Part III - Elliptic Curves

Lectured by Tom Fisher

Artur Avameri

Contents

0 Introduction

19 Jan 2024, Lecture 1

The best books for the course include *The arithmetic of elliptic curves* by Silverman, Springer 1996, and *Lectures on elliptic curves* by Cassels, CUP 1991.

1 Fermat's Method of Infinite Descent

A right–angled triangle Δ has $a^2 + b^2 = c^2$ and $\text{area}(\Delta) = \frac{1}{2}ab$.

Definition 1.1. Δ is **rational** if $a, b, c \in \mathbb{Q}$. Δ is **primitive** if $a, b, c \in \mathbb{Z}$ are coprime.

Note that a primitive triangle has pairwise coprime side lengths because $a^2 + b^2 = c^2$.

Lemma 1.1. Every primitive triangle is of the form $(u^2 - v^2, 2uv, u^2 + v^2)$ for some integers $u > v > 0$.

Proof. WLOG let a, b, c be odd, even, odd. Then $\left(\frac{b}{2}\right)^2 = \frac{c+a}{2}\frac{c-a}{2}$, where we note that the RHS is a product of positive coprime integers. By unique factorization, $\frac{c+a}{2} = u^2$, $\frac{c-a}{2} = v^2$ for $u, v \in \mathbb{Z}$. This gives the desired result. $\square$

Definition 1.2. $D \in \mathbb{Q}_{>0}$ is a **congruent** number if there exists a rational triangle Δ with $\text{area}(\Delta) = D$.

Note that it suffices to consider $D \in \mathbb{Z}_{>0}$ squarefree.

Example 1.1. $D = 5, 6$ are congruent.

Lemma 1.2. $D \in \mathbb{Q}_{>0}$ is congruent $\iff Dy^2 = x^3 - x$ for some $x, y \in \mathbb{Q}, y \neq 0$.

Proof. Lemma 1.1 shows that D congruent $\implies Dw^2 = uv(u^2 - v^2)$ for some $u, v, w \in \mathbb{Q}, w \neq 0$. This implication also obviously goes the other way. To finish, divide through by w^4 and take $x = \frac{u}{v}, y = \frac{w}{v^2}$. $\square$

Fermat showed that 1 is not a congruent number.

Theorem 1.3. There is no solution to $w^2 = uv(u + v)(u - v)$ for $u, v, w \in \mathbb{Z}, w \neq 0$.

Proof. WLOG assume u, v are coprime and that $u, w > 0$. If $v < 0$, then replace (u, v, w) by $(-v, u, w)$. If u, v are both odd, then replace (u, v, w) by $\left(\frac{u+v}{2}, \frac{u-v}{2}, \frac{w}{2}\right)$. Then $u, v, u+v, u-v$ are pairwise coprime positive integers with their product a square, so by unique factorization in $\mathbb{Z}$, $u = a^2, v = b^2, u + v = c^2, u - v = d^2$ for $a, b, c, d \in \mathbb{Z}$.

Since $u \not\equiv v \pmod 2$, both c and d are odd. Then $\left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 = \frac{c^2+d^2}{2} = u = a^2$. This gives a primitive triangle with area $\frac{c^2-d^2}{8} = \frac{v}{4} = \left(\frac{b^2}{2}\right)$.

Let $w_1 = \frac{b}{2}$, then by Lemma 1.1, $w_1^2 = u_1 v_1 (u_1 + v_1)(u_1 - v_1)$ for some $u_1, v_1 \in \mathbb{Z}$. Hence we have a new solution to our original question, with $4w_1^2 = b^2 = v \mid w^2 \implies w_1 \leq \frac{w}{2}$, so we're done by infinite descent. $\square$

A variant for polynomials. In the above, K is a field with char $K \neq 2$. Let $\overline{K}$ be the algebraic closure of K and consider for this whole section K with char $K \neq 2$.

Lemma 1.4. Let $u, v \in K[t]$ be coprime. If $\alpha u + \beta v$ is a square for 4 distinct $(\alpha : \beta) \in \mathbb{P}^1$, then $u, v \in K$.

Proof. WLOG let $K = \overline{K}$ by extending if necessary. Changing coordinates on $\mathbb{P}^1$ (i.e. multiplying by a 2×2 invertible matrix), we may assume that the points $(\alpha : \beta)$ are $(1 : 0)$, $(0 : 1)$, $(1 : -1)$, $(1 : -\lambda)$ for $\lambda \in K \setminus \{0, 1\}$. Since our field is algebraically closed, let $\mu = \sqrt{\lambda}$. Then $u = a^2, v = b^2, u - v = (a + b)(a - b), u - \lambda v = (a + \mu b)(a - \mu b)$.

Unique factorization in $K[t]$ implies that $a + b, a - b, a + \mu b, a - \mu b$ are squares (since the necessary terms are coprime up to units, i.e. constants). But $\max(\deg(a), \deg(b)) \leq \frac{1}{2} \max(\deg(u), \deg(v))$, so by Fermat's method of infinite descent, $u, v \in K$. $\square$

Definition 1.3. (i) An **elliptic curve** E/K is the projective closure of the plane affine curve $y^2 = f(x)$ (this is called a Weierstrass equation) where $f \in K[x]$ is a monic cubic polynomial with distinct roots in $\overline{K}$.

(ii) For L/K any field extension, $E(L) = \{(x, y) \in L^2 \mid y^2 = f(x)\} \cup \{0\}$ (the point at infinity in the projective closure), it turns out that $E(L)$ is naturally an abelian group.

In this course, we study $E(K)$ for K a finite field, local field, number field.

Lemma 1.2 and Theorem 1.3 show that if $E : y^2 = x^3 - x$, then $E(\mathbb{Q}) = \{0, (0, 0), (\pm 1, 0)\}$.

Corollary 1.5. Let E/K be an elliptic curve. Then $E(K(t)) = E(K)$.

Proof. WLOG $K = \overline{K}$. By a change of coordinates, we may assume $y^2 = x(x - 1)(x - \lambda)$ for some $\lambda \in K \setminus \{0, 1\}$. Suppose $(x, y) \in E(K(t))$. Write $x = \frac{u}{v}$ for $u, v \in K(t)$ coprime. Then $w^2 = uv(u - v)(u - \lambda v)$ for some $w \in K[t]$. Unique factorization in $K[t]$ shows that $u, v, u - v, u - \lambda v$ are all squares, so by Lemma 1.4, $u, v \in K$, so $x, y \in K$. $\square$

2 Some remarks on algebraic curves

22 Jan 2024, Lecture 2

In this section, work over an algebraically closed field $K = \overline{K}$.

Definition 2.1. A plane curve $C = \{f(x,y) = 0\} \subset \mathbb{A}^2$ (for $f \in K[x,y]$ irreducible) is **rational** if it has a rational parametrization, i.e. $\exists \phi, \psi \in K(t)$ such that

(i) The map $\mathbb{A}^1 \to \mathbb{A}^2$ by $t \mapsto (\phi(t), \psi(t))$ is injective on $\mathbb{A}^1 \setminus \{\text{finite set}\}$.

(ii) $f(\phi(t), \psi(t)) = 0$ in $K(t)$.

Example 2.1. (a) Any nonsingular conic is rational. For example, for $x^2 + y^2 = 1$, take a line with slope t through $(-1, 0)$ (the anchor) and solve to get the rational parametrization $(x,y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$.

(b) Any singular plane cubic is rational, for example $y^2 = x^3$ giving $(x,y) = (t^2, t^3)$ with the anchor at the singularity $(0,0)$ and $y^2 = x^2(x+1)$ with the parametrization to be computed on Ex. Sheet 1 (anchor still at $(0,0)$).

(c) Corollary 1.5 shows that elliptic curves are not rational.

Remark. The genus $g(C) \in \mathbb{Z}_{\geq 0}$ is an invariant of a smooth projective curve C. If $K = \mathbb{C}$, then $g(C)$ is the genus of the Riemann surface. A smooth plane curve $C \subset \mathbb{P}^2$ of degree d has genus $g(C) = \frac{(d-1)(d-2)}{2}$.

Proposition 2.1. (Here we still assume $K = \overline{K}$). Let C be a smooth projective curve.

- C is rational (see Definition 2.1) $\iff g(C) = 0$.
- C is an elliptic curve $\iff g(C) = 1$.

Proof. (i) Omitted.

(ii) ($\implies$): Check C is a smooth plane curve in $\mathbb{P}^2$ (see Ex. Sheet 1) and use the above remark.

($\impliedby$): We will see this later.

□

Order of vanishing. Let C be an algebraic curve with function field $K(C)$ and let $P \in C$ be a smooth point. Write $\mathrm{ord}_P(f)$ for the order of vanishing of $f \in K(C)$ at P (which is negative if f has a pole at P).

Fact. $\mathrm{ord}_P : K(C)^\times \to \mathbb{Z}$ is a discrete valuation, i.e. $\mathrm{ord}_P(f_1 f_2) = \mathrm{ord}_P(f_1) + \mathrm{ord}_P(f_2)$ and $\mathrm{ord}_P(f_1 + f_2) \geq \min(\mathrm{ord}_P(f_1), \mathrm{ord}_P(f_2))$.

Definition 2.2. We say $t \in K(C)^\times$ is a **uniformizer** at P if $\mathrm{ord}_P(t) = 1$.

Example 2.2. $C = \{g = 0\} \subset \mathbb{A}^2$ for $g \in K[x,y]$. Then $K(C) = \mathrm{Frac}\left(\frac{K[x,y]}{(g)}\right)$. Write $g = g_0 + g_1(x,y) + g_2(x,y) + \dots$ for g_i homogeneous of degree i. Suppose $P = (0,0)$ is a smooth point, e.g. $g_0 = 0$ and let $g_1(x,y) = \alpha x + \beta y$ with α, β not both zero ($\alpha x + \beta y = 0$ gives a tangent to the curve at P). Let $\gamma, \delta \in K$ and consider also the line $\gamma x + \delta y$ through P. Then it is a fact that $\gamma x + \delta y \in K(C)$ is a uniformizer at P if and only if $\alpha\delta - \beta\gamma \neq 0$.

Example 2.3. Consider $\{y^2 = x(x-1)(x-\lambda)\} \subset \mathbb{A}^2$ for $\lambda \neq 0, 1$ and consider its projective closure by taking $x = \frac{X}{Z}, y = \frac{Y}{Z}$ to get $\{Y^2 Z = X(X-Z)(X-\lambda Z)\} \subset \mathbb{P}^2$. This has only one point at infinity, $P = (0:1:0)$. Our aim is to compute $\mathrm{ord}_P(x)$ and $\mathrm{ord}_P(y)$.

For this, put $t = \frac{X}{Y}, w = \frac{Z}{Y}$, so $w \overset{(\dagger)}{=} t(t-w)(t-\lambda w)$. Now P is the point $(t,w) = (0,0)$, which is a smooth point with $\mathrm{ord}_P(t) = \mathrm{ord}_P(t-w) = \mathrm{ord}_P(t-\lambda w) = 1$, so ($\dagger$) gives $\mathrm{ord}_P(w) = 3$. We now find

$$\begin{aligned} \mathrm{ord}_P(x) &= \mathrm{ord}_P\left(\frac{X}{Z}\right) = \mathrm{ord}_P\left(\frac{t}{w}\right) = 1 - 3 = -2 \\ \mathrm{ord}_P(y) &= \mathrm{ord}_P\left(\frac{Y}{Z}\right) = \mathrm{ord}_P\left(\frac{1}{w}\right) = -3. \end{aligned}$$

Riemann–Roch space. Let C be a smooth projective curve.

Definition 2.3. A **divisor** is a formal sum of points on C, say $D = \sum_{P \in C} n_P P$ where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in C$. We say $\deg D = \sum_{P \in C} n_P$.

D is **effective** (written $D \geq 0$) if $n_P \geq 0 \ \forall P \in C$. If $f \in K(C)^\times$, then $\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f) P$. The Riemann–Roch space of $D \in \mathrm{Div}(C)$ is

$$\mathcal{L}(D) = \{f \in K(C)^\times \mid \mathrm{div}(f) + D \geq 0\} \cup \{0\},$$

i.e. the K–vector space of rational functions on C with "poles no worse than specified by D" (i.e. every coefficient of $\mathrm{div}(f) + D$ is nonnegative).

We quote Riemann–Roch for surfaces of genus 1: We have

$$\dim \mathcal{L}(D) = \begin{cases} \deg D & \text{if } \deg D > 0 \\ 0 \text{ or } 1 & \text{if } \deg D = 0 \\ 0 & \text{if } \deg D < 0. \end{cases}$$

Example 2.4. We revisit Example 2.3. We have $\mathcal{L}(2P) = \langle 1, x \rangle$ and $\mathcal{L}(3P) = \langle 1, x, y \rangle$.

We still have char $K \neq 2$ and $\overline{K} = K$. 24 Jan 2024, Lecture 3

Proposition 2.2. Let $C \subset \mathbb{P}^2$ be a smooth plane cubic and let $P \in C$ be a point of inflection. Then we may change coordinates such that $C : Y^2Z = X(X-Z)(X-\lambda Z)$ and $P = (0:1:0)$ (for some $\lambda \neq 0, 1$).

Proof. First change coordinates such that $P = (0 : 1 : 0)$. Then change coordinates such that the tangent line becomes $T_pC = \{Z = 0\}$. Say $C = \{F(X,Y,Z) = 0\} \subset \mathbb{P}^2$. A point on the tangent line is of the form $(t : 1 : 0)$ and since $P \in C$ is a point of inflection, we get $F(t,1,0) = \text{const} \cdot t^3$, i.e. F has no terms X^2Y, XY^2 or Y^3.

Hence $F = \langle Y^2Z, XYZ, YZ^2, X^3, X^2Z, XZ^2, Z^3\rangle$. Notably, Y^2Z has a nonzero coefficient, otherwise $P \in C$ would be singular, a contradition to C being smooth. The coefficient of X^3 is nonzero as well, otherwise $Z \mid F$. We are free to rescale X, Y, Z, F, so WLOG C is defined by

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

Substituting $Y \mapsto Y - \frac{1}{2}a_1X - \frac{1}{2}a_3Z$, we may assume $a_1 = a_3 = 0$. This gives

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

for a monic cubic polynomial f. Since C is smooth, f has distinct roots, WLOG $0, 1, \lambda$, so $C : Y^2Z = X(X-Z)(X-\lambda Z)$. $\square$

The form $Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ is the Weierstrass form. The form $Y^2Z = X(X-Z)(X-\lambda Z)$ is the Legendre form.

Remark. It can be shown that the points of inflection of a plane curve $C = \{F(X_1, X_2, X_3) = 0\} \subset \mathbb{P}^2$ are given by solving the Hessian:

$$\begin{cases} \det H = \det\left(\frac{\partial^2 F}{\partial X_i \partial X_j}\right) = 0 \\ F(X_1, X_2, X_3) = 0. \end{cases}$$

2.1 The degree of a morphism

Let $\phi : C_1 \to C_2$ be a nonconstant morphism of smooth projective curves. Then $\phi^* : K(C_2) \to K(C_1)$ by $f \mapsto f \circ \phi$, giving an injective map $\phi^*K(C_2)$ to $K(C_1)$.

Definition 2.4. The **degree** of ϕ is $\deg \phi = [K(C_1) : \phi^*K(C_2)]$.

We say ϕ is **separable** if $K(C_1)/\phi^*K(C_2)$ is a separable field extension.

Suppose $P \in C_1, Q \in C_2$ and $\phi : P \mapsto Q$. Let $t \in K(C_2)$ be a uniformizer at Q.

Definition 2.5. $e_\phi(P) = \text{ord}_P(\phi^*t)$, which is always ≥ 1 and independent of t.

Theorem 2.3. Let $\phi : C_1 \to C_2$ be a nonconstant morphism of smooth projective curves. Then

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi \ \forall Q \in C_2.$$

Moreover, if ϕ is separable, then $e_\phi(P) = 1$ for all but finitely many $P \in C_1$.

We don't prove this.

In particular, this shows that:

(i) ϕ is surjective (very important here that we're in $\overline{K}$).

(ii) $|\phi^{-1}(Q)| \leq \deg \phi$.

(iii) If ϕ is separable, then equality holds in (ii) for all but finitely many points $Q \in C_2$.

Important remark. Let C be an algebraic curve. A rational map is given by

$$\begin{aligned} C &\to \mathbb{P}^n \\ \phi &\mapsto (f_0, f_1, \dots, f_n) \end{aligned}$$

where $f_0, \dots, f_n \in K(C)$ are not all zero. Then we have a fact: If C is smooth, then ϕ is a morphism. This saves us a lot of time (we can go from a rational map to a morphism immediately).

3 Weierstrass equations

We now drop the assumption that $\overline{K} = K$, but we will still assume that K is perfect.

Definition 3.1. An **elliptic curve** E/K is a smooth projective curve of genus 1 defined over K with a specified K–rational point $O = 0_E$.

Example 3.1. $\{X^3 + pY^3 + p^2Z^3 = 0\} \subset \mathbb{P}^2$ is not an elliptic curve over $\mathbb{Q}$, since it has no $\mathbb{Q}$–rational point.

Theorem 3.1. Every elliptic curve E is isomorphic over K to a curve in Weierstrass form via an isomorphism taking 0_E to $(0 : 1 : 0)$.

Remark. Proposition 2.2 treated the special case where E is a smooth plane cubic and 0_E is a point of inflection.

Fact. If $D \in \mathrm{Div}(E)$ is defined over K, then $\mathcal{L}(D)$ has a basis in $K(E)$ (not just in $\overline{K}(E)$). Here D is defined over K if it is fixed by $\mathrm{Gal}(\overline{K}/K)$ (this is unimportant for us and we just write it down to be rigorous).

Proof. $\mathcal{L}(2\cdot 0_E) \subset \mathcal{L}(3\cdot 0_E)$. Pick bases $1, x$ and $1, x, y$. Note $\mathrm{ord}_{0_E}(x) = -2$ and $\mathrm{ord}_{0_E}(y) = -3$ (else x, y don't give a basis). The 7 elements $1, x, y, x^2, xy, x^3, y^2$ lie in the 6–dimensional vector space $\mathcal{L}(60_E)$ (as they have at most a sixth order pole), so they must satisfy a linear dependence relation.

Leaving out x^3 or y^2 leaves us with 6 elements, all with different order poles, giving a basis for $\mathcal{L}(60_E)$. Hence the coefficients of x^3 and y^2 are nonzero, so by rescaling x, y (if necessary) we get

$$E' : y^2 + a_1xy + a_2y = x^3 + a_2x^2 + a_4x + a_6$$

for some $a_i \in K$. Let E' be the curve defined by this equation (or rather its projective closure). There is a morphism $\phi : E \to E' \subset \mathbb{P}^2$ by $P \mapsto (x(P) : y(P) : 1) = \left(\frac{x}{y}(P) : 1 : \frac{1}{y}(P)\right)$. (Since E is smooth, we know that this rational map is a morphism). Hence $0_E \mapsto (0 : 1 : 0)$.

We have $E \xrightarrow{x} \mathbb{P}^1$ by $x \mapsto (x : 1)$ (and similarly for y), so

$$[K(E) : K(x)] = \deg(E \xrightarrow{x} \mathbb{P}^1) = \mathrm{ord}_{0_E}\left(\frac{1}{x}\right) = 2$$
$$[K(E) : K(y)] = \deg(E \xrightarrow{y} \mathbb{P}^1) = \mathrm{ord}_{0_E}\left(\frac{1}{y}\right) = 3.$$

This gives an inclusion of fields $K(x) \le K(E)$ of degree 2, $K(y) \le K(E)$ of degree 3, while $K(x), K(y) \le K(x, y) \le K(E)$, so tower law gives $[K(E) : K(x, y)] = 1 \implies K(E) = K(x, y) = \phi^*K(E') \implies \deg\phi = 1$. (draw a picture!). This gives us an inverse that is a rational map, which we want to show is a morphism. For this, we just need to show that E' is smooth.

If E' were singular, then E and E' are rational, a contradiction. So E' is smooth and hence ϕ^{-1} is a morphism, so ϕ is an isomorphism. □

Proposition 3.2. Let E, E' be elliptic curves over K in Weierstrass form. Then $E \cong E'$ over $K \iff$ the equations are related by a change of variables

$$x = u^2x' + r$$
$$y = u^3y' + u^2sx' + t$$

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

Proof. $\mathcal{L}(2 \cdot 0_E) = \langle 1, x\rangle = \langle 1, x'\rangle \implies x = \lambda x' + r$ for some $\lambda, r \in K, \lambda \neq 0$. Similarly $\mathcal{L}(3 \cdot 0_E) = \langle 1, x, y\rangle = \langle 1, x', y'\rangle \implies y = \mu y' + \sigma x' + t$ for some $\mu, \sigma, t \in K, \mu \neq 0$.

Looking at the coefficients of x^3 and y^2 tells us that $\lambda^3 = \mu^2$, so $\lambda = u^2, \mu = u^3$ for some $u \in K^\times$. Put $s = \frac{\sigma}{u^2}$ to conclude. □

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

If char $K \neq 2, 3$, we may reduce to the case $E : y^2 = x^3 + ax + b$. In this case, the discriminant is $\Delta = -16(4a^3 + 27b^2)$.

