Diophantine Problems in Polynomial Theory

by

Paul David Lee

B.Sc. Mathematics, The University of British Columbia, 2009

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

in

The College of Graduate Studies

(Mathematics)

THE UNIVERSITY OF BRITISH COLUMBIA

(Okanagan)

August 2011

Abstract

Algebraic curves and surfaces are playing an increasing role in modern mathematics. From the well known applications to cryptography, to computer vision and manufacturing, studying these curves is a prevalent problem that is appearing more often. With the advancement of computers, dramatic progress has been made in all branches of algebraic computation. In particular, computer algebra software has made it much easier to find rational or integral points on algebraic curves. Computers have also made it easier to obtain rational parametrizations of certain curves and surfaces.

Each algebraic curve has an associated genus, essentially a classification, that determines its topological structure. Advancements on methods and theory on curves of genus 0, 1 and 2 have been made in recent years. Curves of genus 0 are the only algebraic curves that you can obtain a rational parametrization for. Curves of genus 1 (also known as elliptic curves) have the property that their rational points have a group structure and thus one can call upon the massive field of group theory to help with their study. Curves of higher genus (such as genus 2) do not have the background and theory that genus 0 and 1 do but recent advancements in theory have rapidly expanded advancements on the topic.

In this thesis, we will first outline some methods used to find rational and integral points on curves of genus 0, 1, and 2. We will then solve some new problems related to polynomial theory that require finding the solutions to systems of Diophantine equations. We are required to find rational or integral points on algebraic curves to garner the solutions to these systems.

Preface

This thesis was written with the collaboration of my supervisor, Dr. Blair Spearman. Dr. Spearman and myself both contributed to the selection of the topic, the research, and the writing of this thesis. All LaTeX document preparation and coding was done by myself.

The contents of Chapter 5 have been published in the International Mathematical Forum under the title *A Diophantine System and a Problem on Cubic Fields* [16]. The contents of Chapter 6 have been published in Scientiae Mathematicae Japonicae under the title *The Factorization of* $x^5 + ax^m + 1$ [17].

Table of Contents

Appendices

List of Tables

List of Symbols

$\mathbb{Z}$	Set of integers
$\mathbb{Q}$	Set of rationals
$\mathbb{C}$	Set of complex numbers
$D(f)$	Discriminant of a polynomial $f(x)$
Δ	Discriminant of a polynomial or integral basis
$\mathbb{P}^2$	The projective plane $\{(X : Y : Z) \mid X, Y, Z \in \mathbb{Z}\}$
$\mathbb{Z}[x]$	The polynomial ring of integers in variable x
$\mathbb{Q}[x]$	The polynomial ring of rationals in variable y
$\mathbb{Z}[x, y]$	The polynomial ring of integers in variables x and y
$\mathbb{Q}[x, y]$	The polynomial ring of rationals in variables x and y
$deg(f), \partial f$	The degree of a polynomial $f(x)$
$\lvert\tilde{E}_p\rvert$	The number of points on $\tilde{E}$ modulo p (plus the point at infinity) of an elliptic curve
O_K	The ring of integers of a number field, K
$U(O_K)$	The group of units of the ring of integers of a number field, K
$\mathbb{R}^*$	The set of non-zero real numbers
$\mathbb{Q}^*$	The set of non-zero rational numbers
$\mathbb{Q}^{*^2}$	The set of square-free rational numbers
$\mathbb{Z}_n$	The cyclic group of n elements
$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$	The direct product of cyclic groups
$\mathcal{C}(\mathbb{Q})$	The algebraic curve $\mathcal{C}$ over the rationals
$J(\mathbb{Q})$	The Jacobian of a curve $\mathcal{C}$ over the rationals

Acknowledgments

I would like to thank my family and friends, especially my parents, whose constant love and support have made my accomplishments possible.

I would also like to thank my supervisor, Dr. Blair Spearman, for his constant help and patience throughout my academic career at UBC Okanagan. My chosen career path is largely thanks to his influence and inspiration.

My gratitude also goes out to all of my colleagues and other professors from UBC Okanagan that have been such a great source of friendship and support.

Chapter 1

Introduction

1.1 Elementary Number Theory

We begin with some elementary number theory that will be used throughout this paper. The majority of the material in this section can be found in [21], chapters 3-5.

Definition 1.1. *The greatest common divisor of two integers a and b, which are not both 0, is the largest integer that divides both a and b.*

Theorem 1.1. *The greatest common divisor of the integers a and b, not both 0, is the least positive integer that is a linear combination of a and b.*

Corollary 1.1. *If a and b are relatively prime integers, then there are integers m and n such that $ma + nb = 1$.*

Theorem 1.2 (The Fundamental Theorem of Arithmetic)**.** *Every positive integer greater than 1 can be written uniquely as a product of primes, with the prime factors in the product written in nondecreasing order.*

Example 1.1. *Some examples of integers written as products of primes:* $385 = 5 \cdot 7 \cdot 11,\ \ 10944 = 2^6 \cdot 3^2 \cdot 19,\ \ 15525 = 3^3 \cdot 5^2 \cdot 23$. *Integer factorization is a well-known problem and Maple has a command* `ifactor` *that will do this.*

Definition 1.2. *A diophantine equation is an equation where integer or rational solutions are sought.*

Definition 1.3. *Let m be a positive integer. If a and b are integers, we say that a is congruent to b modulo m if $m \mid (a - b)$.*

Example 1.2. *Let $a = 22$, $b = 4$. Then 22 is congruent to 4 mod 9 since* $9 \mid (22 - 4) = 18$.

Theorem 1.3. *If a and b are integers, then $a \equiv b \pmod{m}$ if and only if there is an integer k such that $a = b + km$.*

Theorem 1.4 (The Chinese Remainder Theorem)**.** *Let $m_1, m_2, \cdots m_r$ be pairwise relatively prime positive integers. Then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \ (mod\ m_1), \\ x &\equiv a_2 \ (mod\ m_2), \\ &\vdots \\ x &\equiv a_r \ (mod\ m_r), \end{aligned}$$

has a unique solution modulo $M = m_1 m_2 \cdots m_r$.

We now provide some useful tools to find solutions of congruences of the form $f(x) = 0 \pmod{m}$, where $f(x) \in \mathbb{Z}[x]$ with $deg(f) > 1$. If m has the prime power factorization $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, then by the Chinese Remainder Theorem, solving $f(x) = 0 \pmod{m}$ is equivalent to solving the system of congruences

$$f(x) \equiv 0 \pmod{p_i^{a_i}}, \qquad i = 1, 2, \cdots, k.$$

Example 1.3. *We try to solve the congruence*

$$2x^3 + 7x - 4 \equiv 0 \ (mod\ 200).$$

By the Chinese Remainder Theorem, this reduces to finding the solutions of

$$2x^3 + 7x - 4 \equiv 0 \ (mod\ 8)$$

and

$$2x^3 + 7x - 4 \equiv 0 \ (mod\ 25)$$

since $200 = 2^3 5^2 = 8 \cdot 25$. First consider the congruence modulo 8. Assume that x is odd. That is, $x = 2n + 1$ for $n \in \mathbb{Z}$. Then

$$2x^3 + 7x - 4 = 2(8n^3 + 3n^2 + 13n + 2) + 1$$

which is an odd integer. However, an odd integer can never be congruent to 0 modulo 8. Therefore we consider the case where x is even. Let $x = 2m$ where $m \in \mathbb{Z}$. Then

$$2x^3 + 7x - 4 \equiv 14m - 4 \equiv 0 \ (mod\ 8)$$

which is equivalent to finding the solution to the congruence

$$3m \equiv 2 \text{ (mod 4)}.$$

Multiplying by 3 we get

$$m \equiv 2 \text{ (mod 4)}$$

which leads to

$$x \equiv 4 \text{ (mod 8)}.$$

Now consider the congruence modulo 25. To solve the congruence modulo 25, we can first find the solutions modulo 5 and work up to modulo 25. Consider the congruence

$$2x^3 + 7x - 4 \equiv 0 \text{ (mod 5)}.$$

By testing $x = 0, 1, 2, 3,$ *and* 4*, we find that the solution is* $x \equiv 1$ *(mod 5). We therefore substitute* $x = 1 + 5t$ *for* $t \in \mathbb{Z}$ *into the above congruence yielding*

$$2(1 + 5t)^3 + 7(1 + 5t) - 4 \equiv 0 \text{ (mod 25)}.$$

Simplifying this congruence we obtain

$$15t + 5 \equiv 0 \text{ (mod 25)}$$

and eliminate a factor 5 so that

$$3t + 1 \equiv 0 \text{ (mod 5)}.$$

The solutions to this congruence are $t \equiv 3$ *(mod 5). Therefore the solutions modulo 25 are* $x \equiv 1 + 5t \equiv 1 + 5 \cdot 3 \equiv 16$ *(mod 25). In summary we now have the two congruences*

$$x \equiv 4 \text{ (mod 8)},$$
$$x \equiv 16 \text{ (mod 25)}.$$

Using the Chinese Remainder Theorem, we must solve the congruences

$$25y_1 \equiv 1 \text{ (mod 8)}$$
$$8y_2 \equiv 1 \text{ (mod 25)}$$

which lead to the solutions $y_1 \equiv 1$ *(mod 5) and* $y_2 \equiv 22$ *(mod 25). Then* $x \equiv 4 \cdot 25 \cdot 1 + 16 \cdot 8 \cdot 22 \equiv 2916 \equiv 116$ *(mod 200).*

Lemma 1.1. *If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.*

Proof. Since $\gcd(a, b) = 1$, there exists integers x and y such that $ax + by = 1$. Multiplying this equation by c we get $acx + bcy = c$. Since $a \mid bc$ then it is clear that $a \mid acx + bcy$. Therefore a divides the left hand side, and thus must divide the right hand side. In other words, $a \mid c$. □

Lemma 1.2. *If p divides $a_1 a_2 \cdots a_n$, where p is a prime and $a_1, a_2, \cdots, a_n$ are positive integers, then there is an integer i with $1 \leq i \leq n$ such that $p \mid a_i$.*

Proof. This proof is by induction. The case when $n = 1$ is trivial. Assume the result is true for n. Consider the product $a_1 a_2 \cdots a_{n+1}$ that is divisible by the prime p. We know that either $\gcd(p, a_1 a_2 \cdots a_n) = 1$ or $\gcd(p, a_1 a_2 \cdots a_n) = p$. If the former is true, then by the previous lemma, $p \mid a_{n+1}$. On the other hand, if $p \mid a_1 a_2 \cdots a_n$, using the induction hypothesis, there is an integer i with $1 \leq i \leq n$ such that $p \mid a_i$. Consequently, $p \mid a_i$ for some i with $1 \leq i \leq n + 1$. □

We now give some simple results about the squares of integers.

Theorem 1.5. *Squares of integers are congruent to 0 or 1 modulo 3.*

Proof. Assume $x \equiv 0 \pmod 3$. Then clearly $x^2 \equiv 0 \pmod 3$. Now assume $x \equiv 1 \pmod 3$. Then $x = 3n + 1$ for $n \in \mathbb{Z}$. Then $x^2 = (3n + 1)^2 = 9n^2 + 6n + 1 \equiv 1 \pmod 3$. Lastly, assume $x \equiv 2 \pmod 3$. Then $x = 3n + 2$ for $n \in \mathbb{Z}$. Then $x^2 = (3n + 2)^2 = 9n^2 + 12n + 4 \equiv 1 \pmod 3$. □

Theorem 1.6. *Squares of integers are congruent to 0 or 1 modulo 4.*

Proof. Assume x is even. That is, $x = 2n$ for some $n \in \mathbb{Z}$. Then $x^2 = (2n)^2 = 4n^2 \equiv 0 \pmod 4$. Now assume x is odd. That is, $x = 2n + 1$ for some $n \in \mathbb{Z}$. Then $x^2 = (2n + 1)^2 = 4n^2 + 4n + 1 \equiv 1 \pmod 4$. □

Theorem 1.7. *Squares of integers are congruent to 0, 1, 4, or 9 modulo 16*

Proof. Assume $x \equiv 0 \pmod 4$. Then $x = 4n$ for some $n \in \mathbb{Z}$. Then $x^2 = (4n)^2 = 16n^2 \equiv 0 \pmod{16}$. Now assume $x \equiv \pm 1 \pmod 8$. Then $x = 8n \pm 1$ for some $n \in \mathbb{Z}$. Then $x^2 = (8n \pm 1)^2 = 64n^2 \pm 16n + 1 \equiv 1 \pmod{16}$. Now assume $x \equiv \pm 2 \pmod 8$. Then $x = 8n \pm 2$ for some $n \in \mathbb{Z}$. Then $x^2 = (8n \pm 2)^2 = 64n^2 \pm 16n + 4 \equiv 4 \pmod{16}$. Lastly, assume $x \equiv \pm 3 \pmod 8$. Then $x = 8n \pm 3$ for some $n \in \mathbb{Z}$. Then $x^2 = (8n \pm 3)^2 = 64n^2 \pm 48n + 9 \equiv 9 \pmod{16}$. □

Theorem 1.8. *Fourth powers of integers are congruent to 0 or 1 modulo 16.*

Proof. First, assume x is even. That is, $x = 2n$ for some $n \in \mathbb{Z}$. Then $x^4 = (2n)^4 = 16n^4 \equiv 0 \pmod{16}$. Now assume $x \equiv \pm 1 \pmod{4}$. That is, $x = 4m \pm 1$ for some $m \in \mathbb{Z}$. Then $x^4 = 256m^4 \pm 256m^3 + 96m^2 \pm 16m + 1 \equiv 1 \pmod{16}$. □

1.2 Algebraic Number Theory

Some material in this section closely follows online notes from Chapman [8], along with well-known results from algebraic number theory.

Definition 1.4. *An element α in $\mathbb{C}$ is an algebraic number if $f(\alpha) = 0$ for some monic polynomial in $\mathbb{Q}[x]$.*

Example 1.4. *$\alpha = \sqrt{2}$ is an algebraic number since it is a root of $f(x) = x^2 - 2$.*

Example 1.5. *$\alpha = \sqrt{3 - \sqrt{5}}$ is an algebraic number. If we square both sides and subtract 3 we get*

$$\alpha^2 - 3 = -\sqrt{5}.$$

Squaring both sides again we get

$$\alpha^4 - 6\alpha^2 + 9 = 5.$$

Which leads to $\alpha^4 - 6\alpha^2 + 4 = 0$. Thus α is a root of the polynomial $f(x) = x^4 - 6x^2 + 4$.

Definition 1.5. *Let $\alpha \in \mathbb{C}$. If $f(\alpha) = 0$ for some monic polynomial $f(x) \in \mathbb{Z}[x]$, then α is called an algebraic integer.*

Since the previous two examples were roots of monic polynomials over the integers, they were in fact algebraic integers.

Definition 1.6. *Let α be an algebraic number. The monic polynomial $f(x) \in \mathbb{Q}[x]$ of least degree such that $f(\alpha) = 0$ is called the minimal polynomial of α.*

We now introduced some notation that will describe algebraic numbers and integers. Denote A as the set of algebraic numbers and B the set of

algebraic integers. We know that $A \supset B$.

We now give an example of an element that is an algebraic number, not an algebraic integer (i.e. $\alpha \in A \backslash B$).

Example 1.6. *Let $\alpha = 1/\sqrt{2}$. α satisfies $f(x) = x^2 - 1/2 \in \mathbb{Q}[x]$, not $\mathbb{Z}[x]$. $f(x)$ is the minimal polynomial for α.*

In cases where the minimal polynomial is over the rationals, we can perform scaling operations so that the polynomial has integer coefficients. This is extremely useful for reducibility and converting from algebraic numbers to algebraic integers.

