Elliptic Curves Notes

October 13, 2025

These notes are based on a course of the same title given by Professor Tom Fisher at Cambridge during Lent Term 2025. They have been written up by Alexander Shashkov. There are likely plenty of errors, which are my own.

Contents

Silverman and Cassels are good books, we mostly go with Silverman and if not probably from Cassels. Cassel's book is based on lectures that he gave in Part III many years ago.

1 Fermat's Method of Infinite Descent

1.1 Pythagorean triples

Let $\triangle$ be a right triangle with side lengths a, b, c, so $a^2 + b^2 = c^2$ and the area $A(\triangle) = ab/2$.

Definition 1.1. We say that $\triangle$ is *rational* if $a, b, c \in \mathbb{Q}$. We say that $\triangle$ is *primitive* if $a, b, c \in \mathbb{Z}$ and $(a, b) = 1$.

Lemma 1.2. *Every primitive triangle is of the form $(u^2 - v^2, 2uv, u^2 + v^2)$ for some $u > v > 0$.*

Proof. WLOG let a be odd, b even, c odd. Then

$$\left(\frac{b}{2}\right)^2 = \frac{c+a}{2} \cdot \frac{c-a}{2}. \tag{1.1}$$

Since $(a, c) = 1$, $((c + a)/2, (c - a)/2) = 1$, so $(c + a)/2 = u^2, (c - a)/2 = v^2$ are squares, and then $a = u^2 - v^2, c = u^2 + v^2$. □

Definition 1.3. $D \in \mathbb{Q}_{>0}$ is a *congruent number* if there exists a rational triangle $\triangle$ with $A(\triangle) = D$. Multiplying by a square gives another congruent number (equivalent to rescaling the sides by a factor), so we may assume that D is a squarefree positive integer.

Example 1.4. 5 and 6 are congruent numbers, 6 with $(3, 4, 5)$ and 6 with $(9/6, 40/6, 41/6)$.

Lemma 1.5. *$D \in \mathbb{Q}_{>0}$ is congruent if and only if $Dy^2 = x^3 - x$ has a solution for $x, y \in \mathbb{Q}$, $y \neq 0$.*

Proof. Lemma 1.2 shows that D is congruent if and only if $Dw^2 = uv(u^2 - v^2)$ for some $u, v, w \in \mathbb{Q}$, $u, v, w \neq 0$. We set $x = u/v$ and $y = w/v^2$. □

Fermat showed that 1 is not a congruent number, so the area of a right triangle is never a perfect square. This is equivalent to the following theorem.

Theorem 1.6. *There is no solution to $w^2 = uv(u^2 - v^2) = uv(u - v)(u + v)$ with $u, v, w \in \mathbb{Z}$, $w \neq 0$.*

Proof. We may assume that $(u, v) = 1$, $u, w > 0$. This is because if $v < 0$, then we can replace (u, v, w) by $(-v, u, w)$. If $v \geq 0$, then $w > v > 0$.

Now, if u, v are both odd, we can replace (u, v, w) by $(\frac{u+v}{2}, \frac{u-v}{2}, \frac{w}{2})$, and then u and v will have the opposite parity.

Thus since $(u, v) = 1$ and u and v have opposite parity, $u, v, (u+v), (u-v)$ are pairwise coprime positive integers, so they are all squares. Thus $u = a^2, v = b^2, u + v = c^2, u - v = d^2$ for some positive integers.

Since u and v have opposite parity, c, d are both odd, so $\frac{c^2+d^2}{2} = \frac{(u+v)+(u-v)}{2} = u = a^2$. Thus we have a new primitive triangle with side lengths $(\frac{c-d}{2}, \frac{c+d}{2}, a)$, which has area $\frac{c^2-d^2}{8} = v/4 = (b/2)^2$. Now, set $w_1 = b/2$. Then by the previous lemmas there exists u_1, v_1 such that $w_1^2 = u_1 v_1 (u_1 + v_1)(u_1 - v_1)$, so w_1 is a new solution to our equation. But we have that $4w_1^2 = b^2 = v|w^2$, so $w_1 \leq w/2$. But this is impossible, since w_1 is a positive integer, so iterating gives a decreasing infinite sequence of positive integers. □

1.2 A variant for polynomials

Let K be a field with $\operatorname{char} K \neq 2$, and let $\overline{K}$ be the algebraic closure.

Lemma 1.7. *Let $u, v \in K[t]$ be coprime. If $\alpha u + \beta v$ is a square for 4 distinct $(\alpha_i, \beta_i) \in \mathbb{P}^1$, then $u, v \in K$.*

Proof. WLOG we may assume $K = \overline{K}$ as if the result holds over $\overline{K}$ it will hold over K.

Changing coordinates on $\mathbb{P}^1$ using Möbious transformations, we may assume that the (α_i, β_i)s are $(1,0), (0,1), (1,-1), (1,\lambda)$ for some $\lambda \in K \backslash \{0,1\}$. Then $u = a^2, v = b^2$, $u - v = (a+b)(a-b)$, $u - \lambda v = (a + \mu b)(a - \mu b)$ where $\mu = \sqrt{\lambda}$. Then $a+b, a-b, a+\mu b, a-\mu b$ are all coprime, and since they are all squares, this yields a new solution. But since this new solution has

$$\max(\deg a, \deg b) \leq \frac{1}{2} \max(\deg u, \deg v), \tag{1.2}$$

and if $\max(\deg u, \deg v) > 0$, then $\max(\deg a, \deg b) > 0$, we have infinite descent unless $u, v \in K$. □

Definition 1.8. An *elliptic curve* E/K is the projective closure of the plane affine curve $y^2 = f(x)$ where $f \in K[x]$ is a monic cubic separable polynomial. $y^2 = f(x)$ is known as the Weierstrass equation.

For L/K any field extension, we have that

$$E(L) = \{(x, y) \in L^2 | y^2 = f(x)\} \cup \{0\}, \tag{1.3}$$

where $\{0\}$ is the point at infinity.

$E(L)$ is naturally an abelian group. In this course we study $E(K)$ for K a finite field, local field, or number field.

Lemma 1.5 and Theorem 1.6 show that if E is the elliptic curve given by $y^2 = x^3 - x^2$, then $E(\mathbb{Q}) = \{0, (0,0), (\pm 1, 0)\}$.

Corollary 1.9. *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 $\lambda \notin \{0,1\}$. Suppose $(x, y) \in E(K(t))$.

We can write $x = u/v$ with $u, v \in K[t]$ coprime. Then $w^2 = uv(u-v)(u-\lambda v)$ for some $w \in K[t]$. Since $K[t]$ is a UFD, $u, v(u-v), (u-\lambda v)$ are all squares. Then by Lemma 1.7, $u, v \in K$ so $x \in K$, so $y \in K$. □

2 Some remarks on plane curves

In this course, curves are always irreducible. For this section we work over $K = \overline{K}$.

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

1. The map $\mathbb{A}^1 \to \mathbb{A}^2$ given by $t \to (\phi(t), \psi(t))$ is injective on $\mathbb{A}^1$ except for only finitely many points.

2. $f(\phi(t), \psi(t)) = 0$.

Example 2.2. 1. Any nonsingular plane conic is rational. Consider the conic $C : x^2 + y^2 = 1$. Let $y = t(x + 1)$ be the line with slope t through $(-1, 0)$. The second intersection point (x_0, y_0) will satisfy $x_0^2 + t^2(x_0 + 1)^2 = 1$, which has solution $x_0 = (1 - t^2)/(1 + t^2)$, so

$$(x_0, y_0) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right). \tag{2.1}$$

This gives a rational parametrization for C.

2. Any singular plane cubic is rational. Let P be the singular point, then the line through P with slope t has only 1 more point of intersection, the coordinates of this point in t gives a rational parametrization.

3. Corollary 1.9 shows that elliptic curves are not rational.

Remark 2.3. 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 as a 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 2.4. *Let C be a smooth projective curve over $K = \overline{K}$. Then*

1. *C is rational if and only if $g(C) = 0$.*

2. *C is an elliptic curve if and only if $g(C) = 1$.*

Proof. The proof of 1. is omitted. If C is an elliptic curve, we can check that C is a smooth plane curve, and then use the genus formula in the previous remark. □

2.1 Orders of vanishing

If C is an algebraic curve with function field $K(C)$, and $P(C)$ is a smooth point, we write $\mathrm{ord}_P(f)$ to be the order of vanishing of $f \in K(C)^\times$ at P.

Formally this means the valuation of f, when considered as an element of the fraction field of the stalk at P, which is a DVR.

Definition 2.5. $t \in K(C)^\times$ is a uniformizer at P if $\mathrm{ord}_P(t) = 1$.

Example 2.6. Let $C = \{g(x, y) = 0\} \subset \mathbb{A}^2$ for some $g \in K[x, y]$ irreducible. Then $K(C) = \mathrm{Frac}(K[x, y]/(g))$. We can write $g = g_0 + g_1 + \cdots$ as a sum of homogeneous polynomials. Suppose that $P = (0, 0) \in C$, so that $g_0 = 0$ and $g_1 = \alpha x + \beta y$ with α, β both not zero. Then any $\gamma x + \delta y$ is a uniformizer, as long as $\alpha\delta - \beta\gamma \neq 0$

Example 2.7. Let $C^0 = \{y^2 = x(x - 1)(x - \lambda)\} \subset \mathbb{A}^2$, with $\lambda \notin \{0, 1\}$. We homogenize to get the projective variety $\{Y^2Z = X(X - Z)(X - \lambda Z)\} \subset \mathbb{P}^2$. $P = (0, 1, 0)$ is the unique point at infinity. We want to compute $\mathrm{ord}_P(x)$ and $\mathrm{ord}_P(y)$. We look at the affine piece $Y \neq 0$, and set $w = Z/Y$ and $t = X/Y$. We then have that

$$w = t(t - w)(t - \lambda w) \tag{2.2}$$

and P is $(t, w) = (0, 0)$. This is a smooth point, and $\mathrm{ord}_p(t) = \mathrm{ord}_p(t - w) = \mathrm{ord}_p(t - \lambda w) = 1$ by the previous example. So then $\mathrm{ord}_p(w) = 3$, and $\mathrm{ord}_p(x) = \mathrm{ord}_p(t/w) = 1 - 3 = -2$ and $\mathrm{ord}_p(y) = \mathrm{ord}_p(1/w) = -3$.

2.2 Riemann-Roch spaces

Let C be a smooth projective curve over $K = \overline{K}$.

Definition 2.8. A *divisor* D is a formal sum of points on C, $D = \sum_{P \in C} n_P P$ where $n_P \in \mathbb{Z}$, and $n_P = 0$ for all but finitely many $P \in C$.

The *degree* of a divisor is $\deg D = \sum n_P$

D is *effective*, written as $D \geq 0$, if $n_P \geq 0$ for all P. We write $D_1 \geq D_2$ if $D_1 - D_2 \geq 0$.

If $f \in K(C)^\times$, write $\operatorname{div}(f) = \sum_{P \in C} \operatorname{ord}_P(f) P$.

The *Riemann-Roch* space of $D \in \operatorname{Div}(C)$ is

$$\mathcal{L}(D) = \{f \in K(C)^\times \mid \operatorname{div}(f) + D \geq 0\} \cup \{0\} \tag{2.3}$$

This is the k-vector space of rational functions on C with poles and zeros prescribed by D.

The next theorem is a specialized version of Riemann-Roch for genus 1 curves.

Theorem 2.9. *Let C be a smooth projective curve of genus 1 and let $D \in \operatorname{Div}(C)$. Then*

$$\dim \mathcal{L}(D) = \begin{cases} \deg D & \deg D > 0 \\ \in \{0, 1\} & \deg D = 0 \\ 0 & \deg D < 0. \end{cases} \tag{2.4}$$

Example 2.10. In Example 2.7, we have

$$\begin{aligned} \mathcal{L}(2P) &= \langle 1, x \rangle \\ \mathcal{L}(3P) &= \langle 1, x, y \rangle \end{aligned} \tag{2.5}$$

This follows from checking that the generators are in the Riemann-Roch space, are linearly independent, and comparing dimensions on both sides.

Proposition 2.11. *Let $C \subset \mathbb{P}^2$ be a smooth plane cubic and $P \in C$ a point of inflection. Then we may change coordinates so that C is defined by $Y^2Z = X(X - Z)(X - \lambda Z)$ for some $\lambda \neq 0, 1$ and so that $P = (0 : 1 : 0)$ in the new coordinate system.*

Proof. We change coordinates and send $P \to (0 : 1 : 0)$ and so that the tangent line of C at P is $T_P(C) = \{z = 0\}$. Then C is defined by some cubic $F(X, Y, Z) = 0$. Since $P \in C$ is a point of inflection, we have that $F(P) = 0$, and on the tangent line $z = 0$ we further have that the order of vanishing is 2, and since P is further a point of reflection, we have that the order of vanishing is 3. Thus it follows that $F(t, 1, 0) = ct^3$ (see also the remark below).

Thus F has no terms of the form X^2Y, XY^2, Y^3. So F consists of terms of the form $\{Y^2Z, XYZ, YZ^2, X^3, XZ^2, XZ^2, Z$ We need the coefficient of Y^2Z to be nonzero otherwise P will be a singular point (the Jacobian will vanish). We need the coefficient of X^3 to be nonzero otherwise $Z|F$, which will mean F is not irreducible. We can rescale X, Y, Z and F such that C is given by

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^6 + a_6Z^3. \tag{2.6}$$

Substituting $Y - a_1X/2 - a_3Z/2$ into Y, we may assume that $a_1 = a_3 = 0$. So $Y^2Z = Z^3 f(X/Z)$ with f monic, and since C is smooth the roots of f will be distinct. So then we can change coordinates again so that the roots are $0, 1, \lambda$. We then have C in the desired form, which is sometimes called Legendre form. □

Remark 2.12. The points of inflection of a smooth curve $C = \{F(X_1, X_2, X_3) = 0\} \subset \mathbb{P}^2$ are given by those points where $F = 0$ and where the Hessian matrix vanishes:

$$\det \left(\frac{\partial^2 F}{\partial x_i \partial x_j} \right)_{ij} = 0. \tag{2.7}$$

2.3 Degree of a morphism

Let $\phi : C_1 \to C_2$ be a non-constant morphism of smooth projective curves. Then ϕ induces a map $\phi^* : K(C_2) \to K(C_1)$ sending $f \to f \circ \phi$. Thus $K(C_1)$ is a field extension of $\phi^* K(C_2)$.

Definition 2.13. The *degree* of ϕ is $\deg \phi = [K(C_1) : \phi^* K(C_2)]$.

ϕ is *separable* if $K(C_1)/\phi^* K(C_2)$ is separable.

Suppose $P \in C_1$, $Q \in C_2$, and $\phi : P \to Q$, and let $t \in K(C_2)$ be a uniformizer at Q, so $\mathrm{ord}_Q(t) = 1$ and t is a uniformizer in the DVR $K(C_2)_Q$.

Definition 2.14. The *ramification index* of ϕ at P is $e_\phi(P) = \mathrm{ord}_P(\phi^* t)$. This will always be ≥ 1, and is independent of the choice of t.

Theorem 2.15. *Let $\phi : C_1 \to C_2$ be a nonconstant morphism of smooth projective curves. Then for all $Q \in C_2$, we have*

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi. \tag{2.8}$$

Moreover if ϕ is separable, then $e_\phi(P) = 1$ for all but finitely may $P \in C_1$. This is equivalent to saying that if L/K is a separable extension of fields, then only finitely many primes ramify. In particular:

1. *ϕ is surjective on $\overline{K}$-points.*
2. *$\#\phi^{-1}(Q) \leq \deg \phi$.*
3. *If ϕ is separable, then $\#\phi^{-1}(Q) = \deg \phi$ for all but finitely many Q.*

Remark 2.16. Let C be an algebraic curve. A rational map is given $C \to \mathbb{P}^n$, $P \to (f_0(P) : f_1(P) : \cdots : f_n(P))$ where $f_0, \ldots, f_n \in K(C)$ are not all zero. In particular, if for some $P \in C$ we have $f_i(P) = 0$ for all i, we can multiply by some g_P such that $(f_i \cdot g_P)(P) \neq 0$ to define the rational map at C. We do the same procedure if f_i has a pole at P.

If C is smooth, then ϕ is a morphism.

3 Weierstrass equations

Throughout this section, we will assume that K is a perfect field.

Definition 3.1. An *elliptic curve* E/K is a smooth projective curve of genus 1, defined over K, with a specified K-valued point $0_E \in E(K)$.

Example 3.2. The last part of the definition ensures that E/K has a point at all. For instance, $\{X^3 + pY^3 + p^2 Z^3 = 0\} \subset \mathbb{P}^2$ is not an elliptic curve over $\mathbb{Q}$ because it has no $\mathbb{Q}$-rational points.

Theorem 3.3. *Every elliptic curve E/K is isomorphic over K to a curve in Weierstrass form via an isomorphism taking $0_E \to (0,1,0)$.*

Remark 3.4. Proposition 2.11 treated the case where E is a smooth plane cubic and 0_E is a point of inflection.

Remark 3.5. If $D \in Div(E)$ is defined over K (so it is fixed by the natural action of $\mathrm{Gal}(\overline{K}/K)$, then $\mathcal{L}(D)$ has a basis consisting of functions in $K(E)$ (as opposed to the general case where the basis is functions in $\overline{K}(E)$).

Theorem 3.3. Let E/K be an elliptic curve, so a smooth projective curve of genus 1. By Theorem 2.9, we have that

$$\mathcal{L}(2(0_E)) \subseteq \mathcal{L}(3(0_E)) \tag{3.1}$$

with bases $\{1, x\}$, $\{1, x, y\}$, where $x, y \in K(E)$ are some rational functions. We have that $\mathrm{ord}_{0_E}(x) = -2$ and $\mathrm{ord}_{0_E}(y) = -3$ because the dimension of $\mathcal{L}(1(0_E))$ is 1, so it is spanned by constant functions.

Now, $\mathcal{L}(6(0_E))$ is a 6-dimensional vector space, and contains the 7 elements $\{1, x, y, x^2, xy, x^3, y^2\}$. So these 7 elements are not linearly independent, so we can find a relation between them over K. Furthermore, since the functions x^3 and y^2 have order of vanishing 6, the relation necessarily contains these two elements. Thus after rescaling x, y, we get that

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.2}$$

for some $a_i \in K$. Let E' be the projective curve defined by this equation (the projective closure of the affine curve defined by this equation). There is a morphism

$$\begin{aligned} \phi : E &\to E' \subset \mathbb{P}^2 \\ P &\to (x(P), y(P), 1) \end{aligned} \tag{3.3}$$

Further, since $\mathrm{ord}_{0_E}(x) = -2$ and $\mathrm{ord}_{0_E}(y) = -3$, we have that $0_E \to ((x/y)(0_E), 1, (1/y)(0_E)) = (0,1,0)$. We also have that $\phi^* K(E') = K(x,y)$. We want to show that $K(x,y) = K(E)$, as then we will have $E \cong E'$ as curves.

Now, we have a map $x : E \to \mathbb{P}^1$, which induces a field extension $K(E)/x^*K(\mathbb{P}^1) = K(E)/x^*K(T) = K(E)/K(x)$. Now, since x has a pole of order -2 at 0_E. Thus we have that

$$\begin{aligned} \deg x &= \sum_{P \in x^{-1}(\infty)} e_x(P) \\ &= e_x(0_E) \\ &= \mathrm{ord}_{0_E}(x^*(1/t)) \\ &= \mathrm{ord}_{0_E}(1/x) \\ &= 2 \end{aligned} \tag{3.4}$$

so $[K(E) : K(x)] = 2$. Similarly, $[K(E) : K(y)] = 3$. Now, since $K(x), K(y) \subseteq K(x,y) \subseteq K(E)$ and $(2,3) = 1$, we have that $K(x,y) = K(E)$. Thus $K(E) = K(x,y) = \phi^* K(E')$, so $\deg \phi = 1$, so ϕ is birational (bijective and rational).

Now, rational maps are morphisms if they are between smooth curves. If E' is singular, then E, E' are rational, which is not the case as they are elliptic curves. So E' is smooth, so ϕ^{-1} is a morphism, and thus ϕ is an isomorphism. $\square$

Proposition 3.6. *Let E, E' be elliptic curves over K in Weierstrass form. Then $E \cong E'$ (an isomorphism of curves sending $O_E \to O_{E'}$ if and only if the equations are related by a change of variables*

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t, \quad u, r, s, t \in K, u \neq 0. \tag{3.5}$$

Proof. We examine the Riemann-Roch spaces in the previous proof. We have that $\langle 1, x\rangle = \langle 1, x'\rangle$, so $x = \lambda x' + r$. Likewise, $y = \mu y' + \sigma x' + t$. We did some rescaling to get Weierstrass form. This forces $\lambda^3 = \mu^2$, so $\lambda = u^2, \mu = u^3$, and we can put $s = \sigma/u^2$. □

A Weierstrass equation defines an elliptic curve if and only if it defines a smooth curves, as we already have from the equation that the curve is of genus 1 and has the point at infinity. E is smooth if and only if $\Delta(a_1, \ldots, a_6) \neq 0$, where Δ is a certain polynomial. If $\operatorname{char} K \neq 2, 3$, we may reduce to the case $y^2 = x^3 + ax + b$, and then we have $\Delta = -16(4a^3 + 27b^2)$.