Corollary 3.3. Assume char $K \neq 2, 3$. Elliptic curves

$$\begin{aligned} E &: y^2 = x^3 + ax + b \\ E' &: y^2 = x^3 + a'x + b' \end{aligned}$$

are isomorphic over $K \iff \begin{cases} a' = u^4 a \\ b' = u^6 b \end{cases}$ for some $u \in K^\times$.

Proof. E, E' are related by a substitution as in Proposition 3.2 with $r = s = t = 0$. $\square$

Definition 3.2. The j–**invariant** is $j(E) = \frac{1728(4a^3)}{4a^3+27b^2}$.

Corollary 3.4. $E \cong E' \implies j(E) \cong j(E')$ and the converse holds if $K = \overline{K}$.

Proof. $E \cong E' \iff \begin{cases} a' &= u^4 a \\ b' &= u^6 b \end{cases}$ for some $u \in K^\times \implies (a^3 : b^2) = ((a')^3 : (b')^2) \iff j(E) = j(E')$. The middle step is reversible if $K = \overline{K}$. $\square$

4 The Group Law

Let $E \subset \mathbb{P}^2$ be a smooth plane cubic with $0_E \in E(K)$ (not immediately assumed to be in Weierstrass form). E meets any line in 3 points, counted with multiplicity.

For $P, Q \in E$, let S be the 3$^{\text{rd}}$ point of intersction of PQ with E and then let R be the 3$^{\text{rd}}$ intersection of $0_E S$ with E. We define $P \oplus Q = R$. (Later we drop the circle and just write $+$). If $P = Q$, instead take the tangent line at P, i.e. $T_P E$, etc. This is the "chord and tangent process".

Theorem 4.1. $(E, \oplus)$ is an abelian group.

Remark. Here E means $E(\overline{K})$ since we haven't specified a field yet.

Proof. (i) $\oplus$ is commutative trivially.

(ii) 0_E is the identity, since the line through $0_E P$ meets S for the 3$^{\text{rd}}$ time at S and then SP meets E for the 3$^{\text{rd}}$ time at 0_E (drawing a picture makes this obvious).

(iii) Inverses: Let S be the 3rd intersection of T_{0_E} with E and Q the 3rd intersection of PS with E. Then $P \oplus Q = 0_E$.

(iv) Associativity is much harder. We have some setup:

Definition 4.1. $D_1, D_2 \in \text{Div}(E)$ are **linearly equivalent** if $\exists f \in K(E)^\times$ such that $\text{div}(f) = D_1 - D_2$. Write $D_1 \sim D_2$ and $[D] = \{D' \mid D' \sim D\}$.

Definition 4.2. The **Picard group** is $\text{Pic}(E) = \text{Div}(E)/\sim$. Also define $\text{Pic}^0(E) = \text{Div}^0(E)/\sim$ where $\text{Div}^0(E) = \{D \in \text{Div}(E) \mid \deg(D) = 0\}$.

We define $\psi : E \to \text{Pic}^0(E)$ by $P \mapsto [(P) - (0_E)]$.

Proposition 4.2. (i) $\psi(P \oplus Q) = \psi(P) + \psi(Q)$.

(ii) ψ is a bijection.

Proof. (i) WLOG let the lines PQ and $0_E S$ be given by $l = 0$ and $m = 0$. Then

$$\text{div}\left(\frac{l}{m}\right) = (P) + (S) + (Q) - (0_E) - (S) - (R),$$

hence $(P) + (Q) \sim (P \oplus Q) + (0_E)$, so $(P \oplus Q) - (0_E) \sim (P) - (0_E) + (Q) - (0_E)$, so $\psi(P \oplus Q) = \psi(P) + \psi(Q)$.

(ii) Injectivity: Suppose $\psi(P) = \psi(Q)$ for $P \neq Q$. Then $\exists f \in \overline{K}(E)^\times$ such that $\text{div}(f) = (P) - (0_E) - (Q) + (0_E) = (P) - (Q) \implies E \xrightarrow{f} \mathbb{P}^1$ has degree 1 (for example since evaluation at 0 on the affine line gives that P has one root and Q has one pole), so $E \cong \mathbb{P}^1$, a contradiction.

Surjectivity: Let $[D] \in \text{Pic}^0(E)$. Then $D + (0_E)$ has degree 1, so by Riemann–Roch, $\dim \mathcal{L}(D + (0_E)) = 1$, so $\exists 0 \neq f \in \overline{K}(E)$ such that $\text{div}(f) + D + (0_E) \geq 0$, but $\text{div}(f) + D + (0_E)$ has degree 1, so $\text{div}(f) + D + (0_E) = (P)$ for some $P \in E \implies (P) - (0_E) \sim D \implies \psi(P) = [D]$.

□

We conclude that ψ identifies $(E, \oplus)$ with $(\text{Pic}^0(E), +)$, so $\oplus$ is associative.

□

29 Jan 2024, Lecture 5

Formulae for E in Weierstrass form. Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Choose two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on it. Let the line through P_1 and P_2 be given by $y = \lambda x + \nu$ and let it meet E again at $P' = (x', y')$. We want to find $P_1 \oplus P_2 = P_3 = (x_3, y_3) = \ominus P'$ for $\ominus P$ the reflection of P across the x–axis. We easily compute $\ominus P_1 = (x_1, -(a_1x + a_3) - y_1)$.

Substituting $y = \lambda x + \nu$ into our equation for E and looking at the coefficient of x^2 gives $\lambda^2 + a_1\lambda - a_2 = x_1 + x_2 + x' = x_1 + x_2 + x_3$, so $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$. For y_3 we find

$$y_3 = -(a_1 x' + a_3) - y' = -(a_1 x_3 + a_3) - (\lambda x_3 + \nu) = -(\lambda + a_1)x_3 - a_3 - \nu.$$

It remains to find formulas for λ and ν.

- Case 1. $x_1 = x_2$, but $P_1 \neq P_2$. Then $P_1 \oplus P_2 = 0_E$.
- Case 2. $x_1 \neq x_2$. Then $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ and $\nu = y_1 - \lambda x_1 = \frac{x_2 y_1 - x_1 y_2}{x_2 - x_1}$.
- Case 3. $P_1 = P_2$. In this case, compute the equation for the tangent line to get λ, ν as rational expressions in x_1, x_2, y_1, y_2.

Corollary 4.3. $E(K)$ is an abelian group.

Proof. $E(K)$ is a subgroup of $(E, \oplus)$.

- It has identity 0_E by definition.
- We have closure and inverses through the formulae above.
- Associativity and commutativity is inherited.

$\square$

Theorem 4.4. Elliptic curves are group varieties, i.e.

$$[-1] : E \to E, P \mapsto \ominus P$$
$$\oplus : E \times E \to E, (P, Q) \mapsto P \oplus Q$$

are morphisms of algebraic varieties.

Proof. By the above formulae, $[-1] : E \to E$ is a rational map, i.e. a morphism by our important remark.

For $\oplus$, note by the above formulae that $\oplus : E \times E \to E$ is a rational map regular on

$$U = \{(P, Q) \in E \times E \mid 0_E \notin \{P, Q, P \oplus Q, P \ominus Q\}\}.$$

For $P \in E$, let $\tau_P : E \to E$ be the "translation by P" map, given by $X \mapsto P \oplus X$. τ_P is a rational map, hence a morphism. Now for $A, B \in E$, we factor $\oplus$ as

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

This shows $\oplus$ is regular on $(\tau_A \times \tau_B)(U)$, so $\oplus$ is regular on $E \times E$. $\square$

Statement of results. The following isomorphisms in (i), (ii), (iv) respect the relevant topologies.

(i) $K = \mathbb{C}$. Then $E(\mathbb{C}) \cong \mathbb{C}/\Lambda \cong \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ for Λ a lattice.

(ii) $K = \mathbb{R}$. Then

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

(iii) $K = \mathbb{F}_q$. Then $||E(\mathbb{F}_q)| - (q+1)| \leq 2\sqrt{q}$. This is Hasse's Theorem.

(iv) For a local field $[K : \mathbb{Q}_p] < \infty$ with ring of integers $\mathcal{O}_K$, $E(K)$ has a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.

(v) For a number field $[K : \mathbb{Q}] < \infty$, $E(K)$ is a finitely generated abelian group (this is the Mordell–Weil Theorem). Basic group theory says that if A is a finitely generated abelian group, then $A \cong (\text{finite subgroup}) \times \mathbb{Z}^r$. Here r is called the rank of A. The proof of Mordell–Weil gives an upper bound for rank $E(K)$, but there is no known algorithm to compute the rank in all cases.

Brief remarks on the case $K = \mathbb{C}$. Let $\Lambda = \{a\omega_1 + b\omega_2 \mid a, b \in \mathbb{Z}\}$ where ω_1, ω_2 are a basis for $\mathbb{C}$ as an $\mathbb{R}$–vector space. Then meromorphic functions on the Riemann surface $\mathbb{C}/\Lambda$ correspond bijectively with Λ–invariant meromorphic functions in $\mathbb{C}$. The function field of $\mathbb{C}/\Lambda$ is generated by $\wp(z)$ and $\wp'(z)$, where

$$\begin{aligned} \wp(z) &= \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right) \\ \wp'(z) &= -2 \sum_{\lambda \in \Lambda} \frac{1}{(z-\lambda)^3}. \end{aligned}$$

These satisfy $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$ for some constants $g_2, g_3 \in \mathbb{C}$ depending on Λ. One shows $\mathbb{C}/\Lambda \cong E(\mathbb{C})$, where $E : y^2 = 4x^3 - g_2x - g_3$ which is an isomorphism on both groups (via $z \mapsto (\wp(z), \wp'(z))$) and on Riemann surfaces. We have the following result:

Theorem 4.5 (Uniformization theorem)**.** Every elliptic curve over $\mathbb{C}$ arises in this way.

Definition 4.3. For $n \in \mathbb{Z}$, let $[n] : E \to E$ be given by $P \mapsto \underbrace{P \oplus P \oplus \ldots \oplus P}_{n \text{ copies}}$ if $n > 0$ and $[-n] = [-1] \circ [n]$.

Definition 4.4. The n–**torsion subgroup** of E is

$$E[n] = \ker(E \xrightarrow{[n]} E).$$

If $K = \mathbb{C}$, then $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, so $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ and $\deg[n] = n^2$. Call these results (1) and (2). We will show that (2) holds over any field $K = \overline{K}$ and (1) holds if char $K \nmid n$. We sometimes abuse notation and write $E[n] = E[n](\overline{K})$. 31 Jan 2024, Lecture 6

Lemma 4.6. Assume char $K \neq 2$ and $E : y^2 = f(x) = (x - e_1)(x - e_2)(x - e_3)$ (with $e_i \in \overline{K}$). Then $E[2] = \{0, (e_1, 0), (e_2, 0), (e_3, 0)\} \cong (\mathbb{Z}/2\mathbb{Z})^\times$.

Proof. Let $P = (x, y) \in E$. Then $2[P] = 0 \iff P = -P \iff (x, y) = (x, -y) \iff y = 0$. $\square$

5 Isogenies

Let E_1, E_2 be elliptic curves.

Definition 5.1. (i) An **isogeny** $\phi : E_1 \to E_2$ is a nonconstant morphism with $\phi(0_{E_1}) = 0_{E_2}$.

(ii) We say E_1 and E_2 are **isogenous** if there is an isogeny between them.

In (i), nonconstant is equivalent to surjective on $\overline{K}$–points. See Theorem 2.3.

Definition 5.2. $\mathrm{Hom}(E_1, E_2) = \{\text{isogenies } E_1 \to E_2\} \cup \{0\}$ (the constant map at 0_E). This is an abelian group under $(\phi + \psi)(P) := \phi(P) \oplus \psi(P)$.

If $E_1 \xrightarrow{\phi} E_2 \xrightarrow{\psi} E_3$ are isogenies, then $\psi \circ \phi$ is an isogeny. By tower law, $\deg(\psi \circ \phi) = \deg(\psi)\deg(\phi)$.

Proposition 5.1. If $0 \neq n \in \mathbb{Z}$, then $[n] : E \to E$ is an isogeny.

Proof. $[n]$ is a morphism by Theorem 4.4. We need to show $[n] \neq [0]$. Assume char $K \neq 2$.

- Case $n = 2$. Lemma 4.6 implies that $E[2] \neq E$, so $[2] \neq 0$.
- Case n odd. Lemma 4.6 implies that $\exists 0 \neq T \in E[2]$. Then $nT = T \neq 0$, so $[n] \neq [0]$.

Now use $[mn] = [m] \circ [n]$ to conclude.

If char $K = 2$, then we can replace Lemma 4.6 with an explicit lemma about 3–torsion points. $\square$

Corollary 5.2. $\mathrm{Hom}(E_1, E_2)$ is a torsion–free $\mathbb{Z}$–module.

Theorem 5.3. Let $\phi : E_1 \to E_2$ be an isogeny. Then

$$\phi(P + Q) = \phi(P) + \phi(Q) \ \forall P, Q \in E.$$

Sketch proof. ϕ induces a map $\phi_* : \mathrm{Div}^0(E_1) \to \mathrm{Div}^0(E_2)$ by $\sum_{P \in E_1} n_P P \mapsto \sum_{p \in E_1} n_P \phi(P)$. Recall $\phi^* : K(E_2) \hookrightarrow K(E_1)$.

Fact. If $f \in K(E_1)$, then $\mathrm{div}(N_{K(E_1)/K(E_2)} f) = \phi^*(\mathrm{div}\, f)$. So ϕ_* sends principal divisors to principal divisors. Since $\phi(0_{E_1}) = 0_{E_2}$, the following diagram commutes:

$$\begin{tikzcd} E_1 \arrow[r, "\phi"] \arrow[d, "f"] & E_2 \arrow[d, "g"] \\ \mathrm{Pic}^0(E_1) \arrow[r, "\phi_*"] & \mathrm{Pic}^0(E_2) \end{tikzcd}$$

(with $f(P) = [(P) - (0_{E_1})], g(Q) = [(Q) - (0_{E_2})]$). Since ϕ_* is a group homomorphism, ϕ is a group homomorphism. □

Lemma 5.4. Let $\phi : E_1 \to E_2$ be an isogeny. Then there exists a morphism ξ making the following diagram commute:

$$\begin{tikzcd} E_1 \arrow[r, "\phi"] \arrow[d, "x_1"] & E_2 \arrow[d, "x_2"] \\ \mathbb{P}^1 \arrow[r, "\xi"] & \mathbb{P}^1 \end{tikzcd}$$

with x_i the x–coordinate in a Weierstrass equation for E_i. Moreover, if $\xi(t) = \frac{r(t)}{s(t)}$ with $r, s \in K[t]$ coprime, then $\deg(\phi) = \deg(\xi) = \max(\deg(r), \deg(s))$.

Proof. For $i = 1, 2$, $K(E_i)/K(x_i)$ is a degree 2 Galois extension with Galois group generated by $[-1]^*$. By Theorem 5.3, $\phi \circ [-1] = [-1] \circ \phi$, so if $f \in K(x_2)$, then $[-1]^*(\phi^* f) = \phi^*([-1]^* f) = \phi^* f$ and hence $\phi^* f \in K(x_1)$. Hence we find

$$\begin{tikzcd}[column sep=small] & K(E_1) = K(x_1, y_1) \arrow[dl, dash, "2"'] \arrow[d, dash] \\ K(x_1) \arrow[d, dash] & K(E_2) = K(x_2, y_2) \arrow[dl, dash, "2"'] \\ K(x_2) & \end{tikzcd} .$$

In particular, $\phi^* x_2 = \xi(x_1)$ for some $\xi \in K(t)$. By tower law, $2\deg(\phi) = 2\deg(\xi) \implies \deg(\phi) = \deg(\xi)$. Now $K(x_2) \hookrightarrow K(x_1)$ by $x_2 \mapsto \xi(x_1) = \frac{r(x_1)}{s(x_1)}$ for $r, s \in K[t]$ coprime. Then minimal polynomial of x_1 over $K(x_2)$ is $F(t) = r(t) - s(t)x_2 \in K(x_2)[t]$. This is true as $F(x_1) = 0$, F is irreducible on $K[x_2, t]$ (since r, s are coprime) and by Gauss' Lemma, F is irreducible on $K(x_2)[t]$. Hence $\deg(\phi) = \deg(\xi) = [K(x_1) : K(x_2)] = \deg(F) = \max(\deg(r), \deg(s))$. □

Lemma 5.5. $\deg[2] = 4$.

Proof. Assume char $K \neq 2, 3$, so $E : y^2 = x^3+ax+b = f(x)$. If $P = (x, y)$, then $x(2P) = \left(\frac{3x^2+a}{2y}\right)^2 - 2x = \frac{(3x^2+a)^2-2xf(x)}{4f(x)}$. The numerator and denominator are coprime, since otherwise $\exists\theta \in \overline{K}$ with $f(\theta) = f'(\theta) = 0$, meaning f has a multiple root, contradiction. We are now done by Lemma 5.4, since $\deg[2] = \max(3, 4) = 4$. □

Definition 5.3. Let A be an abelian group. Then a map $q : A \to \mathbb{Z}$ is a quadratic form if

(i) $q(nx) = n^2q(x)\ \forall n \in \mathbb{Z}, x \in A$.

(ii) $(x, y) \mapsto q(x + y) - q(x) - q(y)$ is $\mathbb{Z}$–bilinear.

Lemma 5.6. $q : A \to \mathbb{Z}$ is a quadratic form if and only if it satisfies the parallelogram law $q(x + y) + q(x - y) = 2q(x) + 2q(y)\ \forall x, y \in A$.

Proof. ($\implies$). Let $\langle x, y\rangle = q(x+y)-q(x)-q(y)$. Then $\langle x, x\rangle = q(2x)-2q(x) = 2q(x)$ by (i) with $n = 2$. By (ii), $\langle x+y, x+y\rangle + \langle x-y, x-y\rangle = 2\langle x, x\rangle + 2\langle y, y\rangle$, which implies $q(x + y) + q(x - y) = 2q(x) + 2q(y)$.

($\impliedby$). This is on Ex. Sheet 2. □

02 Jan 2024, Lecture 7

Theorem 5.7. $\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ is a quadratic form (with $\deg(0) = 0$).

Proof. Assume char $K \neq 2, 3$ and write $E_2 = y^2 = x^3 + ax + b$. Let $P, Q \in E_2$ with $P, Q, P + Q, P - Q$ all nonzero and let x_1, x_2, x_3, x_4 be the x–coordinates of these points.

Lemma 5.8. There exist polynomials $W_0, W_1, W_2 \in \mathbb{Z}[a, b][x_1, x_2]$ of degree ≤ 2 in x_1 and of degree ≤ 2 in x_2 such that

$$(1 : x_3 + x_4 : x_3x_4) = (W_0 : W_1 : W_2)$$

Proof. Method 1: Direct calculation (results on the formula sheet) gives the result (e.g. $W_0 = (x_1 - x_2)^2$).

Method 2: Let $y = \lambda x + \nu$ be the line through P and Q. Substituting, we get $x^3 + ax + b - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3) = x^3 - s_1x^2 + s_2x - s_3$ where s_i is the i^{th} symmetric polynomial in x_1, x_2, x_3. Comparing coefficients gives $\lambda^2 = s_1, -2\lambda\nu = s_2 - a, \nu^2 = s_3 + b$. Eliminating λ and ν gives

$$F(x_1, x_2, x_3) = (s_2 - a)^2 - 4s_1(s_3 + b) = 0,$$

where F has degree at most 2 in each x_i. Hence x_3 is a root of the quadratic $W(t) = F(x_1, x_2, t)$. Repeating this for the line through P and $-Q$ shows that

x_4 is the other root of $W(t)$. Therefore

$$\begin{aligned} W(t) &= W_0(t-x_3)(t-x_4) = W_0t^2 - W_1t + W_2 \\ \implies & (1 : x_3 + x_4 : x_3x_4) = (W_0 : W_1 : W_2). \end{aligned}$$

□

We now show that if $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$, then $\deg(\phi+\psi) + \deg(\phi-\psi) \leq 2\deg(\phi) + 2\deg(\psi)$. We may assume that $\phi, \psi, \phi+\psi, \phi-\psi$ are not the zero maps (otherwise we're done trivially, or use $\deg[-1] = 1,\ \deg[2] = 4$). Now

$$\begin{aligned} \phi : (x,y) &\mapsto (\xi_1(x), \ldots) \\ \psi : (x,y) &\mapsto (\xi_2(x), \ldots) \\ \phi+\psi : (x,y) &\mapsto (\xi_3(x), \ldots) \\ \phi-\psi : (x,y) &\mapsto (\xi_4(x), \ldots). \end{aligned}$$

Lemma 5.8 implies $(1 : \xi_3 + \xi_4 : \xi_3\xi_4) = ((\xi_1 - \xi_2)^2 : \ldots)$. Say $\xi_i = \frac{r_i}{s_i}$ for $r_i, s_i \in K[t]$ coprime. This gives

$$(s_3s_4 : r_3s_4 + r_4s_3 : r_3r_4) \overset{(\star)}{=} ((r_1s_2 - r_2s_1)^2 : \ldots)$$

where every term is quadratic in r_3, r_4, s_3 and s_4. Hence (as the terms on the LHS of $(\star)$ are coprime)

$$\begin{aligned} \deg(\phi+\psi) + \deg(\phi-\psi) &= \max(\deg(r_3), \deg(s_3)) + \max(\deg(r_4), \deg(s_4)) \\ &= \max(\deg(s_3s_4), \deg(r_3s_4 + r_4s_3), \deg(r_3r_4)) \\ &\leq 2\max(\deg(r_1), \deg(s_1)) + 2\max(\deg(r_2), \deg(s_2)) \\ &= 2\deg(\phi) + 2\deg(\psi). \end{aligned}$$

Now replace ϕ and ψ by $\phi+\psi$ and $\phi-\psi$ and use $\deg[2] = 4$ to get

$$4\deg(\phi) + 4\deg(\psi) = \deg(2\phi) + \deg(2\psi) \leq 2\deg(\phi+\psi) + 2\deg(\phi-\psi).$$

This gives the parallelogram law, so deg is a quadratic form. □

Corollary 5.9. $\deg(n\phi) = n^2\deg(\phi)$. In particular, $\deg[n] = n^2$.

