Elliptic Curves

Lecturer: Tom Fisher
Notes: Zach Baugher

Lent 2021

Contents

0 Fermat's Method of Infinite Descent

To give some motivation and history, we introduce the congruent number problem and Fermat's method of infinite descent. By the end of today's lecture, we will see how these concepts relate to elliptic curves.

Throughout this section, the letters a, b, c will denote the side lengths of a right triangle with hypotenuse of length c.

Definition 0.1. A right triangle is *rational* if a, b, c lie in $\mathbb{Q}$. The triangle is *primitive* if a, b, c lie in $\mathbb{Z}$ and are coprime.

Lemma 0.1. The side lengths of a primitive right triangle can be written as a triple

$$(u^2 - v^2,\ 2uv,\ u^2 + v^2),$$

where $u > v > 0$ are integers.

Proof. Rearrange the Pythagorean theorem to get

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

Unique factorization in $\mathbb{Z}$ implies each factor on the right is itself a square, say u^2 and v^2 respectively. Substitute and solve for a, b, c. □

Definition 0.2. We call a positive rational number D a *congruent number* if it is the area of some rational right triangle. Note that upon scaling we can assume D is a squarefree integer.

Example. The simplest congruent number is $D = 6$, arising from a $3-4-5$ right triangle. It is also true that $D = 5$ is congruent. Indeed, the solution $(-4, 5, 6)$ to the integer equation

$$5w^2 = uv(u - v)(u + v)$$

coming from lemma 1.2 below produces the rational right triangle (10/3, 3/2, 41/6) having area 5.

The connection between congruent numbers and elliptic curves arises from the following criterion.

Lemma 0.2. The rational number D is congruent if and only if there exist $x, y \in \mathbb{Q}$ with $y \neq 0$ such that $Dy^2 = x^3 - x$.

Proof. Apply lemma 1.1 and put $(x, y) = (\frac{u}{v}, \frac{w}{v^2})$. □

The *congruent number problem* asks which squarefree integers are congruent numbers. Fermat proved $D = 1$ is not congruent using the method of infinite descent, which we now demonstrate.

Theorem 0.3 (Fermat)**.** There is no solution to

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

for $u, v, w \in \mathbb{Z}$ with w nonzero.

Proof. First, some simplifying assumptions. WLOG we can take u, v coprime and u, v, w all positive (we may need to make a substitution). If u, v are both odd, swap (u, v, w) by $(\frac{u+v}{2}, \frac{u-v}{2}, \frac{w}{2})$; this substitution ensures we can assume u and v have opposite parity.

Now $u, v, u + v, u - v$ are pairwise coprime positive integers. Unique factorization in $\mathbb{Z}$ along with $(*)$ implies that each of these integers is a square; say a^2, b^2, c^2, d^2 respectively. Then the right triangle with legs $\frac{c+d}{2}, \frac{c-d}{2}$ has hypotenuse a and area $(\frac{b}{2})^2$. Setting $w_1 = b/2$ and using lemma 1.1 gives a new solution to $(*)$. But

$$4w_1^2 = b^2 = v \mid w^2,$$

so $w_1 \leq w/2$. Thus one integral solution to $(*)$ produces an infinite decreasing sequence of positive integers arising from constructing smaller such solutions. This cannot happen, so $(*)$ has no solution. □

We have the following variant for polynomials over a field K of characteristic different from 2.

Lemma 0.4. Let $u, v \in K[t]$ be coprime. If $\alpha u + \beta v$ is a square for four distinct $(\alpha : \beta) \in \mathbb{P}^1$, then $u, v \in K$.

Proof. WLOG assume K is algebraically closed. Changing projective coordinates, we may assume the special values $(\alpha : \beta)$ are $(1 : 0), (0 : 1), (1 : -1), (1 : -\lambda)$ for some $\lambda \in K$ different from 0 or 1.

Using unique factorization in $K[t]$ along with the fact that each $\alpha u + \beta v$ is a square, we may construct u_1, v_1 satisfying the hypotheses of the lemma with degree strictly smaller than $\max(\deg u, \deg v)$. Fermat's method of infinite descent then implies $u, v \in K$. □

We now give our first definition of elliptic curve.

Definition 0.3. An *elliptic curve* E/K is the projective closure of the plane affine curve

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

where $f \in K[x]$ is a monic cubic polynomial with distinct $\bar{K}$-roots.

If L/K is a field extension, we define the *L-rational points of E* by

$$E(L) = \big\{(x, y) \in L^2 : y^2 = f(x)\big\} \cup \{O\},$$

where O is the *point at infinity*. When we put a group structure on $E(L)$, we will use O the identity element.

Remark. As hinted at in the definition, it's true that $E(L)$ is naturally an abelian group. In this course we will study $E(L)$ for L a finite field, a finite extension of $\mathbb{Q}_p$, or a number field.

Example. Lemma 1.2 and theorem 1.3 imply that for the elliptic curve

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

we have $E(\mathbb{Q}) = \{O, (0, 0), (1, 0), (-1, 0)\}$.

We end today's lecture with a corollary of the previous lemma.

Corollary 0.4.1. If E/K is an elliptic curve, then $E(K(t)) = E(K)$.

Proof. Without loss of generality we may take K to be algebraically closed. Then, by changing coordinates, we may assume the equation defining E is of the form

$$y^2 = x(x - 1)(x - \lambda)$$

for some $\lambda \in K \setminus \{0, 1\}$.

Now suppose $(x, y) \in E(K(t))$. Write $x = u/v$ with $u, v \in K[t]$ coprime. Substituting and multiplying by v^4 gives

$$w^2 = uv(u - v)(u - \lambda v)$$

for some $w \in K[t]$. Unique factorization in $K[t]$ implies each factor on the right is a square; applying lemma 1.4 shows that u, v are constant. Thus $x, y \in K$. □

1 Algebraic Curves

In this section we work over a fixed algebraically closed field K and assume curves (and hence their defining polynomials) are irreducible.

1.1 Rational Curves

Definition 1.1. A plane curve $C = \{f(x, y) = 0\} \subset \mathbb{A}^2$ is *rational* if it has a *rational parametrization*. That is, there exist $\phi, \psi \in K(t)$ such that

(i) The map $\mathbb{A}^1 \to \mathbb{A}^2$ given by $t \mapsto (\phi(t), \psi(t))$ is injective on a cofinite subset of $\mathbb{A}^1$;

(ii) We have $f(\phi(t), \psi(t)) = 0$.

Example. Any nonsingular plane conic is rational. We will demonstrate this fact for the unit circle, the curve cut out by $f(x, y) = x^2 + y^2 - 1$.

To find a rational parametrization, pick a point on the circle, say $(-1, 0)$, and draw a line of slope t meeting a different point on the circle. The two points of intersection then have $y = t(x + 1)$; make this substitution into f, and then solve the resulting quadratic for x. We get $x = -1$, which we already knew, and $x = \frac{1-t^2}{1+t^2}$. Plugging this new x value in and solving for y gives the rational parametrization

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

Example. Any singular plane cubic is rational using the same method as in the previous example; in this case, the point through which we draw lines of slope t will be the singular point. We can perform this parametrization for, e.g., the *cuspidal cubic* $y^2 = x^3$ and the *nodal cubic* $y^2 = x^3 + x$. In the first case, we obtain the rational parametrization $(x, y) = (t^2, t^3)$. In the second, we find $(x, y) = (t^2 - 1, t^3 - t)$ to be a suitable rational parametrization.

Example. Elliptic curves are *not* rational: if E is an elliptic curve defined by $y^2 = f(x)$ and $\phi, \psi \in K(t)$ satisfy $\psi^2 = f(\phi)$, then corollary 1.4.1 implies that $\phi, \psi \in K$. Thus the mapping $\mathbb{A}^1 \to \mathbb{A}^2$ given by $t \mapsto (\phi(t), \psi(t))$ is constant, so not injective on a cofinite set.

Now that we've shown that elliptic curves are not rational using an elementary approach, we will do the same by quoting some fancier results.

Fact. The *genus* $g(C) \in \mathbb{Z}_{\geq 0}$ is an invariant of a smooth projective curve C. The following facts hold for $g(C)$:

- If $K = \mathbb{C}$, then $g(C)$ agrees with the topological genus of C as a Riemann surface.
- If $C \subset \mathbb{P}^2$ is a smooth plane curve of degree d, then $g(C) = \frac{(d-1)(d-2)}{2}$.

Proposition 1.1. Let C be a smooth projective curve over an algebraically closed field. Then:

(i) C is rational iff $g(C) = 0$.

(ii) C is an elliptic curve iff $g(C) = 1$.

Thus comparing $g(C)$ for rational C and for C an elliptic curve shows that elliptic curves are not rational.

1.2 Order of Vanishing

Let C be an algebraic curve with function field $K(C)$, and $P \in C$ a smooth point. We write ord_P for the "order of vanishing" of $f \in K(C)^\times$ at P; note that if f has a pole at P, then ord_P will be negative.

Fact. The map $\mathrm{ord}_P : K(C)^\times \to \mathbb{Z}$ is a discrete valuation; it exists since at every point of a smooth curve the local ring is a DVR.

Definition 1.2. We call $t \in K(C)^\times$ a *uniformizer at* P if $\mathrm{ord}_P(t) = 1$.

Example. Let $C = \{(x, y) : g(x, y) = 0\} \subset \mathbb{A}^2$ for $g \in K[x, y]$ an irreducible polynomial. Then $K(C) = \mathrm{Frac}(K[x, y]/(g))$. Break g up into its homogeneous components, writing

$$g = g_0 + g_1(x, y) + \dots.$$

Suppose $P = (0, 0) \in C$ is a smooth point, so that $g_0 = 0$ and $g_1(x, y) = \alpha x + \beta y$ for $(\alpha, \beta) \neq (0, 0)$. Then $\gamma x + \delta y \in K(C)$ is a uniformizer at P if and only if $\alpha\delta - \beta\gamma \neq 0$. This condition says that $\gamma x + \delta y$ is a uniformizer precisely when the line it defines is different to the tangent line at P.

Example. Consider the elliptic curve with affine patch $\{(x, y) : y^2 = x(x - 1)(x - \lambda)\} \subset \mathbb{A}^2$, where $\lambda \neq 0, 1$. To form the projective closure, we homogenize by setting $x = X/Z$ and $y = Y/Z$. The elliptic curve proper is then the subset $\{(X : Y : Z) : Y^2Z = X(X - Z)(X - \lambda Z)\} \subset \mathbb{P}^2$. Analyzing this equation, we see that taking the projective closure adds only the point $P = (0 : 1 : 0)$ to the affine patch we started with.

Example. We compute $\mathrm{ord}_P(x)$ and $\mathrm{ord}_P(y)$ for the curve in the previous example. Putting $t = X/Y$ and $w = Z/Y$, we see that in the $t - w$ plane the equation of the curve is

$$w = t(t - w)(t - \lambda w),$$

where P corresponds to the point $(0, 0)$. This is a smooth point with tangent line $w = 0$, so using the characterization of uniformizers from example 2.4 shows that

$$\mathrm{ord}_P(t) = \mathrm{ord}_P(t - w) = \mathrm{ord}_P(t - \lambda w) = 1.$$

From the equation of the curve, we then see that $\mathrm{ord}_P(w) = 3$. Thus we have

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

1.3 Riemann-Roch Spaces

Let C be a smooth projective curve.

Definition 1.3. A *divisor* is a formal sum of points on C, say $D = \sum_{P \in C} n_P P$, where $n_P \in \mathbb{Z}$ and all but finitely many n_P are zero. The group of divisors on C is denoted $\mathrm{Div}(C)$.

The *degree* of the divisor $D = \sum_{P \in C} P$ is defined to be $\sum_{P \in C} n_P$.

We say D is *effective* and write $D \geq 0$ if $n_P \geq 0$ for all P.

If $f \in K(C)^\times$, define the *divisor of* f by $\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f) P$.

Remark. In order for $\mathrm{div}(f)$ to be a divisor, we must have that $\mathrm{ord}_P(f) = 0$ for all but finitely many $P \in C$. This claim is true, but we do not prove it here.

Definition 1.4. The *Riemann-Roch space* of $D \in \mathrm{Div}(C)$ is

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

Remark. We do not know *a priori* that $\mathcal{L}(D)$ is a vector space, but it does turn out to be one. The slogan by which to remember the definition of $\mathcal{L}(D)$ is then that it is the "K-vector space of all rational functions on C with poles no worse than those specified by D." Note that this slogan is only really true when D is effective. If D is not effective, then an element of $\mathcal{D}$ must have prescribed zeroes of a certain order to compensate.

We quote the Riemann-Roch theorem, specializing to genus 1 as this is the case we are interested in. We will use the theorem to guarantee the existence of explicit equations of a certain form for elliptic curves.

Theorem 1.1 (Riemann-Roch)**.** If $g(C) = 1$, then for any $D \in \mathrm{Div}(C)$, we have

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

Example. Let E be an elliptic curve given by $y^2 = f(x)$ having point at infinity P. Then $\mathcal{L}(2P)$ has dimension 2 by Riemann-Roch and Example 2.6; a basis is $\{1, x\}$. Similarly, we have that $\mathcal{L}(3P)$ is 3-dimensional with basis $\{1, x, y\}$.

Next we consider the relationship between a plane cubic and a curve in Weierstrass form.

Proposition 1.2. Let $C \subset \mathbb{P}^2$ be a smooth plane cubic over an algebraically closed field of characteristic different from 2, and $P \in C$ is a point of inflection (i.e., the tangent line $T_P C$ meets C at P with multiplicity greater than 2). Then we may change coordinates such that C is given by

$$C : Y^2 Z = X(X - Z)(X - \lambda Z)$$

for some $\lambda \neq 0, 1$, and $P = (0 : 1 : 0)$.

Proof. Change coordinates such that $P = (0 : 1 : 0)$ with tangent line $T_P C$ given by $Z = 0$. Say C is the vanishing set of $F(X, Y, Z)$. Then $P \in C$ being

a point of inflection means $F(t,1,0)$ has a triple root at 0, thus is equal to ct^3 for some constant c. Thus, no terms of the form X^2Y, XY^2, Y^3 appear in the expression for $F(X,Y,Z)$. So F is a linear combination of elements chosen from

$$\{Y^2Z, XYZ, YZ^2, X^3, X^2Z, XZ^2, Z^3\}.$$

We see that the coefficient of Y^2Z must be nonzero, as otherwise taking partial derivatives shows that P would be a singular point. Furthermore, the coefficient of X^3 must be nonzero, as otherwise the curve is not irreducible (F is divisible by Z). We are free to rescale X, Y, Z and F; doing so, we find C is defined by

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

Substitute $Y - \frac{1}{2}a_1X - \frac{1}{2}a_3Z$ for Y to eliminate the a_1 and a_3 terms. Now we have

$$C : Y^2Z = Z^3f(X/Z)$$

for some univariate cubic f. Since C is smooth, the polynomial f has distinct roots, say $0, 1, \lambda$; indeed, if f had a repeated root α, then $(0 : \alpha : 1)$ would be a singular point of C. The proposition follows. □

Definition 1.5. The equation

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

above is known as the *Weierstrass form* of C. The equation

$$C : Y^2Z = X(X - Z)(X - \lambda Z)$$

is known as the *Legendre form* of C.

Remark. One can show that the points of inflection of $C = \{F = 0\} \subset \mathbb{P}^2$ (where $\mathbb{P}^2$ has coordinates $(X_1 : X_2 : X_2)$) are given by points at which the determinant of the Hessian matrix $(\partial^2F/\partial X_i\partial X_j)$ vanishes.

1.4 The Degree of a Morphism

Let $\phi : C_1 \to C_2$ be a nonconstant morphism of smooth projective curves. Then ϕ induces a pullback on function fields

$$\phi^* : K(C_2) \to K(C_1)$$

given by $f \mapsto f \circ \phi$. Since ϕ is nonconstant and $K(C_2)$ is a field, the pullback ϕ^* is injective. Thus we may view $K(C_2)$ as a subfield of $K(C_1)$.

Definition 1.6. The *degree* of ϕ as above is the degree of the field extension $K(C_1)/\phi^* K(C_2)$. We say ϕ is *separable* if this field extension is separable.

Definition 1.7. Take C_1, C_2, ϕ as above, and suppose $P \in C_1$ and $Q \in C_2$ with $\phi(P) = Q$. Let $t \in K(C_2)$ be a uniformizer at Q. We define the *ramification index* $e_\phi(P) := \mathrm{ord}_P(\phi^* t)$ (which is always at least 1; consider the induced map on local rings). This quantity is independent of the choice of t, since two uniformizers differ only by a factor of a unit, and this difference is respected by ϕ^*.

Theorem 1.2. Let $\phi : C_1 \to C_2$ be a nonconstant morphism of smooth projective curves. Then for any point $Q \in C_2$ we have

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

Moreover, if ϕ is separable (which is automatic in characteristic zero), then $e_\phi(P) = 1$ for all but finitely many points $P \in C_1$. In particular:

(i) The map ϕ is surjective (uses K algebraically closed; not easy);

(ii) For any $Q \in C_2$, we have a bound on the size of the fiber given by $|\phi^{-1}(Q)| \leq \deg \phi$, and if ϕ is separable then we have equality for all but finitely many Q.

Remark. Let C be an algebraic curve. A *rational map* $C \dashrightarrow \mathbb{P}^n$ is given by $P \mapsto (f_0(P) : \cdots : f_n(P))$ for functions $f_0, \ldots, f_n \in K(C)$ not all vanishing at P. We have the following fact: if C is smooth, then ϕ automatically upgrades to a morphism.

2 Weierstrass Equations

In this section we drop the assumptions that K is algebraically closed and that its characteristic is not 2. We do assume, however, that K is a perfect field.

Definition 2.1. An *elliptic curve E over K* is a smooth projective curve of genus 1 defined over K (i.e. the defining equation can be taken with coefficients in K), with a specified K-rational point O_E.

Example. The curve with equation $X^3 + pY^3 + p^2Z^3 = 0$ is *not* an elliptic curve over $\mathbb{Q}$. Even though it is defined over $\mathbb{Q}$, it has no $\mathbb{Q}$-rational points, as can be seen by reducing modulo p, p^2, and p^3. Hence there is no $\mathbb{Q}$-point we can take for O_E.

Theorem 2.1. Every elliptic curve E as defined above is isomorphic to a curve in Weierstrass form via an isomorphism which sends O_E to the point $(0 : 1 : 0)$. If E is defined over K, then there exists such an isomorphism which is also defined over K.

Remark. Proposition 2.2 treated the special case of E a smooth plane cubic where we chose O_E to be a point of inflection. This case ended up being particularly nice since the isomorphism required was given simply by a change of coordinates.

We make use of the following facts in the proof of the theorem above:

Fact. If $D \in \mathrm{Div}(E)$ is defined over K (i.e. it is invariant under the action of $\mathrm{Gal}(\overline{K}/K)$), then $\mathcal{L}(D)$ has a basis in $K(E)$ (not just in $\overline{K}(E)$).

Fact. Let C be a curve, $V \subset \mathbb{P}^2$ a variety, $P \in C$ a smooth point, and $\phi : C \dashrightarrow$ a rational map. Then ϕ is regular at P; in particular, if C is smooth, then ϕ is a morphism.

Proof of Theorem 3.1. We have an inclusion of Riemann-Roch spaces $\mathcal{L}(2O_E) \subset \mathcal{L}(3O_E)$. Pick a basis $\{1, x\}$ for the former, and extend it to a basis $\{1, x, y\}$ for the latter, recalling that $\mathrm{ord}_{O_E}(x) = -2$ and $\mathrm{ord}_{O_E}(y) = -3$. Then the seven elements $1, x, y, x^2, xy, x^3, y^2$ in the six-dimensional space $\mathcal{L}(6O_E)$ satisfy a linear dependence relation.

Note first that in such a dependence relation the coefficients on x^3 and y^2 must be nonzero. Otherwise, each term in the dependence relation would have a different order of vanishing, forcing all coefficients to be zero.

