

The Birch and Swinnerton-Dyer Conjecture for Elliptic Curves



Duncan Smith

Department of Mathematics
and Applied Mathematics

University of the Western Cape

A thesis submitted for the degree of

Master of Science

October 2014



UNIVERSITY *of the*
WESTERN CAPE

To Farzana and Olga...



UNIVERSITY *of the*
WESTERN CAPE

Declaration

I declare that **The Birch and Swinnerton-Dyer Conjecture for Elliptic Curves** is my own work, that it has not been submitted before for any degree or examination in any other university, and that all the sources I have used or quoted have been indicated and acknowledged as complete reference.

Duncan Alfred Smith

October 2014

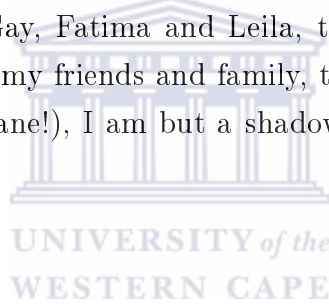
Signed:.....



Acknowledgements

My greatest thanks to my supervisor, Dr Rafiq Omar, for his infinite patience and wisdom. He always has an open door for any mathematical problem I may have, and explains it away succinctly with a smile on his face. To Prof Eric and Prof Patidar, many thanks for your advice over the years, it is immensely appreciated.

To my colleagues Gay, Fatima and Leila, thank you for putting up with my antics. To my friends and family, thank you for keeping me level headed (and sane!), I am but a shadow of myself without your support.



Abstract

The Birch and Swinnerton-Dyer Conjecture for Elliptic Curves

D. A. Smith

MSc Thesis, Department of Mathematics and Applied Mathematics,
The University of the Western Cape

The aim of this dissertation is to provide an exposition of the Birch and Swinnerton-Dyer Conjecture, considered by many to be one of the most important unsolved problems in modern Mathematics.

A review of topics in Algebraic Number Theory and Algebraic Geometry is provided in order to provide a characterisation for elliptic curves over rational numbers. We investigate the group structure of rational points on elliptic curves, and show that this group is finitely generated by the Mordell-Weil Theorem.

The Shafarevich-Tate group is introduced by way of an example. Thereafter, with the use of Galois Cohomology, we provide a general definition of this mysterious group. We also discuss invariants like the regulator and real period, which appear in the Birch and Swinnerton-Dyer Conjecture.

After defining the L -function, we state the Birch and Swinnerton-Dyer Conjecture and discuss results which have been proved and some consequences. We discuss numerical verification of the Conjecture, and show some computations, including an example of our own.

The Birch and Swinnerton-Dyer Conjecture for Elliptic Curves

Duncan A. Smith

KEYWORDS

Elliptic Curve

Mordell-Weil Theorem

Rank

Shafarevich-Tate group

L -function

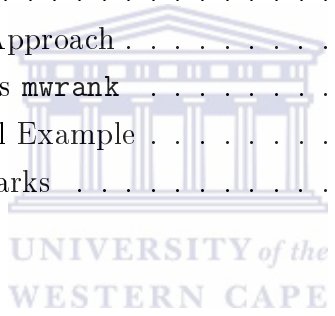
Birch and Swinnerton-Dyer Conjecture



Contents

Contents	vi
1 Introduction	1
2 Preliminaries	4
2.1 Unit Theorem and Class Group	4
2.2 p -adic Integers and p -adic Numbers	11
2.2.1 Absolute Values, Norms and Valuations	11
2.2.2 p -Adic Numbers and p -Adic Integers	18
2.3 Algebraic Varieties	20
2.3.1 Affine and Projective Varieties	20
2.3.2 Maps Between Varieties	25
2.3.3 Maps Between Curves	26
2.3.4 Divisor Group	28
3 Elliptic Curves	33
3.0 Elliptic Curves	34
3.1 Group Structure of Elliptic Curves	39
3.2 Intersection of Two Quadratic Surfaces	48
3.3 Minimal Normal Form of an Elliptic Curve	51
3.4 Reduction Modulo p	53
3.5 The Torsion Subgroup	58
3.5.1 Computing the Torsion Subgroup	59
3.6 Finite Basis for an Elliptic Curve	62
3.6.1 Mordell's Theorem	62

3.6.2	Defining the Regulator	66
3.6.3	Numerical Example	68
3.7	The Shafarevich-Tate Group	70
3.7.1	A First Look at III	71
3.7.2	An Example of a Nontrivial III	73
3.7.3	Galois Cohomology	79
3.8	Elliptic Curves over \mathbb{C}	89
4	The Birch and Swinnerton-Dyer Conjecture	92
4.1	The Birch and Swinnerton-Dyer Conjecture	93
4.2	Discussion and Comments	97
4.3	Computations	99
4.3.1	General Approach	99
4.3.2	Cremona's m rank	101
4.3.3	Numerical Example	106
4.4	Concluding Remarks	109
	Bibliography	111



Chapter 1

Introduction

The study of Diophantine equations, named after Diophantus of Alexandria, involves finding solutions to polynomial equations in integers or rational numbers. Geometrically, linear and quadratic equations in two variables are curves with genus 0. In the simplest case, linear equations can be solved using the Euclidean algorithm. With the use of the Hasse-Minkowski Theorem, a quadratic equation will have a solution in \mathbb{Q} if and only if it has a solution in every p -adic completion of \mathbb{Q} . If there are solutions to quadratic equations, by Hensel's Lemma and quadratic reciprocity, we can piece together all the local information to obtain results for the global field \mathbb{Q} . Thus, the matter of finding solutions to curves of genus 0 is largely settled. The next simplest case considers curves of genus 1. The study of these curves, which are given by cubic equations in two variables, is known as the theory of elliptic curves.

The theory of elliptic curves is a subject where various branches of mathematics such as number theory, complex analysis, algebraic geometry and representation theory converge. One important aspect is the group of rational points found on an elliptic curve. Work by Louis Mordell, and extensions thereof to abelian varieties by Andre Weil, have proven that this group of rational points is finitely generated. The number of these generators is known as the arithmetic rank of the elliptic curve. Currently, there is no known algorithm which is guaranteed to terminate when calculating the rank of an elliptic curve. This shortcoming led Birch and Swinnerton-Dyer in formulating their famous Conjecture.

Brian Birch and Peter Swinnerton-Dyer investigated numerous elliptic curves of a special form. Their computations resulted in the Birch and Swinnerton-Dyer Conjecture, or BSD Conjecture for short. There are two versions:

BSD 1 relates the arithmetic rank of an elliptic curve to its L -function,

BSD 2 provides a formula for the residue of the Taylor series of its L -function in terms of several arithmetic invariants of an elliptic curve.

The main aim of this dissertation is to give an exposition of this important, complex and fascinating Conjecture. Its significance is underlined by its being selected as one of the Millennium Prize Problems by the Clay Mathematics Institute. A secondary aim will be to present a few computations using established software packages such as the **SAGE** platform.

The exposition requires a review of a few essential topics in Algebra, Algebraic Number Theory and Algebraic Geometry as preliminaries; these topics are necessary for a brief account of the basic theory of elliptic curves. We then present, in more detail, those topics in the theory of elliptic curves which are necessary for understanding the BSD Conjecture. Key to this is the Shafarevich-Tate group, an altogether complex and mysterious object in the theory of elliptic curves, which represents a substantial part of the exposition.

In Chapter Two we discuss topics in Algebra, Algebraic Number Theory and Algebraic Geometry. The main topics covered are the Unit Theorem and the Class Number Formula; p -adic integers, numbers and valuations; and Algebraic Varieties. Results are generally stated without proof, but we do give a few proofs of results which are deemed to provide more insight into a subject central to the theory of elliptic curves.

Chapter Three covers the basic theory of elliptic curves, as well as giving an account of more specialised topics which are essential to the BSD Conjectures. These include the Mordell-Weil Theorem, the Shafarevich-Tate Group and elliptic curves over the complex numbers, among others. Our approach in this chapter

is to use explicit equations, as we would like to give concrete examples of some concepts.

Chapter Four focuses on the Birch and Swinnerton-Dyer Conjecture (BSD for short). We introduce the L -function followed by the full statement of the BSD conjecture. We then note developments which have verified the Birch and Swinnerton-Dyer Conjecture in certain cases. Thereafter, we perform calculations to verify the first BSD conjecture for a particular elliptic curve, and then predict the order of the Shafarevich-Tate group of this curve with the use of second BSD conjecture. We conclude the dissertation with a discussion of a few recent developments.



Chapter 2

Preliminaries

This chapter discusses certain topics in Algebra, Algebraic Number Theory and Algebraic Geometry which are used in subsequent chapters. Results within this chapter are generally stated without proof; proofs that have been provided will fall into two categories:

1. proofs that provide a deeper understanding of a result which is central to a later section(s), or
2. proofs which have been left as exercises in their respective sources, e.g. Lemma 2.1.

2.1 Unit Theorem and Class Group

We review basic concepts in Algebraic Number Theory in order to discuss the Unit Theorem and the ideal Class Group. The Unit Theorem and ideal Class Group will be used in Section 3.6.1 to show that the group of rational points on an elliptic curve is finitely generated. In Chapter 4, we will remark on their analogy to the Second Birch and Swinnerton-Dyer Conjecture.

The following section is sourced from [9] and [17].

All rings are commutative with 1.

Definition 1. A ring is *Noetherian* if every ideal is finitely generated.

Remark. It follows that a factor ring of a Noetherian ring is Noetherian.

Proposition 1 ([9], X §1). *Let R be Noetherian. Any nonempty set of ideals contains a member which is maximal for inclusion. If R is nonzero, then it contains a maximal ideal.*

Definition 2. For an ideal I in a ring R , the *radical* is

$$\sqrt{I} = \{a \in R \mid a^n \in I \text{ for some } n\}.$$

The *nilradical*, denoted $\sqrt{0}$, is the ideal which contains all elements $x \in R$ such that $x^n = 0$ for some positive integer n . A ring is said to be *reduced* if $\sqrt{0} = 0$.

Proposition 2 ([9], X). *Let R be a Noetherian ring. The radical of an ideal I is the intersection of all prime ideals containing I . High powers of the radical are contained in the ideal itself*

$$(\sqrt{I})^s \subset I.$$

Theorem 1 ([9], IV §4.). *Let R be a Noetherian ring. The ring of polynomials $R[T]$ is Noetherian.*

Definition 3. Let K be a field. For an ideal I of the ring of polynomials $K[T_1, \dots, T_n]$ the factor ring $K[T_1, \dots, T_n]/I$ is an *affine ring*.

Theorem 2 (Hilbert's Basis Theorem). *An affine ring is Noetherian.*

Proof. Follows from Theorem 1. □

Definition 4. Let R be a ring. An element $b \in R$ is said to be *integral* over a subring A of R if it is a root of a monic polynomial whose coefficients are elements of A , i.e.

$$b^n + a_{n-1}b^{n-1} + \dots + a_1b + a_0 = 0,$$

where $n \geq 1$, and $a_i \in A$ for each $i = 0, 1, \dots, n - 1$.

Definition 5. Elements of R which are not roots of polynomials with coefficients in A are called *transcendental* over A .

Denote the *integral closure* $\mathcal{O} = \mathcal{O}_R$ as the set of all integral elements contained in R , that is $\mathcal{O} = \{b \in R \mid b \text{ is integral over some subring } A \text{ of } R\}$. The set with operators $(\mathcal{O}, +, *)$ satisfies all ring properties, where $+$ and $*$ are the additive and multiplicative operators on R , hence \mathcal{O} is referred to as the *ring of integers* of R .

Suppose K and A are fields with $A \subset K$. We say that K is an *extension field* of A . We may view K as a vector space over A , and we say that K is a *finite* or *infinite* extension of A depending on whether the dimension of the vector space is finite or infinite.

If K is a finite extension of A , then the *degree* of K over A is the dimension of K as a vector space over A .

Definition 6. A *number field* is a finite extension of the field of rational numbers.

Definition 7. A subset S of K is *algebraically independent* over a subfield A of K if the elements of S consists solely of elements transcendental over A .

Define an ordering among algebraically independent subsets of K by ascending inclusion. These subsets are inductively ordered, and thus there exist maximal elements.

Definition 8. Let S be a subset of K which is algebraically independent over A . If the cardinality of S is greatest among all such subsets, then we call this cardinality the *transcendence degree (or dimension)* of K over A .

Definition 9. Let K be a number field. An element $\alpha \in K$ is an *algebraic number* if it is a root of some polynomial with coefficients in \mathbb{Q} . If α is a root of a monic polynomial with coefficients in \mathbb{Z} , then we say that it is an *algebraic integer*.

Definition 10. Let K be a field with $\alpha \in K$. The *minimal polynomial* of $\alpha \in K$ is the monic polynomial $f(X) \in K[X]$ of least positive degree such that $f(\alpha) = 0$.

Definition 11. Let K be a field. A polynomial $f(X) \in K[X]$ is said to be *separable* if it has no multiple roots.

Definition 12. Let K be an algebraic extension of A . We say that K is a *separable extension* of A if, for every $\alpha \in A$, the minimal polynomial of α over K is separable.

Remark. If K is not a separable extension of A , then it is called an *inseparable extension* of A . Moreover, if A has characteristic n and every element of K is a root of an equation of the form $x^m = a$, with m a power of n and $a \in A$, then we say that K is a *purely inseparable extension* of A .

Lemma 1 ([17], V §1). *If α is an algebraic integer, then the minimal polynomial of α has coefficients in \mathbb{Z} .*

Definition 13. The ring of integers of a number field K is the ring

$$\mathcal{O}_K = \{x \in K \mid x \text{ is an algebraic integer}\}.$$

Lemma 2 ([17] V §1). *Let \mathcal{O} be the ring of integers of a number field K . Then $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$ and $\mathbb{Q}\mathcal{O} = K$, where $\mathbb{Q}\mathcal{O}$ is the extension of \mathbb{Q} by \mathcal{O} .*

Proposition 3 ([17] V §1). *The ring of integers \mathcal{O} of a number field K is a lattice in K , i.e., $\mathbb{Q}\mathcal{O} = K$ and \mathcal{O} is an abelian group of rank $[K : \mathbb{Q}]$.*

Corollary 1 ([17] V §1). *The ring of integers \mathcal{O} of K is Noetherian.*

Suppose $K \subset L$ is an inclusion of number fields and let $a \in L$. Then left multiplication by a defines a K -linear transformation $\ell_a : L \rightarrow L$.

Definition 14. The *norm* and *trace* from L to K are

$$N_{L/K}(a) = \text{Det}(\ell_a) \quad \text{and} \quad \text{tr}_{L/K}(a) = \text{tr}(\ell_a).$$

Determinants and traces are multiplicative and additive respectively, so for $a, b \in L$ we have

$$N_{L/K}(ab) = N_{L/K}(a) \cdot N_{L/K}(b)$$

and

$$\text{tr}_{L/K}(a + b) = \text{tr}(a) + \text{tr}(b).$$

Definition 15. An integral domain R is *integrally closed in its field of fractions* if whenever α is in the field of fractions of R and α satisfies a monic polynomial $f \in R[x]$, then $\alpha \in R$.

Proposition 4 ([17] VI §1). *If K is any number field, then \mathcal{O}_K is integrally closed. In particular, the ring \mathbb{Z} of all algebraic integers is integrally closed.*

Definition 16. An integral domain R is a *Dedekind domain* if it is Noetherian, integrally closed in its field of fractions, and every nonzero prime ideal of R is maximal.

Proposition 5 ([17] VI §1). *The ring of integers \mathcal{O} of a number field is a Dedekind domain.*

Definition 17. A *fractional ideal* is an \mathcal{O} -submodule of $I \subset K$ that is finitely generated as an \mathcal{O} -module.

Lemma 3 ([17] VI). *Let I be a non-zero ideal of \mathcal{O} . Then there exist prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_\tau$ of \mathcal{O} such that*

$$\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_\tau \subset I.$$

Let P_K denote the subgroup of the fractional ideal I_K formed by the principal ideals, i.e. ideals of the form $\alpha \mathcal{O}_K, \alpha \in K^\times$.

Definition 18. The ideal class group, denoted by $\text{Cl}(K)$, is

$$\text{Cl}(K) = I_K / P_K.$$

Definition 19. Let $B \subset A$ be rings, and assume B is free of rank m as an A -module. Let β_1, \dots, β_m be elements of B . We define their *discriminant* to be

$$D(\beta_1, \dots, \beta_m) = \det(\text{tr}_{B/A}(\beta_i, \beta_j)).$$

Theorem 3 (Finiteness of the Ideal Class Group, [14] IV §1). *Let K be a number field with discriminant Δ_K . Then:*

(a) *there exists a constant $C = C(r_1, r_2) > 0$ such that every ideal class contains an integral ideal whose norm is at most*

$$C \sqrt{|\Delta_K|}.$$

(b) The group $\text{Cl}(K)$ is finite.

Definition 20. The *class number*, denoted by h_K , is the cardinality of $\text{Cl}(K)$.

Definition 21. The group of units \mathcal{O}^* associated to a number field K is the group of elements of \mathcal{O}_K that have an inverse in \mathcal{O}_K .

Proposition 6 ([17], XII). *An element $a \in \mathcal{O}$ is a unit if and only if $N_{K/\mathbb{Q}}(a) = \pm 1$.*

Let r be the number of real embeddings and s the number of complex conjugate embeddings of K into \mathbb{C} , so $n = [K : \mathbb{Q}] = r + 2s$. Define a map

$$\phi : \mathcal{O}^* \rightarrow \mathbb{R}^{r+s}$$

by

$$\phi(a) = (\log|\sigma_1(a)|, \dots, \log|\sigma_{r+s}(a)|).$$

Lemma 4 ([17], XII). *The image of ϕ lies in the hyperplane*

$$H = \{(x_1, \dots, x_{r+s}) \in \mathbb{R}^{r+s} : x_1 + \dots + x_r + 2x_{r+1} + \dots + 2x_{r+s} = 0\}.$$

Lemma 5 ([17], XII). *The kernel of ϕ is finite.*

Lemma 6 ([17], XII). *The kernel of ϕ is a finite cyclic group.*

Proof. Let G be a finite subgroup of the multiplicative group of a field K . Choose n as the maximum of the orders of the elements in G . Hence, $g^n = 1$ for all $g \in G$, and by extension every element of G is a root of the monic polynomial $x^n - 1 = 0$, which has at most n roots. Thus $|G| \leq n$. Conversely, by Lagrange's theorem n divides $|G|$, so $n \leq |G|$. Hence $|G| = n$. Finally, G contains an element of order $|G|$, so G is cyclic. \square

We define an embedding

$$\sigma : K \hookrightarrow \mathbb{R}^n$$

given by $\sigma(x) = (\sigma_1(a), \dots, \sigma_{r+s}(a))$ where we view $\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$ by way of $a + bi \mapsto (a, b)$.

Lemma 7 ([17], XII). *The image of ϕ is discrete in \mathbb{R}^{r+s} .*

Theorem 4 (Dirichlet's Unit Theorem). *The group \mathcal{O}^* is the product of a finite cyclic group of roots of unity with a free abelian group of rank $r + s - 1$, where r is the number of real embeddings of K and s is the number of complex conjugate pairs of embeddings.*

Explicitly,

$$\mathcal{O}_K^* \cong \mathbb{Z}^{r_1+r_2-1} \times \mu(\mathcal{O}_K).$$



2.2 p -adic Integers and p -adic Numbers

We discuss the basic theory of the p -adics which, as we will see in subsequent chapters, play a significant role in the theory of elliptic curves. Most of the results are stated with proofs, but we include a proof of the theorem of Ostrowski which is of fundamental importance to the completeness of \mathbb{Q}_p .

The sources used are [8] and [9].

2.2.1 Absolute Values, Norms and Valuations

Definition 22 ([8] I, §1). Let X be a nonempty set. A metric d on X is a function $d : X \times X \rightarrow \mathbb{R}_{\geq 0}$ satisfying

M 1. $d(x, y) = 0 \iff x = y.$

M 2. $d(x, y) = d(y, x).$

M 3. $d(x, y) \leq d(x, z) + d(z, y)$ for all $z \in X.$

A set X possessing a metric d is called a metric space and we may write the pair as (X, d) .

Definition 23 ([9] XII, §1). Let K be a field. An *absolute value* on K is a real-valued function $x \mapsto |x|_v$ on K satisfying the following three properties:

AV 1. We have $|x|_v \geq 0$ for all $x \in K$, and $|x|_v = 0$ if and only if $x = 0$.

AV 2. For all $x, y \in K$, we have $|xy|_v = |x|_v |y|_v.$

AV 3. For all $x, y \in K$, we have $|x + y|_v \leq |x|_v + |y|_v.$

If instead of **AV 3** the absolute value satisfies the stronger condition

AV 4. $|x + y|_v \leq \max(|x|_v, |y|_v)$

then we shall say that it is a valuation, or that it is non-archimedean. Note that $(F, |\cdot|_v)$ satisfies all conditions of a metric space if we define $d(x, y) = |x - y|_v.$

Definition 24 ([9] XII, §2). Let K be a field with non-trivial absolute value $|\cdot|_K$, and let V be a vector space over K . A *norm* on V (compatible with $|\cdot|_K$) is a function $\|\cdot\| : V \rightarrow \mathbb{R}$ satisfying

N 1. $\|x\| \geq 0 \forall x \in V$, and $\|x\| = 0 \iff x = 0$.

N 2. For $a \in K, x \in V$ we have $\|ax\| \leq |a|_K \|x\|$.

N 3. $\|x + y\| \leq \|x\| + \|y\|$.

As with the absolute value, the norm $\|\cdot\|$ is called *non-archimedean* if the triangle inequality (**N 3**) can be replaced by the stronger *ultrametric inequality*

$$\|x + y\| \leq \max(\|x\|, \|y\|) \text{ for } x, y \in X.$$

A norm not satisfying the ultrametric inequality is called *archimedean*.

Remark. If we view a field K endowed with absolute value $|\cdot|_K$ as a vector space over itself, then $|\cdot|_K$ is clearly a norm on K .

Let p be a rational prime. Given any nonzero integer a , let $\text{ord}_p a$ be the highest power of p which divides a , i.e. the greatest m such that $a \equiv 0 \pmod{p^m}$. For a rational number $x = \frac{a}{b}$, define $\text{ord}_p x$ to be $\text{ord}_p a - \text{ord}_p b$. We define a map $|\cdot|_p : \mathbb{Q} \rightarrow \mathbb{R}_{\geq 0}$ as follows:

$$|x|_p = \begin{cases} \frac{1}{p^{\text{ord}_p x}}, & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases}$$

Proposition 7 ([8] I, §1). $|\cdot|_p$ is a norm on \mathbb{Q} .

Proof. If $x = 0$ or $y = 0$, or if $x + y = 0$ then property (3) is trivial, so assume x, y and $x + y$ are all nonzero. Let $x = \frac{a}{b}$ and $y = \frac{c}{d}$ in lowest terms. Then we have

$$x + y = \frac{ad + bc}{bd},$$

with

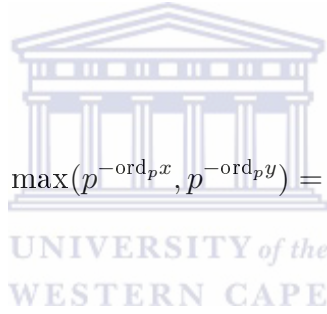
$$\text{ord}_p(x + y) = \text{ord}_p(ad + bc) - \text{ord}_p b - \text{ord}_p d.$$

The highest power of p which divides the sum of two numbers is at least the minimum of the highest power dividing the first and the highest power dividing the second, thus

$$\begin{aligned} \text{ord}_p(x + y) &\geq \min(\text{ord}_p ad, \text{ord}_p bc) - \text{ord}_p b - \text{ord}_p d \\ &= \min(\text{ord}_p a + \text{ord}_p d, \text{ord}_p b + \text{ord}_p c) - \text{ord}_p b - \text{ord}_p d \\ &= \min(\text{ord}_p a - \text{ord}_p b, \text{ord}_p c - \text{ord}_p d) \\ &= \min(\text{ord}_p x, \text{ord}_p y) \end{aligned}$$

Therefore

$$|x + y|_p = p^{-\text{ord}_p(x+y)} \leq \max(p^{-\text{ord}_p x}, p^{-\text{ord}_p y}) = \max(|x|_p, |y|_p) \leq |x|_p + |y|_p.$$



□

Remark. From the final line in the proof above we see that the norm $|\cdot|_p$ is non-archimedean on \mathbb{Q} .

Let $\{x_n\}$ be a sequence in a metric space $(X, |\cdot|)$.

Definition 25. A sequence is said to be *Cauchy* if, given $\epsilon > 0$, there exists an integer N , dependent on ϵ , such that whenever we have integers $m, n > N$ then

$$|x_m - x_n| < \epsilon.$$

Definition 26. Two metrics d_1 and d_2 are said to be *equivalent* if a sequence is Cauchy with respect to d_1 if and only if it is Cauchy with respect to d_2 . We say two norms are *equivalent* if they induce equivalent metrics.