Example 5.1. Let E/K be an elliptic curve. Suppose char $K \neq 2$ and $0 \neq T \in E(K)[2]$. WLOG let $E : y^2 = x(x^2 + ax + b)$ for $a, b \in K, b(a^2 - 4b) \neq 0$ (by moving a root to zero) and WLOG $T = (0, 0)$.

If $P = (x, y)$ and $P' = P + T = (x', y')$, then

$$x' = \left(\frac{y}{x}\right)^2 - a - x = \frac{x^2 + ax + b}{x} - a - x = \frac{b}{x}$$
$$y' = -\left(\frac{y}{x}\right) x' = -\frac{by}{x^2}.$$

We let $\xi = x + x' + a = \left(\frac{y}{x}\right)^2, \eta = y + y' = \frac{y}{x}\left(x - \frac{b}{x}\right)$. Then

$$\eta^2 = \left(\frac{y}{x}\right)^2 \left(\left(x + \frac{b}{x}\right)^2 - 4b\right) = \xi((\xi - a)^2 - 4b) = \xi(\xi^2 - 2a\xi + a^2 - 4b).$$

Let $E' : y^2 = x(x^2 + a'x + b')$ with $a' = -2a, b' = a^2 - 4b$. There is an isogeny $\phi : E \to E'$ given by $(x, y) \mapsto \left(\left(\frac{y}{x}\right)^2 : \frac{y(x^2-b)}{x^2} : 1\right)$.

Sanity check/finding where 0_E maps to: x is a double pole, y is a triple pole, so $\left(\frac{y}{x}\right)^2$ is a double pole and $\frac{y(x^2-b)}{x^2}$ is a triple pole (and the last coordinate 1 has degree 0). Multiplying through by a cube of a uniformizer, the degrees go from $(-2, -3, 0)$ to $(1, 0, 3)$, so $0_E \mapsto (0 : 1 : 0)$.

To compute $\deg(\phi)$, $\left(\frac{y}{x}\right)^2 = \frac{x^2+ax+b}{x}$ with the numerator and denominator coprime as $b \neq 0$, so by Lemma 5.4, $\deg(\phi) = 2$. We say ϕ is a **2–isogeny**.

6 The invariant differential

For C some algebraic curve over $K = \overline{K}$.

Definition 6.1. The space of differentials Ω_C (sometimes called one–forms) is the $K(C)$–vector space generated by $\mathrm{d}f$ for all $f \in K(C)$ subject to the relations

(i) $\mathrm{d}(f + g) = \mathrm{d}f + \mathrm{d}g$.

(ii) $\mathrm{d}(fg) = f\mathrm{d}g + g\mathrm{d}f$.

(iii) $\mathrm{d}a = 0 \ \forall a \in K$.

Fact. Ω_C is a 1–dimensional $K(C)$–vector space. 05 Feb 2024, Lecture 8

Let $0 \neq \omega \in \Omega_C$, let $P \in C$ be a smooth point and let $t \in K(C)$ be a uniformizer at P. Then $\omega = f\mathrm{d}t$ for some $f \in K(C)^\times$. We define $\mathrm{ord}_P(\omega) = \mathrm{ord}_P(f)$, which is independent of the choice of t.

Fact. Suppose $f \in K(C)^\times$ with $\mathrm{ord}_P(f) = n \neq 0$. If $\mathrm{char}\, K \nmid n$, then $\mathrm{ord}_P(\mathrm{d}f) = n - 1$.

We assume that C is a smooth projective curve.

Definition 6.2. We define $\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega) P \in \mathrm{Div}(C)$. Here we use the fact that $\mathrm{ord}_P(\omega) = 0$ for all but finitely many $P \in C$.

Definition 6.3. A differential $\omega \in \Omega_C$ is regular if $\operatorname{div}(\omega) \geq 0$. We define the genus $g(C)$ of C to be

$$g(C) = \dim_K \{\omega \in \Omega_C \mid \operatorname{div}(\omega) \geq 0\},$$

where the set on the RHS is the set of regular differentials.

As a consequence of Riemann–Roch, we have that if $0 \neq \omega \in \Omega_C$, then $\deg(\operatorname{div}(\omega)) = 2g(C) - 2$.

Lemma 6.1. Assume char $K \neq 2$ and let $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$ for e_1, e_2, e_3 distinct. Then $\omega = \frac{\mathrm{d}x}{y}$ is a differential on E with no zeroes or poles, which implies $g(E) = 1$. In particular, the K–vector space of regular differentials on E is 1–dimensional (see previous fact), spanned by ω.

Proof. Let $T_i = (e_i, 0)$. Then $E[2] = \{0, T_1, T_2, T_3\}$ and $\operatorname{div}(y) \overset{(\dagger)}{=} (T_1) + (T_2) + (T_3) - 3(0)$. For $0 \neq P \in E$, $\operatorname{div}(x - x_P) = (P) + (-P) - 2(0)$.

- If $P \in E \setminus E[2]$, then $\operatorname{ord}(x - x_P) = 1 \implies \operatorname{ord}_P(\mathrm{d}x) = 0$.
- If $P = T_i$, then $\operatorname{ord}_P(x - x_P) = 2 \implies \operatorname{ord}_P(\mathrm{d}x) = 1$.
- If $P = 0$, then $\operatorname{ord}_P(x) = -2 \implies \operatorname{ord}_P(\mathrm{d}x) = -3$.

Hence $\operatorname{div}(\mathrm{d}x) = (T_1)+(T_2)+(T_3)-3(0)$, which with (†) gives $\operatorname{div}\left(\frac{\mathrm{d}x}{y}\right) = 0$. □

Definition 6.4. For $\phi : C_1 \to C_2$ a nonconstant morphism, we define

$$\begin{aligned} \phi^* : \Omega_{C_2} &\to \Omega_{C_1} \\ f\mathrm{d}g &\mapsto \phi^* f d(\phi^* g). \end{aligned}$$

Lemma 6.2. Let $P \in E$, $\tau_P : E \to E$ by $X \mapsto X + P$ and $\omega = \frac{\mathrm{d}x}{y}$ as above. Then $\tau_P^* \omega = \omega$. We say ω is the **invariant differential**.

Proof. $\tau_P^*\omega$ is a regular differential on E, so $\tau_P^*\omega = \lambda_P \omega$ for some $\lambda_P \in K^\times$. The map $E \to \mathbb{P}^1$ by $P \mapsto \lambda_P$ is a morphism of smooth projectives curves, but it is not surjective (as it misses 0 and ∞). Hence it is constant by Theorem 2.3, i.e. $\exists \lambda \in K^\times$ such that $\tau_P^*\omega = \lambda\omega \ \forall P \in E$. Taking $P = 0$ shows $\lambda = 1$. □

Remark. If $K = \mathbb{C}$ and $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ by $z \mapsto (\wp(z), \wp'(z)) := (x, y)$, then $\frac{\mathrm{d}x}{y} = \frac{\wp'(z)\mathrm{d}z}{\wp'(z)} = \mathrm{d}z$, which is invariant under $z \mapsto z + \text{const}$.

Lemma 6.3. Let $\phi, \psi \in \operatorname{Hom}(E_1, E_2)$. Let ω be the invariant differential on E_2. Then $(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega$.

Proof. Write E for E_2. We have the maps

$$\begin{aligned} E \times E &\to E \\ \mu : (P, Q) &\mapsto P + Q \\ \mathrm{pr}_1 : (P, Q) &\mapsto P \\ \mathrm{pr}_2 : (P, Q) &\mapsto Q. \end{aligned}$$

Fact. $\Omega_{E \times E}$ is a 2–dimensional $K(E \times E)$–vector space with basis $\mathrm{pr}_1^* \omega$ and $\mathrm{pr}_2^* \omega$. Consequently, $\mu^* \omega \overset{(\dagger)}{=} f \mathrm{pr}_1^* \omega + g \mathrm{pr}_2^* \omega$ for some $f, g \in K(E \times E)$.

For fixed $Q \in E$, let $i_Q : E \to E \times E$ by $P \mapsto (P, Q)$. Applying i_Q^* to $(\dagger)$ gives

$$\begin{aligned} \underbrace{(\mu \circ i_Q)}_{\tau_Q}{}^* \omega &= (i_Q^* f)(\underbrace{\mathrm{pr}_1 \circ i_Q}_{\text{identity map}})^* \omega + (i_Q^* g)(\underbrace{\mathrm{pr}_2 \circ i_Q}_{\text{constant map}})^* \omega \\ \implies \tau_Q^* \omega &= (i_Q^* f) \omega + 0. \end{aligned}$$

As $\tau_Q^* \omega = \omega$ by the previous lemma, we conclude $i_Q^* f = 1\ \forall q \in E$, so $f(P, Q) = 1\ \forall P, Q \in E$. Similarly $g(P, Q) = 1\ \forall P, Q \in E$, so $(\dagger)$ gives $\mu^* \omega = \mathrm{pr}_1^* \omega + \mathrm{pr}_2^* \omega$. Now pull back using

$$\begin{aligned} E_1 &\to E \times E \\ P &\mapsto (\phi(P), \psi(P)) \end{aligned}$$

to get $(\phi + \psi)^* \omega = \phi^* \omega + \psi^* \omega$. □

Lemma 6.4. Let $\phi : C_1 \to C_2$ be a nonconstant morphism. Then ϕ is separable if and only if $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ is nonzero.

Proof. Omitted. □

Example 6.1. Let $\mathbb{G}_m = \mathbb{A}^1 \setminus \{0\}$ be the multiplicative group. For $n \geq 2$ an integer, consider $\phi : \mathbb{G}_m \to \mathbb{G}_m$ by $x \mapsto x^n$. Then $\phi^*(\mathrm{d}x) = \mathrm{d}(x^n) = n x^{n-1} \mathrm{d}x$. So if char $K \nmid n$, then ϕ is separable, so $\left|\phi^{-1}(Q)\right| = \deg \phi$ for all but at most finitely many $Q \in \mathbb{G}_m$.

But ϕ is a group homomorphism, so $\left|\phi^{-1}(Q)\right| = |\ker(Q)|\ \ \forall Q \in \mathbb{G}_m$. Hence $|\ker Q| = \deg \phi = n$. This shows that $K = \overline{K}$ contains exactly n distinct n^{th} roots of unity.

07 Feb 2024, Lecture 9

Theorem 6.5. [1]If char $K \nmid n$, then $E[n] = (\mathbb{Z}/n\mathbb{Z})^2$.

[1]Remember that $\overline{K} = K$ here.

Proof. Lemma 6.3 and induction imply $[n]^*\omega = n\omega$ where char $K \nmid n$, so $[n]$ is separable by Lemma 6.4. Hence $\left|[n]^{-1}(Q)\right| = \deg[n]$ for all but finitely many points $Q \in E$. But $[n]$ is a group homomorphism, so $\left|[n]^{-1}Q\right| = |E[n]|\ \forall Q \in E$. We conclude that $|E[n]| = \deg[n] = n^2$ by Corollary 5.9.

By classification of finite abelian groups, $E[n] \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_t\mathbb{Z}$ with $d_1 \mid d_2 \mid \ldots \mid d_t$, but $d_t \mid n$, and if p is a prime with $p \mid d_1$, then $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^t$, so $|E[p]| = p^2$, so $t = 2$. Hence $d_1 \mid d_2 \mid n$ with $d_1 d_2 = n^2$, so $d_1 = d_2 = n$ and so $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. □

Remark. If char $K = p$, then $[p]$ is inseparable. It can be shown that either $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}\ \forall r \geq 1$ or $E[p^r] = 0\ \forall r \geq 1$ (the "ordinary" case and the "supersingular" case).

Remark about the remark. Do not use this remark to trivialize a question on Ex. Sheet 2.

7 Elliptic curves over finite fields

Lemma 7.1. Let A be an abelian group. Let $q : A \to \mathbb{Z}$ be a positive definite quadratic form. Then

$$\underbrace{|q(x+y) - q(x) - q(y)|}_{\langle x,y\rangle} \leq 2\sqrt{q(x)q(y)}.$$

Proof. We may assume $x \neq 0$, otherwise the result is clear. Hence $q(x) \neq 0$. Let $m, n \in \mathbb{Z}$, then

$$\begin{aligned} 0 \leq q(mx + ny) &= \frac{1}{2}\langle mx + ny, mx + ny\rangle \\ &= m^2 q(x) + mn\langle x, y\rangle + n^2 q(y) \\ &= q(x)\left(m + \frac{\langle x, y\rangle}{2q(x)} n\right)^2 + \left(q(y) - \frac{\langle x, y\rangle^2}{4q(x)}\right) n^2. \end{aligned}$$

Get rid of the first term by taking $m = -\langle x, y\rangle$ and $n = 2q(x)$ to deduce $\langle x, y\rangle^2 \leq 4q(x)q(y)$, so the result follows. □

Theorem 7.2 (Hasse)**.** Let $E/\mathbb{F}_q$ be an elliptic curve. Then

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

Proof. Recall $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ is cyclic of order r, generated by the Frobenius map $x \mapsto x^q$. Let E have Weierstrass equation with coefficients $a_1, \ldots, a_6 \in \mathbb{F}_q$ (and note that $a_i^q = a_i\ \forall i$).

Define the Frobenius endomorphism $\phi : E \to E$ by $(x, y) \mapsto (x^q, y^q)$, which is an isogeny of degree q. Then $E(\mathbb{F}_q) = \{P \in E \mid \phi(P) = P\} = \ker(1-\phi)$. We have

$$\phi^*\omega = \phi^*\left(\frac{\mathrm{d}x}{y}\right) = \frac{d(x^q)}{y^q} = \frac{qx^{q-1}\mathrm{d}x}{y^q} = 0$$

as $q = p^n$, so $p \mid q$. By Lemma 6.3,

$$(1-\phi)^*\omega = \omega - \phi^*\omega = \omega \neq 0,$$

so $1-\phi$ is separable. By Theorem 2.3 and the fact that $1-\phi$ is a group homomorphism, we argue in the proof of Theorem 6.5 that

$$\underbrace{|\ker(1-\phi)|}_{|E(\mathbb{F}_q)|} = \deg(1-\phi).$$

The map deg : $\mathrm{Hom}(E, E) \to \mathbb{Z}$ is a positive definite quadratic form by Theorem 5.7. Hence by Lemma 7.1,

$$\begin{aligned} &|\deg(1-\phi) - 1 - \deg\phi| \leq 2\sqrt{\deg\phi} \\ \implies &|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}. \end{aligned}$$

□

Definition 7.1. For $\phi, \psi \in \mathrm{End}(E) = \mathrm{Hom}(E, E)$, we put $\langle\phi, \psi\rangle = \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$ and $\mathrm{tr}(\phi) = \langle\phi, 1\rangle$.

Corollary 7.3. Let $E/\mathbb{F}_q$ be an elliptic curve and let $\phi \in \mathrm{End}(E)$ be the q^{th} power Frobenius map. Then $\#E(\mathbb{F}_q) = q + 1 - \mathrm{tr}(\phi)$ and $|\mathrm{tr}(\phi)| \leq 2\sqrt{q}$.

Zeta functions. For K a number field,

$$\zeta_K(s) = \sum_{\mathfrak{a}\subset\mathcal{O}_K} \frac{1}{(N(\mathfrak{a}))^s} = \prod_{\mathfrak{p}\subset\mathcal{O}_K, \mathfrak{p} \text{ prime}} \left(1 - \frac{1}{(N(\mathfrak{p}))^s}\right)^{-1}.$$

For K a function field, i.e. $K = \mathbb{F}_q(C)$ where C is a smooth projective curve,

$$\zeta_K(s) = \prod_{x\in|C|} \left(1 - \frac{1}{(Nx)^s}\right)^{-1},$$

where $|C| = \{\text{closed points of } C\} = \{\text{orbits for the action of } \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \text{ on } C(\overline{\mathbb{F}_q})\}$ and $Nx = q^{\deg x}$, where $\deg x$ is the size of the corresponding orbit (these definitions are borrowed from scheme theory). We have $\zeta_K(s) = F(q^{-s})$ for some $F \in \mathbb{Q}[[T]]$. We have

$$
\begin{aligned}
F(T) &= \prod_{x \in |C|} \left(1 - T^{\deg x}\right)^{-1} \\
\implies \log F(T) &= \sum_{x \in |C|} \sum_{m=1}^{\infty} \frac{1}{m} T^{m \deg x} \\
\implies T \frac{\mathrm{d}}{\mathrm{d}T} \log F(T) &= \sum_{x \in |C|} \sum_{m=1}^{\infty} \deg x T^{m \deg x} \\
&\overset{n = m \deg x}{=} \sum_{n=1}^{\infty} \left(\sum_{x \in |C|, \deg x \mid n} \deg x \right) T^n \\
&= \sum_{n=1}^{\infty} \# C(\mathbb{F}_{q^n}) T^n \\
\implies F(T) &= \exp\left(\sum_{n=1}^{\infty} \frac{\# C(\mathbb{F}_{q^n})}{n} T^n \right).
\end{aligned}
$$

Definition 7.2. The zeta function of a smooth projective curve $C/\mathbb{F}_q$ is

$$
Z_C(T) = \exp\left(\sum_{n=1}^{\infty} \frac{\# C(\mathbb{F}_{q^n})}{n} T^n \right).
$$

Theorem 7.4. Let $E/\mathbb{F}_q$ be an elliptic curve with $\# E(\mathbb{F}_q) = q + 1 - a$. Then 09 Feb 2024, Lecture 10

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

Proof. Let $\phi : E \to E$ be the q–power Frobenius map. By Corollary 7.3, $\# E(\mathbb{F}_q) = q + 1 - \mathrm{tr}(q)$, so $\mathrm{tr}(\phi) = a$ and $\deg(\phi) = q$. By a result from Ex. Sheet 2, $\phi^2 - a\phi + q = 0$. Hence $\phi^{n+2} - a\phi^{n+1} + q\phi^n = 0$. As the trace is linear, $\mathrm{tr}(\phi^{n+2}) - a\mathrm{tr}(\phi^{n+1}) + q\mathrm{tr}(\phi^n) = 0$. The second order difference equation with initial conditions $\mathrm{tr}(1) = \langle 1, 1 \rangle = 2^2 - 1^2 - 1^2 = 2$ and $\mathrm{tr}(\phi) = a$ has solution

$$
\mathrm{tr}(\phi^n) = \alpha^n + \beta^n
$$

for $\alpha, \beta \in \mathbb{C}$ are roots of $X^2 - aX + q = 0$.[2] Apply Corollary 7.3 again to get

[2] We don't need to worry about the case where the roots are equal, since we don't want a general solution, just a solution satisfying our initial conditions.

that $\#E(\mathbb{F}_{q^n}) = q^n + 1 - \mathrm{tr}(\phi^n) = 1 + q^n - \alpha^n - \beta^n$. Hence

$$\begin{aligned} Z_E(T) &= \exp \sum_{n=1}^{\infty} \left(\frac{T^n}{n} + \frac{(qT)^n}{n} - \frac{(\alpha T)^n}{n} - \frac{(\beta T)^n}{n} \right) \\ &= \exp\left(-\log(1-T) - \log(1-qT) + \log(1-\alpha T) + \log(1-\beta T)\right) \\ &= \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)} \\ &= \frac{1 - aT + qT^2}{(1-T)(1-qT)}. \end{aligned}$$

□

Remark. Hasse's theorem tells us that $|a| \leq 2\sqrt{q}$, so the discriminant $a^2 - q$ is nonpositive, so the roots are complex conjugates, i.e. $\alpha = \overline{\beta}$, and $|\alpha| = |\beta| \overset{(\dagger)}{=} \sqrt{q}$.

Let $K = \mathbb{F}_q(E)$, then $\zeta_K(s) = 0 \implies Z_E(q^{-s}) = 0 \implies q^{-s} \in \{\frac{1}{\alpha}, \frac{1}{\beta}\} \implies q^s \in \{\alpha, \beta\} \implies q^{\mathrm{Re}(s)} = |\alpha| = |\beta| \implies \mathrm{Re}(s) = \frac{1}{2}$. This proves the Riemann hypothesis for elliptic curves over finite fields.