Lemma 1.3 (An algorithm for scaling)**.** *[8] Given $f(x) \in \mathbb{Q}[x]$ (monic), say*

$$f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0.$$

We can substitute $x = y/c$ where $c \neq 0, c \in \mathbb{Q}$ and multiply by c^n to clear denominators. We get a new polynomial

$$g(y) = y^n + a_{n-1}cy^{n-1} + a_{n-2}c^2y^{n-2} + \cdots + a_1c^{n-1}y + a_0c^n.$$

You can pick c so that $g(y)$ has integer coefficients.

Example 1.7. *Let $f(x) = x^2 - 1/2x - 1/3 \in \mathbb{Q}[x]$. Substituting $x = y/6$ we get $g(y) = 1/36y^2 - 1/12y - 1/3$. Now multiply by 36 and get $h(y) = y^2 - 3y - 12 \in \mathbb{Z}[x]$.*

Theorem 1.9. *[8] Let $\alpha \in A$. Then there is exactly one monic polynomial $f(x) \in \mathbb{Q}[x]$ of minimum degree with $f(\alpha) = 0$. This polynomial has the property that if $g(x) \in \mathbb{Q}[x]$ and $g(\alpha) = 0$ then $f(x) \mid g(x)$.*

Proof. Let P be the set of monic polynomials $h(x) \in \mathbb{Q}[x]$ with $h(\alpha) = 0$. Note that $P \neq \emptyset$ as $\alpha \in A$.

By well-ordering, there is an element of least degree, call it $f(x)$. We have to prove that $f(x)$ is unique and if $g(\alpha) = 0$, then $f(x) \mid g(x)$.

Suppose $f(x)$ is not unique. Then there exists another monic polynomial in P of least degree, say $f_2(x)$.

Consider the function $f - f_2$. Then $(f - f_2)(\alpha) = f(\alpha) - f_2(\alpha) = 0$. However, the degree of $f - f_2$ is less than the degree of f and you could scale $f - f_2$ if necessary so that $f - f_2 \in P$. This contradicts the minimality of f. Therefore, f is unique.

Now suppose $g(x) \in \mathbb{Q}[x], g(\alpha) = 0$. We want to show that $f(x) \mid g(x)$.

By the division algorithm for polynomials, $g(x) = f(x)q(x)+r(x)$ where either $\partial r(x) < \partial f(x)$ or $r(x) = 0$.

Since $r(\alpha) = g(\alpha) - f(\alpha)q(\alpha) = 0 - 0 = 0$ and we can scale $r(x)$ if necessary to be monic, $r(x) \in P$. This contradicts the minimality of $\partial f(x)$ unless $r(x) = 0$.

Therefore, $f(x) \mid g(x)$.

□

Next we quote some results from basic polynomial theory.

Lemma 1.4. *Let $f(x)$ be the minimal polynomial of $\alpha \in A$. Then $f(x)$ is irreducible over $\mathbb{Q}$.*

Theorem 1.10. *[8] If a monic polynomial in $\mathbb{Z}[x]$ factors in $\mathbb{Q}[x]$, it also factors in $\mathbb{Z}[x]$.*

Theorem 1.11. *[8] Let $\alpha \in A$ with minimal polynomial $f(x)$. Then $\alpha \in B \Leftrightarrow f(x) \in \mathbb{Z}[x]$.*

Theorem 1.12 (Eisenstein's Criterion)**.** *[8] Let $f(x) = a_n x^n + a_{n-1}x^{n-2} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. If there exists a prime number p such that all the following conditions are true:*

- *$p \mid a_i$ for $i \neq n$,*
- *$p \nmid a_n$, and*
- *$p^2 \nmid a_0$,*

then $f(x)$ is irreducible over $\mathbb{Q}$.

Theorem 1.13. *[8] If $\alpha \in A$ then $1/\alpha \in A$ ($\alpha \neq 0$).*

Definition 1.7 (Number Field)**.** *Let $\alpha \in A$ with degree n. We define $\mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in \mathbb{Q}, i = 0, 1, \cdots, n-1\}$.*

Theorem 1.14. *[8] For each fixed $\alpha \in A, \mathbb{Q}(\alpha)$ is a field, a subfield of A.*

Definition 1.8. *The degree of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ (denoted as $[\mathbb{Q}(\alpha) : \mathbb{Q}]$) is the dimension of $\mathbb{Q}(\alpha)$ as a vector space over $\mathbb{Q}$. We write it as $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$.*

Definition 1.9. *Let $f(x) \in F[x]$ be a polynomial over a field F. A splitting field for $f(x)$ is a field extension K of F such that*

1. *$f(x)$ factors into a product of linear factors in $K[x]$,*

2. *K is the smallest field with this property.*

Definition 1.10. *An irreducible polynomial $f(x) \in F[x]$ with coefficients in a field F is separable if $f(x)$ factors into distinct linear factors over a splitting field K of $f(x)$.*

Theorem 1.15 (Primitive Element Theorem)**.** *Let F and K be fields and let K be a finite extension of F. Then there exists an element $\alpha \in K$ such that $K = F(\alpha)$ if and only if there are finitely many fields L with $F \subseteq L \subseteq K$.*

Corollary 1.2. *Let F be a field and let $[F(\alpha, \beta) : F]$ be finite and separable. There there exists $\gamma \in F(\alpha, \beta)$ such that $F(\alpha, \beta) = F(\gamma)$.*

Let $\alpha \in A$ and let $f(x)$ be the minimal polynomial of α of degree n. Let $\alpha = \alpha_1, \alpha_2, \cdots, \alpha_n$ be the roots of $f(x)$. These α_i are the conjugates of α.

Suppose now that we form the number fields $\mathbb{Q}(\alpha_1), \mathbb{Q}(\alpha_2), \cdots, \mathbb{Q}(\alpha_n)$. Some of these may be equal but assume they are different. Even though they are different, these number fields are isomorphic.

Let ϕ be the isomorphism mapping $\mathbb{Q}(\alpha_i)$ to $\mathbb{Q}(\alpha_j)$. There are n mapping functions $\sigma_i : \mathbb{Q}(\alpha_1) \to \mathbb{Q}(\alpha_i)$ defined by $\sigma_i(g(\alpha_1)) = g(\alpha_i)$.

Definition 1.11. *Let $\beta \in \mathbb{Q}(\alpha)$. We define the norm $N(\beta)$ and the trace $T(\beta)$ by*

$$N(\beta) = \prod_{i=1}^{n} \sigma_i(\beta)$$

$$T(\beta) = \sum_{i=1}^{n} \sigma_i(\beta)$$

Theorem 1.16.

1. *If $\beta \in \mathbb{Q}(\alpha)$ then $N(\beta), T(\beta) \in \mathbb{Q}$.*
2. *If $\beta \in \mathbb{Q}(\alpha) \cap B$ then $N(\beta), T(\beta) \in \mathbb{Z}$.*

Definition 1.12. *A unit of a ring R is an element $u \in R$ such that $uv = vu = 1_R$ for some v, where 1_R is the multiplicative identity element.*

Definition 1.13. *A quadratic field is an algebraic number field $\mathbb{Q}(\alpha)$ of degree two over $\mathbb{Q}$.*

Definition 1.14. *Let $K = \mathbb{Q}(\alpha)$ be a number field. Define its ring of integers as $O_K = K \cap B$.*

Theorem 1.17. *Let K be a quadratic field. Let m be the unique squarefree integer $m \neq 0, 1$ such that $K = \mathbb{Q}(\sqrt{m})$. Then the set O_K is given by*

$$O_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{m} & \text{if } m \text{ is not of the form } 4t+1, t \in \mathbb{Z}. \\ \mathbb{Z} + \mathbb{Z}\left(\dfrac{1+\sqrt{m}}{2}\right) & \text{if } m = 4t+1, t \in \mathbb{Z}. \end{cases}$$

Definition 1.15. *An integral basis of the ring of integers is a basis $b_1, \cdots b_n \in O_K$ of the $\mathbb{Q}$-vector space K such that each element $x \in O_K$ can be uniquely represented as*

$$x = \sum_{i=1}^{n} a_i b_i,$$

with $a_i \in \mathbb{Z}$.

Definition 1.16. *A fundamental unit is a generator for the torsion-free unit group of the ring of integers of a number field when that group is an infinite cyclic group. For rings of the form $\mathbb{Z}[\sqrt{n}]$, the fundamental unit has the form $x + y\sqrt{n}$, where (x, y) is the smallest nontrivial solution to the Pell equation $x^2 - ny^2 = \pm 1$.*

Theorem 1.18 (Dirichlet's Unit Theorem)**.** *[8] The group of units of the ring of integers of a number field (denoted as $U(O_K)$) is finitely generated and has rank equal to $r = r_1 + r_2 - 1$ where r_1 is the number of real embeddings and r_2 is the number of conjugate pairs of complex embeddings of the number field K.*

Theorem 1.19. *[8] $U(O_K)$ is an abelian group under multiplication*

Lemma 1.5. *Suppose that K is a number field of degree n and $\beta \in O_K$. Then $\beta \in U(O_K)$ if and only if $N(\beta) = \pm 1$.*

Definition 1.17. *For $\beta, \gamma \in O_K$ with $\beta \neq 0$ we say $\beta \mid \gamma$ if $\exists \delta \in O_K$ such that $\gamma = \beta\delta$, or equivalently, $\frac{\gamma}{\beta} \in O_K$.*

Lemma 1.6. *Let $\beta, \gamma \in O_K$. If $\beta \mid \gamma$ then $N(\beta) \mid N(\gamma)$ as integers.*

Definition 1.18. *Let $\beta \in O_K$. β is irreducible if*

1. *$\beta \neq 0$,*
2. *β is not a unit,*
3. *if $\beta = \gamma\delta$ with $\delta, \gamma \in O_K$, then either γ or δ is a unit.*

Definition 1.19. *Let $K = \mathbb{Q}(\alpha)$ and let $\beta \in O_K$. Then β is prime in O_K if*

1. *$\beta \neq 0$,*
2. *β is not a unit,*
3. *if $\beta \mid \gamma\delta$ in O_K, then $\beta \mid \gamma$ or $\beta \mid \delta$.*

Definition 1.20. *Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n. Let $\beta_1, \beta_2, \cdots, \beta_n \in K$. We define a matrix $M(\beta_1, \beta_2, \cdots, \beta_n)$ to be the $n \times n$ matrix whose (j,k) entry is the trace $T(\beta_j\beta_k)$. We define the discriminant of $\{\beta_1, \beta_2, \cdots, \beta_n\}$ by $\Delta(\beta_1, \beta_2, \cdots, \beta_n) = det(M)$. Since each $T(\beta_j\beta_k) \in \mathbb{Q}$ we have the discriminant $\Delta(\beta_1, \beta_2, \cdots, \beta_n) \in \mathbb{Q}$.*

Lemma 1.7. *Let K be a number field of degree n and let $\beta_1, \beta_2, \cdots, \beta_n \in K$. Then $\Delta(\beta_1, \beta_2, \cdots, \beta_n) = det(N)^2$ where $N = N(\beta_1, \beta_2, \cdots, \beta_n)$ is the $n \times n$ matrix whose (j,k) entry is $\sigma_k(\beta_j)$. Recall that $\sigma_1, \sigma_2, \cdots, \sigma_n$ were the embeddings of K into $\mathbb{C}$.*

Consider γ_i, a rational linear combination of β_i. We now give a lemma that describes how the discrimant changes when we consider this linear combination of β.

Lemma 1.8. *Let K be a number field of degree n and $\beta_1, \beta_2, \cdots, \beta_n \in K$. If $B = (b_{jk})$ is any $n \times n$ matrix over $\mathbb{Q}$ and*

$$\gamma_j = \sum_{k=1}^{n} b_{jk}\beta_k$$

then $\Delta(\gamma_1, \gamma_2, \cdots, \gamma_n) = det(B)^2\Delta(\beta_1, \beta_2, \cdots, \beta_n)$.

Theorem 1.20. *All integral bases of O_K have the same discriminant Δ.*

1.3 Group Theory

We now review some group theory that will be very relevant to Chapter 3 on Elliptic Curves. The material in this section follows Fraleigh [10], chapters I-III.

Definition 1.21. *A binary operation $*$ on a set S is a function mapping $S \times S$ into S. For each $(a,b) \in S \times S$, we will denote the element $*((a,b))$ of S by $a * b$.*

Throughout the paper, + and · will denote regular addition and multiplication.

Definition 1.22. *A group $\langle G, * \rangle$ is a set G, closed under a binary operation $*$, such that $*$ is associative, G has an identity element, and every element in G has an inverse under $*$.*

Definition 1.23. *A group G is abelian if its binary operation is commutative.*

Definition 1.24. *If G is a group, then the order $|G|$ of G is the number of elements in G.*

Definition 1.25. *If a subset H of a group G is closed under the binary operation of G and if H with the induced operation from G is itself a group, then H is a subgroup of G. We shall let $H \leq G$ or $G \geq H$ denote that H is a subgroup of G, and $H < G$ or $G > H$ shall mean $H \leq G$ but $H \neq G$.*

Definition 1.26. *An element a of a group G generates G and is a generator for G if $< a >= \{a^n \mid n \in \mathbb{Z}\} = G$. A group G is cyclic if there is some element a in G that generates G.*

Theorem 1.21 (Langrange's Theorem)**.** *Let $H \leq G$ where G is a finite group. Then the order of H is a divisor of the order of G. That is, $|H| \mid |G|$.*

Corollary 1.3. *Every group of prime order is cyclic.*

Theorem 1.22. *Let $G_1.G_2, \cdots, G_n$ be groups. For $(a_1, a_2, \cdots, a_n)$ and $(b_1, b_2, \cdots, b_n)$ in $\prod_{i=1}^{n} G_i$, define $(a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n)$ to be the element $(a_1b_1, a_2b_2, \cdots, a_nb_n)$. Then $\prod_{i=1}^{n} G_i$ is a group, the direct product of the groups G_i, under this binary operation.*

In the event that the operation of each G_i is commutative, we sometimes use additive notation and refer to $\prod_{i=1}^{n} G_i$ as the *direct sum of the groups* G_i. The notation $\bigoplus_{i=1}^{n} G_i$ is sometimes used in this case in place of $\prod_{i=1}^{n} G_i$, especially with abelian groups under addition.

Theorem 1.23 (Fundamental Theorem of Finitely Generated Abelian Groups)**.** *Every finitely generated abelian group is isomorphic to a direct product of cyclic groups in the form*

$$\mathbb{Z}_{{p_1}^{r_1}} \times \mathbb{Z}_{{p_2}^{r_2}} \times \cdots \times \mathbb{Z}_{{p_n}^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

where the p_i are primes, not necessarily distinct, and $r_i \in \mathbb{N}$. The direct prodct is unique except for possible rearrangement of the factors.

1.4 Algebraic Curves

In this section, we give some definitions and results about algebraic curves that will be used throughout the paper.

Definition 1.27. *An algebraic curve over a field K is an equation $f(x, y) = 0$ where $f(x, y) \in K[x, y]$.*

Definition 1.28. *For a curve $f(x, y) = 0$, we make a substitution $x = X/Z, y = Y/Z, X, Y, Z \in \mathbb{Z}$ to get a curve of the form $f(X, Y, Z) = 0$. This new curve is known as the homogeneous form. The new space that this conversion creates is called projective space. The projective plane is denoted by $\mathbb{P}^2$.*

We now introduce the concept of a singular point, that is a point with no well-defined tangent.

