Explicit Computation
on Elliptic Curves

Lucas Rufino Martelotte
Instituto de Matemática Pura e Aplicada

April 2025

Acknowledgments

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001. I would also like to thank Hossein, Jeanine, Olivier and Yunes for all the helpful feedback during the production of this dissertation, as well as Alex, Carlos, Fred, Thales and many more that listened to my talks on the subject.

Contents

Chapter 1

Introduction

Number theory is one of the oldest branches of mathematics. A major problem in number theory is the study of Diophantine equations, specifically integer solutions to polynomial equations with integer coefficients. These equations are notorious for being difficult to analyze. A famous example is

$$x^n + y^n = z^n, \tag{1.1}$$

which was claimed in 1637 by Fermat to have no non-trivial solutions (i.e. solutions where none of the variables are zero) when $n \geq 3$. Despite its apparent simplicity, the claim was only proved more than 300 years later by Andrew Wiles. It turns out that analyzing the (possibly) larger set of *rational* solutions often tends to be more manageable. As an example, let's investigate for which types of polynomial equations we can find all rational solutions.

When solving a one-variable equation

$$f(x) = \alpha_n x^n + ... + \alpha_1 x + \alpha_0 = 0, \quad \alpha_n, \alpha_0 \neq 0, \tag{1.2}$$

in the rationals, it is not difficult to convince oneself that for any solution $a/b \in \mathbb{Q}$, it must be that a divides α_0 and b divides α_n. This reduces the search for rational solutions to a finite number of cases. So this case is completely solved.

The next layer of complexity is that of two-variable polynomial equations $f(x, y) = 0$, with $f(x, y) \in \mathbb{Z}[x, y]$. For degree one polynomials, the equation $f(x, y) = 0$ describes a line L. We can then parametrize it by $t \mapsto vt + w$, where $v, w \in \mathbb{Q}$. And this induces a bijection of sets $\mathbb{Q} \cong \{\text{rational points on } L\}$. So this case is simple.

Next, lets assume $f(x, y)$ has degree two and $C = \{(x, y) \in \mathbb{C}^2 \ : \ f(x, y) = 0\}$ is a smooth curve. There are two possibilities for the set $C(\mathbb{Q})$ of rational points on C. First of all, it may be empty, as in the case of $x^2 + y^2 + 1 = 0$, which has no real solutions, or $x^2 + y^2 - 3 = 0$, which has real solutions but no rational solutions. Using the Hasse-Minkowski Theorem [6, Chapter 6], which is a deep result in modern number theory, it is possible to construct an algorithm for determining if $C(\mathbb{Q})$ is empty or not. If it is not empty, there are methods for finding a single rational point $q \in C(\mathbb{Q})$ in reasonable time [9, 39]. Given such a point, a classic construction in algebraic geometry allows one to get all other rational points simply by tracing lines passing through q (see [36, Chapter 1] for examples of this). The conclusion is that $C(\mathbb{Q})$ is either empty or infinite, and in the latter case there is an algorithm for constructing all the rational points. For a non-smooth curve C, it can be shown by elementary methods that it consists of either a single point or the union of two lines, and both can be distinguished algorithmically. Either of the two cases is easier to handle than the smooth case, so this completes the analysis of two-variable quadratic equations.

Notice that the mere jump from degree 1 to degree 2 introduced a large amount of complexity and case-checking. The general method for finding all rational solutions relies on the Hasse-Minkowski Theorem, which is an advanced result proved only in the twentieth century. The jump from degree 2 to degree 3 is even worse. While degree 1 is easy and degree 2 is hard, it turns out that, as of right now, degree 3 is impossible. More concretely, there is no known method for finding all rational solutions of a cubic equation, or even deciding if there are finitely or infinitely many solutions. In a sense, this poses degree 3 equations as the next big step in understanding rational solutions to polynomial equations.

Let $f(x, y)$ be a degree 3 polynomial and $E := \{(x, y) \in \mathbb{C}^2 \ : \ f(x, y) = 0\}$. If E is a singular curve, it is indeed possible to find all rational points, using a method analogous to the one for degree 2 equations. If E is a smooth curve, then E is what is called an *elliptic curve.* The remarkable property of elliptic curves, which does not occur in any other degree, is that the set of rational points $E(\mathbb{Q})$ (together with an additional "point at infinity" $\mathcal{O}$) forms an abelian group.

Before trying to explicitly construct $E(\mathbb{Q})$ as a set, it is a good idea to understand $E(\mathbb{Q})$ as a group. It turns out that this group has a rich structure and many connections to problems in number theory. For example, the congruence number problem [41] is equivalent to finding a point of infinite order in $E(\mathbb{Q})$ for some elliptic curve. Moreover, $E(\mathbb{Q})$ is the subject of the Modularity Theorem (previously called the Shimura-Taniyama conjecture), of which a particular case was shown by Wiles in order to prove Fermat's Last Theorem. The group $E(\mathbb{Q})$ also gave birth to many open problems. For instance, it is not known exactly which groups can occur as $E(\mathbb{Q})$ for an arbitrary elliptic curve, or if there is an upper bound to the number of independent points in $E(\mathbb{Q})$. Lastly, and more important to our purposes in this work, $E(\mathbb{Q})$ is related to the famous Birch and Swinnerton-Dyer conjecture (or BSD Conjecture), which is one of the seven Millenium Problems.

First posed by Birch and Swinnerton-Dyer in a paper in 1965 [4] after a series of computer calculations, the BSD Conjecture, if proved, would shed light into the structure of $E(\mathbb{Q})$ and connect it to the elusive world of $L-$fuctions. It is a beautiful conjecture with deep consequences for number theory, however much theoretical background is needed before one can even state it precisely. In rough terms, the conjecture states that

$$\mathrm{ord}_{s=1} L(E, s) = r_E,$$

where $L(E, s)$ is a holomorphic function associated to E, called the $L-$function of E, and r_E is the rank of the group $E(\mathbb{Q})$ (which, as we'll see later, is always finitely generated).

The goal of this work is to develop the necessary background to better understand this statement. This will be done in a mostly self-contained way. The only requirements are a basic understanding of group theory, number theory, complex analysis, and algebraic geometry (essentially knowing how to navigate between affine charts). We also use some basic algebraic number theory, but all results are either proven or, at least, stated beforehand. The contents are devised as follows.

(Section 2) Here we provide the background knowledge necessary to understand the rest of the work. The reader is encouraged to skip this section if they are already familiar with these topics, otherwise to read them as they become needed.

(Section 3) A short introduction to elliptic curves and their basic properties is given. We also introduce the notion of an $L-$function attached to an elliptic curve, which is crucial to understanding the BSD Conjecture.

(Section 4) We give a proof of the Mordell-Weil Theorem, a fundamental result about elliptic curves which says $E(\mathbb{Q})$ is a finitely generated group (and thus isomorphic to $\mathbb{Z}^r \oplus T$, where T is a finite group). The number r is called the *rank* of the elliptic curve and is at the core of many conjectures in the area. We also give an algorithm to find reasonable lower and upper bounds for r.

(Section 5) We give a proof of the Nagell-Lutz Theorem, which gives an algorithm for computing the finite group T. We will also show a nice computer visualization based on this Theorem which allows one to easily find some infinite families of elliptic curves with a fixed group $T \subseteq E(\mathbb{Q})$.

(Section 6) We introduce the BSD Conjecture and state it precisely. After, we explain the algorithm Birch and Swinnerton-Dyer used to compute some invariants of an elliptic curve which led to the development of the conjecture. We also provide a pseudo-code, as well as a table reproducing some of the results in the original paper.

Chapter 2

Preliminaries

The purpose of this chapter is to quickly present the necessary background to understand the main proofs of this work. Most of these results are used only in Chapter 6, where calculations by Birch and Swinnerton-Dyer [4], which led to the famous BSD Conjecture, are explained. Much of the notation used throughout the chapters will be fixed here. Proofs will be presented whenever results are not well-known or when a sufficiently simple argument is available. Regardless, references will be provided for each topic for further study.

Section 2.1 showcases some basic results about Gaussian integers and briefly discusses the Gaussian zeta function $\zeta_{\mathbb{Z}[i]}(s)$. Section 2.2 defines the well-known Legendre symbol and its order 4 relative, the quartic symbol. The laws of quadratic and quartic reciprocity are also stated [23]. Section 2.3 presents the fundamental results about finite fields. It also discusses important properties of Gauss and Jacobi sums [16, 22, 18], which are useful tools for counting the number of solutions to polynomial equations over finite fields. Lastly, Section 2.4 develops the necessary background to understand the main results of algebraic number theory, namely the finiteness of the class number and the finite generation of the group of units of a ring of integers, and also Theorem 2.4.32, which will be important later on. It also briefly discusses Dedekind zeta functions and valuations.

2.1 The ring of Gaussian integers

First, we set up some notation.

Notation 2.1.1. The term integer (resp. prime) *always* denotes a number (resp. prime) in $\mathbb{Z}$. A gaussian prime, or a $\mathbb{Z}[i]-$prime, will denote a prime number in $\mathbb{Z}[i]$. Given $a, b, p \in \mathbb{Z}[i]$, the expression $a \overset{p}{\cong} b$ is equivalent to $a = b$ in $\mathbb{Z}[i]/(p)$. The value of a in $\mathbb{Z}[i]/(p)$ is said to be the *Gaussian residue* of a modulo p. Similarly, given $a, b, p \in \mathbb{Z}$, the expression $a \overset{p}{\equiv} b$ is equivalent to $a = b$ in $\mathbb{Z}/(p)$. The value of a in $\mathbb{Z}/(p)$ is said to be the *residue* of a modulo p. We define $\mathbb{N}a := a\overline{a}$, i.e. the standard norm in $\mathbb{Z}[i]$. We say a is odd if $\mathbb{N}a$ is odd, otherwise we say a is even. We say $a \sim b$ if $a = i^k b$ for some integer k. Lastly, we say a is *primary* if $a \overset{2+2i}{\cong} 1$;

The notion of a "primary" number serves as a way to unambiguously choose a generator of an ideal $(z) \subseteq \mathbb{Z}[i]$ when z is odd. Below are some properties about primary numbers.

Proposition 2.1.2 (Properties of primary)**.** The following hold.

1. Any odd Gaussian integer is associated with a unique primary;
2. $a \in \mathbb{Z}[i]$ is primary if and only if $a \overset{4}{\cong} 1$ or $3 + 2i$. Thus, the primary integers are exactly those of the form $4n + 1$.

The primes in $\mathbb{Z}[i]$ are classified as follows.

Proposition 2.1.3 (Primes in $\mathbb{Z}[i]$)**.** A Gaussian integer π is a Gaussian prime if and only if there is some integer k such that one of the following holds.

1. $\pi \sim 1 + i$ (this is the only even Gaussian prime);
2. $\pi \sim 4k + 3$ is a prime;
3. $\pi\overline{\pi} = 4k + 1$ is a prime.

$\mathbb{Z}$	2	3	5	7	11	13	17	19	23	29	31	37	41
$\mathbb{Z}[i]$	$1+i$	3	$2+i$	7	11	$3+2i$	$4+i$	19	23	$5+2i$	31	$6+i$	$5+4i$
	$1-i$		$2-i$			$3-2i$	$4-i$			$5-2i$		$6-i$	$5-4i$

Table 2.1: Splitting of the first few primes in $\mathbb{Z}[i]$

Table 2.1 shows how primes in $\mathbb{Z}[i]$ relate to primes in $\mathbb{Z}$. Given a Gaussian prime π, we know that (π) is a prime ideal, and thus a maximal ideal (since $\mathbb{Z}[i]$ is a PID). So $\mathbb{Z}[i]/(\pi)$ is a finite field. Since finite fields are determined by their cardinality, the next results classify the possible prime quotients in $\mathbb{Z}[i]$.

Lemma 2.1.4. Let $n \in \mathbb{Z}$. Then, $|\mathbb{Z}[i]/(n)| = n^2$.

Proof. It is clear that two elements $a_1 + ib_1$ and $a_2 + ib_2$ are equivalent in this quotient if and only if $a_1 \overset{n}{\equiv} a_2$ and $b_2 \overset{n}{\equiv} b_2$. Therefore, $(\mathbb{Z}[i]/(n), +) \cong \mathbb{Z}_n^2$ and thus has size n^2. □

Proposition 2.1.5. Given a Gaussian prime π, we have $|\mathbb{Z}[i]/(\pi)| = \mathbb{N}\pi$.

Proof. If $\pi = 1 + i$ this can be readily checked by hand. Suppose π is odd. If $\pi = 4k + 3$ for some $k \in \mathbb{Z}$ the result follows by Lemma 2.1.4. Suppose then $\pi\overline{\pi} = 4k + 1 =: p$ is a prime number. Then $(p) \subsetneq (\pi)$, so there is a surjection $\mathbb{Z}[i]/(p) \twoheadrightarrow \mathbb{Z}[i]/(\pi)$ and thus $|\mathbb{Z}[i]/(\pi)|$ is a proper divisor ($\neq 1$) of $|\mathbb{Z}[i]/(p)| = p^2$ (by Lemma 2.1.4). So it must be $p = \mathbb{N}\pi$. □

Remark 2.1.6. Given a prime number $p = 4k + 3$, it follows from Proposition 2.1.3 that p is also a Gaussian prime. And so by Proposition 2.1.5, $\mathbb{Z}[i]/(p) = \mathbb{F}_{\mathbb{N}p} = \mathbb{F}_{p^2}$. So, for example,

$$\mathbb{F}_9 \cong \{0, 1, i, -1, -i, 1 + i, 1 - i, -1 - i, -1 + i\}$$

with the usual addition and multiplication taken in $\mathbb{Z}[i]/(3)$. This gives a quick way of representing some finite fields.

2.2 Quadratic and Quartic Reciprocity

One of the oldest problems in number theory is the study of polynomial equations over the integers modulo p, where p is some prime number. The simplest example is $x^n \overset{p}{\equiv} a$, for an integer a and $n \geq 1$. A solution to such an equation is called a nth-power residue. The study of power residues dates back to the 17th century with letters by Pierre de Fermat. In 1798 Legendre introduced the famous Legendre symbol while studying quadratic (or 2nd-power) residues.

Definition 2.2.1 (Legendre Symbol)**.** Given an odd prime number p and an integer a coprime to p, the Legendre symbol is defined as

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } x^2 \equiv a \mod p \text{ admits a solution,} \\ -1 & \text{otherwise.} \end{cases}$$

Notice that $\left(\frac{a}{p}\right)$ only depends on the value of $a \mod p$. In 1748 Euler had already proven what is now called Euler's criterion.

Proposition 2.2.2. [Euler's criterion] $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$.

This shows the Legendre symbol is multiplicative in the first input (i.e. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$). The law of quadratic reciprocity is stated as follows.

Theorem 2.2.3. [Quadratic Reciprocity Law] Let p, q be different odd primes. Then,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}, \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Often the law is considered to be only the first equation, and the other two are called supplementary laws. To this day the quadratic reciprocity law is considered to be one of the most important results in number theory. Although Legendre was the first to publish a proof attempt, the argument was wrong. As stated by Cox [8]: "some of the cases are proved rigorously, some depend on Dirichlet's theorem on primes in arithmetic progressions and some are a tangle of circular reasoning." It was Gauss, in 1796, who first provided a correct proof. Nowadays there are hundreds of proofs using a variety of different mathematical tools [10, 23, 34].

Remark 2.2.4. Combining quadratic reciprocity with Euler's Criterion we can quickly compute the Legendre symbol even when large numbers are involved. For example, by factoring 42 as $2 \cdot 3 \cdot 7$ we have

$$\left(\frac{-42}{101}\right) = \left(\frac{-1}{101}\right)\left(\frac{2}{101}\right)\left(\frac{3}{101}\right)\left(\frac{7}{101}\right) = -\left(\frac{101}{3}\right)\left(\frac{101}{7}\right) = -\left(\frac{2}{3}\right)\left(\frac{3}{7}\right) = -1.$$

The second inequality used the entirety of the quadratic reciprocity law. In two steps, we reduced the calculation to Legendre symbols involving only single-digit numbers.