8 Formal groups

Definition 8.1. Let R be a ring and $I \subset R$ an ideal. The I–**adic topology** on R has basis $\{r + I^n \mid r \in R, n \geq 1\}$.

Definition 8.2. A sequence (x_n) in R is **Cauchy** if $\forall k$, $\exists N$ such that $x_m - x_n \in I^k$ $\forall m, n \geq N$.

Definition 8.3. R is **complete** if

(i) $\bigcap_{n \geq 0} I^n = \{0\}$ (this is a Hausdorff–type condition).

(ii) Every Cauchy sequence converges.

Useful remark. If $x \in I$, then $\frac{1}{1-x} = 1 + x + x^2 + \ldots$. This exists as the sequence of partial sums form a Cauchy sequence, and then we check that the result it converges to is an inverse for $\frac{1}{1-x}$. Hence $1 - x \in R^\times$.

Example 8.1. Basically the only two examples we care about in this course are:

- $R = \mathbb{Z}_p$, the p–adic integers, and $I = p\mathbb{Z}_p$.
- $R = \mathbb{Z}[[t]]$ and $I = (t)$.

Lemma 8.1 (Hensel's lemma)**.** Let R be complete with respect to an ideal I. Let $F \in R[X]$, $s \geq 1$ with $s \in \mathbb{Z}$. Suppose $a \in R$ satisfies

$$\begin{aligned} &F(a) \equiv 0 \pmod{I^s} \\ &F'(a) \in R^\times \end{aligned}$$

Then there exists a unique $b \in R$ such that $F(b) = 0$ and $b \equiv a \pmod{I^s}$.

Proof. Let $u \in R^\times$ be such that $F'(a) = u \pmod I$ (e.g. we could take $u = F'(a)$). Replacing $F(X)$ by $\frac{F(X+a)}{u}$ we may assume $a = 0$ and $F'(0) \equiv 1 \pmod I$. We put $x_0 = 0$ and $x_{n+1} \overset{(\dagger)}{=} x_n - F(x_n)$. Each induction shows that $x_n \equiv 0 \pmod{I^s}$ $\forall n$ ($\ddagger$). Now use the useful identity

$$F(X) - F(Y) = (X - Y)(F'(0) + XG(X, Y) + YH(X, Y))$$

for some $G, H \in R[X, Y]$. Call this identity ($\star$).

We claim that $x_{n+1} \equiv x_n \pmod{I^{n+s}}$ $\forall n \geq 0$. To prove this, use induction. The case $n = 0$ is clear. Suppose $x_n \equiv x_{n-1} \pmod{I^{n+s-1}}$. By ($\star$),

$$F(x_n) - F(x_{n-1}) = (x_n - x_{n-1})(1 + c)$$

for some $c \in I$. Modulo I^{n+s} we now use ($\dagger$) to get

$$\begin{aligned} &F(x_n) - F(x_{n-1}) \equiv x_n - x_{n-1} \pmod{I^{n+s}} \\ \Longrightarrow\ &x_n - F(x_n) = x_{n-1} - F(x_{n-1}) \pmod{I^{n+s}} \\ \Longrightarrow\ &x_{n+1} \equiv x_n \pmod{I^{n+s}}. \end{aligned}$$

Hence $(x_n)_{n \geq 0}$ is Cauchy, and R is complete, so $x_n \to b$ as $n \to \infty$ for some $b \in R$. Taking the limit in ($\dagger$) gives $b = b - F(b)$ (as the polynomial is continuous in our topology), so $F(b) = 0$. Taking the limit in ($\ddagger$) gives $b \equiv 0 \equiv a \pmod{I^s}$.

For uniqueness, if b_1, b_2 work, then plug them into ($\star$) and use the useful remark that $1 - x$ is a unit to get that $b_1 = b_2$. $\square$

Write $E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ and look at its affine piece $Y \neq 0$ with $t = -\frac{X}{Y}, w = -\frac{Z}{Y}$ (the minus signs are here to match Silverman's book). We get

$$w = t^3 + a_1tw + a_2t^2w + a_3w^2 + a_4tw^2 + a_6w^3 = f(t, w).$$

We apply Hensel's lemma (Lemma 8.1) with $R = \mathbb{Z}[a_1, \ldots, a_6][[t]]$, $I = (t)$ and $F(X) = X - f(t, X) \in R[X]$. We take $s = 3$, $a = 0$ and check that $F(a) = F(0) = -f(t, 0) = -t^3 \equiv 0 \pmod{I^3}$ and $F'(0) = 1 - a_1t - a_2t^2 \in R^x$

by our useful remark, so the assumptions hold. Hence there exists a unique $\omega(t) \in R = \mathbb{Z}[a_1, \ldots, a_6][[t]]$ such that $\omega(t) = f(t, w(t))$ and $w(t) \equiv 0 \pmod{t^3}$.

Remarks.

(i) Taking $u = 1$ in the proof of Hensel's lemma gives $w(t) = \lim_{n\to\infty} w_n(t)$ where $w_0(t) = 0$, $w_{n+1}(t) = f(t, w_n(t))$.

(ii) In fact, $w(t) = t^3(1 + A_1 t + A_2 t^2 + \ldots)$ where $A_1 = a_1$, $A_2 = a_1^2 + a_2$, $A_3 = a_1^3 + 2a_1a_2 + 2a_3$, etc. (i.e. we can compute the series explicitly).

12 Feb 2024, Lecture 11

Lemma 8.2. Let R be an integral domain, complete with respect to an ideal I. Let $a_0, \ldots, a_6 \in R$ and let $K = \mathrm{Frac}(R)$. Then

$$\widehat{E}(I) := \{(t, w) \in E(K) \mid t, w \in I\}$$

is a subgroup of $E(K)$.

Remark. By uniqueness in Hensel's lemma, $\widehat{E}(I) = \{(t, w(t)) \in E(K) \mid t \in I\}$.

Proof. Taking $(t, w) = (0, 0)$ shows $0_E \in \widehat{E}(I)$. So it suffices to show that if $P_1, P_2 \in \widehat{E}(I)$, then $P_3 := -P_1 - P_2 \in \widehat{E}(I)$. Since we're working over an affine piece with the identity at 0, we know three points sum to zero if and only if they lie on the same line. Say $P_i = (t_i, w_i)$ with the line P_1P_2 given by $w = \lambda t + \nu$. We have $P_1, P_2 \in \widehat{E}(I) \implies t_1, t_2 \in I$ and $w_1 = w(t_1), w_2 = w(t_2)$. Write $w(t) = \sum_{n=2}^{\infty} A_{n-2} t^{n+1}$ with $A_0 = 1$. We have

$$\lambda = \begin{cases} \frac{w(t_2) - w(t_1)}{t_2 - t_1} & \text{if } t_1 \neq t_2 \\ w'(t_1) & \text{if } t_1 = t_2 \end{cases} = \sum_{n=2}^{\infty} A_{n-2}(t_1^n + t_1^{n-1}t_2 + \ldots + t_2^n) \in I,$$
$$\nu = w_1 - \lambda t_1 \in I.$$

Substituting $w = \lambda t + \nu$ into $w = f(t, w)$ gives

$$\lambda t + \nu = t^3 + a_1 t(\lambda t + \nu) + a_2 t^2(\lambda t + \nu) + a_3(\lambda t + \nu)^2 + a_4 t(\lambda t + \nu)^2 + a_6(\lambda t + \nu)^3.$$

Let

$$A = (\text{coeff. of } t^3) = 1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3,$$
$$B = (\text{coeff. of } t^2) = a_1\lambda + a_2\nu + a_3\lambda^2 + 2a_4\lambda\nu + 3a_6\lambda^2\nu.$$

We have $A \in R^\times$, $B \in I$. Hence $t_3 = \frac{-B}{A} - t_1 - t_2 \in I$ and $w_3 = \lambda t_3 + \nu \in I$. $\square$

Taking $R = \mathbb{Z}[a_1, \ldots, a_6][[t]]$ and $I = (t)$ and using Lemma 8.2 implies $\exists \iota \in \mathbb{Z}[a_1, \ldots, a_6][[t]]$ with $\iota(0) = 0$ such that $[-1](t, w(t)) = (\iota(t), w(\iota(t)))$.

Taking $R = \mathbb{Z}[a_1, \dots, a_6][[t_1, t_2]]$ and $I = (t_1, t_2)$ and using Lemma 8.2 implies $\exists F \in \mathbb{Z}[a_1, \dots, a_6][[t_1, t_2]]$ with $F(0,0) = 0$ and

$$(t_1, w(t_1)) + (t_2, w(t_2)) = (F(t_1, t_2), w(F(t_1, t_2))).$$

In fact, $F(X,Y) = X + Y - a_1 XY - a_2(X^2 Y + XY^2) + \dots$.

By properties of the group law, we deduce

(i) $F(X,Y) = F(Y,X)$,

(ii) $F(X,0) = X$ and $F(0,Y) = Y$,

(iii) $F(X, F(Y,Z)) = F(F(X,Y),Z)$,

(iv) $F(X, \iota(X)) = 0$.

Definition 8.4. Let R be a ring. A **formal group** over R is a power series $F(X,Y) \in R[[X,Y]]$ satisfying the first three axioms above.

An exercise on Ex. Sheet 2 asks us to show that the first three conditions imply the fourth, i.e. there is a unique $\iota(X) = -X + \ldots \in R[[X]]$ such that $F(X, \iota(X)) = 0$.

Example 8.2. (i) The additive formal group $F(X,Y) = X + Y$, called $\widehat{\mathbb{G}_a}$.

(ii) The multiplicative formal group $F(X,Y) = X + Y + XY = (1+X)(1+Y) - 1$, called $\widehat{\mathbb{G}_m}$.

(iii) The formal group of an elliptic curve, $F(X,Y) =$ [see above], called $\widehat{E}$.

Definition 8.5. Let $\mathcal{F}$ and $\mathcal{G}$ be formal groups over R given by power serise F and G.

(i) A **morphism** $\mathcal{F} \to \mathcal{G}$ is a power series $f \in R[[T]]$ such that $f(0) = 0$ satisfying $f(F(X,Y)) = G(f(X), f(Y))$.

(ii) We say $\mathcal{F}$ is **isomorphic** to $\mathcal{G}$, i.e. $\mathcal{F} \cong \mathcal{G}$ if there exist morphisms $\mathcal{F} \xrightarrow{f} \mathcal{G}$ and $\mathcal{G} \xrightarrow{g} \mathcal{F}$ such that $f(g(T)) = g(f(T)) = T$.

Theorem 8.3. If char $R = 0$, then any formal group { over R is isomorphic to $\widehat{\mathbb{G}_a}$ over $R \otimes \mathbb{Q}$. (In other words, our conditions are char $R = 0$ and "the integers are invertible"). More precisely:

(i) There is a unique power series $\log(T) = T + \frac{a_2}{2} T^2 + \frac{a_3}{3} T^3 + \dots$ with $a_i \in R$ such that

$$\log(F(X,Y)) = \log(X) + \log(Y). \quad (\star)$$

(ii) There is a unique power series $\exp(T) = T + \frac{b_2}{2!}T^2 + \frac{b_3}{3!}T^3 + \dots$ with $b_i \in R$ such that
$$\exp(\log(T)) = \log(\exp(T)) = T.$$

Proof. (i) Notation: Write $F_1(X,Y) = \frac{\partial F}{\partial X}(X,Y)$. Uniqueness: Let $p(T) = \frac{\mathrm{d}}{\mathrm{d}T}\log T = 1 + a_2T + 1_3T^2 + \dots$. Differentiating $(\star)$ with respect to X gives $p(F(X,Y))F_1(X,Y) = p(X) + 0$. Putting $X = 0$ gives $P(Y)F_1(0,Y) = 1$, so $p(Y) = \frac{1}{F_1(0,Y)}$, proving uniqueness.

Existence: Let $p(T) = F_1(0,T)^{-1} = 1 + a_2T + a_3T^2 + \dots$ for some $a_i \in R$. Define $\log T = T + \frac{a_2}{2}T^2 + \frac{a_3}{3}T^3 + \dots$, so $p(T) = \frac{\mathrm{d}}{\mathrm{d}T}\log T$. Then

$$\begin{aligned} & F(F(X,Y),Z) = F(X,F(Y,Z)) \\ \overset{\frac{\mathrm{d}}{\mathrm{d}X}}{\Longrightarrow}\ & F_1(F(X,Y),Z)F_1(X,Y) = F_1(X,F(Y,Z)) \\ \overset{X=0}{\Longrightarrow}\ & F_1(Y,Z)p(Y)^{-1} = p(F(Y,Z))^{-1} \\ \Longrightarrow\ & F_1(Y,Z)p(F(Y,Z)) = p(Y) \\ \overset{\text{intg. wrt } Y}{\Longrightarrow}\ & \log(F(Y,Z)) = \log(Y) + h(Z) \end{aligned}$$

for some power series H. But the symmetry in Y and Z implies that $h(Z) = \log Z$, so we're done. 14 Feb 2024, Lecture 12

(ii) For this, use

Lemma 8.4. Let $f(T) = aT + \dots \in R[[T]]$ with $a \in R^\times$. Then there exists a unique $g(T) = a^{-1}T + \dots \in R[[T]]$ with $f(g(T)) = g(f(T)) = T$.

Proof. We construct polynomials $g_n(T) \in R[T]$ such that $f(g_n(T)) \equiv T \pmod{T^{n+1}}$ and $g_{n+1}(T) \equiv g_n(T) \pmod{T^{n+1}}$. Then $g(T) = \lim_{n\to\infty} g_n(T)$ satisfies $f(g(T)) = T$. To start the induction, set $g_1(T) = a^{-1}T$.

Now suppose $n \geq 2$, so $g_{n-1}(T)$ exists, so $f(g_{n-1}(T)) \equiv T + bT^n \pmod{T^{n+1}}$ for some $b \in R$. We put $g_n(T) = g_{n-1}(T) + \lambda T^n$ for $\lambda \in R$ to be chosen later. Then $f(g_n(T)) = f(g_{n-1}(T) + \lambda T^n) = f(g_{n-1}(T)) + \lambda a T^n \equiv T + (b + \lambda a)T^n \pmod{T^{n+1}}$, so we take $\lambda = -ba^{-1}$ (then $\lambda \in R$ as $b \in R, a \in R^\times$), completing the induction step.

We get $g(T) = a^{-1}T + \dots \in R[[T]]$ such that $f(g(T)) = T$ (†). Applying the same construction to g gives $h(T) = a + \dots \in R[[T]]$ such that $g(h(T)) = T$ (‡). Now note that $f(T) \overset{(‡)}{=} f(g(h(T))) \overset{(†)}{=} h(T)$, so $f = h$. □

The result now follows from this lemma and Ex. Sheet 2 Q5 (which allows us to control the denominators, so they'd be $n!$).

□

Notation. Let $\mathcal{F}$ be a formal group (e.g. $\widehat{\mathbb{G}_a}, \widehat{\mathbb{G}_m}, \widehat{E}$) given by a power series $F \in R[[X,Y]]$. Suppose R is complete with respect to an ideal I. For $x, y \in I$. define $x \oplus_{\mathcal{F}} y = F(x,y) \in I$. Then $\mathcal{F}(I) = (I, \oplus_{\mathcal{F}})$ is an abelian group.

Example 8.3.

- $\widehat{\mathbb{G}_a}(I) = (I, +)$,
- $\widehat{\mathbb{G}_m}(I) = (1 + I, \times)$,
- $\widehat{E}(I) =$ subgroup of $E(K)$ in Lemma 8.2.

Corollary 8.5. Let $\mathcal{F}$ be a formal group over R and $n \in \mathbb{Z}$. Suppose $n \in R^\times$. Then

(i) $[n] : \mathcal{F} \to \mathcal{F}$ is an isomorphism of formal groups.

(ii) If R is complete with respect to an ideal I, then $\mathcal{F}(I) \overset{\times n}{\to} \mathcal{F}(I)$ is an isomorphism of groups. In particular, $\mathcal{F}(I)$ has no n-torsion.

Proof. We define $[I](T) = T$ and $[n](T) = F([n-1]T, T)$ $\forall n \geq 2$. (For $n < 0$, use $[-1](T) = \iota(T)$). Since $F(X,Y) = X + Y + XY(\dots)$, we have $[2](T) = f(T,T) = 2T + \dots$. By induction we get $[n](T) = nT + \dots \in R[[T]]$. Lemma 8.4 shows that if $n \in R^\times$, then $[n]$ is an isomorphism. This proves (i). Part (ii) now follows. $\square$

9 Elliptic curves over local fields

Let K be a field, compelte with respect to a discrete valuation $v : K \to \mathbb{Z}$. (Here complete means complete with respect to the matric given by the absolute value arising from v.)

- The **valuation ring** is $\mathcal{O}_K = \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$.
- The **unit group** is $\mathcal{O}_K^\times = \{x \in K^\times \mid v(x) = 0\}$.
- The **maximal ideal** is $\pi\mathcal{O}_K$, where $v(\pi) = 1$.
- The **residue field** is $k = \mathcal{O}_K / \pi\mathcal{O}_K$.

We assume that char $K = 0$, but $\mathrm{char}(k) = p > 0$ (i.e. we are in the mixed characteristic case). The key example to keep in mind is $K = \mathbb{Q}_p, \mathcal{O}_K = \mathbb{Z}_p, k = \mathbb{F}_p$. Now let E/K be an elliptic curve.

Definition 9.1. A Weierstrass equation for E with coefficients $a_1, \dots, a_6 \in K$ is **integral** if $a_1, \dots, a_6 \in \mathcal{O}_K$ and **minimal** if $v(\Delta)$ is minimal among all integral Weierstrass equations for E.

Remarks.

(i) Rescaling $x = u^2x', y = u^3y'$ gives $a_i = u^ia_i'$, so we can clear denominators, so integral Weierstrass equations exist.

(ii) $a_1, \dots, a_6 \in \mathcal{O}_K \implies \Delta \in \mathcal{O}_K \implies v(\Delta) \geq 0 \implies$ minimal Weierstrass equations exist.

(iii) If $\mathrm{char}(k) \neq 2, 3$, then there exists a minimal Weierstrass equation of the form $y^2 = x^3 + ax + b$.

Lemma 9.1. Let E/K have integral Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Let $0 \neq P = (x, y) \in E(K)$. Then either $x, y \in \mathcal{O}_K$ or $\begin{cases} v(x) = -2s \\ v(y) = -3s \end{cases}$ for some $s \geq 1$. (Compare this with Ex. Sheet 1 Q5.)

Proof.
- Case $v(x) \geq 0$: Suppose $v(y) < 0$. Then $v(\text{LHS}) = v(y^2) < 0$ while $v(\text{RHS}) \geq 0$, a contradiction. Hence $v(y) \geq 0$, so $x, y \in \mathcal{O}_K$.
- Case $v(x) < 0$: We have $v(\text{LHS}) \geq \min(2v(y), v(x) + v(y), v(y))$ and $v(\text{RHS}) = 3v(x)$. Go through 3 cases based on which element is minimal to get $v(y) < v(x)$ in every case. Now $v(\text{LHS}) = 2v(y)$, $v(\text{RHS}) = 3v(x)$, so we're done.

□

If K is complete, then $\mathcal{O}_K$ is complete with respect to $\pi^r\mathcal{O}_K$ for any $r \geq 1$. We fix a minimal Weierstrass equation for E/K. This gives rise to a formal group $\widehat{E}$ over $\mathcal{O}_K$. Take $R = \mathcal{O}_K$, $I = \pi^r\mathcal{O}_K$ for $r \geq 1$ in Lemma 8.2 to get

$$\begin{aligned} \widehat{E}(\pi^r\mathcal{O}_K) &= \left\{(x, y) \in E(K) \mid -\frac{x}{y}, -\frac{1}{y} \in \pi^r\mathcal{O}_K\right\} \cup \{0\} \\ &= \left\{(x, y) \in E(K) \mid v\left(\frac{x}{y}\right) \geq r, v\left(\frac{1}{y}\right) \geq r\right\} \cup \{0\} \\ &= \{(x, y) \in E(K) \mid v(x) = -2s, v(y) = -3s \text{ for some } s \geq r\} \cup \{0\} \\ &= \{(x, y) \in E(K) \mid v(x) \leq -2r, v(y) \leq -3r\} \cup \{0\}. \end{aligned}$$

By Lemma 8.2 this is a subgroup of $E(K)$, call it $E_r(K)$. It is also clear that $\ldots \subset E_3(K) \subset E_2(K) \subset E_1(K) \subset E(K)$. More generally, for $\mathcal{F}$ a formal group over $\mathcal{O}_K$ we have $\ldots \subset \mathcal{F}(\pi^3\mathcal{O}_K) \subset \mathcal{F}(\pi^2\mathcal{O}_K) \subset \mathcal{F}(\mathcal{O}_K)$. We claim that

16 Feb 2024, Lecture 13

- $\mathcal{F}(\pi^r\mathcal{O}_K) \cong (\mathcal{O}_K, +)$ for r sufficiently large,
- $\mathcal{F}(\pi^r\mathcal{O}_K)/\mathcal{F}(\pi^{r+1}\mathcal{O}_K) \cong (k, +)$ $\forall r \geq 1$.

Reminder. Remember that we always have $\mathrm{char}\, K = 0, \mathrm{char}(k) = p > 0$.

