Topics in Number Theory: Elliptic Curves

Yujo Chen

April 29, 2016

CONTENTS

INTRODUCTION

0.1 MOTIVATION

Solving Diophantine equations is one of the main focuses in the field of algebraic number theory. It gives rational or integer solutions to polynomial equations. For example, Fermat's equation,

$$x^3 + y^3 = z^3$$

has been proven by Fermat that it has no nontrivial solutions. More generally,

$$x^n + y^n = z^n$$

for n $>$ 2, has only solutions when at least one of x, y, or z is 0. For example $x = 0$ and $y = z$ works.

In particular, a class of polynomials called Weierstrass equation,

$$ay^2 + bxy + cy = x^3 + dx^2 + ex + f$$

gives an explicit formula for the points on the curve. We will be discussing the Weierstrass equation which helps us study the behavior of elliptic curves over arbitrary algebraic fields.

The study of Diophantine equation uses techniques from algebraic number theory and algebraic geometry. Finding the integer and rational solutions to the equation requires tools of algebraic number theory such as properties and behaviors of rings and fields. In this paper, we will conclude a strong result of elliptic curves over an arbitrary number field, the Mordell-Weil Theorem. In terms of algebraic geometry, the equation describes an algebraic variety that can be expressed as a geometric object.

0.2 SUMMARY AND PURPOSE

The purpose of this paper is to understand and approach integer and rational solutions of elliptic curves. Moreover, the discussion and complete proof of the Mordell-Weil Theorem applying to the field of rational numbers will give us a greater understanding of curves over a global (number) field.

In Chapter 1, we will discuss the generalities of algebraic geometry, including the definitions and maps between varieties. In Chapter 2, we look into the properties of one specific case of projective varieties, algebraic curves, and some special maps between curves and their motivations and applications to the proof of the Mordell-Weil

Theorem. In Chapter 3, we will talk about the basics of elliptic curves such as their algebraic properties and geometric interpretation. The fact that the rational points on the elliptic curves form a group and its group structure are also discussed. Moreover, we will discuss the elliptic curves over local fields on the different types of reduction. Lastly, in Chapter 4, we will apply the results we get from the previous chapters to prove the Mordell-Weil Theorem, which states that the group of rational points on the elliptic curve is finitely generated, the major result of this paper.

1

ALGEBRAIC VARIETIES

1.1 AFFINE VARIETIES

An algebraic variety is an n-dimensional algebraic curve. In other words, a variety is a set of points to a system of polynomial equations. As we are examining the set of points of an elliptic curve, it is important to know that these points form an algebraic variety.

In order to understand affine varieties, we need to understand the general concepts and definitions in algebraic geometry in terms of affine space and projective space. We define affine n-space (over the field K) as the set of n-tuples,

$$\mathbb{A}^n := \{(x_1, ..., x_n) : x_i \in \overline{K}\}.$$

Similarly, we define

$$\mathbb{A}^n(K) := \{(x_1, ..., x_n) : x_i \in K\}$$

as the set of K-rational points of $\mathbb{A}^n$.

Then, a subset of $\mathbb{A}^n$ can be defined as the set of zeros of polynomials over K. Moreover, if I is an ideal of $K[x_1, ..., x_n]$, let V_I be the subset of $\mathbb{A}^n$ consisting of zeros of polynomials in I.

To study the solutions to polynomial equations, or to solve systems of equations, we can look at an algebraic set which consists of solutions to a polynomial equation.

Definition 1.1.1. *An (affine) algebraic set is a set of the form*

$$V_I = \{P \in \mathbb{A}^n : f(P) = 0 \; \forall \, f \in I \; \}.$$

The ideal of V, or I(V), is defined as a set of functions in $\overline{K}$[X] such that the functions vanish for all points in V, i.e.,

$$I(V) = \{f \in \overline{K}[X] : f(P) = 0 \; \forall \; P \in V\}.$$

If I(V) can be generated by polynomials in K[X], then V is defined over K.

Definition 1.1.2. *If V/K is defined, then the set of K-rational points of V is the set $V \cap \mathbb{A}^n(K)$.*

We then can look at the ideal of this set. For the purpose of this paper, we will look at ideals and varieties over K because as we will be discussing the proof of the Mordell-Weil Theorem later in the paper, we will only care about the case when $K = \mathbb{Q}$ rather than the case of its algebraic closure, $\overline{K} = \mathbb{R}$.

Definition 1.1.3. *$I(V/K) = \{f \in K[X] : f(P) = 0 \ \forall \ P \in V\}$ is the ideal of V generated by polynomials in K[X].*

Note that all ideals in $\overline{K}$[X] and K[X] are finitely generated by Hilbert Basis Theorem.

Definition 1.1.4. *An affine algebraic set V is an (affine) variety if I(V) is a prime ideal in $\overline{K}$[X]; e.g. if $fg \in I$, then $f \in I$ or $g \in I$.*

Definition 1.1.5. *Let V/K be a variety. The affine coordinate ring of V/K is defined by*

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

Here, $K[V]$ is an integral domain. Its quotient field, or field of fractions, is denoted by $K(V)$, the function field of V/K. Similarly with $\overline{K}$.

Intuitively, dimension is fairly easy to understand conceptually - at least up to three dimensions. However, in terms of concreteness, dimensions of more than 3 consist of concept more than curve or surface. It is not easy to visualize. Therefore, we define dimension of a variety V, dim(V), as the transcendence degree of $\overline{K}$(V). The transcendence degree is the maximum number of algebraically independent polynomials, similar to linearly independent vectors in $\mathbb{R}^n$.

A variety V is nonsingular (or smooth) at $P \in V$ if the point is defined in the tangent space. Conversely, a variety is singular if the point is not regularly defined in the tangent space. Geometrically, a smooth point does not have an intersection point or "double" point. Moreover, if the Jacobian matrix at P has rank $n = dim(V)$, V is smooth.

Definition 1.1.6. *If V is nonsingular at every point, then V is smooth, or nonsingular.*

Proposition 1.1.7 shows another way to show whether or not a point $P \in V$ is nonsingular.

Proposition 1.1.7. *V is nonsingular at a point P iff*

$$dim_{\overline{K}} M_p/M_p^2 = dim(V),$$

where M_p is the local ring associated to the maximal ideal at point P.

$$M_p = \{ f \in \overline{K}[V] : f(P) = 0 \}$$

1.2 PROJECTIVE VARIETIES

In the affine space, parallel lines, which are represented by a system of equations that does not have a solution, do not intersect. However, we would like these lines to have an intersection point. This is where projective space is useful because in projective space, parallel lines do intersect at "points at infinity". Therefore, in projective spaces, there is one dimension higher than the dimension in affine space to account for these "points at infinity".

