$ then the proof follows immediately from Theorem 5.9 given in the last lecture (and proved in Problem Set 2), since the leading term of ϕ_n is x^{n^2} and $\deg \psi_n^2 < n^2$ (note that ϕ_n' has leading coefficient n^2, which is zero only if p divides n).

So suppose that ϕ_n and ψ_n have a common root $x_0 \in \overline{k}$. Let $y_0 \in \overline{k}$ satisfy $y_0^2 = x_0^3 + Ax_0 + B$, where $y^2 = x^3 + Ax + B$ is the Weierstrass equation for E. Notice that such a y_0 exists because $\overline{k}$ is algebraically closed.

We now consider the point $P = (x_0, y_0)$ (which is not 0, because it is an affine point). We may assume $n > 1$, since $\psi_1^2 = 1$ has no roots. From the definition of ϕ_n we have

$$\phi_n(x_0) = x_0\psi_n(x_0)^2 - \psi_{n+1}(x_0)\psi_{n-1}(x_0).$$

Applying $\phi_n(x_0) = \psi_n(x_0) = 0$ yields

$$0 = \psi_{n+1}(x_0)\psi_{n-1}(x_0).$$

Thus x_0 is a root of either ψ_{n+1} or ψ_{n-1}. Note that $nP = 0$ if and only if x_0 is a root of ψ_n, by the definition of $[n]$, see (**??**). Thus either $(n-1)P = 0$ or $(n+1)P = 0$, but in either case we may add or subtract $nP = 0$ to obtain $P = 0$, which is a contradiction. □

5 Appendix: calculations

5.1 The group law in SAGE

The following code computes the group law.

```
RR.<Px,Py,Qx,Qy,Rx,Ry,A,B> = PolynomialRing(QQ,8)
# represent projective points on E uniquely, as either affine points (x,y,1) or
P=(Px,Py,1); Q=(Qx,Qy,1); R=(Rx,Ry,1); O=(0,1,0);
I=RR.ideal(Py^2-Px^3-A*Px-B, Qy^2-Qx^3-A*Qx-B, Ry^2-Rx^3-A*Rx-B)
SS=RR.quotient(I)

def add(P,Q):
    """ general addition algorithm for an elliptic curve in short Weierstrass fo
    if P == O: return Q
    if Q == O: return P
    x1=P[0]; y1=P[1]; x2=Q[0]; y2=Q[1];
    if x1 != x2:
        m = (y2-y1)/(x2-x1)          # usual case: P and Q are distinct and not o
    else:
        if y1 == -y2: return O       # P = -Q (includes case where P=Q is 2-torsi
        m = (3*x1^2+A) / (2*y1)      # P = Q so we are doubling
    x3 = m^2-x1-x2
    y3 = m*(x1-x3)-y1
    return (x3,y3,1)
```

```
def negate(P):
    if P == O: return O
    return (P[0],-P[1],1)

def reduced_fractions_equal(p,q):
    return SS(p.numerator()*q.denominator()-p.denominator()*q.numerator()) == 0

def on_curve(P):
    return reduced_fractions_equal(P[1]^2*P[2],P[0]^3+A*P[0]*P[2]^2+B*P[2]^3)

def equal(P,Q):
    return reduced_fractions_equal(P[0],Q[0]) and reduced_fractions_equal(P[1],Q
```

As a sanity check, let's first verify that the output of add(P,Q) is always on the curve, and check the identity, inverses, and commutativity.

```
print on_curve(O) and on_curve(negate(P)) and on_curve(add(P,Q)) and on_curve(ad
print add(P,O) == P and add(O,P) == P
print add(P,negate(P)) == O
print add(P,Q) == add(Q,P)
```

Chapter 4

Elliptic curves over finite fields

Now that we know how to do arithmetic in finite fields, we can talk about elliptic curves over finite fields. We know that an elliptic curve over a finite field $E(\mathbb{F}_p)$ forms a finite abelian group. The two main questions we will answer are the following:

1. How big is $E(\mathbb{F}_p)$?
2. What is the structure of $E(\mathbb{F}_p)$?

Hasse's Theorem answers the first question by saying that the size of $E(\mathbb{F}_p)$ is remarkably close to the "expected value" $p+1$.

For the second question, we know that any finite abelian group can be written as a direct sum of cyclic groups. Can any direct sum of cyclic groups show up as a possible $E(\mathbb{F}_p)$, or are there constraints?

1 Hasse's Theorem

Let E be the curve $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. A quadratic function $ay^2 + by + c$ in a finite field $\mathbb{F}_q$ attains about half of the values, so given a value of x, there is about a $\frac{1}{2}$ chance that the equation is solvable in y. When it is solvable, there will usually be 2 solutions. Thus we expect the number of solutions to be close to q. Including the point at infinite, the expected number becomes $q+1$. Hasse's Theorem tells us that the number of solutions is not too far from $q+1$.

Theorem 4.1.1. *Let $E/\mathbb{F}_q$ be an elliptic curve. Then*

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

Proof. The idea is to count the number of points of $E(\overline{\mathbb{F}_q})$ in $E(\mathbb{F}_q)$ by viewing $E(\mathbb{F}_q)$ as the kernel of $1 - \phi_q$, where ϕ_q is the Frobenius map. The kernel equals the degree of the map. We know the degree of 1 and ϕ_q; to get the degree of $1 - \phi_q$ we use the fact that deg is a quadratic form, and a version of the Cauchy-Schwarz inequality.

Let $\phi_q : E \to E$ be the qth power Frobenius morphism. Since $\mathbb{F}_q$ consists of exactly the solutions to $x^q = x$, we have

$$\overline{\mathbb{F}_q}^{\phi_q} = \mathbb{F}_q,$$

i.e. the fixed field of $\overline{\mathbb{F}_q}$ under ϕ_q is $\mathbb{F}_q$. Hence $P \in E(\mathbb{F}_q)$ iff $\phi_q(P) = P$, iff $P \in \ker(1 - \phi_q)$. We have

$$|E(K)| = |\ker(1 - \phi_q)| = \deg(1 - \phi).$$

The latter from CITE. SEPARABLE. Now deg is a positive definite quadratic form. We use the following.

Lemma 4.1.2 (Cauchy-Schwarz inequality for groups)**.** *Let A be an abelian group and $d : A \to \mathbb{Z}$ be a positive definite quadratic form. Then for all $\psi, \phi \in A$,*

$$|d(\psi - \phi) - d(\phi) - d(\psi)| \leq 2\sqrt{d(\phi)d(\psi)}$$

(If $d(\phi) = \langle \phi, \phi \rangle$, then the LHS is $2\langle \phi, \phi \rangle$. We don't divide by 2, just so we can stick to something $\mathbb{Z}$-valued.)

Proof. The proof is similar to the proof for the ordinary Cauchy-Schwarz inequality. Since d is a quadratic form,

$$B(\psi, \phi) = d(\psi - \phi) - d(\psi) - d(\phi)$$

is bilinear. Since d is positive definite,

$$0 \leq d(m\psi - n\phi) = m^2 d(\psi) + mnB(\psi, \phi) + n^2 d(\phi).$$

The RHS is quadratic in m and n, hence obtains minimum at $\frac{m}{n} = -\frac{B(\psi,\phi)}{2d(\psi)}$. So take $m = -B(\psi, \phi)$ and $n = 2d(\psi)$. We get

$$0 \leq d(\psi)[4d(\psi)d(\phi) - L(\psi, \phi)^2].$$

When $\psi \neq 0$, we get $4d(\psi)d(\phi) \geq L(\psi, \phi)^2$, from which the desired inequality follows from taking square roots. For $\psi = 0$ the result is obvious. □

Since $\deg \phi_q = q$, the Cauchy-Schwarz inequality gives

$$||E(\mathbb{F}_q)| - 1 - q| = |\deg(1 - \phi) - \deg(1) - \deg(\phi)| \leq 2\sqrt{q}$$

as needed. □

Application to character sums (Silverman, p. 132).

2 Counting points on elliptic curves over finite fields

We now consider the problem of actually computing $\#E(\mathbb{F}_q)$ for an elliptic curve $E/\mathbb{F}_q$ given by a Weierstrass equation $y^2 = x^3 + Ax + B$. The most naïve approach one could take would be to simply evaluate this equation for every pair $(x, y) \in \mathbb{F}_q^2$, count the number of solutions, and then remember to add 1 for the point at infinity. This take $O(q^2\mathsf{M}(\log q))$ time. Note that the input to this problem is simply the pair of coefficients $A, B \in \mathbb{F}_q$, which each have $O(n)$ bits, where $n = \log q$. Thus in terms of the size of the input, this algorithm takes time $O(\exp(2n)\mathsf{M}(n))$, exponential in n. But we can certainly do better.

Recall that for an odd prime p the Legendre symbol $\left(\frac{a}{p}\right)$ satisfies

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } x^2 = a \text{ has two solutions mod } p, \\ 0 & \text{if } x^2 = a \text{ has one solution mod } p, \\ -1 & \text{if } x^2 = a \text{ has no solutions mod } p. \end{cases}$$

We extend the Legendre symbol to finite fields $\mathbb{F}_q$ of odd characteristic by defining

$$\left(\frac{a}{\mathbb{F}_q}\right) = \begin{cases} 1 & \text{if } x^2 = a \text{ has two solutions in } \mathbb{F}_q, \\ 0 & \text{if } x^2 = a \text{ has one solution in } \mathbb{F}_q, \\ -1 & \text{if } x^2 = a \text{ has no solutions in } \mathbb{F}_q. \end{cases}$$

Note that in every case, $1 + \left(\frac{a}{\mathbb{F}_q}\right)$ counts the solutions to $x^2 = a$ in $\mathbb{F}_q$. It follows that

$$\begin{aligned} \#E(\mathbb{F}_q) &= 1 + \sum_{x \in \mathbb{F}_q} \left(1 + \left(\frac{x^3 + Ax + B}{\mathbb{F}_q}\right)\right) \\ &= q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q}\right). \end{aligned} \tag{4.1}$$

We note that Hasse's Theorem is equivalent to the statement that the sum in (4.1) has absolute value bounded by $2\sqrt{q}$. This is remarkable, given that one might naïvely suppose that the sum could potentially have absolute value as large as q.

We can apply (4.1) to compute $\#E(\mathbb{F}_q)$ in $O(\exp(n)\mathsf{M}(n))$ time by computing a table of quadratic residues in $\mathbb{F}_q$ and then evaluating $x^3 + Ax + B$ for all $x \in \mathbb{F}_q$. Alternatively, we can compute the Legendre symbol using Euler's criterion $\left(\frac{a}{p}\right) = a^{(p-1)/2}$, which generalizes to any finite field $\mathbb{F}_q$. This uses much less space, since we don't need to store a table of quadratic residues, but it increases the running time slightly, to $O(\exp(n)\mathsf{M}(n)n)$.

So far we have not yet taken advantage of Hasse's theorem, which tells us that the integer $\#E(\mathbb{F}_q)$ which roughly the same size as q actually lies in an interval of width $4\sqrt{q}$. This suggests that we ought to be able to compute it more efficiently by exploiting this fact. To do so we first consider the problem of computing the order of a point $P \in E(\mathbb{F}_q)$.

2.1 Computing the order of a point

The least positive integer m for which $mP = 0$ is the *order* of P, which we denote $|P|$. We know that $|P|$ must divide the group order $\#E(\mathbb{F}_q)$, thus the *Hasse interval*

$$\mathcal{H}(q) = \big[q + 1 - 2\sqrt{q},\ q + 1 + 2\sqrt{q}\big],$$

contains at least one multiple M of $|P|$, namely, $\#E(\mathbb{F}_q)$. To find such a multiple, we set $M_0 = \lceil q + 1 - 2\sqrt{q} \rceil$, compute M_0P, and then generate the sequence of points

$$M_0P, (M_0 + 1)P, (M_0 + 2)P, \ldots, MP = 0,$$

using repeated addition by P. We then compute the prime factorization $M = p_1^{e_1} \cdots p_w^{e_w}$, which is easy compared to the time required to find M), and compute $m = |P|$ as follows:

1. Set $m = M$.

2. For each prime $p_i|M$, while $p_i|m$ and $(m/p_i)P = 0$ replace m by m/p_i.

When this procedure is complete we know that $mP = 0$ and $(m/p) \neq 0$ for every prime p dividing m, which implies that $m = |P|$. You will analyze the efficiency of this algorithm and develop several improvements to it in Problem Set 2.

The time to compute $|P|$ is dominated by the time for find the initial multiple M, which involves $O(\sqrt{q})$ operations in $E(\mathbb{F}_p)$, yielding a bit complexity of $O(\sqrt{q}\ \mathsf{M}(\log q))$ or $O(\exp(n/2)\mathsf{M}(n)$. We will shortly see how to improve this to $O(\exp(n/4)\mathsf{M}(n))$, but first we consider how we may use our algorithm for computing $|P|$ to compute $\#E(\mathbb{F}_p)$. If we are lucky (and when q is large we usually will be), the multiple M of $|P$ that we find will actually be the *unique* multiple of $|P|$ in $\mathcal{H}(q)$. If this happens, then we must have $M = \#E(\mathbb{F}_q)$. Otherwise, we might try our luck with a different point P. If we can find any combination of points such that the least common multiple of their orders has a unique multiple in $\mathcal{H}(q)$, then we can determine the group order.

2.2 The group exponent

Definition 4.2.1: For a finite group G, the *exponent* of G, denoted $\lambda(G)$, is defined by

$$\lambda(G) = \operatorname{lcm}\{|\alpha| : \alpha \in G\}.$$

Note that $\lambda(G)$ is a divisor of $|G|$ and is divisible by the order of every element of G. Thus $\lambda(G)$ is the maximal possible order of an element of G, and when G is abelian this maximum is achieved: their necessarily exists an element with order $\lambda(G)$. To see this, note that the structure theorem for finite abelian groups allows us to write

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

with $n_i|n_{i+1}$ for $1 \leq i < r$. Thus $\lambda(G) = n_r$, and any generator for $\mathbb{Z}/n_r\mathbb{Z}$ has order $\lambda(G)$.

It is clear that if we compute the least common multiple of a sufficiently large subset of a finite abelian group G we will obtain $\lambda(G)$. If we pick points at random, how many points do we expect to need in order to obtain $\lambda(G)$? The answer is surprisingly small: just two random points are usually enough.

Theorem 4.2.2. *Let G be a finite abelian group with exponent $\lambda(G)$. Let α and β be uniformly distributed random elements of G. Then*

$$\Pr[\mathrm{lcm}(|\alpha|, |\beta|) = \lambda(G)] > \frac{6}{\pi^2}.$$

Proof. We first reduce to the case that G is cyclic. As noted above, G is isomorphic to a direct product of cyclic groups $C_1 \times C_2 \times \cdots \times C_r$, where C_r has order $\lambda(G)$. Let α_r and β_r be the projection of α and β to C_r. Then $\mathrm{lcm}(|\alpha_r|, |\beta_r|) = \lambda(G)$ implies $\mathrm{lcm}(|\alpha|, |\beta|) = \lambda(G)$, and therefore

$$\Pr[\mathrm{lcm}(|\alpha|, |\beta|) = \lambda(G)] \geq \Pr[\mathrm{lcm}(|\alpha_r|, |\beta_r|) = \lambda(G)].$$

So we now assume that G is cyclic with generator γ. Let $p_1^{e_1} \cdots p_k^{e_k}$ be the prime factorization of $\lambda(G)$. Let $\alpha = a\gamma$, with $0 \leq a < \lambda(G)$. Unless a is a multiple of p_i, which occurs with probability $1/p_i$, the order of α will be divisible by $p_i^{e_i}$, and similarly for β. These two probabilities are independent, thus with probability $1 - 1/p_i^2$ at least one of α and β has order divisible by $p_i^{e_i}$. Call this event E_i. The events $E_1, \ldots, E_k$ are independent, since we may write G as a direct product of cyclic groups of order $p_1^{e_1}, \ldots p_k^{e_k}$, and the projections of α and β in each of these cyclic groups are uniformly and independently distributed. Thus

$$\Pr[\mathrm{lcm}(|\alpha|, |\beta|) = \lambda(G)] = \prod_{p|\lambda(G)} (1 - p^{-2}) > \prod_p (1 - p^{-2}) = \left(\sum_{n=1}^{\infty} \frac{1}{n^2}\right)^{-1} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2},$$

where $\zeta(s) = \sum n^{-s}$ is the Riemann zeta function. □

The theorem implies that if we generate random points $P \in E(\mathbb{F}_q)$ and accumulate the least common multiple N of their orders, we should expect to obtain $\lambda(E(\mathbb{F}_q))$ within $O(1)$ iterations. Regardless of when we obtain $\lambda(E(\mathbb{F}_q))$, at every stage we know that N divides $\#E(\mathbb{F}_q)$, and if we ever find that N has a unique multiple in the Hasse interval, then we know that this multiple is the group order. Unfortunately this might not ever happen, it could be that $\lambda(E(\mathbb{F}_q))$ is smaller than $4\sqrt{q}$ and actually has more than one multiple in the Hasse interval. To deal with this problem we need to consider the *quadratic twist* of E.

2.3 The quadratic twist of an elliptic curve

Suppose d is an element of $\mathbb{F}_q$ that is *not* a quadratic residue, so that $\left(\frac{d}{\mathbb{F}_p}\right) = -1$. If we consider the elliptic curve $\tilde{E}$ defined by $y^2 = d(x^3 + Ax + B)$, then

$$\begin{aligned}\#\tilde{E}(\mathbb{F}_q) &= q + 1 + \sum_{x\in\mathbb{F}_q} \left(\frac{d(x^3 + Ax + B)}{\mathbb{F}_q}\right) \\ &= q + 1 + \sum_{x\in\mathbb{F}_q} \left(\frac{d}{\mathbb{F}_q}\right)\left(\frac{(x^3 + Ax + B)}{\mathbb{F}_q}\right) \\ &= q + 1 - \sum_{x\in\mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q}\right).\end{aligned}$$

Thus if $\#E(\mathbb{F}_q) = q + 1 - t$, then $\#\tilde{E}(\mathbb{F}_q) = q + 1 + t$. The curve $\tilde{E}$ is called the *quadratic twist* of E (by d). We can put the curve equation for $\tilde{E}$ in standard Weierstrass form by substituting x/d for x and y/d for y and then clearing denominators, yielding

$$y^2 = x^3 + d^2Ax + d^3B.$$

If we instead choose d to be a (nonzero) quadratic residue, say $d = a^2$, then $\tilde{E}$ is isomorphic to E over $\mathbb{F}_q$ (substitute a^2x for x and a^3y for y and divide both sides by a^6). Moreover, it does not matter which non-residue d we choose: if d and d' are any two non-residues in $\mathbb{F}_q$, then the corresponding curves $\tilde{E}$ and$\tilde{E}'$ are isomorphic over $\mathbb{F}_q$ (use $a^2 = d/d'$ to obtain the isomorphism).

Note that the curves E and $\tilde{E}$ are isomorphic over the quadratic extension $\mathbb{F}_q[x]/(x^2-d) \simeq \mathbb{F}_{q^2}$. In general, curves defined over a field k that are isomorphic over $\overline{k}$ are called *twists*, and if they are isomorphic over a quadratic extension of k they are called *quadratic twists*, as above. This technically includes the case where the curves are already isomorphic over k, but when we refer to "the" quadratic twist of an elliptic curve E we always mean a curve $\tilde{E}$ constructed as above using a non-residue $d \in k$ so that E and $\tilde{E}$ is not isomorphic.

Our interest in the quadratic twist of E lies in the fact that

$$\#E(\mathbb{F}_q) + \#\tilde{E}(\mathbb{F}_q) = 2q + 2.$$

Thus if we can compute either $\#E(\mathbb{F}_q)$ or $\#\tilde{E}(\mathbb{F}_q)$ than we can easily determine both values.

2.4 Mestre's Theorem

It is not necessarily the case that the group exponent of $\lambda(E(\mathbb{F}_p))$ has a unique multiple in the Hasse interval. But if we also consider the quadratic twist $\tilde{E}(\mathbb{F}_p)$, then a theorem of Mestre (published by Schoof in [**?**]) ensures that for all sufficiently large p, either $\lambda(E(\mathbb{F}_p))$ or $\lambda(\tilde{E}(\mathbb{F}_p))$ has a unique multiple in the Hasse interval $\mathcal{H}(p) = [(\sqrt{p}-1)^2, (\sqrt{p}+1)^2]$.

Theorem 4.2.3 (Mestre)**.** *Let $p > 229$ be prime, and let $E/\mathbb{F}_p$ be an elliptic curve with quadratic twist $\tilde{E}/\mathbb{F}_p$. Then either $\lambda(E(\mathbb{F}_p))$ or $\lambda(\tilde{E}(\mathbb{F}_p)$ has a unique multiple in $\mathcal{H}(p)$.*

Proof. Let $E(\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ and $\tilde{E}(\mathbb{F}_p) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z}$, where $n|N$ and $m|M$. We have $E[n] = E(\mathbb{F}_p)[n]$, so the Frobenius endomorphism π fixes $E[n]$ and the matrix π_n is the identity. Thus $p = \deg \pi \equiv_n \det \pi_n = 1$, thus n divides $p-1$. By the same argument, so does m.

Let $t = p + 1 - nN$ be the trace of Frobenius of E. Then

$$\begin{aligned} 4p - t^2 &= 4p - (p+1-nN)^2 \\ &\equiv_{n^2} 4p - (p+1)^2 = 4p - p^2 - 2p - 1 = -(p-1)^2 \\ &\equiv_{n^2} 0 \end{aligned}$$

Thus n^2 divides $4p - t^2$, and so does m^2, by the same argument.