Theorem 9.2. Let $\mathcal{F}$ be a formal group over $\mathcal{O}_K$. Let $e = v(p)$. If $r > \frac{e}{p-1}$, then

$$\log : \mathcal{F}(\pi^r\mathcal{O}_K) \xrightarrow{\sim} \widehat{\mathbb{G}_a}(\pi^r\mathcal{O}_K)$$

is an isomorphism of groups with inverse

$$\exp : \widehat{\mathbb{G}_a}(\pi^r\mathcal{O}_K) \xrightarrow{\sim} \mathcal{F}(\pi^r\mathcal{O}_K).$$

Remark. We have $\widehat{\mathbb{G}_a}(\pi^r\mathcal{O}_K) = (\pi^r\mathcal{O}_K, +) \cong (\mathcal{O}_K, +)$.

Proof. For $x \in \pi^r\mathcal{O}_K$, we must show that the power series $\log(x)$ and $\exp(x)$ converge to elements in $\pi^r\mathcal{O}_K$. Recall $\exp(T) = T + \frac{b_2}{2!}T^2 + \frac{b_3}{3!}T^3 + \ldots$ with $b_i \in \mathcal{O}_K$.

Claim. $v_p(n!) \le \frac{n-1}{p-1}$.

Proof of claim. Write

$$v_p(n!) = \sum_{r=1}^{\infty} \left\lfloor \frac{n}{p^r} \right\rfloor < \sum_{r=1}^{\infty} \frac{n}{p^r} = \frac{n \cdot \frac{1}{p}}{1 - \frac{1}{p}} = \frac{n}{p-1}.$$

Clearing denominators, $(p-1)v_p(n!) < n \implies v_p(n!) \le \frac{n-1}{p-1}$. □

Now $v\left(\frac{b_n x^n}{n!}\right) \ge nr - e\left(\frac{n-1}{p-1}\right) = (n-1)\underbrace{\left(r - \frac{e}{p-1}\right)}_{>0} + r$. This is always $\ge r$ and tends to infinity as $n \to \infty$. Hence $\exp(x)$ converges to an element of $\pi^r\mathcal{O}_K$. The same argument works for log. □

Lemma 9.3. We have $\mathcal{F}(\pi^r\mathcal{O}_K)/\mathcal{F}(\pi^{r+1}\mathcal{O}_K) \cong (k, +)\ \forall r \ge 1$.

Proof. Our definition of a formal group gives $F(X,Y) = X + Y + XY(\ldots)$. So if $x, y \in \mathcal{O}_K$, then $F(\pi^r x, \pi^r y) \equiv \pi^r(x+y) \pmod{\pi^{r+1}}$. Therefore $\mathcal{F}(\pi^r\mathcal{O}_K) \to (k, +)$ by $\pi^r x \mapsto x \bmod \pi$ is a surjective group homomorphism with kernel $\mathcal{F}(\pi^{r+1}\mathcal{O}_K)$. □

Corollary 9.4. If $|k| < \infty$, then $\mathcal{F}(\pi\mathcal{O}_K)$ has a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.

Notation. Denote reduction mod π, $\mathcal{O}_K \to \mathcal{O}_K/\pi\mathcal{O}_K = k$ by $x \mapsto \widetilde{x}$.

Proposition 9.5. Let E/K be an elliptic curve. Then the reductions mod π of any two minimal Weierstrass equations for E define isomorphic curves over k.

Proof. Say the Weierstrass equations are related by $[u, r, s, t]$ with $u \in K^\times, r, s, t \in K$. Then $\Delta_1 = u^{12}\Delta_2$, but both equations are minimal, so $v(u) = 0 \implies u \in \mathcal{O}_K^\times$. The transformation formulae (on the formula sheet) for the a_i and b_i combined with the fact that $\mathcal{O}_K$ is algebraically closed imply $r, s, t \in \mathcal{O}_K$. The Weierstrass equations of the reduction mod π are now related by $[\widetilde{u}, \widetilde{r}, \widetilde{s}, \widetilde{t}]$ with $\widetilde{u} \in k^\times$, $\widetilde{r}, \widetilde{s}, \widetilde{t} \in k$. $\square$

Definition 9.2. The reduction $\widetilde{E}/k$ of E/K is defined by the reduction mod π of a minimal Weierstrass equation for E. We say E has **good reduction** if $\widetilde{E}$ is nonsingular (and so $\widetilde{E}$ is an elliptic curve), otherwise E has **bad reduction**.

For an integral Weierstrass equation,

- $v(\Delta) = 0 \implies$ good reduction.
- $0 < v(\Delta) < 12 \implies$ bad reduction.
- $v(\Delta) \geq 12 \implies$ beware that the equation might not be minimal, more information is needed.

There is a well-defined map $\mathbb{P}^2(K) \to \mathbb{P}^2(k)$ by $(x : y : z) \mapsto (\widetilde{x} : \widetilde{y} : \widetilde{z})$. (Here we must choose a representative for $(x : y : z)$ such that $\min(v(x), v(y), v(z)) = 0$.) We restrict to get a map $E(K) \to \widetilde{E}(k)$ by $P \mapsto \widetilde{P}$.

IF $P = (x, y) \in E(K)$, then by Lemma 9.1, either $x, y \in \mathcal{O}_K$, so $\widetilde{P} = (\widetilde{x}, \widetilde{y}) \in \widetilde{E}(k)$, or $v(x) = -2s, v(y) = -3s$ for some $s \geq 1$, so $P = (x : y : 1) = (\pi^{3s}x : \pi^{3s}y : \pi^{3s})$, so $\widetilde{P} = (0 : 1 : 0)$. Therefore

$$\widehat{E}(\pi\mathcal{O}_K) = E_1(K) = \{P \in E(K) \mid \widetilde{P} = 0\},$$

the **kernel of reduction**. Let

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

We have a remarkable fact: the chord and tangent process still defines a group law on $\widetilde{E}_{\text{ns}}$. However, in the case of bad reductions, either $\widetilde{E}_{\text{ns}} \cong \mathbb{G}_a$ (over k) or $\widetilde{E}_{\text{ns}} \cong \mathbb{G}_m$ (over k or possibly over a quadratic extension of k). These are the additive reduction and the multiplicative reduction.

19 Feb 2024, Lecture 14

For simplicity, assume char $k \neq 2$. Then for $\widetilde{E} : y^2 = f(x)$, $\deg f = 3$, we have that $\widetilde{E}$ is singular if and only if f has a repeated root.

- If this is a double root, we get $\mathbb{G}_m$ (e.g. for $y^2 = x^2(x + 1)$, a curve with a node).
- If this is a triple root, we get $\mathbb{G}_a$ (e.g. for $y^2 = x^3$, a curve with a cusp).

The proof of the former is on Ex. Sheet 3. For the latter, consider the map $\mathbb{G}_a \to \widetilde{E}_{\text{ns}}$ by $t \mapsto (t^{-2}, t^{-3})$, so $\frac{x}{y} \leftarrow\!\shortmid (x,y)$ and the point at infinity $\leftrightarrow 0$. Suppose we have a line through P_1, P_2 meeting the curve again at P_3 (with none of these points at the origin), so this line is $ax + by = 1$. Write $P_i = (x_i, y_i)$ for $i = 1, 2, 3$, and $t_i = \frac{x_i}{y_i}$. Then

$$
\begin{aligned}
& x_i^3 = y_i^2 = y_i^2(ax_i + by_i) \\
\implies & t_i^3 at_i - b = 0 \\
\implies & t_1, t_2, t_3 \text{ are roots of } X^3 - aX - b = 0.
\end{aligned}
$$

Looking at the coefficient of X^2 gives $t_1 + t_2 + t_3 = 0$, so $\widetilde{E}_{\text{ns}} \cong \mathbb{G}_a$.

Definition 9.3. We define

$$E_0(K) = \{P \in E(K) \mid \widetilde{P} \in \widetilde{E}_{\text{ns}}(k)\}.$$

Proposition 9.6. *$E_0(K)$ is a subgroup of $E(K)$ and reduction mod π is a surjective group homomorphism $E_0(K) \to \widetilde{E}_{\text{ns}}(K)$.*

Proof. The group homomorphism part: A line ℓ in $\mathbb{P}^2$ defined over K has equation $\ell : aX + bY + cZ = 0$ for $a, b, c \in K$, where we may assume that $\min(v(a), v(b), v(c)) = 0$ by scaling.

Reduction mod π gives a line $\widetilde{\ell} : \widetilde{a}X + \widetilde{b}Y + \widetilde{c}Z = 0$. If $P_1, P_2, P_3 \in E(K)$ with $P_1 + P_2 + P_3 = 0$, then these points lie on a line ℓ, so $\widetilde{P}_1, \widetilde{P}_2, \widetilde{P}_3$ lie on the line $\widetilde{\ell}$. If $\widetilde{P}_1, \widetilde{P}_2 \in \widetilde{E}_{\text{ns}}(k)$, then $\widetilde{P}_3 \in \widetilde{E}_{\text{ns}}(k)$. Hence if $P_1, P_2 \in E_0(K)$, then $P_3 \in E_0(K)$ and $\widetilde{P}_1 + \widetilde{P}_2 + \widetilde{P}_3 = 0$. It is left as an exercise to check that this still works if $\#\{\widetilde{P}_1, \widetilde{P}_2, \widetilde{P}_3\} < 3$.

For surjectivity, let $f(x,y) = y^2 + a_1xy + a_3y - (x^3 + \ldots)$. Let $\widetilde{P} \in \widetilde{E}_{\text{ns}}(k) \setminus \{0\}$, say $\widetilde{P} = (\widetilde{x}_0, \widetilde{y}_0)$ for some $x_0, y_0 \in \mathcal{O}_K$. As $\widetilde{P}$ is nonsingular, we either have $\frac{\partial f}{\partial x}(x_0, y_0) \not\equiv 0 \bmod \pi$ or $\frac{\partial f}{\partial y}(x_0, y_0) \not\equiv 0 \bmod \pi$.

In the first case, we put $g(t) = f(t, y_0) \in \mathcal{O}_K[t]$ to get $\begin{cases} g(x_0) \equiv \pmod{\pi}, \\ g'(x_0) \in \mathcal{O}_K^\times, \end{cases}$

so by Hensel's lemma $\exists b \in \mathcal{O}_K$ such that $\begin{cases} g(b) = 0, \\ b \equiv x_0 \pmod{\pi}. \end{cases}$ Then $(b, y_0) \in E(K)$ has reduction $\widetilde{P}$. The second case is analogous. $\square$

Recall that for $r \geq 1$, we put

$$E_r(K) = \{(x,y) \in E(K) \mid v(x) \leq -2r, v(y) \leq -3r\} \cup \{0\}$$

and we have $\ldots \subset E_r(K) \subset \ldots \subset E_1(K) \subset E_0(K) \subset E_K$. Recall that $\widehat{E}(\pi^r\mathcal{O}_K) = E_r(K)$ by definition. We know that we have $E_r(K) \cong (\mathcal{O}_K, +)$

if $r > \frac{e}{p-1}$ and $E_r(K)/E_{r+1}(K) \cong (k,+)\ \forall r \geq 1$. We can extend this to include $E_0(K)/E_1(K) \cong \widetilde{E}_{\text{ns}}(K)$. What about $E_0(K)/E(K)$?

Lemma 9.7. If $|k| < \infty$, then $E_0(K) \subset E_K$ has finite index.

Proof. $|k| < \infty \implies \frac{\mathcal{O}_K}{\pi^r\mathcal{O}_K}$ is finite $\forall r \geq 1$. Hence $\mathcal{O}_K = \varprojlim_r \mathcal{O}_K/\pi^r\mathcal{O}_K$ is a profinite group, hence compact. Then $\mathbb{P}^n(K)$ is a union of sets of the form

$$\{(a_0 : a_1 : a_2 : \ldots : a_{i-1} : 1 : a_{i+1} : \ldots a_n) \mid a_j \in \mathcal{O}_K\}$$

and hence is compact (with respect to the π-adic topology on K). $E(K) \subset \mathbb{P}^2(K)$ is a closed subset and hence compact, so $E(K)$ is a compact topological group. If $\widetilde{E}$ has a singular point $(\widetilde{x}_0, \widetilde{y}_0)$, then

$$E(K) \setminus E_0(K) = \{(x,y) \in E(K) \mid v(x-x_0) \geq 1, v(y-y_0) \geq 1\}$$

is a closed subset of $E(K)$, so $E_0(K)$ is an open subgroup of $E(K)$. But the cosets of $E_0(K)$ are open, so $[E(K) : E_0(K)] < \infty$ by compactness of $E(K)$. $\square$

Definition 9.4. $c_K(E) = [E_K : E_0(K)]$ is called the **Tamagawa number**.

Remarks.

(i) Good reduction implies $c_K(E) = 1$, but the converse is false.

(ii) It can be shown that either $c_K(E) = v(\Delta)$ or $c_K(E) \leq 4$ (here it is essential that we work with a minimal Weierstrass equation).

We deduce the following:

Theorem 9.8. If $[K : \mathbb{Q}_p] < \infty$, then $E(K)$ contains a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.

Some setup: Let $[K : \mathbb{Q}_p] < \infty$, L/K a finite extension with residue fields k and k' and $f = [k' : k]$. This gives us the map
$$\begin{array}{ccc} K^\times & \xrightarrow{v_K} & \mathbb{Z} \\ \cap & & \big\downarrow{\times e} \\ L^\times & \xrightarrow{v_L} & \mathbb{Z} \end{array}.$$

Facts.

(i) $[L : K] = ef$.

(ii) If L/K is Galois, then the natural map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k'/k)$ is surjective with kernel of order e.

Definition 9.5. L/K is **unramified** if $e = 1$.

21 Feb 2024, Lecture 15

Facts.

(i) For each $m \geq 1$, k has a unique extension of degree m (say k_m).

(ii) For each $m \geq 1$, K has a unique unramified extension of degree m (say K_m).

These extensions are Galois with cyclic Galois group.

Definition 9.6. We have the maximal unramified extension of K,

$$K^{\mathrm{nr}} = \bigcup_{m \geq 1} K_m \subset \overline{K}.$$

Theorem 9.9. Let $[K : \mathbb{Q}] < \infty$. Suppose E/K has good reduction and $p \nmid n$. If $P \in E(K)$, then $K([n]^{-1}P)/K$ is unramified.

Notation. We have

$$[n]^{-1}(P) = \{Q \in E(\overline{K}) \mid nQ = P\}$$

and we let

$$K(\{Q_1, \ldots, Q_r\}) = K(x_1, y_1, \ldots, x_r, y_r),$$

where $Q_i = (x_i, y_i)$.

Proof. For each $m \geq 1$, there is a short exact sequence

$$0 \to E_1(K_m) \to E(K_m) \to \widetilde{E}_{k_m} \to 0.$$

Taking the union $\bigcup_{m \geq 1}$ gives us a commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & E_1(K^{\mathrm{nr}}) \arrow[r] \arrow[d, "\times n"] & E(K^{\mathrm{nr}}) \arrow[r] \arrow[d, "\times n"] & \widetilde{E}(\bar{k}) \arrow[r] \arrow[d, "\times n"] & 0 \\
0 \arrow[r] & E_1(K^{\mathrm{nr}}) \arrow[r] & E(K^{\mathrm{nr}}) \arrow[r] & \widetilde{E}(\bar{k}) \arrow[r] & 0
\end{tikzcd},$$

The first multiplication map is an isomorphism by Corollary 8.5 applied to each K_m (using $p \nmid n$).

The third is surjective by Theorem 2.3, and has kernel $\cong (\mathbb{Z}/n\mathbb{Z})^2$ by Theorem 6.5 (again using $p \nmid n$). Using the snake lemma on this diagram gives $E(K^{\mathrm{nr}})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ and $E(K^{\mathrm{nr}})/nE(K^{\mathrm{nr}}) = 0$. So if $P \in E(K)$, then $\exists Q \in E(K^{\mathrm{nr}})$ with $nQ = P$ and $[n]^{-1}P = \{Q + T \mid T \in E[n]\} \subset E(K^{\mathrm{nr}})$. Hence $K([n]^{-1}P) \subset K^{\mathrm{nr}}$ and so $K([n]^{-1}P)/K$ is unramified. $\square$

10 Elliptic curves over number fields

10.1 The torsion subgroup

Notation. Let E/K be an elliptic curve for $[K:\mathbb{Q}] < \infty$. We write $\mathfrak{p}$ for a prime of K (i.e. of $\mathcal{O}_K$), $K_\mathfrak{p}$ for the $\mathfrak{p}$-adic completion of K, and $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$.

Definition 10.1. $\mathfrak{p}$ is a prime of good reduction for E/K if $E/K_\mathfrak{p}$ has good reduction.

Lemma 10.1. E/K has only finitely many primes of bad reduction.

Proof. Take a Weierstrass equation for E with $a_1, \ldots, a_6 \in \mathcal{O}_K$. Since E is nonsingular, $0 \neq \Delta \in \mathcal{O}_K$. Write $(\Delta) = \mathfrak{p}_1^{\alpha_1} \ldots \mathfrak{p}_r^{\alpha_r}$ for the factorization into prime ideals and let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. If $\mathfrak{p} \notin S$, then $v_\mathfrak{p}(\Delta) = 0$, so $E/K_\mathfrak{p}$ has good reduction. Hence $\{\text{bad primes of } E\} \subset S$ is finite. □

Remark. If K has class number 1 (e.g. if $K = \mathbb{Q}$), then we can always find a Weierstrass equation for E with $a_1, \ldots, a_6 \in \mathcal{O}_K$ which is minimal at all primes $\mathfrak{p}$.

Basic group theory. If A is a finitely generated abelian group, then

$$A \cong (\text{finite group}) \times \mathbb{Z}^r$$

for the finite group the **torsion subgroup** and r the **rank**.

Lemma 10.2. $E(K)_{\text{tors}}$ is finite.

Proof. Take any prime $\mathfrak{p}$. We saw that $E(K_\mathfrak{p})$ has a subgroup A of finite index with $A \cong (\mathcal{O}_\mathfrak{p}, +)$. In particular, A is torsion-free. Hence we get

$$E(K)_{\text{tors}} \subset E(K_\mathfrak{p})_{\text{tors}} \hookrightarrow E(K_\mathfrak{p})/A,$$

and this last group is finite. □

Lemma 10.3. Let $\mathfrak{p}$ be a prime of good reduction. Then reduction mod $\mathfrak{p}$ gives an injective group homomorphism $E(K)[n] \hookrightarrow \widetilde{E}(k_\mathfrak{p})$.

Proof. Proposition 9.6 implies that $E(K_\mathfrak{p}) \to \widetilde{E}(k_\mathfrak{p})$ is a group homomorphism with kernel $E_1(K_\mathfrak{p})$. Corollary 8.5 and the fact that $\mathfrak{p} \nmid n$ imply now that $E_1(K_\mathfrak{p})$ has no n-torsion. □

Example 10.1. Let $E/\mathbb{Q}$ be given by $y^2 + y = x^3 - x^2$. Then $\Delta = -11$, so E has good reduction at all $p \neq 11$. We can count

p	2	3	5	7	11	13
$\#\widetilde{E}(\mathbb{F}_p)$	5	5	5	10	–	10

.

By Lemma 10.3, $\#E(\mathbb{Q})_{\mathrm{tors}} \mid 5 \cdot 2^a$ for some $a \geq 0$ and $\#E(\mathbb{Q})_{\mathrm{tors}} \mid 5 \cdot 3^b$ for some $b \geq 0$. This implies that $\#E(\mathbb{Q}) \mid 5$. If we let $T = (0,0) \in E(\mathbb{Q})$, then calculation shows $5T = 0$, so $E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/5\mathbb{Z}$.

Example 10.2. Let $E/\mathbb{Q}$ be given by $y^2 + y = x^3 + x^2$. Then $\Delta = -43$, and we get

p	2	3	5	7	11	13
$\#\widetilde{E}(\mathbb{F}_p)$	5	6	10	8	9	19

By Lemma 10.3, $\#E(\mathbb{Q})_{\mathrm{tors}} \mid 5 \cdot 2^a$ for some $a \geq 0$ and $\#E(\mathbb{Q})_{\mathrm{tors}} \mid 9 \cdot 11^b$ for some $b \geq 0$, so $E(\mathbb{Q})_{\mathrm{tors}} = \{0\}$. Hence the point $P = (0,0)$ is a point of infinite order. In particular, $E(\mathbb{Q})$ is infinite.

23 Feb 2024, Lecture 16

Example 10.3. Let $E_D/\mathbb{Q}$ be given by $E_D : y^2 = x^3 - D^2x$ for $D \in \mathbb{Z}$ squarefree. Then $\Delta = 2^6 D^6$ and we spot

$$E_D(\mathbb{Q})_{\mathrm{tors}} \supset \{0, (0,0), (\pm D, 0)\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

Let $f(x) = x^3 - D^2x$. If $p \nmid 2D$, then

$$\#\widetilde{E}_D(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} \left(\left(\frac{f(x)}{p} \right) + 1 \right).$$

If $p \equiv 3 \bmod 4$, then $\#\widetilde{E}_D(\mathbb{F}_p) = p + 1$, since

$$\left(\frac{f(-x)}{p} \right) = \left(\frac{-f(x)}{p} \right) = \left(\frac{-1}{p} \right) \left(\frac{f(x)}{p} \right) = -\left(\frac{f(x)}{p} \right).$$

Let $m = \#E_D(\mathbb{Q})_{\mathrm{tors}}$. We have $4 \mid m \mid (p+1)$ for all sufficiently large primes p with $p \equiv 3 \bmod 4$ ($p \nmid 2Dm$ suffices).

