Math 844 Notes
Elliptic Curves, Arithmetic Geometry, and Modular Forms

Lectures by Nigel Boston
Notes by Daniel Hast

Fall 2013

Contents

Chapter I

Quadrics, cubics, and elliptic curves

I.1 2013-09-04

I.1.1 Preliminaries

Course information:

- Course website: `http://www.math.wisc.edu/~boston/844bis.html`
- Office hours:
  - W 1:30–3, 3619 Engineering Hall
  - Th 9:30–11, 303 Van Vleck
- The grade is based on 10 homeworks.

Textbooks:

- Rob Rhoades' notes (questionable — contains numerous errors)
- Silverman, *The Arithmetic of Elliptic Curves I, II*
- Silverman–Tate, *Rational Points on Elliptic Curves*
- Knapp (modular curves)
- Koblitz (special family of elliptic curves)
- ⋮
- All derive from Tate, Inv. Math 23 (1974) and Cassels, J. London Math Soc. (1966).

I.1.2 Overview

A few examples:

Example I.1.1. Consider the 3-4-5 triangle, which has area 6. We call an integer n *congruent* if it is the area of a right triangle with rational sides.

Which integers are congruent?

- 5 is congruent.
- 1 is not congruent (Fermat: $x^4 - y^4 = u^2$).

It turns out that

Proposition I.1.2. *An integer n is congruent $\iff$ the only rational solutions of $y^2 = x^3 - n^2x$ are*

$$(0,0), (n,0), (-n,0).$$

This is an elliptic curve: we have turned a question about a diophantine equation into a question about points on an elliptic curve.

Remark I.1.3. We will often work with a homogeneous version:

$$y^2z = x^3 - n^2xz^2.$$

The points are in projective space $\mathbb{P}^2$, i.e., equivalence classes $(x : y : z)$, where $(x, y, z) \neq (0, 0, 0)$ and

$$(x, y, z) \sim (\lambda x, \lambda y, \lambda z)$$

for all $\lambda \neq 0$.

Definition I.1.4. Let K be a field. An *elliptic curve* over K is a nonsingular cubic curve with coefficients in K which has a point.

Remark I.1.5. By "nonsingular", we mean nonsingular (smooth) over *any* extension field.

Example I.1.6. The curve

$$3x^3 + 4y^3 + 5z^3 = 0$$

has no solutions over $\mathbb{Q}$, so it is not an elliptic curve over $\mathbb{Q}$.

Example I.1.7. The curves $y^2 = x^3$ and $y^2 = x^3 - x^2$ are singular cubics, and therefore are not elliptic curves.

Remark I.1.8 (Standard form). The *standard form* for elliptic curves in $\operatorname{char} K \neq 2$ is

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

where $f \in K[x]$ is a cubic with distinct roots in $\overline{K}$.

I.1.3 Some examples by Elkies

Example I.1.9 (Elkies, 1986). Euler (1769) incorrectly claimed that

$$x^4 + y^4 + z^4 = t^4$$

has no nonzero integer solutions. This is the same as asking for rational points on

$$x^4 + y^4 + z^4 = 1.$$

Elkies (1986) showed there are infinitely many counterexamples (dense). The method is to show that this surface contains lots of elliptic curves with lots of rational points.

Example I.1.10. (Trinks) The Galois group of $x^7 - 7x + 3$ over $\mathbb{Q}$ is simple of order 168. Elkies came up with several more equations with the same Galois group:

$$x^7 - 154x + 99$$
$$37^2x^7 - 28x + 9$$
$$499^2x^7 - 23956x + 3^4 \cdot 113$$

Elkies conjectured that these are the only solutions.

Polynomials $ax^7 + bx + c$ having Galois group G_{168} are parametrized by the curve

$$y^2 = x\left(81x^5 + 396x^4 + 738x^3 + 660x^2 + 269x + 48\right),$$

which has genus 2. A conjecture of Mordell, proving by Faltings, is that there are only finitely many rational points on such a curve. In fact, in this case, there are exactly 7 rational points.

Example I.1.11 (Elkies). Over $\operatorname{char} K = 0$, how often does $ax^5 + bx^2 + c$ have Galois group $G_{20} = C_5 \rtimes C_4 \leq S_5$? The solution is parametrized by points on

$$E : y^2 + xy + y = x^3 + x^2 + 35x - 28$$

(154A in Cremona's database).

$E(\mathbb{Q})$ has 8 points, of which 2 give solutions to the original question.

I.1.4 Moral

Many problems lead to us asking for the rational points on some variety.

Say this is a curve. There are basically three flavors, depending on the genus:

(1) Genus 0 is very easy (Diophantus' method).

(2) Genus 1 is the intermediate case (elliptic curves).

(3) Genus > 1 is hard.

Some applications of elliptic curves:

(1) Fermat's Last Theorem

(2) Elliptic curve cryptography

These use an additional fact:

Fact I.1.12. Suppose E is an elliptic curve over a field K. Given a field extension $L \supseteq K$, let

$$E(L) = \{\text{points on } E \text{ defined over } L\}.$$

This is an abelian group.

Remark I.1.13. So, for instance, the question about congruent numbers becomes a question of whether there is a point of infinite order on the corresponding elliptic curve. Similarly, in Example I.1.11, $E(\mathbb{Q})$ is a cyclic group of order 8.

I.1.5 Order of specific topics

(1) Elliptic curves over $\mathbb{R}$ and $\mathbb{C}$

(2) Elliptic curves over finite fields

- Hasse's theorem

(3) Elliptic curves over $\mathbb{Q}$ and $\mathbb{Z}$

- Mordell's theorem

(4) L-functions

$$\sum_{n\geq 1} \frac{a_n}{n^s}$$

(5) Modular forms

$$\sum_{n\geq 1} a_n q^n$$

(6) Shimura–Taniyama

(7) Galois representations

(8) Tate–Shafarevich group

(9) Complex multiplication

(10) Birch–Swinnerton-Dyer conjecture

I.2 2013-09-06

I.2.1 Projective space

Let K be a field.

We define projective space

$$\mathbb{P}^n(K) \stackrel{\text{def}}{=} (K^{n+1} - \{\mathbf{0}\})/\sim,$$

where

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n) \iff x_i = \lambda y_i$$

for some $\lambda \in K^\times$. The equivalence class of $(x_0, \dots, x_n)$ is denoted $(x_0 : \cdots : x_n)$.

I.2.2 Nonsingular/smooth

Consider

$$f(x_0, \dots, x_n) = 0$$

with $f \in K[x_0, \dots, x_n]$ homogeneous, and let $L \subseteq \overline{K}$ be an algebraic extension. A point $P \in \mathbb{P}^n(L)$ is a *singularity* of $f = 0$ provided that $f(P) = 0$ and

$$\frac{\partial f}{\partial x_i} = 0 \qquad \forall i.$$

We say that $\{f = 0\}$ is *nonsingular* $\iff$ it has no singularities in any such L.

Example I.2.1 (elliptic curves). Let $f \in K[x]$ be a cubic with distinct roots in $\overline{K}$ (char $K \neq 2$). Then

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

is nonsingular, so defines an elliptic curve. (Indeed, it has a point at infinity, so it has at least one point.)

Proof. Write

$$y^2 = (x - a)(x - b)(x - c)$$

with $a, b, c \in \overline{K}$ distinct. Then we have

$$y^2 - (x - a)(x - b)(x - c) = 0,$$

and homogenizing, we obtain

$$y^2 z - (x - az)(x - bz)(x - cz) = 0.$$

The points at infinity are where $z = 0$; hence there's only the point $(0 : 1 : 0)$.

To show nonsingularity, simultaneously solve

$$\begin{aligned} F &= y^2z - (x-az)(x-bz)(x-cz) = 0, \\ \frac{\partial F}{\partial x} &= -(x-bz)(x-cz) - (x-cz)(x-az) - (x-az)(x-bz) = 0, \\ \frac{\partial F}{\partial y} &= 2yz = 0, \\ \frac{\partial F}{\partial z} &= y^2 + a(x-bz)(x-cz) + b(x-cz)(x-az) + c(x-az)(x-bz) = 0. \end{aligned}$$

Since $2yz = 0$ and $\operatorname{char} K \neq 2$, we have $y = 0$ or $z = 0$. If $z = 0$, then $x = 0$ and so $y = 0$, which is impossible. But if $y = 0$, then

$$(x-az)(x-bz)(x-cz) = 0.$$

Say (without loss of generality) $x - az = 0$. Then

$$(x-bz)(x-cz) = 0.$$

Say (WLOG) $x - bz = 0$. But $a \neq b$, so this is a contradiction. Hence there are no simultaneous solutions. □

I.2.3 Applications of elliptic curves

(1) $h(\mathbb{Q}(\sqrt{-\Delta}))$ as $\Delta \to \infty$: effective bounds (Gross–Zagier, Goldfeld)

(2) Factoring integers (Lenstra)

(3) Sphere-packings (Elkies)

(4) Inverse Galois problem

(5) Taxicab problem:

$$1729 = 1^3 + 12^3 = 9^3 + 10^3.$$

I.2.4 Favorite curves over $\mathbb{Q}$

Remark I.2.2. Now we start the course proper.

Some favorite curves (with homogeneous $\tilde{f} = 0$ solution on the right, since we'll often look at that):

$$\begin{aligned} x^3 + y^3 &= 1 & x^3 + y^3 - z^3 &= 0 \\ y^2 &= x^3 - x & y^2z - \left(x^3 - xz^2\right) &= 0 \\ y^2 + y &= x^3 - x & y^2z + yz^2 - x^3 - xz^2 &= 0 \end{aligned}$$

Note I.2.3. The solutions of $E : \tilde{f} = 0$ in $K \supseteq \mathbb{Q}$ are denoted

$$E(K) \stackrel{\text{def}}{=} \left\{ (a:b:c) \;\middle|\; \tilde{f}(a,b,c) = 0 \right\}.$$

Example I.2.4. Consider

$$E : y^2z - x^3 + xz^2 = 0.$$

Then you get a graph with two circles (one of which goes off to infinity). But if we look at $y^2 = f(x)$ where f has only 1 real root, then we get only one "circle" in the real plane.

I.2.5 Diophantus' method

We want all the rational solutions to

$$x^2 + y^2 = z^2.$$

The affine equation is

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

the unit circle. Look at the line of slope t through $(-1, 0)$. This intersects the unit circle at a point

$$(-1 + a, at),$$

where a is given by

$$(-1 + a)^2 + (at)^2 = 1.$$

Solving for a, the line has exactly one other intersection point:

$$\begin{aligned} 1 - 2a + a^2 + a^2t^2 &= 1 \\ -2a + a^2\left(1 + t^2\right) &= 0, \end{aligned}$$

whence

$$a = 0 \qquad \text{or} \qquad a = \frac{2}{1 + t^2}.$$

So the point is

$$(-1 + a, at) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right),$$

and the parametrization is

$$(x : y : z) = \left(1 - t^2 : 2t : 1 + t^2\right).$$

I.2.6 Example from Emissary, MSRI newsletter

The numbers $1, 2, \ldots, 8$ have the property

$$1 + 2 + 3 + 4 + 5 = 7 + 8.$$

Say

$$1 + 2 + 3 + 4 + \cdots + (k - 1) = (k + 1) + \cdots + n.$$

Then

$$\begin{aligned} &\frac{1}{2}k(k-1) = \frac{1}{2}n(n+1) - \frac{1}{2}k(k+1) \\ \implies &\frac{1}{2}n(n+1) = k^2. \end{aligned}$$

We want to find lots of solutions to this equation. Say $n = 2m$ (with $m \in \mathbb{Z}$). Then

$$\begin{aligned} m(2m+1) &= k^2, \\ \gcd(m, 2m+1) &= 1, \end{aligned}$$

so $m = x^2$, $2m + 1 = y^2$ yields

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

We now have Pell's equation:

$$y^2 - 2x^2 = 1.$$

We can solve this using some algebraic number theory: the units of $\mathbb{Q}(\sqrt{2})$ have the form $\{\pm 1\} \times \langle u \rangle$ for some fundamental unit u, and $y + \sqrt{2}x$ has norm 1.

For instance, $(3, 2)$ is a solution. More generally,

$$\left(3 + 2\sqrt{2}\right)^n = y_n + \sqrt{2}x_n$$

yields infinitely many integral solutions.

Suppose we want *rational* solutions of

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

We use a method due to Diophantus ($\Delta\iota o\varphi\alpha\nu\tau o\varsigma$). Consider lines of rational slope t through the point $(0, 1)$, with equation

$$y = 1 + tx.$$

This gives

$$\begin{aligned} (1 + tx)^2 &= 2x^2 + 1 \\ 2tx + t^2x^2 &= 2x^2, \end{aligned}$$

so $x = 0$ (the original point) or

$$\begin{aligned} 2t &= \left(2 - t^2\right) x, \\ x &= \frac{2t}{2 - t^2}, \\ y &= 1 + tx = \frac{2 + t^2}{2 - t^2}, \end{aligned}$$

which is the desired rational parametrization.

I.2.7 Diophantus' method in greater generality

Challenge question: Can n be divided into 2 integers whose product is a cube minus a side?

This is given by the equation

$$x(n-x) = y^3 - y.$$

This is an elliptic curve. We will use the "tangent-chord method" to analyze this situation.

I.3 2013-09-09

I.3.1 The tangent-chord method

Last time, we looked at Diophantus's (3rd century) method for solving plane quadratics. What about plane cubics? E.g.,

$$x(6-x) = y^3 - y. \tag{$*$}$$

Consider the tangent at $(0,-1)$. This is

$$6 - 2x = 3y^2\frac{dy}{dx} - \frac{dy}{dx},$$

which gives

$$\frac{dy}{dx} = \frac{6-2x}{3y^2-1} = \frac{6}{2} = 3$$

at $(0,-1)$. Hence the tangent line is

$$y = -1 + 3x.$$

To find the other point of intersection, we have

$$\begin{aligned} 6x - x^2 &= (3x-1)^3 - (3x-1) \\ 6x - x^2 &= 27x^3 - 27x^2 + 9x - 1 - 3x + 1 \\ 26x^2 &= 27x^3 \\ x &= 0, 0, \frac{26}{27}. \end{aligned}$$

In the last case, we have

$$x = \frac{26}{27} \implies y = -1 + \frac{26}{9} = \frac{17}{9}.$$

Take the line joining $(0,0)$ to $\left(\frac{26}{27}, \frac{17}{9}\right)$,

$$\frac{17}{9}x = \frac{26}{27}y.$$

Plug in $(*)$: get rational-coefficient cubic in x, solutions

$$x = 0, \frac{26}{27}, \text{ some rational number.}$$

In fact, the solutions are

$$x = 0, \frac{26}{27}, -\frac{5382}{4913},$$

so the other point of intersection is

$$\left(-\frac{5382}{4913}, -\frac{621}{289}\right).$$

Remark I.3.1. This is known as the *tangent-chord method* for producing points with rational coordinates (rational points).

I.3.2 Rational points on our favorite curves

Let us look at the rational points on some of our favorite elliptic curves.

Example I.3.2. The curve

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

has rational points at ∞, $(-1, 0)$, $(0, 0)$, and $(1, 0)$. In fact,

$$E(\mathbb{Q}) = \{\infty, (-1, 0), (0, 0), (1, 0)\}.$$

Example I.3.3 (a curve with a cusp). The curve

$$y^2 = x^3$$

has a rational parametrization:

$$x = t^2, \qquad y = t^3.$$

Exercise I.3.4 (a curve with a node). Find a rational parametrization of the nodal curve

$$y^2 = x^2(x + 1).$$

Remark I.3.5. In the singular case, a cubic curve's genus degenerates down to zero, which is why rational parametrizations can be found. (Genus zero curves are simpler than genus one.)

Example I.3.6. The curve

$$x^3 + y^3 = 1$$

has points of inflection at $(1, 0)$ and $(0, 1)$. In fact,

$$E(\mathbb{Q}) = \{\infty, (1, 0), (0, 1)\}.$$

Remark I.3.7 (inflection points). We will see later that points of inflection have order 3.

Example I.3.8. It will turn out that

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

has infinitely many rational points.

I.3.3 The group structure

Consider an elliptic curve

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

where $f \in \mathbb{Q}[x]$ is cubic with distinct roots in $\overline{\mathbb{Q}}$. A line intersections the elliptic curve at exactly 3 points P_1, P_2, P_3 (counting multiplicity). We will see that the rule

$$P_1 + P_2 + P_3 = 0$$

defines a group law.

I.3.4 Complex curves

Fact I.3.9. If X is a smooth curve defined over $K \subseteq \mathbb{C}$, then $X(\mathbb{C})$ is a compact, 1-dimensional complex manifold (i.e., a compact Riemann surface).

Fact I.3.10 (Griffiths–Harris, chapter 2). If X is defined by $\tilde{f} = 0$ (smooth), where $\deg \tilde{f} = d$, then the genus is

$$g(X) = \frac{(d-1)(d-2)}{2}.$$

Remark I.3.11. From the above, if $d = 3$, then the genus is 1. In other words, the complex points of an elliptic curve is homeomorphic to a torus $S^1 \times S^1$.

The product of two circles has a group structure:

$$S^1 \times S^1 \cong \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}.$$

If $K \subseteq \mathbb{C}$ is a subfield, then $X(K) \subseteq X(\mathbb{C})$ is a subgroup.

I.3.5 Genus trichotomy

Let X be a smooth curve defined over a number field K.

	Genus 0	Genus 1	Genus ≥ 2
Analysis	Riemann surface $X(\mathbb{C})$ isomorphic to the Riemann sphere	$X(\mathbb{C})$ isomorphic to a complex torus (with group law)	$X(\mathbb{C})$ has universal cover isomorphic to Poincaré disc
Differential geometry	$X(\mathbb{C})$ has Riemannian metric of constant positive curvature	$X(\mathbb{C})$ has flat metric induced from $\mathbb{C}$	$X(\mathbb{C})$ has Riemannian metric of constant negative curvature
Arithmetic geometry	If X has a rational point over K, then $X \cong \mathbb{P}^1$ over K (rational parametrization)	If X has a rational point over K, then $X(K)$ is a subgroup of $X(\mathbb{C})$ (Mordell, 1922: $X(K)$ finitely generated)	(Faltings) $X(K)$ is finite.

Conjecture I.3.12 (Poincaré, 1901)**.** *Given an elliptic curve $E/\mathbb{Q}$, there exist finitely many points such that the tangent-chord method yields all rational points. That is, $E(\mathbb{Q})$ is a finitely generated group.*

I.3.6 Next time

Hasse Principle failing for elliptic curves:

$$3x^3 + 4y^3 + 5z^3 = 0.$$

Why are they called elliptic curves?

I.4 2013-09-11

I.4.1 Hasse Principle

Theorem I.4.1 (Hasse Principle for genus 0 curves)**.** *Suppose $\tilde{f} \in \mathbb{Z}[x, y, z]$ is a homogeneous polynomial defining a curve of genus 0. If*

$$\tilde{f}(x, y, z) \equiv 0 \pmod{p^m}$$

has a solution for all primes p and all $m \geq 1$, and has a real solution, then

$$\tilde{f}(x, y, z) = 0$$

has a solution in $\mathbb{P}^2(\mathbb{Q})$.

Remark I.4.2. This is *not* true for general curves. Lind (1940) and Reichardt (1942) independently came up with a counterexample:

$$x^4 - 17 = 2y^2.$$

Selmer (1951, 1954) came up with another counterexample:

$$3x^3 + 4y^3 + 5z^3 = 0.$$

I.4.2 Elliptic integrals

Consider an integral of the form

$$\int R(x, y)\, dx,$$

where R is a rational function and x, y are related by a curve of genus 0.

Example I.4.3. Setting $y^2 = 1 - x^2$, we have

$$\int_0^x \frac{dx}{\sqrt{1 - x^2}} = \int_0^x \frac{dx}{y}.$$

This has a rational parametrization:

$$x = \frac{2t}{1 + t^2}, \qquad y = \frac{1 - t^2}{1 + t^2}.$$

We have

$$\frac{dx}{dt} = \frac{2(1+t^2) - 2t \cdot 2t}{(1+t^2)^2} = \frac{2-2t^2}{(1+t^2)^2}.$$

Hence we obtain

$$\int_0^x \frac{dx}{y} = \int_0^T \frac{(1+t^2)(2-2t^2)}{(1-t^2)(1+t^2)^2} = \int_0^T \frac{2}{1+t^2}\,dt = 2\tan^{-1}(T) + C.$$

What about

$$\int R(x,y)\,dx,$$

where x and y are related by a genus 1 curve?

Example I.4.4. Consider an *elliptic integral of the second kind* $(0 < k < 1)$:

$$E(k) = \int_0^1 \sqrt{(1-x^2)\,(1-k^2x^2)}\,dx.$$

The name comes from the fact that the arc length of the ellipse $(0 < b < a)$

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

is

$$4a \cdot E\left(\sqrt{1 - \left(\tfrac{b}{a}\right)^2}\right).$$

We can put

$$y^2 = \left(1-x^2\right)\left(1-k^2x^2\right)$$

in the form

$$Y^2 = X(X-1)(X-\lambda)$$

for a suitable change of variables

$$X = \frac{ax+b}{cx+d},$$
$$Y = \frac{ey}{(cx+d)^2},$$

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible and $e \neq 0$. Expanding this out, we get

$$\frac{e^2y^2}{(cx+d)^4} = \left(\frac{ax+b}{cx+d}\right)\left(\frac{(a-c)x+(b-d)}{cx+d}\right)\left(\frac{(a-\lambda c)x+(b-\lambda d)}{cx+d}\right)$$
$$\implies e^2y^2 = (cx+d)(ax+b)\big((a-c)x+(b-d)\big)\big((a-\lambda c)x+(b-\lambda d)\big),$$

from which we can find the right values of a, b, c, d, e.

I.4.3 Branch cuts

Viewing this in terms of branch cuts: For

$$\int \frac{dx}{\sqrt{1-x^2}},$$

we have two branches and poles at $x = 1, -1$, so we can "slit" two copies of the Riemann sphere from 1 to -1, then glue them together to get another sphere (a complex curve of genus 0).

With

$$\int \frac{dx}{\sqrt{x(x-1)(x-\lambda)}},$$

we instead slit from 1 to -1 and from λ to ∞ on both spheres, whence gluing along *both* slits yields a torus (a complex curve of genus 1).

Remark I.4.5 (Periods). Let $\omega = dx/y$, and take

$$\omega_1 = \int_\alpha \omega,$$
$$\omega_2 = \int_\beta \omega,$$

which are linearly independent over $\mathbb{R}$. So

$$\Lambda := \left\{ m\omega_1 + n\omega_2 \;\middle|\; m, n \in \mathbb{Z} \right\} \subseteq \mathbb{C}$$

is a lattice.

We can show

$$E(\mathbb{C}) \to C/\Lambda$$
$$p \mapsto \int_0^p \omega \pmod{\Lambda}$$

is a well-defined complex analytic isomorphism (Abel–Jacobi).

I.4.4 Standard forms of elliptic curves

Question: How do we get a "nice" equation for an elliptic curve?

What is a nice form?

Weierstrass form:

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

If $\operatorname{char} K \neq 2$, then we can complete the square on the LHS to obtain

$$\left(y + \frac{a_1x + a_3}{2}\right)^2 = \text{cubic in } x,$$

which becomes $y^2 = f(x)$ after change of variables.

If $\operatorname{char} K \neq 3$, then we can complete the cube on the right:

$$y^2 = x^3 + ax + b.$$

Another nice form is *Deuring form*: if $\operatorname{char} K \neq 3$, we can write

$$y^2 + \alpha xy + y = x^3.$$

Remark I.4.6 (Idea of going from general smooth cubic to the Weierstrass form). Take a flex point (point of inflection), move it to $(0 : 1 : 0)$, and make the tangent $z = 0$.

Example I.4.7. The Fermat cubic ($\operatorname{char} K = 0$)

$$x^3 + y^3 = 1$$

has a flex point at $P = (1 : 0 : 1)$. The change of coordinates

$$\begin{aligned} x_2 &= x - z \\ x_1 &= x \\ x_0 &= y \end{aligned}$$

sends P to $(0 : 1 : 0)$, and the tangent at the flex point is $x = z$, i.e., $x_2 = 0$. The resulting equation is

$$x_0^3 = -3x_1^2x_2 + 3x_1x_2^2 - x_2^3,$$

which in the affine plane $x_2 = 1$ is

$$x_0^3 = -3x_1^2 + 3x_1 - 1.$$

Now we get

$$\begin{aligned} x_0^3 = -3x_1^2 + 3x_1 - 1 &= -3\left(x_1 - \frac{1}{2}\right)^2 - \frac{1}{4} \\ \left(x_1 - \frac{1}{2}\right)^2 &= -\frac{1}{3}x_0^3 - \frac{1}{12} \\ y^2 &= -\frac{1}{3}x_0^3 - \frac{1}{12} \\ &\vdots \\ &= x_3 - 432. \end{aligned}$$

I.5 2013-09-13

I.5.1 Converting to Weierstrass form

Take a general cubic and put it in Weierstrass form:

$$\begin{aligned} F(x, y, z) = c_{03}y^3 + c_{12}xy^2 + c_{21}x^2y + c_{30}x^3 + c_{02}y^2z \\ + c_{11}xyz + c_{20}x^2z + c_{01}yz^2 + c_{10}xz^2 + c_{00}z^3 = 0. \end{aligned}$$

Want:

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

Impose conditions (remarks before proof):

(1) Make the curve pass through $(0:1:0)$, i.e., $c_{03} = 0$.

(2) Make $(0:1:0)$ a nonsingular point. Do this as always: Let

$$\phi = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Then ϕ maps $(0:1:0)$ to $(0:0:1)$, and

$$f(x,y) = F\big(\phi^{-1}(x,y,1)\big) = F(y,1,x) = \underbrace{(c_{02}x + c_{12}y)}_{f_1} + \underbrace{\big(c_{01}x^2 + c_{11}xy + c_{21}y^2\big)}_{f_2} + \text{cubic terms}$$

with $f_1 \neq 0$, so c_{02}, c_{12} are not both zero.

(3) Want the tangent line at $(0:1:0)$ to be $z = 0$. So $x = 0$ in the new affine coordinates, hence $c_{12} = 0$ (and $c_{02} \neq 0$).

(4) Make $(0:1:0)$ a flex (point of inflection) $\iff$ f_1 divides f_2.

$$\begin{vmatrix} \frac{\partial^2 F}{\partial x^2} & \frac{\partial^2 F}{\partial x \partial y} & \cdots \\ \vdots & \ddots & \\ & & \frac{\partial^2 F}{\partial z^2} \end{vmatrix} = 0$$

We have $f_1 = c_{02}x$, so $f_1 \mid f_2 \iff c_{21} = 0$.

Then

$$F(x,y,z) = c_{30}x^3 + c_{02}y^2z + c_{11}xyz + c_{20}x^2z + c_{01}yz^2 + c_{10}xz^2 + c_{00}z^3 = 0.$$

Remark I.5.1. There is an alternate approach of proving this using Riemann–Roch.

Theorem I.5.2. *If $X : F(x,y,z) = 0$ is a homogeneous smooth cubic over K such that X has a K-rational flex, then there exists a projective transformation Φ defined over K such that $F(\Phi^{-1}(x,y,z))$ is in Weierstrass form.*

Proof. Choose ϕ to map the flex point to $(0:1:0)$. Use ψ such that

$$\psi^{-1} = \begin{pmatrix} a & 0 & b \\ 0 & 1 & 0 \\ c & 0 & d \end{pmatrix}, \qquad ad - bc \neq 0$$

to make the tangent at $(0:1:0)$ be $z = 0$.

By conditions (1) to (4) above, we have a projective transformation θ such that

$$F^\theta(x,y,z) = c_{30}x^3 + c_{02}y^2z + c_{11}xyz + c_{20}x^2z + c_{01}yz^2 + c_{10}xz^2 + c_{00}z^3.$$

Let

$$\chi^{-1} = \begin{pmatrix} t & 0 & 0 \\ 0 & t & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then

$$\left(F^\theta\right)^\chi(x,y,z) = F^\theta(tx,ty,z) = c_{30}t^3x^3 + c_{02}t^2y^2z + \dots.$$

Set $t = c_{02}/c_{30}$. □

Example I.5.3. The point $P = (0:1:1)$ is a flex point of $x^3 + y^3 = z^3$. Take

$$\Phi = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix},$$

so that

$$\Phi \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ z \\ y - z \end{pmatrix} =: \begin{pmatrix} a \\ b \\ c \end{pmatrix}.$$

Then Φ sends $(0:1:1)$ to $(0:1:0)$, and the tangent line at P is $y = z$, which is mapped to $c = 0$. Note that

$$\Phi^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

So if $x = a,\ y = b + c,\ z = b$, then

$$x^3 + y^3 = z^3 \implies a^3 + (b+c)^3 = b^3,$$

and we get

$$a^3 + 3b^2c + 3bc^2 + c^3 = 0,$$

which is in Weierstrass form. In affine coordinates, $c = 1$, so

$$a^3 + 3b^2 + 3b + 1 = 0 \implies 3b^2 + 3b = -a^3 - 1.$$

If we set $b = -3Y$ and $a = -3X$, then

$$2yY^2 - 9Y = 27X^3 - 1$$
$$Y^2 - \frac{1}{3}Y = X^3 - \frac{1}{27}.$$

Taking $Y = y/u^3$ and $X = x/u^2$ (coefficients of y^2 and x^3 still match), for $u = 3$, we get

$$\frac{y^2}{3^6} - \frac{1}{3}\frac{y}{3^3} = \frac{x^3}{3^6} - \frac{1}{3^3}$$
$$y^2 - 9y = x^3 - 27,$$

and completing the square yields

$$y^2 = x^3 - 432.$$

I.5.2 A classical example

Fermat showed by infinite descent that $u^4 + v^4 = w^2$ has no nontrivial ($uvw \neq 0$) integer solutions.

By change of variables

$$Y' = \frac{w}{v^2}, \qquad X' = \frac{u}{v},$$

we obtain

$$(Y')^2 = (X')^4 + 1.$$

Writing $X' = x$ and $Y' = y + x^2$, we get

$$\left(y + x^2\right)^2 = x^4 + 1 \implies y^2 + 2x^2y = 1,$$

which is a smooth cubic. Projectivizing yields

$$y^2z + 2x^2y = z^3,$$

an elliptic curve with a flex at $(1 : 0 : 0)$. The tangent line at the flex is $y = 0$. The transform

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

sends $(1 : 0 : 0)$ to $(0 : 1 : 0)$ and $y = 0$ to $x = 0$. Next apply

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

which fixes $(0 : 1 : 0)$ and sends $x = 0$ to $z = 0$. The composition of these is

$$\Phi = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Setting

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \Phi \begin{pmatrix} x \\ y \\ z \end{pmatrix},$$

we have

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \Phi^{-1} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} b \\ c \\ a \end{pmatrix}.$$

I.6 2013-09-16

I.6.1 Correction

Consider

$$F^\theta(tx, ty, z) = c_{30}t^3x^3 + c_{02}t^2y^2z + \dots.$$

Set $t = -\frac{c_{02}}{c_{30}}$ (coefficients equal but on opposite sides of the equation).

I.6.2 Hessian and flex points

Consider a smooth cubic $F(x, y, z) = 0$. The *Hessian* is the cubic

$$H = \begin{vmatrix} \frac{\partial^2 F}{\partial x^2} & \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial x \partial z} \\ \vdots & \vdots & \vdots \\ & & \frac{\partial^2 F}{\partial z^2} \end{vmatrix}.$$

The flex points are given by $\{F = 0\} \cap \{H = 0\}$. (Bezout: ≤ 9 points.)

Try

$$F(x, y, z) = ax^3 + by^3 + cz^3.$$

Then

$$H = \begin{vmatrix} 6ax & 0 & 0 \\ 0 & 6by & 0 \\ 0 & 0 & 6cz \end{vmatrix} = (216abc)xyz.$$

Say $\operatorname{char} K = 0$. Then

$$\{\text{flex points}\} = \left\{ax^3 + by^3 + cz^3 = 0\right\} \cap \{xyz = 0\}.$$

Suppose $-c = a + b$, e.g.,

$$x^3 + 2y^3 - 3z^3 = 0. \tag{$*$}$$

This has a point. But, if $\frac{a}{b}, \frac{a}{c}, \frac{b}{c}$ are not cubes in K, then there are no flex points defined over K. For example, take $K = \mathbb{Q}$ in $(*)$.

Proposition I.6.1. *Suppose C is a smooth plane cubic curve over K, and $\mathbf{0} \in C(K)$ is a flex point. Then there is a unique group law on $C(K)$ such that $P + Q + R = \mathbf{0}$ whenever P, Q, R are collinear points lying in $C(K)$, and $\mathbf{0}$ is the identity.*

I.6.3 Example from last time, continued

Consider $u^4 + v^4 = w^2$. By some changes of variables described in §I.5.2, the equation becomes

$$c^2a + 2cb^2 = a^3.$$

The affine points at $c = 1$ are $a + 2b^3 = a^3$, so

$$2b^2 = a^3 - a,$$

and taking $b \mapsto 2y,\ a \mapsto 2x$ yields

$$8y^2 = 8x^3 - 2x$$
$$y^2 = x^3 - \frac{1}{4}x.$$

Now we apply (setting $u = 2$)

$$y \mapsto \frac{y}{u^3} = \frac{y}{8}$$
$$x \mapsto \frac{x}{u^2} = \frac{x}{4},$$

so we get

$$\frac{y^2}{64} = \frac{x^3}{64} - \frac{x}{16},$$

which finally gives us the integer Weierstrass form

$$y^2 = x^3 - 4x.$$

I.6.4 Congruent integers

Observe:

$$\left(\frac{3}{2}\right)^2 + \left(\frac{20}{3}\right)^2 = \left(\frac{41}{6}\right)^2,$$

so 5 is congruent! (Fibonacci, 1225)

Recall:

Definition I.6.2. A positive integer n is *congruent* if it is the area of a right triangle with rational sides.

Example I.6.3. 5 and 6 are congruent.

Proposition I.6.4. *If n is a squarefree positive integer, then the following are equivalent:*

(1) n is congruent.

(2) There are three rational squares in arithmetic progression with common difference n.

Proof. Suppose n is congruent. Let $n = \frac{1}{2}ab$ with $a^2 + b^2 = c^2$ $(a, b, c \in \mathbb{Q}_{>0})$. Let $x = \frac{c^2}{4}$. Then

$$x + n = \frac{a^2 + b^2}{4} + \frac{1}{2}ab = \left(\frac{a+b}{2}\right)^2,$$
$$x - n = \frac{a^2 + b^2}{4} - \frac{ab}{2} = \left(\frac{a-b}{2}\right)^2,$$

so $x - n, x, x + n$ is the arithmetic progression.

Conversely, given $x \in \mathbb{Q}$ such that $x, x \pm n$ are all squares, let

$$a = \sqrt{x+n} + \sqrt{x-n},$$
$$b = \sqrt{x+n} - \sqrt{x-n}.$$

Check: $\frac{1}{2}ab = n$, and

$$a^2 + b^2 = 4x,$$

which is a square. □

Proposition I.6.5. *A positive integer n is congruent $\iff$ there exists a $\mathbb{Q}$-rational point on the elliptic curve $y^2 = x^3 - n^2x$ other than the trivial points $\infty, (0,0), (n,0), (-n,0)$.*

Proof. Given three rational squares $x, x \pm n$,

$$x(x+n)(x-n) = \text{square}.$$

This is the nontrivial point. (We will prove the converse later.) □

Remark I.6.6. The fact that 2 is not congruent follows from Fermat's proof that $u^4 + v^4 = w^2$ has no nontrivial integer solutions.

