Elliptic Curves *

Zhiyuan Bai

Compiled on June 8, 2023

This document serves as a set of revision materials for the Cambridge Mathematical Tripos Part III course *Elliptic Curves* in Lent 2022. However, despite its primary focus, readers should note that it is NOT a verbatim recall of the lectures, since the author might have made further amendments in the content. Therefore, there should always be provisions for errors and typos while this material is being used.

Contents

*Based on the lectures under the same name taught by Dr. T. Fisher in Lent 2022.

1 Fermat's Method of Infinite Descent

Let's start with a right-angled triangle with perpendicular sides a, b and hypotenuse c. We know from school that $a^2 + b^2 = c^2$ and the triangle has area $ab/2$.

Definition 1.1. We say a (right-angled) triangle is rational if $a, b, c \in \mathbb{Q}$. We say it is primitive if $a, b, c \in \mathbb{Z}$ are coprime.

Lemma 1.1. *Every primitive triangle has the form* $a = 2uv, b = u^2 - v^2, c = u^2 + v^2$ *for integers* $u > v > 0$.

Proof. Suppose (a, b, c) are the sides of a primitive triangle, then a, b cannot be both odd or both even. WLOG a is odd and b is even, then c is odd. Rearrangement of $a^2 + b^2 = c^2$ gives $(b/2)^2 = ((c + a)/2)((c - a)/2)$. Now $(c \pm a)/2$ are coprime positive integers, so both have to be squares. Writing $(c + a)/2 = u^2, (c - a)/2 = v^2$ gives the result. □

Definition 1.2. $D \in \mathbb{Q}_{>0}$ is a congruent number if there exists a rational triangle whose area is D.

Clearly it suffices to study congruent numbers that are square-free positive integers, since scaling the triangle by a factor of k would result in a factor of k^2 on D.

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

Proof. D is congruent iff $Dw^2 = uv(u^2 - v^2)$ for some $u, v, w \in \mathbb{Q}, w \neq 0$ by the preceding lemma. Putting $x = u/v, y = w/v^2$ gives the result. □

Theorem 1.3 (Fermat)**.** 1 *is not congruent. Equivalently, there are no integers* $(u, v, w) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ *with* $w^2 = uv(u + v)(u - v)$.

Proof. WLOG u, v are coprime and $u, w > 0$. We can also assume $v > 0$ since if $v < 0$ then we can replace (u, v, w) by $(-v, u, w)$. If $u \equiv v \pmod 2$, we can replace (u, v, w) by $((u + v)/2, (u - v)/2, w/2)$.
So we have reduced to a case which make $u, v, u+v, u-v$ all coprime. But their product is a square, so there are integers a, b, c, d with $u = a^2, v = b^2, u + v = c^2, u - v = d^2$. As u, v have opposite parity, c, d both must be odd.
You saw the title of this section, so you know what we are about to do. We have

$$\left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 = \frac{c^2 + d^2}{2} = u = a^2$$

which gives another primitive triangle those area is $(c^2 - d^2)/8 = v/4 = (b/2)^2$. Let $w_1 = b/2$, then Lemma 1.1 shows that $w_1^2 = u_1 v_1 (u_1^2 - v_1^2)$ for some $u_1, v_1 \in \mathbb{Z}$. Now u_1, v_1 are coprime, $u_1, v_1, w_1 > 0$ and u_1, v_1 have distinct parity. Also, $4w_1^2 = b^2 = v \mid w^2$, so $w_1 \leq w/2$. We can apply the reduction we did at the start which then produces a reduced solution (u_2, v_2, w_2) with $0 < w_2 \leq w_1 < w$.
Repeating this construction indefinitely gives a strictly decreasing sequence of positive integers, which is a contradiction. □

Let's see another place where the descent trick shines. Let K be a field with $\operatorname{char} K \neq 2$. We denote the algebraic closure of K by $\bar{K}$.

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

Proof. WLOG $K = \bar{K}$. By a projective change of coordinates, we may also assume that the ratios $(\alpha : \beta)$ are $(1 : 0), (0 : 1), (1 : -1), (1 : -\lambda)$ for some $\lambda \in K, \lambda \neq 0, 1$. Suppose $u = a^2, v = b^2$, then $u - v = (a + b)(a - b), u - \lambda v = (a + \mu b)(a - \mu b)$ where $\mu^2 = \lambda$. $a \pm b$ are coprime since u, v are, so both have to be squares. Similarly $a \pm \mu b$ are also squares. But (a, b) is then a "smaller" solution in the sense that $\max\{\deg a, \deg b\} \leq (1/2) \max\{\deg u, \deg v\}$ which gives a contradiction by Fermat's descent unless $\deg u = \deg v = 0$. □

We now give a preliminary definition of elliptic curves.

Definition 1.3. An elliptic curve E/K over a field K is the projective closure of a plane affine of the form $y^2 = f(x)$ where $f \in K[x]$ is a monic cubic polynomial with distinct roots in $\bar{K}$.
If L/K is a field extension, we write $E(L)$ to denote the set $\{(x, y) \in L^2 : y^2 = f(x)\} \cup \{0_E\}$ where 0_E denotes the "point at infinity".

Turns out, $E(L)$ has the natural structure of an abelian group. The course we will explore properties and significance of $E(L)$ when L is a finite field, local field (finite extension of $\mathbb{Q}_p$) and number field (finite extension of $\mathbb{Q}$).
Theorem 1.3 basically says that $E : y^2 = x^3 - x$ has $E(\mathbb{Q}) = \{0_E, (0, 0), (\pm 1, 0)\}$.

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

Proof. WLOG $K = \bar{K}$. By a change of coordinates, we may assume that the elliptic curve has the form $E : y^2 = x(x-1)(x-\lambda)$ for some $\lambda \in K \setminus \{0,1\}$. Suppose $(x,y) \in E(K(t))$, then we can write $x = u/v$ where $u, v \in K[t]$ are coprime. Then $uv(u-v)(u-\lambda v) = w^2$ for some $w \in K[t]$. But these four factors are coprime, so each of them is a square. By Lemma 1.4, $u, v \in K$, hence $x \in K$ and $y \in K$. □

2 Some Remarks on Algebraic Curves

We work in an algebraically closed field $K = \bar{K}$.

2.1 Rational Curves, Genus, Order of Vanishing

Definition 2.1. A plane curve $C = \{f(x,y) = 0\} \subset \mathbb{A}^2$ is rational if it has a rational parameterisation, in the sense that there exists $\phi, \psi \in K(t)$ such that:
(i) The map $\mathbb{A}^1 \to \mathbb{A}^2, t \mapsto (\phi(t), \psi(t))$ is injective on $\mathbb{A}^1 \setminus \{\text{finitely many points}\}$.
(ii) $f(\phi(t), \psi(t)) = 0$ in $K(t)$.

Example 2.1. (a) Any nonsingular plane conic is rational. For example, on $C : x^2 + y^2 = 1$, a rational parameterisation can be found with the following procedure (we are working over $\mathbb{R}$ which breaks our promise of being algebraically closed, but the same procedure works in general too): Fix an anchor $(-1, 0)$ on the plane, and consider the intersection between C and the slope with slope t passing through $(-1, 0)$. Solving for the coordinates for the intersection gives a rational parameterisation $(x, y) = ((1-t^2)/(1+t^2), 2t/(1+t^2))$.
(b) Any singular plane cubic is rational. We pretty much make use of the same procedure as above, except now we take the anchor to be the singularity, e.g. $(0, 0)$ on $y^2 = x^3$ and on $y^2 = x^2(x+1)$. The former gives the parameterisation (t^2, t^3) and the latter is an exercise.
(c) What about nonsingular plane cubic? Corollary 1.5 tells us that elliptic curves are not rational.

Remark. Recall from algebraic geometry that the genus $g(C) \in \mathbb{Z}_{\geq 0}$ is an invariant of a smooth projective curve C. When $K = \mathbb{C}$, this equals the topological genus of the Riemann surface. Also, a smooth plane curve $C \subset \mathbb{P}^2$ of degree d has genus $g(C) = (d-1)(d-2)/2$.

Proposition 2.1. *Let C be a smooth projective curve, then*
(i) C is rational iff $g(C) = 0$.
(ii) C is (isomorphic to) an elliptic curve iff $g(C) = 1$.

Proof. (i) Omitted.
(ii) The "only if" part is clear. We will cover the "if" part later. □

Definition 2.2. Let C be an algebraic curve with function field $K(C)$. Suppose $P \in C$ is smooth. We write $\mathrm{ord}_P(f) \in \mathbb{Z}$ to denote the order of vanishing of $f \in K(C)$ at P.

It is a fact from algebraic geometry that this can be defined and $\mathrm{ord}_P : K(C)^\times \to \mathbb{Z}$ is a discrete valuation, i.e. $\mathrm{ord}_P(f_1 f_2) = \mathrm{ord}_P(f_1) + \mathrm{ord}_P(f_2)$ and $\mathrm{ord}_P(f_1 + f_2) \geq \min\{\mathrm{ord}_P(f_1), \mathrm{ord}_P(f_2)\}$.

Definition 2.3. A function $f \in K(C)^\times$ is a uniformiser at P if $\mathrm{ord}_P(f) = 1$.

Example 2.2. 1. Let $C = \{g = 0\} \subset \mathbb{A}^2$ for $g \in K[x, y]$ irreducible. Then $K(C) = \mathrm{FF}(K[x, y]/(g))$. Let $g = g_0 + g_1(x, y) + g_2(x, y) + \cdots$ and g_i is homogeneous of degree i. Suppose $g_0 = 0$ and $P = (0, 0) \in C$ is a smooth point (i.e. $g_1(x, y) = \alpha x + \beta y$ with α, β not both zero). Let $\gamma, \delta \in K$, then $\gamma x + \delta y \in K(C)$ is a uniformiser at P iff $\alpha\delta - \beta\gamma \neq 0$.
2. Let $C \subset \mathbb{P}^2$ be the projective closure of $\{y^2 = x(x - 1)(x - \lambda)\} \subset \mathbb{A}^2$ for $\lambda \neq 0, 1$. More precisely, $C = \{Y^2Z = X(X - Z)(X - \lambda Z)\} \subset \mathbb{P}^1$ which has only one point at infinity $P = (0 : 1 : 0)$. Let's work out $\mathrm{ord}_P(x) = \mathrm{ord}_P(X/Z)$ and $\mathrm{ord}_P(y) = \mathrm{ord}_P(Y/Z)$ 'cuz affines are for casuals. Put $t = X/Y, w = Z/Y$, then on the (t, w) affine piece C cuts out as $w = t(t - w)(t - \lambda w)$. P is a smooth point on this affine piece with coordinates $(t, w) = (0, 0)$ with $\mathrm{ord}_P(t) = \mathrm{ord}_P(t - w) = \mathrm{ord}_P(t - \lambda w) = 1$, so $\mathrm{ord}_P(w) = 3$. Consequently, $\mathrm{ord}_P(x) = \mathrm{ord}_P(X/Z) = \mathrm{ord}_P(t/w) = -2$ and $\mathrm{ord}_P(y) = \mathrm{ord}_P(Y/Z) = \mathrm{ord}_P(1/w) = -3$.

2.2 Riemann-Roch, Legendre Form, Degree

Let C be a smooth projective curve.

Definition 2.4. A divisor is a formal sum $D = \sum_{P \in C} n_P[P], n_P \in \mathbb{Z}$ of points on C with $n_P = 0$ for all but finitely many $P \in C$. We write $\mathrm{Div}(C)$ to denote the set of all divisors on C.
The degree of the divisor D is the sum $\deg D = \sum_{P \in C} n_P$. D is effective (sometimes written as $D \geq 0$) if $n_P \geq 0$ for all P.

Recall that a rational function on C can only have finitely many zeros or poles.

Definition 2.5. For $f \in K(C)^\times$, the divisor associated to f is $\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)[P]$.

Definition 2.6. The Riemann-Roch space of $D \in \mathrm{Div}(C)$ is

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

Roughly speaking, $L(D)$ is the K-vector space of all rational functions on C with poles no worse than (and zeros at least as good as) specified by D.
We don't have the budget to define the canonical divisor, so we are just gonna quote the special case of Riemann-Roch when our curve has genus 1.

Theorem 2.2 ((Partial) Riemann-Roch for Genus 1 Curves)**.**

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

Example 2.3. Again consider the curve $E : y^2 = f(x)$ with point P at infinity. Then $\dim L(2[P]) = \langle 1, x\rangle$ and $\dim L(3[P]) = \langle 1, x, y\rangle$.

Proposition 2.3. *Assume* $\mathrm{char}\, K \neq 2$. *Let $C \subset \mathbb{P}^2$ be a smooth plane cubic. Suppose $P \in C$ is a point of inflection (i.e. its tangent meets C at multiplicity at least 3), then via a projective change of coordinates C can be expressed in the form $Y^2Z = X(X - Z)(X - \lambda Z)$ for some $\lambda \neq 0, 1$, on which $P = (0 : 1 : 0)$.*

Proof. Change coordinates such that $P = (0 : 1 : 0)$ and $T_P C = \{Z = 0\}$. Suppose C now has equation $F(X, Y, Z) = 0$. As $P \in C$ is a point of inflection, $F(t, 1, 0)$ has a root at $t = 0$ with multiplicity at least 3. But F is a cubic, so $F(t, 1, 0)$ is a constant multiple of t^3. This means that the monomials X^2Y, XY^2, Y^3 cannot appear in F.
The term Y^2Z has nonzero coefficient since otherwise $P \in C$ would be singular. The term X^3 too has nonzero coefficient as otherwise $\{Z = 0\} \subset C$. Therefore C has equation of the form $Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ ("Weierstrass form") after rescaling. Substituting Y for $Y - (a_1/2)X - (a_3/2)Z$ (noting $\operatorname{char} K \neq 2$) then reduces C to the form $Y^2Z = Z^3 f(X/Z)$ ("Legendre form") for a cubic f, whose roots are distinct by smoothness. The result follows. □

Remark. One can show that the points of inflections on $C = \{F = 0\} \subset \mathbb{P}^2$ are given by the solutions to $F = \det(\partial^2 F / \partial X_i \partial X_j) = 0$.

Definition 2.7. Let $\phi : C_1 \to C_2$ be a nonconstant morphism of smooth projective curves. Then the pullback $\phi^* : K(C_2) \to K(C_1), f \mapsto f \circ \phi$ is a field extension. We define the degree of the morphism ϕ to be the degree $[K(C_1) : \phi^* K(C_2)]$ of the field extension induced by ϕ^*.
The morphism is separable if the field extension $K(C_1)/\phi^* K(C_2)$ is separable. Suppose $P \in C_1$ and $t \in K(C_2)$ is a uniformiser at $\phi(P)$. The ramification index at P is $e_\phi(P) = \operatorname{ord}_P(\phi^* t) \geq 1$, which does not depend on the specific choice of t.

Theorem 2.4. *Let $\phi : C_1 \to C_2$ be a nonconstant morphism of smooth projective curves and $Q \in C_2$, then*

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

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

In particular, ϕ is surjective and $|\phi^{-1}(Q)| \leq \deg \phi$ with equality for all but finitely many $Q \in C_2$.

Definition 2.8. Let C be an algebraic curve. A rational map from C is a map that factors through a map of the form $C \dashrightarrow \mathbb{P}^n, P \mapsto [f_0(P) : \cdots : f_n(P)]$, where $f_0, \ldots, f_n \in K(C)$ not all zero.

Theorem 2.5. *If C is a smooth projective curve, then any rational map is a morphism.*

3 Weierstrass Equations

We now work in a perfect field K, i.e. any finite extension of K is separable.

Definition 3.1. An elliptic curve E over K (sometimes written E/K) is a smooth projective curve over $\bar{K}$ with genus 1 and a specificed K-rational point $0 = 0_E \in E$.

Example 3.1. Let p be a prime, then $\{X^3 + pY^3 + p^3Z^3\} \subset \mathbb{P}^2$ is not an elliptic curve over $\mathbb{Q}$ since it has no $\mathbb{Q}$-rational point.

Theorem 3.1. *Every elliptic curve is isomorphic (over K) to a plane curve in Weierstrass form with the isomorphism taking 0_E to $(0:1:0)$.*

Remark. Proposition 2.3 treated the case where K is algebraically closed and E is a smooth plane cubic and 0_E is a point of inflection.

To prove the theorem, we use the fact that if D is a divisor on a curve E defined over K (i.e. fixed by the natural action of $\mathrm{Gal}(\bar{K}/K)$), then $L(D)$ has a basis in $K(E)$.

Proof. Clearly $L(2[0_E]) \subset L(3[0_E])$. Pick bases $\{1, x\}$ for $L(2[0_E])$ and $\{1, x, y\}$ for $L(3[0_E])$, both in $K(E)$. Then $\mathrm{ord}_{0_E}(x) = -2, \mathrm{ord}_{0_E}(y) = -3$, hence the rational functions $1, x, y, x^2, xy, x^3, y^2$ all reside in the 6-dimensional K-vector space $L(6[0_E])$, so there is a nontrivial K-linear relation between them. If one of x^3 and y^2, the rest would form a K-basis for $L(6[0_E])$ since each of them has a different order pole at 0_E. Consequently, the coefficients of x^3 and y^2 are nonzero in the linear relation. By rescaling, we get another elliptic curve E' which is the projective closure of $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ for some $a_i \in K$.
Consider the rational map $E \dashrightarrow E' \subset \mathbb{P}^2, P \mapsto (x(P) : y(P) : 1)$ which is automatically a morphism $E \to E'$ as we are dealing with curves. We also have $0_E \mapsto ((x/y)(P) : 1 : (1/y)(P)) = (0 : 1 : 0)$.
This morphism is an isomorphism: $[K(E) : K(x)] = \deg(x : E \to \mathbb{P}^1) = \mathrm{ord}_{0_E}(1/x) = 2$ and similarly $[K(E) : K(y)] = \mathrm{ord}_{0_E} = 3$. As $K(x) \subset K(x, y) \subset K(E)$ and $K(y) \subset K(x, y) \subset K(E)$ and $\gcd(2, 3) = 1$, we have $\phi^*K(E') = K(x, y) = K(E)$, thus our morphism has degree 1. E' is smooth and singular elliptic curves are rational. Combining this with the fact that rational maps between smooth curves are morphisms gives the result. □

How about uniqueness?