Definition 1.2.1. *Projective n-space is defined as*

$$\mathbb{P}^n = \{(x_0, ..., x_n) \in \mathbb{A}^{n+1}\}$$

where not all x_i are zero. Also,

$$(x_0, ..., x_n) \sim (y_0, ..., y_n) \text{ iff } \exists\ \lambda \text{ such that } x_i = \lambda\ y_i\ \forall\ i.$$

Definition 1.2.2. $\{(\lambda x_0, ..., \lambda x_n) : \lambda \in \overline{K}\}$, *or* $[x_0, ..., x_n]$, *is an equivalence class, where the x_i are called homogeneous coordinates.*

Note. We can look at $\mathbb{A}^2$ inside of $\mathbb{P}^2$ by setting one of the coordinates in $\mathbb{P}^2$ equal to 1 as follows:

$$[x : y : 1] \in \mathbb{P} \longleftrightarrow (x, y) \in \mathbb{A}^2$$

Since scalar multiples are the same point in projective space, we would like for polynomials when evaluated at these points to carry the same value or to be scalar multiples themselves, so that when viewed in projective space, they are really just the same point. This special type of polynomial is defined as a homogeneous polynomial.

Definition 1.2.3. *A polynomial f is homogeneous of degree d if*

$$f(\lambda p) = \lambda^d f(p)\ \forall\ \lambda \in \overline{K}, \forall p \in V.$$

For example, if we want a polynomial with degree 2 to satisfy the above property, it is easy to see that each term must be of degree 2 itself. This way, when we multiply a point by a scalar λ, we can just pull out λ^2 for each term.

$$f = x^2 + xy + z^2$$

is homogeneous polynomial of degree 2.

Remark. An ideal $I \subset \overline{K}[X]$ is homogeneous if it is generated by homogeneous polynomials.

Definition 1.2.4. *A projective algebraic set is any set of the form,*

$$V_I = \{P \in \mathbb{P}^n : f(P) = 0 \text{ for all homogeneous } f \in I\}$$

Example 1.2.5. $aX + bY + cZ = 0$, *where a, b, c*$\in \overline{K}$ *and not all zero, is a line in* $\mathbb{P}^2$ *is a projective algebraic set given by a linear equation.*

In a more general case of Example 1.2.5, the equation,

$$a_0X_0 + a_1X_1 + ... + a_nX_n = 0$$

with $a_i \in \overline{K}$ not all zero, is called a hyperplane in $\mathbb{P}^n$.

Example 1.2.6. *If V is the projective algebraic set in $\mathbb{P}^2$ given by the equation,*

$$X^2 + Y^2 = Z^2,$$

then for any field K with char(K) $\neq$ 2, the set V(K) is isomorphic to $\mathbb{P}^1$ via the map,

$$\mathbb{P}^1(K) \longrightarrow V(K),\ [s,t] \longmapsto [s^2 - t^2, 2st, s^2 + t^2].$$

This is similar to an affine variety, except we look at homogeneous polynomials in projective space.

Definition 1.2.7. *A projective algebraic set V is a (projective) variety if its homogeneous ideal I(V) is a prime ideal in $\overline{K}[X]$.*

The following definition of projective closure will help us understand Proposition 1.2.9.

Definition 1.2.8. *If V is an affine algebraic set, then $\overline{V}$ is the projective closure of V as follows,*
1. $V \subset \mathbb{A}^n \subset \mathbb{P}^n$.
2. I is the ideal generated by homogeneous ploynomials vanishing on V_I.
3. $\overline{V} = V_I$.

Proposition 1.2.9. *1. Let V be an affine variety. Then $\overline{V}$ is a projective variety, and $V = \overline{V} \cap \mathbb{A}^n$.*
2. Let V be a projective variety. Then $V \cap \mathbb{A}^n = \emptyset$ or $V = \overline{V \cap \mathbb{A}^n}$.
3. If V is defined over K, $\overline{V}$ is also defined over K.

Recall. If $I(V)$ can be generated by polynomials in $K[X]$, then V is defined over K.

Remark. To get a homogeneous equation from some inhomogeneous equation in $\mathbb{A}^n$, "attach" the $(n+1)^{th}$ projective variable to each term to make the equation homogeneous. To find a point at infinity, for example, take the equation in $\mathbb{A}^2$,

$$X + Y^2 = 1,$$

and set

$$X = \bar{X}/\bar{Z},\ Y = \bar{Y}/\bar{Z}.$$

This then becomes

$$\bar{X}/\bar{Z} + \bar{Y}^2/\bar{Z}^2 = 1$$
$$\bar{X}\bar{Z} + \bar{Y}^2 = \bar{Z}^2.$$

Set $\bar{Z} = 0$ to find the point at infinity.

1.3 MAPS BETWEEN VARIETIES

Because we are focusing on rational/integer solutions to polynomial equations, it makes sense to look at rational functions, which are functions that can be expressed as

$$f(X) = \frac{P(X)}{Q(X)}$$

where P and Q are polynomials with Q not equal to 0. Moreover, to define them on projective space, $P(X)$ and $Q(X)$ must be homogeneous of the same degree.

Definition 1.3.1. *Let V_1 and $V_2 \subset \mathbb{P}^n$ be projective varieties. A rational map from V_1 to V_2 is a map of the form*

$$\phi\colon V_1 \longrightarrow V_2,\ \phi = [f_0, ..., f_n],$$

where the functions $f_0, ..., f_n \in \overline{K}(V_1)$ have the property that for every $P \in V_1$ at which $f_0, ..., f_n$ are all defined,

$$\phi(P) = [f_0(P), ..., f_n(P)] \in V_2.$$

Note. If V_1 and V_2 are defined over K, an element of the Galois group, $\sigma \in G_{\overline{K}/K}$ acts on ϕ as usual.

Remark. A rational map, ϕ, from V_1 to V_2, is not always well-defined on V_1. There might be some points $P \in V_1$ such that $f_i(P)$ has a pole, for some i. However, Example 1.3.2 shows that it may be possible to find some $g \in \overline{K}(V_1)$ such that gf_i is defined at P for all i.

Example 1.3.2. *Let $\phi\colon \mathbb{P}^1 \to \mathbb{P}^1$ be a rational map. Take $f_0 = \frac{1}{X}$ and $f_1 = X$ such that $\phi = [\frac{1}{X}\colon X]$. Let $g = X$. Then, if we multiply by g to f_i's, we get*

$$\begin{aligned} gf_0 &= 1 \\ gf_1 &= X^2. \end{aligned}$$

The equivalent map, $[1\colon X^2]$ is defined at any point $P \in \mathbb{P}^1$ except at $X = \infty$. So, for $P = \infty$, we can use $g = \frac{1}{X}$, and get

$$\begin{aligned} gf_0 &= \tfrac{1}{X^2} \\ gf_1 &= 1, \end{aligned}$$

which are both defined at $P = \infty$ except at $\mathcal{O}$. Thus, for each point $P \in \mathbb{P}^1$, we can find a $g_P \in \overline{K}(\mathbb{P}^1)$ so that rescaling makes it defined at P.

Definition 1.3.3. *A rational map*

$$\phi = [f_0, ..., f_n] : V_1 \longrightarrow V_2$$

that is regular (defined) at each point $P \in V_1$ is called a morphism if for each $P \in V_1$ $\exists\, g \in \overline{K}(V_1)$ such that

1. *each gf_i is regular at P;*

2. *there is some i for which* $(gf_i) \neq 0$.

Definition 1.3.4. *A rational map*

$$\phi = [f_0, ..., f_n] : V_1 \longrightarrow V_2$$

is an isomorphism if there are morphisms $\psi = V_2 \longrightarrow V_1$ *such that* $\phi \circ \psi$ *and* $\psi \circ \phi$ *are identity maps on* V_1 *and* V_2*, respectively.*

Note. If ϕ and ψ are defined over a field K, then we say V_1/K and V_2/K are isomorphic over K.