I.6.5 Elliptic curves over $\mathbb{C}$

Genus zero case: X is topologically a circle $x^2 + y^2 = 1$ (S^1). Embed the circle as

$$S^1 \to \mathbb{P}^2(\mathbb{C})$$
$$\theta \mapsto \big(f(\theta) : f'(\theta) : 1\big),$$

where f must satisfy $f(\theta)^2 + f'(\theta)^2 = 1$ and be periodic with period 2π. (Example: $f(\theta) = \sin\theta$.) The image is the circle. Such functions are

$$\mathbb{C}(\cos\theta, \sin\theta) \cong \mathbb{C}(u)[v]/(u^2 + v^2 - 1) \cong \mathbb{C}(t).$$

We want to copy this for genus 1. Let Λ be a lattice in $\mathbb{C}$, i.e., a discrete subgroup of $\mathbb{C}$ containing an $\mathbb{R}$-basis. Write $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

Aim: define a embedding

$$\mathbb{C}/\Lambda \to \mathbb{P}^2(\mathbb{C})$$
$$z \mapsto \big(f(z) : f'(z) : 1\big),$$

where f must be *doubly* periodic.

Chapter II

Elliptic Curves over the Complex Numbers

II.1 2013-09-18

Remark II.1.1. Al-Karaji, 953–1029, Persian mathematician, proved 5 congruent.

II.1.1 Lattices and elliptic functions

Definition II.1.2. A *lattice* is a discrete subgroup of $\mathbb{C}$ containing an $\mathbb{R}$-basis, i.e.,

$$\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2,$$

where ω_1, ω_2 are $\mathbb{R}$-linearly independent.

Goal: to define an embedding

$$\begin{aligned} \mathbb{C}/\Lambda &\to \mathbb{P}^2(\mathbb{C}) \\ z &\mapsto \begin{cases} \big(f(z) : f'(z) : 1\big) & (z \notin \Lambda), \\ (0:1:0) & (z \in \Lambda). \end{cases} \end{aligned}$$

with image an elliptic curve.

We'll need f, f' *doubly periodic*, i.e.,

$$f(z+\omega) = f(z) \qquad \forall \omega \in \Lambda.$$

Definition II.1.3. An *elliptic function* with respect to Λ is a meromorphic function such that

$$f(z+\omega) = f(z) \qquad \forall \omega \in \Lambda,\ z \in \mathbb{C}.$$

Remark II.1.4. The set of elliptic functions forms a field $\mathbb{C}(\Lambda)$.

Definition II.1.5. The *Weierstrass $\wp$-function* for Λ is

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

The *Eisenstein series* of weight $2k$ for Λ is

$$G_{2k}(\Lambda) = \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \omega^{-2k}.$$

Remark II.1.6. This is our first example of a *modular form*.

Theorem II.1.7. *(a) G_{2k} is absolutely convergent for $k > 1$.*

(b) $\wp_\Lambda$ is absolutely convergent and uniformly convergent on every compact subset of $\mathbb{C} - \Lambda$. It defines a meromorphic function on $\mathbb{C}$ with a double pole of residue 0 at each lattice point, and no other poles.

(c) $\wp_\Lambda$ is even, i.e., $\wp_\Lambda(-z) = \wp_\Lambda(z)$.

Proof. (a) Consider the set

$$S = \left\{\omega \in \Lambda \;\middle|\; \omega \in \text{ball of radius } R \text{ with center } (0,0)\right\}.$$

Let A be the area of a fundamental domain of Λ.

Exercise II.1.8.

$$\#S = \frac{\pi R^2}{A} + \mathrm{O}(R).$$

Thus,

$$\#\left\{\omega \in \Lambda \;\middle|\; N \le |\omega| < N+1\right\} < cN$$

for some constant c. So

$$\sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} |\omega|^{-2k} = \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \frac{1}{|\omega|^{2k}} < \sum_{N=1}^{\infty} \frac{cN}{N^{2k}} = \sum_{N=1}^{\infty} \frac{c}{N^{2k-1}},$$

which converges when $k > 1$.

(b) Observe that

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

We have

$$|2\omega - z| \le 2\,|\omega| + |z| \le \frac{5}{2}\,|\omega|,$$
$$|z-\omega| \ge |\omega| - |z| > \frac{1}{2}\omega.$$

Thus, if $|\omega| > 2\,|z|$ (all but finitely many ω), then

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| \le \frac{|z|}{|\omega|^2} \cdot \frac{\frac{5}{2}\,|\omega|}{\left(\frac{1}{2}\omega\right)^2} = \frac{10\,|z|}{|\omega|^3}.$$

By part (a),

$$\sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \frac{1}{|\omega|^3}$$

converges. So $\wp_\Lambda$ converges absolutely for any $z \in \mathbb{C} - \Lambda$, and converges uniformly on compact subsets.

We will show the statement about the poles later.

(c) Since $-\Lambda = \Lambda$, this is clear. □

Theorem II.1.9. *$\wp_\Lambda$ is an elliptic function with respect to Λ.*

Proof. By uniform convergence, we can differentiate term by term:

$$\begin{aligned} \wp'(z) &= -2\sum_{\omega\in\Lambda} \frac{1}{(z-\omega)^3}, \\ \wp'(z+\omega) &= \wp'(z) \qquad \forall \omega \in \Lambda. \qquad\qquad (\Lambda = \Lambda + \omega) \end{aligned}$$

Integrating with respect to z,

$$\wp(z+\omega) = \wp(z) + C,$$

where C is a constant depending only on ω. Let $z = -\frac{\omega}{2}$. Then

$$\wp\left(\frac{\omega}{2}\right) = \wp\left(-\frac{\omega}{2}\right) + C,$$

but $\wp$ is even, so $C = 0$ and therefore $\wp$ is elliptic. □

II.1.2 Embedding elliptic curves

Consider the well-defined map

$$\begin{aligned} &\mathbb{C}/\Lambda \to \mathbb{P}^2(\mathbb{C}) \\ &\quad z \mapsto \big(\wp(z) : \wp'(z) : 1\big) && (z \notin \Lambda) \\ &\quad z \mapsto (0:1:0) && (z \in \Lambda). \end{aligned}$$

Theorem II.1.10.

$$\big(\wp'(z)\big)^2 = 4\wp(z)^3 - 60G_4(\Lambda)\wp(z) - 140G_6(\Lambda).$$

Lemma II.1.11. *The Laurent series for $\wp(z)$ about $z = 0$ is:*

$$\wp(z) = z^{-2} + \sum_{k=1}^{\infty} (2k+1)G_{2k}(\Lambda)z^{2k}.$$

Proof. Observe that

$$\begin{aligned}\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2} &= \omega^{-2}\left(\left(1-\frac{z}{\omega}\right)^{-2}-1\right)\\ &= \omega^{-2}\left[1+(-2)\left(-\frac{z}{\omega}\right)+\frac{(-2)(-3)}{1\cdot 2}\left(-\frac{z}{\omega}\right)^2+\cdots-1\right]\\ &= \omega^{-2}\left[2\frac{z}{\omega}+3\frac{z^2}{\omega^2}+\dots\right]\\ &= \sum_{m=1}^{\infty}\frac{(m+1)z^m}{\omega^{m+2}}.\end{aligned}$$

Thus,

$$\begin{aligned}\wp(z) &= z^{-2}+\sum_{m=1}^{\infty}(m+1)z^m\sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}}\frac{1}{\omega^{m+2}}\\ &= z^{-2}+\sum_{k=1}^{\infty}(2k+1)z^{2k}G_{2k+2}(\Lambda).\end{aligned}$$

□

II.2 2013-09-20

II.2.1 The Weierstrass $\wp$-function, continued

Let us prove the theorem from last time. Recall:

Theorem (II.1.10)**.**

$$\left(\wp'(z)\right)^2 = 4\wp(z)^3-g_2\wp(z)-g_3,$$

where $g_2 = 60G_4(\Lambda)$ *and* $g_3 = 140G_6(\Lambda)$.

Proof of Theorem II.1.10. We have

$$\begin{aligned}\wp(z) &= z^{-2}+3G_4z^2+5G_6z^4+\dots\\ \wp(z)^3 &= z^{-6}+9G_4z^{-2}+\dots\\ \wp'(z)^2 &= 4z^{-6}-24G_4z^{-2}+\dots\end{aligned}$$

Set

$$f(z) = \wp'(z)^2-4\wp(z)^3+60G_4\wp(z)+140G_6 = z^2+\dots$$

This is the Laurent series about $z=0$ for

$$f(z) = \left(\wp'(z)\right)^2-4\wp(z)^3+g_2\wp(z)+g_3. \tag{II.2.1.1}$$

The expansion starts with z^2 (no $z^0, z^{-2}, z^{-4}, z^{-6}$ terms). In particular, $f(z)$ is holomorphic at $z=0$, and $f(0)=0$.

Since f is elliptic, $f(z)=0$ for all $z\in\Lambda$. Since $\wp$ and $\wp'$ are holomorphic away from points of Λ, so is f. Thus, f is everywhere holomorphic.

Let D be a fundamental parallelogram. On $\overline{D}$, f is bounded. Since f is elliptic, it follows that f is bounded everywhere. By Liouville's theorem, f is constant. But $f(0)=0$, so f is identically zero, and the result follows from (II.2.1.1). □

II.2.2 Riemann surfaces

Let us make a brief aside on (connected) Riemann surfaces. A Riemann surface is a "union of patches on $\mathbb{C}$," i.e., a surface $X = \bigcup_\alpha U_\alpha$, where each U_α is homeomorphic to an open subset V_α of $\mathbb{C}$.

We additionally assume that all our Riemann surfaces are connected and Hausdorff.

Denote the homeomorphisms by

$$U_\alpha \xrightarrow{\varphi_\alpha} V_\alpha.$$

We require that the transition functions $\varphi_\alpha \circ \varphi_\beta^{-1}$ be analytic where defined.

Example II.2.1. Our main examples of Riemann surfaces:

- The complex plane $\mathbb{C}$
- The Riemann sphere $\mathbb{C}_\infty$
- An elliptic curve $\mathbb{C}/\Lambda$
- The upper half plane $\mathscr{H}$

Morphisms between Riemann surfaces have corresponding maps between domains in $\mathbb{C}$, analytic where defined. These are called *analytic maps*.

Fact II.2.2 (Open mapping theorem). Suppose $f : R \to S$ is a nonconstant analytic map between connected Riemann surfaces. Then f is open.

Corollary II.2.3. *If R is compact, and $f : R \to S$ is a nonconstant analytic map, then $f(R) = S$ (and S is compact).*

Proof. By the open mapping theorem, $f(R)$ is open in S. Moreover, $f(R)$ is compact and S is Hausdorff, so $f(R)$ is closed. Since S is connected, it follows that $f(R) = S$. □

Corollary II.2.4 (Liouville's theorem)**.** *There is no nonconstant analytic map $f : \mathbb{C}_\infty \to \mathbb{C}$.*

Theorem II.2.5 (Degree of an analytic map)**.** *Suppose $f : R \to S$ is a nonconstant analytic map and R is compact. Then there is an integer $k \geq 1$ such that for all $w \in S$, there are exactly k solutions to $f(z) = w$ (counted with multiplicity), i.e., f is a k-to-1 map from $R \to S$. We write $deg(f) := k$.*

Proof. Let

$$S_q = \left\{ w \in S \;\middle|\; f^{-1}(w) \text{ has } q \text{ preimages counting multiplicity} \right\}.$$

(Note: $|f^{-1}(w)| < \infty$, since $f^{-1}(w)$ is discrete and R is compact.) Exercise: Show S_q is open.

Note that if $p \neq q$, then $S_p \cap S_q = \varnothing$. Since f is surjective,

$$S = S_1 \cup S_2 \cup S_3 \cup \dots$$

is an open cover. By compactness of S, there is a finite open subcover

$$S = S_1 \cup \dots \cup S_n.$$

But S is connected, so $S = S_k$ for some k. □

Example II.2.6. Let us find the degree of the Weierstrass $\wp$-function

$$\mathbb{C}/\Lambda \xrightarrow{\wp_\Lambda} \mathbb{C}_\infty.$$

We showed that $\wp_\Lambda$ has a double pole at any point in Λ, and no other poles. So $\wp_\Lambda$ is a 2-to-1 map.

Likewise, by looking at preimages at infinity, $\wp'_\Lambda : \mathbb{C}/\Lambda \to \mathbb{C}_\infty$ is a 3-to-1 map.

II.2.3 Missing facts about our map

We're still missing some facts about the map

$$\begin{aligned} \mathbb{C}/\Lambda &\to \mathbb{P}^2(\mathbb{C}) \\ z &\mapsto \big(\wp(z) : \wp'(z) : 1\big). \end{aligned}$$

In particular:

(1) $4x^3 - g_2x - g_3$ has distinct roots.

(2) $\mathbb{C}/\Lambda \to E(\mathbb{C})$ is surjective.

(3) $\mathbb{C}/\Lambda \to E(\mathbb{C})$ is injective.

(4) $\mathbb{C}/\Lambda \to E(\mathbb{C})$ is an analytic isomorphism.

Let's show these.

(1) $4x^3 - g_2x - g_3 = 4(x-e_1)(x-e_2)(x-e_3)$, i.e.,

$$\wp'(z)^2 = 4\big(\wp(z) - e_1\big)\big(\wp(z) - e_2\big)\big(\wp(z) - e_3\big).$$

Claim II.2.7. *$e_i = \wp\left(\frac{\omega_i}{2}\right)$, where $\omega_3 = \omega_1 + \omega_2$.*

Proof. Observe that

$$\begin{aligned} \wp'\left(\frac{\omega_i}{2}\right) &= -\wp'\left(-\frac{\omega_i}{2}\right) && \text{since } \wp' \text{ is odd} \\ &= -\wp'\left(\omega_i - \frac{\omega_i}{2}\right) && \text{since } \wp' \text{ is elliptic} \\ &= -\wp'\left(\frac{\omega_i}{2}\right). \end{aligned}$$

Thus $\wp'\left(\frac{\omega_i}{2}\right) = 0$. □

Are the ω_i distinct? The equation $\wp(z) = u$ has two solutions (up to multiplicity). Let

$$f(z) = \wp(z) - \wp\left(\frac{\omega_i}{2}\right).$$

This has a double zero at $\frac{\omega_i}{2}$, and since $f'(z) = \wp'(z)$,

$$f'\left(\frac{\omega_i}{2}\right) = \wp'\left(\frac{\omega_i}{2}\right) = 0.$$

Now if $\wp\left(\frac{\omega_j}{2}\right) = \wp\left(\frac{\omega_i}{2}\right)$ with $j \neq i$, then we get a contradiction, since $\frac{\omega_j}{2}$ is *another* zero of f. □

(2) The point $(0:1:0)$ is hit. Pick $(a:b:1)$ on $y^2 = 4x^3 - g_2x - g_3$. We want z such that

$$\wp(z) = a, \qquad \wp'(z) = b.$$

Say $\wp(z_0) = a$. Then

$$\wp'(z_0)^2 = 4\wp(z_0)^3 - g_2\wp(z_0) - g_3 = 4a^3 - g_2a - g_3 = b^2,$$

so $\wp'(z_0) = \pm b$. If it is b, then we are done. If $\wp'(z_0) = -b$, then

$$\wp(-z_0) = a, \qquad \wp'(-z_0) = b,$$

proving surjectivity. □

II.3 2013-09-23

II.3.1 Embedding elliptic curves, continued

Consider

$$\begin{aligned} \varphi : \mathbb{C}/\Lambda &\to \mathbb{P}^2(\mathbb{C}) \\ z &\mapsto \big(\wp(z) : \wp'(z) : 1\big). \end{aligned}$$

Last time we showed that $4x^3 - g_2x - g_3$ has distinct roots, and that φ is surjective.

(3) φ is injective: Suppose $\wp(z_1) = \wp(z_2)$ and $\wp'(z_1) = \wp'(z_2)$. Then, up to Λ,

$$z_1 = \pm z_2$$

since $\wp$ is 2-to-1 and even. If $z_1 = -z_2$, then

$$\wp'(z_1) = \wp'(-z_2) = -\wp'(z_2).$$

So $\wp'(z_1) = 0$, whence $z_1 = \frac{\omega_i}{2}$ (up to Λ, for some $i \in \{1,2,3\}$). But then $-z_1 = z_1$ (up to Λ), so $z_1 = z_2$. □

(4) φ is an analytic isomorphism: In a neighborhood of a lattice point,

$$\big(\wp(z) : \wp'(z) : 1\big) = \left(\frac{\wp(z)}{\wp'(z)} : 1 : \frac{1}{\wp'(z)}\right) \to (0:1:0)$$

since $\wp$ is a double pole and $\wp'$ is a triple pole at lattice points.

Conversely, starting with an elliptic curve

$$y^2 = 4x^3 - g_2x - g_3 \qquad (g_2, g_3 \in \mathbb{C}),$$

can we find a lattice Λ such that

$$\begin{aligned} g_2 &= 60G_4(\Lambda), \\ g_3 &= 140G_6(\Lambda)? \end{aligned}$$

Yes, but we need some modular function theory.

II.3.2 Examples

Let us first consider some examples.

Example II.3.1. Say $\Lambda = \mathbb{Z}[i]$. Then $g_3(\Lambda) = 0$ and $g_3(\Lambda) \in \mathbb{R}^\times$.

Proof. We have

$$G_6(\Lambda) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{\omega^6}.$$

Consider the automorphism $\varphi(\omega) = i\omega$ of Λ:

$$\varphi(G_6) = G_6,$$

and

$$\varphi(\omega^6) = i^6\omega^6 = -\omega^6 \implies \varphi(G_6) = -G_6,$$

whence $G_6 = 0$, and so $g_3 = 0$. Then $g_2 \neq 0$ (else we have a cusp). Hence

$$G_4(\Lambda) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{\omega^4},$$

and if σ is complex conjugation (an automorphism of Λ), then

$$\sigma(G_4) = G_4,$$

so $G_4 \in \mathbb{R}$, thus $g_2 \in \mathbb{R}$. □

Example II.3.2. Say $\Lambda = \mathbb{Z}\left[\frac{1}{2}(-1 + \sqrt{-3})\right]$. Play the same game: $g_2(\Lambda) = 0$ and $g_3(\Lambda) \in \mathbb{R}^\times$. Get

$$y^2 = 4x^3 - g_3.$$

Example II.3.3. If $c \in \mathbb{C}^\times$, let $c\Lambda = \{c\omega \mid \omega \in \Lambda\}$. Show that

$$g_2(c\Lambda) = c^{-4}g_2(\Lambda),$$
$$g_3(c\Lambda) = c^{-6}g_3(\Lambda).$$

Then we can prove that every elliptic curve with $g_2 = 0$ (resp. $g_3 = 0$) is of the form $\mathbb{C}/\Lambda$ with $\Lambda = c\mathbb{Z}\left[\frac{1}{2}(-1 + \sqrt{-3})\right]$ (resp. $c\mathbb{Z}[i]$).

Proof. Suppose the curve is $y^2 = 4x^3 - ax$ with $a \neq 0$. Say

$$g_2(\mathbb{Z}[i]) = t \neq 0.$$

Then

$$g_2(c\mathbb{Z}[i]) = c^{-4}t.$$

Solve $c^{-4}t = a$ for c. (Note: $g_3(c\mathbb{Z}[i]) = 0$ as desired.) □

Remark II.3.4. In particular, $y^2 = x^3 - x$ and $x^3 + y^3 = 1$ are produced (up to isomorphism) by the above method.

II.3.3 The j-invariant

To an elliptic curve

$$y^2 = 4x^3 - g_2 x - g_3,$$

associate the *j-invariant*

$$j = \frac{1728 g_2^3}{g_2^3 - 27 g_3^2}.$$

(This is the discriminant of the cubic.)

We'll see that, if E, E' are isomorphic elliptic curves, then $j(E) = j(E')$.

II.3.4 Aside: Uniformization of Riemann surfaces

Let R be a (Hausdorff, connected) Riemann surface. There exists a universal cover

$$\tilde{R} \twoheadrightarrow R.$$

There are, up to isomorphism, only three universal covers: $\mathbb{C}$, $\mathbb{C}_\infty$, and the open unit disc Δ.

(1) $\mathbb{C} \twoheadrightarrow \mathbb{C}/\Lambda$ covers tori.

(2) $\mathbb{C}_\infty$ has no proper quotient.

(3) $\Delta \twoheadrightarrow$ lots. (A "generic" Riemann surface has universal cover Δ.)

The unit disc Δ is conformally equivalent to

$$\mathscr{H} = \left\{ z \in \mathbb{C} \;\middle|\; \operatorname{Im} z > 0 \right\}.$$

Let $\Lambda \leq \mathrm{SL}_2(\mathbb{R})$ be a subgroup. Consider the action

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az + b}{cz + d}$$

of Λ on H. We can study H/Λ (*Shimura*, or *modular curves*). Consider the case of $\Lambda = \mathrm{SL}_2(\mathbb{Z})$.

II.3.5 Some modular function theory

Theorem II.3.5. *Given $a, b \in \mathbb{C}$ and an elliptic curve*

$$E : y^2 = 4x^3 - ax - b,$$

there exists a lattice Λ such that $g_2(\Lambda) = a$ and $g_3(\Lambda) = b$.

Proof. Define

$$j(E) = \frac{1728a^3}{a^3 - 27b^2}.$$

If Λ is a lattice, define

$$j_\Lambda = j(E_\Lambda) = \frac{1728g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2}.$$

We saw

$$g_2(c\Lambda) = c^{-4}g_2(\Lambda),$$
$$g_3(c\Lambda) = c^{-6}g_3(\Lambda),$$

so $j_{c\Lambda} = j_\Lambda$.

If $z \in \mathscr{H}$, consider the lattice

$$\Lambda := \langle 1, z\rangle = \left\{m + nz \;\middle|\; m, n \in \mathbb{Z}\right\}.$$

Define $j(z) := j_\Lambda$.

Note: if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, then $\Lambda = \langle az + b, cz + d\rangle$. Thus,

$$j\left(\frac{az+b}{cz+d}\right) = j(z).$$

So j is invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane $\mathscr{H}$.

We now have a map

$$H/\mathrm{SL}_2(\mathbb{Z}) \xrightarrow{j} \mathbb{C}.$$

[Later: give $H/\mathrm{SL}_2(\mathbb{Z})$ the structure of a Riemann surface such that j is an analytic map, and such that $H/\mathrm{SL}_2(\mathbb{Z})$ has a 1-point compactification and j extends to

$$\widehat{H/\mathrm{SL}_2(\mathbb{Z})} \xrightarrow{j} \mathbb{C},$$

an analytic map.]

The image of the extended j is $\mathbb{C}_\infty$. So there exists $z \in H$ such that

$$j(z) = \frac{1728a^3}{a^3 - 27b^2}.$$

Let $\Lambda = \langle 1, z\rangle$. Pick c such that

$$a = c^{-4}g_2(\Lambda).$$

Plugging in $j(E) = j_\Lambda$, we get

$$b^2 = c^{-12}g_3(\Lambda)^2,$$

so $b = \pm c^{-6}g_3(\Lambda)$. If $b = c^{-6}g_3(\Lambda)$, we're done. If $b = -c^{-6}g_3(\Lambda)$, replace c by ci; this does not change a, but replaces b by $-b$. Then

$$a = c^{-4}g_2(\Lambda) = g_2(c\Lambda),$$
$$b = c^{-6}g_3(\Lambda) = g_3(c\Lambda).$$

□

II.4 2013-09-25

Note II.4.1. The galoisrepresentations blog has a link to a video game based on $H/\operatorname{SL}_2(\mathbb{Z})$.[1]

Last time:

$$\begin{array}{ccc} H/\operatorname{SL}_2(\mathbb{Z}) & \xrightarrow{j} & \mathbb{C} \\ \cap\mathrel{|} & & \downarrow \\ \widehat{H/\operatorname{SL}_2(\mathbb{Z})} & \xrightarrow{j} & \mathbb{C}_\infty \end{array}$$

II.4.1 Elliptic functions

Theorem II.4.2. *The field of elliptic functions with respect to Λ is given by*

$$\mathbb{C}(\wp, \wp') = \mathbb{C}(\wp)\left[\sqrt{4\wp^3 - g_2\wp - g_3}\right]$$

Let f be elliptic w.r.t. Λ. Then, splitting into even and odd components,

$$f(z) = \left(\frac{f(z) + f(-z)}{2}\right) + \wp'(z)\left(\frac{f(z) - f(-z)}{2\wp'(z)}\right).$$

So it's enough to prove that, if f is even and elliptic, then $f \in \mathbb{C}(\wp)$.

Idea: Come up with

$$g(z) = \prod_w \big(\wp(z) - \wp(w)\big)^{n_w}$$

having the same zeros and poles as $f(z)$. Then $\frac{f(z)}{g(z)}$ is elliptic, no zeros and poles, so bounded in the fundamental parallelogram, so bounded everywhere. By Liouville, it's constant, so $f(z) = kg(z) \in \mathbb{C}(\wp)$.

The equation $\wp(z) - \wp(w) = 0$ has two solutions (since $\wp$ is 2-to-1), which we can write $w, -w \pmod{\Lambda}$ (also true if $w = -w$, since $\wp'\left(\frac{\omega_i}{2}\right) = 0$).

If $w \neq -w$, set $n_w = v_f(w)$, the order of vanishing of f at w. Note that $v_f(w) = v_f(-w)$ since f is even and elliptic (take product over half the w's).

What about if $w = -w$? $(w = \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_3}{2}, 0)$

Claim II.4.3. *If $2w \in \Lambda$, then $v_f(w)$ is even (set $n_w = \frac{1}{2}v_f(w)$).*

Proof. To show this, differentiate $f(z) = f(-z)$ repeatedly:

$$f^{(i)}(z) = (-1)^i f^{(i)}(-z).$$

So

$$f^{(i)}(w) = (-1)^i f^{(i)}(-w) = (-1)^i f^{(i)}(w).$$

If i is odd, then $f^{(i)}(w) = 0$. Hence, $v_f(w) =$ smallest i such that $f^{(i)}(w) \neq 0$. So $v_f(w)$ is even. □

[1] `https://galoisrepresentations.wordpress.com/2013/09/24/life-on-the-modular-curve/`

Since $\mathbb{C}/\Lambda \xrightarrow{\wp} \mathbb{C}_\infty$ is 2-to-1 and $\mathbb{C}/\Lambda \xrightarrow{\wp'} \mathbb{C}_\infty$ is 3-to-1,

$$[\mathbb{C}(\Lambda) : \mathbb{C}(\wp)] = 2,$$
$$[\mathbb{C}(\Lambda) : \mathbb{C}(\wp')] = 3.$$

Since $(2, 3) = 1$,

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp').$$

This completes the proof of Theorem II.4.2. □

II.4.2 Aside: Big picture

Three perspectives:

(1) Analysis: compact Riemann surfaces, e.g., $\mathbb{C}/\Lambda$.

(2) Algebra: algebraic function fields of 1 variable, e.g.,

$$\mathbb{C}(\wp)\left[\sqrt{4\wp^3 - g_2\wp - g_3}\right].$$

(3) Geometry: smooth irreducible projective curves, e.g.,

$$y^2 = 4x^3 - g_2x - g_3.$$

II.4.3 The addition law

We have a map

$$\begin{aligned} \mathbb{C}/\Lambda &\xrightarrow{\phi} E_\Lambda(\mathbb{C}) \\ z &\mapsto \big(\wp(z) : \wp'(z) : 1\big). \end{aligned}$$

Theorem II.4.4. *The following are equivalent:*

(1) $z_1 + z_2 + z_3 \equiv 0 \pmod{\Lambda}$

(2) $\phi(z_1), \phi(z_2), \phi(z_3)$ *are collinear.*

Proof

Say

$$P_1 = (x_1, y_1) = \phi(z_1),$$
$$P_2 = (x_2, y_2) = \phi(z_2).$$

Suppose $x_1 \neq x_2$. Let $y = mx + k$ be the line through P_1 and P_2. Consider

$$f(z) = \wp'(z) - m\wp(z) - k.$$

This has zeros at z_1 and z_2. Moreover, $f(z)$ is an elliptic function with a triple pole at $z = 0$ and no others.

Hence f is 3-to-1, so f has 3 zeros. Call the other zero z_3.

Claim II.4.5. *If f is elliptic w.r.t. Λ, with zeros at $a_1, \dots, a_n$ and poles at $b_1, \dots, b_n$, then*

$$\sum_{i=1}^{n} a_i - \sum_{j=1}^{n} b_j \equiv 0 \pmod{\Lambda}.$$

Proof of claim. Consider the function

$$\frac{zf'(z)}{f(z)},$$

which has poles at both poles and zeros of f [e.g., if $f(z) = (z-a_1)\dots(z-a_n)$, then

$$\frac{f'(z)}{f(z)} = \frac{1}{z-a_1} + \dots + \frac{1}{z-a_n},$$

which has the desired property]. The residue term of the Laurent expansion of this near $z = a$ is

$$\frac{av_f(a)}{z-a}.$$

Letting Δ be the fundamental domain with vertices $\alpha, \alpha+\omega_1, \alpha+\omega_2, \alpha+\omega_1+\omega_2$, Cauchy's residue theorem yields

$$\frac{1}{2\pi i}\oint_{\partial\Delta} \frac{zf'(z)}{f(z)}\,dz = \sum_{i=1}^{n} a_i - \sum_{j=1}^{n} b_j.$$

Computing this integral,

$$\begin{aligned}
&\frac{1}{2\pi i}\left[\int_{\alpha}^{\alpha+\omega_1} \frac{zf'(z)}{f(z)}\,dz - \int_{\alpha+\omega_2}^{\alpha+\omega_1+\omega_2} \frac{zf'(z)}{f(z)}\,dz\right] \\
&= \frac{1}{2\pi i}\left[\int_{\alpha}^{\alpha+\omega_1} \frac{zf'(z)}{f(z)}\,dz - \int_{\alpha}^{\alpha+\omega_1} \frac{(z+\omega_2)f'(z)}{f(z)}\,dz\right] \\
&= \frac{-\omega_2}{2\pi i}\int_{\alpha}^{\alpha+\omega_1} \frac{f'(z)}{f(z)}\,dz && w = f(z) \\
&= -\omega_2 \underbrace{\frac{1}{2\pi i}\int_{\text{loop}} \frac{dw}{w}}_{\text{integer}} \in \Lambda. && dw = f'(z)\,dz
\end{aligned}$$

So, performing a similar computation for the other edges,

$$\frac{1}{2\pi i}\oint_{\partial\Delta} \frac{zf'(z)}{f(z)}\,dz \in \Lambda. \qquad \square$$

Continuing with the proof of the theorem, recall that

$$f(z) = \wp'(z) - m\wp(z) - k,$$

f has zeros at z_1, z_2, z_3, and f has poles at $0, 0, 0 \pmod{\Lambda}$. So

$$z_1 + z_2 + z_3 - 0 - 0 - 0 \equiv 0 \pmod{\Lambda}.$$

Conversely, suppose $z_1 + z_2 + z_3 \equiv 0 \pmod{\Lambda}$, but $\phi(z_1), \phi(z_2), \phi(z_4)$ are collinear. Then

$$z_1 + z_2 + z_4 \equiv 0 \pmod{\Lambda},$$

whence $z_3 \equiv z_4 \pmod{\Lambda}$, so $\phi(z_4) = \phi(z_3)$.

We will finish with the case $x_1 = x_2$ next time. $\square$

II.5 2013-09-27

II.5.1 Remarks

Note:

(1) $v_a(f)$ should should be used rather than $v_f(a)$ (it's a valuation).

(2) In the proof that $\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp')$, note that the poles are handled the same as the zeros.

As for the behavior at 0, multiply $g(z)$ by the right power of $\wp(z)$ to make $v_0(g) = v_0(f)$, noting that $v_0(f)$ is even, as proven.

II.5.2 Addition law, continued

$$\begin{aligned} &\mathbb{C}/\Lambda \xrightarrow{\phi} E_\Lambda(\mathbb{C}) \\ &\quad z \mapsto \big(\wp(z) : \wp'(z) : 1\big) && (z \notin \Lambda) \\ &\quad z \mapsto (0:1:0) && (z \in \Lambda) \end{aligned}$$

Theorem II.5.1. *$z_1 + z_2 + z_3 \equiv 0 \pmod{\Lambda} \iff \phi(z_1), \phi(z_2), \phi(z_3)$ collinear.*

We already proved this for $x_1 \neq x_2$. Take limits to get the general case. □

II.5.3 Explicit group law

Suppose $\operatorname{char} K \neq 2$, and consider an elliptic curve

$$E : y^2 = f(x) = ax^3 + bx^2 + cx + d.$$

Say (x_1, y_1) and (x_2, y_2) are points on E with coordinates in K. Say $x_1 \neq x_2$. Let (x_3, y_3) be the third point of intersection of the line joining P_1, P_2 and E. Call the line $y = mx + k$. Then

$$(mx + k)^2 = ax^3 + bx^2 + cx + d$$

has roots x_1, x_2, x_3. This yields

$$ax^3 + (b - m^2)x^2 + \cdots = 0,$$

whence

$$x_1 + x_2 + x_2 = \frac{m^2 - b}{a}.$$

So

$$x_3 = -x_1 - x_2 - \frac{b}{a} + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 \frac{1}{a}.$$

Solve

$$\frac{y_3 - y_1}{x_3 - x_1} = \frac{y_2 - y_1}{x_2 - x_1}$$

to get a.

If $x_1 = x_2$, there are two possibilities:

(a) $P_1 = P_2$. Then if $y^2 = f(x)$, we have

$$2y\frac{dy}{dx} = f'(x),$$

so

$$m = \frac{f'(x_1)}{2y_1} \implies x_3 = -2x_1 - \frac{b}{a} + \left(\frac{f'(x_1)}{2y_1}\right)^2 \frac{1}{a}.$$

(b) If $x_1 = x_2$ and $y_1 = -y_2$, then the third point of intersection is the point at ∞.

Remark II.5.2. Note that the group law gives $(x_1, y_1) \oplus (x_2, y_2)$ as an expression in x_1, x_2, y_1, y_2 with coefficients a, b, c, d of E. We could check by brute force that this is a group.

Associativity follows from an identity involving $x_1, x_2, y_1, y_2, a, b, c, d$ with integer coefficients. Since we already know this is a group, we know this identity holds.

If $K \subseteq \mathbb{C}$, then $E(K) \leq E(\mathbb{C})$ (subgroup).

II.5.4 Division points

Say $K = \mathbb{C}$, $E = E_\Lambda$, and m is a positive integer. For $P \in E(\mathbb{C})$, denote

$$[m]P \stackrel{\text{def}}{=} \underbrace{P + \cdots + P}_{m \text{ times}}.$$

Let

$$E[m] = \left\{P \in E(\mathbb{C}) \;\middle|\; [m]P = \text{point at } \infty\right\}.$$

This is a subgroup of $E(\mathbb{C})$.

What are the points of order m in $\mathbb{C}/\Lambda$? In general,

$$\mathbb{C}/\Lambda \cong S^1 \times S^1,$$

so

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Moreover, $E[m] \subseteq E(K) \iff$ all roots of f lie in K.

