Elliptic Curves and the Mordell-Weil Theorem

Jake Marcinek

September 26, 2013

Abstract

This paper introduces the notion of elliptic curves with an emphasis on elliptic curves defined over $\mathbb{Q}$ and their rational points. Some algebraic number theory and algebraic geometry is developed in order to prove the Mordell-Weil Theorem.

Contents

1 Introduction

1.1 Goals of this paper

In Section 1, we will introduce a specific kind of plane curve called an ellilptic curve. We define an addition on the points of such a curve making the set of points in a field into an abelian group. A brief background in algebraic geometry is provided in Section 2 to justify and motivate the definitions of elliptic curves and their group structure. The group structure of the elliptic curve varies greatly depending on the field from which the coordinates of the points are taken. The $\mathbb{R}$-points on an elliptic curve are not discussed in this paper but it is easy to see that they form a group isomorphic to the circle group, S^1, or two copies of the circle group, $S^1 \times \mathbb{Z}/2\mathbb{Z}$, depending on how many times the curve intersects the x-axis. The $\mathbb{C}$-points on an elliptic curve are discussed in Chapter 4. They form a group topologically isomorphic to a torus (see Theorem 4.12). Elliptic curves over finite fields are obviously finite groups (as the projective plane over a finite field has finitely many points) and are used in Sections 5 and 6 to simplify computations and proofs of results for elliptic curves over $\mathbb{Q}$. In Section 6, we conclude with the focus of this paper, the $\mathbb{Q}$-points on elliptic curves. The group structure of the rational points is more subtle than that of points over $\mathbb{R}$, $\mathbb{C}$, or finite fields. Our goal will be to explain the structure theory of this group. The discussion will culminate with

Main Theorem (Mordell-Weil)**.** *The group of $\mathbb{Q}$-points on an elliptic curve defined over $\mathbb{Q}$ is finitely generated.*

This generalizes to the K-points on an elliptic curve defined over K for any number field K. In order to prove this theorem, Section 3 develops some background in algebraic number theory and Section 5 discusses tools for simplifying computation on elliptic curves and aspects of Galois cohomology.

1.2 Introduction to elliptic curves

Fix a field K and an algebraic closure $\overline{K}$. An *elliptic curve* over $\overline{K}$ is a nonsingular curve over $\overline{K}$ of genus 1 with a specified base point. Using algebraic geometry, it can be shown that any such curve can be embedded in $\mathbb{P}^2(\overline{K})$ as the locus of a cubic equation with only one point, the base point, on the line at infinity. Thus any elliptic curve is the solution set of a corresponding *Weierstrass equation*

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

with base point $O = [0, 1, 0]$ and $a_i \in \overline{K}$. We often write the Weierstrass equation using non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$,

$$E : y^2 + a_1xy + a_3y^2 = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

keeping in mind the extra point at infinity, O. If each $a_i \in K$, then we say E *is defined over* K and denote this by E/K. For any field extension L/K, we let

$$E(L) = \{O\} \cup \{(x, y) \in L^2 | x, y \text{ satisfy the Weierstrass equation}\}.$$

Suppose E/K is an elliptic curve and $\mathrm{char}K \neq 2$, then through a change of variables, we may always simplify the Weierstrass equation to the form

$$E : y^2 = f(x) = 4x^3 + b_2x^2 + 2b^4x + b_6. \tag{2}$$

Here we define two fundamental constants associated to such an elliptic curve and Weierstrass equation

Definition 1.1. The *discriminant* of the Weierstrass equation, Δ, and the *j-invariant* of the elliptic curve, j, are given by

$$\Delta = \Delta(E) = 16\mathrm{Disc}(f) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \tag{3}$$

$$j = j(E) = \frac{b_2^2 - 24b_4}{\Delta}. \tag{4}$$

If we further assume $\mathrm{char}K \neq 2, 3$, then the Weierstrass equation may be further simplified to the form

$$E : y^2 = f(x) = x^3 + Ax + B. \tag{5}$$

With a Weierstrass equation of this form, it is easy to check that

$$\Delta = -16(4A^3 + 27B^2) \quad \text{and} \quad j = -1728\frac{(4A)^3}{\Delta}. \tag{6}$$

Proposition 1.2. *Let E and E' be two elliptic curves defined over $\overline{K}$.*

(a) Say E/K is defined over K and is given by the Weierstrass equation in Equation (2). Then

(i) E is nonsingular if and only if $\Delta = 0$,

(ii) E has a node if and only if $\Delta = 0, b_2^2 - 24b_4 \neq 0$,

(iii) E has a cusp if and only if $\Delta = 0, b_2^2 - 24b_4 = 0$. [1]

(b) The two elliptic curves E and E' are isomorphic if and only if $j(E) = j(E')$.

(c) Take any $j_0 \in \overline{K}$. Then there is an elliptic curve $E''/K(j_0)$ with

$$j(E'') = j_0.$$

For a proof, see Chapter 3 of [Si09].

To conclude the introduction, we describe the group law on elliptic curves. Suppose E/K is an elliptic curve, L/K is any field extension, and $P, Q \in E(L)$. Let l be the unique line through P and Q.[2] By the cubic nature of the elliptic curve, counting points with multiplicity, l intersects E at a unique third point, $R \in \mathbb{P}^2(L)$. Let v_R be the unique line through R and O and set $P + Q$ to be the third intersection point of $E(L)$ and v_R.

This construction in fact gives an abelian group structure to $E(L)$. It is clear that $O + P = P + O = P$ for any $P \in E(L)$ so O is the identity. For inverses, it is easy to see that for any $P \in E(L)$, $v_P \cap E(L) = \{O, P, -P\}$. Commutativity is also obvious. The only axiom that is nontrivial to check is associativity which can be shown via heavy yet direct computation. Rather than working through this computation, we give another proof in Section 2 (Proposition 2.16).

[1] Note that for a Weierstrass equation in equation (5), we have $b_2^2 - 24b_4 = 0$ if and only if $A = 0$.

[2] It is worth bringing up two points here. First, O lies on a line if and only if that line is vertical or the line at infinity. Second, if $P = Q$, then let l be the tangent line to E at P (with the tangent line at O being the line at infinity).

2 Some Algebraic Geometry

In order to discuss curves, one needs the language of algebraic geometry. Let K be some field with algebraic closure $\overline{K}$. We say C is a curve when C is a one dimensional projective variety in $\mathbb{P}^n(\overline{K})$. Let $K[X] = K[X_1, \ldots, X_n]$ be the *polynomial ring* in n variables with field of fractions $K(X)$ of *rational functions* (analogously for $\overline{K}$). Let

$$I(C/K) = \{f \in K[X] | f(P) = 0, \forall P \in C\} \subset K[X].$$

We say C is a curve defined over K and denote this by C/K when $I(C)$ has a generating set in $K[X]$. Next let

$$K[C] = \frac{K[X]}{I(C/K)}$$

be the *coordinate ring of* C, whose field of fractions is called the *function field of* C and is denoted $K(C)$. Let $M_P \subset \overline{K}[C]$ be the maximal ideal of functions vanishing at P and $\overline{K}[C]_P$ the localization at M_P. A generator of M_P is called a *uniformizer at* P and $f \in \overline{K}(C)$ is called *regular at* P if $f \in \overline{K}[C]_P$. If

$$\dim_{\overline{K}} M_P/M_P^2 = 1,$$

then we say C is nonsingular (or smooth) at P.

Proposition 2.1. *Let $P \in C$ be a nonsingular point. Then $\overline{K}[C]_P$ is a discrete valuation ring. The valuation is given by*

$$\mathrm{ord}_P : \overline{K}[C]_P \to \mathbb{N} \cup \{\infty\}, \qquad \mathrm{ord}_P(f) = \sup\{d \in \mathbb{Z} | f \in M_P^d\}.$$

Proof. We know $\dim_{\overline{K}} M_P/M_P^2 = 1$ so the result comes from Lemma 3.4. □

2.1 Some notes on $\mathrm{Div}(C)$ and $\mathrm{Pic}(C)$

Fix a perfect field K with algebraic closure $\overline{K}$ and absolute Galois group $G = G(\overline{K}/K)$. Let C/K be a smooth curve. Note that G acts on the points of C by the natural action on each coordinate.

Definition 2.2. A *divisor on* C is a finite formal sum

$$D = \sum_{P \in C} n_P(P), n_P \in \mathbb{Z}$$

of $\overline{K}$-points on C. The *degree* of a divisor D is

$$\deg(D) = \sum_{P \in C} n_P.$$

The *divisor group of* C is the free abelian group generated by the $\overline{K}$-points on C and is denoted $\mathrm{Div}(C)$. The set of degree 0 divisors forms a subgroup and is denoted $\mathrm{Div}^0(C)$.

There is a natural action of G on $\mathrm{Div}(C)$ by

$$\sigma\left(\sum_{P \in C} n_P(P)\right) = \sum_{P \in C} n_P(\sigma P).$$

The divisors fixed by G form a subgroup which is denoted $\mathrm{Div}_K(C)$ and has a subgroup of degree 0 divisors $\mathrm{Div}_K^0(C)$.

Any $f \in \overline{K}(C)^\times$ has an associated divisor

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

Two divisors $D_1, D_2 \in \mathrm{Div}(C)$ are said to be *linearly equivalent* if

$$D_1 - D_2 = \mathrm{div}(f)$$

for some $f \in \overline{K}(C)^\times$ and we write and we write $D_1 \sim D_2$. The *Picard group*,

$$\mathrm{Pic}(C) = \mathrm{Div}(C)/\sim$$

is the group of equivalence classes.

Proposition 2.3. *Let C be a smooth curve and let $f \in \overline{K}(C)^\times$. Then*

(a) $\mathrm{div}(f) = 0$ *if and only if* $f \in \overline{K}^\times$.

(b) $\deg \mathrm{div} f = 0$.

Proof. For (a), if $\mathrm{div}(f) = 0$, then f is constant (see Proposition 4.3 for the idea). The converse is clear. For (b), see [Si09, II, Prop. 3.1, p. 28] or [Ha77, II, Prop. 6.4, p. 132]. □

Theorem 2.4. *The following sequence is exact*

$$1 \to \overline{K}^\times \to \overline{K}(C)^\times \xrightarrow{\mathrm{div}} \mathrm{Div}^0(C) \to \mathrm{Pic}^0(C) \to 0.$$

Proof. This follows from the definitions and the above proposition. □

Definition 2.5. Let C be a curve. The space of (meromorphic) differential forms on C, denoted by Ω_C, is the $\overline{K}$-vector space generated by the symbols of the form dx for $x \in \overline{K}(C)$, modulo the following relations:

1. $d(x+y) = dx + dy$ for all $x, y \in \overline{K}(C)$.
2. $d(xy) = xdy + ydx$ for all $x, y \in \overline{K}(C)$.
3. $da = 0$ for all $a \in \overline{K}$.