If $8 \mid m$ or $l \mid m$ for some odd prime l, then this contradicts Dirichlet's Theorem on primes in arithmetic progressions. Hence $m = 4$ and so $E_D(\mathbb{Q})_{\mathrm{tors}} = (\mathbb{Z}/2\mathbb{Z})^2$. Thus

$$\operatorname{rank} E_D(\mathbb{Q}) \geq 1 \iff \exists x, y \in \mathbb{Q} \text{ with } y \neq 0 \text{ and } y^2 = x^3 - D^2x.$$

By Lecture 1, this is equivalent to D being a congruent number.

Lemma 10.4. Let $E/\mathbb{Q}$ be given by a Weierstrass equation with $a_1, \ldots, a_6 \in \mathbb{Z}$. Suppose $0 \neq T = (x,y) \in E(\mathbb{Q})_{\mathrm{tors}}$. Then

(i) $4x, 8y \in \mathbb{Z}$.

(ii) If $2 \mid a_1$ or $2T \neq 0$, then $x, y \in \mathbb{Z}$.

Proof. The Weierstrass equation defines a formal group $\widehat{E}$ over $\mathbb{Z}$. For $r \geq 1$, we have

$$\widehat{E}(p^r\mathbb{Z}_p) = \{(x,y) \in E(\mathbb{Q}_p) \mid v_p(x) \leq -2r, v_p(y) \leq -3r\} \cup \{0\}.$$

By Theorem 9.2, $\widehat{E}(p^r\mathbb{Z}_p) \cong (\mathbb{Z}_p, +)$ if $r > \frac{1}{p-1}$. Hence $\widehat{E}(4\mathbb{Z}_2)$ and $\widehat{E}(p\mathbb{Z}_p)$ for p odd are torsion-free. This means that $v_2(x) \geq -2, v_2(y) \geq -3$ and $v_p(x), v_p(y) \geq 0$ for all odd primes p, which proves (i).

For the second part, suppose $T \in \widehat{E}(4\mathbb{Z}_2)$, i.e. $v_2(x) = -2, v_2(y) = -3$. Since $\widehat{E}(2\mathbb{Z}_2)/\widehat{E}(4\mathbb{Z}_2) \cong (\mathbb{F}_2, +)$ and $\widehat{E}(4\mathbb{Z}_2)$ is torsion-free, we get $2T = 0$. Also, $(x,y) = T = -T = (x, -y - a_1x - a_3) \implies 2y + a_1x + a_3 = 0$, so $8y + a_1(4x) + 4a_3 = 0$. Since $8y, 4x, 4a_3$ are even, we require a_1 to be odd. So if $2T \neq 0$ or a_1 is even, then $T \notin \widehat{E}(2\mathbb{Z}_2)$, so $x, y \in \mathbb{Z}$. $\square$

Example 10.4. For $E : y^2 + xy = x^3 + 4x + 1$, $\left(-\frac{1}{4}, \frac{1}{8}\right) \in E(\mathbb{Q})[2]$.

Theorem 10.5 (Lutz-Nagell)**.** Let $E/\mathbb{Q}$ be given by $y^2 = x^3 + ax + b = f(x)$ for $a, b \in \mathbb{Z}$. Suppose $0 \neq T = (x,y) \in E(\mathbb{Q})_{\text{tors}}$. Then $x, y \in \mathbb{Z}$ and either $y = 0$ or $y^2 \mid (4a^3 + 27b^2)$.

Proof. Lemma 10.4 implies that $x, y \in \mathbb{Z}$. If $2T = 0$, then $y = 0$. Otherwise, $0 \neq 2T = (x_2, y_2) \in E(\mathbb{Q})_{\text{tors}}$, so by Lemma 10.4, $x_2, y_2 \in \mathbb{Z}$. But $x_2 = \left(\frac{f'(x)}{2y}\right)^2 - 2x \implies y \mid f'(x)$. As E is nonsingular, $f(X)$ and $f'(X)$ are coprime, so $f(X)$ and $f'(X)^2$ are coprime, so $\exists g, h \in \mathbb{Q}[X]$ with $g(X)f(X) + h(X)f'(X)^2 = 1$. In fact, we can check that

$$(3X^2 + 4a)f'(X)^2 - 27(X^3 + aX - b)f(X) = 4a^3 + 27b^2.$$

Since $y \mid f'(x)$ and $y^2 = f(x)$, we get $y^2 \mid (4a^3 + 27b^2)$. $\square$

Remark. Mazur showed that if $E/\mathbb{Q}$ is an elliptic curve, then

$$E(\mathbb{Q})_{\text{tors}} \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} & 1 \leq n \leq 12, n \neq 11, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} & 1 \leq n \leq 4. \end{cases}$$

Moreover, all 15 possibilies occur.

11 Kummer theory

Let K be a field with char $K \nmid n$. Assume $\mu_n \subset K$ for μ_n the set of n^{th} (primitive?) roots of unity.

Lemma 11.1. Let $\Delta \subset K^\times/(K^\times)^n$ be a finite subgroup and let $L = K(\sqrt[n]{\Delta})$. Then L/K is Galois and $\text{Gal}(L/K) \cong \text{Hom}(\Delta, \mu_n)$.

Proof. L/K is Galois since $\mu_n \subset K \implies L/K$ normal and $\operatorname{char} K \nmid n \implies L/K$ separable. Define the **Kummer pairing**

$$\begin{aligned} \langle \ , \ \rangle : \operatorname{Gal}(L/K) \times \Delta &\to \mu_n \\ (\sigma, x) &\mapsto \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}}. \end{aligned}$$

This is well-defined: If $\alpha, \beta \in L$ with $\alpha^n = \beta^n = x$, then $\left(\frac{\alpha}{\beta}\right)^n = 1$, so $\frac{\alpha}{\beta} \in \mu_n \subset K$, so $\sigma\left(\frac{\alpha}{\beta}\right) = \frac{\alpha}{\beta}$ and so $\frac{\sigma(\alpha)}{\alpha} = \frac{\sigma(\beta)}{\beta}$.

This is bilinear: we have

$$\begin{aligned} \langle \sigma\tau, x \rangle &= \frac{\sigma(\tau \sqrt[n]{x})}{(\tau \sqrt[n]{x})} \frac{\tau \sqrt[n]{x}}{\sqrt[n]{x}} = \langle \sigma, x \rangle \langle \tau, x \rangle, \\ \langle \sigma, xy \rangle &= \frac{\sigma \sqrt[n]{xy}}{\sqrt[n]{xy}} = \frac{\sigma \sqrt[n]{x}}{\sqrt[n]{x}} \frac{\sigma \sqrt[n]{y}}{\sqrt[n]{y}} = \langle \sigma, x \rangle \langle \sigma, y \rangle. \end{aligned}$$

This is nondegenerate: Let $\sigma \in \operatorname{Gal}(L/K)$. If $\langle \sigma, x \rangle = 1 \ \forall x \in \Delta$, then $\sigma(\sqrt[n]{x}) = \sqrt[n]{x} \ \forall x \in \Delta$, so σ fixes L pointwise, i.e. $\sigma = 1$. Now let $x(K^\times)^n \in \Delta$. If $\langle \sigma, x \rangle = 1 \ \forall \sigma \in \operatorname{Gal}(L/K)$, then $\sigma(\sqrt[n]{x}) = \sqrt[n]{x} \ \forall \sigma \in \operatorname{Gal}(L/K)$, so $\sqrt[n]{x} \in K$, so $x \in (K^\times)^n$ and so $x(K^\times)^n \in \Delta$ is trivial.

We get injective group homomorphisms

(i) $\operatorname{Gal}(L/K) \hookrightarrow \operatorname{Hom}(\Delta, \mu_n)$,

(ii) $\Delta \hookrightarrow \operatorname{Hom}(\operatorname{Gal}(L/K), \mu_n)$.

From (i), $\operatorname{Gal}(L/K)$ is abelian and of exponent dividing n. Recall the following **Fact**: If G is a finite abelian group of exponent dividing n, then $\operatorname{Hom}(G, \mu_n) \cong G$ (non-canonically). Hence $|\operatorname{Gal}(L/K)| \overset{(i)}{\leq} |\Delta| \overset{(ii)}{\leq} |\operatorname{Gal}(L/K)|$, so (i) and (ii) are isomorphisms. □

Example 11.1. $\operatorname{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3$.

Reminder: we are assuming $\operatorname{char} K \nmid n$ and $\mu_n \subset K$.

26 Feb 2024, Lecture 17

Theorem 11.2. There is a bijection

$$\begin{aligned} \{\text{finite subgroups of } K^\times/(K^\times)^n\} &\leftrightarrow \{\text{finite abelian extensions } L/K \text{ of exponent dividing } n\} \\ \Delta &\mapsto K(\sqrt[n]{\Delta}) \\ ((L^\times)^n \cap K^\times)/(K^\times)^n &\mapsfrom L \end{aligned}$$

Proof. (i). Let $\Delta \subset K^\times/(K^\times)^n$ be a finite subgroup. Let $L = K(\sqrt[n]{\Delta})$ and

$\Delta' = ((L^\times)^n \cap K^\times)/(K^\times)^n$. We must show $\Delta = \Delta'$. Clearly $\Delta \subset \Delta'$. Also

$$\begin{aligned} L = K(\sqrt[n]{\Delta}) &\subset K(\sqrt[n]{\Delta'}) \subset L \\ \implies K(\sqrt[n]{\Delta}) &= K(\sqrt[n]{\Delta'}). \end{aligned}$$

Thus $|\Delta| = |\Delta'|$ by Lemma 11.1. Since $\Delta \subset \Delta'$, we get $\Delta = \Delta'$.

(ii). Let L/K be a finite abelian extension of exponent dividing n. Let $\Delta = ((L^\times)^n \cap K^\times)/(K^\times)^n$, then $K(\sqrt[n]{\Delta}) \subset L$ and we aim to prove that these are equal. Let $G = \mathrm{Gal}(L/K)$. The Kummer pairing gives an injection $\Delta \hookrightarrow \mathrm{Hom}(G, \mu_n)$, which we claim is surjective. Given the claim, we would have $[K(\sqrt[n]{\Delta}) : K] = |\Delta| = |G| = [L : K]$ by Lemma 11.1. Since $K(\sqrt[n]{\Delta}) \subset L$, $L = K(\sqrt[n]{\Delta})$ follows.

It remains to prove the surjectivity claim. For this, let $\chi : G \to \mu_n$ be a group homomorphism. Distinct automorphisms are linearly independent, so $\exists a \in L$ such that $y := \sum_{\tau \in G} \chi(\tau)^{-1}\tau(a) \neq 0$. Let $\sigma \in G$. Then

$$\begin{aligned} \sigma(y) &= \sum_{\tau \in G} \chi(\tau)^{-1}\sigma\tau(a) \\ &\overset{\tau \mapsto \sigma^{-1}\tau}{=} \sum_{\tau \in G} \chi(\sigma^{-1}\tau)^{-1}\tau(a) \\ &= \chi(\sigma) \sum_{\tau \in G} \chi(\tau)^{-1}\tau(a) \\ &= \chi(\sigma) y. \end{aligned}$$

Hence $\sigma(y^n) = y^n \ \forall \sigma \in G$, so $y^n \in K$. Let $x = y^n$, then $x \in (L^\times)^n \cap K^\times$, so $x(K^\times)^n \in \Delta$. Also by the calculation above, $\chi : \sigma \mapsto \frac{\sigma(y)}{y} = \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}}$, so the map $\Delta \hookrightarrow \mathrm{Hom}(G, \mu_n)$ sends $x \mapsto \chi$, which proves the claim. $\square$

Proposition 11.3. Let K be a number field and $\mu_n \subset K$. Let S be a finite set of primes of K. Then there are only finitely many extensions L/K such that

(i) L/K is finite and abelian of exponent dividing n.

(ii) L/K is unramified at all primes $\mathfrak{p} \notin S$.

Proof. Theorem 11.2 implies that this extension is of the form $L = K(\sqrt[n]{\Delta})$ for some finite subgroup $\Delta \subset K^\times/(K^\times)^n$. Let $\mathfrak{p}$ be a prime of K. We have $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$ for $\mathcal{P}_i$ distinct primes of L. If $x \in K^\times$ represents an element of Δ, then $nv_{\mathcal{P}_i}(\sqrt[n]{x}) = v_{\mathcal{P}_i}(x) = e_i v_{\mathfrak{p}}(x)$.

If $\mathfrak{p} \notin S$, then all $e_i = 1$, so $v_{\mathfrak{p}}(x) \equiv 0 \pmod n$. Hence $\Delta \subset K(S, n)$, where

$$K(S, n) = \{x \in K^\times/(K^\times)^n \mid v_{\mathfrak{p}}(x) \equiv 0 \pmod n \ \forall \mathfrak{p} \notin S\}.$$

We now complete the proof using the following lemma. □

Lemma 11.4. $K(S,n)$ is finite.

Proof. The map $K(S,n) \to (\mathbb{Z}/n\mathbb{Z})^{|S|}$ by $x \mapsto (v_\mathfrak{p}(x) \bmod n)_{\mathfrak{p}\in S}$ is a group homomorphism with kernel $K(\varnothing,n)$. Since $|S| < \infty$, it suffices to prove the lemma with $S = \varnothing$.

Now, if $x \in K^\times$ represents an element of $K(\varnothing,n)$, then $(x) = \mathfrak{a}^n$ for some fractional ideal $\mathfrak{a}$. There is an exact short sequence

$$\begin{aligned} 0 \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n \to K(\varnothing,n) &\to \mathrm{Cl}_K[n] \to 0 \\ x &\mapsto [\alpha]. \end{aligned}$$

Since $\mathrm{Cl}_K[n]$ is finite and $\mathcal{O}_K^\times$ is a finitely generated abelian group (by Dirichlet's unit theorem), we conclude that $K(\varnothing,n)$ is finite. □

12 Elliptic curves over number fields continued

12.1 The weak Mordell-Weil theorem

Lemma 12.1. Let E/K be an elliptic curve and L/K a finite Galois extension. Then the natural map $E(K)/nE(K) \to E(L)/nE(L)$ has finite kernel.

Proof. For each element in the kernel, we pick a coset representative $P \in E(K)$ and then $Q \in E(L)$ such that $nQ = P$. For any $\sigma \in \mathrm{Gal}(L/K)$, $n(\sigma(Q) - Q) = \sigma P - P = 0$, so $\sigma(Q) - Q \in E[n]$. Since $\mathrm{Gal}(L/K)$ and $E[n]$ are finite, there are only finitely many possibilities for the map $\mathrm{Gal}(L/K) \to E[n]$ given by $\sigma \mapsto \sigma(Q) - Q$. But if $P_1, P_2 \in E(K)$ with $P_i = nQ_i$ for $Q_i \in E(L)$ and $\sigma(Q_1) - Q_1 = \sigma(Q_2) - Q_2\ \forall \sigma \in \mathrm{Gal}(L/K)$, then $\sigma(Q_1 - Q_2) = Q_1 - Q_2\ \forall\sigma \in \mathrm{Gal}(L/K)$, so $Q_1 - Q_2 \in E(K)$ and so $P_1 - P_2 \in nE(K)$. We conclude that

$$\ker(E(K)/nE(K) \to E(L)/nE(L)) \hookrightarrow \mathrm{Maps}(\mathrm{Gal}(L/K), E[n])$$

and the set on the right is finite, which finishes the proof. □

28 Feb 2024, Lecture 18

Theorem 12.2 (Weak Mordell-Weil Theorem)**.** Let K be a number field, E/K an elliptic curve and $n \geq 2$ an integer. Then $E(K)/nE(K)$ is finite.

Proof. By Lemma 12.1, we may replace K by a finite Galois extension of K. Hence WLOG assume $\mu_n \subset K$ and $E[n] \subset E(K)$. Let

$$S = \{\mathfrak{p} \mid n\} \cup \{\text{primes of bad reduction for } E/K\}.$$

For each $P \in E(K)$, the extension $K([n]^{-1}P)/K$ is unramified outside S by Theorem 9.9. Since $\mathrm{Gal}(\overline{K}/K)$ acts on $[n]^{-1}P$, it follows that $K([n]^{-1}P)/K$ is a Galois extension.

Let $Q \in [n]^{-1}P$. Since $E[n] \subset E(K)$, we have $K(Q) = K([n]^{-1}P)$. Consider the map $\mathrm{Gal}(K(Q)/K) \hookrightarrow E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ by $\sigma \mapsto \sigma Q - Q$ (for $-$ being $\ominus$ here). This is a group homomorphism, as $\sigma\tau Q - Q = \sigma(\tau Q - Q) + \sigma Q - Q$. It is also injective, as $\sigma Q = Q \implies \sigma$ fixes $K(Q)$ pointwise, i.e. $\sigma = 1$. Hence $K(Q)/K$ is an abelian extension of exponent dividing n unramified outside S. So by Proposition 11.3, as we vary $P \in E(K)$, there are only finitely many possibilities for $K(Q)$. Let L be the composite of all such extensions of K. Then L/K is finite and Galois and $E(K)/nE(K) \to E(L)/nE(L)$ is the zero map, so by Lemma 12.1, $|E(K)/nE(K)| < \infty$. □

Remark. If $K = \mathbb{R}$,$K = \mathbb{C}$ or $[K : \mathbb{Q}_p] < \infty$, then $|E(K)/nE(K)| < \infty$, yet $E(K)$ is uncountable, so not finitely generated.

Fact. If K is a number field, then there exists a quadratic form (known as the **canonical height**) $\widehat{h} : E(K) \to \mathbb{R}_{\geq 0}$ with the property that for any $B \geq 0$, the set $\{P \in E(K) \mid \widehat{h}(P) \leq B\}$ is finite.

Theorem 12.3 (Mordell-Weil Theorem)**.** Let K be a number field and E/K an elliptic curve. Then $E(K)$ is a finitely generated abelian group.

Proof. Fix an integer $n \geq 2$. By Weak Mordell-Weil, $|E(K)/nE(K)| < \infty$. Pick coset representatives $P_1, \ldots, P_m$ and let

$$\Sigma = \{P \in E(K) \mid \widehat{h}(P) \leq \max_{1 \leq i \leq m} \widehat{h}(P_i)\}.$$

We claim that Σ generates $E(K)$. Indeed, if not, then there exists an element $P \in E(K) \setminus \{\text{subgroup generated by } \Sigma\}$ of minimal height (using our fact above). Then $P = P_i + nQ$ for some $1 \leq i \leq m$ and $Q \in E(K)$. Note that $Q \in E(K) \setminus \{\text{subgroup gen. by } \Sigma\}$ and the minimal choice of P implies

$$\begin{aligned} 4\hat{h}(P) &\leq 4\hat{h}(Q) \leq n^2\hat{h}(Q) = \hat{h}(nQ) = \hat{h}(P - P_i) \\ &\leq \hat{h}(P - P_i) + \hat{h}(P + P_i) = 2\hat{h}(P) + 2\hat{h}(P_i), \end{aligned}$$

(using the parallelogram law in the last step), so $\hat{h}(P) \leq \hat{h}(P_i)$ and so $P \in \Sigma$, a contradiction to the choice of P. But by our fact, Σ is finite, so we're done. □

13 Heights

For simplicity, take $K = \mathbb{Q}$. Write $P = (a_0 : a_1 : \ldots : a_n)$ for $P \in \mathbb{P}^n(\mathbb{Q})$, where we scale to have $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ and $\gcd(a_0, a_1, \ldots, a_n) = 1$.

Definition 13.1. We define the **height** of P as

$$H(P) = \max_{0 \le i \le n} |a_i| .$$

Lemma 13.1. Let $f_1, f_2 \in \mathbb{Q}[X_1, X_2]$ be coprime homogeneous polynomials of degree d. Let $F : \mathbb{P}^1 \to \mathbb{P}^1$ be given by $(x_1 : x_2) \mapsto (f_1(x_1, x_2), f_2(x_1, x_2))$. Then $\exists c_1, c_2 > 0$ such that

$$c_1 H(P)^d \le H(F(P)) \le c_2 H(P)^d \ \forall P \in \mathbb{P}^1(\mathbb{Q}).$$

Proof. WLOG assume $f_1, f_2 \in \mathbb{Z}[X_1, X_2]$. For the upper bound, write $P = (a : b)$ for $a, b \in \mathbb{Z}$ coprime, so

$$H(F(P)) \le \max(|f_1(a,b)|, |f_2(a,b)|) \le c_2 \max(|a|^d, |b|^d),$$

where $c_2 = \max_{i=1,2}$(sum of abs. values of coeffs. of f_i), so $H(F(P)) \le c_2 H(P)^d$.