Example II.5.3 ($m = 2$). Abstractly, $E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. More concretely,

$$\begin{aligned} E[2] &= \left\{\phi(0), \phi\left(\frac{\omega_1}{2}\right), \phi\left(\frac{\omega_2}{2}\right), \phi\left(\frac{\omega_1+\omega_2}{2}\right)\right\} \\ &= \left\{\infty, \left(\wp\left(\frac{\omega_1}{2}\right), \wp'\left(\frac{\omega_1}{2}\right)\right), \left(\wp\left(\frac{\omega_2}{2}\right), \wp'\left(\frac{\omega_2}{2}\right)\right), \left(\wp\left(\frac{\omega_1+\omega_2}{2}\right), \wp'\left(\frac{\omega_1+\omega_2}{2}\right)\right)\right\} \\ &= \{\infty\} \cup \left\{(a, 0) \;\middle|\; f(a) = 0\right\}. \end{aligned}$$

Example II.5.4 ($m = 3$). $E[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is the *Hesse configuration* of 9 flex points: $3P = \infty \iff P, P, P$ are collinear $\iff P$ is a flex point.

Example II.5.5. Let $E : y^2 = x^3 - x$. Then

$$E[2] = \{\infty, (-1,0), (0,0), (1,0)\}$$
$$E[3] = ?$$

Solve $2P = -P$. If $P = (x, y)$ and $2P = (x_3, y_3)$, then

$$x_3 = -2x + \left(\frac{f'(x)}{2y}\right)^2 = -2x + \frac{(3x^2-1)^2}{4(x^3-x)}.$$

So we want to solve

$$-2x + \frac{(3x^2-1)^2}{4(x^3-x)} = x.$$

Clearing denominators,

$$3x^4 - 6x^2 - 1 = 0,$$

so

$$x^2 = \frac{6 \pm \sqrt{36+12}}{6} = 1 \pm \frac{2\sqrt{3}}{3},$$

and we get

$$x = \pm\sqrt{1 + \frac{2\sqrt{3}}{3}} \notin \mathbb{Q}.$$

Remark II.5.6. The smallest extension field over which these roots are all defined is closely related to the beginnings of non-abelian class field theory.

Example II.5.7. If we do this for

$$y^2 = f(x) = x^3 = ax + b,$$

we get that the x-coordinates of a 3-torsion point (other than ∞) satisfy

$$g(x) = 3x^4 + 6ax^2 + 12bx - a^2 = 0.$$

Note that

$$g'(x) = 12f(x).$$

WHY?

Theorem II.5.8. *Suppose E is defined over K. If $P \in E[m]$, then the coordinates of P lie in $\overline{K}$.*

II.6 2013-09-30

II.6.1 Torsion points, continued

Let E be an elliptic curve over K, and let m be a positive integer. Recall that

$$E[m] \stackrel{\text{def}}{=} \left\{P \in E(\mathbb{C}) \;\middle|\; mP = \text{point at } \infty\right\}.$$

Theorem II.6.1. *If $P \in E[m]$, then the coordinates of P are algebraic over K. In particular,*

$$E[m] \leq E(\overline{K}).$$

Moreover, let L/K be a field extension, and let $\sigma \in \mathrm{Aut}_K(L)$. If $P \in E(L)$ has order m, then $\sigma(P) \in E(L)$ and has order m, where if $P = (x, y)$, we say $\sigma(P) = (\sigma(x), \sigma(y))$.

Remark II.6.2. We saw this for $m = 2, 3$. The idea of the proof is this: Assume $E : y^2 = x^3 + ax + b$ with $\mathrm{char}\, K = 0$. If $P = (x, y)$, then

$$mP = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3} \right),$$

where

$$\begin{aligned} \psi_1 &= 1, \\ \psi_2 &= 2y, \\ \psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2, \\ \psi_4 &= 4y\left(x^6 + 5ax^4 + \dots\right), \\ &\vdots \end{aligned}$$

(the m-division polynomials). Moreover,

$$mP = \infty \iff \psi_m(P) = 0.$$

For m odd, ψ_m is a polynomial in x, so the x-coordinates are algebraic over K, whence the y-coordinates are as well.

For m even, either $y = 0$ (so $P \in E[2]$) or a polynomial in x is zero, so the x-coordinates are again algebraic over K.

Proof of Theorem II.6.1. Apply σ to $y^2 = f(x)$:

$$\sigma(y)^2 = \sigma\big(f(x)\big) = f\big(\sigma(x)\big)$$

since $f \in K[x]$. The addition law has coefficients in K, so

$$\sigma(P_1 + P_2) = \sigma(P_1) + \sigma(P_2).$$

Thus $\sigma(mP) = m\sigma(P)$. □

II.6.2 Galois representations associated to elliptic curves

Say E is an elliptic curve over $\mathbb{Q}$. Recall that

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

We have a representation

$$\rho_m : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Example II.6.3. Say $m = 2$ and E is in the form $y^2 = f(x)$. Then

$$E[2] = \{\infty\} \cup \big\{(\alpha, 0) \;\big|\; f(\alpha) = 0\big\}.$$

The representation

$$\rho_2 : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$$

acts by permuting the roots of f. (It follows that every mod 2 representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ comes from an elliptic curve.)

Remark II.6.4. The fixed field of $\ker \rho_m$ is K_m (the *m-division field*), where

$$K_m = \text{extension of } \mathbb{Q} \text{ generated by the coordinates of } E[m].$$

Furthermore, the image of ρ_m is

$$\rho_m\big(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\big) \cong \mathrm{Gal}(K_m/\mathbb{Q}).$$

This is the starting point of *nonabelian class field theory*.

II.6.3 Modular forms and modular curves

Consider the upper half plane

$$\mathscr{H} = \big\{z \in \mathbb{C} \;\big|\; \mathrm{Im}(z) > 0\big\}.$$

The group $\mathrm{SL}_2(\mathbb{R})$ acts by

$$gz = \frac{az+b}{cz+d}, \qquad\qquad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}).$$

Indeed, this acts on $\mathscr{H}$:

$$\mathrm{Im}(gz) = \frac{\mathrm{Im}(z)}{|cz+d|^2}.$$

Earlier, we considered the case $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ acting on $\mathscr{H}$. Set

$$\bar{\Gamma} := \mathrm{PSL}_2(\mathbb{Z}) = \Gamma / \{\pm I\}.$$

We are interested in $\mathscr{H}/\Gamma$ and functions satisfying

$$f(z) = (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right) \qquad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,\ z \in \mathscr{H}. \tag{II.6.3.1}$$

Example II.6.5. For $k = 0$, the j-invariant is such a function.

Definition II.6.6. If f is meromorphic on H and satisfies (II.6.3.1), then f is called *weakly modular* of weight k on Γ.

Fact II.6.7. The group $\bar{\Gamma}$ is isomorphic to a free product

$$\bar{\Gamma} = \left\langle S, T \;\middle|\; S^2 = (ST)^3 = I \right\rangle \cong \mathbb{Z}/2 * \mathbb{Z}/3,$$

where

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Thus, condition (II.6.3.1) is equivalent to:

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

By the second condition, we can write

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n, \qquad q = e^{2\pi i z}.$$

Definition II.6.8. If $a_n = 0$ for all $n < 0$, we call f a *modular form* (of weight k for Γ). If $a_n = 0$ for all $n \leq 0$, we call f a *cusp form* (or *cuspform*).

II.7 2013-10-02

II.7.1 Modular forms, continued

Exercise II.7.1. If f, g are modular forms of weight k, k', respectively, then fg is a modular form of weight $k + k'$.

Exercise II.7.2. If f, g are modular forms of weight k, and $c \in \mathbb{C}$ is a constant, then $f + g$ and cf are modular forms of weight k. (In other words, the set of weight k modular forms is a $\mathbb{C}$-vector space.)

II.7.2 Example: $G_k(z)$

For $z \in \mathscr{H}$, let $\Lambda_z = \langle 1, z \rangle = \{m + nz \mid m, n \in \mathbb{Z}\}$ (where $z \in \mathscr{H}$), and write

$$G_k(z) = G_k(\Lambda_z) = \sum_{(m,n) \neq (0,0)} \frac{1}{(m+nz)^k}.$$

We can check that $G_k(z)$ is absolutely convergent, and uniformly convergent on compact subsets. Thus, $G_k(z)$ is holomorphic on H.

Moreover, G_k has the following properties:

$$G_k(z+1) = G_k(z),$$
$$G_k\left(-\frac{1}{z}\right) = \sum_{(m,n) \neq (0,0)} \frac{1}{\left(m + n\left(-\frac{1}{z}\right)\right)^k} = \sum_{(m,n) \neq (0,0)} \frac{z^k}{(mz - n)^k} = z^k G_k(z),$$

where the last step is given by a permutation of Λ_z.

So $G_k(z)$ is weakly modular of weight k for Γ.

Claim II.7.3. *For $k \geq 4$ even,*

$$G_k(z) = 2\zeta(k)\left(1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n\right),$$

where ζ is the Riemann zeta function, B_k is the k-th Bernoulli number, and

$$\sigma_\ell(n) = \sum_{d|n} d^\ell.$$

The claim implies that $G_k(z)$ is a modular form, and is not a cusp form.

Proof. Use the identity

$$\pi\cot(\pi z) = \frac{1}{z} + \sum_{m=1}^{\infty}\left(\frac{1}{z+m} + \frac{1}{z-m}\right),$$

which converges uniformly on compact subsets. Let $q = e^{2\pi i z}$, where $\operatorname{Im} z > 0$, so $|q| < 1$. Then

$$\begin{aligned}\pi\cot(\pi z) &= \frac{\pi\cos(\pi z)}{\sin(\pi z)} = \pi i\frac{e^{i\pi z} + e^{-i\pi z}}{e^{i\pi z} - e^{-i\pi z}}\\ &= i\pi\left(\frac{q+1}{q-1}\right) = i\pi - \frac{2\pi i}{1-q}\\ &= i\pi - 2\pi i\sum_{d=0}^{\infty} q^d.\end{aligned}$$

So

$$\frac{1}{z} + \sum_{m=1}^{\infty}\left(\frac{1}{z+m} + \frac{1}{z-m}\right) = i\pi - 2\pi i\sum_{d=0}^{\infty} q^d.$$

Now differentiate $(k-1)$ times:

$$(-1)^{k-1}(k-1)!\sum_{m=-\infty}^{\infty}\frac{1}{(z+m)^k} = -(2\pi i)^k\sum_{d=1}^{\infty} d^{k-1}q^d.$$

Thus,

$$\begin{aligned}G_k(z) &= \sum_{m\neq 0}\frac{1}{m^k} + \sum_{n\neq 0}\sum_{m=-\infty}^{\infty}\frac{1}{(nk+m)^k}\\ &= 2\zeta(k) + 2\sum_{n=1}^{\infty}\sum_{m=-\infty}^{\infty}\frac{1}{(nz+m)^k}\\ &= 2\zeta(k) + 2\sum_{n=1}^{\infty}\frac{(-1)^k}{(k-1)!}(2\pi)^k(-1)^{k/2}\sum_{d=1}^{\infty} d^{k-1}q^{nd}\\ &= 2\zeta(k) + \frac{2(2\pi)^k(-1)^{k/2}}{(k-1)!}\sum_{n=1}^{\infty}\sum_{d=1}^{\infty} d^{k-1}q^{nd}.\end{aligned}$$

Now we need a formula for some special values of the ζ function: setting $k = 2n$, we have

$$\zeta(2n) = (-1)^{n+1}\frac{B_{2n}2^{2n}\pi^{2n}}{2(2n)!} = B_k\frac{(2\pi i)^k}{(-2k)(k-1)!}.$$

Hence,

$$\begin{aligned} G_k(z) &= 2\zeta(k) + \frac{2(2\pi)^k(-1)^{k/2}}{(k-1)!}\sum_{n=1}^{\infty}\sum_{d=1}^{\infty} d^{k-1}q^{nd} \\ &= 2\zeta(k) - 2\zeta(k)\frac{2k}{B_k}\sum_{n=1}^{\infty}\Big(\sum_{d|n} d^{k-1}\Big)q^n \\ &= 2\zeta(k)\left(1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n\right). \end{aligned}$$

□

II.7.3 The discriminant

Some special values of the ζ function:

$$\begin{aligned} \zeta(4) &= \frac{\pi^4}{90}, \\ \zeta(6) &= \frac{\pi^6}{3^3\cdot 5\cdot 7}. \end{aligned}$$

Let

$$\Delta(z) = g_2(z)^3 - 27g_3(z)^2 = \big(60G_4(z)\big)^3 - 27\big(140G_6(z)\big)^2.$$

So, using the claim,

$$\begin{aligned} G_4(z) &= \frac{\pi^4}{45} + \frac{(2\pi)^4}{3}\left(q + 9q^2 + \dots\right), \\ G_6(z) &= \frac{2\pi^6}{3^3\cdot 5\cdot 7} - \frac{(2\pi)^6}{60}\left(q + 33q^2 + \dots\right). \end{aligned}$$

Thus,

$$\Delta(z) = (2\pi)^{12}\left(q - 24q^2 + 252q^3 + \dots\right).$$

In fact,

$$\Delta(z) = (2\pi)^{12}q\prod_{n=1}^{\infty}(1-q^n)^{24}.$$

(We omit the proof, due to Jacobi.)

It follows that G_4, G_6 are weight $4, 6$ modular forms, respectively. Thus, g_2^3 and g_3^2 are weight 12 modular forms. So Δ is a weight 12 modular form for Γ, actually a cusp form.[2]

[2]In fact, there are no cusp forms of weight less than 12 for the whole modular group Γ.

II.7.4 The j-invariant

Recall that

$$j(z) = \frac{1728 g_2^3}{g_2^3 - 27 g_3^2} = \frac{1}{q} + 744 + 196884q + \dots$$

The j-variant is weakly modular of weight 0.

Remark II.7.4 (Monstrous moonshine). If G is the monster simple group, the smallest n such that $G \hookrightarrow \mathrm{GL}_n(\mathbb{C})$ is $n = 196833$. (The monstrous moonshine conjecture was proved by Borcherds, who made a breakthrough on a bus in Tibet.)

II.8 2013-10-04

II.8.1 Fundamental domains in the upper half plane

(Knapp, p. 230)

A fundamental domain D for Γ in the upper half plane: see picture.

(a) Each point of H can be mapped into D by an element of Γ.

(b) The only points of D equivalent to each other under the action of Γ are $z, z+1$ on vertical sides and $z - \frac{1}{2}$ on the circular arc.

(c) The only points fixed by $\gamma \neq 1$ in $\bar{\Gamma} = \Gamma / \{\pm I\}$ are $z = i$ (stabilizer is $\{I, S\}$) and $z = \rho, \rho^2$ (stabilizers are $\{I, ST, (ST)^2\}$ and $\{I, TS, (TS)^2\}$).

II.8.2 Homothety

$$\Lambda \to \mathscr{H}$$

$$\Lambda = \langle \omega_1, \omega_2 \rangle \mapsto \underbrace{\frac{\omega_1}{\omega_2} \text{ or } \frac{\omega_2}{\omega_1}}_{\text{exactly one in } \mathscr{H}}$$

What if we pick another basis $\Lambda = \langle \omega_1', \omega_2' \rangle$, i.e.,

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}, A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}).$$

If $\det A = -1$, then $\mathrm{Im}(\frac{\omega_1}{\omega_2})$ and $\mathrm{Im}(\frac{\omega_1'}{\omega_2'})$ have different signs. If $\det A = 1$, then $\mathrm{Im}(\frac{\omega_1'}{\omega_2'}) = \mathrm{Im}(\frac{\omega_1}{\omega_2})$.

Thus, we have a well-defined map

$$\text{Lattices/Homothety} \to H/\Gamma.$$

This map is clearly surjective. It is also injective: Λ_1 and Λ_2 have the same image $\iff$ $\Lambda_1 = a\Lambda_2$ for some $a \in \mathbb{C}^\times$, i.e., Λ_1 and Λ_2 are homothetic. [In fact, $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are isomorphic elliptic curves $\iff$ Λ_1 and Λ_2 are homothetic.]

Thus, $j : H/\Gamma \to \mathbb{C}$ is the *moduli space* of elliptic curves.

$$H/\Gamma \longleftrightarrow \{\text{Lattices up to homothety}\} \longleftrightarrow \{\text{Elliptic curves over } \mathbb{C} \text{ up to isomorphism}\}$$

II.8.3 The modular curve

For $N \in \mathbb{Z}_+$, consider the finite-index subgroup

$$\Gamma_0(N) \stackrel{\text{def}}{=} \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \;\middle|\; c \equiv 0 \pmod{N} \right\} \leq \Gamma.$$

A *modular curve* $Y_0(N)$ is given by

$$\begin{array}{ccc} Y_0(N) & = & H/\Gamma_0(N) \longleftrightarrow \{(E, C) \mid E \text{ elliptic curve over } \mathbb{C},\ C \text{ subgroup of order } N\} \\ & & \downarrow \qquad\qquad\qquad\qquad\qquad\qquad \downarrow \\ & & H/\Gamma \longleftrightarrow \{\text{isomorphism classes of elliptic curves over } \mathbb{C}\} \end{array}$$

Let

$$H^* = H \cup \overbrace{\mathbb{Q} \cup \{i\infty\}}^{\text{cusps}}.$$

Extend the action of Γ by identifying $\mathbb{Q} \cup \{i\infty\}$ with $\mathbb{P}^1(\mathbb{Q})$, giving a transitive action

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (x : y) = (ax + by : cx + dy).$$

A base of open neighborhoods of $i\infty$ is given by

$$N_C = \{z s t \operatorname{Im}(z) > C\} \cup \{i\infty\}, \qquad C \to \infty,$$

as shown by the map

$$\begin{array}{rl} & z \mapsto e^{2\pi i z} = q, \\ H \to \text{punctured unit open disk}, & \\ & i\infty \mapsto \text{origin} \end{array}$$

We likewise get a compact Riemann surface

$$X_0(N) = H^*/\Gamma_0(N).$$

Note II.8.1. With the given topology, H^*/Γ is compact. Look at $j : H/\Gamma \to \mathbb{C}$ holomorphic ($\Delta = g_2^3 - 27g_3^2 \neq 0$). Extend j to a *meromorphic function*

$$\begin{array}{c} j : H^*/\Gamma \to \mathbb{C}_\infty, \\ j(i\infty) = \infty. \end{array}$$

Note that j has a simple pole at ∞. So j is injective. Also, j is surjective, completing the outstanding proof that given a, b with $a^3 - 27b^2 \neq 0$, there exists Λ such that $g_2(\Lambda) = a$ and $g_2(\Lambda) = b$.

Chapter III

Elliptic Curves over Finite Fields

III.1 2013-10-04

III.1.1 Example over some finite fields

Consider the equation

$$E : x^3 + y^3 = z^3.$$

This defines an elliptic curve over $\mathbb{F}_q$ iff $3 \nmid q$. (In characteristic 3, $x^3 + y^3 = (x + y)^3$, so E is a triple line.)

Note that $E(\mathbb{F}_q) \leq E(\mathbb{F}_{q^2})$, so $|E(\mathbb{F}_q)| \mid |E(\mathbb{F}_{q^2})|$.

q	$\lvert E(\mathbb{F}_q)\rvert$	q	$\lvert E(\mathbb{F}_q)\rvert$	q	$\lvert E(\mathbb{F}_q)\rvert$
2	3	3	4	5	6
2	9	9	10	25	36
8	9	27	28	25	36
16	9	81	82	125	126
64	81				
128	129				

III.1.2 Magma code for size of elliptic curves

```
f := function(q)
K := GF(q)_i
n := 0
for x in K do
for y in K do
for z in K do
if x^3 + y^3 eq z^3 then
n := n + 1;
end if;
end for; end for; end for;
return (n - 1)/(q - 1);
end function;
```

III.2 2013-10-07

III.2.1 Counting points on elliptic curves

Definition III.2.1. Let E be an elliptic curve over $\mathbb{F}_q$. We define

$$N_r \stackrel{\text{def}}{=} |E(\mathbb{F}_{q^r})|,$$
$$Z(T) \stackrel{\text{def}}{=} \exp\left(\sum_{r=1}^{\infty} \frac{N_r T^r}{r}\right),$$

where $Z(T)$ is considered as a formal power series.

Lemma III.2.2.

$$Z(T) = \frac{\prod_i (1-\alpha_i T)}{\prod_j (1-\beta_j T)} \qquad \Longleftrightarrow \qquad N_r = \sum_j \beta_j^r - \sum_i \alpha_i^r,$$

where i, j range over a finite set.

Proof. Observe that

$$\begin{aligned}
\exp\left(\sum_{r=1}^{\infty} \frac{N_r T^r}{r}\right) &= \exp\left(\sum_{r=1}^{\infty}\left(\sum_j \frac{B_j^r T^r}{r} - \sum_i \frac{\alpha_i^r T^r}{r}\right)\right) \\
&= \exp\Big(\sum_j \big(-\log(1-\beta_j T)\big) - \sum_i \big(-\log(1-\alpha_i T)\big)\Big) \\
&= \exp\left(\log\left(\frac{\pi(1-\alpha_i T)}{\pi(1-\beta_j T)}\right)\right) \\
&= \frac{\pi(1-\alpha_i T)}{\pi(1-\beta_j T)}.
\end{aligned}$$

□

Example III.2.3. Let $E : x^3 + y^3 = z^3$ and $q = 2$. Take $\beta_1 = 1$, $\beta_2 = 2$, $\alpha_1 = \sqrt{-2}$, and $\alpha_2 = -\sqrt{-2}$. Then

$$\beta_1 + \beta_2 - \alpha_1 - \alpha_2 = 3,$$
$$\beta_1^2 + \beta_2^2 - \alpha_1^2 - \alpha_2^2 = 9,$$

and so on. So

$$Z(T) = \frac{(1-\sqrt{-2}T)(1+\sqrt{-2}T)}{(1-T)(1-2T)} = \frac{1+2T^2}{(1-T)(1-2T)}.$$

III.2.2 Hasse's theorem

Theorem III.2.4 (Hasse, 1930s)**.** *For all elliptic curve over $\mathbb{F}_q$,*

$$Z(T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)},$$

where $a \in \mathbb{Z}$, $|a| \leq 2\sqrt{q}$.

We will prove this theorem over the next couple of weeks.

Note III.2.5. $N_1 = \beta_1 + \beta_2 - \alpha_1 - \alpha_2 = 1 + q - a$ is the numerator evaluated at $T = 1$.

Proof. We have

$$\frac{(1-\alpha_1 T)(1-\alpha_2 T)}{(1-\beta_1 T)(1-\beta_2 T)} = \frac{1-(\alpha_1+\alpha_2)T+\alpha_1\alpha_2 T^2}{(1-\beta_1)(1-\beta_2 T)} = \frac{1-aT+qT^2}{(1-T)(1-qT)},$$

so $\alpha_1 + \alpha_2 = a$, $\{\beta_1, \beta_2\} = \{1, q\}$. □

Corollary III.2.6. *(a) $Z(T)$ is determined by N_1 (and hence $N_2, N_3, \ldots$ are determined by N_1).*

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

We'll show $|\alpha_1| = |\alpha_2| = \sqrt{q}$.

III.2.3 Weil conjectures

The bigger picture:

Theorem III.2.7 (Deligne, 1972)**.** *Let V be a smooth projective variety over $\mathbb{F}_q$ of dimension m. Let $N_r = |V(\mathbb{F}_{q^r})|$, and set*

$$Z(T) = \exp\left(\sum_{r=1}^{\infty} \frac{N_r T^r}{r}\right).$$

Then

$$Z(T) = \frac{P_1(T) \cdot \ldots \cdot P_{2m-1}(T)}{P_0(T) \cdot P_2(T) \cdot \ldots \cdot P_{2m}(T)},$$

where $P_0 = 1 - T$, $P_{2m}(T) = 1 - q^m T$,

$$P_i(T) = \prod_j (1 - \alpha_{ij} T) \in \mathbb{Z}[T]$$

with $|\alpha_{ij}| = q^{i/2}$,

$$\deg P_i = i\text{-th Betti number of } V,$$

and

$$Z\left(\frac{1}{q^m T}\right) = \pm q^{mE/2} T^E Z(T),$$

where E is the Euler characteristic.

Remark III.2.8. The part stating that $|\alpha_{ij}| = q^{i/2}$ is known as the *Riemann hypothesis for finite fields*. Here's why: The zeros of

$$\frac{(1-\alpha_1 T)(1-\alpha_2 T)}{(1-T)(1-qT)}$$

occurs at $T = \alpha_i^{-1}$. If we set $T = \alpha_i^{-1} = q^{-s}$, then $|\alpha_i| = \sqrt{q} \iff \operatorname{Re} s = \frac{1}{2}$.

III.2.4 Another example

Consider the elliptic curve

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

in characteristic 2. We have

$$|E(\mathbb{F}_2)| = 5 = N_1 = 1 + q - a,$$

so $a = -2$. Thus

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

III.2.5 Complex version of Hasse's theorem

Theorem III.2.9 (Hasse)**.** *Let $X = \mathbb{C}/\Lambda$ be an elliptic curve over $\mathbb{C}$. Let $\pi : X \to X$ be a morphism (i.e., an analytic map of Riemann surfaces and a group homomorphism) with kernel of finite order $q > 1$. Let*

$$N_r = \#\textit{fixed points of } \pi^r.$$

Then $N_r < \infty$, and

$$\exp\left(\sum_{r=1}^{\infty} \frac{N_r T^r}{r}\right) = \frac{P_\pi(T)}{(1 - T)(1 - qT)},$$

where $P_\pi(T)$ is a quadratic in $\mathbb{Z}[t]$, and its roots have absolute value $q^{-1/2}$.

Remark III.2.10. What's the connection between the theorems? In the finite field case, think of $X = E(\overline{\mathbb{F}_q})$, and let

$$\pi : X \to X$$
$$(x, y) \mapsto (x^q, y^q)$$

be the Frobenius map. A point (x, y) is fixed under $\pi^r \iff$ the coordinates satisfy $x^{q^r} = x$ and $y^{q^r} = y \iff x, y \in \mathbb{F}_{q^r}$.

Remark III.2.11. The idea of the proof is to study $\mathrm{End}(X)$.

III.3 2013-10-09

III.3.1 Complex Hasse's theorem

Theorem III.3.1 (Hasse)**.** *Let $X = \mathbb{C}/\Lambda$. Let $\pi : X \to X$ be a morphism (i.e., an analytic map of Riemann surfaces and a group homomorphism), with kernel of finite order $q > 1$. Let N_r be the number of fixed points of π^r. Then $N_r < \infty$ and*

$$\exp\left(\sum_{r=1}^{\infty} \frac{N_r T^r}{r}\right) = \frac{P_\pi(T)}{(1 - T)(1 - qT)},$$

where $P_\pi(T)$ is a quadratic in $\mathbb{Z}[T]$ with all roots of absolute value $q^{-1/2}$.

Idea: Study $\mathrm{End}(X)$.

III.3.2 Preparatory material

Given $a \in \mathbb{C}$, define $\phi_a(x) = ax$. If $a\Lambda_1 \subseteq \Lambda_2$, this defines a well-defined morphism

$$\mathbb{C}/\Lambda_1 \xrightarrow{\phi_a} \mathbb{C}/\Lambda_2,$$

so $\phi_a \in \mathrm{Hom}(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2)$.

Lemma III.3.2 (proved later)**.** *There is a bijection*

$$\begin{aligned} \mathrm{Hom}(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2) &\longleftrightarrow \left\{ a \in \mathbb{C} \;\middle|\; a\Lambda_1 \subseteq \Lambda_2 \right\}, \\ \phi_a &\longleftrightarrow a. \end{aligned}$$

So $\mathbb{C}/\Lambda_1 \cong \mathbb{C}/\Lambda_2 \iff \exists a \in \mathbb{C}^\times$ *such that* $a\Lambda_1 = \Lambda_2$.

Hence we can assume without loss of generality that

$$\Lambda = \langle 1, \tau \rangle = \left\{ m + n\tau \;\middle|\; m, n \in \mathbb{Z} \right\}$$

for some $\tau \in \mathscr{H}$.

Let $X = \mathbb{C}/\Lambda$. Then we have a ring map

$$\begin{aligned} \mathrm{End}(X) &\hookrightarrow \mathbb{C}, \\ \phi_a &\mapsto a \end{aligned}$$

which is an injection by the lemma. Thus $\mathrm{End}(X)$ is a (commutative) integral domain.

If $\phi_a \in \mathrm{End}(X)$, then $1 \in \Lambda \implies a \in \Lambda$, so $\mathrm{End}(X) \hookrightarrow \Lambda$ as abelian groups. So the additive group of $\mathrm{End}(X)$ is free abelian of rank 1 or 2.

Definition III.3.3. If $\mathrm{End}(X)$ has rank 2, we say that X has *complex multiplication*.

Example III.3.4. Let $\Lambda = \mathbb{Z}[i]$. Then $\mathrm{End}(X) = \mathbb{Z}[i]$, and X has complex multiplication. We can see this algebraically: $g_3(\Lambda) = 0$, so we have

$$E : y^2 = 4x^3 - g_2 x.$$

Consider

$$\begin{aligned} \theta : E(\mathbb{C}) &\to E(\mathbb{C}), \\ (x, y) &\mapsto (-x, iy). \end{aligned}$$

Then $\theta^4 = \mathrm{id}$ and $\theta^2 \neq \mathrm{id}$.

Definition III.3.5. Let $a \in \mathrm{End}(X),\ a \neq 0$. The *norm* (*degree*) of a is

$$N(a) = |\ker a| = \left|a^{-1}\Lambda/\Lambda\right| = [\Lambda : a\Lambda].$$

Set $N(0) = 0$.

Example III.3.6. If $a \in \mathbb{Z}$, then $N(a) = a^2$.

III.3.3 Proof of complex Hasse's theorem

Suppose $a = m + n\tau$ $(m, n \in \mathbb{Z})$ (since $a \in \Lambda$). Then $a\tau \in \Lambda$, say $a\tau = m' + n'\tau$. Thus

$$a \mapsto \begin{pmatrix} m & n \\ m' & n' \end{pmatrix}$$

tells us the action of a on Λ. This correspondence yields a ring homomorphism

$$\mathrm{End}(X) \to M_2(\mathbb{Z}).$$

By Cayley–Hamilton, a must satisfy its characteristic polynomial. Thus, a is a root of

$$t^2 - (m + n')t + (mn' - nm') = 0.$$

Call the other root $\bar{a} = m + n' - a$. Then[1]

$$N(a) = \det \begin{pmatrix} m & n \\ m' & n' \end{pmatrix} = mn' - nm' = a\bar{a} = \bar{a}a \in \mathbb{Z}.$$

Hence the map $a \mapsto \bar{a}$ is an involution of $\mathrm{End}(X)$.

Therefore,

$$\begin{aligned} N_r &:= \#\text{fixed points of } \pi^r = |\ker(1 - \pi^r)| \\ &= N(1 - \pi^r) = (1 - \pi^r)\overline{(1 - \pi^r)} \\ &= (1 - \pi^r)\,(1 - \bar{\pi}^r) \\ &= 1 - \pi^r - \bar{\pi}^r + (\pi\bar{\pi})^r. \end{aligned}$$

Since

$$|\pi|^2 = \pi\bar{\pi} = N(\pi) = |\ker \pi| = q,$$

we have $|\pi| = \sqrt{q}$. Thus

$$Z(T) = \frac{(1 - \pi T)(1 - \bar{\pi}T)}{(1 - T)(1 - \pi\bar{\pi}T)} = \frac{P_\pi(T)}{(1 - T)(1 - qT)},$$

where P_π is a quadratic in $Z[T]$ and the zeros of P_π have absolute value $q^{-1/2}$. □

III.3.4 Proof of lemma

Lemma III.3.7. *The map*

$$\begin{aligned} \left\{a \in \mathbb{C} \;\middle|\; a\Lambda_1 \subseteq \Lambda_2\right\} &\to \left\{\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \;\middle|\; \phi \text{ analytic}, \phi(0) = 0\right\}, \\ a &\mapsto \phi_a \end{aligned}$$

is a bijection.

[1] Exercise: If $\Lambda = \langle 1, \tau \rangle$, then the volume of the fundamental parallelogram of $\langle m + n\tau, m' + n'\tau \rangle$ is

$$\det \begin{pmatrix} m & n \\ m' & n' \end{pmatrix} \cdot \text{volume(fundamental parallelogram of } \Lambda).$$

Remark III.3.8. In fact, we'll see this implies that ϕ is a group homomorphism, so the above map is actually a ring isomorphism.

Proof. Injectivity: Say $\phi_a = \phi_b$. Then $az = bz \pmod{\Lambda_2}$ for all $z \in \mathbb{C}$, and so $z \mapsto (a-b)z$ is a map $\mathbb{C} \to \Lambda_2$. The image is discrete, so the map is constant, implying $a = b$.

Surjectivity: $\mathbb{C}$ is simply connected, so we can lift any $\phi \in \mathrm{Hom}(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2)$ to a commutative diagram

$$\begin{array}{ccc} \mathbb{C} & \dashrightarrow & \mathbb{C} \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} \\ \mathbb{C}/\Lambda_1 & \xrightarrow{\phi} & \mathbb{C}/\Lambda_2, \end{array}$$

where f is analytic and $f(0) = 0$. For any $\omega \in \Lambda_1$ and $z \in \mathbb{C}$,

$$f(z+\omega) - f(z) \in \Lambda_2,$$

so $f(z+\omega) - f(z)$ has to be constant. Thus $f'(z+\omega) = f'(z)$ for all $z \in \mathbb{C}$, $\omega \in \Lambda_1$. Hence f' is elliptic with respect to Λ_1, whence f' is constant. Therefore, $f'(z) = a$ for some $a \in \mathbb{C}$. So $f(z) = az + b$ for some $a, b \in \mathbb{C}$, but $b = 0$ because $f(0) = 0$. □

III.4 2013-10-11

III.4.1 Isogenies

Definition III.4.1. Suppose E_1, E_2 are elliptic curves over K. Say that $\phi : E_1 \to E_2$ is an *isogeny* if ϕ is a rational map and $\phi(0) = 0$ (where "0" denotes the identity elements).

Example III.4.2 (American Mathematical Monthly). Consider the elliptic curves

$$\begin{aligned} C &: y^2 = x^3 + 2, \\ J &: w^2 = z^3 - 120z + 506. \end{aligned}$$

The map

$$\begin{aligned} &\pi : C \to J, \\ &(x, y) \mapsto \left(x + \frac{24(x+1)}{(x+2)^2}, y - \frac{24xy}{(x+2)^3} \right) \end{aligned}$$

is an isogeny. Moreover, $|\ker \pi| = 3$, and if $p > 3$, then $|C(\mathbb{F}_p)| = |J(\mathbb{F}_p)|$.

Claim III.4.3. *Every analytic group homomorphism is an isogeny.*

$$\begin{array}{ccc} \mathbb{C}/\Lambda_1 & \xrightarrow{\phi_a} & \mathbb{C}/\Lambda_2 \\ {\scriptstyle (\wp_{\Lambda_1} : \wp'_{\Lambda_1} : 1)}\downarrow & & \downarrow{\scriptstyle (\wp_{\Lambda_2} : \wp'_{\Lambda_2} : 1)} \\ E_1 & \xrightarrow{\psi_a} & E_2 \end{array}$$

The map

$$\begin{gathered}\big(\wp_{\lambda_1}(z) : \wp'_{\Lambda_1}(z) : 1\big) \mapsto \big(\wp_{\Lambda_2}(az) : \wp'_{\Lambda_2}(az) : 1\big) \\ (0:1:0) \mapsto (0:1:0)\end{gathered}$$

makes the above diagram commute.