Definition 1.29. *A singularity of an algebraic curve $f(x, y) = 0$ is a point (x, y) on $f(x, y) = 0$ such that $f_x(x, y) = 0$ and $f_y(x, y) = 0$. For a curve $F(X, Y, Z) = 0$ in homogeneous coordinates, we require $F_X(X, Y, Z) = F_Y(X, Y, Z) = F_Z(X, Y, Z) = 0$.*

Example 1.8. *Consider the unit circle $x^2+y^2 = 1$. We then have the curve $f(x, y) = x^2+y^2-1 = 0$. Taking partial derivatives we get $f_x(x, y) = 2x$ and $f_y(x, y) = 2y$. Setting these both to 0 and solving we get the only solution $(x, y) = (0, 0)$. However, this is not a point on the curve. Therefore, there are no singular points on the unit circle.*

Example 1.9. *Consider the curve $y^2 = x^3$ or $f(x, y) = y^2-x^3 = 0$. Taking partial derivatives we get $f_x(x, y) = -3x^2 = 0, f_y(x, y) = 2y = 0$. Solving these equations we get the solution $(x, y) = (0, 0)$, which is on the curve. Considering the homogeneous form $F(X, Y, Z) = Y^2Z - X^3 = 0$ we get the same point $(0, 0)$.*

Example 1.10. *Consider $f(x, y) = x^4+x^2y^2-2x^2y-xy^2+y^2 = 0$. Taking partial derivatives and solving we get the solutions $(x, y) = (0, 0), (\alpha, -4/3\alpha^2+ 5/3)$ where α is the root of the polynomial $4a^3 - 8a^2 + 10a - 5$. The point $(0, 0)$ is a singular point since it lies on $f(x, y)$; however, the point $(\alpha, -4/3\alpha^2 + 5/3)$ does not. We must also consider the homogeneous form of $f(x, y)$, $F(X, Y, Z) = X^4+X^2Y^2-2X^2YZ-XY^2Z+Y^2Z^2 = 0$. Taking partial derivatives and solving we get the points $(X : Y : Z) = (0 : 0 : Z)$ and $(0 : Y : 0)$. The point $(0 : 0 : Z)$ corresponds to the point $(x, y) = (0, 0)$ and the point $(0 : Y : 0)$ is a new singularity, a point at infinity.*

We now give some definitions about curves that will help us define a curve's genus. The majority of this information can be found in [11].

Definition 1.30. *A double point is a point at which a curve intersects itself, such as a crunode, a point at which two branches of a curve intersect and each has a distinct tangent.*

Definition 1.31. *A delta invariant measures the number of double points concentrated at a point. It is a non-negative integer.*

We denote the sum of delta invariants as $\sum_P \delta_P$ where the sum is taken over all singular points P of the complex projective plane curve [29].

Definition 1.32 (Genus)**.** *The genus of an irreducible algebraic curve is a non-negative integer. It equals* $g = \frac{(d-1)(d-2)}{2} - \sum_P \delta_P$ *where* d *is the degree of the curve. In other words,* $g \leq \frac{(d-1)(d-2)}{2}$*. If the curve is nonsingular, then* $g = \frac{(d-1)(d-2)}{2}$*. Also, if the curve is of the form* $y^2 = f(x)$*, where* $f(x)$ *is a polynomial of degree* n*, then* $g = \lfloor \frac{n-1}{2} \rfloor$*, where* $\lfloor \cdot \rfloor$ *is the floor function.*

Example 1.11. *Consider the curve* $y^2 = x^3$*. We find that the point* $(0, 0)$ *is a singularity. Therefore, the genus is* $g = 1$ *- (at least one)* $= 0$ *since* g *is nonnegative.*

Example 1.12. *Consider the curve* $y^2 = x^7 - 2x^3 + x - 3$*. Then* $g = \lfloor \frac{7-1}{2} \rfloor = 3$*.*

Chapter 2

Algebraic Curves of Genus 0

In a topological sense, curves of genus 0 are relatively simple. Every genus 0 curve over $\mathbb{Q}$ is birationally equivalent to some conic in the projective plane, $\mathbb{P}^2$, given by an equation

$$ax^2 + by^2 + cz^2 = 0,$$

where $a, b, c \in \mathbb{Z}$ are square free and pairwise relatively prime. Let $\mathcal{C}$ be an algebraic curve of genus 0. If $\mathcal{C}$ does in fact have rational solutions (X, Y), they can be parameterized to the form $(X(t), Y(t))$ for some $t \in \mathbb{Q}$. The method of obtaining these parameterizations can be found in [13]. We will outline the method next.

One way to parameterize a curve is using the method of base-point projections. Given a point on the curve, we can find the equation of a line that goes through that point with arbitrary slope t. We then intersect this line with the curve $\mathcal{C}$ and yield an equation for either x or y.

Example 2.1. *We begin with a simple example: the unit circle $x^2 + y^2 = 1$. By observation, we know that the point $(x, y) = (1, 0)$ is on this curve. Using the point-slope form for the equation of a line with slope t,*

$$y - y_0 = t(x - x_0),$$

we get

$$y = t(x - 1).$$

Substituting into $x^2 + y^2 = 1$ and factoring we get

$$(x - 1)((t^2 + 1)x - t^2 + 1) = 0$$

which yields

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

Back substituting, we solve for y and get

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

Letting say $t = 3$ we obtain the point $(\frac{4}{5}, \frac{3}{5})$ which is indeed a point on the unit circle.

Example 2.2. *There may be cases however where one cannot parametrize a curve over $\mathbb{Q}$ because no such solutions exist. For example, the curve*

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

has no rational (or integral) solutions. We can show this by first transforming the problem into projective coordinates by letting $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, $X, Y, Z \in \mathbb{Z}$ and clearing denominators to obtain

$$X^2 + Y^2 = 3Z^2. \tag{2.1}$$

where we may assume that the greatest common divisor of X, Y, Z is equal to 1. Working locally mod 3 we see that since squares are either 0 or 1 mod 3, then both X and Y must be congruent to 0 mod 3. Equivalently, we have the two equations

$$X = 3X_1$$
$$Y = 3Y_1$$

where $X_1, Y_1 \in \mathbb{Z}$. Substituting back into (2.1) we get

$$9X_1^2 + 9Y_1^2 = 3Z^2.$$

This implies that Z must be a multiple of 3, contradicting our assumption that the greatest common divisor of X, Y and Z is 1. Therefore, the curve $x^2 + y^2 = 3$ has no solutions.

2.1 Integral Points on Genus 0 Curves

While finding rational parametrizations for these curves may come easy (especially with the help of computer algebra systems), finding the integral points can prove to be quite difficult. We will now give a few definitions and then outline these steps.

Definition 2.1. *The resultant of two polynomials P and Q over a field K with leading coefficients p and q is defined as the product*

$$res(P, Q) = p^{deg(Q)} q^{deg(P)} \prod_{(x,y):P(x)=0,Q(y)=0} (x - y)$$

of the differences of their roots, where x and y take on values in the algebraic closure of K.

Note: The resultant can also be found by calculating the determinant of the Sylvester matrix or the Bezout matrix of P and Q [5].

Definition 2.2. *A Thue equation is a Diophantine equation of the form*

$$f(x, y) = n$$

where f is a homogeneous, irreducible polynomial of at least degree 3 over $\mathbb{Q}$ and n is a nonzero rational number.

Note: This equation is named after Axel Thue who proved that these equations have finitely many solutions in integers x and y [27].

After obtaining a rational parametrization for the curve, we substitute $t = a/b$ where $a, b \in \mathbb{Z}$ and clear denominators. This leads to a rational equation with integer values on both the numerator and denominator. With the help of resultants, we can calculate a common divisor between the numerator and denominator. This leads to a system of Thue equations $f(x, y) = m$ for $m \in \mathbb{Z}$ and $f(x, y) \in \mathbb{Z}[x, y]$ where $f(x, y)$ is the denominator of our rational equation. Depending on the resultant, there could be a significant number of values for m for which the equation needs to be solved. The number of cases can usually be reduced to a manageable amount using elementary number theory and then the remaining solved using the `Thue` command in Magma.

While these parametrizations may garner solutions, sometimes solutions may be overlooked because the parametrization used may not yield them. In Poulakis [18] [19], a method was given to find the integral points on genus 0 curves. In the paper, Poulakis shows that some points may be found through the singularities of the curve. We give an example from [18] where most of the solutions escape parametrization but can be found by calculating the singularities of the curve.

Example 2.3. *Consider the curve $C : f(X, Y) = X^2Y^3 - 2XY^3 + X^3 - 3XY^2+3Y^3 = 0$. The integer solutions of C are $(X, Y) = (0, 0), (1, 1), (-3, 1)$.*

We start by finding the singularities of the curve. Using the Maple command, `singularities` we find the singularities are the points $(0, 0)$ and $(1, 1)$. It turns out that these points are solutions to the curve C.

Again using Maple, we obtain a parametrization for X in terms of t and then substitute $t = \frac{a}{b}$, $a, b \in \mathbb{Z}$ to get the equation

$$X = \frac{8a^3 + 36a^2b + 27b^3}{8a^3}. \tag{2.2}$$

Using resultants on the numerator and denominator, we determine that the denominator must divide $2^9 3^9$. *That is,*

$$8a^3 \mid 2^9 3^9,$$

or

$$a^3 \mid 2^6 3^9,$$

which implies

$$a \mid 2^2 3^3.$$

This leads to the equation

$$a = \pm 2^i 3^j$$

where $0 \leq i \leq 2$ *and* $0 \leq j \leq 3$.

We now reduce the number of cases of the above down from 12. Suppose a *is even. Then since the* $gcd(a, b) = 1$, b *must be odd. If this is the case, the numerator of (2.2) will be odd and the denominator will be even. This scenario will never produce an integer. So we assume that* a *is odd. That is,* $a = \pm 1, \pm 3, \pm 9, \pm 27$. *Now assume that* $9 \mid a$. *Since* $gcd(a, b) = 1$, *then* $3 \nmid b$. *Looking back at (2.2), we conclude that* $3^6 \mid 27b^3$, *or* $3 \mid b$, *which is a contradiction. Therefore* $a = \pm 1, \pm 3$. *The only one of these four that leads to a solution is* $a = -3$ *so we will follow the steps that lead to the solution.*

Substituting $a = -3$ *into we get*

$$\begin{aligned} X &= 1 - \frac{3}{2}b - \frac{1}{8}b^3 \\ Y &= \frac{27b^3 + 324b - 216}{6(9b^2 + 72)}. \end{aligned}$$

Since b *was even, we substitute* $b = 2k, k \in \mathbb{Z}$ *into ( ) and get*

$$\begin{aligned} X &= 1 - 3k - k^3 \\ Y &= \frac{k^3 + 3k - 1}{k^2 + 2}. \end{aligned}$$

Using resultants on the numerator and denominator of Y, *we find that* $k^2 + 2 \mid 3$ *or in other words,*

$$k^2 + 2 = (-1)^i \cdot 3^j$$

for $0 \leq i \leq 1$ *and* $0 \leq j \leq 1$. *This yields the solution* $k = \pm 1 \Rightarrow (a, b) = (-3, 2) \Rightarrow (X, Y) = (-3, 1)$.

Chapter 3

Algebraic Curves of Genus 1 (Elliptic Curves)

We will now discuss the topic of elliptic curves. The reader can refer to Silverman and Tate [23] for more detail relevant to the material.

The most general form of an elliptic curve over $\mathbb{Q}$ is $ax^3+bx^2y+cxy^2+dy^3+ex^2+fxy+gy^2+hx+iy+j=0$ where $a,b,c,d,e,f,g,h,i,j \in \mathbb{Q}$. However, elliptic curves usually appear in of the form $y^2=x^3+ax^2+bx+c$ where $a,b,c \in \mathbb{Q}$. Any curve of genus 1 with a rational point can be converted into what is known as the Weierstrass normal form $y^2=x^3+Ax+B$ where $A,B \in \mathbb{Q}$ (or $\mathbb{Z}$). One condition for a curve to be elliptic is that it must have distinct roots. For example, $y^2=x^3-x^2=x^2(x-1)$ is not elliptic. In fact, it is a curve of genus 0 and can be parametrized accordingly.

An algorithm for computing this normal form is given in [14]. Maple has a command within the `algcurves` package, called `Weierstrassform` that performs this algorithm on a given elliptic curve and gives the isomorphic function (and inverse function) mappings used to convert the curve form from its original form to the normal form.

Elliptic curves can be defined over any algebraic number field, but for the duration of this chapter, we will only talk about elliptic curves defined over $\mathbb{Q}$ and their corresponding rational solutions.

3.1 Adding Points on an Elliptic Curve

In this section we will outline the method used to add points on an elliptic curve.

Consider rational points $P=(x_1,y_1)$ and $Q=(x_2,y_2)$ on an elliptic curve E and the line going through both P and Q. We construct a third rational point, denoted by $P*Q$, the intersection of this line with the curve E. If $P=Q$ then we consider the tangent line through this point.

Definition 3.1. *The inverse of a point $P=(x,y)$ is $-P=(x,-y)$.*

Once this third point of intersection is found, we reflect across the x-axis by finding its inverse. This method of intersecting and reflecting on points P and Q is denoted in its entirety by $P + Q$. Adding the two points P and $-P$, we get $P + (-P) = \mathcal{O}$, the point at infinity of the elliptic curve E. This is a consequence of the line going through P and $-P$ being vertical and only passing through E at most twice.

The method of intersecting and reflecting points leads to the following important result.

Theorem 3.1. *[23] This operation (intersect and reflect) causes the rational points on the elliptic curve to form an abelian group. The identity element of this group is the point at infinity, $\mathcal{O}$.*

We will now give the formulas for adding points on an elliptic curve. Let E be an elliptic curve defined by $y^2 = x^3 + ax + b$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E with $P_1, P_2 \neq \mathcal{O}$. Define $P_1 + P_2 = P_3 = (x_3, y_3)$ as follows:

1. If $x_1 \neq x_2$, then
   $x_3 = m^2 - x_1 - x_2, \qquad y_3 = m(x_1 - x_3) - y_1, \qquad$ where $m = \frac{y_2 - y_1}{x_2 - x_1}$.
2. If $x_1 = x_2$ but $y_1 \neq y_2$, then $P_1 + P_2 = \mathcal{O}$.
3. If $P_1 = P_2$ and $y_1 \neq 0$, then
   $x_3 = m^2 - 2x_1, \qquad y_3 = m(x_1 - x_3) - y_1, \qquad$ where $m = \frac{3x_1^2 + a}{2y_1}$.
4. If $P_1 = P_2$ and $y_1 = 0$, then $P_1 + P_2 = \mathcal{O}$.

Moreover, define $P + \mathcal{O} = P$ for all points P on E.

3.2 Projective Space and Points at Infinity

In this section, we will discuss projective space and points at infinity of an elliptic curve. We begin with the construction of the real projective plane $\mathbb{P}^2_{\mathbb{R}}$. $\mathbb{P}^2_{\mathbb{R}}$ consists of equivalence classes of triples (X, Y, Z) with X, Y, Z not all zero. Two triples (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) are equivalent if there exists $\lambda \in \mathbb{R}^*$ $(\lambda \neq 0)$ with

$$(X_2, Y_2, Z_2) = (\lambda X_1, \lambda Y_1, \lambda Z_1).$$

Since an equivalence class depends only on ratios, we write our triples $(X : Y : Z)$. Points at infinity occur when $Z = 0$. Therefore we can find

these points by first converting the curve into its homogeneous form. That is, $f(x, y) \to f(X/Z, Y/Z)$.