Proposition 3.2. *Let E, E' be elliptic curves over K, each in Weierstrass form. Then $E \cong E'$ over K iff their equations are related by a change of variables in the form $x = u^2x' + r, y = u^3y' + u^2sx' + t$ for some $u, r, s, t \in K, u \neq 0$.*

Proof. If when picking then basis of $L(2[0_E])$ we had $\langle 1, x\rangle = L(2[0_E]) = \langle 1, x'\rangle$, then $x = \lambda x' + r$ for some $\lambda, r \in K, \lambda \neq 0$. Similarly, suppose we did $\langle 1, x, y\rangle = L(3[0_E]) = \langle 1, x', y'\rangle$, then $y = \mu y' + \sigma x' + t$ for some $\mu, \sigma, t \in K, \mu \neq 0$. Looking at the coefficients of x^3 and y^2, we conclude that $\lambda^3 = \mu^2$ which gives the result. □

Conversely, when does a Weierstrass equation define an elliptic curve? We need only to check smoothness in the affine piece, as the point at infinity is smooth and K-rational. This is equivalent to $\Delta(a_1, \ldots, a_6) \neq 0$ for a certain polynomial Δ that you can look up.
When $\mathrm{char}\, K \neq 2, 3$, we can reduce it further to $E : y^2 = x^3 + ax + b$, in which case we have a shorter form of Δ given by $\Delta(a, b) = -16(4a^3 + 27b^2)$, the discriminant of the cubic $f(x) = x^3 + ax + b$.

Corollary 3.3. *Assume* $\mathrm{char}\, K \neq 2, 3$. *The elliptic curves $E : y^2 = x^3 + ax + b, E' : y^2 = x^3 + a'x + b'$ are isomorphic iff $a' = u^4a, b' = u^6b$ for some $u \in K^\times$.*

Definition 3.2. The j-invariant of an elliptic curve $E : y^2 = x^3 + ax + b$ is $j(E) = 1728(4a^3)/(4a^3 + 27b^2)$.

Corollary 3.4. *$E \cong E' \implies j(E) = j(E')$. If $K = \bar{K}$, then the converse is also true.*

Proof. The first implication follows from our discussion above. The converse when $K = \bar{K}$ can be shown by solving for u. □

4 The Group Law

4.1 Chord-and-tangent Construction; Jacobian

Let $E \subset \mathbb{P}^2$ be a smooth plane cubic and $0_E \in E(K)$. E meets any line at three ($\bar{K}$-)points, counted with multiplicity. For $P, Q \in E$, the line through P, Q (the tangent through P if $P = Q$) thus has a third point of intersection S with E. Similarly, let R be the third point of intersection of the line through $0_E, S$ and E.
This is known as the "chord-and-tangent construction" of the group law on the elliptic curve E, and we define $P \oplus Q = R$.

Theorem 4.1. *$(E(\bar{K}), \oplus)$ is an abelian group.*

Proof. $\oplus$ is clearly commutative. We also have $0_E \oplus P = P$. As for inverses, take the tangent line through 0_E which should meet E at a third point S. The line through P, S meets E at a third point Q, which has $P \oplus Q = 0_E$.
Associativity is messy if done with diagrams and calculations, so we are going to explore another description of the group law. □

Definition 4.1. $D_1, D_2 \in \mathrm{Div}(E)$ are linearly equivalent, sometimes written $D_1 \sim D_2$, if there exists a rational function $f \in \bar{K}(E)^\times$ such that $D_1 - D_2 = \mathrm{div}(f)$. The Picard group $\mathrm{Pic}(E)$ of E is the quotient $\mathrm{Pic}(E) = \mathrm{Div}(E)/\sim$. The Jacobian group $\mathrm{Jac}(E) = \mathrm{Pic}^0(E)$ of E is the quotient $\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\sim$ where $\mathrm{Div}^0(E) = \{D \in \mathrm{Div}(E) : \deg E = 0\}$.

We shall show that the map $E \mapsto \mathrm{Pic}^0(E), P \mapsto [[P] - [0_E]]$ is a bijection and the operation we defined on E is the same as the pullback of the group operation on $\mathrm{Pic}^0(E)$ via this map.

Proposition 4.2. *$\psi(P \oplus Q) = \psi(P) + \psi(Q)$ and ψ is bijective.*

Proof. Suppose the line through P, Q is the vanishing locus of the linear form l and the line through $0_E, S$ is the vanishing of m, then $\mathrm{div}(l/m) = [P] + [Q] - [0_E] - [P \oplus Q]$, thus $[P \oplus Q] - [0_E] \sim ([P] - [0_E]) + ([Q] - [0_E])$.
To see ψ is injective, observe that $[[P] - [0_E]] = [[Q] - [0_E]]$ forces $[P] - [Q]$ to be principal. Suppose $\mathrm{div}(f) = [P] - [Q]$ for $f \in \bar{K}(E)^\times$, then the morphism $E \to \mathbb{P}^1$ induced by f has to have degree 1, which forces $E \cong \mathbb{P}^1$, contradiction.
As for surjectivity, for $[D] \in \mathrm{Pic}^0(E)$, $D + [0_E]$ has degree 1, which means that $L(D + [0_E])$ has dimension $1 > 0$ by Riemann-Roch. In particular, there is some $f \in \bar{K}(E)^\times$ with $\mathrm{div}(f) + D + [0_E] \geq 0$. But $\mathrm{div}(f) + D + [0_E]$ has degree 1, hence equals $[P]$ for some $P \in E$, which means that $[[P] - [0_E]] = [D]$. □

Hence $\oplus$ is associative and $(E(\bar{K}), \oplus) \cong \mathrm{Pic}^0(E)$ as groups.

4.2 Formulae for Elliptic Curves in Weierstrass Form

Suppose $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, then $P = (x, y) \in E$ would have inverse $\ominus P = (x, -(a_1x + a_3) - y)$ by direct computation. So $P_3 = P_1 \oplus P_2 = \ominus P'$ where P_1, P_2, P' are the intersections between E and a line. Suppose the line is (the projective closure of) $\{y = \lambda x + \nu\}$. Substituting this into the Weierstrass Equation and comparing coefficients of x^2 yields

$$\begin{cases} x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_3 = -(\lambda + a_1)x_3 - \nu - a_3 \end{cases}$$

But of course we still need to solve for λ, ν. If $P_1 \neq P_2$ and $x_1 = x_2$, then we simply have $P_1 \oplus P_2 = 0_E$; If instead that $x_1 \neq x_2$, then

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \nu = \frac{x_2y_1 - x_1y_2}{x_2 - x_1}$$

When $P_1 = P_2$, a messy calculation (exercise) also realises λ, ν each as a rational combination of x_1, x_2, y_1, y_2.

Corollary 4.3. *$E(K)$ is a subgroup of $E(\bar{K})$.*

The calculation also gives

Theorem 4.4. *Elliptic curves are group varieties.*

Proof. We shall show that the maps $\ominus : E \to E, P \mapsto \ominus P$ and $\oplus : E \times E \to E, (P, Q) \mapsto P \oplus Q$ are morphisms. The formulae we found tells us that these are rational maps. The map $\ominus$ is then immediately a morphism as it's a rational map between smooth curves. As for $\oplus$, note that the calculation shows that $\oplus$ is regular on the Zariski open

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

For $P \in E$, consider $\tau_P : E \to E, Q \mapsto P \oplus Q$ which is rational and hence a morphism. The diagram

$$\begin{array}{ccc} E \times E & \xrightarrow{\oplus} & E \\ {\scriptstyle \tau_{\ominus A} \times \tau_{\ominus B}} \downarrow & & \uparrow {\scriptstyle \tau_{A \oplus B}} \\ E \times E & \xrightarrow[\oplus]{} & E \end{array}$$

always commutes, so $\oplus$ is also regular on $(\tau_A \times \tau_B)(U)$ for all $A, B \in E$, hence $\oplus$ is regular everywhere. □

4.3 A Survey on the Group Structure

For $K = \mathbb{C}$, we always have $E(K) \cong \mathbb{C}/\Lambda \cong (\mathbb{R}/\mathbb{Z}) \times (\mathbb{R}/\mathbb{Z})$ where Λ is a lattice in $\mathbb{C}$. This is a consequence of the theory of Weierstrass's $\wp$ function: For a lattice $\Lambda \leq \mathbb{C}$, the function field of $\mathbb{C}/\Lambda$ is generated by a function $\wp$ and its derivative $\wp'$ where

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z - \lambda)^2} - \frac{1}{\lambda^2} \right)$$

Turns out we also have $(\wp')^2 = 4\wp^3 - g_2\wp - g_3$ where g_2, g_3 are constants depending on Λ. One can then use this to show that $\mathbb{C}/\Lambda \cong E(\mathbb{C}), E : y^2 = 4x^3 - g_2x - g_3$, both as Riemann surfaces and as groups, via $z \mapsto (\wp(z), \wp'(z))$. The uniformisation theorem (or else) tells us that every elliptic curve over $\mathbb{C}$ arises this way, hence all complex elliptic curves are isomorphic to $(\mathbb{R}/\mathbb{Z})\times(\mathbb{R}/\mathbb{Z})$ as topological groups.
For $K = \mathbb{R}$, we have

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

For a finite field $K = \mathbb{F}_q$, we have the estimate $|E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$ (Hasse's Theorem).
For a local field $K/\mathbb{Q}_p$ with $[K : \mathbb{Q}_p] < \infty$, $E(K)$ has a subgroupd of finite index isomorphic to $(\mathcal{O}_K, +)$.
For a number field $K/\mathbb{Q}$ with $[K : \mathbb{Q}] < \infty$, $E(K)$ is a finitely generated abelian group (Mordell-Weil Theorem). The proof of Mordell-Weil also gives an upper bound for the rank of it, but there has not been a proven algorithm that reliably computes the rank in all cases.
We will show some of these results later in the course.

5 Isogeny

5.1 Torsion Subgroups

Definition 5.1. Suppose E_1, E_2 are elliptic curves. A map $E_1 \to E_2$ is an isogeny if it is a nonconstant morphsm of projective varieties that sends 0_{E_1} to 0_{E_2}.

Note that any nonconstant morphism is automatically surjective on $\bar{K}$-points. Consequently, composition of isogenies is still an isogeny, and (being nonconstant morphisms) we also have $\deg(\psi \circ \phi) = \deg(\psi)\deg(\phi)$ for isogenies ψ, ϕ.

Definition 5.2. We say E_1, E_2 are isogenous if there is an isogeny $E_1 \to E_2$.

It is not obvious that this is indeed an equivalence relation.

Definition 5.3. We write $\mathrm{Hom}(E_1, E_2)$ to denote the collection of all isogenies $E_1 \to E_2$ together with the constant map at 0_{E_2}. This has the natural structure of an abelian group.

For an elliptic curve E and $n \in \mathbb{Z}_{\geq 0}$, we write $[n] : E \to E, P \mapsto P \oplus \cdots \oplus P$ (n copies). As for negative $-n, n \in \mathbb{Z}_{\geq 0}$, we write $[-n] = \ominus \circ [n]$.

Definition 5.4. The n-torsion subgroup of E is $E[n] = \ker([n])$.

By abuse of notation, we sometimes write $E[n]$ to denote $E[n](\bar{K})$.
For $K = \mathbb{C}$, $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ and $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2, \deg[n] = n^2$. Surprisingly, these two results generalise.

Lemma 5.1. *Assume* $\mathrm{char}\, K \neq 2$*, then we know an elliptic curve E has the form $E : y^2 = f(x) = (x - e_1)(x - e_2)(x - e_3), e_1, e_2, e_3 \in \bar{K}$. In this form, we have $E[2] = \{0_E, (e_1, 0), (e_2, 0), (e_3, 0)\} \cong (\mathbb{Z}/2\mathbb{Z})^2$.*

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

Proposition 5.2. *$[n]$ is an isogeny for any $n \neq 0$.*

Proof. It is a morphism by Theorem 4.4 and it certainly maps 0_E to itself. $[0]$ is the zero map, so it suffices to show that $[n] \neq [0]$ whenever $n \neq 0$.
Assume $\operatorname{char} K \neq 2$. The case $n = 2$ is given by the preceding lemma. For odd n, pick $T \in E[2] \setminus \{0\}$ by the preceding lemma, then $[n]T = T \neq 0$ and hence $[n] \neq [0]$. We can then finish by $[mn] = [m][n]$.
For $\operatorname{char} K = 2$, one can obtain a statement similar to the preceding lemma but about $E[3]$ which would do the job. □

Corollary 5.3. *$\operatorname{Hom}(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module.*

Theorem 5.4. *If $\phi : E_1 \to E_2$ is an isogeny, then $\phi(P \oplus Q) = \phi(P) \oplus \phi(Q)$.*

Sketch of proof. WLOG $K = \bar{K}$ by Corollary 4.3.
ϕ induces a pushforward

$$\phi_* : \operatorname{Div}^0(E_1) \to \operatorname{Div}^0(E_2), \sum_P n_P P \mapsto \sum_P n_P \phi(P)$$

At the same time, we have a pullback $\phi^* : K(E_2) \to K(E_1)$ induced by ϕ. By some commutative algebra, we have $\operatorname{div}(N_{K(E_1)/K(E_2)}(f)) = \phi_*(\operatorname{div}(f))$, so ϕ_* sends principal divisors to principal divisors. This means that we can regard ϕ_* as a map $\operatorname{Pic}^0(E_1) \to \operatorname{Pic}^0(E_2)$. The commutative diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ {\scriptstyle P \mapsto [[P] - [0_{E_1}]]}\downarrow & & \downarrow{\scriptstyle Q \mapsto [[Q] - [0_{E_2}]]} \\ \operatorname{Pic}^0(E_1) & \xrightarrow[\phi_*]{} & \operatorname{Pic}^0(E_2) \end{array}$$

then shows that ϕ_* a group homomorphism. □

Lemma 5.5. *If $\phi : E_1 \to E_2$ is an isogeny, then there exists a morphism ξ making*

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

commute, where x_i is the x-coordinate projection on E_i.
Moreover, if $\xi(t) = r(t)/s(t)$ for $r, s \in K[t]$ coprime, then $\deg \phi = \deg \xi = \max\{\deg r, \deg s\}$.

Proof. Again we can take $K = \bar{K}$. Each $K(E_i)/K(x_i)$ is a degree 2 Galois extension with Galois group generated by $\ominus^*$. We know that $\phi \circ \ominus = \ominus \circ \phi$ by Theorem 5.4, so any $f \in K(x_2)$ has $\ominus^*(\phi^* f) = \phi^*(\ominus^* f) = \phi^* f$, and hence $\phi^* f \in K(x_1)$. We take $\xi(x_1) = \phi^* x_2$ which does make the diagram commute.
We have $\deg \xi = \deg \phi$ by tower law. It remains to compute the degree of ξ. Suppose $\xi(t) = r(t)/s(t)$ with $r, s \in K[t]$ coprime, then the minimal polynomial of x_1 over $K(x_2)$ is $f(t) = r(t) - s(t)x_2 \in K(x_2)[t]$. Indeed, $f(x_1) = 0$ and f is irreducible as it is irreducible in $K[x_2, t]$. Hence $\deg \xi = \deg f = \max\{\deg r, \deg s\}$. □

5.2 The Degree Map as a Quadratic Form

Lemma 5.6. $\deg[2] = 4$.

Proof. Assume $\operatorname{char} K \neq 2, 3$. Then our elliptic curve has the form $E : y^2 = f(x) = x^3 + ax + t$. For $P = (x, y) \in E$, we have

$$x(2P) = x(P \oplus P) = \left(\frac{3x^2 + a}{2y}\right)^2 - 2x = \frac{(3x^2 + a)^2 - 8xf(x)}{4f(x)} = \frac{x^4 + \cdots}{4f(x)}$$

The numerator and denomator here are coprime, since otherwise there'll be some $\theta \in \bar{K}$ with $f(\theta) = f'(\theta) = 0$, rendering E singular. The preceding lemma then allows us to conclude. □

Definition 5.5. Let A be an abelian group. A map $q : A \to \mathbb{Z}$ is a quadratic form if $q(nx) = n^2 q(x)$ and $\langle \cdot, \cdot \rangle : (x, y) \mapsto q(x + y) - q(x) - q(y)$ is $\mathbb{Z}$-bilinear.

Lemma 5.7. *$q : A \to \mathbb{Z}$ is a quadratic form iff it satisfies the parallelogram law $q(x + y) + q(x - y) = 2q(x) + 2q(y)$ for all $x, y \in A$.*

Proof. We have $\langle z, z \rangle = 2q(z)$ and $(1/2)\langle x + y, x + y \rangle + (1/2)\langle x - y, x - y \rangle = \langle x, x \rangle + \langle y, y \rangle$, which gives the "only if" direction. The converse will be on example sheet. □

We want to show that the degree map is a quadratic form. Before that, there are some mandatory calculations we must attend to.

Lemma 5.8. *Suppose $E : y^2 = x^3 + ax + b$ is an elliptic curve and $x_1, \ldots, x_4$ are the x-coordinates of $P, Q, P + Q, P - Q \neq 0_E$, then there are polynomials $W_0, W_1, W_2 \in \mathbb{Z}[a, b][x_1, x_2]$, homogeneous in x_1, x_2, with their degrees in x_1 and in x_2 both at most 2, and such that $(1 : x_3 + x_4 : x_3 x_4) = (W_0 : W_1 : W_2)$ (and in fact we can take $W_0 = (x_1 - x_2)^2$).*

Proof. One can either show this by direct calculation, or one can do some geometry. Let $y = \lambda x + \nu$ be the line through P, Q, then $x^3 + ax + b - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3)$. Let $s_i = s_i(x_1, x_2, x_3)$ be the i^{th} symmetric polynomial in x_1, x_2, x_3, then $\lambda^2 = s_1, -2\lambda\nu = s_2 - a, \nu^2 = s_3 + b$. Elliminating λ, ν gives $F(x_1, x_2, x_3) = (s_2 - a)^2 - 4s_1(s_3 + b) = 0$. By inspection F has degree at most 2 in each x_i. Thus x_3 is a root of the quadratic $W(t) = F(x_1, x_2, t)$. Repeating the same arguement but for the line through $P, -Q$ shows that x_4 is the other root, which gives the result. □

Theorem 5.9. $\deg : \operatorname{Hom}(E_1, E_2) \to \mathbb{Z}$ *is a quadratic form, with the convention* $\deg 0 = 0$.