Corollary 3.7. *Assume* $\operatorname{char} K \neq 2, 3$. *Then given elliptic curves*

$$\begin{aligned} E &: y^2 = x^3 + ax + b \\ E' &: y^2 = x^3 + a'x + b' \end{aligned} \tag{3.6}$$

we have that $E \cong E'$ over K if and only if $a' = u^4a$ and $b' = u^6b$ with $u \in K^\times$

Proof. Look at the previous proposition, and see that we need $r = s = t = 0$ so that no xy, y, x^2 terms appear in our equation. □

Definition 3.8. The j-invariant of an elliptic curve $E : y^2 = x^3 + ax + b$ is

$$j(E) = \frac{1728(4a^3)}{4a^3 + 27b^2}. \tag{3.7}$$

The weird scaling factors are due to the j-invariant's connection with modular forms.

Corollary 3.9. *$E \cong E' \implies j(E) = j(E')$ and the converse holds if $K = \overline{K}$.*

Proof. Follows from the previous corollary. □

4 The group law

Let $E \subset \mathbb{P}^2$ be a smooth plane cubic with a point $0_E \in E(K)$. E meets any line in 3 points (counting multiplicities). The chord and tangent process is not worth texing.

Let's prove associativity though.

Definition 4.1. Let $D_1, D_2 \in \operatorname{Div}(E)$. D_1 and D_2 are *linearly equivalent* if $\exists f \in \overline{K}(E)^*$ such that $(f) = D_1 - D_2$ and we write $D_1 \sim D_2$ and $[D_1]$ for the equivalence class.

Definition 4.2. $\operatorname{Pic}(E) = \operatorname{Div}(E)/\sim$, and $\operatorname{Pic}^0(E) = \operatorname{Div}^0(E)/\sim$. Note that (f) always has degree zero, since f is the ratio of polynomials of the same degree.

Proposition 4.3. *Let $\psi : E \to \operatorname{Pic}^0(E)$ be the map $P \to [(P) - (0_E)]$. Then $\psi(P + Q) = \psi(P) + \psi(Q)$ and ψ is a bijection.*

In particular this shows that E is a group.

Proof. Let $\ell = 0$, $m = 0$ be lines in projective space (linear forms), such that ℓ passes through E as P, S, Q and m passes through E at $0_E, S, P+Q$. Then ℓ/m is a rational function on E. We have that $(\ell/m) = (P) + (S) + (Q) - (0_E) - (S) - (P+Q) = (P) + (Q) - (0_E) - (P+Q)$. Thus $(P) + (Q) \sim (P+Q) - (0_E)$ so $\psi(P) + \psi(Q) = \psi(P+Q)$.

To show ψ is injective, suppose that $\psi(P) = \psi(Q)$, for some $P \neq Q$. Then there exists $f \in \overline{K}(E)^*$ such that $(f) = (P) - (Q)$. So $f : E \to \mathbb{P}^1$ has degree 1 (there is only 1 zero), so $E \cong \mathbb{P}^1$, a contradiction. Thus ψ is injective.

To show surjectivity, let $[D] \in \mathrm{Pic}^0(E)$. Then $D + (0_E)$ has degree 1, so by Riemann-Roch we have that $\dim \mathcal{L}(D + (0_E)) = 1$, so there exists $f \in \overline{K}(E)^*$ such that $(f) + D + (0_E) \geq 0$. But since (f) has degree 0, this divisor has degree 1, so it equals (P) for some point P. So $D \sim (P) - (0_E)$ and $\psi(P) = [D]$. □

4.1 Formulae for E in Weierstrass form

We can write out formulae for $P + Q, -P$ using the chord and tangent process. In particular, if $P = (x, y)$ and $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ we have that

$$-P = (x, -(a_1x + a_3) - y) \tag{4.1}$$

The rest is bash, and we get linear equations for $P + Q$.

Corollary 4.4. *$E(K)$ is an abelian group for any field K.*

Proof. By the formulas for $-P$ and $P + Q$ and the fact that $0_E \in E(K)$, we have that $E(K)$ is a subgroup of $E = E(\overline{K})$. □

Theorem 4.5. *Elliptic curves are group varieties, so that multiplication and inversion are morphisms of varieties.*

Proof. We just showed that these are rational maps of varieties. But $E \times E$ is a surface, not a curve, so we still need to show that the map $E \times E \to E$ given by addition of points is smooth.

We have that $+ : E \times E \to E$ is regular on

$$U = \{(P, Q) \in E \times E \mid P, Q, P + Q, P - Q \neq 0_E\} \tag{4.2}$$

For $P \in E$, let $\tau_P : E \to E$ be the translation morphism $Q \to P + Q$. Taking $A, B \in E$, we factor $+$ as

$$E \times E \xrightarrow{\tau_{-A} \times \tau_{-B}} E \times E \xrightarrow{\quad + \quad} E \xrightarrow{\tau_{A+B}} E$$

So $+$ is regular on all $\{\tau_A \times \tau_B(U)\}_{A,B \in E}$, which cover $E \times E$ so $+$ is regular on $E \times E$, so $+$ is a morphism. □

4.2 Statement of results

We will prove some things in this course.

4.3 Torsion

Definition 4.6. The n-multiplication operator if $[n] : E \to E$ sending $P \to nP = P + \cdots + P$. We also have $[-n]P = -[n]P$.

Definition 4.7. The n-torsion subgroup of E is $E[n] = \ker([n] : E \to E)$. If $K = \mathbb{C}$, then $E(\mathbb{C}) = \mathbb{C}/\Lambda$ and

$$E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2 \tag{4.3}$$

and $[n]$ has degree n^2. We'll show the second fact holds for any K, and the first fact holds if $\operatorname{char} K \nmid n$.

Lemma 4.8. *Assume* $\operatorname{char} K \neq 2$. *If* $E : y^2 = f(x) = (x - e_1)(x - e_2)(x - e_3)$, $e_1, e_2, e_3 \in \overline{K}$, *then* $E[2] = \{0_E, (e_1, 0), (e_2, 0), (e_3, 0)\} \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Proof. If $(x, y) = P \in E[2]$, then $P = -P$, so we must have $y = 0$. □

5 Isogenies

Let E_1, E_2 be elliptic curves.

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

We say that E_1, E_2 are *isogenous*.

Note that ϕ being a nonconstant morphism implies that ϕ is surjective on $\overline{K}$ points.

Definition 5.2. Let $\operatorname{Hom}(E_1, E_2) = \{\text{isogenies } E_1 \to E_2\} \cup \{0\}$ be the set of homomorphisms from $E_1 \to E_2$.

Then $\phi \in \operatorname{Hom}(E_1, E_2)$ is a group homomorphism, and $\operatorname{Hom}(E_1, E_2)$ is an abelian group under $(\phi + \psi)(P) = \phi(P) + \psi(P)$. In particular, we have that $\phi + \psi$ is the composition of $E \to E \times E \to E$ sending $P \to (\phi(P), \psi(P)) \to \phi(P) + \psi(P)$.

If $\phi : E_1 \to E_2$ and $\psi : E_2 \to E_3$ are isogenies then $\psi \circ \phi$ is an isogeny, and by the tower law $\deg(\psi \circ \phi) = \deg(\psi) \deg(\phi)$.

We can also consider the constant map $E_1 \to 0_{E_2}$ to be an isogeny (the zero isogeny), but I guess we don't do this.

Proposition 5.3. *If* $0 \neq n \in \mathbb{Z}$ *then* $[n] : E \to E$ *is an isogeny.*

Proof. Addition and hence $[n]$ is a morphism by Theorem 4.5, and $0_E \to N0_E = 0_E$. We must show $[n] \neq [0]$. Assume that $\operatorname{char} K \neq 2$.

If $n = 2$, then by Lemma 4.5, $E[2] \neq E$, so $[2] \neq [0]$.

If n is odd, then there exists a nonzero $T \in E[2]$, so $nT = T \neq 0$, so $[n] \neq [0]$. Then since $[mn] = [m] \circ [n]$, we are done.

If $\operatorname{char} K = 2$, we could replace Lemma 4.8 by a similar result about $E[3]$. □

Corollary 5.4. $\operatorname{Hom}(E_1, E_2)$ *is a torsion-free* $\mathbb{Z}$*-module.*

Proof. $\mathbb{Z}$ acts on $\operatorname{Hom}(E_1, E_2)$ by $n\phi = [n] \circ \phi$. But since $[n] \neq [0]$, there is no torsion. □

Theorem 5.5. *Let* $\phi : E_1 \to E_2$ *be an isogeny. Then* ϕ *is a group homomorphism, so* $\phi(P + Q) = \phi(P) + \phi(Q)$.

Proof. ϕ induces a map on divisors:

$$\begin{aligned} \phi_* : \mathrm{Div}^0(E_1) &\to \mathrm{Div}^0(E_2) \\ \sum n_P P &\mapsto \sum n_P \phi(P) \end{aligned} \tag{5.1}$$

Recall that we have an inclusion of function fields $\phi^* : K(E_2) \to K(E_1)$, and $K(E_1)/K(E_2)$ is a finite extension, so we have a norm map $N_{K(E_1)/K(E_2)} : K(E_1) \to K(E_2)$. It is a fact that if $f \in \overline{K}(E_1)^*$, then

$$\mathrm{div}(N_{K(E_1)/K(E_2)} f) = \phi_*(\mathrm{div}\, f) \tag{5.2}$$

so ϕ_* sends principal divisors to principal divisors.

Since $\phi(0_{E_1}) = 0_{E_2}$, the following diagram commutes:

$$\begin{array}{ccc} E_1 & \xrightarrow{\quad\phi\quad} & E_2 \\ \downarrow\cong & & \downarrow\cong \\ \mathrm{Pic}^0(E_1) & \xrightarrow{\phi_*} & \mathrm{Pic}^0(E_2) \end{array}$$

So since ϕ_* is a group homomorphism, ϕ is a group homomorphism. □

Lemma 5.6. *Let $\phi : E_1 \to E_2$ be an isogeny. Then there exists a morphism ξ making the following diagram commute:*

$$\begin{array}{ccc} E_1 & \xrightarrow{\quad\phi\quad} & E_2 \\ \downarrow{\scriptstyle x_1} & & \downarrow{\scriptstyle x_2} \\ \mathbb{P}^1 & \xrightarrow{\xi} & \mathbb{P}^1 \end{array}$$

where x_i is the coordinate function sending $P = (x, y) \mapsto x$ for $P \in E_i$.

Moreover, if $\xi(t) = r(t)/s(t)$, $r(t), s(t) \in K[t]$ coprime, then $\deg \phi = \deg \xi = \max(\deg r, \deg s)$.

Proof. For $i = 1, 2$, we have that $K(E_i)/K(x_i)$ is a degree 2 Galois extension, where $K(E_i) = K(x_i, y_i)$ is the function field of E_i. To see, this we just need to exhibit a nontrivial element of the Galois group. We have that $[-1]^*$ sending $y_i \to -y_i$ is such a morphism. Furthermore, by Theorem 5.5, we have that $\phi \circ [-1] = [-1] \circ \phi$, so if $f \in K(x_2)$, then

$$[-1]^* \phi^* f = \phi^* [-1]^* f = \phi^* f \tag{5.3}$$

so $\phi^* f$ is fixed by the Galois group, so $\phi^* f \in K(x_1)$. Thus in particular, we can set $\phi^* x_2 = \xi(x_1)$ for some rational function ξ. Then by the tower law, we have that $\deg \phi = \deg \xi$.

Now $K(x_2) \hookrightarrow K(x_1)$ via $x_2 \mapsto \xi(x_1) = r(x_1)/s(x_1)$. We claim that the minimal polynomial of x_1 over x_2 is $F(t) = r(t) - s(t)x_2 \in K(x_2)[t]$. We have $F(x_1) = 0$, and F is irreducible in $K[x_2, t]$ because r, s are coprime. Then F is irreducible in $K(x_2)[t]$ by Gauss's lemma. Thus we have that

$$\deg \xi = [K(x_1) : K(x_2)] = \deg F = \max(\deg r, \deg s). \tag{5.4}$$

□

Lemma 5.7. $\deg[2] = 4$.

Proof. Assume $\operatorname{char} K \neq 2, 3$, so that $E : y^2 = x^3 + ax + b = f(x)$.

If $P = (x, y) \in E$, then $x(2P) = g(x)/4f(x)$ where $\deg g = 4$ (direct calculation). So by Lemma 5.6, we have that $\deg[2] = \max(\deg g, \deg f) = 4$. □

Definition 5.8. Let A be an abelian group. Then $q : A \to \mathbb{Z}$ is a quadratic form if

1. $q(nx) = n^2 q(x)$ for all $n \in \mathbb{Z}, x \in A$.
2. $(x, y) \mapsto q(x + y) - q(x) - q(y)$ is $\mathbb{Z}$-bilinear.

Lemma 5.9. *$q : A \to \mathbb{Z}$ is quadratic form if and only if it satisfies the parallelogram law:*

$$q(x + y) + q(x - y) = 2q(x) + 2q(y). \tag{5.5}$$

Proof. Bash/Sheet 2. □

Theorem 5.10. *We have that the degree map* $\deg : \operatorname{Hom}(E_1, E_2) \to \mathbb{Z}$ *is a quadratic form, where we set* $\deg 0 = 0$.

We will assume that $\operatorname{char} K \neq 2, 3$ for simplicity. Write

$$E_2 : y^2 = x^3 + ax + b \tag{5.6}$$

and assume that $P, Q, P + Q, P - Q \neq 0$ with respective x-coordinates x_1, x_2, x_3, x_4.

Lemma 5.11. *There exist polynomials $W_0, W_1, W_2 \in \mathbb{Z}[a, b][x_1, x_2]$ of degree at most 2 in x_1 and degree at most 2 in x_2 such that*

$$(1 : x_3 + x_4 : x_3 x_4) = (W_0 : W_1 : W_2). \tag{5.7}$$

Proof. Let $y = \lambda x + \nu$ be the line through P and Q. Then

$$x^3 + ax + b - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3) = x^3 - s_1 x^2 + s_2 x - s_3 \tag{5.8}$$

where s_1, s_2, s_3 are the respective symmetric polynomials in x_1, x_2, x_3. Comparing coefficients gives

$$\begin{aligned} \lambda^2 &= s_1 \\ -2\lambda\nu &= s_2 - a \\ \nu^2 &= s_3 + b \end{aligned} \tag{5.9}$$

Eliminating λ and ν gives

$$F(x_1, x_2, x_3) = (s_2 - a)^2 - 4s_1(s_3 + b) = 0 \tag{5.10}$$

which has degree less than 2 in x_1, x_2 x_3 as s_1, s_2, s_3 have degree 1 in x_1, x_2 x_3. Now x_3 is a root of $W(t) = F(x_1, x_2, t)$, and F is a quadratic polynomial in t.

As Q and $-Q$ have the same x-coordinate, if we repeat the above process with the line through P and $-Q$, we find that x_4 is the other root of $F(x_1, x_2, t)$ (which is quadratic in t). Thus writing $F(x_1, x_2, t) = W_0(t - x_3)(t - x_4)$ for some $W_0(x_1, x_2, a, b)$, we have that

$$W_0(t - x_3)(t - x_4) = W_0 t^2 - W_1 t + W_2 \tag{5.11}$$

where W_0, W_1, W_2 all have degree less than 2 in x_1, x_2. Now comparing coefficients gives

$$x_3 + x_4 = \frac{W_1}{W_0}, \quad x_3 x_4 = \frac{W_2}{W_0} \tag{5.12}$$

□

Proof of Theorem 5.10. We show that if $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$, then

$$\deg(\phi + \psi) + \deg(\phi - \psi) \leq 2\deg\phi + 2\deg\psi. \tag{5.13}$$

When we have show this, we can replace ϕ by $\phi + \psi$ and ψ by $\phi - \psi$ to get the inequality going the other way.

We may assume $\phi, \psi, \phi+\psi, \phi-\psi \neq 0$. Otherwise the proof is trivial, or we use that $\deg[-1] = 1$, $\deg[2] = 4$.

Let $\phi, \psi, \phi + \psi, \phi - \psi$ have respective coordinate functions $\xi_1, \xi_2, \xi_3, \xi_4$. Then by Lemma 5.11, we have that

$$(1 : \xi_3 + \xi_4 : \xi_3\xi_4) = (W_0(\xi_1, \xi_2), W_1(\xi_1, \xi_2), W_2(\xi_1, \xi_2)). \tag{5.14}$$

Put $\xi_i = r_i/s_i$ with $r_i, s_i \in K[t]$ coprime. So

$$(1 : \xi_3 + \xi_4 : \xi_3\xi_4) = (s_3 s_4 : r_3 s_4 + r_4 s_3 : r_3 r_4) = (W_0(r_1 s_2, r_2 s_1) : W_1(r_1 s_2, r_2 s_1) : W_2(r_1 s_2, r_2 s_1)) \tag{5.15}$$

and the LHS is coprime as r_i, s_i are coprime. We then have that

$$\begin{aligned} \deg(\phi + \psi) + \deg(\phi - \psi) &= \max(\deg r_3, \deg s_3) + \max(\deg r_4, \deg s_4) \\ &= \max(\deg(s_3 s_4), \deg(r_3 s_4 + r_4 s_3), \deg(r_3 r_4)) \\ &\leq 2\max(\deg r_1, \deg s_1) + 2\max(\deg r_2, \deg s_2) \\ &= 2\deg\phi + 2\deg\psi. \end{aligned} \tag{5.16}$$

Replacing ϕ by $\psi + \psi$ and ψ by $\phi - \psi$ gives

$$\deg 2\phi + \deg 2\psi \leq 2\deg(\phi + \psi) + 2\deg(\phi - \psi). \tag{5.17}$$

Applying Lemma 5.7 gives the reverse inequality, which shows the parallelogram law holds, so we have a quadratic form. □

Corollary 5.12. *We have that* $\deg n\phi = n^2 \deg\phi$ *for all* $n \in \mathbb{Z}$, $\phi \in \mathrm{Hom}(E_1, E_2)$. *In particular, we have that* $\deg[n] = n^2$.

Now we will finally give an example of an isogeny which is not $[n]$.

Example 5.13. Let E/K an elliptic curve, and assume $\mathrm{char}\, K \neq 2$, so there exists nonzero $T \in E(K)[2]$. WLOG we have that

$$E : y^2 = x(x^2 + ax + b), \quad a, b \in K, \quad b(a^2 - 4b) \neq 0 \tag{5.18}$$

and we can take $T = (0, 0)$ to be our 2-torsion point. We want to quotient out by $\langle 0, T\rangle$. If $P = (x, y)$, then we have that $P' = P + T = (x', y')$ with

$$x' = \frac{b}{x}, \quad y' = -\frac{by}{x^2}. \tag{5.19}$$

We want to send (x, y) and (x', y') to the same place. A natural choice for a map is then

$$\xi = x + x' + a = \left(\frac{y}{x}\right)^2, \qquad \eta = y + y' = \frac{y}{x}\left(x - \frac{b}{x}\right). \tag{5.20}$$

Then we have that

$$\eta^2 = \xi(\xi^2 - 2a\xi + a^2 - 4b) \tag{5.21}$$

Let $E' : y^2 = x(x^2 + a'x + b')$ with $a' = -2a$, $b' = a^2 - 4b$. This is an elliptic curve because $b' = a^2 - 4b \neq 0$ and $a'^2 - 4b' = 16b \neq 0$. There's an isogeny

$$\begin{aligned} &\phi : E \to E' \\ &(x, y) \mapsto \left(\left(\frac{y}{x}\right)^2 : \frac{y(x^2 - b)}{x^2} : 1\right). \end{aligned} \tag{5.22}$$

At $0_E = (0 : 1 : 0)$, we can compare orders of vanishing to find that $0_E \to 0_{E'}$.

To compute the degree of this map we write

$$\left(\frac{y}{x}\right)^2 = \frac{x^2 + ax + b}{x} \tag{5.23}$$

and the numerator and denominator are coprime as $b \neq 0$, so $\deg \phi = 2$. We say that ϕ is a 2-isogeny because of its degree.

6 The invariant differential

Let C be an algebraic curve over $K = \overline{K}$.