Remark 2.6. Given a nonconstant map of curves $\phi : C_1 \to C_2$, we get an associated function field map given by

$$\begin{aligned} \phi\colon \overline{K}[C_2] &\to \overline{K}[C_1] \\ [f] &\mapsto [f \circ \phi] \end{aligned}$$

which induces the map on differentials

$$\begin{aligned} \phi^*\colon \Omega_{C_2} &\to \Omega_{C_1} \\ \sum f_i dx_i &\mapsto \sum (\phi f_i) d(\phi x_i). \end{aligned}$$

Proposition 2.7. *Let C be a curve, $P \in C$, $t \in \overline{K}(C)$ a uniformizer at P. Then*

(a) For any differential $\omega \in \Omega_C$, there is a unique $g \in \overline{K}(C)$ satisfying $\omega = gdt$. We denote g by ω/dt.

(b) Let $f \in \overline{K}(C)$ be regular at P. Then $\frac{df}{dt}$ is regular at P.

(c) Let $0 \neq \omega \in \Omega_C$. Then

$$\mathrm{ord}_P(\omega) := \mathrm{ord}_P(\omega/dt)$$

depends only on ω and P (independent of t).

(d) $x, f \in \overline{K}(C)$ with $x(P) = 0$, $p = \mathrm{char}K$. Then

$$\begin{aligned} &\mathrm{ord}_P(fdx) = \mathrm{ord}_P(f) + \mathrm{ord}_P(x) - 1 && \text{if } p = 0 \text{ or } p \nmid \mathrm{ord}_P(x) \\ &\mathrm{ord}_P(fdx) \geq \mathrm{ord}_P(f) + \mathrm{ord}_P(x) && \text{if } p > 0 \text{ and } p \mid \mathrm{ord}_P(x). \end{aligned}$$

(e) Let $0 \neq \omega \in \Omega_C$. *Then* $\mathrm{ord}_P(\omega) = 0$ *for all but finitely many* $P \in C$.

As with divisors associated to functions, there is an analogous definition for divisors associated to differentials.

Definition 2.8. Suppose $\omega \in \Omega_C$, then $\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega)$.

Proposition 2.9. *(a)* Ω_C *is a 1-dimensional* $\overline{K}(C)$*-vector space*

(b) Let $x \in \overline{K}(C)$. *Then* dx *is a* $\overline{K}(C)$ *basis for* Ω_C *if and only if* $\overline{K}(C)/\overline{K}(x)$ *is a finite separable extension.*

(c) Let $\phi : C_1 \to C_2$ *nonconstant, then* ϕ *is separable if and only if* $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ *is injective.*

Remark 2.10. For all nonzero $\omega_1, \omega_2 \in \Omega_C$, there is some $f \in \overline{K}(C)^\times$ such that $\omega_1 = f\omega_2$. Thus $\mathrm{div}(\omega_1) = \mathrm{div}(f) + \mathrm{div}(\omega_2)$.

This shows the following definition makes sense.

Definition 2.11. For any nonzero differential $\omega \in \Omega_C$, $\mathrm{div}(\omega)$ is called a *canonical divisor* and its image in $\mathrm{Pic}(C)$ is called the *canonical divisor class on* C.

Example 2.12. There are no holomorphic differentials on $\mathbb{P}^1(\overline{K})$. Let t be a coordinate function on $\mathbb{P}^1$. Then $t - a$ is a uniformizer at a for all $a \in \overline{K}$ and $1/t$ is a uniformizer at ∞. Thus $\mathrm{ord}_a(dt) = \mathrm{ord}_a(d(t-a)) = 0$. However, $\mathrm{ord}_\infty(dt) = \mathrm{ord}_\infty(-t^2 d(1/t)) = -2$. Therefore $\mathrm{div}(t) = -2(\infty)$. Then for any $\omega \in \Omega_C$, there is some $f \in \overline{K}(C)$ such that $\omega = f dt$. Thus $\deg \mathrm{div}\omega = \deg \mathrm{div} f + \deg \mathrm{div} dt = -2$.

Definition 2.13. Suppose

$$D = \sum_{P \in C} n_P(P), D' = \sum_{P \in C} n'_P(P) \in \mathrm{Div}(C).$$

Then we write $D \geq D'$ if $n_P \geq n'_P$ for all $P \in C$. Given some divisor $D \in \mathrm{Div}(C)$, we associate to D the set of functions

$$\mathcal{L}(D) = \{f \in \overline{K}(C)^\times | \mathrm{div}(f) \geq -D\} \cup \{0\}$$

which is clearly a $\overline{K}$-vector space whose dimension is denoted by

$$l(D) = \dim_{\overline{K}} \mathcal{L}(D).$$

Theorem 2.14 (Riemann-Roch)**.** *Let C be a smooth curve and K_C a canonical divisor on C. There is an integer $g \geq 0$, called the genus of C, such that for every divisor $D \in \mathrm{Div}(C)$,*

$$l(D) - l(K_C - D) = \deg D - g + 1.$$

Proof. See [Ha77, IV, Thm. 1.3, p. 295]. □

2.2 Application to elliptic curves

Lemma 2.15. *Let C be a curve of genus one and let $P, Q \in C$. Then $(P) \sim (Q)$ if and only if $P = Q$.*

Proof. Suppose $(P) \sim (Q)$. Then there exists $f \in \overline{K}(C)$ such that

$$\mathrm{div}(f) = (P) - (Q).$$

Then $f \in \mathcal{L}((Q))$ which has dimension 1 as a $\overline{K}$-vector space by the Riemann-Roch theorem. However, $\mathcal{L}((Q))$ clearly contains the constant functions so $f \in \overline{K}$ and $P = Q$. □

Proposition 2.16. *Let E/K be an elliptic curve.*

(a) For every degree 0 divisor $D \in \mathrm{Div}^0(E)$ there exists a unique point $P \in E$ satisfying $D \sim (P) - (O)$. Define

$$\psi : \mathrm{Div}^0(E) \to E$$

to be the map sending D to its associated P.

(b) ψ is surjective.

(c) Let $D_1, D_2 \in \mathrm{Div}^0(E)$. Then $\psi(D_1) = \psi(D_2)$ if and only if $D_1 \sim D_2$, i.e.

$$\psi : \mathrm{Pic}^0(E) \xrightarrow{\sim} E$$

is a bijection of sets.

(d) The inverse of ψ is

$$\kappa : E \xrightarrow{\sim} \mathrm{Pic}^0(E), \quad P \mapsto (P) - (O).$$

(e) *The group law induced on E via ψ is the addition law described earlier. In particular, the addition law on elliptic curves is associative.*

Proof. (a) E has genus 1 so $l(D + (O)) = 1$ by Riemann-Roch. Take a nonzero function $f \in \mathcal{L}(D + (O))$ as the basis element. Since $\operatorname{div}(f) \geq -D - (O)$ and $\deg \operatorname{div}(f) = 0$, we must have $\operatorname{div}(f) = D - (O) + (P)$ for some $P \in E$. Therefore, $D \sim (P) - (O)$. To show uniqueness, suppose $D \sim (P) - (O) \sim (P') - (O)$. Then $(P) \sim D + (O) \sim (P')$ so $P = P'$ by Lemma 2.15.

(b) Suppose $P \in E$. Then $\psi((P) - (O)) = P$.

(c) Suppose $D_1, D_2 \in \operatorname{Div}^0(E)$ and set $P_i = \psi(D_i)$. Then $(P_1) - (P_2) \sim D_1 - D_2$. Thus, if $P_1 = P_2$, then $D_1 \sim D_2$. Conversely, if $D_1 \sim D_2$, then $P_1 \sim P_2$ so $P_1 = P_2$ by Lemma 2.15.

(d) This is clear.

(e) It suffices to show $\kappa(P + Q) = \kappa(P) + \kappa(Q)$ for all $P, Q \in E$. Let

$$L : f(X, Y, Z) = \alpha X + \beta Y + \gamma Z = 0$$

be the line in $\mathbb{P}^2(\overline{K})$ passing through P and Q. Let R be the unique third point of intersection between L and E and let

$$L' : f'(X, Y, Z) = \alpha' X + \beta' Y + \gamma' Z = 0$$

be the line in $\mathbb{P}^2(\overline{K})$ passing through R and O. Note that L' also passes through $P + Q$ by the definition of addition. Then

$$\operatorname{div}(f/Z) = (P) + (Q) + (R) - 3(O)$$
$$\operatorname{div}(f'/Z) = (R) + (O) + (P + Q) - 3(O).$$

Subtracting the two equation gives

$$(P + Q) - (P) - (Q) + (O) = \operatorname{div}(f'/Z) - \operatorname{div}(f/Z) = \operatorname{div}(f'/f) \sim 0$$

so $\kappa(P + Q) - \kappa(P) - \kappa(Q) = 0$.

□

Remark 2.17. Through the group isomorphism $\operatorname{Pic}^0(E) \xrightarrow{\psi} E$, we see the correspondence $\operatorname{Pic}^0_K(E) \cong E(K)$. This is because for $P \in E$, $P \in E(K)$ if and only if P is fixed by G if and only if the divisor $(P) - (O)$ is fixed by G.

3 Some Algebraic Number Theory

Definition 3.1. A ring R is called a *discrete valuation ring* if it is a principal ideal domain with a unique nonzero prime ideal, $\mathfrak{m}$. The *residue field* of R is $k = R/\mathfrak{m}$.

Definition 3.2. An integral domain A is a *Dedekind domain* if A satisfies either of the equivalent conditions

1. A is Noetherian, integrally closed, and has Krull dimension 1.
2. A is Noetherian and the localization $A_\mathfrak{p}$ is a discrete valuation ring for all primes $\mathfrak{p}$.

Let K be the field of fractions of A. A *fractional ideal of* K, I, is a finitely generated sub-A-module of K.

Definition 3.3. A *number field*, K, is a finite field extension of $\mathbb{Q}$. The *ring of integers of* K is

$$\mathcal{O}_K = \{x \in K | f(x) = 0 \,\text{for some monic}\, f \in \mathbb{Z}[X]\}.$$

Here we state a few preliminary results. See [Se79] and [Mi13] for more on discrete valuation rings, Dedekind domains, and number fields.

Lemma 3.4. *Let R be a Noetherian local domain that is not a field, let $\mathfrak{m}$ be its maximal ideal, and let $k = R/\mathfrak{m}$ be its residue field. The following are equivalent:*

(i) *R is a discrete valuation ring.*

(ii) *$\mathfrak{m}$ is principal.*

(iii) $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$.

Theorem 3.5. *Let A be a Dedekind domain with field of fractions K. The set of nonzero fractional ideals, $Id(A)$, forms a group under multiplication. In fact, $Id(A)$ is free with the prime ideals as a generating set. In particular, Dedekind domains have unique factorization of ideals into primes.*

Note 3.6. Throughout this section, there are instances where general results are presented, but only special cases of these results will be used in our discussion of elliptic curves later. To shorten this background discussion, proofs will be given only for these special cases. In preparation for these special cases, we now give two definitions and two well-known result.

Definition 3.7. A number field K is called a *quadratic field* if $[K : \mathbb{Q}] = 2$.

Proposition 3.8. *If $[K : \mathbb{Q}] = n$, then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.*

Definition 3.9. A finite field extension $K/\mathbb{Q}$ is called *monogenic* if $\mathcal{O}_K = \mathbb{Z}[\omega]$ for some $\omega \in K$.