2

ALGEBRAIC CURVES

For the purpose of this paper, we need to study elliptic curves in detail, which is an important case to consider while looking at algebraic curves. In this chapter, we will focus generally on algebraic curves and their many properties. Algebraic curves are projective varieties with dimension one; one example of such curves is the elliptic curve.

2.1 MAPS BETWEEN CURVES

A curve is a projective variety with dimension one. We will be looking at mostly smooth curves in this paper which are just projective varieties with continuous derivatives up to a certain order.

Proposition 2.1.1. *Let C be a curve and $P \in C$ a smooth point. Then $\overline{K}[C]_p$ is a discrete valuation ring (DVR).*

Recall that a discrete valuation ring is a principal ideal domain with a non-trivial maximal ideal. By being a discrete valuation ring, each point in the ring will have non-negative integer-values up to infinity corresponding to its valuation.

Note. $\overline{K}[C]_p$ is defined as the local ring of C at P. $\overline{K}[C]_p$ is a subring of K(C) which contains all rational functions such that the point P is defined for all of those functions.

Definition 2.1.2. *Let C be a curve and $P \in C$ a smooth point. The (normalized) valuation on $\overline{K}[C]_p$ is given by*

$$ord_p \colon \overline{K}[C]_p \longrightarrow \{0, 1, 2, ...\} \cup \{\infty\},$$
$$ord_p(f) = sup\{d \in \mathbb{Z} \colon f \in M_P^d\}.$$

The valuation can also be defined as a function on a field that provides a measure of the size of multiplicity of elements of the field.

Definition 2.1.3. *A uniformizer for C at P is an element $t \in \{t \in \overline{K}(C) : ord_p(t) = 1\}$, or in other words, t is a generator for M_p, the maximal ideal of $\overline{K}[C]_p$.*

Definition 2.1.4. *Let C be a curve and $P \in C$. Let $f \in \overline{K}(C)$. The order of f at P is $ord_P(f)$.*

$$\text{If } ord_P(f) > 0, \Rightarrow f(P) = 0.$$
$$\text{If } ord_P(f) < 0, \Rightarrow f(P) = \infty \text{ (has a pole at P).}$$
$$\text{If } ord_P(f) \geq 0, \Rightarrow f \text{ is regular at P.}$$

Proposition 2.1.5. *Let C be a curve, let $V \subset \mathbb{P}^N$ be a variety, let $P \in C$ be a smooth point, and let $\phi\colon C \to V$ be a rational map. Then ϕ is regular at P. In particular, if C is smooth, then ϕ is a morphism.*

Proof. Let $\phi = [f_0, ..., f_N]$ with functions $f_i \in \overline{K}(C)$. Pick a uniformizer $t \in \overline{K}(C)$ for C at point P. Define

$$n = \min_{0 \leq i \leq N} ord_P(f_i)$$

Then since t is the generator of the maximal ideal, multiplying $\frac{1}{t^n}$ to f_i will get rid of function in the denominator that causes problem.

$$ord_P(t^{-n} f_i) \geq 0 \ \forall \text{ i}$$
$$ord_P(t^{-n} f_j) = 0 \text{ for some j}$$

Therefore every $t^{-n} f_i$ is defined at P, or no pole at P. Thus ϕ is regular at P and is a morphism. □

Note. For every ϕ, we get a map on function fields ϕ^* defined by, $\phi^*\colon K(C_2) \to K(C_1)$, where $\phi^* f = f \circ \phi$, reads pullback of ϕ. For instance, if ϕ is a function of f, then the pullback of ϕ by the function f is $\phi(f(x))$.

The following result from Theorem 2.1.6 will give a relationship between smooth curves and their function fields. In particular, a curve C defined over K is equivalent to the function field of C over K.

Theorem 2.1.6. *Let C_1/K and C_2/K be curves.*

1. *Let $\phi\colon C_1 \to C_2$ be a nonconstant map defined over K. Then $K(C_1)$ is a finite extension of $\phi^*(K(C_2))$.*
2. *Let $\tau\colon K(C_2) \to K(C_1)$ be an injection of function fields fixing K. Then there exists a unique nonconstant map $\phi\colon C_1 \to C_2$ (defined over K) such that $\phi^* = \tau$.*
3. *Let $\mathbb{K} \subset K(C_1)$ be a subfield of finite index containing K. Then there exist a smooth curve C'/K, unique up to K-isomorphism, and a nonconstant map $\phi\colon C_1 \to C'$ defined over K such that $\phi^* K(C') = \mathbb{K}$.*

Definition 2.1.7. *Let $\phi\colon C_1 \to C_2$ be a map of curves defined over K. If ϕ is constant, we define the degree of ϕ to be 0. Otherwise we say that ϕ is a finite map and we define its degree to be*

$$deg\ \phi = [K(C_1)\colon \phi^* K(C_2)].$$

Definition 2.1.8. *Let $\phi\colon C_1 \to C_2$ be a nonconstant map of curves defined over K. The norm map relative to ϕ^* is defined in the other direction,*

$$\phi_*\colon K(C_1) \mapsto K(C_2),\ \phi_* = (\phi^*)^{-1} \circ N_{K(C_1)/\phi^* K(C_2)}.$$

ϕ_* reads pushforward of ϕ.

2.2 RAMIFICATION

Factoring prime elements of a ring in an algebraic field K into prime ideals is one way of understanding ramification of map between smooth curves. For example, the prime integer 2 is ramified in the algebraic field $\mathbb{Z}[i]$ because it can be expressed as follows:

$$2 = (1+i)^2.$$

The properties of ramification over smooth curves will help us prove the finiteness of a specific field in our proof of Mordell-Weil Theorem.

Definition 2.2.1. *Let $\phi\colon C_1 \to C_2$ be a nonconstant map of smooth curves, and let $P \in C_1$. The ramification index of ϕ at P, denoted by $e_\phi(P)$, is the quantity*

$$e_\phi(P) = ord_P(\phi^* t_{\phi(P)}),$$

where $t_{\phi(P)} \in K(C_2)$ is a uniformizer at $\phi(P)$.

In our analogy of number fields, the prime 2 ramifies with index 2. Primes congruent to 1 mod 4 reduce to two distinct factors in $\mathbb{Z}[i]$, therefore, they have index 2 as well. And primes congruent to 3 mod 4 are unramified since they remain primes in $\mathbb{Z}[i]$.

Note. $e_\phi(P) \geq 1$. If $e_\phi(P) = 1$, ϕ is unramified at P.

Proposition 2.2.2. *Let $\phi\colon C_1 \to C_2$ be a separable nonconstant map of smooth curves.*

1. *For every $Q \in C_2$,*

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

2. *For all but finitely many $Q \in C_2$,*

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

3. *Let $\psi\colon C_2 \to C_3$ be another nonconstant map of smooth curves. Then for all $P \in C_1$,*

$$e_{\psi\circ\phi}(P) = e_\phi(P) e_\psi(\phi P).$$

Proposition 2.2.2 tells us that the preimage of P is finite and is equal to the sum of the ramification indices over the preimage of P. This shows us that the ramification index for an unramified point must be 1 because there is only one point in the preimage.