Definition 6.1. The space of differential Ω_C is a $K(C)$-vector space generated by df for $f \in K(C)$, subject to the relations

1. $d(f + g) = df + dg$.
2. $d(fg) = gdf + fdg$.
3. $da = 0$ for $a \in K$.

Since C is a curve, Ω_C is a 1-dimensional vector space. This is the cotangent space at the generic point of C I think, which is $T^*_{C/K,\eta} = \Omega_{C/K}(\eta)$ or something, for η the generic point of C. Since C is a variety, by a Theorem from Abelian varieties, C is smooth at its generic point, so Ω_C is a 1-dimensional $K(C)$-vector space because C is 1-dimensional.

Let $0 \neq \omega \in \Omega_C$, $P \in C$ be a smooth point, $t \in K(C)$ a uniformizer at P. Then it is a fact that $\omega = fdt$ for some $f \in K(C)^\times$), and we define

$$\mathrm{ord}_P(\omega) = \mathrm{ord}_P(f), \tag{6.1}$$

and this definition is independent of the choice of t.

Now, assume C is a smooth projective curve.

Definition 6.2. The divisor of $0 \neq \omega \in \Omega_C$ is

$$\operatorname{div}(\omega) = \sum_{P \in C} \operatorname{ord}_P(\omega) P \in \operatorname{Div}(C). \tag{6.2}$$

This is a well-defined divisor because $\operatorname{ord}_P(\omega) = \operatorname{ord}_P(f)$ is zero for all but finitely many P.

A differential $\omega \in \Omega_C$ is regular if $\operatorname{div}(\omega) \geq 0$, so it has no poles.

The regular differentials form a K-vector space, and its dimension is the genus $g(C)$ of the curve.

In the case of elliptic curves, this is 1-dimensional K-vector space. Note that the space of all differentials on a curve is a 1-dimensional $K(C)$-vector space, and don't confuse these two vector spaces or think that the fact that they have the same dimension means anything.

As a consequence of the Riemann-Roch theorem, we have that

$$\deg(\operatorname{div} \omega) = 2g - 2 \tag{6.3}$$

Suppose that $f \in K(C)^\times$, and $\operatorname{ord}_P(f) = n \neq 0$. If $\operatorname{char} k \nmid n$, then $\operatorname{ord}_P(df) = n - 1$.

Lemma 6.3. *Assume* $\operatorname{char} K \neq 2$*, and let*

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3), \tag{6.4}$$

with e_1, e_2, e_3 distinct. Then $\omega = dx/y$ is a differential on E with no zeros or poles.

As a consequence, we have that $g(E) = 1$ by (6.3)*.*

In particular, the k-vector space of regular differentials on E is 1-dimensional, and spanned by ω.

Proof. Let $T_i = (e_i, 0)$, so that $E[2] = \{0, T_1, T_2, T_3\}$. Then $\operatorname{div} y = (T_1) + (T_2) + (T_3) - 3(0)$. This follows from the fact that y has a pole of order 3 at 0, and zeros of order 1 at T_i, and since y is principal, has no other poles, and is degree 0, these are all the zeros and poles. For $P = (x_P, y_P) \in E \setminus \{0\}$, a similar calculation gives $\operatorname{div}(x - x_P) = (P) + (-P) - 2(0)$. If $P \in E \setminus E[2]$, then $\operatorname{ord}_P(x - x_P) = 1$, so $\operatorname{ord}_P(dx) = 0$. If $P = T_i$, then $\operatorname{ord}_P(x - x_P) = 2$, so $\operatorname{ord}_P(dx) = 1$. If $P = 0$, then $\operatorname{ord}_P(x) = -2$, so $\operatorname{ord}_P(dx) = -3$. Thus we have that

$$\operatorname{div} dx = (T_1) + (T_2) + (T_3) - 3(0) = \operatorname{div} y, \tag{6.5}$$

so $\operatorname{div}(dx/y) = 0$. □

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

$$\begin{aligned} \phi^* : \Omega_{C_2} &\to \Omega_{C_1} \\ f dg &\mapsto (\phi^* f) d(\phi^* g). \end{aligned} \tag{6.6}$$

Lemma 6.5. *For $P \in E$, let $\tau_P : E \to E$ be the translation map $X \mapsto X + P$, and $\omega = dx/y$ as above. Then $\tau_P^* \omega = \omega$, so ω is an* invariant differential*.*

Proof. $\tau_P^* \omega$ is a regular differential on E (by some divisor pushforward stuff), so $\tau_P^* \omega = \lambda_p \omega$ for some $\lambda_P \in K^\times$ since the space of regular differentials in 1-dimensional.

Now the map $E \to \mathbb{P}^1$ sending $P \mapsto \lambda_P$ is a morphism of projective curves, but it is not surjective, because 0 and ∞ are not in its image, for instance. So it is constant by Theorem 2.15. Thus $\tau_P^* \omega = \lambda \omega$, but taking $P = 0$ we see that $\lambda = 1$. □

Remark 6.6. If $K = \mathbb{C}$, then $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ via the map $z \to (\wp(z), \wp'(z))$, and under this map we have $dx/y = \wp'(z)dz/\wp(z) = dz$ which is clearly translation-invariant.

Lemma 6.7. *Let $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$. Let ω an be invariant differential on E_2. Then $(\phi+\psi)^*\omega = \phi^*\omega + \psi^*\omega$.*

Proof. Write $E = E_2$, and define the following maps $E \times E \to E$:

$$\begin{aligned} \mu &: (P, Q) \mapsto P + Q \\ \mathrm{pr}_1 &: (P, Q) \mapsto P \\ \mathrm{pr}_2 &: (P, Q) \mapsto Q. \end{aligned} \tag{6.7}$$

It is a fact that $\Omega_{E\times E}$ is a 2-dimensional $K(E \times E)$-vector space with basis $\mathrm{pr}_1^*\,\omega, \mathrm{pr}_2^*\,\omega$. Therefore

$$\mu^*\omega = f\,\mathrm{pr}_1^*\,\omega + g\,\mathrm{pr}_2^*\,\omega \tag{6.8}$$

for some $f, g \in K(E \times E)$. We want to show that $f = g = 1$. For $Q \in E$ let $\iota_Q : E \to E \times E$ be the mapping $P \mapsto (P, Q)$. Applying ι_Q^* to (6.8) gives

$$(\mu\iota_Q)^*\omega = (\iota_Q^* f)(\mathrm{pr}_1\,\iota_Q)^*\omega + (\iota_Q^* g)(\mathrm{pr}_2\,\iota_Q)^*\omega. \tag{6.9}$$

Now, we have that $\tau_Q = \mu \circ \iota_Q$, $\mathrm{pr}_1 \circ \iota_Q = \mathrm{id}$, and $\mathrm{pr}_2 \circ \iota_Q = Q$, so simplifying the above gives

$$\tau_Q^*\omega = (\iota_Q^* f)\omega + 0 = \omega \tag{6.10}$$

by Lemma 6.5. Thus $\iota_Q^* f = 1$ for all $Q \in E$, so $f(P, Q) = 1$ for all $P, Q \in E$. Similarly $g(P, Q) = q$ for all $P, Q \in E$. Thus we have that

$$\mu^*\omega = \mathrm{pr}_1^*\,\omega + \mathrm{pr}_2^*\,\omega. \tag{6.11}$$

Now, we pull back by $E_1 \to E \times E$ sending $P \to (\phi(P), \psi(P))$ to get

$$(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega \tag{6.12}$$

as desired. □

Lemma 6.8. *Let $\phi : C_1 \to C_2$ be a non-constant morphism. Then ϕ is separable if and only if $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ is nonzero.*

Proof. Omitted. □

Example 6.9. Let $\widehat{\mathbb{G}}_m = \mathbb{A}^1 \setminus \{0\}$ be the multiplicative group variety of units. Let $\phi : \widehat{\mathbb{G}}_m \to \widehat{\mathbb{G}}_m$ be the morphism $x \mapsto x^n$, for $n \geq 2$ an integer. Then clearly $\deg \phi = n$.

We have that $\phi^*(dx) = d(x^n) = nx^{n-1}dx$ so if $\mathrm{char}\, K \nmid n$ then ϕ is separable.

In this case, by Theorem 2.15 we have that $\#\phi^{-1}(Q) = \deg \phi$ for all but finitely many points $Q \in \widehat{\mathbb{G}}_m$. But ϕ is a group homomorphism, so $\#\phi^{-1}(Q) = \#\ker \phi$ for all $Q \in \widehat{\mathbb{G}}_m$. Thus we have that $\#\ker \phi = \deg \phi = n$.

Therefore $K = \overline{K}$ has exactly n nth roots of unity.

Theorem 6.10. *If $\mathrm{char}\, K \nmid n$, then $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.*

Proof. By Lemma 6.7, we have that $[n]^*\omega = n\omega$. Since $\operatorname{char} k \nmid n$, $[n]$ is separable because $[n]^*$ is nonzero by Lemma 6.8. Thus $\#[n]^{-1}Q = \deg[n]$ for all but finitely many $Q \in E$. But since $[n]$ is a group homomorphism, $[n]^{-1}Q = \#E[n]$ for all points. Thus $\deg[n] = \#E[n] = n^2$ by Corollary 5.12.

By group theory, we have that $E[n] \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_t\mathbb{Z}$ for $1 < d_1 | \cdots | d_t | n$ all dividing each other. Also, we have that $d_i | n$ because $E[n]$ has n-torsion. Let p be a prime, $p | d_1$, then $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^t$, and so $t = 2$. Since $E[p] \subseteq E[n^2]$, we have that $E[n] \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$ with $d_1 | d_2 | n$, and $d_1 d_2 = n^2$, so we must have $d_1 = d_2 = n$ so $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ as desired. □

Remark 6.11. If $\operatorname{char} k = p$, then $[p]$ is separable. It can be shown that either $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ for all $r \geq 1$, which is the "ordinary" case, or that $E[p^r] = 0$, which is the "supersingular" case.

7 Elliptic curves over finite fields

Lemma 7.1. *Let A be an abelian group, $q : A \to \mathbb{Z}$ a positive definite quadratic form. So $q(x) \geq 0$, with equality iff $x = 0$. Then*

$$|q(x+y) - q(x) - q(y)| \leq 2\sqrt{q(x)q(y)} \tag{7.1}$$

for all $x, y \in A$.

Proof. We may assume that $x \neq 0$, otherwise the result is obvious, so $q(x) \neq 0$. Let $m, n \in \mathbb{Z}$. Then

$$\begin{aligned} 0 &\leq q(mx + ny) \\ &= \frac{1}{2}\langle mx + ny, mx + ny\rangle \\ &= m^2 q(x) + n^2 q(y) + mn\langle x, y\rangle \\ &= q(x)\left(m + \frac{\langle x, y\rangle}{2q(x)}n\right)^2 + \left(q(y) - \frac{\langle x, y\rangle}{4q(x)}\right)n^2. \end{aligned} \tag{7.2}$$

Take $m = -\langle x, y\rangle$, $n = 2q(x)$. So $q(y) - \langle x, y\rangle^2/4q(x) \geq 0$, so $\langle x, y\rangle^2 \leq 4q(x)q(y)$, and taking square roots gives the results. □

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 $\operatorname{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ is cyclic of order r, generated by $\operatorname{Frob}_q : x \mapsto x^q$.

Let E have Weierstrass equation with coefficients $a_1, \ldots, q_6 \in \mathbb{F}_q$. Note that $a_i^q = a_i$ since $a_i \in \mathbb{F}_q$. Define the Frobenius endomorphism $\phi : E \to E$ sending $(x, y) \mapsto (x^q, y^q)$. This is an isogeny of degree q (look at the function fields).

Then $E(\mathbb{F}_q) = \{P \in E | \phi(P) = P\} = \ker(\phi - 1)$.

Also, $\phi^*\omega = \phi^*(dx/y) = dx^q/y^q = qx^{q-1}dx/y^q = 0$. Thus by Lemma 6.8, since $(1-\phi)^*\omega = \omega \neq 0$, $1 - \phi$ is separable.

By the same argument as in the proof of 6.10, we then have that $\#(1-\phi)^{-1}(Q) = \#\ker(1-\phi) = \deg(1-\phi) = \#E(\mathbb{F}_q)$.

Since the degree map is a positive definite quadratic form, we have that

$$|\deg(1-\phi) - \deg\phi - \deg 1| = |\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}. \tag{7.3}$$

□

Definition 7.3. 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 7.4. *Let $E/\mathbb{F}_q$ be an elliptic curve. Then $\#E(\mathbb{F}_q) = q+1-\mathrm{tr}(\mathrm{Frob}_q)$ and $|\,\mathrm{tr}(\mathrm{Frob}_q)| \leq 2\sqrt{q}$.*

7.1 Zeta functions

For K a number field, set

$$\zeta_K(s) = \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} (N\mathfrak{a})^{-s} = \prod_{\mathfrak{p} \in \mathrm{Spec}\, \mathcal{O}_K \text{ closed}} \left(1 - (N\mathfrak{p})^{-s}\right)^{-1}. \tag{7.4}$$

For K a function field, in other words $K = \mathbb{F}_q(C)$ where $C/\mathbb{F}_q$ is a smooth projective curve, set

$$\zeta_K(s) = \prod_{x \in |C|} (1 - (Nx)^{-s})^{-1} \tag{7.5}$$

where the product is over all the closed points of C. These are the orbits for the action of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ acting on $C(\overline{F}_q)$, and we set $Nx = q^{\deg x}$, where $\deg x$ is the size of the orbit. In other words, the closed points are the points over $\overline{\mathbb{F}_q}$ modulo equivalence under the Galois group. This is the same as the closed points of the scheme, or the maximal ideals of the underlying rings.

We have that $\zeta_K(s) = F(q^{-s})$ for some $F \in \mathbb{Q}[[T]]$:

$$F(T) = \prod_{x \in |C|} (1 - T^{\deg x})^{-1}. \tag{7.6}$$

Taking logarithms, doing some manipulation, and taking exponents, we get

$$F(T) = \exp\left(\sum_{n=1}^{\infty} \frac{\#C(\mathbb{F}_{q^n})}{n} T^n\right) \tag{7.7}$$

because $x \in C(\mathbb{F}_{q^n})$ if and only if x is in the orbit of $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ with $r|n$.

Definition 7.5. The zeta function $Z_C(T)$ of a smooth projective curve $C/\mathbb{F}_q$ is the $F(T)$ defined above.

Theorem 7.6. *Let $E/\mathbb{F}_q$ be an elliptic curve, and let $\#E(\mathbb{F}_q) = q + 1 - a$. Then*

$$Z_E(T) = \frac{1 - aT + qT^2}{(1-T)(1-qT).} \tag{7.8}$$

Proof. We use a convenient formula for $\#E(\mathbb{F}_{q^n})$. Let $\mathrm{Frob}_q = \phi$. By Hasse, $\#E(\mathbb{F}_q) = q+1-\mathrm{tr}(\phi)$, and we have that $\mathrm{tr}(\phi) = a$, $\deg \phi = q$.

From sheet 2, we have that $\phi^2 - a\phi + q = 0$ in $\mathrm{End}(E)$. Iterating ϕ gives

$$\phi^{n+2} - a\phi^{n+1} + q\phi^n = 0 \tag{7.9}$$

Taking traces gives $a_{n+2} - a_1 a_{n+1} + q a_n = 0$, where $a_n = \mathrm{tr}(\phi^n)$. This is a recurrence relation which we can solve to find $a_n = \alpha^n + \beta^n$ where α, β are roots of $X^2 - aX + q = 0$. In particular, we have $|\alpha|, |\beta| \leq \sqrt{q}$. Then

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - a_n. \tag{7.10}$$

Thus

$$\begin{aligned} Z_E(T) &= \exp\left(\sum_{n=1}^{\infty} \frac{q^n + 1 - a_n}{n} T^n\right) \\ &= \frac{1 - a_1 T + qT^2}{(1-T)(1-qT)} \end{aligned} \tag{7.11}$$

after some derivation. □

8 Formal Groups

Definition 8.1. Let R be a ring equipped with the I-adic topology R is complete with respect to I if

1. Hausdorff: $\bigcap_{n \geq 0} I^n = 0$.
2. Every Cauchy sequence converges.

Remark 8.2. If $x \in I$, then $1/(1-x) = 1 + x + x^2 + \cdots$ in the completion of R, so $U^{(1)} = 1 + I \subseteq R^\times$.

We care about the rings $\mathbb{Z}_p, \mathbb{F}_q[[t]], \mathbb{Z}[[t]]$.

Lemma 8.3 (Hensel)**.** *Let R be complete in the I-adic topology, $F \in R[x]$, and $s \in \mathbb{Z}_{>0}$. Suppose $a \in R$ satisfies $F(a) \cong 0 \mod I^s$, $F'(a) \in R^\times$. Then there exists a unique $b \in R$ such that $F(b) = 0$ and $b \cong a \mod I^s$.*

Proof. After renormalizing, can assume $a = 0$ and $F'(0) \in U^{(1)}$.

Take $x_0 = 0$, $x_{n+1} = x_n - F(x_n)$, and the limit satisfies our conditions.

Uniqueness: exercise, change u. □

Let E be our elliptic curve with its ugly projective Weierstrass equation. We look at the affine piece $Y \neq 0$, setting $t = -X/Y$ and $w = -Z/Y$:

$$w = t^3 + a_1 tw + a_2 t^2 w + a_3 w^2 + a_4 t w^2 + a_6 w^3 = f(t, w). \tag{8.1}$$

Out goal is to solve this equation for a general $w(t) \in \mathbb{Z}[a_1, \ldots, a_6][[t]] = R$ with maximal ideal $I = (t)$. We want to find a root of $F(X) = X - f(t, X) \in R[X]$. We can do this with Hensel's lemma. Take $s = 3, a = 0$, then $F(0) \equiv 0 \mod t^3$, and $F'(0) = 1 \mod t$. So we get a solution $w(t)$ such that $w(t) = f(t, w(t))$ and $w(t) \equiv 0 \mod t^3$.

Remark 8.4. Taking $u = 1$ in the proof of Lemma 8.3 gives $w(t) = \lim_{n \to \infty} w_n(t)$, with $w_0(t) = 0$ and $w_{n+1}(t) = f(t, w_n(t))$.

We in fact have that

$$w(t) = t^3(1 + A_1 t + A_2 t^2 + \cdots) \tag{8.2}$$

where $A_1 = a_1$, and the other A_is involve the coefficients a_i.

Lemma 8.5. *Let R be an integral domain, complete with respect to I. Let E be an elliptic curve with $a_i \in R$, $K = \operatorname{Frac} R$. Then*

$$\widehat{E}(I) \coloneqq \{(t, w) \in E(K) \mid t, w \in I\} \tag{8.3}$$

is a subgroup of $E(K)$.

Remark 8.6. We have that

$$\widehat{E}(I) = \{(t, w(t)) \in E(K) \mid t \in I\}. \tag{8.4}$$

This is because $(t, w(t)) \in I$ because if $t \in I$, then $w(t) \in I$ by completeness. Also, if $(t, w) \in E(K)$ and $t \in I$, then the uniqueness part of Hensel's lemma forces $w = w(t)$.

Proof of Lemma 8.5. Taking $(t, w) = (0, 0)$, we have that $0_E \in \widehat{E}(I)$. So it suffices to show that if $P_1, P_2 \in \widehat{E}(I)$, then $-P_1 - P_2 \in \widehat{E}(I)$. We do this by calculating that the coefficients of $-P_1 - P_2$ are in I. A lot of bash. □

Taking $R = \mathbb{Z}[a_1, \ldots, a_6][[t]]$, $I = (t)$, Lemma 8.5 gives that $(t, w(t)) \in \widehat{E}(I)$ has an inverse in I, so that there exists $\iota \in R$ with $\iota(0) = 0$ and

$$[-1](t, w(t)) = (\iota(t), w(\iota(t))). \tag{8.5}$$

Similarly, taking $R = \mathbb{Z}[a_1, \ldots, a_6][[t_1, t_2]]$ and $I = (t_1, t_2)$, Lemma 8.5 gives that there exists $F \in R$ with $F(0, 0) = 0$ and

$$(t_1, w(t_1)) + (t_2, w(t_2)) = (F(t_1, t_2), w(F(t_1, t_2))). \tag{8.6}$$

We have that $F(X, Y) = X + Y - a_1XY - a_2(X^2Y + XY^2) + \cdots$. F is a formal group law, and satisfies the properties below.

Definition 8.7. Let R be a ring. A (1-dimensional, commutative) formal group over R is a power series $F(X, Y) \in R[[X, Y]]$ satisfying

(i) Commutativity: $F(Y, X) = F(X, Y)$.

(ii) Identity: $F(X, 0) = X$, $F(0, Y) = Y$.