We need to show that $\wp_{\Lambda_2}(az), \wp'_{\Lambda_2}(az)$ are rational functions in $\wp_{\Lambda_1}(z), \wp'_{\Lambda_1}(z)$, i.e., that they are in

$$\mathbb{C}\big(\wp_{\Lambda_1}(z), \wp'_{\Lambda_1}(z)\big) = \mathbb{C}(\Lambda_1),$$

where $\mathbb{C}(\Lambda_1)$ is the field of elliptic functions with respect to Λ_1. So we just have to show that $\wp_{\Lambda_2}(az), \wp'_{\Lambda_2}(az)$ are elliptic with respect to Λ_1.

Indeed, if $\omega \in \Lambda_1$, then

$$\wp'_{\Lambda_2}(a(z+\omega)) = \wp'_{\Lambda_2}(az + a\omega) = \wp'_{\Lambda_2}(az)$$

since $a\omega \in \Lambda_2$. □

Definition III.4.4. Denote

$$\mathrm{End}(E) \stackrel{\text{def}}{=} \{\text{isogenies } E \to E \text{ defined over } K\}.$$

In case $K = \mathbb{C}$ and $E = \mathbb{C}/\Lambda$,

$$\mathrm{End}(E) = \{\text{analytic group homomorphisms } \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda\} \longleftrightarrow \big\{a \in \mathbb{C} \;\big|\; a\Lambda \subseteq \Lambda\big\}.$$

III.4.2 Rosati involutions

Definition III.4.5. A ring R is called a *ring with Rosati involution* provided that

(1) R is a (possibly noncommutative) ring with 1 with characteristic 0, and

(2) R is equipped with an involution

$$\begin{gathered}R \to R, \\ a \mapsto \overline{a}\end{gathered}$$

such that:

- $\overline{\overline{a}} = a$,
- $\overline{(ab)} = \overline{b}\overline{a}$,
- $\overline{(a+b)} = \overline{a} + \overline{b}$,
- for all $n \in \mathbb{Z}$, $\overline{n} = n$,
- $a\overline{a} = \overline{a}a \in \mathbb{Z}$, and
- $a\overline{a} > 0$ if $a \neq 0$.

Definition III.4.6. Define $\deg : R \to \mathbb{Z}$ by $\deg(a) = a\overline{a}$.

Example III.4.7. Let E be an elliptic curve over $\mathbb{C}$. Then $\mathrm{End}(E)$ is a ring with Rosati involution.

Corollary III.4.8. *Let R be any ring with Rosati involution. Then:*

(1) $\deg(0) = 0\overline{0} = 0$.

(2) $\deg(a) \geq 0$, *with* $\deg(a) > 0$ *if* $a \neq 0$.

(3) $\deg(ab) = (ab)\overline{(ab)} = ab\bar{b}\bar{a} = a(\deg b)\overline{a} = a\overline{a}(\deg b) = (\deg a)(\deg b)$.

(4) If $n \in \mathbb{Z}$, *then* $\deg(n) = n\overline{n} = n^2$.

Proposition III.4.9. *R has no zero-divisors.*

Proof. Suppose $ab = 0$. Then $\deg(a)\deg(b) = \deg(ab) = 0$. So $\deg a = 0$ or $\deg b = 0$, whence $a = 0$ or $b = 0$. □

Definition III.4.10. $\mathrm{tr}(a) = a + \overline{a}$.

Proposition III.4.11. *For all $a \in R$,* $\mathrm{tr}(a) \in \mathbb{Z}$.

Proof. We have

$$\deg(1+a) = (1+a)\overline{(1+a)} = (1+a)(\overline{1}+\overline{a}) = 1 + a + \overline{a} + a\overline{a}.$$

Since $\deg(1+a), 1, a\overline{a} \in \mathbb{Z}$, it follows that $a + \overline{a} \in \mathbb{Z}$. □

Definition III.4.12. For all $a \in R$, define

$$P_a(T) = T^2 - (\mathrm{tr}\, a)T + (\deg a) \in \mathbb{Z}[T].$$

III.4.3 Hasse's theorem via involutions

Proposition III.4.13 (Hasse's theorem)**.** $|\mathrm{tr}(a)| \leq 2\sqrt{\deg(a)}$.

Proof. For all $m, n \in \mathbb{Z}$,

$$\begin{aligned} 0 &\leq \deg(m + na) \\ &= (m + na)\overline{(m + na)} \\ &= (m + na)(m + n\overline{a}) \\ &= m^2 + mn\,\mathrm{tr}(a) + n^2 \deg(a) \\ &= n^2 P_a\Big(-\frac{m}{n}\Big). \end{aligned}$$

So $P_a(t) \geq 0$ for all $t \in \mathbb{Q}$. Thus, the discriminant of $P_a(T)$ is negative or zero, i.e.,

$$(\mathrm{tr}\, a)^2 - 4\deg(a) \leq 0.$$

So $|\mathrm{tr}\, a| \leq 2\sqrt{\deg(a)}$. □

Theorem III.4.14. *Let $\pi \in R$ be such that $\deg(\pi) = q$. Let $N_r = \deg(1 - \pi^r)$. Then*

$$\exp\left(\sum_{r=1}^{\infty} \frac{N_r T^r}{r}\right) = \frac{1 - (\operatorname{tr}\pi)T + qT^2}{(1-T)(1-qT)}.$$

Proof. We have

$$\begin{aligned} N_r &= (1-\pi^r)\overline{(1-\pi^r)} \\ &= (1-\pi^r)(1-\overline{\pi}^r) \\ &= 1 - \pi^r - \overline{\pi}^r + (\pi\overline{\pi})^r. \end{aligned}$$

Thus, by Lemma III.2.2,

$$\exp\left(\sum_{r=1}^{\infty} \frac{N_r T^r}{r}\right) = \frac{(1-\pi T)(1-\overline{\pi}T)}{(1-T)(1-\pi\overline{\pi}T)}. \qquad \square$$

III.4.4 Dual isogenies

Tasks:

(1) An elliptic curve E over K yields $\operatorname{End}(E)$, a ring with Rosati involution.

(2) When $K = \mathbb{F}_q$, show that

$$\deg(1-\pi^r) = |\ker(1-\pi^r)|,$$

where π is the Frobenius map $(x, y) \mapsto (x^q, y^q)$. (This amounts to showing separability of $1 - \pi^r$.)

Theorem III.4.15. *If R is a ring with Rosati involution, let $K = R \otimes_{\mathbb{Z}} \mathbb{Q}$. Then K is one of the following: $\mathbb{Q}$, an imaginary quadratic field, or a quaternion algebra.*

III.5 2013-10-14

III.5.1 Preliminaries

Last time: let R be a ring with Rosati involution, $\pi \in R$, $\deg\pi = q$, and $N_r = \deg(1-\pi^r)$. Then

$$\exp\left(\sum_{r=1}^{\infty} \frac{N_r T^r}{r}\right) = \frac{1 - (\operatorname{tr}\pi)T + qT^2}{1-T}$$

and $|\operatorname{tr}\pi| \le 2\sqrt{q}$.

This will be enough to prove Hasse's theorem once we show the following:

(a) If E is an elliptic curve over a field K, then $\operatorname{End}(E)$ is a ring with Rosati involution.

(b) If $K = \mathbb{F}_q$ and π is the Frobenius endomorphism $(x, y) \mapsto (x^q, y^q)$, then

$$|\ker(1 - \pi^r)| = \deg(1 - \pi^r).$$

Remark III.5.1. The fixed points of $1 - \pi^r$ are $E(\mathbb{F}_{q^r})$. In particular,

$$\begin{aligned} N_1 &= \deg(1 - \pi) \\ &= (1 - \pi)\overline{(1 - \pi)} \\ &= (1 - \pi)(1 - \overline{\pi}) \\ &= 1 - (\pi + \overline{\pi}) + \pi\overline{\pi} \\ &= 1 - (\operatorname{tr}\pi) + q. \end{aligned}$$

Since $|\operatorname{tr}\pi| \leq 2\sqrt{q}$, it follows that

$$1 + q - 2\sqrt{q} \leq N_1 \leq 1 + q + 2\sqrt{q}.$$

III.5.2 Classification of rings with Rosati involution

Theorem III.5.2. *If R is a ring with Rosati involution, let $K = R \otimes_{\mathbb{Z}} \mathbb{Q}$. Then K is one of the following:*

(a) $\mathbb{Q}$

(b) an imaginary quadratic field

(c) a quaternion algebra over $\mathbb{Q}$, i.e.,

$$K = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta,$$

where $\alpha^2, \beta^2 \in \mathbb{Q}$, $\alpha^2, \beta^2 < 0$, and $\beta\alpha = -\alpha\beta$.

Remark III.5.3. We shall see (time permitting) that, if E is an elliptic curve over L, then:

(1) if $\operatorname{char} L = 0$, then (c) does not arise (we saw this for $L = \mathbb{C}$); moreover,

- case (a) occurs $\iff$ E does not have complex multiplication, and
- case (b) occurs $\iff$ E has complex multiplication.

(2) if L is a finite field, then (a) does not arise (since Frobenius $\notin \mathbb{Z}$). We say that

- case (b) $\iff$ E is *ordinary*, and
- case (c) $\iff$ E is *supersingular*.

Proof of Theorem III.5.2. Extend $a \mapsto \overline{a}$ to K by

$$\overline{a \otimes q} = \overline{a} \otimes q \qquad\qquad (a \in R,\ q \in \mathbb{Q}),$$

and define as usual

$$\begin{aligned} \deg &: K \to \mathbb{Q}, & \operatorname{tr} &: K \to \mathbb{Q}, \\ \deg(a) &= a\overline{a}, & \operatorname{tr}(a) &= a + \overline{a}. \end{aligned}$$

Observe that K is a *division algebra* since, if $a \in K \setminus \{0\}$, then

$$\deg(a) = a\overline{a} \in \mathbb{Q}_{>0},$$

and $\deg(a) = 0 \iff a = 0$, whence

$$a^{-1} = \left(\frac{1}{\deg a}\right)\overline{a}.$$

Note that

$$0 = (a - \overline{a})(a - a) = a^2 - (a + \overline{a})a + \overline{a}a = a^2 - (\operatorname{tr} a)a + (\deg a).$$

Hence, a is a root of $T^2 - (\operatorname{tr} a)T + (\deg a) \in \mathbb{Q}[T]$. So $[\mathbb{Q}(a) : \mathbb{Q}] \leq 2$ for all $a \in K$.

Let $b = a - \frac{1}{2}\operatorname{tr}(a)$. Then $\operatorname{tr}(b) = 0$ and $\mathbb{Q}(b) = \mathbb{Q}(a)$, and $b^2 - 0b + \deg b = 0$, so $b^2 \in \mathbb{Q}_{\leq 0}$.

Result on classification of division algebras: If K is finite-dimensional over its center F, and M is a maximal subfield, then $[K : M] = [M : F]$.

Note III.5.4 (Bergman). If a division algebra is infinite-dimensional over its center F, then it contains an infinite-dimensional subfield.

In our case, since $\mathbb{Q}$ is perfect, every extension of $\mathbb{Q}$ is simple, so by the above, $[M : \mathbb{Q}] \leq 2$. So the possibilities are:

(1) If $F = \mathbb{Q}$, then $[K : \mathbb{Q}] = 1$ or 4.

(2) If $F > \mathbb{Q}$, then F is quadratic, so $M = F$, whence $n = 1$ and $K = F$, and K is therefore an imaginary quadratic field.

If $K = \mathbb{Q}$, we are done. If $[K : \mathbb{Q}] = 4$, pick $b \in K - \mathbb{Q}$ such that $\operatorname{tr}(b) = 0$. Pick $c \in K - \mathbb{Q}(b)$. Then

$$[\mathbb{Q}(b, c) : \mathbb{Q}(b)] = [\mathbb{Q}(b) : \mathbb{Q}] = 2.$$

Let

$$d = c - \frac{1}{2}\operatorname{tr}(c) - \frac{1}{2}\left(\frac{\operatorname{tr}(bc)}{b^2}\right)b.$$

We can check that

$$\operatorname{tr}(b) = \operatorname{tr}(d) = \operatorname{tr}(bd) = 0.$$

So $\overline{b} = -b$, $\overline{d} = -d$, and $bd = -\overline{(bd)} = -\overline{db} = -db$. Moreover,

$$\begin{aligned} b^2 &= -\deg(b) \in \mathbb{Q}_{<0}, \\ d^2 &= -\deg(d) \in \mathbb{Q}_{<0}, \end{aligned}$$

and $b, d \notin \mathbb{Q}$. Set $\alpha = b$ and $\beta = d$. Thus, K is a quaternion algebra over $\mathbb{Q}$. □

Remark III.5.5. The key fact driving this theorem is that $[\mathbb{Q}(a) : \mathbb{Q}] \leq 2$ for all $a \in K$. This is analogous to the classification of real division algebras.

III.5.3 Dual isogeny

Look at $K = \mathbb{C}$. Say $a : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ such that $a\Lambda_1 \subseteq \Lambda_2$ is an analytic group homomorphism. We have

$$N(a) = [\Lambda_2 : a\Lambda_1] = |\ker a| .$$

Hence, $\Lambda_2/a\Lambda_1$ is a group of order $N(a)$. So $N(a)\Lambda_2 \subseteq a\Lambda_1$, whence

$$\frac{N(a)}{a}\Lambda_2 \subseteq \Lambda_1.$$

Set $\bar{a} = \frac{N(a)}{a}$. Then $\bar{a}\Lambda_2 \subseteq \Lambda_1$. So $\bar{a}$ defines an analytic group homomorphism

$$\bar{a} : \mathbb{C}/\Lambda_2 \to \mathbb{C}/\Lambda_1.$$

This is the dual isogeny to a.

III.6 2013-10-16

References:

- Lorenzini, *An Invitation to Arithmetic Geometry.*
- Stichtenoth, *Algebraic Function Fields and Codes.*

Let $E : y^2 = f(x)$ be an elliptic curve over K. Then

$$\overline{K}(E) = \overline{K}(x)[\sqrt{f(x)}].$$

III.6.1 Function fields of projective curves

We can study smooth projective curves over a field K via function fields. There is a dictionary between maps of curves

$$C_1 \xrightarrow{\phi} C_2$$

and maps of the corresponding function fields

$$\overline{K}(C_2) \xhookrightarrow{\phi^*} \overline{K}(C_1).$$

The map from curve maps to function field maps is easy. The map in the other direction recovers the curve as the "places, valuations, or primes" of the function field.

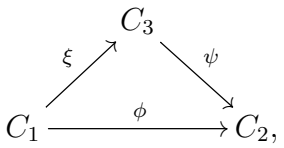
Note III.6.1. The map of curves is either constant or surjective. (This is an analogue of what we saw for compact Riemann surfaces.)

We can decompose the map of function fields into

$$\overline{K}(C_2) \hookrightarrow \overline{K}(C_2)^{\text{sep}} \hookrightarrow \overline{K}(C_1),$$

where the first map is separable of degree $[\overline{K}(C_1) : \overline{K}(C_2)]_{\text{sep}}$ and the second is purely inseparable of degree $[\overline{K}(C_1) : \overline{K}(C_2)]_{\text{insep}}$.

Hence, there is another curve C_3 such that $\phi : C_1 \to C_2$ factors as



where ψ is a *separable map*, and $\chi = (\text{Frob})^e$ is a *purely inseparable map*. (The terms for field extensions are translated to the terms for curves.)

Remark III.6.2 (Algebraic number theory). We have the usual relation

$$\sum_{i=1}^{r} e_i f_i = n.$$

Since $\overline{K}$ is algebraically closed, $f_i = 1$. So

$$\sum_{i=1}^{r} e_i = n,$$

and ϕ is a $(\deg_s \phi)$-to-1 map.

III.6.2 Examples of maps of curves

Example III.6.3. Let $K = \mathbb{F}_q$, and consider the map

$$\begin{aligned} \mathbb{P}^1 &\xrightarrow{\phi} \mathbb{P}^1 \\ t &\mapsto t^q. \end{aligned}$$

Let $c \in \overline{K}$. How many preimages are there? For some $a \in \overline{K}$,

$$t^q - c = (t - a)^q,$$

so $|\phi^{-1}(c)| = 1$. Note that t is a root of $x^q - t^q = 0$. Thus,

$$\overline{K}(t^q) \hookrightarrow \overline{K}(t)$$

is purely inseparable of degree $q = \deg \phi$.

Example III.6.4. Let E be an elliptic curve over K, and suppose $\operatorname{char} K = p > 0$. For $E^{(p)}$, replace each coefficient a_i by a_i^p: for example,

$$\begin{aligned} E &: y^2 = x^3 + ax + b, \\ E^{(p)} &: y^2 = x^3 + a^p x + b^p. \end{aligned}$$

(If $K = \mathbb{F}_p$, then $E^{(p)} = E$.) Consider the map

$$\begin{aligned} E &\xrightarrow{\phi} E^{(p)}, \\ (x : y : 1) &\mapsto (x^p : y^p : 1), \\ (0 : 1 : 0) &\mapsto (0 : 1 : 0). \end{aligned}$$

Then $|\phi^{-1}(P)| = 1$ for all $P \in E^{(p)}$.

Observe that

$$\Delta(E^{(p)}) = \Delta(E)^p \neq 0,$$

so $E^{(p)}$ is an elliptic curve. Moreover,

$$\overline{K}(E)^p = \left\{ f^p \;\middle|\; f \in \overline{K}(E) \right\} = \overline{K}(E^{(p)}) \xhookrightarrow{\phi^*} \overline{K}(E).$$

In fact, if $y^2, y^p \in \overline{K}(E)^p(x)$, then $y \in \overline{K}(E)^p(x)$ (assuming p is odd). So

$$\overline{K}(E) = \overline{K}(E)^p * (x),$$

whence $\deg \phi^* = p$.

Example III.6.5. Let $E : y^2 = f(x)$ be an elliptic curve, and consider the map of curves

$$\begin{aligned} E &\xrightarrow{2} \mathbb{P}^1 \\ (x, y) &\mapsto x. \end{aligned}$$

This is degree 2. The map of function fields is

$$\begin{aligned} \overline{K}(\mathbb{P}^1) &\hookrightarrow \overline{K}(E) \\ \overline{K}(x) &\xhookrightarrow{2} \overline{K}(x)[\sqrt{f(x)}]. \end{aligned}$$

III.6.3 Additivity of isogenies

Theorem III.6.6. *If $\phi : E_1 \to E_2$ is an isogeny, then for all $P, Q \in E_1$,*

$$\phi(P + Q) = \phi(P) + \phi(Q).$$

Preliminaries:

Definition III.6.7 (Divisors)**.** The group of *divisors* on E is

$$\mathrm{Div}(E) = \text{free abelian group on points of } E = \left\{ \sum_{P \in E} n_P P \;\middle|\; n_P = 0 \text{ for all but finitely many } P \right\}.$$

This contains the group of degree zero divisors,

$$\mathrm{Div}^0(E) = \left\{ D \in \mathrm{Div}(E) \;\middle|\; \sum n_P = 0 \right\}.$$

This in turn contains the group of *principal divisors*

$$\mathrm{Div}^1(E) = \text{“principal divisors”} = \left\{ \mathrm{div}(f) \;\middle|\; f \in \overline{K}(E)^* \right\} \cup \{0\},$$

where

$$\mathrm{div}(f) = \sum_{P \in E} \mathrm{ord}_P(f) P,$$

where $\mathrm{ord}_P(f)$ is the order of vanishing of f at P.

We have an exact sequence

$$\begin{aligned} 1 \to \overline{K}^* \to \overline{K}(E)^* \to \mathrm{Div}^0(E) \to \mathrm{Div}^0(E)/\mathrm{Div}^1(E) \to 1 \\ f \mapsto \mathrm{div}(f) \end{aligned}$$

Remark III.6.8. The group

$$\mathrm{Pic}^0(E) \stackrel{\mathrm{def}}{=} \mathrm{Div}^0(E)/\mathrm{Div}^1(E)$$

is important!

Fact III.6.9. By Riemann–Roch, the map

$$\begin{aligned} &E \to \mathrm{Pic}^0(E), \\ &P \mapsto (P) - (0) \pmod{\mathrm{Div}^1(E)} \end{aligned}$$

is bijective. We will see later that this induces the *same* group structure on E. In other words, this is an isomorphism of groups.

Given a map $\phi : E_1 \to E_2$, we get maps

$$\begin{aligned} \phi_* : \mathrm{Div}(E_1) &\to \mathrm{Div}(E_2), & \phi^* : \mathrm{Div}(E_2) &\to \mathrm{Div}(E_1), \\ P &\mapsto \phi(P), & P &\mapsto \sum_{Q \in \phi^{-1}(P)} e_\phi(P) Q. \end{aligned}$$

One can check that ϕ_* and ϕ^* send degree zero divisors to degree zero divisors, and send principal divisors to principal divisors.

Thus, we get an induced map

$$E_2 \xrightarrow{\simeq} \mathrm{Pic}^0(E_2) \xrightarrow{\phi^*} \mathrm{Pic}^0(E_1) \xrightarrow{\simeq} E_1.$$

This is the dual isogeny. (We will fill in more details next time.)

III.7 2013-10-18

III.7.1 Results still not proved

Monday (IOU's):

(1) Centrality of $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$

(2) p is inseparable in characteristic p

(3) $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$

(4) $E \xrightarrow{\simeq} \mathrm{Pic}^0(E)$

(5) $\overline{\phi + \psi} = \overline{\phi} + \overline{\psi}$

(6) $\phi : C_1 \to C_2$ constant or surjective, and $|\phi^{-1}(Q)| = \deg_s \phi$

III.7.2 Additivity of isogenies

We will prove the theorem from last time:

Theorem III.7.1. *If $\phi : E_1 \to E_2$ is an isogeny, then for all $P, Q \in E_1$,*

$$\phi(P + Q) = \phi(P) + \phi(Q).$$

Proof. The following diagram commutes:

$$\begin{array}{ccc} E_1 & \xrightarrow{\simeq} & \mathrm{Pic}^0(E_1) \\ {\scriptstyle\phi}\downarrow & & \downarrow \\ E_2 & \longrightarrow & \mathrm{Pic}^0(E_2), \end{array}$$

where the map $E_1 \xrightarrow{\simeq} \mathrm{Pic}^0(E)$ is given by

$$P \mapsto (P) - (0),$$

and the map $\mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2)$ is induced by

$$\begin{aligned} \mathrm{Div}(E_1) &\to \mathrm{Div}(E_2), \\ (P) &\mapsto \big(\phi(P)\big). \end{aligned}$$

Since the above map is a group homomorphism, so is ϕ. □

Corollary III.7.2. *If $\phi : E_1 \to E_2$ is a nonzero isogeny, then*

$$\ker \phi = \phi^{-1}(0)$$

is a finite subgroup of E_1.

Proof. $|\ker \phi| \leq \deg \phi$, which is finite. □

III.7.3 Degree and kernel of isogenies

Recall: to show Hasse's theorem, we need $\mathrm{End}(E)$ to be a ring with Rosati involution, and

$$N_r = |\ker(1-\pi^r)| = \deg(1-\pi^r),$$

where π is the Frobenius endomorphism.

Theorem III.7.3. *Let $\phi : E_1 \to E_2$ be a nonzero isogeny.*

(a) For every $Q \in E_2$, $|\phi^{-1}(Q)| = \deg_s(\phi)$.

(b) There is an isomorphism

$$\begin{aligned} \ker\phi &\to \mathrm{Gal}\big(\overline{K}(E_1)/\overline{K}(E_2)\big) \\ T &\mapsto \tau_T^*, \end{aligned}$$

where $\tau_T : E_1 \to E_1$ is translation by T.

(c) Suppose ϕ is separable. Then for all $Q \in E_2$,

$$\left|\phi^{-1}(Q)\right| = \deg\phi,$$

so ϕ is "unramified".

Proof. (a) We know this for all but finitely many Q. Given Q', pick R such that $\phi(R) = Q' - Q$. For all $P \in \phi^{-1}(P)$,

$$\phi(P+R) = \phi(P) + \phi(R) = Q + Q' - Q = Q'.$$

Hence, we have a bijection

$$\begin{aligned} \phi^{-1}(Q) &\to \phi^{-1}(Q'), \\ P &\mapsto P + R. \end{aligned}$$

□

(b) [Exercise.]

Remark III.7.4. In particular, taking $Q = 0$,

$$|\ker\phi| = \deg\phi.$$

The isogeny $\phi : E_1 \to E_2$ induces a homomorphism

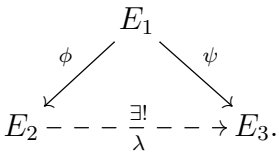
$$\overline{K}(E_2) \overset{\phi^*}{\hookrightarrow} \overline{K}(E_1).$$

We have

$$\left|\mathrm{Gal}\big(\overline{K}(E_1)/\overline{K}(E_2)\big)\right| = |\ker\phi| = \deg\phi = \left[\overline{K}(E_1) : \overline{K}(E_2)\right],$$

so $\overline{K}(E_1)/\overline{K}(E_2)$ is Galois.

Theorem III.7.5. *Suppose $\phi : E_1 \to E_2$ and $\psi : E_1 \to E_3$ are nonzero isogenies, ϕ is separable, and $\ker\phi \subseteq \ker\psi$. Then there is a unique isogeny $\lambda : E_2 \to E_3$ such that $\psi = \lambda\phi$.*



Proof. Since $\ker\phi \subseteq \ker\psi$, every element of $\mathrm{Gal}(\overline{K}(E_1)/\overline{K}(E_2))$ fixes $\psi^*(\overline{K}(E_3))$. Thus, we get an injection $\overline{K}(E_3) \hookrightarrow \overline{K}(E_2)$, which corresponds to an isogeny $\lambda : E_2 \to E_3$. □

Theorem III.7.6. *Let $\phi : E_1 \to E_2$ be a nonzero isogeny of degree m.*

(a) There is a unique isogeny $\overline{\phi} : E_2 \to E_1$ such that $\overline{\phi}\phi = m$.

(b) $\overline{\phi}$ is the composition

$$E_2 \xrightarrow{\simeq} \mathrm{Pic}^0(E_2) \to \mathrm{Pic}^0(E_1) \xrightarrow{\simeq} E_1,$$
$$(P) \mapsto (\deg_i \phi)(Q_1 + \cdots + Q_r),$$

where $\phi^{-1}(P) = \{Q_1, \ldots, Q_r\}$.

Proof. (a) Uniqueness: Say $\psi\phi = m\chi\phi$. Then $(\psi - \chi)\phi = 0$. But ϕ is surjective, so $\psi - \chi = 0$, hence $\psi = \chi$.

Existence: By the dictionary between isogenies and function field homomorphisms, $\phi = \psi\,\mathrm{Frob}^e$, where ψ is separable. Suppose we have proven existence for $\phi : E_1 \to E_2$ and $\psi : E_2 \to E_3$. So we have $\overline{\phi} : E_2 \to E_1$ such that $\overline{\phi}\phi = \deg\phi$, and $\overline{\psi} : E_3 \to E_2$ such that $\overline{\psi}\psi = \deg\psi$. Then

$$(\overline{\phi}\overline{\psi})\psi\phi = \overline{\phi}(\deg\psi)\phi = (\deg\phi)(\deg\psi) = \deg(\phi\psi),$$

whence $\overline{\psi}\overline{\phi} = \overline{\phi\psi}$. We are now reduced to showing the separable and the Frobenius cases.

If ϕ is separable, we proceed à la $\mathbb{C}$: $m = \deg\phi = |\ker\phi|$, so $\ker\phi \subseteq E[m] = \ker m$, whence $m = \overline{\phi}\phi$ for some $\overline{\phi}$.

For the Frobenius case, write $\phi = \psi\phi^e$, where ϕ is the Frobenius. We have $\deg\phi = p = (\psi\phi^{e-1})\phi$, so $\psi\phi^{e-1} = \overline{\phi}$.

(b) Check the given composition $\hat{\phi}$ satisfies $\hat{\phi}\phi = m$. □

III.7.4 Rosati involution of isogenies

We're getting a ring with Rosati involution.

Take $E_1 = E_2 = E_3 = E$. If $\phi = 0$, set $\overline{\phi} = 0$. So far, we have $\overline{\phi} \in \mathrm{End}(E)$ with $\overline{\phi}\phi = \deg\phi$. Also,

$$(\phi\overline{\phi})\phi = \phi(\deg\phi) = (\deg\phi)\phi \implies (\phi\overline{\phi} - \deg\phi)\phi = 0,$$

so since ϕ is surjective, $\phi\overline{\phi} = \deg\phi$.

Likewise, $\overline{\overline{\phi}} = \phi$, $\deg\overline{\phi} = \deg\phi$, and $\overline{\phi\psi} = \overline{\psi}\overline{\phi}$.

The hard part is (5). Given (5), $\overline{1} = 1$, so $\overline{m} = m$ for all $m \in \mathbb{Z}$. We will finish this on Monday.

III.8 2013-10-21

III.8.1 Historical note

Let C be a smooth, projective curve over $\mathbb{F}_q$. Before Hasse, various results showed that

$$||C(\mathbb{F}_q)| - (q+1)| \leq Kq^\alpha,$$

where K is independent of α, and $\frac{1}{2} < \alpha < 1$.

In 1932, Hasse observed that Artin's "Riemann hypothesis" for finite fields implies that $\alpha = \frac{1}{2}$ should be possible.

In 1934, Hasse proved this for $g = 1$, using an analogue of complex multiplication theory for elliptic functions. He and Deuring observed that $g \geq 2$ would require more algebraic geometry.

III.8.2 IOUs from previous classes

(1) Centrality of $\mathbb{Z} \to \mathrm{End}(E)$

(2) p is inseparable in characteristic p

(3) $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$

(4) $E \xrightarrow{\simeq} \mathrm{Pic}^0(E)$

(5) $\overline{\phi + \psi} = \overline{\phi} + \overline{\psi}$

(6) Nonconstant $\phi : C_1 \to C_2$ is surjective, and counting multiplicity, $|\phi^{-1}(Q)| = \deg_s \phi$.

Let's start proving these:

(1) Since ϕ is a homomorphism, $\phi(2P) = 2\phi(P)$, so $\phi(mP) = m\phi(P)$ by induction. Hence, the image of $\mathbb{Z}$ in $\mathrm{End}(E)$ is contained in the center. □

III.8.3 The invariant differential

Let us make a brief aside about the invariant differential. Assume E has Weierstrass form. Then the *invariant differential* of E is

$$\omega = \frac{dx}{2y + a_1 x + a_3}.$$

Define $(\phi^*\omega)(P) = \omega(\phi(P))$, so, for instance,

$$(\tau_Q^*\omega)(P) = \omega(\tau_Q(P)) = \omega(P+Q).$$

Claim III.8.1. *If $Q \in E$, then $\tau_Q^*\omega = \omega$.*

In other words,

$$\frac{dx(P+Q)}{2y(P+Q) + a_1 x(P+Q) + a_3} = \frac{dx(P)}{2y(P) + a_1 x(P) + a_3}.$$

This can be checked by brute force. (Silverman proves this claim in detail.)

III.8.4 Inseparability in characteristic p

We now prove (2).

Claim III.8.2. *If $\phi, \psi : E \to E$ are isogenies, then*

$$(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega.$$

Proof outline. Set $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$. A painful calculation (again, details in Silverman) implies that

$$\omega(x_3, y_3) = \omega(x_1, y_1) + \omega(x_2, y_2).$$

Let $(x, y) \in E$. Set $(x_1, y_1) = \phi(x, y)$, $(x_2, y_2) = \psi(x, y)$, and $(x_3, y_3) = (\phi + \psi)(x, y)$. Then it follows that

$$\omega \circ (\phi + \psi) = \omega \circ \phi + \omega \circ \psi,$$

i.e.,

$$(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega. \qquad \square$$

Corollary III.8.3. *Since $1^*\omega = \omega$, by the last claim, $m^*\omega = m\omega$.*

Corollary III.8.4. *If $\operatorname{char} K = p > 0$, then $p^*\omega = p\omega = 0$.*

Now we need a general result:

Proposition III.8.5 ([Sil], p. 35)**.** *ψ is separable $\iff$ $\psi^*\omega \neq 0$.*

It follows that multiplication by p is inseparable in characteristic $p > 0$.

III.8.5 Injectivity of $\mathbb{Z} \hookrightarrow \operatorname{End}(E)$

In this section, for clarity of notation, we denote the multiplication-by-m isogeny by $[m]$.

Given an integer $m \neq 0$, there exists $P \in E$ such that $[m]P \neq 0$. We divide the proof into cases:

(i) $m = 2$: Suppose $2P = 0$. Then P satisfies

$$4x^3 + b_2x^2 + 2b_4x + b_6 = 0,$$

where b_2, b_4, b_6 are expressions in a_1, a_2, a_3, a_4, a_6. If $\operatorname{char} K \neq 2$, this has at most 3 roots. If $\operatorname{char} K = 2$, then we're fine unless $b_2 = 0 = b_6$, but this would imply $\Delta = 0$.

(ii) $m > 2$: Factor m as $m = 2^{r_1}3^{r_2} \cdot \ldots$. If the isogeny $[m]$ is zero, then the isogeny $[p]$ is zero for some prime factor p of m. (Indeed, if $[mn] = 0$, then $\deg([m])\deg([n]) = \deg([mn]) = 0$, so one of the isogenies $[m], [n]$ is zero.)

So we are reduced to the case where m is an odd prime. We divide this into subcases:

$\operatorname{char} K \neq 2$ There exists $Q \in E$ such that $Q \neq 0$ and $2Q = 0$. So if $[m] = 0$, then $mQ = 0$, implying $Q = 0$, a contradiction.

$\operatorname{char} K = 2$ We have $[m]^*\omega = m\omega \neq 0$, so $[m] \neq 0$.

This proves that $\mathbb{Z} \to \operatorname{End}(E)$ is injective. $\square$

III.8.6 Isomorphism with the Picard group

For each $D \in \mathrm{Div}(E)$, denote

$$L(D) = \left\{ f \in \overline{K}(E)^* \;\middle|\; \mathrm{div}(f) \geq -D \right\} \cup \{0\},$$

where $\mathrm{div}(f) = \sum_{P \in E} \mathrm{ord}_P(f) \cdot (P)$.

By the Riemann–Roch theorem, if $\deg(D) = 0$, then $\dim(L(D + (0))) = 1$.

Claim III.8.6. *If $D \in \mathrm{Div}^0(E)$, then there is a unique point $P \in E$ such that $D \sim (P) - (0)$.*

Proof. Say $f \neq 0$ lies in $L(D + (0))$. This is equivalent to

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

But $\mathrm{div}(f)$ has degree 0, and $-D - (0)$ has degree -1. Thus, there exists $P \in E$ such that

$$\mathrm{div}(f) = -D - (0) + (P),$$

so $D \sim (P) - (0)$. This proves existence.

To show uniqueness, suppose $D \sim (P') - (0)$. Then $(P') \sim (P)$, so there exists f such that

$$\mathrm{div}(f) = (P) - (P').$$

Hence $\mathrm{div}(f) \geq -(P')$, so $f \in L((P'))$, which has dimension 1 by Riemann–Roch.