Theorem 5 (Ostrowski, [8] I §1). *Every nontrivial norm $\|\cdot\|$ on \mathbb{Q} is equivalent to $|\cdot|_p$ for some prime $p \leq \infty$.*

Proof. Case(i). Suppose there exists a positive integer n such that $\|n\| > 1$. Let n_0 be the least such n . Since both $n_0, \|n_0\| > 1$, we can find a positive real number α such that $\|n_0\| = n_0^\alpha$ (simply set $\alpha = \frac{\log \|n_0\|}{\log n_0}$, where both the numerator and denominator are positive since $n_0, \|n_0\| > 1$). We write any positive integer n to the base n_0 ,

$$n = a_0 + a_1 n_0 + \cdots + a_s n_0^s,$$

where $0 \leq a_i \leq n_0$ and $a_s \neq 0$. Then

$$\begin{aligned} \|n\| &< \|a_0\| + \|a_1 n_0\| + \cdots + \|a_s n_0^s\| \\ &= \|a_0\| + \|a_1\| \cdot n_0^\alpha + \cdots + \|a_s\| \cdot n_0^{s\alpha}. \end{aligned}$$

We have that $a_i < n_0$ for each i , by our choice of n_0 we have $\|a_i\| \leq 1$, thus

$$\begin{aligned} \|n\| &\leq 1 + n_0^\alpha + n_0^{2\alpha} + \cdots + n_0^{s\alpha} \\ &= n_0^{s\alpha} (1 + n_0^{-\alpha} + \cdots + n_0^{-s\alpha}) \\ &\leq n_0^{s\alpha} \left[\sum_{i=0}^{\infty} \left(\frac{1}{n_0^\alpha} \right)^i \right], \end{aligned}$$

as $n \geq n_0^s$. The summation in brackets is a finite positive constant, so we may denote it as C . Thus,

$$\|n\| \leq C n^\alpha \quad \text{for all } n = 1, 2, 3, \dots$$

Take any n with any large N , and replace n by n^N in the above inequality; then take N th roots. This results in

$$\|n\| \leq \sqrt[N]{C} n^\alpha.$$

Letting $N \rightarrow \infty$ for n fixed gives $\|n\| \leq n^\alpha$.

We now show that $\|n\| \geq n^\alpha$.

We have $n_0^{s+1} > n \geq n_0^s$. Since $\|n_0^{s+1}\| = \|n + n_0^{s+1} - n\| \leq \|n\| + \|n_0^{s+1} - n\|$, we

have

$$\begin{aligned} \|n\| &\geq \|n_0^{s+1}\| - \|n_0^{s+1} - n\| \\ &\geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n)^\alpha, \end{aligned}$$

since $\|n_0^{s+1}\| = \|n_0\|^{s+1}$. Using $\|n\| \leq n^\alpha$ on the term that is subtracted results in

$$\begin{aligned} \|n\| &\geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n)^\alpha \\ &= n_0^{(s+1)\alpha} \left[1 - \left(1 - \frac{1}{n_0} \right)^\alpha \right] \\ &\geq C' n^\alpha \end{aligned}$$

for some constant $C'(n_0, \alpha)$ independent of n . As before, we introduce a large integer N , take N th roots, and let $N \rightarrow \infty$ to derive $\|n\| \geq n^\alpha$.

Thus $\|n\| = n^\alpha$.

We may now proceed to investigate the rationals.

For any $x \in \mathbb{Q}$, with $x = \frac{a}{b}$ for integers a, b and $b \neq 0$,

$$\begin{aligned} \|x\| &= \left\| \frac{a}{b} \right\| \\ &= \|ab^{-1}\| \\ &= \|a\| \cdot \|b^{-1}\| && \text{Property N 2} \\ &= \|a\| \cdot \|b\|^{-1} \\ &= |a|^\alpha |b|^{-\alpha} \\ &= \left| \frac{a}{b} \right|^\alpha = |x|^\alpha, \end{aligned}$$

Since $\alpha > 0$, it is clear that a sequence is Cauchy with respect to $\|\cdot\|$ if and only if it is Cauchy with respect to $|\cdot|$, and hence $\|\cdot\|$ is equivalent to the usual absolute value $|\cdot|$.

Case(ii). Suppose $\|n\| \leq 1$ for all positive integers n . Let n_0 be the least n such that $\|n\| < 1$; n_0 exists since we have assumed that $\|\cdot\|$ is nontrivial.

If $n_0 = n_1 \cdot n_2$ for some integers $n_1, n_2 < n_0$, then $\|n_1\| = \|n_2\| = 1$ implying that

$\|n_0\| = \|n_1\| \cdot \|n_2\| = 1$. Thus n_0 must be prime. Let us rename it p .

We claim that $\|q\| = 1$ if q is a prime not equal to p . If not, then $\|q\| < 1$ and for some large N we have that $\|q^N\| = \|q\|^N < \frac{1}{2}$. Also, for some large M we have that $\|p^M\| < \frac{1}{2}$. Clearly, p^M and q^N are relatively prime; we can find integers m, n such that $mp^M + nq^N = 1$. It follows that

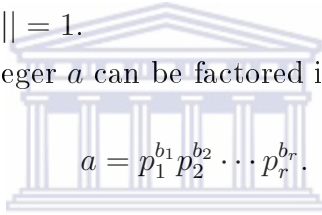
$$1 = \|1\| = \|mp^M + nq^N\| \leq \|mp^M\| + \|nq^N\| = \|m\|\|p^M\| + \|n\|\|q^N\|.$$

However $\|m\|, \|n\| \leq 1$, which implies that

$$1 \leq \|p^M\| + \|q^N\| < \frac{1}{2} + \frac{1}{2} = 1,$$

a contradiction. Hence $\|q\| = 1$.

Note that any positive integer a can be factored into prime divisors:



$$a = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}.$$

Then $\|a\| = \|p_1\|^{b_1} \cdot \|p_2\|^{b_2} \cdots \|p_r\|^{b_r}$. But the only $\|p_i\|$ which is unequal to 1 will be $\|p\|$ on the condition that one of the primes p_i is p . Its corresponding b_i will be $\text{ord}_p a$. Let $\rho = \|p\| < 1$, and

$$\|a\| = \rho^{\text{ord}_p a}.$$

□

Remark. The above theorem is an important one; essentially, every non-trivial absolute value on \mathbb{Q} is equivalent to a p -adic absolute value for some $p \leq \infty$ so we need only consider the p -adic absolute values as metrics when investigating \mathbb{Q} .

Definition 27. If K_1, K_2 are fields with absolute values $|\cdot|_1, |\cdot|_2$ respectively, we say that an isomorphism $\phi : K_1 \rightarrow K_2$ *preserves the absolute values* if for any $x \in K_1$, $|\phi(x)|_2 = |x|_1$.

Definition 28. A field K is said to be *complete* with respect to $|\cdot|$ if every Cauchy sequence with respect to $|\cdot|$ in K converges to a limit in K .

By following the blueprint of constructing \mathbb{R} from \mathbb{Q} , one can show that every field K with absolute value can be extended to a unique field \tilde{K} such that \tilde{K} is complete and every element of \tilde{K} is the limit of some Cauchy sequence in K .

Theorem 6. *Let K be a field with absolute value $|\cdot|$. There is an extension field \tilde{K} of K , unique up to absolute value-preserving isomorphism, called the completion of K , having the following properties:*

- i $|\cdot|$ can be continued to an absolute value on \tilde{K} , also denoted $|\cdot|$, such that \tilde{K} is complete with respect to $|\cdot|$;
- ii K is dense in \tilde{K} , i.e. every element of \tilde{K} is the limit of a sequence in K .

Corollary 2. *If $|\cdot|$ is a non-archimedean absolute value on K , then the extension of $|\cdot|$ to \tilde{K} is also non-archimedean.*

Remark. For a real-valued sequence $\{a_n\}$, it is not necessary for $\sum_n a_n$ to converge if $\lim_{n \rightarrow \infty} a_n = 0$. However, for the p -adics we have:

Lemma 8. *Let K be a field with respect to a non-archimedean absolute value $|\cdot|$. Let $\{a_k\}_{k=0}^{\infty}$ be a sequence in K . Then $\sum_{k=0}^{\infty} a_k$ converges in K if and only if $\lim_{k \rightarrow \infty} a_k = 0$.*

Proof. Suppose that $\alpha = \sum_{k=0}^{\infty} a_k$ converges. Then

$$a_n = \sum_{k=0}^n a_k - \sum_{k=0}^{n-1} a_k \rightarrow \alpha - \alpha = 0.$$

Conversely, suppose that $a_k \rightarrow 0$ as $k \rightarrow \infty$. Let $\alpha := \sum_{k=0}^n a_k$. Then for any integers m, n with $0 < m < n$ we have that

$$|\alpha_n - \alpha_m| = \left| \sum_{k=m+1}^n a_k \right| \leq \max(|a_{m+1}, \dots, a_n|) \rightarrow 0 \text{ as } m, n \rightarrow \infty.$$

Thus, the partial sums α_n form a Cauchy sequence, hence it must converge to a limit in K . □

Lemma 9. *Given K a field with respect to a non-archimedean absolute value $|\cdot|$. Then every series $\sum_{k=0}^{\infty} a_k$ convergent in K with respect to $|\cdot|$ is unconditionally convergent, i.e. neither the convergence nor the value of the series, are affected if the terms of a_k are rearranged.*

2.2.2 p -Adic Numbers and p -Adic Integers

Let p be prime. Let \mathbb{Q}_p be the field which is the completion of \mathbb{Q} with respect to the absolute value $|\cdot|_p$.

Lemma 10. *The value set of $|\cdot|_p$ on \mathbb{Q}_p is $\{0\} \cup \{p^m : m \in \mathbb{Z}\}$.*

The ring of p -adic integers is defined by

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

It indeed is a ring since, for any $x, y \in \mathbb{Z}_p$:

$$\begin{aligned} |x - y|_p &\leq \max(|x|_p, |y|_p) \leq 1 \\ |xy|_p &\leq 1. \end{aligned}$$

Hence, $x - y \in \mathbb{Z}_p, xy \in \mathbb{Z}_p$.

The group of invertible elements of \mathbb{Z}_p is

$$\mathbb{Z}_p^* = \{x \in \mathbb{Q}_p : |x|_p = 1\}.$$

Lemma 11. *For every $\alpha \in \mathbb{Z}_p$ and every integer m there is a unique $a_m \in \mathbb{Z}$ such that*

$$\alpha \equiv a_m \pmod{p^m}, \quad 0 \leq a_m < p^m.$$

Hence, \mathbb{Z} is dense in \mathbb{Z}_p .

We complete this section by stating Hensel's Lemma, which is use in §3.7.2.

Theorem 7 (Hensel's Lemma, [8] I §5). *Let $F(x) = c_0 + c_1x + \cdots + c_nx^n$ be a polynomial whose coefficients are p -adic integers. Let $F'(x) = c_1 + 2c_2x + 3c_3x^2 + \cdots + nc_nx^{n-1}$ be the derivative of $F(x)$. The a_0 be a p -adic integer such that*

$F(a_0) \equiv 0 \pmod{p}$ and $F'(a_0) \not\equiv 0 \pmod{p}$. Then there exists a unique p -adic integer a such that

$$F(a) = 0 \text{ and } a \equiv a_0 \pmod{p}.$$



2.3 Algebraic Varieties

In order to provide a precise definition of elliptic curves, the notion of genus is needed. We therefore sketch the basics of Algebraic Geometry so that we can state the Riemann-Roch Theorem. We shall fleetingly deal with affine and projective varieties; algebraic curves and maps between curves as such; and discuss divisors on algebraic curves. Details not covered may be found in [16].

2.3.1 Affine and Projective Varieties

We use the following notation within this subsection:

K a perfect field, i.e. every finite extension of K is separable.

\bar{K} a fixed algebraic closure of K .

$G_{\bar{K}/K}$ the Galois group of \bar{K}/K .

Definition 29. The *affine n -space over K* , which we denote by \mathbb{A}^n , is the set of n -tuples

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \{P = (x_1, \dots, x_n) \mid x_i \in \bar{K}\}.$$

Similarly, the *set of K -rational points of \mathbb{A}^n* is the set

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

The Galois group $G_{\bar{K}/K}$ acts on \mathbb{A}^n since for $\sigma \in G_{\bar{K}/K}$ and $P \in \mathbb{A}^n$,

$$P^\sigma = (x_1^\sigma, \dots, x_n^\sigma).$$

It then follows that $\mathbb{A}^n(K)$ may be characterised by

$$\mathbb{A}^n(K) = \left\{ P \in \mathbb{A}^n : P^\sigma = P \text{ for all } \sigma \in G_{\bar{K}/K} \right\}.$$

Let $\overline{K}[X] = \overline{K}[X_1, \dots, X_n]$ be a polynomial ring in n variables, and let $I \subset \overline{K}[X]$ be an ideal. To each such I associate a subset of \mathbb{A}^n ,

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

Definition 30. An *affine algebraic set* is any set of the form V_I . If V is an algebraic set, the *ideal of V* is given by

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

An algebraic set is *defined over K* if its ideal $I(V)$ can be generated by polynomials in $K[X]$. We denote this by V/K . If V is defined over K , then the set of *K -rational points of V* is the set

$$V(K) = V \cap \mathbb{A}^n(K).$$

Remark. By the Hilbert Basis Theorem, all ideals in $\overline{K}[X]$ and $K[X]$ are finitely generated.

Let V be an algebraic set. We define the ideal $I(V/K)$ by

$$I(V/K) = \{f \in K[X] : f(P) = 0 \text{ for all } P \in V\} = I(V)/K[X].$$

Thus, V is defined over K iff

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

If V is defined over K , we choose generators $f_1, \dots, f_m \in K[X]$ for $I(V/K)$. Then $V(K)$ is the set of solutions to the simultaneous polynomial equations

$$f_1(X) = \dots = f_m(X) = 0 \quad \text{with } x_1, \dots, x_n \in K.$$

Further, if $f(X) \in K[X]$ and $P \in \mathbb{A}^n$, then for any $\sigma \in G_{\overline{K}/K}$,

$$f(P^\sigma) = f(P)^\sigma.$$

So if V is defined over K then the action of $G_{\overline{K}/K}$ on \mathbb{A}^n induces an action on V , and

$$V(K) = \left\{ P \in V \mid P^\sigma = P \text{ for all } \sigma \in G_{\overline{K}/K} \right\}.$$

Definition 31. An affine algebraic set V is called an affine variety if $I(V)$ is a prime ideal in $\overline{K}[X]$.

Definition 32. Let V/K be a variety. We define the *affine coordinate ring of V/K* as

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

The ring $K[V]$ is an integral domain. Its field of fractions is denoted by $K(V)$ and is called the *function field of V/K* . Similarly $\overline{K}[V]$ and $\overline{K}(V)$ are defined by replacing K with \overline{K} .

Definition 33. Let V be a variety. The *dimension of V* , denoted $\dim(V)$, is the transcendence degree of $\overline{K}(V)$ over \overline{K} .

Definition 34. Let V be a variety, $P \in V$, and $f_1, \dots, f_m \in \overline{K}[X]$ a set of generators for $I(V)$. Then V is *nonsingular* (or *smooth*) at P if the $m \times n$ matrix

$$\left(\frac{\partial f_i}{\partial X_j}(P) \right)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$$

has rank $n - \dim(V)$. If V is nonsingular at every point, then we say that V is *nonsingular*.

A further characterisation for smoothness may also be described. For $P \in V$, define the ideal M_P of $\overline{K}[V]$ by

$$M_P = \{ f \in \overline{K}[V] \mid f(P) = 0 \}.$$

There is an isomorphism

$$\overline{K}[V]/M_P \longrightarrow \overline{K} \quad \text{given by} \quad f \longmapsto f(P),$$

thus M_P is a maximal ideal. The quotient M_P/M_P^2 is a finite-dimensional \overline{K} -vector space.

Proposition 8 ([5], I §5). Let V be a variety. A point $P \in V$ is nonsingular if and only if

$$\dim_{\overline{K}} M_P / M_P^2 = \dim V.$$

Definition 35. The local ring of V at P , denoted $\overline{K}[V]_P$, is the localisation of $\overline{K}[V]$ at M_P . Explicitly,

$$\overline{K}[V]_P = \{F \in \overline{K}(V) \mid F = f/g \text{ for some } f, g \in \overline{K}[V] \text{ with } g(P) \neq 0\}.$$

Definition 36. Projective n -space (over K), denoted \mathbb{P}^n or $\mathbb{P}^n(\overline{K})$, is the set of all $(n+1)$ -tuples

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

with at least one x_i is nonzero, modulo the equivalence relation

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n)$$

if there exists a $\lambda \in \overline{K}^*$ such that $x_i = \lambda y_i$ for all i . An equivalence class

$$\left\{ (\lambda x_0, \dots, \lambda x_n) \mid \lambda \in \overline{K}^* \right\}$$

is denoted by $[x_0, \dots, x_n]$ and the individual x_0, \dots, x_n are called *homogeneous coordinates* for the corresponding point in \mathbb{P}^n . The set of K -rational points in \mathbb{P}^n is the set

$$\mathbb{P}^n(K) = \{[x_0, \dots, x_n] \in \mathbb{P}^n \mid \text{all } x_i \in K\}.$$

Definition 37. Let $P = [x_0, \dots, x_n] \in \mathbb{P}^n(\overline{K})$. The *minimal field of definition for P (over K)* is the field

$$K(P) = K(x_0/x_i, \dots, x_n/x_i) \text{ for any } i \text{ with } x_i \neq 0.$$

Definition 38. Given a polynomial $f \in \overline{K}[X] = \overline{K}[X_0, \dots, X_n]$, we say that f is *homogeneous of degree d* if

$$f(\lambda X_0, \dots, \lambda X_n) = \lambda^d f(X_0, \dots, X_n) \text{ for all } \lambda \in \overline{K}.$$

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

Definition 39. A *projective algebraic set* is any set of the form V_I for a homogeneous ideal I . If V is a projective algebraic set, the *homogeneous ideal of V* denoted $I(V)$, is the ideal of $\overline{K}[X]$ generated by

$$\{f \in \overline{K}[X] \mid f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in V\}.$$

The set V is said to be *defined over K* , which we write in shorthand as V/K , if its ideal $I(V)$ can be generated by homogeneous polynomials in $K[X]$. If V is defined over K , then the *set of K -rational points of V* is the set

$$V(K) = V \cap \mathbb{P}^n(K).$$

We may also characterise $V(K)$ as

$$V(K) = \left\{ P \in V \mid P^\sigma = P \text{ for all } \sigma \in G_{\overline{K}/K} \right\}.$$

Definition 40. A projective algebraic set is called a *projective variety* if its homogeneous ideal $I(V)$ is a prime ideal in $\overline{K}[X]$.

Clearly, \mathbb{P}^n contains many copies of \mathbb{A}^n ; to see that this is the case, we define an inclusion map

$$\begin{aligned} \phi_i : \mathbb{A}^n &\longrightarrow \mathbb{P}^n, \\ (y_1, \dots, y_n) &\longmapsto [y_1, y_2, \dots, y_{i-1}, 1, y_i, \dots, y_n] \end{aligned}$$

Definition 41. Let $V \in \mathbb{A}^n$ be an affine algebraic set with ideal $I(V)$, and consider V as a subset of \mathbb{P}^n by way of

$$V \subset \mathbb{A} \xrightarrow{\phi_i} \mathbb{P}^n.$$

The *projective closure of V* , which we write as \overline{V} , is the projective algebraic set whose homogeneous ideal $I(\overline{V})$ is generated by

$$\{f^*(X) \mid f \in I(V)\}.$$

Definition 42. Let V/K be a projective variety and choose $\mathbb{A}^n \subset \mathbb{P}^n$ such that $V \cap \mathbb{A}^n \neq \emptyset$. The *dimension of V* is the dimension of $V \cap \mathbb{A}^n$.

The *function field of V* , written $K(V)$, is the function field of $V \cap \mathbb{A}^n$ and similarly for $\overline{K}(V)$.

Definition 43. Let V be a projective variety and $P \in V$. Choose $\mathbb{A}^n \subset \mathbb{P}^n$ with $P \in \mathbb{A}^n$. Then V is *nonsingular at P* if $V \cap \mathbb{A}^n$ is nonsingular at P . The *local ring of V at P* , denoted $\overline{K}[V]_P$, is the local ring of $V \cap \mathbb{A}^n$ at P . A function $F \in \overline{K}(V)$ is said to be *regular at P* if it is in $\overline{K}[V]_P$.

2.3.2 Maps Between Varieties

Definition 44. Let $V_1, V_2 \in \mathbb{P}^n$ be projective varieties. A *rational map from $V_1 \rightarrow V_2$* is a map of the form

$$\phi = [f_0, \dots, f_n],$$

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

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

Moreover, if there are $\lambda \in \overline{K}^*$ such that $\lambda f_0, \dots, \lambda f_n \in K(V_1)$, then ϕ is said to be *defined over K* .

Definition 45. A rational map

$$\phi = [f_0, \dots, f_n] : V_1 \rightarrow V_2$$

is *regular at $P \in V_1$* if there is a function $g \in \overline{K}(V_1)$ such that

- (a) each gf_i is regular at P ,
- (b) there is some i for which $(gf_i)(P) \neq 0$.

If such a map g exists, we set

$$\phi(P) = [(gf_0)(P), \dots, (gf_n)(P)].$$

A rational map that is regular at every point is called a *morphism*.

Definition 46. Let V_1 and V_2 be varieties. We say that V_1 and V_2 are *isomorphic*, denoted by $V_1 \cong V_2$, if there are morphisms $\phi : V_1 \rightarrow V_2$ and $\psi : V_2 \rightarrow V_1$ such that $\psi \circ \phi$ and $\phi \circ \psi$ are the identity maps on V_1 and V_2 respectively. We say that V_1/K and V_2/K are *isomorphic over K* if ϕ and ψ can be defined over K .

2.3.3 Maps Between Curves

We define a *curve* as a smooth (nonsingular) projective variety of dimension one.

Proposition 9 ([16], II §1). *Let C be a curve and $P \in C$ be a smooth point. Then $\overline{K}[C]_P$ is a discrete valuation ring.*

Proof. □

The valuation on $\overline{K}[C]_P$ is given by

$$\begin{aligned} \text{ord}_P : \overline{K}[C]_P &\rightarrow \{0, 1, 2, \dots\} \cup \{\infty\} \\ \text{ord}_P(f) &= \sup\{d \in \mathbb{Z} : f \in M_P^d\} \end{aligned}$$

A *uniformizer* for C at P is a function $f \in \overline{K}(C)$ with $\text{ord}_P(f) = 1$.

Definition 47. Let C be a curve with a smooth point P , and let $f \in \overline{K}(C)$. If $\text{ord}_P(f) > 0$, then f has a *zero* at P ; if $\text{ord}_P(f) < 0$, then f has a *pole* at P and we write $f(P) = \infty$. If $\text{ord}_P(f) \geq 0$, then f is *regular* at P .

Proposition 10 ([16], II §1). *Let C be a smooth curve, $f \in \overline{K}(C)$ and $f \neq 0$. There are only finitely many points of C at which f has a pole or zero. If f has no poles, then $f \in \overline{K}$.*

Proposition 11 ([16], II §1). *Let C/K be a curve and let $t \in K(C)$ be a uniformizer at some nonsingular $P \in C(K)$. Then $K(C)$ is a finite separable extension of $K(t)$.*

Proposition 12 ([16], II §2). *Let C be a curve, $V \subset \mathbb{P}^n$ a variety, $P \in C$ a smooth point and $\phi : C \rightarrow V$ a rational map. Then ϕ is regular at P . In particular, if C is smooth, then ϕ is a morphism.*

Proposition 13 ([16], II §2). *Let $\phi : C_1 \rightarrow C_2$ be a morphism of curves. Then ϕ is either constant or surjective.*

Theorem 8 ([16], II §2). *Let C_1/K and C_2/K be curves.*

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

Definition 48. Let $\phi : C_1 \rightarrow C_2$ 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

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

We say that ϕ is *separable*, *inseparable*, or *purely inseparable* if the finite field extension $K(C_1)/\phi^*K(C_2)$ has the corresponding property, and we denote the separable and inseparable degrees of the extension by $\deg_s \phi$ and $\deg_i \phi$ respectively.

Definition 49. Let $\phi : C_1 \rightarrow C_2$ be a nonconstant map of smooth curves, and let $P \in C_1$. The *ramification index of ϕ at P* , denoted $e_\phi(P)$, is the quantity

$$e_\phi(P) = \text{ord}_P(\phi^*t_{\phi(P)}),$$

where $t_{\phi(P)} \in K(C_2)$ is a uniformizer at $\phi(P)$. We say that ϕ is *unramified at P* if $e_\phi(P) = 1$, and that it is *unramified* if it is unramified at every point of C_1 .

Proposition 14 ([16], II §2). *Let $\phi : C_1 \rightarrow C_2$ be a nonconstant map of smooth curves.*

(a) For every $Q \in C_2$,

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

(b) For all but finitely many $Q \in C_2$,

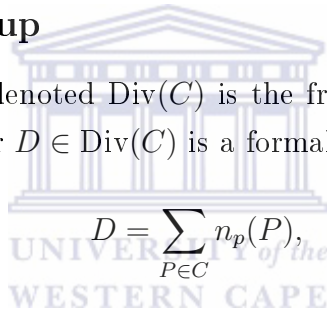
$$\#\phi^{-1}(Q) = \deg_s(\phi).$$

(c) Let $\psi : C_2 \rightarrow C_3$ be another nonconstant map of smooth curves. Then for all $P \in C_1$,

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

2.3.4 Divisor Group

The *divisor group* of C , denoted $\text{Div}(C)$ is the free abelian group generated by the points of C . A divisor $D \in \text{Div}(C)$ is a formal sum


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

where n_p are integers all but finitely many of which are zero. The *degree* of D is defined by

$$\deg D = \sum_{P \in C} n_p.$$

Further, we define the *divisors of degree 0*,

$$\text{Div}^0(C) = \{D \in \text{Div}(C) : \deg D = 0\},$$

which clearly is a subgroup of $\text{Div}(C)$. Suppose C is defined over K . Let $G_{\overline{K}/K}$ act on $\text{Div}(C)$ and $\text{Div}^0(C)$ by

$$D^\alpha = \sum_{P \in C} n_p(P^\alpha).$$

Then D is *defined over K* if $D^\alpha = D$ for all $\alpha \in G_{\overline{K}/K}$. We denote the *group of divisors defined over K* by $\text{Div}_K(C)$, and similarly for $\text{Div}_K^0(C)$.

Let $f \in \overline{K}(C)^*$. We can associate to f the divisor $\operatorname{div}(f)$ given by

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

By definition of $\operatorname{ord}_P(f)$, it is clear that $\operatorname{div}(f)$ is a divisor. If $\alpha \in G_{\overline{K}/K}$, we see that

$$\operatorname{div}(f^\alpha) = (\operatorname{div}(f))^\alpha.$$

In particular, if $f \in K(C)$, then $\operatorname{div}(f) \in \operatorname{Div}_K(C)$.