(iii) Associativity: $F(X, F(Y, Z)) = F(F(X, Y), Z)$.

(iv) Inverse: there exists $\iota(X) \in R[[X]]$ such that $\iota(0) = 0$ and $F(X, \iota(X)) = 0$.

Property (iv) follows from (i)-(iii).

Example 8.8. The additive formal group $\widehat{\mathbb{G}_a}(X, Y) = X + Y$ associated with the group variety $\mathbb{G}_a$.

The multiplicative group law $\widehat{\mathbb{G}_m} = X + Y + XY = (1 + X)(1 + Y) - 1$ associated with the group variety $\mathbb{G}_m$.

The power series associated to an elliptic curve.

Definition 8.9. Let $\mathcal{F}, \mathcal{G}$ be formal groups over R given by power series F and G. A morphism $f : \mathcal{F} \to \mathcal{G}$ is a power series $f(X) \in R[[X]]$ such that $f(0) = 0$, and $f(F(X, Y)) = G(f(X), f(Y))$.

$\mathcal{F}$ and $\mathcal{G}$ are isomorphic if there exist $f : \mathcal{F} \to \mathcal{G}$ and $g : \mathcal{G} \to \mathcal{F}$ such that $f \circ g(X) = g \circ f(X) = X$.

Theorem 8.10. *If* $\operatorname{char} R = 0$ *then any formal group* $\mathcal{F}$ *over* R *is isomorphic to* $\widehat{\mathbb{G}}_a$ *over* $R \otimes_{\mathbb{Z}} \mathbb{Q}$. *More precisely:*

(i) There is a unique power series

$$\log T = T + \frac{a_2}{2}T^2 + \frac{a_3}{3}T^3 + \cdots \tag{8.7}$$

with $a_i \in R$ *such that*

$$\log(F(X, Y)) = \log X + \log Y \tag{8.8}$$

(ii) There is a unique power series

$$\exp(T) = T + \frac{b_2}{2!}T^2 + \frac{b_3}{3!}T^3 + \cdots \tag{8.9}$$

with $b_i \in R$ *such that* $\exp(\log(T)) = \log(\exp(T)) = T$

Proof. (i) We write $F_1(X, Y) = \frac{\partial F}{\partial X}(X, Y)$.

First we show uniqueness. Let $p(T) = (\log T)' = 1 + a_2T + a_3T^2 + \cdots$. Differentiating (8.8) with respect to X gives

$$p(F(X, Y))F_1(X, Y) = p(X) + 0. \tag{8.10}$$

Putting $X = 0$ gives $p(Y)F_1(0, Y) = 1$. So $p(Y) = F_1(0, Y)^{-1}$.

p is uniquely determined, so a_i is uniquely determined, so $\log T$ is uniquely determined.

Now to show existence. Let $p(T) = F_1(0, T)^{-1} = 1 + a_2T + a_3T^2 + \cdots$, for some $a_i \in R$. Set $\log T = T + a_2/2T^2 + \cdots$. Then

$$F(F(X, Y), Z) = F(X, F(Y, Z)) \tag{8.11}$$

by associativity. Taking partial derivatives by X gives

$$F_1(F(X, Y), Z)F_1(X, Y) = F_1(X, F(Y, Z)). \tag{8.12}$$

Setting $X = 0$ gives

$$F_1(Y, Z)F_1(0, Y) = F_1(0, F(Y, Z)) \tag{8.13}$$

Thus we have that

$$F_1(Y, Z)p(Y)^{-1} = p(F(Y, Z))^{-1} \tag{8.14}$$

so $p(Y) = F_1(Y, Z)p(F(Y, Z))$. Taking anti-derivatives/integrating gives

$$\log(F(Y, Z)) = \log(Y) + h(Z) \tag{8.15}$$

for some power series $h(Z) \in R[[Z]]$. But since $F(Y, Z) = F(Z, Y)$, we have that $h(Z) = \log Z$, proving (8.8).

Part (ii) follows immediately from Lemma 8.11 below, with the exact calculation of exp being doing in Sheet 2, question 12. □

Lemma 8.11. *Let $f(T) = aT + \cdots \in R[[T]]$ with $a \in R\times$. Then there exists a unique $g(T) = a^{-1}T + \cdots R[[T]]$ such that $g(f(T)) = f(g(T)) = T$.*

Proof. We construct a series of polynomials $g_n(T)$ such that $\lim g_n(T) = g(T)$ satisfies $f(g(T)) = T$. In particular, we have $f(g_n(T)) = T \mod T^{n+1}$, so $f(g_{n-1}(T)) = T + bT^n \mod T^{n+1}$. We put $g_n(T) = g_{n-1}(T) - b/aT^n$, and we can check that this works. We can then find $h(T)$ such that $g(h(T)) = T$, and then we have that $f(g(h(T))) = f(T) = h(T)$, so $g(f(T)) = T$ as well. If $g'(T)$ is another inverse, we have that $g'(f(g(T))) = g(T) = g'(T)$. □

Example 8.12. If $\mathcal{F} = \widehat{\mathbb{G}}_m$ the multiplicative group law, then $\log, \exp$ are the usual power series but shifted by 1:

$$\begin{aligned} \log(T) &= \log(T+1) \\ \exp(T) &= \exp(T) - 1 \end{aligned} \tag{8.16}$$

where the LHS is the formal group law functions and the right hand side is the ordinary Taylor series.

Definition 8.13. Let $\mathcal{F}$ be a formal group law given by the power series $F(X,Y) \in R[[X,Y]]$. Suppose R is a ring, complete with respect to the ideal I. For $x, y \in I$, we set $x \oplus_{\mathcal{F}} y = F(x,y) \in I$. It is easy to verify using the formal group law axioms that

$$\mathcal{F}(I) \coloneqq (I, \oplus_{\mathcal{F}}) \tag{8.17}$$

is an abelian group.

Example 8.14. $\widehat{\mathbb{G}}_a(I) = (I, +)$ and $\widehat{\mathbb{G}}_m(I) = (1 + I, \times) = (U^{(1)}, \times)$ and $\widehat{E}(I)$, the subgroup of $E(K)$ defined in Lemma 8.5.

Corollary 8.15. *Let $\mathcal{F}$ be a formal group over R and $n \in \mathbb{Z}$. Suppose $n \in R^\times$. Then*

(i) $[n]$ is an isomorphism of formal groups.

(ii) If R is complete with respect to I, then the multiplication by n map $\mathcal{F}(I) \to \mathcal{F}(I)$ sending $x \mapsto nx$ is an isomorphism of groups. In particular, $\mathcal{F}(I)$ has no n-torsion.

Proof. (i) We have that $[1](T) = T$, so $[n](T) = F([n-1]T, T)$ for $n > 0$, and for $n < 0$, we use $[-1](T) = \iota(T)$, and we can set $[-n](T) = F([-n+1](T), \iota(T))$.

Since $F(X,Y) = X + Y \mod \deg 2$, we have that $[n]T = nT \mod \deg 2$ by induction, and by Lemma 8.11 we have that $[n]T$ is invertible so it is an isomorphism.

(ii) It is easy to see that a morphism of formal groups $\mathcal{F} \to \mathcal{G}$ is a morphism of groups $\mathcal{F}(I) \to \mathcal{G}(I)$, and an isomorphism of formal groups is an isomorphism of groups. □

9 Elliptic curves over local fields

Let K be a field which is complete with respect to the discrete valuation $v : K^\times \to \mathbb{Z}$. We define the ring of integers $\mathcal{O}_K$ with maximal ideal $\pi\mathcal{O}_K$ and the residue field $k = \mathcal{O}_K/\pi\mathcal{O}_K$ in the usual way. Assume that $\operatorname{char} K = 0$ and $\operatorname{char} k = p > 0$. For instance, take $K = \mathbb{Q}_p$, $\mathcal{O}_K = \mathbb{Z}_p$ and $k = \mathbb{F}_p$.

Let E/K be an elliptic curve.

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

Remark 9.2.

1. Rescaling any Weierstrass equations appropriately gives an integral one.
2. If $a_1, \dots, a_6 \in \mathcal{O}_K$, then we easily see that $\Delta \in \mathcal{O}_K$, so $v(\Delta) \geq 0$.
3. If $\operatorname{char} k \neq 2, 3$ then there exists a *minimal* Weierstrass equation of the form $y^2 = x^3 + ax + b$. This is because we need $1/2$ and $1/3 \in \mathcal{O}_K$, so $2, 3 \in \mathcal{O}_K{}^\times$, so $\overline{2}, \overline{3} \in k^\times$.

Lemma 9.3. *Let E/K have integral Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and let $0 \neq P = (x, y) \in E(K)$. Then either $x, y \in \mathcal{O}_K$ or $v(x) = -2s$ and $v(y) = -3s$ for some $s \geq 1$.*

Compare this with Sheet 1, Question 5.

Proof. Just do some valuation calculations. □

Since K is complete, $\mathcal{O}_K$ is complete with respect to any ideal $I = \pi^r\mathcal{O}_K$ for $r \geq 1$. Let E/K be an elliptic curve and fix a minimal Weierstrass equation for E. We then get a formal group $\widehat{E}$, and taking $I = \pi^r\mathcal{O}_K$, we get a group

$$\begin{aligned}
\widehat{E}(\pi^r\mathcal{O}_K) &= \{(x, y) \in E(K) \mid \left(-\frac{x}{y}, -\frac{1}{y}\right) \in \pi^r\mathcal{O}_K\} \cup \{0\} \\
&= \{(x, y) \in E(K) \mid v\left(\frac{x}{y}\right), v\left(\frac{1}{y}\right) \geq r\} \cup \{0\} \\
&= \{(x, y) \in E(K) \mid v(x) = -2s, v(y) = -3s, s \geq r\} \cup \{0\} \\
&= \{(x, y) \in E(K) \mid v(x) \leq -2r, v(y) \leq -3r\} \cup \{0\}
\end{aligned} \tag{9.1}$$

so $\widehat{E}(\pi^r\mathcal{O}_K)$ is the subgroup of $E(K)$ with valuations sufficiently negative, and we can set $\widehat{E}(\pi^r\mathcal{O}_K) = E_r(K)$. We have a filtration

$$E(K) \supset E_1(K) \supset E_2(K) \supset \cdots \tag{9.2}$$

More generally, for $\mathcal{F}$ a formal group over $\mathcal{O}_K$, we have a filtration

$$\mathcal{F}(\pi\mathcal{O}_K) \supset \mathcal{F}(\pi^2\mathcal{O}_K) \supset \cdots \tag{9.3}$$

We claim that for r sufficiently large, $\mathcal{F}(\pi^r\mathcal{O}_K) \cong (\mathcal{O}_K, +)$ and $\mathcal{F}(\pi^r\mathcal{O}_K)/\mathcal{F}(\pi^{r+1}\mathcal{O}_K) \cong (k, +)$ for all $r \geq 1$.

Theorem 9.4. *Let $\mathcal{F}$ be a formal group over $\mathcal{O}_K$. Let $e = e_{K/\mathbb{Q}_p} = v(p)$ be the absolute ramification index. If $r > e/(p-1)$, then we have an isomorphism*

$$\log : \mathcal{F}(\pi^r\mathcal{O}_K) \to \widehat{\mathbb{G}}_a(\pi^r\mathcal{O}_K) \tag{9.4}$$

with inverse isomorphism

$$\exp : \widehat{\mathbb{G}}_a(\pi^r\mathcal{O}_K) \to \mathcal{F}(\pi^r\mathcal{O}_K) \tag{9.5}$$

It follows that $\mathcal{F}(\pi^r\mathcal{O}_K) \cong (\pi^r\mathcal{O}_K, +) \cong (\mathcal{O}_K, +)$

Proof. For $x \in \pi^r \mathcal{O}_K$, we must show the power series $\log x$ and $\exp x$ converge to elements in $\pi^r \mathcal{O}_K$. We do this by straightforward calculation and the integer trick. □

Lemma 9.5. *The definition of a formal group gives $F(X,Y) = X+Y+XY(\cdots)$. So if $x, y \in \mathcal{O}_K$, then $F(\pi^r x, \pi^r y) = \pi^r(x+y) \mod \pi^{r+1}$.*

Therefore we have a surjective group homomorphism $\mathcal{F}(\pi^r \mathcal{O}_K) \to (k,+)$ by $\pi^r x \mapsto x \mod \pi$ which has kernel $\mathcal{F}(\pi^{r+1}\mathcal{O}_K)$.

Corollary 9.6. *If $|k| < \infty$, then $\mathcal{F}(\pi\mathcal{O}_K)$ has a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.*

Notation: We write $\overline{x}$ for the image of x under the reduction mod π map $\mathcal{O}_K \to \mathcal{O}_K/\pi\mathcal{O}_K = k$.

Proposition 9.7. *Let E/K be an elliptic curve. Then the reduction mod π of any 2 minimal Weierstrass equations for E defines isomorphic curves over k.*

Proof. Suppose the Weierstrass equations are related by transformation $[u; r, s, t]$ with $u \in K^\times$, $r, s, t \in K$. Then $\Delta_1 = u^{12}\Delta_2$, and since both are minimal we have that $u \in \mathcal{O}_K^\times$. The transformation formula for a_i and b_i and the fact that $\mathcal{O}_K$ is integrally closed implies that $r, s, t \in \mathcal{O}_K$ as well. Then the Weierstrass equations for the reduction modulo π are related by $[\overline{u}; \overline{r}, \overline{s}, \overline{t}]$ and $\overline{u} \in k\times$ and $\overline{r}, \overline{s}, \overline{t} \in k$. □

Definition 9.8. The *reduction* $\overline{E}/k$ of E/K is defined by the reduction of a minimal Weierstrass equations.

The reduction is well-defined, but is it an elliptic curve?

We say that E has *good reduction* if $\overline{E}$ is nonsingular (so it is an elliptic curve).

We say that E has *bad reduction* otherwise.

For an integral Weierstrass equation, if $v(\Delta) = 0$, then the equation is minimal, and $\overline{\Delta} \neq 0$, so we have good reduction.

If $0 < v(\Delta) < 12$, then the equation is minimal, so we have bad reduction.

If $12 \nmid v(\Delta)$, then we always have bad reduction. But if $12|v(\Delta)$, then the equation might not be minimal.

There is a well defined map

$$\begin{aligned} \mathbb{P}^2(K) &\to \mathbb{P}^2(k) \\ (x:y:z) &\mapsto (\overline{x}:\overline{y}:\overline{z}) \end{aligned} \tag{9.6}$$

where we choose representatives $(x:y:z)$ such that $x, y, z \in \mathcal{O}_K$ and at least one of x, y, z is in $\mathcal{O}_K^\times$.

So we can restrict to get a map $E(K) \to \overline{E}(K)$ by sending $P \to \overline{P}$. If $P = (x,y) \in E(K)$, then by Lemma 9.3 either $x, y \in \mathcal{O}_K$ so $\overline{P} = (\overline{x}, \overline{y})$ or $v(x) = -2s, v(y) = -3s$ for some $s \geq 1$, so $P = (x:y:1) = (\pi^{3s}x : \pi^{3s}y : \pi^{3s}) = (0:1:0)$, the point at infinity.

So $\widehat{E}(\pi\mathcal{O}_K) = E_1(K) = \{P \in E(K) | \overline{P} = 0\}$, the "kernel of reduction".

Definition 9.9. Let $\tilde{E}$ be the reduction of E mod π. We set

$$\tilde{E_{\text{ns}}} = \begin{cases} \tilde{E} & E \text{ has good reduction} \\ \tilde{E}\backslash\{*\} & E \text{ has bad reduction} \end{cases} \tag{9.7}$$

where $*$ is the singular point of $\tilde{E}$.

The chord and tangent process still defines a group law on $\tilde{E_{\text{ns}}}$. The main idea is that the chord and tangent process will never hit a singular point.

In the case of bad reduction, we have that either $\tilde{E_{\text{ns}}} \cong \widehat{\mathbb{G}}_m$, in which the isomorphism of varieties is defined K or over a quadratic extension of K. Or, we have that $\tilde{E_{\text{ns}}} \cong \widehat{\mathbb{G}}_a$, in which the isomorphism is defined over K.

For simplicity, assume that $\operatorname{char} k \neq 2$. Then we have that $\tilde{E} : y^2 = f(x)$, and $\deg f = 3$. Then $f(x)$ either has a double root, which is a node, and we say that E has *multiplicative reduction*, or $f(x)$ has a triple root, which is a cusp, and we say that E has *additive reduction.*

If E has multiplicative reduction and the isomorphism $\tilde{E_{\text{ns}}} \cong \widehat{\mathbb{G}}_m$ is defined over K, then we say that E has *split multiplicative reduction.*

In the case of additive reduction, we have that our curve looks like $y^2 = x^3$. We have an isomorphism

$$\begin{aligned} \tilde{E_{\text{ns}}} &\to \widehat{\mathbb{G}}_a \\ (t^{-2}, t^{-3}) &\leftarrow t \\ \infty &\leftarrow 0 \\ (x, y) &\mapsto x/y \end{aligned} \tag{9.8}$$

Now, let $ax + by = 1$ be a line not going through the origin, and write $P_i = (x_i, y_i)$ for the three points of intersection with $\tilde{E_{\text{ns}}}$ and $t_i = x_i/y_i$. Then $x_i^3 = y_i^2 = y_i^2(ax_i + by_i)$. Dividing out by y_i^3, we get $t_i^3 - at_i - b = 0$, so t_1, t_2, t_3 are roots of $T^3 - aT - b$, and the root all sum to zero. Since $t_1 + t_2 + t_3 = 0$ and $P_1 + P_2 + P_3 = 0$, we have a valid chord and tangent process, which defines a group homomorphism. We can check that it is an isomorphism.

In the node case: removing a node is like removing 2 points because the curve passes through the node twice, so $\tilde{E_{\text{ns}}} \cong \mathbb{P}^1 \setminus \{0, \infty\} \cong \widehat{\mathbb{G}}_m$. Details on example sheet 3.

Definition 9.10. Define $E_0(K) = \{P \in E(K) \mid \tilde{P} \in \tilde{E_{\text{ns}}}(K)\}$. If E has good reduction, then $E_0(K) = E(K)$.

Proposition 9.11. *$E_0(K)$ is a subgroup of $E(K)$ and reduction mod π is a surjective group homomorphism $E_0(K) \to \tilde{E_{\text{ns}}}(K)$.*

Note that if E/K has good reduction, then this is a surjective group homomorphism $E(K) \to \tilde{E}(K)$.

Proof. First we will show that we have a group homomorphism $E_0(K) \to \tilde{E_{\text{ns}}}(K)$. A line in $\mathbb{P}^2$ defined over K has equation $\ell : aX + bY + cZ = 0$, with $a, b, c \in K$. We may assume that $\min(v(a), v(b), v(c)) = 0$, so reduction mod π gives a line

$$\tilde{\ell} : \tilde{a}X + \tilde{b}Y + \tilde{c}Z = 0. \tag{9.9}$$

If $P_1, P_2, P_3 \in E(K)$ with $P_1 + P_2 + P_3 = 0$, then these points line on a line ℓ. Thus $\tilde{P_1}, \tilde{P_2}, \tilde{P_3}$ line on $\tilde{\ell}$. If $\tilde{P_1}, \tilde{P_2} \in \tilde{E_{\text{ns}}}(K)$, then $\tilde{p_3} \in \tilde{E_{\text{ns}}}(K)$ as the third point of intersection cannot be singular (as then the line would intersect the cubic at "4" points). So if $P_1, P_2 \in E_0(K)$, then $P_3 \in E_0(K)$ and $\tilde{P_1} + \tilde{P_2} + \tilde{P_3} = 0$. We can check that this still works when one of the reductions is the point at infinity. Thus we have a group homomorphism.

Now to check surjectivity. Let $f(x, y) = y^2 + a_1xy + a_3y - (x^3 + \cdots)$ and let $\tilde{P} \in \tilde{E_{\text{ns}}}(K) \setminus \{0\}$, so $\tilde{P} = (\tilde{x}_0, \tilde{y}_0)$ for some $(x_0, y_0) \in \mathcal{O}_K$. Since $\tilde{P}$ is nonsingular, either (i) $\frac{\partial f}{\partial x}(x_0, y_0) \neq 0 \mod \pi$ or

(ii) $\frac{\partial f}{\partial y}(x_0, y_0) \neq 0 \mod \pi$. WLOG assume (i), case (ii) follows similarly. We put $g(t) = f(t, y_0) \in \mathcal{O}_K[t]$. Then $g(x_0) \equiv 0 \mod \pi$, and $g'(x_0) \in \mathcal{O}_K^\times$ by assumption (i). By Hensel's lemma, then there exists $b \in \mathcal{O}_K$ such that $g(b) = 0$ and $b \equiv x_0 \mod \pi$. Then $(b, y_0) \in E(K)$, and has reduction mod π equal to $\tilde{P}$. □

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

$$E_r(K) = \widehat{E}(\pi^r \mathcal{O}_K) = \{(x, y) \in E(K) \mid v(x) \leq -2r, v(y) \leq -3r\} \cup \{0\}. \tag{9.10}$$

Then we have a filtration

$$E(K) \supset E_0(K) \supset E_1(K) \supset \cdots \tag{9.11}$$

where for $r > e/(p-1)$ we have that $E_r(K) \cong (\mathcal{O}_K, +)$. We also have that $E_i(K)/E_{i+1}(K) \cong (k, +)$ for $i \geq 1$ by Proposition 9.11, we have that

$$E_0(K)/E_1(K) \cong \tilde{E_{\text{ns}}}(K). \tag{9.12}$$

The question remains: what is $E(K)/E_0(K)$. In general, this requires a lot of algebraic geometry to calculate, but we can prove it is finite fairly easily.