Rescaling x and y, we get an equation of the form

$$E' : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for some $a_i \in K$, and we claim E' is isomorphic to E. Note that there is a morphism $\phi : E \to E' \subset \mathbb{P}^2$ arising via the second fact quoted above from the rational map sending P to $(x(P) : y(P) : 1)$. Rewriting the map as $P \mapsto (x/y(P) : 1 : 1/y(P))$ and plugging in O_E, we see that O_E maps to $O_{E'} = (0 : 1 : 0)$ since y has a higher order pole than does x at O_E.

It remains to show that this map is an isomorphism. To do so, we compute the degrees

$$[K(E) : K(x)] = \deg(E \xrightarrow{x} \mathbb{P}^1) = \mathrm{ord}_{O_E}(1/x) = 2,$$

and

$$[K(E) : K(y)] = \deg(E \xrightarrow{y} \mathbb{P}^1) = \mathrm{ord}_{O_E}(1/y) = 3.$$

Applying the tower law for field extensions, we see that $[K(E) : K] = 6$, so that $K(E) = K(x, y) = \phi^* K(E')$. Then $\deg \phi = 1$, so ϕ is birational.

Now we need to show that the inverse to ϕ is a morphism. To do so, note that if E' were singular then E', hence E, would be rational, a contradiction. Thus E' is smooth and ϕ^{-1} is a morphism, making ϕ is an isomorphism. $\square$

Next we examine the amount of choice we had available in picking the terms used in the Weierstrass equation for E.

Proposition 2.1. Let E and E' be elliptic curves over K in Weierstrass form. Then $E \cong E'$ over K if and only if the equations are related by a change of variables

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

where $u, r, s, t \in K$ and $u \neq 0$.

Proof. Pick two bases $\{1, x\}$ and $\{1, x'\}$ for $\mathcal{L}(2O_E)$. Then there exist $\lambda, r \in K$ with $\lambda \neq 0$ such that

$$x = \lambda x' + r.$$

Working similarly for the bases $\{1, x, y\}$ and $\{1, x', y'\}$ of $\mathcal{L}(O_E)$, we find that

$$y = \mu y' + \sigma x' + t$$

for some $\mu, \sigma, t \in K$ with $\mu \neq 0$. Looking at coefficients of x^3 and y^2 upon substituting these expressions, we find $\lambda^3 = \mu^2$, so $\lambda = u^2$ and $\mu = u^3$ for some $u \in K^\times$. Putting $s = \sigma/u^2$ finishes the proof. □

Remark. Given a Weierstrass equation for a curve E, can we be sure E is an elliptic curve? The only obstruction is if the Weierstrass equation for E defines a singular cubic; otherwise, the curve E will be smooth, and Weierstrass form makes it easy to find a K-rational point which we can use as the point at infinity. We can use a formula in terms of the a_i to determine if a Weierstrass equation defines a singular curve; in particular, the curve is smooth if and only if

$$\Delta(a_1, \ldots, a_6) \neq 0,$$

where $\Delta \in \mathbb{Z}[a_1, \ldots, a_6]$ is a certain polynomial (see the formula sheet).

If $\mathrm{char} K \neq 2, 3$, we can reduce to the case $E : y^2 = x^3 + ax + b$ with discriminant $\Delta = -16(4a^3 + 27b^2)$. Note that this Δ makes sense to consider since it detects whether the given polynomial has repeated roots.

Corollary 2.1.1. Suppose $\mathrm{char} K \neq 2, 3$, and suppose we are given elliptic curves

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

Then $E \cong E'$ over K if and only if $a' = u^4 a$ and $b' = u^6 b$ for some $u \in K^\times$.

Proof. In this case, the curves E, E' are related by a change of variables of the form discussed in Proposition 3.1 with $r = s = t = 0$. □

What really matters to distinguish isomorphism classes of curves in short Weierstrass form is the ratio a^3/b^2. This notion is made precise via the *j-invariant*.

Definition 2.2. The *j-invariant* for an equation in the shortened Weierstrass form above is

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

Corollary 2.1.2. If $E \cong E'$, then $j(E) = j(E')$. If K is algebraically closed then the converse holds.

Proof. If $E \cong E'$ and we make a change of variables as above, the ratio $(a^3 : b^2)$, and thus the j-invariant, remains unchanged.

For the converse, finding an isomorphism comes down to solving for u by extracting roots; this is possible to do when K is algebraically closed. $\square$

3 The Group Law

In this section, we write $E \subset \mathbb{P}^2$ for a smooth plane cubic, and $O_E \in E(K)$ a K-rational point of E, if it exists. The curve E meets any line in 3 points (over $\overline{K}$), assuming these are counted with multiplicity.

Thus, for points $P, Q \in E$ (not necessarily distinct), the line through P, Q meets E in a third point S. Now, drawing the line through O_E and S, we obtain a new point R again given by finding the third point of intersection.

Definition 3.1. In the notation of the discussion above, the *sum of P and Q*, written $P \oplus Q$, is defined to be R. This operation is known as the *chord and tangent law*.

Remark. Recall that we did not stipulate that P, Q be distinct. If $P = Q$, we can take the tangent line $T_P E$ instead of PQ, and so on for other *potential pathologies*.

Theorem 3.1. The operation $\oplus$ defines an abelian group structure on $E(\overline{K})$.

Proof. Since containment of a point on a line is not an order-dependent relation, the operation $\oplus$ is immediately seen to be commutative.

Going through the construction of $O_E \oplus P$ for any $P \in E$ shows that $O_E \oplus P = P$, so O_E is an identity for $\oplus$.

To demonstrate the existence of inverses, take $P \in E$ and construct a point Q as follows. The tangent line to O_E meets E in a third point S; then draw the line through P and S and set Q to be the third point of intersection. In calculating $P \oplus Q$, the fact that S lies on the tangent line to O_E forces $P \oplus Q = O_E$, so Q is really an inverse for P.

Associativity is much harder to show; to prove this property, we will develop a bit more divisor theory. □

Definition 3.2. Two divisors $D_1, D_2 \in \mathrm{Div}(E)$ are *linearly equivalent* if there exists $f \in \overline{K}(E)^\times$ such that $\mathrm{div}(f) = D_1 - D_2$. In this case we write $D_1 \sim D_2$ and $[D] = \{D' : D' \sim D\}$.

Definition 3.3. The *Picard group* $\mathrm{Pic}(E)$ is the quotient of $\mathrm{Div}(E)$ by the linear equivalence relation defined above. Write $\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\sim$, where $\mathrm{Div}^0(E) \subset \mathrm{Div}(E)$ is the subgroup consisting of divisors having degree zero. Note that $\mathrm{Pic}^0(E)$ makes sense since the degree of any principal divisor is 0.

Proposition 3.1. Define $\psi : E \to \mathrm{Pic}^0(E)$ given by $P \mapsto [(P) - (O_E)]$. Then

(i) $\psi(P \oplus Q) = \psi(P) + \psi(Q)$;

(ii) ψ is a bijection.

Proof. (i) We have

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

Thus $(P \oplus Q) + (O_E) \sim (P) + (Q)$, and subtracting (O_E) twice gives the desired result.

(ii) First we prove injectivity. Suppose the exist $P \neq Q$ on E such that $\psi(P) = \psi(Q)$. Then there exists $f \in \overline{K}(E)^\times$ such that $\mathrm{div}(f) = (P) - (Q)$ (take a uniformizer at P and at Q and divide them). Then the map $E \xrightarrow{f} \mathbb{P}^1$ is a morphism, being a map from a smooth projective curve to a projective variety. The degree of this map is equal to the size of any fiber. We can read the fibers of 0 and of ∞ off from $\mathrm{div}(f)$; these are P and Q respectively, each a single point, so $\deg f = 1$. So f is a degree-1 map of smooth projective curves, hence an isomorphism. We then have $E \cong \mathbb{P}^1$, an impossibility since these curves do not have the same genus.

Next we do surjectivity. Let $[D] \in \mathrm{Pic}^0(E)$. Then $D + (O_E)$ has degree 1, and by Riemann-Roch we have $\dim \mathcal{L}(D + (O_E))1$. Thus there exists $f \in \overline{K}(E)^\times$ such that $\mathrm{div}(f) + D + (O_E) \geq 0$. But the left-hand side has degree 1, since the degree of $\mathrm{div}(f)$ is zero for any f. Thus the left-hand side is (P) for some $P \in E$, and $(P) - (O_E) \sim D$. So $\psi(P) = [D]$, and we are done.

□

Corollary 3.1.1. The chord-and-tangent process turns E into an abelian group (in particular, the $\oplus$ operation is associative).

Proof. Proposition 4.1 identifies $(E, \oplus)$ with $(\mathrm{Pic}^0(E), +)$ via an additive map. □

Now that we know that E has a group law, we give formulae for the group law on E when E is an elliptic curve in Weierstrass form. Write

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

Write $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, and $P' = (x', y')$ where P' is the third point of intersection of P_1P_2 with E. Then $P_1 \oplus P_2 = P_3 := (x_3, y_3)$.

With this setup, we have

$$-P_1 = (x_1, -(a_1x_1 + a_3) - y_1).$$

Now, writing the equation of the line through P_1 and P_2 as $y = \lambda x + \nu$, we can substitute this expression for y into the Weierstrass equation for E. This gives a cubic, two of whose roots are given by x_1, x_2. Looking at the coefficient of x^2 gives

$$\lambda^2 + a_1\lambda - a_2 = x_1 + x_2 + x',$$

where $x' = x_3$. Thus we have

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2; \\ y_3 &= -(a_1x' + a_3) - y'(\lambda x' + \nu) \\ &= -(\lambda + a_1)x_3 - \nu - a_3. \end{aligned}$$

It remains to find formulae for ν and λ.

(i) If $x_1 = x_2$ and $P_1 \neq P_2$, then $P_1 \oplus P_2 = O_E$.

(ii) If $x_1 \neq x_2$, then $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, and

$$\nu = y_1 - \lambda x_1 = \frac{y_1(x_2 - x_1) - x_1(y_2 - y_1)}{x_2 - x_1} = \frac{x_2y_1 - x_1y_2}{x_2 - x_1}.$$

(iii) If $P_1 = P_2$, the line P_1P_2 is replaced by the tangent line at P_1. We get

$$\begin{aligned} \lambda &= \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}; \\ \nu &= \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}. \end{aligned}$$

Corollary 3.1.2. The set of K-rational points $E(K)$ forms a subgroup of $(E(\overline{K}), \oplus)$.

Proof. The identity O_E is included in $E(K)$ by definition (view this as motivation for including O_E in the definition). The rest follows quickly from the formulae above or from results we have already proven about $\oplus$. $\square$

Theorem 3.2. Elliptic curves are *group varieties*; that is, the group operations

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

are morphisms of algebraic varieties.

Proof. The formulae above show that $[-1] : E \to E$ is a rational map, hence upgrades to a morphism since E is a smooth projective curve. For $\oplus$, the formulae tell us again that the map is rational. In fact $\oplus$ is regular on $U = \{(P, Q) \in E \times E : P, Q, P \oplus Q, P \ominus Q \neq O_E\}$. For $P \in E$, write $\tau_P : E \to E$ for the "translation-by-P" map $X \mapsto P \oplus X$. Then τ_P is a rational map from a smooth curve to a projective variety, hence a morphism.

We can factor $\oplus$ as

$$E \times E \xrightarrow{\tau_{-A} \times \tau_{-B}} E \times E \xrightarrow{\oplus} E \xrightarrow{\tau_{A \oplus B}} E$$

for any $A, B \in E$, so $\oplus$ is regular on each translate $(\tau_A \times \tau_B)(U)$. These translates cover $E \times E$, so $\oplus$ is regular everywhere. $\square$

We conclude the lecture with a statement of results on rational points on elliptic curves over various fields. Cases (iii) through (v) will be our main focus in the course.

Fact. The isomorphisms in (i),(ii),(iv) respect the relevant topologies.

(i) For $K = \mathbb{C}$, we have $E(\mathbb{C}) \cong \mathbb{C}/\Lambda \cong \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ both algebraically and analytically via the Weierstrass $\wp$ function, where $\Lambda \subset \mathbb{C}$ is a lattice.

(ii) For $K = \mathbb{R}$, we have $E(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ if $\Delta > 0$ and $E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ if $\Delta < 0$.

(iii) For $K = \mathbb{F}_q$, we have a bound on the number of points, namely $|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$ (Hasse's bound).

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

(v) If $[K : \mathbb{Q}] < \infty$, then $E(K)$ is a finitely generated abelian group (Mordell-Weil theorem). The proof of Mordell-Weil gives an upper bound on the rank of $E(K)$, and there are techniques that help compute the rank over $\mathbb{Q}$, but it is not known how to compute the rank precisely in the general case.

4 Elliptic Curves over $\mathbb{C}$: Some Brief Remarks

Let $\Lambda = \{a\omega_1 + b\omega_2 : a, b \in \mathbb{Z}\}$, where ω_1, ω_2 form an $\mathbb{R}$-basis for $\mathbb{C}$. Then a meromorphic function on $\mathbb{C}/\Lambda$ is the same as a Λ-invariant meromorphic function on $\mathbb{C}$, and the set of such functions has a nice description.

Fact. The function field of $\mathbb{C}/\Lambda$ is generated over $\mathbb{C}$ by $\wp(z)$ and $\wp'(z)$, where

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

and

$$\wp'(z) = -2 \sum_{\lambda \in \Lambda} \frac{1}{(z-\lambda)^3}.$$

Fact. For any lattice $\Lambda \subset \mathbb{C}$, the functions $\wp(z)$ and $\wp'(z)$ coming from Λ satisfy

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

where $g_2, g_3 \in \mathbb{C}$ depend on Λ. This relationship induces an isomorphism $\mathbb{C}/\Lambda \cong E(\mathbb{C})$, where E is the elliptic curve given by

$$E : y^2 = 4x^3 - g_2 x - g_3.$$

This is an isomorphism of Riemann surfaces and of groups.

Theorem 4.1 (Uniformization theorem)**.** *Every* elliptic curve over $\mathbb{C}$ arises from a lattice $\Lambda \subset \mathbb{C}$ via the construction above.

5 Isogenies

Let E_1, E_2 be elliptic curves.

Definition 5.1. (i) An *isogeny* $\phi : E_1 \to E_2$ is a nonconstant morphism of varieties with $\phi(O_{E_1}) = O_{E_2}$. Being a morphism of smooth projective curves, such a map automatically surjects onto the $\overline{K}$-points of E_2.

(ii) We say E_1, E_2 are *isogenous* if there exists an isogeny $\phi : E_1 \to E_2$.

Fact. There is an abelian group of isogenies $\mathrm{Hom}(E_1, E_2)$ consisting of the isogenies $E_1 \to E_2$ together with the zero map. The group structure is given by

$$(\phi + \psi)(P) := \phi(P) \oplus \psi(P).$$

Fact. We can compose isogenies: if $E_1 \xrightarrow{\phi} E_2 \xrightarrow{\psi} E_3$ is a sequence of isogenies, then the composite $\psi \circ \phi : E_1 \to E_3$ is itself an isogeny. Indeed, the composition of surjective functions is surjective, so $\psi \circ \phi$ is not identically zero. In this situation there is a *tower law* for the degree of the isogeny $\psi \circ \phi$; namely, we have

$$\deg(\phi \circ \psi) = \deg \phi \deg \psi.$$

Definition 5.2 (Multiplication by n)**.** One example of an isogeny is as follows. For $n \in \mathbb{Z}$, define $[n] : E \to E$ by adding P to itself n times (according to the group law) when $n > 0$ and by $[-n]P = [-1]([n]P)$, where $[-1]P$ is as calculated above. This map is the *multiplication-by-n map*, and we show below that it is an isogeny.

Definition 5.3. The *n-torsion subgroup* $E[n] \leq E$ is the kernel of $E \xrightarrow{[n]} E$.

Example. If $K = \mathbb{C}$, then we saw in the previous section that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$. Then $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ and $\deg[n] = n^2$. We will see later that the second statement holds for any field K, and the first holds when $\mathrm{char}\, K \nmid n$.

Lemma 5.1. If $\mathrm{char}\, K \neq 2$ and E is given by

$$E : y^2 = f(x) = (x - e_1)(x - e_2)(x - e_3)$$

for $e_i \in \overline{K}$ pairwise distinct, then

$$E[2] = \{O_E, (e_1, 0), (e_2, 0), (e_3, 0)\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

Proof. Let $P = (x, y) \in E$. Then $[2]P = 0$ if and only if $P = -P$, which for the given equation forces $(x, y) = (x, -y)$, and thus $y = 0$. □

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

Proof. The map $[n]$ is a morphism by repeated application of Theorem 4.2. We must show $[n] \neq [0]$. Assume char $K \neq 2$.

Case $n = 2$: Lemma 6.1 implies $E[2] \neq E$, so $[2] \neq [0]$.

Case n odd: Lemma 6.1 also implies there is a nonzero point $T \in E[2]$. Then $nT = T \neq 0$, so $[n] \neq [0]$.

Then using the fact that $[mn] = [m][n]$, we can extend the proof to all nonzero integers n.

For char $K = 2$, replace Lemma 6.1 with a lemma describing $E[3]$ explicitly; the method of proof is then the same (the cases will be $n = 3$ and n prime to 3). □

Corollary 5.1.1. The abelian group $\mathrm{Hom}(E_1, E_2)$ is torsion-free.

Theorem 5.2 (Isogenies are homomorphisms)**.** Let $\phi : E_1 \to E_2$ be an isogeny. Then for all $P, Q \in E_1$, we have

$$\phi(P + Q) = \phi(P) + \phi(Q).$$

Proof sketch. The map ϕ induces a *pushforward* $\phi_* : \mathrm{Div}(E_1) \to \mathrm{Div}(E_2)$ defined by sending $\sum_{P \in E_1} n_P P$ to $\sum_{P \in E_2} n_P \phi(P)$.

Recall that the pullback φ^* lets us view $K(E_1)$ as a finite extension of $K(E_2)$. The norm map allows us to obtain elements of $K(E_2)$ using elements of $K(E_1)$. Then we have:

Fact. If $f \in K(E)^\times$, then

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

Thus ϕ_* sends principal divisors to principal divisors, hence induces a map on Pic^0.

Since $\varphi(O_{E_1}) = O_{E_2}$, the following diagram commutes, where the vertical arrows are the isomorphisms defined in Proposition 4.1 (namely $P \mapsto [(P) - (O_E)]$):

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

Then since ϕ_* is a group homomorphism, we must have that ϕ is the same. $\square$

Lemma 5.3. Let $\phi : E_1 \to E_2$ be an isogeny. Then there is a morphism ξ making the following diagram commute, where x_i is the x-coordinate on a Weierstrass equation for E_i:

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

Moreover, if $\xi(t) = r(t)/s(t)$ with $r, s \in K[t]$ coprime, then

$$\deg \phi = \deg \xi = \max(\deg(r), \deg(s)).$$

Proof. For $i = 1, 2$, the extension $K(E_i)/K(x_i)$ is a degree 2 Galois extension with Galois group generated by $[-1]^*$. By Theorem 6.2, we have

$$\phi \circ [-1] = [-1] \circ \phi.$$

So if $f \in K(x_2)$, then

$$[-1]^*(\phi^* f) = \phi^*([-1]^* f) = \phi^* f.$$

Thus $\phi^* f \in K(x_1)$. Then we have the following diagram of field extensions, where ξ is determined by $x_2 \mapsto \phi^* x_1$.

$$\begin{array}{ccc} K(x_1) & \xrightarrow{\deg 2} & K(E_1) = K(x_1, y_1) \\ {\scriptstyle \deg \xi}\Big| & & \Big|{\scriptstyle \deg \phi} \\ K(x_2) & \xrightarrow[\deg 2]{} & K(E_2) = K(x_2, y_2) \end{array}$$

The tower law implies that $\deg \phi = \deg \xi$. We claim that the minimal polynomial of x_1 over $K(x_2)$ is

$$f(t) = r(t) - s(t)x_2,$$

where $\frac{r(x_1)}{s(x_1)} = \xi(x_1)$ and $r, s \in K[t]$ are coprime. Noting first that $f(x_1) = 0$, we just need to show it is irreducible in $K[x_2, t]$. But this is true since it is linear in x_2, and since r, s are coprime. So f is irreducible in $K[x_2, t]$, thus in $K(x_2)[t]$ by Gauss' lemma. Then

$$\begin{aligned} \deg \phi &= \deg \xi \\ &= [K(x_1) : K(x_2)] \\ &= \deg f \\ &= \max(\deg r, \deg s), \end{aligned}$$

proving the lemma. □

Lemma 5.4. The degree of $[2] : E \to E$ is 4.