Since n divides nN and $p-1$, we have $t = p - 1 + 2 - nN \equiv_n 2$, and similarly $t \equiv_m -2$. Thus $t = an + 2$ and $t = bm - 2$, for some integers a and b, and subtracting these equations yields $an - bm = 4$, which implies $\gcd(m, n) \leq 4$. Therefore $\gcd(m^2, n^2) \leq 16$, and since m^2 and n^2 both divide $4p - t^2$, we have

$$\frac{m^2 n^2}{16} \leq 4p - t^2 \leq 4p \tag{4.2}$$

Now suppose for the sake of contradiction that $N = \lambda(E(\mathbb{F}_p))$ and $M = \lambda(\tilde{E}(\mathbb{F}_p))$ both have more than one multiple in $\mathcal{H}(p)$. Then M and N are both at most $\sqrt{4p}$, so $MN \leq 4p$. Since mM and nN lie in $\mathcal{H}(p)$, they are both greater than $(\sqrt{p}-1)^2$, hence $mnMN \geq (\sqrt{p}-1)^4$. It follows that $mn \geq (\sqrt{p}-1)^4/(4p)$. Dividing by 4 and squaring both sides yields

$$\frac{m^2 n^2}{16} \geq \frac{(\sqrt{p}-1)^8}{256p^2}. \tag{4.3}$$

Combining (4.2) and (4.3) yields

$$1024p^3 \geq (\sqrt{p}-1)^8. \tag{4.4}$$

This implies that if neither M nor N have a unique multiple in $\mathcal{H}(p)$, then $p \leq 1284$. An exhaustive computer search for $p \leq 1284$ then finds that in fact we must have $p \leq 229$. □

2.5 Computing the group order with Mestre's Theorem

We now give a complete algorithm to compute $\#E(\mathbb{F}_p)$ using Mestre's theorem, assuming that p is a prime greater than 229 (if p is smaller than this we can easily just count points as before).[1] As usual, $\mathcal{H}(p) = [p + 1 - 2\sqrt{p},\ p + 1 + 2\sqrt{p}]$ denotes the Hasse interval.

1. Compute a quadratic twist $\tilde{E}$ of E using a randomly chosen non-residue $d \in \mathbb{F}_q$.
2. Let $E_0 = E$ and $E_1 = \tilde{E}$, set $N_0 = N_1 = 1$ and $i = 0$.

[1] There is a generalization of Mestre's theorem that applies to arbitrary finite fields $\mathbb{F}_q$, and handles all $q > 49$, see [**?**]. With this the algorithm we give here can be modified to handle arbitrary finite fields.

3. While neither N_0 nor N_1 has a unique multiple in $\mathcal{H}(p)$:
   a. Generate a random point $P \in E_i(\mathbb{F}_p)$.
   b. Find an integer $M \in \mathcal{H}p$ such that $MP = 0$.
   c. Use M to compute $|P|$ as in §2.1.
   d. Set $N_i = \operatorname{lcm}(N_i, |P|)$ and set $i = 1 - i$.
4. If N_0 has a unique multiple M in $\mathcal{H}(p)$ then return M, otherwise return $2p + 2 - M$, where M is the unique multiple of N_1 in $\mathcal{H}(p)$.

It is clear that the output of the algorithm is correct, and it follows from Theorems 4.2.2 and 4.2.3 that the expected number of iterations of step 3 is $O(1)$. Thus we have a Las Vegas algorithm to compute $\#E(\mathbb{F}_p)$. Its running time is dominated by the time to find M in step 3b. If we simply compute aP for every integer $a \in \mathcal{H}(p)$, we obtain an expected running time of $O(\sqrt{p}\,\mathsf{M}(\log p)$, or $O(\exp(n/2)\mathsf{M}(n)$, but this can be improved to $O(\exp(n/4)\mathsf{M}(n))$ if we speed up step 3b using the baby-steps giant-steps method discussed below.

2.6 The baby-steps giant-steps method

Let $a = \lceil p+1-2\sqrt{p} \rceil$ and let $b = \lceil p+1+2\sqrt{p} \rceil$, so $[a, b)$ contains every integer in the Hasse interval $\mathcal{H}(p)$. In its simplest form, the baby-steps giant-steps method proceeds as follows:

1. Pick integers r and s such that $rs \geq b - a$.
2. Compute the set $S_{\text{baby}} = \{0, P, 2P, \ldots, (r-1)P\}$ of *baby steps*.
3. Compute the set $S_{\text{giant}} = \{aP, (a+r)P, (a+2r)P, \ldots, (a+(s-1)r)P\}$ of *giant steps*.
4. For each giant step $P_{\text{giant}} = (a + ir)P \in S_{\text{giant}}$, check whether its negation is equal to a baby step $P_{\text{baby}} = jP \in S_{\text{baby}}$, and if so output $M = a + ir + j$.

Note that $-P_{\text{giant}} = P_{\text{baby}}$ implies $P_{\text{giant}} + P_{\text{baby}} = (a + ir)P + jP = MP = 0$, thus M is a multiple of $|P|$. Since *every* integer in $\mathcal{H}(p)$ can be written in the form $a + i + jr$ with $0 \leq i < r$ and $0 \leq j < s$, the algorithm is guaranteed to find such an M.

To implement this algorithm efficiently, we typically store the baby steps S_{baby} in a lookup table (e.g. a binary tree or a hash table) and as each giant step $P_{rmgiant}$ is computed, we lookup $-P_{\text{giant}}$ in this table. Alternatively, one may compute the sets S_{baby} and S_{giant} in their entirety, sort both sets, and then efficiently search for a match. In both cases, we assume that the points in S_{baby} and S_{giant} are uniquely represented, which may require converting them to affine form. In the next lecture we will see how *batching* can be used to do this efficiently. Assuming this is done, if we choose $r \approx s \approx 2p^{1/4}$, then the running time of the algorithm above is $O(\exp(n/4)\mathsf{M}(n))$.

Note that its space complexity is $O(\exp(n/4)n)$, which is actually the limiting factor in practically implementations, thus one may choose to make a time-space trade-off by picking a smaller value for r and a larger values of s. We will discuss this and other optimizations to the baby-steps giant-steps method in the next lecture.

Chapter 5

Cryptography and other applications

Chapter 6

Modular forms

(Placeholder)

Chapter 7

Elliptic cuves over $\mathbb{C}$

Chapter 8

Formal groups

Why are we interested in elliptic curves over different fields? We are interested in elliptic curves over $\mathbb{Q}$ because much of number theory is concerned with solving equations over $\mathbb{Q}$; we are interested in elliptic curves over finite fields k because of its applications to cryptography, factoring, and primality proving.

On the other hand, even if we just wanted information about an elliptic curve E over $\mathbb{Q}$, it helps to investigate it over other fields. $\mathbb{Q}$ is a difficult field to work with because it is a *global* field. So we make two reductions.

1. Consider E over the local fields $\mathbb{Q}_p$ (and $\mathbb{C}$!). Then combine this information to get information on $E(\mathbb{Q})$.

2. Consider E over finite fields $\mathbb{F}_p = \mathbb{Q}_p/p\mathbb{Q}_p$. Use this to get information about E over local fields $\mathbb{Q}_p$.

We look at item 2 more closely. Suppose K is a local field; let k be its residue field. Note that when we reduce an elliptic curve modulo p, some points will get sent to 0; this is the kernel of reduction $E_1(K)$. Thus we get a exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_1(K) & \longrightarrow & E_0(K) & \longrightarrow & \widetilde{E}_{\mathrm{ns}}(k) & \longrightarrow & 0 \\ & & \| & & & & & & \\ & & \widehat{E}(\mathfrak{m}) & & & & & & \end{array}$$

(Here we have the technicality that when we reduce to k, some points may be singular, so $E_0(K)$ is the set of nonsingular points.) How can we study $E_1(K)$? We know these are points whose coordinates are in the maximal ideal $\mathfrak{m}$ associated to K (so get sent to 0 upon reduction). To get these points we take a uniformizer $z \in \mathfrak{m}$, and write the coordinates of a point in $E_0(K)$ as power series in z. Thus we investigate the elliptic curve over a *ring of formal power series*, and the group law becomes a group law for power series, called a *formal group law* (see Section BLAH). We then get to $E(K)$ from the exact sequence $0 \to E_0(K) \to E(K) \to E(K)/E_0(K) \to 0$; fortunately, $E(K)/E_0(K)$ is finite.

To get from E over local fields to E over global fields, we would like to use the Hasse principle as in quadratic forms. However, this fails. There is, however, a way of measuring the failure of the Hasse principle using the Selmer and Shafarevich-Tate groups (see Silverman, X).

! $E_1(K)$ is the set of points which "in the maximal ideal," i.e., are 0 modulo k. But this is with respect to the equation where the point at infinity has been transformed to the origin, so in the original coordinates, they are points with powers of π in the *denominator*, not the numerator.

1 Formal groups

A formal group is basically a group law defined on power series. It can be thought of as a "group law without a group"; for applications we will this group law operate on a maximal ideal in a complete ring. (This way, the power series for the group law will converge.)

Definition 8.1.1: A (1-dimensional commutative) **formal group** $\mathscr{F}$ over the ring R is a power series $F(X,Y) \in R[[X,Y]]$ satisfying the following three conditions.

1. $F(X,Y) = X + Y \pmod{(X,Y)^2}$.
2. (Associativity) $F(F(X,Y),Z) = F(X,F(Y,Z))$.
3. (Commutativity) $F(X,Y) = F(Y,X)$.

We also write $X +_F Y$ for $F(X,Y)$.

Proposition 8.1.2: Keep the above notation. A formal group has the following additional properties:

4. (Inverse) There is a unique power series $i(T) \in R[[T]]$ such that $F(T,i(T)) = 0$.
5. (Identity) $F(X,0) = F(0,X) = X$.

Formal groups originally appeared geometrically: Suppose we are interested in an infinitesimal neighborhood of a point on a variety. Consider the ring of rational functions defined in this infinitesimal neighborhood. Taking the completion of this ring, we get a ring of power series; the variable is an uniformizer.[1]

[1]For the scheme-theoretically inclined, imagine a group law on $\mathbb{A}^1_{\operatorname{Spec} A} = \operatorname{Spec} A[T]$; we have to give a multiplication map

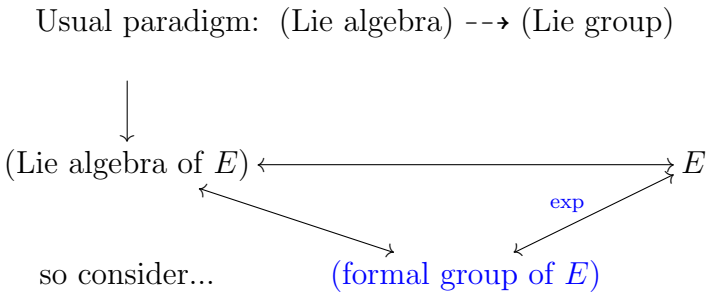
$$\begin{gathered}\mathbb{A}^1_{\operatorname{Spec} A} \to \mathbb{A}^1_{\operatorname{Spec} A} \\ \operatorname{Spec} A[X] \otimes_A A[Y] \to \operatorname{Spec} A[T] \\ A[X,Y] \leftarrow\!\shortmid A[T].\end{gathered}$$

1.1 Formal groups and Lie algebras

One can say that formal groups are like an intermediate between *Lie algebras* and *Lie groups*[2] (in a way we won't make precise), going from

1. the complete local ring (power series ring) R at a point, to
2. a subset of points on the curve.

An elliptic curve is a Lie group, and the tangent space at 0 forms a 1-dimensional (trivial) Lie algebra.



The analogy is the following.

1. The Lie algebra is the tangent space at a point *with a Lie bracket* $[,]$, and that under the *exponential map*, a vector in the tangent space gets sent to a point on the Lie group (manifold) in the the direction and magnitude of that vector. The Lie bracket tells us about how the group law on the Lie group works (and in particular measures the failure of commutativity).
2. Here, the formal group law will take the place of the Lie bracket, "transfering" the group law from the curve to the power series ring. We will see there similarly exists an exponential map that identifies R with the formal group operation, to R with normal addition of power series. (Since the group law is commutative, we don't really want to consider a Lie algebra, which would be trivial; we say that the formal group is an intermediary, in that it gives more information.) There is a caveat that since we plan to work over local rings (rather than over $\mathbb{C}$ as with classical Lie groups), we can map to points on the curve in the maximal ideal, as mentioned in the introduction.

1.2 Basic examples

The formal group law will be easier to study than addition on the curve, because we are just working in a power series ring, and we understand the algebra of a power series ring

This is equivalent to giving the image of T in $A[X,Y]$. Looking at it locally (say at 0) means localizing at (x), giving a power series.

[2] A Lie group is basically a manifold with a continuous group structure. A Lie algebra is an algebra with a *bracket* operation that "measures" noncommutativity.

very well (it's almost like just working with polynomials!). Thus formal groups are useful in simplifying problems in algebraic number theory and geometry.

Example 8.1.3: The formal additive $\hat{\mathbb{G}}_a$ and multiplicative groups $\hat{\mathbb{G}}_m$ are given by

$$F(X,Y) = X + Y$$
$$F(X,Y) = X + Y + XY = (1+X)(1+Y) - 1.$$

To motivate this, consider the group varieties $\mathbb{G}_a(K) = K^+$ and $\mathbb{G}_m(K) = K^\times$. For $\hat{\mathbb{G}}_a$, we consider the local ring at 0, and for $\hat{\mathbb{G}}_m$ we consider the local ring at 1; the law is just "multiplication around 1." Let $s = x - 1$ be a uniformizer. Thinking of the expression $x - 1$ as something where we substitute an actual number for x, if $s = x - 1$ and $t = y - 1$, then the product is xy, and $xy - 1 = (s+1)(t+1) - 1$, hence the formula.

Definition 8.1.4: A homomorphism from $(\mathscr{F}, F)$ to $(\mathscr{G}, G)$ is a power series $f(T) \in R[[T]]$ with

$$f(F(X,Y)) = G(f(X), f(Y)).$$

$\mathscr{F}$ and $\mathscr{G}$ are isomorphic over R if there are homomorphisms $f : \mathscr{F} \to \mathscr{G}$ and $g : \mathscr{G} \to \mathscr{F}$ such that $f(g(T)) = g(f(T)) = T$.

Note we must have $f(X) \in \langle X \rangle$.

2 Formal groups over DVR's

We use the formal group to study p-torsion.

Proposition 8.2.1 (Silverman IV.4.3)**:** Let $\mathscr{F}, \mathscr{G}$ be formal groups with normalized invariant differentials $\omega_{\mathscr{F}}, \omega_{\mathscr{G}}$. Then

$$\omega_{\mathscr{G}}(f) = f'(0)\omega_{\mathscr{F}}$$

The key proposition we will repeatedly use is the following, which tells us what the formal series for multiplication by p looks like.

Proposition 8.2.2: Let $\mathscr{F}/R$ be a formal group and p a prime. Then there exist power series $f, g \in tR[[t]]$ such that

$$[p]T = pf(T) + g(T^p).$$

Proof. □

The "T^p" term above suggests some kind of "ramification" happening when we work over local fields of characteristic p. (Example: $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ is ramified, and ζ_p satisfies $X^p - 1 = 0$.) We now use formal groups to investigate p-torsion points.

Proposition 8.2.3: Let R be complete with maximal ideal $\mathfrak{m}$, and let $\mathscr{F}/R$ be a formal group. Suppose $x \in \mathscr{F}(\mathfrak{m})$ is a p^n-torsion point: $[p^n]x = 0$. Then

$$v(x) \leq \frac{v(p)}{p^n - p^{n-1}}.$$

Example 8.2.4: This already gives us something nonobvious when applied to $\mathbb{G}_m(\mathbb{Q}_p)$. Namely, let $x = \zeta_{p^n} - 1$ (recall that $s \in \mathbb{Q}_p^\times$ will be represented by $s-1$ in the formal group). The above says

$$v(\zeta_{p^n} - 1) \leq \frac{1}{p^n - p^{n-1}}$$

and therefore equality must occur (). Since ζ_{p^n} satisfies $X^{p^n - p^{n-1}} + \cdots + X^{p^{n-1}} + 1 = 0$, we get that $\mathbb{Q}_p[\zeta_{p^n} - 1]/\mathbb{Q}_p$ is totally ramified of degree $p^n - p^{n-1}$, and that $\zeta_{p^n} - 1$ is a uniformizer in the extension.

Proof. □

Now we consider formal groups in characteristic p.

Problem 8.2.5: We showed that $\exp_{\mathscr{F}} : \hat{\mathbb{G}}^a \to \mathscr{F}$ over R when R has characteristic 0. What goes wrong if the residue field of R has positive characteristic? Can you salvage it with a weaker result?

The problem is that the power series for $\exp_{\mathscr{F}}$ may not converge! But when a power series doesn't converge, *look at a smaller neighborhood.* When do they converge? We find a criterion on the coefficients using some basic calcuations with valuations. [3]

Proposition 8.2.6: 1. The power series

$$f(T) = \sum_{n=1}^{\infty} \frac{a_n}{n} T^n$$

converges for $v_p(T) > 0$.

2. The power series

$$g(T) = \sum_{n=1}^{\infty} \frac{b_n}{n!} T^n.$$

converges for $v_p(T) \geq \frac{v(p)}{p-1}$ with $v(g(x)) = v(x)$.

Proof. The valuation of a factorial satisfies $v_p(n!) < (n-1)\frac{v(p)}{p-1}$.
Just do it! □

Thus we get a isomorphism on an open subset of R.

[3] (Note to self: look at subgroup-trivial-cohom in CFT, same stategy of looking at subset?)

Theorem 8.2.7 (Silverman 6.4)**.** *The formal logarithm induces an isomorphism*

$$\log_{\mathscr{F}} \mathscr{F}(\mathfrak{m}^r) \to \hat{\mathbb{G}}^a(\mathfrak{m}^r)$$

when $r > \frac{v(p)}{p-1}$.

Note that we only have trouble defining the reverse map (exp) in the backwards direction, so we can define $\log_{\mathscr{F}} : \mathscr{F}(\mathfrak{m}) \to K^+$, but this will not be a homomorphism of formal groups, and only be a homomorphism of groups.

This theorem will tell us that when K is a local field, there is a subgroup of $E(K)$ isomorphic to K^+.

3 Formal groups in characteristic p

In characteristic p, the first term in 8.2.2 disappears. Then we get $f(T) = g(T^p)$. This reminds us of separability, and we know separability is an issue for isogenies between elliptic curves in characteristic p. (Moreover, this separability can be measured by looking at the powers in the polynomials defining the isogenies.) Is there a way we can naturally connect

1. separability degree of isogenies between elliptic curves with
2. homomorphisms of formal groups?

Yes.

Definition 8.3.1: Let $f : \mathscr{F} \to \mathscr{G}$ be a homomorphism of formal groups over R of characteristic p. Define the **height** $\mathrm{ht}(f)$ to be the largest h such that there exists a power series g with

$$f(T) = g(T^{p^h}).$$

Theorem 8.3.2. *Let K be a field of characteristic $p > 0$, $E_1, E_2/K$ be elliptic curves, and $\phi : E_1 \to E_2$ be an isogeny. Let $\mathscr{F} : \hat{E}_1 \to \hat{E}_2$ be the associated homomorphism of formal groups. Then*

$$p^{ht(f)} = \deg_i(\phi).$$

For any elliptic curve,

$$ht(\hat{E}) = 1 \text{ or } 2.$$

We first prove some basic facts about heights using the invariant differential.

Proposition 8.3.3: Let $f : \mathscr{F} \to \mathscr{G}$ be a homomorphism of formal groups over R.

1. If $h = \mathrm{ht}(f)$ and $f(T) = g(T^{p^h})$, then $g'(0) \neq 0$. In particular, if $f'(0) = 0$, then $\mathrm{ht}(f) \geq 1$, i.e., $f(T) = g(T^p)$ for some $g \in R[[T]]$.

2. (Height is additive) Given $g : \mathscr{G} \to \mathscr{H}$, we have

$$\mathrm{ht}(g \circ f) = \mathrm{ht}(f) + \mathrm{ht}(g).$$

Compare the additivity of height with the multiplicativity of degree.

Proof. 1. We first show the "in particular" part. Let $\omega_{\mathscr{G}} = P(T)\,dT$. We write $\omega_{\mathscr{G}}(f(T))$ in two ways:

$$\omega_{\mathscr{G}}(f(T)) = f'(0)\omega_{\mathscr{F}}(T) = 0$$
$$\omega_{\mathscr{G}}(f(T)) = P(f(T))f'(T)\,dT.$$

Since $P(f(T)) \in R[[T]]$, we get $f'(T) = 0$ in R. Since we are in characteristic p, this implies $f(T) = g(T^p)$ for some $g \in R[[T]]$.

We already have the result for the case $h = 0$. How do we reduce the general case to this? By using the p^hth power Frobenius. Let $\mathscr{F}^{(q)}$ denote the formal group with law $\sum a_{ij}^p X^i Y^j$. Since taking the qth power is a homomorphism in characteristic p, the homomorphism f transfers to a formal group law $g : \mathscr{F}^{(q)} \to \mathscr{G}^{(q)}$.

$$\begin{array}{ccc} (\mathscr{F}, F) & \xrightarrow{f} & (\mathscr{G}, G) \\ \hat{}q \downarrow & & \downarrow \hat{}q \\ (\mathscr{F}, F^{(q)}) & \xrightarrow{g} & (\mathscr{G}^{(q)}, G). \end{array}$$

$$\begin{aligned} g(F^{(q)}(X^q, Y^q)) &= f(F(X, Y)) \\ &= G(f(X), f(Y)) \\ &= G(g(X^q), g(Y^q)), \end{aligned}$$

i.e., g is a homomorphism of formal groups $\mathscr{F} \to \mathscr{G}$.

Now, the fact that $\mathscr{F}$ has height h means that g has height 0. We've shown this means $g = 0$.

2. This follows immediately from the characterization in part 1, after writing $f = f_1(T^{p^{\mathrm{ht}(f)}})$ and $g = g_1(T^{p^{\mathrm{ht}(g)}})$.

□

Proof of Theorem 8.3.2. Every isogeny can be written as a composition of a separable and purely inseparable (namely, the Frobenius) isogeny. Since degree is multiplicative and height is additive (Proposition 8.3.3), it suffices to show the theorem for separable and purely inseparable isogenies.

1. For the Frobenius isogeny, $\deg_i(\phi_q) = q$, and the associated homomorphism of formal groups is T^q, so the theorem checks.

2. For a separable isogeny, $\deg_i(\phi) = 1$. We will use the differential as a way to go between the degree of the isogeny and the height of the associated homomorphism of formal groups. Separability implies $\phi^*\omega \neq 0$. In the realm of formal groups this says $\omega_{\mathscr{G}} \circ f \neq 0$, or $f'(0)\omega_{\mathscr{F}} \neq 0$. (Check that $\omega_{\mathscr{G}}$ corresponds to ω.) Thus $f'(0) \neq 0$, and Proposition 8.3.3 tells us the height is 0.

For the second part, note that $\deg_i([p]) = p$ or p^2, so $\mathrm{ht}([p]) = 1$ or 2. □

cf. ANT inseparability?