When it comes to higher power residues, there are different ways of generalizing the previous ideas. For 2^kth-power residues, namely equations of the form $x^{2^k} \overset{p}{\equiv} a$, it is not hard to derive the analog of Euler's criterion (see Proposition 7.1.2 in the Appendix), provided one knows some fundamental results about finite fields. For different powers, things get a little trickier. Moreover, it is not clear if there are analogs of the law of quadratic reciprocity. It was Gauss who first noticed that the natural domains for such power residues were not the integers, but an "infinite enlargement" of them. (For more information on power residue and reciprocity theories see [23].) In the case of quartic (also called 4th-power, or biquadratic) residues, that ring is $\mathbb{Z}[i]$. In Gauss words: "the theorems on biquadratic residues gleam with the greatest simplicity and genuine beauty only when the field of arithmetic is extended to imaginary numbers, so that without restriction, the numbers of the form $a + bi$ constitute the object of study (...) we call such numbers integral complex numbers." The quartic symbol is defined as follows.

Definition 2.2.5 (Quartic symbol)**.** Given an odd Gaussian prime p and a Gaussian integer a coprime to p, the quartic symbol is defined as

$$\left[\frac{a}{p}\right] := i^k, \quad \text{where } i^k \overset{p}{\cong} a^{\frac{\mathbb{N}p-1}{4}}.$$

At first glance, it is not clear whether or not this is well-defined. First, why is $\mathbb{N}p - 1$ divisible by four? By Proposition 2.1.3, primes $p \in \mathbb{Z}[i]$ are either of the form $p = 4k+3$, in which case $\mathbb{N}p - 1 = 16k^2 + 24k + 8$, or satisfy $p\overline{p} = \mathbb{N}p = 4k+1$. The second issue is why is $a^{(\mathbb{N}p-1)/4}$ always congruent to a power of i. By Proposition 2.1.5, the cardinality of $\mathbb{Z}[i]/(p)$ is $\mathbb{N}p$, and thus by Fermat's Little Theorem $a^{\mathbb{N}p-1} \overset{p}{\cong} 1$. But then $a^{(\mathbb{N}p-1)/4}$ must be a root of the polynomial $x^4 - 1$, i.e., a power of i. From there, it is not difficult to show that $x^4 \overset{p}{\cong} a$ admits a solution if and only if $\left[\frac{a}{p}\right] = 1$.

Notice that $\overline{\left[\frac{a}{p}\right]} = \left[\frac{\overline{a}}{\overline{p}}\right]$. Also, similar to the Legendre symbol, the quartic symbol is multiplicative in the first input and depends only on the Gaussian class of a modulo p. We'll often extend it to also be multiplicative in the second input (i.e., given two odd Gaussian primes p, q, we have $\left[\frac{a}{pq}\right] = \left[\frac{a}{p}\right]\left[\frac{a}{q}\right]$) and set $\left[\frac{a}{p}\right] = 0$ when a and p are not coprime. The following proposition shows that, for a prime p, $\left[\frac{\cdot}{p}\right]$ is not interesting when viewed as a function in $\mathbb{Z}_p$.

Proposition 2.2.6. Let $a, b \in \mathbb{Z}$ with b primary prime, then $\left[\frac{a}{b}\right] = 1$.

Proof. If $b \overset{4}{\equiv} 1$, then it decomposes as $b = \pi\overline{\pi}$. Then, $\left[\frac{a}{b}\right] = \left[\frac{a}{\pi}\right]\left[\frac{a}{\overline{\pi}}\right] = \left[\frac{a}{\pi}\right]\overline{\left[\frac{a}{\pi}\right]} = 1$. If $b \overset{4}{\equiv} 3$, then b is a Gaussian prime and we have

$$a^{\frac{b^2-1}{4}} = a^{\frac{b-1}{2}\frac{b+1}{2}} \overset{b}{\equiv} (\pm 1)^{\frac{b+1}{2}} = 1.$$

Here we used Euler's criterion and the fact that $(b+1)/2$ is even. Then, by the definition of quartic symbol, $\left[\frac{a}{b}\right] \overset{b}{\cong} a^{(b^2-1)/4} \overset{b}{\equiv} 1$. This concludes the proof. □

Theorem 2.2.7 (Quartic Reciprocity Law)**.** Let $\alpha = a + bi$ and β be primary and coprime Gaussian integers. Then,

$$\left[\frac{\alpha}{\beta}\right] = (-1)^{(\mathbb{N}\alpha-1)/4}(-1)^{(\mathbb{N}\beta-1)/4}\left[\frac{\beta}{\alpha}\right],$$

$$\left[\frac{i}{\alpha}\right] = i^{(1-a)/2}, \quad \left[\frac{1+i}{\alpha}\right] = i^{(a-b-b^2-1)/4}, \quad \left[\frac{2}{\alpha}\right] = i^{-b/2}.$$

Remark 2.2.8. We can now perform quick calculations with the quartic symbol, similar to what was done in Remark 2.2.4. For example,

$$\left[\frac{17-5i}{1-4i}\right] = \left[\frac{-1-i}{1-4i}\right] = \left[\frac{i}{1-4i}\right]^2\left[\frac{1+i}{1-4i}\right] = i.$$

In the first equality we reduced $17 - 5i$ modulo $1 - 4i$. After, we used the fact that $[\frac{\cdot}{p}]$ is multiplicative. Lastly we used the supplementary quartic reciprocity laws.

Proposition 2.2.9. Let a, b be primary. Let $\gamma = -1$ if $a, b \overset{4}{\cong} 3 + 2i$, and $\gamma = 1$ otherwise. Then,

$$\left[\frac{a}{b}\right] = \gamma\left[\frac{b}{a}\right].$$

Proof. By the law of quartic reciprocity, we have $\gamma = (-1)^{\frac{\mathbb{N}a-1}{4}\frac{\mathbb{N}b-1}{4}}$. Suppose for instance that $a \overset{4}{\cong} 1$, then $(\mathbb{N}a - 1)/4$ is even and thus $\gamma = 1$. If both $a, b \overset{4}{\cong} 3 + 2i$, then both $(\mathbb{N}a - 1)/4$ and $(\mathbb{N}b - 1)/4$ are odd and thus $\gamma = -1$. □

Corollary 2.2.10. Let a, b be primary. If either a or b is an integer then $[\frac{a}{b}] = [\frac{b}{a}]$.

Proof. By Proposition 2.1.2, either $a \overset{4}{\equiv} 1$ or $b \overset{4}{\equiv} 1$. The result then follows from Proposition 2.2.9. □

Proposition 2.2.11. If $a \sim (1+i)^r$ and b is primary, then

1. $\left[\frac{a}{b}\right]$ depends only on the Gaussian residue of b modulo 16;
2. if $a \in \mathbb{Z}$, then $a = \pm 2^{r/2}$ and $\left[\frac{a}{b}\right]$ depends only on the Gaussian residue of b modulo 8;
3. if $a = \pm 1$, then $\left[\frac{a}{b}\right]$ depends only on the Gaussian residue of b modulo 4.

Proof. Throughout the proof let $b = c+di$. (1) Let $a = i^l(1+i)^r$. We use the law of quartic reciprocity to get

$$\left[\frac{a}{b}\right] = \left[\frac{i}{b}\right]^l \left[\frac{1+i}{b}\right]^r = i^{(1-c)l/2} i^{(c-d-d^2-1)r/4},$$

which clearly depends only on the gaussian class of b mod 16. (2) Now suppose $a \in \mathbb{Z}$. Then, $a = (-1)^l 2^h$ with $2h = r$. We use quartic reciprocity again.

$$\left[\frac{a}{b}\right] = \left[\frac{-1}{b}\right]^l \left[\frac{2}{b}\right]^h = \left[\frac{i}{b}\right]^{2l} \left[\frac{2}{b}\right]^h = i^{(1-c)l} i^{-dh/2},$$

which depends only on the Gaussian class of b mod 8. Lastly, if $a = (-1)^l$ then $\left[\frac{a}{b}\right] = \left[\frac{i}{b}\right]^{2l} = i^{(1-c)l}$ which depends only on the Gaussian class of b mod 4. □

2.3 Characters of Finite Fields

In the previous section we've seen equations of the kind $x^n \overset{p}{\equiv} a$. There are two ways of generalizing this type of equation: (1) we can consider bigger fields (i.e. $\mathbb{F}_{p^r}$ for $r > 1$); (2) we can consider different types of polynomial equations. The first case is closely related to the notion of a multiplicative character. The second case is quite hard to analyze in general, however, particularly nice-behaved polynomial equations, namely those in what is called a "diagonal form", can be analyzed with Gauss and Jacobi sums [22, 16, 18]. These tools are the topic of this section. First, we set some notation and recall some classic results about finite fields.

Notation 2.3.1. From now on, p will always denote a prime number and q will always denote a power of p. $\mathbb{F}_q$ is the only finite field of order q up to isomorphism. $\mathbb{F}_q^* := \mathbb{F}_q - \{0\}$ is the group of invertible elements of $\mathbb{F}_q$. We will denote by $\tau : \mathbb{F}_q \to \mathbb{F}_q$ the Frobenius field homomorphism given by $x \mapsto x^p$.

Proposition 2.3.2. Let G be a finite group of order n. If for each $d \mid n$,

$$\#\{x \in G \,:\, x^d = 1\} \leq d,$$

then G is cyclic.

Proof. Fix some $d \mid n$ and define G_d as the set of elements in G of order d. Suppose there is $g \in G_d$. Then, $\langle g \rangle \subseteq \{x \in G \,:\, x^d = 1\}$. But since $\#\langle g \rangle = d$, these sets must in fact be equal. That means G_d is the set of generators of $\langle g \rangle$, and thus has cardinality $\phi(d)$, where ϕ is Euler's totient function. So we've proved that for any $d \mid n$, $\#G_d = 0$ or $\phi(d)$. But then,

$$n = \#G \leq \sum_{d \mid n} \#G_d \leq \sum_{d \mid n} \phi(d) = n,$$

therefore all G_d are non-empty. In particular, G_n is non-empty, so G has a generator. □

Corollary 2.3.3. Any subgroup $G < \mathbb{F}_q^*$ is cyclic. In particular, $\mathbb{F}_q^*$ is cyclic.

Proof. For any $d \mid n$, the polynomial $x^d - 1 \in \mathbb{F}_q[x]$ has at most d roots. The result follows from Proposition 2.3.2. □

Proposition 2.3.4. There is an inclusion $\mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$ if and only if $m \mid n$.

Proof. ($\Rightarrow$) If $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, then $\mathbb{F}_{p^n}$ is a vector space over $\mathbb{F}_{p^m}$ of dimension $[\mathbb{F}_{p^n} \,:\, \mathbb{F}_{p^m}] =: d$. Then, $p^n = |\mathbb{F}_{p^n}| = |\mathbb{F}_{p^m}|^d = p^{md}$. So $m \mid n$. ($\Leftarrow$) Conversely, note that $\mathbb{F}_q$ is the splitting field of $x^q - x$. Since $m \mid n$, it follows that $x^{p^m} - x \mid x^{p^n} - x$ since

$$\begin{aligned} x^{p^n} - x = x(x^{p^n - 1} - 1) &= x \left(x^{\frac{p^n-1}{p^m-1}(p^m-1)} - 1 \right) \\ &= x(x^{p^m} - 1) \sum_{i=0}^{\frac{p^n-1}{p^m-1}-1} x^{(p^m-1)i} = (x^{p^m} - x) \sum_{i=0}^{\frac{p^n-1}{p^m-1}-1} x^{(p^m-1)i}. \end{aligned}$$

Thus $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$. □

As a consequence of Proposition 2.3.4, we can see $\mathbb{F}_{q^n}/\mathbb{F}_q$ as a field extension and consider the group $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. It turns out that this group has order n and is generated by τ.

Proposition 2.3.5. $\mathbb{F}_{q^n}/\mathbb{F}_q$ is a Galois extension. Moreover, $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is generated by τ and has order n.

Proof. We'll first prove for the case where $q = p$. We have that $x^{p^n} - x$ is separable in $\mathbb{F}_p[x]$ and $\mathbb{F}_q$ is its splitting field. Thus $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois. So $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. To prove that it is generated by the Frobenius homomorphism, it suffices to show that τ has order at least n. Let d be said order. We have, for all $a \in \mathbb{F}_{p^n}$,

$$0 = \tau^d(a) - a = a^{p^d} - a.$$

But the polynomial $x^{p^d} - x \in \mathbb{F}_p[x]$ has at most p^d roots, so $p^n \leq p^d$, thus $n \leq d$. Now, for the general case, note that since $\mathbb{F}_{q^n}/\mathbb{F}_p$ and $\mathbb{F}_q/\mathbb{F}_p$ are Galois, so is $\mathbb{F}_{q^n}/\mathbb{F}_q$. Then, $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is a subgroup of $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_p)$ of order n/m. Since the latter cyclic generated by τ, it follows that $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ must be $\langle \tau^m \rangle$. □

There are two useful maps from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ called *norm* and *trace*.

Definition 2.3.6 (Norm and Trace)**.** Given a finite extension L/K, we define the norm $\mathbb{N}_{L/K} : L \to K$ and trace $\mathrm{Tr}_{L/K} : L \to K$ as

$$\mathbb{N}_{L/K}(x) := \prod_{\sigma \in \mathrm{Hom}_K(L,\overline{K})} \sigma(x), \quad \mathrm{Tr}_{L/K}(x) := \sum_{\sigma \in \mathrm{Hom}_K(L,\overline{K})} \sigma(x).$$

Clearly, the norm is multiplicative and the trace is additive. In the case of $\mathbb{F}_{q^n}/\mathbb{F}_q$, we denote the norm and trace by $\mathbb{N}_{q^n/q}$ and $\mathrm{Tr}_{q^n/q}$ for simplicity. Since the Frobenius homomorphism generates $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, we have explicit formulas for these maps given by

$$\mathbb{N}_{q^n/q}(x) = \prod_{j=0}^{n-1} x^{q^j}, \quad \mathrm{Tr}_{q^n/q}(x) = \sum_{j=0}^{n-1} x^{q^j}. \tag{2.1}$$

Proposition 2.3.7. Let $n \mid m$ (so $\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^m}$), then

(i) $\mathbb{N}_{q^n/q} \circ \mathbb{N}_{q^m/q^n} = \mathbb{N}_{q^m/q}$

(ii) $\mathbb{N}_{q^n/q}$ is surjective

(iii) $\mathbb{N}_{q^n/q}\big|_{\mathbb{F}_q}(x) = x^n$

(iv) $\mathrm{Tr}_{q^n/q} \circ \mathrm{Tr}_{q^m/q^n} = \mathrm{Tr}_{q^m/q}$

(v) $\mathrm{Tr}_{q^n/q}$ is surjective

(vi) $\mathrm{Tr}_{q^n/q}\big|_{\mathbb{F}_q} = nx.$

Proof. The key idea to prove the properties of norm is that $1+q+...+q^{n-1} = (q^n-1)/(q-1)$. (i) Let $\alpha \in \mathbb{F}_{q^m}$, we have

$$\mathbb{N}_{q^n/q} \circ \mathbb{N}_{q^m/q^n}(\alpha) = \alpha^{(1+q^n+...+q^{m-n})(1+q+...+q^{n-1})} = \alpha^{\frac{q^m-1}{q^n-1}\frac{q^n-1}{q-1}} = \alpha^{\frac{q^m-1}{q-1}} = \mathbb{N}_{q^m/q}(\alpha).$$

(ii) Let α be a generator of $\mathbb{F}_{q^n}^*$. We have $\mathbb{N}_{q^n/q}(\alpha) = \alpha^{1+q+...+q^{n-1}} = \alpha^{(q^n-1)/(q-1)} =: \beta$ which clearly must have order $q-1$, so β generates $\mathbb{F}_q$. (iii) Let $\alpha \in \mathbb{F}_q^*$, so $\alpha^q = \alpha$ and thus

$\mathbb{N}_{q^n/q}(\alpha) = \alpha^{1+q+\ldots+q^{n-1}} = \alpha^n$. (iv) Let $\alpha \in \mathbb{F}_{q^m}$. We have

$$\mathrm{Tr}_{q^n/q} \circ \mathrm{Tr}_{q^m/q^n}(\alpha) = \sum_{i=0}^{n-1} \tau^i \left(\sum_{j=0}^{\frac{m}{n}-1} \tau^{nj}(\alpha) \right) = \sum_{i=0}^{n-1} \sum_{j=0}^{\frac{m}{n}-1} \tau^{nj+i}(\alpha) = \sum_{k=0}^{m-1} \tau^k(\alpha) = \mathrm{Tr}_{q^m/q}(\alpha).$$