Definition 50. A divisor $D \in \operatorname{Div}(C)$ is *principal* if it has the form $D = \operatorname{div}(f)$ 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. The *divisor class group*, or *Picard group*, denoted $\operatorname{Pic}(C)$, is the quotient of $\operatorname{Div}(C)$ by its subgroup of principal divisors. We let $\operatorname{Pic}_K(C)$ be the subgroup of $\operatorname{Pic}(C)$ fixed by $G_{\overline{K}/K}$.

Proposition 15 ([16], II §3). *Let C be a smooth curve and let $f \in \overline{K}(C)^*$.*

- (a) *$\operatorname{div}(f) = 0$ if and only if $f \in \overline{K}^*$.*
- (b) *$\deg(\operatorname{div}(f)) = 0$.*

Remark. The degree-zero part of the Picard group is denoted $\operatorname{Pic}^0(C)$. We have an exact sequence

$$1 \rightarrow \overline{K}^* \rightarrow \overline{K}(C)^* \rightarrow \operatorname{Div}^0(C) \rightarrow \operatorname{Pic}^0(C) \rightarrow 1,$$

which is the function-field analogue of the exact sequence

$$1 \rightarrow \{\text{units}\} \rightarrow K^* \rightarrow \{\text{fractional ideals}\} \rightarrow \operatorname{Cl}(K) \rightarrow 1.$$

Let $\phi : C_1 \rightarrow C_2$ be a non-constant map of smooth curves. As we have seen, ϕ induces maps on the function fields of C_1 and C_2 ,

$$\phi^* : \overline{K}(C_2) \longrightarrow \overline{K}(C_1) \quad \text{and} \quad \phi_* : \overline{K}(C_1) \longrightarrow \overline{K}(C_2).$$

Similarly, define maps of divisor groups as follows:

$$\begin{aligned} \phi^* : \text{Div}(C_2) &\longrightarrow \text{Div}(C_1), & \phi_* : \text{Div}(C_1) &\longrightarrow \text{Div}(C_2), \\ (Q) &\longmapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P), & (P) &\longmapsto (\phi P), \end{aligned}$$

and extend \mathbb{Z} -linearly to arbitrary divisors.

Proposition 16 ([16], II §3). *Let $\phi : C_1 \rightarrow C_2$ be a non-constant map of smooth curves.*

(a) $\deg(\phi^* D) = (\deg \phi) \deg D$ for all $D \in \text{Div}(C_2)$.

(b) $\phi^*(\text{div } f) = \text{div}(\phi^* f)$ for all $f \in \overline{K}(C_2)^*$.

(c) $\deg(\phi_* D) = \deg D$ for all $D \in \text{Div}(C_1)$.

(d) $\phi_*(\text{div } f) = \text{div}(\phi_* f)$ for all $f \in \overline{K}(C_1)^*$.

(e) $\phi_* \circ \phi^*$ acts as multiplication by $\deg \phi$ on $\text{Div}(C_2)$.

(f) if $\psi : C_2 \rightarrow C_3$ is another such map, then

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

Remark. From the previous proposition we see that ϕ^* and ϕ_* take divisors of degree 0 to divisors of degree 0, and principal divisors to principal divisors. They thus induce maps

$$\phi^* : \text{Pic}^0(C_2) \longrightarrow \text{Pic}^0(C_1) \quad \text{and} \quad \phi_* : \text{Pic}^0(C_1) \longrightarrow \text{Pic}^0(C_2).$$

In particular, if $f \in \overline{K}(C)$ gives the map $f : C \rightarrow \mathbb{P}^1$, then

$$\deg \text{div}(f) = \deg f^*((0) - (\infty)) = \deg f - \deg f = 0.$$

We now discuss the vector space of differential forms on a curve. It provides a useful criterion for determining if an algebraic map is separable.

Definition 51. Let C be a curve. The *space of differential forms* on C , denoted Ω_C is the \overline{K} -vector space generated by symbols of the form dx for $x \in \overline{K}(C)$, subject to

(i) $d(x + y) = dx + dy$ for all $x, y \in \overline{K}(C)$.

(ii) $d(xy) = xdy + ydx$ for all $x, y \in \overline{K}(C)$.

(iii) $da = 0$ for all $a \in \overline{K}$.

Proposition 17 ([16], II §3). *Let C be a curve.*

(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 $\phi : C_1 \rightarrow C_2$ be a non constant map of curves. Then ϕ is separable if and only if the map

$$\phi^* : \Omega_{C_2} \rightarrow \Omega_{C_1}$$

is injective.

Definition 52. Let $\omega \in \Omega_C$. The *divisor associated with ω* is

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

The differential $\omega \in \Omega_C$ is *regular* if

$$\text{ord}_P(\omega) \geq 0 \text{ for all } P \in C.$$

It is *nonvanishing* if

$$\text{ord}_P(\omega) \leq 0 \text{ for all } P \in C.$$

Definition 53. The *canonical divisor class* on C is the image in $\text{Pic}(C)$ of $\text{div}(\omega)$ for any nonzero differential $\omega \in \Omega_C$. Any divisor in this divisor class is called a *canonical divisor*.

We apply a partial order on $\text{Div}(C)$ in the following way.

Definition 54. A divisor $D = \sum n_P(P)$ is *effective*, denoted by

$$D \geq 0,$$

if $n_P \geq 0$ for every $P \in C$. Similarly, given any two divisors $D_1, D_2 \in \text{Div}(C)$ we write

$$D_1 \geq D_2$$

to indicate that $D_1 - D_2$ is effective.

Definition 55. Let $D \in \text{Div}(C)$. Associate to D the set of functions

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

The set $\mathcal{L}(D)$ is a finite-dimensional \overline{K} -vector space and we denote its dimension by

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

Proposition 18 ([16], II §5). **(a)** If $\text{deg}D < 0$ then $\mathcal{L}(D) = \{0\}$ and $\ell(D) = 0$.

(b) $\mathcal{L}(D)$ is a finite-dimensional \overline{K} -vector space.

(c) If $D' \in \text{Div}(C)$ is linearly equivalent to D , then

$$\mathcal{L}(D) \cong \mathcal{L}(D'), \quad \text{and so} \quad \ell(D) = \ell(D').$$

Theorem 9 (Riemann-Roch, [16] §5). Let C be a smooth curve and let K_C be a canonical divisor on C . There is an integer $g \geq 0$, called the genus of C , such that for every divisor $D \in \text{Div}(C)$,

$$\ell(D) - \ell(K_C - D) = \text{deg}D - g + 1.$$

Corollary 3 ([16] §5). **(a)** $\ell(K_C) = g$.

(b) $\text{deg}K_C = 2g - 2$.

(c) If $\text{deg}D > 2g - 2$, then

$$\ell(D) = \text{deg}D - g + 1.$$

Chapter 3

Elliptic Curves

We introduce the main focus of the dissertation: elliptic curves over the rational numbers.

It will be shown that a group structure can be defined on rational points on elliptic curves. Furthermore we will show, by Mordell's Theorem, that this group of rational points is finitely generated. Explicitly, if E is an elliptic curve over \mathbb{Q} then

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{Tors}}$$

where r is the rank of the free abelian group which contains the points of infinite order and $E(\mathbb{Q})_{\text{Tors}}$ is the torsion subgroup, the points of finite order. Moreover, by the Mordell-Weil Theorem, we may replace \mathbb{Q} as above with arbitrary numberfields K resulting in E being finitely generated over K .

Mordell's Theorem does not provide an effective method for determining the exact value of the rank r . This shortcoming led Birch and Swinnerton-Dyer to investigate elliptic curves on the EDSAC computer in the 1960s, culminating in their groundbreaking conjecture, covered in Chapter 4.

We provide a precise definition for elliptic curves in the next section, and also define useful invariants needed in later sections. We show that the rational points on an elliptic curve form a group, then investigate how this group behaves under reduction modulo primes. We then turn to the points of finite order where we

first show that only points with integer coordinates can qualify as torsion points, and secondly determine a bound on the number of points which can occur.

Thereafter, the weak Mordell Theorem is investigated. The computation of the Mordell Group involves computing the generators for the group $E(K)/mE(K)$ where E is an elliptic curve over a numberfield K . This computation is reduced to the problem of determining whether each of a certain finite set of auxiliary curves, called *homogeneous spaces*, has a single rational point. The existence (or non-existence) of this rational point is often shown by finding a point (resp. not finding a point) in each (resp. some) completion K_v of K . However, it may occur that each completion K_v has a K_v -rational point yet there is no K -rational point. The extent of the failure is quantified by the *Shafarevich-Tate group*. Surprisingly, the second Birch and Swinnerton-Dyer conjecture makes use of the cardinality of the Shafarevich-Tate group, which itself is conjectured to be finite.

We complete the chapter by investigating elliptic curves over the complex plane.

The sources used in this chapter are mainly, but not limited to, [6, 13, 15, 16, 18].

3.0 Elliptic Curves

Let k be a numberfield.

Definition 56 ([13]). An *elliptic curve* over k can be defined as

- (a) a nonsingular projective plane curve E over k of degree 3 together with a point $\mathcal{O} \in E(k)$;
- (b) precisely as (a) except that \mathcal{O} is required to be a point of inflection;
- (c) a nonsingular projective plane curve over k with *generalised Weierstrass* equation

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

(d) a nonsingular projective curve E of genus 1 together with a point $\mathcal{O} \in E(k)$.

The reference [13] proves the equivalence of statements (a) \Rightarrow ... \Rightarrow (d) \Rightarrow (a); we shall prove that (d) \Rightarrow (c).

Proof. [13] II §1, [16] III §3. Let E be a nonsingular projective curve of genus 1 over a field k and let $\mathcal{O} \in E(k)$. By Riemann-Roch, the rational functions on E , having no poles except at \mathcal{O} and having at worst a pole of order $m \geq 1$ at \mathcal{O} , form a vector space of dimension m over k , i.e., $k(m[\mathcal{O}])$ has dimension m for $m \geq 1$. The constant functions lie on $\mathcal{L}([\mathcal{O}])$, and by Riemann-Roch, there are no other. Thus $\{1\}$ is a basis for $\mathcal{L}([\mathcal{O}])$. Choose x so that $\{1, x\}$ is a basis for $\mathcal{L}(2[\mathcal{O}])$. Choose y so that $\{1, x, y\}$ is a basis for $\mathcal{L}(3[\mathcal{O}])$. Then $\{1, x, y, x^2\}$ is a basis for $\mathcal{L}(4[\mathcal{O}])$ - if it were linearly dependent, x^2 would have to be a linear combination of $1, x, y$, but then we would have a quadruple pole at \mathcal{O} . Further, $\{1, x, y, x^2, xy\}$ is a basis for $\mathcal{L}(5[\mathcal{O}])$ for a similar reason as in the previous sentence.

The subset $\{1, x, y, x^2, xy, x^3, y^2\}$ of $\mathcal{L}(6[\mathcal{O}])$ contains 7 elements, so it must be linearly dependent: there exist $a_i \in k$ such that

$$a_0 y^2 + a_1 xy + a_3 y = a'_0 + a_2 x^2 + a_4 x + a_6.$$

Moreover, a_0 and a'_0 must be nonzero otherwise the set with either x^3 or y^2 omitted is linearly independent, so without loss of generality we may scale both x and y to make these two coefficients both equal to 1. The map $P \mapsto (x(P), y(P))$ sends $E \setminus \{\mathcal{O}\}$ onto the plane affine curve

$$C : Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6.$$

The function x has a double pole at \mathcal{O} and no other pole, and so it has only two zeros. Similarly, $x + c$ has two zeros for any $c \in k$ (with multiplicities), so the composite

$$E \setminus \{\mathcal{O}\} \rightarrow C \rightarrow \mathbb{A}^1, \quad P \mapsto (x(P), y(P)) \mapsto x(P)$$

has degree 2 by Proposition 14. Similarly, the composite

$$E \setminus \{\mathcal{O}\} \rightarrow C \rightarrow \mathbb{A}^1, \quad P \mapsto (x(P), y(P)) \mapsto y(P)$$

has degree 3. The degree of $E \setminus \{\mathcal{O}\} \rightarrow C$ divides both 2 and 3, so it must be 1. If C were singular, it would have genus 0, a contradiction. Therefore C is nonsingular, and so the map is an isomorphism and it extends to an isomorphism of E onto

$$\bar{C} : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

proving our assertion. □

Remark. The above result means that we may think of an elliptic curve E as an affine curve with Weierstrass equation with an additional point called *the point at infinity*, denoted \mathcal{O} . We define the point at infinity as the identity of the group of rational points on E . The point at infinity is found above (and below) every vertical line in the affine plane. We may thus write the Weierstrass equation for our elliptic curve using non-homogeneous coordinates with $x = X/Z$ and $y = Y/Z$ as

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (3.1)$$

while being cognisant of the point at infinity $\mathcal{O} = [0, 1, 0]$.

In the above proof, we started by choosing functions $x, y \in k(E)$ to define our basis points for E . If we had chosen different functions x', y' , the resulting Weierstrass equation would be different. However, one would think that the two curves should have some sort of relationship. We now characterise that relationship with the following proposition.

Proposition 19 ([16] III §3). *Any two Weierstrass equations for an elliptic curve E are related by a linear change of variables of the form*

$$X = u^2X' + r, \quad Y = u^3Y' + su^2X' + t,$$

with $u \in k^*, r, s, t \in k$.

Remark. Such a change of variables is called an *admissible change of variables*.

Depending on the characteristic of the algebraic extension \bar{k} of k , we may simplify an elliptic curve's generalised Weierstrass equations [16]. If $\text{char}(\bar{k}) \neq$

2, simplification of the equation can be done by completing the square. The substitution

$$y \mapsto \frac{1}{2}(y - a_1x - a_3)$$

yields an equation for E of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where

$$b_2 = a_1^2 + 4a_4, \quad (3.2)$$

$$b_4 = 2a_4 + a_1a_3, \quad (3.3)$$

$$b_6 = a_3^2 + 4a_6. \quad (3.4)$$

Before providing further simplifications of Weierstrass equations, we also introduce the quantities

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \quad (3.5)$$

$$c_4 = b_2^2 - 24b_4, \quad (3.6)$$

$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6, \quad (3.7)$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \quad (3.8)$$

$$j = c_4^3/\Delta, \quad (3.9)$$

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}. \quad (3.10)$$

where j is known as the j -invariant of the elliptic curve, Δ is known as the *discriminant* of the Weierstrass equation and ω is known as the *invariant differential* associated to the Weierstrass equation. These newly introduced quantities (Δ, j, ω) will be elaborated upon in later sections.

We now return to the simplification of Weierstrass equations. If $\text{char}(\bar{k}) \neq 2, 3$, then the substitution

$$(x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108} \right)$$

eliminates the x^2 term, resulting in

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

We provide a table for admissible change of variable formulas for Weierstrass equations

$$\begin{aligned} ua'_1 &= a_1 + 2s \\ u^2a'_2 &= a_2 - sa_1 + 3r - s^2 \\ u^3a'_3 &= a_3 + ra_1 + 2t \\ u^4a'_4 &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \\ u^6a'_6 &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \\ u^2b'_2 &= b_2 + 12r \\ u^4b'_4 &= b_4 + rb_4 + 6r^2 \\ u^6b'_6 &= b_6 + 2rb_4 + r^2b_2 + 4r^3 \\ u^8b'_8 &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \\ u^4c'_4 &= c_4 \\ u^6c'_6 &= c_6 \\ u^12\Delta' &= \Delta \\ j' &= j \\ u^{-1}\omega' &= \omega \end{aligned}$$

We now return to the j -invariant and discriminant. If the characteristic of k is not 2 nor 3, our elliptic curve E has Weierstrass equation

$$E : y^2 = x^3 + Ax + B.$$

We can define quantities

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

The only change of variables preserving the Weierstrass form of the equation is

$$x = u^2x' \quad \text{and} \quad y = u^3y' \quad \text{for some } u \in \bar{k}^*.$$

Then

$$u^4A' = A, \quad u^6B' = B, \quad u^12\Delta' = \Delta.$$

Proposition 20 ([16], III §1). **(a)** *The curve given by a Weierstrass equation is nonsingular if and only if $\Delta \neq 0$.*

(b) *Let $j_0 \in \bar{k}$. There exists an elliptic curve defined over $k(j_0)$ whose j -invariant is equal to j_0 .*

Proposition 21 ([16], III §1). *Let E be an elliptic curve. The invariant differential ω associated to a Weierstrass equation for E is holomorphic and nonvanishing, i. e., $\text{div}(\omega) = 0$.*

Definition 57. A Weierstrass equation is in *Legendre Form* if it can be written as

$$y^2 = x(x-1)(x-\lambda) \tag{3.11}$$

for some $\lambda \in k$.

We shall use the Weierstrass equation characterisation (3.1) as the basis of our study of elliptic curves. We can then give a concrete interpretation of the Shafarevich-Tate group, as well as cover some of the computational aspects of the Birch and Swinnerton-Dyer Conjecture.

3.1 Group Structure of Elliptic Curves

Let E be an elliptic curve with respective Weierstrass equation. Let $L \subset \mathbb{P}^2$ be a line. Since the equation of E has degree three, the line L intersects E at exactly three points, say P, Q, R . If L is tangent to E , then P, Q, R need not be distinct. The fact that $L \cap E$, with multiplicities, consists of exactly three points is a consequence of Bézout's theorem [16].

We define a Composition Law \oplus on E by the following rule:

Composition Law ([16]). Let $P, Q \in E$, let L be the line through P and Q (if $P = Q$ then L is a tangent to E at P), and let R be the third point of intersection of L with E . Let L' be the line through R and \mathcal{O} . Then L' intersects E at R , \mathcal{O} and a third point. We denote that third point by $P \oplus Q$.

Proposition 22 ([16], III §2). The Composition Law has the following properties:

(a) If a line L intersects E at the (not necessarily distinct) points P, Q, R , then

$$(P \oplus Q) \oplus R = \mathcal{O}.$$

(b) $P \oplus \mathcal{O} = P$ for all $P \in E$.

(c) $P \oplus Q = Q \oplus P$ for all $P, Q \in E$.

(d) Let $P \in E$. There is a point of E , denoted by $\ominus P$, satisfying

$$P \oplus (\ominus P) = \mathcal{O}.$$

(e) Let $P, Q, R \in E$. then

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

That is, the composition law makes E into an abelian group with identity element \mathcal{O} . Further:

(f) Suppose that E is defined over k . Then

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

is a subgroup of E .

Group Law. Let E be an elliptic curve given by a Weierstrass equation

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

(a) Let $P_0 = (x_0, y_0)$. Then

$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3).$$

Next let

$$P_1 + P_2 = P_3 \quad \text{with } P_i = (x_i, y_i) \in E \text{ for } i = 1, 2, 3.$$

(b) If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then

$$P_1 + P_2 = \mathcal{O}.$$

Otherwise define λ and ν by the following formulas:

$$\begin{aligned} x_1 \neq x_2 &\Rightarrow \lambda = \frac{y_2 - y_1}{x_2 - x_1}, & \nu &= \frac{y_1x_2 - y_2x_1}{x_2 - x_1} \\ x_1 = x_2 &\Rightarrow \lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, & \nu &= \frac{-x_1^3 + a_4x_1 + 2a_6 - a_4y_1}{2y_1 + a_1x_1 + a_3} \end{aligned}$$

Then $y = \lambda x + \nu$ is the line through P_1 and P_2 or tangent to E if $P_1 = P_2$.

(c) The point $P_3 = P_1 + P_2$ thus has coordinates

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

(d) For $P_1 \neq \pm P_2$,

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 + a_1 \left(\frac{y_2 - y_1}{x_2 - x_1} \right) - a_2 - x_1 - x_2,$$

and the duplication formula for $P = (x, y) \in E$,

$$x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6},$$

where b_2, b_4, b_6, b_8 are the polynomials in the a_i 's of (3.2) - (3.10).

Remark. The group law on an elliptic curve can be proved with the use of the Riemann-Roch theorem. We provide an overview of the method:

Group Law by Riemann-Roch. Let E be a projective curve as in Definition 56 (d) defined over a field k . For every degree-zero divisor D , there exists a unique point $P \in E$ such that $D \sim (P) - (\mathcal{O})$. If $\sigma : \text{Div}^0(E) \rightarrow E$ denotes this map, then σ is a bijection between $\text{Pic}^0(E)$ and E . The group law induced from $\text{Pic}^0(E)$ via σ is equivalent to the geometric group law.

Further details regarding uniqueness of P , or that σ as above is not only a bijection but also homomorphic can be found in [16] Proposition 3.4 or [13] IV Proposition 4.10. □

Theorem 10 ([16] Theorem 3.6). *The group law defines morphisms*

$$\begin{array}{ccc} + : E \times E & \longrightarrow & E, & \text{and} & - : E & \longrightarrow & E, \\ (P_1, P_2) & \longmapsto & P_1 + P_2 & & P & \longmapsto & -P \end{array}$$

Proof. The negative map

$$(x, y) \longmapsto (x, -y - a_1x - a_3)$$

is clearly a rational map $E \rightarrow E$. Since E is smooth, it follows from proposition 12 that negation is a morphism.

Fix a point $Q \neq \mathcal{O}$ and consider the *translation-by- Q* map

$$\tau : E \longrightarrow E, \quad \tau(P) = P + Q.$$

From the addition formula in the Group Law (c), this is a rational map and a morphism by Proposition 12. Moreover, since τ has an inverse $P \mapsto P - Q$, it is an isomorphism.

Now consider the general addition map $+ : E \times E \rightarrow E$. From the Group Law (c), it is a morphism with the possible exceptions of points having one of the following forms,

$$(P, P), \quad (P, -P) \quad (P, \mathcal{O}) \quad (\mathcal{O}, P),$$

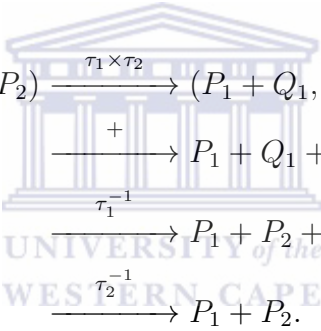
since for pairs of points not of this form, the rational functions

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{and} \quad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

on $E \times E$ are well-defined. We investigate the exceptions by defining τ_1 and τ_2 as translation maps as above for points Q_1 and Q_2 respectively, thereafter considering the composition of maps:

$$\phi : E \times E \xrightarrow{\tau_1 \times \tau_2} E \times E \xrightarrow{+} E \xrightarrow{\tau_1^{-1}} E \xrightarrow{\tau_2^{-1}} E.$$

Since the group law on E is associative and commutative, the above maps are essentially as follows:



$$\begin{aligned} (P_1, P_2) &\xrightarrow{\tau_1 \times \tau_2} (P_1 + Q_1, P_2 + Q_2) \\ &\xrightarrow{+} P_1 + Q_1 + P_2 + Q_2 \\ &\xrightarrow{\tau_1^{-1}} P_1 + P_2 + Q_2 \\ &\xrightarrow{\tau_2^{-1}} P_1 + P_2. \end{aligned}$$

Thus the rational map ϕ agrees with the addition map wherever they are both defined.

Since the translation maps are isomorphisms, it follows from the above that ϕ is a morphism with the possible exceptions at pairs of points of the form

$$(P - Q_1, P - Q_2), (P - Q_1, -P - Q_2) (P - Q_1, -Q_2) (-Q_1, P - Q_2).$$

However, both Q_1 and Q_2 were arbitrarily chosen. Hence by varying Q_1 and Q_2 , we can find a finite set of rational maps

$$\phi_1, \phi_2, \dots, \phi_n : E \times E \longrightarrow E$$

with the following properties:

- (i) ϕ_1 is the addition map given in the Group Law (c).

(ii) For each $(P_1, P_2) \in E \times E$, some ϕ_i is defined at (P_1, P_2) .

(iii) If ϕ_i and ϕ_j are both defined at (P_1, P_2) , then $\phi_i(P_1, P_2) = \phi_j(P_1, P_2)$.

It follows that addition is defined on all of $E \times E$, so it is a morphism. \square

We have seen that the set of rational points on an elliptic curve E together with the composition law form a group. We now investigate maps between elliptic curves.

Definition 58. Let E and E' be elliptic curves defined over a field k . An *isogeny* from E_1 to E_2 is a morphism

$$\phi : E_1 \rightarrow E_2 \text{ satisfying } \phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}.$$

Two elliptic curves E_1 and E_2 are *isogenous* if there is an isogeny from E_1 to E_2 with $\phi(E_1) \neq \{\mathcal{O}_{E_2}\}$. It turns out that this is an equivalence relation.

It would be natural to suppose that we should focus on isogenies which are homomorphisms. In fact, isogenies are automatically homomorphisms.

Theorem 11 ([16] Theorem 4.8). *Let*

$$\phi : E_1 \rightarrow E_2$$

be an isogeny. Then $\phi(P + Q) = \phi(P) + \phi(Q)$ for all $P, Q \in E_1$.

Proof. If $\phi(P) = \mathcal{O} \forall P \in E_1$, the assertion is satisfied. Otherwise, ϕ is a finite map, so by 2.3.4, it induces a homomorphism

$$\phi_* : \text{Pic}^0(E_1) \rightarrow \text{Pic}^0(E_2)$$

defined by

$$\phi_* \left(\text{class of } \sum n_i(P_i) \right) = \text{class of } \sum n_i(\phi P_i).$$

On the other hand, by 2.3.4, we have *group homomorphisms*

$$\kappa_i : E_i \rightarrow \text{Pic}^0(E_i), \quad P \mapsto \text{class of } (P) - (\mathcal{O}).$$

We can obtain the following commutative diagram since $\phi(\mathcal{O}) = \mathcal{O}$:

$$\begin{array}{ccc}
 E_1 & \xrightarrow[\kappa_1]{\cong} & \text{Pic}^0(E_1) \\
 \phi \downarrow & & \downarrow \phi_* \\
 E_2 & \xrightarrow[\kappa_2]{\cong} & \text{Pic}^0(E_2)
 \end{array}$$

Since κ_1, κ_2 and ϕ_* are all group homomorphisms with κ_2 injective, it follows that ϕ is also a homomorphism. \square

The maps between elliptic curves form groups since the elliptic curves themselves are abelian groups. Denote the set of isogenies from E_1 to E_2 by

$$\text{Hom}(E_1, E_2) = \{\text{isogenies } E_1 \rightarrow E_2\}.$$

Proposition 23 ([16], III §4). *Let E_1 and E_2 be elliptic curves. Then the group of isogenies*

$$\text{Hom}(E_1, E_2)$$

is a torsion-free \mathbb{Z} -module.