Chapter 9

Elliptic curves over local fields

1 Introduction

Let K be a field.

Definition 9.1.1: $v : K^\times \to \mathbb{Z}$ is a **discrete valuation** if

1. $v(xy) = v(x) + x(y)$.
2. $v(x + y) \geq \min(v(x), v(y))$.

($v(0)$ is either 0 or undefined.)

Example 9.1.2: 1. $K = \mathbb{Q}$ prime. $v = v_p$ where $v_p(p^r \frac{a}{b}) = r$ with $a, b \in \mathbb{Z}$ coprime to p.

2. $[K : \mathbb{Q}] < \infty$, ring of integers $\mathscr{O}_K$ where $\mathfrak{p} \subseteq \mathscr{O}_K$ is a prime ideal.
We have $v = v_\mathfrak{p}$ where $v_\mathfrak{p}(x)$ is the power of $\mathfrak{p}$ in the factorization of $x\mathscr{O}_K$ into prime ideals.

Remark 9.1.3: Let $x, y \in K$. The definition gives

$$\begin{cases} v(x+y) & \geq \min(v(x), v(y)) \\ v(x) & \geq \min(v(x+y), v(y) = v(-y)). \end{cases}$$

So if $v(x) < x(y)$ then $v(x+y) = v(x)$. Hence if $v(x) \neq v(y)$, then $v(x+y) = \min(v(x), v(y))$.

Lemma 9.1.4. *Let E/K be an elliptic curve, with Weierstrass equation*

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

Assume $v(a_i) \geq 0$ for all i. Let $O \neq P = (x, y) \in E(K)$. Then either

1. *$v(x), v(y) \geq 0$, or*

2. $v(x) = -2r, v(y) = -3r$ *for some* $r \geq 1$.

Proof. Case $v(x) \geq 0$: Suppose $v(y) < 0$. Then $v(y^2 + a_1xy + a_3y) = 2v(y) < 0$ and $v(RHS) \geq 0$, contradiction. Thus $v(y) \geq 0$.

Case $v(x) < 0$: We have $v(LHS) \geq \min(2v(y), v(x) + v(y), v(y))$, $v(RHS) = 3v(x)$, and therefore (checking a few cases) $v(y) < v(x) < 0$. Then $v(LHS) = 2v(y)$. Thus $v(x) = -2r$, $v(y) = -3r$ for some $r \geq 1$. □

Notation: Denote the valuation ring, unit group, maximal ideal, and residue field by

$$\begin{aligned} \mathscr{O}_K &= \{x \in K^\times : v(x) \geq 0\} \cup \{0\} \\ \mathscr{O}_K^\times &= \{x \in K^\times : v(x) = 0\} \cup \{0\} \\ \pi\mathscr{O}_K &= \{x \in K^\times : v(x) \geq 1\} \qquad \text{picking } \pi \in K, v(\pi) = 1. \\ k &= \mathscr{O}_K/\pi\mathscr{O}_K. \end{aligned}$$

Definition 9.1.5: A Weierstrass equation for E with coefficients $a_1, \ldots, a_6 \in K$ is

1. **integral** if $a_1, \ldots, a_6 \in \mathscr{O}_K$.

2. **minimal** if $v(\Delta)$ is minimal among all integral models for E (among all the Weierstrass equations you can write down).

Remark 9.1.6:

1. Putting $x = u^2x'$ and $y = u^3y'$ gives $a_i = u^ia_i'$, therefore integral models exist.

2. $a_1, \ldots, a_6 \in \mathscr{O}_K$ gives $\Delta \in \mathscr{O}_K$ and $v(\Delta) \in \mathbb{N}_0$.

We'd like to apply formal groups to elliptic curves over local fields.
Fixing any $0 < c < 1$ we define a metric on K by

$$\begin{cases} c^{v(x-y)} & \text{if } x \neq y \\ 0 & \text{if} x = y. \end{cases}$$

Definition 9.1.1 gives

$$d(x, z) \leq \max(d(x, y), d(y, z)),$$

the ultrametric inequality (much stronger than the triangle inequality). Let $\hat{K}$ be the completion of K with respect to d. By continuity, $+, \times$ extend to $\hat{K}$, so $\hat{K}$ is a field. v extends to $\hat{K}$ and is a discrete valuation. Note that the residue field does not change.

In examples 1 and 2, we write $\hat{K} = \mathbb{Q}_p$ and $K_\mathfrak{p}$. For the rest of this section, K is a field complete with respect to a discrete valuation $v : K^\times \to \mathbb{Z}$. $\mathscr{O}_K, \pi, k$ are defined as before.

We further assume $\mathrm{char}(K) = 0$ and $\mathrm{char}(k) = p > 0$. (For example, $K = \mathbb{Q}_p$, $\mathscr{O}_K = \mathbb{Z}_p$, $\pi\mathscr{O}_K = p\mathbb{Z}_p$, $k = \mathbb{F}_p$.) K is complete so $\mathscr{O}_K$ is complete with respect to $\pi^r\mathscr{O}_K$ for any $r \geq 1$. In §7 we put $t = -\frac{x}{y}$ we put $t = -\frac{x}{y}$, $w = -\frac{1}{y}$. Then

$$\begin{aligned}\hat{E}(\pi^r\mathscr{O}_K) &= \left\{(x,y) \in E(K) : -\frac{x}{y}, -\frac{1}{y} \in \pi^r\mathscr{O}_K\right\} \cup \{0\} \\ &= \left\{(x,y) \in E(K) : v\left(\frac{x}{y}\right), v\left(\frac{1}{y}\right) \geq r\right\} \cup \{0\} \\ &\overset{\text{Lem. 9.1.4}}{=} \{(x,y) \in E(K) : v(x) \leq -2r, v(y) \leq -3r\} \cup \{0\}.\end{aligned}$$

By Lemma **??**, this is a subgroup of $E(K)$, say $E_r(K)$.

Thu. 7/11

We get a filtration

$$\cdots \subseteq E_3(K) \subseteq E_2(K) \subseteq E_1(K) = \hat{E}(\pi\mathscr{O}_K).$$

More generally, if $\mathscr{F}$ is a formal group over $\mathscr{O}_K$,

$$\cdots \subseteq \mathscr{F}(\pi^3\mathscr{O}_K) \subseteq \mathscr{F}(\pi^2\mathscr{O}_K) \subseteq \mathscr{F}(\pi\mathscr{O}_K).$$

Proposition 9.1.7: Let $\mathscr{F}$ be a formal group over $\mathscr{O}_K$. Let $e = v(p)$. If $r > \frac{e}{p-1}$, then

$$\begin{aligned}\log &: \mathscr{F}(\pi^r\mathscr{O}_K) \to \widehat{\mathbb{G}}_a(\pi^r\mathscr{O}_K) \\ \exp &: \widehat{\mathbb{G}}_a(\pi^r\mathscr{O}_K) \to \mathscr{F}(\pi^r\mathscr{O}_K)\end{aligned}$$

are inverse homomorphisms.

Proof. Let $x \in \pi^r\mathscr{O}_K$. We must show the power series exp and log of Theorem **??** converge. Then the fact they are homomorphism and inverses will follow from what we've already shown. Recall

$$\exp(T) = T + \frac{b_2}{2!}T^2 + \frac{b_3}{3!}T^3 + \cdots$$

for $b_2, b_3, \ldots, \in \mathscr{O}_K$. We have

$$\begin{aligned}v(n!) &= ev_p(n!) \\ &= e\left(\sum_{j=1}^{m}\left\lfloor\frac{n}{p^j}\right\rfloor\right), \qquad p^m \leq n < p^{m+1} \\ &\leq e\sum_{j=1}^{m}\frac{n}{p^j} \\ &= en\frac{\frac{1}{p} - \frac{1}{p^{m+1}}}{1-\frac{1}{p}} \\ &= en\frac{1}{p-1}(1-p^{-m}) \leq \frac{e}{p-1}(n-1).\end{aligned}$$

Therefore

$$\begin{aligned} v\left(\frac{b_n}{n!}x^n\right) &\geq nr - \frac{e}{p-1}(n-1) \\ &= (n-1)\underbrace{\left(r - \frac{e}{p-1}\right)}_{>0} + r. \end{aligned}$$

This is $\geq r$ and goes to ∞ as $n \to \infty$. Because we have the ultrametric law, convergence of terms in a sum implies convergence of the sum. Thus $\exp(x)$ converges and belongs to $\pi^r \mathscr{O}_K$.

For log the denominators are smaller, so a fortiori the series for log converges.[1] □

So for r sufficiently large,

$$\mathscr{F}(\pi^r \mathscr{O}_K) \cong \widehat{\mathbb{G}}_a(\pi^r \mathscr{O}_K) \cong (\pi^r \mathscr{O}_K, +) \cong (\mathscr{O}_K, +).$$

Lemma 9.1.8 (Filtration of formal groups)**.** *If $r \geq 1$ then $\frac{\mathscr{F}(\pi^r \mathscr{O}_K)}{\mathscr{F}(\pi^{r+1} \mathscr{O}_K)} \cong (k, +)$.*

Proof. note $F(X, Y) = X + Y + XY(\cdots)$. If $x, y \in \mathscr{O}_K$ then $F(\pi^r x, \pi^r y) \equiv \pi^r(x + y) \pmod{\pi^{r+1}}$. We get a group homomorphism

$$\begin{aligned} \mathscr{F}(\pi^r \mathscr{O}_K) &\to k \\ \pi^r x &\mapsto x \pmod{\pi} \end{aligned}$$

surjective (by definition of k as a residue field) with kernel $\mathscr{F}(\pi^{r+1} \mathscr{O}_K)$. Hence

$$\frac{\mathscr{F}(\pi^r \mathscr{O}_K)}{\mathscr{F}(\pi^{r+1} \mathscr{O}_K)} \xrightarrow{\cong} (k, +).$$

□

Corollary 9.1.9. *If $|k| < \infty$ then $\mathscr{F}(\pi \mathscr{O}_K)$ has a subgroup of finite index isomorphic to $(\mathscr{O}_K, +)$.*

We use the following notation for reduction modulo π:

$$\begin{aligned} \mathscr{O}_K &\to \frac{\mathscr{O}_K}{\pi \mathscr{O}_K} = k \\ x &\mapsto \widetilde{x}. \end{aligned}$$

Let E/K be an elliptic curve.

Proposition 9.1.10: The reductions modulo π of two minimal Weierstrass equations for E define isomorphic curves over k.

[1] In complex analysis we're used to exp having better convergence, but here it's the other way around.

Proof. Say the Weierstrass equations are related by $[u; r, s, t]$, $u \in K^\times$ and $r, s, t \in K$. Then $\Delta_1 = u^{12}\Delta_2$. If both equations are minimal, then $v(\Delta_1) = v(\Delta_2)$, then $v(u) = 0$, i.e., $u \in \mathscr{O}_K^\times$.

In the case where $\mathrm{char}(k) \neq 2, 3$, we can work with shorter Weierstrass forms, and we only need to worry about u.

In the general case, the transformation formulae for a_i's and b_i's (for example $u^2 b_2' = b_2 + 12r$) gives $r, s, t \in \mathscr{O}_K$. The Weierstrass equations for the reduction π are now related by $[\widetilde{u} \neq 0; \widetilde{r}, \widetilde{s}, \widetilde{t}]$. □

Definition 9.1.11: The **reduction** $\widetilde{E}/k$ of E/K is defined by the reduction of the reduction of a minimal Weierstrass equation modulo pi. We say E has **good reduction** if $\widetilde{E}$ is non-singular (i.e., $\widetilde{E}$ is an elliptic curve). Otherwise, it has **bad reduction**.

For an integral Weierstrass equation,

- $v(\Delta) = 0$ implies good reduction,
- $0 < v(\Delta) < 12$ implies bad reduction (we can only change Δ by powers of 12 so we can't get $v(\Delta) = 0$; the discriminant vanishes when you reduce modulo π.), and
- when $v(\Delta) \geq 12$, the Weierstrass equation might not be minimal.

There is a well-defined map

$$\begin{aligned} \mathbb{P}^2(K) &\to \mathbb{P}^2(k) \\ (x : y : z) &\mapsto (\widetilde{x} : \widetilde{y} : \widetilde{z}) \end{aligned}$$

where we choose the representative with $\min(v(x), v(y), v(z)) = 0$.

We restrict this map to get

$$\begin{aligned} E(K) &\to \widetilde{E}(k) \\ P &\mapsto \widetilde{P}. \end{aligned}$$

Lemma 9.1.4 gives that $E_1(K) = \left\{P \in E(K) : \widetilde{P} = O\right\}$.

Why should $\widetilde{E}(k)$ be a group? In the case of bad reduction we don't have a group law... but we can get one by deleting a singular point. Let

$$\widetilde{E}_{ns} = \begin{cases} \widetilde{E} & \text{if } E \text{ has good reduction,} \\ \widetilde{E} \backslash \{\text{singular point}\} & \text{if } E \text{ has bad reduction.} \end{cases}$$

The chord and tangent process defines a group law on $\widetilde{E}_{ns}$: If the line passes through the singular point, it passes through with multiplicity 2. Hence the third point of intersection will not be the singular point.

In the case of bad reduction, then over $\overline{k}$, $\widetilde{E} \cong \mathbb{G}_a$ or $\mathbb{G}_m$.

For simplicity, assume $\mathrm{char}(k) \neq 2$. Note $\widetilde{E} : y^2 - f(x)$ has $\deg(f) = 3$. There are two possibilities.

1. The singular point is a double root, for example $y^2 = x^2(x+1)$. This is a curve with a node, and we get multiplicative reduction.

2. The singular point is a triple root, for example, $y^2 = x^3$. This is a curve with a cusp, and we get additive reduction.

Lecture 9/11
(Picture)

We check that we have a group law on a singular curve with the singular point removed. We'll just do the special case of $y^2 = x^3$. We have

$$\begin{aligned} \mathbb{G}_a &\xrightarrow{\cong} \widehat{E}_{ns} \\ t &\mapsto (t^{-2}, t^{-3}) \\ O &\mapsto O \text{ (point at } \infty) \\ \frac{x}{y} &\longmapsto (x, y). \end{aligned}$$

We check this is a group homomorphism. Let P_1, P_2, P_3 be on the line $ax + by = 1$. Let $P_i = (x_i, y_i)$. Then $x_i^3 = y_i^2 = y_i^2(ax_i + by_i)$, so $t_i = \frac{x_i}{y_i}$ is a root of $x^3 - aX - b$, and $t_1 + t_2 + t_3$.

This is the additive case; there is a similar calculation for the multiplicative case. The one thing to notice is that rational parametrizations aren't unique, because we can compose by a Mobius transformation. We want to make sure that the point at ∞ on $\mathbb{P}^1$ goes to the singular line. In the multiplicative case, 2 points on the projective line map to the singular point. We get a rational map between the curve and $\mathbb{P}^1$ with $0, \infty$ deleted, the multiplicative group. We want 1 to be mapped to the identity; this helps us pick the right Mobius map.

Definition 9.1.12: Define

$$E_0(K) = \left\{ P \in E(K) : \widetilde{P} \in \widetilde{E}_{ns}(k) \right\}.$$

Proposition 9.1.13: $E_0(K) \subseteq E(K)$ is a subgroup, and reduction modulo π is a surjective group homomorphism, $E_0(K) \twoheadrightarrow \widetilde{E}_{ns}(k)$.

Proof. (Group homomorphism) A line in $\mathbb{P}^2$ defined over K is given by $\ell : aX + bY + cZ = 0$ for some $a, b, c \in K$ not all 0. We may assume $\min(v(a), v(b), v(c)) = 0$. Reduction modulo π gives a line $\widetilde{\ell} : \widetilde{a}X + \widetilde{b}Y + \widetilde{c}Z$ where $\widetilde{a}, \widetilde{b}, \widetilde{c}$ re not all 0. Thinking of lines as points in dual projective space, our method of reducing lines is the same as our method of reducing points.

If $P_1, P_2, P_3 \in E(k)$ with $P_1 + P_2 + P_3 = O$, then they lie on a line ℓ. Then $\widetilde{P}_1, \widetilde{P}_2, \widetilde{P}_3 \in \widetilde{E}(k)$ lie on the line $\widetilde{\ell}$.

If $\widetilde{P}_1, \widetilde{P}_2 \in \widetilde{E}_{ns}(k)$, then $\widetilde{P}_3 \in \widetilde{E}_{ns}(k)$. So of $P_1, P_2 \in E_0(K)$ then $P_3 \in E_0(K)$ and $\widetilde{P}_1 + \widetilde{P}_2 + \widetilde{P}_3 = 0$.

(Surjective) Let $f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$. Let $\widetilde{P} \in \widetilde{E}_{ns}(k) \backslash \{0\}$, say $\widetilde{P} = (\widetilde{x}_0, \widetilde{y}_0)$ for some $x_0, y_0 \in \mathcal{O}_K$. Since $\widetilde{P}$ is nonsingular, either $\frac{\partial f}{\partial x}(x_0, y_0) \not\equiv 0 \pmod{\pi}$ or $\frac{\partial f}{\partial y}(x_0, y_0) \not\equiv 0 \pmod{\pi}$. If $\frac{\partial f}{\partial x}(x_0, y_0) \not\equiv 0 \pmod{\pi}$ then let $g(t) = f(t, y_0) \in \mathcal{O}_K[t]$. We will use Hensel's lemma **??** to turn our approximate root into an exact root.

Then

$$\begin{cases} g(x_0) \equiv 0 \pmod{\pi} \\ g'(x_0) \in \mathscr{O}_K^\times. \end{cases}$$

Hensel's lemma gives $b \in \mathscr{O}_K$ such that $g(b) = 0$, $b \equiv x_0 \pmod{\pi}$. Then $P = (b, y_0) \in E(K)$ reduces to $\widetilde{P} = (\widetilde{x}_0, \widetilde{y}_0)$. (In fact, $P \in E_0(K)$.) The case where $\frac{\partial f}{\partial y}(x_0, y_0) \not\equiv 0 \pmod{\pi}$ works in the same way. □

This is a general argument to lift points on curves by Hensel's lemma; the form of f didn't really matter.

We have for $r > \frac{e}{p-1}$,

$$\begin{array}{ccccccccccc} \hat{E}(\pi^r \mathscr{O}_K) & & & & & & \hat{E}(\pi \mathscr{O}_K) & & & & \\ \| & & & & & & \| & & & & \\ E_r(K) & \xhookrightarrow[(k,+)]{} & \cdots & \xhookrightarrow[(k,+)]{} & E_2(K) & \xhookrightarrow[(k,+)]{} & E_1(K) & \xhookrightarrow[\widetilde{E}_{ns}(k)]{} & E_0(K) & \hookrightarrow & E(K) \\ \| & & & & & & & & & & \\ (\mathscr{O}_K, +) & & & & & & & & & & \end{array}$$

where each quotient before $E_1(K)$ is isomorphic to $(k, +)$ and $\frac{E_0(K)}{E_1(K)} \cong \widetilde{E}_{ns}(k)$. Our goal is to show $E(K)$ contains a subgroup of finite index isomorphic to $(\mathscr{O}_K, +)$; it remains to study the top layer, how $E_0(K)$ sits inside $E(K)$. If good reduction we're already done; we just need to consider bad reduction.

Lemma 9.1.14. *If $|k| < \infty$, then $\mathbb{P}^n(K)$ is compact with respect to the π-adic topology.*

Proof. We have

$$\frac{\pi^r \mathscr{O}_K}{\pi^{r+1} \mathscr{O}_K} \cong \frac{\mathscr{O}_K}{\pi \mathscr{O}_K} \cong k$$

by $\pi^r x \bmod \pi^{r+1} \mapsto x \bmod \pi$. Because k is finite, $\frac{\mathscr{O}_K}{\pi^r \mathscr{O}_K}$ is finite for all r.

Let (x_n) be a squence in $\mathscr{O}_K$. (x_n) has a subsequence $(x_n^{(1)})$ that is constant modulo π, and inductively $(x_n^{(i)})$ has a subsequence $(x_n^{(i+1)})$ that is constant modulo π^{i+1}. Then $(x_n^{(n)})$ is a Cauchy sequence, and hence converges. Thus $\mathscr{O}_K$ is sequentially compact and hence compact. (In general, profinite groups are compact.)

$\mathbb{P}^n(K)$ is the union of compact sets $\{[a_0 : \cdots a_{i-1} : 1 : a_{i+1} : \cdots a_n] : a_i \in \mathscr{O}_K\}$ and hence compact. □

Lemma 9.1.15. *Suppose $E_0(K) \subseteq E(K)$ has finite index.*

Proof. $E(K) \subseteq \mathbb{P}^2(K)$ is a closed subset and hence a compact topological group. If $\widetilde{E}$ has a singular point $(\widetilde{x}_0, \widetilde{y}_0)$, $E(K) \backslash E_0(K) = \{(x, y) \in E(K) : v(x - x_0) \geq 1, v(y - y_0) \geq 1\}$ is a closed subset (as v is continuous). Thus $E_0(K) \subseteq E(K)$ is an open subgroup. The cosets of

$E_0(K)$ in $E(K)$ form an open cover of $E(K)$. Then $E(K)$ is compact, and $[E(K) : E_0(K)] < \infty$. The index

$$c_K(E) = [E(K) : E_0(K)] < \infty$$

is called the **Tamagawa number**. □

Remark 9.1.16: If E has good reduction, then $c_K(E) = 1$, but the converse is false. If you do more geometry, using Neron models, then you get a better understanding of c_K.

If you work in a more abstract setting, reduction consists of several components. When we look at the Weierstrass equation, we see only one component; the other ones get contracted to a singular point and we don't see them. (c_K is the number of components.) One can prove various nice facts about c_K: either $c_K(E) = v(\Delta)$ or $c_K(E) \leq 4$. We've insisted on the minimal Weierstrass equation, but only needed it in two places: the reduction is well-defined, and in the above fact on c_K.

Split multiplicative reduction is where get multiplicative reduction without having to make a field extension.

Theorem 9.1.17. *Let K be a field complete with respect to a discrete valuation,* $\mathrm{char}(K) = 0$ *with finite residue field. Then $E(K)$ contains a subgroup of finite index isomorphic to K^+. In particular, $E(K)_{tors}$ is finite.*

Remark 9.1.18: The fields in Theorem 9.1.17 are exactly the finite extensions of $\mathbb{Q}_p$.

Next time we'll prove a result useful when we look at elliptic curves over global fields, about unramified extensions.