In the last step we simply reindexed the sum by setting $k = nj + i$. (v) If we look at $\mathbb{F}_{q^n}$ as a vector space over $\mathbb{F}_q$, then $\mathrm{Tr}_{q^n/q}$ is a linear map from a $n-$dimensional vector space to a $1-$dimensional one. Therefore, it must be surjective provided it is not zero. But it can't be zero since $\mathrm{Tr}_{q^n/q}(x) = \sum_{i=0}^{n-1} x^{q^i}$ is a polynomial of degree q^{n-1} in $\mathbb{F}_q[x]$ and thus can have at most $q^{n-1} < |\mathbb{F}_{q^n}|$ roots. (vi) Let $\alpha \in \mathbb{F}_q$, then $\mathrm{Tr}_{q^n/q}(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i} = \sum_{i=0}^{n-1} \alpha = n\alpha$. □

Corollary 2.3.8 (Reduction Formula)**.** Let $k \mid n$ and $\alpha \in \mathbb{F}_{q^k}$. Then,

$$\left(\mathbb{N}_{q^k/q}(\alpha)\right)^{n/k} = \mathbb{N}_{q^n/q}(\alpha), \quad \frac{n}{k}\left(\mathrm{Tr}_{q^k/q}(\alpha)\right) = \mathrm{Tr}_{q^n/q}(\alpha).$$

Proof. Since $\alpha \in \mathbb{F}_{q^k} \subseteq \mathbb{F}_{q^n}$,

$$\left(\mathbb{N}_{q^k/q}(\alpha)\right)^{n/k} = \mathbb{N}_{q^k/q}(\alpha^{n/k}) = \mathbb{N}_{q^k/q} \circ \mathbb{N}_{q^n/q^k}(\alpha) = \mathbb{N}_{q^n/q}(\alpha).$$

The proof for the trace is similar. □

Theorem 2.3.9. Let $P(x) \in \mathbb{F}_q[x]$ be irreducible of degree n. Then, we have that $\mathbb{F}_{q^n} \cong \mathbb{F}_q[x]/(P(x))$ and there is some $\alpha \in \mathbb{F}_{q^n}$ such that

$$P(x) = \prod_{i=0}^{n-1} (x - \alpha^{q^i}).$$

Proof. Since $\mathbb{F}_q[x]$ is a UFD, $P(x)$ is prime, so $L := \mathbb{F}_q[x]/(P(x))$ is a finite domain and hence a finite field. Its cardinality is clearly q^n since for any $h(x)$ in the quotient there are p options for each of the m coefficients. Since fields are determined by their cardinality it follows that $L \cong \mathbb{F}_{q^n}$.

For the second claim, we know that, formally, $x \in L$ is a root of P. Let $\beta(x)$ be a generator of L^* (which is cyclic). Then, there is some $s \geq 1$ such that $q^n \nmid s$ and $x = \beta(x)^s$. Recall that $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \{\mathrm{id}, \tau, \tau^2, ..., \tau^{n-1}\}$. Now, each $\tau^i(x) = \beta(x)^{sq^i}$ must be a distinct root of P. To see this, suppose $\beta(x)^s = \beta(x)^{sq^i}$ for some i, so $q^n \mid s(1 - q^i)$ which is only true when $i = 0$. Therefore, by setting $\alpha := x$ we get the desired result. □

This gives a nice way of representing finite fields provided one is able to find irreducible polynomials. Unfortunately, this task is far from trivial. The two main algorithms for searching irreducible polynomials in $\mathbb{F}_q$ are the Berlekamp's algorithm [3] and the currently fastest Cantor-Zassenhaus algorithm [5].

Proposition 2.3.10. Let p be an odd prime number and $k \geq 1$. The equation

$$x^{2^{k-1}} = -1$$

has a solution in $\mathbb{F}_q$ if and only if $q \overset{2^k}{\equiv} 1$.

Proof. ($\Rightarrow$) Suppose there is some α such that $\alpha^{2^{k-1}} = -1$. Since $-1 \neq 1$ (since p is odd), it follows that α has order 2^k and by Lagrange's Theorem 2^k must divide the order of $\mathbb{F}_q^*$, which is $q-1$. ($\Leftarrow$) We proceced by induction on $k \geq 1$. If $k = 1$ there is nothing to prove. Assume by induction that there is some $\alpha \in \mathbb{F}_q$ such that $\alpha^{2^{k-2}} = -1$. By Theorem 2.3.9, the equation $x^2 = \alpha$ must have a solution β in $\mathbb{F}_{q^2}$. But β is fixed by all elements in $\mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$ since this group is generated by $x \mapsto x^q$ and

$$\beta^q = \beta^{2^k m+1} = \beta\alpha^{2^{k-1}m} = \beta(-1)^{2m} = \beta.$$

In the first equality, we used $q \overset{2^k}{\equiv} 1$. Since the Galois group fixes β, it follows that $\beta \in \mathbb{F}_q$. □

Remark 2.3.11. If $p \overset{4}{\equiv} 1$, then (x^2+1) is irreducible by Proposition 2.3.10. That means $\mathbb{F}_{p^2} \cong \mathbb{F}_p[x]/(x^2+1)$. This gives us another simple way of representing some finite fields. For example,

$$\mathbb{F}_9 \cong \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$$

with addition and multiplication taken mod x^2+1.

We can now start the discussion about characters.

Definition 2.3.12. Let G be a group. The group of characters of G is defined as $\hat{G} := \mathrm{Hom}(G, \mathbb{C}^*)$, where $\mathbb{C}^*$ is the multiplicative group of complex numbers. The operation is multiplication of maps and the indentity element is called the *principal character* and is denoted by $\mathbb{1}_G$ (or simply $\mathbb{1}$, when there is no ambiguity around the group G). We say a character χ is non-principal if $\chi \neq \mathbb{1}_G$.

If G is finite, notice that any character χ must send elements in $\mathbb{F}_q$ to elements of finite order in $\mathbb{C}^*$, i.e. roots of unity. This implies that inversion is simply complex conjugation, namely $\chi^{-1} = \overline{\chi}$.

Proposition 2.3.13. Let χ be a non-principal character of a group G. Then,

$$\sum_{g\in G}\chi(g)=0.$$

Proof. Since χ is non-principal there must be some $h\in G$ such that $\chi(h)\neq 1$. Then,

$$\sum_{g\in G}\chi(g)=\sum_{g\in G}\chi(hg)=\sum_{g\in G}\chi(h)\chi(g)=\chi(h)\sum_{g\in G}\chi(g).$$

Therefore the sum must be zero. □

Proposition 2.3.14. Let $(G,+)$ be a finite abelian group. Then, $\hat{G}\cong G$.

Proof. By the fundamental theorem of abelian groups, we know G must be isomorphic to $\mathbb{Z}_{n_1}\times ...\times\mathbb{Z}_{n_k}$. Let ζ_n be the nth root of unity. We define the isomorphism explicitly by $(a_1,...,a_k)\mapsto\chi_{a_1,...,a_k}$ where

$$\chi_{a_1,...,a_k}(x_1,...,x_k):=\zeta_{n_1}^{a_1x_1}...\zeta_{n_k}^{a_kx_k}.$$

To prove injectiveness, suppose $\chi_{a_1,...,a_k}=\mathbb{1}$. Let $e_i=(0,...,0,1,0,...,0)$ be the element of G with only one non-zero component, in the ith position. We have $1=\chi_{a_1,...,a_k}(e_i)=\zeta_{n_i}^{a_i}$. Therefore each a_i is congruent to zero and $(a_1,...,a_k)=0$. For surjectiveness, let $\chi\in\hat{G}$. For each i, $\chi(e_i)=\zeta_{n_i}^{a_i}$, so $\chi=\chi_{a_1,...,a_k}$. □

A character of $(\mathbb{F}_q,+)$ is called an *additive character of* $\mathbb{F}_q$ and a character of $(\mathbb{F}_q^*,\cdot)$ is called a *multiplicative character of* $\mathbb{F}_q$. The simplest additive character is the exponential $\psi_p:\mathbb{F}_p\to\mathbb{C}^*$ defined as $\psi(x):=e^{2\pi ix/p}$. From there, we can build additive characters for bigger fields by setting $\psi_q:=\psi_p\circ\mathrm{Tr}_{q/p}$. Multiplicative characters are usually denoted by the letter χ. Given a multiplicative character χ of $\mathbb{F}_q$, we have $\chi^{(n)}:=\chi\circ\mathbb{N}_{q^n/q}$ a multiplicative character of $\mathbb{F}_{q^n}$. Below we prove that this construction preserves order.

Proposition 2.3.15. Let $\chi:\mathbb{F}_q^*\to\mathbb{C}^*$ be a multiplicative character of order m. Define the character $\chi^{(n)}:=\chi\circ\mathbb{N}_{q^n/q}$. Then, $\chi^{(n)}$ also has order m and $\chi^{(n)}\Big|_{\mathbb{F}_q^*}=\chi^n$.

Proof. For any $\alpha\in\mathbb{F}_q^*$ we have $\chi^{(n)}(\alpha)=\chi\left(\prod_{j=0}^{n-1}\alpha^{q^j}\right)=\chi\left(\prod_{j=0}^{n-1}\alpha\right)=\chi\left(\alpha^n\right)=\chi^n(\alpha)$. The order of $\chi^{(n)}$ must be m since the norm is a surjective map. More concretely, suppose k is the order of $\chi^{(n)}$. Then, k is the first natural number such that

$$\chi^k\circ\mathbb{N}_{q^n/q}=(\chi^{(n)})^k=\mathbb{1}_{\mathbb{F}_{q^n}}=\mathbb{1}_{\mathbb{F}_q}\circ\mathbb{N}_{q^n/q}.$$

Since the norm is surjective, this occurs if and only if $\chi^k=\mathbb{1}_{\mathbb{F}_q}$. Therefore $k=m$. □

Multiplicative characters have already appeared in this chapter. Let p be an odd prime. First, given any finite field $\mathbb{F}_q$, there is a unique multiplicative character of order two (since it must send a generator to -1). In the field $\mathbb{F}_p$, that character is the Legendre symbol $\left(\frac{\cdot}{p}\right)$. For the bigger field $\mathbb{F}_q$, Proposition 2.3.15 tells us that the character is given by $\left(\frac{\cdot}{p}\right) \circ \mathbb{N}_{q/p}$. The situation is similar for order 4. First, if $q \overset{4}{\equiv} 3$, there cannot be any characters of order 4 since that would imply 4 divides $|\widehat{\mathbb{F}_q^*}| = |\mathbb{F}_q^*| = q - 1$. If $q \overset{4}{\equiv} 1$, there are only two of them, namely the ones that send a generator to i and $-i$. In the case of $\mathbb{F}_p$ with $p \overset{4}{\equiv} 1$, these are precisely the quartic symbol $\left[\frac{\cdot}{\pi}\right]$ and its conjugate $\overline{\left[\frac{\cdot}{\pi}\right]}$, where $p = \pi\overline{\pi}$; from there, we can use Proposition 2.3.15 to build characters for $\mathbb{F}_q$ in the same way as before. When $p \overset{4}{\equiv} 3$, there are characters of order 4 of $\mathbb{F}_q$ when $q \overset{4}{\equiv} 1$, but they cannot be expressed in terms of the quartic symbol. These results are summarized in the following Proposition.

Proposition 2.3.16. Let p be an odd prime. Then, $\mathbb{F}_q$ always has exactly one character χ_2 of order 2. Moreover, it has exactly two characters $\chi_4, \overline{\chi}_4$ of order 4 when $q \overset{4}{\equiv} 1$. These characters are given explicitly by

1. $\chi_2 = \left(\frac{\cdot}{p}\right) \circ \mathbb{N}_{q/p}$;
2. $\chi_4 = \left[\frac{\cdot}{\pi}\right] \circ \mathbb{N}_{q/p}$ (up to conjugation) when $p \overset{4}{\equiv} 1$, with $p = \pi\overline{\pi}$.

Example 2.3.17. With the tools we developed so far it is possible to evaluate some characters explicitly. As an example, let χ_4 be a multiplicative character of order 4 of the field $\mathbb{F}_q$, with $q = p^r \overset{4}{\equiv} 1$. We'll show that $\chi_4(-4) = 1$.

Case 1: $q \overset{8}{\equiv} 1$: by Proposition 2.3.10 there is some $\xi \in \mathbb{F}_q$ such that $\xi^4 = -1$. Then, we use Proposition 2.3.16 and quadratic reciprocity to get

$$\chi_4(-4) = \chi_4^4(\xi)\chi_4^2(2) = \chi_2(2) = \left(\frac{\mathbb{N}_{q/p}(2)}{p}\right) = \left(\frac{2^r}{p}\right) = \left(\frac{2}{p}\right)^r = (-1)^{r(p^2-1)/8}.$$

We must show 16 divides $r(p^2-1)$. If $p = 4k+3$ then r must be even (since $q \overset{8}{\equiv} 1$), so $r = 2r'$ and $r(p^2-1) = 2r'(16k^2+8k+8) = 16r'(8k^2+k+1)$. The case where $p \overset{8}{\equiv} 1$ is trivial. Lastly, if $p = 8k+5$ we have again $r = 2r'$ and $r(p^2-1) = 2r'(64k^2+16k+24) = 16r'(4k^2+k+1)$.

(Case 2: $q \overset{8}{\equiv} 5$) In this case, p must be of the form $8k+5$ and r must be odd. Then, by Proposition 2.3.10, there is $\xi \in \mathbb{F}_p$ such that $\xi^2 = -1$, but -1 is *not* a 4th-power residue in $\mathbb{F}_q$. So we have

$$\chi_4(-4) = \chi_4^2(2\xi) = \left(\frac{\xi}{p}\right)\left(\frac{2}{p}\right) = (-1) \cdot (-1)^{r(p^2-1)/8}.$$

We have $r(p^2-1) = r(64k^2+16k+24)$, which is not divisible by 16, so the result is $(-1) \cdot (-1) = 1$. We conclude that $\chi(-4) = 1$ in all cases.

The next proposition relates multiplicative characters with counting the number of mth-power residues of a finite field.

Proposition 2.3.18. Let $a \in \mathbb{F}_q^*$ and $\chi_m : \mathbb{F}_q^* \to \mathbb{C}^*$ be a multiplicative character of order m. Then,

$$\#\{x \in \mathbb{F}_q \ : \ x^m = a\} = \sum_{j=1}^{m} \chi_m^j(a).$$

Proof. We know $\mathbb{F}_q^*$ is cyclic and hence generated by some ζ. So, $a = \zeta^\alpha$ and the solutions for $x^m = a$ are exactly the solutions in k for $\zeta^{km} = \zeta^\alpha$, or, in other words, the pairs (k, n) such that

$$km + n(q-1) = \alpha.$$

This of course has no solutions if $m = \gcd(m, q-1) \nmid \alpha$. Otherwise, we have at least one solution x_0. But then the set

$$\{\zeta^{k(q-1)/m} x_0 \ : \ 0 \leq k < m\}$$

contains *all* solutions. Hence there must be m solutions. Now, for the right-hand side, we know that $\chi_m(\zeta) = e^{2\pi i s/m}$ where $\gcd(s, m) = 1$. Then,

$$\sum_{j=1}^{m} \chi_m^j(a) = \sum_{j=1}^{m} \chi_m^{j\alpha}(\zeta) = \sum_{j=1}^{m} e^{2\pi i j(s\alpha/m)}.$$

If $m \mid \alpha$, then all the terms in the sum are $= 1$, so the sum is equal to m. If $\alpha \nmid m$, this is the sum over all mth roots of unity, and hence is equal to zero. □

We now get to the definition of Gauss and Jacobi sums.

Definition 2.3.19 (Gauss sum)**.** Let χ be a multiplicative character of $\mathbb{F}_q$. The Gauss sum of χ is defined as

$$g(\chi) := \sum_{x \in \mathbb{F}_q^*} \chi(x)\psi_q(x), \quad \text{where } \psi_q(x) := \exp\left(\frac{2\pi i}{p}\mathrm{Tr}_{q/p}(x)\right).$$

Definition 2.3.20 (Jacobi sum)**.** The Jacobi sum of two multiplicative characters $\chi, \upsilon : \mathbb{F}_q^* \to \mathbb{C}^*$ is defined as

$$J(\chi, \upsilon) := \sum_{\substack{a,b \in \mathbb{F}_q^* \\ a+b=1}} \chi(a)\upsilon(b).$$

Below are some basic properties of Gauss and Jacobi sums.