If $E_1 = E_2$, let $\text{End}(E) = \text{Hom}(E, E)$ be the endomorphism ring with addition and multiplicative laws

$$(\phi + \psi)(P) = \phi(P) + \psi(P)$$

$$(\phi\psi)(P) = \phi(\psi(P))$$

respectively, with the latter being composition.

Definition 59. If the endomorphism ring $\text{End}(E)$ is strictly larger than \mathbb{Z} , then E is said to have *complex multiplication* (CM curves for short).

Remark. There are special properties attributed to CM curves. We will briefly elaborate on one such property in Chapter 4.

We return to the quantity j . Define the j -invariant of E to be

$$j = j(E) = 1728 \frac{c_4^3}{\Delta}.$$

Theorem 12 ([6] III (4.2)). *Let $y_1^2 = x_1^3 + A_1x_1 + B_1$ and $y_2^2 = x_2^3 + A_2x_2 + B_2$ be two elliptic curves with j -invariants j_1 and j_2 resp and \bar{k} (which has characteristic unequal to 2 or 3) be the algebraic closure of k . If $j_1 = j_2$ then there exists $\mu \neq 0$ in \bar{k} such that*

$$A_2 = \mu^4 A_1, \quad B_2 = \mu^6 B_1.$$

The transformation

$$x_2 = \mu^2 x_1, \quad y_2 = \mu^3 y_1$$

takes one equation to the other.

Remark. Under an admissible change of variable we have, for the corresponding \bar{c}_i and \bar{j} , the relations

$$u^4 \bar{c}_4 = c_4, \quad u^6 \bar{c}_6 = c_6 \quad \text{and} \quad \bar{j} = j.$$

For the j -invariant we have $j = \bar{j}$. This means that $j(E)$ is an invariant of an elliptic curve E up to isomorphism. Moreover, if k is a field of characteristic different from 2 and 3, then for $y'' = y'$ and $x'' = x' + b_2/12$ the equation in normal form becomes

$$y'' = (x'')^3 - \frac{c_4}{48} x'' - \frac{c_6}{864} \tag{3.12}$$

and $\omega = dx''/2y''$.

Let $\phi : E_1 \rightarrow E_2$ be a nonconstant isogeny. By Remark (2.3.4), ϕ induces a map

$$\phi^* : \text{Pic}^0(E_2) \rightarrow \text{Pic}^0(E_1).$$

We also have, for $i = 1, 2$, group isomorphisms by Remark (2.3.4)

$$\kappa_i : E_i \rightarrow \text{Pic}^0(E_i), \quad P \mapsto \text{class of } (P) - (\mathcal{O}).$$

This gives a homomorphism in the opposite direction to ϕ

$$E_2 \xrightarrow{\kappa_2} \text{Pic}^0(E_2) \xrightarrow{\phi^*} \text{Pic}^0(E_1) \xrightarrow{\kappa_1^{-1}} E_1.$$

We want to show that if $Q \in E_2$ and any $P \in E_1$ satisfying $\phi(P) = Q$ that

$$\kappa_1^{-1} \circ \phi^* \circ \kappa_2(Q) = [\deg \phi](P).$$

Theorem 13 ([16] III Theorem 6.1). *Let $E_1 \rightarrow E_2$ be a nonconstant isogeny of degree m .*

(a) *There exists a unique isogeny*

$$\hat{\phi} : E_2 \rightarrow E_1 \text{ em satisfying } \hat{\phi} \circ \phi = [m].$$

(b) *As a group homomorphism, $\hat{\phi}$ equals the composition*

$$\begin{array}{ccccccc} E_2 & \longrightarrow & \text{Div}^0(E_2) & \xrightarrow{\phi^*} & \text{Div}^0(E_1) & \xrightarrow{\text{sum}} & E_1, \\ Q & \mapsto & (Q) - (\mathcal{O}) & & \sum n_p(P) & \mapsto & \sum [n_p]P. \end{array}$$

Definition 60. Let $\phi : E_1 \rightarrow E_2$ be an isogeny. The *dual isogeny* to ϕ is the isogeny

$$\hat{\phi} : E_2 \rightarrow E_1$$

given by Theorem 13 (a) where $\phi \neq [0]$. If $\phi = [0]$, then $\hat{\phi} = [0]$ is suitable as a dual.

Theorem 14 ([16] III Theorem 6.2). *Let*

$$\phi : E_1 \rightarrow E_2$$

be an isogeny.

(a) *Let $m = \deg \phi$. Then*

$$\hat{\phi} \circ \phi = [m] \text{ on } E_1 \quad \text{and} \quad \phi \circ \hat{\phi} = [m] \text{ on } E_2.$$

(b) Let $\lambda : E_2 \rightarrow E_3$ be another isogeny. Then

$$\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}.$$

(c) Let $\psi : E_1 \rightarrow E_2$ be another isogeny. Then

$$\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}.$$

(d) For all $m \in \mathbb{Z}$,

$$[\widehat{m}] = [m] \quad \text{and} \quad \deg[m] = m^2.$$

(e) $\deg \hat{\phi} = \deg \phi$.

(f) $\hat{\hat{\phi}} = \phi$.

3.2 Intersection of Two Quadratic Surfaces

We take a brief detour to show that the intersection of two quadratic curves define an elliptic curve over K if the intersection contains a K -rational point. These intersections are the *homogeneous spaces* we alluded to earlier in the introduction to Chapter 3; the homogeneous spaces are used extensively in Sections 3.7 and 4.3.3. We follow [18] §2.5.3-2.5.4.

Let C be the curve defined as

$$C : v^2 = au^4 + bu^3 + cu^2 + du + e, \tag{3.13}$$

with $a \neq 0$. If we have a point $(p, q) \in C$ with $p, q \in K$, then the equation, if it is nonsingular, it can be transformed into a Weierstrass equation by an invertible change of variables that uses rational functions with coefficients in the field K . We provide the details for this transformation in Theorem 15. Note that curves of the form as in (3.13) are not required to have points with coordinates in K . Suppose $(p, q) \in C$ where C has the form (3.13) and $p, q \in K$. By changing u to $u + p$, we may assume $p = 0$, so the point has the form $(0, q)$.

Suppose $q = 0$. If $d = 0$, the curve has a singularity at $(u, v) = (0, 0)$. Therefore, assume $d \neq 0$. Then

$$\left(\frac{v}{u^2}\right)^2 = d\left(\frac{1}{u^2}\right)^3 + c\left(\frac{1}{u^2}\right)^2 + b\left(\frac{1}{u^2}\right) + a,$$

which can be transformed into a Weierstrass equation in d/u and dv/u^2 .

For $q \neq 0$, we have the following theorem.

Theorem 15 ([18], II §5.3). *Let K be a field with characteristic unequal to 2. Consider the equation*

$$v^2 = au^4 + bu^3 + cu^2 + du + q^q$$

with $a, b, c, d, q \in K$. Let

$$x = \frac{2q(v+q) + du}{u^2}, \quad y = \frac{4q^2(v+q) + 2q(du + cu^3) - (d^2u^2/2q)}{u^3}.$$

Define

$$a_1 = d/q, \quad a_2 = c - (d^2/4q^2), \quad a_3 = 2qp, \quad a_4 = -4q^2a, \quad a_6 = a_2a_4.$$

where the elliptic curve E has Weierstrass form (3.1). The inverse transformation is

$$u = \frac{2q(x+c) - (d^2/2q)}{y}, \quad v = -q + \frac{u(ux-d)}{2q}.$$

The point $(u, v) = (0, q)$ corresponds to the point $(x, y) = \infty$ and $(u, v) = (0, -q)$ corresponds to $(x, y) = (-a_2, a_1a_2 - a_3)$.

The intersection of two quadratic surfaces in three-dimensional space, along with a point on this intersection, usually results in an elliptic curve. For the sake of simplicity, we opt not to fully generalise the idea, but rather consider pairs of equations of the form

$$au^2 + bv^2 = e, \quad cu^2 + dw^2 = f,$$

where a, b, c, d, e, f are nonzero elements of a field K of characteristic not 2.

Each separate equation may be regarded as a surface in the uvw -space, and they intersect in a curve. If we have a point P in this intersection, we can transform this curve into an elliptic curve in Weierstrass form.

The equations above can be regarded as giving a curve C in the uv -plane. Let $P = (u_0, v_0)$ be a point on C . Let L be the line through P with slope m :

$$u = u_0 + t, \quad v = v_0 + mt.$$

We wish to find other points where L intersects C . By way of substitution and $au_0^2 + bv_0^2 = e$, we obtain

$$a(2u_0t + t^2) + b(2v_0mt + m^2t^2) = 0.$$

Since $t = 0$ corresponds to (u_0, v_0) , factoring out t results in

$$t = -\frac{2au_0 + 2bv_0m}{a + bm^2}.$$

Therefore,

$$u = u_0 - \frac{2au_0 + 2bv_0m}{a + bm^2}, \quad v = v_0 - \frac{2amu_0 + 2bv_0m}{a + bv_0m^2}.$$

We use the convention that $m = \infty$ yields $(u_0, -v_0)$. If the denominator $a + bm^2$ vanishes, we get points at infinity in the uv -projective plane.

If (u, v) is any point on C with coordinates in K , then the slope m of the line through (u, v) and P is in K (or is infinite). Thus, we have obtained a bijection, save for a few technicalities, between values of m and points on C . The overarching idea is that we have obtained a parametrisation of the points on C . Similar procedures work for any conic section containing a point with coordinates in K . We now check which value of m corresponds to the original point (u_0, v_0) . Let m be the slope of the tangent line at (u_0, v_0) . The second point of intersection of the tangent line with the curve is again the point (u_0, v_0) , so this slope is the desired value of m . If $m = 0$, we obtain $(-u_0, v_0)$.

We now want to intersect C with the surface $cu^2 + dw^2 = f$. We substitute the

expression just obtained for u to obtain

$$dw^2 = f - c \left(u_0 - \frac{2au_0 + 2bv_0m}{a + bm^2} \right)^2.$$

We rewrite the above as

$$\begin{aligned} d(w(a + bm^2))^2 &= (a + bm^2)^2 f - c(bu_0m^2 - 2bv_0m - au_0)^2 \\ &= (b^2f - cb^2u_0^2)m^4 + \dots \end{aligned}$$

This can be changed to Weierstrass form by the procedure given earlier. The leading coefficient $b^2f - cb^2u_0^2$ equals $b^2dw_0^2$. If $w_0 = 0$, the fourth degree polynomial becomes a cubic polynomial, hence the equation just obtained can easily be put into Weierstrass form. The leading term of the resultant cubic polynomial vanishes if $v_0 = 0$. However, then the point $(u_0, v_0, w_0) = (u_0, 0, 0)$ is a singular point of the uvw curve, a situation we wish to avoid.

The procedure for changing "square = quartic polynomial" into Weierstrass form requires a point satisfying this equation. We could let m be the slope of the tangent line at (u_0, v_0) , which corresponds to the point (u_0, v_0) . The formula of Theorem 15 requires that we shift the value of m to obtain $m = 0$. However, it is expedient to use $m = 0$ directly, since this value corresponds to $(-u_0, v_0)$, as pointed out in the discussion above.

3.3 Minimal Normal Form of an Elliptic Curve

This entire section is sourced from [6], V §2.

We have been using admissible changes of variables throughout much of the previous sections. A natural question thus arises: Is there an optimal change of variables, i.e. is there a change of variables which results in the simplest normal form for an elliptic curve?

We shall shortly see that there is such an optimal form, referred to as the *minimal normal form* for an elliptic curve.

Proposition 24 ([6], V Prop 2.1). *Let R be an integral domain with field of fractions k , and E an elliptic curve over k . Then there is a cubic equation for E in normal form with all $a_i \in R$.*

Proof. Choose any normal form for $E(k)$ with coefficients \bar{a}_i in variables \bar{x} and \bar{y} . Let u be a common denominator for all coefficients \bar{a}_i , thus $u\bar{a}_i \in R$. Let $x = u^2\bar{x}$ and $y = u^3\bar{y}$ be a change of variable. Then the coefficients $a_i = u^i\bar{a}_i \in R$ for all i . \square

Definition 61. Let K be a field with discrete valuation v , and let $E(K)$ be an elliptic curve. A minimal normal form for E is a normal form with all a_j in the valuation ring R of K such that $v(\Delta)$ is minimal among all such equations with coefficients a_j in R .

We will use the terms minimal model, minimal normal form, and minimal Weierstrass model interchangeably.

Proposition 25 ([6], V Prop 2.3). *Let E and E' be elliptic curves in minimal normal form having coefficients a_j and a'_j resp. Suppose $f : E' \rightarrow E$ be an isomorphism with $f(x) = u^2x' + r$ and $f(y) = u^3y' + su^2x' + t$. Then $v(\Delta) = v(\Delta')$, $u \in R^*$, and $r, s, t \in R$. The differential ω is unique up to a unit in R .*

Proof. By definition, $v(\Delta) = v(\Delta')$, and hence $v(u) = 0$ so $u \in R^*$ from $u^{12}\Delta' = \Delta$. The relation $u^8b'_8 = b_8 + \dots$ in R implies that $3r$ is in R , and the relation $u^6b'_6 = b_6 + \dots$ in R implies that $4r$ is in R . Hence the difference r is in R . The relation $u^2a'_2 = a_2 + \dots$ in R implies that s is in R and the relation $u^6a'_6 = a_6 + \dots$ implies that t is in R . The last assertion follows from the formula $f(\omega) = u^{-1}\omega'$. \square

Proposition 26 ([6], V Prop 2.4). *If all a_j are in R , and if $0 \leq v(\Delta) < 12$, then the model is minimal.*

Proposition 27 ([6], V Prop 2.5). *Let $E(K)$ be an elliptic curve, and further assume that the characteristic of K is unequal to 2 or 3. For a minimal model the valuation of the discriminant satisfies*

$$v(\Delta) + \min\{v(j), 0\} < 12 + 12v(2) + 6v(3).$$

In addition, assuming that the residue class characteristic is different from 2 and 3, it follows that a model over R is minimal if and only if $v(\Delta) + \min\{v(j), 0\} < 12$.

Proof. Since $c_4^3 = \Delta \cdot j$ and $c_6^2 = \Delta(j - 12^3)$, we have the relations $v(\Delta) + v(j) = 3v(c_4)$ and $v(\Delta) + v(j - 12^3) = 2v(c_6)$. By equation 3.12, we can thus transform the equation of the cubic into the form

$$y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}.$$

Hence, if $48p^4 | c_4$ and $864p^6 | c_6$, then the equation is not minimal. Since the equation is minimal it follows that

$$v(\Delta) + v(j) = 3v(c_4) < 12 + 3v(48) = 12 + 12v(2) + 3v(3),$$

or

$$v(\Delta) + v(j - 12^3) = 2v(c_6) < 12 + 2v(864) = 12 + 10v(2) + 6v(3).$$

As $v(\Delta) + \{v(j), 0\} \leq v(\Delta) + v(j)$ or $v(\Delta) + v(j - 12^3)$, the first inequality is obtained.

For the second statement note that for $v(2) = v(3) = 0$, the minimal model satisfies $v(\Delta) + \min\{v(j), 0\} < 12$. The converse holds since $0 < v(\Delta) + \min\{v(j), 0\}$ and the relation between the two valuations of the discriminants. \square

3.4 Reduction Modulo p

We provide motivation for investigating elliptic curves modulo primes by stating the following theorem:

Theorem (Hasse-Minkowski). *Let $F(X_1, \dots, X_n) \in \mathbb{Q}[X_1, \dots, X_n]$ be a quadratic form (homogeneous polynomial of degree 2 in n variables). The equation*

$$F(X_1, \dots, X_n) = 0$$

has non-trivial solutions in \mathbb{Q} if and only if it has non-trivial solutions in \mathbb{Q}_p for each $p \leq \infty$.

The thrust of the theorem above, also known as the local-global principle, is that local solutions, i.e. reduction modulo p , may provide information for global solutions. As elliptic curves are quite complicated structures, it may be useful to investigate curves locally.

We use [6], V §3.

Let R be a factorial ring with field of fractions k . Given any irreducible p in R we can form $R/p = R/Rp$ and denote its field of fractions by $k(p)$. Each element a in k can be decomposed as

$$a = p^n \frac{u}{v}$$

where n is an integer uniquely determined by a and $p \nmid u, v$.

Define an order function $\text{ord}_p(a) = n$ associated with p . Let $r_p(a) = \bar{a}$ denote the canonical reduction modulo p defined from $R \rightarrow k(p)$. If $R_{(p)} = \{a \in k \mid \text{ord}_p(a) \geq 0\}$, then the mod p reduction is well defined on $R_{(p)} \rightarrow k(p)$.

The order function satisfies the valuation properties

$$\text{ord}_p(ab) = \text{ord}_p(a) + \text{ord}_p(b)$$

and

$$\text{ord}_p(a + b) \geq \min\{\text{ord}_p(a), \text{ord}_p(b)\}.$$

Definition 62. The *reduction modulo p* function $r_p : \mathbb{P}(k) \rightarrow \mathbb{P}_n(k(p))$ is defined by the relation

$$r_p(y_0 : \cdots : y_n) = (\bar{y}_0 : \cdots : \bar{y}_n)$$

where $(y_0 : \cdots : y_n)$ are the homogeneous coordinates of a point $\mathbb{P}_n(k)$ with all y_i in R without a common irreducible factor. Such a representative of a point is called *reduced*.

Definition 63. Let E be an elliptic curve in minimal normal form over k with equation $y^2 + a_1xy + a_3y = x^3 + a_2x + a_4x + a_6$. The reduction \bar{E} of E modulo p is given by

$$y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x + \bar{a}_4x + \bar{a}_6.$$

The discriminant of the reduced curve \bar{E} is $\bar{\Delta}$, the reduction modulo p of the discriminant Δ of E . The curve \bar{E} is nonsingular if and only if $\bar{\Delta} \neq 0$, or alternatively, if and only if $\text{ord}_p \Delta = 0$.

Definition 64. An elliptic curve E defined over k has *good reduction* at p provided \bar{E} , the reduced curve at p is nonsingular. When \bar{E} is singular, we say that E has bad reduction at p .

Proposition 28 ([6], V Prop 3.4). *Let E be an elliptic curve over k which has good reduction at p . Then the reduction function $r_p : E(k) \rightarrow \bar{E}(k(p))$ is a group morphism.*

Proof. Certainly the identity is preserved as $r_p(0 : 1 : 0) = (0 : 1 : 0)$. For any $P, Q \in E(k)$ let L be the line connecting P and Q with $P \neq Q$, or the tangent line to E when $P = Q$. The line L reduces to \bar{L} , the line through $r_p(P)$ and $r_p(Q)$. Then for any $P, Q \in E(k)$,

$$r_p(P + Q) = r_p((PQ)\mathcal{O}) = (r_p(P)r_p(Q))r_p(\mathcal{O}) = r_p(P) + r_p(Q).$$

Thus r_p is a group morphism. □

Remark. The identity $\mathcal{O} = (0 : 1 : 0)$ is found both on E and the reduced curve over $k(p)$. Thus, the p -reduced points $(X : Y : Z)$ on $E(k)$ is in $\ker(r_p)$ if and only if $\text{ord}_p(Y) = 0$, $\text{ord}_p(Z) > 0$ and $\text{ord}_p(X) > 0$. We can thus divide by Y and assume that the point is of the form $(X : 1 : Z)$.

For the sake of completeness, we state the following:

- (a) **Good Reduction.** If $p \neq 2$ and $p \nmid \Delta$, then \bar{E} is an elliptic curve over \mathbb{F}_p . Given a point $P = (x : y : z)$ on E , we can choose a representative (x, y, z) for P with $x, y, z \in \mathbb{Z}$ and having no common factor, then $\bar{P} \stackrel{\text{def}}{=} (\bar{x} : \bar{y} : \bar{z})$ is a well-defined point on \bar{E} . Since $(0 : 1 : 0)$ reduces to $(0 : 1 : 0)$ and lines reduce to lines, the map $E(\mathbb{Q}) \rightarrow \bar{E}(\mathbb{F}_p)$ is a homomorphism.
- (b) **Additive Reduction (Cusp).** This is the case in which the reduced curve \bar{E} has a cusp if and only if $\text{ord}_p(c_4) > 0$ or $\text{ord}_p(b_2) > 0$

(c) **Multiplicative Reduction (Node).** This is the case in which the reduced curve \bar{E} has a node if and only if $\text{ord}_p(c_4) = 0$ or $\text{ord}_p(b_4) = 0$. The tangents at the node are rational over \mathbb{F}_p if and only if $-2ab$ becomes a square in \mathbb{F}_p . As a result $\bar{E}^{\text{ns}} \approx \mathbb{G}_m$. The curve E is said to have split multiplicative reduction in this case. If $-2ab$ is not a square modulo p , then $\bar{E}^{\text{ns}} \approx \mathbb{G}_m[-2\bar{ab}]$. The curve E is said to have nonsplit multiplicative reduction in this case.

If E has good or nodal reduction, then the minimal equation remains minimal after replacing the ground field by a larger field. However, this is not so for cuspidal reduction. As an example, consider the curve

$$E : Y^2Z = X^3 + pXZ^2 + pZ^3.$$

After passing to an extension field in which p becomes a sixth power, say $p = \pi^6$, we can make a change of variables so that the equation becomes

$$E : Y^2Z = X^3 + \pi^2XZ^2 + Z^3.$$

This reduces modulo π to

$$Y^2Z = X^3 + Z^3,$$

which is nonsingular. In fact, for any curve E with cuspidal reduction at p , there exists a finite extension of the ground field such that E will have either good or nodal reduction at the primes over p . Thus, good or nodal reduction are not changed by a field extension (further, the minimal equation remains minimal) but cuspidal reduction always becomes good or nodal reduction in an appropriate finite extension. For this reason a curve is said to have semistable reduction at p if it has good or nodal reduction there.

Remark. If E has multiplicative reduction at p then $\text{ord}_p(j(E)) < 0$ since $j(E) = c_4^3/\Delta$ and $\text{ord}_p(c_4) = 0$.

Let E be an elliptic curve over k with $j(E) \in R$, that is, with $\text{ord}_p(j(E)) \geq 0$ for all p , even at those irreducibles p where E has bad reduction.

Proposition 29 ([6], V Prop 4.1). *Let E be an elliptic curve over k , and $(X, 1, Z) \in E(k)$. If $\text{ord}_p(Z) > 0$, then $\text{ord}_p(X) > 0$, and the relation $\text{ord}_p(Z) = 3 \text{ord}_p(X)$ holds.*

Proof. For $Y = 1$, the projective normal form for E has the form

$$Z + a_1ZX + a_3Z^2 = X^3 + a_2ZX^2 + a_4Z^2X + a_6Z^3.$$

We prove by contradiction, so assume that $\text{ord}_p(Z) > 0$ and $\text{ord}_p(X) \leq 0$. For the right hand side of the equation RHS,

$$\text{ord}_p(\text{RHS}) = \text{ord}_p(X^3) = 3 \text{ord}_p(X) \leq 0,$$

and for the left hand side LHS,

$$\text{ord}_p(\text{LHS}) = \min\{\text{ord}_p(Z), \text{ord}_p(X) + \text{ord}_p(Z) + \text{ord}_p(a_1)\}.$$

Since $\text{ord}_p(Z) > 0$, we have the relation

$$3 \text{ord}_p(X) \geq \text{ord}_p(X) + \text{ord}_p(Z) \quad \text{or} \quad 0 \geq 2 \text{ord}_p(X) \geq \text{ord}_p(Z),$$

a contradiction.

Observe that $\text{ord}_p(Z) = \text{ord}_p(Z + a_1ZX + a_3Z^2)$ since $\text{ord}_p(Z) < \min\{\text{ord}_p(a_1ZX), \text{ord}_p(a_3Z^2)\}$.

Thus we obtain

$$\text{ord}_p(Z) = \text{ord}_p(X^3 + a_2ZX^2 + a_4Z^2X + a_6Z^3) = 3 \text{ord}_p(X)$$

where we have checked the four possible minima in

$$\text{ord}_p(Z) \geq \min\{\text{ord}_p(X^3), \text{ord}_p(a_2ZX^2), \text{ord}_p(a_4Z^2X), \text{ord}_p(a_6Z^3)\},$$

proving the proposition. □

3.5 The Torsion Subgroup

Reference [6] is used, while we have provided an alternative proof of Theorem 17. For primes p , we use the notation \mathbb{F}_p for the finite field of p elements.

The main results here, Theorems 16, 17 and 18, were discovered independently by Lutz and Nagell in the 1930s; different authors ([6], [16], [7]) refer to any one or more of them as "the Lutz-Nagell Theorem".

We restrict ourselves to \mathbb{Q} in this section. In the next section we will see that by applying Dirichlet's Unit Theorem and the finiteness of the Ideal Class group to an elliptic curve E defined over \mathbb{Q} ,

$$E(\mathbb{Q}) \cong \mathbb{Z}^{r_E} \times \mu(E(\mathbb{Q})),$$

where r_E is the arithmetic rank of the curve. In this section we investigate $E(\mathbb{Q})_{\text{Tors}} = \mu(E(\mathbb{Q}))$, points P which satisfy $nP = \mathcal{O}$ for some integer n ; i.e. points with finite order.