Lecture 12-11 We recall some facts on local fields. Let K be a finite extension of $\mathbb{Q}_p$. Let K be a finite extension of $\mathbb{Q}_p$. Note that K is complete wrt v_K. Let L/K be a finite extension. Then we have a commutative diagram

$$\begin{array}{ccc} K^\times & \xrightarrow{v_K} & \mathbb{Z} \\ \downarrow & & \downarrow \times e \\ L^\times & \xrightarrow{v_L} & \mathbb{Z}. \end{array}$$

where $[L : K] = ef, f = [k' : k]$, and k, k' are the residue fields of K and L (and have characteristic p). If L/K is Galois then there is a natural group homomorphism

$$G(L/K) \to G(k'/k)$$

(since the Galois action preserves the valuation). This map is surjective with kernel of order e.

Definition 9.1.19: L/K is unramified if $e = 1$.

Proposition 9.1.20: For each integer $m \geq 1$,

1. k has a unique extension of degree m, and
2. K has a unique unramified extension of degree m.

Moreover, these extensions are Galois with cyclic Galois group.

The takeaway is that given any extension of residue fields, you can find an unramified extension with that residue field.

Theorem 9.1.21. *Let $[K : \mathbb{Q}_p] < \infty$. Suppose E/K has good reduction and $p \nmid n$. If $P \in E(K)$ then $K([n]^{-1}P)/K$ is unramified.*

(We use the notation $[n]^{-1}P = \{Q \in E(\overline{K}) : nQ = P\}$, $K(\{P_1, \dots, P_r\}) = K(x_1, \dots, x_r, y_1, \dots, y_r)$ where $P_i = (x_i, y_i)$.)

Proof. $[n] : \widetilde{E} \to \widetilde{E}$ is a separable isogeny, since $p \nmid n$. Thus $|[n]^{-1}\widetilde{P}| = \deg[n] = n^2$. Here $[n]^{-1}\widetilde{P} = \{Q' \in \widetilde{E}(\overline{k}) : nQ' = \widetilde{P}\}$. Consider the extension of residue fields $k' = k([n]^{-1}\widetilde{P})$. Let $m = [k' : k]$. let L/K be the unramified extension of degree m, so L has residue field k'. We claim that each $Q' \in \widetilde{E}(k')$ with $nQ' = \widetilde{P}$ is the reduction of some $Q \in E(L)$ with $nQ = P$.

By Proposition 9.1.13, there exists $Q_0 \in E(L)$ reducing to Q'. Then $nQ_0 - P \in E_1(L)$. Since $p \nmid n$, Corollary **??** tells us multiplication by n on $E_1(L)$ is an isomorphism, so there exists $Q_1 \in E_1(L)$ such that $nQ_0 - P = nQ_1$. Then $P = n(Q_0 + Q_1)$. Taking $Q = Q_0 + Q_1$ proves the claim.

We found n^2 points just by finding points defined over L. Thus all n^2 points in $[n]^{-1}P$ are defined over L.

Thus $K([n]^{-1}P) = L$ and $K([n]^{-1}P)/K$ is unramified. □

Chapter 10

Elliptic curves over global fields

Chapter 11

Computing the Mordell-Weil group

Introduction

Let K be a global field. Our end goal is to understand the group $E(K)$, specifically what its rank is.

1. Computation of the rank:

    a. We can reduce the computation of the rank to the computation of $\left|\frac{E'(K)}{\phi E(K)}\right|$.

    b. To compute this, we map $\alpha_{E'} : \left|\frac{E'(K)}{\phi E(K)}\right| \hookrightarrow K^\times/K^{\times m}$ (for a 2-isogeny ϕ this turns out to just be taking the x-coordinate); we will find a point b_1 will be in the image (i.e., the x-coordinate of a solution) precisely when a certain curve C_{b_1}, called a homogeneous space, has a rational point.

    We can get a lower bound for the rank this way. In order to get a precise value, in each case where the curve does not have a rational point, we have to prove this. This might be hard; the one major tool at our disposal is showing the nonexistence of solutions modulo K_v (or by Hensel's lemma, equivalently the nonexistence of solutions modulo a sufficiently high power of $p = n_v$).

    Thus we would like a local-global principle—that a point in K_v for all v gives a point in K. More precisely, we'd like to see whether the fact that $b_1 \in \text{im}\alpha_{E'}$ in all K_v (C_{b_1} has a rational point for all K_v) implies $b_1 \in \text{im}\alpha_{E'}$ (C_{b_1} has a rational point for K). In the 2-isogeny case, this means if b_1 is a valid x-coordinate for all K_v, then it is a valid x-coordinate for K.

    However the local-global principle fails. Hence there could be a gap between the b_1 we show are in the image—where we could find rational points on C_{b_1}—and the b_1 that are in the image for each K_v; this forms the Selmer group. The quotient between them measures the failure of the local-global principle and is measured in the Tate-Shafarevich group.

1 Selmer and Shafarevich-Tate groups

Recall the Kummer sequence

$$0 \to \frac{E'(K)}{\phi E(K)} \xrightarrow{\delta} H^1(K, E[\phi]) \to H^1(K, E)[\phi_*] \to 0.$$

Take K to be a number field. We fix an embedding $\overline{K} \subseteq \overline{K}_v$. Then by restriction $\mathrm{Gal}(\overline{K}_v/K_v) \subseteq \mathrm{Gal}(\overline{K}/K)$. For $v \in M_K$, $K \subseteq K_v$, take the completion with respect to the v-adic topology. We now get maps

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \frac{E'(K)}{\phi E(K)} & \longrightarrow & H^1(K, E[\phi]) & \longrightarrow & H^1(K, E)[\phi_*] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}_v} & \nearrow & \downarrow{\scriptstyle \mathrm{res}_v} & & \\
0 & \longrightarrow & \frac{E'(K_v)}{\phi E(K_v)} & \xrightarrow{\delta_v} & H^1(K_v, E[\phi]) & \longrightarrow & H^1(K_v, E)[\phi_*] & \longrightarrow & 0
\end{array}$$

We want to bound the rank on $\frac{E'(K)}{\phi E(K)}$. It is isomorphic to its image under δ. When you restrict it it must be in the image of δ_v. Thus we can bound the rank by bounding the rank of the image under δ_v.

Definition 11.1.1: The **ϕ-Selmer group** is

$$\begin{aligned}
S^{(\phi)}(E/K) &= \ker\left(H^1(K), E[\phi] \to \prod_{v \in M_K} H^1(K_v, E)\right) \\
&= \left\{\alpha \in H^1(K, E[\phi]) : \mathrm{res}_v(\alpha) \in \mathrm{im}(\delta_v) \text{ for all } v \in M_K\right\}
\end{aligned}$$

They are points which "on the basis of local information look like it might be in the image of δ."

Definition 11.1.2: The **Tate-Shafarevich group** is

$$Ш(E/K) = \ker(H^1(K, E) \to \prod_{v \in M_K} H^1(K_v, E)).$$

The role of the Tate-Shafarevich group is to capture the failure to compute ranks of elliptic curves following the proof of Weak Mordell-Weil. Compare to how we capture the failure of unique factorization in number fields by defining the class group. We've "named our problem."

Theorem 11.1.3 (Selmer and Tate-Shafarevich exact sequence)**.** *If $\phi = [n] : E \to E$, then the following is exact:*

$$0 \to \frac{E(K)}{nE(K)} \to S^{(n)}(E/K) \to Ш(E/K)[n] \to 0.$$

Proof. The horizontal and vertical sequences in the following are exact. The top row is exact by the Nine Lemma (or it can be shown more easily, in a direct fashion).

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \frac{E'(K)}{\phi E(K)} & \longrightarrow & S^{(\phi)}(E/K) & \longrightarrow & Ш(E/K) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \frac{E'(K)}{\phi E(K)} & \xrightarrow{\delta} & H^1(K, E[\phi]) & \longrightarrow & H^1(K,E)[\phi_*] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & 0 & \longrightarrow & \prod_v H^1(K_v, E)[\phi_*] & \xrightarrow{\text{id}} & \prod_v H^1(K_v,E)[\phi_*] & \longrightarrow & 0.
\end{array}$$

□

Q: How do we come up with the map? We somehow reduce the calculation of $E(K)/mE(K)$ to the existence of a rational point, reduce a rank calculation question to a point-finding question. A: We have three pairings, let's see how to combine them. (The "pp" is to remind us the pairing is perfect.)

$$\begin{array}{rccccc}
(1)\ \kappa: & E'(K)/\phi E(K) & \overset{pp}{\times} & G(L_1/K) & \to & E[\phi] \\
(2)\ e_\phi: & E[\phi] & \times & E'[\widehat{\phi}] & \to & \mu_m \\
(0)\ \text{Kummer:} & K^\times/K^{\times m} & \overset{pp}{\times} & G(L_2/K) & \to & \mu_m
\end{array}$$

where

$$L_1 = K(\phi^{-1}(E(K))) \qquad L_2 = K(\sqrt[m]{K});$$

L_2 is the maximal abelian extension of exponent m. Alternatively, we can restrict (0) to $L \subseteq L_2$ to get $K^\times \mathcal{L}^{\times m}/K^{\times m} \overset{pp}{\times} G(L/K) \to \mu_m$. Thinking in a "computer science" way, how can we combine pairings to get what we want? We can "compose" pairings to get "triplings."

$$\begin{array}{cccccc}
A & \times & B & \to & C \\
C & \times & D & \to & E \\
\hline
A \times B \times D & & & \to & E
\end{array}$$

We can switch between pairings and maps:

$$A \times B \to C \quad \iff \quad A \to (B \to C).$$

where we write $B \to C$ for $\text{Hom}(B, C)$ (in this context, as groups) for visual effect. If the pairing is perfect, then the map $A \overset{\cong}{\to} (B \to C)$ map is a bijection.

We construct the map.

1.

(1)+(2) gives by rule A

$$\times G(L/K) \times E'[\widehat{\phi}] \to \mu_m.$$

which gives by rule B

$$\times E'[\widehat{\phi}] \to (G \to \mu_m)$$

which gives by rule B again

$$\times E'[\widehat{\phi}] \to K^\times/K^{\times m}.$$

Careful: the L's are not the same. Was it justified?

To motivate this more, look at what was tractable:

$$\begin{array}{rccccc} (1)\ \kappa: & & \overset{pp}{\times} & G(L_1/K) & \to & E[\phi] \\ (2)\ e_\phi: & E[\phi] & \times & E'[\widehat{\phi}] & \to & \mu_m \\ (0)\ \text{Kummer:} & K^\times/K^{\times m} & \overset{pp}{\times} & G(L_2/K) & \to & \mu_m \end{array}$$

And note how we moved from what we wanted information about to what we had information about.

ADD: why the different L's wasn't a problem.

For ϕ a 2-isogeny, there's only one nonzero element of $E'[\widehat{\phi}]$, and it corresponds to an element in

$$\to K^\times/K^{\times m}.$$

So if we can find the preimage, we're done! Let's trace through to find what the map is:

Q: (lemma 15.3) How can we calculate rank $E(K)$ from our info? We want to calculate $E(K)/2E(K)$. However, it's more convenient to deal with ϕ than [2] (the reason being we just get 1 map we have to worry about above). We know this is going to be an exact sequence of some sort; first we want to change the [2] into ϕ, so we start

$$\frac{E'(K)}{\phi E(K)} \xrightarrow{\widehat{\phi}} \frac{E(K)}{2E(K)} \to \frac{E(K)}{\widehat{\phi}E'(K)} \to 0.$$

Find the kernel of the first map:

$$0 \to \frac{E'[\widehat{\phi}]}{\phi E(K)} \to \frac{E'(K)}{\phi E(K)} \xrightarrow{\widehat{\phi}} \frac{E(K)}{2E(K)} \to \frac{E(K)}{\widehat{\phi}E'(K)} \to 0.$$

Expand the first:

$$0 \to E[\phi] \to E[2] \xrightarrow{\phi} E'[\widehat{\phi}] \to \frac{E'(K)}{\phi E(K)} \xrightarrow{\widehat{\phi}} \frac{E(K)}{2E(K)} \to \frac{E(K)}{\widehat{\phi}E'(K)} \to 0.$$

Idea: it "tells us what residue classes of $E(K)$ to look for independent generators."

Chapter 12

Integral points of elliptic curves

Chapter 13

Complex multiplication

In this chapter, we combine class field theory with the theory of elliptic curves, first to characterize the maximal abelian extension of K, then to illustrate the relationships in Section **??.??** for CM elliptic curves. We will assume basic facts about elliptic curves (for an introduction see Silverman [2, Chapter III]).

We know that every elliptic curve over $\mathbb{C}$ has endomorphism ring either equal to $\mathbb{Z}$ or a quadratic order. In the second case, the elliptic curve is said to have **complex multiplication**. This gives the elliptic curve a lot more structure. On one hand, it is useful algebraically—as we will see, torsion points of a CM elliptic curve give abelian extensions of imaginary quadratic fields. In general, because of the added structure, much more is known about CM elliptic curves than other elliptic curves, and they can act as a kind of "testing ground" or "first case" of general conjectures.

On the other hand, CM elliptic curves have practical uses—for instance, if we take an CM elliptic curve corresponding to a specific endomorphism ring, we can easily compute its order. Hence we can generate an elliptic curve with near-prime order, useful in cryptography. This is much more efficient than generating random elliptic curves and using Schoof's algorithm to find their orders.

There are several big theorems about complex multiplication. In Section 2, we specialize our knowledge about the relationship between elliptic curves over $\mathbb{C}$ and complex tori to CM elliptic curves and build a toolbox of basic facts. However, since we are interested in number theory, we want to take curves defined over $\mathbb{C}$ and define them over $\overline{\mathbb{Q}}$ instead—which we do in Section 3. Once we have these basics, we can then prove the big theorems.

We suppose E has CM by a quadratic order $\mathscr{O} \subset K$ (i.e. $\mathrm{End}(E) \cong \mathscr{O}$), where K is a quadratic extension of $\mathbb{Q}$. Then the following hold.

1. The j-invariant $j(E)$ generates the *ring class field* of $\mathscr{O}$ over K. In particular, if $\mathscr{O} = \mathscr{O}_K$, then $j(E)$ generates the *Hilbert class field* of K, the maximal unramified abelian extension (Theorem 13.4.4):
$$K(j(E)) = H_K.$$
2. If E is defined over H_K, and we adjoin certain functions of torsion points of E, then

we get the *maximal abelian extension* of K (Theorem 13.5.4):

$$K(j(E), h(E_{\text{tors}})) = K^{\text{ab}}.$$

Compare this with the Kronecker-Weber Theorem, which says the maximal abelian extension of $\mathbb{Q}$ is generated by roots of unity (torsion points of $\overline{\mathbb{Q}}^{\times}$).

3. $j(E)$ is moreover an *algebraic integer* (We omit this; see Silverman AT, [3, II.6].)

4. The action of the idele class group sending $K/\mathfrak{a}$ to $K/\mathbf{x}^{-1}\mathfrak{a}$ corresponds to the Galois action on the corresponding elliptic curves, where the Galois action is given by the Frobenius element of σ. This is the Main Theorem of Complex Multiplication 13.6.2, and plays an important part in taking moduli spaces initially defined only over $\mathbb{C}$ and defining them over algebraic number fields.

5. The L-series of a CM elliptic curve is particularly easy to understand, because it is a product of 2 Hecke L-series (Theorem 13.7.5).

Two "big ideas" we'll consistently see are the following.

1. We expect abelian extensions because for CM elliptic curves (with endomorphism ring $\mathscr{O}_K$, say), the image of the map $G(L/H_K) \hookrightarrow \text{Aut}(E[m])$ commutes with $\mathscr{O}_K$, not just $\mathbb{Z}$ and hence must be abelian, with appropriate L.

2. We can use torsion points $E[m]$ to "keep book" on the action of Frobenius, in the same way that we used the roots of unity μ_m to keep book on the action of Frobenius on $G(\mathbb{Q}(\mu_m)/\mathbb{Q})$.

1 Elliptic curves over $\mathbb{C}$

The following theorem helps us understand elliptic curves over $\mathbb{C}$.

Theorem 13.1.1. *Let $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$, where G_n is the Eisenstein series. Let Λ be a lattice in $\mathbb{C}$ and $\wp$ be the associated Weierstrass $\wp$-function.*

There is a complex analytic isomorphism between the complex torus $\mathbb{C}/\Lambda$ and the elliptic curve over $\mathbb{C}$,

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

given by

$$\Phi(z) = (\wp(z), \wp'(z)).$$

The map Φ gives an equivalence of categories between the following.

1. *Objects: Complex tori $\mathbb{C}/\Lambda$, where Λ is a lattice in $\mathbb{C}$.*
   Maps: Multiplication-by-α $\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ where $\alpha\Lambda_1 \subseteq \Lambda_2$.

2. *Objects: Elliptic curves over* $\mathbb{C}$.
   Maps: Isogenies.

Proof. Silverman [2, VI.5.1.1, 5.3] □

The endomorphism ring of a lattice $\Lambda \subset \mathbb{C}$ is either $\mathbb{Z}$ or an imaginary quadratic order, so the same is true of an elliptic curve E over $\mathbb{C}$. If the endomorphism ring is a quadratic order $\mathscr{O}$, we say E has **complex multiplication** by $\mathscr{O}$.

2 Complex multiplication over $\mathbb{C}$

2.1 Embedding the endomorphism ring

We know the endomorphism ring $\mathrm{End}(E)$ of a CM elliptic curve corresponds to a quadratic order $\mathscr{O}$ but since any quadratic order has conjugation as an isomorphism, we need to specify a way to embed $\mathrm{End}(E)$ into $\mathbb{C}$.

Example 13.2.1: Consider the curve $E : y^2 = x^3 + x$. We note that the endomorphisms

$$\phi_1(x, y) = (-x, iy)$$
$$\phi_2(x, y) = (-x, -iy)$$

both square to -1. Which one should we call $[i]$, multiplication by i?

Fortunately, we have a way of embedding $\mathrm{End}(\Lambda)$ into $\mathbb{C}$, where Λ is the lattice corresponding to E, because Λ itself is in $\mathbb{C}$. This to give a canonical way of embedding $\mathrm{End}(E)$ into $\mathbb{C}$.

Proposition 13.2.2: Let $E/\mathbb{C}$ be a CM elliptic curve with complex multiplication by $\mathscr{O}$. There is a unique isomorphism $[\cdot] : \mathscr{O} \xrightarrow{\cong} \mathrm{End}(E)$ satisfying either of the following equivalent conditions.

1. $[\alpha]$ is the unique morphism making the following diagram commute, where the top map is multiplication by α.

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{m_\alpha} & \mathbb{C}/\Lambda \\ \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \Phi} \\ E_\Lambda & \xrightarrow{[\alpha]} & E_\Lambda \end{array}$$

2. For any invariant differential $\omega \in \Omega_E$, $[\alpha]^*\omega = \alpha\omega$.

Moreover, we have the following.

3. Define $[\cdot]_1$ and $[\cdot]_2$ for elliptic curves E_1 and E_2. For any morphism $\phi : E_1 \to E_2$,

$$\phi \circ [\alpha]_1 = [\alpha]_2 \circ \phi.$$

   In other words, multiplication by α commutes with all morphisms.

4. For any $\sigma \in \mathrm{Aut}(\mathbb{C})$,
$$[\alpha]_E^\sigma = [\sigma(\alpha)]_{\sigma(E)},$$
i.e. it commutes with Galois action.

The pair $(E, [\cdot])$ is called a **normalized** elliptic curve. After we prove this proposition, we will assume all CM elliptic curves are normalized.

Proof. The uniqueness and existence of $[\alpha]$ satisfying item 1 follows directly from the equivalence of categories (Theorem 13.1.1).

Define $[\alpha]$ as in item 1. For any invariant differential ω on E_Λ, since Φ is an analytic isomorphism, we can consider its pullback to $\mathbb{C}/\Lambda$; it will be $c\,dz$ for some c (The space of invariant differentials on $\mathbb{C}/\Lambda$ is 1-dimensional.) Clearly, $m_\alpha^*(c\,dz) = c\,d(\alpha z) = \alpha c\,dz$. Transferring this to the bottom row of the commutative diagram gives $[\alpha]^*\omega = \alpha\omega$. For uniqueness, note the map

$$\begin{aligned} \mathrm{Hom}(E_1, E_2) &\hookrightarrow \mathrm{Hom}(\Omega_{E_2}, \Omega_{E_1}) \\ \phi &\to \phi^* \end{aligned} \tag{13.1}$$

is injective when all isogenies $E_1 \to E_2$ are separable (in particular, in characteristic 0), i.e. the action of an isogeny of elliptic curves on an invariant differential completely determines the morphism. Taking $E_1 = E_2$ and considering the preimage of multiplication-by-α gives uniqueness in item 2.

A simple diagram chase shows that $(\phi \circ [\alpha]_1)^*$ and $([\alpha]_2 \circ \phi)^*$ act the same way on $\omega \in \Omega_{E_2}$. Then (13.1) gives item 3.

The proof of item 4 is similar. □

Example 13.2.3: The definition using differentials is useful for calculations. Revisiting the above Example 13.2.1, we see that we should let

$$[i](x, y) = (-x, iy).$$

Indeed, defining $[i]$ in this way, we check that

$$[i]^* \frac{dx}{y} = \frac{d(-x)}{iy} = i\frac{dx}{y}.$$

2.2 The class group parameterizes elliptic curves

Let K be an imaginary quadratic field and $\mathscr{O}$ an order inside K.

Definition 13.2.4: Let L be a field. Define

$$\begin{aligned} \mathrm{Ell}_L(\mathscr{O}) &= \{\text{elliptic curves } E/L \text{ with } \mathrm{End}(E) \cong \mathscr{O}\} \\ \mathcal{E}\mathrm{ll}_L(\mathscr{O}) &= \frac{\{\text{elliptic curves } E/L \text{ with } \mathrm{End}(E) \cong \mathscr{O}\}}{\text{isomorphism over } L}, \end{aligned}$$

i.e. $\mathcal{E}\mathrm{ll}_L(\mathscr{O})$ is the set of elliptic curves over L whose endomorphism ring is $\mathscr{O}$. If we omit L, we assume $L = \mathbb{C}$.