From this, it is clear that all quadratic fields are monogenic. A stronger classification is now given.

Proposition 3.10. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field.*[3] *By multiplying by elements of $\mathbb{Q}^{\times 2}$, we may assume $d \in \mathbb{Z}$ is square free, $d \neq 0, 1$. Then $\mathcal{O}_K = \mathbb{Z}[\omega]$ where*

$$\omega = \begin{cases} \sqrt{d} & \text{if } d \not\equiv 1 \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \end{cases} \pmod 4.$$

The minimal polynomial of ω is

$$f(X) = \begin{cases} X^2 - d & \text{if } d \not\equiv 1 \\ X^2 - X + \frac{1-d}{4} & \text{if } d \equiv 1 \end{cases} \pmod 4.$$

In particular,

$$\mathrm{Disc}(K) = \mathrm{Disc}(f) = \begin{cases} 4d & \text{if } d \not\equiv 1 \\ d & \text{if } d \equiv 1 \end{cases} \pmod 4.$$

Now we return to the general theory with the following proposition.

Proposition 3.11. *Let K be a number field. Then $\mathcal{O}_K$ is a Dedekind domain.*

[3] Any quadratic field, K, is of the form $\mathbb{Q}(\sqrt{d}), d \in \mathbb{Q}$. This follows from Theorem 5.11 since $G(K/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$ is cyclic.

Definition 3.12. Let L/K be a degree n field extension of number fields and let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$. By Theorem 3.5,

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \dots \mathfrak{q}_g^{e_g}$$

uniquely for some $\mathfrak{q}_i \subset \mathcal{O}_L$ prime. The $\mathfrak{q}_i$ are said to *divide* $\mathfrak{p}$ or lay *above* $\mathfrak{p}$ and this is denoted by $\mathfrak{q}_i|\mathfrak{p}$. We say L/K is *unramified at* $\mathfrak{q}_i$ if $e_i = 1$ and say *unramified above* $\mathfrak{p}$ if $e_i = 1$ for all i. Otherwise, L/K is *ramified* above $\mathfrak{p}$. When $g = 1$ and $e_1 = n$, we say L/K is totally ramified at $\mathfrak{p}$.

By Definition 3.2, given a prime $\mathfrak{p}$ in a Dedekind domain A with field of fractions K, $A_\mathfrak{p}$ is a discrete valuation ring so we may make the following definition.

Definition 3.13. The *residue field of K with respect to* $\mathfrak{p}$ is the residue field of $A_\mathfrak{p}$. The *completion of K with respect to* $\mathfrak{p}$ is the field of fractions of the completion of $A_\mathfrak{p}$ with respect to the unique maximal ideal $\mathfrak{p}$ and is denoted $K_\mathfrak{p}$.

Proposition 3.14. *Let L/K be a finite Galois extension and $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal. Then $G(L/K)$ acts transitively on S, the set of primes $\mathfrak{q} \subset \mathcal{O}_L$ above $\mathfrak{p}$.*

Definition 3.15. Using the setup from Proposition 3.14, for $\mathfrak{q} \in S$, the *decomposition group of* $\mathfrak{q}$ is

$$D_\mathfrak{q}(L/K) = Stab(\mathfrak{q}) \leq G(L/K).$$

Proposition 3.16. *$D_\mathfrak{q}(L/K)$ is precisely the Galois group of the corresponding extension of completions. That is,*

$$G(L_\mathfrak{q}/K_\mathfrak{p}) = D_\mathfrak{q}(L/K).$$

Proposition 3.17. *With the same setup as above, let k (resp. l) be the residue field of K (resp. L) with respect to $\mathfrak{p}$ (resp. $\mathfrak{q}$). Via passage to the quotient, the map*

$$\varepsilon : D_\mathfrak{q}(L/K) \to G(l/k)$$

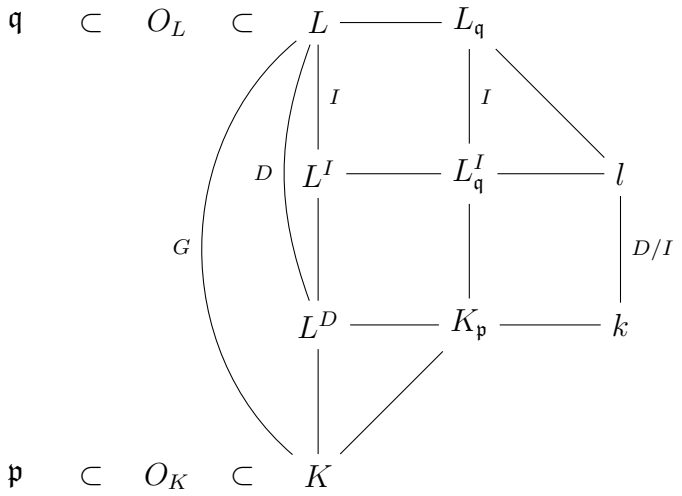
is a surjection.

Definition 3.18. The *inertia subgroup of* $\mathfrak{q}$ is

$$I_{\mathfrak{q}}(L/K) = \mathrm{Ker}(\varepsilon)$$

where ε is as in the previous proposition.

Theorem 3.19. *Using the previous setup, let* $G = G(L/K)$, $D = D_{\mathfrak{q}}(L/K)$, *and* $I = I_{\mathfrak{q}}(L/K)$. *We have the following picture.*



Here the columns are field extensions. The Galois group of an extension from the first row to the fourth row is G, *second to fourth is* D, *third to fourth is* I, *second to third is* D/I. *The third to fourth row extensions are totally ramified at* $\mathfrak{q}$ *and all extensions below the fourth row are unramified at* $\mathfrak{q}$.

Theorem 3.20. *Let* K *be a number field and* p *a rational prime. Then* $K/\mathbb{Q}$ *is ramified above* p *if and only if* $p|\mathrm{Disc}(K)$.

Proof. We prove the special case where $K/\mathbb{Q}$ is monogenic with $\mathcal{O}_K = \mathbb{Z}[\omega]$. Let $f \in \mathbb{Z}[X]$ be the minimal polynomial for ω and suppose p is a rational prime. Say $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$ is the decomposition into a product of primes. Let $\widetilde{f} \in \mathbb{F}_p[X]$ be the reduction of f modulo p. Since $\mathbb{F}_p$ is a field, $\mathbb{F}_p[X]$ is a PID. In particular, $\widetilde{f}$ factors uniquely into irreducibles as $\widetilde{f} = g_1^{b_1} \dots g_r^{b_r}$. With two applications of the Chinese Remainder Theorem, we can form the following sequence of isomorphisms

$$A := \frac{\mathcal{O}_K}{\mathfrak{p}_1^{e_1}} \times \dots \times \frac{\mathcal{O}_K}{\mathfrak{p}_g^{e_g}} \cong \frac{\mathcal{O}_K}{(p)} \cong \frac{\mathbb{Z}[X]}{(f,p)} \cong \frac{\mathbb{F}_p[X]}{(\widetilde{f})} \cong \frac{\mathbb{F}_p[X]}{(g_1)^{b_1}} \times \dots \times \frac{\mathbb{F}_p[X]}{(g_r)^{b_r}} := B.$$

Now $K/\mathbb{Q}$ is ramified above p if and only if some e_i is greater than 1 if and only if A contains a nilpotent element if and only if B contains a nilpotent element if and only if some b_i is greater than 1 if and only if $\widetilde{f}$ has a multiple root if and only if $\text{Disc}(\widetilde{f}) = 0$ if and only if $p|\text{Disc}(f) = \text{Disc}(K)$. □

Theorem 3.21 (Hermite's Theorem)**.** *Given $N \in \mathbb{Z}$ and a finite set of rational primes S, there are only finitely many extensions over $\mathbb{Q}$ of degree at most N that are unramified above all primes outside S.*

Proof. We prove the special case where $N = 2$. For a proof of the general theorem, see [La94]. From Kummer Theory, we know the number fields of degree at most 2 are in one-to-one correspondence with $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ (via $d \leftrightarrow \mathbb{Q}(\sqrt{d})$). From Proposition 3.10, $d \mid \text{Disc}(\mathbb{Q}(\sqrt{d}))$. From Proposition 3.20, if $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is unramified above p, then $p \nmid d$. Therefore, if $\mathbb{Q}(\sqrt{d})$ is unramified above all primes $p \notin S$, then $d = \pm\prod_{p\in S} p^{\alpha_p}$ of which there are only finitely many up to equivalence in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. □

We now prove another special case which will be used in our proof of the Mordell-Weil Theorem in Section 6.

Theorem 3.22. *Let K be a number field containing the m^{th} roots of unity, μ_m. Let $\mathcal{C}$ be the collection of cyclic extensions of K of degree dividing m that are unramified above all primes, $\mathfrak{p} \subset \mathcal{O}_K$, outside a finite set of primes, S. Then $\mathcal{C}$ is finite.*

For this proof, we use an important result of algebraic number theory, the finiteness of the ideal class group. For the purposes of this paper, we state this result as

Theorem 3.23. *There exists a finite set of ideals in $\mathcal{O}_K$, $I_1, \ldots, I_n$, such that for any ideal $I \in \mathcal{O}_K$, II_k is principal for some $1 \le k \le n$.*

We will also need

Definition 3.24. For $\mathfrak{p} \subset \mathcal{O}_K$ prime, let $v_\mathfrak{p}$ be the normalized valuation defined on $K_\mathfrak{p}$. Given a finite set of primes S in K, let the *S-units* be

$$K_S^\times = \{x \in K^\times | v_\mathfrak{p}(x) = 0, \mathfrak{p} \in S\}.$$

Theorem 3.25 (Dirichlet's S-unit Theorem)**.** *For S a finite set of primes in $\mathcal{O}_K$, $K_S^\times$ is finitely generated. In particular, for any $2 \le m \in \mathbb{Z}$, $K_S^\times/{K_S^\times}^m$ is finite. (If $K_S^\times$ is finitely generated, then $K_S^\times \cong T \times \mathbb{Z}^r$ for some finite group T and some $0 \le r \in \mathbb{Z}$. Then $K_S^\times/{K_S^\times}^m \cong T/mT \times (\mathbb{Z}/m\mathbb{Z})^r$ is finite.)*

For proofs of these two theorems, see [La94].