We begin by defining a filtration

$$E(\mathbb{Q}_p) \supset E^0(\mathbb{Q}_p) \supset E^1(\mathbb{Q}_p) \supset \cdots \supset E^n(\mathbb{Q}_p) \supset \cdots$$

and identify the quotients. First, we define

$$E^0(\mathbb{Q}_p) = \{P \mid \bar{P} \text{ is nonsingular}\}.$$

It is a subgroup since $(0 : 1 : 0)$ is always nonsingular. A line through two nonsingular points on a cubic will either meet the cubic again at another unique nonsingular point for a total of three unique points, or it will be a tangent at one point and intersect the curve at another unique point (possibly at \mathcal{O}) for a total of two points. If a line is tangent to the curve at a point P , we say that P has multiplicity two.

Let $\bar{E}^{ns} = \{\bar{P} \in \bar{E} \mid \bar{P} \text{ is nonsingular}\}$. The reduction map

$$P \mapsto \bar{P} : E^0(\mathbb{Q}_p) \rightarrow \bar{E}^{ns}(\mathbb{F}_p)$$

is a homomorphism, and we define $E^1(\mathbb{Q}_p)$ to be its kernel. Thus, $E^1(\mathbb{Q}_p)$ consists of points P which can be represented as $(x : y : z)$ with $p|x, z$ but $p \nmid y$. Define

$$E^n(\mathbb{Q}_p) = \left\{ P \in E^1(\mathbb{Q}_p) \mid \frac{x(P)}{y(P)} \in p^n \mathbb{Z}_p \right\}.$$

Theorem 16 ([6], V Corollary 5.3). *Let E be an elliptic curve over \mathbb{Q} .*

(a) *The subgroup $E(\mathbb{Q})_{\text{Tors}} \cap E^1(\mathbb{Q})$ is zero for each odd prime p and*

$$E(\mathbb{Q})_{\text{Tors}} \cap E^2(\mathbb{Q})$$

is zero for $p = 2$.

(b) *The restriction of the reduction homomorphism $r_p|_{E(\mathbb{Q})_{\text{Tors}}} : E(\mathbb{Q})_{\text{Tors}} \rightarrow E^p(\mathbb{F}_p)$ is injective for any odd prime p where E has good reduction and $r_2|_{E(\mathbb{Q})_{\text{Tors}}} : E(\mathbb{Q})_{\text{Tors}} \rightarrow E^2(\mathbb{F}_2)$ has kernel at most $\mathbb{Z}/2\mathbb{Z}$ when E has good reduction at 2.*

Remark. If C is a cubic defined by an equation over \mathbb{F}_q in normal form, then for each x in \mathbb{F}_q we have at most two corresponding y -values on the curve $C(\mathbb{F}_q)$, thus the cardinality $\#C(\mathbb{F}_q) \leq 2q + 1$.

Corollary 4 ([6], V Corollary 5.3). *Let E be an elliptic curve defined over \mathbb{Q} . If E has good reduction at an odd prime p , then the cardinality of the torsion subgroup satisfies $\#E(\mathbb{Q})_{\text{Tors}} \leq 2p + 1$. If E has good reduction at 2, the $\#E(\mathbb{Q})_{\text{Tors}} \leq 10$.*

Corollary 5 ([6], V Corollary 5.4). *For every elliptic curve E defined over \mathbb{Q} , the torsion subgroup $E(\mathbb{Q})_{\text{Tors}}$ of $E(\mathbb{Q})$ is finite and is either cyclic or cyclic direct sum with $\mathbb{Z}/2\mathbb{Z}$.*

3.5.1 Computing the Torsion Subgroup

Theorem 17 ([6], V §6). *Let E be an elliptic curve defined over \mathbb{Q} with an equation in normal form with integer coefficients. If $(x, y) \in E(\mathbb{Q})_{\text{Tors}}$ then the coordinates x and y are integers.*

Proof. If $y = 0$, then x is a solution to

$$0 = x^3 + a_2x^2 + a_4x + a_6 \quad (3.14)$$

where $a_i \in \mathbb{Z}$. Since x is rational, we may write $x = \frac{m}{n}$ for some integers m, n with $\gcd(m, n) = 1$. Thus, we may write (3.14) as

$$0 = m^3 + a_2m^2n + a_4mn^2 + a_6n^3,$$

and any prime dividing n must divide m . Thus $x = m$ is an integer.

If $y \neq 0$, then the point with homogeneous coordinates has the form $(x' : 1 : w) = (x : y : 1)$ where $w = 1/y$ and $x' = x/y$. By Proposition 29, we have $\text{ord}_p(w) \leq 0$ for p odd and $\text{ord}_2(w) \leq -1$ at 2. This condition means that $\text{ord}_p(y) \geq 0$ for all odd p and $\text{ord}_2(y) \leq -1$ at w . Thus y has the form $\frac{h}{2}$ for an integer h . Write $x = \frac{m}{n}$ where $\gcd(m, n) = 1$, and note that it satisfies a cubic equation

$$\left(\frac{h}{2}\right)^2 = \left(\frac{m}{n}\right)^3 + c \left(\frac{m}{n}\right)^2 + \frac{d}{2} \left(\frac{m}{n}\right) + \frac{e}{4} \quad (3.15)$$

for integers c, d, e .

We show that n is odd.

Suppose n is even; we may write $n = 2t$ for some integer t . It follows that

$$\begin{aligned} \frac{(h^2 - e)}{4} &= \frac{m^3}{8t^3} + c \cdot \frac{m^2}{4t^2} + \frac{d}{2} \cdot \frac{m}{2t} \\ &= \frac{m^3 + 2ctm^2 + 2dt^2m}{8t^3} \\ &= \frac{m^3 + 2ctm^2 + 2dt^2m}{4(2t^3)} \end{aligned} \quad (3.16)$$

The numerator on the RHS in (3.16) contains a factor of $2t^3$ (a necessary condition for the LHS's denominator to be 4), thus it is divisible by $2t = n$. Since $2t$ is a factor found in the latter two of the three terms in the numerator, the first term, i.e. m^3 , is forced to be divisible by $2t = n$. Our supposition that n is even results in a contradiction. Hence n is odd.

All that is required is to show that $n = 1$.

We currently have

$$\frac{m^3}{n^3} + c \cdot \frac{m^2}{n^2} + \frac{d}{2} \cdot \frac{m}{n} = \frac{h^2 - e}{4}.$$

Clearing denominators results in

$$4m^3 + 4cm^2n + 2dmn^2 = (h^2 - e)n^3.$$

As per the previous argument, n divides each term in the LHS, especially the term $4m^3$. We may now say that

$$n|4m^3$$

$$\implies n|4m$$

$$\implies n|4 \text{ or } n|m$$

Since n is odd, the only outcome is that $n = 1$. Thus, $x = m$. It follows that $y^2 = \text{integer}$ since a_2, a_4, a_6 are integers, so y itself must be an integer since it is rational by definition. □

The following and preceding Theorems are interchangeably called the Lutz-Nagell Theorem.

Theorem 18 ([6], V Theorem 6.2). *Let E be an elliptic curve over \mathbb{Q} , and let $y^2 = f(x)$ be a Weierstrass equation for E where $f(x)$ has integer coefficients. If (x, y) is a torsion point on E , then the integer y is zero or y divides the discriminant of the cubic polynomial $f(x)$.*

Proof. If $y = 0$ then $(x, 0)$ is of order 2. Otherwise, $2(x, y) = (x', y')$ unequal to \mathcal{O} on $E(\mathbb{Q})$. The tangent line to E at (x, y) has slope $\frac{f'(x)}{2y}$, and when its equation $y = \lambda x + \beta$ is substituted into the Weierstrass equation $y^2 = f(x) = x^3 + ax^2 + bx + c$, we obtain a cubic equation with x as double root and x' as single root. This equation has coefficient $a - (\frac{f'(x)}{2y})^2$ of x^2 , and hence the sum

of the roots of the cubic in x is the negative of this coefficient, so

$$2x + x' = a - \left(\frac{f'(x)}{2y} \right)^2.$$

Since x, x' and a are integers, it follows that $\frac{f'(x)}{2y}$ is an integer, and $2y$ divides $f'(x)$.

We can write the discriminant Δ_f of $f(x)$ as a linear combination $\Delta_f = u(x)f(x) + v(x)f'(x)$ where $u(x), v(x) \in \mathbb{Z}[x]$. Since $y = f(x)$ and y divides $f'(x)$ for the point (x, y) on E , we deduce that y divides Δ_f . This proves the theorem. \square

3.6 Finite Basis for an Elliptic Curve

The following section investigates Mordell's Theorem, which is the basis for the formulation of the Birch and Swinnerton-Dyer conjecture. This theorem was proven in 1922 by Louis Mordell after a Henri Poincare conjecture in 1901. Further, it was generalised to abelian varieties by Andre Weil in 1928.

3.6.1 Mordell's Theorem

This section is sourced from [6], VI §4.

Let R be a factorial ring with field of fractions k . Observe that c is a square in k if and only if $\text{ord}_p(c)$ is an even number for all irreducibles p . Let (x, y) be a point on the elliptic curve $E(k)$ defined by a factored Weierstrass equation $y^2 = (x - r_1)(x - r_2)(x - r_3)$. A point $(x, y) \in 2E(k)$ if and only if all $x - r_i$ are squares for $i = 1, 2, 3$. In particular, $\text{ord}_p(x - r_i)$ is even for such points. We have the following proposition.

Proposition 30 ([6], VI Prop 4.1). *Let E be an elliptic curve defined by*

$$y^2 = (x - r_1)(x - r_2)(x - r_3) \tag{3.17}$$

where distinct r_1, r_2 and r_3 are in R . If (x, y) is a point of $E(k)$, then $\text{ord}_p(x - r_i)$ is even for all irreducibles p not dividing any elements $r_i - r_j$ for $i \neq j$.

Proof. Let p be an irreducible not dividing $r_i - r_j$, or equivalently, $\text{ord}_p(r_i - r_j) = 0$ for $i \neq j$. If $\text{ord}_p(x - r_i) < 0$ for one i , then for all $j = 1, 2, 3$ we have $\text{ord}_p(x) = \text{ord}_p(x - r_i) = \text{ord}_p(x - r_j)$ since each $\text{ord}_p(r_j) \geq 0$. It follows that

$$2\text{ord}_p(y) = \text{ord}_p(y^2) = \text{ord}_p((x - r_1)(x - r_2)(x - r_3)) = 3\text{ord}_p(x),$$

and hence $\text{ord}_p(x) = \text{ord}_p(x - r_j)$ is even for each j . Hence, if $\text{ord}_p(x - r_i) > 0$, for one root r_i , then we have the relation

$$2\text{ord}_p(y) = \text{ord}_p(y^2) = \text{ord}_p(x - r_i),$$

and thus all $\text{ord}_p(x - r_j)$ are even. This proves the proposition. \square

Remark. The equation (3.17), written as $y^2 = f(x)$, may seem to be a special case of an elliptic curve in that $f(x)$ is separable in R , but in fact it is not. If any of the roots $r_i \in k$ but $r_i \notin R$, an admissible change of variables transforms the equation to one with all $r_i \in R$ [18]. We comment later on the general case, where the r_i may not even be in k (see Remark C).

Notation. Let E be an elliptic curve defined by the equation

$$y^2 = (x - r_1)(x - r_2)(x - r_3)$$

where each $r_i \in R$.

(a) Let $P(E)$ denote the set of all irreducibles p (up to units in R) such that p divides some $r_i - r_j$, where $i \neq j$. Then $P(E)$ is a finite set. Let $A(E)$ denote the subgroup of all cosets $a(k^*)^2$ in $k^*/(k^*)^2$ such that $\text{ord}_p(a)$ is even for $p \notin P(E)$.

(b) Let $\theta_1, \theta_2, \theta_3$ be three functions with $\theta_i : E(k) \rightarrow A(E) \subset k^*/(k^*)^2$ for $i = 1, 2, 3$ given by the relations

(i) $\theta_i(0) = 1$;

(ii) $\theta_i((r_i, 0)) = (r_i - r_j)(r_k - r_i) \text{mod}(k^*)^2$ for $\{i, j, k\} = \{1, 2, 3\}$;

(iii) $\theta_i((x, y)) = (x - r_i) \text{mod}(k^*)^2$ otherwise.

Proposition 31 ([6], VI Prop 4.3). *The functions $\theta_i : E(k) \rightarrow A(E)$ are group homomorphisms and*

$$\ker(\theta_1) \cap \ker(\theta_2) \cap \ker(\theta_3) \subset 2E(k).$$

Proof. Consider three points $P_i = (x_i, y_i)$ on $E(k) \cap L$, where L is a line intersecting E . The line is vertical if and only if some $P_j = \mathcal{O}$, and then by inspection $\theta_i(P_1)\theta_i(P_2)\theta_i(P_3) = 1$ in $k^*/(k^*)^2$. Otherwise the line is of the form $y = \lambda x + \beta$, and x_1, x_2 and x_3 are roots of the equation $(\lambda x + \beta)^2 = (x - r_1)(x - r_2)(x - r_3)$. Hence $x_1 - r_i, x_2 - r_i, x_3 - r_i$ are roots of the equation

$$(\lambda(x + r_i) + \beta)^2 = f(x + r_i) = x^3 + ax^2 + bx,$$

where $f(r_i) = 0$. Rearranging, we obtain

$$0 = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda(\lambda r_i + \beta))x - (\lambda r_i + \beta)^2,$$

which lead to the following cases.

Case 1. All $P_j = (r_j, 0)$ for $j = 1, 2, 3$. Then we calculate

$$\begin{aligned} \theta_i(P_1)\theta_i(P_2)\theta_i(P_3) &= (x_1 - r_i)(x_2 - r_i)(x_3 - r_i) = -[-(r_i + \beta)^2] \\ &\equiv 1 \pmod{(k^*)^2}. \end{aligned}$$

Case 2. Some $P_j = (r_i, 0)$ which we can take to be $P_i = (r_i, 0)$. Then $0, x_2 - r_1, x_3 - r_1$ are the roots of the cubic which means $\beta = -\lambda r_i$, and the equation becomes $0 = x^3 + (a - \lambda^2)x^2 + bx$. Now we have

$$(x_2 - r_1)(x_3 - r_1) = b = (r_2 - r_1)(r_3 - r_1),$$

and we calculate for $\{i, j, k\} = \{1, 2, 3\}$

$$\begin{aligned}\theta_i(P_i)\theta_i(P_j)\theta_i(P_k) &= (r_j - r_i)(r_k - r_i)(x_j - r_i)(x_k - r_i) \\ &= (r_j - r_i)^2(r_k - r_i)^2 \\ &\equiv 1 \pmod{(k^*)^2}.\end{aligned}$$

Hence, each θ_i is a group morphism. \square

Remark (A). The three morphisms of the previous proposition combine to define a group homomorphism

$$\theta = (\theta_1, \theta_2, \theta_3) : E(k) \rightarrow A(E)^3, \quad (3.18)$$

where $\ker(\theta) \subset 2E(k)$ by the previous proposition. Thus $E(k)/2E(k)$ is a sub-quotient of $A(E)^3$, and $(E(k) : 2E(k))$ is finite whenever $A(E)$ is finite. This map θ is known as the *descent map* in honour of Fermat, who first used descent arguments.

Remark (B). The group $A(E)$ is finite for any principal ideal ring R where each $k(p)$ and $R^*/(R^*)^2$ are finite. This holds for $R = \mathbb{Z}$ and $k = \mathbb{Q}$, hence we have:

Theorem 19 (Weak Mordell Theorem, [6] VI §4). *Let $y^2 = (x-r_1)(x-r_2)(x-r_3)$ define an elliptic curve E over \mathbb{Q} where each $r_i \in \mathbb{Z}$. Then the index $(E(\mathbb{Q}) : 2E(\mathbb{Q}))$ is finite.*

Remark (C). If $f(x)$ is not separable in k , we extend to a number field K where $f(x)$ is separable, then $(E(k) : 2E(k))$ is finite if $(E(K) : 2E(K))$ is finite. We then have:

Theorem 20 (Weak Mordell-Weil Theorem, [6] VI §4). *Let E be an elliptic curve over an algebraic number field k . Then the index $(E(k) : 2E(k))$ is finite.*

Proof. We may assume E is defined by an expression $y^2 = f(x)$ where $f(x)$ is a cubic with three integral roots in k by Remark C. We take for R in k the principal ideal ring equal to the ring of integers in k with a finite set of primes in k localised. By the finiteness of the ideal class group we could localise at those

primes which divide a finite set of representatives of the ideal class group. If the ideal class group is zero, the ring is principal.

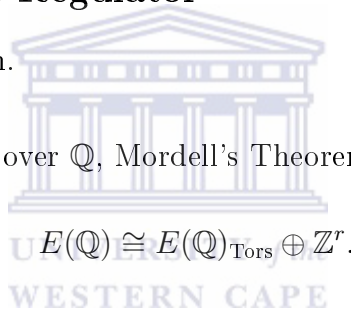
The group of units R^* is finitely generated by the Dirichlet Unit Theorem, thus $R^*/(R^*)^2$ is finite. Now $A(E)$ is finite by Remark B and we can apply Remark A to prove the theorem. \square

Among the elementary quantities associated with elliptic curves over \mathbb{Q} , the rank is usually the most computationally intensive to determine. With this in mind, we now consider a useful approach with which to find generators for elliptic curves.

3.6.2 Defining the Regulator

We use [11] in this section.

Given an elliptic curve E over \mathbb{Q} , Mordell's Theorem states that



$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{Tors}} \oplus \mathbb{Z}^r.$$

We will investigate a method which can determine if a set of points is linearly independent or not, thereby giving, at least, a lower bound for the rank of a curve. Note that as these computations can be demanding, we will check whether the linear combination of a set of points results not only in \mathcal{O} but possibly other torsion points as well. Ultimately, some scalar multiple of a torsion point will take us to \mathcal{O} , but being open to linear combinations resulting in torsion points should, in theory at least, allow computations to terminate more quickly.

Definition 65. Let curve E be an elliptic curve over \mathbb{Q} . The rational points $P_1, \dots, P_m \in E(\mathbb{Q})$ are *linearly dependent* over \mathbb{Z} if there are integers $n_1, \dots, n_m \in \mathbb{Z}$ such that

$$n_1P_1 + \dots + n_mP_m = T$$

where T is a torsion point. If no such expression exists, we say that the points are *linearly independent* over \mathbb{Z} .

We introduce the height function $h : \mathbb{Q} \rightarrow \mathbb{Z}$ defined by

$$h\left(\frac{m}{n}\right) = \log(\max\{|m|, |n|\})$$

for $m, n \in \mathbb{Z}$. We now define the *canonical height* of $P \in E(\mathbb{Q})$ by

$$\hat{h}(P) = \frac{1}{2} \lim_{N \rightarrow \infty} \frac{H(2^N \cdot P)}{4^N}.$$

Proposition (Neron-Tate). *Let E/\mathbb{Q} be an elliptic curve and \hat{h} the canonical height on E .*

- (i) *For all $P, Q \in E(\mathbb{Q})$, $\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q)$.*
- (ii) *For all $P \in E(\mathbb{Q})$ and $m \in \mathbb{Z}$, $\hat{h}(mP) = m^2 \cdot \hat{h}(P)$.*
- (iii) *Let $P \in E(\mathbb{Q})$. Then $\hat{h}(P) \geq 0$, and $\hat{h}(P) = 0$ if and only if P is a torsion point.*

We now give the framework for determining if a set of points is linearly independent.

Definition 66. The *Neron-Tate pairing* attached to an elliptic curve is defined by

$$\langle \cdot, \cdot \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \rightarrow \mathbb{R}, \quad \langle P, Q \rangle = \hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q).$$

Let P_1, \dots, P_r be r rational points on $E(\mathbb{Q})$. The *elliptic height matrix* associated to $\{P_i\}_{i=1}^r$ is

$$\mathcal{H} = \mathcal{H}(\{P_i\}_{i=1}^r) := (\langle P_i, P_j \rangle)_{1 \leq i \leq r, 1 \leq j \leq r}.$$

The determinant of \mathcal{H} is called the *elliptic regulator* of the set of points $\{P_i\}_{i=1}^r$. If $\{P_i\}_{i=1}^r$ is a complete set of generators of the free part of $E(\mathbb{Q})$, then the determinant $\mathcal{H}(\{P_i\}_{i=1}^r)$ is called the *elliptic regulator of E/\mathbb{Q}* , denoted $\text{Reg}(E/\mathbb{Q})$.

Theorem 21 ([11] II §7). *The Néron-Tate pairing $\langle \cdot, \cdot \rangle$ associated to E is a non-degenerate symmetric bilinear form on $E(\mathbb{Q})/E_{\text{Tors}}(\mathbb{Q})$, that is*

- (i) *For all $P, Q \in E(\mathbb{Q})$, $\langle P, Q \rangle = \langle Q, P \rangle$.*

(ii) For all $P, Q, R \in E(\mathbb{Q})$ and all $m, n \in \mathbb{Z}$,

$$\langle P, mQ + nR \rangle = m \langle P, Q \rangle + n \langle P, R \rangle.$$

(iii) Suppose $P \in E(\mathbb{Q})$ and $\langle P, Q \rangle = 0$ for all $Q \in E(\mathbb{Q})$. Then $P \in E_{tors}(\mathbb{Q})$.
In particular, P is a torsion point if and only if $\langle P, P \rangle = 0$.

The previous theorem has the following important corollary:

Corollary 6 ([11] II §7). Let E/\mathbb{Q} be an elliptic curve and let $P_1, \dots, P_r \in E(\mathbb{Q})$ be rational. Let \mathcal{H} be the elliptic height matrix associated to $\{P_i\}_{i=1}^r$.

(i) Suppose $\det(\mathcal{H}) = 0$ and $u = (n_1, \dots, n_r) \in \text{Ker}(\mathcal{H})$, with $n_i \in \mathbb{Z}$. Then the points $\{P_i\}_{i=1}^r$ are linearly dependent and $\sum_{k=1}^r n_k P_k = T$ where T is a torsion point on $E(\mathbb{Q})$.

(ii) If $\det(\mathcal{H}) \neq 0$ then the points $\{P_i\}_{i=1}^r$ are linearly independent and the rank of $E(\mathbb{Q})$ is greater than or equal to r .

3.6.3 Numerical Example

We discuss the numerical example [18], VIII §2 Example 8.5. We then generalise the concepts used in this section to provide a link with the Shafarevich-Tate group.

Let $E(\mathbb{Q})$ be an elliptic curve with Weierstrass equation

$$E : y = x(x - 2)(x + 2).$$

If $y = 0$, then $x = 0, \pm 2$. Therefore, assume $y \neq 0$. The product of $x, x - 2, x + 2$ is a square; each of these factors should, in some sense, be close to being square.

Write

$$\begin{aligned} x &= au^2 \\ x - 2 &= bv^2 \\ x + 2 &= cw^2 \end{aligned}$$

for rationals a, b, c, u, v, w . Then $y = abc(uvw)^2$, so abc must be a square. We adjust u, v, w to have a, b, c as squarefree integers. We claim that

$$a, b, c \in \{\pm 1, \pm 2\}.$$

Suppose p is an odd prime dividing a . Since a is squarefree, $p^2 \nmid a$, so the exact power p^k dividing $x = au^2$ has k odd. If $k < 0$, then p^k is the exact power of p in the denominator of $x \pm 2$, so p^{3k} is the power of p in the denominator of $y^2 = x(x-2)(x+2)$. However, this is a contradiction since $3k$ is odd and y^2 is a square. If $k > 0$, then $x \equiv (\text{mod } p)$, so $x \pm 2 \not\equiv (\text{mod } p)$. There p^k is the power of p dividing y^2 . Again, k is odd so this is impossible. Thus, $p \nmid a$. Similarly, no odd prime divides b or c . Therefore, each of a, b, c is, up to sign, a power of 2. They are squarefree, proving the claim.

The procedure we are using is called *descent*; precisely, it is a *2-descent*. If x is rational with at most N digits in its numerator and denominator, then u, v, w should have at most $N/2$ digits approximately in their numerators and denominators. So if we are searching for points (x, y) , we can instead search for smaller numbers u, v, w . This method is named so in honour of Fermat.

We have four choices for a and a further four for b . Since a and b together determine c (abc is a square), there are 16 possibilities for a, b, c , some of which can be eliminated fairly easily. Since $x(x-2)(x+2) = y^2 > 0$, we have $cw^2 = x+2 > 0$, so $c > 0$. Since $abc > 0$, it follows that a and b must have the same sign. This, there are now 8 possible combinations.

Consider $(a, b, c) = (1, 2, 2)$. We have

$$x = u^2, \quad x - 2 = 2v^2, \quad x + 2 = 2w^2$$

for rationals u, v, w . Therefore,

$$u^2 - 2v^2 = 2, \quad u^2 - 2w^2 = -2.$$

If v has 2 in its denominator, then $2v^2$ has an odd power of 2 in its denominator. But u^2 has an even power of 2 in its denominator, so $u^2 - 2v^2$ cannot be an integer. Therefore, u and v have odd denominators, meaning we may consider

u, v mod powers of 2. Since $2|u^2$, we have $2|u$, and hence $4|u^2$. Therefore, $-2v^2 \equiv 2 \pmod{4}$, which implies that $2 \nmid v$. Similarly, $-2w^2 \equiv -2 \pmod{4}$, so $2 \nmid w$. It follows that $v^2 \equiv w^2 \equiv 1 \pmod{8}$, so

$$2 \equiv u^2 - 2v^2 \equiv u^2 - 2 \equiv u^2 - 2w^2 \equiv -2 \pmod{8},$$

a contradiction. It follows that $(a, b, c) = (1, 2, 2)$ is impossible. Similarly, we can eliminate $(-1, -1, 1)$, $(2, 1, 2)$ and $(-2, -2, 1)$ for (a, b, c) , and the points

$$(a, b, c) = (1, 1, 1), (-1, -2, 2), (2, 2, 1), (-2, -1, 2)$$

remain. These combinations correspond to

$$\mathcal{O}, (0, 0), (2, 0), (-2, 0).$$

By Lutz-Nagell, there are no nontrivial points of odd order. Therefore we have found all rational points on E .