Proposition 2.3.21. Let $\chi, \upsilon : \mathbb{F}_q^* \to \mathbb{C}^*$ be non-principal characters. Then,

$$\begin{array}{rl|rl}
\text{(i)} & J(\chi,\upsilon) = J(\upsilon,\chi) & \text{(v)} & \overline{g(\chi)} = \chi(-1)g(\overline{\chi}), \quad g(\mathbb{1}) = -1 \\
\text{(ii)} & J(\chi,\mathbb{1}) = -1 & \text{(vi)} & g(\chi)g(\overline{\chi}) = \chi(-1)q \\
\text{(iii)} & J\left(\chi,\overline{\chi}\right) = -\chi(-1) & \text{(vii)} & |g(\chi)| = \sqrt{q} \\
\text{(iv)} & J(\mathbb{1},\mathbb{1}) = q-2 & \text{(viii)} & J(\chi,\upsilon) = g(\chi)g(\upsilon)/g(\chi\upsilon) \text{ if } \chi \neq \overline{\upsilon}.
\end{array}$$

Proof. (i) This is clear from the definition. (ii) We have

$$J(\chi,\mathbb{1}) = \sum_{\substack{a,b\in\mathbb{F}_q^* \\ a+b=1}} \chi(a) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a\neq 1}} \chi(a) = -1 + \sum_{a\in\mathbb{F}_q^*} \chi(a) = -1,$$

where in the last step we used Proposition 2.3.13. (iii) This case is similar.

$$J(\chi,\overline{\chi}) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a\neq 1}} \chi(1-a)\overline{\chi}(a) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a\neq 1}} \chi(a^{-1}-1)\chi(a)\overline{\chi}(a) = \sum_{\substack{a\in\mathbb{F}_q^* \\ a\neq 1}} \chi(a^{-1}-1) = -\chi(-1).$$

In the last equality, the sum ranges over all elements of the form $\chi(x)$ except $\chi(-1)$, so again the result follows by Proposition 2.3.13. (iv) $J(\mathbb{1},\mathbb{1}) = \sum_{a\in\mathbb{F}_q^*-\{1\}} 1 = q-2$. (v) Here, note that $\overline{\psi_q(a)} = \psi_q^{-1}(a) = \psi_q(-a)$. So,

$$\overline{g(\chi)} = \sum_{a\in\mathbb{F}_q^*} \overline{\chi}(a)\psi_q(-a) = \sum_{a\in\mathbb{F}_q^*} \overline{\chi}(-a)\psi_q(a) = \overline{\chi}(-1)\sum_{a\in\mathbb{F}_q^*} \overline{\chi}(a)\psi_q(a) = \overline{\chi}(-1)g(\overline{\chi}).$$

But $\overline{\chi}(-1) = \chi(-1)$ since -1 has order 2. For the second part, $g(\mathbb{1}) = \sum_{a\in\mathbb{F}_q^*} \psi_q(a) = -1 + \sum_{a\in\mathbb{F}_q} \psi_q(a) = -1$. (vi) Here, we first prove

$$g(\chi)g(\upsilon) = \left(\sum_{a\in\mathbb{F}_q^*} \chi(a)\psi_q(a)\right)\left(\sum_{b\in\mathbb{F}_q^*} \upsilon(b)\psi_q(b)\right) = \sum_{a,b\in\mathbb{F}_q^*} \chi(a)\upsilon(b)\psi_q(a+b).$$

By summing over $c = a+b$ we get the following equation.

$$g(\chi)g(\upsilon) = \sum_{c\in\mathbb{F}_q} \sum_{\substack{a,b\in\mathbb{F}_q^* \\ a+b=c}} \chi(a)\upsilon(b)\psi_q(c). \tag{2.2}$$

We apply this equation for $\upsilon = \overline{\chi}$. The term $c = 0$ is calculated as

$$\sum_{\substack{a,b\in\mathbb{F}_q^* \\ a+b=0}} \chi(a)\overline{\chi}(b) = \sum_{a\in\mathbb{F}_q^*} \chi(a)\overline{\chi}(-a) = \overline{\chi}(-1)\sum_{a\in\mathbb{F}_q^*} 1 = \chi(-1)(q-1).$$

For the terms where $c \neq 0$, we have

$$\sum_{c\in\mathbb{F}_q^*} \sum_{\substack{a,b\in\mathbb{F}_q^* \\ a+b=c}} \chi(a)\upsilon(b)\psi_q(c) = \sum_{c\in\mathbb{F}_q^*} \sum_{\substack{a,b\in\mathbb{F}_q^* \\ a+b=1}} \chi(ca)\upsilon(cb)\psi_q(c) \tag{2.3}$$

$$= \left(\sum_{c\in\mathbb{F}_q^*} (\chi\upsilon)(c)\psi_q(c)\right) \left(\sum_{\substack{a,b\in\mathbb{F}_q^* \\ a+b=1}} \chi(a)\upsilon(b)\right) = g(\chi\upsilon)J(\chi,\upsilon). \tag{2.4}$$

Again applying this to $\upsilon = \overline{\chi}$, we have $g(\mathbb{1})J(\chi,\overline{\chi}) = (-1)(-\chi(-1)) = \chi(-1)$. Summing everything we have $g(\chi)g(\overline{\chi}) = \chi(-1)q$. (vii) Here we have $|g(\chi)|^2 = g(\chi)\overline{g(\chi)} = \chi(-1)g(\chi)g(\overline{\chi}) = \chi^2(-1)q = q$. (viii) We use once more Equation 2.2. However, this time, the term $c = 0$ is

$$\sum_{\substack{a,b\in\mathbb{F}_q^* \\ a+b=0}} \chi(a)\upsilon(b) = \sum_{a\in\mathbb{F}_q^*} \chi(a)\upsilon(-a) = \upsilon(-1) \sum_{a\in\mathbb{F}_q^*} (\chi\upsilon)(a) = 0.$$

The last sum is equal to zero since $\chi\upsilon \neq \mathbb{1}$ by hypothesis. The terms for $c \neq 0$ are equal to $g(\chi\upsilon)J(\chi,\upsilon)$ by Equation 2.4. We then have

$$g(\chi)g(\upsilon) = g(\chi\upsilon)J(\chi,\upsilon).$$

To conclude we have to divide both sides by $g(\chi\upsilon)$. This can be done since $|g(\chi\upsilon)| = \sqrt{q}$, so in particular it is non-zero. And this concludes the proof. □

Theorem 2.3.22 (Hasse-Davenport)**.** $-g(\chi^{(n)}) = [-g(\chi)]^n$

Proof. The argument amounts to some clever manipulation of formal expressions. Let M be the set of monic polynomials in $\mathbb{F}_q[x]$, and $I \subseteq M$ the set of monic, irreducible polynomials. Let $f = (x - a_1)\dots(x - a_k) \in M$, with $a_i \in \overline{F}_q$. Define a function $\rho : M \to \mathbb{C}^*$ by

$$\rho(f) := \chi\left(\prod_i a_i\right) \psi_q\left(\sum_i a_i\right),$$

where we set $\chi(0) := 0$. This is well-defined since the sum and product of the a_i's are, respectively, the coefficient of x^{k-1} and constant term of f. Notice that ρ is multiplicative (i.e. $\rho(fg) = \rho(f)\rho(g)$). Now, let $\alpha \in \mathbb{F}_{q^n}$ with minimal polynomial $f_\alpha \in I$ of degree k. Then, by Theorem 2.3.9 we have $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^k}$, and $f = \prod_{i=0}^{k-1}(x - \alpha^{q^i})$. Then,

$$\rho(f_\alpha)^{n/k}$$

$$
\begin{aligned}
&= \chi^{n/k}\left(\prod_{i=0}^{k-1}\alpha^{q^i}\right)\psi_q^{n/k}\left(\sum_{i=0}^{k-1}\alpha^{q^i}\right) && \text{(Definition of } \rho\text{)}\\
&= \chi^{n/k}\left(\mathbb{N}_{q^k/q}(\alpha)\right)\psi_q^{n/k}\left(\mathrm{Tr}_{q^k/q}(\alpha)\right) && \Big(\text{Equation (2.1): norm and trace of } \mathbb{F}_{q^k}\Big)\\
&= \chi\left(\mathbb{N}_{q^k/q}(\alpha)^{n/k}\right)\psi_q\left(\frac{n}{k}\mathrm{Tr}_{q^k/q}(\alpha)\right) && (\chi \text{ and } \psi_q \text{ are characters})\\
&= \chi\left(\mathbb{N}_{q^n/q}(\alpha)\right)\psi_q\left(\mathrm{Tr}_{q^n/q}(\alpha)\right) && \text{(Corollary 2.3.8: Reduction Formula)}\\
&= \chi^{(n)}(\alpha)\psi_{q^n}(\alpha) && \Big(\text{Definition of } \chi^{(n)} \text{ and } \psi_q\circ\mathrm{Tr}_{q^n/q}=\psi_{q^n}\Big).
\end{aligned}
$$

From there, we have

$$
\begin{aligned}
&g(\chi^{(n)})\\
&= \sum_{a\in\mathbb{F}_{q^n}^*}\chi^{(n)}(a)\psi_{q^n}(a) && \text{(Definition 2.3.19: Gauss sum)}\\
&= \sum_{\substack{f\in I\\ \deg f\mid n}}\sum_{\substack{a\in\overline{\mathbb{F}}_q\\ f(a)=0}}\chi^{(n)}(a)\psi_{q^n}(a) && (a\in\mathbb{F}_{q^n} \iff \exists f\in I, \deg f\mid n, f(a)=0)\\
&= \sum_{\substack{f\in I\\ \deg f\mid n}}\sum_{\substack{a\in\overline{\mathbb{F}}_q\\ f(a)=0}}\rho(f)^{n/\deg f} && \text{(Calculation from before)}\\
&= \sum_{\substack{f\in I\\ \deg f\mid n}}(\deg f)\rho(f)^{n/\deg f} && \Big(f \text{ has } \deg f \text{ roots in } \overline{\mathbb{F}}_q\Big).
\end{aligned}
$$

Now, let t be a formal variable. The expression $\rho(f)t^{\deg f}$ is multiplicative on f, so we can use Euler's product identity to get

$$\prod_{f\in I}\left(1-\rho(f)t^{\deg f}\right)^{-1} = \sum_{f\in M}\rho(f)t^{\deg f} = \sum_{i\geq 0}\overbrace{\left(\sum_{\substack{f\in M\\ \deg f=i}}\rho(f)\right)}^{A_i}t^i. = \sum_{i\geq 0}A_it^i.$$

Let's calculate the coefficients A_i explicitly. First, we have

$$A_0 = \sum_{\substack{f\in M\\ \deg f=0}}\rho(f)=1, \quad A_1 = \sum_{\substack{f\in M\\ \deg f=1}}\rho(f) = \sum_{a\in\mathbb{F}_q}\rho(x-a) = \sum_{a\in\mathbb{F}_q}\chi(a)\psi_q(a) = g(\chi). \tag{2.5}$$

For $i>1$, we have

$$A_i$$

$$\begin{aligned}
&= \sum_{\substack{f\in M\\ \deg f=i}} \rho(f) && \text{(Definition of } A_i\text{)}\\
&= \sum_{a_0,\dots,a_{i-1}\in\mathbb{F}_q} \rho(x^i - a_{i-1}x^{i-1} + \dots + (-1)^i a_0) && \text{(Reindexing)}\\
&= \sum_{a_0,\dots,a_{i-1}\in\mathbb{F}_q} \chi(a_0)\psi_q(a_{i-1}) && \text{(Product and sum of roots in terms of } a_i\text{'s)}\\
&= q^{i-2}\sum_{a_0\in\mathbb{F}_q}\chi(a_0)\sum_{a_{i-1}\in\mathbb{F}_q}\psi_q(a_{i-1}) && \text{(Summand is independent of } a_1,\dots,a_{i-2}\text{)}\\
&= 0 && \text{(Proposition 2.3.13: } \textstyle\sum \psi_q(a)=0\text{).}
\end{aligned}$$

Thus formally $\prod_{f\in I}(1-\rho(f)t^{\deg f})^{-1} = 1+g(\chi)t$. We take the log on both sides, obtaining

$$-\sum_{f\in I}\log\left(1-\rho(f)t^{\deg f}\right) = \log\left(1+g(\chi)t\right). \tag{2.6}$$

Differentiating on both sides we get

$$\sum_{f\in I}\frac{(\deg f)\rho(f)t^{\deg f-1}}{1-\rho(f)t^{\deg f}} = \frac{g(\chi)}{1+g(\chi)t}. \tag{2.7}$$

The left-hand side is the sum of a geometric progression, so we can simplify it to

$$\begin{aligned}
& t^{-1}\sum_{f\in I}\sum_{j\geq 1}(\deg f)\rho(f)^j t^{j\deg f}\\
&= t^{-1}\sum_{n\geq 1}\left(\sum_{\substack{f\in I\\ \deg f\mid n}}(\deg f)\rho(f)^{n/\deg f}\right)t^n && \text{(Exchange summations by reindexing)}\\
&= \sum_{n\geq 1} g(\chi^{(n)})t^{n-1} && \text{(Calculations from before).}
\end{aligned}$$

The right-hand side is also the sum of a geometric progression equal to

$$\sum_{n\geq 1}(-1)^{n-1}g(\chi)^n t^{n-1}.$$

Comparing coefficients of t^{n-1} we get $g(\chi^{(n)}) = (-1)^{n-1}g(\chi)^n$. □

2.4 Basics of algebraic number theory

In this section we present a brief introduction to algebraic number theory. The final goal is to prove Theorem 2.4.32, which will be necessary in the proof of the Mordell-Weil Theorem.

To do this, we must first be able to state the two main theorems of algebraic number theory: the finiteness of the class number and the finite generation of the group of units. We start off by defining number fields and proving some of their basic properties [33, 29, 31]. Next, we quickly discuss the relations between local rings, Dedekind domains and discrete valuation rings. A more in-depth characterization of these properties can be found in [19, Page 599]. In the end, we also talk briefly about Dedekind zeta functions and valuations.

2.4.1 Integrality

Definition 2.4.1. Let A be an $R-$algebra. We say $a \in A$ is *integral* over R if $P(a) = 0$ for some $P \in R[x]$ monic. We say A is integral over R if all elements of A are integral over R.

Proposition 2.4.2. Let A be a finitely generated $R-$algebra. Then, the following are equivalent.

(i) A is integral over R,

(ii) A is generated (as a $R-$algebra) by integral elements,

(iii) A is a finitely generated $R-$module,

(iv) There is a finitely generated $R-$submodule $M \subseteq A$ with $AM \subseteq M$.

Proof. (i $\Rightarrow$ ii) Since A is integral, any generating set contains only integral elements. (ii $\Rightarrow$ iii) Let $\{r_1, ..., r_n\}$ be such a generating set. Since each r_i is integral, we have $P_i(r_i) = 0$ with $\deg(P_i) =: d_i$. But then, the set $\{r_1^{k_1}...r_n^{k_n} \quad k_i \leq d_i\}$ generates A as a $R-$module. (iii $\Rightarrow$ iv) Just take $M = A$, so $AA \subseteq A$. (iv $\Rightarrow$ i) Pick $a \in A$ and $\{x_1, ..., x_n\}$ a generating set for M. So for all i we have $ax_i = \sum_j c_{ij}x_j$, with $c_{ij} \in R$. Define a matrix S by $S_{i,j} = (a\delta_{ij} - c_{ij})$, so $S(x_1, ..., x_n)^t = 0$, thus $\det(S) = \det(a\delta_{ij} - c_{ij}) = 0$, which is a monic polynomial over R evaluated at a. □

Corollary 2.4.3. The set $\text{int}_R(A) := \{a \in A \ : \ a \text{ is integral over } R\} \subseteq A$, called the *integral closure of R in A*, is a ring.