Proof of Theorem 3.22. Let $\mathcal{C}_m$ be the collection of cyclic extensions of K of degree dividing m and let $\mathcal{C}$ be the subcollection described in the theorem. Let

$$S' = S \cup \{\mathfrak{p} \subset \mathcal{O}_K \text{ prime} | \mathfrak{p} \text{ divides } I_k, \text{ for some } 1 \leq k \leq n\},$$

a finite set of primes containing S. First, we wish to show that if $L \in \mathcal{C}$, then $L = K(\sqrt[m]{a})$ for some $a \in K$ with $v_\mathfrak{p}(a) = 0$ for all primes $\mathfrak{p}$ outside S'. Fix $L \in \mathcal{C}$. Theorem 5.9 says,

$$\Phi : K^\times / {K^\times}^m \to \mathcal{C}_m, \qquad \text{by} \qquad a{K^\times}^m \mapsto K(\sqrt[m]{a})$$

is surjective so $L = K(\sqrt[m]{a})$ for some $a \in K$. Say $(a) = \prod_\mathfrak{p} \mathfrak{p}^{e_\mathfrak{p}}$ is the unique prime factorization in $\mathcal{O}_K$. If $\mathfrak{p} \notin S$, then $m | e_\mathfrak{p}$, say $e_\mathfrak{p} = m a_\mathfrak{p}$. Therefore,

$$(a) = (\prod_{\mathfrak{p} \in S} \mathfrak{p}^{e_\mathfrak{p}})(\prod_{\mathfrak{p} \notin S} \mathfrak{p}^{a_\mathfrak{p}})^m.$$

Let $I = \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{a_p}$. Then there is some $1 \leq k \leq n$ such that $I^{-1} I_k = (b)$ is principal. Then

$$(ab^m) = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{e_\mathfrak{p}} I^m I^{-m} I_k^m = \prod_{p \in S} \mathfrak{p}^{e_\mathfrak{p}} I_k^m$$

and $L = K(\sqrt[m]{a}) = K(\sqrt[m]{ab^m})$ as we were to show.

Under the Kummer theory correspondence, $\Phi : K^\times / {K^\times}^m \to \mathcal{C}_m$, we have shown that $\mathcal{C}$ is contained in the image of the composition

$$K_S^\times / {K_S^\times}^m \to K^\times / {K^\times}^m \xrightarrow{\Phi} \mathcal{C}_m$$

where the first map is the natural quotient. By Theorem 3.25, $K_S^\times / {K_S^\times}^m$ is finite so $\mathcal{C}$ is also finite. □

4 Elliptic curves over $\mathbb{C}$

Definition 4.1. A *lattice* $\Lambda = \langle \omega_1, \omega_2 \rangle \subset \mathbb{C}$ is a rank 2 free discrete subgroup of $\mathbb{C}$. A *fundamental parallelogram* for Λ is a set of the form

$$\Pi = \{\alpha + a\omega_1, b\omega_2 | 0 \leq a, b < 1\}$$

for some $\alpha \in \mathbb{C}$ and $\{\omega_1, \omega_2\}$ any generators for Λ. A meromorphic function, $f : \mathbb{C} \to \mathbb{C}$, is called an *elliptic function* relative to Λ if $f(z) = f(z + \lambda)$ for all $\lambda \in \Lambda$. Denote the set of elliptic functions relative to Λ by $\mathcal{E}_\Lambda$.

Note 4.2. The fundamental parallelogram is in natural bijection with $\mathbb{C}/\Lambda$ so I will sometimes abuse notation and identify the two. The elliptic functions can be thought of as the meromorphic functions f that factor through $\mathbb{C}/\Lambda$.

Proposition 4.3. *If $f \in \mathcal{E}_\Lambda$ has no pole, then f is constant.*

Proof. By the note above,

$$\begin{array}{ccc} \mathbb{C} & \twoheadrightarrow & \mathbb{C}/\Lambda \\ & \searrow^{f} & \downarrow{\scriptstyle f|_\Pi} \\ & & \mathbb{C} \end{array}$$

commutes. Since $\overline{\Pi}$ is compact, $f|_\Pi$ is bounded, so f is bounded. Then Liouville's theorem says f is constant. □

Proposition 4.4. *Suppose f has no poles on $\partial\Pi$. Then*

$$\sum_{w \in \Pi} \operatorname{res}_w(f) = 0.$$

Proof. By the residue theorem,

$$\sum_{w \in \Pi} \operatorname{res}_w(f) = \frac{1}{2\pi i} \int_{\partial\Pi} f dz.$$

However, f takes the same values on opposite edges of $\partial\Pi$ and these edges are traversed in reverse direction so the integral is 0. □

Note 4.5. Holomorphic functions only have finitely many poles in any bounded region so there is some α such that $\partial\Pi$ misses all poles.

Corollary 4.6. *All nonconstant elliptic functions have at least two poles (counted with multiplicity) in Π.*

Proof. Pick α so that $\partial\Pi$ misses all poles. If there is exactly one pole of multiplicity 1 at $w_0 \in \Pi$, then $\operatorname{res}_{w_0}(f) = \sum_{w \in \Pi} \operatorname{res}_w(f) = 0$ by Proposition 4.4 so f must have 0 poles in which case f is constant by 4.3. □

Corollary 4.7. *Let m_i (resp. n_j) be the orders of the poles (resp. zeros) of $f \in \Pi$. Then $\sum m_i = \sum n_j$.*

Proof. Let $P = \sum m_i, N = \sum n_j$. By the argument principle,

$$\int_{\partial \Pi} \frac{f'(z)}{f(z)} dz = 2\pi(N - P).$$

However, f is Λ-periodic so f' is Λ-periodic, and therefore so is f'/f and we have already shown that integrating an elliptic function over $\partial\Pi$ gives 0. $\square$

Definition 4.8. The Weierstrass $\wp$-function is given by

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

I refer the reader to Chapter 1 of [Ko84] for proofs of the following four propositions and main theorem.

Proposition 4.9. *The Weierstrass $\wp$-function, $\wp(z, \Lambda)$, converges absolutely and is uniformly convergent in any compact subset $K \subset \mathbb{C} \backslash \Lambda$.*

Proposition 4.10. *$\wp(z, \Lambda) \in \mathcal{E}_\Lambda$ and the poles of $\wp$ are precisely the double poles at each $\lambda \in \Lambda$.*

Proposition 4.11. *$\mathcal{E}_\Lambda = \mathbb{C}(\wp, \wp')$, i.e. $\mathcal{E}_\Lambda$ is generated as a field over $\mathbb{C}$ by $\wp$ and its derivative.*

Theorem 4.12. *Consider the elliptic curve $E : y^2 = 4x^3 - g_2 x - g_3$ where $g_2 = 60 \sum_{0 \neq \lambda \in \Lambda} \lambda^{-4}$ and $g_3 = 140 \sum_{0 \neq \lambda \in \Lambda} \lambda^{-6}$.*

$$\begin{aligned} \mathbb{C}/\Lambda &\to E(\mathbb{C}) \\ z &\mapsto (\wp(z, \Lambda), \wp'(z, \Lambda)) \end{aligned}$$

is a complex analytic isomorphism. Moreover, for any elliptic curve $E/\mathbb{C}$, there exists lattice Λ such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$.

This identification of any elliptic curve with the torus is very powerful and has many corollaries such as the following two.

Corollary 4.13. *Suppose $E/\mathbb{C}$ is an elliptic curve. Then the m-torsion subgroup $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.*

Proof. There exists lattice Λ such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$. Then

$$E[m] \cong (\mathbb{C}/\Lambda)[m] \cong \frac{\frac{1}{m}\Lambda}{\Lambda} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

□

Corollary 4.14. *The multiplication by m map on $E(\mathbb{C})$,*

$$E(\mathbb{C}) \xrightarrow{m} E(\mathbb{C}) \quad \text{by} \quad P \mapsto mP,$$

is surjective.

Proof. There exists lattice Λ such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$. The map $\mathbb{C}/\Lambda \xrightarrow{m} \mathbb{C}/\Lambda$ is clearly surjective (the kernel of the composition of surjections $\mathbb{C} \xrightarrow{m} \mathbb{C} \xrightarrow{\pi} \mathbb{C}/\Lambda$ is $\frac{1}{m}\Lambda \supset \Lambda$). □

Remark 4.15. For an elliptic curve E/K defined over an arbitrary field K, Corollary 4.13 holds when $\mathrm{char}K \nmid m$ (see [Wa08, III, Thm. 3.2, p. 79]) and Corollary 4.14 holds when K is algebraically closed (see [Si09, III, Prop. 4.2, p. 68]).

5 Preliminary constructions on elliptic curves

5.1 Weil Pairing

Let K be a number field and let E/K be an elliptic curve defined over K. By 4.13 $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank 2.[4] Thus $E[m]$ is equipped with a natural nondegenerate multilinear map, namely the determinant. Picking some basis $\{T_1, T_2\}$ for $E[m]$, the determinant pairing is given by

$$\begin{aligned} \det : E[m] \times E[m] &\to \mathbb{Z}/m\mathbb{Z} \\ (aT_1 + bT_2, cT_1 + dT_2) &\mapsto ad - bc \end{aligned}$$

However, this pairing is not necessarily Galois invariant. Our goal is to construct a pairing which is Galois invariant and we aim for this pairing to be of the form $\zeta^{\det(P,Q)}$ for some primitive m^{th} root of unity, ζ. For this construction, we will use the following result on divisors which follows directly from the isomorphism in Theorem 2.16.

[4] In general, by Remark 4.15, this isomorphism is valid for an elliptic curve over any field K of characteristic not dividing m.

Theorem 5.1. *A divisor $\sum_P n_P(P) \in Div(E)$ is principal if and only if*

$$\sum_P n_P = 0 \quad \text{and} \quad \sum_P n_P P = O.$$

To begin the construction, take $T \in E[m]$. By the theorem, there exists a function $f_T \in \overline{K}(E)$ such that

$$\text{div}(f_T) = m(T) - m(\infty).$$

Then take some $T' \in E$ such that $mT' = T$. Again, by the theorem above, there exists a function $g_T \in \overline{K}(E)$ such that

$$\text{div}(g_T) = \sum_{R \in E[m]} (T' + R) - (R)$$

since $m^2 T' = \infty$. It is easy to see that $\text{div}(f_T \circ m) = m\text{div}(g_T) = \text{div}(g_T^m)$. Therefore, $f_T \circ m = c g_T^m$ for some $c \in \overline{K}^\times$ (WLOG $c = 1$).

Next, let $S \in E[m]$. Then

$$g_T^m(X + S) = f_T(mX + mS) = f_T(mX) = g_T^m(X)$$

so $g_T(X + S)/g_T(X) \in \mu_m$ for all $X \in E$. In particular,

$$\begin{aligned} E &\to \mathbb{P}^1 \\ X &\mapsto g_T(X + S)/g_T(X) \end{aligned}$$

is not surjective, so it must be constant. Hence, we may define the pairing

$$\begin{aligned} \langle \cdot, \cdot \rangle_m : E[m] \times E[m] &\to \mu_m \\ (S, T) &\mapsto g_T(X + S)/g_T(X) \end{aligned}$$

where $X \in E$ is any point such that $g_T(X + S)$ and $g_T(X)$ and both defined and nonzero. This pairing is called the Weil pairing and satisfies the following properties.

Proposition 5.2. *The Weil pairing $\langle \cdot, \cdot \rangle_m$ is*

1. *bilinear. That is, $\langle S_1 + S_2, T \rangle_m = \langle S_1, T \rangle_m \langle S_2, T \rangle_m$ and $\langle S, T_1 + T_2 \rangle_m = \langle S, T_1 \rangle_m \langle S, T_2 \rangle_m$.*

2. *alternating. That is,* $\langle T, T\rangle_m = 1$ *for all* $T \in E[m]$*. In particular,*

$$\langle S, T\rangle_m = \langle T, S\rangle_m^{-1}.$$

3. *nondegenerate. That is,* $\langle S, T\rangle_m = 1$ *for all* $S \in E[m]$ *if and only if* $T = O$*.*

4. *Galois invariant. That is,* $\sigma\langle S, T\rangle_m = \langle \sigma S, \sigma T\rangle_m$ *for all* $S, T \in E[m], \sigma \in G(\overline{K}/K)$*.*

5. *compatible. That is,* $\langle S, T\rangle_{mm'} = \langle m'S, T\rangle_m$ *for all* $0 < m, m' \in \mathbb{Z}$ *and* $S \in E[mm'], T \in E[m]$

From this, we can prove the following corollary.