2.3 FROBENIUS MAP

Let K be a field, C be a curve, and $char(K) = p > 0$. q is r^{th} power of p. $C^{(q)}/K$ contains the polynomial $f^{(q)}$ obtained from f by raising each coefficient of f to the q^{th} power. There is a morphism from C to $C^{(q)}$ called the Frobenius map defined as follows.

$$\phi\colon C \to C^{(q)},\ \phi([x_0, ..., x_n]) = [x_0^q, ..., x_n^q].$$

Proposition 2.3.1 describes some properties of the Frobenius map.

Proposition 2.3.1. *Let K be a field, C be a curve, and $char(K) = p > 0$. q is r^{th} power of p. $\phi\colon C \to C^{(q)}$ Frobenius morphism.*

1. $\phi^* K(C^{(q)}) = K(C)^q = \{f^q\colon f \in K(C)\}$.
2. *ϕ is purely inseparable.*
3. *deg $\phi = q$.*

2.4 DIVISORS

Divisors are a way of expressing the locations along with their respective orders of zeros and poles of a curve. For example, if a curve C has a zero of order 2 at P and a pole of order 4 at Q, then the divisor of C can be written as the formal sum,

$$Div(C) = 2\langle P\rangle - 4\langle Q\rangle.$$

Definition 2.4.1. *The divisor group of curve C, denoted by Div(C), is the free abelian group generated by the points of C. For instance, a divisor $D \in Div(C)$ is*

$$D = \textstyle\sum_{P\in C} n_p(P),$$

where $n_p \in \mathbb{Z}$ and $n_p = 0$ for all but finitely many $P \in C$.
Also, the degree of D is defined as

$$degD = \textstyle\sum_{P\in C} n_p.$$

In short, the elements of a divisor group are called formal sums, the sums of the points on the curve. Moreover, the divisors of degree 0 form a subgroup of $Div(C)$, denoted as

$$Div^0(C) = \{D \in Div(C)\colon degD = 0\}.$$

Definition 2.4.2. *Let C be a smooth curve and $f \in \overline{K}(C)^*$. Then we can relate f to the divisor as*

$$div(f) = \textstyle\sum_{P\in C} ord_P(f)(P).$$

By defining $div(f)$, we then can look at the principal divisor as follows:

Definition 2.4.3. *A divisor $D \in Div(C)$ is principal if it has the form $D = div(f)$ for some $f \in \overline{K}(C)^*$. Two divisors are linearly equivalent, written $D_1 \sim D_2$, if $D_1 - D_2$ is principal.*

Some maps between divisor groups are as follow:
$\phi^*: Div(C_2) \to Div(C_1)$, a "composition function" from one point to another.
$\phi_*: Div(C_1) \to Div(C_2)$, a "dual" relationship with ϕ^*.
These maps are associated to any non-constant morphism $\phi: C_1 \to C_2$.

Definition 2.4.4. *The quotient of $Div(C)$ by subgroup of principal divisors is the divisor class group, or Picard group, of C, denoted as $Pic(C)$.*

The Picard group is important because it allows us to show the associativity of the group law fairly easily by first noting that the Picard group is indeed a group, and therefore, its operation is associative, and then showing that the Picard group, $Pic^0(E)$, is isomorphic to the curve.

Proposition 2.4.5. *Let $\phi: C_1 \to C_2$ be a nonconstant map of smooth curves.*

1. $deg(\phi^* D) = (deg\phi)(degD) \ \forall \ D \in Div(C_2)$.
2. $\phi^*(divf) = div(\phi^* f) \ \forall \ f \in \overline{K}(C_2)^*$.
3. $deg(\phi_* D) = degD \ \forall \ D \in Div(C_1)$.
4. $\phi_*(divf) = div(\phi_* f) \ \forall f \in \overline{K}(C_1)^*$.
5. $\phi_* \circ \phi^*$ *acts as multiplication by* $deg\phi$ *on* $Div(C_2)$.
6. *If* $\psi: C_2 \to C_3$ *is another such map, then*

$$(\psi \circ \phi)^* = \phi^* \circ \psi^* \text{ and } (\psi \circ \phi)_* = \psi_* \circ \phi_*.$$

2.5 DIFFERENTIAL

Suppose a function $f: \mathbb{R}^n \to \mathbb{R}$. For each differentiable function f, we have a differential form df. One important thing to know is that the gradient of f is different than a differential form of f. The differential form give a dual vector, or a linear function from $\mathbb{R}^n$ to $\mathbb{R}$, this function can be applied to a vector v with properties as follows:

Definition 2.5.1. *Let C be a curve. The space of (meromorphic) differential forms on C, denoted as Ω_C, is the $\overline{K}$-vector space generated by symbols modulo the relations:*

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

2.6 THE RIEMANN-ROCH THEOREM

Definition 2.6.1. *A divisor $D = \sum n_P(P)$ is positive, or effective, denoted by $D \geq 0$, if $n_P \geq 0$ for every $P \in C$. Similarly, for any two divisors D_1, $D_2 \in Div(C)$, if $D_1 - D_2$ is positive, then $D_1 \geq D_2$.*

Divisorial inequalities can also be used to describe the poles and/or zeros of a function. If a function f is defined everywhere except at $P \in C$, and the pole at P is at most order n, then

$$div(f) \geq -n(P).$$

Definition 2.6.2. *Let $D \in Div(C)$. Define the set $\mathcal{L}(D)$ as below,*

$$\mathcal{L}(D) = \{f \in \overline{K}(C)^* : div(f) \geq -D\} \cup \{0\}.$$

$\mathcal{L}(D)$ is a finite-dimensional $\overline{K}$-vector space. Its dimension de denoted by

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

The following result helps us understand the proof of Proposition 2.6.4.

Proposition 2.6.3. *Let C be a smooth curve and $f \in \overline{K}(C)^*$.*

1. *$div(f) = 0$ iff $f \in \overline{K}^*$.*
2. *$deg(div(f)) = 0$.*

Proposition 2.6.4. *Let $D \in Div(C)$.*

1. *If $degD < 0$, then $\mathcal{L}(D) = \{0\}$ and $\ell(D) = 0$.*
2. *$\mathcal{L}(D)$ is a finite-dimensional $\overline{K}$-vector space.*
3. *If $D' \in Div(C)$ is linearly equivalent to D, then*

$$\mathcal{L}(D) \cong \mathcal{L}(D') \Rightarrow \ell(D) = \ell(D').$$

With Proposition 2.6.4, the following theorem proves the existence of the group law on elliptic curves.

Theorem 2.6.5. *(Riemann-Roch) Let C be a smooth curve and let K_C be a canonical divisor on C. The genus of C, $g \in \mathbb{Z}_{\geq 0}$, such that for every divisor $D \in Div(C)$,*

$$\ell(D) - \ell(K_C - D) = degD - g + 1.$$

The Riemann-Roch Theorem is significant because it tells us that for a curve with genus 1, there is a surjection that takes the curve onto its degree-0 Picard group. This proves the existence of a group structure on the curve because the Picard group has a group structure.