Proof. Assume $\mathrm{char} K \neq 2, 3$ (the result is still true otherwise, but this assumption simplifies the proof). Then E is given by

$$E : y^2 = x^3 + ax + b =: f(x).$$

If $P = (x, y)$, then

$$\begin{aligned} x(2P) &= \left(\frac{3x^2 + a}{2y}\right)^2 - 2x \\ &= \frac{(3x + a)^2 - 8xf(x)}{4f(x)} \\ &= \frac{x^4 + \text{lower}}{4f(x)}. \end{aligned}$$

We claim that this fraction is already in lowest terms. Indeed, otherwise there exists $\theta \in \overline{K}$ which is a root of both numerator and denonimator. Then $f(\theta) = 0$, and from the numerator we have $f'(\theta) = 0$, contradicting the assumption that f has distinct roots. By Lemma 6.3, we then have $\deg[2] = 4$. □

More is true of the degree of isogenies; in fact the degree map is a *quadratic form*, which we will show below.

Definition 5.4. Let A be an abelian group. A map $q : A \to \mathbb{Z}$ is a *quadratic form* if

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

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

Lemma 5.5 (Parallelogram law)**.** The map $q : A \to \mathbb{Z}$ as in Definition 6.4 is a quadratic form if and only if it satisfies the *parallelogram law*:

$$q(x + y) + q(x - y) = 2q(x) + 2q(y),\ \forall x, y \in A.$$

Proof. ($\Longrightarrow$): Let $\langle x, y\rangle = q(x + y) - q(x) - q(y)$. Then

$$\langle x, x\rangle = q(2x) - 2q(x) = 2q(x).$$

But by (ii) in the definition of quadratic form,

$$\frac{1}{2}\langle x + y,\ x + y\rangle + \frac{1}{2}\langle x - y,\ x - y\rangle = \langle x, x\rangle + \langle y, y\rangle,$$

and interpreting in terms of q gives the desired result.

($\Longleftarrow$): Examples Sheet 2 □

Theorem 5.6. Let E_1, E_2 be elliptic curves. The map $\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ is a quadratic form, taking $\deg[0] = 0$.

Proof. To simplify the proof, assume $\mathrm{char} K \neq 2, 3$. Write

$$E_2 : y^2 = x^3 + ax + b,$$

and let $P, Q \in E_2$ with $P, Q, P + Q, P - Q \neq O_{E_2}$. Let $x_1, \ldots, x_4$ be the respective x-coordinates of these four points. We use the following fact:

Lemma 5.7. There exist $W_0, W_1, W_2 \in \mathbb{Z}[a, b][x_1, x_2]$ of degree at most 2 in x_1 and x_2 individually, such that

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

Proof. One method is to use direct calculation. We give another method here. Let $y = \lambda x + \nu$ be the line between P and Q. Then

$$x^3 + ax + b - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3) = x^3 - s_1 x^2 + s_2 x - s^3,$$

where s_i is the i^{th} symmetric polynomial in x_1, x_2, x_3.

Comparing coefficients, we see

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

Eliminating λ and ν gives

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

which has degree at most 2 in each x_i. Then x_3 is a root of the quadratic polynomial $W(t) = F(x_1, x_2, t)$. Repeating this argument for the line through P and $-Q$ shows that x_4 is the other root of $F(x_1, x_2, t)$. Then equating coefficients in

$$W_0(t - x_3)(t - x_4) = W(t) = W_0 t^2 - W_1 t + W_2$$

gives W_0, W_1, W_2 with

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

as desired. □

Now, we 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 all isogenies under consideration are nonzero, since the resulting inequality is either straightforward (if ϕ or $\psi = 0$) or follows from Lemma 6.5 and the fact that $\deg[-1] = 1$ (if $\phi = \pm\psi$).

We write

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

By Lemma 6.7, we have

$$(1 : \xi_3 + \xi_4 : \xi_3\xi_4) = ((\xi_1 - \xi_2)^2 : \dots).$$

Put $\xi_i = r_i/s_i$ where $r_i, s_i \in K[t]$ are coprime. Substituting into the previous equation, we get

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

Calculating degrees, we have

$$\begin{aligned}\deg(\phi+\psi) + \deg(\phi-\psi) &= \max(\deg r_3, \deg s_3) + \max(\deg r_4, \deg 2_4) \\ &= \max(\deg(s_3s_4), \deg(r_3s_4 + r_4s_3), \deg(r_3r_4))\end{aligned}$$

upon doing some case work.

Note that the polynomials s_3s_4, $r_3s_4 + r_4s_3$, r_3r_4 are coprime (use casework and the fact that all fractions were written in lowest terms). Thus we have

$$\begin{aligned}\max(\deg(s_3s_4), \deg(r_3s_4 + r_4s_3), \deg(r_3r_4)) &\le 2\max(\deg r_1, \deg s_1) + 2\max(\deg r_2, \deg s_2) \\ &= 2\deg\phi + 2\deg\psi.\end{aligned}$$

To turn this inequality into an equality, replace ϕ, ψ by $\phi+\psi$, $\phi-\psi$ to get

$$\deg(2\phi) + \deg(2\psi) \le 2\deg(\phi+\psi) + 2\deg(\phi-\psi),$$

and since $\deg[2] = 4$, we can cancel a factor of 2 to get

$$2\deg\phi + 2\deg\psi \le \deg(\phi+\psi) + \deg(\phi-\psi).$$

Thus the two are equal, and the result follows by the parallelogram law (Lemma 6.5). □

Corollary 5.7.1. For all $n \in \mathbb{Z}$ and all $\phi \in \mathrm{Hom}(E_1, E_2)$, we have

$$\deg(n\phi) = n^2 \deg\phi.$$

In particular, taking $\phi = [1] \in \mathrm{Hom}(E, E)$ we see $\deg[n] = n^2$.

Example (Construction of a 2-isogeny)**.** Take E/K an elliptic curve, and suppose char$K \neq 2$. Take $T \in E(K)[2]$, and note that without loss of generality we may assume E has the form

$$E : y^2 = x(x^2 + ax + b),$$

where $a, b \in K$ and $b(a^2 - 4b) \neq 0$, and $T = (0, 0)$.

If $P = (x, y)$ and $P' = P + T = (x', y')$. Using the formula sheet, we get

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

Define

$$\begin{aligned} \xi &= x + x' + a \\ &= \left(\frac{y}{x}\right)^2; \\ \eta &= y + y' \\ &= \frac{y}{x}\left(x - \frac{b}{x}\right). \end{aligned}$$

Then

$$\begin{aligned} \eta^2 &= \left(\frac{y}{x}\right)^2 \left[\left(x\frac{b}{x}\right)^2 - 4b\right] \\ &= \xi((\xi - a)^2 - 4b) \\ &= \xi(\xi^2 - 2a\xi + a^2 - 4b). \end{aligned}$$

Now let

$$E' : y^2 = x(x^2 + a'x + b'),$$

where $a' = -2a$ and $b^2 = a^2 - 4b$. This is an isogeny $\phi : E \to E'$ given by

$$(x : y : 1) \mapsto \left(\left(\frac{y}{x}\right)^2 : \frac{y(x^2 - b)}{x^2} : 1 \right).$$

Analyzing the orders of vanishing of each coordinate function, multiplying all three by a suitable rational function where necessary, we see that $O_E \mapsto (0 : 1 : 0)$, so ϕ is indeed an isogeny. Via Lemma 6.3, we have $\deg \phi = 2$, and we call ϕ a 2-*isogeny*.

6 The Invariant Differential

6.1 Geometric Facts on Differentials

Let C be a smooth projective curve over an algebraically closed field K.

Definition 6.1. The *space of differentials* Ω_C is the $K(C)$-vector space generated by symbols $\mathrm{d}f$ for each $f \in K(C)$, subject to the relations

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

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

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

Fact. The space Ω_C is one-dimensional over $K(C)$.

Definition 6.2 (Order of vanishing for differentials)**.** Let $\omega \in \Omega_C$ be nonzero, and let $P \in C$ with $t \in K(C)$ a uniformizer at P. Then $\omega = f\mathrm{d}t$ for some $f \in K(C)^\times$ by the fact above, and we define

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

to be the *order of vanishing* of ω at P. This quantity is independent of the choice of uniformizer t, and $\mathrm{ord}_P(\omega) = 0$ for all but finitely many $P \in C$.

Definition 6.3. For $\omega \in \Omega_C$, the *divisor of* ω is

$$\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega) P.$$

Definition 6.4. The space of *regular differentials* is defined to be

$$\{\omega \in \Omega_C : \mathrm{div}(\omega) \geq 0\};$$

that is, it is the K-vector space of differentials on C having no poles. This space is finite-dimensional, and we define the *genus* of C to be the K-dimension of this vector space.

Fact. As a consequence of Riemann-Roch, for any $0 \neq \omega \in \Omega_C$ we have

$$\deg(\mathrm{div}(\omega)) = 2g(C) - 2.$$

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

6.2 Specializing to Elliptic Curves: The Invariant Differential

Lemma 6.1. Assume $\mathrm{char} K \neq 2$, and let E be given by

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3).$$

Then the differential $\omega = \frac{\mathrm{d}x}{y}$ has no zeros or poles on E (and thus $g(E) = 1$). In particular, the element ω is a basis of the 1-dimensional K-vector space of regular differentials on E.

Proof. Let $T_i = (e_i, 0)$; then $E[2] = \{O_E, T_1, T_2, T_3\}$. Then we have

$$\mathrm{div}(y) = (T_1) + (T_2) + (T_3) - 3(O_E).$$

Next, we calculate $\mathrm{div}(x)$. If $P \in E \setminus E[2]$, then $\mathrm{ord}_P(x - x_P) = 1$, so $\mathrm{ord}_P(\mathrm{d}x) = 0$. If $P = T_i$, then $\mathrm{ord}_P(x - e_i) = 2$, so $\mathrm{ord}_P(\mathrm{d}x) = 1$. Finally, if $P = O_E$, then $\mathrm{ord}_P(x) = -2$ and $\mathrm{ord}_P(\mathrm{d}x) = -3$.

Putting this information together, we get

$$\mathrm{div}(\mathrm{d}x) = (T_1) + (T_2) + (T_3) - 3(O_E),$$

which agrees with $\mathrm{div}(y)$. The result follows. □

Definition 6.5. If $\phi : C_1 \to C_2$ is a nonconstant morphism, define the *pullback* $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ by

$$f\,\mathrm{d}g \mapsto \phi^* f\,\mathrm{d}(\phi^* g),$$

where in this equation ϕ^* is the usual pullback on function fields.

Lemma 6.2. Let $P \in E$ and denote by τ_P the isogeny $E \to E$ sending X to $X + P$. If $\omega = \frac{\mathrm{d}x}{y}$, then $\tau_P^* \omega = \omega$ for all P. (We call ω the *invariant differential*.)

Proof. We have that $\tau_P^* \omega$ is a regular differential on E (e.g. since taking div commutes with pullback), so $\tau_P^* \omega = \lambda_P \omega$ for some $\lambda_P \in K^\times$. The map $E \to \mathbb{P}^1$ given by $P \mapsto \lambda_P$ is a morphism of smooth projective curves, but is not surjective, since it misses 0 and ∞. So the morphism is constant, and there exists $\lambda \in K^\times$ such that $\tau_P^* \omega = \lambda \omega$ for all $P \in E$. Taking $P = O_E$ forces $\lambda = 1$, hence the result. □

Remark. Recall that if $K = \mathbb{C}$ then $E \cong \mathbb{C}/\Lambda$ via $\wp$ and $\wp'$. Then the invariant differential becomes

$$\frac{\mathrm{d}x}{y} = \frac{\wp'(z)\,\mathrm{d}z}{\wp'(z)} = \mathrm{d}z,$$

which is clearly invariant under addition.

Lemma 6.3. Let $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$, and let ω be an invariant differential on E_2. Then

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

Remark. This statement is less innocent than it may seem: notice that on the left we are using the group law on E_2, whereas on the right we are using addition in Ω_{E_1}.

Proof. Write $E = E_2$, and consider the maps μ, π_1, $\pi_2 : E \times E \to E$ given by

$$\begin{aligned} \mu &: (P, Q) \mapsto P + Q; \\ \pi_1 &: (P, Q) \mapsto P; \\ \pi_2 &: (P, Q) \mapsto Q. \end{aligned}$$

It is a fact that $\Omega_{E\times E}$ is a 2-dimensional $K(E \times E)$-vector space with basis $\{\pi_1^*\omega, \pi_2^*\omega\}$. Thus

$$\mu^*\omega = f\pi_1^*\omega + g\pi_2^*\omega$$

for some $f, g \in K(E \times E)$. For $Q \in E$, let $\iota_Q : E \to E$ be the map given by $P \mapsto (P, Q)$. Applying ι_Q^* to the equation above, we get

$$(\mu\iota_Q)^*\omega = \iota_Q^* f(\pi_1\iota_Q)^*\omega + \iota_Q^* g(\pi_2\iota_Q)^*\omega.$$

Thus

$$\tau_Q^*\omega = \iota_Q^*\omega + 0.$$

By Lemma 7.2, we have $\iota_Q^* f = 1 \in K(E)$ for all $Q \in E$, so $f(P, Q) = 1$ for all $P, Q \in E$. Similarly for g, thus

$$\mu * \omega = \pi_1^*\omega + \pi_2^*\omega.$$

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

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

□

We now come to our reason for developing the theory of differentials: it can be a useful means to check *separability of a morphism.*

Lemma 6.4. Let $\phi : C_1 \to C_2$ be a non-constant morphism. Then ϕ is separable iff $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ is nonzero.

Example. Write $\mathbb{G}_m = \mathbb{A}^1 \setminus \{0\} = \mathbb{P}^1 \setminus \{0, \infty\}$, and define a map $\phi : \mathbb{G}_m \to \mathbb{G}_m$ for any $n \in \mathbb{Z}_{\geq 1}$ by $x \mapsto x^n$. Then

$$\phi^*(\mathrm{d}x) = \mathrm{d}(x^n) = nx^{n-1}\mathrm{d}x.$$

So, if $\mathrm{char}K \not| n$, then ϕ is separable. Then $\#\phi^{-1}(Q) = \deg \phi$ for all but finitely many $Q \in \mathbb{G}_m$. But ϕ is a group homomorphism, so

$$\begin{aligned} \#\phi^{-1}(Q) &= \#\ker(\phi)\, \forall Q \in \mathbb{G}_m \\ \implies \#\ker(\phi) &= \deg \phi \\ &= n, \end{aligned}$$

so $K = \overline{K}$ contains exactly n n^{th} roots of unity.

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

Proof. By Lemma 7.3 and induction, we find $[n]^*\omega = n\omega$ for all $n \in \mathbb{Z}$. Since $\mathrm{char}K \not| n$, the map $[n]$ is separable, so $\#[n]^{-1}Q = \deg[n]$ for all but finitely many $Q \in E$. Since $[n]$ is a group homomorphism, we also have

$$\#[n]^{-1}Q = \#E[n],\ \forall Q \in E.$$

Thus

$$\#E[n] = \deg[n] = n^2.$$

Now by group theory, we have

$$E[n] \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \cdots \mathbb{Z}/d_t\mathbb{Z},$$

where $d_1 \mid \cdots \mid d_t$ and all d_i divide n. If p is a prime with $p \mid d_1$, then

$$E[p] \cong (\mathbb{Z}/p\mathbb{Z})^t.$$

But $\#E[p] = p^2$, so $t = 2$ and $d_1 = d_2 = n$. The desired result follows. $\square$

Remark. When $\mathrm{char}K = p$, then $[p]$ is inseparable. One can show that there are two possibilities for $E[p^r]$: either $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ for all $r \geq 1$, the "ordinary case," or $E[p^r] = 0$ for all $r \geq 1$, the "supersingular" case.

7 Elliptic Curves over Finite Fields

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

$$|\langle \phi, \psi \rangle| = |q(\phi + \psi) - q(\phi) - q(\psi)| \leq 2\sqrt{q(\phi)q(\psi)}.$$

Proof. We may assume that $\phi \neq 0$ and indeed that $q(\phi) \neq 0$, as otherwise the result is clear. Let $m, n \in \mathbb{Z}$, then we have

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

Take $m = -\langle \phi, \psi \rangle$ and $n = 2q(\phi)$ to deduce

$$\begin{aligned} q(\psi) - \frac{\langle \phi, \psi \rangle^2}{4q(\phi)} &\geq 0 \\ \implies \langle \phi, \psi \rangle^2 &\leq 4q(\phi)q(\psi) \\ \implies |\langle \phi, \psi \rangle| &\leq 2\sqrt{q(\phi)q(\psi)}. \end{aligned}$$

□

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

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

Proof. Recall that $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ is cyclic of order r, and is generated by the Frobenius map $x \mapsto x^q$. Let E have a Weierstrass equation with coefficients $a_1, \ldots, a_6 \in \mathbb{F}_q$. Then define the Frobenius endomorphism $\phi : E \to E$ by sending $(x, y) \mapsto (x^q, y^q)$. Note that this is really an isogeny since ϕ fixes the a_i and $x \mapsto x^q$ is a ring homomorphism in characteristic p where $q = p^r$. Note also that $\deg \phi = q$. Then

$$\begin{aligned} E(\mathbb{F}_q) &= \{P \in E : \phi(P) = P\} \\ &= \ker(1 - \phi). \end{aligned}$$

To check that $1-\phi$ is separable, we let ω be an invariant differential on E, and calculate

$$\begin{aligned}\phi^*\omega &= \phi^*\left(\frac{\mathrm{d}x}{y}\right)\\ &= \frac{\mathrm{d}(x^q)}{y^q}\\ &= q\frac{x^{q-1}\mathrm{d}x}{y^q}\\ &= 0.\end{aligned}$$

Thus by Lemma 7.3, we have

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

so $1-\phi$ is separable.

Now using Theorem 2.2 (interpreting sizes of fibers using the degree) and the fact that $1-\phi$ is a group homomorphism, arguing as for $\mathbb{G}_m$, we see

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

Recall that $\deg : \mathrm{Hom}(E,E) \to \mathbb{Z}$ is a positive definite quadratic form. Using Lemma 8.1, we get

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

which is what we wanted. □

7.1 Zeta Functions

For K a number field, there is a *Dedekind zeta function*

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

We can also define zeta functions for curves over finite fields. More explicitly, if $K = \mathbb{F}_q(C)$ where $C/\mathbb{F}_q$ is a smooth projective curve, we can define

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

where $|C|$ is the set of closed points of C (i.e. orbits for the action of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ on $C(\overline{\mathbb{F}}_q)$, and $Nx = q^{\deg x}$ where $\deg x$ is the size of the orbit. Then we have

$$\zeta_K(s) = F(q^{-s}),$$

where

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

We construct an alternate definition for $F(T)$. Taking logs and using the power series for log, then differentiating, we get

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

Definition 7.1. Let $\phi, \psi \in \mathrm{End}(E)$. Recall

$$\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg(\phi) - \deg(\psi).$$

Define the *trace of* ϕ by

$$\mathrm{tr}(\phi) = \langle \phi, 1 \rangle.$$

Lemma 7.3. If $\psi \in \mathrm{End}(E)$, then

$$\psi^2 - [\mathrm{tr}\psi]\psi + [\deg \psi] = 0.$$

(Think of this as an analogue of Cayley-Hamilton.)