Lemma 9.12. *If $|k| < \infty$, then $E_0(K) \subset E(K)$ has finite index.*

Proof. If E has good reduction, we are done as $E(K) = E_0(K)$. So assume $E(K)$ has bad reduction.

If $|k| < \infty$, then $\mathcal{O}_K/\pi^r\mathcal{O}_K$ is finite for all $r \geq 1$. So

$$\mathcal{O}_K \cong \lim_{\to} \mathcal{O}_K/\pi^r\mathcal{O}_K \tag{9.13}$$

is a profinite group, and hence compact. Then since $\mathbb{P}^n(K)$ is the union of the standard open affines, it is compact for the π-adic topology (as the affines are themselves compact).

Then $E(K) \subset \mathbb{P}^2(K)$ is a closed subset, and hence compact. So $E(K)$ is a compact topological group, so if $E_0(K)$ is open, then it is of finite index.

If $\tilde{E}$ has singular point $(\tilde{x}_0, \tilde{y}_0)$, then

$$E(K) \backslash E_0(K) = \{(x, y) \in E(K) \mid v(x - x_0) \geq 1, v(y - y_0) \geq 1\}. \tag{9.14}$$

This is a closed set, so $E_0(K)$ is open. □

Definition 9.13. Set $c_K(E) = [E(K) : E_0(K)]$, this is called the *Tamagawa number*.

If we have good reduction, then $c_K(E) = 1$. On sheet 3, we will show the converse is false.

Remark 9.14. It can be shown that if E has split multiplicative reduction, then $c_K(E) = v(\Delta)$. Otherwise, $c_K(E) \leq 4$. The proofs of these facts work with the minimal Weierstrass equation.

Summing up all the results up to this point, we deduce the following.

Theorem 9.15. *If $[K : \mathbb{Q}_p] < \infty$, then $E(K)$ contains a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.*

We next recall some facts about local fields. Let L/K be p-adic fields with $[L : K] = n$, with residue fields k_L/k of degree $[k_L : k] = f$. If $x \in K^\times$, we have that $v_L(x) = ev_K(x)$. This gives a commutative diagram

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

We have that $[L:K] = ef$, and if L/K is Galois, then we have a reduction

$$\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(k_L/k) \tag{9.15}$$

with kernel $I(L/K)$ of size e. We have an exact sequence.

$$1 \to I(L/K) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k) \to 1 \tag{9.16}$$

If L/K is unramified, then it is Galois, and we have a classification using roots of unity, Frobenius, etc. because L/K is determine pretty much uniquely by the isomorphic extension k_L/k. In particular, if k_m/k is the unique degree m extension of k, then K_m/K is a unique degree m unramified extension of K, where uniqueness is determined in some separable closure.

We have

$$K^{\mathrm{ur}} = \cup_{m \geq 1} K_m \subseteq K^{\mathrm{sep}} \tag{9.17}$$

which is the maximal unramified extension. Unfortunately, K^{ur} is not complete.

Theorem 9.16. *Let K be a p-adic field. Let E/K be an elliptic curve with good reduction. If $P \in E(K)$, and $p \nmid n$, then*

$$K([n]^{-1}P)/K \tag{9.18}$$

is unramified, where $K([n]^{-1}P)$ is the smallest field containing x, y for each $(x,y) \in [n]^{-1}P$. We consider the n-torsion points points $[n]^{-1}P$ over $\overline{K}$.

Proof. For each $m \geq 1$, since E has good reduction, there exists a short exact sequence

$$0 \to E_1(K_m) \to E(K_m) \to \tilde{E}(k_m) \to 0. \tag{9.19}$$

Taking the union over all m (we avoid completing K^{ur} this way) gives a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_1(K^{\mathrm{ur}}) & \longrightarrow & E(K^{\mathrm{ur}}) & \longrightarrow & \tilde{E}(\overline{k}) & \longrightarrow & 0 \\ & & \big\downarrow{\scriptstyle \cdot n} & & \big\downarrow{\scriptstyle \cdot n} & & \big\downarrow{\scriptstyle \cdot n} & & \\ 0 & \longrightarrow & E_1(K^{\mathrm{ur}}) & \longrightarrow & E(K^{\mathrm{ur}}) & \longrightarrow & \tilde{E}(\overline{k}) & \longrightarrow & 0 \end{array}$$

The first vertical arrow is an isomorphism by Corollary 8.15 because $n \in \mathcal{O}_{K^{\mathrm{ur}}}^\times$, as $n \in \mathcal{O}_{K^m}^\times$ for m large, because $p \nmid n$.

The last vertical arrow is a nonconstant morphism of smooth projective curves, so it is surjective. The kernel is $(\mathbb{Z}/n\mathbb{Z})^2$ by Theorem 6.10 because $p \nmid n$. Thus by the snake lemma, we have that the middle term is surjective and the kernel is $(\mathbb{Z}/n\mathbb{Z})^2$. Thus we have an exact sequence

$$0 \to (\mathbb{Z}/n\mathbb{Z})^2 \to E(K^{\mathrm{ur}}) \to E(K^{\mathrm{ur}}) \to 0 \tag{9.20}$$

Therefore if $P \in E(K)$, then there exists $Q \in E(K^{\mathrm{ur}})$ such that $[n]Q = P$ and by the group law we have that

$$[n]^{-1}P = \{Q + T \mid T \in E[n] = E[K^{\mathrm{ur}}](n)\} \tag{9.21}$$

so the extension is unramified because all the coordinates lie in an unramified extension. □

10 Elliptic curves over number fields I: The torsion subgroup

Let K be a number field, and $\mathfrak{p}$ a prime of K (so a prime ideal of $\mathcal{O}_K$. Then completing at K gives a local field $K_\mathfrak{p}$ with ring of integers $\mathcal{O}_\mathfrak{p}$, and residue field $k_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{p}$. We say that $\mathfrak{p}$ is a prime of *good reduction* for E/K if $E/K_\mathfrak{p}$ has good reduction.

Lemma 10.1. *There exists only finitely many primes of bad reduction, and the all divide $\Delta(E)$.*

Proof. Take a Weierstrass equation for E/K with $a_1, \dots a_6 \in \mathcal{O}_K$. Since E is nonsingular, we have that $\Delta \neq 0$ and $\Delta \in \mathcal{O}_K$. Thus we can factor

$$(\Delta) = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}. \tag{10.1}$$

If $\mathfrak{p} \nmid \Delta$, then $v_\mathfrak{p}(\Delta) = 0$, so our Weierstrass equation is minimal over $K_\mathfrak{p}$ and E has good reduction at $\mathfrak{p}$. □

Note that the converse is not true: there could be primes dividing the discriminant which have good reduction. The problem is $\mathcal{O}_K$ might not be a PID, so you can't get minimality at all the different places. But if $\mathcal{O}_K$ is a PID, you can.

Jack notes that you should be able to do this if you work with two different Weierstrass equations, which feels right. This is sort of the result that any ideal in a Dedekind domain can be generated by 2 elements.

Definition 10.2. Let A be a finitely generated abelian group. Then $A \cong T \times \mathbb{Z}^r$, where T is the finite torsion group, and r is the *rank* of A.

Lemma 10.3. *Let $E(K)_{\text{tors}}$ be the torsion subgroup of E. Then $E(K)_{\text{tors}}$ is finite.*

Proof. For all primes p, $E(K_\mathfrak{p})$ has a subgroup A of finite index isomorphic to $(\mathcal{O}_\mathfrak{p}, +)$. Since A is torsion free, we have an inclusion of finite groups

$$E(K)_{\text{tors}} \subseteq E(K_\mathfrak{p})_{\text{tors}} \subseteq E(K)/A \tag{10.2}$$

so $E(K)_{\text{tors}}$ is finite. □

If we take $\mathfrak{p}$ a prime of good reduction, we can determine $E(K)_{\text{tors}}$ explicitly.

Lemma 10.4. *Let $\mathfrak{p}$ be a prime of good reduction for E/K, and let $\mathfrak{p} \nmid n$. Then reduction mod $\mathfrak{p}$ gives an injective group homomorphism*

$$E(K)[n] \hookrightarrow \tilde{E}(k_\mathfrak{p}) \tag{10.3}$$

Proof. By Proposition 9.11, $E(K_\mathfrak{p}) \to \tilde{E}(k_\mathfrak{p})$ is a group homomorphism with kernel $E_1(K_\mathfrak{p})$. But since $\mathfrak{p} \nmid n$, by Corollary 8.15, $E_1(K_\mathfrak{p})$ has no n-torsion because $\times n$ is an isomorphism. Thus we have injections

$$E(K)[n] \hookrightarrow E(K_\mathfrak{p})[n] \hookrightarrow E(K_\mathfrak{p})/E_1(K_\mathfrak{p}) \cong \tilde{E}(k_\mathfrak{p}) \tag{10.4}$$

as desired. □

Example 10.5. Let $E/\mathbb{Q}$ have equation $y^2 + y = x^3 - x^2$, $\Delta = -11$. So E has good reduction at $p \neq 11$, and we can calculate

p	2	3	5	7	11	13
$\tilde{E}(\mathbb{F}_p)$	5	5	5	5	?	10

and Lemma 10.4 gives that $\#E(\mathbb{Q})_{\text{tors}}|5$, and in fact the point $(0,0)$ has nontrivial 5-torsion, so $E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/5\mathbb{Z}$.

Example 10.6. Let $E/\mathbb{Q}$ has equation $y^2 + y = x^3 + x^2$, $\Delta = -43$. So we have good reduction at $p \neq 43$. We calculate

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

and thus the torsion is trivial. Thus $P = (0,0)$ must be a point of infinite order, so $\#E(\mathbb{Q}) = \infty$, so we have found an elliptic curve with infinitely many rational points.

Example 10.7. Let E_D be the congruent number elliptic curve given by $y^2 = x^3 - D^2x = f(x)$, and let $D \in \mathbb{Z}$ be squarefree. Then $\Delta = 2^6D^6$, and if $p \nmid 2D$ (so we have good reduction), then

$$\#\tilde{E}_D(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} \left(\left(\frac{f(x)}{p} \right) + 1 \right) \tag{10.5}$$

where $\left(\frac{\bullet}{\bullet}\right)$ is the Legendre symbol. If $p \equiv 3 \mod 4$, then since f is odd, $\#\tilde{E}_D(\mathbb{F}_p) = p + 1$ since $\left(\frac{-1}{p}\right) = -1$. We have that $E_D(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$, so if $m = \#E_D(\mathbb{Q})_{\text{tors}}$, then $4|m|p+1$ for all sufficiently large primes p (for all $p \nmid 2mD$). Then $m = 4$ by the PNTAP.

Thus $\operatorname{rank} E_D(\mathbb{Q}) \geq 1$ if and only if $\exists x, y \in \mathbb{Q}$ with $y \neq 0$ such that $y^2 = x^3 - D^2x$ as in this case $E_D(\mathbb{Q})$ has a point which is not 2-torsion, so it must have infinite order. Further, this is the case if and only if D is a congruent number (see Lecture 1).

Lemma 10.8. *Let $E/\mathbb{Q}$ be given by a Weierstrass equation with $a_1, \ldots, a_6 \in \mathbb{Z}$. Suppose $0 \neq T = (x,y) \in E(\mathbb{Q})_{\text{tors}}$. Then*

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

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

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

$$\widehat{E}(p^r\mathbb{Z}_p) = \{(x,y) \in \mathbb{Q}_p | v_p(x) \leq -2r, v_p(y) \leq -3r\} \cup \{0_E\} \tag{10.6}$$

Theorem 9.4 implies that $\widehat{E}(p^r\mathbb{Z}_p) \cong (\mathbb{Z}_p, +)$ if $r > \frac{1}{p-1}$ since the ramification index is 0 because we are working over $\mathbb{Q}$. Then if $p = 2$, we can take $r = 2$, otherwise we can take $r = 1$. Thus if $0 \neq T = (x,y) \in E(\mathbb{Q})_{\text{tors}}$, then $v_2(x) \geq -2, v_2(y) \geq -3$, and $v_p(x), v_p(y) \geq 0$ if $p > 2$. This prove (i).

For (ii), if $T \in \widehat{E}(2\mathbb{Z}_2)$, then we must have $v_2(x) = -2, v_2(y) = -3$ exactly by (i). 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 that $2T = 0$. Also, since $(x,y) = T = -T = (x, -y - a_1x - a_3)$, we have that $y - (-y - a_1x - a_3) = 2y + a_1x + a_3 = 0$, so $8y + a_1(4x) + 4a_3 = 0$, so a_1 is odd. So if $2T \neq 0$ or a_1 is even, then $T \notin \widehat{E}(2\mathbb{Z}_2)$, so $x, y \in \mathbb{Z}$. □

Example 10.9. Part (i) is not completely vacuous. Take $y^2 + xy = x^3 + 4x + 1$. Then $(-1/4, 1/8) \in E(\mathbb{Q})[2]$, and we can see that a_1 is odd and the point has 2-torsion.

Theorem 10.10 (Lutz-Nagell)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with equation $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$. 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. By Lemma 10.8, $x, y \in \mathbb{Z}$. If $2T = 0$, then $y = 0$. Otherwise $2T \neq 0$ so $2T = (x_2, y_2) \in E(\mathbb{Q})_{\text{tors}}$. By Lemma 10.8, $x_2, y_2 \in \mathbb{Z}$.

Since $x_2 = \left(\frac{f'(x)}{2y}\right)^2 - 2x$, we have that $y | f'(x)$ since $x_2 \in \mathbb{Z}$. Since E is nonsingular, $f(x)$ and $f'(x)$ are coprime, so $f(x), f'(x)^2$ are coprime. Pulling a rabbit out a hat, we have the identity

$$(3x^2 + 4a)f'(x)^2 - 27(x^3 + ax - b)f(x) = 4a^3 + 27b^2. \tag{10.7}$$

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

Remark 10.11. Mazur showed that if $E/\mathbb{Q}$ is an elliptic curve, then

$$E(\mathbb{Q})_{\text{tors}} \in \{\mathbb{Z}/n\mathbb{Z} \mid 1 \leq n \leq 12, n \neq 11\} \cup \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \mid 1 \leq n \leq 4\} \tag{10.8}$$

and in fact, all of these torsion subgroups occur.

11 Kummer theory

K a field, $\operatorname{char} K \nmid n$. Let μ_n be the group of nth roots of unity and assume $\mu_n \subset K$.

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

Proof. Since $\mu_n \subset K$, L/K is normal. Since $\operatorname{char} K \nmid n$, L/K is separable. Thus L/K is Galois.

Define the Kummer pairing (a bilinear form)

$$\begin{aligned} \langle \cdot, \cdot, \rangle : \operatorname{Gal}(L/K) \times \Delta &\to \mu_n \\ (\sigma, x) &\mapsto \sigma(\sqrt[n]{x})/\sqrt[n]{x} \end{aligned} \tag{11.1}$$

First we will show it is well-defined. If $\alpha, \beta \in L$ with $\alpha^n = \beta^n = x$, then $(\alpha/\beta)^n = 1$, so $\alpha/\beta \in \mu_n \subset K$, so $\sigma(\alpha/\beta) = \alpha/\beta$, so $\sigma(\alpha)/\alpha = \sigma(\beta)/\beta$.

To show it is bilinear, we have

$$\begin{aligned} \langle \sigma\tau, x \rangle &= \frac{\sigma\tau(\sqrt[n]{x})}{\sqrt[n]{x}} \\ &= \frac{\sigma\tau\sqrt[n]{x}}{\tau\sqrt[n]{x}} \cdot \frac{\tau\sqrt[n]{x}}{\sqrt[n]{x}} \\ &= \langle \sigma, x \rangle \langle \tau, x \rangle \end{aligned} \tag{11.2}$$

since $(\tau\sqrt[n]{x})^n = x$, so $\tau\sqrt[n]{x}$ is also an nth root of x. We can also calculate that $\langle \sigma, xy \rangle = \langle \sigma, x \rangle \langle \sigma, y \rangle$.

To show it is nondegenerate, let $\sigma \in \operatorname{Gal}(L/K)$. If $\langle \sigma, x \rangle = 1$ for all $x \in \Delta$, then $\sigma\sqrt[n]{\alpha} = \sqrt[n]{\alpha}$ for all $x \in \Delta$, so $\sigma = \mathrm{id}$.

If $x \in K^\times$ and $\langle \sigma, x \rangle = 1$ for all $\sigma \in \operatorname{Gal}(L/K)$, then $\sigma\sqrt[n]{\alpha} = \sqrt[n]{\alpha}$ for all $\sigma \in \operatorname{Gal}(L/K)$, so $\sqrt[n]{x} \in K$, so $x \in (K^\times)^n$ is the identity in Δ. Then we get injective group homomorphisms

$$\operatorname{Gal}(L/K) \hookrightarrow \operatorname{Hom}(\Delta, \mu_n) \tag{11.3}$$

$$\Delta \hookrightarrow \operatorname{Hom}(\operatorname{Gal}(L/K), \mu_n). \tag{11.4}$$

We want to show that these are isomorphisms. By (11.3), $\mathrm{Gal}(L/K)$ is abelian and of exponent dividing n.

Recall that the exponent of an abelian group G is the least common multiple of the orders of all of its elements. It is a fact that if G is a finite abelian group of exponent dividing n, then $\mathrm{Hom}(G, \mu_n) \cong G$, although this isomorphism is non-canonical. Thus we have injections $\mathrm{Gal}(L/K) \to \Delta$ and $\Delta \to \mathrm{Gal}(L/K)$, so these are isomorphisms. □

Example 11.2. We have that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3$.

Theorem 11.3 (Main theorem of Kummer theory)**.** *There is a bijection*

$$\{\textit{finite subgroups } \Delta \subset K^\times/(K^\times)^n\} \leftrightarrow \{\textit{finite abelian extensions } L/K \textit{ of exponent dividing } n\} \tag{11.5}$$

where we send $\Delta \mapsto K(\sqrt[n]{\Delta})$ *with inverse* $L/K \mapsto \left((L^\times)^n \cap K^\times\right)/(K^\times)^n$.

Proof. Let $\Delta \subset K^\times/(K^\times)^n$ be a finite subgroup. Let $L = K(\sqrt[n]{\Delta})$ and $\Delta' = \left((L^\times)^n \cap K^\times\right)/(K^\times)^n$. Clearly, $\Delta \subset \Delta'$, so $K(\sqrt[n]{\Delta}) \subset K(\sqrt[n]{\Delta'}) \subset L$, so $K(\sqrt[n]{\Delta}) = K(\sqrt[n]{\Delta'})$ by Lemma 11.1, so $\Delta = \Delta'$.

Now let L/K be a finite abelian extension of exponent dividing n. Let $\Delta = \left((L^\times)^n \cap K^\times\right)/(K^\times)^n$. Then $K(\sqrt[n]{\Delta}) \subseteq L$, and we want to show equality. Let $G = \mathrm{Gal}(L/K)$. Then the Kummer pairing gives an injection $\Delta \hookrightarrow \mathrm{Hom}(G, \mu_n)$, and we want to show that it is surjective.

Suppose that it is. By Lemma 11.1, we have that $[K(\sqrt[n]{\Delta}) : K] = |\Delta| = |G| = [L : K]$, so since $K(\sqrt[n]{\Delta}) \subseteq L$, it follows that $K(\sqrt[n]{\Delta}) = L$ so we are done.