Note. The canonical divisor is a subgroup of the divisor class group.

$$K_C \subset Pic(C).$$

3

BASICS OF ELLIPTIC CURVES

Elliptic curves are curves of genus 1 and each with one specified base point. More specifically, an elliptic curve over field K is a pair $(E, \mathcal{O})$ where E is a smooth, genus 1 projective curve over field K and $\mathcal{O} \in E$ is a point defined over K, or the base point of E. To begin, we first understand the geometry and basic properties of elliptic curves over arbitrary algebraically closed fields. Since the points of an elliptic curve form a group, we can look at the important relations between the algebraic maps of these curves.

3.1 WEIERSTRASS EQUATIONS

As mentioned in the introduction of this paper, each curve has its Weierstrass equation, which gives explicit formula for the points on the curve. Precisely, every elliptic has a representation of a Weierstrass equation as below.

$$ay^2 + bxy + cy = x^3 + dx^2 + ex + f$$

Suppose $\phi\colon E \to \mathbb{P}^2$ and let x and y be non-trivial rational functions with poles of order 2 and 3 at $\mathcal{O}$, then the image of E under this map is always the set of zeros of a Weierstrass equation. And, $\mathcal{O} = [0 : 1 : 0]$, is also called the point at infinity.

Let K be a field. $\mathrm{Char}(K) \neq 2, 3$. By performing an appropriate change of variables, we may ensure that the coefficient a in the Weierstrass equation is 1, such that the general Weierstrass equation for genus 1 elliptic curve is as follows,

$$y^2 = x^3 - 27c_4x - 54c_6.$$

And we define the parameter Δ by, $1728\Delta = c_4^3 - c_6^2$, which detects whether the equation is singular.

3.2 GROUP LAW

In this section, let E be an elliptic curve given by a Weierstrass equation. Then, $E \subset \mathbb{P}^2$ includes the points $P = (x, y)$ of the Weierstrass equation, along with the "point at infinity," $\mathcal{O} = [0, 1, 0]$. $L \subset \mathbb{P}^2$

defined as a line. Because the degree of elliptic curve is 3, we know that the line L at exactly three points with multiplicity. If L is tangent to E, then these three points, labeled them as P, Q, and R, are not necessarily distinct.

Composition Law 3.2.1. *Let $P, Q \in E$, let L be the line through P and Q (if $P = Q$, let L be the tangent line to E at P), and let R be the third point of intersection of L with E. Let L' intersects E at R, O, and a third point. We denote that third point by $P \oplus Q$.*

The following proposition states the properties of the composition law.

Proposition 3.2.2. 1. *If a line L intersects E at the points P, Q, R, then*

$$(P \oplus Q) \oplus R = O.$$

2. $P \oplus O = P \; \forall \; P \in E$.

3. $P \oplus Q = Q \oplus P \; \forall \; P, Q \in E$.

4. *Let $P \in E$. There is a point of E, denoted by P', satisfying*

$$P \oplus (P') = O.$$

5. *Let $P, Q, R \in E$. Then*

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

6. *Suppose that E is defined over K. Then*

$$E(K) = \{(x, y) \in K^2 \colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}$$

is a subgroup of E.

Note. Items 1-5 show that the composition law makes E into an abelian group with identity element $\mathcal{O}$. Also, the group operation on an elliptic curve is denoted as follows:

$$[m]P = P \oplus ... \oplus P, \text{ m times. } [0]P = \mathcal{O}.$$

3.3 ISOGENIES

Now we look at maps between elliptic curve. Recall that a map $\phi \colon V_1 \to V_2$ is a morphism if for each point $P \in V_1$, there exists $g \in \overline{K}(V_1)$ for each i such that gf_i is regular at P.

Definition 3.3.1. *Let E_1 and E_2 be elliptic curves. An isogeny from E_1 to E_2 is a morphism*

$$\phi\colon E_1 \to E_2 \text{ satisfying } \phi(\mathcal{O}) = \mathcal{O}.$$

Remark. An isogeny between elliptic curves is a homomorphism if their group laws.

Example 3.3.2. *Let $m \in \mathbb{Z}$. Define the multiplication-by-m isogeny as below. For $m > 0$,*

$$[m](P) = P + P + ... + P. \text{ (m times)}$$

For $m < 0$, set $[m](P) = [-m](-P)$. Define $[0](P) = 0$. It is clearly a morphism. This map sends $\mathcal{O}$ to $\mathcal{O}$, thus, by the definition, this is an isogeny.

3.4 TORSION SUBGROUP

On an elliptic curve, there are points with finite order and with infinite order. To have a finite order means there exists an integer n such that if a point P is added to itself n times, it gives $\mathcal{O}$. On the other hand, to have an infinite order means no matter how many times P is added to itself, it will never give $\mathcal{O}$.

Definition 3.4.1. *Let E be an elliptic curve. A point $P \in E$ is called a torsion point of order n if P has order n.*

Note. If the group of points on the elliptic curve is torsion-free, then the group has infinite order. For example, $\mathbb{R}$ is torsion-free ring because for $n \in \mathbb{Z}$ and $\alpha \in \mathbb{R}$ satisying $n\alpha = 0$, either $n = 0$ or $\alpha = 0$. For $\alpha \neq 0$, no matter how many times α is added to itself, it will never give 0.

Definition 3.4.2. *Let E be an elliptic curve. Let $m \in \mathbb{Z}$ with $m \geq 1$. The m-torsion subgroup of E is the set of points of E of order m,*

$$E[m] = \{P \in E\colon [m]P = \mathcal{O}\}.$$

The torsion subgroup of E is the set of points of finite order,

$$E_{tors} = \bigcup_{m=1}^{\infty} E[m].$$

If E elliptic curve is defined over K, prime $p = Char(K)$ and $m \not| p$, then the group of m-torsion points $E[m]$ has the form

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

This congruence relation will be important as we discuss about the proof of Mordell-Weil Theorem in the following chapter.

3.5 INVARIANT DIFFERENTIALS

In this section, we will look at the differential of the Weierstrass equation of an elliptic curve over K. Let the following be the Weierstrass equation of E/K,

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

The differential,

$$\omega = \frac{dx}{2y+a_1x+a_3} \in \Omega_E$$

clearly has neither zeros nor poles at (x_0, y_0) or at $\mathcal{O}$. We want to justify that this differential is invariant under translation.

Proposition 3.5.1. *Let E/K be an elliptic curve. Its Weierstrass equation and differential are as above. Let $Q \in E$ and $\tau_Q\colon E \to E$ be the translation-by-Q map. Then*

$$\tau_Q^*\omega = \omega.$$

Proof. One way to prove this proposition is through direction calculation. By writing $x(P+Q)$ and $y(P+Q)$ in terms of $x(P)$, $x(Q)$, $y(P)$, and $y(Q)$ using addition group law. Then calculate $dx(P+Q)$ as rational function times $dx(P)$ while treating $x(Q)$ and $y(Q)$ as constants. Then,

$$\frac{dx(P+Q)}{2y(P+Q)+a_1x(P+Q)+a_3} = \frac{dx(P)}{2y(P)+a_1x(P)+a_3}$$

is verified by a constant value Q. □

Based on the formula of ω, the invariant differential on an elliptic curve has neither zeros nor poles, it helps us linearize the tedious addition law on the curve.

3.6 ELLIPTIC CURVES OVER LOCAL FIELDS

In this section, we will talk some types of reduction along with some important results of group cohomology as we would be using them in the proof of Mordell-Weil Theorem in the next chapter.