Proof. ES 2. □

Theorem 7.4. Let $E/\mathbb{F}_q$ be an elliptic curve, and define a by

$$\#E(\mathbb{F}_q) = q + 1 - a.$$

Then

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

Proof. Let $\phi : E \to E$ be the q-power Frobenius map. By the proof of Hasse's theorem, we have

$$\#E(\mathbb{F}_q) = \deg(1 - \phi) = q + 1 - \mathrm{tr}(\phi).$$

Thus $\mathrm{tr}(\phi) = a$, and we know $\deg(\phi) = q$. Using Lemma 8.3, we get

$$\begin{aligned} \phi^2 - a\phi + q &= 0 \\ \implies \phi^{n+2} - a\phi^{n+1} + q\phi^n &= 0 \\ \implies \mathrm{tr}(\phi^{n+2}) - a\mathrm{tr}(\phi^{n+1}) + q\mathrm{tr}(\phi^n) &= 0. \end{aligned}$$

This is a second order difference equation with initial conditions $\mathrm{tr}(1) = 2$ and $\mathrm{tr}(\phi) = a$, and has solution

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

where $\alpha, \beta \in \mathbb{C}$ are the roots of $X^2 - aX + q = 0$. Thus we have

$$\begin{aligned} \#E(\mathbb{F}_q) &= \deg(1 - \phi^n) \\ &= 1 + \deg(\phi^n) - \mathrm{tr}(\phi^n) \\ &= 1 + q^n - \alpha^n - \beta^n. \end{aligned}$$

So,

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

□

Remark. By Hasse's theorem, we have $a \leq 2\sqrt{q}$ in the notation of our setup above. Then considering the quadratic $X^2 - aX + 2$, we see $\alpha = \overline{\beta}$, so $|\alpha| = |\beta| = \sqrt{q}$. Letting $K = \mathbb{F}_q(E)$, we have

$$\begin{aligned} \zeta_K(s) = 0 &\implies Z_E(q^{-s}) = 0 \\ &\implies q^s = \alpha \text{ or } \beta \\ &\implies \Re(s) = \frac{1}{2}, \end{aligned}$$

proving the Riemann hypothesis for function fields of elliptic curves.

8 Formal Groups

Definition 8.1. Let R be a ring and $I \subset R$ an ideal. The *I-adic topology on R* has as basis

$$\{r + I^n : r \in R,\, n \geq 1\}.$$

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

Definition 8.3. R is *complete* if

(i) $\bigcap_{n\geq 0} I^n = \{0\}$ (equiv. to I-adic topology being Hausdorff);

(ii) Every Cauchy sequence converges.

Remark. If $x \in I$, then

$$\frac{1}{1-x} = 1 + x + x^2 + \dots.$$

In particular, when R is complete for the I-adic topology, this power series converges to an inverse for $1 - x$ in R.

Example. Some nice pairs R, I:

- $R = \mathbb{Z}_p$, $I = p\mathbb{Z}_p$.
- $R = \mathbb{Z}[[t]]$, $I = (t)$.

Lemma 8.1 (Hensel's Lemma)**.** Let R be an integral domain which is complete with respect to an ideal I. Let $F \in R[X]$, and $s \geq 1$. Suppose $a \in R$ satisfies $F(a) \equiv 0 \pmod{I^s}$, and that $F'(a) \in R^\times$. Then there is a unique $b \in R$ such that $F(b) = 0$ and $b \equiv a \pmod{I^s}$.

Proof. Let $u \in R^\times$ with $F'(a) \equiv u \pmod{I}$ (e.g. could take $u = F'(a)$, but not necessary. See remark below). Replacing $F(X)$ by $u^{-1}F(X + a)$, we can assume $a = 0$ and $F'(a) = F'(0) \equiv 1 \pmod{I}$. We put $x_0 = 0$ and recursively define

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

Using induction, we see that $x_n \equiv 0 \pmod{I^s}$ for all n.

Now write

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

for some $G, H \in R[X, Y]$. We claim that for all $n \geq 0$, we have

$$x_{n+1} \equiv x_n \pmod{I^{n+s}}.$$

We prove this by induction on n. The case $n = 0$ follows from the induction used above. Now, suppose

$$x_n \equiv x_{n-1} \pmod{I^{n+s-1}}.$$

By the polynomial identity above, we have

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

for some $c \in I$. Then

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

proving the claim. Thus (x_n) is Cauchy, and completeness of R implies $(x_n) \to b \in R$. Then taking the limit as $n \to \infty$ of the recursive definition of (x_n) and noting that polynomials are continuous for the I-adic topology (consider the preimage I^s under x^k), we get

$$b = b - F(b),$$

so $F(b) = 0$. Doing the same for $x_n \equiv 0 \pmod{I^s}$ gives

$$b \equiv 0 \pmod{I^s}.$$

Finally, uniqueness is proved using the polynomial factorization above and the fact that R is an integral domain. The second factor cannot be zero since $F'(0) \equiv 1 \pmod{I}$, so we get that any two roots satisfying the required conditions must be equal. □

How do we apply Hensel's lemma to elliptic curves? We can use it to study behavior near $(0 : 1 : 0)$. Consider the homogeneous Weierstrass equation

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

On the affine patch where $Y \neq 0$, setting $t = -X/Y$ and $w = -Z/Y$ gives

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

We will use Hensel's lemma to solve for w as a power series in t. Let $R = \mathbb{Z}[a_1, \ldots, a_6][[t]]$ and $I = (t)$, so that R is I-adically complete. Taking $F(X) = X - f(t, X) \in R[X]$, $s = 3$, and $a = 0$ in the notation of Hensel's lemma, we have

$$\begin{aligned} F(0) &= -f(t,0) \\ &= -t^3 \\ &\equiv 0 \pmod{t^3}; \\ F'(0) &= 1 - a_1 t - a_2 t^2 \in R^\times. \end{aligned}$$

Thus there is a unique $w(t) \in \mathbb{Z}[a_1, \ldots, a_6][[t]]$ such that $w(t) = f(t, w(t))$ and $w(t) \equiv 0 \pmod{t^3}$.

Remark. (i) One can find $w(t)$ explicitly. It has the form

$$w(t) = t^3(1 + A_1 t + A_2 t^2 + \ldots)$$

where $A_1 = a_1$, $A_2 = a_1^2 + a_2$, and so on. Each coefficient is homogeneous in $a_1, \ldots, a_6$.

(ii) Taking $u = 1$ in the proof of Hensel's lemma gives

$$w(t) = \lim_{n \to \infty} w_n(t),$$

where

$$\begin{aligned} w_0(t) &= 0; \\ w_{n+1}(t) &= f(t, w(t)). \end{aligned}$$

Lemma 8.2. Let R be an integral domain with field of fractions K, and suppose R is complete with respect to an ideal $I \subset R$. Pick $a_1, \ldots, a_6 \in R$. Then

$$\begin{aligned} \widehat{E}(I) &= \{(t, w(t)) \in E(K) : t \in I\} \\ &= \{(t, w) \in E(K) : t, w \in I\} \end{aligned}$$

is a subgroup of $E(K)$.

Remark. The second equality above follows by the uniqueness in Hensel's lemma. Note also that we cannot use the formulas we have already derived for the group law in this case, since we are considering a different affine piece of E.

Proof. Taking $(t, w) = (0, 0)$ shows $O_E \in \widehat{E}(I)$. So it's enough to show that if $P_1, P_2 \in \widehat{E}(I)$, then $-P_1 - P_2 \in \widehat{E}(I)$. We note that since O_E is a point of inflection, the point $-P_1 - P_2$ is simply the third point on the line through P_1 and P_2.

Write $P_1 = (t_1, w_1)$ and $P_2 = (t_2, w_2)$. Since $P_1, P_2 \in \widehat{E}(I)$, we have $t_1, t_2 \in I$, and

$$w_i = w(t_i) = \sum_{n=2}^{\infty} A_{n-2} t^{n+1} \in I,$$

for $i = 1, 2$. We have a couple of cases for the slope λ of the line through P_1, P_2:

$$\lambda = \begin{cases} \frac{w(t_2)-w(t_1)}{t_2-t_1}, & \text{if } t_1 \neq t_2; \\ w'(t_1), & \text{if } t_1 = t_2. \end{cases}$$

Working out λ explicitly, we see it has the form

$$\sum_{n=2}^{\infty} = A_{n-2}(t_1^n + t^{n-1}t_2 + \cdots + t_2^n) \in I.$$

We have also $\nu = w_1 - \lambda t_1 \in I$. Substituting $w = \lambda t + \nu$ into $w = f(t, w)$, we get

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

Let

$$\begin{aligned} A &= 1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3; \\ B &= a_1\lambda + a_2\nu + a_3\lambda^2 + 2a_4\lambda\nu + 3a_6 + \lambda^2\nu \end{aligned}$$

be the coefficients of t^2 and t^3 in the equation above, respectively, and note that $A \in R^\times$ while $B \in I$. Relating the sum of roots of the polynomial to its coefficients and to the roots t_1, t_2 we already know, we find

$$\begin{aligned} t_3 &= \frac{-B}{A} - t_1 - t_2 \in I; \\ w_3 &= \lambda t_3 + \nu \in I. \end{aligned}$$

Thus $\widehat{E}(I)$ passes the subgroup criterion. □

Example. Taking $R = \mathbb{Z}[a_1, \ldots, a_6][[t]]$ and $I = (t)$, using Lemma 9.2 shows that there exists $\iota \in \mathbb{Z}[a_1, \ldots, a_6][[t]]$ with $\iota(0) = 0$, and

$$[-1](t, w(t)) = (\iota(t), w(\iota(t))).$$

In fact, we have

$$\iota(X) = -X - a_1X^2 - a_2X^3 - (a_1^3 + a_3)X^4 + \ldots.$$

In two variables we have $R = \mathbb{Z}[a_1, \ldots, a_6][[t_1, t_2]]$ with $I = (t_1, t_2)$, applying Lemma 9.2 shows that there exists $F \in \mathbb{Z}[a_1, \ldots, a_6][[t_1, t_2]]$ with $F(0, 0) = 0$ and

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

Explicitly, we have

$$F(X, Y) = X + Y - a_1XY - a_2(X^2Y + XY^2) + \ldots.$$

We've now discovered power series which respect the group law on E. The fact that these power series arose in this way gives them certain properties, namely

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

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

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

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

Definition 8.4. Let R be a ring. A *formal group* over R is a power series $F(X, Y) \in R[[X, Y]]$ satisfying (i)-(iii) in the list immediately above.

Remark. We don't include (iv) in the definition of a formal group since it actually follows from (i)-(iii) (exercise!).

Example. Some examples of formal groups include:

(i) The *additive formal group* $\widehat{\mathbb{G}}_a$ given by

$$F(X, Y) = X + Y.$$

(ii) The *multiplicative formal group* $\widehat{\mathbb{G}}_m$ given by

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

(iii) The power series $F(X,Y)$ obtained from our work with elliptic curves (denoted $\widehat{E}$).

Definition 8.5. Let $\mathscr{F}$ and $\mathscr{G}$ be formal groups over R given by power series F, G (note that we often use distinct names for the formal group and its power series).

(i) A *morphism* $f : \mathscr{F} \to \mathscr{G}$ is a power series $f \in R[[T]]$ such that $f(0) = 0$, and such that

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

(ii) $\mathscr{F} \cong \mathscr{G}$ if there are morphisms $f : \mathscr{F} \to \mathscr{G}$ and $g : \mathscr{G} \to \mathscr{F}$ such that

$$f(g(X)) = g(f(X)) = X.$$

We now proceed with classifying formal groups up to isomorphism in nice cases. One such case is that of characteristic 0.

Theorem 8.3. If $\mathrm{char} R = 0$, then any formal group $\mathscr{F}$ over R is isomorphic to $\widehat{\mathbb{G}}_a$ over $R \otimes \mathbb{Q}$. More precisely,

(i) There is a unique power series

$$\log(T) = T + \frac{a_2}{2}T^2 + \frac{a_3}{3}T^3 + \dots$$

with $a_i \in R$, such that

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

(ii) There is a unique power series

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

with $b_i \in R$, such that

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

Proof. (i) Write $F_1(X,Y) = \frac{\partial F}{\partial X}(X,Y)$. We demonstrate uniqueness first. Let

$$\begin{aligned} p(T) &= \frac{d}{dT}\log(T) \\ &= 1 + a_2 T + a_3 T^2 + \dots . \end{aligned}$$

Then the definition of p and the stipulated properties of log give

$$p(F(X,Y))F_1(F,Y) = p(X) + 0.$$

Now putting $X = 0$ gives

$$\begin{aligned} & p(Y)F_1(0,Y) = 1 \\ \implies\ & p(Y) = F_1(0,Y)^{-1}, \end{aligned}$$

showing that p (hence log) is unique.

Now we prove existence. Write

$$\begin{aligned} p(T) &= F_1(0,T)^{-1} \\ &= 1 + a_2 T + a_3 T^2 + \dots , \end{aligned}$$

with the $a_i \in R$. Let

$$\log(T) = T + \frac{a_2}{2}T^2 + \frac{a_3}{3}T^3 + \dots .$$

Differentiate the associative law for formal groups wrt X to get

$$\begin{aligned} & F(F(X,Y),Z) = F(X,F(Y,Z)) \\ \implies\ & F_1(F(X,Y),Z)F_1(X,Y) = F_1(X,F(Y,Z)) \\ \implies\ & F_1(Y,Z)F_1(0,Y) = F_1(0,F(Y,Z)) \quad \text{(on setting } X=0\text{)} \\ \implies\ & F_1(Y,Z)p(Y)^{-1} = p(F(Y,Z))^{-1} \\ \implies\ & F_1(Y,Z)p(F(Y,Z)) = p(Y) \\ \implies\ & \log(F(Y,Z)) = \log(Y) + h(Z) \quad \text{(on integrating wrt } Y\text{)} \\ \implies\ & h(Z) = \log(Z) \quad \text{(symmetry)}. \end{aligned}$$

(ii) We prove a more general result:

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

$$f(g(T)) = g(f(T)) = T.$$

Proof of Lemma 9.4. We construct polynomials $g_n \in R[T]$ such that $f(g_n(T)) \equiv T \pmod{T^{n+1}}$, and $g_{n+1}(T) \equiv g_n(T) \pmod{T^{n+1}}$. Then $g(T) = \lim_{n\to\infty} g_n(T)$ will satisfy $f(g(T)) = T$.

To start the induction constructing the g_n, set $g_1(T) = a^{-1}T$ and check that it satisfies the conditions we've set. Now suppose $n \geq 2$ and we've got $g_{n-1}(T)$ satisfying the properties we want. Then

$$f(g_{n-1}(T)) = T + bT^n \pmod{T^{n+1}}.$$

We put

$$g_n(T) = g_{n-1}(T) + \lambda T^n,$$

with $\lambda \in R$ to be chosen. Then

$$\begin{aligned} f(g_n(T)) &= f(g_{n-1}(T) + \lambda T^n) \\ &\equiv f(g_{n-1}(T)) + \lambda a T^n \pmod{T^{n+1}} \\ &\equiv T + (b + \lambda a)T^n \pmod{T^{n+1}}. \end{aligned}$$

We take $\lambda = -b/a$, which lies in R since $a \in R^\times$ and $b \in R$. We thus get $g(T) = a^{-1}T + \cdots \in R[[T]]$ with $f(g(T)) = T$ upon taking the limit. Applying the same argument, we obtain $h(t) = aT + \cdots \in R[[T]]$ such that $g(h(T)) = T$. It remains to show $h = f$; this holds because

$$f(T) = f(g(h(T))) = h(T)$$

using the relationships between f, g, h we just described. □

Now the theorem follows from question 12 on Examples Sheet 2 (Fill in later!).

□

Before continuing, we introduce some notation. Let $\mathscr{F}$ be a formal group given by the power series $F \in R[[X, Y]]$. Suppose R is complete wrt an ideal I. Then for $x, y \in I$, put

$$x \oplus_{\mathscr{F}} y = F(x, y) \in I,$$

which makes sense since R is I-adically complete. Then write

$$\mathscr{F}(I) := (I, \oplus_{\mathscr{F}})$$

for the abelian group structure on I defined by $\oplus_{\mathscr{F}}$.

Example. The formal groups we have seen to date take this form. For instance,

$$\widehat{\mathbb{G}}_a(I) = (I, +);$$
$$\widehat{\mathbb{G}}_m(I) = (1 + I, \times);$$

and $\widehat{E}(I)$ is the subgroup of $E(K)$ given by the formal group law, as shown in Lemma 9.2.

Corollary 8.4.1. Let $\mathscr{F}$ be a formal group over R, and $n \in \mathbb{Z}$. Suppose $n \in R^\times$. Then

(i) $[n] : \mathscr{F} \to \mathscr{F}$ is an isomorphism.

(ii) If R is complete wrt an ideal I, then

$$\mathscr{F}(I) \xrightarrow{\times n} \mathscr{F}(I)$$

is an isomorphism. In particular, $\mathscr{F}(I)$ has no n-torsion.

Proof. First, define $[n]$ recursively by

$$[1](T) = T;$$
$$[n](T) = F([n-1]T, T) \quad \forall n \geq 2.$$

For $n < 0$, we use $[-1](T) = \iota(T)$ where ι is as defined as in Example 9.2. By induction, $[n](T) = nT + \cdots \in R[[T]]$, so Lemma 9.4 shows that if $n \in R^\times$ then $[n]$ is an isomorphism. $\square$

9 Elliptic Curves over Local Fields

In this section, we suppose K is a field complete wrt a discrete valuation $v : K^\times \twoheadrightarrow \mathbb{Z}$. We write $\mathcal{O}_K$ for the valuation ring

$$\mathcal{O}_K := \{x \in K^\times : v(x) \geq 0\} \cup \{0\},$$

and note that its unit group $\mathcal{O}_K^\times$ consists precisely of those elements of $\mathcal{O}_K$ having valuation 0. We write π for a uniformizer of K, and k for the residue field, and note that $\mathcal{O}_K$ is complete with respect to any ideal $\pi^r\mathcal{O}_K$ for $r \geq 1$. We assume char $K = 0$ and char $k = p > 0$, so for example we could have $K = \mathbb{Q}_p,\ \mathcal{O}_K = \mathbb{Z}_p,\ k = \mathbb{F}_p$. Finally, let E/K be an elliptic curve.

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

Remark. (i) Putting $x = u^2x'$ and $y = u^3y'$ gives $a_i = u^ia_i'$, so we can always clear denominators to obtain an integral Weierstrass equation.

(ii) If $a_1, \ldots, a_6 \in \mathcal{O}_K$, then $\Delta \in \mathcal{O}_K$, so $v(\Delta) \geq 0$. Hence minimal Weierstrass equations exist as well.

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

Lemma 9.1. Let E/K have integral Weierstrass equation

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

Let $O_E \neq P = (x, y) \in E(K)$. Then either $x, y \in \mathcal{O}_K$, or

$$\begin{aligned} v(x) &= -2s, \\ v(y) &= -3s \end{aligned}$$

for some integer $s \geq 1$.

Proof. If $x \in \mathcal{O}_K$, suppose for the sake of contradiction that $v(y) < 0$. Then the valuation of the LHS of the Weierstrass equation is negative. Indeed, upon factoring out y we are left with $y + a_1x + a_3$, where the latter two summands lie in $\mathcal{O}_K$ while the first does not. So the full sum cannot lie in

$\mathcal{O}_K$, hence has negative valuation. On the other hand, the right-hand side is an element of $\mathcal{O}_K$, so has nonnegative valuation, a contradiction.