Proof. Let $x, y \in \text{int}_R(A)$. Then, the algebra $A[x, y]$ is generated by integral elements, and hence, by Proposition 2.4.2, integral over R. Since $xy, x+y \in A[x, y]$, the result follows. □

Remark 2.4.4. Take $A = \mathbb{R}, R = \mathbb{Z}$. The proof of Proposition 2.4.2 gives us a way of, given some $a \in \mathbb{R}$, finding a polynomial $P(x) \in \mathbb{Z}[x]$ with $P(a) = 0$. For instance, let $a = \sqrt{2} + \sqrt{3}$. Then, $a \in \mathbb{Z}[\sqrt{2}, \sqrt{3}] = \text{span}_{\mathbb{Z}}\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Since this generating set has cardinality 4, the set $\{1, a, a^2, a^3, a^4\}$ must be linearly dependent. By calculating each of these terms we quickly find $P(x) = x^4 - 10x^2 + 1$.

Definition 2.4.5. Given a domain R, we define its *integral closure* as $\text{int}(R) := \text{int}_R(\text{Frac}(R))$. R is said to be *integrally closed* if $\text{int}(R) = R$.

Remark 2.4.6. Any UFD must be integrally closed. Pick $x = a/b \in \text{Frac}(R)$ with a, b not sharing any common factors. Suppose $x^n + c_{n-1}x^{n-1} + ... + c_0 = 0$. Then, by substituting $x = a/b$ and multiplying both sides by b^n we get $c_{n-1}a^{n-1}b + ... + c_0 b^n = -a^n$ and so b divides a^n, but these two share no common factors, so b must be invertible. Hence, $x \in R$.

Proposition 2.4.7 (Transitivity of integrality)**.** Let $A \supseteq B \supseteq C$ be rings. Suppose A is integral over B and B over C. Then, A is integral over C.

Proof. Take $a \in A$. Then, a is a root of $a^n + b_{n-1}a^{n-1} + ... + b_0 = 0$ for some $b_i \in B$. Let $R := C[b_0, ..., b_{n-1}]$. Then, $R[a]$ is a finitely generated $R-$module, with generating set $\{1, a, ..., a^{n-1}\}$. But also R is a finitely generated $C-$algebra and integral over C, so by Proposition 2.4.2 R is a finitely generated $C-$module. Joining these two facts we have that $R[a]$ is a finitely generated $C-$module, and thus by Proposition 2.4.2 integral over C. □

Remark 2.4.8. Any ring of the form $L := \text{int}_A(\text{Frac}(R))$ is integrally closed. To see this, note that

$$\text{int}(L) \text{ is integral over } L; \quad L \text{ is integral over } A. \tag{2.8}$$

Therefore, by Proposition 2.4.7 $\text{int}(L)$ is integral over A. But $\text{int}(L) \subseteq \text{Frac}(R)$. So it must be that $\text{int}(L) \subseteq L$.

2.4.2 Number fields

Definition 2.4.9. A *number field* is a finite extension $K/\mathbb{Q}$. We define its *ring of integers* as

$$\mathcal{O}_K := \text{int}_{\mathbb{Z}}(K) = \{x \in K \ : \ P(x) = 0 \text{ for some } P \in \mathbb{Z}[x] \text{ monic}\}.$$

Notice that, if we take $K = \mathbb{Q}$, then $\mathcal{O}_K = \mathbb{Z}$. This shows why this object is called the ring of integers of K, as it is a generalization of the ordinary integers. In general, the ring $\mathcal{O}_K$ is not even a UFD. One of the simplest examples is $K = \mathbb{Q}(\sqrt{-5})$. It is not difficult to show that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. In this ring we have two distinct factorizations of 6 as irreducible elements, namely $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$. Soon, we'll show that $\mathcal{O}_K$ can always be extended in a reasonable way to become a PID. Besides not having unique factorization of elements, $\mathcal{O}_K$ has the remarkable property of having unique factorization of *ideals*. This will be proven later. As an example, in $\mathbb{Z}[\sqrt{-5}]$, the ideal generated by 6 can be decomposed as the product of prime ideals

$$(6) = (2, 1+\sqrt{-5})^2(3, 1-\sqrt{-5})(3, 1+\sqrt{-5}). \tag{2.9}$$

For the remainder of this section, K will always denote a number field. We can define a trace operator $\mathrm{Tr}_{K/\mathbb{Q}} : K \to \mathbb{Q}$ as in Definition 2.3.6.

Proposition 2.4.10. We have

(i) $\mathrm{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) \subseteq \mathbb{Z}$,

(ii) The bilinear form $(x, y) := \mathrm{Tr}_{K/\mathbb{Q}}(xy)$ is non-degenerate.

Proof. (i) Pick $x \in \mathcal{O}_K$. For any embedding $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$, the term $\sigma(x)$ is still integral over $\mathbb{Z}$ (since σ fixes $\mathbb{Z}$). But then, $\mathrm{Tr}_{K/\mathbb{Q}}(x) = \sum_\sigma \sigma(x) \in \mathbb{Q} \cap \mathrm{int}_{\mathbb{Z}}(\mathbb{C}) = \mathrm{int}_{\mathbb{Z}}(\mathbb{Q}) = \mathbb{Z}$. (ii) To prove non-degeneracy, pick $x \in K \setminus \{0\}$. We need to find an element y such that $(x, y) \neq 0$. Simply set $y = 1/x$. We have $(x, 1/x) = \mathrm{Tr}_{K/\mathbb{Q}}(1) = \sum_\sigma \sigma(1) = \sum_\sigma 1 \neq 0$. □

Remark 2.4.11 (Basis of K)**.** Any element $\alpha \in K$ is algebraic, so we have its equation $a_n\alpha^n + a_{n-1}\alpha^{n-1}... + a_0 = 0$. But then, by multiplying both sides by a_n^{n-1} we have

$$(a_n\alpha)^n + a_{n-1}(a_n\alpha)^{n-1} + a_{n-2}a_n(a_n\alpha)^{n-2} + ... + a_n^{n-1}a_0 = 0. \tag{2.10}$$

So $a_n\alpha \in \mathcal{O}_K$. In particular, this tells us that any base $\{\alpha_1, ..., \alpha_n\}$ of the vector space K can be rescaled so that each elements belongs to $\mathcal{O}_K$. Therefore, we'll often pick bases of K already contained in $\mathcal{O}_K$ without further remarks.

Proposition 2.4.12. Let $\{\alpha_1, ..., \alpha_n\} \subseteq \mathcal{O}_K$ be a basis of K. Then, there is an integer d such that $d\mathcal{O}_K \subseteq \mathrm{span}_{\mathbb{Z}}\{\alpha_1, ..., \alpha_n\}$.

Proof. Pick $\beta \in \mathcal{O}_K$. Then, $\beta = \sum a_i\alpha_i$, for $a_i \in \mathbb{Q}$. Then, we have

$$\overbrace{\begin{bmatrix}(\alpha_1,\beta)\\ \vdots \\ (\alpha_n,\beta)\end{bmatrix}}^{b} = \overbrace{\begin{bmatrix}(\alpha_1,\alpha_1) & \dots & (\alpha_1,\alpha_n)\\ \vdots & \ddots & \vdots \\ (\alpha_n,\alpha_1) & \dots & (\alpha_n,\alpha_n)\end{bmatrix}}^{M}\overbrace{\begin{bmatrix}a_1\\ \vdots \\ a_n\end{bmatrix}}^{a} \tag{2.11}$$

where M is the Gram matrix of the bilinear form $(x, y) := \mathrm{Tr}_{K/\mathbb{Q}}(xy)$. This matrix is invertible and both M and b have integer coordinates by Proposition 2.4.10. If we set $d := \det(M)$, we have

$$\mathrm{adj}(M)b = \mathrm{adj}(M)Ma = da. \tag{2.12}$$

Therefore, $d\beta = \sum da_i\alpha_i = \sum(\mathrm{adj}(M)b)_i\alpha_i$ which is a combination of α_i's with integer coefficients. □

Proposition 2.4.13. $\mathcal{O}_K$ is a free $\mathbb{Z}-$module of rank $[K : \mathbb{Q}]$.

Proof. Pick a basis $\{\alpha_1, ..., \alpha_n\} \subseteq \mathcal{O}_K$ of K, with $n = [K : \mathbb{Q}]$. In particular it is a linearly independent set of $\mathcal{O}_K$, so $\text{rank}(\mathcal{O}_K) \geq n$. Now, by Proposition 2.4.12, $\{\alpha_1, ..., \alpha_n\}$ generates $d\mathcal{O}_K$, so $\text{rank}(d\mathcal{O}_K) \leq n$. But since $\mathbb{Z}$ is a domain, the map $x \mapsto dx$ is a injection, so $\text{rank}(\mathcal{O}_K) = \text{rank}(d\mathcal{O}_K) \leq n$. It remains to show that $\mathcal{O}_K$ is free. But notice that $\mathcal{O}_K$ is a $\mathbb{Z}-$submodule of the free module with basis $\{\alpha_1/d, ..., \alpha_n/d\}$. Since $\mathbb{Z}$ is a PID, it follows that $\mathcal{O}_K$ is also free. □

We can generalize this to the following.

Proposition 2.4.14. Let $M \subseteq K$ be a finitely generated $R-$submodule, $R \supseteq \mathbb{Z}$.

(i) If $R \subseteq \mathcal{O}_K$, then M is a free $\mathbb{Z}-$module of rank $\leq [K : \mathbb{Q}]$,

(ii) Moreover, if $R = \mathcal{O}_K$, then rank $= [K : \mathbb{Q}]$.

Proof. (i) Pick a generating set $\{x_1, ..., x_m\}$ of M. Since $x_i \in K$, there is an integer $n_i \neq 0$ such that $n_i x_i \in \mathcal{O}_K$. Set $n := \prod n_i$. Then, we have an injection

$$M \hookrightarrow nM \subseteq \mathcal{O}_K. \tag{2.13}$$

That means M is free and $\text{rank}(M) = \text{rank}(nM) \leq \text{rank}(\mathcal{O}_K) = [K : \mathbb{Q}]$. (ii) In this case we also have an injection going the other way around. Fix a non-zero $x \in M$, then

$$\mathcal{O}_K \hookrightarrow \mathcal{O}_K x \subseteq M, \tag{2.14}$$

so $\text{rank}(M) \geq \text{rank}(x\mathcal{O}_K) = \text{rank}(\mathcal{O}_K) = [K : \mathbb{Q}]$ □

Remark 2.4.15. Notice that any $\mathbb{Z}-$basis of $\mathcal{O}_K$ is a $\mathbb{Q}-$basis of K. To see that, pick a basis $\{x_1, ..., x_n\}$ of $\mathcal{O}_K$. If there were a non-trivial relation $\sum a_i x_i = 0$ with $a_i \in \mathbb{Q}$, then we could multiply by a sufficiently large integer N to find a non-trivial relation $\sum N a_i x_i = 0$ with $N a_i \in \mathbb{Z}$, which would be a contradiction. Therefore $\{x_1, ..., x_n\}$ is linear independent in K, but also of cardinality $n = [K : \mathbb{Q}]$, so it must be a basis. As an example, consider $\mathbb{Q}(i)/\mathbb{Q}$. Its ring of integers is $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$ which has a $\mathbb{Z}-$basis $\{1, i\}$. This set is also a basis for the vector space $\mathbb{Q}(i)$.

2.4.3 Dedekind domains

Definition 2.4.16. We define the following.

(i) A **local ring** is a ring with a unique maximal ideal $\mathfrak{p}$,

(ii) A **discrete valuation ring** is a local ring where $\mathfrak{p} \neq 0$ that is also a PID,

(iii) A **Dedekind domain** is a Noetherian, integrally closed domain in which every prime ideal is maximal.

This section aims to prove some relations between these three definitions and, in the end, show that $\mathcal{O}_K$ is a Dedekind domain. Before that, we have to introduce the notion of ring localization.

Definition 2.4.17. Let R be a domain, $K = \text{Frac}(R)$ and $U \subseteq R$ a subset (not necessarily a subring!) closed under multiplication, with $1 \in U$ and $0 \notin U$. We define the localization of R at U as the subring

$$\text{loc}_U(R) := \{a/b \ : \ a \in R, b \in U\} \subseteq K.$$

The intuition behind ring localization is that it is similar to the field of fraction, but we only allow some elements to have a multiplicative inverse. So, for instance, $\text{loc}_{\{1\}}(R) = R$ and $\text{loc}_{R\setminus\{0\}}(R) = \text{Frac}(R)$. Localizations can also be defined for rings that aren't domains, but we will not need this level of generality. We have a natural inclusion $i : R \to \text{loc}_U(R)$ given by $i(x) := x/1$. Under this inclusion, we have the following.

Lemma 2.4.18. We have a bijection

$$\phi : \left\{\begin{matrix}\text{Prime ideals } \mathfrak{p} \subseteq R \\ \text{with } \mathfrak{p} \cap U = \varnothing\end{matrix}\right\} \xrightarrow{\sim} \left\{\text{Prime ideals } \mathfrak{q} \subseteq \text{loc}_U(R)\right\}$$

given by $\phi(\mathfrak{p}) = \mathfrak{p}\text{loc}_U(R)$ and $\phi^{-1}(\mathfrak{q}) = \mathfrak{q} \cap R$.

Proof. Let $\mathfrak{p} \subseteq R$ be prime disjoint from U. Let $\mathfrak{q} = \mathfrak{p}\text{loc}_U(R)$. This ideal is proper because otherwise, it would contradict the disjointness assumption. Let $(a_1/b_1)(a_2/b_2) \in \mathfrak{q}$. Then, there is $a \in \mathfrak{p}$ with $a_1a_2 = ab_1b_2 \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, we may assume $a_1 \in \mathfrak{p}$. But then $(a_1/b_1) \in \mathfrak{q}$, so it is a prime ideal. Conversely, let $\mathfrak{q} \subseteq \text{loc}_U(R)$ be a prime ideal and $\mathfrak{p} = \mathfrak{q} \cap R$. $\mathfrak{p}$ is proper and disjoint from U because otherwise $\mathfrak{q}$ would not be proper. Pick $ab \in \mathfrak{p} \subseteq \mathfrak{q}$. Since $\mathfrak{q}$ is prime, we may assume $a \in \mathfrak{q}$, but $a \in R$ also, so $a \in \mathfrak{q} \cap R = \mathfrak{p}$. It remains to check the inverses. We have $\phi(\phi^{-1}(\mathfrak{q})) = (\mathfrak{q} \cap R)\text{loc}_U(R) = \mathfrak{q}$ and $\phi^{-1}(\phi(\mathfrak{p})) = \mathfrak{p}\text{loc}_U(R) \cap R = \mathfrak{p}$. □

Remark 2.4.19. This map still makes sense when considering an arbitrary ideal. In this case, however, it is not a bijection. But we still have

$$(\mathfrak{h} \cap R)\operatorname{loc}_U(R) = \mathfrak{h} \tag{2.15}$$

for any ideal $\mathfrak{h} \subseteq \operatorname{loc}_U(R)$.

Given a prime ideal $\mathfrak{p} \subseteq R$, its complement $U := R \setminus \mathfrak{p}$ is always closed by multiplication and satisfies $1 \in U$, $0 \notin U$. The corresponding localization at U is so common that it has a specific notation $R_\mathfrak{p} := \operatorname{loc}_U(R)$.

Proposition 2.4.20. Let R be a domain and $\mathfrak{p} \subsetneq R$ an ideal. We have

(i) If $\mathfrak{p}$ is prime, $R_\mathfrak{p}$ is a local ring with unique maximal ideal $\mathfrak{p}R_\mathfrak{p}$.

(ii) If $\mathfrak{p}$ is maximal, $R/\mathfrak{p}^n$ is a local ring with *unique prime ideal* $\mathfrak{p}R/\mathfrak{p}^n$ for all $n \geq 1$.

Proof. (i) Pick $x \notin \mathfrak{p}R_\mathfrak{p}$. Then, $x = a/b$ with $a, b \notin \mathfrak{p}$. So $x^{-1} := b/a \in R_\mathfrak{p}$ is an inverse for x. So we have that $x \notin \mathfrak{p}R_\mathfrak{p} \Rightarrow x$ is invertible. Then it clearly is maximal since any ideal $I \supsetneq \mathfrak{p}R_\mathfrak{p}$ would contain an invertible element. Moreover if A is a maximal ideal, then $x \notin \mathfrak{p}R_\mathfrak{p} \Rightarrow x$ invertible $\Rightarrow x \notin A$, so $A \subseteq \mathfrak{p}R_\mathfrak{p}$ and by maximality $A = \mathfrak{p}R_\mathfrak{p}$.