Let E be elliptic curve over field K. For a minimal Weierstrass equation for E/K, we can reduce its coefficient modulo π to obtain a possibly singular curve over K,

$$\tilde{E}\colon y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6,$$

which is called the reduction of E modulo π. There are several different reduction types based on the properties of the reduced curve.

Definition 3.6.1. *Let E/K by an elliptic curve, and let $\tilde{E}$ be the reduction modulo $\mathcal{M}$ of a minimal Weierstrass equation for E.*

1. *E has good reduction if $\tilde{E}$ is nonsingular.*
2. *E has multiplicative reduction if $\tilde{E}$ has a node.*
3. *E has additive reduction if $\tilde{E}$ has a cusp.*

If $\tilde{E}$ has multiplicative or additive reduction, we call that bad reduction.

Understanding the notion of reduction, we can let look at the some subsets of $E(K)$ based on the types of reduction.

Definition 3.6.2. 1. *$E_0(K)$ is the set of points with nonsingular reduction.*

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

where $\tilde{E}_{ns}(k)$ is the set of nonsingular points and $k = R/\pi R$.

2. *$E_1(K)$ is the kernel of reduction.*

$$E_1(K) = \{P \in E(K) \colon \tilde{P} = \tilde{\mathcal{O}}\}.$$

The following proposition will help us prove the Weak Mordell-Weil Theorem on the unramification of an extension field, which will be discussed later.

Proposition 3.6.3. *There exists an exact sequence of abelian groups*

$$0 \to E_1(K) \to E_0(K) \to \tilde{E}_{ns}(k) \to 0,$$

where the right-hand map is reduction modulo π.

4

MORDELL-WEIL THEOREM

Around 1092, Poincare introduced the conjecture of the group of rational points on an elliptic curve being finitely generated. However, it was not until 1922, Louis Mordell proved this conjecture. Moreover, in 1928, Andre Weil proved that this conjecture is actually extended to abelian varieties over the number fields. For the purpose of this paper, I will prove the Mordell part of this theorem.

We already know from the previous chapter that the rational points on the elliptic curve form a group under the operation of group law. Mordell-Weil Theorem tells us that this group is actually finitely generated. More generally, it states that for an abelian variety, A, over a number field, E, the group $A(K)$ of K-rational points of A is finitely generated.

K is a finite extension of $\mathbb{Q}$
E is an elliptic curve over K
$E(K)$ is Mordell-Weil group (points on the curve)

Theorem 4.0.1. *Mordell-Weil Theorem*
The group $E(K)$ is finitely generated.

The proof of the theorem consists of two parts: The Weak Mordell-Weil Theorem and the Descent Theorem. By proving both of the theorems and understanding the relationship and correlation between the two, one will be able to complete the proof for the Mordell-Weil Theorem.

4.1 THE WEAK MORDELL-WEIL THEOREM

Theorem 4.1.1. *The Weak Mordell-Weil Theorem*
Let K be a finite extension of $\mathbb{Q}$, let E/K be an elliptic curve, and $m \geq 2$ be in $\mathbb{Z}$. Then $E(K)/mE(K)$ is a finite group.

Note. The Weak Mordell-Weil Theorem does not by itself imply that $E(K)$ is finite.

In Lemma 4.1.2, We want to look a finite Galois extension of K because we will need to apply the Kummer pairing to the field and show that it is finite.

Lemma 4.1.2. *Let L/K be a finite Galois extension. If $E(L)/mE(L)$ is finite, then $E(K)/mE(K)$ is also finite.*

Proof. We can start the proof with the exact sequence:

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

Then through Galois cohomology, we get the exact sequence:

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

where $H = \frac{E(K) \cap mE(L)}{mE(K)}$. And since G and $E(L)[m]$ are finite, H is also finite. Therefore if $E(L)/mE(L)$ is finite, then $E(K)/mE(K)$ is also finite.

□

Remark. Lemma is proven by using Galois cohomology to show that $E(K)/mE(K)$ lies between two finite groups, and thus it is also finite. We will use the concept of Kummer pairing and its properties to show that there exists an abelian group maps from the Galois group injectively by perfect pairing.

Because of Lemma 4.1.2, we can make K larger in order to assume that $E[m]$ is defined over K to define the Kummer pairing.

Definition 4.1.3. *The Kummer pairing*

$$\kappa \colon E(K) \times G_{\overline{K}/K} \to E[m]$$

is defined as follows. Let $P \in E(K)$ and choose any point $Q \in E(\overline{K})$ satisfying $[m]Q = P$. Then

$$\kappa(P, \sigma) = Q^\sigma - Q.$$

The following proposition helps us understand the properties of the Kummer pairing. As you'll see, Kummer pairing then induces a perfect bilinear pairing maps $E(K)/mE(K) \times G_{L/K}$ to $E[m]$.

Proposition 4.1.4. 1. *The Kummer pairing is well-defined.*

2. *The Kummer pairing is bilinear.*

3. *The kernel of the Kummer pairing on the left is $mE(K)$.*

4. *The kernel of the Kummer pairing on the right is $G_{\overline{K}/L}$, where*

$$L = K([m]^{-1}E(K))$$

is the compositum of all fields $K(Q)$ as Q ranges over the points in $E(\overline{K})$ satisfying $[m]Q \in E(K)$.

There's a perfect pairing between $G_{L/K}$ and $E(K)/mE(K)$ into the m-torsion of E. Since L is a particular Galois extension, (Take K and adjoin all the x and y coordinates, and as they are multiplied by m, it will give the points in E.) A linear pairing resulting from the Kummer pairing would be as follows.

$$E(K)/mE(K) \times G_{L/K} \to E[m]$$

Remark. The field L is called a Kummer extension by adjoining all m^{th} roots of K. For each element in L, take K, and multiply by m to all the points, it will give you points in $E(K)$.

Proof.

1. To prove the Kummer pairing is well defined, take two distinct points $Q, Q' \in E(\overline{K})$ such that $mQ = mQ' = P$, where $P \in E(K)$. Since multiplication by m commutes with Galois action, we get $m(Q^\sigma - Q) = mQ^\sigma - mQ = P^\sigma - P = 0$. Then, $Q - Q' \in E[m] \subset E(K)$. Finally, $(Q^\sigma - Q) - (Q'^\sigma - Q') = (Q - Q')^\sigma - (Q - Q') = 0$ This shows that Galois action is trivial because P is defined over K.

2. To show that the Kummer pairing is bilinear, we look at two parts. First, take $P, P' \in E(K)$. We have $\kappa(P + P', \sigma)$, and since $mQ = P$ and $mQ' = P'$, it gives $m(Q + Q') = P + P'$. Then, we have $(Q + Q')^\sigma - (Q + Q') = (Q^\sigma - Q) + (Q'^\sigma - Q')$. Secondly, we look at $\kappa(P, \sigma\tau) = Q^{\sigma\tau} - Q = (Q^{\sigma\tau} - Q^\tau) + (Q^\tau - Q)$. Since Galois action is trivial on $E[m]$, $(Q^{\sigma\tau} - Q^\tau) = (Q^\sigma - Q)^\tau = \kappa(P, \sigma)^\tau = \kappa(P, \sigma)$. This concludes that the Kummer pairing is bilinear.