If $v(x) < 0$, then we have

$$\begin{aligned} v(\text{LHS}) &\geq \min(2v(y),\, v(x)+v(y),\, v(y)); \\ &= \min(2v(y), v(x)+v(y)); \\ v(\text{RHS}) &= 3v(x). \end{aligned}$$

To get the final equality, note that if $x = u\pi^n$ where $u \in \mathcal{O}_K^\times$, then putting the right-hand side under the common denominator π^{3n}, we see that the numerator has valuation zero.

Now, if $\min(2v(y), v(x)+v(y)) = v(x)+v(y)$, we quickly see

$$2v(x) \geq v(y) \leq v(x),$$

contradicting $v(x) < 0$. So $2v(y) < v(x)+v(y)$, hence $v(y) < v(x)$. By the argument we gave for $v(\text{RHS})$, we now see

$$\begin{aligned} v(LHS) &= 2v(y) \\ v(RHS) &= 3v(x), \end{aligned}$$

and the result follows. □

Now fix a minimal Weierstrass equation for E/K and write $\widehat{E}$ for the formal group over $\mathcal{O}_K$ defined in the previous section. Taking $I = \pi^r\mathcal{O}_K$ in Lemma 9.2, we see that

$$\widehat{E}(\pi^r\mathcal{O}_K) = \left\{(x,y) \in E(K) : \frac{-x}{y},\, \frac{-1}{y} \in \pi^r\mathcal{O}_K\right\} \cup \{O_E\}$$

is a subgroup of $E(K)$. Applying Lemma 10.1, we can rewrite the set on the right, giving

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

We write $E_r(K)$ for this subgroup, and note that we have a filtration

$$\cdots \subset E_3(K) \subset E_2(K) \subset E_1(K).$$

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

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

We will show:

- For r sufficiently large, we have $\mathscr{F}(\pi^r\mathcal{O}_K) \cong (\mathcal{O}_K, +)$;
- For all $r \geq 1$, we have $\mathscr{F}(\pi^r\mathcal{O}_K)/\mathscr{F}(\pi^{r+1}\mathcal{O}_K) \cong (k, +)$.

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

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

is an isomorphism with inverse

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

Remark. We have

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

Proof of Theorem 10.2. For $x \in \pi^r\mathcal{O}_K$, we must show that the power series $\log(x)$ and $\exp(x)$ converge to an element of $\pi^r\mathcal{O}_K$.

Recall

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

where $b_i \in \mathcal{O}_K$. We use

Lemma 9.3.

$$v_p(n!) \leq \frac{n-1}{p-1}$$

Proof. We have

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

Therefore

$$(p-1)v_p(n!) < n,$$

and since both sides lie in $\mathbb{Z}$ we conclude

$$(p-1)v_p(n!) \leq n-1,$$

as desired. □

Returning to the proof of Theorem 10.2, we have (using $v(p) = e$)

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

But $r - \frac{e}{p-1} > 0$, so as $n \to \infty$ the terms of $\exp(x)$ tend to 0 with valuation at least r. Thus $\exp(x)$ converges to an element of $\pi^r \mathcal{O}_K$. The same method works for log, since

$$v\left(\frac{a_n x^n}{n}\right) \geq v\left(\frac{a_n x^n}{n!}\right),$$

so we are done. □

Lemma 9.4. We have

$$\mathscr{F}(\pi^r \mathcal{O}_K)/\mathscr{F}(\pi^{r+1}\mathcal{O}_K) \cong (k, +)$$

for all $r \geq 1$.

Proof. By the definition of formal group, we have

$$F(X, Y) = X + Y + XY(\dots).$$

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 we have a surjective group homomorphism $\mathscr{F}(\pi^r \mathcal{O}_K) \to (k, +)$ given by $\pi^r x \mapsto x \pmod{\pi}$ with kernel $\mathscr{F}(\pi^{r+1}\mathcal{O}_K)$, hence the result. □

Corollary 9.4.1. If $|k| < \infty$ (i.e. K is a finite extension of $\mathbb{Q}_p$), then $\mathscr{F}(\pi\mathcal{O}_K)$ has a finite index subgroup isomorphic to $(\mathcal{O}_K, +)$.

Before continuing, we introduce some notation: for $x \in \mathcal{O}_K$, we denote by $\tilde{x}$ its reduction modulo π. Our aim now is to study the reduction of an elliptic curve mod π. Our next proposition elucidates our reason for working with minimal Weierstrass equations.

Proposition 9.1. If E/K is an elliptic curve, the reductions mod π of any two *minimal* Weierstrass equations for E are isomorphic over k.

Proof. Say the minimal Weierstrass equations are related by a substitution given by a tuple (u, r, s, t), with $u \in K^\times$ and $r, s, t \in K$. Then the discriminants Δ_1, Δ_2 are related by

$$\Delta_1 = u^{12}\Delta_2.$$

Since both equations are minimal, we have $v(\Delta_1) = v(\Delta_2)$, so $u \in \mathcal{O}_K^\times$. The transformation formulae for the Weierstrass equations of the forms

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6;$$
$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

under the given substitution, along with the fact that $\mathcal{O}_K$ is integrally closed, show that $r, s, t \in \mathcal{O}_K$. Indeed, choosing the proper formula (depending on char k) from (4) on the formula sheet gives r as the root of a monic polynomial in $\mathcal{O}_K[x]$. A similar choice among formulae (3) shows $s \in \mathcal{O}_K$ as well, and then it is immediate that $t \in \mathcal{O}_K$.

The Weierstrass equations of the reductions mod π are then related by the substitution given by $(\tilde{u}, \tilde{r}, \tilde{s}, \tilde{t})$, where $\tilde{u} \in k^\times$ and $\tilde{r}, \tilde{s}, \tilde{t} \in k$. □

Definition 9.2. The *reduction* $\tilde{E}/k$ of E/K is the reduction of a minimal Weierstrass equation. We say E has *good reduction* if $\tilde{E}$ is nonsingular (i.e. remains an elliptic curve), and *bad reduction* otherwise.

Remark. For an integral (not necessarily minimal) Weierstrass equation, if $v(\Delta) = 0$, then the equation is already minimal, and E/K has good reduction. If $0 < v(\Delta) < 12$, then the equation again must be minimal, and we must have bad reduction. When $v(\Delta) \geq 12$, the equation might not be minimal, and we cannot immediately draw conclusions about the reduction.

On $\mathbb{P}^2(K) \to \mathbb{P}^2(k)$, the map $(X : Y : Z) \mapsto (\tilde{X} : \tilde{Y} : \tilde{Z})$ is well defined, upon multiplying by a power of π placing $X, Y, Z \in \mathcal{O}_K$ with at least one of these lying in $\mathcal{O}_K^\times$. Restricting this map to $E(K)$ gives $E(K) \to \tilde{E}(k)$.

If $P = (x, y) \in E(K)$, then by Lemma 9.1 we need to consider two cases if we wish to reduce mod π. If $x, y \in \mathcal{O}_K$, then $\tilde{P} = (\tilde{x}, \tilde{y})$. When $v(x) = -2s$ and $v(y) = -3s$, we can clear denominators in $P = (x : y : 1)$ by multiplying through by π^{3s}, and we find that $\tilde{P} = (0 : 1 : 0)$ is the point at infinity on $\tilde{E}(k)$. We write $E_1(K)$ for the collection of points in $E(K)$ which reduce to $(0 : 1 : 0)$ mod π.

Let us study the ways in which E/K might reduce mod π in more depth. In any case, the nonsingular locus $\tilde{E}_{ns}$ of the reduction will be isomorphic either to $\tilde{E}$ or to $\tilde{E} \setminus \{\text{singular point}\}$ via the chord and tangent law. There are two possibilities when E has bad reduction:

Definition 9.3. (i) If $\tilde{E}$ gives a curve with a node (i.e. double root, such as $y^2 = x^2(x + 1)$) we have $\tilde{E}_{ns} \cong \mathbb{G}_m$ over k or possibly a quadratic extension of k (ES3). When this holds for E/K mod π, we say E has *multiplicative reduction* mod π.

(ii) If $\tilde{E}$ gives a curve with a cusp (i.e. triple root, such as $y^2 = x^3$) we have $\tilde{E}_{ns} \cong \mathbb{G}_a$ (again over k or a quadratic extension). In this case we say E has *additive reduction* mod π. The isomorphism for $y^2 = x^3$ is given by $(x, y) \mapsto x/y$ in one direction and $t \mapsto (t^{-2}, t^{-3})$ in the other.

Definition 9.4. For an elliptic curve E/K, define

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

Proposition 9.2. The set $E_0(K)$ is a subgroup of $E(K)$, and reduction mod π is a surjective group homomorphism $E_0(K) \to \tilde{E}(k)$.

Proof. We show first that reduction mod π is a group homomorphism. Let $\ell \subset \mathbb{P}^2$ be a line defined over K with equation

$$\ell : aX + bY + cZ = 0.$$

Multiplying through by a power of π, we may assume $\min(v(a), v(b), v(c)) = 0$. Then reduction mod π gives a line $\tilde{\ell}$ with coefficients $\tilde{a}, \tilde{b}, \tilde{c}$.

Now if $P_1, P_2, P_3 \in E(K)$ sum to O_E, then they lie on a line ℓ. So $\tilde{P}_1, \tilde{P}_2, \tilde{P}_3$ (for now, assumed distinct) lie on the line $\tilde{\ell}$. If $\tilde{P}_1, \tilde{P}_2 \in \tilde{E}_{ns}(k)$, then $\tilde{P}_3 \in \tilde{E}_{ns}(k)$ as well. So if $P_1, P_2 \in E_0(K)$, then $P_3 \in E_0(K)$, and $\tilde{P}_1 + \tilde{P}_2 + \tilde{P}_3 = 0$. If the reductions are not distinct, the fact that $\tilde{\ell}$ is a line and the reduced Weierstrass equation a cubic means that there will

still be three points of intersection, counting multiplicities. Thus $E_0(K)$ is a subgroup of $E(K)$, and reduction mod π is a group homomorphism.

It remains to check that the reduction map on $E_0(K)$ is surjective. Let $f(x,y)$ be the polynomial coming from a Weierstrass equation for E. Let $\tilde{P} \in \tilde{E}_{ns}(k) \setminus \{\tilde{O}_E\}$, say $\tilde{P} = (\tilde{x}_0, \tilde{y}_0)$ for some $x_0, y_0 \in \mathcal{O}_K$. Since $\tilde{P}$ is nonsingular, we have either

(i) $\frac{\partial f}{\partial x}(x_0, y_0) \not\equiv 0 \pmod{\pi}$, or

(ii) $\frac{\partial f}{\partial y}(x_0, y_0) \not\equiv 0 \pmod{\pi}$.

In case (i), we put $g(t) = f(t, y_0) \in \mathcal{O}_K[t]$. Then $g(x_0) \equiv 0 \pmod{\pi}$ and $g'(x_0) \in \mathcal{O}_K^\times$. So Hensel's lemma guarantees the existence of $b \in \mathcal{O}_K$ such that $g(b) = 0$ and $b \equiv x_0 \pmod{\pi}$; then $(b, y_0) \in E(K)$ has reduction $\tilde{P}$. Case (ii) is similar. □

We now have a filtration of subgroups

$$E_r(K) \cong (\mathcal{O}_K, +) \subset \cdots \subset E_2(K) \subset E_1(K) \subset E_0(K) \subset E(K),$$

where $r > \frac{e}{p-1}$ and we can understand $E_r(K)$ for $r > 0$ as being given by the formal group as $\widehat{E}(\pi^r \mathcal{O}_K)$. By Lemma(..) we have that the quotients of successive subgroups given by the formal group are isomorphic to $(k, +)$, and we see by our work preceding that $E_0(K)/E_1(K) \cong \tilde{E}_{ns}(k)$.

A compactness argument (Lemma (..) below) shows that if $|k| < \infty$ then $[E(K) : E_0(K)] < \infty$. We deduce

Theorem 9.5. If $[K : \mathbb{Q}_p] < \infty$, then $E(K)$ contains a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.

We now briefly review ramification is local fields. Let $[K : \mathbb{Q}_p] < \infty$ and L/K be a finite extension, having residue fields k' and k, and write $f = [k' : k]$. Then $[L : K] = ef$, where $e = v_L(\pi)$ for π a uniformizer for K.

If L/K is Galois, then there is a natural map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k'/k)$. This map is surjective, and its kernel has order e.

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

Fact. For each $m \geq 1$,

(i) k has a unique extension of degree m (say k_m).

(ii) K has a unique *unramified* extension of degree m (say K_m).

(iii) These extensions are Galois with cyclic Galois group.

Definition 9.6. The *maximal unramified extension of* K is given by

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

where the union is taken inside a fixed algebraic closure $\overline{K}$.

Theorem 9.6. Let $[K : \mathbb{Q}_p] < \infty$. Suppose E/K has good reduction and $p \nmid n$. Let $P \in E(K)$. Then $K([n]^{-1}P)/K$ (given by adjoining x and y coordinates) is unramified, where $[n]^{-1}P = \{Q \in E(\overline{K}) : [n]Q = P\}$.

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

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

Taking the union over all m, we get a commutative diagram

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

The multiplication-by-n map is an isomorphism by Corollary 9.5 applied to each K_m (using $p \nmid n$). Moreover, the multiplication map on the right is surjective (Theorem (2.8)) with kernel isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$ (Theorem 6.5), again using $p \nmid n$. Applying the snake lemma to the kernels and cokernels of the vertical arrows, we see $E(K^{\mathrm{nr}})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ and $E(K^{\mathrm{nr}})/nE(K^{\mathrm{nr}}) = 0$. So if $P \in E(K)$, then there exists $Q \in R(K^{\mathrm{nr}})$ such that $nQ = P$, and $[n]^{-1}P = \{Q + T : T \in E[n]\} \subset E(K^{\mathrm{nr}})$. Thus $K([n]^{-1}P) \subset K^{\mathrm{nr}}$, and $K([n]^{-1}P)/K$ is unramified. □

Now we give the compactness argument required to complete the proof of Proposition 10.2.

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

Proof. Since $|k| < \infty$, all quotients $\mathcal{O}_K/\pi^r\mathcal{O}_K$ are finite for $r \geq 1$. From this it may be shown (as in Local Fields) that $\mathcal{O}_K$ is compact. Then $\mathbb{P}^n(K)$ is the union of the sets

$$\{(a_0 : \cdots : a_{i-1} : 1 : a_{i+1} : \cdots : a_n) : a_j \in \mathcal{O}_K\},$$

and hence compact with respect to the π-adic topology on K. Now $E(K) \subset \mathbb{P}^2(K)$ is closed, hence compact, so $E(K)$ is a compact topological group (since morphisms of varieties are continuous for the Zariski topology).

If $\tilde{E}$ has a singular point $(\tilde{x_0}, \tilde{y_0})$, then

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

is a closed subset of $E(K)$. Thus $E_0(K)$ is an open subgroup of $E(K)$, and its cosets form a disjoint open cover of $E(K)$. So there can only be finitely many such cosets, by compactness. □

Remark. The index $[E(K) : E_0(K)]$ (denoted $c_K(E)$) is called the *Tamagawa number* of $E(K)$. Some first properties are as follows:

(i) If $E(K)$ has good reduction then $c_K(E) = 1$, but the converse is not true (ES3).

(ii) It can be shown that either $c_K(E) = v(\Delta)$ (split multiplicative reduction) or $c_K(E) \leq 4$ (this result requires that we work with a *minimal* Weierstrass equation).

10 Elliptic Curves over Number Fields I: The Torsion Subgroup

In this section, we denote by K a number field and E/K an elliptic curve. Write $\mathcal{O}_K$ for the ring of integers of K, write $\mathfrak{p}$ for a prime ideal of $\mathcal{O}_K$, and write $K_\mathfrak{p}$ for the completion of K with respect to the $\mathfrak{p}$-adic valuation. Finally, write $k_\mathfrak{p}$ for the residue field $\mathcal{O}_K/\mathfrak{p}$.

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

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

Proof. Take a Weierstrass equation for E with $a_1, \ldots, a_6 \in \mathcal{O}_K$. Then E is nonsingular, so $0 \neq \Delta \in \mathcal{O}_K$. Write

$$(\Delta) = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$$

as a product of prime ideals. Let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. If $\mathfrak{p} \notin S$, then $v_\mathfrak{p}(\Delta) = 0$, and $E/K_\mathfrak{p}$ has good reduction (quote result). Thus any prime of bad reduction is contained in S, which is finite. □

Remark. If K has class number 1 (e.g. $K = \mathbb{Q}$), then we can find a Weierstrass equation for E with $a_1, \ldots, a_6 \in \mathcal{O}_K$ which is minimal at all primes $\mathfrak{p}$ (i.e. E has a *globally minimal* Weierstrass equation). This is not true when the class number is larger than 1.

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

Proof. Take any prime $\mathfrak{p}$. We saw that $E(K_\mathfrak{p})$ has a subgroup A of finite index isomorphic to $(\mathcal{O}_{K_\mathfrak{p}}, +)$. So A is torsion-free. Now

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

and as the final group in this sequence is finite, we see that $E(K)_{\text{tors}}$ is as well. □

Remark. We have used a bit more machinery than is really needed in this proof. If we took $\mathfrak{p}$ to be a prime of good reduction, then the rest of the proof goes through without needing to employ the compactness argument of Lemma 9.7.

Lemma 10.3. Let $\mathfrak{p}$ be a prime of good reduction with $\mathfrak{p} \nmid n$. Then reduction mod $\mathfrak{p}$ gives an injective group homomorphism

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

Proof. We already showed (proposition 9.5) that $E(K_{\mathfrak{p}}) \to \tilde{E}(k_{\mathfrak{p}})$ is a group homomorphism with kernel $E_1(K_{\mathfrak{p}})$. Then (Corollary 9.5) since $\mathfrak{p} \nmid n$ we see that $E_1(K_{\mathfrak{p}})$ has no n-torsion, as the multiplication-by-n map on formal groups is an isomorphism. Since $E(K)$ injects into $E(K_{\mathfrak{p}})$, we get the result. □

Example. Let $E/\mathbb{Q}$ be given by

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

and note its discriminant $\Delta = -11$. This is a globally minimal Weierstrass equation, and E has good reduction at all $p \neq 11$. We count points on the reduced curves $\tilde{E}(\mathbb{F}_p)$.

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

By Lemma 11.3, we have $\#E(\mathbb{Q})_{\text{tors}} \mid 5 \cdot 2^a$ for some $a \geq 0$. Turning our attention to the prime 3, we see that also $\#E(\mathbb{Q})_{\text{tors}} \mid 5 \cdot 3^b$ for $b \geq 0$, so $\#E(\mathbb{Q})_{\text{tors}} \mid 5$. We see that $(0, 0)$ is a point of order 5 in $E(\mathbb{Q})$, so $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/5\mathbb{Z}$.

Example. Now let $E/\mathbb{Q}$ be given by

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

This equation has discriminant $\Delta = -43$, so again is globally minimal, and E has bad reduction only at $p = 43$. Counting points on reduced curves gives the following data.

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

Playing the same game as last time, we find $\#E(\mathbb{Q})_{\text{tors}} \mid 5 \cdot 2^a$ and $\#E(\mathbb{Q})_{\text{tors}} \mid 9 \cdot 11^b$ for some $a, b \geq 0$. These statements combined show that $E(\mathbb{Q})$ is torsion-free, and we see that $P = (0, 0) \in E(\mathbb{Q})$ is a point of infinite order. Thus the rank of $E(\mathbb{Q})$ is at least 1.