Corollary 5.3. *If* $E[m] \subset E(K)$*, then* $\mu_m \subset K$*.*

Proof. Suppose $E[m] \subset E(K)$. I claim there exist $S, T \in E[m]$ such that $\langle S, T\rangle_m = \zeta$, a primitive m^{th} root of unity. Say $\mathrm{Im}(\langle \cdot, \cdot\rangle_m) = \mu_d \leq \mu_m$. As $\langle \cdot, \cdot\rangle_m$ is bilinear, $1 = \langle S, T\rangle_m^d = \langle dS, T\rangle_m$ for all $S, T \in E[m]$. By the nondegeneracy of $\langle \cdot, \cdot\rangle_m$, $dS = O$ for all $S \in E[m]$. This means $E[m] \subseteq E[d]$ so we must have $d = m$. Therefore, $\langle S, T\rangle_m = \zeta$ for some $S, T \in E[m]$. By the Galois invariance of $\langle \cdot, \cdot\rangle_m$, we see that $\sigma\zeta = \sigma\langle S, T\rangle_m = \langle \sigma S, \sigma T\rangle_m = \langle S, T\rangle_m = \zeta$ for all $\sigma \in G(\overline{K}/K)$. This means $\zeta \in K$ so $\mu_m = \langle \zeta\rangle \subset K$. □

5.2 Reduction of elliptic curves

Let K be a local field, complete with respect to a discrete valuation v with ring of integers $R = \{x \in K | v(x) \geq 0\}$, maximal ideal $\mathfrak{m}$, uniformizer π, and residue field $k = R/\mathfrak{m}$ with characteristic p. We denote reduction modulo $\mathfrak{m}$ by a tilde.

Example 5.4. There is a natural reduction map

$$R \xrightarrow{\pi} \!\!\!\rightarrow R/\mathfrak{m}$$

given by $t \mapsto \widetilde{t}$. This extends to the map of polynomial rings

$$R[X] \xrightarrow{\pi} \!\!\!\rightarrow R/\mathfrak{m}[X]$$

given by $\sum a_i X^i \mapsto \sum \widetilde{a_i} X^i$.

Example 5.5. There is also a reduction of the projective plane

$$\mathbb{P}^2(K) \xrightarrow{\pi} \twoheadrightarrow \mathbb{P}^2(k)$$

which works as follows. Take some $[a, b, c] \in \mathbb{P}^2(K)$. By multiplying through by some element of R, we may "clear the denominators" and assume $a, b, c \in R$. Then by dividing through by an appropriate power of π, we may assume

$$\min\{v(a), v(b), v(c)\} = 0. \tag{7}$$

Then using the natural reduction of R from Example 5.4, $\widetilde{[a, b, c]} = [\widetilde{a}, \widetilde{b}, \widetilde{c}]$ is well-defined since the situation $\widetilde{a} = \widetilde{b} = \widetilde{c} = 0$ is impossible by Equation 7.

Let E/K be an elliptic curve over K. That is, E is the solution set to a Weierstrass equation $f(X, Y, Z) = 0$ with discriminant Δ.[5] Via the reduction of Example 5.4 $\widetilde{f}(X, Y, Z) = \widetilde{0}$ defines another curve $\widetilde{E}/k$ over k with discriminant $\widetilde{\Delta}$. Then $\widetilde{E}$ is an elliptic curve as long as $\widetilde{\Delta} \neq \widetilde{0}$ (as long as $\Delta \notin \mathfrak{m}$). In this case, there is a natural reduction map of elliptic curves $\rho : E/K \to \widetilde{E}/k$ given by the projective space reduction from Example 5.5.

Theorem 5.6. *Let m be a positive integer not divisible by p. When restricted to the m-torsion points, $\rho : E[m] \to \widetilde{E}[m]$ is an isomorphism.*

Proof. I prove the case where $p \neq m = 2$. This is the only case we will need to use below but a proof of the general statement can be found in [Wa08] or [Si09].

Suppose E/K is given by the Weierstrass equation $E : y^2 = f(x) = x^3 + Ax + B$ from Equation 5. After a suitable change of variables, we may assume $A, B \in R$. Let L be the splitting field of f over K with corresponding ring of integers, R', and say the roots of f are e_1, e_2, e_3. We will be concerned with the reduction from L to the residue field l, $\rho : E/L \to \widetilde{E}/l$. For $O \neq P \in E$, $2P = O$ if and only if the tangent line at P is vertical if and only if $P = (e_i, 0)$. Therefore,

$$E[2] = \{O, (e_1, 0), (e_2, 0), (e_3, 0)\}.$$

[5] By clearing denominators, there exists $d \in R$ such that $df \in R[X, Y, Z]$. Since f is homogeneous, f and df share the same zero set. Thus we may assume $f \in R[X, Y, Z]$.

Similarly, $\widetilde{f} = (x - \widetilde{e_1})(x - \widetilde{e_2})(x - \widetilde{e_3})$. Note that the e_i have well-defined reduction as described in Example 5.4 since we assume $A, B \in R \subseteq R'$ which means $e_i \in R'$ by Gauss' Lemma. Furthermore, the $\widetilde{e_i}$ are distinct since the discriminant of $\widetilde{f}$ is a multiple of $\widetilde{\Delta} \neq 0$. Therefore,

$$\widetilde{E}[2] = \{\widetilde{O}, (\widetilde{e_1}, \widetilde{0}), (\widetilde{e_2}, \widetilde{0}), (\widetilde{e_3}, \widetilde{0})\}$$

and $\rho : E[m] \to \widetilde{E}[m]$, by $\rho(O) = \widetilde{O}$ and $\rho((e_i, 0)) = (\widetilde{e_i}, \widetilde{0})$, is an isomorphism. □

5.3 Galois Cohomology and Kummer Theory

Before moving onto elliptic curves over $\mathbb{Q}$, we recall some results from Galois Cohomology and Kummer Theory.

Theorem 5.7 (Hilbert's Theorem 90)**.** *Consider a Galois extension L/K with corresponding Galois group G. Then $\mathrm{H}^1(G, L)$ and $\mathrm{H}^1(G, L^\times)$ are trivial.*

Example 5.8. Let K be a number field, $G = G(\overline{K}/K)$, and $0 < m \in \mathbb{Z}$ a positive integer. Start with the short exact sequence

$$0 \to \mu_m \to \overline{K}^\times \xrightarrow{\cdot^m} \overline{K}^\times \to 0$$

and use Galois cohomology to induce

$$0 \to \mu_m \to K^\times \xrightarrow{\cdot^m} K^\times \xrightarrow{\delta} \mathrm{H}^1(G, \mu_m) \to \mathrm{H}^1(G, \overline{K}^\times) = 0$$

the right end is trivial by Theorem 5.7. Therefore, $\mathrm{H}^1(G, \mu_m) \cong K^\times / {K^\times}^m$ with explicit isomorphism

$$\begin{aligned} K^\times / {K^\times}^m &\xrightarrow{\delta} \mathrm{H}^1(G, \mu_m) \\ a &\mapsto \left[\sigma \mapsto \frac{\sigma \sqrt[m]{a}}{\sqrt[m]{a}}\right] \end{aligned}$$

Now we turn our focus to certain cyclic extensions and prove the following classification.

Theorem 5.9. *If $\mu_n \subset K$ is a number field, then*

$$\begin{aligned} \Phi : K^\times / {K^\times}^n &\to \{L/K \text{ cyclic extension } |[L : K]|n\} := \mathcal{C}_n \\ a &\mapsto K(\sqrt[n]{a}) \end{aligned}$$

is surjective and $\Phi^{-1}(L) = \{K(\alpha^k) | (k, [L : K]) = 1\}$ *for some* $\alpha \in L$. *In particular,*

$$\#\Phi^{-1}(L) = \varphi([L : K]),$$

where φ *is the Euler* φ*-function.*

We split the proof into two parts. First we show Φ is well-defined and investigate $\Phi^{-1}(K(\alpha))$.

Proof. For all $a \in K$, let $L_a = K(\alpha)$ be the splitting field of

$$X^n - a = \prod_{i=0}^{n-1} (X - \zeta^i \alpha)$$

where $\alpha^n = a$ and $\zeta \in \mu_n$ is a primitive n^{th} root of unity. The extension L_a/L is Galois since $\zeta \in K$ and $G(L_a/L)$ is cyclic with generator $[\alpha \mapsto \zeta\alpha]$. For $a, b \in K^\times$, we say $a \sim b$ if $L_a = L_b$. Clearly, $\sim$ is an equivalence relation. Moreover, $a \sim ab^n$ for all $a, b \in K^\times$ so $\sim$ factors to an equivalence relation on $K^\times/K^{\times n}$. Therefore, Φ is well-defined.

By Example 5.8, $K^\times/K^{\times n} \cong \mathrm{H}^1(G(\overline{K}/K), \mu_n) = \mathrm{Hom}(G(\overline{K}/K), \mu_n)$ since $\mu_n \subset K$ is fixed by $G(\overline{K}/K)$. For $a \in K^\times/K^{\times n}$, consider the restriction map ρ_a

$$0 \longrightarrow \mathrm{Ker}(f_a) \longrightarrow G(\overline{K}/K) \xrightarrow{\rho_a} G(L_a/K) \longrightarrow 0.$$

Now, $\rho_a(\sigma) = id$ if and only $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}$ so $\mathrm{Ker}(\rho_a) = \mathrm{Ker}(\delta(a))$ and $L_a = \overline{K}^{\mathrm{Ker}(\delta(a))}$ by elementary Galois theory.

Suppose $b \in K^\times/K^{\times n}$ such that $b \sim a$. Let

$$L := L_a = L_b \qquad \text{and} \qquad H := \mathrm{Ker}(\delta(a)) = \mathrm{Ker}(\rho_a) = \mathrm{Ker}(\rho_b) = \mathrm{Ker}(\delta(b)).$$

Let $m = [L : K] = [G : H]$. Then m divides n and μ_m is the unique subgroup of μ_n of m elements[6]. Therefore, $\delta(a), \delta(b) : G \twoheadrightarrow \mu_m$ are two cokernels of the inclusion $H \hookrightarrow G(\overline{K}/K)$. However, cokernels are unique up to isomorphism, so there exists an isomorphism $h_{a,b} : \mu_m \to \mu_m$ such that $\delta(b) = h_{a,b} \circ \delta(a)$. Since δ is an isomorphism, $\Phi^{-1}(L_a) \hookrightarrow \mathrm{Aut}(\mu_m)$ by $b \mapsto h_{a,b}$ is an injection. This means

$$\#\Phi^{-1}(L_a) \leq \#\mathrm{Aut}(\mu_m) = \varphi(m).$$

[6]Cyclic groups of order n have a unique subgroup of order m for each m dividing n.