Now to show that it is surjective. Let $\chi : G \to \mu_n$ be a group homomorphism, so $\chi \in \mathrm{Hom}(G, \mu_n)$. Then since elements of the Galois group are linearly independent, we have that there exists $a \in L^\times$ such that

$$y \coloneqq \sum_{\tau \in G} \chi(\tau)^{-1}\tau(a) \neq 0. \tag{11.6}$$

Let $\sigma \in G$. Then

$$\sigma(y) = \chi(\sigma) \cdot y \tag{11.7}$$

since $\mu_n \subset K$. Thus $\sigma(y^n) = y^n$, so $x \coloneqq y^n \in K^\times$, so $x(K^\times)^n \in \Delta$. We have that

$$\chi : \sigma \to \frac{\sigma(y)}{y} = \frac{\sigma\sqrt[n]{x}}{\sqrt[n]{x}}, \tag{11.8}$$

so the injection $\Delta \hookrightarrow \mathrm{Hom}(G, \mu_n)$ sends $x \mapsto \chi$ by the definition of the Kummer pairing. □

Proposition 11.4. *Let K be a number field, and $\mu_n \subset K$. Let S be a finite set of primes of K. There are only finitely many extension L/K such that*

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

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

Proof. By Theorem 11.3, $L = K(\sqrt[n]{\Delta})$ for some $\Delta \subset K^\times/(K^\times)^n$ a finite subgroup. Let $\mathfrak{p}$ be a prime of K Then $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, and if $x \in K^\times$ represents an element of Δ, then

$$n v_{\mathfrak{P}_i}(\sqrt[n]{x}) = v_{\mathfrak{P}_i}(x) = e_i v_{\mathfrak{p}}(x). \tag{11.9}$$

If $\mathfrak{p} \notin S$, then $e_i = 1$ for all i, so

$$v_{\mathfrak{p}}(x) \equiv 0 \mod n \tag{11.10}$$

Then $\Delta \subset K(S,n)$, where

$$K(S,n) = \{x \in K^\times/(K^\times)^n \mid v_{\mathfrak{p}}(x) \equiv 0 \mod n \ \forall \mathfrak{p} \notin S\} \tag{11.11}$$

So if $K(S,n)$ is finite, we are done. We prove this in the next lemma. □

Lemma 11.5. *Let*

$$K(S,n) = \{x \in K^\times/(K^\times)^n \mid v_{\mathfrak{p}}(x) \equiv 0 \mod n \ \forall \mathfrak{p} \notin S\} \tag{11.12}$$

Then $K(S,n)$ is finite.

Proof. The map

$$\begin{aligned} K(S,n) &\to (\mathbb{Z}/n\mathbb{Z})^{|S|} \\ x &\mapsto (v_{\mathfrak{p}}(x) \mod n)_{\mathfrak{p}\in S} \end{aligned} \tag{11.13}$$

is a group homomorphism because $v_{\mathfrak{p}}$ is a group homomorphism, and the kernel is $K(\emptyset,n)$. Since $|S| < \infty$, it suffices to prove the lemma with $S = \emptyset$.

If $x \in K^\times$ represents an element of $K(\emptyset,n)$, then $(x) = \mathfrak{a}^n$ for some fractional ideal $\mathfrak{a}$, because $v_{\mathfrak{p}}(x) \equiv 0 \mod n$ for all $\mathfrak{p}$. There is a short exact sequence

$$\begin{aligned} 0 \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n \to K(\emptyset) \to \mathrm{Cl}_k[n] \to 0 \\ x(K^\times)^n \mapsto [\mathfrak{a}] \end{aligned} \tag{11.14}$$

Since $|\mathrm{Cl}_k| < \infty$ and $\mathcal{O}_K^\times$ is a finitely generated abelian group by Dirichlet's unit theorem, $K(\emptyset,n)$ is finite. □

12 Elliptic curves over number fields II: The Weak Mordell-Weil Theorem

Lemma 12.1. *Let E/K be an elliptic curve and L/K a finite Galois extension. The natural map*

$$\begin{aligned} E(K)/nE(K) &\to E(L)/nE(L) \\ P + nE(K) &\mapsto P + nE(L) \end{aligned} \tag{12.1}$$

has finite kernel.

Proof. For each element of the kernel, pick a coset representative $P \in E(K)$, and then $P \in nE(L)$ so there exists $Q \in E(L)$ such that $nQ = P$. For any $\sigma \in \mathrm{Gal}(L/K)$, we have that

$$n(\sigma Q - Q) = \sigma P - P = 0, \tag{12.2}$$

so $\sigma Q - Q \in E[n]$. Since $\mathrm{Gal}(L/K)$ and $E[n]$ are finite, the set of maps from $\mathrm{Gal}(L/K)$ to $E[n]$ is finite. We can define a map from our kernel to this set of maps by

$$P + nE(K) \mapsto (\sigma \mapsto \sigma Q - Q). \tag{12.3}$$

If we show that this map is injective, then the kernel is finite. Suppose $P_1, P_2 \in E(K)$, and $P_i = nQ_i$ for $Q_i \in E(L)$. Then if $\sigma(Q_1) - Q_1 = \sigma Q_2 - Q_2$ or all $\sigma \in \mathrm{Gal}(L/K)$, then $\sigma(Q_1 - Q_2) = Q_1 - Q_2$ so $Q_1 - Q_2 \in E(K)$, so $P_1 - P_2 \in nE(K)$ so $P_1 + nE(K) = P_2 + nE(K)$. □

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. So WLOG we may assume $\mu_n \subset K$ and $E[n] \subset E(K)$. Let

$$S = \{\mathfrak{p} | n\} \cup \{\text{primes of bad reduction for } E/K\}. \tag{12.4}$$

For each $P \in E(K)$, the extension $K([n]^{-1}P/K)$ is unramified outside S by Theorem 9.16. Since $\mathrm{Gal}(\overline{K}/K)$ acts on $[n]^{-1}P$, it follows that $\mathrm{Gal}(\overline{K}/K([n]^{-1}P))$ is a normal subgroup of $\mathrm{Gal}(\overline{K}/K)$ and hence $K([n]^{-1}P)/K$ is a Galois extension. Let $Q \in [n]^{-1}P$. Since $E[n] \subset E(K)$, $K(Q) = K([n]^{-1}P)$. We have a map

$$\begin{aligned} \mathrm{Gal}(K(Q)/K) &\to E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2 \\ \sigma &\mapsto \sigma Q - Q \end{aligned} \tag{12.5}$$

This is a group homomorphism, as

$$\begin{aligned} \sigma\tau Q - Q &= \sigma(\tau Q - Q) + (\sigma Q - Q) \\ &= (\tau Q - Q) + (\sigma Q - Q) \end{aligned} \tag{12.6}$$

because $\tau Q - Q \in E[n] \subset E(K)$. It is injective because if $\sigma Q = Q$, then σ fixes $K(Q)$, so $\sigma = 1$.

So $K(Q)/K$ is an abelian extension of exponent dividing n, unramified outside S.

Proposition 11.4 shows that as we vary $P \in E(K)$, there are only finitely many possibilities for $K(Q)$. Let L be the compositum of all such extensions $K(Q)/K$. 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 12.3. If $k = \mathbb{R}, \mathbb{C}$, or $[K : \mathbb{Q}_p] < \infty$, then $E(K)/nE(K)$ is finite yet $E(K)$ is uncountable, so not finitely generated.

Remark 12.4. If K is a number field, then there exists a quadratic form, the *canonical height* $\hat{h} : E(K) \to \mathbb{R}_{\geq 0}$ with the property that for any $B \geq 0$, $\{P \in E(K) | \hat{h}(P) \leq B\}$ is finite.

We will study the height later and prove these properties, but first assume them and prove the Mordell-Weil Theorem.

Theorem 12.5 (Mordell-Weil Theorem)**.** *Let K be a number field, E/K an elliptic curve. Then $E(K)$ is finitely generated.*

Proof. Fix an integer $n \geq 2$. Then the weak Mordell-Weil theorem implies that $|E(K)/nE(K)| < \infty$. Pick coset representatives $P_1, \ldots, P_m$. Let $\Sigma = \{P \in E(K) \mid \hat{h}(P) \leq \max_i \hat{h}(P_i)\}$ which is finite. We claim that Σ generates $E(K)$. If note, then there exists $P \in E(K) \backslash \langle \Sigma \rangle$ of minimal height (the things with smaller height then a given P are a finite set). Then $P = P_i + nQ$ for

$1 \leq i \leq m$, $Q \in E(K)$. Note that $Q \in E(K)\backslash\langle\Sigma\rangle$. But the minimal choice of P and the fact that $\hat{h}$ is a quadratic form gives

$$\begin{aligned} 4\hat{h}(P) &\leq 4\hat{h}(Q) \\ &\leq n^2\hat{h}(Q) \\ &= \hat{h}(nQ) \\ &= \hat{h}(P - P_i) \\ &\leq \hat{h}(P - P_i) + \hat{h}(P + P_i) \\ &= 2\hat{h}(P) + 2\hat{h}(P_i) \end{aligned} \tag{12.7}$$

which is a contradiction. □

13 Heights

For simplicity, $K = \mathbb{Q}$. These results generalize to K, but let's not worry for now. We will remark about this later.

For a given $P \in \mathbb{P}^N(\mathbb{Q})$, we can write $P = (a_0 : a_1 : \cdots : a_n)$ with $a_0, \ldots, a_n \in \mathbb{Z}$ and $\gcd(a_0, \ldots, a_n) = 1$. We define the height of P to be

$$H(P) = \max_{0 \leq i \leq n} |a_i| \tag{13.1}$$

Lemma 13.1. *Let $f_1, f_2 \in \mathbb{Q}[x_1, x_2]$ be coprime homogeneous polynomials of degree d. Let*

$$\begin{aligned} F : \mathbb{P}^1 &\to \mathbb{P}^2 \\ (x_1 : x_2) &\mapsto (f_1(x_1, x_2) : f_2(x_1, x_2)) \end{aligned} \tag{13.2}$$

Then there exists $c_1, c_2 > 0$ depending on f_1, f_2, such that for all $P \in \mathbb{P}^1(\mathbb{Q})$,

$$c_1 H(P)^d \leq H(F(P)) \leq c_2 H(P)^d \tag{13.3}$$

Proof. WLOG we may assume $f_1, f_2 \in \mathbb{Z}[x_1, x_2]$ because $H(NF(P)) = H(F(P))$.

For the upper bound, write $P = (a_1 : a_2)$, $a_1, a_2 \in \mathbb{Z}$ with $(a_1, a_2) = 1$. Then

$$H(F(P)) \leq \max(|f_1(a_1, a_2)|, |f_2(a_1, a_2)|) \leq c_2 \max(|a_1|^d, |a_2|^d) \tag{13.4}$$

where c_2 is the sums of the absolute values of the coefficients of f_i. This is pretty much just the triangle inequality.

For the lower bound, we need to work harder. We claim there exists $g_{ij} \in \mathbb{Z}[x_1, x_2]$ homogeneous of degree $d - 1$ and $\kappa \in \mathbb{Z}_{>0}$ such that

$$\sum_{j=1}^{2} g_{ij} f_j = \kappa x_i^{2d-1} \tag{13.5}$$

for $i = 1, 2$. Indeed, applying the Euclidean algorithm to $f_1(x, 1)$ and $f_2(x, 1)$ gives $r, s \in \mathbb{Q}[x]$ of degree $d - 1$ such that $r(x)f_1(x, 1) + s(x)f_2(x, 1) = 1$. Homogenizing and clearing denominators

gives (13.5) for $i = 2$ (just multiply through by some κ_2. Repeat this with $f_i(1, x)$ to get (13.5) for $i = 1$, and then multiply out and set $\kappa = \text{lcm}[\kappa_1, \kappa_2]$ to get the full result.

Write $P = (a_1 : a_2)$, $a_1, a_2 \in \mathbb{Z}$ coprime. Then (13.5) implies that

$$\sum_{j=1}^{2} g_{ij}(a_1, a_2) f_j(a_1, a_2) = \kappa a_i^{2d-1}. \tag{13.6}$$

So $\gcd(f_1(a_1, a_2), f_2(a_1, a_2)$ divides $\gcd(\kappa a_1^{2d-1}, \kappa a_2^{2d-1})$ so it divides κ. Then

$$|\kappa a_i^{2d-1}| \leq \max_{j=1,2} |f_j(a_1, a_2)| \sum_{j=1}^{2} |g_{ij}(a_1, a_2)| \tag{13.7}$$

and the first term is less than $\kappa H(F(P))$ and second is less than $\gamma_i H(P)^{d-1}$ where γ is the sum of the absolute value of the coefficients of the g_{ij}s. So

$$\kappa H(P)^{2d-1} \leq \kappa H(F(P)) \cdot \max(\gamma_1, \gamma_2) H(P)^{d-1} \tag{13.8}$$

so

$$c_1 H(P)^d = \frac{1}{\max(\gamma_1, \gamma_2)} H(P)^d \leq H(F(P)). \tag{13.9}$$

□

Definition 13.2. For $x \in \mathbb{Q}$, let $H(x) = H((x : 1)) = \max(|a|, |b|)$, where $x = a/b$ with $(a, b) = 1$.

Let $E/\mathbb{Q}$ be an elliptic curve with equation $y^2 = x^3 + ax + b$.

Definition 13.3. The *height* $H : E(\mathbb{Q}) \to \mathbb{R}_{\geq 1}$ of a point P is $H(x)$ is $P = (x, y)$ or 1 if $P = 0_E$.

The *logarithmic height* $h : E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ is $h(P) = \log H(P)$.

Lemma 13.4. *Let E, E' be elliptic curves over $\mathbb{Q}$, and $\phi : E \to E'$ an isogeny defined over $\mathbb{Q}$. Then there exists $c > 0$ depending on E, E', ϕ such that for all $P \in E(\mathbb{Q})$*

$$|h(\phi(P)) - (\deg \phi) h(P)| \leq c. \tag{13.10}$$

Proof. Recall by Lemma 5.6 we have a commuting diagram

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ \downarrow{\scriptstyle x} & & \downarrow{\scriptstyle x} \\ \mathbb{P}^1 & \xrightarrow{\xi} & \mathbb{P}^1 \end{array}$$

such that $\deg \phi = \deg \xi = d$. Then by Lemma 13.1, there exists c_1, c_2 such that $c_1 H(P)^d \leq H(\phi(P)) \leq c_2 H(P)^d$ for all $P \in E(\mathbb{Q})$. Taking logs gives

$$|h(\phi(P)) - dh(P)| \leq \max(\log c_2, -\log c_2) = c. \tag{13.11}$$

□

Example 13.5. We have that $|h(2P) - 4h(P)| \leq c$ for all $P \in E(\mathbb{Q})$.

Definition 13.6. The *canonical height* is

$$\hat{h}(P) = \lim_{n\to\infty} \frac{1}{4^n} h(2^n P) \tag{13.12}$$

We check that this limit converges by checking that it is Cauchy. We have that

$$\left| \frac{1}{4^m} h(2^m P) - \frac{1}{4^n} h(2^n P) \right| \leq \frac{1}{3 \cdot 4^n} \to 0 \tag{13.13}$$

so $\hat{h}(P)$ exists.

Lemma 13.7. *For all $P \in E(\mathbb{Q})$, $|h(P) - \hat{h}(P)|$ is bounded uniformly.*

Proof. Put $n = 0$ in the above calculation. □

Lemma 13.8. *For any $B > 0$, we have that $\#\{P \in E(\mathbb{Q}) \mid \hat{h}(P) \leq B\} < \infty$.*

Proof. If $\hat{h}(P)$ is bounded, then $h(P)$ is bounded by Lemma 13.7. So there are only finitely many choices of x-coordinate, so only finitely many choices for (x, y). □

Lemma 13.9. *Let $\phi : E \to E'$ be an isogeny defined over $\mathbb{Q}$. Then for all $P \in E(\mathbb{Q})$,*

$$\hat{h}(\phi(P)) = (\deg \phi)\hat{h}(P). \tag{13.14}$$

Proof. By Lemma 13.4, there exists $c > 0$ such that

$$|h(\phi(P)) - (\deg \phi)h(P)| < c \tag{13.15}$$

for all $P \in E(\mathbb{Q})$. Replacing P by $2^n P$, dividing and taking $n \to \infty$ gives the lemma. □

Corollary 13.10. *$\hat{h}$ is independent of choice of Weierstrass equation.*

Proof. Change Weierstrass equation is an isomorphism. □

Corollary 13.11. *For all $P \in E(\mathbb{Q})$ and all $n \in \mathbb{Z}$, $\hat{h}(nP) = n^2 \hat{h}(P)$.*

Proof. Trivial. □

Lemma 13.12. *Let $E/\mathbb{Q}$ be an elliptic curve. Then there exists $c > 0$ depending on E such that for all $P, Q \in E(\mathbb{Q})$ with $P, Q, P + Q, P - Q \neq 0$,*

$$H(P + Q)H(P - Q) \leq cH(P)^2 H(Q)^2. \tag{13.16}$$

Proof. The above result holds even if some of $P, Q, P + Q, P - Q = 0$, but we leave this as an exercise.

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 $x_1, \ldots, x_4$. By Lemma 5.11, there exists W_0, W_1, W_2 of degree less than 2 in x_1 and x_2 separately such that

$$(1 : x_3 + x_4 : x_3 x_4) = (W_0 : W_1 : W_2). \tag{13.17}$$

Write $x_i = r_i/s_i$, with $r_i, s_i \in \mathbb{Z}$ coprime. Then

$$(s_3 s_4 : r_3 s_4 + r_4 s_3 : r_3 r_4) = (\_\_ : \_\_ : \_\_) \tag{13.18}$$

where the LHS are all coprime and the RHS are the homogenizations of the W_is. In particular, after homogenizing, the degree of W_i in r_j plus the degree of W_i in s_j is 2. We have that

$$\begin{aligned} H(P+Q)H(P-Q) &= \max(|r_3|, |s_3|) \max(|r_4|, |s_4|) \\ &\leq c \max(|s_3 s_4|, |r_3 s_4 + r_4 s_3|, |r_3 r_4|) \\ &\leq c \max(\_\_, \_\_, \_\_) \\ &\leq c \max(|r_1|^2, |s_1|^2) \max(|r_2|^2, |s_2|^2) \\ &\leq c H(P)^2 H(Q)^2 \end{aligned} \tag{13.19}$$

for some c depending on E. □

Theorem 13.13. *$\hat{h}$ is a quadratic form.*

Proof. By Lemma 13.12 and the fact that $|h(2P) - 4h(P)|$ is bounded, we have that there exists $c \in \mathbb{R}$ such that

$$h(P+Q) + h(P-Q) \leq 2h(P) + 2h(Q) + c \tag{13.20}$$

for all $P, Q \in E(\mathbb{Q})$. Replacing P, Q by $2^n P, 2^n Q$, dividing and taking the limit gives

$$\hat{h}(P+Q) + \hat{h}(P-Q) \leq 2\hat{h}(P) + 2\hat{h}(Q). \tag{13.21}$$

Replacing P, Q by $P+Q, P-Q$ and using that $\hat{h}(2P) = 4\hat{h}(P)$ gives the reverse inequality. □

Note that Lemma 13.1 was essential in all this.

Remark 13.14. For K a number field and $P = (a_0 : a_1 : \cdots : a_n) \in \mathbb{P}^n(K)$, define

$$H(P) = \prod_v \max_{0 \leq i \leq n} |a_i|_v \tag{13.22}$$

where the product is over all places v, and the absolute values are normalized so that

$$\prod_v |\lambda|_v = 1 \tag{13.23}$$

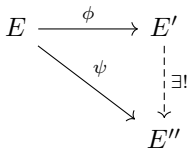
for all $\lambda \in K^\times$.

All results in this section generalize to K, with the height function given as above.

14 Dual isogenies and the Weil pairing

Let K be a perfect field, and E/K an elliptic curve.

Proposition 14.1. *Let $\Phi \subset E(\overline{K})$ be a finite subgroup stable under the action of $\mathrm{Gal}(\overline{K}/K)$. Then there exists E'/K and a separable isogeny $\phi : E \to E'$ defined over K with kernel Φ such that for every isogeny $\psi : E \to E''$ with $\Phi \subset \ker \psi$, ψ factors uniquely through ϕ. In diagram form:*



Proof. This was omitted in class, see Silverman Prop III.4.12. □

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

Proof. If ϕ is separable, let $\Phi = \ker \phi$, $|\ker \phi| = n$. Then $\ker \phi \subset E[n]$, and we can apply Proposition 14.1 with $\psi = [n]$.

If ϕ is inseparable, see Silverman Theorem III.6.1.

For uniqueness, suppose $\psi_1\phi = \psi_2\phi = [n]$. Then ψ_1 and ψ_2 agree on $\operatorname{im}\phi$, and since ϕ is surjective, $\psi_1 = \psi_2$. □

Remark 14.3.