Example. Consider the family of *congruent number curves*

$$E_D : y^2 = x^3 - D^2 x$$

for $D \in \mathbb{Z}$ squarefree. The discriminant here is $\Delta = 2^6 \cdot D^6$. Then $E(\mathbb{Q})_{\text{tors}}$ contains a copy of $(\mathbb{Z}/2\mathbb{Z})^2$ generated by the 2-torsion points $(0,0)$, $(\pm D, 0)$. Now let $f(x) = x^3 - D^2 x$. If $p \nmid 2D$, then

$$\tilde{E}_D(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} (\chi_p(f(x)) + 1),$$

where χ_p is the Legendre symbol. If $p \equiv 3 \pmod 4$, since f is an odd function we have $\chi_p(f(-x)) = -\chi_p(f(x))$ and

$$\begin{aligned} \#\tilde{E}_D(\mathbb{F}_p) &= 1 + \sum_{x \in \mathbb{F}_p} (\chi_p(f(x)) + 1) \\ &= 1 + p + \sum_{x \in \mathbb{F}_p} \chi_p(f(x)) \\ &= p + 1, \end{aligned}$$

since negatives in the sum will cancel.

Now let $m = \#E_D(\mathbb{Q})_{\text{tors}}$. We have $4 \mid m \mid p+1$ for all sufficiently large (i.e. $p \nmid 2D,\ p \nmid m$) primes $p \equiv 3 \pmod 4$. Suppose for the sake of contradiction that $m = 4k$ with $k > 1$. Then the divisibility chain above shows that only finitely many primes congruent to 3 (mod 4) are not congruent to $-1 \pmod m$. This finiteness contradicts Dirichlet's theorem on primes in arithmetic progressions. So

$$E_D(\mathbb{Q})_{\text{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^2,$$

and rank $E_D(\mathbb{Q}) \geq 1$ iff there exist $x, y \in \mathbb{Q}$ with $y \neq 0$ such that $y^2 = x^3 - D^2 x$ iff (lecture 1) D is a congruent number.

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

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

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

Note that we are *not* saying any integer point has to be torsion; see above for a counterexample.

Proof. (i) The Weierstrass equation defines a formal group $\widehat{E}$ over $\mathbb{Z}$. For $r \geq 1$, recall the subgroups

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

By proposition 9.2, we have $\widehat{E}(p^r\mathbb{Z}_p) \cong (\mathbb{Z}_p, +)$ when $r > \frac{1}{p-1}$. Thus $\widehat{E}(4\mathbb{Z}_2)$ and $\widehat{E}(p\mathbb{Z}_p)$ for p odd are torsion-free. Since $O_E \neq T \in E(\mathbb{Q})_{\text{tors}}$, we then have $v_2(x) \geq -2,\ v_2(y) \geq -3$ and $v_p(x),\ v_p(y) \geq 0$ for odd p.

(ii) Suppose $T \in \widehat{E}(2\mathbb{Z}_2)$, i.e. $v(x) = -2,\ v(y) = -3$. Since $\widehat{E}(2\mathbb{Z}_2)/\widehat{E}(4\mathbb{Z}_2) \cong (\mathbb{F}_2, +)$ and $\widehat{E}(4\mathbb{Z}_2)$ is torsion-free, we have $2T = O_E$. Also, we have

$$(x,y) = T = -T = (x, -y - a_1x - a_3),$$

so

$$\begin{aligned} & 2y + a_1x + a_3 = 0 \\ \implies\ & 8y + a_1(4x) + 4a_3 = 0. \end{aligned}$$

Using the valuations of x, y, we see that this is only possible when a_1 is odd. So if $2T \neq O_E$ or a_1 is even we have $T \notin \widehat{E}(2\mathbb{Z}_2)$, so $x, y \in \mathbb{Z}$. □

Example. The curve

$$E : y^2 + xy = x^3 + 4x + 1$$

admits the 2-torsion point $(-1/4,\ 1/8) \in E(\mathbb{Q})[2]$. This point agrees with the powers of 2 allowable in the denominators of a torsion point per Lemma 10.4. We also see that $a_1 = 1$ is odd, as it must be if the coordinates of a torsion point are not integers.

Theorem 10.5 (Lutz-Nagell)**.** Let

$$E/\mathbb{Q} : y^2 = x^3 + ax + b =: f(x)$$

be an elliptic curve with $a, b \in \mathbb{Z}$. Suppose $O_E \neq T = (x,y) \in E(\mathbb{Q})_{\text{tors}}$. Then $x, y \in \mathbb{Z}$, and either $y = 0$ or $y^2 \mid (4a^3 + 27b^2)$.

Proof. Our situation satisfies the hypothesis of Lemma 10.4, so $x, y \in \mathbb{Z}$. If $2T = O_E$, then $y = 0$. Otherwise $O_E \neq 2T = (x_2, y_2) \in E(\mathbb{Q})_{\text{tors}}$. Again using Lemma 10.4, we have $x_2, y_2 \in \mathbb{Z}$. But

$$x_2 = \left(\frac{f'(x)}{2y}\right)^2 - 2x \in \mathbb{Z},$$

so $y \mid f'(x)$. Since E is nonsingular, we know $f(X)$ and $f'(X)$ (hence $f'(X)^2$) are coprime. So there exist $g, h \in \mathbb{Q}[X]$ such that $g(X)f(X) + h(X)f'(X) = 1$. Doing this calculation and clearing denominators gives

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

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

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

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

11 Kummer Theory

In this section, we write K for a field with $\operatorname{char} K \nmid n$, and we assume K contains all n^{th} roots of unity (i.e. $\mu_n \subset K$).

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

Proof. The extension L/K is Galois since $\mu_n \subset K$ (normal) and $\operatorname{char} K \nmid n$ (separable). Define the *Kummer pairing* $\langle \cdot, \cdot \rangle : \operatorname{Gal}(L/K) \times \Delta \to \mu_n$ by $(\sigma, x) \mapsto \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}}$. This is well-defined, since if $\alpha, \beta \in L$ with $\alpha^n = \beta^n = x$, then $(\alpha/\beta)^n = 1$, so $\alpha/\beta \in \mu_n \subset K$. Then

$$\begin{aligned} \sigma\left(\frac{\alpha}{\beta}\right) &= \frac{\alpha}{\beta} \\ \implies \frac{\sigma(\alpha)}{\alpha} &= \frac{\sigma(\beta)}{\beta}. \end{aligned}$$

This pairing is bilinear: indeed, for $\sigma, \tau \in \operatorname{Gal}(L/K)$, we have

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

since $\tau(\sqrt[n]{x})$ is an n^{th} root of x and the value of the Kummer pairing doesn't depend on which root we pick. Linearity in the second argument follows immediately.

We claim also that the pairing is nondegenerate. Fixing $\sigma \in \operatorname{Gal}(L/K)$, we see that if $\langle \sigma, x \rangle = 1$ for all $x \in \Delta$, then $\sigma(\sqrt[n]{x}) = \sqrt[n]{x}$ for all $x \in \Delta$. Thus σ fixes $L = K(\sqrt[n]{\Delta})$ pointwise, so must be the identity in $\operatorname{Gal}(L/K)$.

Now let $x \in \Delta$. If $\langle \sigma, x \rangle = 1$ for all $\sigma \in \operatorname{Gal}(L/K)$, then

$$\begin{aligned} \sigma(\sqrt[n]{x}) &= \sqrt[n]{x} \quad \forall \sigma \in \operatorname{Gal}(L/K) \\ \implies \sqrt[n]{x} &\in K \\ \implies x &\in (K^\times)^n, \end{aligned}$$

so $x(K^\times)^n$ is trivial in Δ. So the Kummer pairing is nondegenerate.

We now have injective group homomorphisms

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

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

From (i), we have that $\mathrm{Gal}(L/K)$ is abelian and of exponent dividing n. The structure theory of finite abelian group then shows $\mathrm{Hom}(G, \mu_n) \cong G$ (though non-canonically). So

$$|\operatorname{Gal}(L/K)| \leq |\Delta| \leq |\operatorname{Gal}(L/K)|,$$

so $|\operatorname{Gal}(L/K)| = |\Delta|$, and the maps (i) and (ii) are isomorphisms, proving the lemma. □

Example. One can use the result to quickly show, e.g., that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3$.

Theorem 11.2. There is a bijection

$$\{\text{finite subgroups } \Delta \subset K^\times/(K^\times)^n\} \cong \{\text{finite abelian extensions } L/K \text{ of exponent dividing } n\},$$

mapping Δ to $K(\sqrt[n]{\Delta})$ and L/K to $((L^\times)^n \cap K^\times)/(K^\times)^n$.

Proof. We prove that the maps given in the statement are mutually inverse.

(i) Let $\Delta \subset K^\times/(K^\times)^n$ by a finite subgroup. Let $L = L(\sqrt[n]{\Delta})$ and $\Delta' = ((L^\times)^n \cap K^\times)/(K^\times)^n$. We must show $\Delta = \Delta'$. Clearly $\Delta \subset \Delta'$, so

$$L = K(\sqrt[n]{\Delta}) \subset K(\sqrt[n]{\Delta'}) \subset L.$$

Thus $K(\sqrt[n]{\Delta}) = K(\sqrt[n]{\Delta'})$, and by Lemma 11.1 we have $|\Delta| = |\Delta'|$. Since $\Delta \subset \Delta'$, we get $\Delta = \Delta'$.

(ii) Let L/K be a finite abelian extension whose Galois group has exponent dividing n. Let $\Delta = ((L^\times)^n \cap K^\times)/(K^\times)^n$. Then $K(\sqrt[n]{\Delta}) \subset L$, and we aim to show equality. Let $G = \mathrm{Gal}(L/K)$. The Kummer pairing gives an injection

$$\Delta \hookrightarrow \mathrm{Hom}(G, \mu_n),$$

which we claim is surjective. Given the claim, we get (again using Lemma 11.1)

$$[K(\sqrt[n]{\Delta}) : K] = |\Delta| = |G| = [L : K].$$

Then we will have $K(\sqrt[n]{\Delta}) \subset L$ with the same degree over K, giving $K(\sqrt[n]{\Delta}) = L$.

We now prove the claim. Let $\chi : G \to \mu_n$ be a group homomorphism. Distinct automorphisms are linearly independent, so there exists $a \in L$ such that

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

Let $\sigma \in G$. Then

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

so $\sigma(y^n) = y^n$ for all $\sigma \in G$. Let $x = y^n$. Then $x \in K^\times \cap (L^\times)^n$ (i.e. $x(K^\times)^n \subset \Delta$). The calculation above also shows

$$\begin{aligned} \chi(\sigma) &= \frac{\sigma(y)}{y} \\ &= \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}}, \end{aligned}$$

so the map $\Delta \hookrightarrow \mathrm{Hom}(G, \mu_n)$ sends $x(K^\times)^n$ to χ, proving the claim.

□

Looking forward to the proof of the Mordell-Weil theorem, we now turn to an application to number fields.

Proposition 11.1. Let K be a number field containing μ_n, and let S be a finite set of primes of K. Then there are only finitely many extensions L/K such that

(i) L/K is an abelian extension of exponent dividing n, and

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

Proof. Theorem 11.2 implies that $L = K(\sqrt[n]{\Delta})$ for some finite subgroup $\Delta \subset K^\times/(K^\times)^n$. Let $\mathfrak{p}$ be a prime of K, and factor

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$$

where the $\mathfrak{P}_i$ are distinct primes of L. If $x \in K^\times$ represents an element of Δ, we have

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

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

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

Thus any L of the required form comes from a subgroup of $K(S,n)$, so it's enough now to show

Lemma 11.3. *$K(S,n)$ is finite.*

Proof of Lemma 11.4. The map $K(S,n) \to (\mathbb{Z}/n\mathbb{Z})^{|S|}$ given by $x \mapsto (v_{\mathfrak{p}}(x) \pmod{n})_{\mathfrak{p}\in S}$ is a group homomorphism with kernel $K(\emptyset,n)$. Since $|S| < \infty$, by the first isomorphism theorem it suffices to prove the lemma for $S = \emptyset$. If $x \in K^\times$ represents an element of $K(\emptyset,n)$, then $(x) = \mathfrak{a}^n$ for some fractional ideal $\mathfrak{a} \subset K$. There is an exact sequence

$$0 \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n \to K(\emptyset,n) \to \mathcal{CL}(K)[n] \to 0$$

where $K(\emptyset,n) \to \mathcal{CL}(K)$ is given by $x(K^\times)^n \mapsto [\mathfrak{a}]$. But $\mathcal{CL}(K)$ is finite, and as a consequence of Dirichlet's unit theorem we have that $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n$ is finite as well. It follows that $K(\emptyset,n)$. □

□

12 Elliptic Curves over Number Fields II: The Mordell-Weil Theorem

Notation in this section is as in section 10.

Lemma 12.1 ("A fairly brutal, low-tech thing we bash out"). Let E/K be an elliptic curve and L/K a finite Galois extension. The natural map

$$E(K)/nE(K) \to E(L)/nE(L)$$

has finite kernel.

Proof. We show that the kernel injects into a finite set. For each element in the kernel, we pick a coset representative $P \in E(K)$ and a point $Q \in E(L)$ with $nQ = P$. Note that for $\sigma \in \mathrm{Gal}(L/K)$, the point $\sigma Q - Q$ is n-torsion since $nQ = P$ is defined over K, hence fixed by Galois. Since $\mathrm{Gal}(L/K)$ and $E[n]$ are both finite, there are only finitely many possibilities for the map $\mathrm{Gal}(L/K) \to E[n]$ given by $\sigma \mapsto \sigma Q - Q$. But if $P_1, P_2 \in E(K)$ with $P_i = nQ_i$ for $Q_1, Q_2 \in E(L)$, and $\sigma Q_1 - Q_1 = \sigma Q_2 - Q_2$ for all $\sigma \in \mathrm{Gal}(L/K)$, then

$$\begin{aligned} &\sigma(Q_1 - Q_2) = Q_1 - Q_2 \ \forall \sigma \in \mathrm{Gal}(L/K) \\ \implies &Q_1 - Q_2 \in E(K) \\ \implies &P_1 - P_2 \in nE(K). \end{aligned}$$

□

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

Remark. The proof of Mordell-Weil only requires $n = 2$ in the statement of the theorem, but for further results (e.g. bounding ranks) having more possibilities for n is useful.

Proof of Weak Mordell-Weil. By Lemma 12.1, we may replace K by a finite Galois extension, so WLOG assume $\mu_n \subset K$ and $E[n] \subset E(K)$. We claim that for any $P \in E(K)$, the extension $K([n]^{-1}P)/K$ satisfies the hypotheses of Proposition 11.1 with

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

Given the claim, we have that $\bigcup_{P \in E(K)} K([n]^{-1}P)$ is a finite union, so generates (via taking composita) a finite extension L/K. Then L/K is finite (and WLOG Galois), and

$$E(K)/nE(K) \to E(L)/nE(L)$$

is the zero map. Then Lemma 12.1 implies $E(K)/nE(K)$ is finite.

It remains to prove the claim. First we show that $K([n]^{-1}P)/K$ is an abelian extension of exponent dividing n. Recall that we have by hypothesis $E[n] \subset E(K)$, and we've fixed $P \in E(K)$. Note that $\mathrm{Gal}(\overline{K}/K)$ acts on $[n^{-1}]P$ since $P \in E(K)$. Pick $Q \in [n]^{-1}P$, and consider the map

$$\mathrm{Gal}(\overline{K}/K) \to E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$$

defined by $\sigma \mapsto \sigma Q - Q$ (note the analogy to the Kummer pairing; here we've just written it in additive notation). We claim this map is a group homomorphism. Indeed, we have

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

since $\tau Q - Q \in E[n] \subset E(K)$ and Galois fixes $E(K)$. Furthermore, if $\sigma Q = Q$, then $\sigma(Q + T) = Q + T$ for all $T \in E[n]$. In particular σ fixes $E[n]$, and therefore $K([n]^{-1}P)$ pointwise, so $\sigma \in \mathrm{Gal}(\overline{K}/K([n^{-1}]P)$. We get an injection

$$\mathrm{Gal}(\overline{K}/K)/\mathrm{Gal}(\overline{K}/K([n^{-1}]P)) \cong \mathrm{Gal}(K([n^{-1}]P)/K) \hookrightarrow E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2,$$

showing that $K([n^{-1}]P)/K$ is an abelian extension of exponent dividing n.

It remains to show that $K([n]^{-1}P)/K$ is unramified outside the set $\{\mathfrak{p} \mid n\} \cup \{\text{primes of bad reduction}\}$; this follows from Theorem 9.6. $\square$

Remark. If $K = \mathbb{R}$ or $\mathbb{C}$ or $[K : \mathbb{Q}_p] < \infty$, then $|E(K)/nE(K)| < \infty$, yet $E(K)$ is uncountable, so not finitely generated. These examples illustrate that Weak Mordell-Weil is not enough on its own to get the full Mordell-Weil Theorem. What distinguishes number fields is its theory of *heights*: there exists a quadratic form (the *canonical height*) $\hat{h} : E(K) \to \mathbb{R}_{\geq 0}$ with the property that for any $B \geq 0$, the set $\{P \in E(K) : \hat{h}(P) \leq B\}$ is finite. We call this property "property $(*)$."

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

Proof. Fix an integer $n \geq 2$. By Weak Mordell-Weil, the quotient $E(K)/nE(K)$ is finite. Pick coset representatives $P_1, \ldots, P_m$. Let $\Sigma = \{P \in E(K) : \hat{h}(P) \leq \max_{1 \leq i \leq m} \hat{h}(P_i)\}$. Property $(*)$ ensures Σ is finite; we claim that Σ generates $E(K)$. If not, there's a point $P \in E(K) \setminus \langle \Sigma \rangle$, and by property $(*)$ we can assume P minimizes $\hat{h}$ on this set. Then $P = P_i + nQ$ for some $1 \leq i \leq m$ and $Q \in E(K)$, noting that $Q \notin \langle \Sigma \rangle$. By our choice of P, we have $\hat{h}(P) \leq \hat{h}(Q)$. Then

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

where the last equality comes from the parallelogram law. Subtracting off $2\hat{h}(P)$ gives

$$\hat{h}(P) \leq \hat{h}(P_i),$$

which by definition of Σ implies $P \in \Sigma$. This fact contradicts our choice of P, so we have $E(K) = \langle \Sigma \rangle$, and we're done. $\square$

13 Heights

The theory of heights will make precise how "arithmetically complicated" a point of $\mathbb{P}^n(K)$ is. For simplicity, we take $K = \mathbb{Q}$; note, however, that the theory can be extended to work over an arbitrary number field without too many changes.

Write $P \in \mathbb{P}^n(\mathbb{Q})$ as $P = (a_0 : \cdots : a_n)$ where all a_i's are integers with greatest common divisor 1.

Definition 13.1. The *height* $H(P)$ is $\max_{0 \le i \le n} |a_i|$. ("Amount of chalk you'd need to write the point down on the board")

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

$$c_1 H(P)^d \le H(F(P)) \le c_2 H(P)^d$$

for all $P \in \mathbb{P}^1(\mathbb{Q})$.

Proof. WLOG we can take $f_1, f_2 \in \mathbb{Z}[X_1, X_2]$. We prove the upper bound first. Write $P = (a : b)$ for $a, b \in \mathbb{Z}$ with $(a, b) = 1$. Then

$$\begin{aligned} H(F(P)) &\le \max(|f_1(a, b)|, |f_2(a, b)|) \\ &\le c_2 \max(|a|, |b|)^d \\ &= c_2 H(P)^d \end{aligned}$$

by the triangle inequality. Note that we can take c_2 to be the larger between f_1, f_2 of the sums of absolute values of coefficients of these polynomials.

It remains to show the lower bound. We claim there exist $g_{ij} \in \mathbb{Z}[X_1, X_2]$ $(1 \le i, j \le 2)$ homogeneous polynomials of degree $d - 1$ and $\kappa \in \mathbb{Z}_{>0}$ such that

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

Indeed, running Euclid's algorithm on $f_1(x, 1)$ and $f_2(x, 1)$ gives $r, s \in \mathbb{Q}[x]$ of degree less than d such that

$$r(x) f_1(x, 1) + s(x) f_2(x, 1) = 1,$$

since f_1 and f_2 are relatively prime. Homogenizing and clearing denominators gives the claim for $i = 2$, and repeating the process for $i = 1$ gives the full claim.