Proof. Assume again that $\operatorname{char} K \neq 2, 3$. Then we can always write E_2 in the form $E_2 : y^2 = x^3 + ax + b$ and the preceding lemma applies.
We will show that if $\phi, \psi \in \operatorname{Hom}(E_1, E_2)$ then $\deg(\phi + \psi) + \deg(\phi - \psi) \leq 2\deg\phi + 2\deg\psi$. We may assume that $\phi, \psi, \phi + \psi, \phi - \psi \neq 0$ since otherwise the statement is either trivial or follows from Lemma 5.6. Suppose $\phi(x, y) = (\xi_1(x), \ldots), \psi(x, y) = (\xi_2(x), \ldots), (\phi + \psi)(x, y) = (\xi_3(x), \ldots), (\phi - \psi)(x, y) = (\xi_4(x), \ldots)$ (noting Lemma 5.5), then the preceding lemma shows that $(1 :$

$\xi_3 + \xi_4 : \xi_3\xi_4) = (W_0 : W_1 : W_2)$. Putting $\xi_i = r_i/s_i$ with $r_i, s_i \in K[t]$ coprime, we have $(s_3s_4 : r_3s_4 + r_4s_3 : r_3r_4) = ((r_1s_2 - r_2s_1)^2 : \cdots)$. Thus

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

which is what we wanted. The parallelogram law then follows from replacing ϕ, ψ by $\phi + \psi, \phi - \psi$. □

Corollary 5.10. *For all $n \in \mathbb{Z}, \phi \in \mathrm{Hom}(E_1, E_2)$, we have $\deg(n\phi) = n^2 \deg\phi$.*

In particular $\deg[n] = n^2$.

Example 5.1. Suppose E/K is an elliptic curve and $\mathrm{char}\, K \neq 2, 0_E \neq T \in E[2]$. WLOG $T = (0,0)$ and $E : y^2 = x(x^2+ax+b)$ for $a, b \in K, b(a^2-4b) \neq 0$. Suppose $P = (x,y)$ and $P' = P \oplus T = (x', y')$, then we have

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

Let $\xi = x + x' + a = (y/x)^2$ and $\eta = y + y' = (y/x)(x - b/x)$, then by calculations we have $\eta^2 = \xi(\xi^2 - 2a\xi + a^2 - 4b)$.
Take $E' : y^2 = x(x^2 + a'x + b'), a' = -2a, b' = a^2 - 4b$, then we get an isogeny $E \to E', (x,y) \mapsto ((y/x)^2, y(x^2-b)/x^2)$ of degree 2 (a "2-isogeny").

6 The Invariant Differential

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

Definition 6.1. The space Ω_C of Kähler differentials on C is the K-vector space generated by symbols $\mathrm{d}f, f \in K(C)$ subject to the relations:
(i) $\mathrm{d}(f+g) = \mathrm{d}f + \mathrm{d}g$.
(ii) $\mathrm{d}(fg) = f\,\mathrm{d}g + g\,\mathrm{d}f$.
(iii) $\forall a \in K, \mathrm{d}a = 0$.

It's a result from the theory of curves that Ω_C a one-dimensional $K(C)$-vector space.
Let $\omega \in \Omega_C \setminus \{0\}, P \in C$ and $t \in K(C)$ a uniformiser at P. Then $\omega = f\,\mathrm{d}t$ for some rational function $f \in K(C)^\times$.

Definition 6.2. The order of vanishing $\mathrm{ord}_P(\omega)$ at P is the order of vanishing of f at P.

It's clear that this is independent of the choice of the uniformiser t. Moreover, $\mathrm{ord}_P(\omega) = 0$ for all but finitely many points $P \in C$.

Definition 6.3. The divisor $\mathrm{div}(\omega)$ of $\omega \in \Omega_C$ is $\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega)[P]$.

Definition 6.4. A differential $\omega \in \Omega_C$ is regular if $\mathrm{div}(\omega) \geq 0$. The dimension $\dim_K\{\omega \in \Omega_C : \mathrm{div}(\omega) \geq 0\}$ is called the genus $g(C)$ of C.

As a consequence of (the general version of) Riemann-Roch, if $\omega \in \Omega_C \setminus \{0\}$, we have $\deg \operatorname{div}(\omega) = 2g(C) - 2$. Also, suppose $f \in K(C)^\times, \operatorname{ord}_P(f) = n \neq 0$ and $\operatorname{char} K \nmid n$, then $\operatorname{ord}_P(\mathrm{d}f) = n - 1$.

Lemma 6.1. *Assume* $\operatorname{char} K \neq 2$. *Consider an elliptic curve* $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$ *for* $e_1, e_2, e_3 \in K = \bar{K}$. *Then* $\omega = y^{-1}\,\mathrm{d}x$ *has* $\operatorname{div}\omega = 0$. *In particular,* $\{\omega\}$ *is a basis for the* 1*-dimensional* K*-vector space of regular differentials on* E.

Proof. Let $T_i = (e_i, 0)$, then $E[2] = \{0_E, T_1, T_2, T_3\}$. We have $\operatorname{div}(y) = [T_1] + [T_2] + [T_3] - 3[0_E]$. For $P \in E \setminus E[2]$, we have $\operatorname{ord}_P(x - x(P)) = 1$, thus $\operatorname{ord}_P(\mathrm{d}x) = 0$. For $P = T_i$, $\operatorname{ord}_P(x - e_i) = 2$, so $\operatorname{ord}_P(\mathrm{d}x) = 1$. For $P = 0_E$, $\operatorname{ord}_P(x) = -2$, so $\operatorname{ord}_P(\mathrm{d}x) = -3$. Consequently $\operatorname{div}(\mathrm{d}x) = [T_1] + [T_2] + [T_3] - 3[0_E] = \operatorname{div}(y)$, hence the result. □

Definition 6.5. For a nonconstant morphism $\phi : C_1 \to C_2$, its pullback on differentials is $\phi^* : \Omega_{C_2} \to \Omega_{C_1}, f\,\mathrm{d}g \mapsto \phi^* f\,\mathrm{d}(\phi^* g)$.

Lemma 6.2. *Let* $P \in E, \tau_P : E \to E, X \mapsto X + P$. *Then* $\tau_P^* \omega = \omega$ *where* $\omega = y^{-1}\,\mathrm{d}x$ *as before.*

We therefore call ω an invariant differential.

Proof. $\tau_P^*\omega$ is a regular differential on E, thus $\tau_P^*\omega = \lambda_P \omega$ for some $\lambda_P \in K^\times$. The map $E \to \mathbb{P}^1, P \mapsto \lambda_P$ is a morphism of smooth projective curves. This map is not surjective (as it misses $0, \infty$), hence necessarily constant, i.e. there is some $\lambda \in K^\times$ with $\tau_P^*\omega = \lambda\omega$ for all $P \in C$. Taking $P = 0$ gives $\lambda = 1$. □

Remark. In the case $K = \mathbb{C}$ where $\mathbb{C}/\Lambda \cong E$ via $z \mapsto (\wp(z), \wp'(z))$, we simply have $\mathrm{d}x/y = \mathrm{d}z$.

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

This is very not obvious, since the sum $\phi + \psi$ makes use of the structure given by the group law $\oplus$.

Proof. Write $E = E_2$ for brevity. Consider the maps $E \times E \to E$ given by $\mu : (P, Q) \mapsto P \oplus Q, \mathrm{pr}_1 : (P, Q) \mapsto P, \mathrm{pr}_2 : (P, Q) \mapsto Q$. It's a fact from algebraic geometry that $\Omega_{E \times E}$ (defined analogously as the case of curves and admits similar properties) is a 2-dimensional $K(C)$-vector space with a basis given by $\mathrm{pr}_1^*\omega, \mathrm{pr}_2^*\omega$. We thus have $\mu^*\omega = f\,\mathrm{pr}_1^*\omega + g\,\mathrm{pr}_1^*\omega$ for some $f, g \in K(E \times E)$. For $Q \in E$ we can consider $\iota_Q : E \to E \times E, P \mapsto (P, Q)$. Applying ι_Q^* gives

$$\tau_Q^*\omega = (\mu \circ \iota_Q)^*\omega = (\iota_Q^* f)(\mathrm{pr}_1 \circ \iota_Q)^*\omega + (\iota_Q^* g)(\mathrm{pr}_2 \circ \iota_Q)^*\omega = (\iota_Q^* f)\omega + 0$$

Thus $\iota_Q^* f = 1$ for all $Q \in E$, therefore $f \equiv 1$. Similarly $g \equiv 1$ and therefore $\mu^*\omega = \mathrm{pr}_1^*\omega + \mathrm{pr}_1^*\omega$.
Pulling these back by $E_1 \to E \times E, P \mapsto (\phi(P), \psi(P))$ gives $(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega$. □

Lemma 6.4. *Suppose* $\phi : C_1 \to C_2$ *is a nonconstant morphism between smooth projective curves, then* ϕ *is separable iff* $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ *is nonzero.*

Proof. Omitted. □

Example 6.1. Let $\mathbb{G}_m = \mathbb{A}^1 \setminus \{0\} = \mathbb{P}^1 \setminus \{0, \infty\}$. Consider $\phi = \phi_n : \mathbb{G}_m \to \mathbb{G}_m, x \mapsto x^n$, then $\phi^*(\mathrm{d}x) = \mathrm{d}(x^n) = nx^{n-1}\,\mathrm{d}x$. So if $\operatorname{char} K \nmid n$, then ϕ is separable, hence $|\phi^{-1}(Q)| = \deg \phi$ for all but finitely many $Q \in \mathbb{G}_m$.
On the other hand, ϕ is also a group homomorphism as $\mathbb{G}_m$ has the structure of a group given by multiplication in the field. So $|\phi^{-1}(Q)| = |\ker \phi|$ for all $Q \in \mathbb{G}_m$, consequently $n = |\ker \phi| = \deg \phi$.
This is a very elaborate proof of the fact that an algebraically closed field K with $\operatorname{char} K \nmid n$ has exactly n roots of unity.

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

Proof. We know that $[n]^*\omega = n\omega$ by Lemma 6.3. Thus $[n]$ is separable by Lemma 6.4 as $\operatorname{char} K \nmid n$. Consequently $|[n]^{-1}(Q)| = \deg[n]$ for all but finitely many $Q \in E$. On the other hand, $[n]$ is a group homomorphism, so $|[n]^{-1}(Q)| = |E[n]|$. Therefore $|E[n]| = \deg[n] = n^2$.
Now $E[n]$ is a finite abelian group, so $E[n] = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_t\mathbb{Z}$ with $d_1 \mid \cdots \mid d_t$. But of course $d_t \mid n$. Also, if p is a prime with $p \mid d_1$ (which implies $p \mid n$), then $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^t$ and hence $t = 2$ as $|E[p]| = p^2$. The only way $t = 2$ can happen is if $d_1 = d_2 = n$ which gives $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. □

Remark. If $\operatorname{char} K = p$, then $[p]$ is inseparable and it can be shown that either $E[p^r]$ is isomorphic to $\mathbb{Z}/p^r\mathbb{Z}$ (the "ordinary" case) for all r or $E[p^r]$ is trivial for all r (the "supersingular" case).

7 Elliptic Curves over Finite Fields

7.1 Hasse's Theorem

Lemma 7.1. *Let A be an abelian group and $q : A \to \mathbb{Z}$ a positive-definite quadratic form. If $\phi, \psi \in A$, then $|q(\phi + \psi) - q(\phi) - q(\psi)| \le 2\sqrt{q(\phi)q(\psi)}$.*

Proof. Assume that $\phi \neq 0$ since the result is clear otherwise. Then $q(\phi) > 0$ as q is positive-definite.
As usual write $\langle \phi, \psi \rangle = q(\phi + \psi) - q(\phi) - q(\psi)$. Then for any $m, n \in \mathbb{Z}$,

$$\begin{aligned} 0 \le q(m\phi + n\psi) &= \frac{1}{2}\langle m\phi + n\psi, m\phi + n\psi \rangle = m^2 q(\phi) + mn\langle \phi, \psi \rangle + n^2 q(\psi) \\ &= q(\phi)\left(m + \frac{\langle \phi, \psi \rangle}{2q(\phi)} n\right)^2 + n^2\left(q(\psi) - \frac{\langle \phi, \psi \rangle^2}{4q(\phi)}\right) \end{aligned}$$

Taking $m = -\langle \phi, \psi \rangle$ and $n = 2q(\phi)$ gives the result. □

Theorem 7.2 (Hasse)**.** *Let $\mathbb{F}_q$ be the finite field with q elements. Then*

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

Proof. Suppose E is in Weierstrass form with coefficients $a_1, \ldots, a_6 \in \mathbb{F}_q$. Then $a_i^q = a_i$ for all i, so the Frobenius endomorphism $\phi : E \to E, (x, y) \mapsto (x^q, y^q)$ is well-defined and is an isogeny of degree q. And we have $E(\mathbb{F}_q) = \{P \in E : \phi(P) = P\} = \ker(1 - \phi)$.
Let $\omega = y^{-1}\,\mathrm{d}x$ be the invariant differential, then we have $\phi^*\omega = y^{-q}\,\mathrm{d}(x^q) = qx^{q-1}y^{-q}\,\mathrm{d}x = 0$ and hence $(1 - \phi)^*\omega = \omega \neq 0$. This means that $1 - \phi$ is

separable. Therefore $|E(\mathbb{F}_q)| = |\ker(1-\phi)| = \deg(1-\phi)$ as $1-\phi$ is a group homomorphism.
We already know that deg is a quadratic form, so by the preceding lemma we have $|\deg(1-\phi) - 1 - \deg(\phi)| \le 2\sqrt{\deg\phi}$ and we are done. □

7.2 Zeta Function

For a number field K, we can define its Dedekind ζ function by

$$\zeta_K(s) = \sum_{\mathfrak{o}\le\mathcal{O}_K} \frac{1}{(N\mathfrak{o})^s} = \prod_{\mathfrak{p}\le\mathcal{O}_K} \left(1 - \frac{1}{(N\mathfrak{p})^s}\right)^{-1}$$

Similarly, for K a function field over $\mathbb{F}_q$, i.e. $K = \mathbb{F}_q(C)$ for a smooth projective curve C over $\mathbb{F}_q$, we can define its ζ function to be

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

where $|C|$ is the set of closed points of C, i.e. the orbits of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ on $C(\bar{\mathbb{F}}_q)$, and $Nx = q^{\deg x}$ where $\deg x$ is the size of the said orbit.
Then $\zeta_K(s) = F(q^{-s})$ where

$$F(T) = \prod_{x\in|C|} (1 - T^{\deg x})^{-1} \in \mathbb{Q}[[T]]$$

Formally, we have

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

So $F(T) = \exp(\sum_n n^{-1}|C(\mathbb{F}_{q^n})|T^n)$, which is also denoted as $Z_C(T)$.

Definition 7.1. Let $\phi,\psi : \mathrm{End}(E) = \mathrm{Hom}(E,E)$. Write $\langle\phi,\psi\rangle = \deg(\phi+\psi) - \deg\phi - \deg\psi$ as the bilinear form associated to the quadratic form q. The trace of ϕ is defined as $\operatorname{tr}\phi = 1 + \deg\phi - \deg(1-\phi) = \langle\phi, 1\rangle$.

It's clear that tr is linear.

Lemma 7.3. *If $\psi \in \mathrm{End}(E)$, then $\psi^2 - (\operatorname{tr}\psi)\psi + \deg\psi = 0$.*

Proof. Example sheet. □

Theorem 7.4. *Let $E/\mathbb{F}_q$ be an elliptic curve. Write $|E(\mathbb{F}_q)| = q+1-a$ where $|a| \le 2\sqrt{q}$, then $Z_E(T) = (1 - aT + qT^2)/((1-T)(1-qT))$.*

Proof. Let $\phi : E \to E$ be the q-power Frobenius endomorphism. As seen in the proof of Theorem 7.2, we have $|E(\mathbb{F}_q)| = \deg(1-\phi) = q + 1 - \operatorname{tr}\phi$. So indeed $a = \operatorname{tr}\phi$. We also have $\deg\phi = q$, so $\phi^2 - a\phi + q = 0$. Thus $\operatorname{tr}(\phi^{n+2}) - a\operatorname{tr}(\phi^{n+1}) + q\operatorname{tr}(\phi^n) = 0$. Solving this difference equation (whose initial conditions are $\operatorname{tr} 1 =$

$2, \operatorname{tr}\phi = a)$ yields $\operatorname{tr}(\phi^n) = \alpha^n + \beta^n$ where α, β are the roots of $X^2 - aX + q = 0$. Thus $|E(\mathbb{F}_{q^n})| = \deg(1-\phi) = 1 + \deg(\phi^n) - \operatorname{tr}(\phi^n) = 1 + q^n - \alpha^n - \beta^n$ and therefore

$$\begin{aligned} Z_E(T) &= \exp\left(\sum_{n=1}^{\infty} \frac{1}{n}|E(\mathbb{F}_{q^n})|T^n\right) \\ &= \exp\left(\sum_{n=1}^{\infty} \frac{T^n}{n} + \frac{(qT)^n}{n} - \frac{(\alpha T)^n}{n} - \frac{(\beta T)^n}{n}\right) \\ &= \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)} = \frac{1 - aT + qT^2}{(1-T)(1-qT)} \end{aligned}$$

which is what we wanted. □

Remark. 1. This generalises to (part of) Weil's conjectures, which was proved by Grothendieck and Deligne.
2. Theorem 7.2 tells us that $|a| \leq 2\sqrt{q}$, so $\alpha = \bar{\beta}$ and hence $|\alpha| = |\beta| = \sqrt{q} = q^{1/2}$. We can rephrase this as saying that $\zeta_K(s) = 0 \implies Z_E(q^{-s}) = 0 \implies \operatorname{Re} s = 1/2$ (the "the Riemann hypothesis for function fields (of an elliptic curve)"), the generalisation of which to higher dimensions is also part of Weil's conjectures.

8 Formal Groups

8.1 Expansion near the Identity

Definition 8.1. Suppose R is a ring and $I \subset R$ an ideal. The I-adic topology on R is the topology with basis $\{r + I^n : r \in R, n \geq 1\}$.
A sequence $(x_n)_n \in R$ is Cauchy if for all $k \geq 1$, there is some $N \in \mathbb{N}$ such that $x_m - x_n \in I^k$ for all $m, n \geq \mathbb{N}$. We say $x_n \to x$ in R if for all $k \geq 1$, there is some $N \in \mathbb{N}$ such that $x - x_n \in I^k$ for all $n \geq N$.
R is called complete if $\bigcap_{n\geq 1} I^n = \{0\}$ and every Cauchy sequence in R converges.

Remark. 1. It is trivial to check that this notion of convergence is compatible with the ring operations.
2. Suppose R is complete with respect to $I \ni x$, then $1 + x + x^2 + \cdots$ is Cauchy and hence converges to some $y \in R$. It's then clear that $(1-x)y = 1$, i.e. $x \in R^\times$.

Example 8.1. 1. $R = \mathbb{Z}_p, I = p\mathbb{Z}_p$.
2. $R = \mathbb{Z}[[t]], I = (t)$.