1. In general, given an isogeny $\phi : E \to E'$ and isogenies $\psi_1, \psi_2 : E' \to E''$ such that $\psi_1 \circ \phi = \psi_2 \circ \phi$, we have that $\psi_1 = \psi_2$ by the same reasoning as above.
2. Write $E_1 \sim E_2$ if E_1 and E_2 are isogenous. The previous proposition verifies that $\sim$ is an equivalence relation by showing it is symmetric.
3. We have that $\deg[n] = n^2$, so $\widehat{[n]} = [n]$ and $\deg \widehat{\phi} = \deg \phi$.
4. We have that $\phi\widehat{\phi}\phi = \phi[n]_E = [n]_{E'}\phi$, so $\phi\widehat{\phi} = [n]_{E'}$, so $\widehat{\widehat{\phi}} = \phi$.
5. If $E \xrightarrow{\psi} E' \xrightarrow{\phi} E''$, then $\widehat{\phi\psi} = \widehat{\psi}\widehat{\phi}$.
6. If $\phi : E \to E$, then $\phi^2 - [\operatorname{tr}\phi]\phi + [\deg\phi] = 0$, so $([\operatorname{tr}\phi] - \phi)\phi = [\deg\phi]$, so $[\operatorname{tr}\phi] = \phi + \widehat{\phi}$.

Lemma 14.4. *If $\phi, \psi \in \operatorname{Hom}(E, E')$, then $\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}$.*

Proof. If $E = E'$, then $\widehat{\phi} = [\operatorname{tr}\phi] - \phi$, so $\widehat{\phi + \psi} = [\operatorname{tr}(\phi + \psi)] - \phi - \psi = \widehat{\phi} + \widehat{\psi}$.

In general, let $\alpha : E' \to E$ be any isogeny. Then

$$\alpha\widehat{\phi + \alpha}\psi = \widehat{\alpha\psi} + \widehat{\alpha\phi}, \tag{14.1}$$

so $\widehat{\phi + \psi}\widehat{\alpha} = (\widehat{\phi} + \widehat{\psi})\widehat{\alpha}$, so $\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}$. □

Remark 14.5. In Silverman's book, he proves Lemma 14.4 much earlier, and then uses this to show that the degree is a quadratic form.

Here is some notation. Define

$$\begin{aligned} \operatorname{sum} : \operatorname{Div}(E) &\to E \\ \sum n_P(P) &\mapsto \sum n_P P \end{aligned} \tag{14.2}$$

where the LHS is a formal sum of divisors and the RHS is a group element of E. Recall that we have an isomorphism

$$\begin{aligned} \sigma : E &\xrightarrow{\sim} \mathrm{Pic}^0(E) \\ P &\mapsto [(P) - (0_E)] \end{aligned} \tag{14.3}$$

Given $D = \sum n_P[(P) - (0_E)] \in \mathrm{Pic}^0(E)$, we have that $\operatorname{sum} D = \sum n_P P$, and this gets mapped back to D under σ. Thus sum is the inverse of σ, and we have that $\ker \operatorname{sum}$ is the divisors such that $\sum n_P P = 0_E$, so we deduce the following lemma.

Lemma 14.6. *Let $D \in \mathrm{Div}(E)$. Then $D \sim 0$ if and only if both $\deg D = 0$ and $\operatorname{sum} D = 0_E$.*

Now, let $\phi : E \to E'$ be an isogeny of degree n with dual $\widehat{\phi}$. Assume $\operatorname{char} K \nmid n$, so that $\phi, \widehat{\phi}$ are separable. Set $\ker \phi = E[\phi]$ and $\ker \hat{\phi} = E'[\hat{\phi}]$ We define the *Weil pairing*

$$e_\phi : E[\phi] \times E'[\widehat{\phi}] \to \mu_n \tag{14.4}$$

where $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$ is the group of nth roots of unity. Let $T \in E'[\widehat{\phi}]$. Then $nT = 0$, so there exists $f \in \overline{K}(E')^\times$ such that $\mathrm{div}(f) = n(T) - n(0_E)$ by Lemma 14.6. Pick $T_0 \in E(K')$ with $\phi(T_0) = T$, and pull back:

$$\phi^*(T) - \phi^*(0_E) = \sum_{P \in E[\phi]} (P + T_0) - (P). \tag{14.5}$$

By Lemma 14.6, this divisor is principal because

$$\operatorname{sum}(\phi^*(T) - \phi^*(0_E)) = nT_0 = \widehat{\phi}\phi T_0 = \widehat{\phi} T = 0. \tag{14.6}$$

Thus there exists $g \in \overline{K}(E)^\times$ such that $\mathrm{div}(g) = \phi^*(T) - \phi^*(0)$. Now, $\mathrm{div}(\phi^* f) = \phi^*(\mathrm{div}\, f) = n(\phi^*(T) - \phi^*(0)) = \mathrm{div}(g^n)$, so $\phi^* f = c g^n$ for some $c \in \overline{K}^\times$, and we can normalize so that $c = 1$, so $\phi^* f = g^n$. For any $s \in \ker \phi$, we have that $\tau_S^*(\mathrm{div}\, g) = \mathrm{div}\, g$ because

$$\begin{aligned} \tau_S^*(g^n) &= \tau_S^*(\phi^* f) \\ &= (\phi \circ \tau_S)^* f \\ &= \phi^* f = g^n \end{aligned} \tag{14.7}$$

so

$$\begin{aligned} n\tau_S^* \operatorname{div} g &= \tau_S^* \operatorname{div} g^n \\ &= \operatorname{div}(\tau_S^* g^n) \\ &= \operatorname{div} g^n \\ &= n \operatorname{div} g. \end{aligned} \tag{14.8}$$

So $\tau_S^* g = \zeta g$ for some $\zeta \in \overline{K}^\times$, so we have that $\zeta = g(X + S)/g(X)$ for any $X \in E(K)$. But

$$\begin{aligned} \zeta^n &= \frac{g(X+S)^n}{g(X)^n} \\ &= \frac{f \circ \phi(X+S)}{f \circ \phi(X)} \\ &= 1, \end{aligned} \tag{14.9}$$

so $\zeta = \mu_n$. So we define

$$e_\phi(S,T) \coloneqq \frac{g(X+S)}{g(X)}. \tag{14.10}$$

Proposition 14.7. *e_ϕ is linear and nondegenerate.*

Proof. (i) First we show linearity in the first argument:

$$\begin{aligned} e_\phi(S_1+S_2,T) &= \frac{g(X+S_1+S_2)}{g(X+S_1)} \cdot \frac{g(X+S_1)}{g(X)} \\ &= e_\phi(S_1,T)e_\phi(S_2,T). \end{aligned} \tag{14.11}$$

(ii) Next we show linearity in the second argument: Let $T_1, T_2 \in E'[\widehat{\phi}]$. Then there exists f_1, f_2, g_1, g_2 such that

$$\begin{aligned} \operatorname{div}(f_1) &= n(T_1) - n(0), \qquad & \phi^* f_1 &= g_1^n \\ \operatorname{div}(f_2) &= n(T_2) - n(0), \qquad & \phi^* f_2 &= g_2^n \end{aligned} \tag{14.12}$$

as in the construction of the pairing. Then there exists $h \in \overline{K}(E')$ such that

$$\operatorname{div} h = (T_1) + (T_2) - (T_1+T_2) - (0). \tag{14.13}$$

Then put $f = \frac{f_1 f_2}{h^n}$ and $g = \frac{g_1 g_2}{\phi^* h}$. We can check that $\operatorname{div} f = n(T_1+T_2) - n(0)$. So then

$$\phi^* f = \frac{\phi^* f_1 \phi^* f_2}{(\phi^* h)^n} = \left(\frac{g_1 g_2}{\phi^* h}\right)^n = g^n, \tag{14.14}$$

so

$$\begin{aligned} e_\phi(S, T_1+T_2) &= \frac{g(X+S)}{g(X)} \\ &= \frac{g_1(X+S)}{g_1(X)} \cdot \frac{g_2(X+S)}{g_2(X)} \cdot \frac{h(\phi(X))}{h(\phi(X+S))} \\ &= e_\phi(S,T_1)e_\phi(S,T_2) \end{aligned} \tag{14.15}$$

since $S \in E[\phi]$.

(iii) Lastly we will show that e_ϕ is nondegenerate. Fix $T \in E'[\widehat{\phi}]$. Suppose $e_\phi(S,T) = 1$ for all $S \in E[\phi]$. Then $\tau_S^* g = g$ for all $S \in E[\phi]$ since $\frac{g(X+S)}{g(X)} = 1$ for all X, so $g(X+S) = \tau_S^* g(X) = g(X)$ for all X.

We have that $\overline{K}(E)$ is a Galois extension of $\phi^*\overline{K}(E')$ with Galois group $E[\phi]$ as $S \in E[\phi]$ acts on $\overline{K}(E)$ via τ_S^*. Since $\tau_S^* g = g$ for all S, we have that $g \in \phi^*\overline{K}(E')$, so $g = \phi^* h$ for some $h \in \overline{K}(E')$, so $\phi^* f = g^n = \phi^*(h^n)$, so $f = h^n$ because ϕ is surjective, so $\operatorname{div} h = (T) - (0)$, so $(T) - (0)$ is a principal divisor, so $T = 0$.

We shown that $E'[\widehat{\phi}]$ is in bijection with $\operatorname{Hom}(E[\phi], \mu_n)$, and the reverse bijection holds by some counting argument involving $\#E[\phi] = \#E'[\widehat{\phi}] = n$.

□

Remark 14.8. 1. If E, E', ϕ are all defined over K, then e_ϕ is Galois equivariant, so

$$e_\phi(\sigma S, \sigma T) = \sigma(e_\phi(S,T)) \tag{14.16}$$

for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$, $S \in E[\phi]$, $T \in E'[\widehat{\phi}]$.

2. Taking $\phi = [n] : E \to E$, so that $\widehat{\phi} = [n]$, we have that $e_n : E[n] \times E[n] \to \mu_{n^2}$, but since $E[n]$ has exponent n, the image lies in μ_n.

Corollary 14.9. *If $E[n] \subset E(K)$, then $\mu_n \subset K$.*

Proof. Let $T \in E[n]$ have order n. The nondegeneracy of e_n implies that there exists $S \in E[n]$ such taht $e_n(S,T) = \zeta_n$, where ζ_n is some primitive nth root of unity. Then

$$\begin{aligned} \sigma(\zeta_n) &= \sigma(e_n(S,T)) \\ &= e_n(\sigma S, \sigma T) \\ &= e_n(S,T) \\ &= \zeta_n \end{aligned} \tag{14.17}$$

for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$, so $\zeta_n \in K$. □

Example 14.10. Since $\mathbb{Q}$ does not contain μ_3, there is no elliptic curve $E/\mathbb{Q}$ with $E(\mathbb{Q})_{\mathrm{tors}} \cong (\mathbb{Z}/3\mathbb{Z})^2$.

Remark 14.11. In fact, e_n is alternating, so $e_n(T,T) = 1$ for all $T \in E[n]$, so $e_n(S,T) = e_n(T,s)^{-1}$.

15 Galois cohomology

Let G be a group (a Galois group in all further applications), and let A be a G-module, so A is an abelian group with an action of G, or A is a $\mathbb{Z}[G]$-module.

Definition 15.1. We set

$$H^0(G,A) \coloneqq A^G = \{a \in A \mid \sigma(a) = a \forall \sigma \in G\} \tag{15.1}$$

We have a filtration of sets

$$\begin{aligned} &C^1(G,A) = \{\text{maps } G \to A\} && \text{“cochains”} \\ &\quad \cup \\ &Z^1(G,A) = \{(a_\sigma)_{\sigma \in G} \mid a_{\sigma\tau} = \sigma(a_\tau) + a_\sigma \ \forall \sigma, \tau \in G\} && \text{“cocycles”} \\ &\quad \cup \\ &B^1(G,A) = \{(\sigma b - b)_{\sigma \in G} \mid b \in A\} && \text{“coboundaries”} \end{aligned} \tag{15.2}$$

and we set

$$H^1(G,A) = Z^1(G,A)/B^1(G,A) \tag{15.3}$$

Remark 15.2. If G acts trivially on A then $H^1(G,A) = \mathrm{Hom}(G,A)$.

Lemma 15.3. *Given a short exact sequence of G-modules*

$$0 \to A \xrightarrow{\phi} B \xrightarrow{\psi} C \to 0 \tag{15.4}$$

we have a long exact sequence of abelian groups

$$0 \to A^G \xrightarrow{\phi} B^G \xrightarrow{\psi} C^G \xrightarrow{\delta} H^1(G,A) \xrightarrow{\phi_*} H^1(G,B) \xrightarrow{\psi_*} H^1(G,C). \tag{15.5}$$

Proof. Omitted. □

Definition 15.4. The connecting homomorphism δ is given as follows. Let $c \in C^G$. Then there exists $b \in B$ such that $\psi(b) = c$. Then $\psi(\sigma b - b) = \sigma c - c = 0$ for all $\sigma \in G$, so $\sigma b - b \in \ker \psi$, so $\sigma b - b = \phi(a_\sigma)$ for some $a_\sigma \in A$ and we set

$$\delta(c) = [(a_\sigma)_{\sigma \in G}] \in Z^1(G,A)/B^1(G,A). \tag{15.6}$$

Theorem 15.5. *Let A be a G-module, and $H \leq G$ a normal subgroup. There is an "inflation-restriction" exact sequence*

$$0 \to H^1(G/H, A^H) \xrightarrow{\text{inf}} H^1(G,A) \xrightarrow{\text{res}} H^1(H,A). \tag{15.7}$$

Proof. Omitted. □

Let K be a perfect field. Then $\mathrm{Gal}(\overline{K}/K)$ is a topological group with basis of open subgroups $\mathrm{Gal}(\overline{K}/L)$ with $[L:K] < \infty$. 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.

We then have that

$$H^1(\mathrm{Gal}(\overline{K}/K), A) = \varinjlim_{L/K \text{ finite, Galois}} H^1(\mathrm{Gal}(L/K), A^{\mathrm{Gal}(\overline{K}/L)}) \tag{15.8}$$

where the direct limit is with respect to the inflation maps.

Theorem 15.6 (Hilbert's Theorem 90)**.** *Let L/K be a finite Galois extension. Then*

$$H^1(\mathrm{Gal}(L/K), L^\times) = 0. \tag{15.9}$$

Proof. Let $G = \mathrm{Gal}(L/K)$, and let $(a_\sigma)_{\sigma \in G} \in Z^1(G, L^\times)$. Then there exists $y \in L$ such that

$$x \coloneqq \sum_{\tau \in G} a_\tau^{-1} \tau(y) \neq 0 \tag{15.10}$$

as the elements of $\mathrm{Gal}(L/K)$ are linearly independent. Then (note the switch from additive to multiplicative notation)

$$\begin{aligned} \sigma(x) &= \sum_{\tau \in G} \sigma(a_\tau)^{-1} \sigma\tau(y) \\ &= a_\sigma \sum_{\tau \in G} a_{\sigma\tau}^{-1} \sigma\tau(y). \end{aligned} \tag{15.11}$$

Thus $a_\sigma = \frac{\sigma(x)}{x}$ for all $\sigma \in G$, so $(a_\sigma)_{\sigma \in G} \in B^1(G, L^\times)$, so $H^1(G, L^\times) = 0$. □

Corollary 15.7. *Taking direct limits, we have that*

$$H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times) = 0. \tag{15.12}$$

As an application, assume $\mathrm{char}\, K \nmid n$. Then there is a short exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$0 \to \mu_n \to \overline{K}^\times \xrightarrow{x^n} \overline{K}^\times \to 0 \tag{15.13}$$

and we get a long exact sequence

$$K^\times \to K^\times \to H^1(\mathrm{Gal}(\overline{K}/K), \mu_n) \to 0 \tag{15.14}$$

so $H^1(\mathrm{Gal}(\overline{K}/K), \mu_n) \cong (K^\times)/(K^\times)^n$. If $\mu_n \subset K$, then $\mathrm{Gal}(\overline{K}/K)$ acts trivially on μ_n, so

$$\mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(\overline{K}/K), \mu_n) \cong K^\times/(K^\times)^n. \tag{15.15}$$

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 K with exponent dividing n. Compare to class field theory. This gives another proof of Theorem 11.3.

From now on, 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 over K. We have a short exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules:

$$0 \to E[\phi] \to E \xrightarrow{\phi} E' \to 0 \tag{15.16}$$

which gives a long exact sequence

$$E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(K, E[\phi]) \to H^1(K, E) \xrightarrow{\phi_*} H^1(K, E') \tag{15.17}$$

and at the central term we get a short exact sequence

$$0 \to E'(K)/\phi E(K) \to H^1(K, E[\phi]) \to H^1(K, E)[\phi_*] \to 0. \tag{15.18}$$

Now take K a number field, and for each place v fix an embedding $\overline{K} \subset \overline{K}_v$. Then $\mathrm{Gal}(\overline{K}_v/K_v) \subset \mathrm{Gal}(\overline{K}/K)$. At each place we get a short exact sequence (and a commutative diagram)

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

Taking the product over all places, we get a commutative diagram

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

The ϕ-Selmer group $S^{(\phi)}(E/K)$ is the kernel of the dashed line. It equals (by going through the diagram and using exactness)

$$\begin{aligned} S^{(\phi)}(E/K) &= \ker\left(H^1(K, E[\phi]) \to \prod_v H^1(K_v, E)[\phi_*]\right) \\ &= \{\alpha \in H^1(K, E[\phi]) \mid \mathrm{res}_v(\alpha) \in \mathrm{im}\,\delta_v \forall v\}. \end{aligned} \tag{15.19}$$

Definition 15.8. The *Tate-Shafarevich group* is defined as

$$Ш(E/K) \coloneqq \ker\left(H^1(K, E) \to \prod_v H^1(K_v, E)\right). \tag{15.20}$$

This gives a short exact sequence (the Selmer and Ш term are just subgroups of the terms in the previous exact sequence)

$$0 \to E'(K)/\phi E(K) \to S^{(\phi)}(E/K) \to Ш(E/K)[\phi_*] \to 0 \tag{15.21}$$

Taking $\phi = [n]$ gives

$$0 \to E(K)/nE(K) \to S^{(n)}(E/K) \to Ш(E/K)[n] \to 0 \tag{15.22}$$

We can reorganize the proof of weak Mordell-Weil to instead prove the following stronger result.

Theorem 15.9. *$S^{(n)}(E/K)$ is finite.*

Proof. For L/K a finite Galois extension, we have the inflation/restriction exact sequence

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

We have that $H^1(\mathrm{Gal}(L/K), E(L)[n])$ is finite because $\mathrm{Gal}(L/K)$ and $E(L)[n]$ are finite. Thus $S^{(n)}(E/K)$ is finite if and only if $S^{(n)}(E/L)$ is finite, so we can extend to a finite extension L. In particular, we may assume $E[n] \subset E(K)$ and hence by the Weil pairing that $\mu_n \subset K$. So $E[n] \cong \mu_n \times \mu_n$ as $\mathrm{Gal}(\overline{K}/K)$-modules, as they are both trivial under the action of $\mathrm{Gal}(\overline{K}/K)$. So

$$\begin{aligned} H^1(K, E[n]) &\cong H^1(K, \mu_n) \times H^1(K, \mu_n) \\ &\cong K^\times/(K^\times)^n \times K^\times/(K^\times)^n. \end{aligned} \tag{15.23}$$

Let S be the set of primes of bad reduction as well as all the places v with $v \mid n\infty$. Then S is a finite set of places.

Definition 15.10. The subgroup of $H^1(K, A)$ *unramified outside of S* is

$$H^1(K, A; S) = \ker\left((H^1(K, A) \to \prod_{v \notin S} H^1(K_v^{\mathrm{ur}}, A)\right) \tag{15.24}$$

There is a commutative diagram with exact rows

$$\begin{array}{ccccc} & & & & H^1(K, E[n]) \\ & & & & \downarrow{\scriptstyle \mathrm{res}_v} \\ E(K_v) & \xrightarrow{[n]} & E(K_v) & \xrightarrow{\delta_v} & H^1(K_v, E\,[n]) \\ \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}_{\mathrm{ur}}} \\ E(K_v^{\mathrm{ur}}) & \xrightarrow{[n]} & E(K_v^{\mathrm{ur}}) & \xrightarrow{0} & H^1(K_v^{\mathrm{ur}}, E\,[n]) \end{array}$$

If $v \notin S$, then the morphism $[n]$ on the lower row is surjective by Theorem 9.16, so the next morphism will be 0. Recall that if $\alpha \in H^1(K, E[n])$, then $\alpha \in S^{(n)}(E/K)$ if and only if $\mathrm{res}_v(\alpha) \in \operatorname{im} \delta_v$ for all v (see (15.19)). But if this is the case, then $\mathrm{res}_{\mathrm{ur}} \circ \mathrm{res}_v = 0$ by the above diagram. So

$$S^{(n)}(E/K) \subset H^1(K, E[n]; S) \cong H^1(K, \mu_n; S) \times H^1(K, \mu_n; S) \tag{15.25}$$

and

$$H^1(K, \mu_n; S) = \ker\left(K^\times/(K^\times)^n \to \prod_{v \notin S} (K_v^{\mathrm{ur}})^\times/(K_v^{\mathrm{ur}\,\times})^n \right) \tag{15.26}$$

Thus it is the elements of $K^\times$ which are nth powers in K_v^{ur}. But in K_v^{ur}, the valuations are the same because it is an unramified extension, so $v_v(a) = 0 \mod n$ for every place v, so

$$H^1(K, \mu_n; S) \subset K(S, n) \tag{15.27}$$

as defined in Lemma 11.5, the same Lemma shows that it is finite. □

Remark 15.11.