We can now think of the projective plane as the intersection of the real points of the curve E with the points at infinity.

Example 3.1 (Two distinct parallel lines intersect at infinity)**.** *We define the two lines*

$$\begin{aligned} y &= mx + b_1 \\ y &= mx + b_2. \end{aligned}$$

Converting to homogenous coordinates and clearing denominators we get

$$\begin{aligned} Y &= mX + Zb_1 \\ Y &= mX + Zb_2. \end{aligned}$$

Setting $Z = 0$ we get the two equations $Y = mX$ and $Y = mX$. Thus the solutions are $(X, Y) = (X, mX)$. In projective coordinates this is equivalent to $(X : Y : Z) = (X : mX : 0)$. Scaling by $1/X$ we simplify it to $(1 : m : 0)$.

Example 3.2. *Consider the elliptic curve $y^2 = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$. We want to find the point(s) at infinity of this curve. Converting to homogenous form and clearing denominators we get the equation*

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3.$$

Setting $Z = 0$ we get the equation $0 = X^3$ which yields the solution $X = 0$. Therefore the point at infinity is $(0 : Y : 0)$ which scales to $(0 : 1 : 0)$.

3.3 The Group of Rational Points, Γ

The set of rational points on an elliptic curve, together with the point at infinity, form a group. One of the most interesting results about this group, which we will denote as Γ, is that it is finitely generated and abelian. We now state some definitions and important theorems about Γ.

Definition 3.2. *The torsion subgroup of an abelian group is the subgroup consisting of all elements that have finite order.*

Definition 3.3. *The rank of an elliptic curve is the number of copies of $\mathbb{Z}$ in its group of rational points.*

Theorem 3.2 (Mordell-Weil Theorem [23])**.** *Let $E : y^2 = x^3+ax^2+bx+c \in \mathbb{Q}[x]$ be an elliptic curve. Let Γ denote the group of rational points on E. Then*

$$\Gamma \cong T \oplus \mathbb{Z}^r$$

where T is the torsion subgroup and r is the rank.

3.3.1 The Torsion Subgroup of an Elliptic Curve

As stated above, the torsion subgroup contains all points of finite order. We state some theorems and definitions about the order of a point on an elliptic curve. Note that the point at infinity has order 1 as it is the identity element.

Definition 3.4. *Let $P = (x, y)$ be a point on an elliptic curve $E : y^2 = f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x, y]$. P has order m if $mP = P + P + \cdots + P$ (m times)$= \mathcal{O}$, the point at infinity but $m'P \neq \mathcal{O}$ if $1 \leq m' < m$.*

Theorem 3.3. *[23] The rational points of order 2 in Γ (if they exist) have the form $(x, 0)$ where $x \in \mathbb{Q}$.*

Proof. Suppose $P = (x, y), (x, y \in \mathbb{Q})$ has order 2 in Γ. Then $P \neq \mathcal{O}$ and $2P = \mathcal{O}$ implies that $P + P = \mathcal{O}$ or $P = -P$. This means that P is its own inverse. So $P = (x, y) = (x, -y)$ implies $y = 0$. □

Example 3.3. *Let $E : y^2 = x^3 - 25x$ be an elliptic curve. Setting $y = 0$ we get $0 = x^3 - 25x = x(x - 5)(x + 5)$. So the points of order 2 are $(0, 0)$ and $(\pm 5, 0)$.*

Theorem 3.4. *[23] Let $P = (x, y)$ be a point on an elliptic curve $E : y^2 = f(x) = x^3 + ax^2 + bx + c$, where $a, b, c \in \mathbb{Z}$. Then P has order 3 if x is a root of $3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2$.*

We now state a theorem that classifies points of finite order.

Theorem 3.5 (The Theorem of Nagell-Lutz)**.** *[23] Let $E : y^2 = f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ be an elliptic curve. Let D be the discriminant of $f(x)$ where*

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Let P be a rational point on E of finite order with $P = (x, y)$. Then

1. *$x, y \in \mathbb{Z}$,*
2. *either $y = 0$ or $y^2 \mid D$.*

The problem with this theorem is that there may be many candidates for possible points where $y^2 \mid D$. Nagell-Lutz doesn't tell you which group the torsion subgroup is isomorphic to, only the points themselves. We now state a definition and another theorem that will further help to find the torsion subgroup.

Definition 3.5. *Let $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ be an elliptic curve with $a, b, c \in \mathbb{Z}$ and let D be the discriminant of $f(x)$. Then a bad prime is a prime that divides $2D$ and a good prime is every prime that is not a bad prime.*

Theorem 3.6 (Reduction mod p)**.** *[23] Let $E : y^2 = f(x) = x^3+ax^2+bx+c$ be an elliptic curve with $a, b, c \in \mathbb{Z}$ and let D be the discriminant of $f(x)$. Let T be the torsion subgroup of Γ, the group of rational points of E.*

For any good prime p, let $P \to \tilde{P}$ be the reduction map mod p mapping T into $\tilde{E}$ (mod p). This mapping $\sim: T \to \tilde{E}$ is an isomorphism.

That is, the order of T divides the number of points of $\tilde{E}$ (reduced mod p) plus the one point at infinity.

Example 3.4. *Consider $E : y^2 = f(x) = x^3 + x + 1$. The discriminant of $f(x)$ is -31 so that the bad primes are 2 and 31. We first reduce modulo 3, solve using the `msolve` command in Maple, and get a total of 3 solutions plus the point at infinity. Reducing modulo 5, we get a total of 8 solutions plus the point at infinity. Therefore we have $|T| \mid 4$ and $|T| \mid 9$ which imples that $|T| = 1$. So then $T \cong \{0\}$.*

From now on, we will use the notation $|\tilde{E}_p|$ for the number of points on E mod p plus the one point at infinity.

Example 3.5. *Consider $E : y^2 = f(x) = x^3 + 4x = x(x^2 + 4)$. We can see that the point $(0, 0)$ is a point of order 2 on E. From this, we know that $|T| > 1$. We also have $D = -256$ so that the bad prime is $p = 2$. We see that $|\tilde{E}_3| = 4$ so $|T| \mid 4 \Rightarrow |T| = 2$ or $|T| = 4$. We then use Nagell-Lutz to determine if there are any more points than the one point of order 2 that we found. If there is at least one more point, then the order of T must be equal to 4.*

We now give one more theorem that will help find the torsion subgroup.

Theorem 3.7 (Mazur's Theorem)**.** *[23] Let E be an elliptic curve. The torsion subgroup T of the group of rational points Γ is one of the following 15 groups:*

1. $\mathbb{Z}_N$ *with* $1 \leq N \leq 10$ *or* $N = 12$ *(cyclic group of order* N*),*

2. $\mathbb{Z}_2 \times \mathbb{Z}_{2N}$ *with* $N = 1, 2, 3, 4$ *(direct products).*

We now give some examples that will show how to fully find the torsion subgroup of a given elliptic curve.

Example 3.6. *Consider* $y^2 = f(x) = x^3 - 432x + 8208$ *where discrim*$(f(x)) = -2^8 \cdot 3^{12} \cdot 11$*. Reducing modulo 5, we find* $|\tilde{E}_5| = 5$*. This implies that* $|T| = 1$ *or* $|T| = 5$*.*

Using Nagell-Lutz, we know that $y^2 = 2^{2i} \cdot 3^{2j}$ *where* $0 \leq i \leq 4$ *and* $0 \leq j \leq 6$*. Running through all the values we yield the solutions* $(x, y) = (-12, \pm 108)$ *and* $(x, y) = (24, \pm 108)$*. Using Magma, we find that the order of these points is 5. So we now know that* $|T| = 5$ *and the only group of order 5 listed in Mazur's Theorem is* $\mathbb{Z}_5$*. Thus* $T \cong \mathbb{Z}_5$*.*

Example 3.7. *Consider* $y^2 = f(x) = x^3 - 1386747x + 368636886 = (x + 1293)(x - 282)(x - 1011)$ *where* $D(f) = 2^{16} \cdot 3^{20} \cdot 5^4 \cdot 7^2$*. By observation, we see that there are 3 points of order 2. From this, we know that the torsion subgroup cannot be cyclic, it must be one of the direct products. Reducing modulo 11, we find* $|\tilde{E}_{11}| = 16$*.*

Using Nagell-Lutz, we yield a solution $(x, y) = (1227, 22680)$ *and using Magma, we find that the order of this point is equal to 8. The only direct product in Mazur's Theorem that this applies to is* $T \cong \mathbb{Z}_2 \times \mathbb{Z}_8$*.*

3.3.2 The Rank of an Elliptic Curve

Before we get into rank, we introduce a tool called the height of a rational point. We will use this to prove that Γ is finitely generated later on. This concept is used to measure how complicated a rational point is from a number theory perspective.

Definition 3.6. *Let* $x = m/n$ *be a rational number in lowest terms. Then the height of* x *is defined to be* $H(x) = max\{|m|, |n|\}$*.*

Theorem 3.8 (Finiteness Property of Height)**.** *[23] The set of all rational numbers whose height is less than some bound is finite.*

If $P = (x, y)$ is a rational point on $E : Y^2 = X^3 + aX^2 + bX + c$, where $a, b, c \in \mathbb{Q}$, we define the height of P to be

$$H(P) = H(x).$$

Definition 3.7. *We define logarithmic height as* $h(P) = ln(H(P))$.

We now state some lemmas that will be used to prove that Γ is a finitely generated group. These lemmas and their proofs can be found in Silverman and Tate [23].

Lemma 3.1. *For every real number* M*, the set*

$$\{P \in \Gamma : h(P) \leq M\}$$

is finite.

Lemma 3.2. *Let* P_0 *be a fixed rational point on a curve* C*. There is a constant* κ_0*, depending on* P_0 *and on* a, b, c*, so that*

$$h(P + P_0) \leq 2h(P) + \kappa_0 \qquad \text{for all } P \in \Gamma.$$

Lemma 3.3. *There is a constant* κ*, depending on* a, b, c*, so that*

$$h(2P) \geq 4h(P) - \kappa \qquad \text{for all } P \in \Gamma.$$

Lemma 3.4. *The index* $(\Gamma : 2\Gamma)$ *is finite.*

Theorem 3.9 (Descent Theorem)**.** *[23] Let* Γ *be a commutative group. Suppose that there is a function*

$$h : \Gamma \to [0, \infty)$$

with the following three properties.

1. *For every real number* M*, the set* $\{P \in \Gamma : h(P) \leq M\}$ *is finite.*

2. *For every* $P_0 \in \Gamma$*, there is a constant* κ_0 *so that*

$$h(P + P_0) \leq 2h(P) + \kappa_0 \qquad \text{for all } P \in \Gamma.$$

3. *There is a constant* κ *so that*

$$h(2P) \geq 4h(P) - \kappa \qquad \text{for all } P \in \Gamma.$$

Suppose further that

4. *The subgroup* 2Γ *has finite index in* Γ.

Then Γ *is finitely generated.*

With this knowledge, we introduce some concepts that will enable us to calculate rank using the algorithm 2-descent by isogeny.

Consider the set $Q^{*^2} = \{r^2 = (\frac{a}{b})^2 \mid r \in \mathbb{Q}^*\}$. Let $G = \langle \mathbb{Q}^*, \cdot \rangle$ be a group and let $H \leq G$ be the subgroup of G where $H = \langle \mathbb{Q}^{*^2}, \cdot \rangle$. Then the quotient group with respect to G and H is $\mathbb{Q}^*/\mathbb{Q}^{*^2}$. Elements of this quotient group are $r \cdot \mathbb{Q}^{*^2}$ where r is a squarefree rational.

We will now outline the algorithm for finding rank of an elliptic curve of the form $E : y^2 = x^3 + ax^2 + bx$ where $a, b \in \mathbb{Z}$.

Consider the curve $\bar{E} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$ where $\bar{a} = -2a$ and $\bar{b} = a^2 - 4b$. Define the squarefree maps $\alpha : \Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*^2}$ and $\bar{\alpha} : \bar{\Gamma} \to \mathbb{Q}^*/\mathbb{Q}^{*^2}$ by

$$\alpha(P) = \begin{cases} 1 \pmod{\mathbb{Q}^{*^2}} & \text{if } P = \mathcal{O} \\ b \pmod{\mathbb{Q}^{*^2}} & \text{if } P = (0,0) \\ x \pmod{\mathbb{Q}^{*^2}} & \text{if } P \neq (0,0), P = (x,y) \end{cases}$$

and

$$\bar{\alpha}(\bar{P}) = \begin{cases} 1 \pmod{\mathbb{Q}^{*^2}} & \text{if } \bar{P} = \bar{\mathcal{O}} \\ \bar{b} \pmod{\mathbb{Q}^{*^2}} & \text{if } \bar{P} = (0,0) \\ \bar{x} \pmod{\mathbb{Q}^{*^2}} & \text{if } \bar{P} \neq (0,0), \bar{P} = (\bar{x}, \bar{y}). \end{cases}$$

Furthermore, $\alpha(P) \mid b$ and $\bar{\alpha}(\bar{P}) \mid \bar{b}$. Each of $\alpha(\Gamma)$ and $\bar{\alpha}(\bar{\Gamma})$ is a finite subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*^2}$ and if $r = rank(E)$ then

$$2^{r+2} = |\alpha(\Gamma)||\bar{\alpha}(\bar{\Gamma})|$$

Theorem 3.10. *[23] Let E and $\bar{E}$ be elliptic curves given by $E : y^2 = x^3 + ax^2 + bx, \bar{E} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$ where $\bar{a} = -2a$ and $\bar{b} = a^2 - 4b$.*

Let $\Gamma, \bar{\Gamma}$ be the respective groups of rational points on E and $\bar{E}$. Let $P = (x, y)$ be a point on E and $\bar{P} = (\bar{x}, \bar{y})$ be a point on $\bar{E}$.

1. *There is a homomorphism*
   $\phi : \Gamma \to \bar{\Gamma}$ defined by

$$\phi(P) = \begin{cases} (\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}) & \text{if } P = (x,y), P \neq \mathcal{O}, P \neq (0,0) \\ \bar{\mathcal{O}} & \text{if } P = \mathcal{O} \text{ or } P = (0,0). \end{cases}$$

   The kernel of ϕ is $\{\mathcal{O}, (0,0)\}$.

2. *There is a homomorphism*
   $\psi : \bar{\Gamma} \to \Gamma$ *defined by*

$$\psi(\bar{P}) = \begin{cases} (\frac{\bar{y}^2}{4\bar{x}^2}, \frac{\bar{y}(\bar{x}^2-\bar{b})}{8\bar{x}^2}) & \text{if } P = (\bar{x}, \bar{y}), P \neq \mathcal{O}, P \neq (0,0) \\ \mathcal{O} & \text{if } \bar{P} = \bar{\mathcal{O}} \text{ or } \bar{P} = (0,0). \end{cases}$$

   The kernel of ψ *is* $\{\bar{\mathcal{O}}, (0,0)\}$.

As a consequence, $\psi \circ \phi(P) = 2P$.

Recall $\alpha(\Gamma)$ (respectively $\bar{\alpha}(\bar{\Gamma})$) as the set of square-free values of the x-coordinates of points in Γ. Furthermore, $\alpha(\Gamma) \subseteq \{$square-free divisors of b$\}$ and $\bar{\alpha}(\bar{\Gamma}) \subseteq \{$square-free divisors of $\bar{b}\}$.