UNIVERSITY of the
WESTERN CAPE

3.7 The Shafarevich-Tate Group

References [4, 6, 16, 18] are used.

Let E be an elliptic curve defined over \mathbb{Q} . As noted earlier, one of the methods used to calculate the rank of the Mordell-Weil group $E(\mathbb{Q})$ is to look for generators for $E(\mathbb{Q})/mE(\mathbb{Q})$ by way of homogeneous spaces [4]. These homogeneous spaces are twists of E , i.e. curves of genus 1 isomorphic to E over some number field. Further, these homogeneous spaces are not required to have rational points, thus they are not required to be elliptic curves. If they do have rational points, those points map to rational points on E . The homogeneous spaces have equations of the form

$$H : y^2 = g(x) = ax^4 + bx^3 + cx^2 + dx + e \tag{3.19}$$

where $g(x)$ is a quartic with rational coefficients. Whether H has points over \mathbb{Q} or some completion, i.e. the p -adics \mathbb{Q}_p or the reals \mathbb{R} , will be of interest to us. The set of all the rational points on the quartics will cover the cosets of $2E(\mathbb{Q})$ in $E(\mathbb{Q})$. Quartics with no rational point but which are locally soluble in each completion arise from non-trivial elements in the Shafarevich-Tate group, denoted III . The non-triviality of the Shafarevich-Tate group means there is no general procedure for finding the rank of $E(\mathbb{Q})$. However, the conjectured finiteness of the Shafarevich-Tate group is closely linked with the BSD Conjecture. This will be discussed in more detail in Chapter 4.

3.7.1 A First Look at III

We begin by generalising the procedure used in Section 3.6.3.

Let E be an elliptic curve of the form

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

with $e_1, e_2, e_3 \in \mathbb{Z}$. If $y = 0$, we have that $x = e_1, e_2$ or e_3 . Therefore assume $y \neq 0$. Since the product of $x - e_1, x - e_2$ and $x - e_3$ is a square, each of these factors should not be squarefree. Write

$$x - e_1 = au^2$$

$$x - e_2 = bv^2$$

$$x - e_3 = cw^2$$

with rationals a, b, c, u, v, w . Then $y^2 = abc(uvw)^2$, and hence

abc is a square.

Assume that a, b, c are squarefree as we can adjust u, v, w if necessary.

Proposition 32 ([18], VIII Proposition 8.3). *Let*

$$S = \{p \mid p \text{ is a prime and } p \mid (e_1 - e_2)(e_1 - e_3)(e_2 - e_3)\}.$$

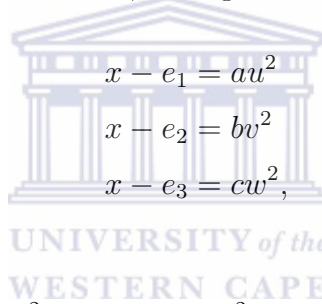
If p is a prime and $p|abc$, then $p \in S$.

Proof. Suppose that $p|a$. Then p^k , with k odd, is the exact power of p dividing $x - e_1$. If $k < 0$, then p^k is the power of p in the denominator of $x - e_2$ and $x - e_3$. Therefore $k > 0$. This means that $x \equiv e_1 \pmod{p}$. Also, x has no p in its denominator, so the same is true for $bv^2 = x - e_2$ and $cw^2 = x - e_3$. Moreover, $bv^2 \equiv e_1 - e_2$ and $cw^2 \equiv e_1 - e_3 \pmod{p}$. If $p \notin S$, then the power of p in

$$y^2 = (au^2)(bv^2)(cw^2)$$

is $p^k p^0 p^0 = p^k$, a contradiction as k is odd. Therefore, $p \in S$. □

Further, for the elliptic curve E , noting the equations



$$\begin{aligned} x - e_1 &= au^2 \\ x - e_2 &= bv^2 \\ x - e_3 &= cw^2, \end{aligned}$$

it follows that

$$au^2 - bv^2 = e_2 - e_1, \quad au^2 - cw^2 = e_3 - e_1.$$

This defines a curve $C_{a,b,c}$ in u, v, w . To be precise, it is the intersection of two quadratic surfaces. If it has a rational point, it can be transformed into an elliptic curve; in fact, it can be shown that this is the original elliptic curve. See [18] 2.5.4 for more details. If $C_{a,b,c}$ does not have a rational point, then the triple (a, b, c) is eliminated. Elimination of points usually depends on whether they do not have points in some completion \mathbb{Q}_p for $p \leq \infty$ ($p = \infty$ means the reals). The 2-Selmer group S_2 is defined to be the set of (a, b, c) such that $C_{a,b,c}$ has a real point and has p -adic points for $p \leq \infty$.

$$S_2 = \{(a, b, c) | C_{a,b,c}(\mathbb{Q}_p) \text{ is nonempty for all } p \leq \infty\},$$

i.e., those points that cannot be eliminated by sign or congruence considerations.

We regard

$$S_2 \subset (\mathbb{Q}^\times / \mathbb{Q}^{\times 2}) \oplus (\mathbb{Q}^\times / \mathbb{Q}^{\times 2}) \oplus (\mathbb{Q}^\times / \mathbb{Q}^{\times 2}).$$

The prime divisors of a, b, c divide $(e_1 - e_2)(e_1 - e_3)(e_2 - e_3)$, which implies that S_2 is a finite group.

The descent map ϕ gives a map

$$\phi : E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow S_2. \quad (3.20)$$

The 2-torsion in the Shafarevich-Tate group is the cokernel of this map:

$$\text{III}_2 = S_2/\text{Im}\phi,$$

so we can construct an exact sequence

$$0 \rightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \rightarrow S_2 \rightarrow \text{III}_2 \rightarrow 0. \quad (3.21)$$

The group III_2 represents those triples (a, b, c) such that $C_{a,b,c}$ has a p -adic point for all $p \leq \infty$, but has no rational point. If (a, b, c) represents a nontrivial element of III then it is usually difficult to show that $C_{a,b,c}$ does not have rational points. The possible nontriviality of III means that we do not have an efficient algorithm for finding the rank of the group $E(\mathbb{Q})$. The group S_2 can be computed exactly, and provides an upper bound for the rank.

3.7.2 An Example of a Nontrivial III

The following is sourced from [18] VIII.

Let $E(\mathbb{Q})$ be an elliptic curve given by

$$y^2 = x(x - 2p)(x + 2p),$$

with p prime. We encounter the following equations after applying 2-descent on E ,

$$\begin{aligned}x &= u^2, \\x - 2p &= pv^2, \\x + 2p &= pw^2.\end{aligned}$$

These equations define an intersection of two quadratic surfaces

$$C_{1,p,p} : u^2 - pv^2 = 2p, \quad u^2 = pw^2 = -2p. \quad (3.22)$$

Theorem 22 ([18], VIII Theorem 8.28). *If $p \equiv 9 \pmod{16}$, then $C_{1,p,p}$ has q -adic points for all primes $q \leq \infty$, but has no rational points.*

Proof. We show that there are no rational points by contradiction. Suppose there is a rational point (u, v, w) . Without loss of generality, we may assume $u, v, w > 0$. If p divides the denominator of v , then an odd power of p is present in the denominator of pv^2 , an even power of p is found in the denominator of u^2 , so $u^2 - pv^2$ cannot be an integer, a contradiction. Thus, u, v, w have no p in their denominators.

We show that the denominators of u, v, w are equal. Since $u^2 = 2p + pv^2$, we have $u \equiv 0 \pmod{p}$. Write

$$u = \frac{pr}{e}, \quad v = \frac{s}{e}, \quad w = \frac{t}{e},$$

for positive integers r, s, t, e and with

$$\gcd(r, e) = \gcd(s, e) = \gcd(t, e) = 1.$$

The equations for $C_{1,p,p}$ become

$$pr^2 - s^2 = 2e^2, \quad pr^2 - t^2 = -2e^2.$$

Subtraction yields

$$s^2 + 4e^2 = t^2.$$

If s is even, then $pr^2 = s^2 + 2e^2$ is even, so r is even. Then $2e^2 = pr^2 - s^2 \equiv 0 \pmod{4}$, which implies that e is even, a contradiction to $\gcd(s, e) = 1$. Therefore s is odd, and

$$\gcd(s, 2e) = 1.$$

By Euclid's formula for Pythagorean triples (hereafter EFPT), there are integers m, n with $\gcd(m, n) = 1$ such that

$$2e = 2mn, \quad s = m^2 - n^2, \quad t = m^2 + n^2.$$

So

$$pr^2 = s^2 + 2e^2 = (m^2 - n^2)^2 + 2(mn)^2 = m^4 + n^4.$$

Let q be a prime divisor of r . With $m \not\equiv n \pmod{2}$ by EFPT, we see that pr^2 must be odd. Thus, $q \neq 2$. Since $\gcd(m, n) = 1$, at least one of m, n is not divisible by q . Hence, both m and n are not multiples of q since $m^4 + n^4 \equiv 0 \pmod{q}$. Therefore,

$$(m/n) \equiv -1 \pmod{q}.$$

It follows that m/n has order 8 in \mathbb{F}_q^\times , so $q \equiv 1 \pmod{8}$. Since r is a positive integer and all prime factors of r are $1 \pmod{8}$, we obtain

$$r \equiv 1 \pmod{8}.$$

Therefore, $r^2 \equiv 1 \pmod{16}$, so

$$m^4 + n^4 = pr^2 \equiv 9 \pmod{16}.$$

But, for any integer j , we have $j^4 \equiv 0, 1 \pmod{16}$. Thus,

$$m^4 + n^4 \equiv 0, 1, 2 \pmod{16},$$

so $pr^2 \neq m^4 + n^4$, a contradiction, proving that $C_{1,p,p}$ has no rational points.

We now show that $C_{1,p,p}$ has q -adic points for all primes $q \leq \infty$. We consider four cases, namely: $q = \infty$, $q = 2$, $q = p$ and all other q .

We first consider the case of the reals, i.e. $q = \infty$. We choose u large so that

$u^2 > 2p$. Then choose v, w satisfying (3.22).

For $q = 2$, write

$$u = 1/2, \quad v = v_1/2, \quad w = w_1/2.$$

The equations for $C_{1,p,p}$ become

$$1 - pv_1^2 = 8p, \quad 1 - pw_1^2 = -8p.$$

We need to solve

$$v_1^2 = \frac{1 - 8p}{p}, \quad w_1^2 = \frac{1 + 8p}{p}$$

in the 2-adics. Since

$$\frac{1 \pm 8p}{p} \equiv 1 \pmod{8},$$

and since any number congruent to 1 mod 8 has a 2-adic square root, v_1, w_1 exist.

Thus, $C_{1,p,p}$ has a 2-adic point.

Consider $q = p$. Since $p \equiv 1 \pmod{4}$, there is a square root of $-1 \pmod{p}$. Since $p \equiv 1 \pmod{8}$, there is a square root of $-2 \pmod{p}$. Thus, both 2 and -2 have square roots mod p . by Hensel's Lemma, both 2 and -2 have square roots in the p -adics. Let

$$u = 0, \quad v = \sqrt{-2}, \quad w = \sqrt{2}.$$

Then u, v, w is a p -adic point on $C_{1,p,p}$.

We now consider $q \neq \infty, 2, p$. Subtracting the two equations for $C_{1,p,p}$ results in

$$w^2 - v^2 = 4, \quad u^2 - pv^2 = 2p.$$

Suppose there is a solution $(u_0, v_0, w_0) \pmod{q}$. We cannot have that $u_0 = w_0 = 0 \pmod{q}$.

Suppose $u_0 \equiv 0 \pmod{q}$. Then $w_0 \not\equiv 0 \pmod{q}$. Also, $v_0 \not\equiv 0 \pmod{q}$. Let $u = 0$. Since $-pv_0^2 \equiv 2p \pmod{q}$, Hensel's Lemma implies that there exists $v \equiv v_0 \pmod{q}$ in the q -adics such that $-pv^2 = 2p$. Hensel's Lemma applied again provides the existence of $w = w_0$ satisfying $w^2 - v^2 = 4$. Therefore, we have found a q -adic point. Similarly, if $w_0 = 0 \pmod{q}$, there is a q -adic point. Finally, suppose $u_0 \not\equiv 0 \pmod{q}$ and $w_0 \not\equiv 0 \pmod{q}$. Choose any $v \equiv v_0 \pmod{q}$.

We use Hensel's Lemma to find u, w . This yields a q -adic point.

We now need to prove that there is indeed a point mod q . Let n be a quadratic nonresidue mod q . Then every element of \mathbb{F}_q^\times is either of the form u^2 or nu^2 . Define a curve

$$C' : w^2 - v^2 = 4, \quad nu^2 - pv^2 = 2p.$$

Let N be the number of points mod q on $C_{1,p,p}$ and let N' be the number of points mod q on C' .

If $N > 0$, the result follows. If $N' > 0$, then C' can be transformed into an elliptic curve with approximately N' points. Hasse's theorem provides a bound on N' which, extending to $N = 2(q-1) - N' > 0$, shows that there must be points on $C_{1,p,p}$. It remains to show that $N > 0$, which will follow from the next 3 Lemmas.

Lemma 12 ([18], VIII Lemma 8.29). $N + N' = 2(q-1)$.

Proof. Let $x \not\equiv 0 \pmod{q}$. We solve

$$w + v \equiv x, \quad w - v \equiv 4/x \pmod{q},$$

yielding a pair (v, w) for each x we have $q-1$ choices for x , hence there are $q-1$ pairs (v, w) satisfying $w^2 - v^2 = 4$. Let (v, w) be such a pair. Consider

$$y^2 \equiv 2p + pv^2, \quad nu^2 \equiv 2p + pv^2 \pmod{q}.$$

If $2p + pv^2 \not\equiv 0 \pmod{q}$, then exactly one of these has a solution, and it has two solutions. If $2p + pv^2 \equiv 0 \pmod{q}$, then both congruences have one solution. therefore, each of the $q-1$ pairs (v, w) contributes 2 to the sum of $N + N'$, so $N + N' = 2(q-1)$. \square

Lemma 13 ([18], VIII Lemma 8.30). *If $q \geq 11$, then $N > 0$.*

Proof. If $N = 0$ then $N' = 2(q-1) > 0$, by lemma 12. We may transform C' to an elliptic curve E' ; by Hasse's theorem, E' has less than $q+1+2\sqrt{q}$ points. We parameterise $w^2 - v^2 = 4$:

$$v = \frac{4t}{1-t^2}, \quad w = \frac{2+2t^2}{1-t^2},$$

where the value $t = \infty$ corresponds to $(v, w) = (0, -2)$. All other points (v, w) correspond to finite values of t . No finite pair corresponds to $t = \pm 1$. Substituting the parameterisation into $nu^2 - pv^2 = 2p$ yields the curve

$$Q' : u_1^2 = \frac{2p}{n}(t^4 + 6t^2 + 1),$$

where $u_1 = (1 - t^2)u$. A point C' with $(v, w) \neq (0, -2)$ yields a finite point on the quartic curve Q' . Since C' has $2(q - 1) > 1$ points mod q , there is at least one finite point on Q' . Every point mod q on Q' yields a point on E' (points at infinity on Q' yield points of order 2 on E'). Thus, the number of points on C' is less than or equal to the number of points on E' . By Hasse's theorem,

$$2(q - 1) = N' \leq q + 1 + 2\sqrt{q}.$$

We may rearrange to obtain

$$(\sqrt{q} - 1)^2 \leq 4,$$

yielding $q \leq 9$. Therefore, if $q \geq 11$ we must have $N \neq 0$. □

Lemma 14 ([18], VIII Lemma 8.31). *If $q = 3, 5$ or 7 , then $N > 0$.*

Proof. First, suppose p is a square mod q . There are no points $C_{1,p,p}$ with coordinates in \mathbb{F}_3 , so we introduce denominators,

$$u = u_1/q, \quad v = 1/q, \quad w = w_1/q.$$

We solve for

$$w_1^2 + 4q^2, \quad u_1^2 = p + 2pq^2.$$

Since p is assumed to be a square mod q , Hensel's lemma implies that there are q -adic solutions u_1, w_1 .

Suppose that p is not a square mod q . We divide the equation in 8.15 to obtain

$$w^2 - v^2 = 4, \quad \frac{1}{p}u^2 - v^2 = 2.$$

Let n be any fixed quadratic nonresidue mod q , and write $1/p \equiv nx^2 \pmod{q}$.

Letting $u_1 = xu$, we obtain

$$w^2 - v^2 = 4, \quad nu_1^2 - v^2 = 2.$$

For $q = 3$ and $q = 5$, we may take $n = 2$ and obtain

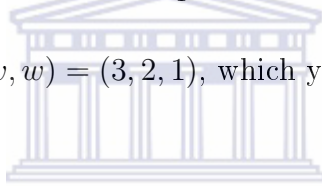
$$w^2 - v^2 \equiv 4, \quad 2u_1^2 - v^2 \equiv 2 \pmod{q}.$$

This has the solution $(u_1, v, w) = (1, 0, 2)$. As above, Hensel's lemma yields a q -adic solution.

For $q = 7$, take $n = 3$ to obtain

$$w^2 - v^2 \equiv 4, \quad 3u_1^2 - v^2 \equiv 2 \pmod{7}.$$

this has the solution $(u_1, v, w) = (3, 2, 1)$, which yields a 7-adic solution. □



UNIVERSITY of the
WESTERN CAPE

3.7.3 Galois Cohomology

We now provide the definition of the full Shafarevich-Tate group. We shall utilise Galois cohomology to interpret the descent calculations.

Let G be a group acting on an additive abelian group M , i.e. for any $g \in G$, there is an automorphism $g : M \rightarrow M$, such that

$$(g_1g_2)m = g_1(g_2m)$$

for all $m \in M$ and all $g_1, g_2 \in G$. The group M is termed a G -module.

A *homomorphism* $\phi : M_1 \rightarrow M_2$ of G -modules is a homomorphism of abelian groups that is compatible with the action of G , that is:

$$\phi(gm_1) = g\phi(m_1)$$

for all $g \in G$ and all $m_1 \in M$. Recall that in a short exact sequence (of modules and homomorphisms),

$$0 \rightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \rightarrow 0,$$

f_1 is injective, f_2 is surjective, and the image of f_1 equals the kernel of f_2 . In general, a sequence of abelian groups and homomorphisms

$$\cdots \rightarrow A \rightarrow B \rightarrow C \rightarrow \cdots$$

is said to be *exact at B* if the image of $A \rightarrow B$ is the kernel of $B \rightarrow C$. Such a sequence is said to be *exact* if it is exact at each group in the sequence.

We define the *zeroth cohomology group* to be

$$H^0(G, M) = M^G = \{m \in M \mid gm = m \text{ for all } g \in G\}.$$

We see that if G acts trivially, then $H^0(G, M) = M$.

Further, we define the *cocycles*

$$Z(G, M) = \{ \text{maps } f : G \rightarrow M \mid f(g_1g_2) = f(g_1) + g_1f(g_2) \text{ for all } g_1, g_2 \in G \}.$$

The maps f are maps of sets that are required to satisfy the given conditions. The set Z is often referred to as the set of *twisted homomorphisms* from G to M . It is a group under addition of maps.

We may construct elements of $Z(G, M)$ in the following manner: Let m be a fixed element of M and define

$$f_m(g) = gm - m.$$

Clearly, f_m gives a map from G to M , and since

$$\begin{aligned} f_m(g_1g_2) &= g_1(g_2m) - m \\ &= g_1m - m + g_1(g_2m - m) \\ &= f_m(g_1) + g_1f_m(g_2), \end{aligned}$$

we find that $f_m \in Z(G, M)$. Let

$$B(G, M) = \{f_m | m \in M\}.$$

Then $B(G, M) \subset Z(G, M)$ is called the set of *coboundaries*. Define the *first cohomology group*

$$H^1(G, M) = Z/B.$$

A homomorphism $\phi : M_1 \rightarrow M_2$ of G -modules induces a map

$$\phi_* : H^j(G, M_1) \rightarrow H^j(G, M_2)$$

of cohomology groups for $j = 0, 1$. For H^0 , this is simply the restriction of ϕ to M_1^G . Note that if G acts trivially, then $g\phi(m_1) = \phi(gm_1) = \phi(m_1)$, so ϕ maps M_1^G into M_2^G . For H^1 , we obtain ϕ_* by taking an element $f \in Z$ and defining

$$(\phi_*(f))(g) = \phi(f(g)).$$

Proposition 33 ([18], VIII §9). *An exact sequence*

$$0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$$

of G -modules induces a long exact sequence

$$\begin{aligned} 0 \rightarrow H^0(G, M_1) \rightarrow H^0(G, M_2) \rightarrow H^0(G, M_3) \\ \rightarrow H^1(G, M_1) \rightarrow H^1(G, M_2) \rightarrow H^1(G, M_3) \end{aligned} \quad (3.23)$$

of cohomology groups.

Now that we have our first two cohomology groups H^0 and H^1 defined, we consider an elliptic curve E defined over \mathbb{Q} . Let n be a positive integer. By Theorem 10, multiplication by n gives an endomorphism of E . By [18] II Theorem 2.22, it is surjective from $E(\overline{\mathbb{Q}}) \rightarrow E(\overline{\mathbb{Q}})$ since $\overline{\mathbb{Q}}$ is algebraically closed. Therefore, we have an exact sequence

$$0 \rightarrow E[n] \rightarrow E(\overline{\mathbb{Q}}) \xrightarrow{n} E(\overline{\mathbb{Q}}) \rightarrow 0.$$

Let

$$G = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$$

be the Galois group of $\overline{\mathbb{Q}}/\mathbb{Q}$. We have the property that

$$H^0(G, E(\overline{\mathbb{Q}})) = E(\overline{\mathbb{Q}})^G = E(\mathbb{Q}).$$

Applying Proposition 3.23 to the exact sequence yields the long exact sequence

$$\begin{aligned} 0 \rightarrow E(\mathbb{Q})[n] \rightarrow E(\mathbb{Q}) \xrightarrow{n} E(\mathbb{Q}) \\ \rightarrow H^1(G, E[n]) \rightarrow H^1(G, E(\overline{\mathbb{Q}})) \xrightarrow{n} H^1(G, E(\overline{\mathbb{Q}})) \end{aligned}$$

This induces the short exact sequence

$$0 \rightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \rightarrow H^1(G, E[n]) \rightarrow H^1(G, E(\overline{\mathbb{Q}}))[n] \rightarrow 0.$$

This sequence is similar to the sequence

$$0 \rightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \rightarrow S_2 \rightarrow \text{III}_2 \rightarrow 0.$$

We shall now investigate how the two sequences relate when $n = 2$, then later consider arbitrary n .

Let C be a curve defined over \mathbb{Q} such that C is isomorphic to E over $\overline{\mathbb{Q}}$. Hence, there are maps $\phi : E \rightarrow C$ and $\phi^{-1} : C \rightarrow E$ given by rational functions with coefficients in $\overline{\mathbb{Q}}$. Choose $g \in G$, and let ϕ^g denote the map obtained by applying g to the coefficients of the rational functions defining ϕ . Since C is defined over \mathbb{Q} , ϕ^g maps E to $gC = C$. Note that

$$g(\phi(P)) = (\phi^g)(gP)$$

for all $P \in E(\overline{\mathbb{Q}})$.

We say that a map ϕ is *defined over* \mathbb{Q} if $\phi^g(P) = \phi(P)$ for all $P \in E(\overline{\mathbb{Q}})$ and all $g \in G$.

The map $\phi^{-1}\phi^g$ gives a map from E to E . We assume the following: There is a

point $T_g \in E(\overline{\mathbb{Q}})$ such that

$$\phi^{-1}(\phi^g(P)) = P + T_g$$

for all $P \in E(\mathbb{Q})$. The above can be rewritten as

$$\phi^g(P) = \phi(P + T_g)$$

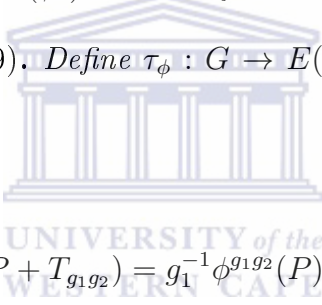
for all $P \in E(\mathbb{Q})$. If $P = (\phi^g)^{-1}(Q)$ for a point $Q \in C(\overline{\mathbb{Q}})$, the assumption becomes

$$\phi^{-1}(Q) = (\phi^g)^{-1}(Q) + T_g,$$

which implies that ϕ^{-1} and $(\phi^g)^{-1}$ differ by translation.

Lemma 15 ([18], VIII §9). *Define $\tau_\phi : G \rightarrow E(\overline{\mathbb{Q}})$ by $\tau_\phi(g) = T_g$. Then $\tau_\phi \in Z(G, E(\overline{\mathbb{Q}}))$.*

Proof.



$$\begin{aligned} g_1^{-1}\phi(P + T_{g_1g_2}) &= g_1^{-1}\phi^{g_1g_2}(P) \\ &= \phi^{g_2}(g_1^{-1}P) \\ &= \phi(g_1^{-1}P + T_{g_2}) \\ &= g_1^{-1}\phi^{g_1}(P + g_1T_{g_2}) \\ &= g_1^{-1}\phi(P + g_1T_{g_2} + T_{g_1}). \end{aligned}$$

Applying g_1 then ϕ^{-1} yields

$$T_{g_1g_2} = g_1T_{g_2} + T_{g_1}.$$

□

Suppose we have curves C_i and maps $\phi_i : E \rightarrow C_i$ for $i = 1, 2$ as above. The pairs (C_1, ϕ_1) and (C_2, ϕ_2) are *equivalent* if there is a map $\theta : C_1 \rightarrow C_2$ defined over \mathbb{Q} and a point $P_0 \in E(\overline{\mathbb{Q}})$ such that

$$\phi_2^{-1}\theta\phi_1(P) = P + P_0$$

for all $P \in E(\overline{\mathbb{Q}})$. Thus, if we identify C_1 and C_2 with E by ϕ_1 and ϕ_2 , then θ is a translation by P_0 .