Write $P = (a_1 : a_2)$ with $a_1, a_2 \in \mathbb{Z}$ coprime. The claim implies

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

Then $\gcd(f_1(a_1, a_2), f_2(a_1, a_2))$ divides $\gcd(\kappa a_1^{2d-1}, \kappa a_2^{2d-1}) = \kappa$. But also

$$\begin{aligned} |\kappa a_i^{2d-1}| &\leq \max_{j=1,2} |f_j(a_1, a_2)| \sum_{j=1}^{2} |g_{ij}(a_1, a_2)| \\ &\leq \kappa H(F(P)) \gamma_i H(P)^{d-1}, \end{aligned}$$

where

$$\gamma_i = \sum_{j=1}^{2} \text{sum of absolute values of coeffs of } g_{ij}.$$

So

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

Set $c_1 = 1/\max(\gamma_1, \gamma_2)$, and we're done. □

Going forward, for $x \in \mathbb{Q}$ we write

$$H(x) = H((x : 1)) = \max(|u|, |v|)$$

where $x = u/v$ for $u, v \in \mathbb{Z}$ coprime.

Now we turn our attention to an elliptic curve $E/\mathbb{Q}$ given by a short Weierstrass equation

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

Definition 13.2. The *height* $H : E(\mathbb{Q}) \to \mathbb{R}_{\geq 1}$ is defined by

$$P \mapsto \begin{cases} H(x), & P = (x, y) \\ 1, & P = O_E. \end{cases}$$

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

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

$$|h(\phi(P)) - \deg \phi \, h(P)| \leq c$$

for all $P \in E(\mathbb{Q})$.

Remark. Note that c depends on E, E', ϕ, but does *not* depend on P.

Proof. Recall (Lemma 5.3) the commutative diagram

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

where $\deg \phi = \deg \xi = d$. By Lemma 13.1, there exist $c_1, c_2 > 0$ such that

$$c_1 H(P)^d \leq H(\phi(P)) \leq c_2 H(P)^d$$

for all $P \in E(\mathbb{Q})$, and taking logs gives

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

hence the result. □

Example. For $\phi = [2] : E \to E$, the lemma says there exists $c > 0$ such that

$$|h(2P) - 4h(P)| < c$$

for all $P \in E(\mathbb{Q})$.

Definition 13.3. The *canonical height* is

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

We need to check that the limit exists. Let $m \geq n$; then using Lemma 13.2

we get

$$\begin{aligned}\left|\frac{1}{4^m}h(2^mP)-\frac{1}{4^n}h(2^nP)\right| &\le \sum_{r=n}^{m-1}\left|\frac{1}{4^{r+1}}h(2^{r+1}P)-\frac{1}{4^r}h(2^rP)\right| \\ &= \sum_{r=n}^{m-1}\frac{1}{4^{r+1}}\left|h(2(2^rP))-4h(2^rP)\right| \\ &\le c\sum_{r=n}^{\infty}\frac{1}{4^{r+1}} \\ &= \frac{c}{3\cdot 4^n},\end{aligned}$$

which goes to 0 as $n\to\infty$. So the sequence on the right is Cauchy, and $\hat{f}(P)$ exists.

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

Proof. Put $n=0$ in the calculation above to get

$$\left|\frac{1}{4^m}h(2^mP)-h(P)\right|\le\frac{c}{3}.$$

Take the limit as $m\to\infty$ to get the result. □

Corollary 13.3.1. For any $B>0$, the set $\{P\in E(\mathbb{Q}):\hat{h}(P)\le B\}$ is finite.

Proof. Using Lemma 13.3, we see that if $h(P)$ is bounded, then $\hat{h}(P)$ is bounded as well. There are only finitely many possibilities for $x(P)$ giving $h(P)\le B$, and since y depends on x according to the Weierstrass equation, we get the result. □

Lemma 13.4. Let $\phi:E\to E'$ be an isogeny over $\mathbb{Q}$. Then $\hat{h}(\phi(P))=\deg\phi\,\hat{h}(P)$ for all $P\in E(\mathbb{Q})$.

Proof. By lemma 13.2, there is a $c>0$ such that

$$|h(\phi(P))-\deg\phi h(P)|\le c$$

for all $P\in E(\mathbb{Q})$. Replace P by 2^nP, divide by 4^n, and take the limit as $n\to\infty$ to get $\hat{h}$'s on the left (ϕ is a group homomorphism) and 0 on the right. □

Remark. The same proof shows that $\hat{h}$, unlike h, *does not* depend on the choice of Weierstrass equation for E (take $\phi \in \mathrm{Aut}(E)$). If we instead take $\phi = [n]$, we see

$$\hat{h}(nP) = n^2 \hat{h}(P)$$

for all $P \in E(\mathbb{Q})$, suggesting $\hat{h}$ might be a quadratic form. This is indeed true (as we might hope it is, since we've already used that fact!).

Lemma 13.5. Let $E/\mathbb{Q}$ be an elliptic curve, and fix a Weierstrass equation

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

with $a, b \in \mathbb{Z}$. Then there exists $c > 0$ such that

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

for all $P, Q \in E(\mathbb{Q})$, with $P, Q, P+Q, P-Q \neq O_E$.

Proof. Let $P, Q, P+Q, P-Q$ have x-coordinates $x_1, \ldots, x_4 \in \mathbb{Q}$. Write $x_i = r_i/s_i$ where $r_i, s_i \in \mathbb{Z}$ are coprime. As in the proof of Lemma 5.7,

$$(s_3 s_4 : r_3 s_4 + r_4 s_3 : r_3 r_4) = (W_0 : W_1 : W_2)$$

with $W_0 = (r_1 s_2 - r_2 s_1)^2$ and all coordinates on the left coprime. We also have that W_0, W_1, W_2 have degree at most 2 in r_1, s_1, and the same for r_2, s_2. So

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

for some positive constant c. work out in more detail? □

Theorem 13.6. The canonical height $\hat{h}$ is a quadratic form.

Proof. By Lemma 13.5 and the fact that $|h(2P) - 4h(P)|$ is bounded (if one of the points involved is O_E), we have (upon taking logs)

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

Replace P, Q by $2^n P, 2^n Q$, divide by 4^n, and take the limit as $n \to \infty$ to swap h for $\hat{h}$ and to get rid of the constant. Now replace P, Q by $P+Q, P-Q$ and use $\hat{h}(2P) = 4\hat{h}(P)$ to get the reverse inequality. So $\hat{h}$ satisfies the parallelogram law, and is therefore a quadratic form. □

Remark. Now we discuss how to generalize to a number field $K/\mathbb{Q}$. In this case, some care is needed when defining height. Picking suitable normalizations for the places of K, we have the *product formula*

$$\prod_{\text{places } v} |x|_v = 1$$

for all $x \in K^\times$. Given $P = (a_0 : a_1 : \cdots : a_n) \in \mathbb{P}^n(K)$, we define

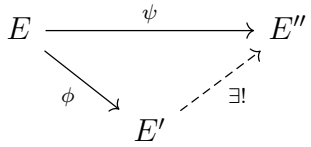
$$H(P) = \prod_v \max_{0 \le i \le n} (|a_i|_v).$$

The product formula ensures this quantity is well-defined. All results in this section then generalize from $\mathbb{Q}$ to K.

14 Dual Isogenies and the Weil Pairing

In this section, we let K be a perfect field and E/K an elliptic curve.

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



Proof. See Silverman ch. III. □

Proposition 14.2. Let $\phi : E \to E'$ be an isogeny of degree n. Then there is a unique isogeny $\hat{\phi} : E' \to E$ such that $\hat{\phi}\phi = [n]$. We call $\hat{\phi}$ the *dual isogeny.*

Proof. We have two cases.

ϕ separable: In this case we have $|\ker \phi| = n$, so $\ker \phi \subset E[n]$. Applying Proposition 14.1 with $\psi = [n]$ gives the unique $\hat{\phi}$.

ϕ inseparable: Omitted. See Silverman III.

□

Remark. (i) Proposition 14.2 shows that "E_1 is isogenous to E_2" is an equivalence relation; the existence of the dual isogeny shows that the relation is symmetric.

(ii) The fact that $\deg[n] = n^2$ and the uniqueness of $\hat{\phi}$ imply that $\deg \phi = \deg \hat{\phi}$ and $\widehat{[n]} = [n]$.

(iii) We have

$$\begin{aligned} \phi\hat{\phi}\phi &= \phi[n]_E \\ &= [n]_{E'}\phi, \end{aligned}$$

so $\phi\hat{\phi} = [n]_{E'}$ since ϕ is nonconstant. In particular, we have $\hat{\hat{\phi}} = \phi$.

Definition 14.1. Write "sum" for the map $\operatorname{div}(E) \to E$ sending $\sum n_P(P) \mapsto \sum n_P P$ (sending a formal sum to a sum of points under the group law on E). Note that this map gives an inverse to the isomorphism $E \cong \operatorname{Pic}^0(E)$ sending P to $[(P) - (O_E)]$, since the sum of coefficients on a point coming from a degree 0 divisor is 0.

Lemma 14.1. Let $D \in \operatorname{div}(E)$. Then $D \sim 0$ iff $\deg D = 0$ and sum $D = O_E$.

Definition 14.2. Let $\phi : E \to E'$ be an isogeny of degree n with dual isogeny $\hat{\phi} : E' \to E$. Assume char $K \nmid n$, so that $\phi, \hat{\phi}$ are separable. We define the *Weil pairing* (writing $E[\phi] = \ker \phi$)

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

Let $T \in E'[\hat{\phi}]$. Then $nT = O_E$, so by Lemma 14.1 there exists $f \in \overline{K}(E')^\times$ such that $\operatorname{div}(f) = n(T) - n(O_E)$. Pick $T_0 \in E(\overline{K})$ such that $\phi T_0 = T$. Then

$$\begin{aligned}
\phi^*(T) - \phi^*(O_E) &= \sum_{P \in E[\phi]} (P + T_0) - \sum_{P \in E[\phi]} (P) \\
&= nT_0 \\
&= \hat{\phi}\phi(T_0) \\
&= \hat{\phi}(T) \\
&= 0,
\end{aligned}$$

so there exists $g \in \overline{K}(E)^\times$ such that

$$\operatorname{div}(g) = \phi^*(T) - \phi^*(O_E).$$

Now

$$\begin{aligned}
\operatorname{div}(\phi^* f) &= \phi^*(\operatorname{div} f) \\
&= \phi^*(n(T) - n(O_E)) \\
&= \operatorname{div}(g^n),
\end{aligned}$$

so $\phi^* f = c g^n$ for some $c \in \overline{K}^\times$ since the only rational functions without zeroes or poles on a projective variety are constant. Rescaling our choice of f, we can assume WLOG $\phi^* f = g^n$.

Now if $S \in E[\phi]$, then $\phi \tau_S = \phi$. So $\tau_S^* \phi^* = \phi^*$, and τ_S^* fixes $\operatorname{div}(g)$. Thus

$$\operatorname{div}(\tau_S^* g) = \operatorname{div} g,$$

so $\tau_S^* g = \zeta g$ for some $\zeta \in \overline{K}^\times$. Then we have

$$\zeta = \frac{g(X+S)}{g(X)}$$

for all $X \in E(\overline{K}) \setminus \{\text{zeros/poles of } g\}$. We have

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

since $S \in E[\phi]$. It follows that $\zeta \in \mu_n$, and we can define

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

Proposition 14.3. The map e_ϕ is a nondegenerate bilinear form.

Proof. (i) We first check linearity in the first argument. We have

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

(ii) Next we check linearity in the second argument. Let $T_1, T_2 \in E'[\hat{\phi}]$, and pick f_1, f_2 with

$$\begin{aligned}\operatorname{div}(f_1) &= n(T_1) - n(O_E) \\ \operatorname{div}(f_2) &= n(T_2) - n(O_E),\end{aligned}$$

and

$$\begin{aligned}\phi^* f_1 &= g_1^n, \\ \phi^* f_2 &= g_2^n.\end{aligned}$$

There exists $h \in \overline{K}(E)^\times$ such that

$$\operatorname{div}(h) = (T_1) + (T_2) - (T_1 + T_2) - (O_E).$$

Put $f = \frac{f_1 f_2}{h^n}$, and check that

$$\begin{aligned}\phi^* f &= \frac{\phi^* f_1 \phi^* f_2}{(\phi^* h)^n} \\ &= \left(\frac{g_1 g_2}{\phi^* h}\right)^n \\ &= g^n\end{aligned}$$

for $g = \frac{g_1 g_2}{\phi^* h}$. Thus

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

where the last line follows since $S \in E[\phi]$.

(iii) We conclude by proving that e_ϕ is nondegenerate. Fix $T \in E[\hat{\phi}]$ and suppose $e_\phi(S, T) = 1$ for all $S \in E[\phi]$. Using the definition of e_ϕ, we see that this means $\tau_S^* g = g$ for all $S \in E[\phi]$. Then $\overline{K}(E)/\phi^* \overline{K}(E')$ is Galois with Galois group $E[\phi]$, since $S \in E[\phi]$ acts as τ_S^*. Since g is fixed by τ_S^* for all $S \in E[\phi]$, we have $g = \phi^* h$ for some $h \in \overline{K}(E')$. Then

$$\phi^* f = g^n = \phi^*(h^n),$$

so $f = h^n$ since ϕ^* is injective. Therefore $\div(h) = (T) - (O_E)$, so $T = 0$.

We've now shown the map $E'[\hat{\phi}] \hookrightarrow \operatorname{Hom}(E[\phi], \mu_n)$ is injective, and since $\#E[\phi] = \#E'[\hat{\phi}] = n$, it's an isomorphism, so e_ϕ is nondegenerate. □

Remark. (i) If E, E', ϕ are defined over K, then e_ϕ is Galois-equivariant; that is, for all $\sigma \in \operatorname{Gal}(\overline{K}/K)$ and $S \in E[\phi], T \in E'[\hat{\phi}]$, we have

$$e_\phi(\sigma S, \sigma T) = \sigma(E_\phi(S, T)).$$

(ii) Taking $\phi = [n] : E \to E$ gives $e_n : E[n] \times E[n] \to \mu_n \subset \mu_{n^2}$.

Corollary 14.1.1. If $E[n] \subset E(K)$, then $\mu_n \subset K$.

Proof. Since the Weil pairing e_n is nondegenerate, there exist $S, T \in E[n]$ such that $e_n(S,T)$ is a primitive n^{th} root of unity, say ζ_n. Indeed, if S is a point of order n, we can always find a suitable T, as otherwise S would be in the kernel of the pairing. Then

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

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

Example. This corollary immediately cuts down the possible torsion subgroups for $\mathbb{Q}$ points of $E/\mathbb{Q}$. For example, there is no elliptic curve $E/\mathbb{Q}$ with $E(\mathbb{Q})_{\text{tors}} \cong (\mathbb{Z}/3\mathbb{Z})^2$ since $\mathbb{Q}$ does not contain all cube roots of unity.

Remark. The Weil pairing is alternating: for all $T \in E[n]$ we have $e_n(T,T) = 1$, and in particular expanding $e_n(S+T, S+T)$ implies that $e_n(S,T) = e_n(T,S)^{-1}$.

15 Galois Cohomology

Throughout this section, we will denote by G a group and A a G-module (i.e. an abelian group with an action of G via group homomorphisms).

Definition 15.1. We define

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

We also want to define $H^1(G, A)$; this takes more work. By a *cochain* we mean a map of sets $G \to A$, and we denote the collection of cochains by $C^1(G, A)$. Within $C^1(G, A)$ live the *cocycles* $Z^1(G, A)$, whose elements are maps $(a_\sigma)_{\sigma \in G}$ satisfying the *cocycle condition*

$$a_{\sigma\tau} = \sigma(a_\tau) + a_\sigma.$$

By a *coboundary* we mean a map $(\sigma b - b)_{\sigma \in G}$ for some $b \in A$. We denote the set of coboundaries by $B^1(G, A)$ and note $B^1(G, A) \subset Z^1(G, A)$. Note also that C^1, Z^1, B^1 are all naturally abelian groups.

Definition 15.2. In the notation of the preceding discussion, we define

$$H^1(G, A) = Z^1(G, A)/B^1(G, A)$$

("cocycles modulo coboundaries").

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

Theorem 15.1. A short exact sequence of G-modules

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

gives rise to a long exact sequence of abelian groups

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

where the map δ is as defined as follows: for any $c \in C^G$, there is $b \in B$ such that $\psi(\sigma) = c$. Then

$$\begin{aligned} \psi(\sigma b - b) &= \sigma c - c \\ &= 0 \end{aligned}$$

for all $\sigma \in G$, so

$$\sigma b - b = \phi(a_\sigma)$$

for some $a_\sigma \in A$. Upon checking $(a_\sigma)_{\sigma \in G} \in Z^1(G, A)$, we can define $\delta(c)$ to be the class in $H^1(G, A)$ of $(a_\sigma)_{\sigma \in G}$.

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

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

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

If $G = \mathrm{Gal}(\overline{K}/K)$, we modify the definition of $H^1(G, A)$ by insisting

1. The stabilizer of each $a \in A$ is an open subgroup of G, and
2. All cochains $G \to A$ are continuous for the Krull topology on G and the discrete topology on A.

Then

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

The maps in the direct system are the inflation maps defined above.

Theorem 15.3 (Hilbert's theorem 90)**.** Let L/K be a finite Galois extension. Then

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

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

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

Let us see how G acts on x. For $\sigma \in G$, we have

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

where we have applied the cocycle condition written multiplicatively to get from the first line to the second. Therefore

$$a_\sigma = \sigma(x)/x,$$

and $(a_\sigma)_{\sigma \in G} \in B^1(G, L^\times)$. The desired result follows. □

Corollary 15.3.1.

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

Example. Assume char $K \nmid n$. There is an exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

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

We get a long exact sequence

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

By Hilbert 90, the rightmost group is 0, so we have

$$H^1(\mathrm{Gal}(\overline{K}/K), \mu_n) \cong K^\times/(K^\times)^n.$$

If $\mu_n \subset K$, then we get (considering only continuous homomorphisms)

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

In fact, finite subgroups of $\mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mu_n)$ correspond to finite abelian extensions of K with exponent dividing n; hence we have recovered the main result of the Kummer theory section in the language of Galois cohomology. Explicitly, if L/K is a finite Galois extension, then $\mathrm{Gal}(\overline{K}/K)$ surjects onto $\mathrm{Gal}(L/K)$ via a map π. We therefore get an injection

$$\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n) \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mu_n)$$

sending χ to $\chi \circ \pi$. The image is a finite subgroup $\Delta \subset K^\times/(K^\times)^n$. If $\mathrm{Gal}(L/K)$ is abelian of exponent dividing n, then

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

(compare to Theorem 11.2: in particular, unpacking the Galois-cohomological proof recovers the Kummer pairing as the connecting map in the long exact sequence for cohomology, and the proof ends up being the same as the one we gave earlier).

Going forward, we write $H^1(K, -)$ as a shorthand for $H^1(\mathrm{Gal}(\overline{K}/K, -))$.

Lemma 15.4. Let $K/\mathbb{Q}_p$ be a finite extension. 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. Use Hilbert 90 to identify $H^1(K, \mu_n)$ with $K^\times/(K^\times)^n$ and $H^1(K^{\mathrm{nr}}, \mu_n)$ with $K^{\mathrm{nr}\,\times}/(K^{\mathrm{nr}\,\times})^n$. The discrete valuation $v : K^\times \to \mathbb{Z}$ extends to $K^{\mathrm{nr}\,\times}$. If $x \in K^\times$ with $x = y^n$ for some $y \in K^{\mathrm{nr}}$, then

$$v(x) = nv(y) \equiv 0 \pmod{n}.$$

□

Remark. If $p \nmid n$, one can show the inclusion in the lemma is an equality.

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

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

Taking Galois cohomology gives a long exact sequence

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

We then get the short exact sequence below, augmented with the data of K a number field and for each place v, an embedding $\overline{K} \subset \overline{K_v}$. Note that we are identifying $\mathrm{Gal}(\overline{K_v}/K_v)$ naturally with a subgroup of $\mathrm{Gal}(\overline{K}/K)$.