(ii) Let $\pi : A \to A/\mathfrak{p}^n$ the projection. Let $I \subseteq A/\mathfrak{p}^n$ be a prime ideal. Then $\pi^{-1}(I) \supseteq \mathfrak{p}^n$ is also prime. But then $a \in \mathfrak{p} \Rightarrow a^n \in \pi^{-1}(I) \Rightarrow a \in \pi^{-1}(I)$. So $\mathfrak{p} \subseteq \pi^{-1}(I)$. By maximality $\mathfrak{p} = \pi^{-1}(I)$, hence $I = \pi(\mathfrak{p}) = \mathfrak{p}R/\mathfrak{p}^n$. □

Proposition 2.4.21. Let R be a domain and $\mathfrak{p} \subsetneq R$ a maximal ideal. Then, the natural map $R/\mathfrak{p}^n \to R_\mathfrak{p}/\mathfrak{p}^n R_\mathfrak{p}$ induced by the identity is an isomorphism.

Proof. We first show injectivity. If $a \in \mathfrak{p}^n R_\mathfrak{p}$, then $a = x/y$ with $x \in \mathfrak{p}^n$, $y \notin \mathfrak{p}$. Then $ay = 0$ in $R/\mathfrak{p}^n$. Now, since $R/\mathfrak{p}^n$ is local and $y \notin \mathfrak{p}R/\mathfrak{p}^n$, it follows that y must be a unit in $R/\mathfrak{p}^n$. Therefore we may cancel it to get $a \in \mathfrak{p}^n$.

Now we show surjectivity. Pick $[a/b] \in R_\mathfrak{p}/\mathfrak{p}^n R_\mathfrak{p}$, $a \in \mathfrak{p}^n$, $b \notin \mathfrak{p}$. Since $\mathfrak{p}$ is maximal, (b) and $\mathfrak{p}$ are coprime. Thus (b) and $\mathfrak{p}^n$ are coprime (see Proposition 7.0.2 in the Appendix). Therefore there is some $s \in R$ such that $bs - 1 \in \mathfrak{p}^n$. Therefore the element sa maps to $[sa] = [bsa/b] = [a/b]$. □

Proposition 2.4.22. Let R be a domain. The following are equivalent.

(i) R is a discrete valuation ring,

(ii) R is Noetherian, integrally closed with a unique prime ideal $\mathfrak{p}$,

(iii) There is $\pi \in R$ such that any non-zero ideal is of the form (π^N) for some $N \geq 0$.

Proof. (i ⇒ ii) R is Noetherian because it is a PID; it is integrally closed because it is a UFD (see Remark 2.4.6); it has a unique prime ideal because any prime ideal I is maximal since R is a PID, and hence equal to the unique maximal ideal.

(ii ⇒ iii) Fix $c \in \mathfrak{p} \setminus \{0\}$. Given $r \in R$ with $r \not\equiv 0 \mod c$ (for example, $r = 1$) we define

$$\mathcal{A}_r := \{x \in R \ : \ xr \equiv 0 \mod c\} \subseteq R. \tag{2.16}$$

We may choose r such that $\mathcal{A}_r$ is maximal among all the $\mathcal{A}_r$'s (otherwise we would have $\mathcal{A}_{r_1} \subsetneq \mathcal{A}_{r_2} \subsetneq ...$, but R is Noetherian). Notice that $\mathcal{A}_r$ is a proper (since $1 \notin \mathcal{A}_r$) non-zero (since $c \in \mathcal{A}_r$ and $c \neq 0$) ideal. Now, $\mathcal{A}_r$ must be prime, otherwise, given $x, y \notin \mathcal{A}_r$ with $xy \in \mathcal{A}_r$, we would have $\mathcal{A}_{ry} \supsetneq \mathcal{A}_r$ (because $x \in \mathcal{A}_{ry}$), which would contradict the maximality of $\mathcal{A}_r$.

We'll prove $\mathcal{A}_r = (c/r)$. We have $\mathfrak{p}r \subseteq (c)$, so $\mathfrak{p}(r/c) \subseteq R$ is an ideal. If $\mathfrak{p}(r/c) \subseteq \mathfrak{p}$, then (r/c) would be integral by Proposition 2.4.2 and thus $r/c \in R$ since R is integrally closed. But then $r = c(r/c) \in (c)$, which means $\mathcal{A}_r = R$, a contradiction. So $\mathfrak{p}(r/c) \not\subseteq \mathfrak{p}$. Now, if $\mathfrak{p}(r/c)$ were proper, it would be contained in a maximal ideal different from $\mathfrak{p}$, a contradiction, therefore $\mathfrak{p}(r/c) = R$, hence $\mathfrak{p} = (c/r)$. Set $\pi := c/r$.

Let $I \subsetneq R$ be a non-zero ideal. It must be that $I \subseteq \mathfrak{p} = (\pi)$. Consider the sequence

$$I \subseteq \pi^{-1}I \subseteq \pi^{-2}I \subseteq ... \tag{2.17}$$

If this sequence stays contained in R, then since R is Noetherian there must be N such that $\pi(\pi^{-N-1}I) = \pi^{-N}I = \pi^{-N-1}I$. So π^{-1} is integral by Proposition 2.4.2, and thus $\pi^{-1} \in R$ since R is integrally closed. But this is impossible since π is not a unit. Therefore there must be a maximal N such that $\pi^{-N}I \subseteq R$. But then $\pi^{-N}I \not\subseteq (\pi) = \mathfrak{p}$. Again, if $\pi^{-N}I$ were proper it would be contained in a maximal ideal different from $\mathfrak{p}$, so it must be that $\pi^{-N}I = R$, thus $I = (\pi^N)$.

(iii ⇒ i) Clearly R is a PID with unique maximal ideal $= (\pi) \neq \{0\}$. □

Corollary 2.4.23. If R is a Dedekind domain and a local ring with a non-zero maximal ideal $\mathfrak{p}$, then R is a discrete valuation ring.

Proof. Any prime ideal is maximal since R is Dedekind, and hence equal to $\mathfrak{p}$ since R is local. The result follows by Proposition 2.4.22. □

Lemma 2.4.24. Let R be Noetherian and $\mathfrak{p} \subseteq R$ a non-zero ideal. Then $\mathfrak{p}$ contains a product of prime ideals.

Proof. Let $\mathfrak{M}$ be the set of non-zero ideals that do not contain a product of primes. Suppose by contradiction that $\mathfrak{M} \neq \varnothing$. We may pick a maximal element $\mathfrak{m} \in \mathfrak{M}$ (otherwise we would have an infinite ascending chain $\mathfrak{m}_1 \subsetneq \mathfrak{m}_2 \subsetneq ...$, but R is Noetherian). This ideal cannot be prime, so there are $x, y \notin \mathfrak{m}$ such that $xy \in \mathfrak{m}$. But then $\mathfrak{m} + (x)$ and $\mathfrak{m} + (y)$ are strictly bigger ideals, so they contain a product of primes. Moreover $(\mathfrak{m} + (x))(\mathfrak{m} + (y)) \subseteq \mathfrak{m}$. □

Proposition 2.4.25. Let R be a domain. The following are equivalent.

(i) R is a Dedekind domain,

(ii) R is Noetherian and $R_{\mathfrak{p}}$ is a discrete valuation ring for all prime ideals $\mathfrak{p}$.

Proof. (i ⇒ ii) By Corollary 2.4.23 we must show that $R_{\mathfrak{p}}$ is Dedekind and local. It is local by Proposition 2.4.20. First, it is Noetherian because, given an ideal $\mathfrak{a} \subseteq R_{\mathfrak{p}}$, we have $\mathfrak{a} = (R \cap \mathfrak{a})R_{\mathfrak{p}}$, so $\mathfrak{a}$ is generated by the generators of $R \cap \mathfrak{a}$. To show it is integrally closed, let $\alpha \in \operatorname{Frac}(R)$ and

$$\alpha^n + c_{n-1}\alpha^{n-1} + ... + c_0 = 0 \tag{2.18}$$

where $c_i = a_i/b_i \in R_{\mathfrak{p}}$. Let $b := \prod_i b_i$, then $(b\alpha)^n + bc_{n-1}(b\alpha)^{n-1} + b^n c_0 = 0$ is an equation with coefficients in R, so since R is integrally closed, $b\alpha \in R$, which means $\alpha = b\alpha/b \in R_{\mathfrak{p}}$. Lastly, we must show that every prime ideal is maximal. Let $\mathfrak{q} \subseteq R_{\mathfrak{p}}$ be prime and $\mathfrak{q} \subseteq \mathfrak{a} \subsetneq R_{\mathfrak{p}}$. Then, $\mathfrak{q} \cap R$ is prime, thus maximal, contained in $\mathfrak{a} \cap R \subsetneq R$, thus $\mathfrak{q} \cap R = \mathfrak{a} \cap R$. But then $\mathfrak{q} = (\mathfrak{q} \cap R)R_{\mathfrak{p}} = (\mathfrak{a} \cap R)R_{\mathfrak{p}} = \mathfrak{a}$.

(ii ⇒ i) First, any prime ideal $\mathfrak{q}$ must be maximal since given a maximal ideal $\mathfrak{q} \subseteq \mathfrak{h}$, we have the prime ideal $\mathfrak{q}R_{\mathfrak{h}} \subseteq R_{\mathfrak{h}}$. But $R_{\mathfrak{h}}$ has a unique prime ideal (see Proposition 2.4.22), so $\mathfrak{q}R_{\mathfrak{h}} = \mathfrak{h}R_{\mathfrak{h}}$. Hence $\mathfrak{q} = \mathfrak{q}R_{\mathfrak{h}} \cap R = \mathfrak{h}R_{\mathfrak{h}} \cap R = \mathfrak{h}$. It remains to show R is integrally closed. Let $x \in \operatorname{Frac}(R)$ be integral over R. Then, for all prime ideals $\mathfrak{p}$, x automatically is integral over $R_{\mathfrak{p}}$, and hence $x \in R_{\mathfrak{p}}$. Let $\mathfrak{a} = \{y \in R \ : \ yx \in R\}$. This is an ideal and for any prime ideal $\mathfrak{p}$, we have $x = c/d \in R_{\mathfrak{p}}$ with $c \in R, d \notin \mathfrak{p}$, so $d \in \mathfrak{a}$. That means $\mathfrak{a}$ is not contained in any prime ideal, so it must be that $\mathfrak{a} = R$. In particular, $1 \in \mathfrak{a}$ so $x \in R$. □

We are now ready to prove that the ideals in a Dedekind domain factor into a product of prime ideals. This, in fact, is equivalent to being a Dedekind domain, but we won't need this stronger result. A more complete characterization of Dedekind domains can be found at [19].

Theorem 2.4.26. Let R be a Dedekind domain. Then, every non-zero proper ideal of R factors uniquely as a product of prime ideals.

Proof. (ii $\Rightarrow$ iii) Let $\mathfrak{a} \subsetneq R$ be non-zero ideal. By Lemma 2.4.24, $\mathfrak{a} \supseteq \mathfrak{q} := \mathfrak{p}_1^{e_1}...\mathfrak{p}_n^{e_n}$, where the $\mathfrak{p}_i$'s are distinct prime ideals. Each $\mathfrak{p}_i$ must be maximal since given a maximal ideal $\mathfrak{p}_i \subseteq \mathfrak{h}$, we have the prime ideal $\mathfrak{p}R_\mathfrak{h} \subseteq R_\mathfrak{h}$. But $R_\mathfrak{h}$ has a unique prime ideal (see Proposition 2.4.22), so $\mathfrak{p}R_\mathfrak{h} = \mathfrak{h}R_\mathfrak{h}$. Hence $\mathfrak{p} = \mathfrak{p}R_\mathfrak{h} \cap R = \mathfrak{h}R_\mathfrak{h} \cap R = \mathfrak{h}$. Since the $\mathfrak{p}_i$'s are maximal, we use Proposition 2.4.21 and the Chinese Remainder Theorem (see Theorem 7.0.4 in the Appendix) to get an isomorphism

$$\frac{R}{\mathfrak{q}} \cong \frac{R}{\mathfrak{p}_1^{e_1}} \times ... \times \frac{R}{\mathfrak{p}_n^{e_n}} \cong \frac{R_{\mathfrak{p}_1}}{\mathfrak{g}_1^{e_1}} \times ... \times \frac{R_{\mathfrak{p}_n}}{\mathfrak{g}_n^{e_n}}, \tag{2.19}$$

where $\mathfrak{g}_i := \mathfrak{p}_i R_{\mathfrak{p}_i}$. Define $\mathfrak{a}/\mathfrak{q}$ as the image of $\mathfrak{a}$ in the map $R \to R/\mathfrak{q}$. Now, the image of $\mathfrak{a}/\mathfrak{q}$ in the ith component is an ideal, and hence equal to $\mathfrak{g}_i^{s_i}/\mathfrak{g}_i^{e_i}$ for some $s_i < e_i$ since $R_{\mathfrak{p}_i}$ is a discrete valuation ring. But this is also the image of $\mathfrak{b}/\mathfrak{q} = \mathfrak{p}_1^{s_1}...\mathfrak{p}_n^{s_n}/\mathfrak{q}$. Since this map is an isomorphism, we conclude that $\mathfrak{a}/\mathfrak{q} = \mathfrak{b}/\mathfrak{q}$. But $\mathfrak{q}$ is contained in both $\mathfrak{a}$ and $\mathfrak{b}$, so it must be that $\mathfrak{a} = \mathfrak{b} = \mathfrak{p}_1^{s_1}...\mathfrak{p}_n^{s_n}$. To show uniqueness, pick another factorization $\mathfrak{p}_1^{r_1}...\mathfrak{p}_n^{r_n}$ (where some exponents may be zero, to guarantee the factors p_i are the same). Then, both factorizations must map to the same components, i.e. $\mathfrak{g}_i^{r_i}/\mathfrak{g}_i^{e_i} = \mathfrak{g}_i^{s_i}/\mathfrak{g}_i^{e_i}$. Since $\mathfrak{g}_i^{e_i}$ is contained in both of $\mathfrak{g}_i^{r_i}$ and $\mathfrak{g}_i^{s_i}$, they must be equal, so we conclude $r_i = s_i$. □

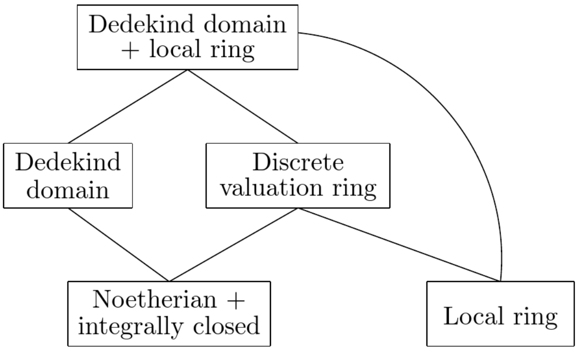


Figure 2.1: Property relations for a ring R which is not a field.
A lower node X connects to a higher node Y if $Y \Rightarrow X$.

The important relations between the three definitions given in 2.4.16 is summarized in Figure 2.1. We now return into the matter of the ring of integers $\mathcal{O}_K$.

Proposition 2.4.27. The ring $\mathcal{O}_K$ is a Dedekind domain.