But constant functions are in $L((P'))$, so $L((P'))$ consists only of constant functions. Thus f is constant, which implies that

$$(P) - (P') = \mathrm{div}(f) = 0.$$

Therefore, $P = P'$. □

Define a map

$$\begin{aligned} \sigma : \mathrm{Div}^0(E) &\to E \\ D &\mapsto \text{unique } P. \end{aligned}$$

This is surjective, since $(P) - (0) \mapsto P$. We will finish the proof next time.

III.9 2013-10-23

[Note: I missed class this day. These notes are from Vladimir Sotirov. —Daniel]

III.9.1 Isomorphism with the Picard group, continued

Let $P, Q \in E$. If

$$x(P+Q) = \lambda^2 + \lambda - a_2 - x_1 - x_2,$$

where $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$, then to obtain $dx(P+Q)$, we differentiate with respect to x_0 (hold Q fixed, vary P).

Last time: we showed that if $D \in \mathrm{Div}^0(E)$, then there exists a unique $P \in E$ such that

$$D \sim (P) - (0) \mod \mathrm{Div}^1(E).$$

(This was done using the fact that if $L(D) = \left\{ f \in \overline{K}(E)^* \mid \mathrm{div}(f) \geq -D \right\} \cup \{0\}$ and $\deg(D) = 1$, then $\dim_{\overline{K}} L(D) = 1$.)

We have $\sigma : \mathrm{Div}^0(E) \to E$ sending $D \mapsto P$ (where P is from the last claim). Suppose $\sigma(D_1) = \sigma(D_2)$. Then

$$D_1 \sim (\sigma(D_1)) - (0) = (\sigma(D_2)) - (0) \sim D_2.$$

So $D_1 \sim D_2$, and conversely. So we get a bijection $\mathrm{Pic}^0(E) \to E$.

Why is this an isomorphism? Let $f(X,Y,Z) = \alpha X + \beta Y + \gamma Z = 0$ be the line in $\mathbb{P}^2$ through P and Q, and let R be the third point of intersection. Let $f'(X,Y,Z) = \alpha' X + \beta' Y + \gamma' Z = 0$ be the line in $\mathbb{P}^2$ through R and 0. Then the third point of intersection is equal to $P+Q$. Then

$$\mathrm{div}(f/Z) = (P) + (Q) + (R) - 3(0),$$
$$\mathrm{div}(f'/Z) = (R) + (P+Q) + (0) - 3(0).$$

So we get

$$\mathrm{div}(f'/f) = \mathrm{div}(f'/Z) - \mathrm{div}(f/Z) = (P+Q) - (P) - (Q) + (0).$$

So $(P+Q) - (P) - (Q) + (0) \in \mathrm{Div}^1(E)$, which implies that

$$(P+Q) - (0) \sim (P) - (0) + (Q) - (0).$$

Thus, we have an isomorphism. □

III.9.2 Last couple facts

We still have two more facts to show:

(5) $\overline{\phi + \psi} = \overline{\phi} + \overline{\psi}$ for isogenies $\phi, \psi : E_1 \to E_2$.

Proof. Let

$$D = \big((\phi+\psi)(x_1,y_1)\big) - \big(\phi(x_1,y_1)\big) - \big(\psi(x_1,y_1)\big) + (0) \in \mathrm{Div}^0(E_2).$$

Then $\sigma(D) = 0$, so D is principal, so $D = \mathrm{div}(f)$, where $f \in \overline{K}(x_1,y_1)(E_2)$. Hence, $f \in \overline{K}(x_1,y_1,x_2,y_2)$, where x_1, y_1 are constants, but x_2, y_2 are variables.

Now we switch perspective and consider x_1, y_1 as variables and x_2, y_2 as constants, and compute $\mathrm{div}(f)$ on E_1. □

(6) $\phi : C_1 \to C_2$ is surjective, and $|\phi^{-1}(Q)| = \deg_s \phi$.

Proof. [Sha], chapter I, §5, theorem 4. □

III.9.3 Proof of the Riemann hypothesis for elliptic curves over finite fields

It remains to prove that

$$N_r := |E(\mathbb{F}_{q^r})| = \deg(1 - \pi^r),$$

where π is the Frobenius map $(x, y) \mapsto (x^q, y^q)$. Let ϕ be the p-th Frobenius map $(x, y) \mapsto (x^p, y^p)$. If $q = p^k$, then $\pi = \phi^k$. We need to show that $1 - \pi^r$ is separable (then the degree is equal to the size of the kernel).

Say $1 - \phi^{rk} = \psi\phi^e$ (where ψ is separable). We want to show $e = 0$. If $e \geq 1$, then

$$(\underbrace{\phi^{rk-1} + \psi\phi^{e-1}}_{\theta})\phi = 1.$$

But then $1 = \deg(1) = \deg(\theta\phi) = (\deg\theta)(\deg\phi) = (\deg\theta) \cdot p$, which is a contradiction.

So, $\deg(1 - \pi^r) = (1 - \pi^r)(\overline{1 - \pi^r}) = 1 - \pi^r - \overline{\pi^r} + (\pi\overline{\pi})^r$. Then

$$Z(T) = \frac{(1 - \pi T)(1 - \overline{\pi}T)}{(1 - T)(1 - \pi\overline{\pi}T)} = \frac{1 - (\operatorname{tr}\pi)T + qT^2}{(1 - T)(1 - qT)}.$$

We showed $|\operatorname{tr}\pi| \leq 2\sqrt{q}$.

III.9.4 Torsion points and separability

Theorem III.9.1. *Suppose* $\operatorname{char} K \nmid m$, *and let* E *be an elliptic curve over* K. *Then*

$$E[m] \cong \mathbb{Z}/m \times \mathbb{Z}/m.$$

Proof. We write the isogeny $[m] = \psi\phi^e$, where ψ is separable. Then

$$m^2 = \deg m = (\deg\psi)(\deg\phi)^e = (\deg\psi)p^e.$$

Since $p \nmid m$, this implies $e = 0$, so m is separable and $\deg_s m = \deg m = m^2$. For all $d \mid m$, we have $|E[d]| = d^2$, so $E[m] \cong \mathbb{Z}/m \times \mathbb{Z}/m$ (see homework). □

Suppose $\operatorname{char} K = p > 0$ and K is perfect (so $x \mapsto x^p$ is surjective). If E is an elliptic curve over K, what is $E[p]$? Well, the isogeny $[p]$ is inseparable, which implies $[p] = \psi\phi^e$. Taking degrees, we get $p^2 = (\deg\psi)p^e$, so $e \leq 2$.

The situation can be summed up as follows:

Theorem III.9.2. *The following are equivalent:*

$e = 2$	$e = 1$
the isogeny $[p]$ *is purely inseparable*	$[p]$ *is inseparable, not purely*
$\overline{\phi} = -\phi$	$\overline{\phi}$ *is separable*
$\phi^2 = -p$	$\phi^n \notin \mathbb{Z}$ *for any* $n > 0$
$\operatorname{tr} \phi = 0$	$\operatorname{tr} \phi \neq 0$
$E[p] = 0$	$E[p] \cong \mathbb{Z}/p$
$\operatorname{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ *is a quaternion algebra*	$\operatorname{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ *is an imaginary quadratic field*
E *is* supersingular	E *is* ordinary

Example III.9.3. Consider the elliptic curve $x^3 + y^3 = z^3$. It has an automorphism of order 3:

$$[x : y : z] \to [\omega x : y : z],$$

where ω is a third root of unity. So E considered as an elliptic curve over $\mathbb{Q}$ has complex multiplication (by $\mathbb{Z}[\omega]$).

Now consider it as an elliptic curve over $\mathbb{F}_p$ for $p \neq 3$. If $p \equiv 2 \pmod 3$, then $x \mapsto x^3$ is a bijection, so counting solutions to $x^3 + y^3 = z^3$ is the same as counting solutions to $u + v = w$. Thus,

$$|E(\mathbb{F}_p)| = p + 1.$$

Since $|E(\mathbb{F}_p)| = p + 1 - \operatorname{tr} \phi$, it follows that E is supersingular at every $p \equiv 2 \pmod 3$.

If $p \equiv 1 \pmod 3$, Gauss proved that

$$|E(\mathbb{F}_p)| = p + 1 - A,$$

where A is the unique integer such that $A \equiv -1 \pmod 3$ and $4p = A^2 + 27B^2$. Hence, E is ordinary at $p \equiv 1 \pmod 3$.

III.10 2013-10-25

III.10.1 Supersingular curves

Theorem III.10.1. *Suppose K is a perfect field,* $\operatorname{char} K = p > 0$*, and E is an elliptic curve over K. The following are equivalent:*

(1) $E[p] = 0$.

(2) $[p]$ *is a purely inseparable isogeny, and* $j(E) \in \mathbb{F}_{p^2}$.

(3) $\overline{\phi}$ *is a purely inseparable isogeny.*

(4) $\operatorname{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ *is a quaternion algebra.*

(5) $\operatorname{tr} \phi \equiv 0 \pmod p$*, where ϕ is given by*

$$E \xrightarrow{\phi} E^{(p)},$$
$$(x, y) \mapsto (x^p, y^p).$$

In this case, we call E supersingular*, else E is* ordinary*.*

Proof. We know already that ϕ is a purely inseparable isogeny of degree p. Write $[p] = \overline{\phi}\phi$, where $\overline{\phi} : E^{(p)} \to E$. Any isogeny can be factored as $\psi\phi^e$ (where ψ is separable).

(a) $\iff$ **(c)** $|E[p]| = |\ker[p]| = \deg_s p = (\deg_s \overline{\phi})(\deg_s \phi) = \deg_s \overline{\phi}$ since ϕ is purely inseparable. Hence,

$$p = \deg \overline{\phi} = (\deg_s \overline{\phi})(\deg_i \overline{\phi}).$$

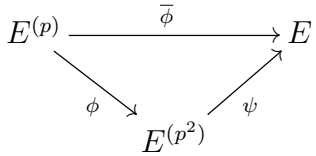
Two possibilities:

(i) $\deg_i \overline{\phi} = p,\ \deg_s \overline{\phi} = 1 \iff \overline{\phi}$ is purely inseparable.

(ii) $\deg_i \overline{\phi} = 1,\ \deg_s \overline{\phi} = p \iff \overline{\phi}$ is separable.

In case (i), $|E[p]| = 1 \iff E[p] = 0$. In case (ii), $|E[p]| = p \iff E[p] \cong \mathbb{Z}/p$.

(c) $\iff$ **(b)** $p = \overline{\phi}\phi$, ϕ purely inseparable implies that p is purely inseparable $\iff$ $\overline{\phi}$ is purely inseparable. Consider the diagram



In case (b), $\overline{\phi} = \psi\phi^d$ for some d. Since $\overline{\phi}$ is purely inseparable, $d \geq 1$. So

$$p = \deg \overline{\phi} = (\deg \psi)(\deg \phi)^d = (\deg \psi)p^d,$$

hence $d = 1$ and $\deg \psi = 1$, so ψ is an isomorphism. Finally,

$$j(E) = j(E^{(p^2)}) = j(E)^{p^2},$$

thus $j(E) \in \mathbb{F}_{p^2}$.

(c) $\iff$ **(e)** $\operatorname{tr} \phi = \phi + \overline{\phi}$, so $\overline{\phi} = \operatorname{tr} \phi - \phi$. Recall that ψ is separable $\iff$ $\psi^*\omega \neq 0$ (where ω is the invariant differential). So $\overline{\phi}$ is inseparable iff

$$0 = \overline{\phi}^*\omega = -\phi^*\omega + (\operatorname{tr} \phi)^*\omega = (\operatorname{tr} \phi)^*\omega = (\operatorname{tr} \phi)\omega$$

iff $\operatorname{tr} \phi \equiv 0 \pmod{p}$. (Recall that $[m]^*\omega = m\omega$ for $m \in \mathbb{Z}$.)

The proof of equivalence of (d) is omitted. □

III.10.2 Examples of supersingular curves

Suppose E is an elliptic curve over $\mathbb{F}_p$ (p prime). We have

$$|E(\mathbb{F}_p)| = p + 1 - \operatorname{tr}\phi,$$

so E is supersingular $\iff |E(\mathbb{F}_p)| \equiv 1 \pmod{p}$.

By Hasse's theorem, $|\operatorname{tr}\phi| \leq 2\sqrt{p}$. So if $p \geq 5$, then $\operatorname{tr}\phi \equiv 0 \pmod{p} \iff \operatorname{tr}\phi 0$. Hence, for $p \geq 5$, E is supersingular $\iff |E(\mathbb{F}_p) = p + 1|$.

Example III.10.2. Last time, we considered $E : x^3 + y^3 = z^3$ for $p \neq 3$.

- If $p \equiv 2 \pmod{3}$, then $|E(\mathbb{F}_p)| = p + 1$, so E is supersingular over $\mathbb{F}_p$.
- If $p \equiv 1 \pmod{3}$, then $|E(\mathbb{F}_p)| \neq p + 1$, so E is ordinary over $\mathbb{F}_p$.

Example III.10.3. The curve $E : y^2 = x^3 - x$ has CM by $\mathbb{Z}[i]$, so

$$(x, y) \overset{\phi}{\mapsto} (-x, iy)$$

has order 4. Also, E is an elliptic curve over $\mathbb{F}_p$, so long as $p \neq 2$.

- If $p \equiv 3 \pmod{4}$, then $|E(\mathbb{F}_p)| = p + 1$, so E is supersingular over $\mathbb{F}_p$.
- If $p \equiv 1 \pmod{4}$, then $|E(\mathbb{F}_p)| = p + 1 - 2\operatorname{Re} J(\chi, \chi^2) \neq p + 1$, so E is ordinary over $\mathbb{F}_p$.

Remark III.10.4. In each of the preceding two examples, p is insert in the CM field in the supersingular case, and split in the CM field in the ordinary case. These examples are shown in detail in [IR].

What about $y^2 + y = x^3 - x$? We find it's supersingular for

$$p = 2, 3, 17, 19, 257, 311, 577, \ldots$$

Theorem III.10.5 (Elkies, PhD thesis, 1987)**.** *Every elliptic curve over $\mathbb{Q}$ has infinitely many supersingular primes.*

Serre, earlier, had shown that the set of supersingular primes has density 0 if the curve does not have CM.

Conjecture III.10.6 (Lang–Trotter)**.** *Say E is an elliptic curve over $\mathbb{Q}$ without CM. Then*

$$\left|\left\{p < x \;\middle|\; E \text{ supersingular at } p\right\}\right| \sim \frac{c_E\sqrt{x}}{\log x}.$$

Remark III.10.7 (How to prove that $y^2 + y = x^3 - x$ has no CM). Idea: $\operatorname{End}(E)$ acts as endomorphisms of $E[m]$, and $G_{\mathbb{Q}} = \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E[m]$. Let K be a CM field of E (assuming it exists).

Claim. $\phi\sigma = \sigma\phi$ *for all* $\phi \in \operatorname{End}(E)$ *and* $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/K)$.

Example III.10.8. Consider $E : y^2 = x^3 - x$, and let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Then

$$\begin{aligned}\phi(x,y) &= (-x, iy)\\ \sigma\phi(x,y) &= \big(-\sigma(x), \sigma(iy)\big) = \big(-\sigma(x), i\sigma(y)\big)\\ &= \phi(\sigma x, \sigma y) = \phi\sigma(x,y).\end{aligned}$$

Key point: Isogenies are defined over the CM field. ([Shi], p. 114)

Strategy: let $\tilde{\phi} \in \mathrm{End}(E[3])$ be induced by ϕ, and $\tilde{\sigma} \in \mathrm{GL}_2(\mathbb{Z}/3) = \mathrm{Aut}(E[3])$ the image of σ. Then $\tilde{\sigma}\tilde{\phi} = \tilde{\phi}\tilde{\sigma}$.

If we show the image in $\mathrm{GL}_2(\mathbb{Z}/3)$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ is large, then $\tilde{\phi}$ is scalar, a contradiction.

Chapter IV

L-functions of Elliptic Curves over $\mathbb{Q}$

IV.1 2013-10-28

IV.1.1 Curves without CM

To show a curve $E/\mathbb{Q}$ does not have CM: $\phi \in \mathrm{End}(E)$ and $\sigma \in G_{\mathbb{Q}}$ both act on $E[m]$. Suppose K is the CM field of E.

Claim IV.1.1. *If $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$, then $\phi\sigma = \sigma\phi \in \mathrm{End}(E[m])$.*

Upshot: if the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ in $\mathrm{GL}_2(\mathbb{Z}/m)$ is "large", then the action of ϕ is scalar, a contradiction.

We have representations associated to E (an elliptic curve over $\mathbb{Q}$):

$$\rho_m : G_{\mathbb{Q}} \to \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m)$$

(since $E[m] \cong \mathbb{Z}/m \times \mathbb{Z}/m$).

Fact IV.1.2. If E has CM by K, then the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/K) = G_K$ is abelian (contained in a *Cartan subgroup*).

Hence, the image of $G_{\mathbb{Q}}$ has an abelian subgroup of index 1 or 2 (contained in the normalizer of a Cartan subgroup).

Remark IV.1.3 (Cartan subgroups). There are two types of Cartan subgroups:

(1) split Cartan, order $(p-1)^2$:
$$\left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\}$$

(2) nonsplit Cartan, order $p^2 - 1$:
$$\mathbb{F}_{p^2}^{\times} \hookrightarrow \mathrm{GL}_2(\mathbb{F}_p)$$

Aside IV.1.4 (Kronecker's Jugendtraum). What about other K? We want to describe finite abelian extensions L/K. In the case $K = \mathbb{Q}$, the Kronecker–Weber theorem yields $L \leq \mathbb{Q}(\zeta_m)$. CM elliptic curves do this for imaginary quadratic K.

IV.1.2 Frequency of certain types of elliptic curves

A few remarks:

(1) If $j(E) \in \mathbb{F}_{p^2}$ for E supersingular in characteristic p, then there are only finitely many supersingular elliptic curves in characteristic p up to isomorphism over $\overline{K}$.

(2) CM curves over $\mathbb{Q}$ are rare, corresponding to only 13 j-invariants. If $E/\mathbb{Q}$ has CM, then $j(E) \in \mathbb{Z}$.

(3) For a density 1 collection of $A, B \in \mathbb{Z}$, the curve $E : y^2 = x^3 + Ax + B$ has ρ_m surjective for all m.

IV.1.3 Reduction of curves

Be careful about reduction!

Example IV.1.5. The curve $y^2 = x^3 + 16$ has discriminant $\Delta = -2^{12} \cdot 3^3$. It does *not* define an elliptic curve mod 2 and mod 3, but it does mod p for all $p > 3$.

But, let us make some substitutions: $x = 4x'$ and $y = 8y' + 4$. This gives us an elliptic curve

$$E' : (y')^2 + y' = (x')^3,$$

which has discriminant $\Delta = -3^3$. This *does* define an elliptic curve mod 2.

We say that E has *good reduction* at 2, since $E \cong E'$ over $\mathbb{Q}$, and E' has good reduction at 2. (The *model* has bad reduction at 2, but the curve intrinsically has good reduction at 2.)

We should suspect this might happen by considering the change of variables $x = u^2x'$ and $y = u^3y' + c$, which changes the discriminant by u^{12}.

Definition IV.1.6. We say that $E/\mathbb{Q}$ has *good reduction* at a prime p if there exists $E' \cong E$ over $\mathbb{Q}$ such that $E' \pmod p$ is an elliptic curve. Otherwise, we say E has *bad reduction*.

We will soon develop this theory more formally via minimal models.

IV.1.4 L-functions of elliptic curves over $\mathbb{Q}$

Let E be an elliptic curve over $\mathbb{Q}$, and let p be a prime of good reduction.

Look at $E/\mathbb{F}_p$. It has the zeta function

$$Z(T) = \frac{1 - a_pT + pT^2}{(1 - T)(1 - pT)},$$

where $|E(\mathbb{F}_p)| = p + 1 - a_p$, and $|a_p| \leq 2\sqrt{p}$.

Definition IV.1.7. Define the *L-series* of E by

$$L(E, s) = \prod_{p \text{ good}} \frac{1}{(1 - a_pp^{-s} + pp^{-2s})} \prod_{p \text{ bad}} \frac{1}{(1 - a_pp^{-s})} = \sum_{n=1}^{\infty} \frac{c_n}{n^s},$$

where for p bad,

$$a_p = \begin{cases} 1 & \text{if } E/\mathbb{F}_p \text{ has a node with tangent slopes} \in \mathbb{F}_p, \\ -1 & \text{if } E/\mathbb{F}_p \text{ has a node with tangent slopes} \notin \mathbb{F}_p, \\ 0 & \text{if } E/\mathbb{F}_p \text{ has a cusp.} \end{cases}$$

Note IV.1.8. (1) The term coming from p of good reduction comes from $T \mapsto p^{-s}$ in the zeta function.

(2) For p prime, $c_p = a_p$. Moreover, $c_1 = 1$.

IV.1.5 Examples of L-series

Example IV.1.9. Consider $E : y^2 = x^3 - x = x(x+1)(x-1)$. This has good reduction at every $p > 2$.

What if $p = 2$? We have $a_3 = 0,\ a_5 = -2,\ a_7 = 0,\ a_{11} = 0,\ a_{13} = 16, \ldots$. (We can see that $a_p = 0$ for $p \equiv 3 \pmod 4$ because E has CM by $\mathbb{Q}(i)$.) In projective coordinates, the curve is

$$y^2 z = x^3 - xz^2,$$

which has a singularity at $(1:0:1)$ in characteristic 2.

Translate the singularity to $(0:0:1)$. Set $u = x - 1$. Then

$$y^2 = (u+1)^3 - (u+1) = u^3 + u^2.$$

To see whether this has a node or a cusp, look at the leading quadratic factors. It has a node $\iff$ the quadratic has distinct factors. But, since we are in characteristic 2,

$$y^2 - u^2 = (y-u)(y+u) = (y+u)^2.$$

So $E/\mathbb{F}_2$ has a cusp, and $a_2 = 0$. Hence

$$\begin{aligned} L(E,s) &= \left(\frac{1}{1 - 0 \cdot 2^{-s}}\right)\left(\frac{1}{1 - 0 \cdot 3^{-s} + 3 \cdot 3^{-2s}}\right)\left(\frac{1}{1 + 2 \cdot 5^{-s} + 5 \cdot 5^{-2s}}\right) \cdot \ldots \\ &= 1 - \frac{2}{5^s} - \frac{3}{9^s} + \frac{6}{13^s} + \ldots \end{aligned}$$

Example IV.1.10. Consider $y^2 + y = x^3 - x^2$. Then

$$L(E,s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s},$$

where

$$\sum_{n=1}^{\infty} c_n q^n = q \prod_{n=1}^{\infty} (1-q^n)^2 \left(1 - q^{11n}\right)^2.$$

This, as we will see later, is a modular form.

Remark IV.1.11. We will later show a deep result: Every elliptic curve has bad reduction at some prime.

IV.2 2013-10-30

Let E be an elliptic curve over $\mathbb{Q}$.

IV.2.1 L-series

Last time, we defined an L-series

$$L(E,s) = \prod_{p \text{ good}} \frac{1}{(1 - a_p p^{-s} + p^{1-2s})} \prod_{p \text{ bad}} \frac{1}{(1 - a_p p^{-s})} = \sum_{n=1}^{\infty} \frac{c_n}{n^s},$$

where $c_p = a_p$ for p prime, $c_1 = 1$, and

$$a_p = \begin{cases} p + 1 - |E(\mathbb{F}_p)|, & p \text{ good}, \\ 1, & \text{node with tangent slopes in } \mathbb{F}_p, \\ -1, & \text{node with tangent slopes not in } \mathbb{F}_p, \\ 0, & \text{cusp}. \end{cases}$$

Moreover, if $(m,n) = 1$, then $c_{mn} = c_m c_n$.

Example IV.2.1. For $E : y^2 + y = x^3 - x^2$, we have

$$L(E,s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s},$$

where

$$\sum_{n=1}^{\infty} c_n q^n = q \prod_{n=1}^{\infty} (1 - q^n)^2 \left(1 - q^{11n}\right)^2.$$

IV.2.2 The Taniyama–Shimura conjecture

If f is a cuspform, say $f = \sum_{n=1}^{\infty} c_n q^n$, set

$$L(f,s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s}.$$

Conjecture IV.2.2 (Taniyama–Shimura)**.** *If E is an elliptic curve over $\mathbb{Q}$, then there exists a cuspform of weight 2 and level N such that $L(f,s) = L(E,s)$. (Here, N is the* conductor *of E.)*

This is now a theorem by Breuil, Conrad, Diamond, Taylor, Wiles, et al.

So far, we've met level 1 cuspforms (on the whole of $\mathrm{SL}_2(\mathbb{Z})$). Level N cuspforms transform nicely under

$$\gamma \in \Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod{N} \right\}.$$

For a summary of different forms of the Taniyama–Shimura conjecture, see [Maz].

IV.2.3 Weak Birch–Swinnerton-Dyer conjecture

Set

$$\Lambda(E,s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s).$$

Theorem IV.2.3. *$\Lambda(E,s)$ has an analytic continuation to the whole s-plane such that*

$$\Lambda(E,s) = w\Lambda(E,2-s),$$

where $w = \pm 1$ is the root number.

This is now known by Taniyama–Shimura.

Conjecture IV.2.4 (Weak Birch–Swinnerton-Dyer)**.** *$L(E,s)$ has a zero at $s=1$ of order r, where $r = \operatorname{rank}(E(\mathbb{Q}))$.*

Remark IV.2.5. By the Mordell theorem, which we shall see later in this course, $E(\mathbb{Q})$ is finitely generated.

Remark IV.2.6. The Birch–Swinnerton-Dyer conjecture is a sophisticated "local-to-global" principle. (The strong form of the conjecture also gives information about the leading terms of the Taylor expansion.)

IV.2.4 Minimal Weierstrass models

Let E be an elliptic curve over K.

Definition IV.2.7. An *admissible* change of variables in a Weierstrass equation is given by

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

where $u, r, s, t \in K$ and $u \neq 0$.

One can check that $\Delta' = u^{-12}\Delta$.

Proposition IV.2.8. $E \cong E' \iff j(E) = j(E')$.

If $E \cong E'$, then we can show $j(E) = j(E')$ by brute force calculation. The converse is also a painful calculation, which we illustrate by example:

Example IV.2.9. Consider two elliptic curves

$$\begin{aligned} E &: y^2 = x^3 + Ax + B, \\ E' &: y^2 = x^3 + A'x + B'. \end{aligned}$$

The j-invariant is of the form

$$j(E) = c \cdot \frac{4A^3}{4A^3 + 27B^2}$$

for some constant c (probably involving 1728). We need to find u such that $A' = Au^4$ and $B' = Bu^6$.

Now we can define the minimal Weierstrass form. To avoid difficulties with fields of class number > 1, let us work over $\mathbb{Q}$. Assume the coefficients are integers. Then $\Delta \in \mathbb{Z}$.

Definition IV.2.10. Call the equation *minimal at prime* p if the power of p dividing Δ cannot be decreased by an admissible change of variables. (Hence, if the exponent of p in Δ is < 12, then the equation is minimal at p.)

Call the Weierstrass equation (globally) *minimal* if it is minimal at all primes.

IV.2.5 Convergence of $L(E, s)$

Is the power series $L(E, s)$ convergent? By Hasse,

$$|a_p| \le 2\sqrt{p} \implies |c_n| \ll O(n^{1/2+\varepsilon}).$$

Hence, $L(E, s)$ converges for $\mathrm{Re}(s) > \frac{3}{2}$.

IV.2.6 Birch–Swinnerton-Dyer conjecture

Let $L_p(E, s)$ be the p-th factor of $L(E, s)$. If p is good, then

$$L_p(E, 1) = \frac{1}{1 - a_p p^{-1} + p^{-1}} = \frac{p}{p + 1 - a_p} = \frac{p}{|E(\mathbb{F}_p)|}.$$

If p is bad, then we study the group of nonsingular points $E_{\mathrm{ns}}(\mathbb{F}_p)$, which has order $p - a_p$:

cusp $E_{\mathrm{ns}}(\mathbb{F}_p) \cong \mathbb{F}_p^+$, which has order p.

node, split $E_{\mathrm{ns}}(\mathbb{F}_p) \cong \mathbb{F}_p^\times$, which has order $p - 1$.

node, nonsplit $E_{\mathrm{ns}}(\mathbb{F}_p) \cong \ker(N : \mathbb{F}_{p^2}^\times \to \mathbb{F}_p^\times)$, which has order $p + 1$.

So

$$L_p(E, 1) = \frac{1}{1 - a_p p^{-1}} = \frac{p}{p - a_p} = \frac{p}{|E_{\mathrm{ns}}(\mathbb{F}_p)|}.$$

The Birch–Swinnerton-Dyer heuristic states, roughly, that

$$\mathrm{rank}(E(\mathbb{Q})) > 0 \iff |E(\mathbb{F}_p)| \text{ large on average} \iff \frac{p}{|E(\mathbb{F}_p)|} \text{ small of average} \iff L(E, 1) = 0.$$

IV.3 2013-11-01

IV.3.1 Convergence of L-series

Let E be an elliptic curve over $\mathbb{Q}$. We can bound the terms of the L-series (recall that $|\alpha_p| = \sqrt{p}$):

$$\begin{aligned}
\left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1} &= \left(1 - \alpha_p p^{-s}\right)^{-1} \left(1 - \overline{\alpha_p} p^{-s}\right)^{-1} \\
&= \left(1 + \alpha_p p^{-s} + \alpha_p^2 p^{-2s} + \dots\right) \left(1 + \overline{\alpha_p} p^{-s} + \overline{\alpha_p}^2 p^{-2s} + \dots\right) \\
&= 1 + (\alpha_p + \overline{\alpha_p}) p^{-s} + (\alpha_p^2 + \alpha_p \overline{\alpha_p} + \overline{\alpha_p}^2) p^{-2s} \\
&\quad + \dots + \underbrace{(\alpha_p^k + \alpha_p^{k-1}\overline{\alpha_p} + \dots + \overline{\alpha_p}^k)}_{c_{p^k}} p^{-ks} + \dots
\end{aligned}$$

So $\left|c_{p^k}\right| \leq (k+1)(\sqrt{p})^k = d(p^k)\sqrt{p^k}$.

If $(m,n) = 1$, then $c_{mn} = c_m c_n$. So for all n,

$$|c_n| \leq d(n)\sqrt{p^k}.$$

So $|c_n| \ll \mathrm{O}(n^{1/2+\varepsilon})$, whence

$$\left|\frac{c_n}{n^s}\right| \ll \mathrm{O}(n^{-s+1/2+\varepsilon}).$$

If $\mathrm{Re}(s) > \frac{3}{2}$, choose $\varepsilon > 0$ such that $-s+\frac{1}{2}+\varepsilon < k < -1$. Compare $\sum_{n=1}^{\infty} \frac{c_n}{n^s}$ with $\sum_{n=1}^{\infty} n^k$. So $L(E,s)$ converges absolutely for $\mathrm{Re}(s) > \frac{3}{2}$.

Conjecture IV.3.1 (Hasse)**.** *$L(E,s)$ has an analytic continuation to $\mathbb{C}$.*

Deuring (1941) proved this for elliptic curves with CM; the general case follows from Taniyama–Shimura.

IV.3.2 Birch–Swinnerton-Dyer conjecture

Conjecture IV.3.2 (Weak BSD)**.** *$L(E,s)$ has a zero of order $r_E := \mathrm{rank}(E(\mathbb{Q}))$ at $s = 1$.*

Conjecture IV.3.3 (Strong BSD)**.**

$$\lim_{s\to 1}(s-1)^{-r_E} L(E,s) = |Ш| \frac{\det\langle P_i, P_j\rangle}{[E(\mathbb{Q}) : B]^2} c_\infty \prod_{p \text{ prime}} c_p,$$

where:

- Ш *is the* Tate–Shafarevich group *(conjectured to be finite);*
- $\langle P_i, P_j\rangle$ *is the* "regulator"*;*
- c_∞ *is a small multiple of the period; and*
- c_p *is the p-th* Tanagawa number*.*

Progress:

Theorem IV.3.4 (Coates–Wiles, 1977)**.** *Suppose E has CM. Then $r_E \geq 1$ implies analytic rank $r^{an} \geq 1$ (that is, $L(E,1) = 0$).*

Theorem IV.3.5 (Gross–Vagier, 1986)**.** *Suppose E is modular (i.e., $L(E,s) = L(f,s)$ for some f). Then $r^{an} = 1$ implies $r_E \geq 1$.*

Theorem IV.3.6 (Rubin, 1987)**.** *Suppose E has CM. Then $r^{an} = 0$ implies $r_E = 0$,* Ш *is finite, and BSD holds for E.*

Theorem IV.3.7 (Kolyragin, 1988)**.** *Suppose E is modular (which, by the modularity theorem, is always true). Then $r^{an} = 0$ implies $r_E = 0$ and* Ш *is finite, and $r^{an} = 1$ implies $r_E = 1$ and* Ш *is finite.*

IV.3.3 The conductor and semistability

Definition IV.3.8. The *conductor* of E is the integer $N = \prod_p p^{f_p}$, where

$$f_p = \begin{cases} 0 & \text{if } p \text{ is good,} \\ 1 & \text{if } p \text{ is bad, multiplicative (node) reduction,} \\ \geq 2 & \text{if } p \text{ is bad, additive (cusp) reduction.} \end{cases}$$

(If $p \geq 5$, replace the last case with $f_p = 2$.)

The conductor is the smallest N such that $L(E,s) = L(f,s)$ for f a cuspform of weight 2, level N (transforms under $\Gamma_0(N)$).

Definition IV.3.9. If N is squarefree ($f_p = 1$ for all bad p), then call E *semistable*.

IV.3.4 The functional equation

Recall the completed L-series

$$\Lambda(E,s) \stackrel{\text{def}}{=} \underbrace{N^{s/2}(2p)^{-s}\Gamma(s)}_{L_\infty(E,s)} L(E,s).$$

We have the functional equation

$$\Lambda(E, 2-s) = w_E \Lambda(E,s),$$

where $w = \pm 1$ is the root number.

How does this follow from Taniyama–Shimura?

Let $f(z) = \sum_{n=1}^\infty a_n q^n$ (where $q = e^{2\pi i z}$) be a cuspform, weight k, for $\mathrm{SL}_2(\mathbb{Z})$. In particular, $f(-\frac{1}{z}) = z^k f(z)$. Set

$$g(s) = \int_0^\infty z^{s-1} f(iz)\, dz.$$

This is the *Mellin transform* of f.

Claim IV.3.10. $|a_n| = \mathrm{O}(n^{k/2})$ *(proven next).*

Suppose $\operatorname{Re} s > \frac{k}{2} + 1$. Set $t = 2\pi n z,\ dt = 2\pi n\, dz$. Then

$$\begin{aligned} g(s) &= \int_0^\infty z^{s-1} \Big(\sum_{n=1}^\infty a_n e^{-2\pi n z} \Big)\, dz \\ &= \sum_{n=1}^\infty a_n \int_0^\infty z^{s-1} e^{-2\pi n z}\, dz \\ &= \sum_{n=1}^\infty a_n \int_0^\infty \left(\frac{t}{2\pi n} \right)^{s-1} e^{-t} \frac{dt}{2\pi n} \\ &= \sum_{n=1}^\infty \frac{a_n}{(2\pi n)^s} \Gamma(s) = (2\pi)^{-s}\Gamma(s) L(f,s) = \Lambda(f,s), \end{aligned}$$

where $L(f,s) = \sum_{n=1}^\infty \frac{a_n}{n^s}$.