For the lower bound, we claim $\exists (g_{ij})_{1 \le i,j \le 2} \in \mathbb{Z}[X_1, X_2]$, homogeneous of degree $d-1$ and $\kappa \in \mathbb{Z}_{>0}$ such that

$$\sum_{j=1}^{2} g_{ij} f_j = \kappa X_i^{2d-1}$$

for $i = 1, 2$. Indeed, running Euclid's algorithm on $f_1(X, 1)$ and $f_2(X, 1)$ gives $r, s \in \mathbb{Q}[X]$ of degree $< d$ such that $r(X) f_1(X, 1) + s(X) f_2(X, 1) = 1$. Homogenizing and clearing denominators gives the desired result for $i = 2$. The case for $i = 1$ is analogous. Write $P = (a_1 : a_2)$ for $a_1, a_2 \in \mathbb{Z}$ coprime. The expression above implies $\sum_{j=1}^{2} g_{ij}(a_1, a_2) f_j(a_1, a_2) = \kappa a_i^{2d-1}$ for $i = 1, 2$. Hence $\gcd(f_1(a_1, a_2), f_2(a_1, a_2))$ divides $\gcd(\kappa a_1^{2d-1}, \kappa a_2^{2d-1}) = \kappa$, but also

$$\left|\kappa a_i^{2d-1}\right| \le \underbrace{\max_{j=1,2} |f_j(a_1, a_2)|}_{\le \kappa H(F(P))} \underbrace{\sum_{j=1}^{2} |g_{ij}(a_1, a_2)|}_{\le \gamma_i H(P)^{d-1}},$$

where $\gamma_i = \sum_{j=1}^{2}$(sum of abs. values of coefficients of g_{ij}). This implies that

$$\begin{aligned} &\kappa |a_i|^{2d-1} \le \kappa H(F(P)) \gamma_i H(P)^{d-1} \\ \implies &H(P)^{2d-1} \le \max(\gamma_1, \gamma_2) H(F(P)) H(P)^{d-1} \\ \implies &\frac{1}{\max(\gamma_1, \gamma_2)} H(P)^d \le H(F(P)). \end{aligned}$$

Taking $c_2 = \frac{1}{\max(\gamma_1, \gamma_2)}$ finishes the proof. $\square$

Notation. For $x \in \mathbb{Q}$, write $H(x) = H((x:1)) = \max(|r|, |s|)$ for $x = \frac{r}{s}$ for $r, s \in \mathbb{Z}$ coprime. 01 Mar 2024, Lecture 19

Definition 13.2. Let $E/\mathbb{Q}$ be an elliptic curve given by $y^2 = x^3 + ax + b$. The **height** is defined as

$$\begin{aligned} H : E(\mathbb{Q}) &\to \mathbb{R}_{\geq 1} \\ P &\mapsto \begin{cases} H(x) & \text{if} P = (x, y). \\ 1 & \text{if} P = 0_E. \end{cases} \end{aligned}$$

We also define the **logarithmic height** $h : E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ by $P \mapsto \log H(P)$.

Lemma 13.2. Let E, E' be elliptic curves defined over $\mathbb{Q}$ and let $\phi : E \to E'$ be an isogeny defined over $\mathbb{Q}$. Then $\exists c > 0$ such that

$$|h(\phi(P)) - (\deg \phi)h(P)| < c \ \forall P \in E(\mathbb{Q}).$$

Importantly, note that c depends on E and E', but not on P.

Proof. Recall from Lemma 5.4 that we have a morphism ξ making our diagram commute with $\deg \phi = \deg \xi := d$. By Lemma 13.1, $\exists c_1, c_2 > 0$ such that $c_1 H(P)^d \leq H(\phi(P)) \leq c_2 H(P)^d \ \forall P \in E(\mathbb{Q})$. Taking logarithms gives

$$|h(\phi(P)) - dh(P)| \leq \max(\log c_2, -\log c_1) := c$$

as desired. □

Example 13.1. Take $\phi = [2] : E \to E$. Then $\exists c > 0$ such that $|h(2P) - 4h(P)| \leq c \ \forall P \in E(\mathbb{Q})$.

Definition 13.3. The **canonical height** is defined as

$$\widehat{h}(P) = \lim_{n \to \infty} \frac{1}{4^n} h(2^n P).$$

We need to check that this converges. Let $m \geq n$, then

$$\begin{aligned} \left| \frac{1}{4^m} h(2^m P) - \frac{1}{4^n} h(2^n P) \right| &\leq \sum_{r=n}^{m-1} \left| \frac{1}{4^{r+1}} h(2^{r+1} P) - \frac{1}{4^r} h(2^r P) \right| \\ = \sum_{r=n}^{m-1} \frac{1}{4^{r+1}} \left| h(2(2^r P)) - 4h(2^r P) \right| &< c \sum_{r=n}^{\infty} \frac{1}{4^{r+1}} = c \cdot \frac{1}{3 \cdot 4^n} \to 0 \end{aligned}$$

as $n \to \infty$. Hence the sequence is Cauchy, so converges, so $\widehat{h}(P)$ exists.

Lemma 13.3. $\left| h(P) - \widehat{h}(P) \right|$ is bounded for $P \in E(\mathbb{Q})$.

Proof. Put $n = 0$ in the above calculation to get $\left|\frac{1}{4^m}h(2^m P) - h(P)\right| \leq \frac{c}{3}$. Take the limit as $m \to \infty$ to conclude. □

Lemma 13.4. For any $B > 0$,

$$\#\{P \in E(\mathbb{Q}) \mid \widehat{h}(P) \leq B\} < \infty.$$

Proof. $\widehat{h}(P)$ is bounded $\implies$ $h(P)$ is bounded by Lemma 13.3. But there are only finitely many possibilities for x, and each of them gives ≤ 2 choices of y, so we're done. □

Lemma 13.5. Let $\phi : E \to E'$ be an isogeny over $\mathbb{Q}$. Then

$$\widehat{h}(\phi(P)) = (\deg\phi)\widehat{h}(P)\ \forall P \in E(\mathbb{Q}).$$

Proof. By Lemma 13.2, $\exists c > 0$ such that $|h(\phi(P)) - (\deg\phi)h(P)| < c\ \forall P \in E(\mathbb{Q})$. Replace P by $2^n P$, divide by 4^n and take the limit as $n \to \infty$ to conclude. □

Remarks.

(i) The case $\deg\phi = 1$ shows that $\widehat{h}$ (unlike h) is independent of the choice of Weierstrass equation for E.

(ii) Taking $\phi = [n] : E \to E$ shows $\widehat{h}(nP) = n^2\widehat{h}(P)\ \forall P \in E(\mathbb{Q})$.

Lemma 13.6. Let $E/\mathbb{Q}$ be an elliptic curve. Then $\exists c > 0$ such that

$$H(P+Q)H(P-Q) \leq cH(P)^2H(Q)^2$$

for all $P, Q \in E(\mathbb{Q})$ with $P, Q, P \pm Q \neq 0_E$.

Proof. Let E have Weierstrass equation $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$. Let $P, Q, P+Q, P-Q$ have x-coordinates x_1, x_2, x_3, x_4. By Lemma 5.8, there exist $W_0, W_1, W_2 \in \mathbb{Z}[x_1, x_2]$ of degree ≤ 2 in both x_1 and x_2 such that $(1 : x_3 + x_4 : x_3x_4) = (W_0 : W_1 : W_2)$ (and $W_0 = (x_1 - x_2)^2$). Write $x_i = \frac{r_i}{s_i}$ for $r_i, s_i \in \mathbb{Z}$ coprime. Then we get

$$(s_3s_4 : r_3s_4 + r_4s_3 : r_3r_4) = ((r_1s_2 - r_2s_1)^2 : \ldots).$$

Then

$$\begin{aligned} H(P+Q)H(P-Q) &= \max(|r_3|, |s_3|)\max(|r_4|, |s_4|) \\ &\leq 2\max(|s_3s_4|, |r_3s_4 + r_4s_3|, |r_3r_4|) \\ &\leq 2\max(\left|(r_1s_2 - r_2s_1)^2\right|, \ldots) \\ &\leq cH(P)^2H(Q)^2. \end{aligned}$$

where c depends on E, but not on P, Q.[3] □

Theorem 13.7. $\widehat{h} : E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ is a quadratic form.

Proof. By Lemma 13.6 and the fact that $|h(2P) - 4h(P)|$ is bounded, $\exists c \in \mathbb{R}$ such that

$$h(P+Q) + h(P-Q) \leq 2h(P) + 2h(Q) + c \;\forall P, Q \in E(\mathbb{Q}).$$

Replacing P, Q by $2^n P, 2^n Q$, dividing by 4^n and taking the limit as $n \to \infty$ gives

$$\widehat{h}(P+Q) + \widehat{h}(P-Q) \leq 2\widehat{h}(P) + 2\widehat{h}(Q).$$

Replacing P, Q by $P+Q, P-Q$ and using $\widehat{h}(2P) = 4\widehat{h}(P)$ gives the reverse inequality. Hence $\widehat{h}$ satisfies the parallelogram law, so it is a quadratic form. □

Remark. For K a number field and $P = (a_0 : a_1 : \ldots : a_n) \in \mathbb{P}^n(K)$, we define

$$H(P) = \prod_v \max_{0 \leq i \leq n} |a_i|_v$$

where the product is over all places v of K, and the absolute values are normalized such that $\prod_v |\lambda|_v = 1 \;\forall \lambda \in K^\times$. All results proved in this section then generalize from $\mathbb{Q}$ to K. Note further that the places are the finite places given by $|x|_{\mathfrak{p}} = c^{v_{\mathfrak{p}}(x)}$ for some $c < 1$ and the infinite places $|x|_\sigma = |\sigma(x)|^d$ for some $d > 0$ (and now we choose appropriate c, d to satisfy the product formula).

14 Dual isogenies and the Weil pairing

Let K be a perfect field and E/K an elliptic curve. 04 Mar 2024, Lecture 20

Proposition 14.1. Let $\Phi \subset E(\overline{K})$ be a finite $\mathrm{Gal}(\overline{K}/K)$-stable subgroup. Then there exists an elliptic curve E'/K and a separable isogeny $\phi : E \to E'$ defined over K with kernel Φ such that every isogeny $\psi : E \to E''$ with $\Phi \subset \ker(\psi)$ factors uniquely via ϕ as

$$\begin{tikzcd} E \arrow[rr, "\psi"] \arrow[dr, "\phi"'] & & E'' \\ & E' \arrow[ur, "\exists \text{ unique}"'] & \end{tikzcd}.$$

Proof. Omitted. (See e.g. Silverman, Chapter 3, Proposition 4.12). □

[3] I watched this lecture online and Fisher spent a few minutes explaining how the above inequalities follow, so it might be nontrivial to deduce this (shouldn't be too hard though).

Proposition 14.2. Let $\phi : E \to E'$ be an isogeny of degree n. Then there exists a unique isogeny $\widehat{\phi} : E' \to E$ (called the **dual isogeny**) such that $\widehat{\phi}\phi = [n]$.

Proof. If ϕ is separable, then $|\ker(\phi)| = n$, so $\ker(\phi) \subset E[n]$. Apply Proposition 14.1 with $\psi = [n]$ to get the result.

The case where ϕ is inseparable is omitted.

For uniqueness, if $\psi_1\phi = \psi_2\phi$, then $(\psi_1 - psi_2)\phi = 0$, so $\deg(\psi_1 - \psi_2)\deg(\phi) = 0$, but $\deg(\phi) \neq 0$, so $\psi_1 = \psi_2$. ☐

Remarks.

(i) Write $E_1 \sim E_2 \iff E_1, E_2$ are isogenous. Then $\sim$ is an equivalence relation.

(ii) $\deg\,[n] = n^2 \implies \begin{cases} \deg\,\phi = \deg\,\widehat{\phi}, \\ \widehat{[n]} = [n]. \end{cases}$

(iii) $\phi\widehat{\phi}\phi = \phi[n]_E = [n]_{E'}\phi$, so $\phi\widehat{\phi} = [n]_{E'}$. In particular, $\widehat{\widehat{\phi}} = \phi$.

(iv) If $E \xrightarrow{\psi} E' \xrightarrow{\phi} E''$, then $\widehat{\phi\psi} = \widehat{\psi}\widehat{\phi}$.

(v) If $\phi \in \mathrm{End}(E)$, then $\phi^2 - [\mathrm{tr}(\phi)]\phi + [\deg\,\phi] = 0$, so $\phi([\mathrm{tr}(\phi)] - \phi) = [\deg\,\phi]$, so $\widehat{\phi} = [\mathrm{tr}(\phi)] - \phi$, so $[\mathrm{tr}(\phi)] = \phi + \widehat{\phi}$.

Lemma 14.3. If $\phi, \psi \in \mathrm{Hom}(E, E')$, then $\widehat{\phi + \psi}\widehat{\phi} + \widehat{\psi}$.

Proof. (i) If $E = E'$, then this follows from $\mathrm{tr}(\phi + \psi) = \mathrm{tr}(\phi) + \mathrm{tr}(\psi)$.

(ii) In general, let $\alpha : E' \to E$ be any isogeny (e.g. $\alpha = \widehat{\phi}$) and we get

$$\begin{aligned} &\widehat{\alpha\phi + \alpha\psi} = \widehat{\alpha\phi} + \widehat{\alpha\psi} \\ \implies &\widehat{\phi + \psi}\widehat{\alpha} = (\widehat{\phi} + \widehat{\psi})\widehat{\alpha} \\ \implies &\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi} \end{aligned}$$

where the first line follows by (i).

☐

Remark. In Silverman's book, he proves Lemma 14.3 first and uses this to show that $\deg\ : \mathrm{Hom}(E, E') \to \mathbb{Z}$ is a quadratic form.

Definition 14.1. We define the following map: sum : $\mathrm{Div}(E) \to E$ by $\sum n_P P \mapsto \sum n_P P$ where on the left we have a formal sum and on the right we sum using the group law.

Recall that $E \xrightarrow{\sim} \mathrm{Pic}^0(E)$ by $P \mapsto [(P) - (0_E)]$. Hence $\mathrm{sum}(D) \mapsto [D]\ \forall D \in \mathrm{Div}^0(E)$. Thus we conclude:

Lemma 14.4. Let $D \in \mathrm{Div}(E)$. Then

$$D \sim 0 \iff \begin{cases} \deg D = 0, \\ \mathrm{sum}\ D = 0_E. \end{cases}$$

Now let $\phi : E \to E'$ be a isogeny of degree n with dual isogeny $\widehat{\phi} : E' \to E$. Assume that char $K \nmid n$ (so $\phi, \widehat{\phi}$ are separable). Write $E[\phi]$ for $\ker(\phi)$. We define the **Weil pairing**

$$e_\phi : E[\phi] \times E'[\widehat{\phi}] \to \mu_n$$

as follows: Let $T \in E'[\widehat{\phi}]$. Then $nT = 0$, so there exists $f \in \overline{K}(E')^\times$ such that $\mathrm{div}(f) = n(T) - n(0)$. Pick $T_0 \in E(\overline{K})$ with $\phi(T_0) = T$. Then $\phi^*(T) - \phi^*(0) = \sum_{P \in E[\phi]}(P + T_0) - \sum_{P \in E[\phi]}(P)$ has sum $nT_0 = \widehat{\phi}\phi T_0 = \widehat{\phi}(T) = 0$. So there exists $g \in \overline{K}(E)^\times$ such that $\mathrm{div}(g) = \phi^*(T) - \phi^*(0)$. Now $\mathrm{div}(\phi^* f) = \phi * (\mathrm{div}\ f) = n(\phi^*(T) - \phi^*(0)) = \mathrm{div}(g^n)$. Hence $\phi^* f = cg^n$ for some $c \in \overline{K}^\times$. Rescaling f allows us to wlog assume $c = 1$, i.e. $\phi^* f = g^n$.

If $S \in E[\phi]$, then $\tau_S^*(\mathrm{div}\ g) = \mathrm{div}\ g$, so $\mathrm{div}(\tau_S^* g) = \mathrm{div}\ g$ and so $\tau_S^* g = \zeta g$ for some $\times \in \overline{K}^\times$, i.e. $\zeta = \frac{g(X+S)}{g(X)}$ is independent of the choice of $X \in E(\overline{K})$. Now $\zeta^n = \frac{g(X+S)^n}{g(X)^n} = \frac{f(\phi(X+S))}{f(\phi(X))} = 1$ since $S \in E[\phi]$, so $\zeta \in \mu_n$. We hence define $e_\phi(S, T) = \frac{g(X+S)}{g(X)}$.

Proposition 14.5. e_ϕ is bilinear and nondegenerate.

Proof. (i) Linearity in the first argument:

$$e_\phi(S_1 + S_2, T) = \frac{g(X + S_1 + S_2)}{g(X + S_2)} \frac{g(X + S_2)}{g(X)} = e_\phi(S_1, T) e_\phi(S_2, T).$$

(ii) Linearity in the second argument: Let $T_1, T_2 \in E'[\widehat{\phi}]$ with $\mathrm{div}(f_i) n(T_i) - n(0)$ and $\phi^* f_i = g_i^n$ for $i = 1, 2$. There exists $h \in \overline{K}(E')^\times$ such that $\mathrm{div}(h) = (T_1) + (T_2) - (T_1 + T_2) - (0)$. We put $f = \frac{f_1 f_2}{h^n}$ and $g = \frac{g_1 g_2}{\phi^* h}$.

We can check $\mathrm{div}(f) = n(T_1 + T_2) - n(0)$ and $\phi^* f = \frac{\phi^* f_1 + \phi^* f_2}{(\phi^* h)^n} = \left(\frac{g_1 g_2}{\phi^* h}\right)^n = g^n$, so

$$\begin{aligned} e_\phi(S, T_1 + T_2) = \frac{g(X + S)}{g(X)} &= \frac{g_1(X + S)}{g_1(X)} \frac{g_2(X + S)}{g_2(X)} \frac{h(\phi(X_1))}{h(\phi(X + S))} \\ &= e_\phi(S, T_1) e_\phi(S, T_2) \end{aligned}$$

where the last term cancels since $S \in E[\phi]$.

(iii) e_ϕ is nondegenerate. Fix $T \in E'[\widehat{\phi}]$ and suppose $e_\phi(S, T) = 1\ \forall S \in E[\phi]$, so

$\tau_S^* g = g \ \forall S \in E[\phi]$. We get that $\overline{K}(E)/\phi^*\overline{K}(E')$ is a Galois extension with Galois group $E[\phi]$ (here $S \in E[\phi]$ acts via τ_S^*). Hence $\tau_S^* g = g \ \forall S \in E[\phi]$, so $g = \phi^* h$ for some $h \in \overline{K}(E')$, so $\phi^* f = g^n = (\phi^* h)^n = \phi^*(h^n)$, so $f = h^n$, whence $\operatorname{div}(h) = (T) - (0)$. This implies $T = 0$ (using, I think, the sum function). We've shown $E'[\widehat{\phi}] \hookrightarrow \operatorname{Hom}(E[\phi], \mu_n)$, which is actually an isomorphism as $\#E[\phi] = \#E'[\widehat{\phi}] = n$, so e_ϕ is nondegenerate.

□

Remarks. 06 Mar 2024, Lecture 21

(i) If E, E', ϕ are defined over K, then e_ϕ is Galois invariant, i.e. $e_\phi(\sigma(S), \sigma(T)) = \sigma(e_\phi(S,T)) \ \forall \sigma \in \operatorname{Gal}(\overline{K}/K), S \in E[\phi], T \in E'[\widehat{\phi}]$.

(ii) Taking $\phi = [n] : E \to E$ (so $\widehat{\phi} = [n]$) gives $e_n = E[n] \times E[n] \to \mu_{n^2}$, but in fact the image is contained in $\mu_n \subset \mu_{n^2}$, as $E[n] \times E[n]$ has exponent n.

Corollary 14.6. If $E[n] \subset E(K)$, then $\mu_n \subset K$.

Proof. Let $T \in E[n]$ have order n. Since e_n is nondegenerate, $\exists S \in E[n]$ such that $e_n(S,T)$ is a primitive n^{th} root of unity, say ζ_n. Then $\sigma(\zeta_n) = \sigma(e_n(S,T)) = e_n(\sigma(S), \sigma(T)) = e_n(S,T) = \zeta_n \ \forall \sigma \in \operatorname{Gal}(\overline{K}/K)$, so $\zeta_n \in K$. □

Example 14.1. There does not exist $E/\mathbb{Q}$ with $E(\mathbb{Q})_{\text{tors}} = (\mathbb{Z}/3\mathbb{Z})^2$, since $\zeta_3 \notin \mathbb{Q}$.

Remark. In fact, e_n is alternating, i.e. $e_n(T,T) = 1 \ \forall T \in E[n]$. This implies $e_n(S,T) = e_n(T,S)^{-1}$.

15 Galois cohomology

Let G be a group and let A be an abelian group that's a G-module, i.e. it's an abelian group equipped with a homomorphism $G \to \operatorname{Aut}(A)$.