On the other hand, for all integers k relatively prime to m, $sk + tm = 1$ for some $s, t \in \mathbb{Z}$. Thus, $\alpha^k \in K(\alpha) = L_a$ while

$$\alpha = (\alpha^k)^s(\alpha^m)^t \in K(\alpha^k) = L_{a^k}$$

so $a \sim a^k$. Therefore, $\{a^k | (k, m) = 1\} \subseteq \Phi^{-1}(L_a)$, and in fact this is equality since $\#\{a^k | (k, m) = 1\} = \varphi(m) \geq \#\Phi^{-1}(L_a)$. □

Remark 5.10. During this proof, we saw $\Phi : K^\times/K^{\times n} \to \mathcal{C}_n$ factors through $\mathrm{Hom}(G(\overline{K}/K), \mu_n)$ as

$$K^\times/K^{\times n} \xrightarrow{\delta} \mathrm{Hom}(G(\overline{K}/K), \mu_n) \xrightarrow{\kappa_n} \mathcal{C}_n, \qquad \Phi = \kappa_n \circ \delta$$

where $\kappa_n : \mathrm{Hom}(G(\overline{K}/K), \mu_n) \to \mathcal{C}_n$ by $\sigma \mapsto \overline{K}^{\mathrm{Ker}(\sigma)}$.

We have shown above that $\Phi^{-1}(L_a)$ has exactly $[L_a : K]$ elements. The next result says that are all the cyclic extensions are of the form L_a for some $a \in K^\times/K^{\times n}$, i.e. that Φ is surjective.

Theorem 5.11 (Kummer Theory)**.** *Suppose L/K is a cyclic extension of degree n and assume $\mu_n \subseteq K$. Then $L = K(\sqrt[n]{a})$ for some $a \in K$. Furthermore, there are at most m^2 such classes a in $K^\times/K^{\times n}$ corresponding to a given cyclic extension L.*

Proof. Let $G = G(L/K) = \langle\sigma\rangle \cong \mathbb{Z}/n\mathbb{Z}$. Let $\zeta \in \mu_n$ be a primitive n^{th} root of unity. Since $\mu_n \subseteq K^\times$, the action of G on μ_n is trivial so the 1-cocycles (resp. 1-coboundaries), $G(L/K) \to \mu_n$, are the homomorphisms (resp. trivial), i.e. $\mathrm{H}^1(G, \mu_n) = \mathrm{Hom}(G, \mu_n)$. From the Example 5.8, we have the exact sequence

$$\begin{array}{ccccccc} \ldots \longrightarrow K^\times & \xrightarrow{\delta} & \mathrm{H}^1(G, \mu_n) & \longrightarrow & \mathrm{H}^1(G, \overline{K}^\times) & = & 0 \\ & & \| & & & & \\ & & \mathrm{Hom}(G, \mu_n) & & & & \end{array}$$

In other words, all homomorphisms are coboundaries. In particular, the isomorphism $F : G(L/K) \to \mu_n$ given by $F(\sigma) = \zeta$ is in fact also realized

as $F(\sigma^i) = \frac{\sigma^i\alpha}{\alpha}$ for some $\alpha \in L^\times$. Thus α has n conjugates so $L = K(\alpha)$. Furthermore, the minimal polynomial of α in L/K is

$$\prod_{i=0}^{n-1}(X - \sigma^i\alpha) = \prod_{i=0}^{n-1}(X - \zeta^i\alpha) = X^n - \alpha^n$$

so $a = \alpha^n \in K$. □

This concludes the proof of Theorem 5.9. An immediate consequence is a finite result of the map Φ.

Corollary 5.12. *The map $\Phi : K^\times/K^{\times n} \to \mathcal{C}_n$ is at most $\varphi(n)$-to-1.*

Proof. By Theorem 5.9, $\#\Phi^{-1}(L) = \varphi([L : K])$ which divides $\phi(m)$ since $[L : K]$ divides m. □

Now we look at the special case where $K = \mathbb{Q}$ and $n = 2$.

Example 5.13. Let $G = G(\overline{\mathbb{Q}}/\mathbb{Q})$. Note that $\{\pm 1\} = \mu_2 \subset \mathbb{Q}$ so G fixes μ_2. By Example 5.8,

$$\delta : \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \to \mathrm{H}^1(G, \mu_2) = \mathrm{Hom}(G, \mu_2) \quad \text{via} \quad a \mapsto \left[\sigma \mapsto \sigma\frac{\sqrt{a}}{\sqrt{a}}\right]$$

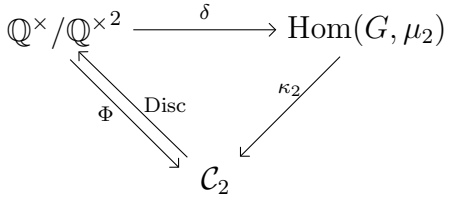
is an isomorphism. We want to find an explicit inverse of δ. By Theorem 5.9, the map

$$\Phi : K^\times/K^{\times n} \to \mathcal{C}_n \quad \text{via} \quad a \mapsto L_a = \mathbb{Q}(\sqrt{a})$$

is surjective and Corollary 5.12 says Φ is at most $\varphi(2)$-to-1. However, $\varphi(2) = 1$ so Φ is a bijection. By Remark 5.10, Φ factors as $\kappa_2 \circ \delta$ so it suffices to find an inverse to Φ. By Proposition 3.10, the discriminant map $\mathrm{Disc} : \mathcal{C}_2 \to \mathbb{Q}^\times$ behaves as follows;

$$\mathrm{Disc}(L_a) = \begin{cases} a & \text{if } a \not\equiv 1 \pmod 4 \\ 4a & \text{if } a \equiv 1 \pmod 4 \end{cases}$$

which are equivalent in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Thus, the triangle



commutes. Then the composition

$$\begin{aligned}\mathrm{Disc} \circ \kappa_2 : \mathrm{Hom}(G, \mu_2) &\to \mathbb{Q}^\times/{\mathbb{Q}^\times}^2 \\ f &\mapsto \mathrm{Disc}(\overline{\mathbb{Q}}^{\mathrm{Ker}(f)}),\end{aligned}$$

which we will denote by Disc^*, is the inverse of δ.

6 Elliptic curves over $\mathbb{Q}$

For this first subsection, let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$. Say E is defined by the Weierstrass equation $y^2 = x^3 + Ax + B$. After an appropriate change of variables, we may assume $A, B \in \mathbb{Z}$. Let Δ be the discriminant of E.

6.1 Lutz-Nagell

Theorem 6.1 (Lutz-Nagell)**.** *Suppose $P = (x, y) \in E(\mathbb{Q})$ has finite order. Then $x, y \in \mathbb{Z}$ and either $y^2 \mid \Delta$ or $y = 0$.*

Proof. See Chapter 7 of [Si09] or Chapter 8 of [Wa08]. □

Corollary 6.2. *Let E be an elliptic curve defined over $\mathbb{Q}$. Then the torsion subgroup $E(\mathbb{Q})_{\mathrm{tors}}$ is finite.*

Proof. Suppose $P = (x, y) \in E(\mathbb{Q})_{\mathrm{tors}}$. By Lutz-Nagell, $y \mid \Delta$ or $y = 0$ so there are only finitely many possibilities for y. Fixing y, there are at most 3 solutions to the Weierstrass equation in x, thus $E(\mathbb{Q})_{\mathrm{tors}}$ is finite. □

Corollary 6.3. *Let p be an odd prime not dividing Δ. Then the reduction map $\rho : E(\mathbb{Q})_{\mathrm{tors}} \hookrightarrow \widetilde{E}(\mathbb{F}_p)$ is injective on the torsion points.*

Proof. By Lutz-Nagell, all nontrivial torsion points have integer coordinates and thus reduce to well-defined points over $\mathbb{F}_p$. In particular, the only torsion point reduced to $\widetilde{O}$ is O so the reduction map restricted to torsion points has trivial kernel. □

Example 6.4. We determine the torsion subgroup, $E(\mathbb{Q})_{\mathrm{tors}}$, of the elliptic curve $E : y^2 = f(x) = x^3 + 31x + 96$.

Note that

$$\Delta = 4A^3 + 27B^2 = 4 \cdot 31^3 + 27 \cdot 96^2 \equiv 1 \mod 3$$

and

$$\Delta = 4 \cdot 31^3 + 27 \cdot 96^2 \equiv -1 + 2 \equiv 1 \mod 5.$$

Thus the corollary tells us that $E(\mathbb{Q})_{\text{tors}}$ embeds in $E(\mathbb{F}_3)$ and $E(\mathbb{F}_5)$. By computing $f(x) \in \mathbb{F}_3$ for each $x \in \mathbb{F}_3$ and noting which are squares, we can easily find every point on $E(\mathbb{F}_3)$. The results are

$$E(\mathbb{F}_3) = \{\infty, (0,0), (-1,-1), (-1,1)\}.$$

Thus, either $E(\mathbb{Q})$ contains a nontrivial 2-torsion point or $E(\mathbb{Q})_{\text{tors}}$ is trivial. However, the 2-torsion points correspond to roots of f and the reader can quickly check that $\widetilde{f}$ has no roots in $\mathbb{F}_5$. Therefore $E(\mathbb{Q})_{\text{tors}}$ is trivial.

We conclude this subsection by stating (without proof) a theorem of Mazur classifying all possible torsion subgroups.

Theorem 6.5 (Mazur)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$. Then the torsion subgroup, $E(\mathbb{Q})_{\text{tors}}$, is either*

- $\mathbb{Z}/n\mathbb{Z}$ *with* $1 \leq n \leq 10$ *or* $n = 12$ *or*
- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ *with* $1 \leq n \leq 4$.

6.2 Mordell-Weil

For the remainder of this section, fix some number field K and let E/K be an elliptic curve defined over K with discriminant Δ. We now come to the main theorem of this paper.

Theorem 6.6 (Mordell-Weil)**.** *$E(K)$ is finitely generated.*

The proof of this theorem will be split into two parts. We begin by proving

Theorem 6.7 (Weak Mordell-Weil)**.** *$E(K)/mE(K)$ is finite.*

Then we will continue with a descent procedure to complete the proof.

6.2.1 Weak Mordell-Weil

Turning our attention to Weak Mordell-Weil, we begin with a lemma.

Lemma 6.8. *Suppose L/K is a finite Galois extension. If $E(L)/mE(L)$ is finite, then $E(K)/mE(K)$ is finite.*

Proof. Begin with the short exact sequence of $G = G(L/K)$-modules

$$0 \to E(L)[m] \to E(L) \xrightarrow{m} mE(L) \to 0.$$

Through Galois cohomology, this induces the long exact sequence

$$0 \to E(K)[m] \to E(K) \xrightarrow{m} E(K) \cap mE(L) \xrightarrow{\delta} \mathrm{H}^1(G(L/K), E(L)[m]) \to \dots$$

and in particular

$$H \hookrightarrow \mathrm{H}^1(G, E(L)[m]),$$

where $H = \frac{E(K) \cap mE(L)}{mE(K)}$. However, G and $E(L)[m]$ are finite so $\mathrm{H}^1(G, E(L)[m])$ is finite so H is finite. Then

$$0 \to H \to E(K)/mE(K) \to E(L)/mE(L)$$

is exact, so $E(K)/mE(K)$ is finite as it lies between two finite groups. □

From this lemma, by taking L to be the Galois closure of the finite extension $K(E[m])/K$, it suffices to prove Mordell-Weil under the assumption $E[m] \subset E(K)$.