Theorem 3.11. *[23] For* $E : y^2 = x^3 + ax^2 + bx$, *let* b_1 *be a square-free divisor of* b. *Let* $b_2 = b/b_1$. *Then* $b_1 \in \alpha(\Gamma) \iff \exists$ *integers* N, M, e *with* $\gcd(M, e) = \gcd(N, e) = \gcd(b_1, e) = \gcd(b_2, M) = \gcd(M, N) = 1$ *and*

$$N^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4.$$

The above quartic equation is known as a torsor. The above theorem applies for $\bar{\alpha}(\bar{\Gamma})$ *by replacing* $a, b, b_1, b_2, \alpha, \Gamma$ *with their corresponding counterparts,*

Example 3.8. *Let* $E : y^2 = x^3 - 97x$ *be an elliptic curve. We have* $b = -97$. *We begin by finding* $\alpha(\Gamma)$. *We know* $\alpha(\Gamma) \subseteq \{$*square-free divisors of* $b\} = \{1, -1, 97, -97\}$.

Since $\alpha(\mathcal{O}) = 1$ *and* $\alpha(0,0) = b = -97$ *we know* $\alpha(\Gamma) \supseteq \{1, -97\}$. *We now consider torsors for values of* b_1. *Let* $b_1 = 97$. *Then the torsor is*

$$N^2 = 97M^4 - e^4.$$

This equation has solution $(N, M, e) = (9, 1, 2)$ *that satisfies all 5 gcd conditions. Thus* $97 \in \alpha(\Gamma)$. *By closure,* $(97)(-97) = -1$ *is in* $\alpha(\Gamma)$ *as well. Therefore we have all of the elements for* $\alpha(\Gamma) = \{1, -1, 97, -97\}$.

Now consider $\bar{E} : y^2 = x^3 + 388x$. *We now find* $\bar{\alpha}(\Gamma)$. *We know* $\bar{\alpha}(\Gamma) \subseteq \{1, -1, 2, -2, 97-, 97, 194, -194\}$ *and* $\bar{\alpha}(\Gamma) \supseteq \{1, 97\}$. *We first consider the torsor*

$$N^2 = -M^4 - 388e^4.$$

This is insolvable as the left hand side is positive while the right hand side is negative. Therefore $-1 \notin \bar{\alpha}(\bar{\Gamma})$. *By similar reasoning we can also eliminate -2, -97, and -194. We now consider the torsor*

$$N^2 = 2M^4 + 194e^4$$

This torsor has solution $(N, M, e) = (14, 1, 1)$ *that satisfies the gcd conditions. Therefore,* $2 \in \bar{\alpha}(\bar{\Gamma})$ *and thus* $184 \in \bar{\alpha}(\bar{\Gamma})$ *as well by closure. Then* $\bar{\alpha}(\bar{\Gamma}) = \{1, 2, 97, 194\}$.

We then have $2^{r+2} = |\alpha(\Gamma)||\bar{\alpha}(\bar{\Gamma})| = 4 \cdot 4 = 16 \Rightarrow r = 2$.

Chapter 4

Algebraic Curves of Genus 2

While curves of genus 1 are known as elliptic curves, any algebraic curve with any genus ≥ 1 is known as hyperelliptic. We now explore algebraic curves of genus 2 whose rational points have a corresponding structure similar to the group of rational points of elliptic curves. Curves of genus 2 generally appear in the form

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

where $f(x)$ is a quintic or sextic polynomal over $\mathbb{Q}$ with no repeated roots in $\mathbb{C}$. However, just like elliptic curves, curves of genus 2 can appear in a very general form. For example, the curve

$$y^2 - xy - y = x^5 - 3x^2 + 7$$

is of genus 2.

Curves of genus 2 cannot be parametrized like curves of genus 0 nor do their rational points form a group like elliptic curves. One of the most important problems with curves of genus 2 is trying to find their rational points. Even though finding these points can be very difficult or impossible, a very nice result about these curves comes in form of the following theorem:

Theorem 4.1 (Faltings' Theorem)**.** *[6] Let $\mathcal{C}$ be a curve of genus greater than or equal to 2 over a number field K. Then $\mathcal{C}$ has only finitely many rational points.*

As mentioned above, the rational points on genus 2 curves do not form a group structure. We can, however, consider a parallel structure based from the curve $\mathcal{C}$ known as the Jacobian.

4.1 The Jacobian

We first describe the Jacobian in the language of algebraic geometry used in Freiberg [11].

Definition 4.1. *The divisor group of a curve $\mathcal{C}$, denoted Div($\mathcal{C}$), is the free abelian group generated by the points of $\mathcal{C}$. Thus a divisor $D \in Div(\mathcal{C})$ is a formal sum*

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

with $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in \mathcal{C}$. In other words, the points $P \in \mathcal{C}$ form a basis for the divisor group. The degree of D is defined by

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

The divisors of degree 0 form a subgroup of Div($\mathcal{C}$),

$$Div^0(\mathcal{C}) = \{D \in Div(\mathcal{C}) : deg(D) = 0\}.$$

We define some notation that will be used below. If $f \in \bar{k}(\mathcal{C})^*$, then f is a nonzero rational function defined over the curve $\mathcal{C}$ with coefficients in $\bar{k}$, the algebraic closure of the field k.

Definition 4.2. *Let f be a rational function. A pole is a point at which f is undefined. The exponent of this factor determines the multiplicity of this pole.*

Proposition 4.1. *Let $\mathcal{C}$ be a smooth curve and $f \in \bar{k}(\mathcal{C})^*$. Then there are only finitely many points of $\mathcal{C}$ at which f has a pole or a zero. Futher, if f has no poles, then $f \in \bar{k}$.*

Definition 4.3. *Let $\mathcal{C}$ be a smooth curve, and let $f \in \bar{k}(\mathcal{C})^*$. We define a map*

$$div : \bar{k}(\mathcal{C})^* \mapsto Div(\mathcal{C})$$
$$f \mapsto \sum_{P \in \mathcal{C}} ord_P(f)(P).$$

(div(f) is a divisor by Proposition 4.1.) A divisor $D \in Div(\mathcal{C})$ is called principal if $D = div(f)$ for some $f \in \bar{k}(\mathcal{C})^*$.

Definition 4.4. *By Proposition 4.1, the set of principal divisors form a subgroup of $Div^0(\mathcal{C})$, denoted $Pr(\mathcal{C})$. We say divisors D_1, D_2 are linearly equivalent, and write $D_1 \sim D_2$ if $D_1 \equiv D_2$ modulo the subgroup $Pr(\mathcal{C})$. The Picard group of $\mathcal{C}$, $Pic(\mathcal{C})$, is the quotient group $Div(\mathcal{C})/Pr(\mathcal{C})$.*

We are now ready to give the definition of the Jacobian.

Definition 4.5. *While $Pic(\mathcal{C}) = Div(\mathcal{C})/Pr(\mathcal{C})$, similarily we have $Pic^0(\mathcal{C}) = Div^0(\mathcal{C})/Pr(\mathcal{C})$. This group, $Pic^0(\mathcal{C})$, is the subgroup of $Pic(\mathcal{C})$, called the Jacobian of $\mathcal{C}$.*

This representation of the Jacobian in geometric terms is definitely non-trivial. Luckily, we can express the Jacobian in a different way. Cassels and Flynn [6] describes the Jacobian in the following way:

Let $\mathcal{C}$ be a curve of genus 2 over $\mathbb{Z}$ and let $J(\mathbb{Q})$ be the Jacobian of the curve $\mathcal{C}$. It is easy to find the Weierstrass points $(x, 0)$ as they are simply the rational roots of the curve. Therefore we consider the non-Weierstrass points in $\mathcal{C}(\mathbb{Q})$.

Let $P \in \mathcal{C}(\mathbb{Q})$ be a non-Weierstrass point. Then there exists a correspondence

$$P \in \mathcal{C}(\mathbb{Q}) \longleftrightarrow \{P, P\} \in J(\mathbb{Q}).$$

Essentially, the Jacobian can be viewed as pairs of points on $\mathcal{C}$. The Jacobian also has a finite part, which we will denote as $J(\mathbb{Q})_{tors}$ and an infinite part, which we will denote as $\mathcal{D}$. This leads into an important result analogous to that of elliptic curves.

Theorem 4.2. *Consider the rational points on $\mathcal{C}$ denoted as $P_i = (x_i, y_i)$. Now consider all pairs of points $\{P_i, P_k\}$. These pairs of points, with the identity element $\{\infty, \infty\}$ form a finitely generated abelian group.*

Now that we have a group structure, we can use it to calculate these pairs of points. Once we have found the structure of the Jacobian, we can work backwards to get the actual rational points on the original curve.

4.2 Adding Points on the Jacobian

While adding points directly on a genus 1 curve is quite simple, adding points on the Jacobian of a genus 2 curve is not at all trivial. We consider a curve $\mathcal{C} : y^2 = f(x) = a_6x^6 + \cdots + a_0$ where $a_i \in \mathbb{Z}$ and $f(x)$ is a quintic or sextic with no repeated roots in $\mathbb{C}$. We want to uniquely represent adding pairs of points $\{P_1, P_2\} + \{P_3, P_4\}$ as a single pair of points $\{P_5, P_6\}$.

Note that $\infty^{\pm} = (0, \pm\sqrt{a_6})$ denotes the points at infinity on $\mathcal{C}$.

4.2.1 The Interpolating Polynomial

We now discuss the interpolating cubic (or quadratic as seen later). As outlined in Freiberg [11], adding points on the Jacobian requires one to find

the intersection of a interpolating cubic $y = m(x)$ with the curve $\mathcal{C} : y^2 = f(x)$. This intersection leads to the equation

$$f(x_i) - m^2(x_i) = 0, \quad i = 1, \cdots 4.$$

These x_i are the four of the six roots of the sextic

$$f(x) - m^2(x).$$

These four roots of this sextic correspond to the original points that are being added together, while the remaining two are the x-coordinates of the new pair of points $\{P_5, P_6\}$. (If one of the $P_i = \infty^{\pm}$, then $m(x)$ is in fact a quadratic and there are five points of intersection).

Some methods of interpolating include Lagrange Interpolation or Newton Interpolation. We will interpolate by forming a set of linear equations whose solution defines the coefficients of our interpolating cubic or quadratic. The idea behind this method is given in [11]. For our purposes we will avoid the theory and just stick to outlining the methods for the different cases.

For all our cases, we start with a general equation of a cubic $g = ax^3 + bx^2 + cx + d$ and our curve $y^2 = f(x)$. Note that $y_k = \sqrt{f}(x_k)$ and $y_k^{(n)} = \sqrt{f}^{(n)}(x_k)$.

Case 4.1 (Four distinct points)**.** *We start with the case that all four points are entirely distinct. In this situation, we have the four equations*

$$\begin{aligned} g(x_1) = y_1 &\Longrightarrow ax_1^3 + bx_1^2 + cx_1 + d = y_1 \\ g(x_2) = y_2 &\Longrightarrow ax_2^3 + bx_2^2 + cx_2 + d = y_2 \\ g(x_3) = y_3 &\Longrightarrow ax_3^3 + bx_3^2 + cx_3 + d = y_3 \\ g(x_4) = y_4 &\Longrightarrow ax_4^3 + bx_4^2 + cx_4 + d = y_4. \end{aligned}$$

Solving these four equations for a, b, c, d gives us the coefficients for our interpolating cubic.

Case 4.2 (Three distinct points)**.** *If only three points are distinct, then we have to treat it slightly differently than Case 4.1. Suppose without loss of generality, P_1 is the non-distinct point. That is, we are adding say $\{P_1, P_1\}$ and $\{P_2, P_3\}$. We then get the four equations*

$$\begin{aligned} g(x_1) = y_1 &\Longrightarrow ax_1^3 + bx_1^2 + cx_1 + d = y_1 \\ g'(x_1) = y_1' &\Longrightarrow 3x_1^2 + 2bx_1 + cx_1 = y_1' \\ g(x_2) = y_2 &\Longrightarrow ax_2^3 + bx_2^2 + cx_2 + d = y_2 \\ g(x_3) = y_3 &\Longrightarrow ax_3^3 + bx_3^2 + cx_3 + d = y_3. \end{aligned}$$

Case 4.3 (Two distinct points)**.** *Say for example we are adding the pairs of points* $\{P_1, P_1\} + \{P_1, P_2\}$*. Then we get the equations*

$$\begin{aligned} g(x_1) = y_1 &\Longrightarrow ax_1^3 + bx_1^2 + cx_1 + d = y_1 \\ g'(x_1) = y_1' &\Longrightarrow 3ax_1^2 + 2bx_1 + cx_1 = y_1' \\ g''(x_1) = y_1'' &\Longrightarrow 6ax_1 + 2b = y_1'' \\ g(x_2) = y_2 &\Longrightarrow ax_2^3 + bx_2^2 + cx_2 + d = y_2. \end{aligned}$$

If we are adding say $\{P_1, P_1\} + \{P_2, P_2\}$ *then we get*

$$\begin{aligned} g(x_1) = y_1 &\Longrightarrow ax_1^3 + bx_1^2 + cx_1 + d = y_1 \\ g'(x_1) = y_1' &\Longrightarrow 3ax_1^2 + 2bx_1 + cx_1 = y_1' \\ g(x_2) = y_2 &\Longrightarrow ax_2^3 + bx_2^2 + cx_2 + d = y_2 \\ g'(x_2) = y_2' &\Longrightarrow 3ax_2^2 + 2bx_2 + cx_2 = y_2' \end{aligned}$$

Case 4.4 (One point)**.** *In this case we are adding the pairs of points* $\{P_1, P_1\} + \{P_1, P_1\}$*.*

$$\begin{aligned} g(x_1) = y_1 &\Longrightarrow ax_1^3 + bx_1^2 + cx_1 + d = y_1 \\ g'(x_1) = y_1' &\Longrightarrow 3ax_1^2 + 2bx_1 + cx_1 = y_1' \\ g''(x_1) = y_1'' &\Longrightarrow 6ax_1 + 2b = y_1'' \\ g'''(x_1) = y_1''' &\Longrightarrow 6a = y_1''' \end{aligned}$$

Case 4.5 (A point at infinity)**.** *Say for example we are adding the points* $\{\infty, P_1\} + \{P_1, P_1\}$*. Then instead of a cubic, we start with a quadratic* $g = ax^2 + bx + c$ *and get the equations*

$$\begin{aligned} g(x_1) = y_1 &\Longrightarrow ax_1^2 + bx_1 + c = y_1 \\ g'(x_1) = y_1' &\Longrightarrow 2ax_1 + b = y_1' \\ g''(x_1) = y_1'' &\Longrightarrow 2a = y_1''. \end{aligned}$$

If the three non-infinite points are distinct from each other such as in the previous cases, then the same methodology applies as above except with three linear equations instead of four.

We outline this method by using an example from [11].