If $E \in \mathrm{Ell}(\mathscr{O})$, then its corresponding lattice Λ must be homothetic to a fractional ideal of $\mathscr{O}$: indeed, we can scale the lattice so that $1 \in \Lambda$; then $\mathscr{O} \subseteq \Lambda$ so $\Lambda \subseteq K$; since it is a lattice it must be a fractional $\mathscr{O}$-ideal. Now note an $\mathscr{O}$-ideal $\mathfrak{a}$ has endomorphism ring $\mathscr{O}$ iff $\mathfrak{a}$ is a *proper* ideal (see Definition **??.??**).[1] Hence we get a correspondence between isomorphism classes of elliptic curves $[E] \in \mathcal{E}\mathrm{ll}(\mathscr{O})$ and proper $\mathscr{O}$-ideals up to homothety. However, two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ are homothetic iff $\lambda\mathfrak{a} = \mathfrak{b}$ for some λ, i.e. iff they are equivalent in the class group. Thus the class group of $\mathscr{O}$ parameterizes all isomorphism classes of elliptic curves with endomorphism ring $\mathscr{O}$. This is summarized in the following.

$$\mathcal{E}\mathrm{ll}(\mathscr{O}) = \frac{\{\text{elliptic curves } E/\mathbb{C} \text{ with } \mathrm{End}(E) \cong \mathscr{O}\}}{\text{isomorphism over } \mathbb{C}} = \frac{\{\text{proper fractional } \mathscr{O}\text{-ideal}\}}{\text{principal } \mathscr{O}\text{-ideals}} = \mathrm{Cl}(\mathscr{O}).$$

We state this as a theorem.

Theorem 13.2.5. *We have a bijection*

$$\mathcal{E}\mathrm{ll}(\mathscr{O}) \cong \mathrm{Cl}(\mathscr{O})$$

where $[E] \in \mathcal{E}\mathrm{ll}(\mathscr{O})$ is sent to a $[\mathfrak{a}]$, where $\mathfrak{a}$ is a fractional ideal homothetic to the lattice corresponding to E.

We get much more than this, however. $\mathcal{E}\mathrm{ll}(\mathscr{O})$ is a priori just a set; however, $\mathrm{Cl}(\mathscr{O})$ is a *group*. We can define the action of $I(\mathscr{O})$ on $\mathrm{Ell}(\mathscr{O})$ since $I(\mathscr{O})$ acts on lattices. This action will descend to an action of $\mathrm{Cl}(\mathscr{O})$ on $\mathcal{E}\mathrm{ll}(\mathscr{O})$, since isomorphic elliptic curves correspond to equivalent ideals.

Theorem 13.2.6. *There is a group action of $\mathrm{Id}(\mathscr{O})$ on Ell$(\mathscr{O})$ given by*

$$\mathfrak{a}E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}$$

where E_Λ denotes the elliptic curve corresponding to the lattice Λ.

This descends to a simply transitive group action of $\mathrm{Cl}(\mathscr{O})$ on $\mathcal{E}\mathrm{ll}(\mathscr{O})$.

Proof. Just check that if Λ has endomorphism ring $\mathscr{O}$, then so does the lattice $\mathfrak{a}^{-1}\Lambda$. (Note that $\mathfrak{b}L$ is defined by $\{s\alpha : s \in \mathfrak{b}, \alpha \in L\}$.)

For the second part, note that $E_\Lambda \cong \mathfrak{a}E = E_{\mathfrak{a}^{-1}\Lambda}$ iff Λ and $\mathfrak{a}^{-1}\Lambda$ are homothetic, i.e. $\mathfrak{a}$ is principal. □

Remark 13.2.7: Another way of saying that $\mathrm{Cl}(\mathscr{O})$ acts simply transitively on $\mathcal{E}\mathrm{ll}(\mathscr{O})$ is that $\mathcal{E}\mathrm{ll}(\mathscr{O})$ is a **torsor** or **principal homogeneous space** for $\mathrm{Cl}(\mathscr{O})$.

This action will be fundamental to our understanding of CM elliptic curves. Later on we will relate this to the Galois action. The interplay between these two actions is the source for much of the richness of CM theory.

[1] When $R = \mathscr{O}_K$, all ideals are proper, so this distinction is not important. The reader unfamiliar with non-maximal orders can take $R = \mathscr{O}_K$ throughout.

2.3 Ideals define maps

For any $n \in \mathbb{Z}$ and any elliptic curve E, n defines the multiplication by n map $[n] : E \to E$. When E has CM, we saw in Theorem 13.2.2 that $\alpha \in \mathscr{O}$ defines (canonically) the multiplication by α map $[\alpha] : E \to E$. We now extend this to *ideals*: if $\mathfrak{a}$ is a proper $\mathscr{O}$-ideal, $\mathfrak{a}$ determines a "multiplication by $\mathfrak{a}$" map. The only difference is that $[\mathfrak{a}]$ is now a map $E \to \mathfrak{a}E$.

Definition 13.2.8: Let $E \in \mathrm{Ell}(\mathscr{O})$ correspond to the lattice Λ. Let $\mathfrak{a}$ be a proper integral ideal of $\mathscr{O}$. We have $\mathfrak{a}R \subseteq R$, so $\mathfrak{a}$ determines a map $\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{a}^{-1}\Lambda$, sending $z \mapsto z$. Define the multiplication by $\mathfrak{a}$-map as the corresponding map on elliptic curves

$$[\mathfrak{a}] : E \to E_{\mathfrak{a}^{-1}\Lambda} = \mathfrak{a}E.$$

Proposition 13.2.9: Let $E \in \mathrm{Ell}(\mathscr{O}_K)$. We have the following.

1. The kernel of $[\mathfrak{a}]$ (the "$\mathfrak{a}$-torsion points") is

$$E[\mathfrak{a}] := \{P \in E : [\alpha]P = 0 \text{ for all } \alpha \in \mathfrak{a}\} \cong \mathscr{O}_K/\mathfrak{a}.$$

2. The degree of $[\mathfrak{a}]$ is

$$\deg([\mathfrak{a}]) = |E[\mathfrak{a}]| = \mathfrak{N}(\mathfrak{a}),$$

and in particular, $\deg([\alpha]) = |E[\alpha]| = \mathrm{Nm}_{K/\mathbb{Q}}(\alpha)$.

Proof. Silverman AT [3, pg. 102-3]. □

3 Defining CM elliptic curves over $\overline{\mathbb{Q}}$

We show that we do not lose anything if we just consider elliptic curves over $\overline{\mathbb{Q}}$ instead of over $\mathbb{C}$. To do this, we look at the j-invariants.

Proposition 13.3.1: Suppose E is an elliptic curve with CM by a quadratic order $\mathscr{O}$. Then $j(E) \in \overline{\mathbb{Q}}$, i.e. $j(E)$ is algebraic.

Proof. Let σ be any automorphism of $\mathbb{C}$ over $\mathbb{Q}$. We look at how σ acts on $j(E)$.

Note that E^σ is defined by taking any equation for E and operating on all the coefficients of E by σ, so $\sigma(j(E)) = j(E^\sigma)$.

First note that $\mathrm{End}(E) \cong \mathrm{End}(E^\sigma)$ by the map $\phi \mapsto \phi^\sigma$. Hence $\mathrm{End}(\sigma(E)) = \mathscr{O}$ as well. But $\mathrm{Cl}(\mathscr{O})$ is finite, and as $|\mathrm{Cl}(\mathscr{O})| = |\mathcal{E}\ell\ell(\mathscr{O})|$ (Theorem 13.2.5) we see that the E^σ lie in finitely many isomorphism classes. Because isomorphic elliptic curves have the same j-invariant, there are a finite number of possibilities for $j(E^\sigma)$.

As $\{\sigma(j(E)) : \sigma \in \mathrm{Aut}(\mathbb{C})\}$ is finite, $j(E)$ must be algebraic. □

This allows us to prove the following.

Theorem 13.3.2. *We have*

$$\mathcal{E}\mathrm{ll}_{\mathbb{C}}(\mathscr{O}) \cong \mathcal{E}\mathrm{ll}_{\overline{\mathbb{Q}}}(\mathscr{O}).$$

Proof. We use the following properties of the j-invariant. ([2, III.1.4])

1. For every $j \in K$, there exists an elliptic curve E/K with $j(E) = j$.

2. Let K be an algebraically closed field and E_1, E_2 be elliptic curves defined over K. Then $E_1 \cong E_2$ over K iff $j(E_1) = j(E_2)$. (The backwards direction does not necessarily hold if K is not algebraically closed.)

We show that the map

$$\mathcal{E}\mathrm{ll}_{\overline{\mathbb{Q}}}(\mathscr{O}) \to \mathcal{E}\mathrm{ll}_{\mathbb{C}}(\mathscr{O}) \tag{13.2}$$

is an isomorphism (of sets, in fact, of $\mathrm{Cl}(\mathscr{O})$-modules). The map is well-defined, because any automorphism over $\overline{\mathbb{Q}}$ is an automorphism over $\mathbb{C}$.

By Lemma 13.3.1, if $[E] \in \mathcal{E}\mathrm{ll}_{\mathbb{C}}(\mathscr{O})$ then $j(E) \in \overline{\mathbb{Q}}$. By item 1, there exists an elliptic curve E' defined over $\overline{\mathbb{Q}}$ with $j(E') = j(E)$. Then E' is isomorphic to E over $\mathbb{C}$. Thus the map (13.2) above is surjective. It is injective because if E, E' are defined over $\overline{\mathbb{Q}}$ and isomorphic over $\mathbb{C}$, then item 2 says $j(E) = j(E')$; and the other direction of item 2 says that $E \cong E'$ over $\overline{\mathbb{Q}}$. □

It is also important to know what fields we can define elliptic curves and isogenies over.

Proposition 13.3.3: Suppose E is an elliptic curve with CM by $\mathscr{O} \subset K$, where K is an imaginary quadratic field.

1. If E is defined over L then endomorphisms of E can be defined over LK.

2. If E_1, E_2 are defined over L then there exists a finite extension M/L, so that every isogeny $E_1 \to E_2$ is defined over M.

Proof. For item 1, note that all endomorphisms are in the form $[\alpha]$ and use Proposition 13.2.2(4).

For item 2, first we claim that any isogeny ϕ is defined over a finite extension of L. For any $\sigma \in \mathrm{Aut}(\mathbb{C})$ fixing L, ϕ^σ is a map $E_1 \to E_2$ having the same degree as ϕ. Any isogeny is determined by its kernel, up to automorphism of E_1 and E_2. As E_1 has a finite number of subgroups of given index and $\deg(\phi) = \ker(\phi)$, there are finitely many isogenies of a given degree. Hence $\{\phi^\sigma : \sigma \in G(\mathbb{C}/L)\}$ is finite, showing ϕ is defined over a finite extension of L.

Now $\mathrm{Hom}(E_1, E_2)$ is a finitely generated group, so we can take the field of definition for a finite set of generators. □

4 Hilbert class field

4.1 Motivation: Class field theory for $\mathbb{Q}(\zeta_n)$ and Kronecker-Weber

4.1.1 The case of $\mathbb{Q}$

First we give some motivation for the next two sections by making an analogy with class field theory for $\mathbb{Q}(\zeta_n)$. We can think of μ_n, the nth roots of unity, as the analogue of $E[n]$: μ_n are the n-torsion points of the group variety $\overline{\mathbb{Q}}^\times$ under multiplication, and $E[n]$ are the n-torsion points of an elliptic curve. To emphasize this analogy, we write $K^\times[n]$ to denote the nth roots of unity in $\overline{K}$.

Recall how we established class field theory for $\mathbb{Q}(\zeta_n)$: given a prime p, we want to find $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q})$. To do this we looked at the action of $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q})$ on $\mathbb{Q}^\times[n] = \mu_n$, by taking everything modulo p. We know by definition of $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q})$ how it must act on the residue field extension $l/\mathbb{F}_p$ and hence on $\mathbb{F}_p^\times[n]$. Suppose $p \nmid n$. Because the maps

$$\begin{aligned} \mathbb{Q}^\times[n] &\hookrightarrow \mathbb{F}_p^\times[n] \\ \mathrm{End}(\mathbb{Q}^\times[n]) &\hookrightarrow \mathrm{End}(\mathbb{F}_p^\times[n]) \end{aligned} \tag{13.3}$$

are injective (the first is because $p \nmid n$ and the second is a direct consequence of the first), once we know how $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q})$ acts on $\mathbb{F}_p^\times[n]$, we know it acts on $\mathbb{Q}_p^\times[n]$, so we know exactly what automorphism it is:

$$(p, \mathbb{Q}(\zeta_n)/\mathbb{Q})(\zeta_n) = \zeta_n^p.$$

In particular, since ζ_n is a n-torsion point (i.e. $\zeta_n^n = 1$) this only depends on $p \pmod n$. Hence we get the Artin map $\psi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}$ factoring through the modulus ∞n:[2]

$$\psi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} : I_\mathbb{Q}/I_\mathbb{Q}(1, n\infty) \xrightarrow{\cong} G(\mathbb{Q}(\zeta_n)/\mathbb{Q}).$$

Finally, since every modulus divides ∞n for some n, we get the Kronecker-Weber Theorem

$$\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\zeta_\infty) = \mathbb{Q}(\mathbb{Q}^\times[\infty]).$$

In summary, we found the ray class groups and thus the maximal abelian extension by looking at how $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q})$ acted on $\mathbb{Q}^\times[n]$:

$$\begin{array}{ccc} \mathbb{Q}^\times[n] & \xrightarrow[\text{reduction}]{\widetilde{\bullet}} & \mathbb{F}_p^\times[n] \\ \circlearrowleft & & \circlearrowleft \\ I_\mathbb{Q}/P_\mathbb{Q}(1, n\infty) & \xrightarrow{\psi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}} G(\mathbb{Q}(\zeta_n)/\mathbb{Q}) & \xrightarrow{\widetilde{\bullet}} G(\mathbb{F}_p(\zeta_n)/\mathbb{F}_p). \end{array} \tag{13.4}$$

[2] The ∞ is a technical detail coming from the fact that $\mathbb{Q}$ is totally real.

4.1.2 The case of K

One big difference when we're working over an imaginary quadratic field K is that while we had $\mathrm{Cl}_{\mathbb{Q}} = 1$, we have Cl_K is nontrivial in general. This corresponds to the fact that there is only 1 nonisomorphic "version" of $\mathbb{G}_m(\mathbb{Q}) = \mathbb{Q}^\times$, but multiple elliptic curves with endomorphism ring by the same order $\mathscr{O}$. Hence $G(K^{\mathrm{ab}}/K)$ no longer operates on the same elliptic curve. Instead we have to analyze it in two steps.

1. Consider the action of $G(H_K/K)$ on $\mathcal{E}\mathrm{ll}_{\overline{\mathbb{Q}}}(\mathscr{O})$, i.e. equivalence classes of elliptic curves with CM by $\mathscr{O}$.
2. Consider the action of $G(K^{\mathrm{ab}}/H_K)$ on the torsion points E_{tors} of a single elliptic curve.

In both cases, we will understand the action by looking at how the Frobenius elements of the Galois groups act.

4.1.3 The case of K: Part 1

We have two natural actions on the set of elliptic curve $\mathcal{E}\mathrm{ll}_{\overline{\mathbb{Q}}}(\mathscr{O}_K)$, namely the action of $G(\overline{K}/K)$ and $\mathrm{Cl}(\mathscr{O}_K)$. Our first task is to relate these, i.e. find a dotted map that preserves the action on $\mathcal{E}\mathrm{ll}_{\overline{\mathbb{Q}}}(\mathscr{O}_K)$:

$$\begin{array}{ccc} & \mathcal{E}\mathrm{ll}_{\overline{\mathbb{Q}}}(\mathscr{O}_K) & \\ \circlearrowright & & \circlearrowright \\ G(\overline{K}/K) & \dashrightarrow & \mathrm{Cl}(\mathscr{O}_K). \end{array} \tag{13.5}$$

We'll see that this map factors through $G(L/K)$ where $L = K(j(E))$. We have a map $\psi_{L/K} : I_K^{\mathfrak{f}}/P_K(1,\mathfrak{f}) \to G(L/K)$; we show that $\mathfrak{f} = 1$ and the composition of the two maps is an isomorphism, and that in fact we have

$$\begin{array}{ccccc} & & & \mathcal{E}\mathrm{ll}_{\overline{\mathbb{Q}}}(\mathscr{O}_K) & \\ & & \circlearrowright & & \circlearrowright \\ I_K/P_K & \xrightarrow{\Psi_{L/K}} & G(L/K) & \longrightarrow & \mathrm{Cl}(\mathscr{O}_K). \end{array} \qquad I_K/P_K \overset{\mathfrak{a}\mapsto[\mathfrak{a}]}{\dashrightarrow} \mathrm{Cl}(\mathscr{O}_K) \tag{13.6}$$

We establish (13.6) by looking at the reduction of the elliptic curves modulo some $\mathfrak{P}$.

Since $G(H_K/K) \cong \mathrm{Cl}(\mathscr{O}_K)$ this will show that $L = H_K$, the Hilbert class field of K.

4.1.4 The case of K: Part 2

We can now do the same thing we did with $\mathbb{Q}$, use the torsion points of elliptic curves to find the ray class fields and the maximal abelian extensions. We can't work directly over K because Cl_K is nonzero, but if we imitate the argument (with some modifications) over

$\mathbb{Q}$ for H_K we will get the ray class fields of K. We let $L_n = K(j(E), h(E[n]))$ where h is a Weber function (to be defined).

Let l_n, l be the residue fields of L_n and H_K modulo some prime. We show L_n is the ray class field for (n) by constructing the diagram

$$\begin{array}{ccc} E[n] & \xrightarrow[\text{reduction}]{\widetilde{\bullet}} & \widetilde{E}[n] \\ \circlearrowleft & & \circlearrowleft \\ \mathrm{Nm}_{H_K/K}(I_{H_K}^n)/P_K(1,n) & \xrightarrow{\psi_{L_n/K}}_{\cong} & G(L_n/H_K) \xrightarrow{\widetilde{\bullet}} G(l_n/l). \end{array} \tag{13.7}$$

We now carry out these two parts.

4.2 The Galois group and class group act compatibly

We establish the map in (13.5).

Theorem 13.4.1. *There exists a map $F : G(\overline{K}/K) \to \mathrm{Cl}(\mathscr{O}_K)$ such that for any elliptic curve E,*

$$[E^\sigma] = F(\sigma)E.$$

This map factors through $G(K^{ab}/K)$.

As a reminder, the action of $\mathrm{Cl}(\mathscr{O}_K)$ on $\mathcal{E}\mathrm{ll}_{\overline{\mathbb{Q}}}(\mathscr{O}_K)$ is such that if $E = E_\Lambda$, then $F(\sigma)E = E_{F(\sigma)^{-1}\Lambda}$. Theorem 13.4.1 expresses a deep relationship because the left-hand side expresses an algebraic action, while the right-hand side expresses an analytic action, as it is defined on lattices and the map between E and $\mathbb{C}/\Lambda$ is inherently analytic.

Proving this theorem essentially boils down to showing the Galois action commutes with the action on $\mathrm{Cl}(\mathscr{O}_K)$.

Proposition 13.4.2: For all E,

$$\sigma([\mathfrak{a}][E]) = [\sigma(\mathfrak{a})][\sigma(E)].$$

Proof. Suppose E corresponds to Λ, i.e. $E \cong \mathbb{C}/\Lambda\mathbb{C}$. Then we have the exact sequence

$$0 \to \Lambda \to \mathbb{C} \to E \to 0.$$

Then $\mathfrak{a}E$ corresponds to $\mathfrak{a}^{-1}\Lambda$. Take a resolution for $\mathfrak{a}$:

$$R^m \xrightarrow{A} R^n \to \mathfrak{a} \to 0.$$

Take a "Hom product" and use the Snake Lemma. See [3, II.2.5]. □

Proof of Theorem 13.4.1. See [3, II.2.4]. □

4.3 Hilbert class field

Before we proceed with finding the Hilbert class field, we need to show injectivity of the reduction map like in (13.3).

Theorem 13.4.3. *Suppose E_1 and E_2 are elliptic curves defined over L with good reduction at $\mathfrak{P}$. Then the reduction map*

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(\widetilde{E_1}, \widetilde{E_2})$$

is injective and preserves degrees.

Proof. See Silverman AT [3, pg. 124] (Also see Silverman's errata). □

The main theorem of this section is the following.

Theorem 13.4.4 ($j(E)$ generates the Hilbert class field)**.** *Let E be an elliptic curve with CM by $\mathscr{O}_K$. Then*

1. *$K(j(E)) = H_K$, the Hilbert class field of K.*
2. *$G(\overline{K}/K)$ acts transitively on the isomorphism classes of curves in $\mathcal{E}\mathrm{ll}(\mathscr{O}_K)$.*
3. *For any ideal $\mathfrak{a} \in I_K$,*
$$[E^{\psi_{H_K/K}(\mathfrak{a})}] = [\mathfrak{a}][E].$$
In particular, the action of Frobenius on the j-invariant is given by operating by $[\mathfrak{p}]$ on the elliptic curve:
$$[E^{(\mathfrak{p}, H_K/K)}] = [\mathfrak{p}][E].$$

Proof. Step 1: First we show the following: There exists a finite set of primes S of $\mathbb{Z}$ such that for any $p \notin S$ that splits completely in K, $p = \mathfrak{p}\overline{\mathfrak{p}}$, we have

$$F((\mathfrak{p}, L/K)) = [\mathfrak{p}] \in \mathrm{Cl}(\mathscr{O}_K).$$

This will show the dotted map in (13.6) is the identity for a large number of primes $\mathfrak{p}$.

We have the map $[\mathfrak{p}] : E \to \mathfrak{p}E$. We show that this is "like" the pth power Frobenius map. To do this, we show that it is inseparable of degree p (this is why we needed p to be split)[3], and then look at the j-invariants of the reduced maps modulo $\mathfrak{p}$.

As $\mathcal{E}\mathrm{ll}_{\overline{\mathbb{Q}}}(\mathscr{O}_K) = \mathcal{E}\mathrm{ll}_{\mathbb{C}}(\mathscr{O}_K)$ is finite, we can find a finite extension L/K and representatives $E_1, \ldots, E_h$ of classes in $\mathcal{E}\mathrm{ll}_{\mathbb{C}}(\mathscr{O}_K)$, that are defined over L. Let S be a set of primes containing the primes that satisfy one of the following conditions.

1. p ramifies in L. (Primes that ramify always cause trouble.)
2. E or some E_i has bad reduction at some prime of L lying over p.