3. We want to show that kernel on the left is $mE(K)$. Take $P \in Ker(\kappa) \Rightarrow Q = \frac{1}{m}P \Rightarrow Q^\sigma - Q = 0 \; \forall \; \sigma \Rightarrow Q^\sigma = Q \Leftrightarrow Q \in E(K)$ (because Q is Galois invariant).

4. To show that kernel on the right is $G_{\overline{K}/L}$,we need to show that any element in the kernel fixes the field L. Take $\sigma \in Ker(\kappa) \Leftrightarrow \forall$ Q such that $mQ = P \in E(K)$, $Q^\sigma = Q$. Since σ fixes $[m]^{-1}K(E) \Rightarrow$ σ fixes L. Now, assume σ fixes all $Q \in [m]^{-1}E(K)$. Since L is an algebraic extension of K, $L = K(x_1, y_1, ..., x_n, y_n, ...)$. σ fixes L if and only if σ fixes $x_i, y_i \; \forall \; i$. So, since σ fixes $L \; \forall \; Q \in [m]^{-1}E(K)$, σ also fixes L.

□

Then by Proposition 4.1.4, we have a non degenerate bilinear pairing, we have the mapping:

$$E(K)/mE(K) \times G_{L/K} \to E[m]$$

The next step to prove the Weak Mordell-Weil Theorem is to show that L/K is finite, or to show that $G_{L/K}$ is finite. Then, it will give an injection from $E(K)/mE(K) \to Hom(G_{L/K}, E[m])$.

To show that $[L\colon K]$ is finite, we need to first define places as follows.

Definition 4.1.5. *Places is a field K are the non-trivial norms up to equivalence which has $f\colon K \to \mathbb{R}_{\geq 0}$ that satisfies multiplicative and triangle inequality properties.*

The places of K are in natural bijection with the set, $\{P \subset \mathbb{O}_K$ a prime ideal p-adic norm$\} \cup \{\sigma\colon K \to \mathcal{C}$ (up to conjugation) $|x|_\sigma = |\sigma(x)|\}$

Note. $\{P \subset \mathbb{O}_K$ a prime ideal p-adic norm$\}$, while $\{\sigma\colon K \to \mathcal{C}$ (up to conjugation) $|x|_\sigma = |\sigma(x)|\}$.

Now we have the definition of places, by looking at the following proposition, we can then study the abelian and m-torsion Galois field L over K, given that there exists a places with bad reduction points of E. To show that L finite, we first need to look at some properties of the field L.

Proposition 4.1.6. *Let*

$$L = K([m]^{-1}E(K))$$

1. *The extension L/K is abelian and has exponent m, i.e., the Galois group $G_{L/K}$ is abelian and every element of $G_{L/K}$ has order dividing m.*

2. *Let*

$$S = \{v \in M_K^0\colon E \text{ has bad reduction at } v\} \cup \{v \in M_K^0\colon v(m) \neq 0\} \cup M_K^\infty.$$

   The L/K is unramified outside S, i.e., if $v \in M_K$ and $v \notin S$, then L/K is unramified at v.

Note. M_K^0 is a set of finite places of K. M_K^∞ is a set of infinite places of K.

Remark. If a local field is unramified, its set valuation, $V(L) = \{V(x)\colon x \in L\}$, is equivalent to the set valuation of K, $V(L) = V(K)$. In other words, the inertia group acts trivially on the field. If we look over the complex plane, $\mathbb{C}$, there is no notion of bad reduction. If we look over the real plane, $\mathbb{R}$, there are torsion points.

Proof. 1. First, we want to show that L is Galois. Take $P \in [m]^{-1}E(K)$, we want to know that all of their Galois conjugates are also in L. $mP = Q \in E(K)$; note that this is just some polynomial relation in $X(P)$ and $Y(P)$. So if we look at $mP^\sigma = Q^\sigma = Q$ (because Q is defined over E), we see that if we take X, Y coordinate of P and apply σ, Galois element, we get P^σ which also has the same properties. This implies that L is

Galois.
Once we know that L is Galois, we are then able to use the fact of perfect pairing to prove that it is actually abelian and m-torsion. By perfect pairing, we know that there is an injection from $G_{L/K} \hookrightarrow Hom(E(K)/mE(K), E[m])$. Since $Hom(E(K)/mE(K), E[m])$ is an abelian group with m-torsion, $G_{L/K}$ is also m-torsion abelian group.

2. Take $v \notin S$, we want to show that the inertia group, I_v, acts trivially on L. So if we take $P \in [m]^{-1}E(K)$ and $\sigma \in I_v$, then we need to show that $P^\sigma = P$. Consider this as $mP = Q \in E(K_v)$, in particular, because $v \notin S$, v is in place with good reduction. This means we have the following exact sequence by Proposition 3.6.3:

$$0 \to E_1(K_v) \to E_0(K_v) \to \tilde{E}(K) \to 0$$

where $E_0(K_v) = E(K(v))$, because of good reduction.
$[m]^{-1}(Q) = P_1, P_2, ..., P_{m^2} \in E(\overline{K_v})$. Since v does not divide by m, and $\tilde{E}(L)$ has full m-torsion, $\tilde{P}_i \in \tilde{E}(\overline{K})$ are distinct elements of $\tilde{E}(\overline{K})$. Because of definition, inertia group is subgroup of Galois group that fixes elements modulo maximum ideal, we know that I_v acts trivially on $\tilde{E}(\overline{K})$. And $P_1^\sigma \neq P_i$ for $i \neq 1$. Therefore, L is unramified outside of S.

□

Now, we want to show that by having the above properties, L is finitely generated.

Proposition 4.1.7. *K is a number field and $\mu_m \subset K$ (μ is m^{th} root of unity). S is a finite set of places. L is an m-torsion abelian extension of K, unramified outside of S. Then, $[L : K]$ is finite.*

In addition, by Proposition 4.1.7, we have explicit bounds of extension as conclusion. And along with Proposition 4.1.6, we can combine with Kummer pairing and conclude that $E(K)/mE(K)$ is finite.

Proof. To show that $[L : K]$ is finite, we need to show an injection to a finite group, $Hom(G_{L/K}, \mathbb{Z}/m\mathbb{Z})$. In particular, by Galois Theory, kernel of such a homomorphism defines a cyclic m-torsion extension of K, unramified outside of S.

Remark. Kummer Theory
Since we have all m^{th} roots of unity, that any m-torsion extension of K is $K(x^{\frac{1}{m}})$ for some $x \in K^*/(K^*)^m$.

Now, we want to see that when is $K(x^{\frac{1}{m}})/K$ unramified at finite place v. We can look at extension $K_v(x^{\frac{1}{m}})/K_v$ and the valuation of x. Because there cannot be any wild ramification, $K_v(x^{\frac{1}{m}})$ will be ramified if and only if $v(x) \neq 0 \bmod m$. If $v(x) = 1$, then $v(x^{\frac{1}{m}}) = \frac{1}{m}$.