Example 4.1. *Consider the curve* $\mathcal{C} : y^2 = f(x) = x^5 - 2x$ *defined over* $\mathbb{Q}$. *The points on this curve are* $(0,0), (-1, \pm 1)$, *and* ∞. *We want to add the pairs of points* $\{(-1,1),(-1,1)\} + \{(-1,1),(-1,1)\} = \{(x_5, y_5), (x_6, y_6)\}$. *In this case, our four equations are*

$$\begin{aligned} a(-1)^3 + b(-1)^2 + c(-1) + d &= 1 \\ 3a(-1)^2 + 2b(-1) + c &= \frac{3}{2} \\ 6a(-1) + 2b &= -\frac{49}{4} \\ 6a &= \frac{681}{8} \end{aligned}$$

which leads to

$$\begin{aligned} -a + b - c + d - 1 &= 0 \\ 3a - 2b + c - \frac{3}{2} &= 0 \\ -6a + 2b + \frac{49}{4} &= 0 \\ 6a - \frac{681}{8} &= 0 \end{aligned}$$

After solving the system above, we obtain our solution for a, b, c, d *and our interpolating cubic is*

$$m(x) = \frac{227}{16}x^3 + \frac{583}{16}x^2 + \frac{509}{16}x + \frac{169}{16}.$$

Factoring the equation $f(x) - m^2(x)$, *we get*

$$f(x) - m^2(x) = -\frac{1}{256}(51529x^2 + 58310x + 28561)(x+1)^4.$$

The four points $(x = -1)$ *come from the quartic factor. We are interested in the other two points from the quadratic above. Solving the quadratic, we obtain the solutions*

$$\begin{aligned} x_5 &= -\frac{29155}{51529} + \frac{132}{51529}\sqrt{35681} \\ x_6 &= -\frac{29155}{51529} - \frac{132}{51529}\sqrt{35681}. \end{aligned}$$

Then $y_5 = -m(x_5)$ *and* $y_6 = -m(x_6)$.

Example 4.2. *We now add the pairs of points* $\{\infty, (-1,1)\}+\{(-1,1),(-1,1)\}$. *Since one of the points is a point at infinity, we only need to consider three linear equations. They are as follows.*

$$\begin{aligned} a - b + c - 1 &= 0 \\ -2a + b - \frac{3}{2} &= 0 \\ 2a + \frac{49}{4} &= 0. \end{aligned}$$

The solution to this system leads to the interpolating quadratic

$$m(x) = -\frac{49}{8}x^2 - \frac{43}{4}x - \frac{29}{8}.$$

We now find the difference $f(x) - m^2(x)$ *and factor to get*

$$\frac{1}{64}(64x^2 - 2593x - 841)(x+1)^3.$$

Finding the solution to the above quadratic yields

$$x_5, x_6 = \frac{1}{128}(2593 \pm \sqrt{6938945})$$

where $y_5, y_6 = -m(x_5), -m(x_6)$.

We now introduce a method of finding points on a curve $\mathcal{C}$ that applies when the rank of the Jacobian is strictly less than the genus of $\mathcal{C}$.

4.3 Chabauty's Method

We begin this section with a relevant theorem to curves of genus 2.

Theorem 4.3. *[6] Let* $\mathcal{C}$ *be a curve of genus* $g > 1$ *defined over a number field* K. *If the Jacobian has rank less than* g *then* $\mathcal{C}(K)$ *is finite.*

Since we are considering curves $\mathcal{C}$ with genus equal to 2, we only need to consider curves with the rank of the Jacobian of 0 and 1. First we consider the case when the rank of the Jacobian is 0. If $J(\mathbb{Q})$ has rank 0, then $J(\mathbb{Q}) = J(\mathbb{Q})_{tors}$. This group $J(\mathbb{Q})_{tors}$ is finite and the points are easy to find.

If the rank of $J(\mathbb{Q})$ is 1, then it becomes necessary to find a generator for the infinite part of $J(\mathbb{Q})$, denoted by $\mathcal{D}$ so that

$$J(\mathbb{Q}) =< J(\mathbb{Q})_{tors}, \mathcal{D} > .$$

Once this generator is found, then some local calculations are done at some prime $p \nmid 2\Delta$ where $\mathcal{C}$ has good reduction. The algorithm then uses a p-adic method involving Strassman's Theorem to bound the number of rational points.

Theorem 4.4 (Strassman's Theorem)**.** *[6] Let $\theta(X) = c_0 + c_1X + \cdots \in \mathbb{Z}_p[[X]]$ satisfy $c_k \to 0$ in $\mathbb{Z}_p$. Define l uniquely by: $|c_l|_v \geq |c_j|_v$ for all $j \geq 0$, and $|c_l|_v > |c_j|_v$ for all $j > l$. Then there are at most l values of $x \in \mathbb{Z}_p$ such that $\theta(x) = 0$ and $|x|_v \leq 1$.*

Cassels and Flynn [6] outlines the steps of this algorithm as follows:

1. Try to find $J(\mathbb{Q})_{tors}$ and $J(\mathbb{Q})/2J(\mathbb{Q})$, and show that the Jacobian has rank 1.
2. Use heights to find a generator $\mathcal{D}$ such that $J(\mathbb{Q}) =< J(\mathbb{Q})_{tors}, \mathcal{D} >$.
3. Find the Chabauty bound with respect to some good prime p.

We now provide some interesting results about curves of genus 2 and then talk about using Magma when confronted with a genus 2 curve.

Theorem 4.5. *[6] Let $\mathcal{C}$ be a curve of genus 2 over $\mathbb{Q}$ and $p \geq 5$ be a prime of good reduction. If $J(\mathbb{Q})$ has rank at most 1 and $\widetilde{\mathcal{C}}$ is the reduction of $\mathcal{C}$ mod p. Then*

$$|\mathcal{C}(\mathbb{Q}| \leq |\widetilde{\mathcal{C}}(\mathbb{F}_p)| + 2$$

Theorem 4.6. *[6] Let $\mathcal{C}$ be the curve of genus 2*

$$C : Y^2 = X(X^2 - 1)(X - 1/\lambda)(X^2 + aX + b) \qquad (\lambda, a, b \in \mathbb{Z}).$$

Suppose $3^{2r} \mid \lambda$ for some $r > 0$ and $3 \nmid b(1 - a + b)(1 + a + b)$ and that the Jacobian of $\mathcal{C}$ has rank at most 1. Then $\mathcal{C}(\mathbb{Q})$ contains precisely the points $(0, 0), (1, 0), (1/\lambda, 0)$ and the two rational points at infinity.

4.4 Chabauty's Method in Magma

The previous algorithm has been implemented into Magma and uses a combination of this algorithm, along with the Mordell-Weil sieve [1] to precisely determine the rational points on the curve.

There are two different cases that require two slightly different methods in order to find all of the rational points on the curve.

Case 4.6 (When the rank of the Jacobian is equal to 0)**.**
In this case, known as the trivial case, we can use the Magma command `ChabautyO` *to enumerate all of the points on the curve. This command only requires the Jacobian of the curve as input.*

Case 4.7 (When the rank of the Jacobian is equal to 1)**.**
This case requires a little more calculation and work. Let $\mathcal{C}$ *be a hyperelliptic curve and let* $J(\mathbb{Q})$ *be the Jacobian. In order to use the* `Chabauty` *command, we require a point on the Jacobian that is a generator of* $J(\mathbb{Q})/J(\mathbb{Q})_{tors}$*. Let* $C_i = (x_i, y_i)$ *be the points of* C*. The generator point can be found by finding a point* $\{C_i, C_j\}$ *on the Jacobian for some* i, j *that has infinite order in* $J(\mathbb{Q})$*. Once this point is found, we can input it into the* `Chabauty` *command to enumerate all of the points.*

Case 4.8 (When the rank of the Jacobian is ≥ 2)**.**
This case requires going to Elliptic Chabauty methods that we will omit in this thesis. For more information on these methods, see [4].

4.4.1 Some Examples

We now give some examples outlined in the Magma handbook [1] that use Chabauty's method to solve.

Example 4.3. *Consider the curve*

$$\mathcal{C} : y^2 = x^6 + 4.$$

Using a height search with the command `Points`*, Magma finds the points* $(x, y) = (0, \pm 2)$ *and the two rational points at infinity. The command* `RankBounds` *finds that the rank of the Jacobian is 0. Thus, we can enumerate all the points on* $\mathcal{C}$ *using the command* `ChabautyO`*. The 4 points listed above are reiterated as the only points on* $\mathcal{C}$*.*

Example 4.4. *Consider the curve*

$$\mathcal{C} : y^2 = x^6 + x^2 + 2.$$

Using the command `Points`*, Magma finds the 4 points* $(x, y) = (\pm 1, \pm 2)$ *plus the 2 rational points at infinity. Using the command* `RankBounds` *we find that the rank of the Jacobian is 1. We now need to find points on* $\mathcal{C}$ *that give us points of infinite order on the Jacobian* $J(\mathbb{Q})$*.*

Now consider the point $\{(1, -2), \infty^-\}$*. The order of this point is infinite and it can be shown that it generates* $J(\mathbb{Q})/J(\mathbb{Q})_{tors}$*, thus being able to use it in the* `Chabauty` *command. Using this command, we find that the points listed above are the only points on this curve.*

4.5 A Special Case: The Curve $\mathcal{C}_k : y^2 = x^5 + k$

We are now going to talk about the family of genus 2 curves $\mathcal{C}_k : y^2 = x^5 + k$ where k is a tenth-power-free integer considered in a paper by Stoll [25]. Stoll proved a very nice result concerning these curves stated in the following theorem:

Theorem 4.7. *Let $\mathcal{C}_k = x^5 + k$ be a genus 2 curve with k a tenth-free-power integer. Let $J(\mathbb{Q})$ be the Jacobian of C_k. Assume rank$(J(\mathbb{Q}))$=1. Then $|C_k| \leq 7$. The bound of 7 is achieved only for $k = 324$. For all other values of k, the bound is 6 if there exists any Weierstrass points (points of the form $(x, 0)$) and 5 otherwise.*

The idea behind this theorem comes from counting the number of rational points on the curve $\mathcal{C}_k$. Stoll showed that the number of rational points on the curve (denoted by $\#\mathcal{C}_k(\mathbb{Q})$) is equal to $2n_k + d_k$ where n_k is half the number of "nontrivial" points in $\mathcal{C}_k(\mathbb{Q})$, i.e., finite points with nonvanishing x and y coordinates, and $d_k = 1, 2, 3$, or 4 if k is neither a square nor a fifth power, a fifth power but $k \neq 1$, a square but $k \neq 1$, or $k = 1$, respectively.

The bound stated in the theorem is a very nice result since we can use a height search to find points on a hyperelliptic curve using Magma. If we have found, say 5 points (if $k \neq 324$) and there are no points of the form $(x, 0)$ then we know we have found them all. The usefulness of this theorem will become more apparent in Chapter 6.

Chapter 5

A Diophantine System and a Problem on Cubic Fields

In this chapter we will discuss a problem from Kaneko [15] who considered families of cubic fields and their fundamental units. Kaneko proved that there are finitely many triples (A, B, b) of integers satisfying the system

$$\begin{aligned} A^2 - 2B &= 3(b^2+1), \\ B^2 - 2A &= 3(b^4+b^2+1), \end{aligned} \tag{5.1}$$

and the following solutions were given.

$$(A, B, b) = (-1, -1, 0), (3, 3, 0), \text{ and } (0, -3, \pm 1).$$

The study of this system was related to the following problem about cubic fields. Let θ be a root of the irredicble cubic polynomial $f(x)$ given by

$$f(x) = x^3 - 3x - b^3, \ b(\neq 0) \in \mathbb{Z}.$$

Let $K = \mathbb{Q}(\theta)$ be the cubic field defined by $f(x)$ and set

$$\varepsilon = \frac{1}{1 - b(\theta - b)}.$$

As proved in [15] $\varepsilon(> 1)$ is the fundamental unit of K for infinitely many values of b. A solution of the above system of equations would yield a value of b for which ϵ was not the fundamental unit of K. In [16], we gave a simple complete solution of this Diophantine system, finding a total of six solutions.

We begin by stating our main result, follow with some relevant lemmas and then finish with a proof.

Theorem 5.1. *The Diophantine system (5.1) has the solutions*

$$(A, B, b) = (0, -3, \pm 1), \ (-1, -1, 0), (3, 3, 0) \text{ and } (8, 17, \pm 3).$$

Our method of proof involves finding the integral points on a genus 0 curve. A general method for solving this type of problem is given in [18], [19]. As described in Section 2.1, we parametrize the rational points on the curve then reduce the determination of the integral solutions to a finite set of Thue equations. These can be solved for example with the assistance of Magma [1]. In Section 5.1 we prove some lemmas involving the integral solutions of certain quartic equations and then prove our theorem in Section 5.2.

5.1 Relevant Lemmas

Lemma 5.1. *If c, d and m are integers with* $\gcd(c, d) = 1$ *and*

$$c^4 - 6c^2d^2 - 3d^4 = m$$

then $m \not\equiv 2, 3 (\mathrm{mod}\, 4)$ *and* $m \not\equiv 2 (\mathrm{mod}\, 3)$.

Proof. We can rearrange the given equation to obtain

$$(c^2 - 3d^2)^2 - 12d^4 = m$$

which yields the pair of congruences

$$(c^2 - 3d^2)^2 \equiv m (\mathrm{mod}\, 3)$$

and

$$(c^2 - 3d^2)^2 \equiv m (\mathrm{mod}\, 4).$$

The solvability of these congruences impose the conditions on m stated in this lemma. □

Lemma 5.2. *If c, d and m are integers with* $\gcd(c, d) = 1$ *and*

$$c^4 - 6c^2d^2 - 3d^4 = m$$

then either m is odd or $8 \parallel m$.

Proof. Suppose that m is even. Clearly c and d must both be odd. This forces m to be a multiple of 8. Rearranging the given equation gives

$$(c^2 - 3d^2)^2 - 12d^4 = m$$

If $16 \mid m$ then we deduce the congruence

$$(c^2 - 3d^2)^2 \equiv 12d^4 \equiv 12 (\mathrm{mod}\, 16)$$

which is insolvable, completing the proof. □

Lemma 5.3. *If c, d and m are integers with $\gcd(c, d) = 1$ then*

$$c^4 - 6c^2d^2 - 3d^4 = -24$$

is insolvable.