Lemma 8.1 (Hensel's Lemma)**.** *Let R be an integral domain which is complete in the I-adic topology for some $I \leq R$. Let $F \in R[X]$ and $s \geq 1$. Suppose $a \in R$ satisfies $F(a) \equiv 0 \pmod{I^s}, F'(a) \in R^\times$, then there is some unique $b \in R$ such that $F(b) = 0$ and $b \equiv a \pmod{I^s}$.*

Proof. Let $u \in R^\times$ be such that $F'(a) = u \pmod{I}$. By replacing $F(X)$ by $u^{-1}F(X + a)$, we may assume WLOG that $a = 0, F'(0) \equiv 1 \pmod{I}$.
Consider the sequence $x_0 = 0, x_{n+1} = x_n - F(x_n)$. Then by induction we

know that $x_n \in I^s$ for all n. We also have $F(X) - F(Y) = (X - Y)(F'(0) + XG(X,Y) + YH(X,Y))$ for some $G, H \in R[X,Y]$, which means that $x_{n+1} \equiv x_n \pmod{I^{n+s}}$ for all $n \geq 0$ (another easy induction).
$(x_n)_n$ is then Cauchy and hence converges to some $b \in R$ which has $b = b - F(b)$, i.e. $F(b) = 0$, and $b \equiv 0 \pmod{I^s}$. Uniqueness is clear as R is an integral domain. □

Let's see how these relate to elliptic curves. Suppose our elliptic curve has Weierstrass form $E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$. On the affine piece $Y \neq 0$, we have the coordinates $t = -X/Y, w = -Z/Y$ under which E has affine equation $w = f(t,w)$ where $f(t,w) = t^3 + a_1tw + a_2t^2w + a_3w^2 + a_4tw^2 + a_6w^3$.
We apply the preceding lemma to $R = \mathbb{Z}[a_1, \ldots, a_6][[t]], I = (t), F(X) = X - f(t,X) \in R[X], s = 3, a = 0$, which is valid since $F(0) = -f(t,0) = -t^3 \equiv 0 \pmod{t^3}$ and $F'(0) = 1 - a_1t - a_2t^2 \in R^\times$. This gives a unique $w(t) \in \mathbb{Z}[a_1, \ldots, a_6][[t]]$ with $w(t) = f(t, w(t))$ and $w(t) \equiv 0 \pmod{t^3}$.

Remark. In fact, $w(t) = t^3(1 + A_1t + A_2t^2 + \cdots)$ where $A_1 = a_1, A_2 = a_1^2 + a_2, \ldots$ (look it up ...?). Taking $u = 1$ in the proof of the preceding lemma provides a convenient way to compute this, as it gives $w_n(t) \to w(t)$ where $w_0(t) = 0, w_{n+1}(t) = f(t, w_n(t))$.

Lemma 8.2. *Suppose R is an integral domain (with field of fractions K) that's complete with respect to an ideal $I \leq R$. For $a_1, \ldots, a_6 \in R$, we consider the elliptic curve $E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$. Then $\hat{E}(I) = \{(t, w(t)) \in E(K) : t \in I\} = \{(t,w) \in E(K) : t, w \in I\}$ is a subgroup of $E(K)$.*

Proof. The two expressions for $\hat{E}(I)$ are equivalent by Lemma 8.1.
Taking $(t,w) = (0,0)$ shows that $0_E \in \hat{E}(I)$. It suffices to show that $P_1, P_2 \in \hat{E}(I) \implies -P_1 - P_2 \in \hat{E}(I)$. Calculations strike again.
Suppose $P_1 = (t_1, w_1), P_2 = (t_2, w_2)$ where $w_1 = w(t_1), w_2 = w(t_2)$ and $w(t) = \sum_{n=2}^{\infty} A_{n-2}t^{n+1}$ is as before. As per usual consider $\lambda = (w(t_2) - w(t_1))/(t_2 - t_1)$ if $t_1 \neq t_2$ and $\lambda = w'(t_1)$ if $t_1 = t_2$. In any case, we have $\lambda = \sum_{n=2}^{\infty} A_{n-2}(t_1^n + t_1^{n-1}t_2 + \cdots + t_2^n) \in I$. On the other hand, $\nu = w_1 - \lambda t_1 \in I$. Substituting $w = \lambda t + \nu$ into $w = f(t,w)$ gives

$$\lambda t + \nu = t^3 + a_1t(\lambda t + \nu) + a_2t^2(\lambda t + \nu) + a_3(\lambda t + \nu)^2 + a_4t(\lambda t + \nu)^2 + a_6(\lambda t + \nu)^3$$

Let A, B be the coefficients of t^3, t^2 respectively, then $A = 1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3, B = a_1\lambda + a_2\nu + a_3\lambda^2 + 2a_4\lambda\nu + 3a_6\lambda^2\nu$. We have $A \in R^\times, B \in I$, so $t_3 = -B/A - t_1 - t_2 \in I$ and $w_3 = \lambda t_3 + \nu \in I$. □

Corollary 8.3. *(i) There exists $\iota \in \mathbb{Z}[a_1, \ldots, a_6][[t]]$ with $\iota(0) = 0$ such that $\ominus(t, w(t)) = (\iota(t), w(\iota(t)))$. (ii) There exists $F \in \mathbb{Z}[a_1, \ldots, a_6][[t_1, t_2]]$ with $F(0,0) = 0$ and $(t_1, w(t_1)) \oplus (t_2, w(t_2)) = (F(t_1,t_2), w(F(t_1,t_2)))$.*

Proof. (i) Take $R = \mathbb{Z}[a_1, \ldots, a_6][[t]], I = (t)$.
(ii) $R = \mathbb{Z}[a_1, \ldots, a_6][[t_1, t_2]], I = (t_1, t_2)$. □

In fact, $\iota(X) = -X - a_1X^2 - a_2X^3 - (a_1^3 + a_3)X^4 + \cdots, F(X,Y) = X + Y - a_1XY - a_2(X^2Y + XY^2) + \cdots$. Also, the properties of group law immediately shows that

Proposition 8.4. *(i)* $F(X,Y) = F(Y,X)$.
(ii) $F(X,0) = X, F(0,Y) = Y$.
(iii) $F(X,F(Y,Z)) = F(F(X,Y),Z)$.
(iv) $F(X,\iota(X)) = 0$.

Definition 8.2. Let R be a ring. A (one-parameter commutative) formal group over R is a power series $F(X,Y) \in R[X,Y]$ satisfying (i), (ii) and (iii) in the preceding proposition.

One can show that for any formal group F, there is a unique $\iota = -X + \cdots \in R[[X]]$ satisfying (iv).

Example 8.2. (i) $F(X,Y) = X + Y$ is a formal group, known as the additive formal group $\hat{\mathbb{G}}_a$.
(ii) $F(X,Y) = X + Y + XY = (1+X)(1+Y) - 1$ is a formal group which is called the multiplicative formal group $\hat{\mathbb{G}}_m$.
(iii) To an elliptic curve, we can associate a formal group F as per previous discussion. This is usually denoted as $\hat{E}$.

8.2 Abstract Formal Groups

Definition 8.3. Let $\mathcal{F}, \mathcal{G}$ be formal groups over a ring R given by power series F, G. A morphism $f : \mathcal{F} \to \mathcal{G}$ is a power series $f \in R[[T]]$ such that $f(0) = 0$ with $f(F(X,Y)) = G(f(X), f(Y))$. We say $\mathcal{F}$ is isomorphic to $\mathcal{G}$ (written $\mathcal{F} \cong \mathcal{G}$) if there are morphisms $f : \mathcal{F} \to \mathcal{G}, g : \mathcal{G} \to \mathcal{F}$ with $f(g(X)) = g(f(X))$.

Theorem 8.5. *If* $\operatorname{char} R = 0$*, then any formal group* $\mathcal{F}$ *over* R *(given by the power series* F*) is isomorphic to* $\hat{\mathbb{G}}_a$ *over* $R \otimes \mathbb{Q}$*. More precisely,*
(i) There is a unique power series $\log(T) \in (R \otimes \mathbb{Q})[[T]]$ *given in the form*

$$\log(T) = T + \frac{a_2}{2}T^2 + \frac{a_3}{3}T^3 + \cdots, a_i \in R$$

such that $\log(F(X,Y)) = \log X + \log Y$.
(ii) There is a unique power series $\exp(T) \in (R \otimes \mathbb{Q})[[T]]$ *given in the form*

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

such that $\exp(\log(T)) = \log(\exp(T)) = T$.

Proof. (i) Write $F_1 = \partial F/\partial X$. For uniqueness, let $p(T) = \mathrm{d}\log/\mathrm{d}T = 1 + a_2T + a_3T^2 + \cdots$. Differentiating $\log(F(X,Y)) = \log X + \log Y$ with respect to X gives $p(F(X,Y))F_1(X,Y) = p(X)$. Putting $X = 0$ gives $p(Y)F_1(0,Y) = 1$, so $p(Y) = F_1(0,Y)^{-1}$ and hence we can recover p (hence log) from F.
As for existence, we are of course going to start with $p(T) = F_1(0,T)^{-1} = 1 + a_2T + a_3T^2 + \cdots$, say. Define $\log(T) = T + (a_2/2)T^2 + (a_3/3)T^3 + \cdots$. Differentiating $F(F(X,Y),Z) = F(X,F(Y,Z))$ with respect to X shows that $F_1(F(X,Y),Z)F_1(X,Y) = F_1(X,F(Y,Z))$. Throwing in $X = 0$ gives $F_1(Y,Z)F_1(0,Y) = F_1(0,F(Y,Z))$, so $F_1(Y,Z)p(Y)^{-1} = p(F(Y,Z))^{-1}$ which means that $F_1(Y,Z)p(F(Y,Z)) = p(Y)$. We can then "integrate" (formally on power series) to conclude that $\log(F(Y,Z)) = \log Y + h(Z)$ for some power series h. Commutativity of F then forces $h(Z) = \log Z + C$ for some constant C. Checking the constant term in both sides shows that $C = 0$, and we are done.
(ii) We shall show a stronger result, namely the next lemma. □

Lemma 8.6. *Let $f(T) = aT + \cdots \in R[[T]]$ be such that $a \in R^\times$, then there exists a unique $g(T) = a^{-1}T + \cdots \in R[[T]]$ such that $f(g(T)) = g(f(T)) = T$.*

Proof. Let's construct a sequence $g_n \in R[[T]]$ with the property that $f(g_n(T)) \equiv T \pmod{T^{n+1}}$ and $g_{n+1}(T) \equiv g_n(T) \pmod{T^{n+1}}$.
To start with, we set $g_1(T) = a^{-1}T$. Now suppose $n \geq 1$ and g_{n-1} is already chosen. We have $f(g_{n-1}(T)) \equiv T + bT^n \pmod{T^{n+1}}$ for some b. If we put $g_n(T) = g_{n-1}(T) + \lambda T^n$, then $f(g_n(T)) \equiv f(g_{n-1}(T)) + \lambda a T^n \equiv T + (b + \lambda a)T^n \pmod{T^{n+1}}$. Taking $\lambda = -ba^{-1}$ then gives our desired g_n.
Sending $n \to \infty$ gives $g = a^{-1}T + \cdots \in R[[T]]$ such that $f(g(T)) = T$. Repeating the procedure on g yields some $h(T) = aT + \cdots \in R[[T]]$ with $g(h(T)) = T$. Then $f(T) = f(g(h(T))) = h(T)$. □

Let $\mathcal{F}$ be a formal group given by a power series $F \in R[[X, Y]]$. Suppose R is complete with respect to an ideal I. For $x, y \in I$, we notate $x \oplus_{\mathcal{F}} y = F(x, y)$. We write $\mathcal{F}(I) = (I, \oplus_{\mathcal{F}})$ to denote the abelian group structure induced by $\oplus_{\mathcal{F}}$.

Example 8.3. $\hat{\mathbb{G}}_a(I) = (I, +), \hat{\mathbb{G}}_m(I) \cong (1 + I, \times)$, and $\hat{E}(I)$ is the subgroup of $E(K)$ as in Lemma 8.2.

For an integer n, we can define an endomorphism of a formal group $\mathcal{F}$ (with power series F) via $[1]T = T$, $[n]T = F([n-1]T, T)$ for $n \geq 2$, and $[-1]T = \iota(T)$.

Corollary 8.7. *Let $\mathcal{F}$ be a formal group over R and $n \in \mathbb{Z}$. Suppose $n \in R^\times$, then:*
(i) $[n] : \mathcal{F} \to \mathcal{F}$ is an isomorphism of formal groups.
(ii) If R is complete with respect to an ideal I, then $\mathcal{F}(I) \to \mathcal{F}(I), x \mapsto nx$ is an isomorphism of groups.

In particular, (ii) means that $\mathcal{F}(I)$ has no n-torsion.

Proof. (i) $[n]T = nT + \cdots \in R[[T]]$ by induction, so we conclude by Lemma 8.6.
(ii) follows directly. □

9 Elliptic Curves over Local Fields

9.1 Integral and Minimal Weierstrass Equations

Suppose K is a field which is complete with respect to a discrete valuation $v : K^\times \to \mathbb{Z}$. The valuation ring (aka the ring of integers) is denoted as $\mathcal{O}_K = \{x \in K^\times : v(x) \geq 0\} \cup \{0\}$. Its unit group is $\mathcal{O}_K^\times = \{x \in K^\times : v(x) = 0\}$. Turns out $\mathcal{O}_K \setminus \mathcal{O}_K^\times$ is a principal ideal (so $\mathcal{O}_K$ is a discrete valuation ring). We denote a choice of the uniformiser by $\pi = \pi_K$ who has $v(\pi) = 1$. The completeness of K then implies the $\pi^r \mathcal{O}_K$-adic completeness of $\mathcal{O}_K$ for all $r \geq 1$. We denote the residue field as $k = \mathcal{O}_K / \pi \mathcal{O}_K$. We'll be interested in the mixed characteristic case, i.e. $\operatorname{char} K = 0, \operatorname{char} k = p > 0$. The chief example of this is $K = \mathbb{Q}_p$.
Let E/K be an elliptic curve.

Definition 9.1. A Weierstrass equation of E with coefficients $a_1, \ldots, a_6 \in K$ is:
(i) Integral if $a_1, \ldots, a_6 \in \mathcal{O}_K$.
(ii) Minimal if $v(\Delta)$ is minimal among all integral Weierstrass equations of E.

Remark. 1. The change-of-variable $x = u^2x', y = u^3y'$ rescales the coefficients by $a_k = u^k a'_k$. This shows the existence of integral Weierstrass equations.
2. If $a_1, \ldots, a_6 \in \mathcal{O}_K$ gives an integral Weierstrass equation, then $\Delta \in \mathcal{O}_K$ and hence $v(\Delta) \geq 0$. This shows the existence of minimal Weierstrass equations.
3. If $\operatorname{char} k \neq 2, 3$, there exists minimal Weierstrass equations of the form $y^2 = x^3 + ax + b$.

Lemma 9.1. *Suppose E/K is defined by an integral Weierstrass equation. Let $0_E \neq P = (x, y) \in E(K)$, then either $x, y \in \mathcal{O}_K$ or $v(x) = -2s, v(y) = -3s$ for some $s \geq 1$.*

Proof. If $v(x) \geq 0$ but $v(y) < 0$, then the left hand side of the Weierstrass equation has negative valuation but the right hand side has nonnegative valuation, contradiction.
Suppose now that $v(x) < 0$. Then the left hand side has valuation at least $\min\{2v(y), v(x) + v(y), v(y)\}$ while the right hand side has valuation exactly $3v(x)$. We then immediately have $v(y) < v(x)$ and, in turn, that $2v(y) = 3v(x)$. □

9.2 Subgroup Structures

Fix a minimal Weierstrass equation $a_1, \ldots, a_6$ for E/K which induces a formal group $\hat{E}$ over $\mathcal{O}_K$. Taking $I = \pi^r\mathcal{O}_K$ in Lemma 8.2 yields the subgroup

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

by the preceding lemma. We use the shorthand $E_r(K) = \hat{E}(\pi^r\mathcal{O}_K)$. This gives the chain $\cdots \hookrightarrow E_3(K) \hookrightarrow E_2(K) \hookrightarrow E_1(K)$.
More generally, if $\mathcal{F}$ is a formal group over $\mathcal{O}_K$, we have the chain $\cdots \hookrightarrow \mathcal{F}(\pi^3\mathcal{O}_K) \hookrightarrow \mathcal{F}(\pi^2\mathcal{O}_K) \hookrightarrow \mathcal{F}(\pi\mathcal{O}_K)$.
We'll now show that $\mathcal{F}(\pi^r\mathcal{O}_K) \cong (\mathcal{O}_K, +)$ for sufficiently large r and that $\mathcal{F}(\pi^r\mathcal{O}_K)/\mathcal{F}(\pi^{r+1}\mathcal{O}_K) \cong (k, +)$ for all $r \geq 1$.

Theorem 9.2. *Let $\mathcal{F}$ be a formal group over $\mathcal{O}_K$ and $e = v(p)$. If $r > e/(p-1)$, then* $\log : \mathcal{F}(\pi^r\mathcal{O}_K) \to \hat{\mathbb{G}}_a(\pi^r\mathcal{O}_K)$ *is an isomorphism with inverse* $\exp : \hat{\mathbb{G}}_a(\pi^r\mathcal{O}_K) \to \mathcal{F}(\pi^r\mathcal{O}_K)$.

Remark. As groups, we have $\hat{\mathbb{G}}_a(\pi^r\mathcal{O}_K) = (\pi^r\mathcal{O}_K, +) \cong (\mathcal{O}_K, +)$.

Proof. For $x \in \pi^r\mathcal{O}_K$, we want to show that the power series $\log(x), \exp(x)$ converge to something in $\pi^r\mathcal{O}_K$. We shall first show the convergence of

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

It's clear that $v_p(n!) \leq (n-1)/(p-1)$, so

$$v\left(\frac{b_n x^n}{n!}\right) \geq nr - e\frac{n-1}{p-1} = (n-1)\left(r - \frac{e}{p-1}\right) + r$$

which is always greater than r and goes to ∞ as $n \to \infty$. This gives the convergence of $\exp(x)$. The same method (but easier) works for log. $\square$

Lemma 9.3. *$\mathcal{F}(\pi^r\mathcal{O}_K)/\mathcal{F}(\pi^{r+1}\mathcal{O}_K) \cong (k,+)$ for all $r \geq 1$.*

Proof. Let F be the power series associated with $\mathcal{F}$. By the definition of formal group, we can write $F(X,Y) = X + Y + XYg(X,Y)$ for some power series g. So if $x, y \in \mathcal{O}_K$ then $F(\pi^r x, \pi^r y) \equiv \pi^r(x+y) \pmod{\pi^{r+1}}$. Therefore the map $\mathcal{F}(\pi^r\mathcal{O}_K) \to (k,+), \pi^r x \mapsto x \bmod \pi$ is a surjective group homomorphism, and it has kernel $\mathcal{F}(\pi^{r+1}\mathcal{O}_K)$. $\square$

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

Remark. The assumption $|k| < \infty$, together with our standing assumptions (mixed characteristics etc.), means that K would have to be a finite extension of $\mathbb{Q}_p$ for some p.