Since its valuation is not an integer, by definition, it is a ramified extension. Then, we need to show that $K^*_{m,s}/(K^*)^m$ is finite, where

$$K^*_{m,s} = \{x \in K^* \ \forall\ v \neq S \text{ and } v_v(x) = 0 \bmod m\}.$$

because the x where $K(x^{\frac{1}{m}})$ is unramified outside of S must have x in $K_{m,s}$. Now, we want to show that map below is finite:

$$\begin{aligned} K^*_{m,s}/(K^*)^m &\to (\mathbb{Z}/m)^{S-\infty places} \\ x &\mapsto v_0(x) \bmod m, \end{aligned}$$

where $v \in S$.
Even though the map,

$$K^*_{m,s}/(K^*)^m \to (\mathbb{Z}/m)^{S-\infty places},$$

is clearly finite, it suffices to consider the kernel. The kernel must map into fractional ideals mod m, which are just m^{th} power.

$$\begin{aligned} K^*_m/(K^*)^m &\to \text{principle ideals mod } m/(K^*)^m, \\ x &\mapsto (x). \end{aligned}$$

So, there's a bijection of the unit group:

$$\mathcal{O}^*_K/(K^*)^m = \mathcal{O}^*_K/((\mathcal{O})K^*)^m$$

is finite by the structure of unit group. Therefore, $K^*_{m,s}/(K^*)^m$ is finite. □

Recall that the Weak Mordell-Weil Theorem states that $E(K)/mE(K)$ is a finite group.

Proof. Weak Mordell-Weil Theorem
Let $L = K([m]^{-1}E(K))$ be defined as Proposition 4.0.5. Since $E[m]$ is finite, by perfect pairing, $E(K)/mE(K) \times G_{L/K} \to E[m]$ shows that $G_{L/K}$ is finite if and only if $E(K)/mE(K)$ is finite. By Proposition 4.0.7, if L/K is abelian and m-torsion Galois group, with S finite set of places, and L is unramified outside of S. Then by Proposition 4.0.8, if L is an m-torsion abelian extension of K with S finite set of places, as stated as the result of Proposition 4.0.7, then $[L\colon K]$ is finite. Thus by perfect pairing, $E(K)/mE(K)$ is finite. □

4.2 DESCENT STEP

In the second part of the proof, we use the height functions to show the boundedness of the group. In other words, we want to show that on an elliptic curve over a number field, there exists a height function which bounds the number of elements that are divisible by m. By definition, heights function is the measure of arithmetic complexity of points.

Theorem 4.2.1. *Descent Theorem*
Let A be an abelian group. Supoose there exists a height function

$$h\colon A \to \mathbb{R}$$

with the following properties:

1. *Let $Q \in A$. There is a constant C_1, depending on A and Q, such that*

$$h(P+Q) \leq 2h(P) + C_1 \; forall \; P \in A$$

2. *There are an integer $m \geq 2$ and a constant C_2, depending on A, such that*

$$h(mP) \geq m^2 h(P) - C_2 \; \forall \; P \in A$$

3. *For every constant C_3, the set $\{P \in A\colon h(P) \leq C_3\}$ is finite.*

If A/mA is finite for some m, then A is finitely generated.

Proof. Let $Q_1, ...Q_r \in A$ be the finitely many cosets in A, and an arbitrary $P \in A$. We want to show that P and a linear combination of Q_i's have difference of multiple of a point whose height is smaller than a constant which is independent of P. Then we will show that Q_i's and the finitely many points with heights less than that constant are generators of A. First, we write P as follows,

$$P = mP_1 + Q_{i_1} \text{ for some } 1 \leq i_1 \leq r.$$

Then we do the same with P_1, P_2, etc.

$$\begin{gathered} P = mP_1 + Q_{i_1} \\ P_1 = mP_2 + Q_{i_2} \\ \dots \\ P_{n-1} = mP_n + Q_{i_n} \end{gathered}$$

By Theorem 4.2.1, part 2, for any index j,

$$\begin{gathered} h(P_j) \leq \tfrac{1}{m^2}(h(mP_j) + C_2) \\ = \tfrac{1}{m^2}(h(P_{j-1} - Q_{i_j}) + C_2) \\ \leq \tfrac{1}{m^2}(2h(P_{j-1} + C_1' + C_2) \end{gathered}$$

where C_1' is the maximum of the constants from Theorem 4.2.1, part 1, for $Q \in \{-Q_1, ..., -Q_r\}$. Realize that C_1' and C_2 do not depend on P. Then we use this inequality again and again, to work back to P.

$$\begin{gathered} h(P_n) \leq (\tfrac{2}{m^2})^n h(P) + (\tfrac{1}{m^2} + \tfrac{2}{m^2} + \tfrac{4}{m^2} + \dots \tfrac{2^{n-1}}{m^2})(C_1' + C_2) \\ < (\tfrac{2}{m^2})^n h(P) + \tfrac{C_1' + C_2}{m^2 - 2} \\ \leq \tfrac{1}{2^n} h(P) + \tfrac{1}{2}(C_1' + C_2) \\ \text{since } m \geq 2. \end{gathered}$$

Then if n is large enough, then

$$h(P_n) \leq 1 + \tfrac{1}{2}(C_1' + C_2)).$$

And clearly, since P is a linear combination of P_n and Q_i's, every P in A is a linear combination of points in the set

$$\{Q_1, ...Q_r\} \cup \{Q \in A : h(Q) \leq 1 + \tfrac{1}{2}(C_1' + C_2)\}$$

Therefore, by Theorem 4.2.1, part 3, A is finitely generated. □

The following definitions will help us understand the height function over the field $\mathbb{Q}$. discussed in Theorem 4.2.1.

In general the height function of a rational number is simply the maximum number between denominator and numerator.

Definition 4.2.2. *Let $t \in \mathbb{Q}$, and $t = \frac{p}{q}$ as a fraction in lowest terms. The height of t is defined by,*

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

Definition 4.2.3 states the height function defined over $E(\mathbb{Q})$.

Definition 4.2.3. *The (logarithmic) height on $E(\mathbb{Q})$, relative to the given Weierstrass equation, is the function*

$$h_x : E(\mathbb{Q}) \to \mathbb{R},$$
$$h_x(P) = \begin{cases} log\ H(x(P)) & if\ P \neq \mathcal{O}, \\ 0 & if\ P = \mathcal{O}. \end{cases}$$

Lastly, we will need the Descent Theorem applied to the field, $E(\mathbb{Q})$ to complete the proof.

Lemma 4.2.4. *1. Take $P_0 \in E(\mathbb{Q})$. There is a constant C_{P_0} such that*

$$h(P + P_0) \leq 2h(P) + C_{P_0} \ \forall\ P \in E(\mathbb{Q}).$$

2. There is a constant C_2 such that

$$h(2P) \geq 4h(P) - C \ \forall\ P \in E(\mathbb{Q}).$$

3. For any $C_3 \in \mathbb{R}$, the set $\{P \in E(\mathbb{Q}) | h(P) \leq D\}$ is finite.

Theorem 4.2.5. *Mordell-Weil*
$E(\mathbb{Q})$ is finitely generated.

Proof. By the Weak Mordell-Weil Theorem and Lemma 4.2.4, $E(\mathbb{Q})$ and h_x satisfy the hypothesis conditions of Theorem 4.2.1 (Descent Theorem) at $m = 2$. Therefore, the result from Lemma 4.2.4 shows that $E(\mathbb{Q})$ is finitely generated. Thus completes the proof of Mordell-Weil Theorem. □