Lemma 6.9. *For any point $P \in E(K)$, the field extension $K(m^{-1}P)/K$ is unramified above all primes $\mathfrak{p} \nmid m\Delta$.*

Proof. Let $L = K(m^{-1}P)$, $\mathfrak{q} \subset L$ a prime above $\mathfrak{p}$, $D = D_{\mathfrak{q}}(L/K)$, and $I = I_{\mathfrak{q}}(L/K)$. By Proposition (3.19), we have the following situation,

$$\begin{array}{ccccc}
L & - & L_{\mathfrak{q}} & & \\
{\scriptstyle I}\,| & & {\scriptstyle I}\,| & \diagdown & \\
L^I & - & L_{\mathfrak{q}}^I & - & l \\
| & & | & & |\,{\scriptstyle D/I} \\
L^D & - & K_{\mathfrak{p}} & - & k \\
| & \diagup & & & \\
K & & & &
\end{array}$$

where all extensions below the fourth row are unramified at $\mathfrak{q}$. To show L/K is unramified above $\mathfrak{p}$, it suffices to show that I is trivial.

Suppose $\sigma \in I$. Then for any $Q \in m^{-1}P$, $\widetilde{\sigma Q - Q} = \sigma\widetilde{Q} - \widetilde{Q} = \widetilde{O}$ so $\sigma Q = Q$ by the isomorphism in Theorem 5.6. Therefore, $\sigma = id$ so I is trivial and L/K is unramified at P. □

We are now ready to complete the proof of the Weak Mordell-Weil Theorem.

Proof. Let $G = G(\overline{\mathbb{Q}}/\mathbb{Q})$. By Corollary 4.14, the multiplication-by-m map,

$$E(\mathbb{C}) \xrightarrow{m} E(\mathbb{C})$$

is surjective. Note that this is a polynomial map.[7] Thus any preimage of an algebraic point is an algebraic point so m restricts to a surjection on the $\overline{\mathbb{Q}}$-points, $E(\overline{\mathbb{Q}}) \xrightarrow{m} E(\overline{\mathbb{Q}})$. This gives a short exact sequence of G-modules

$$0 \to E[m] \to E(\overline{\mathbb{Q}}) \xrightarrow{m} E(\overline{\mathbb{Q}}) \to 0.$$

Through Galois cohomology, this induces the long exact sequence

$$0 \to E[m] \to E(K) \xrightarrow{m} E(K) \xrightarrow{\delta} \mathrm{H}^1(G, E[m]) \to \dots$$

Since we are assuming $E[m] \subset E(K)$, the action of G on $E[m]$ is trivial so $\mathrm{H}^1(G, E[m]) = \mathrm{Hom}(G, E[m])$. In particular, we get an injection $E(K)/mE(K) \xrightarrow{\delta} \mathrm{Hom}(G, E[m])$ given by $\delta(P)(\sigma) = \sigma Q - Q$ for any $P \in E(K)/mE(K), \sigma \in G$ where $Q \in m^{-1}P$.

Take $f \in \mathrm{Hom}(G, E[m])$. Since $\mathrm{Ker}(f) \trianglelefteq G$, Galois Theory gives an associated fixed field $L = \overline{\mathbb{Q}}^{\mathrm{Ker}(f)}$. Furthermore,

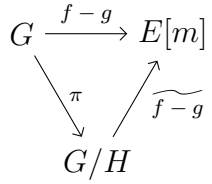
$$G(L/K) \cong G/G(\overline{\mathbb{Q}}/L) \cong G/\mathrm{Ker}(f) \cong \mathrm{Im}(f) \leq E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$$

so L/K is the composite of at most two cyclic extensions of degrees dividing m. Thus the following function is well-defined

$$\begin{aligned} \Psi : \mathrm{Hom}(G, E[m]) &\to \{\text{Galois Extensions } L/K | G(L/K) \leq (\mathbb{Z}/m\mathbb{Z})^2\} \\ f &\mapsto L. \end{aligned}$$

[7] The multiplication-by-m map can be computed explicitly by following the definition of addition on elliptic curves. The computations involve calculating intersection points of E with certain lines which gives rise to a polynomial map.

Suppose $\Psi(f) = \Psi(g)$. Then $\mathrm{Ker}(f) = \mathrm{Ker}(g) =: H$ so their difference factors through G/H.



However, $G/H \cong G(L/K) \leq (\mathbb{Z}/m\mathbb{Z})^2$, so

$$\mathrm{Hom}(G/H, E[m]) \subseteq \mathrm{Maps}((\mathbb{Z}/m\mathbb{Z})^2, (\mathbb{Z}/m\mathbb{Z})^2)$$

which has order m^4. Therefore, any homomorphism $f : G \to E[m]$ shares an associated field with no more than m^4 other homomorphisms. In other words, Ψ is at most m^4-to-1. To finish the proof, it suffices to show $\mathrm{Im}(\Psi \circ \delta)$ is finite.

Suppose $P \in E(K)/mE(K)$. Then

$$\mathrm{Ker}(\delta(P)) = \{\sigma \in G(\overline{\mathbb{Q}}/K) | \sigma Q - Q = 0, \forall Q \in m^{-1}P\}$$

so $\Psi\delta(P) = \overline{\mathbb{Q}}^{\mathrm{Ker}(\delta(P))} = K(m^{-1}P)$. Now, $\Psi\delta(P)/K$ is unramified above all primes $\mathfrak{p} \not\ni m\Delta$ by Lemma 6.9. Let S be the set of primes in $\mathcal{O}_K$ containing $m\Delta$ and let $\mathcal{C}$ be the collection of cyclic extensions of K of degree dividing m that are unramified above all primes $\mathfrak{p} \notin S$. Since $E[m] \subset E(K)$, Corollary 5.3 says $\mu_m \subset K$ so we may apply Theorem 3.22 to see that $\mathcal{C}$ is finite. Any field extension $L/K \in \mathrm{Im}(\Psi\delta)$ is the composite of two fields in $\mathcal{C}$. This means $\mathrm{Im}(\Psi\delta)$ is finite so $E(K)/mE(K)$ is finite. □

This completes the proof of Weak Mordell-Weil in the general case, however before moving on to the descent procedure, it is worth mentioning an argument for a special case of Weak Mordell-Weil which has the advantage of being completely explicit. When $m = 2$, $K = \mathbb{Q}$, and $E[2] \subset E(\mathbb{Q})$, the argument may be stated more concretely as follows.

Theorem 6.10 (Weak Mordell-Weil, Special Case)**.** *Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$ such that $E[2] \subset E(\mathbb{Q})$. Then $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.*

Proof. Suppose $E/\mathbb{Q}$ is given by the Weierstrass equation

$$y^2 = f(x) = x^3 + Ax + B = (x - e_1)(x - e_2)(x - e_3).$$

After a change of variables, we may assume $A, B \in \mathbb{Z}$ (and hence $e_i \in \mathbb{Z}$). Again, set $G = G(\overline{\mathbb{Q}}/\mathbb{Q})$. From the same Galois cohomology argument as before, we have an injection

$$E(\mathbb{Q})/2E(\mathbb{Q}) \xhookrightarrow{\delta} \mathrm{Hom}(G, E[2]).$$

Let $T_1 = (e_1, 0), T_2 = (e_2, 0)$ be generators for $E[2]$ as a $\mathbb{Z}/2\mathbb{Z}$-module. The nondegeneracy of the Weil-pairing allows us to explicitly identify the target, $\mathrm{Hom}(G, E[2])$, with the more familiar group, $\mathrm{Hom}(G, \mu_2)^2$.

$$\mathrm{Hom}(G, E[2]) \overset{u}{\xrightarrow{\sim}} \mathrm{Hom}(G, \mu_2^2) = \mathrm{Hom}(G, \mu_2)^2$$

$$f \longmapsto [\sigma \mapsto (\langle f(\sigma), T_1 \rangle_2, \langle f(\sigma), T_2 \rangle_2)]$$

From Example 5.13, we have the isomorphism $\mathrm{Disc}^* : \mathrm{Hom}(G, \mu_2) \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Let $\pi_i : \mathrm{Hom}(G, \mu_2)^2 \to \mathrm{Hom}(G, \mu_2)$ be the i^{th} projection map and define

$$(\mathrm{Disc}^*)^2 : \mathrm{Hom}(G, \mu_2)^2 \to (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^2$$

by $(\mathrm{Disc}^*)^2 = \mathrm{Disc}^* \circ \pi_1 \times \mathrm{Disc}^* \circ \pi_2$. Then, by Lemma 6.11 below, the following composition of injections and isomorphisms is given explicitly by

$$E(\mathbb{Q})/2E(\mathbb{Q}) \xrightarrow{\delta} \mathrm{H}^1(G, E[2]) \xrightarrow{u} \mathrm{Hom}(G, \mu_2)^2 \xrightarrow{(\mathrm{Disc}^*)^2} (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^2$$

$$\begin{aligned} P = (x, y) &\mapsto (x - e_1, x - e_2), \qquad \text{where } P \neq O, T_1, T_2 \\ O &\mapsto (1, 1) \\ T_1 = (e_1, 0) &\mapsto ((e_2 - e_1)(e_3 - e_1), e_1 - e_2) \\ T_2 = (e_2, 0) &\mapsto ((e_2 - e_1), (e_1 - e_2)(e_3 - e_2)) \end{aligned}$$

so it suffices to show that the image of $E(\mathbb{Q})/mE(\mathbb{Q})$ in $(\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^2$ is finite. Since $E[2]$ is finite, we do this by showing that for $P = (x, y) \in E(\mathbb{Q})\backslash E[2]$, if some prime p divides the square-free part of $x - e_i$, then p divides Δ.

Fix $P = (x, y) \in E(\mathbb{Q})\backslash E[2]$ and let $x - e_i = a_i u_i^2$ where $u_i \in \mathbb{Q}$ and $a_i \in \mathbb{Z}$ is square-free. We may also write $x - e_i = p^{k_i} v_i$ where $v_i \in \mathbb{Q}$ and $k_i \in \mathbb{Z}$ is the exact power of p dividing $x - e_i$. Suppose $p | a_i$ for some $i = 1, 2, 3$. To simplify notation, assume $p | a_1$. Then k_1 is odd. If $k_1 < 0$,

then $k_1 = k_2 = k_3$ since e_i are integers. Therefore, p^{3k_1} is the exact power of p dividing $y^2 = \prod(x - e_i)$, which is impossible as $3k_1$ is odd. On the other hand, if $k_1 > 0$, then $k_2, k_3 \geq 0$ as well since $e_i \in \mathbb{Z}$. If $k_2 = k_3 = 0$, then the exact power of p dividing y^2 is $p^{k_1+k_2+k_3} = p^{k_1}$, an odd power. Thus $k_i > 0$ for some $i = 2, 3$ which means $p|(x - e_i) - (x - e_1) = e_1 - e_i|\Delta$. □

Lemma 6.11. *Let $E/\mathbb{Q}$ be an elliptic curve such that*

$$E[2] = \{O, T_1, T_2, T_3\} \subset E(\mathbb{Q})$$

where $T_i = (e_i, 0)$. Suppose $P \in E(\mathbb{Q})$ and $\sigma \in G(\overline{\mathbb{Q}}/\mathbb{Q})$. Let $\delta(P)(\sigma) = \sigma Q - Q$, where $Q \in E(\overline{\mathbb{Q}})$ such that $2Q = P$, as above.