9.3 Reduction

Proposition 9.5. *Suppose E/K is an elliptic curve, then the modulo π reduction of any two minimal Weierstrass equations for E define isomorphic curves over k.*

Proof. Under the change of variables with coefficients $[u; r, s, t], u \in K^\times, r, s, t \in K$, we have $\Delta_1 = u^{12}\Delta_2$. So if $[u; r, s, t]$ is a change of variables relating two minimal Weierstrass equations, then $u \in \mathcal{O}_K^\times$. Some more calculations (together with the fact that $\mathcal{O}_K$, as a discrete valuation ring, is integrally closed) reveal that $r, s, t \in \mathcal{O}_K$ as well. The reduced Weierstrass equations are then related by the change of variables $[\tilde{u}; \tilde{r}, \tilde{s}, \tilde{t}]$ where $x \mapsto \tilde{x}$ is the modulo π reduction map $\mathcal{O}_K \to k$. $\square$

Definition 9.2. The reduction $\tilde{E}/k$ of an elliptic curve E/K is the reduction of a minimal Weierstrass equation of it.

Note that $\tilde{E}/k$ doesn't have to be an elliptic curve since it might have some singularities.

Definition 9.3. We say E has good reduction if $\tilde{E}$ is nonsingular. Otherwise we say E has bad reduction.

We can check whether E has good reduction by reducing the discriminant modulo π, if we already have a minimal Weierstrass equation. What if we just have an integral Weierstrass equation? If $v(\Delta) = 0$, then the equation is minimal and we indeed have good reduction. If $0 < v(\Delta) < 12$, then again the equation has to be minimal but we must have bad reduction.
There is a well-defined map $\mathbb{P}^2(K) \to \mathbb{P}^2(k), (X : Y : Z) \mapsto (\tilde{X} : \tilde{Y} : \tilde{Z})$ (noting that by recaling with a proper power of π every point in $\mathbb{P}^2(K)$ can be represented by $(X : Y : Z)$ with $\min\{v(x), v(y), v(z)\} = 0$). This map restricts to $E(K) \to \tilde{E}(k), P \mapsto \tilde{P}$. In the affine patch, if $P = (x, y) \in E(K)$, then either $x, y \in \mathcal{O}_K$ in which case $\tilde{P} = (\tilde{x}, \tilde{y})$, or $v(x) = -2s, v(y) = -3s$, in which case $\tilde{P} = (0 : 1 : 0)$. Thus $E_1(K) = \hat{E}(\pi\mathcal{O}_K)$ is essentially $\{P \in E(K) : \tilde{P} = 0\}$ (the "kernel of reduction").

Note that if E has bad reduction, then $\tilde{E}$ has a unique singularity. We introduce the notation

$$\tilde{E}_{\text{ns}} = \begin{cases} \tilde{E} & \text{if } E \text{ has good reduction} \\ \tilde{E} \setminus \{S\} & \text{if } E \text{ has bad reduction with singularity } S \end{cases}$$

The chord-and-tangent process always determines a group law on $\tilde{E}_{\text{ns}}$ in either case. Furthermore, $\tilde{E}_{\text{ns}}$ is either $\mathbb{G}_a$ or $\mathbb{G}_m$ in the case of bad reduction, with isomorphism over either k or a quadratic extension of k. Indeed, if $\operatorname{char} k \neq 2$, then we can write $\tilde{E} : y^2 = f(x), \deg f = 3$ and $\tilde{E}$ is singular iff f has repeated roots. The double roots case gives $\mathbb{G}_m$ whereas the triple roots gives $\mathbb{G}_a$. The proof of the former is on example sheet; As for the latter:
By a translation we may assume that $f(x) = x^3$. $\tilde{E}_{\text{ns}}$ has a parameterisation $\mathbb{G}_a, \to \tilde{E}_{\text{ns}}, t \mapsto (t^{-2}, t^{-3})$. The point at infinity is thus identified as $0 \in \mathbb{G}_a$ and (x, y) as x/y. Suppose the line through P_1, P_2, P_3 (whose parameters are $t = t_1, t_2, t_3$ respectively) does not pass through the origin, then it has equation $ax+by = 1$ for some a, b. Then by substitution $t_i^3 = at_i+b$ and thus $t_1+t_2+t_3 = 0$, which means that $\tilde{E}_{\text{ns}} \cong \mathbb{G}_a$.

Definition 9.4. Write $E_0(K) = \{P \in E(K) : \tilde{P} \in \tilde{E}_{\text{ns}}(k)\}$.

Proposition 9.6. *$E_0(K)$ is a subgroup of $E(K)$ and the modulo π reduction map $E_0(K) \to \tilde{E}_{\text{ns}}(k)$ is a surjective group homomorphism.*

Proof. A line ℓ in $\mathbb{P}^2_K$ has equation $aX + bY + cZ = 0$ for some $(a : b : c) \in \mathbb{P}^2_K$. By multiplying through with an appropriate multiple of π, we can choose a, b, c such that $\min\{v(a), v(b), v(c)\} = 0$. Reduction modulo π then yields a (unique) line $\tilde{\ell} : \tilde{a}X + \tilde{b}Y + \tilde{c}Z = 0$ in $\mathbb{P}^2_k$.
If $P_1, P_2, P_3 \in E(K)$ has $P_1 \oplus P_2 \oplus P_3 = 0$, i.e. they lie on a line ℓ, then $\tilde{P}_1, \tilde{P}_2, \tilde{P}_3$ lie on $\tilde{\ell}$. So if $P_1, P_2 \in E_0(K)$, then $\tilde{P}_1, \tilde{P}_2 \in \tilde{E}_{\text{ns}}(k)$, thus $\tilde{P}_3 \in \tilde{E}_{\text{ns}}(k)$. This means that $P_3 \in E_0(K)$ and $\tilde{P}_1 + \tilde{P}_2 + \tilde{P}_3 = 0$.
As for surjectivity, let $f(x, y) = y^2 + a_1xy + a_3 - (x^3 + a_2x^2 + a_4x + a_6)$. Let $\tilde{P} = (\tilde{x}, \tilde{y}) \in \tilde{E}_{\text{ns}}(k) \setminus \{0\}$. As $\tilde{P}$ is not a singular point on $\tilde{E}$, either $f_x(x_0, y_0) \in \mathcal{O}_K^\times$ or $f_y(x_0, y_0) \in \mathcal{O}_K^\times$.
In the former case, we put $g(t) = f(t, y_0) \in \mathcal{O}_K[t]$, then $g(x_0) \equiv 0 \pmod{\pi}$ and $g'(x_0) \in \mathcal{O}_K^\times$. Lemma 8.1 then gives $b \in \mathcal{O}_K$ with $g(b) = 0$ and $b \equiv x_0 \pmod{\pi}$. Then (b, y_0) has reduction $\tilde{P}$.
The latter case is exactly the same. □

Recall that for any $r \geq 1$ we've put $E_r(K) = \{(x, y) \in E(K) : v(x) \leq -2r, v(y) \leq -3r\} \cup \{0\}$ which gives a chain $\cdots \hookrightarrow E_3(K) \hookrightarrow E_2(K) \hookrightarrow E_1(K)$. We've shown that $E_r(K) \cong (\mathcal{O}_K, +)$ for $r > e/(p-1)$ and $E_n(K)/E_{n+1}(K) \cong (k, +)$ for any $n \geq 1$. We can extend this chain to include $\cdots \hookrightarrow E_1(K) \hookrightarrow E_0(K) \hookrightarrow E(K)$ where we have $E_0(K)/E_1(K) \cong \tilde{E}_{\text{ns}}(k)$.

Theorem 9.7. *If K is a finite extension of $\mathbb{Q}_p$, then $E(K)$ contains a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.*

Proof. Let's show that $[E(K) : E_0(K)] < \infty$, which implies the result. Since $|k| < \infty$, $\mathcal{O}_K/\pi^r\mathcal{O}_K$ is finite for any $r \geq 1$, which implies that $\mathcal{O}_K$ is compact. $\mathbb{P}^n(K)$ is the union of the sets $\{(a_0 : \cdots : a_{i-1} : 1 : a_{i+1} : \cdots : a_n) : a_j \in \mathcal{O}_K\}$, so this mean that $\mathbb{P}^n(K)$ is compact with respect to the π-adic topology on K.

As $E(K) \subset \mathbb{P}^2(K)$ is a closed subset, it is a compact topological group. $E_0(K)$ is an open subgroup in $E(K)$. Indeed, if $\tilde{E}$ is singular at $(\tilde{x}_0, \tilde{y}_0)$, then $E(K) \setminus E_0(K) = \{(x,y) \in E(K) : v(x-x_0) \geq 1, v(y-y_0) \geq 1\}$ which is closed in $E(K)$. But then every coset of $E_0(K)$ has to be open, which means that it has finite index by compactness of $E(K)$. □

Remark. $c_K(E) = [E(K) : E_0(K)]$ is called the Tamagawa number of E/K. If E has good reduction, then $c_K(E) = 1$, but the converse is not true. It can also be shown that either $c_K(E) = v(\Delta)$ or $c_K(E) \leq 4$ (where we work over a minimal Weierstrass equation).

Let's recall some facts about local fields.
Let K be a finite extension of $\mathbb{Q}_p$ and L/K a finite extension. Suppose L has residue field k' and K has residue field k. Set $f = [k' : k]$, then $[L : K] = ef$ where e is the ramification index of L/K, i.e. the map $\mathbb{Z} \to \mathbb{Z}$ via multiplication by e makes

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

commute. If L/K is Galois, then there is a natural surjection $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k'/k)$ whose kernel has order e.
We say L/K is unramified if $e = 1$. For each $m \geq 1$, k has a unique extension k_m of degree m and K has a unique unramified extension K_m of degree m. These extensions are Galois with cyclic Galois group. We write

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

to denote the "maximal unramified extension" of K.

Theorem 9.8. *Suppose $[K : \mathbb{Q}_p] < \infty$, E/K has good reduction and $p \nmid n$. Let $P \in E(K)$, then $K([n]^{-1}P)/K$ is unramified, where $[n]^{-1}P = \{Q \in E(\bar{K}) : nQ = P\}$ and $K(\{P_1, \ldots, P_r\}) = K(x(P_1), y(P_1), \ldots, x(P_r), y(P_r))$.*

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

$$0 \longrightarrow E_1(K_m) \longrightarrow E(K_m) \longrightarrow \tilde{E}(k_m) \longrightarrow 0$$

Taking union gives another exact sequence which fits into the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_1(K^{\mathrm{nr}}) & \longrightarrow & E(K^{\mathrm{nr}}) & \longrightarrow & \tilde{E}(\bar{k}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle [n]} & & \downarrow{\scriptstyle [n]} & & \downarrow{\scriptstyle [n]} & & \\ 0 & \longrightarrow & E_1(K^{\mathrm{nr}}) & \longrightarrow & E(K^{\mathrm{nr}}) & \longrightarrow & \tilde{E}(\bar{k}) & \longrightarrow & 0 \end{array}$$

The map $E_1(K^{\mathrm{nr}}) \to E_1(K^{\mathrm{nr}})$ is an isomorphism (Corollary 8.7), and $\tilde{E}(\bar{k}) \to \tilde{E}(\bar{k})$ is surjective (Theorem 2.4) with its kernel isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$ (Theorem 6.5).
By Snake Lemma $E(K^{\mathrm{nr}})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ and $E(K^{\mathrm{nr}})/nE(K^{\mathrm{nr}}) = 0$. So if $P \in E(K)$, then $P = nQ$ for some $Q \in E(K^{\mathrm{nr}})$ and $[n]^{-1}P = \{Q \oplus T : T \in E[n]\} \subset K^{\mathrm{nr}}$, so $K([n]^{-1}P) \leq K^{\mathrm{nr}}$ which means that $K([n]^{-1}P)/K$ is unramified. □

10 Elliptic Curves over Number Fields

Suppose K is a number field, i.e. a finite extension of $\mathbb{Q}$, and E/K is an elliptic curve. For a prime $\mathfrak{p}$ of K, we write $K_\mathfrak{p}$ to denote the $\mathfrak{p}$-adic completion of K with respect to $\mathfrak{p}$. Write $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p} = \mathcal{O}_{K_\mathfrak{p}}/\pi_\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$ to denote the residue field.

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

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

Proof. Take a Weierstrass equation $a_1, \ldots, a_6 \in \mathcal{O}_K$. Then as E is nonsingular, $\Delta \neq 0$. We also have $\Delta \in \mathcal{O}_K$ as an integer polynomial in $a_1, \ldots, a_6$. Suppose we have the factorisation $(\Delta) = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}$. If $\mathfrak{p} \notin S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$, then $v_\mathfrak{p}(\Delta) = 0$ and hence $E/K_\mathfrak{p}$ has good reduction. □

Remark. If K has class number 1 (but, alas, not in general), we can find a Weierstrass equation $a_1, \ldots, a_6 \in \mathcal{O}_K$ which is minimal at all primes.

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

Proof. Take any prime $\mathfrak{p}$, we saw $E(K_\mathfrak{p})$ has a subgroup A of finite index with $A \cong (\mathcal{O}_{K_\mathfrak{p}}, +)$ which is torsion-free. So we have $E(K)_{\text{tors}} \hookrightarrow E(K_\mathfrak{p})_{\text{tors}} \hookrightarrow E(K_\mathfrak{p})/A$ which is finite. □

This is very much an overkill proof. Let's see another way to do it.

Lemma 10.3. *Let $\mathfrak{p}$ be a prime of good reduction with $n \notin \mathfrak{p}$. Then the reduction modulo $\mathfrak{p}$ gives an injective group homomorphism $E(K)[n] \hookrightarrow \tilde{E}(k_\mathfrak{p})[n]$.*

Proof. Proposition 9.6 gives a surjective group homomorphism $E(K_\mathfrak{p}) \to \tilde{E}(k_\mathfrak{p})$ with kernel $E_1(K_\mathfrak{p})$, which has no n-torsion by Corollary 8.7. □

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

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

The preceding lemma then shows that $|E(\mathbb{Q})_{\text{tors}}| \mid 5 \times 2^a$ for some $a \geq 0$ and $|E(\mathbb{Q})_{\text{tors}}| \mid 5 \times 3^b$ for some $b \geq 0$, which gives $|E(\mathbb{Q})_{\text{tors}}| \mid 5$. Let $T = (0, 0) \in E(\mathbb{Q})$, then after some calculation we find $5T = 0$, so indeed $|E(\mathbb{Q})_{\text{tors}}| = 5$.

Example 10.2. Suppose $E/\mathbb{Q}$ has $E : y^2 + y = x^3 + x^2$ which has $\Delta = -43$. Then we have

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

So $|E(\mathbb{Q})_{\text{tors}}| \mid 5 \times 2^a$ for some $a \geq 0$ and $|E(\mathbb{Q})_{\text{tors}}| \mid 9 \times 11^b$ for some $b \geq 0$, so $|E(\mathbb{Q})_{\text{tors}}| = 1$. Therefore $(0, 0)$ has infinite order, consequently $E(\mathbb{Q})$ has positive rank.

Example 10.3. Consider the congruent number curves $E_D/\mathbb{Q}$ given by $y^2 = x^3 - D^2x$ with D square-free. Then $\Delta = 2^6D^6$. We can spot some torsion points, e.g. E_D in facts contains all of its 2-torsions $0, (0,0), (\pm D, 0)$. Let $f(x) = x^3 - D^2x$. If $p \nmid 2D$, then

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

So if $p \equiv 3 \pmod 4$, then

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

Therefore $|\tilde{E}_D(\mathbb{F}_p)| = p + 1$. Let $m = |E_D(\mathbb{Q})_{\text{tors}}|$. We then have $4 \mid m \mid p + 1$ for all sufficiently large primes $p \equiv 3 \pmod 4$ ($p \nmid 2Dm$ would be sufficient). This then means that $m = 4$ by Dirichlet's theorem on primes in arithmetic progressions. Thus $E_D(\mathbb{Q})_{\text{tors}} = E_D[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$. Consequently, $E_D(\mathbb{Q})$ has positive rank iff D is a congruent number.

Lemma 10.4. *Let $E/\mathbb{Q}$ be given by a Weierstrass equation $a_1, \ldots, a_6 \in \mathbb{Z}$. Suppose $0 \neq T = (x, y) \in E(\mathbb{Q})_{\text{tors}}$. Then $4x, 8y \in \mathbb{Z}$. Furthermore, $x, y \in \mathbb{Z}$ if either $2 \mid a_1$ or $2T \neq 0$.*

Proof. The Weierstrass equation defines a formal group $\hat{E}$ over $R = \mathbb{Z}$. For $r \geq 1$, we have $\hat{E}(p^r\mathbb{Z}_p) = \{(x, y) \in E(\mathbb{Q}_p) : v_p(x) \leq -2r, v_p(y) \leq -3r\} \cup \{0\}$ with $\hat{E}(p^r\mathbb{Z}_p) \cong (\mathbb{Z}_p, +)$ for $r > 1/(p-1)$. So $\hat{E}(4\mathbb{Z}_2)$ and $\hat{E}(p\mathbb{Z}_p)$ (for odd p) are torsion-free. Since $0 \neq T \in E(\mathbb{Q})_{\text{tors}}$, we have $v_2(x) \geq -2, v_2(y) \geq -3$ and $v_p(x) \geq 0, v_p(y) \geq 0$ for all odd primes p, which shows that $4x, 8y \in \mathbb{Z}$.
Now suppose $T \in \hat{E}(2\mathbb{Z}_2)$, i.e. $v_2(x) = -2, v_2(y) = -3$, as $\hat{E}(2\mathbb{Z}_2)/\hat{E}(4\mathbb{Z}_2) \cong (\mathbb{F}_2, +)$ and $\hat{E}(4\mathbb{Z}_2)$ is torsion-free, we get $2T = 0$. Also, $(x, y) = T = -T = (x, -y - a_1x - a_3)$, so $2y + a_1x + a_3 = 0$ and therefore a_1 is odd. □

Example 10.4. On $E : y^2 + xy = x^3 + 4x + 1$, $(-1/4, 1/8) \in E(\mathbb{Q})[2]$ is a 2-torsion.