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

Definition 15.3. The *ϕ-Selmer group* is

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

The *Tate-Shafarevich group* is

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

From these definitions, we get a short exact sequence

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

Taking $\phi = [n]$ gives

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

Now we can rearrange the proof of weak Mordell-Weil to get the

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

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

$$0 \to H^1(\mathrm{Gal}(L/K), E(L)[n]) \xrightarrow{\inf} H^1(K, E[n]) \xrightarrow{\mathrm{res}} H^1(L, E[n])$$

where res restricts to a map $S^{(n)}(E/K) \to S^{(n)}(E/L)$ and $H^1(\mathrm{Gal}(L/K), E(L)[n])$ is finite. So we can extend our field to assume $E[n] \subset E(K)$ (and so by the Weil pairing $\mu_n \subset K$). It follows that $E[n] \cong \mu_n \times \mu_n$ as a $\mathrm{Gal}(\overline{K}/K)$-module, since we've extended K to make Galois act trivially. Then

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

Now let

$$S = \{\text{primes of bad reduction for } E/K\} \cup \{v \mid n\infty\},$$

noting that this is a finite set of places. We have

Definition 15.4. The subgroup $H^1(K, A)$ unramified outside S is

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

There is a commutative diagram with exact rows

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & E(K_v) & \xrightarrow{\times n} & E(K_v) & \xrightarrow{\delta_v} & H^1(K_v, E[n]) & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}} & & \\ \cdots & \longrightarrow & E(K_v^{\mathrm{nr}}) & \xrightarrow{\times n} & E(K_v^{\mathrm{nr}}) & \xrightarrow{0} & H^1(K_v^{\mathrm{nr}}, E[n]) & \longrightarrow & \cdots \end{array}$$

where multiplication by n on the bottom is surjective for all $v \notin S$ (Theorem 9.7). So

$$\mathrm{Im}(\delta_v) \subset \ker(\mathrm{res}).$$

Therefore

$$\begin{aligned} S^{(n)}(E/K) &= \{\alpha \in H^1(K, E[n]) : \mathrm{res}_v(\alpha) \in \mathrm{Im}(\delta_v)\, \forall v\} \\ &\subset H^1(K, E[n]; S) \\ &\cong H^1(K, \mu_n; S) \times H^1(K, \mu_n; S) \\ &\subset K(S, n) \times K(S, n). \end{aligned}$$

But $K(S, n)$ is finite by lemma 11.4, so $S^{(n)}(E/K)$ is finite as well. □

Remark. $S^{(n)}(E/K)$ is finite and effectively computable. It is conjectured that $Ш(E/K)$ is finite. This would imply that the rank of $E(K)$ is effectively computable (also not known).

16 Descent by Cyclic Isogeny

Here we let E, E' be elliptic curves over a number field K, and $\phi : E \to E'$ an isogeny of degree n. Suppose $E'[\hat{\phi}] \cong \mathbb{Z}/n\mathbb{Z}$ 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 have a short exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

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

which becomes a long exact sequence

$$\cdots \to E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(K, \mu_n) \to \dots$$

where $H^1(K, \mu_n) \cong K^\times/(K^\times)^n$ by Hilbert 90. Let $\alpha : E'(K) \to K^\times/(K^\times)^n$ be the composite of this isomorphism with δ.

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

$$\alpha(P) = f(P) \pmod{(K^\times)^n}$$

for all $P \in E'(K) \setminus \{O_E, T\}$.

Proof. Let $Q \in \phi^{-1}P$. Then $\delta(P)$ is represented by the cocycle

$$\sigma \mapsto \sigma Q - Q \in E[\phi] \cong \mu_n.$$

Then

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

for any $X \in E \setminus \{\text{zeros and poles of } g\}$. Taking $X = Q$, this becomes

$$\begin{aligned} \frac{g(\sigma Q)}{g(Q)} &= \frac{\sigma(g(Q))}{g(Q)} \\ &= \frac{\sigma \sqrt[n]{f(P)}}{\sqrt[n]{f(P)}}. \end{aligned}$$

So $\delta(P)$ is represented by the cocycle

$$\sigma \mapsto \frac{\sigma(\sqrt[n]{f(P)})}{\sqrt[n]{f(P)}}.$$

But $H^1(K, \mu_n) \cong K^\times/(K^\times)^n$ via sending $x \in K^\times/(K^\times)^n$ to

$$\sigma \mapsto \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}}.$$

The result follows. □

We now specialize to *descent by* 2*-isogeny.* We assume E has Weierstrass equation

$$y^2 = x(x^2 + ax + b)$$

with discriminant

$$\Delta = b(a^2 - 4ab) \neq 0$$

and 2-isogeny to the curve

$$E' : y^2 = x(x^2 + a'x + b')$$

with

$$\begin{aligned} a' &= -2a; \\ b' &= a^2 - 4b. \end{aligned}$$

The isogeny $\phi : E \to E'$ is given by

$$(x, y) \mapsto \left(\left(\frac{y}{x}\right)^2, \frac{y(x^2 - b)}{x^2} \right).$$

Repeating this construction gives the dual isogeny $\hat{\phi} : E' \to E$ given by

$$(x, y) \mapsto \left(\frac{1}{4}\left(\frac{y}{x}\right)^2, \frac{y(x^2 - b')}{8x^2} \right).$$

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

Proposition 16.1. There is a group homomorphism

$$E'(K) \to K^\times/(K^\times)^2$$

given by

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

having kernel $\phi E(K)$.

Proof. We give two proofs. For the first, apply Theorem 16.1 with $f = x \in K(E')$ and $g = y/x \in K(E)$.

Alternatively, one can calculate directly; for this proof see ES4. □

We now have an injective group homomorphism

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

and via symmetry we have another injection

$$\alpha_E : E(K)/\hat{\phi}E'(K) \hookrightarrow K^\times/(K^\times)^2.$$

Lemma 16.2. $2^{\mathrm{rk}\ E(K)} = \frac{|\operatorname{Im}\alpha_E||\operatorname{Im}\alpha_{E'}|}{4}$.

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

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

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

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

We know $E(K)[\phi]$ and $E'(K)[\hat{\phi}]$ are both isomorphic to $\mathbb{Z}/2\mathbb{Z}$, and that $E'(K)/\phi E(K)$ and $E(K)/\hat{\phi}E'(K)$ are isomorphic to $\operatorname{Im}\alpha_{E'}$ and $\operatorname{Im}_{\alpha_E}$ respectively. We now use a general fact about exact sequences of finite abelian groups: the product of the order of every other group in the sequence taken one way is the same as that taken the other way. From this fact we find

$$\frac{|E(K)/2E(K)|}{|E(K)[2]|} = \frac{|\operatorname{Im}\alpha_E| \cdot |\operatorname{Im}\alpha_{E'}|}{2 \cdot 2}.$$

Since K is a number field, by Mordell-Weil we have

$$E(K) \cong \Delta \times \mathbb{Z}^r$$

where Δ is a finite abelian group and r the rank of $E(K)$. In this notation we have

$$E(K)/2E(K) \cong \Delta/2\Delta \times (\mathbb{Z}/2\mathbb{Z})^r;$$
$$E(K)[2] \cong \Delta[2].$$

Since Δ is finite, the groups $\Delta/2\Delta$ and $\Delta[2]$ have the same order. So we have

$$\frac{|E(K)/2E(K)|}{|E(K)[2]|} = 2^r,$$

hence the result. □

Lemma 16.3. If K is a number field and $a, b \in \mathcal{O}_K$, then

$$\mathrm{Im}(\alpha_E) \subset K(S, 2),$$

where $S = \{\text{primes dividing } b\}$.

Proof. We must show that if $x, y \in K$ and $y^2 = x(x^2 + ax + b)$ with $v_\mathfrak{p}(b) = 0$ then $v_\mathfrak{p}(x) \equiv 0 \pmod 2$. We use two cases.

- If $v_\mathfrak{p}(x) < 0$, then lemma 9.1 says $v_\mathfrak{p}(x)$ is even.
- If $v_\mathfrak{p}(x) > 0$, then $v_\mathfrak{p}(x^2 + ax + b) = 0$ since $\mathfrak{p} \nmid b$, and from the Weierstrass equation $v_\mathfrak{p}(x)$ is forced to be even.

□

Lemma 16.4. If $b_1 b_2 = b$ then $b_1(K^\times)^2 \in \mathrm{Im}(\alpha_E)$ if and only if

$$w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4$$

has a solution $u, v, w \in K$ not all zero.

Proof. We handle special cases first. If b_1 is a square or b_2 is a square, then both conditions are satisfied. So, assume that they are not squares. Then $b_1(K^\times) \in \mathrm{Im}(\alpha_E)$ if and only if there exists $(x, y) \in E(K)$ such that $x = b_1 t^2$ for some $t \in K^\times$. Substituting, we get

$$\begin{aligned} y^2 &= b_1 t^2((b_1 t^2)^2 + a b_1 t^2 + b) \\ \implies \left(\frac{y}{b_1 t}\right)^2 &= b_1 t^4 + a t^2 + b_2, \end{aligned}$$

and the equation in the statement of the lemma has solution

$$u = t,\ v = 1,\ w = \frac{y}{b_1 t}.$$

Conversely, if (u, v, w) is a solution to that equation, then $uv \neq 0$ and

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

□

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

Example. Take

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

so that in the notation of this section we have $a = 0$ and $b = -1$. Then

$$\mathrm{Im}(\alpha_E) = \langle -1 \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

To calculate the rank of E, we need to consider also

$$E' : y^2 = x^3 + 4x.$$

Now

$$\mathrm{Im}(\alpha_{E'}) \subset \langle -1, 2 \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

To determine the exact image, we need to check the solvability of the equations

$$\begin{aligned} w^2 &= -u^4 - 4v^4, \\ w^2 &= 2u^4 + 2v^4, \\ w^2 &= -2u^4 - 2v^4. \end{aligned}$$

Of these, the first and last have no solution over $\mathbb{R}$, so certainly not over $\mathbb{Q}$. The second has rational solution $(u, v, w) = (1, 1, 2)$. So

$$\mathrm{Im}(\alpha_{E'}) = \langle 2 \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

Now

$$2^r = \frac{2 \cdot 2}{4},$$

so rank $E(\mathbb{Q}) = 0$ and 1 is not a congruent number.

Example. Consider now the curves of the form

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

where p is a prime and $p \equiv 5 \pmod 8$. For $b_1 = -1$, the resulting equation

$$w^2 = -u^4 - pv^4$$

has no real solutions, so

$$\mathrm{Im}(\alpha_E) = \langle p \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

The 2-isogenous curve E' is given by

$$E' : y^2 = x^3 - 4px$$

with

$$\mathrm{Im}(\alpha_{E'}) \subset \langle -1, 2, p \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

Note that

$$\alpha_{E'}(T') = (-4p)(\mathbb{Q}^\times)^2 = (-p)(\mathbb{Q}^\times)^2.$$

We only need to check three more values of b_1; we use the b_1-values and corresponding equations

$$\begin{aligned} b_1 = 2 &: w^2 = 2u^4 - 2pv^2, \\ b_1 = -2 &: w^2 = -2u^4 + 2pv^4, \\ b_1 = p &: w^2 = pu^4 - 4v^4. \end{aligned}$$

Equations 1 and 2 are not solvable since $\left(\frac{2}{p}\right) = \left(\frac{-2}{p}\right) = -1$: indeed, if equation 2 had a solution $u, v, w \in \mathbb{Q}_p$ not all zero and WLOG $u, v \in \mathbb{Z}_p$ coprime, then if $p \mid u$ then $p \mid w, v$, a contradiction. Therefore

$$w^2 \equiv -2u^4 \not\equiv 0 \pmod{p},$$

which shows -2 is a square mod p. This contradicts $p \equiv 5 \pmod 8$.

We conclude that

$$\text{rank } E(\mathbb{Q}) = \begin{cases} 0, & \text{if equation 3 is not solvable over } \mathbb{Q} \\ 1, & \text{if equation 3 is solvable over } \mathbb{Q}. \end{cases}$$

Equation 3 *is* solvable in $\mathbb{Q}_p$, since -1 is a square $\pmod p$ and hence a square in $\mathbb{Z}_p$ by Hensel's lemma. It's also solvable over $\mathbb{Q}_2$: indeed, since $p - 4 \equiv 1 \pmod 8$, Hensel's lemma says $p - 4 \in (\mathbb{Z}_2^\times)^2$. Finally, it's solvable over $\mathbb{R}$ since $\sqrt{p} \in \mathbb{R}$. So by the fact below, there's no local obstruction to the existence of a $\mathbb{Q}$-point of infinite order on the curve. Specializing p, we see that for small values, equation 3 is known to have a rational solution:

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

Conjecturally rank $E(\mathbb{Q}) = 1$ for all primes $p \equiv 5 \pmod 8$. There is evidence for this conjecture: Selmer noticed that actual ranks tend to be off from upper bounds by an even amount, so since our best upper bound is 1 we expect the rank to really be 1. Cassels proved Selmer's observation conditional on the finiteness of the Tate-Shafarevich group.

Before doing another example, we discuss the concept of descent by 2-isogeny in the language of the Selmer and Tate-Shafarevich groups. For the curve

$$E : y^2 = x(x^2 + ax + b)$$

and its 2-isogenous curve E' with coefficients a', b' and 2-isogeny $\phi : E \to E'$, we get an exact sequence

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

To calculate $\mathrm{Im}(\alpha_E)$, we are interested in finding solutions to the equations

$$\begin{aligned} w^2 &= b_1u^4 + au^2v^2 + b_2v^4 \quad (*) \\ w^2 &= b_1u^4 + a'u^2v^2 + b_2v^4 \quad (*)', \end{aligned}$$

where in equation $(*)$ we have $b_2 = b/b_1$ and in equation $(*)'$ we have $b_2 = b'/b_1$.

We know that

$$\mathrm{Im}(\alpha_E) = \{b_1(\mathbb{Q}^\times)^2 : (*)' \text{ is solvable over } \mathbb{Q}\}$$

sits inside

$$S^{(\phi)}(E/\mathbb{Q}) = \{b_1(\mathbb{Q}^\times)^2 : (*)' \text{ is solvable over all completions of } \mathbb{Q}\},$$

and often $S^{(\phi)}(E/\mathbb{Q})$ will be easier to calculate. The hope, then, is that the inclusion $\mathrm{Im}(\alpha_E) \subset S^{(\phi)}(E/\mathbb{Q})$ is an equality, showing that the upper bound on the rank given by the Selmer group is really the exact rank.

The following fact is useful for calculating the Selmer group.

Fact (Uses ES3 Q9 and Hensel's Lemma)**.** If $a, b_1, b_2 \in \mathbb{Z}$ and $p \nmid 2b(a^2 - 4b)$ then $(*)$ is solvable over $\mathbb{Q}_p$.

Now we'll see an example where the inclusion $\mathrm{Im}(\alpha_E) \subset S^{(\phi)}(E/\mathbb{Q})$ is strict.

Example (Lind)**.** Let $E/\mathbb{Q}$ be given by

$$E : y^2 = x^3 + 17x.$$

Then

$$\mathrm{Im}(\alpha_E) = \langle 17 \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

Now the 2-isogenous curve is given by

$$E' : y^2 = x^3 - 68x.$$

For $b_1 = 2$ we get an equation of the form

$$w^2 = 2u^4 - 34v^4,$$

which upon replacing w by $2w$ and dividing by 2 becomes

$$C : 2w^2 = u^4 - 17v^4.$$

We think of C as defining a curve, and write

$$C(K) = \{(u, v, w) \in K^3 \setminus \{0\} \text{ satisfying the equation for } C\}/\sim,$$

where $(u, v, w) \sim (\lambda u, \lambda v, \lambda^2 w)$ for all $\lambda \in K^\times$.

Now $C(\mathbb{Q}_2) \neq \emptyset$, since $17 \in (\mathbb{Q}_2^\times)^4$. Also $C(\mathbb{Q}_{17}) \neq \emptyset$, since $2 \in (\mathbb{Q}_{17}^\times)^2$, and $C(\mathbb{R}) \neq \emptyset$. Then by the fact above, we know $C(\mathbb{Q}_v) \neq \emptyset$ for all places v of $\mathbb{Q}$. However, the set $C(\mathbb{Q})$ is empty! We show this now.

Suppose $(u, v, w) \in C(\mathbb{Q})$ with WLOG $u, v, q \in \mathbb{Z}$ and $(u, v) = 1$ and $w > 0$. If $17 \mid w$ then $17 \mid u$, and then $17 \mid v$, contradicting coprimality. Now if $p \mid w$ is an odd prime, we know $p \neq 17$, and 17 is a square mod p. By quadratic reciprocity, we have

$$\left(\frac{p}{17}\right) = \left(\frac{17}{p}\right) = 1,$$

and note $\left(\frac{2}{17}\right) = 1$. Therefore $\left(\frac{w}{17}\right) = 1$. But reducing the equation for C mod 17 gives

$$\begin{aligned} 2w^2 &\equiv u^4 \pmod{17} \\ \implies 2 &\in (\mathbb{F}_{17}^{\times})^4 = \{\pm 1, \pm 4\}, \end{aligned}$$

a contradiction. We conclude that $C(\mathbb{Q}) = \emptyset$, so C is a "counterexample to the Hasse principle" (that global solutions come from local ones). It represents a nontrivial element of $Ш(E/\mathbb{Q})$.

17 The Birch and Swinnerton-Dyer Conjecture

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

Definition 17.1. The *L-function of* E is defined by the Euler product

$$L(E,s) = \prod_p L_p(E,s),$$

where

$$L_p(E,s) = \begin{cases} (1 - a_p p^{-s} + p^{1-2s})^{-1}, & \text{if } E \text{ has good reduction at } p \\ (1 \pm p^{-s})^{-1}, & \text{if } E \text{ has multiplicative reduction at } p \\ 1, & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

Here a_p is the trace of Frobenius at p.

By Hasse's theorem we have $|a_p| \leq 2\sqrt{p}$, which is enough to guarantee that $L(E,s)$ converges for $\mathrm{Re}(s) > 3/2$. BSD is concerned with the behavior of $L(E,s)$ near 1. At the time the conjecture was made, it was not known whether $L(E,s)$ had an analytic continuation; now we do, as a consequence of

Theorem 17.1 (Wiles, Breuil, Conrad, Diamond, Taylor)**.** $L(E,s)$ is the L-function of a weight 2 modular form, and hence has an analytic continuation to $\mathbb{C}$ and a functional equation relating $L(E,s)$ to $L(E,2-s)$.

We can now state two forms of the BSD conjecture.

Conjecture 17.1 (Weak BSD)**.** $\mathrm{ord}_{s=1} L(E,s) = \mathrm{rank}\ E(\mathbb{Q})$. The order of vanishing $\mathrm{ord}_{s=1} L(E,s)$ is known as the *analytic rank*, so one can state the conjecture as "analytic rank = algebraic rank."

Conjecture 17.2 (Strong BSD)**.**

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

Here,

- c_p is the Tamagawa number of $E/\mathbb{Q}_p$, i.e. $[E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$.

- Reg $E(\mathbb{Q}) = \det([P_i, P_j])_{i,j=1,\ldots,r}$, where $\{P_1, \ldots, P_r\}$ is a basis for the free part of $E(\mathbb{Q})$, and

$$[P, Q] = \hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q)$$

  is the bilinear form associated to the quadratic from $\hat{h}$.

- $\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{2y+a_1x+a_3}$ is the integral of an invariant differential for E over $E(\mathbb{R})$. Here the a_i's come from a global minimal Weierstrass equation for $E/\mathbb{Q}$.

Theorem 17.2 (Kolyvagin)**.** If $\mathrm{ord}_{s=1}L(E, s)$ is 0 or 1, then weak BSD holds for E, and $Ш(E/\mathbb{Q})$ is finite.