Theorem IV.3.11. $\Lambda(f, k-s) = (-1)^{k/2}\Lambda(f, s)$.

Proof. We have $f(-\frac{1}{2}) = z^k f(z)$. Set $z = iu$: then

$$f\left(\frac{i}{u}\right) = (-1)^{k/2} u^k f(iu).$$

Thus, setting $z = \frac{1}{u},\ dz = -\frac{1}{u^2}\,du$,

$$\begin{aligned}
\Lambda(f,s) &= \int_0^\infty z^{s-1} f(iz)\,dz \\
&= \int_1^\infty z^{s-1} f(iz)\,dz + \int_\infty^1 \left(\frac{1}{u}\right)^{s-1} f\left(\frac{i}{u}\right)\left(-\frac{1}{u^2}\right)\,du \\
&= \int_1^\infty z^{s-1} f(iz)\,dz + \int_1^\infty \frac{1}{u^{s+1}}(-1)^{k/2} u^k f(iu)\,du \\
&= \int_1^\infty \left[z^{s-1} f(iz) + (-1)^{k/2} z^{k-1-s} f(iz)\right]\,dz.
\end{aligned}$$

The above is invariant under replacing s with $k-s$ if $\frac{k}{2}$ is even, and swaps the sign if $\frac{k}{2}$ is odd. □

Proof of Claim IV.3.10 (Hecke). As $q \to 0$,

$$f(z) = \sum_{n=1}^\infty = \mathrm{O}(q) = \mathrm{O}(e^{-2\pi y}).$$

Set $\phi(z) = |f(z)|\, y^{k/2}$. This is invariant under $\mathrm{SL}_2(\mathbb{Z})$ and continuous on the fundamental domain. Also, $\phi \to 0$ as $y \to \infty$, hence ϕ is bounded on $\mathscr{H}$. Thus, $|f(z)| \le My^{-k/2}$ for some M. Fixing y and letting $0 \le x \le 1$, q follows a circle C of radius $e^{-2\pi y}$. If we write $z = x + iy$, then

$$q = e^{2\pi i z} = e^{2\pi i x} e^{-2\pi y}.$$

Applying Cauchy's integral formula,

$$\begin{aligned}
a_n &= \frac{1}{2\pi i}\int_C f(z) q^{-n-1}\,dq \\
&= \frac{1}{2\pi i}\int_0^1 f(z) q^{-n-1} 2\pi i q\,dz\,dx \\
&= \int_0^1 f(z) q^{-n}\,dx.
\end{aligned}$$

Hence $|a_n| \le My^{-k/2} e^{2\pi n y}$. Set $y = \frac{1}{n}$. Then

$$|a_n| \le M\left(\frac{1}{n}\right)^{-k/2} e^{2\pi} = (\text{const}) \cdot n^{k/2}.$$

□

IV.4 2013-11-04

IV.4.1 Modular functions of weight k

[Thanks to Vladimir Sotirov for the first half of today's notes. —Daniel]

We had that if $f(z) = \sum_{n=1}^{\infty} a_n q^n$ is a cuspform for $\mathrm{SL}_2(\mathbb{Z})$ (level 1) of weight k, and

$$\Lambda(f, s) = (2\pi)^{-s}\Gamma(s)L(f, s),$$

where $L(f, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$, then we have the following:

Theorem IV.4.1 (Hecke)**.** $\Lambda(f, k - s) = (-1)^{k/2}\Lambda(f, s)$.

We want to generalize this. Let

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod{N} \right\},$$
$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0,\ d \equiv 1 \pmod{N} \right\}.$$

Define

$$f \mid [\gamma]_k(z) = (cz + d)^{-k} f(\gamma z),$$

where $\gamma z = \dfrac{az + b}{cz + d}$ if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Definition IV.4.2. A *modular function of weight k for Γ* is a meromorphic function satisfying $f \mid [\gamma]_k = f$ for all $\gamma \in \Gamma$. We say "level N" if $\Gamma = \Gamma_0(N)$.

Suppose $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma$, so then $f(z + 1) = f(z)$. For each $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, expand $f \mid [\gamma]_k$ as $\sum a_n q^n$. This is a *modular form* if $a_n = 0$ for all $n < 0$ (and all γ), and is a *cusp form* if $a_n = 0$ for all $n \leq 0$ (and all γ).

Let $f(z)$ be such a cusp form, $\sum_{n=1}^{\infty} a_n q^n$, for $\Gamma_0(N)$. Let

$$L(f, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$
$$\Lambda(f, s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(f, s).$$

Then (similarly to last time — Koblitz, p. 140)

$$\Lambda(f, k - s) = w_f \Lambda(f, s),$$

where $w_f = \pm 1$.

In particular, if E is an elliptic curve over $\mathbb{Q}$ that is modular, i.e., $L(E, s) = L(f, s)$ for some cuspform f of weight 2 and level N, then $L(E, s)$ extends to an entire function, and

$$\Lambda(E, 2 - s) = w_E \Lambda(E, s),$$

where $w_E = \pm 1$.

IV.4.2 Examples

(1) $y^2 = x^3 - x$ has bad reduction only at $p = 2$. The conduction is $N = 2^5$.

(2) $x^3 + y^3 = z^3$ has bad reduction only at $p = 3$. The conduction is $N = 3^3$.

(3) Consider $E : y^2 + y = x^3 - x$. The only prime of bad reduction is $p = 37$; the point $(-5, 18)$ is singular (mod 37).

Let $u = x + 5$ and $v = y - 18$. Then the equation becomes $v^2 = u^3 - 15u^2$. The leading quadratic terms are

$$v^2 + 15u^2 = \left(v + \sqrt{-15}u\right)\left(v - \sqrt{-15}u\right).$$

These are different, so the singularity is a node.

Is it split or nonsplit, i.e., is $\sqrt{-15} \in \mathbb{F}_{37}$? By quadratic reciprocity, no. So E has nonsplit multiplicative reduction, and so $a_{37} = -1$; we get that $N = 37$. Compute $a_2 = -2,\ a_3 = -3, \ldots$

$$\begin{aligned} L(E, s) &= \left(\frac{1}{1 + 37^{-s}}\right)\left(\frac{1}{1 + 2 \cdot 2^{-s} + 2^{1-2s}}\right)\left(\frac{1}{1 + 3 \cdot 3^{-s} + 3^{1-2s}}\right)\cdots \\ &= 1 - \frac{2}{2^s} - \frac{3}{3^s} + \frac{2}{4^s} - \frac{2}{5^s} + \frac{6}{6^s} + \ldots \end{aligned}$$

There is a cuspform of weight 2, level 37,

$$f = q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + 6q^6 + \ldots$$

In fact, $L(E, s) = L(f, s)$.

IV.4.3 A curve with CM by $\mathbb{Z}[i]$

As we saw before, $E : y^2 = x^3 - x$ has CM by the Gaussian integers $\mathbb{Z}[i]$. A prime p factors in $\mathbb{Z}[i]$ as

$$p\mathbb{Z}[i] = \begin{cases} \mathfrak{p}^2 & \text{if } p = 2, \\ \mathfrak{p}\mathfrak{p}' & \text{if } p \equiv 1 \pmod 4, \\ p\mathbb{Z}[i] & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Define a map $\chi : \{\text{nonzero ideals of } \mathbb{Z}[i]\} \to \mathbb{C}$ as follows:

- If $\mathfrak{p} \mid 2$ ($\mathfrak{p}$ lies over 2), set $\chi(\mathfrak{p}) = 0$.
- If $\mathfrak{p} = p\mathbb{Z}[i]$ is prime (i.e., $p \equiv 3 \pmod 4$), set $\chi(\mathfrak{p}) = -p$.
- If $p\mathbb{Z}[i] = \mathfrak{p}\mathfrak{p}'$ (i.e., $p \equiv 1 \pmod 4$), then since $\mathbb{Z}[i]$ is a PID,

$$\mathfrak{p} = \langle a + bi \rangle, \qquad \mathfrak{p}' = \langle a - bi \rangle.$$

Pick a, b such that $a + bi \equiv 1 \pmod{2 + 2i}$. (We can do so for a unique a, b.) Then set

$$\begin{aligned} \chi(\mathfrak{p}) &= a + bi, \\ \chi(\mathfrak{p}') &= a - bi. \end{aligned}$$

Extend to all nonzero ideals of $\mathbb{Z}[i]$ multiplicatively.

If $p \equiv 3 \pmod 4$, then E is supersingular at p, and $a_p = 0$. So

$$1 - a_p p^{-s} + p^{1-2s} = 1 + pp^{-2s} = 1 - \chi(\mathfrak{p})(N\mathfrak{p})^{-s},$$

where $N\mathfrak{p} = |\mathbb{Z}[i]/\mathfrak{p}|$.

If $p \equiv 1 \pmod 4$, then [IR] p is ordinary for E, and so $a_p = 2a = \pi + \overline{\pi}$, where $\pi\overline{\pi} = p$. So

$$\begin{aligned} 1 - a_p p^{-s} + p^{1-2s} &= \left(1 - \pi p^{-s}\right)\left(1 - \overline{\pi} p^{-s}\right) \\ &= \left(1 - \chi(\mathfrak{p})(N\mathfrak{p})^{-s}\right)\left(1 - \chi(\mathfrak{p}')N(\mathfrak{p}')^{-s}\right). \end{aligned}$$

So

$$L(E,s) = \prod_{\mathfrak{p}\neq 0} \left(1 - \chi(\mathfrak{p})(N\mathfrak{p})^{-s}\right)^{-1} = \sum_{I \neq 0} \frac{\chi(I)}{(NI)^s} = L(\chi, s),$$

where the product is over nonzero prime ideals of $\mathbb{Z}[i]$, and the sum is over nonzero ideals of $\mathbb{Z}[i]$.

If E has CM, then $L(E,s) = L(\chi,s)$ for some χ. (Hecke)

Chapter V

The Mordell–Weil Theorem

V.1 2013-11-06

[I missed class this day; thanks again to Vladimir Sotirov for these notes. —Daniel]

V.1.1 Remarks

Last time we saw an example of the fact that if E has CM, then there is a Hecke character χ so that

$$L(E,s) = L(\chi,s) = \sum_I \frac{\chi(I)}{(NI)^s},$$

where I ranges over the non-zero ideals of the CM ring.

Shimura published in Crelle (in the 1950s) a computation that for $E : y^2 + y = x^3 - x^2$,

$$\sum_{n=1}^{\infty} a_n q^n = q \prod_{n=1}^{\infty} (1-q^n)^2 \left(1-q^{11n}\right)^2$$

up to a hundred or so terms.

Suppose for each prime p we have $\rho_p : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/p)$ such that there is a finite set S for which ρ_p is unramified outside $S \cup \{p\}$. Suppose for $\ell \notin S \cup \{p\}$, $\rho_p(\mathrm{Frob}_\ell)$ has characteristic polynomial independent of p (for an elliptic curve E: $1 - a_\ell + \ell T^2$). This is a compatible system of p-adic representations, to which we can associate an L-function

$$\prod_{\ell \text{ good}} \frac{1}{(\text{char. poly}) \cdot (\ell)^{-s}} \prod_{\ell \in S} \cdots .$$

V.1.2 The Mordell–Weil theorem

Theorem V.1.1 (Mordell–Weil)**.** *If K is a number field and E an elliptic curve over K, then $E(K)$ is a finitely generated abelian group.*

The proof will last three weeks (for $K = \mathbb{Q}$).

Definition V.1.2. A *height function* h on an abelian group A is a function $h : A \to \mathbb{R}$ satisfying:

(1) $h(P) \geq 0$ for all $P \in A$.

(2) $h(mP) = |m|\, h(P)$ for all $m \in \mathbb{Z}$.

(3) $h(P+Q) \leq h(P) + h(Q)$ for all $P, Q \in A$.

(4) For all $r \in \mathbb{R}$, $\{P : h(P) \leq r\}$ is finite.

Corollary V.1.3.

(1) If $h(0) = 0$, set $m = 0$ in (2).

(2) If P is torsion, then $h(P) = 0$. In particular, if A has a height function, then $\mathrm{Tor}(A)$ *is finite.*

(3) If A_1, A_2 have height functions, set

$$h(P_1, P_2) = h(P_1) + h(P_2)$$

to get a function on $A_1 \oplus A_2$.

Theorem V.1.4. *A is a finitely generated abelian group if and only if $|A/mA| < \infty$ for some integer $m > 1$ and A has a finite function.*

Proof. If $A \cong$ (finite abelian group) $\oplus\, \mathbb{Z}^r$, then $A/mA \cong$ (finite abelian group) $\oplus\, (\mathbb{Z}/m)^r$, so A/mA is finite.

Now, $\mathbb{Z}$ has a height function, namely $h(P)$. Finite groups have finite functions, namely $h(P) = 0$ for all P. So A has a height function.

In the reverse direction, let $n = |A/mA|$. Let $Q_1, \ldots, Q_n \in A$ be a transversal. Let $C = \max_{1 \leq i \leq n} h(Q_i) + 1$. We let $X = \{P \in A : h(P) \leq c\}$. Then $|X| < \infty$. Let G be the subgroup of A generated by X. We claim that $G = A$.

Indeed, we know the Q_i are in G (since $Q_i \in X$). Suppose there was $P \in A \backslash G$, of minimal height ($h(P) > c$). Then $P + mA \in A/mA$, so there exists an i so that $Q_i + mA = P + mA$. That implies that $P - Q_i \in mA$, say $P - Q_i = mR$ (for $m > 1$) with $R \in A$. Then

$$2h(R) \leq mh(R) = h(mR) = h(P - Q_i) \leq h(P) + h(-Q_i) < h(P) + c.$$

So $2h(R) < h(P) + c < 2h(P)$. Thus, $h(R) < h(P)$, and so $R \in G$. But then $P = Q_i + mR \in G$, which is a contradiction. □

V.1.3 Height functions on elliptic curves

Goals: for E an elliptic curve over $\mathbb{Q}$, we want to show that:

(1) $|E(\mathbb{Q})/2E(\mathbb{Q})| < \infty$.

(2) $E(\mathbb{Q})$ has a height function.

We will take care of (2) first; this will take a few days.

Definition V.1.5. Define $h : \mathbb{P}^n(\mathbb{Q}) \to \mathbb{R}$ as follows. If $\underline{x} = (x_0 : \cdots : x_n) \in \mathbb{P}^n(\mathbb{Q})$, write it so that all $x_i \in \mathbb{Z}$ and $\gcd(x_1, \ldots, x_n) = 1$ (i.e., multiply by the lcm of the denominators). Set

$$H(\underline{x}) = \max_{0 \le i \le n} |x_i| ,$$

and set $h(\underline{x}) = \log H(x)$.

Now, we have $E(\mathbb{Q}) \xrightarrow{x} \mathbb{P}^1(\mathbb{Q})$ given by $P \mapsto (1 : x(P))$ (and $\infty \mapsto (0 : 1)$).

Definition V.1.6. We define $H(P) = H(x(P))$ and $h(P) = h(x(P))$; this is the *naive height* on E.

Idea: we want to define $T : \mathbb{P}^2(\mathbb{Q}) \to \mathbb{P}^2(\mathbb{Q})$ so that the diagram

$$\begin{array}{ccc} A \times A & \xrightarrow{(P,Q)\mapsto(P+Q,P-Q)} & A \times A \\ \downarrow & & \downarrow \\ \mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q}) & & \mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q}) \\ \downarrow \sigma & & \downarrow \sigma \\ \mathbb{P}^2(\mathbb{Q}) & \xrightarrow{T} & \mathbb{P}^2(\mathbb{Q}) \end{array}$$

commutes, where $\sigma : (a : b) \times (c : d) \mapsto (ac : bc + ad : bd)$.

The *canonical height* (due to Tate) is

$$\hat{h}(P) = \lim_{n \to \infty} \frac{h(2^n P)}{4^n}.$$

V.2 2013-11-08

Aims: To show

(1) $|E(\mathbb{Q})/2E(\mathbb{Q})| < \infty$.

(2) $E(\mathbb{Q})$ has a height function.

V.2.1 Height function on E

We're starting with (2). Idea:

(a) Define $h : E(\mathbb{Q}) \to \mathbb{R}$.

(b) Show $h(P + Q) + h(P - Q) = 2h(P) + h(Q) + \mathrm{O}(1)$.

(c) Let $\hat{h}(P) = \lim_{n\to\infty} \frac{1}{4^n} h(2^n P)$. Show

$$\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q).$$

(d) Show $P \mapsto \sqrt{\hat{h}(P)}$ is a height function on $E(\mathbb{Q})$.

We did (a) on Wednesday by defining

$$h(P) = \log H(x(P)) = \log(\max\{|a|, |b|\})$$

for $x(P) = (a : b) \in \mathbb{P}^1(\mathbb{Q})$, where $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$.

Denote $A = E(\mathbb{Q})$. To prove (b), we must find T such that the following diagram commutes:

$$\begin{array}{ccc} A \times A & \xrightarrow{(P,Q)\mapsto(P+Q,P-Q)} & A \times A \\ \downarrow & & \downarrow \\ \mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q}) & & \mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q}) \\ \downarrow \sigma & & \downarrow \sigma \\ \mathbb{P}^2(\mathbb{Q}) & \xrightarrow{\quad T \quad} & \mathbb{P}^2(\mathbb{Q}) \end{array}$$

Recall that σ is defined by

$$\begin{aligned} &\mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q}) \xrightarrow{\sigma} \mathbb{P}^2(\mathbb{Q}), \\ &\big((a : b), (c : d)\big) \mapsto (ac : ad + bc : bd). \end{aligned}$$

Write $P = (x_1, y_1),\ Q = (x_2, y_2),\ P + Q = (x_3, y_3),\ P - Q = (x_4, y_4)$. Writing $E : y^2 = x^3 + ax + b$, a computation shows that

$$\begin{aligned} x_3 + x_4 &= \frac{2(x_1 + x_2)(a + x_1x_2) + 4b}{(x_1 - x_2)^2}, \\ x_3x_4 &= \frac{(x_1x_2 - a)^2 - 4b(x_1 + x_2)}{(x_1 - x_2)^2}. \end{aligned}$$

We need

$$T\big((1 : x_1 + x_2 : x_1x_2)\big) = (1 : x_3 + x_4 : x_3x_4).$$

Let $s = x_1 + x_2$ and $p = x_1x_2$, i.e.,

$$\begin{aligned} T\big((1 : s : p)\big) &= \left(1 : \frac{2s(a + p) + 4b}{s^2 - 4p} : \frac{(p - a)^2 4bs}{s^2 - 4p}\right), \\ T\big((t : s : p)\big) &= \big(s^2 - 4pt : 2s(at + p) + 4bt^2 : (p - at)^2 - 4bst\big). \end{aligned}$$

We have

$$T\big(\sigma(x(P), x(Q))\big) = \sigma\big(x(P + Q), x(P - Q)\big),$$

and T is a degree 2 map $\mathbb{P}^2(\mathbb{Q}) \to \mathbb{P}^2(\mathbb{Q})$.

Lemma V.2.1.

(1) If $T : \mathbb{P}^n(\mathbb{Q}) \to \mathbb{P}^n(\mathbb{Q})$ has degree d, then

$$h(T(\alpha)) - dh(\alpha) = \mathrm{O}(1).$$

(2) $h(\sigma(x(P),x(Q))) = h(P)+h(Q)+\mathrm{O}(1)$.

This lemma implies (b):

$$\begin{aligned} 2h(P)+2h(Q)+\mathrm{O}(1) &= 2h\big(\sigma(x(P),x(Q))\big)+\mathrm{O}(1) && \text{by (2)}\\ &= h\big(T(\sigma(x(P),x(Q)))\big) && \text{by (1)}\\ &= h\big(\sigma(x(P+Q),x(P-Q))\big)\\ &= h(P+Q)+h(P-Q)+\mathrm{O}(1) && \text{by (2)}. \end{aligned}$$

V.2.2 Proof of Lemma V.2.1

Let $\alpha \in \mathbb{P}^n(\mathbb{Q})$. We show

$$c_1 H(\alpha)^d \le H(T(\alpha)) \le c_2 H(\alpha)^d.$$

Say $T : \alpha = (\alpha_0 : \cdots : \alpha_n) \mapsto (T_0(\alpha) : \cdots : T_n(\alpha))$, where $T_i \in \mathbb{Z}[x_0,\dots,x_n]$. Write $T_i = \sum_j \beta_{ij} m_j$ (where m_j are monomials). Suppose the a_i are integers with no common divisor. Then

$$|T_i(\alpha)| \le \sum_j |\beta_{ij}|\,|m_j(\alpha)| \le \Big(\sum_j |\beta_{ij}|\Big)(\max_k |\alpha_k|)^d = c(T_i)H(\alpha)^d,$$

where $c(T_i)$ is a constant depending on T_i. So, setting $c_2 = \max_i c(T_i)$,

$$H(T(\alpha)) = \frac{\max_i(|T_i(\alpha)|)}{\gcd(T_i(\alpha)} \le \max_i(|T_i(\alpha)|) \le c_2 H(\alpha)^d. \tag{V.2.2.1}$$

Now we need the projective Nullstellensatz. The T_i have no common zero in $\overline{\mathbb{Q}}$. Hence, there exist $g_{ij} \in \mathbb{Q}[x_0,\dots,x_n]$ and $m \in \mathbb{Z}^+$ such that

$$x_i^{m+d} = \sum_{j=0}^n g_{ij} T_j.$$

Clear the denominators, and get some $e \in \mathbb{Z}_{\neq 0}$ and $h_{ij} \in \mathbb{Z}[x_0,\dots,x_n]$ such that

$$e x_i^{m+d} = \sum_{j=0}^n h_{ij} T_j.$$

Evaluate at α:

$$\begin{aligned} |e|\,\big|\alpha_i^{m+d}\big| = \left|\sum_{j=0}^n h_{ij}(\alpha)T_j(\alpha)\right| &\le \sum_{j=0}^n |h_{ij}(\alpha)|\,|T_j(\alpha)|\\ &\le \sum_{j=0}^n c(h_{ij})H(\alpha)^m \max_j |T_j(\alpha)|\\ &\le (n+1)\max_j c(h_{ij})H(\alpha)^m \max_j |T_j(\alpha)|\,. \end{aligned}$$

Claim V.2.2. $\max_j |T_j(\alpha)| \le |e|\, H(T(\alpha))$.

Proof. Suppose $p^r \mid T_j(\alpha)$ for all j. Then $p^r \mid e\alpha^{m+d}$ for all i. But $\gcd(\alpha_i) = 1$, so $p \nmid \alpha_i$ for some i. Thus, $p^r \mid e$, so $\gcd(T_j(\alpha)) \mid e$. Use (V.2.2.1). □

Thus, for all i,

$$|e|\, |\alpha_i|^{m+d} \le kH(\alpha)^m\, |e|\, H(T(\alpha)),$$

where k is a constant not depending on α. Take the maximum over i:

$$|e|\, H(\alpha)^{m+d} \le kH(\alpha)^m\, |e|\, H(T(\alpha)),$$

whence $H(T(\alpha)) \ge c_1 H(\alpha)^d$. This completes the proof of part (1) of Lemma V.2.1. □

Now we prove part (2) of the lemma. Suppose $x_1 = (a : b)$ and $x_2 = (c : d)$. Then

$$\sigma(x_1, x_2) = (ac : ad + bc : bd).$$

We want to show

$$h\big((ac : ad + bc : bd)\big) = h\big((a : b)\big) + h\big((c : d)\big) + \mathrm{O}(1).$$

Let $M = \max(|a|, |b|)$, $M' = \max(|c|, |d|)$, and $M'' = \max(|ac|, |ad + bc|, |bd|)$. Show (case by case) that $\frac{1}{2}MM' \le M'' \le 2MM'$. So

$$\log M + \log M' - \log 2 \le \log M'' \le \log M + \log M' + \log 2,$$

whence

$$|\log M'' - \log M - \log M'| \le \log 2,$$

and we are done. □

V.3 2013-11-11

V.3.1 Heights, continued

Let E be an elliptic curve defined over $\mathbb{Q}$.

Goals:

(a) Define $h : E(\mathbb{Q}) \to \mathbb{R}$.

(b) Show $h(P + Q) + h(P - Q) = 2h(P) + 2h(Q) + \mathrm{O}(1)$.

(c) Set

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h(2^n P)}{4^n}.$$

Show $\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q)$.

(d) Show that $P \mapsto \sqrt{\hat{h}(P)}$ is a height function on $E(\mathbb{Q})$.

V.3.2 A theorem of Tate

Theorem V.3.1 (Tate)**.** *Suppose S is a set, $T : S \to S$, $h : S \to \mathbb{R}$, $d > 1$ is an integer, and*

$$h(T(\alpha)) - dh(\alpha) = \mathrm{O}(1)$$

for all $\alpha \in S$. Then there is a unique $\hat{h} : S \to \mathbb{R}$ satisfying

(1) $\hat{h}(\alpha) - h(\alpha) = \mathrm{O}(1)$ ($\hat{h}$ is boundedly different *from h), and*

(2) $\hat{h}(T(\alpha)) = d\hat{h}(\alpha)$ for all $\alpha \in S$.

Proof. **Uniqueness** Suppose $\hat{h}_1, \hat{h}_2$ both satisfy. Then for all $\alpha \in S$,

$$\hat{h}_1(T(\alpha)) - \hat{h}_2(T(\alpha)) = d\left(\hat{h}_1(\alpha) - \hat{h}(\alpha)\right).$$

Note that $j(\alpha) := \hat{h}_1(\alpha) - \hat{h}_2(\alpha)$ is bounded by a constant, call it C. Thus

$$C \geq |j(T(\alpha))| = d\,|j(\alpha)|,$$

so $|j(\alpha)| \leq \frac{C}{d}$. Rinse and repeat, replacing C by $\frac{C}{d}$. Since $d > 1$, it follows that $j(\alpha) = 0$ for all $\alpha \in S$, whence $\hat{h}_1(\alpha) = \hat{h}_2(\alpha)$.

Existence Let

$$\hat{h}(\alpha) = \lim_{n\to\infty} \frac{1}{d^n} h(T^n\alpha).$$

Say $|h(T(\alpha)) - dh(\alpha)| \leq C'$ for all α. Use Cauchy's criterion:

$$\left|\frac{1}{d^{n+1}}h(T^{n+1}\alpha) - \frac{1}{d^n}h(T^n\alpha)\right| = \frac{1}{d^{n+1}}\left|h\big(T(T^n\alpha)\big) - dh(T^n\alpha)\right| \leq \frac{C'}{d^{n+1}}.$$

Thus,

$$\left|\frac{1}{d^{n+1}}h(T^{n+1}\alpha) - \frac{1}{d^n}h(T^n\alpha)\right| \leq \frac{C'}{d^{n+1}} \cdot \frac{1}{\left(1 - \frac{1}{d}\right)}.$$

Hence the limit exists and satisfies $\hat{h}(\alpha) - h(\alpha) = \mathrm{O}(1)$ (take $n = 0$ in the above estimate). Furthermore,

$$\hat{h}(T(\alpha)) = \lim_{n\to\infty} \frac{1}{d^n} h(T^{n+1}(\alpha)) = \lim_{n\to\infty} \frac{1}{d^{n+1}} dh(T^{n+1}(\alpha)) = d\hat{h}(\alpha). \qquad \square$$

V.3.3 Behavior of heights under doubling

Let us find T to make this diagram commute:

$$\begin{array}{ccc} E(\mathbb{Q}) & \xrightarrow{2} & E(\mathbb{Q}) \\ {\scriptstyle x}\downarrow & & \downarrow{\scriptstyle x} \\ \mathbb{P}^1(\mathbb{Q}) & \xrightarrow{T} & \mathbb{P}^1(\mathbb{Q}) \end{array}$$

Suppose $E : y^2 = x^3 + ax + b$. Recall the *duplication formula*:

$$T(1 : x) = \left(1 : \frac{x^4 + \cdots + a^2}{4(x^3 + ax + b)}\right)$$
$$T\big((u : v)\big) = \left(4(v^3u + avu^3 + bu^4) : v^4 + \cdots + a^2u^4\right).$$

In particular, T has degree 4. Define

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h(2^nP)}{4^n}.$$

Remark V.3.2. So we have $\hat{h}(2P) = 4\hat{h}(P)$. In fact, we'll later see that $\hat{h}(nP) = n^2\hat{h}(P)$ in general.

V.3.4 The parallelogram law

We want to show that

$$\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q).$$

Indeed,

$$\text{LHS} - \text{RHS} = \lim_{n\to\infty} \frac{1}{4^n} \underbrace{\big(h(2^n(P + Q)) + h(2^n(P - Q)) - 2h(2^nP) - 2h(2^nQ)\big)}_{\text{by (b), |this| } \le C' \text{ for all } P, Q} = 0.$$

This proves (c). □

V.3.5 The height function

For (d), define $|P| = \sqrt{\hat{h}(P)}$. We'll show this is a height function.

Recall the properties of a height function:

(1) $|P| \ge 0$ for all P.

(2) $|mP| = |m|\,|P|$ for all $m \in \mathbb{Z}$ and all $P \in E(\mathbb{Q})$.

(3) $|P + Q| \le |P| + |Q|$.

(4) $\{P : |P| \le r\}$ is finite.

We prove these in order:

(1) For all P, $h(P) \ge 0$, so $\hat{h}(P) \ge 0$, whence (1).

(2) Note that P and $-P$ have the same x-coordinate. So $h(-P) = h(P)$, hence (2) is true for $m = 0, 1, -1$, and it's enough to show (2) for $m \ge 1$. We proceed by induction, setting $P = (m - 1)Q$ in (c). Then

$$\begin{aligned}\hat{h}([m - 1]Q + Q) + \hat{h}([m - 1]Q - Q) &= 2\hat{h}([m - 1]Q) + 2\hat{h}(Q)\\ \hat{h}(mQ) + (m - 2)^2\hat{h}(Q) &= 2(m - 1)^2\hat{h}(Q) + 2\hat{h}(Q)\\ \hat{h}(mQ) &= \left[2(m - 1)^2 - (m - 2)^2 + 2\right]\hat{h}(Q) = m^2\hat{h}(Q).\end{aligned}$$

Thus, $|mQ| = |m|\,|Q|$, proving (2).

(3) Define the *height pairing*

$$\langle P, Q\rangle = \frac{\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)}{2}.$$

So, for example, $\langle P, P\rangle = \frac{1}{2}(\hat{h}(2P) - 2\hat{h}(P)) = \hat{h}(P)$.

Claim. $\langle P+R, Q\rangle = \langle P, Q\rangle + \langle R, Q\rangle$.

Indeed,

$$\begin{aligned} 2\left(\langle P+R, Q\rangle - \langle P, Q\rangle - \langle R, Q\rangle\right) = \hat{h}(P+R+Q) - \hat{h}(P+R) - \hat{h}(Q) \\ - \hat{h}(P+Q) + \hat{h}(P) + \hat{h}(Q) \\ - \hat{h}(R+Q) + \hat{h}(R) + \hat{h}(Q). \end{aligned}$$

We use the following four facts, which follow from (c):

(I) $\hat{h}(P+R+Q) + \hat{h}(P+R-Q) - 2\hat{h}(P+R) - 2\hat{h}(Q) = 0$
(II) $\hat{h}(P-R+Q) + \hat{h}(P-Q+R) - 2\hat{h}(P) - 2\hat{h}(R-Q) = 0$
(III) $\hat{h}(P-R+Q) + \hat{h}(P+R+Q) - 2\hat{h}(P+Q) - 2\hat{h}(R) = 0$
(IV) $2\left(\hat{h}(Q+R) + \hat{h}(R-Q) - 2\hat{h}(R) - 2\hat{h}(Q)\right) = 0$

The claim then follows by looking at I − II + III − IV:

$$4(\text{LHS} - \text{RHS}) = 0.$$

We'll finish this next time.

V.4 2013-11-13

V.4.1 Height function, continued

From last time, $\hat{h}(nP) = n^2\hat{h}(P)$ and $h(nP) \approx n^2 h(P)$. Recall the height pairing

$$\langle P, Q\rangle = \frac{\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)}{2}.$$

We have $|P| = \sqrt{\hat{h}(P)} = \sqrt{\langle P, P\rangle}$. Properties:

$$\begin{aligned} \langle P, P\rangle &= \hat{h}(P) \geq 0 \\ \langle P, Q\rangle &= \langle Q, P\rangle \\ \langle P+R, Q\rangle &= \langle P, Q\rangle + \langle R, Q\rangle && \text{(just saw this)} \\ \langle P, Q+R\rangle &= \langle P, Q\rangle + \langle P, R\rangle && \text{(by symmetry)} \end{aligned}$$

For $\lambda, \mu \in \mathbb{Z}$ and P, Q,

$$0 \leq \langle \lambda P - \mu Q, \lambda P - \mu Q \rangle = \lambda^2 \langle P, P \rangle - 2\lambda\mu \langle P, Q \rangle + \mu^2 \langle Q, Q \rangle .$$

This is true for all λ, μ, so

$$\begin{aligned} (2 \langle P, Q \rangle)^2 - 4 \langle P, P \rangle \langle Q, Q \rangle &\leq 0 \\ \langle P, Q \rangle^2 &\leq \langle P, P \rangle \langle Q, Q \rangle \\ |\langle P, Q \rangle| &\leq |P| \, |Q| . \end{aligned}$$

Hence

$$\begin{aligned} |P + Q|^2 &= \langle P + Q, P + Q \rangle \\ &= \langle P, P \rangle + 2 \langle P, Q \rangle + \langle Q, Q \rangle \\ &\leq |P|^2 + |Q|^2 + 2 |P| \, |Q| \\ &= (|P| + |Q|)^2 . \end{aligned}$$

So we get (3): $|P + Q| \leq |P| + |Q|$. □

To finish proving that $P \mapsto |P|$ is a height function on $E(\mathbb{Q})$, we now prove (4): $|P : |P| \leq r|$ is finite (for given r). Indeed, since bounding $|P|$ bounds $H(x(P))$ with coordinates of $x(P)$ integers, this bounds coordinates of $x(P)$. □

Aside V.4.1. $\langle \cdot, \cdot \rangle$ is positive semi-definite. In particular, $\langle P, P \rangle = 0 \iff P$ is torsion. (We already proved $\Longleftarrow$. For the other direction, if P has infinite order, this contradicts (4).)

The *elliptic regulator* $|\det \langle P_i, P_j \rangle|$ appeared in the strong Birch–Swinnerton-Dyer conjecture. Here $\{P_i\}$ is a basis of $E(\mathbb{Q})$ mod torsion.

V.4.2 Remarks on torsion

Suppose we've shown $E(\mathbb{Q}) \cong \mathbb{Z}^{r_E} \oplus (\text{Tors})$. In practice, r_E is the hard one to find, and $\text{Tors}(E(\mathbb{Q}))$ is easy to find.

Facts:

(1) $\text{Tors}(E(\mathbb{Q})) \hookrightarrow E(\mathbb{F}_p)$ for all odd primes p of good reduction. (If $p = 2$ has good reduction, then $|\text{kernel}| \leq 2$.)

(2) (Lutz–Nagell) If $y^2 = f(x)$, $f \in \mathbb{Z}[x]$, then (u, v) torsion $\implies u, v \in \mathbb{Z}$ and $v = 0$ or $v^2 \mid \text{Disc}(f)$.