Theorem 10.5 (Lutz-Nagell)**.** *Suppose $E/\mathbb{Q}$ is given by $y^2 = f(x) = x^3 + ax + b$ and $0 \neq T = (x, y) \in E(\mathbb{Q})_{\text{tors}}$. We know that $x, y \in \mathbb{Z}$ (by the preceding lemma), and we have either $y = 0$ or $y^2 \mid 4a^3 + 27b^2$.*

Proof. If $2T = 0$ then $y = 0$ and we are done. Otherwise $0 \neq 2T = (x_2, y_2) \in E(\mathbb{Q})_{\text{tors}}$. Then x_2, y_2 are integers too. But $x_2 = (f'(x)/2y)^2 - 2x$, so $y \mid f'(x)$. Since E is nonsingular, f, f' are coprime, so there are polynomials $g, h \in \mathbb{Q}[X]$ such that $gf + h(f')^2 = 1$. In fact $(3X^2 + 4a)f'(X)^2 - 27(X^3 + aX - b)f(X) = 4a^3 + 27b^3$. Since $y \mid f'(x)$ and $y^2 = f(x)$ we conclude $y^2 \mid (4a^3 + 27b^2)$. □

Remark. Mazur showed that if $E/\mathbb{Q}$ is an elliptic curve, then $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to either $\mathbb{Z}/n\mathbb{Z}$ for some $1 \leq n \leq 12, n \neq 11$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ for some $1 \leq n \leq 4$. Moreover, all 15 possibilities occur.

11 Kummer Theory

Suppose K is a field and $\operatorname{char} K \nmid n$. Assume $\mu_n \subset K$.

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

Proof. L/K is Galois since $\mu_n \in K$ and $\operatorname{char} K \nmid n$. Consider the Kummer pairing $\langle , \rangle : \operatorname{Gal}(L/K) \times \Delta \to \mu_n, (\sigma, x) \mapsto \sigma(\sqrt[n]{x})/\sqrt[n]{x}$. This is well-defined: If $\alpha, \beta \in L$ have $\alpha^n = \beta^n = x$, then $\alpha/\beta \in K$, so $\sigma(\alpha/\beta) = \alpha/\beta$. The pairing is bilinear: We have

$$\langle \sigma\tau, x\rangle = \frac{\sigma\tau(\sqrt[n]{x})}{\tau(\sqrt[n]{x})}\frac{\tau(\sqrt[n]{x})}{\sqrt[n]{x}} = \langle \sigma, x\rangle\langle \tau, x\rangle$$

$$\langle \sigma, xy\rangle = \frac{\sigma(\sqrt[n]{xy})}{\sqrt[n]{xy}} = \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}}\frac{\sigma(\sqrt[n]{y})}{\sqrt[n]{y}} = \langle \sigma, x\rangle\langle \sigma, y\rangle$$

The pairing is also nondegenerate: If $\langle \sigma, x\rangle = 1$ for any $x \in \Delta$, then $\sigma(\sqrt[n]{x}) = \sqrt[n]{x}$ for all $x \in \Delta$, so σ fixes everything in L, i.e. $\sigma = \mathrm{id}_L$. Conversely, if $\langle \sigma, x\rangle = 1$ for all $\sigma \in \operatorname{Gal}(L/K)$, then $\sigma(\sqrt[n]{x}) = \sqrt[n]{x}$ for every $\sigma \in \operatorname{Gal}(L/K)$, so $\sqrt[n]{x} \in K$, which means that $x \in (K^\times)^n$.
The pairing gives injective group homomorphisms $\operatorname{Gal}(L/K) \to \operatorname{Hom}(\Delta, \mu_n)$ and $\Delta \to \operatorname{Hom}(\operatorname{Gal}(L/K), \mu_n)$. The first injection shows that $\operatorname{Gal}(L/K)$ is abelian and of exponent divide n (i.e. every element has order dividing n). Recall that is G is a finite abelian group of exponent dividing n, then $\operatorname{Hom}(G, \mu_n) \cong G$. So the injections give $|\operatorname{Gal}(L/K)| \leq |\Delta| \leq |\operatorname{Gal}(L/K)|$ which then implies the isomorphism. □

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

Theorem 11.2. *There is a bijection between finite subgroups $\Delta \leq K^\times/(K^\times)^n$ and finite abelian extensions L/K of exponent dividing n via $\Delta \mapsto K(\sqrt[n]{\Delta}), L \mapsto ((L^\times)^n \cap K^\times)/(K^\times)^n$.*

Proof. Suppose $\Delta \leq K^\times/(K^\times)^n$ be a finite subgroup and let $L = K(\sqrt[n]{\Delta})$. Consider $\Delta' = ((L^\times)^n \cap K^\times)/(K^\times)^n$. Clearly $\Delta \subset \Delta'$, so we need only to show that $|\Delta| = |\Delta'|$ to deduce $\Delta = \Delta'$. Indeed, the inclusion gives $L = K(\sqrt[n]{\Delta}) \subset K(\sqrt[n]{\Delta'}) \subset L$, so $K(\sqrt[n]{\Delta}) = K(\sqrt[n]{\Delta'})$ and therefore $|\Delta| = |\Delta'|$ by Lemma 11.1.
Conversely, let L/K be a finite abelian extension of exponent dividing n and let $\Delta = ((L^\times)^n \cap K^\times)/(K^\times)^n$. Now $K(\sqrt[n]{\Delta}) \subset L$. So to show that they are equal it suffices to show that they have the same degree over K.
Let $G = \operatorname{Gal}(L/K)$. The Kummer pairing gives an injection $\Delta \hookrightarrow \operatorname{Hom}(G, \mu_n)$. We want to show its surjectivity which would give the result by Lemma 11.1 since $|\operatorname{Hom}(G, \mu_n)| = |G|$ (noting that G has exponent dividing n).
Let $\chi : G \to \mu_n$ be a group homomorphism. By linear independence of characters, we know that there is a nonzero $a \in L$ with $y = \sum_{\tau \in G} \chi(\tau)^{-1}\tau(a) \neq 0$. For $\sigma \in G$, we have

$$\sigma(y) = \sum_{\sigma \in G} \sigma\tau(a) = \sum_{\tau \in G} \chi(\sigma^{-1}\tau)^{-1}\tau(a) = \chi(\sigma)y$$

So $\sigma(y^n) = y^n$ which means that $x = y^n \in K^\times \cap (L^\times)^n$, i.e. $x(K^\times)^n \in \Delta$. Also $\chi(\sigma) = \sigma(y)/y = \sigma(\sqrt[n]{x})/\sqrt[n]{x}$, so $\Delta \hookrightarrow \mathrm{Hom}(G, \mu_n)$ sends $x(K^\times)^n$ to χ. □

Proposition 11.3. *Suppose K is a number field that contains its μ_n. Let S be a finite set of primes of K. There are only finitely many finite abelian extensions L/K of exponent dividing n such that L/K is unramified at all $\mathfrak{p} \notin S$.*

Proof. The preceding theorem shows that any finite abelian extensions L/K of exponent dividing n must be of the form $K(\sqrt[n]{\Delta})$ for some finite subgroup $\Delta \subset K^\times/(K^\times)^n$. Suppose $\mathfrak{p}$ is a prime of K, then $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ where $\mathfrak{P}_i$ are distinct primes of L. If $x \in K^\times$ represents an element of Δ, then $nv_{\mathfrak{P}_i}(\sqrt[n]{x}) = v_{\mathfrak{P}_i}(x) = e_i v_{\mathfrak{p}}(x)$.
If $\mathfrak{p} \notin S$, then all e_i would be 1, which means that $v_{\mathfrak{p}}(x) \equiv 0 \pmod{n}$. This implies that $\Delta \subset K(S, n)$ where $K(S, n) = \{x \in K^\times/(K^\times)^n : \forall \mathfrak{p} \notin S, v_{\mathfrak{p}}(x) \equiv 0 \pmod{n}\}$. We will get our result if we can show that $K(S, n)$ is always finite. Let's give this result the glory of a separate lemma. □

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

Proof. It suffices to prove the lemma for $S = \varnothing$ as the map $K(S, n) \to (\mathbb{Z}/n\mathbb{Z})^{|S|}$ given by $x \mapsto (v_{\mathfrak{p}}(x) \bmod n)_{\mathfrak{p} \in S}$ has kernel $K(\varnothing, n)$.
If $x \in K^\times$ represents an element of $K(\varnothing, n)$, then $(x) = \mathfrak{a}^n$ for some fractional ideal $\mathfrak{a}$. There is an exact sequence

$$0 \longrightarrow \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n \longrightarrow K(\varnothing, n) \xrightarrow{x(K^\times)^n \mapsto [\mathfrak{a}]} \mathrm{Cl}_K[n] \longrightarrow 0$$

But $\mathrm{Cl}_K[n]$ is finite and $\mathcal{O}_K^\times$ is finitely generated, so $K(\varnothing, n)$ has to be finite. □

12 Mordell-Weil Theorem

Lemma 12.1. *Suppose E/K is an elliptic curve and L/K is a finite Galois extension. The natural map $E(K)/nE(K) \to E(L)/nE(L)$ has finite kernel.*

Proof. For each element in the kernel, we pick a coset representative $P \in E(K)$ and $Q \in E(L)$ with $nQ = P$. Note that if $\sigma \in \mathrm{Gal}(L/K)$, then $n(\sigma Q \ominus Q) = \sigma P \ominus P = P \ominus P = 0$, which means that $\sigma Q \ominus Q \in E[n]$. Since $\mathrm{Gal}(L/K)$ and $E[n]$ are finite, there are only finitely many possibilities for the map $\mathrm{Gal}(L/K) \to E[n], \sigma \mapsto \sigma Q \ominus Q$. But if $P_1, P_2 \in E(K)$ have $P_i = nQ_i$ for $Q_1, Q_2 \in E(L)$ and $\sigma Q_1 \ominus Q_1 = \sigma Q_2 \ominus Q_2$ for every $\sigma \in \mathrm{Gal}(L/K)$, then $Q_1 \ominus Q_2 \in E(K)$, which means that $P_1 \ominus P_2 \in nE(K)$. □

Theorem 12.2 (Weak Mordell-Weil)**.** *Suppose K is a number field and E/K is an elliptic curve. For any $n \geq 2$, the quotient $E(K)/nE(K)$ is finite.*

Proof. By the preceding lemma, we can replace K by any finite Galois extension of K, so WLOG $\mu_n \subset K$ and $E[n] \subset E(K)$. We claim that for any $P \in E(K)$, the extension $K([n]^{-1}P)/K$ satisfies the hypothesis of Proposition 11.3 with

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

If this were true, then

$$\bigcup_{P \in E(K)} K([n]^{-1}P)$$

is a finite union, hence generates a finite extension L of K. L/K is finite and Galois; Moreover, $E(K)/nE(K) \to E(L)/nE(L)$ is the zero map. Using the preceding lemma again shows the result.
So why is our claim true? As $E[n] \subset E(K)$, for any $P \in E(K)$, $\mathrm{Gal}(\bar{K}/K)$ acts on $[n]^{-1}P$. So $\mathrm{Gal}(\bar{K}/K([n]^{-1}P))$ is a normal subgroup of $\mathrm{Gal}(\bar{K}/K)$ and hence $K([n]^{-1}P)/K$ is Galois. Pick $Q \in [n]^{-1}P$ and consider the map $\mathrm{Gal}(K([n]^{-1}P)/K) \to E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2, \sigma \mapsto \sigma Q \ominus Q$. It's clear that this is a group homomorphism. Suppose $\sigma Q = Q$, then $\sigma(Q+T) = Q+T$ for any n-torsions T, which means that σ fixes $K([n]^{-1}P)$ pointwise, which forces it to be the identity. Thus $K([n]^{-1}P)/K$ is abelian and has exponent dividing n.
$K([n]^{-1}P)/K$ is unramified at all $\mathfrak{p} \notin S$ by Theorem 9.8. □

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

For a number field K and an elliptic curve E/K, there is a quadratic form ("canonical height") $\hat{h} : E(K) \to \mathbb{R}_{\geq 0}$ with the property that for any $B \geq 0$ we have $\{P \in E(K) : \hat{h}(P) \leq B\}$ is finite. We'll cover the theory of heights in a moment, but first let's see the consequences.

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

Proof. Fix an integer $n \geq 2$. By the preceding theorem, $m = |E(K)/nE(K)| < \infty$. Pick coset representatives $P_1, \ldots, P_m$. Let $\Sigma = \{P \in E(K) : \hat{h}(P) \leq \max\{\hat{h}(P_i) : 1 \leq i \leq m\}\}$. We claim that Σ generates $E(K)$. Indeed, if not, then there is some $P \in E(K) \setminus \langle \Sigma \rangle$ of minimal height. Then $P = P_i + nQ$ for some $1 \leq i \leq m, Q \in E(K)$ and we must have $Q \in E(K) \setminus \langle \Sigma \rangle$. We have $\hat{h}(P) \leq \hat{h}(Q)$ by minimality, so $4\hat{h}(P) \leq 4\hat{h}(Q) \leq n^2\hat{h}(Q) \leq \hat{h}(nQ) = \hat{h}(P - P_i) \leq \hat{h}(P - P_i) + \hat{h}(P + P_i) = 2\hat{h}(P) + 2\hat{h}(P_i)$. So $\hat{h}(P) \leq \hat{h}(P_i)$, which however means that $P \in \Sigma$, contradiction. □

13 Heights

For simplicity, we'll take our number field to be $K = \mathbb{Q}$, but it's not hard (just notationally chaotic) to extend to arbitrary number fields.

Definition 13.1. For $P \in \mathbb{P}^n(\mathbb{Q})$, we express it in projective coordinates $(a_0 : \cdots : a_n)$ such that $a_0, \ldots, a_n \in \mathbb{Z}$ have $\gcd(a_0, \ldots, a_n) = 1$. The height of P is $H(P) = \max_{0 \leq i \leq n} |a_i|$.

Lemma 13.1. *Let $f_1, f_2 \in \mathbb{Q}[X_1, X_2]$ be coprime homogenous polynomials of degree d. Let $F : \mathbb{P}^1 \to \mathbb{P}^1, (x_1, x_2) \mapsto (f_1(x_1, x_2) : f_2(x_1, x_2))$. Then there are constants $c_1, c_2 > 0$ such that $c_1 H(P)^d \leq H(F(P)) \leq c_2 H(P)^d$ for all $P \in \mathbb{P}^1(\mathbb{Q})$.*

Proof. WLOG f_1, f_2 have integer coefficients. Write $P = (a : b)$ with a, b coprime integers. Then $H(F(P)) \leq \max\{|f_1(a,b)|, |f_2(a,b)|\} \leq c_2(\max\{a,b\})^d$ where c_2 is the bigger one between the sums of absolute values of the respective coefficients of f_i.
As for the lower bound, we claim that there exists polynomials $(g_{ij})_{1 \leq i,j \leq 2} \in$

$\mathbb{Z}[X_1, X_2]$ of degree $d-1$ with some integer $\kappa \in \mathbb{Z}_{>0}$ such that $\sum_{j=1}^{2} g_{ij} f_j = \kappa X_i^{2d-1}$. Indeed, this comes from running Euclid's algorithm on the pairs $f_1(X,1), f_2(X,1)$ and $f_1(1,X), f_2(1,X)$.
Write $P = (a_1 : a_2)$ with a_1, a_2 coprime integers, then $\sum_j g_{ij}(a_1,a_2) f_j(a_1,a_2) = \kappa a_i^{2d-1}$. Thus $\gcd(f_1(a_1,a_2), f_2(a_1,a_2)) \mid \gcd(\kappa a_1^{2d-1}, \kappa a_2^{2d-1}) = \kappa$. Then

$$|\kappa a_i^{2d-1}| \leq \max_j |f_j(a_1,a_2)| \sum_j |g_{ij}(a_1,a_2)| \leq \kappa H(F(P)) \gamma_i H(P)^{d-1}$$

where γ_i is the sum of the absolute values of the coefficients of g_{i1}, g_{i2}. So $|a_i|^{2d-1} \leq H(F(P))\gamma_i H(P)^{d-1}$ and therefore

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

which rearranges to give the result. □

For $x \in \mathbb{Q}$, we write $H(x) = H((x:1))$.
Suppose $E/\mathbb{Q}$ is an elliptic curve $E : y^2 = x^3 + ax + b$.

Definition 13.2. The height on the elliptic curve E is defined as

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

The logarithmic height is $h = \log H$.

Lemma 13.2. *Let E, E' be elliptic curves over $\mathbb{Q}$ and $\phi : E \to E'$ an isogeny defined over $\mathbb{Q}$. Then there is $c > 0$ such that $|h(\phi(P)) - (\deg \phi) h(P)| \leq c$ for all $P \in E(\mathbb{Q})$.*

Proof. Let ξ be as in Lemma 5.5 and $d = \deg \phi = \deg \xi$. By the preceding lemma, there are $c_1, c_2 > 0$ with $c_1 H(P)^d \leq H(\phi(P)) \leq c_2 H(P)^d$ for all $P \in E(\mathbb{Q})$, and taking logs gives $|h(\phi(P) - dh(P)| \leq c = \max\{\log c_2, -\log c_1\}$. □

Example 13.1. Take $\phi = [2] : E \to E$, then we conclude by the preceding lemma that there is some $c > 0$ with $|h(2P) - 4h(P)| < c$ for all $P \in E(\mathbb{Q})$.

This example in particular gives the convergence of

Definition 13.3. The canonical height is

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

Indeed, we have, for $m \geq n$,

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

as $n \to \infty$. So the limit defining $\hat{h}$ does always exist.
A special case of the calculation (i.e. taking $n = 0$) reveals that

Lemma 13.3. *$|h(P) - \hat{h}(P)|$ is bounded over $P \in E(\mathbb{Q})$.*

Corollary 13.4. *For any $B > 0$, $|\{P \in E(\mathbb{Q}) : \hat{h}(P) \leq B\}|$ is finite.*

Proof. The same statement is clearly true if we replace $\hat{h}$ by h, so we conclude by the preceding lemma. □

So the only thing left to show is that $\hat{h}$ is a quadratic form.