1. $S^{(n)}(E/K)$ is finite and effectively computable.
2. It is conjectured that $|Ш(E/K)| < \infty$, if so we could take $n \nmid |Ш(E/K)|$ and then we would have $E(K)/nE(K) \cong S^{(n)}(E/K)$.

   This would imply that $\operatorname{rank} E(K)$ is effectively computable.

16 Descent by cyclic isogeny

Let E, E' be elliptic curves over a number field K. Let $\phi : E \to E'$ be an isogeny of degree n. Suppose $\ker \widehat{\phi} \cong \mathbb{Z}/n\mathbb{Z}$, and is generated by some $T \subset E'(K)$.

Then $E[\phi] \cong \mu_n$ as a $\mathrm{Gal}(\overline{K}/K)$-module, by the Weil pairing $S \mapsto e_\phi(S, T)$. We have a short exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$0 \to \mu_n \to E \xrightarrow{\phi} E' \to 0 \tag{16.1}$$

which gives a long exact sequence

$$\begin{array}{ccccccc} E(K) & \xrightarrow{\phi} & E'(K) & \xrightarrow{\delta} & H^1(K,\mu_n) & \longrightarrow & H^1(K,E) \\ & & & \searrow^{\alpha} & \downarrow \cong & & \\ & & & & K^\times/(K^\times)^n & & \end{array}$$

Theorem 16.1. *Let $f \in K(E')$ and $g \in K(E)$ with $\operatorname{div}(f) = n(T) - n(0)$ and $\phi^* f = g^n$. Let $\alpha : E'(K) \to K^\times/(K^\times)^n$ be the map given in the commutative diagram above. Then $\alpha(P) = f(P) \mod (K^\times)^n$ for all $P \in E'(K) \setminus \{0, T\}$.*

Proof. Let $P \in E'(K)$ and $Q \in \phi^{-1}(P)$. Then $\delta(P) \in H^1(K, \mu_n)$ is represented by the map $\sigma \mapsto (\sigma Q - Q)$ (see Definition 15.4), and we have that $\sigma Q - Q \in E[\phi] \cong \mu_n$. So

$$e_\phi(\sigma Q - Q, T) = \frac{g(\sigma Q - Q + X)}{g(X)} \tag{16.2}$$

for any $X \in E$, avoiding the zeros and poles of g, and taking $X = Q$ gives

$$\begin{aligned} e_\phi(\sigma Q - Q, T) &= \frac{g(\sigma Q)}{g(Q)} \\ &= \frac{\sigma(g(Q))}{g(Q)} \\ &= \frac{\sigma \sqrt[n]{f(P)}}{\sqrt[n]{f(P)}} \end{aligned} \tag{16.3}$$

as $\phi^* f = g^n$, so $f(P) = g(Q)^n$. Now, we have that the isomorphism $K^\times/(K^\times)^n \to H^1(K, \mu_n)$ is given by sending

$$x \mapsto \left(\sigma \mapsto \frac{\sigma \sqrt[n]{x}}{\sqrt[n]{x}} \right) \tag{16.4}$$

Thus α sends $P \mapsto (\sigma \mapsto \sigma Q - Q) \in H^1(K, E[\phi])$, and this is sent to $\left(\sigma \mapsto \frac{\sigma \sqrt[n]{f(P)}}{\sqrt[n]{f(P)}} \right) \in H^1(K, \mu_n)$, and this is sent to $f(P) \in K^\times/(K^\times)^n$, so $\alpha(P) = f(P) \mod (K^\times)^n$. □

16.1 Descent by 2-isogeny

We simplify to the case where E/K has 2-torsion, and work over the isogeny given in Example 5.13, which we now recall. Let

$$\begin{aligned} E &: y^2 = x(x^2 + ax + b) \\ E' &: y^2 = x(x^2 + a'x + b') \end{aligned} \tag{16.5}$$

with $b(a^2 - 4b) \neq 0$, $a' = -2a$, $b' = a^2 - 4b$. Then we have an isogeny

$$\begin{aligned} \phi &: E \to E' & (x, y) &\mapsto \left(\left(\frac{y}{x}\right)^2, \frac{y(x^2 - b)}{x^2} \right) \\ \widehat{\phi} &: E' \to E & (x, y) &\mapsto \left(\frac{1}{4}\left(\frac{y}{x}\right)^2, \frac{y(x^2 - b')}{8x^2} \right) \end{aligned} \tag{16.6}$$

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

Proposition 16.2. *There is a group homomorphism*

$$\begin{aligned} E'(K) &\to K^\times/(K^\times)^2 \\ (x,y) &\mapsto \begin{cases} x \mod (K^\times)^2 & x \neq 0 \\ b' \mod (K^\times)^2 & x = 0 \end{cases} \end{aligned} \tag{16.7}$$

with kernel $\phi E(K)$.

Note that we need to treat $x = 0$ separately because $0 \notin K^\times$.

Proof. One method is to apply Theorem 16.1 with $f = x \in K(E')$ and $g = \frac{y}{x} \in K(E)$.
Another is by direct calculation, as on Sheet 4. □

So we have injections

$$\begin{aligned} \alpha_E &: E(K)/\widehat{\phi}E'(K) \hookrightarrow K^\times/(K^\times)^2 \\ \alpha_{E'} &: E'(K)/\phi E(K) \hookrightarrow K^\times/(K^\times)^2. \end{aligned} \tag{16.8}$$

We can use these two calculate the rank of our elliptic curve.

Lemma 16.3. *We have that*

$$2^{\operatorname{rank} E(K)} = \frac{|\operatorname{im}\alpha_E| \cdot |\operatorname{im}\alpha_{E'}|}{4} \tag{16.9}$$

Note that everything above are $\mathbb{F}_2$ vectors spaces, so divisible by 2.

Proof. If $A \xrightarrow{f} B \xrightarrow{g} C$ are homomorphisms of abelian groups (not necessarily exact), then there is an exact sequence

$$0 \to \ker f \to \ker gf \xrightarrow{f} \ker g \to \operatorname{coker} f \xrightarrow{g} \operatorname{coker} gf \to \operatorname{coker} g \to 0 \tag{16.10}$$

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

$$0 \to \mathbb{Z}/2\mathbb{Z} \to E(K)[2] \xrightarrow{\phi} \mathbb{Z}/2\mathbb{Z} \to \operatorname{im}\alpha_{E'} \xrightarrow{\widehat{\phi}} E(K)/2E(K) \to \operatorname{im}\alpha_E \to 0 \tag{16.11}$$

By some standard exact sequence stuff (everything above is a finite abelian group), we get

$$\frac{|E(K)/2E(K)|}{|E(K)[2]|} = \frac{|\operatorname{im}\alpha_E| \cdot |\operatorname{im}\alpha_{E'}|}{4} \tag{16.12}$$

By Mordell-Weil, $E(K) \cong \Delta \times \mathbb{Z}^r$ with Δ finite, and $r = \operatorname{rank} E(K)$. We have that $E(K)[2] \cong \Delta[2]$, and $E(K)/2E(K) \cong \Delta/2\Delta \times (\mathbb{Z}/2\mathbb{Z})^r$ and $|\Delta/2\Delta| = |\Delta[2]|$ by the short exact sequence

$$0 \to \Delta[2] \to \Delta \to 2\Delta \to 0 \tag{16.13}$$

so we are done. □

Lemma 16.4. *Let K be a number field, and suppose that $a, b \in \mathcal{O}_K$. Then $\operatorname{im}(\alpha_E) \subset K(S,2)$, where $S = \{\mathfrak{p} \in \operatorname{Spec}\mathcal{O}_K \mid \mathfrak{p}|b\}$, where $K(S,n)$ is defined as in* (11.11).

Proof. We must show that if $x, y \in K$ with $y^2 = x(x^2 + ax + b)$ and if $\mathfrak{p} \nmid b$ (so $v_\mathfrak{p}(b) = 0$), then $v_\mathfrak{p}(x) = 0 \mod 2$.

In the case where $v_\mathfrak{p}(x) = 0$, we are done.

In the case where $v_\mathfrak{p}(x) < 0$, by Lemma 9.3 $v_\mathfrak{p}(x) = -2r$ for some $r \geq 1$, so we are done.

In the case where $v_\mathfrak{p}(x) > 0$, we have that $v_\mathfrak{p}(x^2 + ax + b) = 0$, so $v_\mathfrak{p}(x) = v_\mathfrak{p}(y^2)$, so $v_\mathfrak{p}(x) = 0 \mod 2$. □

In particular, the image of α_E lies in those cosets $x(K^\times)^2$ with $x|b$.

Lemma 16.5. *If $b_1 b_2 = b$, then $b_1(K^\times)^2 \in \mathrm{im}(\alpha_E)$ if and only if*

$$w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4 \tag{16.14}$$

has a solution 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 since $b(K^\times)^2, (K^\times)^2 \in \mathrm{im}(\alpha_E)$. So assume $b_1, b_2 \notin (K^\times)^2$, so $b_1(K^\times)^2 \in \mathrm{im}(\alpha_E)$ if and only if there exists $(x, y) \in E(K)$ such that $x = b_1 t^2$ or some $t \in K^\times$. Then $y^2 = (b_1 t^2)(b_1^2 t^4 + a b_1 t^2 + b)$, so dividing gives

$$\left(\frac{y}{b_1 t}\right)^2 = b_1 t^4 + a t^2 + b_2. \tag{16.15}$$

so (16.14) has a solution $(u, v, w) = (t, 1, y/(b_1 t))$. Conversely, if (u, v, w) is a solution to (16.14) then $uv \neq 0$, and

$$\left(b_1 \left(\frac{u}{v}\right)^2, b_1 \frac{uw}{v^3}\right) \in E(K), \tag{16.16}$$

so $b_1(K^\times)^2 \in \mathrm{im}\, \alpha_E$. □

Now we look at some examples with $K = \mathbb{Q}$.

Example 16.6. Let $E : y^2 = x^3 - x$ so $a = 0, b = -1$. By Lemma 16.4 and Proposition 16.2, $\mathrm{im}(\alpha_E) = \langle -1 \rangle \in (\mathbb{Q}^\times)/(\mathbb{Q}^\times)^2$.

We have $E' : y^2 = x^3 + 4x$, so $\mathrm{im}\, \alpha_{E'} \subset \langle -1, 2 \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. We need to consider $b_1 = -1, 2, -2$, and after checking we find that $\mathrm{Im}(\alpha_{E'}) = \langle 2 \rangle$, so $\mathrm{rank}(E(\mathbb{Q})) = 0$, so 1 is not a congruent number.

Example 16.7. Let $E : y^2 = x^3 + px$ with $p \equiv 5 \mod 8$. We have $\mathrm{im}\, \alpha_E = \langle p \rangle$.

We have $E' : y^2 = x^3 - 4px$, so $\mathrm{im}(\alpha_{E'}) \subset \langle -1, 2, p \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Note that $\alpha_{E'}(T') = (-4p)(\mathbb{Q}^*)^2 = (-p)(\mathbb{Q}^*)^2$. So it remains to check

$$b_1 = 2 : \qquad w^2 = 2u^4 - 2pv^4 \tag{16.17}$$

$$b_1 = -2 : \qquad w^2 = -2u^4 + 2pv^4 \tag{16.18}$$

$$b_1 = p : \qquad w^2 = pu^4 - 4v^4 \tag{16.19}$$

$$\tag{16.20}$$

Suppose that (16.17) is soluble, and WLOG let $u, v, w \in \mathbb{Z}$ with $\gcd(u, v) = 1$. If $p \mid u$, then $p \mid w$ so then $p \mid v$, which is a contradiction on the assumption that $\gcd(u, v) = 1$. So $w^2 = 2u^4 \neq 0 \mod p$, so $\left(\frac{2}{p}\right) = 1$, which is a contradiction as $p \equiv 5 \mod 8$. Thus (16.17) is insoluble.

Likewise, (16.18) has no solution since $\left(\frac{-2}{p}\right) = -1$.

We will return to (16.19) later as it is more difficult.

Let's return to the general 2-isogeny case. Let $E : y^2 = x(x^2 + ax + b)$, and $\phi : E \to E'$ be our friendly neighborhood 2-isogeny. We have a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(\mathbb{Q})/\widehat{\phi}E'(\mathbb{Q}) & \longrightarrow & S^{(\widehat{\phi})}(E'/\mathbb{Q}) & \longrightarrow & Ш(E'/\mathbb{Q})[\widehat{\phi}_*] & \longrightarrow & 0 \\ & & & \searrow^{\alpha_E} & \downarrow & & & & \\ & & & & \mathbb{Q}^*/(\mathbb{Q}^*)^2 & & & & \end{array}$$

Recall our equation

$$w^2 = b_1u^4 + au^2v^2 + b^2v^4 \qquad b_1b_2 = b. \tag{16.21}$$

We have that

$$\operatorname{im}\alpha_E = \{b_1(\mathbb{Q}^*)^2 \mid (16.21) \text{ is soluble over } \mathbb{Q}\}. \tag{16.22}$$

Determining whether (16.21) has a solution over $\mathbb{Q}$ is hard, but we might be able to apply the local global (Hasse) principle. In particular, we have that

$$\operatorname{im}\alpha_E \subset S^{(\widehat{\phi})}(E'/\mathbb{Q}) = \{b_1(\mathbb{Q}^*)^2 \mid (16.21) \text{ is soluble over } \mathbb{R} \text{ and over } \mathbb{Q}_p \forall p\}. \tag{16.23}$$

Solving things locally is easier. In fact, by Sheet 3 Question 9 and Hensel's Lemma we have that if $a, b_1, b_2 \in \mathbb{Z}$, and $p \nmid 2b(a^2 - 4b)$ then (16.21) is soluble over $\mathbb{Q}_p$.

Now we return to the previous example, and (16.19) in particular. We have that $\operatorname{rank} E(\mathbb{Q}) = 0$ if (16.19) is insoluble and 1 if it is soluble.

We have that (16.19) is soluble over $\mathbb{Q}_p$ since $\left(\frac{-1}{p}\right) = 1$, so $-1 \in (\mathbb{Z}_p^*)^2$ by Hensel's lemma and setting $(u, v) = (0, 1)$ we can find a w which solves the equation.

We have that (16.19) is soluble over $\mathbb{Q}_2$ because $p - 4 \equiv 1 \mod 8$, so $p - 4 \in (\mathbb{Z}_2^*)^2$ by Hensel's, so setting $(u, v) = (1, 1)$, we can find a w which solves the equation.

We have that (16.19) is soluble over $\mathbb{R}$ because $\sqrt{p} \in \mathbb{R}$.

People have found rational solutions to (16.19) for many values of p, but we don't know if there is always a solution in general. It is conjectured that the rank is always 1, so the equation always has a solution and the Hasse principle holds.

This is believable because Selmer conjectured that if the Hasse principle fails, it fails by an even amount, so since our only other option is the rank being 0, the rank should be 1. Someone has proved this conjecture assuming that Ш is finite.

Now lets give an example where we know that the Hasse principle fails.

Example 16.8 (Lind)**.** Let $E : y^2 = x^3 + 17x$, so $\operatorname{im}(\alpha_E) \subset \langle 17\rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$, and $E' : y^2 = x^3 - 68x$, and $\operatorname{im}(\alpha_{E'}) \subset \langle -1, 2, 17\rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$.

If $b_1 = 2$, then $w^2 = 2u^4 - 34v^4$ and doing a change of variables $w \to 2w$ and simplifying gives

$$C : 2w^2 = u^4 - 17v^4. \tag{16.24}$$

This is not homogeneous in the normal sense, but we can work in weighted projective space, which we now define. Let

$$C(K) = \{(u, v, w) \in K^3 \setminus \{0\} \mid C(u, v, w) = 0\}/\sim \tag{16.25}$$

where $(u, v, w) \sim (\lambda u, \lambda v, \lambda^2 w)$ for all $\lambda \in K^\times$.

We have that $C(\mathbb{Q}_2) \neq \emptyset$ because $17 \in (\mathbb{Z}_2^*)^4$ so we have a solution $(17^{1/4}, 1,)$.

We have that $C(\mathbb{Q}_{17}) \neq \emptyset$ since $2 \in (\mathbb{Z}_{17}^*)^2$, so we have a solution $(1, 0, 1/\sqrt{2})$.
We have that $C(\mathbb{R}) \neq 0$ since $\sqrt{2} \in \mathbb{R}$.
So $C(\mathbb{Q}_v) \neq 0$ at every place of $\mathbb{R}$.

But $C(\mathbb{Q}) = \emptyset$, as we now show. Suppose $(u, v, w) \in C(\mathbb{Q})$. WLOG $u, v, w \in \mathbb{Z}$, $w > 0$ and $\gcd(u, v) = 1$. If $17 \mid w$ then $17 \mid u$ and then $17 \mid v$, which is a contradiction. So if $p \mid w$ then $p \neq 17$, and in fact we need $\left(\frac{17}{p}\right) = 1$ (look at reduction mod p). By quadratic reciprocity, if p is odd then

$$\left(\frac{p}{17}\right) = \left(\frac{17}{p}\right) = 1 \tag{16.26}$$

and we also have $\left(\frac{2}{17}\right) = 1$. So $\left(\frac{w}{17}\right) = 1$, but $2w^4 \equiv u^4 \mod 17$, so this would imply $2 \in (\mathbb{F}_1 7^*)^4 = \{\pm 1, \pm 4\}$, which is a contradiction. Thus $C(\mathbb{Q}) = \emptyset$.

Thus the Hasse principle fails, so C represents a nontrivial element of $Ш(E/\mathbb{Q})$.

17 Birch and Swinnerton-Dyer Conjecture

Let $E/\mathbb{Q}$ be an elliptic curve.

Definition 17.1. The L-function of E is

$$L(E, s) = \prod_p L_p(E, s) \tag{17.1}$$

where

$$L_p(E, s) = \begin{cases} (1 - a_p p^{-s} + p^{1-2s})^{-1} & p \text{ has good reduction} \\ (1 - p^{-s})^{-1} & p \text{ has split multiplicative reduction} \\ (1 + p^{-s})^{-1} & p \text{ has nonsplit multiplicative reduction} \\ 1 & p \text{ has additive reduction} \end{cases} \tag{17.2}$$

and $\#\tilde{E}(\mathbb{F}_p) = 1 + p - a_p$ and $a_p = \mathrm{Tr}(\mathrm{Frob}_p)$.

By Hasse's Theorem, we have that $|a_p| \leq 2\sqrt{p}$, so $L(E, s)$ converges for $\mathrm{Re}(s) > 3/2$.

By the modularity theorem, we can write $L(E, s) = L(f, s)$ for f a modular form of weight 2, so we can analytic continuation to $\mathbb{C}$ and a functional equation.

Conjecture 17.2 (Weak BSD)**.**

$$\mathrm{ord}_{s=1} L(E, s) = \mathrm{rank}\, E(\mathbb{Q}) \tag{17.3}$$

If true, we can compute the rank by computing $L(E, s)$, which is tractable.

Conjecture 17.3 (Strong BSD)**.** *The coefficient of $(s-1)^r$ in the expansion of $L(E, s)$ at $s = 1$ is*

$$\frac{\Omega_E \,\mathrm{Reg}\, E(\mathbb{Q}) |Ш(E/\mathbb{Q})| \prod_p c_p(E)}{|E(\mathbb{Q})_{\mathrm{tors}}|^2} \tag{17.4}$$

where $c_p(E)$ are the Tamagawa numbers, $\mathrm{Reg}\, E(\mathbb{Q})$ is the regulator, and

$$\Omega_E = \int_{E(\mathbb{R})} \left| \frac{dx}{2y + a_1 x + a_3} \right| \tag{17.5}$$

where $a_1, \ldots, a_6 \in \mathbb{Z}$ are the coefficients of a globally minimal Weierstrass equation for $E/\mathbb{Q}$.

We have no idea how to solve this in general, you get \$1,000,000 if you do.

Theorem 17.4 (Kolyvagin)**.** *If the analytic rank is* ≤ 1*, then weak BSD holds and* $|Ш(E/\mathbb{Q})| < \infty$.