(3) (Mazur, 1977) $|\text{Tors}| \leq 16$.

(4) (Doud) The torsion subgroup can be computed by analytic methods.

V.4.3 Finiteness of 2-torsion

Aim: Show $|E(\mathbb{Q})/2E(\mathbb{Q})|$ is finite.

Remark V.4.2 (Strategy/idea). Suppose $E : y^2 = f(x)$, where $f(x) \in \mathbb{Z}[x]$ is completely factorizable:

$$f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3) \qquad (\alpha_i \in \mathbb{Z}).$$

We can define a map

$$\begin{aligned} E(\mathbb{Q})/2E(\mathbb{Q}) &\to \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \times \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \\ P &\mapsto \left(x-\alpha_1 \left(\mathrm{mod}^\times \mathbb{Q}^{\times 2}\right), x-\alpha_2 \left(\mathrm{mod}^\times \mathbb{Q}^{\times 2}\right)\right), \end{aligned}$$

where $x = x(P)$. Can do this and get an injective homomorphism. All we have to do is to characterize the image.

Note V.4.3. $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ is an abelian group of exponent 2 (basis $-1, 2, 3, 5, 7, 11, \dots$).

Suppose E has a point of order 2, say $(0,0)$. Say $E = E[a,b] : y^2 = x^3 = ax^2 + bx$. Define

$$\begin{aligned} &E(\overline{\mathbb{Q}}) \xrightarrow{\phi} E'(\overline{\mathbb{Q}}), \\ &(x,y) \mapsto \left(\frac{y^2}{x^2}, y\left(1-\frac{b}{x^2}\right)\right), \quad (0,0) \qquad \mapsto \text{point at } \infty, \end{aligned}$$

where $E' = E[-2a, a^2-4b]$.

We'll define $\alpha : E'(\mathbb{Q}) \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ such that

$$E(|Q) \xrightarrow{\phi} E'(\mathbb{Q}) \xrightarrow{\alpha} \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$$

is exact, i.e., $E'(\mathbb{Q})/\operatorname{Im}(\phi) = E'(\mathbb{Q})/\ker(\alpha) \cong \operatorname{Im}(\alpha)$.

Why? If we show $\operatorname{Im}(\alpha)$ is finite, then $E'(\mathbb{Q})/\phi E(\mathbb{Q})$ is finite. Show likewise that $E(\mathbb{Q})/\overline{\phi}E'(\mathbb{Q})$ is finite. But $2 = \overline{\phi}\phi$ since ϕ has degree 2, so $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

Define α as follows:

$$\begin{aligned} E[c,d] &\xrightarrow{\alpha} \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \\ \text{point at } \infty &\mapsto 1 \\ (x,y) &\mapsto x \left(\mathrm{mod}^\times \mathbb{Q}^{\times 2}\right) \\ (0,0) &\mapsto d. \end{aligned}$$

Need to check:

- α is a homomorphism;
- $\ker(\alpha) = \operatorname{Im}(\alpha)$;
- $\operatorname{Im}(\alpha) \subseteq \{\pm \prod p_i^{e_i} \mid p \mid d,\ e_i = 0 \text{ or } 1\}$. (This implies $\operatorname{Im}(\alpha)$ is finite.)

V.5 2013-11-15

V.5.1 Finiteness of 2-torsion, continued

Let α be as defined last time.

Lemma V.5.1. *For $(x, y) \in E(\mathbb{Q})$, where E is defined by*

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

there exist $m, n, e \in \mathbb{Z}$ with $(m, e) = (n, e) = 1$ such that $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$.

Proof. Say $x = \frac{m}{r}$, $y = \frac{n}{s}$ with $(m, r) = 1 = (n, s)$. For p a prime, set $a = \operatorname{ord}_p(r)$, $b = \operatorname{ord}_p(s)$. Then $a > 0$ if and only if $b > 0$. The exact power of p in the denominator of the right-hand side of the defining equation is p^{3a}, whereas on the left-hand side it is $\leq p^{2a}$ if $a \geq b$, and for $b > a$ it is p^{2b}. So $2b = 3a$, so set $a = 2d_p$ and $b = 3d_p$, and $e = \prod_p p^{d_p}$. □

Recall that $E[a, b] : y^2 = x^3 + ax^2 + bx$ has a point of order 2, namely $(0, 0)$.

Definition V.5.2. We define a map

$$\begin{aligned} E[c, d] &\xrightarrow{\alpha} \mathbb{Q}^\times/\mathbb{Q}^{\times 2}, \\ \infty &\mapsto 1, \\ (x, y) &\mapsto x \left(\operatorname{mod}^\times \mathbb{Q}^{\times 2}\right) && \text{if } x \neq 0, \\ (0, 0) &\mapsto d. \end{aligned}$$

We want to check α is a group homomorphism, $\ker\alpha = \operatorname{Im}\phi$, and $\operatorname{Im}\alpha$ is finite. We will prove the first in greater generality in a moment. We easily have the second since $\ker\alpha = \operatorname{Im}\phi$, so the composite

$$E(\mathbb{Q}) \xrightarrow{\phi} E'(\mathbb{Q}) \xrightarrow{\overline{\phi}} E(\mathbb{Q})$$

is multiplication by 2. We prove the third.

Claim V.5.3. $\operatorname{Im}(\alpha) \subseteq \{\pm \prod p_i^{e_i} \mid p_i \mid d,\ e_i = 0 \text{ or } 1\}\, \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$.

[We will see later that if $r_E = \operatorname{rank}(E(\mathbb{Q}))$, then $2^{r_E} = \frac{1}{4}\,|\operatorname{Im}\alpha_E|\,|\operatorname{Im}\alpha_{E'}|$.]

We prove the claim. Let $(x, y) \in E[c, d](\mathbb{Q})$. Then $x = \frac{m}{e^2}$, $y = \frac{n}{e^3}$, where $(m, e) = 1 = (n, e)$, whence

$$\begin{aligned} y^2 &= x^3 + cx^2 + dx \\ \frac{n^2}{e^6} &= \frac{m^3}{e^6} + c\frac{m^2}{e^4} + d\frac{m}{e^2} \\ n^2 &= m^3 + cm^2e^2 + dme^4 = m\left(m^2 + cme^2 + de^4\right). \end{aligned}$$

Case 1 Factors on RHS are relatively prime. Then $m = \pm$ square, which implies $x = \pm$ square, so

$$\alpha\big((x, y)\big) = x = 1 \left(\operatorname{mod}^\times \mathbb{Q}^{\times 2}\right).$$

Case 2 $\gcd(m, m^2 + cme^2 + de^4) = g \neq 1$. Then $g \mid de^4$, so $(m, e) = 1$ implies $g \mid d$. But $m = \pm(\text{square})g$, so $\alpha((x, y)) = \pm g$.

V.5.2 General case

Let $E : y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ with $\alpha_1, \alpha_2, \alpha_3 \in R$, where R is a UFD with fraction field K. Let

$$P(E) = \left\{\text{irreducibles (up to associates) } p \;\middle|\; p \mid \alpha_i - \alpha_j \text{ for some } i \neq j\right\},$$
$$A(E) = \left\{a \in K^\times/K^{\times 2} \;\middle|\; \operatorname{ord}_p(a) \text{ even } \forall p \notin P(E)\right\}.$$

Note that $P(E)$ is a finite set.

Define

$$\theta_i : E(K) \to K^\times/K^{\times 2}$$
$$\text{point at } \infty \mapsto 1$$
$$(x, y) \mapsto x - \alpha_i \left(\operatorname{mod}^\times K^{\times 2}\right) \qquad (\text{if } x \neq \alpha_i)$$
$$(\alpha_i, 0) \mapsto (\alpha_j - \alpha_i)(\alpha_k - \alpha_i) \qquad \text{where } \{i, j, k\} = \{1, 2, 3\}.$$

Claim V.5.4.

(1) $\operatorname{Im}\theta_i \subseteq A(E)$.

(2) θ_i *is a group homomorphism.*

(3) $\bigcap_{i=1}^3 \ker(\theta_i) \subseteq 2E(K)$.

(4) $A(E)$ *is finite if* $R^\times/R^{\times 2}$ *is finite (where* $R^\times = U(R)$ *is the unit group of* R*).*

Corollary V.5.5. *Let* $\theta = (\theta_1, \theta_2, \theta_3) : E(K) \to A(E)^3$. *Then* $E(K)/\ker\theta \twoheadrightarrow E(K)/2E(K)$ *is a surjection by (3), and* $E(K)/\ker\theta \cong \operatorname{Im}\theta \subseteq A(E)^3$ *is finite, so* $E(K)/2E(K)$ *is finite.*

V.5.3 Proof of claims

(1) We need to show that if $(x, y) \in E(K)$, then $\operatorname{ord}_p(x - \alpha_i)$ is even for all $p \notin P(E)$. Recall that

$$\operatorname{ord}_p(a + b) \geq \min\big(\operatorname{ord}_p(a), \operatorname{ord}_p(b)\big)$$

with equality if $\operatorname{ord}_p(a) \neq \operatorname{ord}_p(b)$.

Case (i): Suppose $\operatorname{ord}_p(x - \alpha_i) < 0$ for at least one i. Then $\operatorname{ord}_p(\alpha_i) \geq 0$ for $\alpha_i \in R$, and $\operatorname{ord}_p(\alpha_i - \alpha_j) = 0$ for $p \notin P(E)$, so

$$\operatorname{ord}_p(x - \alpha_i) = \operatorname{ord}_p(x) = \operatorname{ord}_p(\alpha_i).$$

Since $y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$,

$$2\operatorname{ord}_p(y) = \sum_{i=1}^{3} \operatorname{ord}_p(x - \alpha_i) = 3\operatorname{ord}_p(x).$$

So for all i, if $\operatorname{ord}_p(x)$ is even, then $\operatorname{ord}_p(x - \alpha_i)$ is even.

Case (ii): Say $\operatorname{ord}_p(x-\alpha_i), \operatorname{ord}_p(x-\alpha_j) > 0$. This can't happen since $\operatorname{ord}_p(\alpha_i - \alpha_j) = 0$.

Case (iii): Suppose exactly one $x - \alpha_i$ has $\operatorname{ord}_p(x - \alpha_i) > 0$, say $i = 1$. Then the rest have $\operatorname{ord}_p = 0$, so

$$2\operatorname{ord}_p(y) = \sum_{i=1}^{3} \operatorname{ord}_p(x - \alpha_i) = \operatorname{ord}_p(x - \alpha_1),$$

hence $\operatorname{ord}_p(x - \alpha_1)$ is even. □

(2) Suppose P_1, P_2, P_3 are collinear in $E(K)$. We need to show $\theta_i(P_1)\theta_i(P_2)\theta_i(P_3) = 1$.

We will finish this next time.

V.6 2013-11-18

V.6.1 Finiteness of 2-torsion, continued

Recall our setup: R is a UFD with fraction field K, and $E : y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ an elliptic curve. We defined

$$P(E) = \left\{\text{irreducibles (up to associates) } p \;\middle|\; \alpha_i - \alpha_j \text{ for some } i \neq j\right\},$$
$$A(E) = \left\{a \in K^\times/K^{\times 2} \;\middle|\; \operatorname{ord}_p(a) \text{ even } \forall p \notin P(E)\right\}.$$

Define

$$\begin{aligned} \theta_i : E(K) &\to K^\times/K^{\times 2}, \\ \text{point at } \infty &\mapsto 1 \\ (x, y) &\mapsto x - \alpha_i \qquad\qquad (x \neq \alpha_i) \\ (\alpha_i, 0) &\mapsto (\alpha_j - \alpha_i)(\alpha_k - \alpha_i). \end{aligned}$$

Claims:

(1) $\operatorname{Im}(\theta_i) \subseteq A(E)$.

(2) θ_i is a group homomorphism.

(3) $\bigcap_{i=1}^{3} \ker(\theta_i) \subseteq 2E(K)$.

(4) $A(E)$ is finite if $U(R)/U(R)^2$ is finite.

Together, these imply that $E/2E(K)$ is finite.

Last time, we showed claim (1), and we were in the process of showing (2).

V.6.2 Proof of claim (2)

Suppose P_1, P_2, P_3 are collinear in $E(K)$. We need to show that $\theta_i(P_1)\theta_i(P_2)\theta_i(P_3) \in K^{\times 2}$.

Case (i): Suppose $P_1 = \infty,\ P_2 = (x, y),\ P_3 = (x, -y)$. Then $\theta_i(P_1) = 1$, $\theta_i(P_2) = x - \alpha_i$, and $\theta_i(P_3) = x - \alpha_i$, so

$$\theta_i(P_1)\theta_i(P_2)\theta_i(P_3) = (x - \alpha_i)^2 \in K^{\times 2}.$$

Case (ii): Suppose $P_i = (\alpha_i, 0)$. Then $\theta_1(P_1) = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)$, $\theta_1(P_2) = \alpha_2 - \alpha_1$, and $\theta_1(P_3) = \alpha_3 - \alpha_1$, so the product is a square.

Case (iii): Suppose no P_i is of the form $(\alpha_i, 0)$. Let $P_i = (x_i, y_i)$. Then $\theta_i(P_j) = x_j - \alpha_i$. Let $y = \lambda x + \mu$ be the line joining them. Then x_1, x_2, x_3 are the roots of

$$(x - \alpha_1)(x - \alpha_2)(x - \alpha_3) = (\lambda x + \mu)^2.$$

Then $x_1 - \alpha_i, x_2 - \alpha_i, x_3 - \alpha_i$ are the roots of

$$(x + \alpha_i - \alpha_1)(x + \alpha_i - \alpha_2)(x + \alpha_i - \alpha_3) - \big(\lambda(x + \alpha_i) + \mu\big)^2 = 0. \qquad \text{(V.6.2.1)}$$

Expand this out:

$$x^3 + ax^2 + bx - \lambda^2 x^2 - 2\lambda(\lambda\alpha_i + \mu)x - (\lambda\alpha_i + \mu)^2 = 0. \qquad \text{(V.6.2.2)}$$

The constant term is

$$-(\lambda\alpha_i + \mu)^2 = -(x_1 - \alpha_1)(x_2 - \alpha_i)(x_3 - \alpha_i) = -\theta_i(P_1)\theta_i(P_2)\theta_i(P_3),$$

so $\theta_i(P_1)\theta_i(P_2)\theta_i(P_3) \in K^{\times 2}$.

Case (iv): Suppose exactly one point is on the x-axis; say $P_1 = (\alpha_1, 0)$. For $i = 2, 3$, as in the previous case, $\theta_i(P_1)\theta_i(P_2)\theta_i(P_3) = (x_1 - \alpha_i)(x_2 - \alpha_i)(x_3 - \alpha_i) \in K^{\times 2}$.

What about $i = 1$? Plug $x = \alpha_1$ in (V.6.2.1) to get $\lambda\alpha_1 + \mu = 0$. So (V.6.2.2) gives

$$\text{LHS} = x^3 + (a - \lambda^2)x^2 + bx.$$

This has roots $0, x^2 - \alpha_1, x_3 - \alpha_1$. We get $b = (x_2 - \alpha_1)(x_3 - \alpha_1)$. But also

$$x(x + \alpha_1 - \alpha_2)(x + \alpha_1 - \alpha_3) = x^3 + ax^2 + bx.$$

So $b = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)$. Thus,

$$\theta_1(P_1)\theta_1(P_2)\theta_1(P_3) = b^2 \in K^{\times 2}.$$

This completes the proof of claim (2). □

V.6.3 Proof of claim (3)

Lemma V.6.1. *Let $(x', y') \in E(K)$. Then $(x', y') \in 2E(K)$ iff $x' - \alpha_i$ is a square in K for all i.*

This lemma implies claim (3). Indeed, suppose $(x', y') \in \bigcap_{i=1}^{3} \ker(\theta_i)$. Say $x' \neq \alpha_i$ for any i. Then $x' - \alpha_i$ is a square for all i, so by the lemma, $(x', y') \in 2E(K)$. On the other hand, if $x' = \alpha_1$, then $x' - \alpha_1 = 0$ is a square, and since we are in the kernel of each θ_i, $x' - \alpha_2$ and $x' - \alpha_3$ are also squares, whence by the lemma, $(x', y') \in 2E(K)$. □

Now we prove the lemma. Suppose $P = (x', y') \in 2E(K)$. Then Q has coordinates in K. Let $Q = (u, v)$ and $y = \lambda x + \mu$ be tangent at Q. Then

$$(x - \alpha_1)(x - \alpha_2)(x - \alpha_3) - (\lambda x + \mu)^2 = (x - u)^2(x - x').$$

Set $x = \alpha_1$. Then $-(\lambda\alpha_1 + \mu)^2 = (\alpha_1 - u)^2(\alpha_1 - x')$. So $x' - \alpha_1$ is a square, and likewise for $i = 2, 3$.

Conversely, we get Q and need to show $u, v \in K$. Suppose $x' - \alpha_i = \beta_i^2$, where $\beta_i \in K$. Then u satisfies

$$(\lambda\alpha_1 + \mu)^2 = (\alpha_1 - u)^2\beta_1^2,$$

where λ, μ depend on u, v, e.g., λ is the tangent slope at (u, v). Observe that

$$\begin{aligned} y^2 &= \prod_{i=1}^{3}(x - \alpha_i), \\ 2y\frac{dy}{dx} &= \sum_{j \neq i}(x - \alpha_i)(x - \alpha_j), \end{aligned}$$

so $2v\lambda = n$, where $n = \sum_{j \neq i}(u - \alpha_i)(u - \alpha_j)$.

Hence, $v = \lambda u + \mu$ since Q is on its tangent, so $\mu = v - \lambda u$, whence

$$\begin{aligned} \pm\beta_1(\alpha_1 - u) &= \lambda\alpha_1 + \mu = \frac{n}{2v}\alpha_1 + \left(v - \frac{n}{2v}u\right), \\ \pm 2v\beta_1(\alpha_1 - u) &= n(\alpha_1 - u) + 2v^2, \end{aligned}$$

which is a cubic in u that vanishes at $u = \alpha_1$. Divide by $\alpha_1 - u$:

$$\pm 2v\beta_1 = n - 2(u - \alpha_1)(u - \alpha_3),$$

which is quadratic in u. Likewise,

$$\pm 2v\beta_2 = n - 2(u - \alpha_1)(u - \alpha_3).$$

Eliminate v to get a quadratic in u. Solve for u by the quadratic formula. The discriminant turns out to be $4(\alpha_2 - \alpha_1)^2\beta_3^2$, which is a square. Hence $u \in K$, so $v \in K$ and $P \in 2E(K)$. □

V.7 2013-11-20

V.7.1 Proof of claim (4)

Continuing from before, it remains to prove:

(4) $A(E)$ is finite if $U(R)/U(R)^2$ is finite.

[Here $E : y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$, $\alpha_i \in R$ UFD, field of fractions K.]

Once (4) is done, assuming $U(R)/U(R)^2$ is finite, we have $E(K)/2E(K)$ is finite.

Proof of (4). Let $a \in K^\times$ with image $\bar{a} \in A(E)$. Since R is a UFD, $a = u\prod_{i=1}^s p_i^{k_i}$ for some unit $u \in R^\times$, k_i even if $p_i \notin P(E)$. So

$$\bar{a} = \bar{u}\prod_{i=1}^s p_i^{\bar{k}_i} \ \left(\mathrm{mod}^\times\, K^{\times 2}\right),$$

where $\bar{k}_i \in \{0,1\} = k_i \pmod 2$. Since $P(E)$ and $U(R)/U(R)^2$ are finite, there are finitely many possibilities and we can omit any primes not in $P(E)$. □

V.7.2 Finiteness of 2-torsion

We assume E is an elliptic curve over $\mathbb{Q}$, defined by

$$y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3),$$

where $\alpha_i \in \overline{\mathbb{Q}}$. Let $K = \mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)$. This is a Galois extension of $\mathbb{Q}$.

Let $\mathcal{O}$ be the ring of integers of K. The ring $\mathcal{O}$ might not be a UFD. So, for any finite set S of prime ideals of $\mathcal{O}$, let $\mathcal{O}_S = \bigcap_{\mathfrak{p}\notin S}\mathcal{O}_\mathfrak{p}$, where $\mathcal{O}_\mathfrak{p}$ is the localization at $\mathfrak{p}$.

Fact V.7.1 (Tate, "Stark's Conjecture", p. 22). There exists S such that $\mathcal{O}_S$ is a PID, hence a UFD. (This follows from the finiteness of the ideal class group of $\mathcal{O}$.)

Fact V.7.2. The group of units $U(\mathcal{O}_S)$ is finitely generated (Dirichlet's unit theorem), so $U(\mathcal{O}_S)/U(\mathcal{O}_S)^2$ is finite.

Taking $R = \mathcal{O}_S$, we can now conclude that $E(K)/2E(K)$ is finite.

V.7.3 Mordell's theorem

Theorem V.7.3. *If L/K is a finite Galois extension such that $E(L)/mE(L)$ is finite, then $E(K)/mE(K)$ is finite.*

Corollary V.7.4. *$E(\mathbb{Q})/2E(\mathbb{Q})$ is finite for any elliptic curve E over $\mathbb{Q}$.*

Corollary V.7.5 (Mordell)**.** *$E(\mathbb{Q})$ is a finitely generated abelian group for any elliptic curve E over $\mathbb{Q}$.*

Proof of Theorem V.7.3. Let $K \hookrightarrow L$ be a finite Galois extension. Let

$$\Phi = \ker\big(E(K)/mE(K) \to E(L)/mE(L)\big) = \frac{E(K) \cap mE(L)}{mE(K)}.$$

Let $P \in E(K) \cap mE(L)$, and let $Q_P \in E(L)$ such that $P = mQ_P$. Define a map

$$\begin{aligned} \lambda_P : \mathrm{Gal}(L/K) &\to E[m] \\ \sigma &\mapsto \sigma(Q_P) - Q_P. \end{aligned}$$

(This is a 1-cocycle.) This is indeed well-defined: since $P \in E(K)$,

$$m\big(\sigma(Q_P) - Q_P\big) = \sigma(P) - P = 0.$$

Suppose $\lambda_P = \lambda_{P'}$. Then, for all σ,

$$\begin{aligned} \sigma(Q_P) - Q_P &= \sigma(Q_{P'}) - Q_{P'}, \\ \sigma(Q_P - Q_{P'}) &= Q_P - Q_{P'}, \end{aligned}$$

so $Q_P - Q_{P'} \in E(K)$. Thus $P - P' = mQ_P - mQ_{P'} \in mE(K)$, so

$$\begin{aligned} \Phi &\to \mathrm{Hom}_{\mathbf{Set}}(\mathrm{Gal}(L/K), E[m]) \\ P &\mapsto \lambda_P \end{aligned}$$

is injective. Since $\mathrm{Gal}(L/K)$ and $E[m]$ are finite, so is Φ. Hence, we have an exact sequence

$$0 \to \Phi \to E(K)/mE(K) \to E(L)/mE(L),$$

and since $E(L)/mE(L)$ is finite by assumption, it follows that $E(K)/mE(K)$ is finite. □

So $E(\mathbb{Q}) \cong \mathbb{Z}^{r_E} \oplus \mathrm{Tors}(E(\mathbb{Q}))$, where r_E is finite and $\mathrm{Tors}(E(\mathbb{Q}))$ is a finite abelian group.

V.7.4 Descent by 2-isogeny

Recall the isogeny

$$\begin{aligned} E = E[a, b] &\xrightarrow{\phi} E[-2a, a^2 - 4b] = E', \\ (x, y) &\mapsto \left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2}\right). \end{aligned}$$

We also have a map

$$\begin{aligned} \alpha_E : E(\mathbb{Q}) &\to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}, \\ (x, y) &\mapsto x \ \big(\mathrm{mod}^\times\, \mathbb{Q}^{\times 2}\big). \end{aligned}$$

Earlier, we saw that $\mathrm{Im}\,\phi = \ker \alpha_E$, and

$$\mathrm{Im}\,\alpha_E \subseteq \left\{ \pm \prod p_i^{\varepsilon_i} \;\middle|\; p_i \text{ factor of } b,\ \varepsilon_i \in \{0, 1\} \right\}.$$

How to find $\operatorname{Im}\alpha_E$? Go back to the method:

$$x = \frac{m}{e^2}, \qquad\qquad y = \frac{n}{e^3},$$

where $(m, e) = (n, e) = 1$. Plug into the equation for E:

$$n^2 = m\left(m^2ame^2 + be^4\right).$$

Let $d = \gcd(m, m^2+ame^2+be^4)$. Then $d \mid be^4$, so $d \mid b$. Write $m = M^2d$ and $m^2+ame^2+be^4 = N^2d$ for some M, N. So,

$$x = \frac{dM^2}{e^2} \implies \alpha_E(x, y) = d\left(\operatorname{mod}^\times \mathbb{Q}^{\times 2}\right).$$

Which divisors d of b actually arise? Say $b = dd'$, and ask if $d \in \operatorname{Im}\alpha_E$. We want to solve

$$\begin{aligned} m &= M^2d, \\ m^2 + ame^2 + be^4 &= N^2d. \end{aligned}$$

Plug the first into the second:

$$\begin{aligned} M^4d^2 + aM^2de^2 + be^4 &= N^2d \\ N^4d + aM^2e^2 + d'e^4 &= N^2. \end{aligned}$$

Question: Does this have rational points (M, N) on it? (Check for each $dd' = b$.)

In fact, this is a genus 1 curve which is isomorphic over $\overline{\mathbb{Q}}$ to the original curve E. This is called a *homogeneous space* for E.

Example V.7.6. Take $y^2 = x^3 + 4x$ ($a = 0,\ b = 4$). Then C_d is given by $M^4d + d'e^4 = N^2$. Possible d: $\pm1, \pm2$.

Chapter VI

Computing Rank and Torsion

VI.1 2013-11-22

Continuing from last time, we have $\alpha_E : E(\mathbb{Q}) \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, where $E = E[a,b] : y^2 = x^3 + ax^2 + bx$. Recall that

$$\operatorname{Im}\alpha_E \subseteq \left\{ \pm \prod p_i^{e_i} \mid p_i \text{ prime factors of } b,\ e_i \in \{0,1\} \right\}.$$

Which factors of b arise? Say $d \mid b$, and write $b = dd'$. We reduced the question to: Does

$$C_d : M^4 d + aM^2e^2 + d'e^4 = N^2$$

have rational points?

VI.1.1 Homogeneous spaces example

Consider $y^2 = x^3 + 4x$, $b = 4$. Consider $d = \pm 1, \pm 2$:

d	C_d	points? (M,N,e)
1	$M^4 + 4e^4 = N^2$	$(0,2,1)$
2	$2M^4 + 2e^4 = N^2$	$(1,2,1)$
-1	$-M^4 - 4e^4 = N^2$	No (no solutions over $\mathbb{R}$)
-2	$-2M^4 - 2e^4 = N^2$	No (no solutions over $\mathbb{R}$)

So $|\operatorname{Im}\alpha_E| = 2$. In particular, $\operatorname{Im}\alpha_E = \{1,2\}$.

Let $E' = E[-2a, a^2 - 4b]$, so $E' : y^2 = x^3 - 16x$. What about $\alpha_{E'}$? Possible d: $\pm 1, \pm 2, \pm 4, \pm 8, \pm 16$, but we can rule out $\pm 4, \pm 8, \pm 16$.

d	C_d	(M,N,e)?
1	$M^4 - 16e^4 = N^2$	$(2,0,1)$
2	$2M^4 - 8e^4 = N^2$	No solutions (argue mod 2^k)
-1	$-M^4 + 16e^4 = N^2$	$(2,0,1)$
-2	$-2M^4 + 8e^4 = N^2$	No solutions (argue mod 2^k)

(If n is even, then $4 \mid N^2 \implies 2 \mid M \implies 32 \mid 2M^4 \implies 8 \mid N^2 \implies 16 \mid N^2 \implies 2 \mid e$, a contradiction by reason of infinite descent.) So $|\operatorname{Im} \alpha_{E'}| = 2$.

Coming soon:

$$2^{r_E} = \frac{1}{4} |\operatorname{Im} \alpha_E| \, |\operatorname{Im} \alpha_{E'}| \, ,$$

so for this E, $2^{r_E} = \frac{1}{4} 2 \cdot 2 = 1$, so $r_E = 0$.

Remark VI.1.1. This proves Fermat's Last Theorem for $n = 4$: If $y^2 = x^3 + 4x$, set $x = \frac{2(u+1)}{v^2}$, $y = \frac{4(u+1)}{v^3}$, so $u^2 = 1 - v^4$. IF $a^4 + b^4 = c^4$, then

$$\left(\left(\frac{a}{c} \right)^2 \right)^2 = 1 - \left(\frac{b}{c} \right)^4 .$$

VI.1.2 Tate–Shafarevich group

Each elliptic curve over $\mathbb{Q}$ has a *Tate–Shafarevich group* Ш:

$$Ш(E) \stackrel{\text{def}}{=} \ker \Big(H^1\big(G_{\mathbb{Q}}, E(\overline{\mathbb{Q}})\big) \to \prod_{p \le \infty} H^1\big(G_{\mathbb{Q}_p}, E(\overline{\mathbb{Q}_p})\big) \Big).$$

Theorem VI.1.2 (Rubin, 1987)**.** *For $y^2 = x^3 + 4x$,* $Ш = \{1\}$.

Conjecture VI.1.3. Ш *is always finite.*

[Several cases proven by Rubin, Kolyvagin.]

Example VI.1.4. Consider

$$E : y^2 = x^3 + 17x,$$
$$E' : y^2 = x^3 - 68x.$$

C_d for E' ($d = 2$) is: $2M^4 - 34e^4 = N^2$. This has local solutions in every completion of $\mathbb{Q}$, but no global solutions.

Set $u = \frac{M}{e}$, $v = \frac{N}{2e^2}$. Then $2u^4e^4 - 32e^4 = 4e^4v^2$, so $u^4 - 17 = 2v^2$ (Lind 1940, Reichardt 1942).

Example VI.1.5 (Selmer). $3x^3 + 4y^3 = 5z^3$ has no global, but everywhere local solutions. [This is a homogeneous space for $x^3 + y^3 = 60$.]

VI.1.3 Systematic computation of α_E

Consider $E : y^2 = x^3 + Dx$, where D is a prime. The image $\operatorname{Im} \alpha_E$ contains possibly $\pm 1, \pm D$.

d	C_d	(M, N, e)?
1	$M^4 + De^4 = N^2$	$(1, 1, 0)$
D	$DM^4 + e^4 = N^2$	$(0, 1, 1)$
-1	$-M^4 - De^4 = N^2$	None over $\mathbb{R}$
$-D$	$-DM^4 - e^4 = N^2$	None over $\mathbb{R}$

So $|\operatorname{Im}\alpha_E| = 2$.

What about $E' : y^2 = x^3 - 4Dx$? Suppose $D \equiv 5 \pmod 8$. We can rule out $2, 2D, -2, -2D$ by 2-adic or D-adic arguments.

d	C_d	(M, N, e)?
1		
D		
-1		
$-D$		

So $|\operatorname{Im}\alpha_{e'}| \le 4$. If it is equal to 4, then $2^{r_E} = \frac{1}{4}|\operatorname{Im}\alpha_E|\,|\operatorname{Im}\alpha_{E'}| = 2$, so $r_E = 1$.

So, in general, $r_E = 0$ or 1, but $r_E = 0$ should never happen here. In fact, for $D \equiv 5 \pmod 8$, $L(E, s)$ has odd analytic rank since $\Lambda(E, s) = -\Lambda(E, 2 - s)$.

Example VI.1.6 (Cassels–Bremner). For $D = 877$, C_D is given by

$$\begin{aligned} e &= 4612160965, \\ M &= 8547136197, \\ N &= 61277608318794736811. \end{aligned}$$

VI.2 2013-11-25

VI.2.1 Rank and torsion, continued

If D is a positive prime $\equiv 5 \pmod 8$, then $E : y^2 = x^3 + Dx$ has $r_E = 0$ or 1, by looking at homogeneous spaces C_d.

Fact VI.2.1. $\Lambda(E, 2 - s) = -\Lambda(E, s)$, so the analytic rank is odd.

Then by the weak BSD conjecture, $r_E = 1$ for the above curve E.

Greenberg showed that E has CM and $L(E, s)$ has a zero of odd order at $s = 1$. Thus, $r_E \ge 1$ or Ш is monstrous. So whenever Rubin shows Ш is finite, then $r_E = 1$. (Consequently, $E(\mathbb{Q}) \cong \mathbb{Z}/2 \oplus \mathbb{Z}$, and $n^2 = DM^2 - 4e^4$ has an integer solution with $e \ne 0$.) (cf. Pell's equation $x^2 + Dy^2 = 1$)

Theorem VI.2.2. *If $E = E[a, b]$ and $E' = E[-2a, a^2 - 4b]$, then $2^{r_E} = \frac{1}{4}|\operatorname{Im}\alpha_E|\,|\operatorname{Im}\alpha_{E'}|$.*

Proof. Calculate $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ in two ways:

(1) $E(\mathbb{Q}) \cong \operatorname{Tors} \oplus \mathbb{Z}^{r_E}$, so $E(\mathbb{Q})/2E(\mathbb{Q}) \cong \operatorname{Tors}/2\operatorname{Tors} \oplus (\mathbb{Z}/2)^{r_E}$, and so

$$|E(\mathbb{Q})/2E(\mathbb{Q})| = 2^{t+1+r_E}.$$

Indeed, consider points in E if order 2: We have at least one point, $(0, 0)$. Writing $y^2 = x(x^2 + ax + b)$, we have more points of order 2 if $x^2 + ax + b$ factors over $\mathbb{Q}$, which happens $\iff$ $a^2 - 4b$ is a square. Thus,

$$2^{t+1} = \#\{\text{points in } E(\mathbb{Q}) \text{ of order 1 or 2}\} = \begin{cases} 2 & \text{if } a^2 - 4b \ne \square \quad (t = 0), \\ 4 & \text{if } a^2 - 4b = \square \quad (t = 1). \end{cases}$$

(2) We have a filtration $E(\mathbb{Q}) \supseteq \overline{\phi}E'(\mathbb{Q}) \supseteq \overline{\phi}\phi E(\mathbb{Q}) = 2E(\mathbb{Q})$, and exact sequences

$$E'(\mathbb{Q}) \xrightarrow{\overline{\phi}} E(\mathbb{Q}) \xrightarrow{\alpha_E} \mathbb{Q}^\times/\mathbb{Q}^{\times 2},$$
$$E(\mathbb{Q}) \xrightarrow{\phi} E'(\mathbb{Q}) \xrightarrow{\alpha_{E'}} \mathbb{Q}^\times/\mathbb{Q}^{\times 2}.$$

So $\left|E(\mathbb{Q})/\overline{\phi}E'(\mathbb{Q})\right| = |E(\mathbb{Q})/\ker\alpha_E| = |\operatorname{Im}\alpha_E|$. We have

$$E'(\mathbb{Q}) \xrightarrow{\overline{\phi}} \overline{\phi}E'(\mathbb{Q}) \longrightarrow \overline{\phi}E'(\mathbb{Q})/\overline{\phi}\phi E(\mathbb{Q}),$$

and P is in the kernel $\iff P \in \phi E(\mathbb{Q}) + \ker\overline{\phi}$. So

$$\left[\overline{\phi}E'(\mathbb{Q}) : \overline{\phi}E'(\mathbb{Q})/\overline{\phi}\phi E(\mathbb{Q})\right] = \begin{cases} [E'(\mathbb{Q}) : \phi E(\mathbb{Q})] & \text{if } (0,0) \in \phi E(\mathbb{Q}), \\ \frac{1}{2}[E'(\mathbb{Q}) : \phi E(\mathbb{Q})] & \text{if } (0,0) \notin \phi E(\mathbb{Q}). \end{cases}$$

But $(0,0) \in \operatorname{Im}\phi \iff (0,0) \in \ker\alpha_{E'} \iff a^2 - 4b = \alpha_{E'}((0,0)) = \square \iff t = 1$, so

$$[E(\mathbb{Q}) : 2E(\mathbb{Q})] = |\operatorname{Im}\alpha_E| \cdot 2^{t-1} \left|\operatorname{Im}\alpha_{E'}\right|.$$

Equating the two expressions for $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ and dividing by 2^{t+1} yields the result. $\square$

VI.2.2 Complete 2-descent

Consider $E : y^2 = (x-e_1)(x-e_2)(x-e_3)$ with $e_i \in R$, where R is a UFD with fraction field K. Recall the maps

$$\theta_i : E(K) \to K^\times/K^{\times 2}$$
$$(x,y) \mapsto x - e_i \quad (x \neq e_i)$$

As before,

$$\operatorname{Im}(\theta_i) \subseteq A(E) = \left\{a \in K^\times/K^{\times 2} \;\middle|\; \operatorname{ord}_p(a) \text{ even } \forall p \in P(E)\right\},$$
$$P(E) = \{\text{primes (up to associates) dividing } e_i - e_j \text{ for some } i \neq j\}.$$

We used the map $(\theta_1, \theta_2, \theta_3) : E(K) \to A(E)^3$ and the fact that $(x,y) \in 2E(K) = \bigcap_{i=1}^3 \ker\theta_i = \ker\theta_1 \cap \ker\theta_2$ if and only if $x - e_i$ is a square for all i.