Proof. $\mathcal{O}_K$ is a domain because K is. It is Noetherian because any ideal $I \subseteq \mathcal{O}_K$ is a $\mathbb{Z}-$submodule of $\mathcal{O}_K$, which is free by Proposition 2.4.13, so since $\mathbb{Z}$ is a PID, it follows that I is also free, and in particular finitely generated. It is integrally closed by Remark 2.4.8 (note that $K = \text{Frac}(\mathcal{O}_K)$). Lastly, pick a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ and a non-zero class $[a] \in \mathcal{O}_K/\mathfrak{p}$. Since $a \in \mathcal{O}_K$, there are $c_0, ..., c_{n-1} \in \mathbb{Z}$ with

$$a^n + c_{n-1}a^{n-1} + ... + c_0 = 0, \quad c_0 \neq 0, n > 0. \tag{2.20}$$

The natural map $\mathbb{Z} \to \mathcal{O}_K/\mathfrak{p}$ has kernel $\mathfrak{p} \cap \mathbb{Z}$, which is a prime ideal in $\mathbb{Z}$, hence equal to (p) for some prime $p \in \mathbb{Z}$. So we have an inclusion $\mathbb{Z}_p \to \mathcal{O}_K/\mathfrak{p}$, whose image corresponds to the classes of integers. In particular, since $\mathbb{Z}_p$ is a field, any integer coprime with p has an inverse in $\mathcal{O}_K$. Let c_N be the first coefficient coprime with p (if no such N existed, then $[a]$ would be the zero class). We have

$$a^N(a^{n-N} + c_{n-1}a^{n-N-1} + ... + c_N) = 0 \mod \mathfrak{p}. \tag{2.21}$$

Since $\mathfrak{p}$ is prime, $\mathcal{O}_K/\mathfrak{p}$ is a domain, hence we can eliminate a^N and multiply by the inverse of c_N to get

$$-ac_N^{-1}(a^{n-N-1} + c_{n-1}a^{n-N-2} + ... + c_{N+1}) = 1 \mod \mathfrak{p}, \tag{2.22}$$

which is an inverse of a in $\mathcal{O}_K/\mathfrak{p}$, hence it is a field, so $\mathfrak{p}$ is maximal. □

2.4.4 The ideal class group

Definition 2.4.28 (Fractional Ideal)**.** A fractional ideal J of $\mathcal{O}_K$ is a non-zero $\mathcal{O}_K-$submodule $J \subseteq K$ such that $rJ \subseteq \mathcal{O}_K$ for some $r \in \mathcal{O}_K$.

Proposition 2.4.29. The set of fractional ideals of $\mathcal{O}_K$ forms an abelian group denoted J_K. The operation is multiplication of ideals, i.e.

$$IJ := \left\{ \sum_{i=1}^{N} a_i b_i \ : \ a_i \in I, b_i \in J \right\}$$

and the identity element is $\mathcal{O}_K$.

Proof. The only non-obvious point is the existence of inverses. Since any ideal factors into primes, it suffices to exhibit an inverse for a prime ideal $\mathfrak{p}$. Define

$$\mathfrak{p}^{-1} := \{x \in K \ : \ x\mathfrak{p} \subseteq \mathcal{O}_K\}. \tag{2.23}$$

First, we check that $\mathfrak{p}^{-1}$ is fractional ideal. Pick $x, y \in \mathfrak{p}^{-1}$ and $m \in \mathcal{O}_K$. We have

$$mx\mathfrak{p} \subseteq m\mathcal{O}_K \subseteq \mathcal{O}_K, \quad (x+y)\mathfrak{p} \subseteq x\mathfrak{p} + y\mathfrak{p} \subseteq \mathcal{O}_K + \mathcal{O}_K = \mathcal{O}_K, \tag{2.24}$$

so $x + y, mx \in \mathfrak{p}^{-1}$. Hence $\mathfrak{p}^{-1}$ is a $\mathcal{O}_K-$submodule. Now, pick $p \in \mathfrak{p} \setminus \{0\}$. By definition $p\mathfrak{p}^{-1} \subseteq \mathcal{O}_K$, so $\mathfrak{p}^{-1}$ is a fractional ideal. It remain to show that the ideal $\mathfrak{p}\mathfrak{p}^{-1}$ is equal to $\mathcal{O}_K$. Since $\mathcal{O}_K \subseteq \mathfrak{p}^{-1}$, we have $\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}_K$. By maximality of $\mathfrak{p}$, either $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$ or $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$.

Suppose by contradiction the latter holds. For all $x \in \mathfrak{p}^{-1}$, we have $x\mathfrak{p} \subseteq \mathfrak{p}$, so x is integral by Proposition 2.4.2, thus $x \in \mathcal{O}_K$ since $\mathcal{O}_K$ is integrally closed. This means $\mathfrak{p}^{-1} = \mathcal{O}_K$. On the other hand, let $y \in \mathfrak{p} \setminus \{0\}$. We have a factorization $\mathfrak{p}_1 ... \mathfrak{p}_n = (y) \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is prime, one of these factors, say, $\mathfrak{p}_1$, must be equal to $\mathfrak{p}$ (otherwise we would have $x_i \in \mathfrak{p}_i \setminus \mathfrak{p}$ with $x_1 ... x_n \in \mathfrak{p}$, but $\mathfrak{p}$ is prime). Now, pick $b \in \mathfrak{p}_2 ... \mathfrak{p}_n \setminus (a)$ (set $b = 1$ if there are no other factors beside $\mathfrak{p}_1$). Then, $b \notin (a)$ but $b\mathfrak{p} \subseteq (a)$. So $b/a \notin \mathcal{O}_K$ but $b/a\mathfrak{p} \subseteq \mathcal{O}_K$. Thus $b/a \in \mathfrak{p}^{-1} \setminus \mathcal{O}_K$. A contradiction, since we concluded earlier that $\mathfrak{p}^{-1} = \mathcal{O}_K$. Therefore, it must be that $\mathfrak{p}\mathfrak{p}^{-1} \neq \mathfrak{p}$, and therefore equal to $\mathcal{O}_K$. □

Any ideal of $\mathcal{O}_K$ is automatically a fractional ideal. Given $q \in K$, we have the *principal fractional ideal* $(q) = q\mathcal{O}_K := \{qx \ : \ x \in \mathcal{O}_K\}$. For example, in $K = \mathbb{Q}$ we have the principal fractional ideal $(1/2) = \frac{1}{2}\mathbb{Z}$. The set of principal fractional ideals forms a subgroup of J_K denoted I_K. The quotient group

$$Cl_K := J_K/I_K \tag{2.25}$$

is an important invariant of a number field and is called the *ideal class group*. Informally speaking, it measures how far the ring $\mathcal{O}_K$ is from being a PID. For instance, if $\mathcal{O}_K$ is a principal ideal domain, Cl_K is the trivial group as any ideal $(a) \in J_K$ has an inverse $(1/a)$. The following are fundamental results in algebraic number theory. Their proofs are long and technical but can be found at [31].

Theorem 2.4.30. The following hold.

(i) The ideal class group Cl_K is finite,

(ii) The group of units $\mathcal{O}_K^\times$ is finitely generated.

Remark 2.4.31. Oddly enough there often are infinitely many units in $\mathcal{O}_K$. For instance, in $K = \mathbb{Q}(\sqrt{2})$, we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$. The element $\sqrt{2} + 1$ has infinite order, but it also has inverse $\sqrt{2} - 1$. The group of units is generated by $\{-1, \sqrt{2} + 1\}$, so $\mathcal{O}_K^\times \cong \mathbb{Z} \times \mathbb{Z}_2$.

We will now prove that $\mathcal{O}_K$ can be extended to become a PID. Of course, the field K is an example of such an extension. However, it is too big, in the sense that the group of units K^* is not finitely generated. We would like an extension that not only is a PID but also has a finitely generated group of units.

Theorem 2.4.32. There exists a ring $K \supseteq R \supseteq \mathcal{O}_K$ such that (i) R is a PID and (ii) $R^\times$ is a finitely generated group.

Proof. Let $h := h_K$ and let $\{I_1, ..., I_h\}$ be a set of representatives for the classes in Cl_K. Pick $u_j \in I_j \cap \mathcal{O}_K$ for each j and define $u := \prod u_j \in \bigcap I_j$. Let $S := \{1, u, u^2, ...\}$. The set S is closed by multiplication and $1 \in S$, $0 \notin S$. Therefore, we can define the localization $R := \text{loc}_S(\mathcal{O}_K)$. We have $\mathcal{O}_K \subseteq R \subseteq K$. We'll now prove R satisfies the desired properties.

(i) Let $I_R \subseteq R$ be an ideal of R. Then, $I := I_R \cap \mathcal{O}_K$ is an ideal of $\mathcal{O}_K$. Thus, we have $I = (a)I_j$ for some $1 \leq j \leq h$, $a \in K^*$. Now, notice that, since $u \in I_j$, then $1 \in I_jR$, hence $I_jR = R$. We then obtain

$$I_R = IR = (a)I_jR = (a)R. \tag{2.26}$$

Therefore, I_R is generated by (a).

(ii) This is the hard part. It turns out that the set $O_K^\times \cup \{u\} \subseteq R^\times$ is not enough to generate all units. In fact, $R^\times = \{\text{divisors of } u^r \text{ in } \mathcal{O}_K \text{ with } r \geq 0\}$. To show this, pick a unit α/u^s with inverse β/u^t. Then, $\alpha\beta = u^{s+t}$. Conversely, pick a divisor $\alpha\beta = u^s$. Then, $\alpha\left(\beta/u^s\right) = 1$, so α is a unit. Therefore, we must find a finite set of generators for the divisors of u^r. Pick $\alpha\beta = u^r$ and factor $(u) = \mathfrak{p}_1^{e_1}...\mathfrak{p}_N^{e_N}$.

$$(\alpha)(\beta) = (\alpha\beta) = (u^r) = (u)^r = \mathfrak{p}_1^{e_1 r}...\mathfrak{p}_N^{e_N r}. \tag{2.27}$$

By unique factorization of ideals we get

$$(\alpha) = \mathfrak{p}_1^{s_1}...\mathfrak{p}_N^{s_N}, \quad \text{with } s_j \leq e_j r. \tag{2.28}$$

By Lagrange's Theorem, $\mathfrak{p}_j^h$ is the identity element on Cl_K, i.e. a principal fractional ideal. Still, it also is an integral ideal, hence $\mathfrak{p}_j^h = (\gamma_j)$ for some $\gamma_j \in \mathcal{O}_K$. We write $s_j = q_j h + r_j$ with $r_j < h$ in Equation (2.28) to get $(\alpha) = \prod_j (\gamma_j)^{q_j} \mathfrak{p}_j^{r_j}$. Thus, $\prod_j \mathfrak{p}_j^{r_j} = (\gamma)$, where $\gamma := \alpha \prod_j \gamma_j^{-q_j}$. We then have the final decomposition

$$(\alpha) = (\gamma_1)^{q_1} \dots (\gamma_N)^{q_N}(\gamma) = (\gamma_1^{q_1}...\gamma_N^{q_N}\gamma). \tag{2.29}$$

Since these two elements generate the same ideals in $\mathcal{O}_K$, they must differ by multiplication by a unit. So $\alpha = \gamma_1^{q_1}...\gamma_N^{q_N}\gamma\epsilon$, where $\epsilon \in \mathcal{O}_K^\times$. This means we have the following generating set of $R^\times$.

$$R^\times \text{ is generated by } \mathcal{O}_K^\times \cup \{u\} \cup \{\gamma_1, ..., \gamma_N\} \cup \Gamma, \tag{2.30}$$

where Γ contains one generator $\delta_{r_1,...,r_N}$ for each set of indices $r_j < h$ such that the ideal $\mathfrak{p} := \prod_{j=1}^N \mathfrak{p}_j^{r_j}$ is principal and $\mathfrak{p} = (\delta_{r_1,...,r_N})$. The set Γ is clearly finite and $\mathcal{O}_K$ is finitely generated, hence $R^\times$ is finitely generated. □

2.4.5 Valuations

Definition 2.4.33. Let R be a UFD and $p \in R$ a prime element. Any non-zero $x \in \text{Frac}(R)$ can be written in the form $p^n a/b$, where $n \in \mathbb{Z}$ and p doesn't divide a or b. The number n is uniquely determined by x. Define the $p-$adic valuation $v_p : R \to \mathbb{Z} \cup \{\infty\}$ as

$$v_p(x) := n, \quad v_p(0) := \infty.$$

Many problems in number theory have the nice property that they can be solved by analyzing them "one prime at a time". That is, if one can prove a specific local version of the problem concerning a prime p, the original, global version follows easily. This local version often relates to valuations. For example, to prove a non-zero rational number $q \in \mathbb{Q}$ is an integer, it is enough to show that, for any prime $p \in \mathbb{Z}$, we have $v_p(q) \geq 0$. This exact application will be used to prove the Nagell-Lutz Theorem in later chapters. Valuations will also be used to finish the proof of the Mordell-Weil Theorem.

Proposition 2.4.34. A $p-$adic valuation satisfies the following.

$$\begin{array}{llll} \text{(i)} & v_p(x) = \infty \iff x = 0 & \text{(iii)} & v_p(x+y) \geq \min\left(v_p(x), v_p(y)\right) \\ \text{(ii)} & v_p(xy) = v_p(x) + v_p(y) & \text{(iv)} & v_p(x) \neq v_p(y) \Rightarrow v_p(x+y) = \min\left(v_p(x), v_p(y)\right). \end{array}$$

Proof. Properties (i) and (ii) are clear. To show the other two, let $x = p^n a/b$, $y = p^m c/d$ where p does not divide a, b, c, d and $k := \min(m, n)$. Then,

$$x + y = p^k \left(\frac{p^{n-k}ad + p^{m-k}cb}{bd} \right). \tag{2.31}$$

Since p does not divide bd, the valuation of the right-hand side has to be at least k. Moreover, if $m \neq n$, then we may assume $k = n$ and we have $(x+y)/p^k = (ad + p^{m-n}cb)/bd$. The numerator of this expression is not divisible by p, so it has valuation $= 0$. Thus, $v_p(x+y) = k$. □

Proposition 2.4.35. Given a prime $p \in R$ and $\mathfrak{p} := (p)$. We have

$$R_{\mathfrak{p}} = \{x \in \text{Frac}(R) \ : \ v_p(x) \geq 0\}, \quad \mathfrak{p}R_{\mathfrak{p}} = \{x \in \text{Frac}(R) \ : \ v_p(x) > 0\}.$$

Proof. Let $x \in \text{Frac}(R)$. We have that $x \in R_{\mathfrak{p}}$ if and only if $x = a/b$ with $b \notin \mathfrak{p}$, which happens if and only if $v_p(x) \geq 0$. The other equality follows similarly. □

2.4.6 Dedekind zeta function

The last topic of this Section is the Dedekind zeta function, which can be seen as a generalization of the famous Riemann zeta function $\zeta(s)$. Both are examples of what is called a $L-$function. The Riemann zeta function is defined as

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 - p^{-s}\right)^{-1}. \tag{2.32}$$

In the second equality we've written its famous representation as an Euler Product. The summation can be seen as iterating over all the non-zero ideals of $\mathbb{Z}$ (since $\mathbb{Z}$ is a PID, ideals in $\mathbb{Z}$ are the same as integers). By this perspective, we can generalize $\zeta(s)$ to any number field.