Proposition 34 ([18], VIII §9). *The pairs (C_1, ϕ_1) and (C_2, ϕ_2) are equivalent if and only if the cocycles τ_{ϕ_1} and τ_{ϕ_2} differ by a coboundary. This means that there is a point $P_1 \in E(\overline{\mathbb{Q}})$ such that*

$$\tau_{\phi_1}(g) - \tau_{\phi_2}(g) = gP_1 - P_1$$

for all $g \in G$.

Proof. If $\tau_{\phi_i}(g) = T_g^i$ for $i = 1, 2$, then

$$\phi_i^g(P) = \phi_i(P + T_g^i)$$

for all $P \in E(\overline{\mathbb{Q}})$. Suppose (C_1, ϕ_1) and (C_2, ϕ_2) are equivalent, i.e. there exist $\theta : C_1 \rightarrow C_2$ and P_0 as above. For any $P \in E(\overline{\mathbb{Q}})$, we have

$$\begin{aligned} P + T_g^1 + P_0 &= \phi_2^{-1}\theta\phi_1(P + T_g^1) \\ &= \phi_2^{-1}\theta\phi_1^g(P) \\ &= \phi_2^{-1}\phi_2^g(\phi_2^{-1}\theta\phi_1)^g(P) \\ &= (\phi_2^{-1}\theta\phi_1)^g(P) + T_g^2 \\ &= g(\phi_2^{-1}\theta\phi_1)(g^{-1}P) + T_g^2 \\ &= g(g^{-1}P + P_0) + T_g^2 \\ &= P + gP_0 + T_g^2. \end{aligned}$$

Therefore

$$T_g^1 - T_g^2 = \tau_{\phi_1}(g) - \tau_{\phi_2}(g) = gP_0 - P_0.$$

Conversely, suppose there exists P_1 such that

$$\tau_{\phi_1}(g) - \tau_{\phi_2}(g) = gP_1 - P_1.$$

Define $\theta : C_1 \rightarrow C_2$ by

$$\theta(Q) = \phi_2(\phi_1^{-1}(Q) + P_1).$$

It is clear that θ defines an equivalence relation on the set of cocycles. However, we need to show that θ is defined over \mathbb{Q} . If $Q \in C(\overline{\mathbb{Q}})$, then

$$\begin{aligned}
\theta^g(Q) &= g\theta(g^{-1}Q) \\
&= g\phi_2(\phi_1^{-1}(g^{-1}Q) + P_1) \\
&= \phi_2^g((\phi_1^g)^{-1}(Q) + gP_1) \\
&= \phi_2(\phi_2^{-1}\phi_2^g)((\phi_1^g)^{-1}(Q) + gP_1) \\
&= \phi_2((\phi_1^g)^{-1}(Q) + gP_1 + T_g^2) \\
&= \phi_2(\phi_1^{-1}(Q) - T_g^1(g) + gP_1 + T_g^2) \\
&= \phi_2(\phi_1^{-1}(Q) + P_1) \\
&= \theta(Q)
\end{aligned}$$

Thus, θ is defined over \mathbb{Q} , so the pairs (C_1, ϕ_1) and (C_2, ϕ_2) are equivalent. \square

The above proposition says that we have a map

$$\text{equivalence classes of pairs } (C, \phi) \leftrightarrow H^1(G, E(\overline{\mathbb{Q}})).$$

It can be shown that this is a bijection (see [16] for further details). The following is an important property.

Proposition 35 ([18], VIII §9). *Let τ_ϕ correspond to the pair (C, ϕ) . Then $\tau_\phi \in B(G, E(\overline{\mathbb{Q}}))$ if and only if C has a rational point.*

Proof. Let $P \in E(\overline{\mathbb{Q}})$. Then

$$gP + T_g = \phi^{-1}\phi^g(gP) = \phi^{-1}(g\phi(P))$$

and

$$P = \phi^{-1}(\phi(P)).$$

Thus,

$$T_g = P - gP \iff g\phi(P) = \phi(P).$$

If C has a rational point Q , choose P such that $\phi(P) = Q$. then $gQ = Q$ for all

g implies that

$$T_g = g(-P) - (-P)$$

for all $g \in G$. Conversely, if $T_g = g(-P) - (-P)$ for all g , then $g\phi(P) = \phi(P)$ for all $g \in G$, so $\phi(P)$ is a rational point. \square

The above two propositions give us a reinterpretation in terms of cohomology groups of the fundamental question: when do certain curves have rational points?

Example. Consider the curve $C_{1,p,p}$ from the previous section. We have equations

$$x = u^2$$

$$x - 2p = pv^2$$

$$x + 2p = pw^2.$$

These were rewritten as

$$w^2 - v^2 = 4, \quad u^2 - pv^2 = 2p.$$

We may change this to

$$C : s^2 = 2p(t^4 + 6t^2 + 1).$$

Finally, the transformation

$$t = \frac{\sqrt{2p}(x + 2p)}{y}, \quad s = -\sqrt{2p} + \frac{2t^2(x - p)}{\sqrt{2p}} = \sqrt{2p} \frac{x^2 + 4px - 4p^2}{x(x - 2p)}$$

changes the equation to

$$E : y^2 = x(x - 2p)(x + 2p).$$

Now we attempt to relate the curve $C_{1,p,p}$ to a cohomology class in $H^1(G, E(\overline{\mathbb{Q}}))$.

The map

$$\phi : E \rightarrow C$$

$$(x, y) \mapsto (t, s)$$

gives a map from E to C . Since the equations for E and C have coefficients in

\mathbb{Q} , these curves are defined over \mathbb{Q} . However, ϕ is not defined over \mathbb{Q} . Computation shows that

$$(x, y) + (-2p, 0) = (x_1, y_1)$$

on E , where

$$x_1 = 2p \frac{2p - x}{2p + x}, \quad y_1 = \frac{-8p^2 y}{(x + 2p)^2}$$

Further calculations show that

$$\phi(x_1, y_1) = (-t, -s).$$

Choose $g \in G$ such that $g(\sqrt{2p}) = -\sqrt{2p}$. Then ϕ^g is the transformation obtained by changing $\sqrt{2p}$ to $-\sqrt{2p}$ in the formulae for ϕ . Therefore,

$$\phi^g(x, y) = (-t, -s) = \phi(x_1, y_1).$$

We obtain

$$\phi^{-1}\phi^g(x, y) = (x, y) + (-2p, 0).$$

Now suppose $g \in G$ satisfies $g(\sqrt{2p}) = +\sqrt{2p}$. Then $\phi^g = \phi$, so

$$\phi^{-1}\phi^g(x, y) = (x, y).$$

Putting everything together, we see that the pair (C, ϕ) is of the type considered above. We obtain an element of $H^1(G, E[2])$ that can be regarded as an element of $H^1(G, E(\overline{\mathbb{Q}}))$. The cocycle τ_ϕ is given by

$$\tau_\phi(g) = T_g = \begin{cases} \infty & \text{if } g(\sqrt{2p}) = +\sqrt{2p} \\ (-2p, 0) & \text{if } g(\sqrt{2p}) = -\sqrt{2p} \end{cases}$$

The cohomology class of τ_ϕ is nontrivial in $H^1(G, E(\overline{\mathbb{Q}}))$, and hence also in $H^1(G, E[2])$ since C has no rational points.

In general, if E is given by $y^2 = (x - e_1)(x - e_2)(x - e_3)$ with $e_1, e_2, e_3 \in \mathbb{Q}$, then a 2-descent yields curves $C_{a,b,c}$. These curves yield elements of $H^1(G, E[2])$. The

curves that have rational points give cocycles in $Z(G, E(\overline{\mathbb{Q}}))$ that are coboundaries. We also saw in the descent procedure that a rational point on a curve $C_{a,b,c}$ comes from a rational point on E . All of this may be summarised by the exact sequence

$$0 \rightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \rightarrow H^1(G, E[2]) \rightarrow H^1(G, E(\overline{\mathbb{Q}})[2]) \rightarrow 0.$$

We may replace \mathbb{Q} by the p -adic field \mathbb{Q}_p with $p \leq \infty$. We have an exact sequence

$$0 \rightarrow E(\mathbb{Q}_p)/2E(\mathbb{Q}_p) \rightarrow H^1(G_p, E[2]) \rightarrow H^1(G_p, E(\overline{\mathbb{Q}}_p)[2]) \rightarrow 0.$$

where

$$G_p = \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p).$$

The group G_p can be regarded as a subgroup of G . Recall that cocycles in $Z(G, E[2])$ are maps from G to $E[2]$ with certain properties. Such maps may be restricted to G_p to obtain elements of $Z(G_p, E[2])$. A curve $C_{a,b,c}$ yields an element of $H^1(G, E[2])$, which, in turn, yields an element of $H^1(G_p, E[2])$ that becomes trivial in $H^1(G_p, E(\mathbb{Q}_p))$ if and only if $C_{a,b,c}$ has a p -adic point.

We had previously defined S_2 to be those triples (a, b, c) such that $C_{a,b,c}$ has a p -adic point for all $p \leq \infty$. This means that S_2 is the set of triples (a, b, c) such that the corresponding cohomology class in $H^1(G, E[2])$ becomes trivial in $H^1(G_p, E(\overline{\mathbb{Q}}_p))$ for all $p \leq \infty$. Moreover, III_2 is S_2 modulo those triples coming from points in $E(\mathbb{Q})$. All of this can be expressed in terms of cohomology. We can also replace 2 by an arbitrary $n \geq 1$. Define the *Shafarevich-Tate* group to be

$$\text{III} = \text{Ker} \left(H^1(G, E(\overline{\mathbb{Q}})) \rightarrow \prod_{p \leq \infty} H^1(G_p, E(\overline{\mathbb{Q}})_p) \right)$$

and define the *n -Selmer group* to be

$$S_n = \text{Ker} \left(H^1(G_p, E[n]) \rightarrow \prod_{p \leq \infty} H^1(G_p, E(\overline{\mathbb{Q}})_p) \right).$$

The Shafarevich-Tate group can be thought of as consisting of equivalence classes of pairs (C, ϕ) such that C has a p -adic point for all $p \leq \infty$. This group is

nontrivial if there exists such a C that has no rational points. The n -Selmer group S_n can be regarded as the generalisation to n -descents of the curves $C_{a,b,c}$ that arise in 2-descents. We deduce the basic descent sequence with the use of the definitions, resulting in

$$0 \rightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \rightarrow S_n \rightarrow \text{III}[n] \rightarrow 0,$$

where $\text{III}[n]$ is the n -torsion in III . During descent, the aim is to obtain information about $E(\mathbb{Q})/nE(\mathbb{Q})$. However, the calculations are done in S_n . The group $\text{III}[n]$ is the obstruction to transferring information back to $E(\mathbb{Q})/nE(\mathbb{Q})$.

The group S_n is dependent on n , whereas the group III is not. Since S_n is finite, so is $\text{III}[n]$ ($\text{III}[n]$ is the quotient group of S_n). It has been conjectured that III is finite in general.

3.8 Elliptic Curves over \mathbb{C}

We provide a brief overview of elliptic curves over \mathbb{C} in order to define the invariant Ω which is central to the BSD Conjecture. We use [6, 16, 18].

Definition 67 ([6] IX, §1). A *lattice* L in \mathbb{C} is a discrete subgroup of the form $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, where ω_1, ω_2 are linearly independent over \mathbb{R} . A *complex torus* T is the quotient group \mathbb{C}/L of the complex plane \mathbb{C} by a lattice with projection usually denoted $p : \mathbb{C} \rightarrow T = \mathbb{C}/L$.

Definition 68 ([6] IX, §1). Two lattices L and L' in \mathbb{C} are *equivalent* if there exists $\lambda \in \mathbb{C}^* = \mathbb{C} - \{0\}$ with $\lambda L = L'$, i.e., L and L' are homothetic. Multiplication by λ defined $\mathbb{C} \rightarrow \mathbb{C}$ induces an isomorphism $T = \mathbb{C}/L \rightarrow \mathbb{C}/L' = T'$, also denoted

by λ , defined by the commutative diagram

$$\begin{array}{ccc}
 \mathbb{C} & \xrightarrow{\lambda} & \mathbb{C} \\
 \downarrow & & \downarrow \\
 T = \mathbb{C}/L & \xrightarrow{\lambda} & \mathbb{C}/L' = L'
 \end{array}$$

Theorem 23 ([18] IX, §2). *If L is a lattice in \mathbb{C} , there exists an elliptic curve E over \mathbb{C} so that \mathbb{C}/L and $E_L(\mathbb{C})$ are isomorphic as groups.*

Conversely, we have the following.

Theorem 24 ([18] IX, §3). *If E is an elliptic curve over \mathbb{C} , there exists a lattice L_E over \mathbb{C} so that $E(\mathbb{C})$ and \mathbb{C}/L_E are isomorphic as groups.*

Theorem 25 ([16], VI §4). *Let E/\mathbb{C} and E'/\mathbb{C} be elliptic curves corresponding to lattices L and L' respectively. Then E and E' are isomorphic over \mathbb{C} if and only if L and L' are homothetic.*

The above theorems state that for any elliptic curve E over \mathbb{C} , there is a lattice L such that $\mathbb{C}/L \cong E(\mathbb{C})$. To find the corresponding lattice L of E , we need to find ω_1, ω_2 where $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

These can be computed using *elliptic integrals* [18], IX §4. A fast and efficient method for calculating these integrals is the *arithmetic-geometric mean*, due to Gauss.

We now define the invariant Ω which appears in the Birch and Swinnerton-Dyer Conjecture. Let E be an elliptic curve over \mathbb{R} , and let L be the lattice corresponding to E . Then we can choose a basis $\{\omega_1, \omega_2\}$ for L with $\omega_2 \in \mathbb{R}$ [18].

Definition 69. Let E be an elliptic curve over \mathbb{Q} . Then

$$\Omega_E = \begin{cases} 2\omega_2 & \text{if } E[2] \subset E(\mathbb{R}) \\ \omega_2 & \text{otherwise.} \end{cases}$$

Remark. Ω is the number of components of $E(\mathbb{R})$ times the real period of E . We may alternatively define $\Omega_E = \int_{E(\mathbb{R})} |\omega|$, where $\omega = \frac{dx}{2y + a_1x + a_3}$ is the differential form associated with a global minimal model for E .



Chapter 4

The Birch and Swinnerton-Dyer Conjecture

In the early 1960s, Brian Birch and Peter Swinnerton-Dyer investigated a special class of elliptic curves over \mathbb{Q} with the use of the British computer EDSAC. The general aim of the investigation was to relate the arithmetic rank r of an elliptic curve $E(\mathbb{Q})$ to the densities of the p -adic points on E , for all primes p . It was thought that greater densities of p -adic points would generally correspond to larger values of r .

A useful measure for the density of p -adic points is $\lim_{n \rightarrow \infty} N_{p^n}/p^n$, where N_{p^n} denotes the number of solutions to the congruence $y^2z \equiv x^3 - Axz^2 - Bz^3 \pmod{p^n}$. By Hensel's Lemma, this limit is N_p/p for all but finitely many p . Hence, Birch and Swinnerton-Dyer examined the function $f(P) = \prod_{p \leq P} (N_p/p)$ for large P for a number of curves $E(\mathbb{Q})$. The results of the examination suggested that $f(P) \sim C(\log P)^r$ as $P \rightarrow \infty$, where C is dependent on the elliptic curve $E(\mathbb{Q})$.

The ζ -function associated with E can be expressed as $\zeta_E(s) = \zeta(s)\zeta(s-1)/L_E(s)$, where, for all but finitely many p ,

$$L_E(s) = \prod_p (1 + (N_p - p - 1)p^{-s} + p^{1-2s})^{-1}.$$

Thus, $L_E(1) = \prod (N_p/p)^{-1}$. However, at that time it was not known whether $L_E(s)$ converged as $s \rightarrow 1$ for all elliptic curves E , but it had been proven by Deuring that $L_E(s)$ could be analytically continued to all of \mathbb{C} if E admits *complex multiplication*. This occurs when the endomorphism ring of a given elliptic curve is larger than \mathbb{Z} ; these are the special curves alluded to at the beginning of this section with which Birch and Swinnerton-Dyer studied in the formulation of their groundbreaking conjecture.

The sources for this chapter are [1, 3, 4, 6, 10, 19].

4.1 The Birch and Swinnerton-Dyer Conjecture

The L -series of an elliptic curve is an analytic function that is used to encode arithmetic information about the curve. One then hopes to deduce further arithmetic properties of the elliptic curve by studying the analytic properties of its L -series, much as one uses the Riemann ζ function to study the set of rational primes.

The BSD Conjecture makes explicit this link between the arithmetic invariants of an elliptic curve and the analysis of its L -function. The L -function is defined in terms of local arithmetic invariants of E , but encodes information about the global arithmetic invariants of E , e.g. the rank. We follow [18] for the discussion involving the L -function.

Let E be an elliptic curve over \mathbb{Q} and Δ the discriminant of E .

For primes p of good reduction, define $a_p = p + 1 - \#E(\mathbb{F}_p)$. Otherwise, for primes p of bad reduction,

$$a_p = \begin{cases} 0 & \text{if } E \text{ has additive reduction at } p, \\ 1 & \text{if } E \text{ has split multiplicative reduction at } p, \\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } p. \end{cases}$$

The L -function of E is the product

$$L_E(s) = \prod_{p|\Delta} (1 - a_p p^{-s})^{-1} \cdot \prod_{p \nmid \Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

It follows from the estimate $|a_p| < 2\sqrt{p}$ that the product converges for $\operatorname{Re}(s) > \frac{3}{2}$. Each "good" factor can be expanded in the form

$$(1 - a_p p^{-s} + p^{1-2s})^{-1} = 1 + a_p p^{-s} + a_{p^2} p^{-2s} + \dots,$$

where $a_{p^2} = a_p^2 - p$, $a_{p^3} = a_p^3 - 2pa_p$, \dots , and for "bad factors" $a_{p^k} = a_p^k$. The product over all p yields $L_E(s) = \sum_{n=1}^{\infty} a_n n^{-s}$, where

$$a_n = \prod_j a_{p_j}^{e_j} \text{ if } n = \prod_j p_j^{e_j}.$$

As the L -function is closely related to the zeta function $\zeta(s)$, it would be natural to ask whether $L_E(s)$ has an analytic continuation to all of \mathbb{C} ; In fact, this deep property of $L_E(s)$ is a consequence of modularity (Breuil, Conrand, Diamond, Taylor, Wiles, 1995, 2001):

Corollary 7 ([18], XIV, §2). $L_E(s)$ admits an analytic continuation to \mathbb{C} .

Remark. The L -function $L_{E/K}(s)$ can be defined for an elliptic curve over a number field K . $L_{E/K}$ is analytic for $\operatorname{Re}(s) > 1$, but it is only *conjectured* that $L_{E/K}(s)$ has analytic continuation to the entire complex plane. This is known as the Hasse-Weil Conjecture.

We can now finally state the first (weak) version of the BSD Conjecture.

Let E be an elliptic curve defined over \mathbb{Q} . By Mordell's Theorem,

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{Tors}} \oplus \mathbb{Z}^r,$$

for some non-negative integer r called the *arithmetic rank* of E often denoted r_E or $r(E)$, and $E(\mathbb{Q})_{\text{Tors}}$ denotes the finite subgroup of torsion points of E .

First Birch and Swinnerton-Dyer Conjecture (Millennium Prize Problem 7, [11] V §2). *Let $L_E(s)$ be the L -function of $E(\mathbb{Q})$. Then the Taylor expansion of $L_E(s)$ at $s = 1$ has the form*

$$L_E(s) = c_r(s-1)^r + c_{r+1}(s-1)^{r+1} + \dots,$$

where c_r is a non-zero constant and r (often denoted as r_E or $r(E)$) is the arithmetic rank.

We will refer to this as the *Rank Conjecture*. Due to this conjecture, we call the order of the zero of $L_E(s)$ at $s = 1$ the *analytic rank* of E , denoted $r_{\text{an}}(E)$.

Birch and Swinnerton-Dyer later refined the Rank Conjecture to provide rich information on elliptic curves. The second BSD Conjecture makes the link between arithmetic invariants of the elliptic curve and the L -function more explicit.

Second Birch and Swinnerton-Dyer Conjecture ([11] V §2). *Let E be an elliptic curve over \mathbb{Q} such that the Shafarevich-Tate group of E is finite. The residue of $L_E(s)$ at $s = 1$, i.e. the coefficient C_0 , has a concrete expression in terms of invariants of E/\mathbb{Q} . Explicitly,*

$$C_0 = \lim_{s \rightarrow 1} \frac{L(E, s)}{(s-1)^r} = \frac{|\text{III}| \cdot \Omega_E \cdot \text{Reg}(E/\mathbb{Q}) \cdot \prod_p c_p}{|E_{\text{Tors}}(\mathbb{Q})|^2}.$$

The invariants on the right hand side of the above equation are

- r the arithmetic rank of $E(\mathbb{Q})$.
- Ω_E either the real period or twice the real period of a minimal model for E dependent on whether $E(\mathbb{R})$ is connected or not. See Section 3.8.
- III_E the Shafarevich-Tate group for E/\mathbb{Q} . See Section 3.7. The BSD conjecture is dependent on the cardinality of III , which itself is conjecturally finite.

$\text{Reg}(E/\mathbb{Q})$ is the elliptic regulator of $E(\mathbb{Q})$. See Section 3.6.2

- c_p is an elementary local factor, equal to the cardinality of $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$, where $E_0(\mathbb{Q}_p)$ is the set of points in $E(\mathbb{Q}_p)$ whose reduction modulo p

is non-singular in $E(\mathbb{F}_p)$. The number c_p is usually referred to as the *Tamagawa number* of E at p .

$E(\mathbb{Q})_{\text{Tors}}$ is the set of torsion points on E/\mathbb{Q} . See Section 3.5.

The profound depth and scope of the BSD Conjecture is succinctly stated in a quote attributed to Tate in 1974:

This remarkable conjecture relates the behavior of a function L at a point where it is not at present known to be defined to the order of a group III which is not known to be finite!

Corollary 7 takes care of the first unknown; we will comment on the second unknown later.

The second BSD conjecture is very similar to that of the analytic class number formula. We now discuss analogies between the two, with the use of the source [18].

Given an imaginary quadratic field K , the zeta function of K satisfies

$$\zeta_K(s) = (s-1)^{-1} \frac{2\pi h}{w\sqrt{|d|}} + \dots,$$

where h is the class number of K , d the discriminant of K , and w is the number of roots of unity in K .

In the case real quadratic fields K , by the class number formula,

$$\zeta_K(s) = (s-1)^{-1} \frac{4h\log(\nu)}{2\sqrt{d}},$$

where h is the class number of K , d the discriminant and ν is the fundamental unit. We now compare these two formulae with the residues of the Taylor expansion of the L -function of elliptic curves E at $s = 1$ with rank $r = 0$ and $r = 1$, namely

$$c_r = \frac{\Omega \cdot \prod_p c_p \cdot \#(\text{III}_E) \cdot \text{Reg}(E)}{|E(\mathbb{Q})_{\text{Tors}}|^2}.$$

For an elliptic curve E with rank $r = 0$, we compare the residue c_r to that of the zeta function of an imaginary quadratic field K . The group III_E can be regarded

as the analogue of the ideal class group, $\Omega \prod_p c_p$ is the analogue to $2\pi/\sqrt{|d|}$, and $|E(\mathbb{Q})_{\text{Tors}}|$ is the analogue of w .

For an elliptic curve of rank $r = 1$, we compare the residue c_r to that of the real quadratic field K . Again, III_E can be regarded as the analogue of the ideal class group, however Ω is now the analogue of $4/\sqrt{d}$ and $\#E(\mathbb{Q})_{\text{Tors}}$ has analogue 2, which is the number of roots of unity in K . The elliptic regulator $\text{Reg}(P)$ is the analogue to $\log(\nu)$.

Recall that we used the Unit Theorem in the proof of the Mordell-Weil Theorem; in fact the Unit Theorem in algebraic number theory can be seen as the analogue of the Mordell-Weil Theorem for abelian varieties. Moreover, the finiteness of the ideal class group in algebraic number theory can be seen as the analogue of the conjectured finiteness of the Shafarevich-Tate group III_E . This lends credence to the conjecture of the finiteness of III_E .

4.2 Discussion and Comments

In this section we do not give any proofs as they require concepts and results which are beyond the scope of this thesis.

We begin by discussing partial results. The most significant of these is:

Theorem 26 ([3], Theorem 5.16). *If $r_{an} \leq 1$, then $r = r_{an}$ and $\text{III}(E/\mathbb{Q})$ is finite.*

This result is built on work of Gross-Zagier (1986), Zhang (2001), Kolyvagin (1990), Bump et. al. (1990) and Murty-Murty (1991). Instances of these results were established earlier for curves with complex multiplication by Coates-Wiles (1977) and Rubin (1987).

There is a weaker form of the Conjecture. Some results on this have been proved.

Conjecture 1 (Parity Conjecture, [3], Conjecture 4.1).

$$r(E) \equiv r_{an}(E) \pmod{2}.$$

Theorem 27 (Monsky, 1996). *The Parity Conjecture holds true for an elliptic curve E over \mathbb{Q} if $\text{III}(E)$ is finite.*

Theorem 28 (Dokchitser-Dokchitser, 2009, [1]). *If the p -primary part of $\text{III}(E/\mathbb{Q})$ is finite for at least one prime p then the parity conjecture for E/\mathbb{Q} holds.*

Remark. BSD Conjecture generalises to elliptic curves over number fields [3] and to abelian varieties [19].

There is an analogous conjecture for elliptic curves over function fields [19] and the following has been proven.