[3] If $\mathfrak{p}$ is not split, one can still show the map is inseparable of degree p^2, with some more work.

3. $v_p(\mathrm{Nm}_{L/\mathbb{Q}}(j(E_i)-j(E_k))) \neq 0$ for some $i \neq k$. (This allows us to know what equivalence class an elliptic curve lies in, just by looking at its reduction modulo p.)

Let Λ be the lattice such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, and let $\mathfrak{a}$ be an integral ideal relatively prime to $\mathfrak{p}$ such that $\mathfrak{a}\mathfrak{p} = (\alpha)$ is principal (This exists by Corollary ??.??). By the equivalence of categories 13.1.1, the following maps on complex tori correspond to isogenies of elliptic curves:

$$\begin{array}{ccccccc} \mathbb{C}/\Lambda & \xrightarrow{i} & \mathbb{C}/\mathfrak{p}^{-1}\Lambda & \xrightarrow{i} & \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a}^{-1}\Lambda & \xrightarrow[\cong]{[\alpha]} & \mathbb{C}/\Lambda \\ \cong\downarrow\Phi & & \cong\downarrow\Phi & & \cong\downarrow\Phi & & \cong\downarrow\Phi \\ E & \xrightarrow{\phi_1} & \mathfrak{p}E & \xrightarrow{\phi_2} & \mathfrak{a}\mathfrak{p}E & \xrightarrow[\cong]{\phi_3} & E \end{array}$$

Let the composition of the top maps be f and the composition of the bottom maps be g.

Let ω be an invariant differential on E. Then $\omega' = \Phi^*\omega$ is an invariant differential on $\mathbb{C}/\Lambda$. It is in the form $c\,dz$. The composition of the top maps is just multiplication by α, so $f^*\omega' = \alpha\omega'$. By commutativity, we get $g^*\omega = \alpha\omega$ as well.

Let $p \notin S$ and $\mathfrak{P} \mid \mathfrak{p} \mid p$ in L, K, $\mathbb{Q}$, respectively. Since E has good reduction at $\mathfrak{P}$, we can reduce the elliptic curves and maps modulo $\mathfrak{P}$ to get

$$\widetilde{g}^*\widetilde{\omega} = \widetilde{\alpha}\widetilde{\omega} = 0$$

since $\mathfrak{P} \mid \alpha$. By a criterion for separability (g is separable iff g^* does not act as 0 on Ω_E), $\widetilde{g}$ is inseparable. Now

$$\begin{aligned} \deg(\phi_1) &= \mathfrak{N}\mathfrak{p} = p, \\ \deg(\phi_2) &= \mathfrak{N}\mathfrak{a} \perp p, \\ \deg(\phi_3) &= 1. \end{aligned}$$

An inseparable map must have degree divisible by p, and the composition of separable maps is separable, so $\widetilde{\phi_1}$ must be inseparable.

Any inseparable map factors through the Frobenius map:

$$\begin{array}{ccc} \widetilde{E} & \xrightarrow[\phi_p]{} & \widetilde{E}^{(p)} \\ & \searrow^{\widetilde{\phi_1}} & \cong\downarrow\varepsilon \\ & & \widetilde{\mathfrak{p}E}. \end{array} \tag{13.8}$$

We have $p\deg(\varepsilon) = \deg(\phi_p)\deg(\varepsilon) = \deg(\widetilde{\phi_1}) = p$ so $\deg(\varepsilon) = 1$. This shows ε is an isomorphism.

Thus we have

$$\widetilde{\mathfrak{p}E} \cong \widetilde{E}^{(p)}.$$

Now by definition of the Frobenius element (it is the pth power map modulo $\mathfrak{P}$), we have $j(\widetilde{E}^{(p)}) = j(\widetilde{E})^p = j(E)^{(\mathfrak{p},L/K)}$ modulo $\mathfrak{P}$. Putting everything together,

$$j(\mathfrak{p}E) \equiv j(\widetilde{E}^{(p)}) \equiv j(E^{(\mathfrak{p},L/K)}) \pmod{\mathfrak{P}}.$$

But we chose p so that nonisomorphic curves have j-invariants that are not congruent modulo p (item 3). Therefore, $\mathfrak{p}E \cong E^{(\mathfrak{p},L/K)}$. This shows that the action of $\mathfrak{p}$ is the same as the action of $(\mathfrak{p}, L/K)$, i.e. $F((\mathfrak{p}, L/K)) = [\mathfrak{p}]$.

Step 2: We show that $F : G(\overline{K}/K) \to \mathrm{Cl}(\mathscr{O}_K)$ has kernel equal to $G(\overline{K}/K(j(E)))$, and so factors through $G(K(j(E))/K) \hookrightarrow \mathrm{Cl}(\mathscr{O}_K)$. Indeed,

$$\begin{aligned}
\ker(F) &= \{\sigma : F(\sigma)E = E\} \\
&= \{\sigma : E^\sigma = E\} && \text{definition of } \sigma \\
&= \{\sigma : j(E)^\sigma = j(E)\} && j \text{ parameterizes isomorphism classes} \\
&= G(\overline{K}/K(j(E))).
\end{aligned}$$

We let $L = K(j(E))$.

Step 3: Let $\mathfrak{f}$ be the conductor of L/K. We extend Step 1 to all ideals $\mathfrak{a}$: for all $\mathfrak{a}$ we have

$$F((\mathfrak{a}, L/K)) = [\mathfrak{a}] \in \mathrm{Cl}(\mathscr{O}_K);$$

in other words $\mathfrak{f} = 1$ and the following composition is the identity map.

$$I_K/P_K \xrightarrow{\psi_{L/K}} G(L/K) \xhookrightarrow{F} \mathrm{Cl}(\mathscr{O}_K). \qquad (13.9)$$

$$I_K/P_K \xrightarrow{\cong} \mathrm{Id}$$

Given $\mathfrak{a} \in I_K^{\mathfrak{f}}$, there are infinitely many $\mathfrak{p} \in I_K^{\mathfrak{f}}$ in the same class as $\mathfrak{a}$ with degree 1 by Corollary **??.??**. Choose such a prime $\mathfrak{p}$, that does not divide a prime in S. Note $\mathfrak{a}, \mathfrak{p}$ differ by an ideal in $P_K(1, \mathfrak{f})$ so they have the same image by the Artin symbol. Step 1 shows that

$$F((\mathfrak{a}, L/K)) = F((\mathfrak{p}, L/K)) \overset{\text{Step 1}}{=} [\mathfrak{p}] = [\mathfrak{a}].$$

In particular, for any principal ideal $(\alpha) \in I_K^{\mathfrak{f}}$, we have $F(((\alpha), L/K)) = 1$. However, by definition the conductor is the smallest $\mathfrak{p}$ such that $\alpha \equiv 1 \pmod{\mathfrak{f}}$ implies $((\alpha), L/K) = 1$, so we must have $\mathfrak{f} = (1)$.[4] Thus the map $F : I_K^{\mathfrak{f}}/P_K(1, \mathfrak{f}) \to G(L/K)$ we had originally is actually just $F : I_K/P_K \to G(L/K)$, and we get (13.9).

Step 4: Since the conductor is divisible by exactly the ramifying primes, L/K is unramified, and $L \subseteq H_K$. On the other hand, the map $F \circ \psi_{L/K} : I_K/P_K \to \mathrm{Cl}(\mathscr{O}_K)$ is an isomorphism because $F \circ \psi_{L/K}$ is just the identity map. This gives $[L : K] = |\mathrm{Cl}(\mathscr{O}_K)| = [H_K : K]$. Hence $L = H_K$. This shows item 1.

[4] Technically, we only have $((\alpha), L/K) = 1$ for $(\alpha) \perp \mathfrak{f}$, and a priori $((\alpha), L/K)$ is not defined for $(\alpha) \perp \mathfrak{f}$. (We don't know $\mathfrak{f} = 1$ yet.) The proper way to conclude $\mathfrak{f} = (1)$ is transfer the problem over to ideles: We know $\psi_{L/K}(P_K^{\mathfrak{f}}) = 1$, so $\phi_{L/K}(K^\times \mathbb{U}_K^{\mathfrak{f}}) = 1$. By $\mathbb{I}_K^{\mathfrak{f}}/K(1, \mathfrak{f})\mathbb{U}_K(1, \mathfrak{f}) \cong \mathbb{I}_K/K^\times \mathbb{U}_K(1, \mathfrak{f})$ we conclude that $\phi_{L/K}(K^\times \mathbb{U}_K) = 1$. Hence $\mathfrak{f} = 1$.

Step 5: Item 3 now follows immediately, since we already showed $E^{\psi_{L/K}(\mathfrak{a})} = [\mathfrak{a}]E$ and we now know $L = H_K$. Item 2 follows since the fact that the composition in (13.9) is an isomorphism means the map $F : G(L/K) \to \mathrm{Cl}(\mathscr{O}_K)$ is surjective. Since F transfers the action of $G(L/K)$ on $\mathcal{E}\mathrm{ll}_{\overline{\mathbb{Q}}}(\mathscr{O}_K)$ to $\mathrm{Cl}(\mathscr{O}_K)$, and $\mathrm{Cl}(\mathscr{O}_K)$ acts simply transitively on $\mathcal{E}\mathrm{ll}_{\overline{\mathbb{Q}}}(\mathscr{O}_K)$, we get that the same is true for $G(L/K)$. □

5 Maximal abelian extension

We next carry out part 2 of our outline in Section 4.1. We construct the ray class fields for K, then take their compositum to get the maximal abelian extension.

Definition 13.5.1: Suppose E has CM by an order in K, and E is defined over H_K. A **Weber function** is an isomorphism $h : E/\operatorname{Aut}(1) \to \mathbb{P}^1$ defined over H_K. (So if $f : E \to E'$ is an automorphism, then $h(P) = h(f(P))$.)

We can always fix a concrete Weber function.

Example 13.5.2: The simplest Weber function is the following. If E has the form

$$y^2 = x^3 + Ax + B, \quad A, B \in H_K,$$

then take

$$h(P) = \begin{cases} x, & AB \neq 0 \\ x^2, & B = 0 \\ x^3, & C = 0. \end{cases}$$

In the 3 cases, respectively, $\operatorname{Aut}(E)$ is 1, $\mathbb{Z}/2$ or $\mathbb{Z}/4$, and $\mathbb{Z}/3$ or $\mathbb{Z}/6$.

We can define a Weber function that is "model independent," i.e. doesn't change under if we change to an isomorphic elliptic curve, by

$$h(f(z)) = \begin{cases} \frac{g_2(\Lambda)g_3(\Lambda)}{\Delta(\Lambda)}\wp(z,\Lambda), & j(E) \neq 0, 1728 \\ \frac{g_2(\Lambda)^2}{\Delta(\Lambda)}\wp(z,\Lambda)^2, & j(E) = 1728 \\ \frac{g_3(\Lambda)}{\Delta(\Lambda)}\wp(z,\Lambda)^3, & j(E) = 0. \end{cases}$$

This is because the expressions have "weight 0."

The importance of the Weber function is given below. It would not be true if $h(P)$ were just defined as $h(x, y) = x$.

Lemma 13.5.3. *Let E be an elliptic curve with CM by $\mathscr{O}$.*

1. *The extension $K(j(E), E_{tors})/K(j(E))$ is abelian.*
2. *The extension $K(j(E), h(E_{tors}))/K$ is abelian.*

The first statement is important because it tells us $G(\overline{K}/K(j(E)))$ acts in an abelian way on E_{tors}. Thus the "Galois representation" of the Galois group on E_{tors} is abelian. Thus, as we will see, it will decompose into two Grössencharacters.

Proof. We have an injective map $G(K(j(E), E[m])/K(j(E))) \hookrightarrow \text{Aut}(E[m])$.[5] Now, the image of G in $\text{Aut}(E[m])$ commutes with $\mathscr{O}_K$, so is contained in

$$\text{Aut}_{\mathscr{O}_K/m\mathscr{O}_K}(E[m]) \cong \text{Aut}_{\mathscr{O}_K/m\mathscr{O}_K}(\mathscr{O}_K/m\mathscr{O}_K) \cong (\mathscr{O}_K/m\mathscr{O}_K)^\times$$

which is abelian.

For the second, suppose $\sigma, \tau \in G(K(j(E), h(E_{\text{tors}}))/K)$. We show that $\sigma\tau = \tau\sigma$. Since $K(j(E))/K$ is abelian, $\sigma\tau\sigma^{-1}\tau^{-1}$ fixes $j(E)$. Now $\sigma\tau\sigma^{-1}\tau^{-1}$ gives an automorphism of $E' = \tau\sigma(E)$ because

$$(\sigma\tau\sigma^{-1}\tau^{-1})\tau\sigma(E) = \sigma\tau(E) \cong \tau\sigma(E),$$

as the Galois action factors through $G(K^{\text{ab}}/K)$ and hence is abelian (Theorem 13.4.1) (alternatively, because $\sigma\tau\sigma^{-1}\tau^{-1}$ fixes $j(E)$). As E is defined over H_K, we actually have equality.

Since h is invariant under automorphism, for any $P \in E_{\text{tors}}$,

$$h(P) = h(\sigma\tau\sigma^{-1}\tau^{-1}P) = \sigma\tau\sigma^{-1}\tau^{-1}h(P).$$

(We know h is defined over H_K and $\sigma\tau\sigma^{-1}\tau^{-1}$ fixes $H_K = K(j(E))$.) Hence $\sigma\tau\sigma^{-1}\tau^{-1}$ fixes $h(E_{\text{tors}})$ as well, and $\sigma\tau\sigma^{-1}\tau^{-1} = 1$. □

Theorem 13.5.4. *Suppose K is a quadratic imaginary field and E has CM by $\mathscr{O}_K$.*

1. *For an integral ideal $\mathfrak{a}$ of $\mathscr{O}_K$, $L_\mathfrak{a} := H_K(h(E[\mathfrak{a}])) = K(j(E), h(E[\mathfrak{a}]))$ is the ray class field of K modulo $\mathfrak{a}$.*

2. *The maximal abelian extension of K is*

$$K(j(E), h(E_{tors})).$$

Proof. Step 1: We need the following lemma.

Lemma 13.5.5. *Suppose E is an elliptic curve defined over L with CM by $\mathscr{O}_K$, and has good reduction at $\mathfrak{P}$. Let $\widetilde{E}$ be the reduction modulo $\mathfrak{P}$. Let $\theta : \text{End}(E) \to \text{End}(\widetilde{E})$ be the reduction map on endomorphisms. Then for any $\gamma \in \text{End}(\widetilde{E})$,*

$$\gamma \in im(\theta) \iff \gamma \text{ commutes with every element in } im(\theta).$$

Proof. Since E has good reduction, the map $\text{End}(E) \hookrightarrow \text{End}(\widetilde{E})$ in injective. Consider 2 cases.

[5] Since $E[m] = \mathbb{Z}/m \times \mathbb{Z}/m$, if we choose a basis for $E[m]$, we have $\text{Aut}(E[m]) \cong \text{GL}_2(\mathbb{Z}/m)$, so we have a Galois representation.

1. $\mathrm{End}(\widetilde{E})$ is a quadratic order. Then $\mathrm{End}(E) = \mathrm{End}(\widetilde{E})$ (as $\mathrm{End}(E)$ is a maximal order) so this case is clear.

2. $\mathrm{End}(\widetilde{E})$ is an order in a quaternion algebra. Then $\mathrm{End}(E) \otimes \mathbb{Q}$ is its own centralizer in the quaternion algebra $\mathrm{End}(\widetilde{E}) \otimes \mathbb{Q}$, by the Double Centralizer Theorem **??.??**.

□

Step 2: We show that in general, we can lift the Frobenius map.

Proposition 13.5.6: Suppose E has CM by $\mathscr{O}_K$ and is defined over H_K. Let $\mathfrak{P} \mid \mathfrak{p} \mid p$ in H_K, K, $\mathbb{Q}$, respectively, with $\mathfrak{p}$ having degree 1 and $p \notin S$, S being defined as in the proof of Theorem 13.4.4. Then the pth power Frobenius map can be lifted to a map on E, i.e. there is λ making the following commute:

$$\begin{array}{ccc} E & \xrightarrow{\lambda} & E^{(\mathfrak{p},H_K/K)} \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow{\widetilde{\lambda}=\phi_p} & \widetilde{E}^{(p)}. \end{array}$$

Moreover, if E corresponds to the complex torus $\mathbb{C}/\Lambda$, then up to isomorphism, λ corresponds to the map $\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{p}^{-1}\Lambda$. (Recall that $E^{(\mathfrak{p},H_K/K)} \cong \mathfrak{p}E$ by Theorem 13.4.4.)

Proof. We need to show ϕ_p is the reduction of some map; we do this by first reducing the problem to showing a certain endomorphism is in the image of θ and then showing the conditions of the previous lemma hold.

Again we use (13.8): $\widetilde{\phi_1} : \widetilde{E} \to \widetilde{\mathfrak{p}E}$ is "like" the Frobenius map. We know $\widetilde{\phi_1}$ is the reduction of a map, namely the map $\phi_1 : E \to \mathfrak{p}E$. Now note $\widetilde{\mathfrak{p}E} \cong \widetilde{E^{(\mathfrak{p},L/K)}} = \widetilde{E}^{(p)}$, the first from Thm 13.4.4 and the second from definition of the Frobenius element.

Let $\sigma = (\mathfrak{p}, L/K)$. It remains to show that $\varepsilon : \widetilde{E^\sigma} \to \widetilde{\mathfrak{p}E} \cong \widetilde{E^\sigma}$ is the reduction of a map ε', because then $\varepsilon'^{-1} \circ \phi_1$ will be the desired map. Let $[\widetilde{\alpha}] \in \mathrm{Aut}(\widetilde{E^\sigma})$ be the reduction of a map $[\alpha]$. To show ε commutes with $[\alpha]$, we consider $\widetilde{\phi_1} = \varepsilon \circ \phi_p$, and consider how $[\alpha]$ "commutes" with $\widetilde{\phi_1}$ and ϕ_p.

1. $\widetilde{\phi_1}$: By normalization (Proposition 13.2.2(3)), we know

$$\phi_1 \circ [\alpha]_E = [\alpha]_{E^\sigma} \circ \phi_1.$$

2. ϕ_p: Note that for any morphism of varieties $f : V \to W$ over a field of characteristic p, the following commutes, where ϕ_V, ϕ_W are the pth power Frobenius maps on V and W:

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ \downarrow{\scriptstyle \phi_V} & & \downarrow{\scriptstyle \phi_W} \\ V^{(p)} & \xrightarrow{f^\sigma} & W^{(p)} \end{array} \qquad \phi_W \circ f = f^\sigma \circ \phi_V.$$

Applying this to $[\alpha]_E$,

$$\phi_p \circ \widetilde{[\alpha]_E} = \widetilde{[\alpha]_E^\sigma} \circ \phi_p = \widetilde{[\alpha]_{E^\sigma}} \circ \phi_p,$$

where in the last step we used Theorem 13.2.2(4), noting $\sigma(\alpha) = \alpha$ since $\alpha \in K$ and $\sigma \in G(H_K/K)$.

Hence

$$\widetilde{[\alpha]_{E^\sigma}} \circ \underbrace{\varepsilon \circ \phi_p}_{\phi_1} \overset{1}{=} \varepsilon \circ \phi_p \circ \widetilde{[\alpha]_E} \overset{2}{=} \varepsilon \circ \widetilde{[\alpha]_{E^\sigma}} \circ \phi_p.$$

Cancelling ϕ_p gives $\widetilde{[\alpha]_{E^\sigma}} \circ \varepsilon = \varepsilon \circ \widetilde{[\alpha]_{E^\sigma}}$, so Lemma 13.5.5 shows ε is the reduction of some ε', as needed.

To finish, note that ϕ_1 does indeed correspond to $\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{p}^{-1}\Lambda$. Hence λ corresponds to $\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{p}^{-1}\Lambda$, up to some automorphism. □

Step 3: When $(\mathfrak{p}, H_K/K) = 1$, λ is just an endomorphism of E, hence equals $[\alpha]$ for some α. In fact, the following proposition shows it is $[\pi]$ for some π generating $\mathfrak{p}$, so that multiplication by π corresponds to the pth power Frobenius in the reduction.

Proposition 13.5.7: Suppose E has CM by $\mathscr{O}_K$ and is defined over H_K. For all but finitely many degree 1 prime ideals $\mathfrak{p}$ with $(\mathfrak{p}, H_K/K) = 1$ (equivalently, such that $\mathfrak{p}$ is principal), there exists a unique π such that $\mathfrak{p} = (\pi)$ and the following commutes.

$$\begin{array}{ccc} E & \xrightarrow{[\pi]} & E \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow{\phi_p} & \widetilde{E}. \end{array}$$

Proof. Since $(\mathfrak{p}, H_K/K) = 1$, Proposition 13.5.6 gives a diagram

$$\begin{array}{ccc} E & \xrightarrow{\lambda} & E \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow{\phi_p} & \widetilde{E}. \end{array}$$

for some λ. We know λ is in the form $[\pi]$, and show π satisfies the desired conditions. We have by Proposition 13.2.9 that

$$\mathrm{Nm}_{K/\mathbb{Q}}(\pi) = \deg([\pi]) = \deg(\phi) = p = \mathfrak{N}\mathfrak{p}$$

so either $(\pi) = \mathfrak{p}$ or $(\pi) = \overline{\mathfrak{p}}$. As always, when we're deciding between conjugates, normalization comes to the rescue. Take $\omega \in \Omega_E$ whose reduction modulo $\mathfrak{P}$ is nonzero. Normalization says that $[\pi]^*\omega = \pi\omega$ so

$$\widetilde{\pi}\widetilde{\omega} = \widetilde{[\pi]}^*\widetilde{\omega} = \phi_p^*\widetilde{\omega} = 0,$$

the last step since the Frobenius map is inseparable. We get $\mathfrak{P} \mid \pi$, forcing $(\pi) = \mathfrak{p}$.