Lemma 13.5. *Suppose $\phi : E \to E'$ is an isogeny over $\mathbb{Q}$, then $\hat{h}(\phi(P)) = (\deg \phi)\hat{h}(P)$.*

Proof. Take $c > 0$ with $|h(\phi(P)) - (\deg \phi)h(P)| \leq c$ for all $P \in E(\mathbb{Q})$. Replace P by $2^n P$, divide through by 4^n, and take $n \to \infty$. □

Corollary 13.6. *$\hat{h}$ (unlike h) does not depend on the choice of Weierstrass equation for E.*

Corollary 13.7. *$\hat{h}(nP) = n^2\hat{h}(P)$ for all $P \in E(\mathbb{Q})$.*

Lemma 13.8. *Let $E/\mathbb{Q}$ be an elliptic curve and fix a Weiertrass equation $y^2 = x^3 + ax + b, a, b \in \mathbb{Z}$ for it. Then there is some $C > 0$ such that*

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

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

Proof. Suppose $P, Q, P+Q, P-Q$ have x-coordinates $x_1, \ldots, x_4$. Write $x_i = r_i/s_i$ where $r_i, s_i \in \mathbb{Z}$ are coprime. We then have $(s_3s_4 : r_3r_4 + r_4s_3 : r_3r_4) = (W_0 : W_1 : W_2)$ where W_0, W_1, W_2 are integer polynomials in r_1, s_1, r_2, s_2 with degrees at most 2 both in r_1, s_1 and r_2, s_2, and $W_0 = (r_1s_2 - r_2s_1)^2$. Then

$$\begin{aligned} H(P+Q)H(P-Q) &= \max\{|r_3|, |s_3|\} \max\{|r_4|, |s_4|\} \\ &\leq 2\max\{|s_3s_4|, |r_3s_4 + r_4s_3|, |r_3r_4|\} \\ &\leq 2\max\{|W_0|, |W_1|, |W_2|\} \leq CH(P)^2H(Q)^2 \end{aligned}$$

for some constant C. □

Theorem 13.9. *$\hat{h} : E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ is a quadratic form.*

Proof. Taking logarithm in the preceding lemma gives (the cases when some of $P, Q, P \pm Q$ is 0_E are either trivial or follows from the preceding discussion)

$$h(P+Q) + h(P-Q) \leq 2h(P) + 2h(Q) + c$$

for some constant c. Taking a limit gives $\hat{h}(P+Q) + \hat{h}(P-Q) \leq 2\hat{h}(P) + 2\hat{h}(Q)$. Replacing P, Q by $P+Q, P-Q$ gives the reverse inequality, so we have the parallelogram law. □

Remark. How about the case where we work over a general number field that's not $\mathbb{Q}$? Well, most things pretty much follows in exactly the same fashion. The only intricacy is to generalise our original definition of height on a projective space.
Recall that the places of a number field K are the finite places given by $|x|_{\mathfrak{p}} =$

$c^{-v_\mathfrak{p}(x)}$ for some constant $c > 1$, and the infinite places (arising from real and complex embeddings) $|x|_\sigma = |\sigma(x)|^d$ for some $d > 0$. Appropriate choices of c, d gives rise to the so-called product formula $\prod_v |\lambda|_v = 1$ for all $\lambda \in K$, where v runs through all places.
Given $P = (a_0 : a_1 : \cdots : a_n) \in \mathbb{P}^n(K)$, we can then define

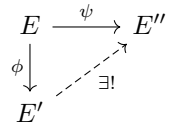
$$H(P) = \prod_{v \text{ place}} \left(\max_{0 \le i \le n} |a_i|_v \right)$$

which, as it turns out, works.

14 Dual Isogenies and Weil Pairing

Suppose K is a perfect field and E/K an elliptic curve.

Proposition 14.1. *Let $\Phi \subset E(\bar{K})$ be a finite subgroup that's stable under the $\mathrm{Gal}(\bar{K}/K)$-action. Then there is an elliptic curve E'/K and a separable isogeny $\phi : E \to E'$ defined over K with kernel Φ such that every isogeny $\psi : E \to E''$ with kernel containing Φ uniquely factors through ϕ.*



Proof. Omitted. □

Proposition 14.2. *Let $\phi : E \to E'$ be an isogeny and $\deg \phi = n$, then there is a unique isogeny $\hat{\phi} : E' \to E$ with $\hat{\phi} \circ \phi = [n]$.*

Definition 14.1. $\hat{\phi}$ as thus is called the dual isogeny of ϕ.

Proof. When ϕ is separable, this follows directly from the preceding proposition since $|\ker \phi| = n \implies \ker \phi \subset \ker[n]$.
The inseparable case is omitted. □

Remark. 1. If we write $E_1 \sim E_2$ to say that E_1, E_2 are isogenous, then $\sim$ is an equivalence relation.
2. As $\deg[n] = n^2$, we have $\deg \hat{\phi} = n = \deg \phi$. Moreover, $\hat{[n]} = [n]$.
3. We have $\phi \circ \hat{\phi} \circ \phi = \phi \circ [n]_E = [n]_{E'} \circ \phi$, so $(\phi \circ \hat{\phi} - [n]_{E'}) \circ \phi = 0$, which means that $\phi \circ \hat{\phi} = [n]_{E'}$ as ϕ is nonconstant hence surjective on $\bar{K}$-points. In particular, $\hat{\hat{\phi}} = \phi$.

Definition 14.2. We have a map $\mathrm{sum} : \mathrm{Div}(E) \to E, \sum_P n_P[P] \mapsto \bigoplus_P n_P P$.

Recall that we have an isomorphism $E \cong \mathrm{Pic}^0(E), P \mapsto [[P] - [0_E]]$. This sends $\mathrm{sum}\, D$ to $[D]$ for any divisor $D \in \mathrm{Div}^0(E)$. Consequently,

Lemma 14.3. *$D \in \mathrm{Div}(E)$ is principal iff $\deg D = 0$ and $\mathrm{sum}\, D = 0$.*

For an isogeny $\phi : E \to E'$, we write $E[\phi]$ for $\ker \phi$.
Let $\phi : E \to E'$ be an isogeny of degree n with dual $\hat{\phi} : E' \to E$. Assume $\operatorname{char} K \nmid n$ (so $\phi, \hat{\phi}$ are separable).
The Weil pairing $e_\phi : E[\phi] \times E'[\hat{\phi}] \to \mu_n$ (on $\bar{K}$-points) is defined as follows: Let $T \in E'[\hat{\phi}]$, then $nT = 0$, so $\exists f \in \bar{K}(E')^\times$ such that $\operatorname{div}(f) = n[T] - n[0]$. Pick $T_0 \in E(\bar{K})$ such that $\phi T_0 = T$, then

$$\phi^*[T] - \phi^*[0] = \sum_{P \in E[\phi]} [P \oplus T_0] - \sum_{P \in E[\phi]} [P]$$

has sum $nT_0 = \hat{\phi}(\phi(T_0)) = \hat{\phi}(T) = 0$. So there is some $g \in \bar{K}(E)^\times$ with $\operatorname{div} g = \phi^*[T] - \phi^*[0]$.
Now $\operatorname{div}(\phi^* f) = \phi^*(\operatorname{div}(f)) = \phi^*(n[T] - n[0]) = \operatorname{div}(g^n)$. That is, $\phi^* f = c g^n$ for some $c \in \bar{K}^\times$. By rescaling f we can assume WLOG that $c = 1$, i.e. $\phi^* f = g^n$.
If $S \in E[\phi]$, then $\phi \circ \tau_S = \phi, \tau_S^* \circ \phi^* = \phi^*$. Therefore $\operatorname{div}(\tau_S^* g) = \tau_S^*(\operatorname{div} g) = \operatorname{div} g$, which means that $\tau_S^* g = \zeta g$ for some $\zeta \in \bar{K}^\times$. In other words, $\zeta = g(X \oplus S)/g(X)$ for all $X \in E(\bar{K})$ at which g has order 0. Now $\zeta^n = f(\phi(X \oplus S))/f(\phi(X)) = 1$ since $S \in E[\phi]$, so $\zeta \in \mu_n$ and we can set $e_\phi(S, T) = \zeta$.

Proposition 14.4. *e_ϕ is bilinear and nondegenerate.*

Proof. Linearity in first argument is easy:

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

As for linearity in second argument, let $T_1, T_2 \in E'[\hat{\phi}]$ have $\operatorname{div}(f_i) = n[T_i] - n[0], \phi^* f_i = g_i^n$. Choose $h \in \bar{K}(E)^\times$ with $\operatorname{div}(h) = [T_1] + [T_2] - [T_1 \oplus T_2] - [0]$ and set $f = f_1 f_2 / h^n$. Then we have $\operatorname{div} f = n[T_1 \oplus T_2] - n[0]$ and $\phi^* f = (\phi^* f_1)(\phi^* f_2)/(\phi^* h)^n = (g_1 g_2 / \phi^* h)^n$. So we can set $g = g_1 g_2 / \phi^* h$. Thus

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

Non-degeneracy is a wittle harder. For $T \in E'[\hat{\phi}]$, suppose $e_\phi(-, T) = 0$, then $\tau_S^* g = g$ for all $s \in E[\phi]$. Now $\bar{K}(E)/\phi^* \bar{K}(E')$ is a Galois extension with Galois group $E[\phi]$ ($S \in E[\phi]$ acts on E via τ_S^*). So $g \in \phi^* \bar{K}(E')$, i.e. $g = \phi^* h$ for some $h \in \bar{K}(E')$. Consequently $\phi^* f = g = \phi^*(h^n)$ which means that $f = h^n$, i.e. $\operatorname{div} h = [T] - [0]$. But $\operatorname{sum}([T] - [0]) \neq 0$ unless $T = 0$.
So $E'[\hat{\phi}] \to \operatorname{Hom}(E[\phi], \mu_n), T \mapsto (S \mapsto e_\phi(S, T))$ is injective, so this is an isomorphism by counting, which forces e_ϕ to be nondegenerate. □

Remark. 1. If E, E', ϕ are defined over K, then e_ϕ is Galois-equivariant, in the sense that $e_\phi(\sigma S, \sigma T) = e_\phi(S, T)$ for all $\sigma \in \operatorname{Gal}(\bar{K}/K)$.
2. When $\phi = [n] : E \to E$ (so $\hat{\phi} = [n]$), we have $e_\phi = e_n : E[n] \times E[n] \mapsto \mu_{n^2}$. The image is contained in $\mu_n \subset \mu_{n^2}$ since $E[n] \times E[n]$ has exponent n.

Corollary 14.5. *If $E[n] \subset E(K)$, then $K \supset \mu_n$.*

Proof. As e_n is nondegenerate, there are $S, T \in E[n]$ such that $\zeta_n = e_n(S, T)$ is a primitive n^{th} root of unity. By Galois equivariance, we have $\sigma \zeta_n = e_n(\sigma S, \sigma T) = e_n(S, T) = \zeta_n$ for any $\sigma \in \operatorname{Gal}(\bar{K}/K)$. Thus $\zeta_n \in K$. □

Example 14.1. There is no elliptic curve $E/\mathbb{Q}$ with $E(\mathbb{Q})_{\text{tors}} \cong (\mathbb{Z}/3\mathbb{Z})^2$ since the preceding corollary would imply $\mu_3 \in \mathbb{Q}$ which is false.

Remark. The Weil pairing is in fact alternating, i.e. $e_n(T,T) = 0$ for all $T \in E[n]$. In particular, by expanding $e_n(S \oplus T, S \oplus T)$ we conclude that $e_n(S,T) = e_n(T,S)^{-1}$.

15 Galois Cohomology

15.1 Group and Galois Cohomology

Let G be a group and A an abelian group that's a G-module, i.e. equipped with a homomorphism $G \to \text{Aut}(A)$. Equivalently, A is a module over the group ring $\mathbb{Z}[G]$.

Definition 15.1. The 0^{th} group cohomology is $H^0(G,A) = A^G = \{a \in A : \forall \sigma \in G, \sigma(a) = a\}$.
The collection of the 1^{st} cochains is $C^1(G,A) = \{\text{maps } G \to A\}$; The collection of the 1^{st} cocycles is $Z^1(G,A) = \{(a_\sigma)_{\sigma \in G} : a_{\sigma\tau} = \sigma(a_\tau) + a_\sigma\}$; The collection of the 1^{st} coboundaries is $B^1(G,A) = \{(\sigma b - b)_{\sigma \in A} : b \in A\}$.
Clearly $B^1(G,A) \subset Z^1(G,A) \subset C^1(G,A)$. We set the 1^{st} group cohomology to be $H^1(G,A) = Z^1(G,A)/B^1(G,A)$.

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

Theorem 15.1. *A short exact sequence of G-modules*

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

gives rise to a long exact sequence of abelian groups

$$0 \longrightarrow A^G \xrightarrow{\phi} B^G \xrightarrow{\psi} C^G \xrightarrow{\delta} H^1(G,A) \xrightarrow[\phi_*]{} H^1(G,B) \xrightarrow[\psi_*]{} H^1(G,C)$$

Proof. Omitted, but we're gonna cover what δ is.
Suppose $c \in C^G$, then there is some $b \in B$ with $\psi(b) = c$. For any $\sigma \in G$, we know that $\psi(\sigma b - b) = \sigma c - c = 0$, so $\sigma b - b \in \ker \psi = \text{Im}\, \phi$. Therefore $\sigma b - b = \phi(a_\sigma)$ for some $a_\sigma \in A$. We define $\delta(c) = (a_\sigma)_{\sigma \in G} \bmod B^1(G,A)$, which is well-defined as one can check. □

Theorem 15.2. *Let A be a G-module and $H \lhd G$ is a normal subgroup, then there is an "inflation-restriction" exact sequence*

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

Proof. Omitted. □

Let K be a perfect field. $\text{Gal}(\bar{K}/K)$ is a topological group whose topology is generated by the basis of open sets given by subgroups of the form $\text{Gal}(\bar{K}/L)$ where L is a finite extension of K. In the case $G = \text{Gal}(\bar{K}/K)$, we modify

the definition of a G-module by insisting that $\mathrm{Stab}(a)$ is always open; And we modify the definition of H^1 by insisting that all cochains $G \to A$ considered are continuous, where A is given the discrete topology. As usual one can check that nothing really breaks.
Consequently,

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

with the direct limit taken with respect to the inflation maps.

15.2 Hilbert's Theorem 90; Kummer Theory

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

Proof. Let $G = \mathrm{Gal}(L/K)$ and let $(a_\sigma)_{\sigma\in G} \in Z^1(G, L^\times)$. By linear independence of characters, there is some $y \in L$ such that $x = \sum_{\tau\in G} a_\tau^{-1}\tau(y) \neq 0$. For $\sigma \in G$, we have

$$\sigma(x) = \sum_{\tau\in G} \sigma(a_\tau)^{-1}\sigma\tau(y) = a_\sigma \sum_{\tau\in G} a_{\sigma\tau}^{-1}\sigma\tau(y) = a_\sigma x$$

So $a_\sigma = \sigma(x)/x$ which means that $(a_\sigma)_{\sigma\in G} \in B^1(G, L^\times)$, hence the result. □

Corollary 15.4. $H^1(\mathrm{Gal}(\bar{K}/K), \bar{K}^\times) = 0$.

Assume $\mathrm{char}\, K \nmid n$, then there is an exact sequence of $\mathrm{Gal}(\bar{K}/K)$-modules

$$0 \longrightarrow \mu_n \longrightarrow \bar{K}^\times \xrightarrow{x\mapsto x^n} \bar{K}^\times \longrightarrow 0$$

So we get another exact sequence

$$\bar{K}^\times \xrightarrow{x\mapsto x^n} \bar{K}^\times \longrightarrow H^1(\mathrm{Gal}(\bar{K}/K), \mu_n) \longrightarrow H^1(\mathrm{Gal}(\bar{K}/K), \bar{K}^\times)$$

But $H^1(\mathrm{Gal}(\bar{K}/K), \bar{K}^\times) = 0$ by the last corollary, so $H^1(\mathrm{Gal}(\bar{K}/K), \mu_n) \cong K^\times/(K^\times)^n$. If $\mu_n \subset K$ then $\mathrm{Hom}_{\mathrm{cts.}}(\mathrm{Gal}(\bar{K}/K), \mu_n) \cong K^\times/(K^\times)^n$.
Suppose now that L/K is a finite Galois extension. The surjective homomorphism $\pi : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Gal}(L/K)$ induces an embedding

$$\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n) \hookrightarrow \mathrm{Hom}_{\mathrm{cts.}}(\mathrm{Gal}(\bar{K}/K), \mu_n) \cong K^\times/(K^\times)^n, \chi \mapsto \chi \circ \pi$$

whose image is a finite subgroup $\Delta \subset K^\times/(K^\times)^n$. Suppose $\mathrm{Gal}(L/K)$ is abelian of exponent dividing n, then

$$[L : K] = |\,\mathrm{Gal}(L/K)| = |\,\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)| = |\Delta|$$

which can be compared with Theorem 11.2.

15.3 Mordell-Weil with Cohomology

We write $H^1(K, -) = H^1(\mathrm{Gal}(\bar{K}/K), -)$.

Lemma 15.5. *Suppose K is a finite extension of $\mathbb{Q}_p$, then*

$$\ker(H^1(K, \mu_n) \to H^1(K^{\mathrm{nr}}, \mu_n)) \subset \{x \in K^\times/(K^\times)^n : v(x) \equiv 0 \pmod{n}\}$$

Proof. By Theorem 15.3, we have the identifications $H^1(K, \mu_n) = K^\times/(K^\times)^n$ and $H^1(K^{\mathrm{nr}}, \mu_n) = (K^{\mathrm{nr}})^\times/((K^{\mathrm{nr}})^\times)^n$. The discrete valuation $v : K^\times \to \mathbb{Z}$ extends to a discrete valuation $v : (K^{\mathrm{nr}})^\times \to \mathbb{Z}$. So if $x \in K^\times$ is such that $x = y^n$ for some $y \in (K^{\mathrm{nr}})^\times$, then $v(x) = nv(y) \equiv 0 \pmod{n}$. □

Remark. One can also show that if $p \nmid n$ then this is actually an equality.

Let $\phi : E \to E'$ be an isogeny of elliptic curves over K. Then there is a short exact sequence of $\mathrm{Gal}(\bar{K}/K)$-modules

$$0 \longrightarrow E[\phi] \longrightarrow E \xrightarrow{\phi} E' \longrightarrow 0$$

which then gives rise to a long exact sequence of abelian groups

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

Modifying this gives a short exact sequence

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

Now take K a number field. For each place v, we fix an emedding $\bar{K} \subset \bar{K}_v$. Then we have a natural inclusion $\mathrm{Gal}(\bar{K}_v/K_v) \subset \mathrm{Gal}(\bar{K}/K)$. Taking product over all places, we have a commutative diagram

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

Definition 15.2. The ϕ-Selmer group is

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

The Tate-Shafarevich group is

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

We get a short exact sequence

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

Taking $\phi = [n]$ gives

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

Theorem 15.6. *$S^{(n)}(E/K)$ is finite.*

Of course this implies Theorem 12.2.