Theorem 29 (Artin-Tate, 1960s). *The BSD Conjecture holds for an elliptic curve E over a function field k if and only if $\text{III}(E)$ is finite.*

Finding III is impossible in general; it is only known to be finite when $r^{an} \leq 1$ [1].

The second BSD Conjecture implies an algorithm to compute a basis for $E(\mathbb{Q})$, by Manin [3, 19].

It is hoped that a proof of BSD would also yield a proof of the finiteness of III [19]. We note two consequences of the BSD Conjecture.

Theorem 30 (Tunnell's Theorem, [8] I §1). *Let n be an odd squarefree natural number. Consider the two conditions:*

(A) *n is congruent;*

(B) *the number of triples of integers (x, y, z) satisfying $2x^2 + y^2 + 8z^2 = n$ is equal to twice the number of triples satisfying $2x^2 + y^2 + 32z^2 = n$.*

Then (A) implies (B), and, if the weak form of the Birch-Swinnerton-Dyer conjecture is true, then (B) implies (A).

In 2010, Mazur and Rubin proved that if III is finite, then Hilbert's 10th problem has a negative answer over \mathcal{O}_K for any number field K [10].

4.3 Computations

The main purpose of this section is to perform computations to

- (a) verify BSD1, and
- (b) assuming the BSD conjecture is true, predict the order of the Shafarevich-Tate (S-T) group.

We first investigate the general approach to performing (a) and (b) by discussing J.E. Cremona's conference proceedings on the BSD conjecture [1]. As an example, we verify BSD1 for an elliptic curve of rank 3, and predict the order of its S-T group. Thereafter, we discuss the `mwrnk` package which is used for rank calculations. We provide a detailed overview of how `mwrnk` approaches 2-descent by 2-isogeny since, with the theory to be provided, we will perform simplified calculations for determining the rank of an elliptic curve.

Finally, for the rank 2 elliptic curve $E : y^2 = x^3 + 33x$, we verify BSD1 and predict the order of its S-T group.

This section makes extensive use of the `SAGE` package as it incorporates various algorithms for elliptic curves. These include rank calculation, determining analytic rank and calculation of various other invariants.

Sources used are [1, 4].

4.3.1 General Approach

We give an overview of the conference proceeding given by J. E. Cremona in 2011 [1].

Let E be an elliptic curve over \mathbb{Q} with rank r , $L_E(s)$ the L -function of E , and r_{an} the analytic rank of $L_E(s)$.

We note the following:

-
- (1) The root number $w(E/\mathbb{Q})$ can be computed, which in effect gives us the parity of the analytic rank $r_{\text{an}}(E)$.
 - (2) Although beyond the scope of this thesis, by the Modularity Theorem, the ratio $L(E, 1)/\Omega(E)$ is rational and can be determined exactly using modular symbols. We note this development as it is possible to determine whether or not $L(E, 1)$ is zero, and equivalently whether $r_{\text{an}}(E) = 0$.

We can thus determine whether

$$r_{\text{an}}(E) = 0 \quad \text{or} \quad r_{\text{an}}(E) = 1, 3, 5, \dots \quad \text{or} \quad r_{\text{an}}(E) = 2, 4, 6, \dots$$

If $r_{\text{an}}(E)$ is odd, then evaluating $L'(E, 1)$ approximately can prove that it is non-zero, and hence that $r_{\text{an}}(E) = 1$ if it is. Similarly, if $r_{\text{an}}(E)$ is even and positive, then evaluating $L''(E, 1)$ approximately can prove that it is non-zero, and hence that $r_{\text{an}}(E) = 2$ if it is. Further, if $r_{\text{an}}(E)$ is odd, $L'(E, 1)$ is approximately zero, then we can show that it is exactly zero by finding at least two independent points in $E(\mathbb{Q})$. This implies that $r(E) > 1$, and hence that $r_{\text{an}}(E) > 1$. So computing $L'''(E, 1)$ approximately can establish that $r_{\text{an}}(E) = 3$ if it is.

If $r_{\text{an}}(E) \leq 3$, we can find the exact value of $r_{\text{an}}(E)$ using

- (1) the root number for the parity;
- (2) modular symbols to determine whether $r_{\text{an}}(E) = 0$;
- (3) the works of Kolyvagin and Gross-Zagier to distinguish $r_{\text{an}}(E) = 1$ from $r_{\text{an}}(E) = 3$; and
- (4) numerical evaluation of $L^{(j)}(E, 1)$.

However, if $r_{\text{an}}(E) > 3$, we cannot determine it rigorously.

We now verify a rank 3 example found in [1]. The author of the conference proceedings has used the computing package SAGE; we shall follow that syntax.

Let $E = 234446a1 = [1, 1, 0, -696, 6784]$, which has conductor 234446. The

root number $w_E = -1$, thus $r_{\text{an}}(E)$ is odd.

$|L'(E, 1)| < 10^{-22}$, so we should have $r_{\text{an}}(E) \geq 3$. Applying 2-descent finds generators (15,-7),(16,-16) and (19,20) where $\text{Reg}(E) = 2.159011 \dots$ and $\text{III}(E/\mathbb{Q})[2] = 0$. Thus $r(E) = 3$.

By Kolyvagin and Gross-Zagier, $r_{\text{an}}(E) > 1$. Now $L'''(E, 1) = 59.09365958 \dots$ implies that $r_{\text{an}}(E) = 3$. Also, $\Omega(E) = 2.2808923 \dots$, so $L'''(E, 1)/(3!\Omega(E)\text{Reg}(E)) = 2.00000 \dots$ approximately.

Finally, $\prod c_p = 2 \cdot 1 = 2$ and $\#E(\mathbb{Q})_{\text{extrmTors}} = 1$.

BSD predicts that $\#\text{III}(E/\mathbb{Q}) = \frac{L'''(E,1)/6 \cdot \text{Reg}(E) \cdot \Omega(E)}{\prod c_p / (\#E(\mathbb{Q})_{\text{Tors}})^2} = 1$.

In closing, we note the general approach to quantifying, if possible, III_E exactly.

III is a torsion abelian group. Let $\text{III}(p)$ denote the p -primary part of III . Then finding $|\text{III}|$ involves finding $|\text{III}(p)|$ for all p . In practice, one could try to show:

- (a) $|\text{III}(p)|$ is trivial for almost all p ,
- (b) Use p -descent and p -adic methods to determine $|\text{III}(p)|$ for the remaining primes.

(a) is currently only possible when $r_{\text{an}} \leq 1$, and (b) is often possible for individual primes when $r_{\text{an}} \geq 2$.

4.3.2 Cremona's mwrank

We now consider the computing package `mwrank` authored by J. E. Cremona, used extensively in the SAGE computing package for rank calculations of elliptic curves.

The following is sourced from [4].

We start by noting two procedures.

General two-descent: determine the image of the descent map ϕ (3.18). If the image of the descent map has order 2^t , then the rank of $E(\mathbb{Q})$ is $t, t - 1$ or $t - 2$, depending on whether the number of points of order 2 in $E(\mathbb{Q})$ is 0, 1 or 3 respectively.

Two-descent via 2-isogeny: used when E has a rational point P of order two. This procedure has the advantage of being easier to calculate than general two-descent, provided that we know of a rational point P on E of order two.

We will cover two-descent via 2-isogeny as we will provide a crude example in the following section based on it. Further details regarding general descent can be found in [4] III §6.

We consider homogeneous spaces H of the form (3.13) and check if they have a rational point. To do this, both methods used by `mwrnk` make use of algorithms which determine local solubility and, if at all possible, determine global solubility.

Let H be a curve of the form (3.13). The local solubility algorithm used by `mwrnk` can easily determine solubility of H over the reals. If $g(x)$ has a real root then it takes positive values, so H has real points. If however $g(x)$ has no real roots then the values of $g(x)$ have constant sign, thus `mwrnk` merely has to check that $a > 0$.

Next, if p is an odd prime not dividing the discriminant of g , then H has points modulo p which are nonsingular. These points lift to p -adic points.

For the other primes, it suffices to check solubility in \mathbb{Z}_p for either $g(x)$ or $g^*(x) = ex^4 + dx^3 + cx^2 + bx + a$. If $g^*(x)$ is used, assume $x \in p\mathbb{Z}_p$. Given x_k modulo p^k , `mwrnk` tries to lift to a p -adic point (x, y) with $x \equiv x_k \pmod{p^k}$. There are three cases: lifting is definitely possible; lifting is definitely not possible; or it cannot be computed without considering x_k modulo a higher power of p . The third case essentially makes use of Hensel's Lemma to effectively determine if lifting is possible or not. Finally, the prime $p = 2$ needs to be considered separately.

The algorithm for global solubility used by `mwrnk` starts by searching for a small

rational point. If the search fails, local solubility is checked. If the local solubility check passes, then a more thorough search is attempted using a quadratic sieving procedure. The main point of departure is that it is of no use to do a thorough search for points if local solubility everywhere is not assured, but also that there is no point in checking local solubility if an obvious global point can be found. The sieve-assisted search works as follows. For each possible denominator of x `mwrnk` precomputes, for each of several sieving moduli m , the residues to which the numerator of x must belong if the right-hand side of the equation is to be a square modulo m . For every odd prime p dividing the denominator of the x -coordinate of a rational point, we must have $\left(\frac{a}{p}\right) = +1$, otherwise it would mean that the leading coefficient a is a square. Further, `mwrnk` precomputes a list of primes p for which $\left(\frac{a}{p}\right) = -1$, and discards the possible denominators divisible by any of these primes. For $p = 2$, a similar condition holds. The searches are restricted to ranges of x for which $g(x)$ is positive. For two-descent via 2-isogeny, `mwrnk` simply restricts to positive x as the quartics are polynomials in x^2 .

We now provide an overview of 2-descent by 2-isogeny.

Let E be an elliptic curve with point P of order 2. We may translate P to the origin by a change of coordinates, so assume E has equation

$$E : y^2 = x(x^2 + cx + d) \tag{4.1}$$

with $c, d \in \mathbb{Z}$. Let x_0 be a root of the cubic $x^3 + b_2x^2 + 8b_4x + 16b_6$, and set $c = 3x_0 + b_2, d = (c + b_2)x_0 + 8b_4$. If $a_1 = a_3 = 0$, we can avoid a scaling factor of 2 by letting x_0 be the root of $x^3 + a_2x^2 + a_4x + a_6$, and set $c = 3x_0 + a_2, d = (c + a_2)x_0 + a_4$. Now, the 2-isogenous curve $E' = E / \langle P \rangle$ has equation

$$E' : y^2 = x(x^2 + c'x + d')$$

where

$$c' = -2c \quad \text{and} \quad d' = c^2 - 4d.$$

E is nonsingular if and only if $dd' \neq 0$. The 2-isogeny $\phi : E \rightarrow E'$ has kernel $\{\mathcal{O}, P\}$ and maps (x, y) to $\left(\frac{y^2}{x^2}, \frac{y(x^2-d)}{x^2}\right)$. On the other hand, the dual isogeny $\phi' : E' \rightarrow E$ maps (x, y) to $\left(\frac{y^2}{4x^2}, \frac{y(x^2-d')}{8x^2}\right)$.

For each factorisation $d = d_1d_2$ with d_1 squarefree, we consider the homogeneous space

$$H(d_1, c, d_2) : v^2 = d_1up^4 + cu^2 + d_2.$$

Let $N_1 = n_1(c, d)$ be the number of factorisations of d for which the quartic $H(d_1, c, d_2)$ has a rational point, and $n_2 = n_2(c, d)$ the number for which the quartic has a point everywhere locally. Similarly, define $n'_1 = n_1(c', d')$ and $n'_2 = n_2(c', d')$. By an explicit calculation, $E(\mathbb{Q})/\phi'(E'(\mathbb{Q}))$ is isomorphic to the subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ generated by the factors d_1 for which $H(d_1, c, d_2)$ has a rational point. Thus we have

$$|E(\mathbb{Q})/\phi'(E'(\mathbb{Q}))| = n_1,$$

which must be a power of 2, say $n_1 = 2^{e_1}$; similarly

$$|E'(\mathbb{Q})/\phi(E(\mathbb{Q}))| = n'_1 = 2^{e'_1}.$$

Thus,

$$\text{rank}(E(\mathbb{Q})) = \text{rank}(E'(\mathbb{Q})) = e_1 + e'_1 - 2.$$

If we find rational points on all quartics which have them everywhere locally, then $n_1 = n_2$. However, there are possible cases where $n_1 < n_2$; these correlate with either

- (1) the rational point on the quartic could not be found as the search bound was too small, or
- (2) there being points everywhere locally but no rational point on some quartic.

In the case of (1), we could increase our search bound and hope that the program terminates by finding a rational point. However, it could be that case (2) is in effect. Those quartics in case (2) above arise from elements of order 2 in III_E , investigated in section 3.7. We derived the exact sequence (3.21) which we can

apply to our current case as

$$0 \rightarrow E(\mathbb{Q})/\phi'E'(\mathbb{Q}) \rightarrow S(\phi') \rightarrow \text{III}(E'/\mathbb{Q})[\phi'] \rightarrow 0. \quad (4.2)$$

The injective map $E(\mathbb{Q})/\phi'E'(\mathbb{Q}) \rightarrow S(\phi')$ is induced by taking a point $(x, y) \in E(\mathbb{Q})$ with $x \neq 0$ to the space $H(d_1, c, d_2)$ where $d_1 = x$ modulo squares: if $x = d_1u^2$ and $v = uy/x$ then (u, v) is a rational point on $H(d_1, c, d_2)$. $P = (0, 0)$ maps to d modulo squares. Conversely, if (u, v) is a rational point on $H(d_1, c, d_2)$ then $(x, y) = (d_1u^2, d_1uv) \in E$ is rational. It follows that n_1 is the order of $E(\mathbb{Q})/\phi'(E'(\mathbb{Q}))$, and so

$$|\text{III}(E'/\mathbb{Q})[\phi']| = n_2/n_1.$$

Similarly we find that

$$|\text{III}(E/\mathbb{Q})[\phi]| = n'_2/n'_1,$$

when we construct an exact sequence similar to (4.2) by replacing E' with E and ϕ' with ϕ .

Local solubility of $H(d_1, c, d_2)$ follows for all primes p which do not divide $2dd'$; for all other p we follow the criteria of Birch and Swinnerton-Dyer. For local solubility in \mathbb{R} , if $d' < 0$ then we require $d_1 > 0$. If either $d' < 0$, or $d' > 0$ and $c + \sqrt{d'} < 0$, we only consider positive divisors d_1 of d , and need not apply the general test for solubility in \mathbb{R} .

Each rational point (u, v) maps to the point (d_u^2, d_1uv) on E . Similarly, a rational point (u, v) on $H(d'_1, c', d'_2)$ maps to a point on E' , and hence via the dual isogeny ϕ' to the point

$$\left(\frac{v^2}{4u^2}, \frac{v(d'_1u^4 - d'_2)}{8u^2} \right)$$

in $E(\mathbb{Q})$. Thus, the $n_1n'_1$ many points in $E(\mathbb{Q})$ determined cover the cosets of $E(\mathbb{Q})/2E(\mathbb{Q})$, either once each, or twice each. When $|E(\mathbb{Q}[2])| = 2$,

$$\frac{n_1n'_1}{2} = |E(\mathbb{Q})/2E(\mathbb{Q})| = 2^{r+1},$$

while if $|E(\mathbb{Q}[2])| = 4$,

$$n_1n'_1 = |E(\mathbb{Q})/2E(\mathbb{Q})| = 2^{r+2}.$$

So $2^r = n_1 n'_1 / 4$ in both cases. This concludes two-descent via 2-isogeny.

4.3.3 Numerical Example

In this section we will give our own numerical example. We will verify that this example satisfies the first BSD conjecture, and then calculate the order of III_E predicted by the second BSD conjecture. We have used [15] and [11], along with the computational package Sage. Also, we follow the blueprint laid out in section 4.3.2.

Consider the elliptic curve

$$E : y^2 = x^3 + 33x.$$

We can factor E as $y^2 = x(x^2 + 33)$. E has the point $(0, 0)$ which is of order 2, so we may use 2-descent via 2-isogeny.

Comparing E to equation (4.1), we see that $c = 0$, thus

$$c' = 0 \quad \text{and} \quad d' = -4d.$$

We can now attempt to calculate the rank r_E of E to verify BSD1.

First BSD Conjecture. We calculate r_E : We have that $a = 0$ and $b = 33$. We factor b in all possible ways:

$$33 = 33 \times 1 \quad \text{and} \quad 33 = -33 \times -1.$$

The equations we consider are

(i) $N^2 = -M^4 - 33e^4$

(ii) $N^2 = M^4 + 33e^4$

(iii) $N^2 = 33M^4 + e^4$

(iv) $N^2 = -33M^4 - e^4$

We may disregard equations (i) and (iv) since we are required to calculate a real-valued N . Further, note that equations (ii) and (iii) are similar with the variables

M and e reversed.

We have solutions

$$\begin{aligned} 23^2 &= 1 \cdot 1^4 + 33 \cdot 2^4, \\ 92^2 &= 33 \cdot 4^4 + 2^4 \end{aligned}$$

Next, we consider $\bar{E} : \bar{y}^2 = \bar{x}^3 - 132\bar{x}$. The possibilities for \bar{b}_1 are

$$\bar{b}_1 = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 11, \pm 12 \pm 22, \pm 33, \pm 44 \pm 66, \pm 132.$$

We can eliminate $\pm 12, \pm 44, \pm 66$ and ± 132 as they are not squarefree. Thus, we need check which of following 16 diophantine equations are solvable:

$$\left| \begin{array}{l} N^2 = M^4 - 132e^4 \\ N^2 = 6M^4 - 22e^4 \\ N^2 = 33M^4 - 4e^4 \\ N^2 = -2M^4 + 66e^4 \\ N^2 = -11M^4 + 12e^4 \end{array} \right| \left| \begin{array}{l} N^2 = 2M^4 - 66e^4 \\ N^2 = 11M^4 - 12e^4 \\ N^2 = 66M^4 - 2e^4 \\ N^2 = -3M^4 + 44e^4 \\ N^2 = -22M^4 + 6e^4 \\ N^2 = -66M^4 + 2e^4 \end{array} \right| \left| \begin{array}{l} N^2 = 3M^4 - 44e^4 \\ N^2 = 22M^4 - 6e^4 \\ N^2 = -M^4 + 132e^4 \\ N^2 = -6M^4 + 22e^4 \\ N^2 = -33M^4 + 4e^4 \end{array} \right|$$

We find 8 solutions:

$$\left| \begin{array}{l} 1^2 = 1^4 - 132 \times 0^4 \\ 34^2 = -33 \times 4^4 + 4 \times 7^4 \\ 2^2 = 3 \times 2^4 - 44 \times 1^4 \end{array} \right| \left| \begin{array}{l} 4^2 = 22 \times 1^4 - 6 \times 1^4 \\ 1^2 = -11 \times 1^4 + 12 \times 1^4 \end{array} \right| \left| \begin{array}{l} 4^2 = -6 \times 1^4 + 22 \times 1^4 \\ 8^2 = -2 \times 1^4 + 66 \times 1^4 \\ 8^2 = 66 \times 1^4 - 2 \times 1^4 \end{array} \right|$$

Thus, we find that

$$2^r = \frac{2 \times 8}{4} = 4 = 2^2,$$

so the rank of the curve E is 2.

With the use of **SAGE**, we want to show that L_E has a zero of order 2 at $s = 1$:

Firstly, we define the elliptic curve $E : y^2 = x^3 + 33x$ by the following command

```
e = EllipticCurve([0,0,0,33,0])
Output: Elliptic Curve defined by  $y^2 = x^3 + 33 * x$  over Rational
Field
```

Although determined already, for educational purposes we use `mwrnk` to determine the rank:

```
e.rank()
Output: 2
```

We determine the root number $w(E/\mathbb{Q})$. The function returns 1 if the root number is even, and -1 if it is odd.

```
e.root_number()
Output: 1
```

BSD predicts that the Taylor series expansion of the $L_E(s)$ has a zero of order equal to the rank of the E at $s = 1$. We run the commands:

```
l = e.lseries()dokchitser();
l.taylor_series(1,4)
Output: -1.14596351251186e-23 + (3.62222607041402e-23)*z +
8.23392136922372*z2 - 26.0262428251028*z3 + 0(z4)
```

The root number $w(E/\mathbb{Q})$ implies that the parity of $r_{\text{an}}(E)$ is even, so $r_{\text{an}}(E) \neq 1$. Also, by the Modularity theorem we can show that $r_{\text{an}}(E) \neq 0$. Finally, $L''(E, 1)$ is approximately non-zero, and thus $r_{\text{an}}(E) = 2$. Hence, the rank conjecture corresponds with our findings that E has rank 2 as the Taylor series expansion of E at $s = 1$ indeed has a zero of order two.

Second BSD Conjecture. We now calculate the invariants attached to the elliptic curve.

Regulator

```
r = e.regulator();  
Output:  r => 5.32203813587631
```

Cardinality of Torsion Subgroup

```
tor = e.torsion_subgroup();  
len(tor)  
Output:  2
```

Real Period

```
e.period_lattice().real_period()  
Output:  1.54713685979027
```

Tamagawa Product

```
e.tamagawa_product()  
Output:  4
```

We now have all the invariants needed to predict the order of III_E . By BSD2,

$$\begin{aligned}\text{III} &= \frac{L_E(1) \cdot |E_{\text{tors}}(\mathbb{Q})|^2}{\Omega_E \cdot \text{Reg}(E/\mathbb{Q}) \cdot \prod_p c_p} \\ &= \frac{8, 23392136922372 \times 2^2}{1.54713685979027 \times 5.32203813587631 \times 4} \\ &\approx 1.\end{aligned}$$

4.4 Concluding Remarks

The first BSD Conjecture has been proven for elliptic curves E over \mathbb{Q} with $r_{\text{an}} \leq 1$ (Kolyvagin et. al.). Using theoretical and computational methods, the

full BSD Conjecture can be proved for many elliptic curves, all of rank at most 1 and all but a finite number with complex multiplication.

It is possible (in principle and in practice) to determine the exact value of r_{an} when at most 3, and it is also often possible to determine the (arithmetic) rank in these cases, and hence verify BSD1 in many cases where $r_{\text{an}} \leq 3$. [1].

No example of a verification of BSD for E for which $r_{\text{an}} > 3$ is known, although infinitely many equations for which rank greater than 3 can be written down (there exists an example, done by Elkies in 2006, which has rank at least 28) [3]. For no curve with $r_{\text{an}} > 2$ is III known to be finite, so there is no hope of verifying BSD2 in these cases.[1]

Despite these obstacles to proving the Conjecture, the results discussed in Section 4.2 constitute theoretical evidence for its validity. Since isogenous elliptic curves have the same L -function, the BSD Conjecture can be true only if the product $\frac{|\text{III}| \cdot \Omega_E \cdot \text{Reg}(E/\mathbb{Q}) \cdot \prod_p c_p}{|E_{\text{Tors}}(\mathbb{Q})|^2}$ is isogeny invariant; this result was proved by Cassels (1965) assuming the finiteness of $\text{III}(E)$. Note that the individual factors may change under isogeny, the product however does not[16].

The numerical evidence, in cases where computation is possible, is also positive. Stein et. al. has verified BSD for any elliptic curve $E(\mathbb{Q})$ with $r_{\text{an}} \leq 1$, and conductor ≤ 5000 [12].

We have the following result.

Theorem 31 (Bhargava-Shankar [2]). *The average size of the 3-Selmer group of all elliptic curves over \mathbb{Q} , when ordered by height, is 4. This implies that the average rank of all elliptic curves over \mathbb{Q} , when ordered by height, is less than 1.17*

This last result may suggest that proving the Conjecture for small rank covers most elliptic curves, but it is entirely possible that failure may occur in higher rank cases.

Bibliography

- [1] *Numerical Evidence for the Birch-Swinnerton-Dyer conjecture*, BSD Conference, Cambridge, UK, 2011. <https://www.dpmms.cam.ac.uk/research/BSD2011/bsd2011-Cremona.pdf>.
- [2] Bhargava M.; Shankar A. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. something, 2014.
- [3] Massimo Bertolini. Report on the birch and swinnerton-dyer conjecture. *Milan J. Math. Val. 78*, 2010.
- [4] J. E. Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, 1997.
- [5] R. Hartshorne. *Algebraic Geometry*. Springer-Verlag, 1977.
- [6] D. Husemoller. *Elliptic Curves*. Springer-Verlag, 2nd edition, 2000.
- [7] A. W. Knapp. *Elliptic Curves*. Princeton University Press, 1992.
- [8] N. Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. Springer-Verlag, 2nd edition, 1984.
- [9] S. Lang. *Algebra*. Springer-Verlag, 3rd edition, 2002.
- [10] Chao Li. What is the birch and swinnerton-dyer conjecture? <http://www.math.harvard.edu/chaoli/BSD.html>, 2010.
- [11] A. Lozano-Robledo. *Elliptic Curves, Modular Forms, and Their L-functions*, volume 58. AMS, Student Mathematical Library, 2011.

BIBLIOGRAPHY

- [12] Robert L. Miller. *Empirical Evidence for the Birch and Swinnerton-Dyer Conjecture*. PhD thesis, Univeristy of Washington, 2010.
- [13] J. S. Milne. *Elliptic Curves*. BookSurge Publishers, 2nd edition, 2006.
- [14] F. Oggier. *Introduction to Algebraic Number Theory*. Online reference, 2011.
- [15] J. Silverman, J. H.; Tate. *Rational Points on Elliptic Curves*. Springer-Verlag, 1992.
- [16] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 2nd edition, 2008.
- [17] W. Stein. *A Brief Introduction to Classical and Adelic Algebraic Number Theory*. online reference, 2004.
- [18] L. C. Washington. *Elliptic Curves, Number Theory and Cryptography*. Chapman and Hall/CRC, 2nd edition, 2008.
- [19] Andrew Wiles. The birch and swinnerton-dyer conjecture. <http://www.claymath.org/millennium/>, 2000.