For uniqueness, note the map

$$\mathscr{O}_K \xrightarrow[\cong]{[\cdot]} \mathrm{End}(E) \xrightarrow{\widetilde{E}} \mathrm{End}(\widetilde{E})$$

is injective for E having good reduction at $\mathfrak{P}$ (Theorem 13.4.3). □

Step 4: Consider (13.7). We need to show that $P_K(1, \mathfrak{a})$ is exactly the kernel of the Artin map $\psi_{L_\mathfrak{a}/K}$. Note that $P_K(1, \mathfrak{a})$ and $\ker(\psi_{L_\mathfrak{a}/K})$ are both subgroups of $P_K^\mathfrak{a} = \ker(\psi_{H_K/K}) = \ker(\psi_{L_\mathfrak{a}/K}(\bullet)|_{H_K})$. It suffices to show that for all but finitely many primes $\mathfrak{p}$ of degree 1 such that $(\mathfrak{p}, H_K/K) = 1$, we have $\mathfrak{p} \in P_K(1, \mathfrak{a})$ iff $\mathfrak{p} \in \ker(\psi_{L_\mathfrak{a}/K})$.

Let $\mathfrak{p}$ satisfy the conditions of Proposition 13.5.7. Since the reduction of $\psi_{L/K}(\mathfrak{p})$ is the Frobenius map, we get that $\psi_{L/K}(\mathfrak{p}) = [\pi]$, for some π such that $(\pi) = \mathfrak{p}$.[6] Since $(\mathfrak{p}, H_K/K) = 1$, we have the commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{\psi_{L/K}(\mathfrak{p})=[\pi]} & E \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow{\phi_p} & \widetilde{E}. \end{array} \tag{13.10}$$

We have the following string of equivalences, for all but finitely many degree 1 primes $\mathfrak{p}$ with $(\mathfrak{p}, H_K/K) = 1$,

1. $\mathfrak{p} \in P_K(1, \mathfrak{a})$.
2. $\mathfrak{p} = (\pi)$ where $\pi = u\alpha$ where u is a unit and $\alpha \equiv 1 \pmod{\mathfrak{a}}$.
3. For all $\mathfrak{a}$-torsion points $P \in E[\mathfrak{a}]$, $h([\pi]P) = h(P)$.

3′. For all $\mathfrak{a}$-torsion points $P \in \widetilde{E}[\mathfrak{a}]$, $\widetilde{h}(\widetilde{[\pi]}\widetilde{P}) = \widetilde{h}(\widetilde{P})$.

4. $(\mathfrak{p}, L_\mathfrak{a}/K)$ fixes $h(E[\mathfrak{a}])$.
5. $\mathfrak{p} \in \ker(\psi_{L_\mathfrak{a}/K})$.

(1) $\iff$ (2) is clear.

For (2) $\implies$ (3), note that for all $\mathfrak{a}$ torsion points $P \in E[\mathfrak{a}]$,

$$\begin{aligned} h([\pi]P) &= h([u][\alpha]P) \\ &= h([\alpha]P) && h \text{ is } \mathrm{Aut}(E)\text{-invariant} \\ &= h(P) && \alpha \equiv 1 \pmod{\mathfrak{a}} \text{ and } P \in E[\mathfrak{a}]. \end{aligned}$$

Note it is important that h be $\mathrm{Aut}(E)$-invariant.

[6] Note the analogy with the cyclotomic case. $\psi_{L/K}(\mathfrak{p})$ acts on torsion points as $[\pi]$, just as in the cyclotomic case it acted as the pth power map, that corresponds to $[p]$ if we consider the natural map $\mathbb{Z} \to \mathrm{End}(\mathbb{Q}(\zeta_n))$.

For (3′) $\implies$ (2), let $P \in E[\mathfrak{a}]$ be a torsion point. By [2, VII.3.1b], $E[\mathfrak{a}] \hookrightarrow \widetilde{E}[\mathfrak{a}]$ is injective for $\mathfrak{p} \nmid \mathfrak{a}$ and E with good reduction at $\mathfrak{p}$. Since h is an isomorphism (in particular, an injection) $E/\operatorname{Aut}(E) \to \mathbb{P}^1$, we get that $[\pi]P = [u]P$ for some $[u] \in \operatorname{Aut}(E)$. But $E[\mathfrak{a}] \cong \mathscr{O}_K/\mathfrak{a}$, so we can choose u such that $\pi \equiv u \pmod{\mathfrak{a}}$. Then there exists α such that $\pi = u\alpha$, with $\alpha \equiv 1 \pmod{\mathfrak{a}}$.

For (3) $\implies$ (4), we calculate the action of $(\mathfrak{p}, L/K)$ on a torsion point $P \in E[\mathfrak{a}]$, in the reduced curve:

$$\widetilde{P^{(\mathfrak{p},L/K)}} = \phi_p(\widetilde{P}) = \widetilde{[\pi]P},$$

the second equality from Proposition 13.5.7. This allows us to understand the action on the nonreduced curve, since $E[\mathfrak{a}] \hookrightarrow \widetilde{E}[\mathfrak{a}]$ is injective for $\mathfrak{p} \nmid \mathfrak{a}$ and $\mathfrak{p}$ of good reduction. We get

$$P^{(\mathfrak{p},L/K)} = [\pi]P.$$

Thus (3) implies

$$\begin{aligned} h(P)^{(\mathfrak{p},L/K)} &= h(P^{(\mathfrak{p},L/K)}) && (\mathfrak{p}, L/K) \text{ fixes } H_K \text{ and } E \text{ defined over } H_K \\ &= h([\pi]T) \\ &= h(T) && \text{by (3).} \end{aligned}$$

Now we prove (4) $\implies$ (3′). Let $\sigma \in G(\overline{K}/K)$ be an automorphism such that $\sigma|_{K^{\mathrm{ab}}} = (\mathfrak{p}, K^{\mathrm{ab}}/K)$. Then for any $P \in E[\mathfrak{a}]$,

$$\widetilde{h}(\widetilde{[\pi]}\widetilde{P}) \overset{(13.10)}{=} \widetilde{h}(\phi(\widetilde{P})) = \widetilde{h(P^\sigma)} = \widetilde{h(P)}^\sigma = \widetilde{h}(\widetilde{P}),$$

the last two equalities since $\sigma|_H = 1$, h is defined over H, and $\sigma|_{L_\mathfrak{a}}$ fixes $h(E[\mathfrak{a}])$ by assumption. Thus (3′) holds.

Now (4) $\iff$ (5) comes from the fact that $(\mathfrak{p}, L_\mathfrak{a}, K)$ already fixes $K(j(E))$, so to fix $L_\mathfrak{a}$ it only needs to fix $h(E[\mathfrak{a}])$.

Step 7: The maximal abelian extension is the union of the all ray class fields. Note every $\mathfrak{c}$ divides n for some n so we can just restrict to ray class fields corresponding to (n) for some $n \in \mathbb{N}$:

$$K^{\mathrm{ab}} = \bigcup_n K(j(E), h(E[n])) = K(j(E), h(E_{\mathrm{tors}})).$$

□

6 The Main Theorem of Complex Multiplication

Given $\sigma \in \operatorname{Aut}(\mathbb{C}/K)$, consider the map $\sigma : E(\mathbb{C}) \to E^\sigma(\mathbb{C})$. We would like to know how this map acts on torsion points. This is since to get Galois representations of elliptic curves, we look at how σ acts on torsion points—often specializing to torsion points that are a power of a prime.

Because we are considering CM elliptic curves, we can identify the torsion points with $K/\mathfrak{a}$, for some ideal $\mathfrak{a}$. Namely, given an analytic isomorphism $f : \mathbb{C}/\mathfrak{a} \xrightarrow{\cong} E(\mathbb{C})$, we can restrict it to $K/\mathfrak{a}$ to get

$$f|_{K/\mathfrak{a}} : K/\mathfrak{a} \xrightarrow{\cong} E_{\text{tors}} \hookrightarrow E(\mathbb{C}).$$

The main theorem of complex multiplication tells us we can transfer the map $\sigma : E(\mathbb{C}) \to E^\sigma(\mathbb{C})$ via an *analytic isomorphism* to a multiplication-by-an-idele map $[\mathbf{x}^{-1}] : K/\mathfrak{a} \to K/\mathbf{x}^{-1}\mathfrak{a}$, where $\mathbf{x}$ and σ are related in terms of the Artin map (to be made precise).

Definition 13.6.1: Let $\mathbf{x} = \prod_{\mathfrak{p}\in V_K^0} \mathfrak{p}^{m(\mathfrak{p})} \prod_{v\in V_K^\infty} v^{m(v)} \in \mathbb{I}_K$ be an idele. Let $\mathfrak{a}$ be an ideal, and define $\mathbf{x}\mathfrak{a}$ by

$$\mathbf{x}\mathfrak{a} = p(\mathbf{x})\mathfrak{a} = \left(\prod_{\mathfrak{p}\in V_K} \mathfrak{p}^{m(\mathfrak{p})}\right)\mathfrak{a}.$$

Define the map

$$[\mathbf{x}] : K/\mathfrak{a} \to K/\mathbf{x}\mathfrak{a} \tag{13.11}$$

as follows. Note $K/\mathfrak{a} \cong \prod_{\mathfrak{p}} K_{\mathfrak{p}}/\mathfrak{a}K_{\mathfrak{p}}$ by the Chinese Remainder Theorem, where x is just identified with its images in the $K_{\mathfrak{p}}/\mathfrak{a}K_{\mathfrak{p}}$: $(x_{\mathfrak{p}})_{\mathfrak{p}\in V_K^0}$. Then (13.11) sends

$$(a_{\mathfrak{p}}) \mapsto (x_{\mathfrak{p}} a_{\mathfrak{p}}) \text{ where } \mathbf{x} = (x_{\mathfrak{p}}). \tag{13.12}$$

Theorem 13.6.2 (Main Theorem of Complex Multiplication)**.** *Suppose E is an elliptic curve with CM by $\mathscr{O}_K$. Let $\sigma \in \mathrm{Aut}(\mathbb{C}/K)$ and $\mathbf{x} \in \mathbb{I}_K$ be such that*

$$\sigma|_{K^{ab}} = \phi_K(\mathbf{x}).$$

Fix an analytic isomorphism $f : \mathbb{C}/\mathfrak{a} \xrightarrow{\cong} E(\mathbb{C})$. Then there exists a unique analytic isomorphism $f' : K/\mathbf{x}^{-1}\mathfrak{a} \to E^\sigma(\mathbb{C})$ such that the following commutes:

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\mathbf{x}^{-1}} & K/\mathbf{x}^{-1}\mathfrak{a} \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f'} \\ E(\mathbb{C}) & \xrightarrow{\sigma} & E^\sigma(\mathbb{C}). \end{array}$$

Remark 13.6.3: The map (13.12) can be a bit weird to think about: For instance, consider the simpler case $K = \mathbb{Q}$, $\mathfrak{a} = \mathbb{Z}$. Take the idele $\mathbf{x}$ with 1's everywhere except $x_5 = 2$. Then $[\mathbf{x}]$ sends $\frac{1}{2} \mapsto \frac{1}{2}, \frac{1}{3} \to \frac{1}{3}, \frac{1}{7} \to \frac{1}{7}$ and so forth but sends $\frac{1}{5} \to \frac{2}{5}$. So it is surprising that $\mathbf{x}^{-1} : K/\mathfrak{a} \to K/\mathbf{x}^{-1}\mathfrak{a}$ can be related analytically to $E(\mathbb{C}) \to E^\sigma(\mathbb{C})$.

Compare this theorem to Proposition 13.5.7. Rather tan just dealing with the Frobenius element of a prime, we deal with the Artin map of an idele.

Proof. Note uniqueness follows from the fact that topologically, the closure of $K/\mathbf{x}^{-1}\mathfrak{a}$ is $\mathbb{C}/\mathbf{x}^{-1}\mathfrak{a}$, and any continuous function is determined by its values on a dense set.

First we prove this for E defined over $\mathbb{Q}(j(E))$ and $\mathfrak{a}$ integral. We do this in 2 steps. Step 1: Approximate σ by a field automorphism λ that is the Frobenius element of a prime $\mathfrak{p}$. (The Frobenius element is something much more concrete to work with than the abstract Artin map of an idele.) We will take better and better approximations, which determine the action on $E[m]$ for larger and larger m, and take an inverse limit.

So let L'_m be the Galois closure of $K(j(E), E[m])/K$. By Corollary **??.??**, there are infinitely many primes with $\mathfrak{P} \mid \mathfrak{p}$ in K and L such that

$$(\mathfrak{P}, L/K) = \sigma|_{L'_m}, \quad \mathfrak{N}(\mathfrak{p}) = 1.$$

We can furthermore choose $\mathfrak{p}$ satisfying the following, because each condition excludes only finitely many primes.

1. $\mathfrak{p}$ is unramified in L'_m.
2. $\mathfrak{p} \notin S$, where S is defined as in the proof of Theorem 13.4.4.
3. $\mathfrak{p} \nmid m$.

By Proposition 13.5.6, there exists a map $\lambda : E \to E^\sigma$ that reduces to ϕ_p modulo $\mathfrak{P}$. On $\widetilde{E}[m]$, both λ and σ act as ϕ_p. Because $\mathfrak{P} \nmid m$ by item 3, the reduction map modulo $\mathfrak{P}$, $E[m] \to \widetilde{E}[m]$, is injective. Hence λ and σ act the same on $E[m]$:

$$\lambda|_{E[m]} = \sigma|_{E[m]} : E[m] \to E^\sigma[m]. \tag{13.13}$$

But we know how the map λ acts: Proposition 13.5.6 tells us that the map $\lambda : E \to E^\sigma$ corresponds to the map on complex tori $i : \mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a}$.[7] Hence we have the commutative diagram

$$\begin{array}{ccc} \mathbb{C}/\mathfrak{a} & \xrightarrow{i} & \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a} \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} \\ E(\mathbb{C}) & \xrightarrow{\lambda} & E^\sigma(\mathbb{C}) \end{array} \tag{13.14}$$

for some analytic isomorphism f''.

Step 2: By Theorem 13.5.4, the ray class group modulo m is $K_m = K(j(E), h(E[m]))$. Note $K_m \subseteq L'_m$. Now by assumption, $\mathfrak{p}$ was chosen so that the images of $\mathfrak{p}$ and $\mathbf{x}$ under the Artin map both project to $\sigma|_{K_m}$:

$$\phi_{K_m/K}(\mathbf{x}) = \sigma|_{K_m} = \psi_{K_m/K}(\mathfrak{p}) = \phi_{K_m/K}(i_{\mathfrak{p}}(\pi))$$

where ψ, ϕ denote the Artin map on ideals and on ideles, respectively, and π is the uniformizer of $\mathfrak{p}$ in $K_{\mathfrak{p}}$. We have

$$\ker \psi_{K_m/K} = K^\times \mathbb{U}_K(1, m).$$

[7] The map σ and $\mathbf{x}^{-1}$ appearing in the theorem statement are bijections, while λ and i are not. This is okay, though, because we only use λ, i to approximate σ on m-torsion, and λ, i are injective on m-torsion, since $\mathfrak{P} \nmid m$.

(See Definition **??.??** for notation.) This follows from the definition of the ray class field and from the correspondence between ray class groups in Definition **??.??** and idele class groups in Example **??.??**. We have $\mathbf{x} \in i_{\mathfrak{p}}(\pi) \ker \phi_{K_m/K}$, giving

$$\mathbf{x} = \alpha \cdot i_{\mathfrak{p}}(\pi) \cdot \mathbf{u}, \quad \alpha \in K^\times, \quad \mathbf{u} \in \mathbb{U}_K(1, m).$$

We now compose (13.14) with the homothety α^{-1}, and note $(\mathbf{x}) = (\alpha)\mathfrak{p}$, to get the desired map $\mathbb{C}/\mathbf{x}^{-1}\mathfrak{a} \to E^\sigma(\mathbb{C})$:

$$\begin{array}{ccccc} \mathbb{C}/\mathfrak{a} & \xrightarrow{i} & \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a} & \xrightarrow{\alpha^{-1}} & \mathbb{C}/\mathbf{x}^{-1}\mathfrak{a} \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & \swarrow{\scriptstyle f'_m} & \\ E(\mathbb{C}) & \xrightarrow{\lambda} & E^\sigma(\mathbb{C}) & & \end{array} \tag{13.15}$$

Here, $f'_m(z) := f''(\alpha z)$.

This isn't quite what we want yet, though, because the top row is the map α^{-1} rather than the map $\mathbf{x}^{-1}$. We need to show that for m-torsion points, α^{-1} acts the same as $\mathbf{x}^{-1}$. Then we would have

$$\sigma(f(t)) = \lambda(f(t)) = f'_m(\alpha^{-1}t) = f'_m(\mathbf{x}^{-1}t), \quad t \in m^{-1}\mathfrak{a}/\mathfrak{a}.$$

The first equality is since σ, λ were by construction the same on $E[m]$ (13.13), so $\sigma \circ f$ and $\lambda \circ f$ are the same on $m^{-1}\mathfrak{a}/\mathfrak{a}$. The second is by commutativity of (13.15).

To show the third equality, we note that

$$\begin{array}{rll} & f'_m(\alpha^{-1}t) = f'_m(\mathbf{x}^{-1}t) & \text{for all } t \in m^{-1}\mathfrak{a}/\mathfrak{a} \\ (f'_m \text{ bijective}) & \iff \alpha^{-1}t - \mathbf{x}^{-1}t \in \mathfrak{a} & \text{for all } t \in m^{-1}\mathfrak{a} \\ & \iff \alpha^{-1}t_{\mathfrak{q}} - x_q^{-1}t_{\mathfrak{q}} \in \mathfrak{a}_{\mathfrak{q}} & \text{for all } t \in m^{-1}\mathfrak{a},\ \mathfrak{q} \\ (\text{multiplying by } x_{\mathfrak{q}} = \alpha[i_{\mathfrak{p}}(\pi)]_{\mathfrak{q}}u_{\mathfrak{q}}) & \iff [i_{\mathfrak{p}}(\pi)]_{\mathfrak{q}}u_{\mathfrak{q}}t - t \in \mathfrak{a}_{\mathfrak{q}} & \text{for all } t \in m^{-1}\mathfrak{a}_{\mathfrak{q}} \\ & \iff ([i_{\mathfrak{p}}(\pi)]_{\mathfrak{q}}u_{\mathfrak{q}} - 1)\mathfrak{a}_{\mathfrak{q}} \subseteq m\mathfrak{a}_{\mathfrak{q}} & \\ u_{\mathfrak{q}} \in \mathbb{U}_K(1, m) & \iff ([i_{\mathfrak{p}}(\pi)]_{\mathfrak{q}} - 1)\mathfrak{a}_{\mathfrak{q}} \subseteq m\mathfrak{a}_{\mathfrak{q}}. & \end{array}$$

Consider 2 cases.

1. $\mathfrak{q} \neq \mathfrak{p}$. In this case, $[i_{\mathfrak{p}}(\pi)]_{\mathfrak{q}} = 1$, so this is trivial.

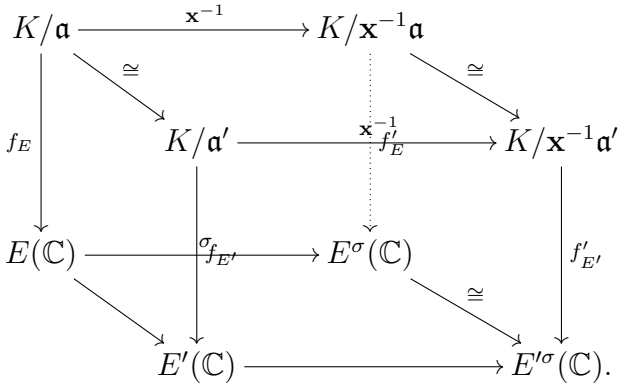
2. $\mathfrak{q} = \mathfrak{p}$: $[i_{\mathfrak{p}}(\pi)]_{\mathfrak{p}} = \pi$, and $\pi - 1$ is a unit. By assumption $\mathfrak{p} \nmid m$. hence $(\pi - 1)\mathfrak{a} = \mathfrak{a} = m\mathfrak{a}$.

Step 3: We now show that the maps f'_m are all actually the same for $m \geq 3$. Indeed, $f'_m|_{E[m]} = f'_{mn}|_{E[m]}$ by construction, so f'_m, f'_{mn} differ by an automorphism that fixes $E[m]$. This automorphism must be $[\zeta]$ for some element of norm 1 in K, and $f'_m = [\zeta] \circ f'_{mn}$. Since f'_m, f'_{mn} are isomorphisms, this says

$$E[m] \subseteq \ker[1 - \zeta]$$

The only possibilities are ζ a 4th or 6th root of unity, and if $\zeta \neq 1$, then $[1-\zeta]$ has norm at most 4. So for $m \geq 3$, $\zeta = 1$, and $f'_m = f'_{mn}$.

Step 4: Finally, we show the theorem holds for general E/L. Any elliptic curve E has a model E' defined over $M' = \mathbb{Q}(j(E))$, corresponding to a complex torus $\mathbb{C}/\mathfrak{a}'$ with $\mathfrak{a}'$ an integral ideal (see the left face below). Let $E \to E'$ be an isomorphism and $K/\mathfrak{a} \to K/\mathfrak{a}'$ be the corresponding map on torsion. Then the existence of $f'_{E'}$ for E'/L gives the existence of f'_E for E/L, by choosing f'_E to make the below diagram commute.



□

6.1 The associated Grössencharacter

The Main Theorem involved 2 different elliptic curves, and 2 different analytic isomorphisms. In the special case that σ fixes E, the curves will be the same, and by nudging the map upstairs by a constant depending on $\mathbf{x}$, we can restate the theorem using a consistent choice of f. (Compare to how we specialized from Proposition 13.5.6 to 13.5.7.) The action of $\phi_L(\mathbf{x})$ on the elliptic curve will "essentially" correspond to multiplication by $\chi_{E/L}$ on $K/\mathfrak{a}$.