Proof. Solvability requires

$$4c^4 - 3(c^2 + d^2)^2 = -24.$$

Clearly this implies that $3 \mid c$ so that

$$-3(c^2 + d^2)^2 \equiv -24 (\mathrm{mod}\, 9).$$

This in turn implies that

$$(c^2 + d^2)^2 \equiv 2 (\mathrm{mod}\, 3)$$

which is impossible. □

Lemma 5.4. *If $m \in \{1, -3, -8, 24\}$ then the quartic equation $Y^2 = 12X^4 + m$ has the integral solutions given in the table below.*

Table 5.1: Values of m and corresponding solutions (X, Y) to $Y^2 = 12X^4 + m$

$m = 1$	$(X, Y) = (0, \pm 1)$
$m = -3$	$(X, Y) = (\pm 1, \pm 3)$
$m = -8$	$(X, Y) = (\pm 1, \pm 2)$
$m = 24$	$(X, Y) = (\pm 1, \pm 6)$

Proof. The elliptic curve $Y^2 = 12X^4 + 1$ has rank 0 so the given integral points are easy to determine. The three remaining curves have rank 1. At any rate all of them can be solved using the Magma command `IntegralQuarticPoints`. The solutions are as listed. □

5.2 Proof of Theorem

If we solve the first equation in (5.1) for B, substitute into the second equation in (5.1) and simplify we obtain

$$A^4 - 6(b^2 + 1)A^2 - 8A - 3(b^2 - 1)^2 = 0. \tag{5.2}$$

This polynomial equation defines an algebraic curve of genus 0. We give a parametrization over $\mathbb{Q}$ of the rational points on this curve. First suppose that $b = 0$. Then using (5.1) we obtain the values $A = -1, 3$, and once again using (5.1) we obtain the solutions

$$(A, B, b) = (3, 3, 0) \text{ and } (-1, -1, 0).$$

Now assuming that $b \neq 0$ we may choose a rational number r such that

$$A = br - 1.$$

Substituting this expression for A into (5.2) yields

$$b^3((r^4 - 6r^2 - 3)b - 4r(r^2 - 3)) = 0.$$

As $b \neq 0$ we may solve for b giving

$$b = \frac{4r(r^2 - 3)}{r^4 - 6r^2 - 3}. \tag{5.3}$$

Recalling that $A = br - 1$ we obtain

$$A = \frac{3(r^2 - 1)^2}{r^4 - 6r^2 - 3}. \tag{5.4}$$

Having obtained this parametric formula for A we derive a set of Thue equations in order to solve the original system. Choosing relatively prime integers c and $d \neq 0$ so that $r = c/d$ we substitute into (5.4) giving gives

$$A = \frac{3(c^2 - d^2)^2}{c^4 - 6c^2d^2 - 3d^4}. \tag{5.5}$$

For convenience we rewrite (5.5) as

$$A = \frac{3F^2}{G}, \tag{5.6}$$

where $F = (c^2 - d^2)$ and $G = c^4 - 6c^2d^2 - 3d^4$. From the two identities

$$G - (c^2 - 5d^2)F = -8d^4$$

and

$$G - (9c^2 + 3d^2)F = -8c^4$$

we deduce that $\gcd(F, G)$ is a divisor of 8. Thus the gcd of the numerator and denominator of (5.6) is a divisor of $2^6 \cdot 3$. It follows that in order for (5.6) to yield an integer value for A we must have

$$G \mid 3F^2$$

which is only possible if

$$G \mid 2^6 \cdot 3.$$

Thus we deduce that

$$c^4 - 6c^2d^2 - 3d^4 = m \text{ with } m = \pm 2^e 3^f,\ 0 \le e \le 6,\ 0 \le f \le 1. \qquad (5.7)$$

Now it remains to consider these 28 Thue equations given by (5.7). We can reduce the number of these equations as follows. By Lemma 5.1

$$m \neq -1, -2, 2, 3, -4, -6, 6, 8, -16, 32, -64,$$

and by Lemma 5.2 we further deduce that

$$m \neq 4, -12, 12, 16, -32, -48, 48, 64, -96, 96, -192, 192.$$

Lemma 5.3 shows that

$$m \neq -24$$

so that our list of admissible values of m is reduced to

$$m = 1, -3, -8, 24.$$

Completing the square in (5.7) yields

$$(c^2 - 3d^2)^2 = 12d^4 + m.$$

If $m = 1$ then Lemma 5.4 gives

$$\begin{aligned} d &= 0 \\ c^2 - 3d^2 &= \pm 1 \end{aligned}$$

which is impossible as $d \neq 0$.

If $m = -3$ then Lemma 5.4 gives

$$\begin{aligned} d &= \pm 1 \\ c^2 - 3d^2 &= \pm 3 \end{aligned}$$

which yields integral solutions $(c, d) = (0, \pm 1)$. Using $r = c/d = 0$, equations (5.3), (5.4) and (5.1) give us the solutions

$$(A, B, b) = (-1, 1, 0)$$

which was obtained already in the first part of this proof.

If $m = -8$ then Lemma 5.4 gives

$$\begin{aligned} d &= \pm 1 \\ c^2 - 3d^2 &= \pm 2 \end{aligned}$$

which yields the integral solutions $(c, d) = (\pm 1, \pm 1)$. Using $r = c/d = \pm 1$, equations (5.3), (5.4) and (5.1) give us the solutions

$$(A, B, b) = (0, -3, \pm 1).$$

If $m = 24$ then Lemma 5.4 gives

$$\begin{aligned} d &= \pm 1 \\ c^2 - 3d^2 &= \pm 6 \end{aligned}$$

which yields the integral solutions $(c, d) = (\pm 3, \pm 1)$. Using $r = c/d = \pm 3$, equations (5.3), (5.4) and (5.1) give us the solutions

$$(A, B, b) = (8, 17, \pm 3).$$

This completes the proof.

□

5.3 Another System

In his proof showing that ϵ is the fundamental unit of $\mathbb{Q}(\theta)$, Kaneko [15] considered cases where there exists a unit $\epsilon_0 (> 1)$ of $\mathbb{Q}(\theta)$ such that $\epsilon = \epsilon_0^n$ with some $n \in \mathbb{Z}, n > 1$. The above system was considered when $\epsilon = \epsilon_0^2$. As an exercise, we will now completely solve the system that was considered when $\epsilon = \epsilon_0^3$. Solving this system will produce two of the same b values as the previous system.

Theorem 5.2. *The Diophantine system*

$$\begin{aligned} A^3 - 3AB + 3 &= 3(b^2 + 1) \\ B^3 - 3AB + 3 &= 3(b^4 + b^2 + 1) \end{aligned}$$

has solutions $(A, B, b) = (0, 0, 0), (-3, 6, \pm 3)$ *and* $(3, 3, 0)$

Proof. Consider the Diophantine system

$$A^3 - 3AB + 3 = 3(b^2 + 1)$$
$$B^3 - 3AB + 3 = 3(b^4 + b^2 + 1).$$

Eliminating B from the two equations we get

$$A^9 - 9A^6b^2 - 54A^3b^4 + 27b^6 + 27A^6 = 0. \tag{5.8}$$

This is a curve of genus 4. We then make the substitution $b = \sqrt{c}$ where $c \in \mathbb{Z}$. This yields the new equation

$$A^9 - 9A^6c - 54A^3c^2 - 27c^3 - 27A^6 = 0. \tag{5.9}$$

This new equation (5.9) is now a genus 1 (elliptic) curve. Using the `Weierstrassform` command in Maple we yield the curve

$$x^3 - 109418989131512359209/4 + y^2 = 0. \tag{5.10}$$

Using the command `Rank` in Magma, we find that the rank of this curve is 0. This implies that the curve has finitely many solutions. From the birational mappings given by Maple between the curves (5.9) and (5.10) we have the relation

$$x = -\frac{1594323(7A^6 - 6A^5 - 18A^4 + 21cA^3 - 9cA^2 + 9c^2)}{A^4(A-3)^2}. \tag{5.11}$$

Looking at the denominator of (5.11) we see that possible solutions $A = 0$ and $A = 3$ may escape the solutions (x, y) of the curve (5.10). Substituting $A = 3$ and $A = 0$ into our curve and solving for B and b we get the solutions $(A, B, b) = (3, 3, 0)$ and $(A, B, b) = (0, 0, 0)$ respectively. We now perform some variable changes and scaling to the above Weierstrass cubic to convert it into the pure Weierstrass form. Solving for y^2, substituting $x = -x$ and factoring the integers we are now considering

$$y^2 = x^3 + \frac{3^{42}}{2^2}. \tag{5.12}$$

We now divide the equation by 3^{42} and substitute $x = 3^{14}x$ and $y = 3^{21}y$ and get

$$y^2 = x^3 + \frac{1}{4} \tag{5.13}$$

Now multiplying the equation by 4^3 and substituting $x = x/4$ and $y = y/8$ we get

$$y^2 = x^3 + 16. \tag{5.14}$$

We find that the torsion subgroup of this curve is isomorphic to $\mathbb{Z}_3$ and the rank is 0. By observation, we see that the curve has solutions $(x, y) = (0, \pm 4)$. These two solutions, plus the point at infinity, make up the necessary three points to satisfy the torsion subgroup. After back substituting the two solutions through all the scaling and variable changes, we yield the solutions $(A, B, b) = (-3, 6, \pm 3)$ and $(A, B, b) = (0, 0, 0)$. □

Chapter 6

The Factorization of $x^5 + ax^m + 1$

Let $f(x)$ be a polynomial with rational coefficients. The determination of those polynomials $f(x)$ with a specific form and a prescribed factorization often leads to interesting Diophantine problems. A general source of information on this type of problem is [22] where Schinzel classified many forms of reducible trinomials.

In a paper by Rabinowitz [20] the factorization of $x^5 \pm x + n$, for n an integer, into the product of an irreducible quadratic and an irreducible cubic over the rational numbers $\mathbb{Q}$ was studied and a finite number of polynomials was determined. The results of this paper are given in the folllowing theorems:

Theorem 6.1. *[20] The only integral n for which $x^5 + x + n$ factors into the product of an irreducible quadratic and an irreducible cubic are $n = \pm 1$ and $n = \pm 6$. The factorizations are*

$$x^5 + x \pm 1 = (x^2 \pm x + 1)(x^3 \mp x^2 \pm 1)$$
$$x^5 + x \pm 6 = (x^2 \pm x + 2)(x^3 \mp x^2 - x \pm 3).$$

Theorem 6.2. *[20] The only integral n for which $x^5 - x + n$ factors into the product of an irreducible quadratic and an irreducible cubic are $n = \pm 15, n = \pm 22,400,$ and $n = \pm 2,759,640$. The factorizations are*

$$x^5 - x \pm 15 = (x^2 \pm x + 3)(x^3 \mp x^2 - 2x \pm 5)$$
$$x^5 - x \pm 22400 = (x^2 \mp 12x + 55)(x^3 \pm 12x^2 + 89x \pm 408)$$
$$x^5 - x \pm 2759640 = (x^2 \pm 12x + 377)(x^3 \mp 12x^2 - 233x \pm 7320).$$

This type of result was extended by Spearman and Williams [24] to polynomials of the form $x^5 \pm x^m + n$, for $1 \leq m \leq 4$ and is outlined in the following theorems:

Theorem 6.3. *[24] The only integers n for which $x^5 + x^2 + n$ factors into the product of an irreducible quadratic and an irreducible cubic are $n = -90, -4, 18,$ and 11466.*

The only integers nn for which $x^5 - x^2 + n$ factors into the product of an irreducible quadratic and an irreducible cubic are $n = -11466, -18, 4,$ and 90.

Theorem 6.4. *[24] The only integers n for which $x^5 - x^3 + n$ factors into the product of an irreducible quadratic and an irreducible cubic are $n = \pm 8$.*

There are no integers n for which $x^5 + x^3 + n$ factors into the product of an irreducible quadratic and an irreducible cubic.

Theorem 6.5. *[24] The only integers n for which $x^5 \pm x^4 + n$ factors into the product of an irreducible quadratic and an irreducible cubic are $n = \pm 1$. In addition, every quintic of the form*

$$x^5 + \theta(-1)^k x^4 + \theta F_{k-1}^2 F_{k+1}^4 F_{k+2}^4$$

and

$$x^5 + \theta(-1)^k x^4 - \theta F_{k-1}^4 F_k^4 F_{k+2}^2$$

factors into the product of an irreducible quadratic and irreducible cubic where $\theta = \pm 1$, k is an integer with $k \geq 2$, and F_k is the k^{th} Fibonacci number.

The purpose of this chapter is to study in a similar manner to [20] and [24] the particular class of quintic polynomials $f(x)$ given by

$$f(x) = x^5 + ax^m + 1,$$

where a is a rational number and $1 \leq m \leq 4$. This factorization is an analogous problem whose solution is accessible thanks to recent powerful methods. We shall determine those rational values of a for which $f(x)$ is equal to the product of an irreducible quadratic and an irreducible cubic over $\mathbb{Q}$. In doing so, we take full advantage of a recent theoretical result of Stoll, described in Section 4.5, on rational points on certain genus 2 curves.

We also take advantage of the computer algebra system Magma [1]. We note that such a factorization for $f(x) = x^5 + ax^m + 1$ immediately yields a factorization for the polynomial $x^5 + ax^{5-m} + 1$, by using the reverse polynomial $x^5 f\left(1/x\right)$. We state all of the factorizations of $f(x)$ for m satisfying $1 \leq m \leq 4$, for completeness.

Finally, a factorization of $x^5 + ax^m + 1$ immediately yields a factorization for $x^5 + ax^m - 1$ if m is odd and $x^5 - ax^m - 1$ if m is even by scaling with

$x \to -x$. Therefore we only treat the case where the constant term of $f(x)$ is equal to positive 1.

Our new result is summarized in the following theorem.

Theorem 6.6. *Let $f(x) = x^5 + ax^m + 1$ where a is a rational number and m is an integer with $1 \leq m \leq 4$. Then $f(x)$ factors into the product of an irreducible quadratic and an irreducible cubic if and only if a and m assume the values listed in the following table. In each case the factorization is given.*

Table 6.1: The factorizations of the quintic trinomial $x^5 + ax^m + 1$ for corresponding values of a and m

(a, m)	factorization of $x^5 + ax^m + 1$
$(1, 1)$	$x^5 + x + 1 = (x^2 + x + 1)(x^3 - x^2 + 1)$
$(-11/4, 1)$	$x^5 - 11/4x + 1 = (x^2 + x - 1/2)(x^3 - x^2 + 3/2x - 2)$
$(1, 4)$	$x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 - x + 1)$
$(-11/4, 4)$	$x^5 - 11/4x^4 + 1 = (x^2 - 2x - 2)(x^3 - 3/4x^2 + 1/2x - 1/2)$

In Section 6.1 we give some preliminary results concerning rational points on specific genus 2 curves. In Section 6.2 we give the proof of our theorem.

6.1 Some Lemmas on Rational Points

In this section we give two lemmas which determine the set of rational points on two genus 2 curves. We refer the reader to Cassels and Flynn [6] as a reference for these types of algebraic curves. We will use a theorem of Stoll [25] which bounds the number of rational points on $\mathcal{C}_k : y^2 = x^5 + k$ where k is a tenth-power-free integer. These results are discussed in a paper by Bremner [3] as well.

This theorem of Stoll states that if the rank of the Jacobian of this curve is at most one then the number of rational points is bounded above by 7 (this bound is achieved only for $k = 324$). Assuming that $\mathcal{C}_k$ has no rational point of the form $(x, 0)$ for $k \neq 324$, the bound is 5. Magma will be used to determine the rank of the Jacobian for our curves using the command `RankBounds`. Finding the rank of the Jacobian is an extremely difficult and complicated problem to do by hand so we rely on computers to aid with the calculation.

Additionally we use the fact that if the Jacobian of a genus 2 curve has a rank of zero, then one can enumerate all points in the Jacobian and consequently find all rational points on $\mathcal{C}_k$. The Magma command that does this is `Chabauty0`. Now we analyze the rational points on two relevant genus 2 curves.

Lemma 6.1. *The only finite rational points on the genus 2 curve* $y^2 = x^5+4$ *are* $(0, \pm 2), (2, \pm 6)$.

Proof. We observe the four given points $(0, \pm 2), (2, \pm 6)$ on the curve. Magma confirms, using `RankBounds` that the rank of the Jacobian of this curve is equal to 1. Consequently the theorem of Stoll applies. The bound in this case, including the point at infinity, is 5 so that all of them are determined. □

Lemma 6.2. *The only finite rational points on the genus 2 curve* $y^2 = x^5 + 256$ *are* $(0, \pm 16)$.