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

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

So we are free to replace our field by a finite Galois extension of it, in particular we can assume that $E[n] \subset E(K)$ (hence $\mu_n \subset K$). Therefore $E[n] \cong \mu_n \times \mu_n$ as a $\mathrm{Gal}(\bar{K}/K)$-module. Hence $H^1(K, E[n]) \cong H^1(K, \mu_n) \times H^1(K, \mu_n) \cong (K^\times/(K^\times)^n) \times (K^\times/(K^\times)^n)$.
Let $S = \{\text{primes of bad reduction for } E/K\} \cup \{v \mid n\infty\}$, which is a finite set of primes. The subgroup of $H^1(K, A)$ unramified outside S is

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

Exact sequence time.

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & E(K_v) & \xrightarrow{[n]} & E(K_v) & \xrightarrow{\delta_v} & H^1(K_v, E[n]) & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & E(K_v^{\mathrm{nr}}) & \xrightarrow{[n]} & E(K_v^{\mathrm{nr}}) & \longrightarrow & H^1(K_v^{\mathrm{nr}}, E[n]) & \longrightarrow & \cdots \end{array}$$

Now $[n] : E(K_v^{\mathrm{nr}}) \to E(K_v^{\mathrm{nr}})$ is surjective for any $v \notin S$ (recall Theorem 9.8), so $E(K_v^{\mathrm{nr}}) \to H^1(K_v^{\mathrm{nr}}, E[n])$ is actually the zero map and thus $\mathrm{Im}\,\delta_v \subset \ker(H^1(K_v, E[n]) \to H^1(K_v^{\mathrm{nr}}, E[n]))$. We package the rest of the proof in the following lemma. □

Lemma 15.7. *Let K be a finite extension of $\mathbb{Q}_p$, then*

$$\ker(H^1(K, \mu_n) \to H^1(K^{\mathrm{nr}}, \mu_n)) \subset \left\{x \in \frac{K^\times}{(K^\times)^n} : v(x) \equiv 0 \pmod{n}\right\}$$

Therefore $S^{(n)}(E/K) \subset H^1(K, E[n]; S) \cong H^1(K, \mu_n; S)^2 \subset K(S, n)^2$.

$K(S, n)$ is finite by Lemma 11.4, so we conclude the finiteness of $S^{(n)}(E/K)$.

Remark. $S^{(n)}(E/K)$ is finite and effectively computable. On the other hand, it's conjectured that $|Ш(E/K)| < \infty$, which would imply the effective computability of the rank of $E(K)$.

16 Descent by Cyclic Isogeny

16.1 Basic Idea

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

$E[\phi] \cong \mu_n$ as a Galois module via $S \mapsto e_\phi(S, T)$. We get a short exact sequence

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

which gives rise to a long exact sequence

$$\cdots \longrightarrow E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(K, \mu_n) \longrightarrow \cdots$$
$$\alpha \searrow \quad \downarrow \cong$$
$$K^\times/(K^\times)^n$$

Theorem 16.1. *Let $f \in K(E')$ and $g \in K(E)$ be such that $\operatorname{div}(f) = n[T] - n[0]$ and $\phi^* f = g^n$. Then $\alpha(P) = f(P) \bmod (K^\times)^n$ for any $P \in E'(K) \setminus \{0, T\}$.*

Proof. Let $Q \in \phi^{-1}P$, then $\delta(P)$ is represented by the cocycle $\sigma \mapsto \sigma(Q) \ominus Q \in E[\phi] \cong \mu_n$. We have

$$e_\phi(\sigma Q \ominus Q, T) = \frac{g(\sigma Q \ominus Q \oplus Q)}{g(Q)} = \frac{g(\sigma Q)}{g(Q)} = \frac{\sigma(g(Q))}{g(Q)} = \frac{\sigma(\sqrt[n]{f(P)})}{\sqrt[n]{f(P)}}$$

Therefore δP is represented by the cocycle $\sigma \mapsto \sigma(\sqrt[n]{f(P)})/\sqrt[n]{f(P)}$. But $K^\times/(K^\times)^n \cong H^1(K, \mu_n)$ via exactly $x \mapsto (\sigma \mapsto \sigma(\sqrt[n]{x})/\sqrt[n]{x})$, which gives the result. □

16.2 Descent by 2-Isogeny

Let's now see what happens when we set $n = 2$. Consider $E : y^2 = x(x^2 + ax + b), \Delta = b(a^2 - 4ab) \neq 0$ and $E' = y^2 = x(x^2 + a'x + b'), a' = -2a, b' = a^2 - 4b$. Recall that we have a 2-isogeny $\phi : E \to E', (x, y) \mapsto ((y/x)^2, y(x^2 - b)/x^2)$ whose dual is $\hat{\phi} : E' \to E, (x, y) \mapsto ((1/4)(y/x)^2, (1/8)y(x^2 - b)/x^2)$. Then $E[\phi] = \{0, T\}, T = (0, 0) \in E$ and $E'[\hat{\phi}] = \{0, T'\}, T' = (0, 0) \in E'$.

Proposition 16.2. *There is a group homomorphism $E'(K) \to K^\times/(K^\times)^2$ via*

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

with kernel $\phi E(K)$.

Proof. Apply the preceding theorem with $f = x \in K(E')$ and $g = y/x \in K(E)$. □

One can alternatively show this by direct calculation (example sheet).
So we have injective group homomorphisms

$$\alpha_E : \frac{E(K)}{\hat{\phi}E'(K)} \hookrightarrow \frac{K^\times}{(K^\times)^2}, \alpha_{E'} : \frac{E'(K)}{\phi E(K)} \hookrightarrow \frac{K^\times}{(K^\times)^2}$$

Lemma 16.3. $2^{\operatorname{rank} E(K)} = 2^{\operatorname{rank} E'(K)} = |\operatorname{Im} \alpha_E||\operatorname{Im}(\alpha_{E'})|/4$.

Proof. Suppose we have homomorphisms $f : A \to B, g : B \to C$ of abelian groups. There is an exact sequence

$$0 \longrightarrow \ker(f) \longrightarrow \ker(g \circ f) \xrightarrow{f} \ker g \longrightarrow \operatorname{coker}(f) \xrightarrow[g]{} \operatorname{coker}(g \circ f) \longrightarrow \operatorname{coker}(g) \longrightarrow 0$$

Applying this to $g = \hat{\phi}, f = \phi$ gives

$$0 \longrightarrow E(K)[\phi] \longrightarrow E(K)[2] \xrightarrow{\phi} E'(K)[\hat{\phi}] \longrightarrow E'(K)/\phi E(K) \xrightarrow[\hat{\phi}]{} E(K)/2E(K) \longrightarrow E(K)/\hat{\phi}E'(K) \longrightarrow 0$$

which gives $|E(K)/2E(K)|/|E(K)[2]| = |\operatorname{Im}\alpha_E||\operatorname{Im}(\alpha_{E'})|/4$.
Write $E(K) = \Delta \times \mathbb{Z}^r$ with Δ finite by Theorem 12.3. Then $E(K)/2E(K) \cong (\Delta/2\Delta) \times (\mathbb{Z}/2\mathbb{Z})^r$ and $E(K)[2] \cong \Delta[2]$. We know that $\Delta[2]$ and $\Delta/2\Delta$ have the same order since Δ is finite. So we conclude $|E(K)/2E(K)|/|E(K)[2]| = 2^r$, as desired. □

Lemma 16.4. *Suppose $a, b \in \mathcal{O}_K$, then $\operatorname{Im}\alpha_E \subset K(S, 2)$ where S consists of primes dividing b.*

Proof. We want to show that if $x, y \in K$ have $y^2 = x(x^2 + ax + b)$ and $v_\mathfrak{p}(b) = 0$, then $v_\mathfrak{p}(x) \equiv 0 \pmod 2$.
If $v_\mathfrak{p}(x) < 0$, then Lemma 9.1 shows that $v_\mathfrak{p}(x) = -2r$ for some $r \geq 1$.
If $v_\mathfrak{p}(x) > 0$ (the case $v_\mathfrak{p}(x) = 0$ is vacuously true), then $v_\mathfrak{p}(x^2 + ax + b) = 0$, thus $v_\mathfrak{p}(x) = v_\mathfrak{p}(y^2) = 2v_\mathfrak{p}(y) \equiv 0 \pmod 2$. □

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

Proof. If $b_1 \in (K^\times)^2$ or $b_2 \in (K^\times)^2$, then both conditions are clearly satisfied. Assume henceforth that b_1, b_2 are not squares.
$b_1(K^\times)^2 \in \operatorname{Im}(\alpha_E)$ iff there is some $(x, y) \in E(K)$ such that $x = b_1 t^2$ for some $t \in K^\times$. Suppose this is true, then $y^2 = b_1 t^2((b_1 t^2)^2 + a b_1 t^2 + b)$. We divide through to get $(y/(b_1 t))^2 = b_1 t^4 + a t^2 + b_2$ which gives the solution $u = t, v = 1, w = y/(b_1 t)$ to the equation.
Conversely, if we have a nontrivial solution (u, v, w), then $uv \neq 0$ and hence $(b_1(u/v)^2, b_1 uw/v^3) \in E(K)$. □

Now take $K = \mathbb{Q}$.

Example 16.1. Let's go back to our friend $E : y^2 = x^3 - x$ (so $a = 0, b = -1$). Then $\operatorname{Im}\alpha_E = \langle -1 \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. We have $E' : y^2 = x^3 + 4x$ and $\operatorname{Im}\alpha_{E'} \subset \langle -1, 2 \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.
Applying the preceding lemma to $b_1 = -1, b_1 = 2$ and $b_1 = -2$ gives the equations $w^2 = -u^4 - 4v^4, w^2 = 2u^4 + 2v^4, w^2 = -2u^4 - 2v^4$. The first and third equations clearly have no nontrivial solution over $\mathbb{Q}$ (even over $\mathbb{R}$). The second one has solution $(u, v, w) = (1, 1, 2)$. Thus $\operatorname{Im}\alpha_{E'} = \langle 2 \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, giving rank $E(\mathbb{Q}) = 0$. Consequently, 1 is not a congruent number.

Example 16.2. Let's look at the curves $E : y^2 = x^3 + px$ where p is a prime and $p \equiv 5 \pmod 8$. For $b_1 = -1$, we get the equation $w^2 = -u^4 - pv^4$ which doesn't have nontrivial solutions. Therefore $\operatorname{Im} \alpha_E = \langle p \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.
We have $E' : y^2 = x^3 - 4px$ and $\operatorname{Im} \alpha_{E'} \subset \langle -1, 2, p \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Note that $\alpha_{E'}(T') = (-4p)(\mathbb{Q}^\times)^2 = (-p)(\mathbb{Q}^\times)^2$. So to check the rest it suffices to check the cases $b_1 = 2, b_1 = -2, b_1 = p$, giving equations $w^2 = 2u^4 - 2pv^4, w^2 = -2u^4 + 2pv^4, w^2 = pu^4 - 4v^4$.
Suppose $w^2 = 2u^4 - 2pv^4$ has a nontrivial solution (u, v, w) in $\mathbb{Q}$. WLOG $u, v \in \mathbb{Z}$ (hence $w \in \mathbb{Z}$) and u, v are coprime. If $p \mid u$, then $p \mid w, p \mid v$ which is a contradiction. So $w^2 \equiv 2u^4 \not\equiv 0 \pmod p$, meaning that 2 is a quadratic residue modulo p, contrading $p \equiv 5 \pmod 8$.
A similar argument shows that $w^2 = -2u^4 + 2pv^4$ doesn't have any nontrivial solution either, as -2 too is a quadratic non-residue modulo p. We'll continue the argument after a remark about the general case.

If we want to use argue the unsolvability of some Diophantine equation, the most frequently used tools in our repertoire would be localising to some finite or infinite places and deduce a contradiction there. In general, for $E : y^2 = x(x^2 + ax + b)$ with the 2-isogeny $\phi : E \to E' : y^2 = x(x^2 + a'x + b')$, we'll be interested in equations of the form $w^2 = b_1u^4 + a'u^2v^2 + b_2v^4$. We have an exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E'(\mathbb{Q})/\phi E(\mathbb{Q}) & \longrightarrow & S^{(\phi)}(E/\mathbb{Q}) & \longrightarrow & Ш(E/\mathbb{Q})[\phi_*] & \longrightarrow & 0 \\ & & & \searrow^{\alpha_{E'}} & \downarrow & & & & \\ & & & & \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 & & & & \end{array}$$

The image of $\alpha_{E'}$, which are those $b_1(\mathbb{Q}^\times)^2$ such that the second equation is solvable over $\mathbb{Q}$, must be contained in $S^{(\phi)}(E/\mathbb{Q})$, which consists of those such that the second equation is solvable over all $\mathbb{Q}_p$ and over $\mathbb{R}$.
We don't really need to do a lot of work to check all places. From example sheet, you know that any genus 1 curve must have a point defined over a finite field. Combining this with Lemma 8.1 shows that if $a, b_1, b_2 \in \mathbb{Z}$ and $p \nmid 2b(a^2 - 4b)$ then the first equation is always soluble over $\mathbb{Q}_p$. This conclude the local result for all but finitely many places.

Example 16.3. Back to our previous example. We now know that

$$\operatorname{rank} E(\mathbb{Q}) = \begin{cases} 0 & \text{if } w^2 = -2u^4 + 2pv^4 \text{ is insoluble over } \mathbb{Q} \\ 1 & \text{if } w^2 = -2u^4 + 2pv^4 \text{ is soluble over } \mathbb{Q} \end{cases}$$

Now $w^2 = -2u^4 + 2pv^4$ is soluble over $\mathbb{Q}_p$ as -1 is a quadratic residue modulo p, so $-1 \in (\mathbb{Z}_p^\times)^2$ by Lemma 8.1. It's soluble over $\mathbb{Q}_2$ as $p - 4 \equiv 1 \pmod 8$, which means that $p - 4 \in (\mathbb{Z}_2^\times)^2$. It's also soluble over $\mathbb{R}$ since $\sqrt{p} \in \mathbb{R}$.
A conjecture of Selmer says that, in fact, the rank of $E(\mathbb{Q})$ is 1 for all primes $p \equiv 5 \pmod 8$. Indeed, this is in accordance with small numerical examples

p	u	v	w
5	1	1	1
13	1	1	3
29	1	1	5
37	5	3	151
53	1	1	7

The conjecture was proved by Cassels, conditioning on the finiteness of Ш.

Example 16.4 (Lind)**.** Consider $E : y^2 = x^3 + 17x$. We have $\operatorname{Im} \alpha_E = \langle 17 \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2, E' : y^2 = x^3 - 68x$. Taking $b_1 = 2$ gives $w^2 = 2u^4 - 34v^4$. Replace w by $2w$ gives the equation $C : 2w^2 = u^4 - 17v^4$.
We write $C(K) = \{(u, v, w) : u, v, w \text{ not all zero}, 2w^2 = u^4 - 17v^4\}$ up to the equivalence relation defining a $(1, 1, 2)$-weighted projective space. $C(\mathbb{Q}_2) \neq \varnothing$ using the fact that $17 \in (\mathbb{Q}_2^\times)^4$ (using Lemma 8.1); $C(\mathbb{Q}_{17}) \neq \varnothing$ since $2 \in (\mathbb{Q}_{17}^\times)^2$; $C(\mathbb{R}) \neq \varnothing$ since $\sqrt{2} \in \mathbb{R}$. In other words, $C(\mathbb{Q}_v)$ is nonempty for all places v.
However, it turns out that $C(\mathbb{Q})$ is empty. Suppose $(u, v, w) \in C(\mathbb{Q})$ where WLOG $u, v, w \in \mathbb{Z}$ and u, v are coprime, $w > 0$. Now if $17 \mid w$ then $17 \mid u$ which means that $17 \mid v$, contradicting coprimality assumption. So if $p \mid w$ is an odd prime, then $p \neq 17$ and 17 is a quadratic residue modulo p. By quadratic reciprocity, p has to be a square modulo 17. 2 is also a square modulo 17. This forces w to be a square modulo 17. But $2w^2 \equiv u^4 \pmod{17}$, so 2 is a fourth power modulo 17, which it isn't.
C here serves as a counterexample to the Hasse principle. It represents a non-trivial element of $Ш(E/\mathbb{Q})$.

16.3 The Birch and Swinnerton-Dyer (BSD) Conjecture

Let $E/\mathbb{Q}$ be an elliptic curve.

Definition 16.1. The L-function of $E/\mathbb{Q}$ is $L(E, s) = \prod_p L_p(E, s)$ where $L_p(E, s) = (1 - a_p p^{-s} + p^{1-2s})^{-1}$ if E has good reduction modulo p, $L_p(E, s) = (1 - p^{-s})^{-1}$ if E has split multiplicative reduction, $L_p(E, s) = (1 + p^{-s})^{-1}$ has nonsplit multiplicative reduction, and $L_p(E, s) = 1$ if E has additive reduction.

Theorem 7.2 gives the bound $|a_p| \leq 2\sqrt{p}$ when E has good reduction modulo p, which shows that $L(E, s)$ converges for $\operatorname{Re} s > 3/2$.

Theorem 16.6 (Modularity Theorem)**.** *$L(E, s)$ is the L-function of a modular form of weight 2. In particular, it has an analytic continuation to all of $\mathbb{C}$, and a functional equation relating $L(E, s)$ to $L(E, 2 - s)$.*

Proposition 16.7 (Weak BSD Conjecture)**.** $\operatorname{ord}_{s=1} L(E, s) = \operatorname{rank} E(\mathbb{Q})$.

Proposition 16.8 (Strong BSD Conjecture)**.** *Let $r = \operatorname{ord}_{s=1} L(E, s)$, then*

$$\lim_{s \to 1} \frac{1}{(s-1)^r} L(E, s) = \frac{\Omega_E \operatorname{Reg} E(\mathbb{Q}) Ш(E/\mathbb{Q}) \prod_p c_p}{|E(\mathbb{Q})_{\text{tors}}|^2}$$

There are a few terms we haven't come across yet.

Definition 16.2. Suppose $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}} = \langle P_1, \ldots, P_r \rangle$, then the regulator of $E(\mathbb{Q})$ is $\operatorname{Reg} E(\mathbb{Q}) = \det([P_i, P_j]), [P, Q] = \hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q)$.

Definition 16.3.

$$\Omega_E = \int_{E(\mathbb{R})} \frac{\mathrm{d}x}{2y + a_1 x + a_3}$$

where a_i are the coefficients of a globally minimal Weierstrass equation.

This conjecture is still largely open to this point. Some partial results are known.

Theorem 16.9 (Kolyvagin)**.** *If $\operatorname{ord}_{s=1} L(E, s) \in \{0, 1\}$, then the weak BSD is true and $Ш(E/\mathbb{Q})$ is finite.*