(i) If $P = (x, y) \neq O, T_i$, then $\langle \delta(P)(\sigma), T_i \rangle_2 = 1$ if and only if σ fixes $\sqrt{x - e_i}$.

(ii) If $P = O$, then $e_2(\delta(P)(\sigma), T_i) = 1$.

(iii) If $P = T_i$, then $\langle \delta(P)(\sigma), T_i \rangle_2 = 1$ if and only if σ fixes

$$\sqrt{(e_{i+1} - e_i)(e_{i+2} - e_i)} \text{ (subscripts are taken } \mod 3).$$

Proof. For $i = 1, 2, 3$, there exists $T_i' \in E(\overline{\mathbb{Q}})$ such that $2T_i' = T_i$. Using the notation from the Weil pairing construction in Subsection 5.1, there exists $f_{T_i}, g_{T_i} \in \overline{\mathbb{Q}}(E)$ such that

$$\operatorname{div}(f_{T_i}) = 2(T_i) - 2(O) \quad \text{and} \quad \operatorname{div}(g_T) = \sum_{R \in E[2]} (T_i' + R) - (R).$$

It is not hard to see that $f_{T_i} = X - e_i$ satisfies this condition. As in the construction in Subsection 5.1, $f_{T_i} \circ 2 = g_{T_i}^2$ and

$$\langle \sigma Q - Q, T_i \rangle_2 = \frac{g_{T_i}(X + \sigma Q - Q)}{g_{T_i}(X)}, \tag{8}$$

where $X \in E$ is any point such that $g_{T_i}(X + \sigma Q - Q), g_{T_i}(X) \neq 0, \infty$.

Note that E is defined over $\mathbb{Q}$ so the multiplication-by-2 map is defined over $\mathbb{Q}$. Furthermore, T_i is defined over $\mathbb{Q}$, so $2^{-1}T_i = \{T_i' + R | R \in E[2]\}$ are precisely the Galois conjugates of T_i'. Thus $\operatorname{div}(g_{T_i})$ is fixed by the G-action, so g_{T_i} can be chosen in $\mathbb{Q}(E)$ by [Si09, II, Ex. II.2.13].

(i) Suppose $P = (x, y) \neq O, T_i$. Then, by setting $X = Q$ in Equation 8,

$$\langle \sigma Q - Q, T_i \rangle_2 = \frac{g_{T_i}(\sigma Q)}{g_{T_i}(Q)} = \frac{\sigma\sqrt{x - e_i}}{\sqrt{x - e_i}}$$

is trivial if and only if σ fixes $\sqrt{x - e_i}$.

(ii) Suppose $P = O$. Then $\langle \sigma Q - Q, T_i \rangle_2 = 1$ as $\langle \cdot, \cdot \rangle_m$ is a bilinear form and $\sigma Q - Q = O$ since $Q = O$.

(iii) Suppose $P = T_i$. Then

$$\begin{aligned}\langle \delta(T_i), T_i \rangle_2 &= \langle \delta(T_{i+1} + T_{i+2}), T_i \rangle_2 = \langle \delta(T_{i+1}), T_i \rangle_2 \langle \delta(T_{i+2}), T_i \rangle_2 \\ &= \frac{\sigma\sqrt{e_{i+1} - e_i}}{\sqrt{e_{i+1} - e_i}} \frac{\sigma\sqrt{e_{i+2} - e_i}}{\sqrt{e_{i+2} - e_i}}\end{aligned}$$

by *(i)*. Therefore, $\langle \delta(T_i), T_i \rangle_2$ is trivial if and only if σ fixes

$$\sqrt{(e_{i+1} - e_i)(e_{i+2} - e_i)}.$$

□

6.2.2 Descent Procedure

In this section, we discuss the descent procedure which brings us from the Weak Mordell-Weil Theorem to the full Mordell-Weil Theorem. The general process is described in the Descent Theorem below. The problem is then reduced to finding a satisfactory "height function" on the curve.

Theorem 6.12 (Descent Theorem)**.** *Suppose A is an abelian group with some function $h : A \to \mathbb{R}$ satisfying*

(i) Fix $Q \in A$. There exists a constant C_Q such that $h(P + Q) \leq 2h(P) + C_Q$ for all $P \in A$.

(ii) There exists some integer $m \geq 2$ and a constant C such that $h(mP) \geq m^2 h(P) - C$ for all $P \in A$.

(iii) For any $D \in \mathbb{R}$, the set $\{P \in A \mid h(P) \leq D\}$ is finite.

If A/mA is finite, then A is finitely generated.

Proof. Let $Q_1, \ldots, Q_r \in A$ be coset representatives for A/mA. Suppose $P \in A$. As the cosets partition A, $P - Q_{i_1} \in mA$ for some $1 \leq i_1 \leq r$. Say $P = P_0 = mP_1 + Q_{i_1}$. Similarly, we can recursively construct the sequence of points $P_{j-1} = mP_j + Q_{i_j}$, $P_j \in A$, $i_j \in 1, \ldots, r$. Then for all j,

$$\begin{aligned} h(P_j) &\leq \frac{1}{m^2}(h(mP_j) + C) = \frac{1}{m^2}(h(P_{j-1} - Q_{i_j}) + C) && \text{by (ii)} \\ &\leq \frac{1}{m^2}(2h(P_{j-1}) + C' + C) && \text{by (i)} \end{aligned}$$

where $C' = \max\{C_{-Q_1}, \ldots, C_{-Q_r}\}$. Repeated use of this inequality gives us a formula for $h(P_n)$ in terms of (P)

$$\begin{aligned} h(P_n) &\leq (\frac{2}{m^2})^n h(P) + (\frac{1}{m^2} + \ldots + \frac{2^{n-1}}{m^{2n}})(C' + C) \\ &< (\frac{2}{m^2})^n h(P) + \frac{1}{m^2 - 2}(C' + C) \\ &\leq (\frac{1}{2})^n h(P) + \frac{1}{2}(C' + C) && \text{as } m \geq 2 \\ &\leq 1 + \frac{1}{m^2 - 2}(C' + C) && \text{for } n \text{ large.} \end{aligned}$$

Then

$$P = m^n P_n + \sum_{j=1}^{n} m^{j-1} Q_{i_j}$$

so $E(\mathbb{Q})$ is generated by

$$\{Q_1, \ldots, Q_r\} \cup \{P \in A \mid h(P) \leq 1 + (C' + C)/2\}$$

which is finite by (iii). □

We now give a height function on a rational curve. There is a slightly more complicated height function for the K-points on an elliptic curve where K is any number field. However, this will not be discussed here (see Chapter 8 of [Si09]). Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$. By the Weak Mordell-Weil Theorem, $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

Definition 6.13. Suppose $t \in \mathbb{Q}$ and $t = p/q$ with $(p, q) = 1$. The *height* of t is given by

$$H(t) = \max\{|p|, |q|\}.$$

The *(log) height on* $E(\mathbb{Q})$ is the function

$$h_x : E(\mathbb{Q}) \to \mathbb{R}_{\leq 0}$$

given by $h_x(0) = 0$ and $h_x(x, y) = logH(x)$.

Lemma 6.14. *(i) Pick* $P_0 \in E(\mathbb{Q})$. *There exists a constant* C_{P_0} *such that* $h(P + P_0) \leq 2h(P) + C_{P_0}$ *for all* $P \in E(\mathbb{Q})$.

(ii) There exists a constant C *such that* $h(2P) \geq 4h(P) - C$ *for all* $P \in E(\mathbb{Q})$.

(iii) For any $D \in \mathbb{R}$, *the set* $\{P \in E(\mathbb{Q}) \mid h(P) \leq D\}$ *is finite.*

Very brief justification / Method of proof. (i). By increasing C_{P_0} as needed, we may ignore finitely many $P \in E(\mathbb{Q})$. In particular, assume $P_0 \neq P$ and neither are the point at infinity. Use the formula for sums of distinct points

$$x(P + P_0) = \left(\frac{y_1 - y_0}{x_1 - x_0}\right)^2 - x_1 - x_0$$

which has degree 2 so we would expect $h(P + P_0) \approx 2h(P)$. (For a complete proof, plug in $x = a/b^2, y = c/d^3$ and similar forms for x_0, y_0, expand, and keep track of gcd's.)
(ii). The main inspiration for this part is that the "doubling isogeny" is of degree 4. This is clear since the kernel of this isogeny (when considered over $E(\overline{\mathbb{Q}})$) is $E[2]$ which has four points. The same general approach as above would give a complete proof.
(iii). Pick any $D \in \mathbb{R}$. Then

$$\{P \in E(\mathbb{Q}) \mid h_x(P) \leq D\} \subset \{0\} \cup \{(p/q, y) \in E(\mathbb{Q}) \mid \max\{|p|, |q|\} \leq D\}$$

but there are at most $2D + 1$ values for p and q and for each p/q there are at most 2 values for y so $\#\{P \in E(\mathbb{Q}) \mid h_x(P) \leq D\} \leq 1 + 2(2D + 1)^2$.

Theorem 6.15 (Mordell-Weil)**.** $E(\mathbb{Q})$ *is finitely generated.*

Proof. By the Weak Mordell-Weil Theorem and Lemma (6.14), $E(\mathbb{Q})$ and h_x satisfy the conditions of Theorem (6.12) at $m = 2$ so by the Descent Theorem, $E(\mathbb{Q})$ is finitely generated. □

Acknowledgments

I would like to thank my mentor, Sean Howe, for his guidance throughout this project and for explaining useful ways to think about new concepts. His support is greatly appreciated. I would also like to thank Peter May for conducting and including me in this REU.

References

[Ha77] Hartshorne, Robin. *Algebraic Geometry.* New York: Springer-Verlag, 1977. Print.

[Ko84] Koblitz, Neal. *Introduction to Elliptic Curves and Modular Forms.* New York: Springer-Verlag, 1984. Print.

[La94] Lang, Serge. Algebraic Number Theory. New York, NY [u.a.: Springer, 1994. Print.

[Mi13] Milne, James S. "Algebraic Number Theory." *Milne's Notes.* N.p., 21 Mar. 2013. Web.

[Se79] Serre, Jean-Pierre. *Local Fields.* New York: Springer-Verlag, 1979. Print.

[Si09] Silverman, Joseph H. *The Arithmetic of Elliptic Curves.* New York: Springer, 2009. Print.

[Wa08] Washington, Lawrence C. *Elliptic Curves: Theory and Cryptography.* Boca Raton, Fla. [u.a.: Chapman & Hall/CRC, 2008. Print.