Proof. The `RankBounds` command in Magma confirms that the rank of the Jacobian of the given curve is equal to 0. `Chabauty0` shows that the the finite points on this curve are indeed those listed in the statement of this lemma. □

6.2 Proof of Theorem

As mentioned in the introduction we need only treat the cases $m = 1, 2$. Suppose that $x^5 + ax + 1$ is divisible by a quadratic polynomial $x^2 + ux + v$ where $a, u, v \in \mathbb{Q}$. Division of these two polynomials leads to

$$\begin{aligned} x^5 + ax + 1 = (x^2 + ux + v)(x^3 - x^2u + (-v + u^2)x + 2uv - u^3) \\ +(v^2 - 3vu^2 + a + u^4)x + 1 + vu^3 - 2uv^2. \end{aligned} \quad (6.1)$$

In equation (1) we equate the coefficients of x and 1 in the remainder to zero yieldng the pair of equations

$$\begin{aligned} v^2 - 3vu^2 + a + u^4 = 0, \\ 1 + vu^3 - 2uv^2 = 0. \end{aligned} \quad (6.2)$$

The second equation in (6.2) shows that $u \neq 0$ and $v \neq 0$. Eliminating v from (6.2), using a resultant, produces the equation

$$-11u^5 + 1 + 4ua - u^{10} + 3u^6a + 4u^2a^2 = 0. \quad (6.3)$$

The discriminant of (6.3), viewed as quadratic equation in a is equal to

$$25u^7(8+u^5). \tag{6.4}$$

If (6.3) has a rational root a then (6.4) must be equal to a square in $\mathbb{Q}$, so that

$$25u^7(8+u^5) = w^2, \tag{6.5}$$

for some rational number w. Since $u \neq 0$, it follows from (6.5) that $\left(\frac{2}{u}, \frac{2w}{5u^6}\right)$ is a point on

$$y^2 = x^5 + 4. \tag{6.6}$$

From Lemma 6.1, we know that $x = 2$, so that $u = 1$. Substituting $u = 1$ into (6.3) and factoring gives

$$(4a+11)(a-1) = 0.$$

The two choices of $a = 1, a = -11/4$ produce the factorizations given in the table in the theorem.

In this case, suppose similarily to the first case, that $f(x) = x^5 + ax^2 + 1$ is divisible by a quadratic polynomial $x^2 + ux + v$ where $a, u, v \in \mathbb{Q}$. Division of these two polynomials leads to

$$\begin{aligned} x^5 + ax^2 + 1 = (x^2 + ux + v)(x^3 - ux^2 + (-v + u^2)x + a + 2uv - u^3) \\ + (v^2 - ua - 3vu^2 + u^4)x + 1 + vu^3 - 2uv^2 - va. \end{aligned} \tag{6.7}$$

In equation (6.7) we equate the coefficients of x and 1 in the remainder to zero yielding the pair of equations

$$\begin{aligned} v^2 - 3vu^2 - ua + u^4 = 0, \\ 1 + vu^3 - 2uv^2 - va = 0. \end{aligned} \tag{6.8}$$

If there exists a solution to this pair of equations with $u = 0$, then the first equation simplifies to

$$v^2 = 0$$

so that $v = 0$. It would then follow that the irreducible quadratic factor of $f(x)$ is $x^2 + ux + v = x^2$ which violates irreducibility of the quadratic factor. Then since $u \neq 0$, we may solve the first equation in (6.8) to give

$$a = \frac{u^4 + v^2 - 3u^2v}{u} \tag{6.9}$$

Substituting the value of a given in (6.9) into the second equation in (6.8) yields

$$\frac{u - v^3 + u^2v^2}{u} = 0$$

so that

$$u - v^3 + u^2v^2 = 0. \tag{6.10}$$

The existence of a rational solution u to (6.10) requires the discriminant of this quadratic in u to be equal to a square in $\mathbb{Q}$. That is

$$1 + 4v^5 = z^2 \tag{6.11}$$

for some rational number z. From (6.11) we see that $(x, y) = (4v, 16z)$ is a rational point on the genus 2 curve

$$y^2 = x^5 + 256. \tag{6.12}$$

Lemma 6.2 tells us that the only rational solution to (6.12) has $x = 0$ and since $x = 4v$ we must have $v = 0$. However this contradicts the assumption that $x^2 + ux + v$ is irreducible over $\mathbb{Q}$. Thus $f(x) = x^5 + ax^2 + 1$ cannot factor over $\mathbb{Q}$ as the product of an irreducible quadratic and an irreducible cubic.

□

Chapter 7

Conclusion and Future Work

7.1 Conclusion

The purpose of this thesis was to solve some Diophantine problems that required finding integral or rational points on algebraic curves of genus 0, 1, and 2.

We started in Chapters 2, 3, and 4 by outlining the methods used to find the points on these curves. We hope that interested readers could use this thesis as a guide to solving algebraic curves and that it would be layed out in a structured, easy to follow manner.

In Chapter 5, we solved a Diophantine system related to a problem on cubic fields based off a family of cubics of the form $x^3 - 3x - b^3$. We provided six solutions that yielded five different values of b for which a given formula was not the fundamental unit of the cubic field. Finding these solutions required adapting an algorithm to find integral points on genus 0 curves.

In Chapter 6, we then considered the factorization of a family of quintic trinomials $x^5 + ax^m + 1$. This problem took advantage of a recent result from Stoll [25] that bounded the number of rational points on a family of genus 2 curves. Without this result, the problem would most likely remain unsolved as we would not have been able to determine if a computer search yielded all of the points on the curve. We concluded that the family of quintic trinomials only factored for two different values of a and gave the factorizations.

As shown in this thesis, finding points on algebraic curves are necessary for solving different problems of varying topics of mathematics. An algebraic number theory problem on cubic fields and a polynomial theory problem on factorization are only a small fraction of problems that require finding solutions to algebraic curves. The difficulty of finding the points on these curves can range from following a simple algorithm to using complicated methods and nontrivial theory. However, the advancements of computers and theory are making the more difficult problems easier to solve.

These problems are extremely interesting and are becoming more prevalent in mathematics, which make them all the more desirable to research.

7.2 Future Work

Possible research that would extend past this thesis are:

1. Can rational points be found on curves of genus 3 or higher?

2. Can the idea of the Jacobian be extended to curves of genus 3 or higher?

3. Are there other unsolved problems that require finding rational points on genus 2 curves that could take advantage of recent results?

4. Let $f(x)$ be a polynomial with rational coefficient. We say that $f(x)$ is $\mathbb{Q}-$ derived if $f(x)$ and all of its derivatives have rational roots. An example of such a polynomial is

$$f(x) = x^2(x - 308)(x - 360).$$

An extended study of these polynomials is found in [5]. The current state and description of the research into these problems is given next.

Over the rational numbers $\mathbb{Q}$, these polynomials are almost completely classified with the notable exception of whether or not there exists a rational derived quartic with distinct roots. In each case of the classification, a parametrizing algebraic curve is produced, whose rational points yield the desired polynomials. A variety of algebraic curves is studied including curves of genus 0, 1 and 2. Over algebraic number fields, much less is known about derived polynomials. The above mentioned reference [5] considers some cases where the coefficients belong to quadratic fields. The paper [26] also considers the quadratic field case.

The main idea on this problem would be to concentrate on completing the quadratic case, with many separate classifications depending on suitable algebraic curves. For example even treating the polynomial

$$g(x) = x^2(x - 1)^2(x - a)$$

and trying to determine the rational numbers a for which $g(x)$ is $k-$ derived for some quadratic field k requires the study of the rational points on the genus 2 curve

$$y^2 = x^6 - 75x^4 + 600x^2 + 50000.$$

This is a difficult problem by itself. Returning to the rational derived quartic for a moment, introductory calculations show that it

may be possible to reduce its solution to an infinite family of genus 2 curves. If any of these curves have a rational point, the problem will be solved in the affirmative.

Bibliography

[1] W. Bosma, J. Cannon, and C. Playoust, *The Magma Algebra System I: The User Language*, J. Symbolic Comput. **24** (1997), 235-265.

[2] B. Buchberger, G.E. Collins, and R. Loos, eds. *Computer Algebra: Symbolic & Algebraic Computation*. New York. Springer-Verlag, 1982

[3] A. Bremner, *On the equation* $Y^2 = X^5 + k$, Exp. Math. **17:3** (2008), 371-374.

[4] N. Bruin, *Chabauty methods using elliptic curves*, J. reine angew. Math. **562** (2003), 27-49.

[5] R. Buchholz and J. MacDougall, *When Newton met Diophantus: a study of rational-derived polynomials and their extension to quadratic fields*, J. Number Theory **81:2** (2000), 210–233.

[6] J. W. S. Cassels and E. V. Flynn, *Prolegomena To A Middlebrow Arithmetic of Curves of Genus 2*, Cambridge University Press, 1996.

[7] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882-885 (French).

[8] R. Chapman. *Algebraic Number Theory - Summary of Notes*, Home page. U. of Exeter. 3 May. 2000 <http://empslocal.ex.ac.uk/people/staff/rjchapma/courses/ant99/notes5.dvi>.

[9] H. Cohen. *A Course in Computational Algebraic Number Theory*, Springer–Verlag, Germany, 1993.

[10] J. B. Fraleigh, *A First Course in Abstract Algebra*, Addison Wesley, Boston, 2003.

[11] T. Freiberg, *An Outline of the Flynn-Chabauty Method for Curves of Genus 2 with an Application to the Curve* $\mathcal{C} : y^2 = x^5 - 2x$, Master's Thesis, University of Queensland, 2006.

[12] M. van Hoeij, *Computing Parametrizations of Rational Algebraic Curves*, Conf. ISSAC94, July 2022, 1994, Oxford, 1994.

[13] M. van Hoeij, *Rational parametrizations of algebraic curves using a canonical divisor*, J. Symbolic Comput. **23** (1997), 209-227.

[14] M. van Hoeij, *An algorithm for computing the Weierstrass normal form*, ISSAC'95 Proceedings, p. 90-95 (1995).

[15] K. Kaneko, *Integral bases and fundamental units of certain cubic number fields*, SUT J. Math. **39:2** (2003), 117-124.

[16] P. D. Lee and B. K. Spearman, *A Diophantine system and a problem on cubic fields*, International Mathematical Forum **6:3** (2011), 141-146.

[17] P. D. Lee and B. K. Spearman, *The Factorization of* $x^5 + ax^m + 1$, Scientiae Mathematicae Japonicae **73:2-3** (2011), 171-174: e-2011, 77-80.

[18] D. Poulakis and E. Voskos, *On the practical solution of genus zero Diophantine equations*, J. Symbolic Comput. **30** (2000), 573-582.

[19] D. Poulakis and E. Voskos, *Solving genus zero Diophantine equations with at most two infinite valuations*, J. Symbolic Comput. **33** (2002), 479-491.

[20] S. Rabinowitz, *The factorization of* $x^5 \pm x + n$, Math. Mag. **61** (1988), 191-193.

[21] K. H. Rosen, *Elementary Number Theory and its Applications*, Addison Wesley, Boston, 2005.

[22] A. Schinzel, *On reducible trinomials*, Dissertationes Math. (Rozprawy Mat.) **329** (1993), 1-83.

[23] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer, New York, 1992.

[24] B. K. Spearman and K. S. Williams, *The factorization of* $x^5 \pm x^a + n$, Fibonacci Quart. **36** (1998), 158-170.

[25] M. Stoll, *On the number of rational squares at fixed distance from a fifth power*, Acta Arith. **125:1** (2006), 79-88.

[26] R.J. Stroeker, *On* $\mathbb{Q}-$ *derived polynomials*, Rocky Mountain J. Math. **36:5** (2006), 1705-1713.

[27] A. Thue, *ber Annherungswerte algebraischer Zahlen*, Journal für die reine und angewandte Mathematik **135** (1909), 284-305.

[28] N. Tzanakis and B. M. M. De Weger, *On the practical solution of the Thue equation*, J. Number Theory **31** (1989), 99-132.

[29] ————. *Algebraic Curve*. Wikipedia. 4 September. 2010. <http://en.wikipedia.org/wiki/Algebraic_curve>.

Appendix A

Magma Code

This appendix includes relevant Magma code for chapters 4, 5 and 6.

A.1 Chapter 4 Magma Code

A.1.1 Example 4.3

```
P<x>:=PolynomialRing(Rationals());
C:=HyperellipticCurve(x^6+4);
C;
```

Hyperelliptic Curve defined by y^2 = x^6 + 4 over Rational Field

```
Points(C:Bound:=1000);
```

{@ (1 : -1 : 0), (1 : 1 : 0), (0 : -2 : 1), (0 : 2 : 1) @}

```
J:=Jacobian(C);
RankBounds(J);
```

0 , 0 \\ gives both a lower and upper bound of 0

```
Chabauty0(J);
```

{@ (1 : -1 : 0), (1 : 1 : 0), (0 : -2 : 1), (0 : 2 : 1) @}

A.1.2 Example 4.4

```
P<x>:=PolynomialRing(Rationals());
C:=HyperellipticCurve(x^6+x^2+2;
C;
```

Hyperelliptic Curve defined by y^2 = x^6+x^2 + 2 over Rational Field

```
ptsC:=Points(C:Bound:=1000); ptsC;
```

{@ (1 : -1 : 0), (1 : 1 : 0), (-1 : -2 : 1), (-1 : 2 : 1), (1 : -2 : 1), (1 : 2 : 1) @}

```
J:=Jacobian(C);
RankBounds(J);
```

1 , 1 \\ gives both a lower and upper bound of 1

```
PT1:=J![ptsC[3], ptsC[1]];                \\ The point {(-1,-2), ∞⁻}
Order(PT1);
```

8

```
PT2:=J![ptsC[5], ptsC[1]];                \\ The point {(1,-2), ∞⁻}
Order(PT2);
```

no output \\ therefore, PT2 has infinite order

```
Chabauty(PT2);
```

{ (1 : -2 : 1), (-1 : -2 : 1), (1 : 2 : 1), (1 : -1 : 0), (1 : 1 : 0), (-1 : 2 : 1) }

A.2 Chapter 5 Magma Code

A.2.1 Lemma 5.4

```
IntegralQuarticPoints([12,0,0,0,1]);
```

[[0, 1]]

```
IntegralQuarticPoints([12,0,0,0,-3]);
```

[[1,3] [-1,3]]

```
IntegralQuarticPoints([12,0,0,0,-8]);
```

[[1,2] [-1,2]]

```
IntegralQuarticPoints([12,0,0,0,24]);
```

[[1,6] [-1,6]]

A.2.2 Proof of Theorem 5.2

```
P<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([0,109418989131512359209/4]);
E;
```

Elliptic Curve defined by y^2 = x^3 + 109418989131512359209/4
over Rational Field

```
Rank(E);
```

0

A.3 Chapter 6 Magma Code

A.3.1 Lemma 6.1

```
P<x>:=PolynomialRing(Rationals());
C:=HyperellipticCurve(x^5+4);
C;
```

Hyperelliptic Curve defined by y^2 = x^5 + 4 over Rational Field

```
RationalPoints(C:Bound:=1000);
```

{@ (1 : 0 : 0), (0 : -2 : 1), (0 : 2 : 1), (2 : -6 : 1), (2 : 6 : 1) @}

```
J:=Jacobian(C);
RankBounds(J);
```

1 , 1 \\ gives both a lower and upper bound of 1

A.3.2 Lemma 6.2

```
P<x>:=PolynomialRing(Rationals());
C:=HyperellipticCurve(x^5+256);
C;
```

Hyperelliptic Curve defined by y^2 = x^5 + 256 over Rational Field

```
RationalPoints(C:Bound:=1000);
```

{@ (1 : 0 : 0), (0 : -16 : 1), (0 : 16 : 1) @}

```
J:=Jacobian(C);
RankBounds(J);
```

```
                0 , 0          \\ gives both a lower and upper bound of 0
Chabauty0(J);
                {@ (1 : 0 : 0), (0 : -16 : 1), (0 : 16 : 1) @}
```