In fact, we only need θ_1, θ_2 since if $x - e_1, x - e_2$ are squares, then so is $x - e_3$. Let

$$\theta = (\theta_1, \theta_2) : E(K)/2E(K) \hookrightarrow A(E)^2.$$

When is $(a,b) \in \operatorname{Im}\theta$? (Suppose for now that $(a,b) \neq$ image of $\infty, (e_1,0), (e_2,0)$.)

Suppose $(a,b) \in \operatorname{Im}\theta$. Then there exists $(x,y) \in E(K)$ satisfying

$$x - e_1 = au^2, \qquad x - e_2 = bv^2, \qquad x - e_3 = abw^2.$$

Hence, the equations

$$\begin{aligned} au^2 - bv^2 &= e_2 - e_1, \\ au^2 - abw^2 &= e_3 - e_1 \end{aligned} \tag{VI.2.2.1}$$

have solutions $(u, v, w) \in K^\times \times K^\times \times K^\times$. Conversely, if such a solution exists, then

$$x = au^2 + e_1, \qquad y = abuvw$$

is a point on $E(K)$ mapping to (a, b).

In fact, the equations (VI.2.2.1) define a homogeneous space for E, which is an elliptic curve if it has a point. Let

$$S_2 = \left\{(a,b) \in A(E)^2 \;\middle|\; \text{(VI.2.2.1) has a solution } (u,v,w) \text{ locally everywhere}\right\}.$$

We "hope" that for any $(a, b) \in S_2$, a global solution exists. We have a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 1 & \longrightarrow & E(K)/2E(K) & \xrightarrow{\theta} & S_2 & \longrightarrow & Ш[2] & \longrightarrow & 1 \\ & & \uparrow & & \uparrow{\scriptstyle \beta_m} & & \uparrow{\scriptstyle [2^{m-1}]} & & \\ 1 & \longrightarrow & E(K)/2^mE(K) & \longrightarrow & S_{2^m} & \longrightarrow & Ш[2^m] & \longrightarrow & 1 \end{array}$$

This yields an exact sequence

$$E(K) \to \operatorname{Im}\beta_m \to 2^{m-1}Ш[2^m] \to 1.$$

VI.3 2013-11-27

VI.3.1 2-descent, continued

As before, consider $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$ with $e_1, e_2, e_3 \in K$. We have a map

$$\theta = (\theta_1, \theta_2) : E(K)/2E(K) \hookrightarrow A(E)^2$$

and the group

$$S_2 = \left\{(a,b) \in A(E)^2 \;\middle|\; \begin{array}{c} au^2 - bv^2 = e_2 - e_1 \\ au^2 - abw^2 = e_3 - e_1 \end{array} \text{ has a solution locally everywhere}\right\}.$$

Find $\operatorname{Im}\theta = \{\ldots \text{has a solution globally everywhere}\} \subseteq S_2$.

Example VI.3.1 ([Sil]). Let $K = \mathbb{Q}$ and $E : y^2 = x(x-2)(x-10)$, so that $e_1 = 0,\ e_2 = 2,\ e_3 = 10$. Then $P(E) = \{2, 5\}$ and

$$\mathbb{Q}^\times/\mathbb{Q}^{\times 2} \geq A(E) = \{\pm 1, \pm 2, \pm 5, \pm 10\} = \langle -1, 2, 5\rangle.$$

The equations under consideration are:

$$au^2 - bv^2 = 2, \qquad au^2 - abw^2 = 10.$$

If $a < 0$ and $b > 0$ (resp., $b < 0$), then the first equation (resp., the second equation) has no solutions in $\mathbb{R}$, so none in $\mathbb{Q}$. A computation yields the following table:

	1	2	5	10
1	✓	✓	X	X
2	X	X	✓	✓
5	X	X	X	X
10	X	X	X	X
-1	✓	✓	X	X
-2	X	X	✓	✓
-5	X	X	X	X
-10	X	X	X	X

$$\begin{aligned}\theta(\infty) &= (1,1)\\ \theta((0,0)) &= (20,-2) = (5,-2)\\ \theta((2,0)) &= (2,-16) = (2,-1)\\ \theta((10,0)) &= (10,8) = (10,2)\end{aligned}$$

Let $(a,b) = (1,-1)$. The equations $u^2+v^2 = 2,\ u^2+w^2 = 10$ have a solution $(1,1,3)$, giving a point $(au^2 = e_1, abuvw) = (1,-3)$. So $(1,-1) \in \operatorname{Im}\theta$, whence $(5,2),(2,1),(10,-2) \in \operatorname{Im}\theta$.

- Case: $5 \nmid a,\ 5 \mid b$. Let $u = \frac{U}{e},\ v = \frac{V}{e},\ w = \frac{W}{e}$, where U,V,W,e are integers. The equations become:

$$\begin{aligned}aU^2 - bV^2 &= 2e^2,\\ aU^2 - abW^2 &= 10e^2.\end{aligned}$$

  So $5 \mid aU^2$, hence $5 \mid U$, so $5 \mid 2e^2$, so $5 \mid e$. Set $U = 5U'$ and $e = 5e'$. Then

$$25a(U')^2 - bV^2 = 50(e')^2,$$

  whence $5 \mid V$. Likewise, $5 \mid W$. But by infinite descent, this is a contradiction.

- Next case: Multiply by $(5,2)$.

- Case: $(a,b) = (1,2)$. Equations:

$$u^2 - 2v^2 = 2, \qquad\qquad u^2 - 2w^2 = 10.$$

  Note that 2 is not a square mod 5, so $u^2 \equiv 2w^2 \pmod 5$, so $u^2 - 2w^2 \equiv 0 \pmod{25}$. But $10 \not\equiv 0 \pmod{25}$. Exclude it 5-adically.

Conclusion: $|E(\mathbb{Q})/2E(\mathbb{Q})| = 8$. Moreover, $|S_2| = 8$, so $|Ш[2]| = 1$ (no local-to-global problems).

VI.3.2 Computation of $E(\mathbb{Q})$

What is $E(\mathbb{Q})$? Need to know $\mathrm{Tors}(E(\mathbb{Q})) \hookrightarrow E(\mathbb{F}_p)$, where p is an odd prime of good reduction. Here, $p = 3$ works. We have

$$E(\mathbb{F}_3) = \{\infty, (0,0), (2,0), (1,0)\} \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2.$$

But $\mathrm{Tors}(E(\mathbb{Q}))$ has order at least 4, because $\infty, (0,0), (2,0), (10,0) \in \mathrm{Tors}(E(\mathbb{Q}))$. Hence $\mathrm{Tors}(E(\mathbb{Q})) \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$. But

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong \mathrm{Tors}\,/(2\,\mathrm{Tors}) \oplus (\mathbb{Z}/2)^{r_E},$$

so $r_E = 1$. Thus,

$$E(\mathbb{Q}) \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}.$$

We'd also like to know the generators of the above decomposition. We know the generators of each $\mathbb{Z}/2$, and can find a generator of the $\mathbb{Z}$-component using height estimations.

VI.3.3 Rank and congruence

Theorem VI.3.2. *Let p be an odd prime. Let $E : y^2 = x^3 - p^2x = x(x-p)(x+p)$. Then:*

(1) $r_E = 0$ *if* $p \equiv 3 \pmod 8$,

(2) $r_E \leq 1$ *if* $p \equiv 5$ *or* $7 \pmod 8$,

(3) $r_E \leq 2$ *if* $p \equiv 1 \pmod 8$.

Remark VI.3.3. Recall that p is congruent $\iff r_E = 1$. So the above theorem implies there are infinitely many non-congruent primes.

VI.4 2013-12-02

VI.4.1 Rank and congruence

We now prove the theorem from last time:

Theorem VI.4.1. *Let p be an odd prime. Let $E : y^2 = x^3 - p^2x = x(x-p)(x+p)$. Then:*

(1) $r_E = 0$ *if* $p \equiv 3 \pmod 8$,

(2) $r_E \leq 1$ *if* $p \equiv 5$ *or* $7 \pmod 8$,

(3) $r_E \leq 2$ *if* $p \equiv 1 \pmod 8$.

Observe that $P(E) = \{2, p\}$ and

$$A(E) = \{\pm 1, \pm 2, \pm p, \pm 2p\} = \langle -1, 2, p\rangle \leq \mathbb{Q}^\times/\mathbb{Q}^{\times 2},$$

an $\mathbb{F}_2$-vector space written multiplicatively.

Remark VI.4.2. Recall that if $r = \text{rank}(E(\mathbb{Q}))$, then

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2)^r \oplus \underbrace{(\text{Tors}\,/2\,\text{Tors})}_{\text{order 4}}.$$

We can write $E : y^2 = (x-p)x(x+p)$, so $e_1 = -p$, $e_2 = 0$, and $e_3 = p$. We have corresponding maps $\theta_1, \theta_2, \theta_3$ (in general, $\theta_i(x,y) = x - e_i$).

Map	Image of $(-p,0)$	-1	2	p
θ_1	$2p^2$	0	1	0
θ_2	$-p$	1	0	1
θ_3	$-2p$	1	1	1

Map	Image of $(0,0)$	-1	2	p
θ_1	p	0	0	1
θ_2	$-p^2$	1	0	0
θ_3	$-p$	1	0	1

Map	Image of $(p,0)$	-1	2	p
θ_1	$2p$	0	1	1
θ_2	p	0	0	1
θ_3	$2p^2$	0	1	0

Map	Image of (x,y) $(y \neq 0)$	-1	2	p
θ_1	$x+p$	0, 0	0, 1	0, 0, 1, 1
θ_2	x	0, 1	0, 0	0, 1, 0, 1
θ_3	$x-p$	0, 1	0, 1	0, 1, 1, 0

(In the last column of the last table above, all three nontrivial possibilities arise in the last columns of $(e_i, 0)$.)

To find the image of θ, by adding a 2-torsion point to P, we can assume that $\theta(P)$ has last column $0, 0, 0$ (for generic P). So there are now 4 possibilities for $\theta(P)$, whence $r_E \leq 2$.

Let us consider which of these cases can actually arise:

- The trivial possibility can always arise.
-1	2	p
0	0	0
1	0	0
1	0	0

  $\implies$ $x+p = \square$, $x = -\square$, $x-p = -\square$, so $p = \square + \square$. Hence, $p \equiv 1 \pmod 4$.
-1	2	p
0	1	0
0	0	0
0	1	0

  $\implies$ $x+p = 2\square$, $x = \square$, $x-p = 2\square$, so $p = 2\square - \square$, so $2 \equiv \square \pmod p$.

  By quadratic reciprocity, $p \equiv \pm 1 \pmod 8$.

-1	2	p
0	1	0
1	0	0
1	1	0

$\implies x+p=2\square,\ x=-\square,\ x-p=-2\square$, so $p=2\square+\square$ and $p=2\square-\square$.
Hence, $2, -2$ are both squares mod p, so by quadratic reciprocity, $p\equiv 1 \pmod 8$.

The theorem follows. □

VI.4.2 Root numbers and congruence

If $p\equiv 5$ or $7 \pmod 8$, then the root number of $L(E,s)$ is -1, i.e.,

$$\Lambda(E,2-s)=-\Lambda(E,s).$$

Hence, the order of vanishing of $L(E,s)$ at $s=1$ is odd. The weak BSD conjecture then implies $r=1$ (so p is congruent).

If $p\equiv 1$ or $3 \pmod 8$, then the root number of $L(E,s)$ is $+1$. In this case, weak BSD implies r is even. For $p\equiv 1 \pmod 8$, there are examples with $r=0$ and $r=2$.

Remark VI.4.3. Say $p\equiv 5 \pmod 8$. Then weak BSD implies $r_E=1$. Our analysis says $r_E=1$ if and only if

$$\begin{aligned} x+p&=a^2,\\ x&=-b^2,\\ x-p&=-c^2 \end{aligned}$$

for some $a,b,c\in\mathbb{Q}$. Thus, $a^2=c^2-2b^2$. Diophantus's method finds all rational points on $1=u^2-2v^2$, yielding

$$(a,b,c)=\left((2s^2-r^2)\lambda, 2rs\lambda, (2s^2+r^2)\lambda\right)$$

for some $\lambda\in\mathbb{Q}$. In fact, we can take $\lambda=\frac{1}{n}$ for some n.

VI.4.3 Remarks on 3-descent

Suppose we want to study rational points on $E: x^3+y^3=dz^3$ (Mazur–Rubin). The associated homogeneous spaces are of the form

$$ax^3+by^3=cz^3 \tag{VI.4.3.1}$$

with $abc=d$. A rational solution of (VI.4.3.1) leads to a rational solution of $X^3+Y^3=dZ^3$ with $Z\neq 0$ (but *not* conversely[1]). Euler found

$$\begin{aligned} X+Y&=-9abcx^3y^3z^3,\\ X-Y&=\left(ax^3-by^3\right)\left(by^3-cz^3\right)\left(cz^3-ax^3\right),\\ Z&=3\left(abx^3y^3+bcy^3z^3+caz^3x^3\right)xyz. \end{aligned}$$

[1]Consider, for example, Selmer's example $3x^3+4y^3=5z^3$ of a curve with solutions everywhere locally but not globally ($Ш[3]\neq 0$ for $X^3+Y^3=60Z^3$).

VI.5 2013-12-04 [missing]

VI.6 2013-12-06 [missing]

VI.7 2013-12-09

VI.7.1 Integer points on a curve

Consider $E : y^2 + y = x^3 - x$. Observe:

$$\begin{aligned} P &= (0,0) & 5P &= \left(\frac{1}{4}, -\frac{5}{8}\right) \\ 2P &= (1,0) & 6P &= (6,14) \\ 3P &= (-1,-1) & 7P &= \left(-\frac{5}{9}, \frac{8}{27}\right) \\ 4P &= (2,-3) & 8P &= \left(\frac{21}{25}, -\frac{69}{125}\right) \end{aligned}$$

Claim VI.7.1.

(1) $E(\mathbb{Z}) = \{\pm P, \pm 2P, \pm 3P, \pm 4P, \pm 6P\}$.

(2) $E(\mathbb{Q}) = \langle P \rangle$.

We will return to this example later and prove the claim.

VI.7.2 Torsion over $\mathbb{Q}$

Proposition VI.7.2 (Lutz–Nagell)**.** *Let $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. Then:*

(1) Suppose $P = (x, y)$ and $2P$ have integer coordinates. Then either $y = 0$ or $y^2 \mid \mathrm{Disc}(E)$.

(2) If P is torsion, then P has integer coordinates.

If $2P = \infty$, then $y = 0$. So assume $2P \neq \infty$. Let

$$\begin{aligned} \phi(X) &= X^4 - 2AX^2 - 8BX + A^2, \\ \psi(X) &= X^3 + AX + B. \end{aligned}$$

Recall the *duplication formula*:

$$x(2P) = \frac{\phi(x(P))}{4\psi(x(P))}.$$

But $f(x)\phi(x) - g(x)\psi(x) = 4A^3 + 27B^2$, where $f(x) = 3x^2 + 4A$ and $g(x) = 3x^3 - 5Ax - 27B$. Since $x = x(P)$ and $y(P)^2 = \psi(x(P))$, we have

$$f(x(P))x(2P)4y(P)^2 - g(x(P))y(P)^2 = 4A^3 + 27B^2,$$

we obtain $y(P)^2 \mid 4A^3 + 27B^2$. This completes the proof of (1). □

Now we prove (2). Suppose $(x, y) \in E(\mathbb{Q})$, and p is a prime dividing the denominator of x (i.e., $\mathrm{ord}_p(x) < 0$). Recall $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$ (lowest terms), so

$$\mathrm{ord}_p(x) = \frac{3}{2}\,\mathrm{ord}_p(y).$$

Define a filtration $E(\mathbb{Q}) \supseteq E_1(\mathbb{Q}) \supseteq E_2(\mathbb{Q}) \supseteq \dots$ by

$$E_k(\mathbb{Q}) = \{\infty\} \cup \left\{(x, y) \in E(\mathbb{Q}) \;\middle|\; \mathrm{ord}_p(x) \le -2k,\ \mathrm{ord}_p(y) \le -3k\right\}$$

for $k \ge 1$. This is a subgroup: Let $t = \frac{x}{y}$ and $s = \frac{1}{y}$ (so $y = \frac{1}{s}$ and $x = \frac{t}{s}$). In the (t, s)-plane, we get all points except where $y = 0$. The point at ∞ corresponds to $(0, 0)$ in the (t, s)-plane. Let

$$R = \mathbb{Z}_{(p)} = \{0\} \cup \left\{x \in \mathbb{Q}^\times \;\middle|\; \mathrm{ord}_p(x) \ge 0\right\}.$$

This is a DVR with unique nonzero prime ideal pR. One can check that $(x, y) \in E_k(\mathbb{Q})$ if and only if $t \in p^k R$ and $s \in p^{3k}R$. (Assume $a_1 = 0$.) Furthermore, if $P_1, P_2 \in E_k(\mathbb{Q})$, then $t(P_1)+t(P_2)-t(P_1+P_2) \in p^{3k}$, so $E_k(\mathbb{Q})$ is indeed a subgroup. We also get a homomorphism

$$E_k(\mathbb{Q}) \xrightarrow{t} p^k R/p^{3k}R$$

with kernel $E_{3k}(\mathbb{Q})$, giving an injective homomorphism

$$E_k(\mathbb{Q})/E_{3k}(\mathbb{Q}) \hookrightarrow p^k R/p^{3k}R \cong \mathbb{Z}/p^{2k}\mathbb{Z}.$$

So $E_k(\mathbb{Q})/E_{3k}(\mathbb{Q})$ is cyclic of order p^m, where $0 \le m \le 2k$.

Lemma VI.7.3. *$E_1(\mathbb{Q})$ contains no points of finite order (other than the point at ∞).*

Proof. Say the order of $P \in E_1(\mathbb{Q})$ is $m \ne 1$. Then $P \in E_k(\mathbb{Q})$ and $P \notin E_{k+1}(\mathbb{Q})$ for some $k \ge 1$.

Case 1: If $p \nmid m$, then $t(mP) \equiv mt(P) \pmod{p^{3k}R}$, so $mP = \infty$, whence $mt(P) \equiv 0$, and so $t(P) \equiv 0 \pmod{p^{3k}R}$. But then $P \in E_{3k}(\mathbb{Q})$, a contradiction since $3k \ge k + 1$.

Case 2: If $p \mid m$, write $m = pn$ and $P' = nP$. Then P' has order p, and $P \in E_1(\mathbb{Q})$, so $P' \in E_1(\mathbb{Q})$. Say $P' \in E_k(\mathbb{Q}) \setminus E_{k+1}(\mathbb{Q})$. Then

$$0 \equiv pt(P') \pmod{p^{3k}R},$$

whence $t(P') \in p^{3k-1}R$. But $3k - 1 \ge k + 1$, contradiction. □

Now we finish the proof of (2). If $P \in \mathrm{Tors}(E(\mathbb{Q}))$, then $P \notin E_1(\mathbb{Q})$ for any prime p. Thus, the denominators of x and y are not divisible by any prime p, whence $x, y \in \mathbb{Z}$. □

Example VI.7.4. The curve $E : y^2 = x^3 + 3$ has discriminant -3^5. By Lutz–Nagell, look at $y \in \{0, \pm 1, \pm 3, \pm 9\}$; none work. Thus $|E(\mathbb{F}_5)| = 6$ and $|E(\mathbb{F}_7)| = 13$, so $\mathrm{Tors}(E(\mathbb{Q})) = \{\infty\}$.

VI.8 2013-12-11

VI.8.1 Integer points on a curve, continued

Let us return to the example $E : y^2 + y = x^3 - x$ from the beginning of last class. Recall:

$$\begin{aligned} P &= (0,0) & 5P &= \left(\frac{1}{4}, -\frac{5}{8}\right) \\ 2P &= (1,0) & 6P &= (6,14) \\ 3P &= (-1,-1) & 7P &= \left(-\frac{5}{9}, \frac{8}{27}\right) \\ 4P &= (2,-3) & 8P &= \left(\frac{21}{25}, -\frac{69}{125}\right) \end{aligned}$$

Moreover,

$$|E(\mathbb{F}_2)| = 5, \qquad |E(\mathbb{F}_3)| = 7, \qquad |E(\mathbb{F}_5)| = 8.$$

Theorem VI.8.1.

(1) The only integer-valued points on E are $\pm P, \pm 2P, \pm 3P, \pm 4P, \pm 6P$.

(2) $E(\mathbb{Q}) = \langle P \rangle$.

Remark VI.8.2. $E^0(\mathbb{R})$, the connected component of identity, is a subgroup of $E(\mathbb{R})$ of index 2.

Proof of theorem. If p is odd and of good reduction, then we have an injection $\mathrm{Tors}(E(\mathbb{Q})) \hookrightarrow E(\mathbb{F}_p)$. Thus, $|\mathrm{Tors}(E(\mathbb{Q}))| = 1$.

Suppose for now that $\mathrm{rank}(E(\mathbb{Q})) = 1$. (We'll prove this in a moment.) Then $E(\mathbb{Q}) \cong \mathbb{Z}$; let Q be a generator. Then Q is on the "egg" (the connected component of $E(\mathbb{R})$ not containing the identity) (else $E(\mathbb{Q}) \leq E^0(\mathbb{R})$). If Q has p in the denominator of its coordinates, then so does any multiple of $\mathbb{Q}$, so every point in $E(\mathbb{Q})$ would. So Q has integer coordinates.

The egg is bounded, so by compactness, there are only finitely many points on the egg with integer coordinates. Check them: $\pm P, \pm 3P$. So $Q = \pm Q$, whence $E(\mathbb{Q}) = \langle P \rangle$.

Next, suppose mP has integer coordinates (where $m \geq 1$ is an integer). Say $m = m_0 2^r$ (with m_0 odd). Then $m_0 P$ is on the egg, so $m_0 \in \{1, 3\}$.

Claim. $r \leq 2$.

Indeed, look at $8P$. The image in $E(\mathbb{F}_5)$ is the point at ∞. If $8 \mid m$, then the same is true for mP, which has 5 in the denominator. Thus $8P$ has non-5-integer coordinates, so $m \mid 12$. □

VI.8.2 Rank of the curve

Now we show that $\operatorname{rank}(E(\mathbb{Q})) = 1$.

It's enough to prove $|E(\mathbb{Q})/2E(\mathbb{Q})| = 2$, hence enough to show $E^0(\mathbb{R}) \cap E(\mathbb{Q}) \subseteq 2E(\mathbb{Q})$ since $[E(\mathbb{Q}) : E^0(\mathbb{R}) \cap E(\mathbb{Q})] = 2$. Let α be a root of $x^3 - 4x + 2$. Then $\frac{\alpha}{2}$ is a root of $x^3 - x + \frac{1}{4}$, so

$$\left(y + \frac{1}{2}\right)^2 = x^3 - x + \frac{1}{4} = N_{K/\mathbb{Q}}\left(x - \frac{\alpha}{2}\right),$$

where $K = \mathbb{Q}(\alpha)$. (Note that $K/\mathbb{Q}$ is a cubic extension.) We have the homomorphism

$$\begin{aligned} E(\mathbb{Q}) &\xrightarrow{\theta} K^\times/K^{\times 2}, \\ (x, y) &\mapsto x - \frac{\alpha}{2}. \end{aligned}$$

Claim. $\ker\theta = 2E(\mathbb{Q})$.

Indeed, $x - \frac{\alpha}{2}$ is a square in $\mathbb{Q}(\alpha) \iff x - \frac{\sigma(\alpha)}{2}$ is a square in $\mathbb{Q}(\sigma(\alpha))$, where σ is a permutation of $\{\alpha, \beta, \gamma\}$, where α, β, γ are the roots of $x^3 - 4x + 2$, proving the claim.

So $E(\mathbb{Q})/2E(\mathbb{Q}) \overset{\theta}{\hookrightarrow} K^\times/K^{\times 2}$.

Claim. $\operatorname{Im}\theta \subseteq B/K^{\times 2}$, *where* B *is the subgroup of* $K^\times$ *of elements with norm in* $\mathbb{Q}^{\times 2}$.

Say $(x, y) \in E(\mathbb{Q})$. Then $(x, y) \in E^0(\mathbb{R}) \iff x - \frac{\alpha}{2}, x - \frac{\beta}{2}, x - \frac{\gamma}{2}$ are all positive $\iff x - \frac{\alpha}{2}$ is *totally positive*.[2]

It's enough to prove that, if $x \in \mathbb{Q}$ has $N_{K/\mathbb{Q}}\left(x - \frac{\alpha}{2}\right) \in \mathbb{Q}^{\times 2}$ and $x - \frac{\alpha}{2}$ is totally positive, then $x - \frac{\alpha}{2}$ is a square in K.

Claim. *(i)* K *has class number* 1, *so* $\mathcal{O}_K = \mathbb{Z}[\alpha]$ *is a PID.*

(ii) The totally positive units of K *are all squares.*

Proof. (i) If $\alpha \in \mathcal{O}_K$, then $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$. Let $f(x) = x^3 - 4x + 2$ (Eisenstein at 2). Then $\operatorname{Disc}(f) = 148 = 2^2 \cdot 37$, and $\operatorname{Disc}(\mathcal{O}_K) \mid \operatorname{Disc}(\mathbb{Z}[\alpha])$ with quotient a square. Thus $\operatorname{Disc}(\mathcal{O}_K) = 37$ or 148. But if $\operatorname{Disc}(\mathcal{O}_K) = 37$, then 2 is unramified, which contradicts f Eisenstein because $(2) = (\alpha)^3$. So $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

By the Minkowski bound, every ideal class contains an integral ideal with norm $< \frac{3!}{3^3}\sqrt{148} < 3$. Since $(2) = (\alpha)^3$ is principal, it follows that $\mathcal{O}_K$ is a PID.

(ii) Note that $f(-2) = 2$, $f(1) = -1$, and $f(2) = 2$. So $\alpha < -2 < \beta < 1 < \gamma < 2$. By Dirichlet's unit theorem,

$$\mathcal{O}_K^\times = U_K \cong \mathbb{Z}^2 \oplus \{\pm 1\}.$$

What are the fundamental units? Set $\epsilon = \frac{2+\alpha}{2-\alpha}$ and $\eta = 1 - \alpha$. Note that $N(2 + \alpha) = N(2 - \alpha) = 2$ and $N(1 - \alpha) = 1$, so ϵ and η are units. We have

$$U_K = \langle \epsilon, \eta \rangle \oplus \{\pm 1\},$$

[2] This means that every embedding in the reals is positive.

so all units are of the form $\pm\epsilon^i\eta^j$. Let U_K^+ denote the set of totally positive units. Then

$$U_K^2 \subseteq U_K^+ \subseteq U_K,$$

and the index $[U_K : U_K^2]$ is 8. Since all sign possibilities are, the index $[U_K : U_K^+]$ is also 8. Hence, $U_K^2 = U_K^+$. □

Now we return to prove that, if $x \in \mathbb{Q}$ has $N_{K/\mathbb{Q}}\left(x - \frac{\alpha}{2}\right) \in \mathbb{Q}^{\times 2}$ and $x - \frac{\alpha}{2}$ is totally positive, then $x - \frac{\alpha}{2} \in K^{\times 2}$, i.e., that $\operatorname{ord}_p\left(x - \frac{\alpha}{2}\right)$ is even $\forall p$.

VI.9 2013-12-13

VI.9.1 Rank of the curve, continued

Recall: $K = \mathbb{Q}(\alpha)$, where α is a root of $x^3 - 4x + 2 = 0$. It's enough to prove: If $x \in \mathbb{Q}$ has $N_{K/\mathbb{Q}}\left(x - \frac{\alpha}{2}\right) \in \mathbb{Q}^{\times 2}$ and $x - \frac{\alpha}{2}$ is totally positive, then $x - \frac{\alpha}{2}$ is a square in K.

We showed that $U_K^2 = U_K^+$. Since K is a PID, it remains to show $\operatorname{ord}_p\left(x - \frac{\alpha}{2}\right)$ is even $\forall p$. Let $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ be a prime over p.

Suppose $\mathfrak{p} \nmid 2, 37$ (the bad primes). The minimal polynomial of $\frac{\alpha}{2}$ is

$$g(x) = x^3 - x + \frac{1}{4} = \left(x - \frac{\alpha}{2}\right)^3 + B\left(x - \frac{\alpha}{2}\right)^2 + C\left(x - \frac{\alpha}{2}\right) = N_{K/\mathbb{Q}}\left(x - \frac{\alpha}{2}\right),$$

where B, C are $\mathfrak{p}$-integral for $\mathfrak{p} \nmid 2$. Set $\operatorname{ord}_\mathfrak{p}(B) = b \geq 0$, $\operatorname{ord}_\mathfrak{p}(C) = c \geq 0$, and $\operatorname{ord}_\mathfrak{p}\left(x - \frac{\alpha}{2}\right) = m$. (We're trying to show m is even.) We know $\operatorname{ord}_\mathfrak{p}\left(N_{K/\mathbb{Q}}\left(x - \frac{\alpha}{2}\right)\right)$ is a square, and

$$\operatorname{ord}_\mathfrak{p}\left(N_{K/\mathbb{Q}}\left(x - \frac{\alpha}{2}\right)\right) \geq \min(3m, 3m + b, m + c).$$

If $m = 0$, then m is even. If $m < 0$, then the above is equal to $3m$, so m is even. If $m > 0$ and $c = 0$, then the above is equal to $m + c = m$, so m is even.

The only remaining case is $m > 0$ and $c > 0$. Let $C = g'\left(\frac{\alpha}{2}\right)$ be the *different*. If $\mathfrak{p} \mid C$, then $p \mid N(C) = \operatorname{Disc} g(x)$, so $p = 2$ or 37.

With a little more number theory (748 Fall), we can do cases $p = 2, 37$. □

VI.9.2 The curve from homework 9

The problem is to find the integer solutions of

$$\frac{u}{v} + \frac{v}{w} + \frac{w}{u} = n.$$

Make a substitution $u = -x$, $v = -y/x$, $w = 1$:

$$\frac{x^2}{y} - \frac{y}{x} - \frac{1}{x} = n$$
$$x^3 - y^2 - y = nxy$$
$$E_n : y^2 + nxy + y = x^3 \qquad (*)$$

To study 2-torsion and rank, put this in the form $y^2 = f(x)$, so that $2y + a_1x + a_3 = 0$. Our case: $2y + nx + a_3 = 0$ (plug back in $(*)$).

Example VI.9.1. If $n = 6$, then $y = -3x - \frac{1}{2}$, so we get $x^3 + 9x^2 + 3x + \frac{1}{4} = 0$, which has $\frac{\alpha}{2}$ as a root. The x-coordinates of 2-torsion points are roots of this polynomial. Search $n = 6$: $u = 2,\ v = 12,\ w = 9$, corresponding to the rational point $\left(-\frac{2}{9}, \frac{8}{27}\right)$.

Let α be a root of $f(x) = x^3 + 18x^2 + 12x + 2$. This is irreducible, Eisenstein at 2, has all real roots, etc. So, let $K = \mathbb{Q}(\alpha)$. In fact, $\mathcal{O}_K = \mathbb{Z}[\alpha]$ is a PID, $U_K \cong \mathbb{Z}^2 \oplus \{\pm 1\}$ and $U_K^+ = U_K^2$ has index 8 in U_K. The map

$$\begin{aligned} E(\mathbb{Q}) &\xrightarrow{\theta} K^\times / K^{\times 2} \\ (x, y) &\mapsto x - \frac{\alpha}{2} \end{aligned}$$

has kernel $2E(\mathbb{Q})$, and $E(\mathbb{Q})/2E(\mathbb{Q}) \overset{\theta}{\hookrightarrow} K^\times/K^{\times 2}$. Moreover, $\mathrm{Im}(B) \subseteq B/K^{\times 2}$, where B is the set of totally positive elements of $K^\times$ with square norm.

By the methods of last time, $\operatorname{rank} E(\mathbb{Q}) = 1$. In particular,

$$E(\mathbb{Q}) \cong \mathbb{Z}/3 \oplus \mathbb{Z},$$

where $\mathbb{Z}$ is generated by $P = \left(-\frac{2}{9}, \frac{8}{27}\right)$.

Extra credit: We want $u, v > 0$, i.e., $x < 0$ and $y > 0$. If you graph $E_6(\mathbb{R})$, it looks like it has a node; however, zooming in shows that there's actually a small gap between the "egg" and the other component. Since there are two components, P must lie on the egg. So the points with $x < 0$ and $y > 0$ are exactly the points on the egg, i.e., nP for n odd.

The next solution is $(u, v, w) = (17415354473, 90655886250, 19286662788)$.

How can we compute things like this in general? Recall that $|h(P) - \hat{h}(P)|$ is bounded; find an explicit bound. Say $P = mQ$ for $m > 1$. Since

$$\hat{h}(Q) = \frac{1}{m^2}\hat{h}(P) \leq \frac{1}{4}\hat{h}(P),$$

we get a bound on $h(Q) = \log(\text{max coordinate})$.

Bibliography

[IR] K. Ireland, M. Rosen (2010). *A Classical Introduction to Modern Number Theory.*

[Maz] B. Mazur, *Number Theory as Gadfly.*

[Sha] I. Shafarevich (1988). *Basic Algebraic Geometry 1.*

[Shi] G. Shimura (1971). *Introduction to Arithmetic Theory of Automorphic Forms.*

[Sil] J. Silverman (2010). *The Arithmetic of Elliptic Curves.*

[ST] J. Silverman and J. Tate (1994). *Rational Points on Elliptic Curves.*

Index