Definition 15.1. We define the 0^{th} cohomology group as

$$H^0(G,A) = A^G = \{a \in A \mid \sigma(a) = a \ \forall \sigma \in G\}.$$

We define the collection of 1^{st} cochains as

$$C^1(G,A) = \{\text{maps } G \to A\}.$$

This contains the collection of 1^{st} cocycles

$$Z^1(G,A) = \{(a_\sigma)_{\sigma \in G} \mid a_{\sigma\tau} = \sigma(a_\tau) + a_\sigma \ \forall \sigma, \tau \in G\},$$

which contains the collection of 1^{st} coboundaries

$$B^1(G,A) = \{(\sigma(b) - b)_{\sigma \in G} \mid b \in A\}.$$

We set the 1^{st} group cohomology to be

$$H^1(G,A) = \frac{Z^1(G,A)}{B^1(G,A)} = \frac{\text{cocycles}}{\text{coboundaries}}.$$

Remark. If G acts trivially on A, then $H^1(G,A) = \mathrm{Hom}(G,A)$.

Theorem 15.1. A short exact sequence of G-modules

$$0 \to A \xrightarrow{\phi} B \xrightarrow{\psi} C \to 0$$

gives rise to a long exact sequence

$$0 \to A^G \xrightarrow{\phi} B^G \xrightarrow{\psi} C^G \xrightarrow{\delta} H^1(G,A) \xrightarrow{\phi^*} H^1(G,B) \xrightarrow{\psi^*} H^1(G,C).$$

Proof. Omitted. □

However, we give the definition of δ. Let $c \in C^G$. There exists some $b \in B$ with $\psi(b) = c$. Then $\psi(\sigma(b) - b) = \sigma\psi(b) - \psi(b) = \sigma c - c = 0$ $\forall \sigma \in G$, so $\sigma b - b = \phi(a_\sigma)$ for some $a_\sigma \in A$. We can check that $(a_\sigma)_{\sigma \in G} \in Z^1(G,A)$, so we define $\delta(c) =$ the class of $(a_\sigma)_{\sigma \in G}$ in $H^1(G,A)$.

Theorem 15.2. Let A be a G-module and $H \leq G$ a normal subgroup. Then there is an inflation-restriction exact sequence

$$0 \to H^1(G/H, A^H) \xrightarrow{\text{inf}} H^1(G,A) \xrightarrow{\text{res}} H^1(H,A).$$

Proof. Omitted. □

Let K be a perfect field. $\mathrm{Gal}(\overline{K}/K)$ is a topological group with its topology generated by the basis of open subgroups of the form $\mathrm{Gal}(\overline{K}/L)$ for L a finite extension of K. If $G = \mathrm{Gal}(\overline{K}/K)$, we modify the definition of $H^1(G,A)$ by insisting that

(1) The stabilizer of each $a \in A$ is an open subgroup of G.

(2) All cochains $G \to A$ are continuous, where A is given the discrete topology.

Then

$$H^1(\mathrm{Gal}(\overline{K}/K), A) = \varinjlim_{\substack{L/K \text{ finite} \\ L/K \text{ Galois}}} = H^1(\mathrm{Gal}(L/K), A^{\mathrm{Gal}(\overline{K}/L)}),$$

the direct limit with respect to inflation maps.

Theorem 15.3 (Hilbert's Theorem 90)**.** Let L/K be a finite Galois extension. Then $H^1(\mathrm{Gal}(L/K), L^\times) = 0$.

Proof. Let $G = \mathrm{Gal}(L/K)$ and let $(a_\sigma)_{\sigma\in G} \in Z^1(G, L^\times)$. Distinct automorphisms are linearly independent, so $\exists y$ such that

$$x := \sum_{\tau\in G} a_\tau^{-1}\tau(y) \neq 0.$$

Then, using the fact that $a_{\sigma\tau} = \sigma(a_\tau)a_\sigma$, so $\sigma(a_\tau)^{-1} = a_\sigma a_{\sigma\tau}^{-1}$, we get

$$\begin{aligned}
\sigma(x) &= \sum_{\tau\in G} \sigma(a_\tau^{-1})\sigma\tau(y) \\
&= a_\sigma \sum_{\tau\in G} a_{\sigma\tau}^{-1}\sigma\tau(y) \\
&= a_\sigma x \\
&\implies a_\sigma = \frac{\sigma(x)}{x} \\
&\implies (a_\sigma)_{\sigma\in G} \in B^1(G, L^\times).
\end{aligned}$$

Hence $H^1(G, L^\times) = 0$. □

Corollary 15.4. With the setup as before, $H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times) = 0$.

Application. Assume char $K \nmid n$. Then there is a short exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$0 \to \mu_n \to \overline{K}^\times \xrightarrow[x\mapsto x^n]{} \overline{K}^\times \to 0$$

giving a long exact sequence

$$K^\times \xrightarrow[x\mapsto x^n]{} K^\times \to H^1(\mathrm{Gal}(\overline{K}/K), \mu_n) \to H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times) = 0$$

by Hilbert's Theorem 90. Consequently, $H^1(\mathrm{Gal}(\overline{K}/K), \mu_n) \cong K^\times/(K^\times)^n$. If $\mu_n \subset K$, then

$$\mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(\overline{K}/K), \mu_n) \cong K^\times/(K^\times)^n.$$

Here the finite subgroups of the LHS are of the form $\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)$ for L/K a finite abelian extension of exponent dividing n. This gives another proof of Theorem 11.2.

08 Mar 2024, Lecture 22

Notation. We write $H^1(K,-)$ to mean $H^1(\mathrm{Gal}(\overline{K}/K),-)$.

Let $\phi : E \to E'$ be an isogeny of elliptic curves of K. We have a short exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$0 \to E[\phi] \to E \xrightarrow{\phi} E' \to 0,$$

and a long exact sequence

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

We get a short exact sequence

$$0 \to E'[K]/\phi E[K] \to H^1(K, E[\phi]) \to H^1(K,E)[\phi_*] \to 0.$$

Now take K a number field. For each place v of K, we fix an embedding $\overline{K} \subset \overline{K}_v$. Then $\mathrm{Gal}(\overline{K}_v/K_v) \subset \mathrm{Gal}(\overline{K}/K)$. Taking the product over all places gives another short exact sequence compatible with the one above as

$$\begin{tikzcd}
0 \arrow[r] & E'[K]/\phi E[K] \arrow[r] \arrow[d] & H^1(K,E[\phi]) \arrow[r] \arrow[d, "\mathrm{res}_v"] \arrow[dr] & H^1(K,E)[\phi_*] \arrow[r] \arrow[d, "\mathrm{res}_v"] & 0 \\
0 \arrow[r] & \prod_v E'[K_v]/\phi E[K_v] \arrow[r] & \prod_v H^1(K_v, E[\phi]) \arrow[r] & \prod_v H^1(K_v,E)[\phi_*] \arrow[r] & 0.
\end{tikzcd}$$

Definition 15.2. The **ϕ-Selmer group** is

$$\begin{aligned}
S^{(\phi)}(E/K) &= \ker(\searrow) \\
&= \ker\left(H^1(K,E[\phi]) \to \prod_v H^1(K_v,E)\right) \\
&= \{\alpha \in H^1(K,E[\phi]) \mid \mathrm{res}_v(\alpha) \in \mathrm{Im}(\delta_v) \forall v\}.
\end{aligned}$$

The **Tate-Shafarevich group** is

$$Ш(E/K) = \ker\left(H^1(K,E) \to \prod_v H^1(K_v,E)\right).$$

We get a short exact sequence

$$0 \to E'[K]/\phi E[K] \to S^{(\phi)}(E/K) \to Ш(E/K)[\phi_*] \to 0.$$

Taking $\phi = [n]$ gives

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

Rearranging the proof of weak Mordell-Weil (Theorem 12.2) gives

Theorem 15.5. $S^{(n)}(E/K)$ is finite.

Proof. For L/K a finite Galois extension, there is an exact sequence

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(\mathrm{Gal}(L/K), E(L)[n]) & \xrightarrow{\mathrm{inf}} & H^1(K, E[n]) & \xrightarrow{\mathrm{res}} & H^1(L, E[n]) \\ & & & & \cup & & \cup \\ & & & & S^{(n)}(E/K) & & S^{(n)}(E/L). \end{array}$$

Consequently, by extending our field we may assume $E[n] \subset E(K)$ and hence $\mu_n \subset K$. Hence $E[n] \cong \mu_n \times \mu_n$ as a $\mathrm{Gal}(\overline{K}/K)$-module, so

$$H^1(K, E[n]) \cong H^1(K, \mu_n) \times H^1(K, \mu_n) \cong K^\times/(K^\times)^n \times K^\times/(K^\times)^n.$$

Let $S = \{\text{primes of bad reduction for } E\} \cup \{v \mid n\infty\}$, which is a finite set of places.

Definition 15.3. The subgroup of $H^1(K, A)$ unramified outside S is

$$H^1(K, A; S) = \ker\left(H^1(K, A) \to \prod_{v \notin S} H^1(K_v^{\mathrm{nr}}, A)\right).$$

There is a commutative with exact rows

$$\begin{array}{ccccc} E(K_v) & \xrightarrow{\times n} & E(K_v) & \xrightarrow{\delta_v} & H^1(K_v, E[n]) \\ \cap & & \cap & & \downarrow{\scriptstyle \mathrm{res}} \\ E(K_v^{\mathrm{nr}}) & \xrightarrow{\times n} & E(K_v^{\mathrm{nr}}) & \longrightarrow & H^1(K_v^{\mathrm{nr}}, E[n]), \end{array}$$

where the first arrow on the second row is surjective $\forall v \notin S$ (Theorem 9.9). Hence

$$S^{(n)}(E/K) \subset H^1(K, E[n]; S) \cong H^1(K, \mu_n; S) \times H^1(K, \mu_n; S).$$

But

$$H^1(K, \mu_n; S) \cong \ker\left(K^\times/(K^\times)^n \to \prod_{v \notin S} (K_v^{\mathrm{nr}})^\times/((K_v^{\mathrm{nr}})^\times)^n\right) \subset K(S, n)$$

which is finite by Lemma 14.4. (For the last inclusion we have an optional exercise: we can check that the $\subset$ is actually a $=$ using $\{v \mid n\} \subset S$.) $\square$

Remark. $S^{(n)}(E/K)$ is finite and effectively computable. It is conjectured that $|Ш(E/K)| < \infty$. This would imply that $\mathrm{rank} E(K)$ is effectively computable.

16 Descent by cyclic isogeny

Let E, E' be elliptic curves over a number field K and let $\phi : E \to E'$ be an isogeny of degree n defined over K. Suppose $E'[\widehat{\phi}] \cong \mathbb{Z}/n\mathbb{Z}$, generated by $T \in E'(K)$. Then $E[\phi] \cong \mu_n$ as a $\mathrm{Gal}(\overline{K}/K)$-module via $S \mapsto e_\phi(S, T)$. This gives a short exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$0 \longrightarrow \mu_n \longrightarrow E \xrightarrow{\phi} E' \longrightarrow 0$$

and a long exact sequence

$$\begin{tikzcd}
E(K) \arrow[r] & E'(K) \arrow[r, "\delta"] \arrow[dr, "\alpha"'] & H^1(K, \mu_n) \arrow[r] \arrow[d, phantom, "\cong{,}\ H90"] & H^1(K, E) \arrow[r] & \dots \\
& & K^\times/(K^\times)^n. & &
\end{tikzcd}$$

Theorem 16.1. Let $f \in K(E')$ and $g \in K(E)$ with $\mathrm{div}(f) = n(T) - n(0)$ and $\phi^* f = g^n$. Then

$$\alpha(P) = f(P) \pmod{(K^\times)^n} \ \forall P \in E'(K) \setminus \{0, T\}.$$

Proof. Let $Q \in \phi^{-1}P$. Then $\delta(P) \in H^1(K, \mu_n)$ is represented by the cocycle $\sigma \mapsto \sigma Q - Q \in E[\phi] \cong \mu_n$ and

$$\begin{aligned}
e_\phi(\sigma Q - Q, T) &= \frac{g(\sigma Q - Q + X)}{g(X)} \\
&= \frac{g(\sigma Q)}{g(Q)} \\
&= \frac{\sigma(g(Q))}{g(Q)} \\
&= \frac{\sigma \sqrt[n]{f(P)}}{\sqrt[n]{f(P)}},
\end{aligned}$$

where the first equality holds for any $X \in E$ avoiding the zeros and poles of g, so we take $X = Q$ in the second equality, and for the last equality use $\phi^* f = g^n$, so $g(Q)^n = f(P)$. But $H^1(K, \mu_n) \cong K^\times/(K^\times)^n$ via $\left(\sigma \mapsto \frac{\sigma \sqrt[n]{x}}{\sqrt[n]{x}}\right) \leftarrow\!\shortmid x$, so $\alpha(P) \equiv f(P) \pmod{(K^\times)^n}$. $\square$

16.1 Descent by 2-isogeny

11 Mar 2024, Lecture 23

Consider $E : y^2 = x(x^2+ax+b)$ with $b(a^2-4b) \neq 0$ and $E' : y^2 = x(x^2+a'x+b')$ with $a' = -2a, b' = a^2 - 4b$. Recall we have a 2-isogeny $\phi : E \to E'$ via $(x, y) \mapsto \left(\left(\frac{y}{x}\right)^2, \frac{y(x^2-b)}{x^2}\right)$ with dual $\widehat{\phi} : E' \to E$ via $(x, y) \mapsto \left(\frac{1}{4}\left(\frac{y}{x}\right)^2, \frac{y(x^2-b')}{8x^2}\right)$.

We have $E[\phi] = \{0, T\}$ for $T = (0, 0) \in E(K)$ and $E'[\widehat{\phi}] = \{0, T'\}$ for $T' = (0, 0) \in E'(K)$.

Proposition 16.2. There is a group homomorphism

$$\begin{aligned} E'(K) &\to K^\times/(K^\times)^2 \\ (x, y) &\mapsto \begin{cases} x \bmod (K^\times)^2 & \text{if } x \neq 0 \\ b' \bmod (K^\times)^2 & \text{if } x = 0. \end{cases} \end{aligned}$$

with kernel $\phi(E(K))$.

Proof. Either apply Theorem 16.1 with $f = x \in K(E')$ and $g = \frac{y}{x} \in K(E)$, or we can prove this via direct calculation (see Ex. Sheet 4). □

This gives injective group homomorphisms

$$\begin{aligned} \alpha_E &= E(K)/\widehat{\phi}E'(K) \hookrightarrow K^\times/(K^\times)^2 \\ \alpha_{E'} &= E'(K)/\phi E(K) \hookrightarrow K^\times/(K^\times)^2. \end{aligned}$$

Lemma 16.3. We have

$$2^{\operatorname{rank} E(K)} = \frac{|\text{Im } \alpha_E|\,|\text{Im } \alpha_{E'}|}{4}.$$

Proof. If $A \xrightarrow{f} B \xrightarrow{g} C$ are homomorphisms of abelian groups, then there is an exact sequence

$$0 \to \ker(f) \to \ker(gf) \xrightarrow{f} \ker(g) \to \operatorname{coker}(f) \xrightarrow{g} \operatorname{coker}(gf) \to \operatorname{coker}(g) \to 0.$$

Since $\widehat{\phi}\phi = [2]_E$, we get an exact sequence

$$0 \to \underbrace{E(K)[\phi]}_{\cong \mathbb{Z}/2\mathbb{Z}} \to E(K)[2] \xrightarrow{\phi} \underbrace{E'(K)[\widehat{\phi}]}_{\cong \mathbb{Z}/2\mathbb{Z}} \to \underbrace{E'(K)/\phi E(K)}_{\text{Im } \alpha_{E'}} \xrightarrow{\widehat{\phi}} E(K)/2E(K) \to \underbrace{E(K)/\widehat{\phi}E'(K)}_{\text{Im } \alpha_E} \to 0.$$

Consequently, $\frac{|E(K)/2E(K)|}{|E(K)[2]|} \overset{(\dagger)}{=} \frac{|\text{Im } \alpha_E||\text{Im } \alpha_{E'}|}{4}$. By Mordell-Weil, write $E(K) \cong$

$\Delta \times \mathbb{Z}^r$ for Δ a finite group and $r = \mathrm{rank} E(K)$. We have

$$\begin{aligned} E(K)/2E(K) &\cong \Delta/2\Delta \times (\mathbb{Z}/2\mathbb{Z})^r \\ E(K)[2] &\cong \Delta[2] \end{aligned}$$

and $\Delta/2\Delta, \Delta[2]$ have the same order as Δ is finite. Hence $\frac{|E(K)/2E(K)|}{|E(K)[2]|} = 2^r$, which with (†) implies the claim. □

Lemma 16.4. If K is a number field and $a, b \in \mathcal{O}_K$, then $\mathrm{Im}(\alpha_E) \subset K(S, 2)$, where S is the set of primes dividing b.

Proof. We want to show that for $x, y \in K$, if $y^2 = x(x^2 + ax + b)$ and $v_\mathfrak{p}(b) = 0$, then $v_\mathfrak{p}(x)$ is even.

If $v_\mathfrak{p}(x) < 0$, then Lemma 9.1 implies $\begin{cases} v_\mathfrak{p}(x) = -2r \\ v_\mathfrak{p}(y) = -3r \end{cases}$ so we're done.

If $v_\mathfrak{p}(x) > 0$, then $v_\mathfrak{p}(x^2 + ax + b) > 0$, so $v_\mathfrak{p}(x) = v_\mathfrak{p}(y^2) = 2v_\mathfrak{p}(y)$ and we're done (and of course $v_\mathfrak{p}(x) = 0$ is clear). □

Lemma 16.5. If $b_1 b_2 = b$, then $b_1 (K^\times)^2 \in \mathrm{Im}(\alpha_E) \iff w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4$ is soluble for $u, v, w \in K$ not all zero.

Proof. If $b_1 \in (K^\times)^2$ or $b_2 \in (K^\times)^2$, then both conditions are satisfied. Hence now assume that $b_1, b_2 \notin (K^\times)^2$, i.e. they are not squares in K.

Now $b_1 (K^\times)^2 \in \mathrm{Im}(\alpha_E) \iff \exists (x, y) \in E(K)$ such that $x = b_1 t^2$ for some $t \in K^\times$, so $y^2 = b_1 t^2 ((b_1 t^2)^2 + a b_1 t^2 + b)$ and so $\left(\frac{y}{b_1 t}\right)^2 = b_1 t^4 + a t^2 + \underbrace{\frac{b}{b_1}}_{b_2}$, so our equation has a solution $(u, v, w) = \left(t, 1, \frac{y}{b_1 t}\right)$.

Conversely, if (u, v, w) is a solution to our equation, then $uv \neq 0$ and hence $\left(b_1 \left(\frac{u}{v}\right)^2, b_1 \frac{uw}{v^3}\right) \in E(K)$. □

Not take $K = \mathbb{Q}$.

Example 16.1. $E : y^2 = x^3 - x$, so $a = 0, b = -1$. Then $\mathrm{Im}(\alpha_E) = \langle -1 \rangle \subset \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$. We have $E' : y^2 = x^3 + 4x$ and $\mathrm{Im}(\alpha_{E'}) \subset \langle -1, 2 \rangle \subset \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$.

Applying the previous lemma (Lemma 16.5) to $b_1 = 1, b_1 = 2, b_1 = -2$ gives the equations $w^2 = -u^4 - 4v^4$, $w^2 = 2u^4 + 2v^4, w^2 = -2u^4 - 2v^4$. The first and third have no nontrivial solutions over $\mathbb{R}$, while for the second we can take $(u, v, w) = (1, 1, 2)$. Hence $\mathrm{Im}(\alpha_{E'}) = \langle 2 \rangle \subset \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$ and so $2^{\mathrm{rank} E(\mathbb{Q})} = \frac{2 \cdot 2}{4} = 1$, so $\mathrm{rank} E(\mathbb{Q}) = 0$ and hence 1 is not a congruent number.

Example 16.2. Take $E : y^2 = x^3 + px$ for p a prime that is 5 modulo 8. Taking $b_1 = -1$ gives $w^2 = -u^4 - pv^4$, which has no nontrivial solutions over $\mathbb{R}$, so $\mathrm{Im}(\alpha_E) = \langle p \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

Note that $\alpha_{E'}(T') = (-4p)(\mathbb{Q}^\times)^2 = (-p)(\mathbb{Q}^\times)^2$, so we check $b_1 = 2, b_1 = -2, b_1 = p$ which give $w^2 = 2u^4 - 2pv^4, w^2 = -2u^4 + 2pv^4, w^2 = pu^4 - 4v^4$.

Suppose the first of these is soluble and WLOG take $u, v, w \in \mathbb{Z}$ with $\gcd(u, v) = 1$. If $p \mid u$, then $p \mid w$, so $p \mid v$, contradiction, so $w^2 \equiv 2u^4 \not\equiv 0 \pmod p$, so $\left(\frac{2}{p}\right) = +1$, a contradiction as $p \equiv 5 \pmod 8$.

Likewise the second equation has no solutions since $\left(\frac{-2}{p}\right) = -1$. Hence $\mathrm{Im}(\alpha_{E'}) \subset \langle -1, p \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ and so

$$\mathrm{rank} E(\mathbb{Q}) = \begin{cases} 0 & \text{if } w^2 = pu^4 - 4v^4 \text{ has no nontrivial solutions over } \mathbb{Q}, \\ 1 & \text{if } w^2 = pu^4 - 4v^4 \text{ has a nontrivial solution over } \mathbb{Q}. \end{cases}$$