Theorem 13.6.4 (Grössencharacter of an elliptic curve)**.** *Let E/L be an elliptic curve with complex multiplication by $\mathscr{O}_K$, and suppose $K \subseteq L$. Let $\mathbf{x} \in \mathbb{I}_L$ and $\mathbf{y} = \mathrm{Nm}_{L/K}(\mathbf{x}) \in \mathbb{I}_K$. Then there exists a unique $\alpha = \alpha_{E/L}(x) \in K^\times$ with the following properties.*

1. *$\alpha\mathscr{O}_K = (\mathbf{y})$.*

2. *For any fractional ideal $\mathfrak{a} \subseteq K$ and any analytic isomorphism $f : \mathbb{C}/\mathfrak{a} \to E(\mathbb{C})$, the following commutes.*

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\alpha\mathbf{y}^{-1}} & K/\mathfrak{a} \\ \downarrow f & & \downarrow f \\ E(L^{ab}) & \xrightarrow{\phi_L(\mathbf{x})} & E(L^{ab}). \end{array}$$

Moreover, defining $\chi_{E/L} : \mathbb{I}_L \to \mathbb{C}^\times$ *by*

$$\chi_{E/L}(\mathbf{x}) := \alpha_{E/L}(\mathbf{x})[\mathrm{Nm}_{L/K}(\mathbf{x}^{-1})]_\infty,$$

$\chi_{E/L}$ *is a Grössencharacter of* K*, and* $\chi_{E/L}$ *is ramified at* $\mathfrak{P}$ *(i.e.* $\chi_{E/L}(U_\mathfrak{P})$ *is not identically 1) iff* E *has bad reduction at* $\mathfrak{P}$*.*

Proof. Part 1: Since f is an isomorphism, uniqueness is clear. To construct α, choose any $\sigma \in \mathrm{Aut}(\mathbb{C}/L)$ such that $\sigma|_{L^{\mathrm{ab}}} = \phi_L(\mathbf{x})$. We use Theorem 13.6.2 with σ and $\mathbf{y} \in \mathbb{I}_K$, noting the following points.

1. $E^\sigma = E$ since E is defined over L and σ fixes L.
2. The image of f is contained in $E(L^{\mathrm{ab}})$ as $E_{\mathrm{tors}} \in E(L^{\mathrm{ab}})$ by Lemma 13.5.3.
3. By compatibility of the Artin map, $\phi_L(\mathbf{x})|_{K^{\mathrm{ab}}} = \phi_K(\mathrm{Nm}_{L/K}\,\mathbf{x}) = \phi_K(\mathbf{y})$.

We obtain an analytic map f' making the following commute.

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\mathbf{y}^{-1}} & K/\mathbf{y}^{-1}\mathfrak{a} \\ \downarrow f & & \downarrow f' \\ E(L^{\mathrm{ab}}) & \xrightarrow{\phi_L(\mathbf{x})} & E(L^{\mathrm{ab}}). \end{array}$$

Because

$$\mathbb{C}/\mathbf{y}^{-1}\mathfrak{a} \cong E^\sigma(\mathbb{C}) \cong E(\mathbb{C}) \cong \mathbb{C}/\mathfrak{a},$$

we have that $\mathbf{y}^{-1}\mathfrak{a}$ is homothetic to $\mathfrak{a}$, i.e. there exists β so that β takes $K/\mathbf{y}^{-1}\mathfrak{a}$ back to $K/\mathfrak{a}$. Defining $f''(x) = f'(\beta^{-1}x)$, we have that it differs from f by some automorphism $[\zeta]$: $f \circ [\zeta] = f''$. Let $\alpha = \beta\zeta$. Then we can extend the above diagram as follows.

$$\begin{array}{ccccc} K/\mathfrak{a} & \xrightarrow{\mathbf{y}^{-1}} & K/\mathbf{y}^{-1}\mathfrak{a} & \xrightarrow{\alpha} & K/\mathfrak{a} \\ \downarrow f & & \downarrow f' & \swarrow f & \\ E(L^{\mathrm{ab}}) & \xrightarrow{\phi_L(\mathbf{x})} & E(L^{\mathrm{ab}}) & & \end{array}$$

As $\alpha\mathbf{y}^{-1}\mathfrak{a} = \mathfrak{a}$, we get $(\alpha) = (\mathbf{y})$.

To see that α is independent of f and the ideal $\mathfrak{a}$, let f' be another analytic isomorphism $K/\mathfrak{a}' \to E(L^{\mathrm{ab}})$. Let the map $K/\mathfrak{a}' \to K/\mathfrak{a}$ be multiplication-by-γ. Then $f(\gamma x)$ is also an analytic isomorphism $K/\mathfrak{a}' \to E(L^{\mathrm{ab}})$. Hence $\gamma^{-1}f^{-1} \circ f'$ is an automorphism $[\zeta]$ of $K/\mathfrak{a}'$, i.e. $f'(x) = f([\zeta]\gamma x)$. Thus $\phi_L(\mathbf{x})[f'(x)] = f'(\alpha\mathbf{y}^{-1}x)$ as well.

Part 2: $\alpha_{E/L}$ and hence $\chi_{E/L}$ is a homomorphism since it's clear that $\phi_L(\mathbf{x}\mathbf{x}') \circ f = f \circ \alpha\alpha'\mathbf{y}\mathbf{y}'^{-1}$, and $\phi_L(\mathbf{x}^{-1}) \circ f = f \circ \alpha^{-1}\mathbf{y}$.

We need to check that $\chi_{E/L}(L^\times) = 1$ and that $\chi_{E/L}$ factors through a modulus.

For the first point, note $\phi_L(L^\times) = 1$, the identity element of $G(L^{\text{ab}}/L)$. Let $i : K^\times \to \mathbb{I}_K$, $L^\times \to \mathbb{I}_L$ be the diagonal maps, and suppose $\mathbf{x} = i(x)$. We have $\mathbf{y} = \text{Nm}_{L/K}(i(x)) = i(\text{Nm}_{L/K}(x))$. Then α is just the element such that $\alpha \,\text{Nm}_{L/K}(x)^{-1}$ induces the identity map, i.e. $\alpha = \text{Nm}_{L/K}(x) = [\text{Nm}_{L/K}\,\mathbf{x}]_\infty$, so $\chi_{E/L}(\mathbf{x}) = 1$.

For the second point, fix $m \geq 3$ ($m = 3$ works fine). We'll show that for any idele $\mathbf{x}$ in a small enough open subset of finite index, $\phi_L(\mathbf{x})$ acts just like multiplication by $\alpha_{E/L}(\mathbf{x})$ *and* fixes $E[m]$, without the extra $\text{Nm}_{L/K}(\mathbf{x})_\infty$ factor, so that α will actually be 1.

Let B_m be the kernel of the Artin map $\mathbb{I}_L \to G(L(E[m])/L)$ (abelian by Lemma 13.5.3), so that it induces an isomorphism

$$\phi_{L(E[m])/L} : \mathbb{I}_L/B_m \xrightarrow{\cong} G(L(E[m])/L). \tag{13.16}$$

We show that

$$U_m := B_m \cap L^\times \left(\text{Nm}_{L/K}^{-1}\, \mathbb{U}_K(1,m)\right) \subseteq \ker \chi_{E/L}.$$

This is of finite index in $\mathbb{I}_L$ since B_m is open of finite index in $\mathbb{I}_L$ and $K^\times \mathbb{U}_K(1,m)$ is open of finite index in $\mathbb{I}_K$.

Fixing an analytic isomorphism $f : \mathbb{C}/\mathfrak{a} \xrightarrow{\cong} E(\mathbb{C})$, we get that for any $t \in m^{-1}\mathfrak{a}/\mathfrak{a}$ and any $\mathbf{x} \in U_m$, $f(t) \in E[m]$ so

$$\begin{aligned} f(t) &= f(t)^{\phi_L(\mathbf{x})} && \text{by (13.16) and } \mathbf{x} \in B_m \\ &= f(\alpha\, \text{Nm}_{L/K}(\mathbf{x})^{-1} t) && \text{by the Main Theorem 13.6.2} \\ &= f(\alpha t) && t \in m^{-1}\mathfrak{a}/\mathfrak{a} \text{ and } \text{Nm}_{L/K}(\mathbf{x})_\mathfrak{p} \equiv 1 \pmod{m\mathscr{O}_{K_\mathfrak{p}}} \text{ for all } \mathfrak{p}. \end{aligned}$$

Thus multiplication by α fixes $m^{-1}\mathfrak{a}/\mathfrak{a}$, i.e. $\alpha \equiv 1 \pmod{m\mathscr{O}_K}$. Note $\text{Nm}_{L/K}(\mathbf{x})^{-1} \in \mathbb{U}_K(1,m)$, so

$$(\alpha) = (\mathbf{y}) = (\text{Nm}_{L/K}(\mathbf{x})) = \mathscr{O}_K$$

and α is a unit. Together with $\alpha \equiv 1 \pmod{m\mathscr{O}_K}$, we get $\alpha = 1$.[8]

Part 3: The relationship between ramification and bad reduction hinges on the Néron-Ogg-Shafarevich Criterion. See [3, pg. 169-170]. □

Note that if $\chi_{E/L}$ is unramified at $\mathfrak{P}$, then $\chi_{E/L}(i_\mathfrak{P}(U_\mathfrak{P})) = 1$, so it makes sense to talk about $\chi_{E/L}(\mathfrak{P})$ (defined as $\chi_{E/L}(i_\mathfrak{P}(\pi))$ for any uniformizer π).

Proposition 13.6.5: Let E/L be an elliptic curve with CM by $\mathscr{O}_K$, with $K \subseteq L$. Let $\mathfrak{P}$ be a prime of L of good reduction, let $\widetilde{E}$ be the reduction of E modulo $\mathfrak{P}$. Let $\phi_\mathfrak{P}$ be the Frobenius on $\widetilde{E}$. Then the following commutes.

$$\begin{array}{ccc} E & \xrightarrow{[\chi_{E/L}(\mathfrak{P})]} & E \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow{\phi_\mathfrak{P}} & \widetilde{E} \end{array}$$

[8] Any number in the form $m\tau + 1$, $\tau \in \mathscr{O}_K$ with norm 1 has norm at least $(\text{Nm}_{K/\mathbb{Q}}(m) - 1)^2 - 1$, by the triangle inequality. In order for it to have norm 1, $\tau = 0$.

Proof. Let π be a uniformizer of $L_{\mathfrak{P}}$, and let $\varpi = i_{\mathfrak{P}}(\pi)$. Note that $\varpi_\infty = 1$. Hence $\mathrm{Nm}_{L/K}(\varpi)_\infty = 1$, giving

$$\chi_{E/L}(\mathfrak{P}) = \chi_{E/L}(\varpi) = \alpha_{E/L}(\varpi).$$

If m is an integer such that $\mathfrak{P} \nmid m$, then $\mathrm{Nm}_{L/K}(\varpi)$ fixes $m^{-1}\mathfrak{a}/\mathfrak{a}$ (since it is 1 at all $\mathfrak{Q}$ with $\mathfrak{Q} \mid m$). Then

$$\begin{aligned} f(t)^{\phi_L(\varpi)} &= f([\alpha_{E/L}(\varpi)]\,\mathrm{Nm}_{L/K}(\varpi)^{-1}t) && \text{definition of } \alpha_{E/L} \\ &= f([\chi_{E/L}(\mathfrak{P})]\,\mathrm{Nm}_{L/K}(\varpi)^{-1}t) \\ &= [\chi_{E/L}(\mathfrak{P})]f(\mathrm{Nm}_{L/K}(\varpi)^{-1}t) && f \text{ preserves the action of } \mathscr{O}_K \\ &= [\chi_{E/L}(\mathfrak{P})]f(t) && \mathrm{Nm}_{L/K}(\varpi) \text{ fixes } m^{-1}\mathfrak{a}/\mathfrak{a}. \end{aligned}$$

Modulo $\mathfrak{P}$, $\phi_L(\varpi)$ is just the qth power Frobenius map, so we get

$$\phi_{\mathfrak{P}}|_{\widetilde{E}[m]} = \widetilde{[\chi_{E/L}(\mathfrak{P})]}|_{E[m]}.$$

Since an isogeny is determined by its action on $E[m]$ for $m \to \infty$ (the kernel of a nonzero isogeny is finite), we get that this is true for E, not just $E[m]$, as needed. □

To study the Galois representation $G(\overline{K}/H_K) \to \mathrm{Aut}\, E_{\mathrm{tors}}$ of E, we reduce modulo a prime $\mathfrak{P}$ of L, and show that on this reduced curve, the qth power Frobenius acts exactly as multiplication by the Grössencharacter. In particular, the qth power Frobenius is represented by multiplication by $\chi_{E/L}(\mathfrak{P})$ when we think of E_{tors} as $K/\mathfrak{a}$. Thinking of E_{tors} as a 2-dimensional space $\mathbb{Q}^2$, this says exactly that the eigenvalues of the Frobenius acting on E_{tors} is exactly $\chi_{E/L}(\mathfrak{P})$ and $\overline{\chi}_{E/L}(\mathfrak{P})$. Typically we just restrict our attention to ℓ-power torsion points for some ℓ.

7 L-series of CM elliptic curve

7.1 Defining the L-function

We define the L-series of an elliptic curve as the L-series of the corresponding Galois representation.

Definition 13.7.1: Let E be an elliptic curve defined over K, and ρ_ℓ the associated Galois representation $G(\overline{K}/K) \to \mathrm{Aut}\, V_\ell E \cong \mathrm{GL}_2(\mathbb{Q}_\ell)$.

Define the **local L-factor** of E at a prime $\mathfrak{p}$ of K as follows. Choose ℓ such that $\mathfrak{p} \nmid \ell$, and let

$$L_{\mathfrak{p}}(E, s) := L_{\mathfrak{p}}(\rho_\ell, s) = \det(1 - q^{-s}\,\mathrm{Frob}(\mathfrak{p})|(V_\ell E)^{I_{\mathfrak{p}}})^{-1},$$

where $q = \mathfrak{N}\mathfrak{p}$ and $I_{\mathfrak{p}}$ is the inertia subgroup of $G(\overline{K}/K)$. (Choose an embedding $\mathbb{Q}_\ell \hookrightarrow \mathbb{C}$.) The **$L$-series** of E is the product of local factors

$$L_{\mathfrak{p}}(E/K, s) := \prod_{\mathfrak{p}} L_{\mathfrak{p}}(E, s).$$

Remark 13.7.2: This is (almost) the same as saying: fix a prime ℓ and let $L(E/K, s) := L(\rho_\ell, s)$. The only difference is that we run into trouble with the local factor $L_\mathfrak{p}(\rho_\ell, s)$ on the right hand side, so we have to choose a different ℓ' and let this local factor be $L_\mathfrak{p}(\rho_{\ell'}, s)$ instead.

The following is an equivalent definition (that is more concrete).

Definition 13.7.3: Let N be the conductor[9] of the elliptic curve E. Define the local L-factor by

$$L_\mathfrak{P}(E, s) = 1 - a_q q^{-s} + \chi(q) q q^{-2s}, \quad a_q = q + 1 - |E(\mathbb{F}_q)|, \quad \chi(q) = \begin{cases} 1, & m \perp N \\ 0, & \text{else} \end{cases}$$

where $q = \mathfrak{N}\mathfrak{p}$. Thus

$$L_v(E, s) = \begin{cases} 1 - a_q q^{-s} + q q^{-2s}, & \text{good reduction} \\ 1 - q^{-s}, & \text{split multiplicative reduction} \\ 1 + q^{-s}, & \text{non-split multiplicative reduction} \\ 1, & \text{additive reduction.} \end{cases}$$

Note that a_q, the "trace of Frobenius," is related to the number of points of E over $\mathbb{F}_q$. Hence the L-function contains information about the number of points of E over each $\mathbb{F}_q$.

Showing that these two definitions are equivalent requires us to show that $(V_\ell E)^{I_\mathfrak{p}}$ is 2, 1, or 0-dimensional when E has good, multiplicative, and additive reduction, respectively. The general idea is that the action of $I_\mathfrak{p}$ on $V_\ell E$ contains exactly the information lost by looking at the reduced elliptic curve, since $I_\mathfrak{p}$ is exactly the kernel of $D_\mathfrak{p}(\overline{K}/K) \to G(\overline{k}/k)$, so nontrivial action of $I_\mathfrak{p}$ corresponds to bad reduction.

In the CM case, we cannot have multiplicative reduction, so the L-series is particularly simple. We will show that the two definitions are equivalent in this case.

Theorem 13.7.4. *Let E/K be a CM elliptic curve. Then E cannot have multiplicative reduction at any prime.*

Proof. An elliptic curve E has potential good reduction iff its j-invariant is integral [2, VII.5.5]. CM have integral j-invariants, so have potential good reduction, i.e. have good or multiplicative reduction. □

Proof that Definitions 13.7.1 and 13.7.3 are equivalent in the CM case. Suppose E has CM by an order $\mathscr{O}$ in K, and E is defined over L. By Néron-Ogg-Shafarevich, $I_\mathfrak{p}$ acts trivially on $V_\ell E$ iff E has good reduction at $\mathfrak{p}$. Let $q = \mathfrak{N}\mathfrak{p}$.

In the case of good reduction we need to show $\det(1 - q^{-s}\operatorname{Frob}(\mathfrak{p})|V_\ell E) = 1 - a_q a^{-s} + q q^{-2s}$. Every endomorphism ϕ on E satisfies $\phi^2 - \operatorname{tr}(\phi)\phi + \deg(\phi) = 0$, where $\operatorname{tr}(\phi) = 1 + \deg(\phi) -$

[9] N is divisible by exactly the primes of bad reduction

$\deg(1-\phi)$. Since $\mathrm{Frob}(\mathfrak{p})$ acts as the Frobenius morphism $\phi_{\mathfrak{p}}$, its characteristic polynomial is

$$\det(\lambda - \mathrm{Frob}(\mathfrak{p})) = \lambda^2 - \mathrm{tr}(\phi_{\mathfrak{p}})\lambda + \deg(\phi_{\mathfrak{p}}).$$

But

$$\begin{aligned}\deg(\phi_{\mathfrak{p}}) &= q \\ \mathrm{tr}(\phi_{\mathfrak{p}}) &= 1 + \deg(\phi_{\mathfrak{p}}) - \deg(1-\phi_{\mathfrak{p}}) \\ &= q + 1 - \ker(1-\phi_{\mathfrak{p}}) \\ &= q + 1 - |E(\mathbb{F}_q)|.\end{aligned}$$

(This part of the proof doesn't use the fact that E has CM.)

Since E has no multiplicative reduction by Theorem 13.7.4, it remains to prove that $W := (V_\ell E)^{I_{\mathfrak{p}}} = 0$ when E has multiplicative reduction. We know by Néron-Ogg-Shafarevich that $\dim(W) \leq 1$. But because E is CM, $V_\ell E \cong (\varprojlim_n \ell^{-n}\mathfrak{a}/\mathfrak{a}) \otimes \mathbb{Q}$ has the structure of a $\mathscr{O}_K \otimes \mathbb{Q}_\ell$-vector space. If $a \in W$, then for any $\alpha \in K$, $\alpha a \in W$ because $[\alpha]$ commutes with the Galois action. Hence W is not just a $\mathbb{Q}_\ell$-subspace of V, but also a $\mathscr{O}_K \otimes \mathbb{Q}_\ell$-subspace. Hence its dimension over $\mathbb{Q}_\ell$ is even, and must be 0. □

7.2 Analytic continuation

Theorem 13.7.5 (Deuring)**.** *Let E/L be an elliptic curve with CM by $\mathscr{O}_K$ with $K \subseteq L$. Then*

$$L(E/L, s) = L(s, \psi_{E/L})L(s, \overline{\psi_{E/L}}).$$

Corollary 13.7.6 (Analytic continuation of L-function for CM elliptic curves)**.** *Let E/L be an elliptic curve with CM by $\mathscr{O}_K$. Then L admits an analytic continuation to $\mathbb{C}$ and satisfies a functional equation relating its values at s and $2-s$.*

This theorem for general elliptic curves is very deep (it follows from the Modularity Theorem and the analytic properties of L-functions associated to modular forms).

Proof of Theorem 13.7.5. By Theorem 13.7.4, E has no multiplicative reduction. Let $\mathfrak{P}$ be a prime, and consider 2 cases.

1. E has good reduction at $\mathfrak{P}$. Choose any ℓ not dividing $\mathfrak{P}$. The characteristic polynomial of the action of $\phi_{\mathfrak{P}}$ on $V_\ell E$ is $\det(\lambda - \phi_{\mathfrak{P}}|V_\ell E)$. However, if we make the identification $E_{\mathrm{tors}} \cong K/\mathfrak{a}$, we have

   $$V_\ell E = \varprojlim \ell^{-n}\mathfrak{a}/\mathfrak{a},$$

   and we know that $\phi_{\mathfrak{P}}$ acts on $E_{\mathrm{tors}} \cong K/\mathfrak{a}$ as multiplication by $\chi_{E/L}(\mathfrak{P})$. Therefore, the eigenvalues of the action of $\phi_{\mathfrak{P}}$ on $V_\ell E$ are just $\chi_{E/L}(\mathfrak{P})$ and $\overline{\chi}_{E/L}(\mathfrak{P})$, and

   $$\det(\lambda - \phi_{\mathfrak{P}}|V_\ell E) = (\lambda - \chi_{E/L}(\mathfrak{P}))(\lambda - \overline{\chi}_{E/L}(\mathfrak{P})).$$

   Taking $\lambda = p^s$ and dividing by p^{2s} gives

   $$L_{\mathfrak{P}}(E/L, s) = \det(1 - p^{-s}\phi_{\mathfrak{P}}|V_\ell E) = L_{\mathfrak{P}}(s, \chi_{E/L})L(s, \overline{\chi}_{E/L}).$$

2. E has bad reduction at $\mathfrak{P}$. Then $\chi_{E/L}(\mathfrak{P}) = 0$ by definition, and $L_{\mathfrak{P}}(E/L, s) = 1 = (1 - \chi_{E/L}(\mathfrak{P}))(1 - \overline{\chi}_{E/L}(\mathfrak{P})) = L_{\mathfrak{P}}(s, \chi_{E/L})L(s, \overline{\chi}_{E/L})$.

Multiplying together all the local factors gives the result. □

Proof of Corollary 13.7.6. The L-functions of Grössencharacters have analytic continuation (Theorem **??.??**, which works for Grössencharacters as well). Thus the result follows directly from Theorem 13.7.5. □

Thus we have carried out the program in Section **??.??** for CM elliptic curves, to get the correspondences.

$$\text{(CM Elliptic curves)} \to \text{(Galois representation)} \to \text{(2 Grössencharacters)}$$

Remember Grössencharacters are 1-dimensional automorphic representations. If we wanted a modular form, we can use the technique of *automorphic induction* to construct a modular form from 2 Grössencharacters.

Chapter 14

Modular curves

Bibliography

[1] N. Koblitz. *Elliptic Curves and Modular Forms*. Number 97 in GTM. Springer, 1984.

[2] J. Silverman. *The Arithmetic of Elliptic Curves*. Number 106 in GTM. Springer, 1986.

[3] J. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Number 151 in GTM. Springer, 1994.

[4] R. Vakil. Algebraic geometry, 2013.

[5] L. Washington. *Elliptic Curves and Cryptography*. 2008.

Index