Definition 2.4.36 (Dedekind zeta function)**.** Given a non-zero ideal $I \subseteq \mathcal{O}_K$, its norm is defined as $\mathbb{N}I = |\mathcal{O}_K/I|$. The Dedekind zeta function is

$$\zeta_K(s) := \sum_{I \neq 0}^{\infty} \frac{1}{(\mathbb{N}I)^s} = \prod_{I \text{ prime}} (1 - (\mathbb{N}I)^{-s})^{-1}.$$

The Dedekind zeta function is meromorphic and convergent for $\mathrm{Re}(s) > 1$. The quotient $\mathcal{O}_K/I$ is always finite for a non-zero ideal, so the norm operator makes sense. It is also multiplicative (i.e. $\mathbb{N}IJ = (\mathbb{N}I)(\mathbb{N}J)$). Given an ideal $(n) \subseteq \mathbb{Z}$, it is clear that $\mathbb{N}(n) = |\mathbb{Z}/n\mathbb{Z}| = n$. Therefore, $\zeta(s) = \zeta_{\mathbb{Q}}(s)$. We can also consider the extension $\mathbb{Q}(i)/\mathbb{Q}$. Its ring of integers is $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$. The Gaussian zeta function is then defined as $\zeta_{\mathbb{Q}(i)}(s)$. Given an ideal $(\mu) \subseteq \mathbb{Z}[i]$, we have by Proposition 2.1.5 that $\mathbb{N}(\mu) = |\mathbb{Z}[i]/(\mu)| = |\mu|^2$. The Gaussian zeta function is also usually written as

$$\zeta_{\mathbb{Q}(i)}(s) = \frac{1}{4} \sum_{\substack{\mu \in \mathbb{Z}[i] \\ \mu \neq 0}} \frac{1}{|\mu|^{2s}}. \tag{2.33}$$

Notice that the term 1/4 appears merely to avoid overcount, since each non-zero ideal (μ) has four generators, namely $\{\pm\mu, \pm i\mu\}$. Let's find a more convenient formula for $\zeta_{\mathbb{Q}(i)}$ in terms of the usual Riemann zeta function. We already know all the prime ideals in $\mathbb{Z}[i]$. We have

$$\begin{align}
\zeta_{\mathbb{Q}(i)}(s) &= \frac{1}{1-2^{-s}} \prod_{\substack{p \text{ prime} \\ p=4k+1}} \left(\frac{1}{1-p^{-s}}\right)^2 \prod_{\substack{p \text{ prime} \\ p=4k+3}} \frac{1}{1-p^{-2s}} \tag{2.34} \\
&= \frac{1}{1-2^{-s}} \prod_{\substack{p \text{ prime} \\ p=4k+1}} \left(\frac{1}{1-p^{-s}}\right)^2 \prod_{\substack{p \text{ prime} \\ p=4k+3}} \frac{1}{1-p^{-s}} \frac{1}{1+p^{-s}} \tag{2.35} \\
&= \prod_{p \text{ prime}} \frac{1}{1-p^{-s}} \prod_{p \text{ prime}} \frac{1}{1-\chi(p)p^{-s}} = \zeta_{\mathbb{Q}}(s) L(\chi, s). \tag{2.36}
\end{align}$$

Here, χ is an example of a Dirichlet character and is defined as

$$\chi(n) := \begin{cases} 0 & \gcd(n, 4) \neq 1, \\ 1 & n \overset{4}{\equiv} 1, \\ -1 & n \overset{4}{\equiv} 3. \end{cases} \tag{2.37}$$

Notice that this function is multiplicative. The term $L(\chi, s)$ is called the $L-$function attached to the character χ and is defined as

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \text{ prime}} (1 - \chi(n)p^{-s})^{-1}. \tag{2.38}$$

We know $\zeta(s)$ has a simple pole at $s = 1$ with residue 1. It turns out that $L(\chi, s)$ is convergent at $s = 1$, so this tells us $\zeta_{\mathbb{Q}(i)}(s)$ has a simple pole at $s = 1$. We can also calculate the residue explicitly.

Proposition 2.4.37. $\zeta_{\mathbb{Q}(i)}(s)$ has a simple pole at $s = 1$ with residue equal to $\pi/4$.

Proof. We have

$$\lim_{s\to 1}(s-1)\zeta(s)L(\chi, s) = L(\chi, 1) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \ldots = \sum_{n\geq 0} \frac{(-1)^n}{2n+1}.$$

This sum can be readily calculated by methods of calculus. More concretely,

$$\sum_{n\geq 0} \frac{(-1)^n}{2n+1} = \sum_{n\geq 0} \int_0^1 (-x^2)^n dx = \int_0^1 \sum_{n\geq 0} (-x^2)^n dx = \int_0^1 \frac{1}{1+x^2} dx = \arctan x \Big|_0^1 = \pi/4.$$

In the second equality we used the Dominated Convergence Theorem to exchange integral with summation. □

Chapter 3

Elliptic curves

Elliptic curves are abstractly defined as smooth projective curves of genus 1 with a specified point (often called $\mathcal{O}$). As a consequence of the Riemann-Roch Theorem (see [35, Section III.3]), any elliptic curve E over a field of characteristic zero can be written as the vanishing set of a single homogeneous equation in three variables

$$y^2z = x^3 + Ax^2z + Bxz^2 + Cz^3. \tag{3.1}$$

Notice that the only point outside the affine chart $z = 1$ is $[0 : 1 : 0]$. Such an equation is called a *Weierstrass equation*. An elliptic curve given by such an equation is said to be in *Weierstrass form*. The point $[0 : 1 : 0]$ is usually denoted $\mathcal{O}$. For this work, we are interested in the arithmetic aspects of elliptic curves, thus we consider only the case where the coefficients A, B, C are integers. By dehomogenizing (3.1), we arrive at the following definition.

Definition 3.0.1. An elliptic curve E in Weierstrass form is the set of complex solutions to the equation

$$E : y^2 = F(x) = x^3 + Ax^2 + Bx + C,$$

together with a "point at infinity" $\mathcal{O}$, where $F(x) \in \mathbb{C}[x]$ has distinct complex roots. Moreover, we say E is defined over R, for some ring $R \subseteq \mathbb{C}$, if $F(x) \in R[x]$.

In this work, the term elliptic curve will always mean an elliptic curve in Weierstrass form. Also, unless stated otherwise, all elliptic curves will be assumed to be defined over $\mathbb{Z}$. The condition that $F(x)$ must have three distinct complex roots is equivalent to the curve being smooth. If we plot the real points $E \cap \mathbb{R}^2$, the image will be like one of the two curves in Figure 3.1.

As we said in the Introduction, a surprising property of elliptic curves is that the set of rational points

$$E(\mathbb{Q}) := E \cap (\mathbb{Q}^2 \cup \{\mathcal{O}\}) \tag{3.2}$$

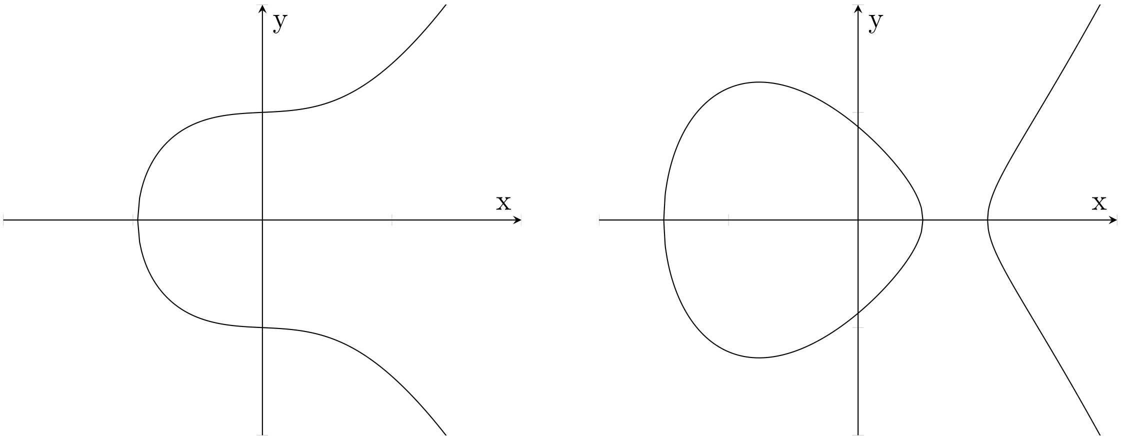
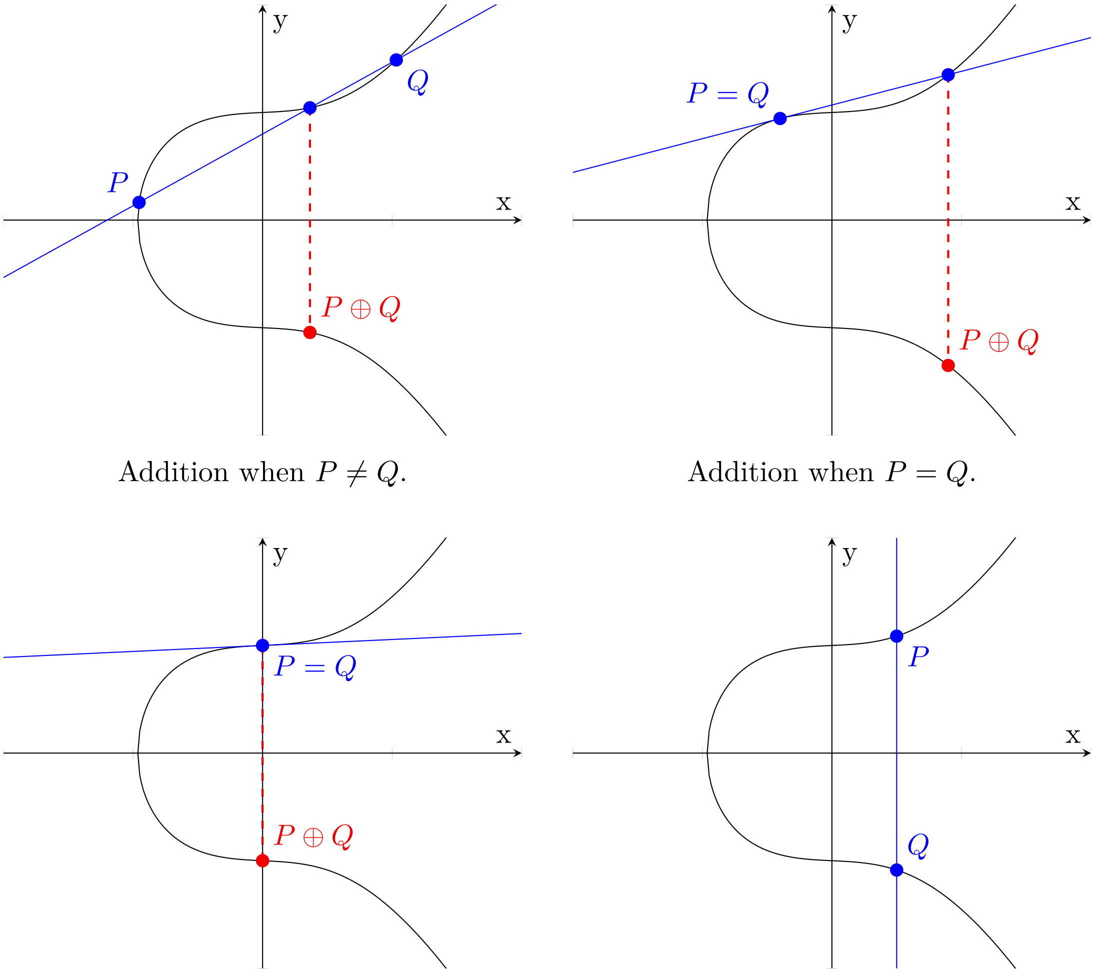


Figure 3.1: Graphs of elliptic curves.

forms an abelian group, where $\mathcal{O}$ is the identity element. The group law is a consequence of Bezout's Theorem: given two distinct points $P, Q \in E(\mathbb{Q})$, the unique line L passing through P and Q must intersect E at a third point H. Since P, Q are rational points and E is given by rational (in fact, integer) coefficients, it follows that H must be a rational point as well. When $P = Q$, we can still find a point H in the same way, by taking the line L as the tangent line at P. The group structure is then described as follows: (i) the point $\mathcal{O}$ is the identity element, (ii) the inverse of a point $H = (h_1, h_2)$ is defined as $-H := (h_1, -h_2)$, (iii) the group operation is $P \oplus Q := -H$. The group law is explained geometrically in Figure 3.2.

Consider any subfield $K \subseteq \mathbb{C}$. We denote by $E(K) := E \cap (K^2 \cup \{\mathcal{O}\})$ the set of $K-$rational points of E. The same procedure just described still works for the field K, and thus $E(K)$ also forms an abelian group. In particular we have the chain of subgroups $E(\mathbb{Q}) \subseteq E(K) \subseteq E(\mathbb{C})$. In this work, we are interested in $E(\mathbb{Q})$, $E(\mathbb{C})$, and $E(K)$ when K is a number field. Since the group law is defined as intersections of lines and curves, we can find explicit formulas for it in terms of the coefficients A, B, C appearing in the equation for E and the coordinates for P, Q:



Addition when $P \neq Q$.

Addition when $P = Q$.

When $P = Q$ is an inflection point, $P \oplus Q = -P$.

When $P = -Q$, the line L is a vertical line, passing through $\mathcal{O}$ at infinity.

Figure 3.2: The group law of an elliptic curve.

Proposition 3.0.2. Let E be an elliptic curve defined over K, where $K \subseteq \mathbb{C}$ is a subfield. Then, $(E(K), \oplus, \mathcal{O})$ is an abelian group. The group law is defined as follows. Let $P_1, P_2 \in E(K) \setminus \{\mathcal{O}\}$ be $K-$rational points, $P = (x_1, y_1), Q = (x_2, y_2)$.

(i) The inverse operator is $-P := (x_1, -y_1)$.

(ii) For $P \neq -Q$, we write $P \oplus Q = (x_3, y_3)$ with

$$\begin{aligned} x_3 &:= u^2 - A - x_1 - x_2, \\ y_3 &:= ux_3 + (y_1 - ux_1), \end{aligned} \qquad u := \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } P \neq Q, \\ (3x_1^2 + 2Ax_1 + B)/2y_1 & \text{if } P = Q. \end{cases}$$

We write nP to denote $\overbrace{P \oplus ... \oplus P}^{n \text{ times}}$. Given $P = (x_1, y_1) \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$, the formula for $2P = (x_2, y_2)$ is often called the *duplication formula* and is written below.

$$x_2 = u^2 - A - 2x_1, \quad y_2 = ux_2 + (y_1 - ux_1). \tag{3.3}$$

Notice that $P, Q, H \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$ are collinear points if and only if $P \oplus Q = -H$, or, in other words, $P \oplus Q \oplus H = \mathcal{O}$. This is a particular fact about elliptic curves in Weierstrass form, i.e. given by equation (3.1).

Proposition 3.0.3. Let E be an elliptic curve and $P, Q, H \in E(\mathbb{C})$. Then,

$$P \oplus Q \oplus H = \mathcal{O} \iff P, Q, H \text{ are collinear.}$$

Proof. If $P, Q, H \neq \mathcal{O}$, this is evident by the definition of the group law. If, say, $P = \mathcal{O}$, then $Q = -H$, thus they have the same x coordinate, say, x_0. Then, the line parametrized by $\phi : \mathbb{P}^1 \to \mathbb{P}^3, \phi(a, b) := [x_0 b : a : b]$ clearly passes through P, Q and $\mathcal{O} = [0 : 1 : 0]$. □

We now prove some general useful facts about elliptic curves. Let $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ be the standard $p-$adic valuation defined in 2.4.33. It turns out that the Weierstrass equation imposes a tight condition on the valuation of the coordinates of a rational point.

Proposition 3.0.4. If $v_p(x) < 0$ or $v_p(y) < 0$, then there is some $r \geq 1$ such that $v_p(x) = -2r$ and $v_p(y) = -3r$.

Proof. First of all, suppose that $v_p(y) < 0$. Then, $0 > 2v_p(y) = v_p(y^2) = v_p(x^3 + Ax^2 + Bx + C) \geq \min(v_p(x^3), v_p(A) + v_p(x^2), v_p(B) + v_p(x), v_p(C))$. Since $v_p(A), v_p(B), v_p(C) \geq 0$, this can only be true if $v_p(x) < 0$. So we've reduced the problem to the case where $v_p(x) < 0$. In this case, we have an equality $2v_p(y) = v_p(x^3) = 3v_p(x)$ since $v_p(x^3)$ is strictly less than $v_p(Ax^2 + Bx + C)$. So, there must be some $r \geq 1$ such that $v_p(y) = -3r$ and $v_p(x) = -2r$. And this completes the proof. □

Corollary 3.0.5. Let E be an elliptic curve and $P = (x, y) \in E(\mathbb{Q})$. Then, there are $a, b, c \in \mathbb{Z}$, $c \neq 0$, such that

$$(x, y) = (a/c^2, b/c^3), \quad \gcd(a, c) = \gcd(b, c) = 1.$$

Proof. Write $(x, y) = (a/c_1, b/c_2)$, both in lowest terms. Proposition 3.0.4 says that any prime dividing c_1 or c_2 must occur exactly $2r$ times in c_1 and $3r$ times in c_2. This means there is some integer c such that $c_1 = c^2, c_2 = c^3$. □

We now discuss the discriminant Δ of the polynomial $F(x)$, which is given by

$$\Delta = -4B^3 - 27C^2 - 4A^3C - 27C^2 + 18ABC + A^2B^2. \tag{3.4}$$

As we know, $F(x)$ has three distinct complex roots if and only if $\Delta \neq 0$. A classic formula relates the discriminant of any polynomial to the resultant of itself with its derivative,

$$\Delta = \frac{(-1)^{n(n-1)/2}}{a_n} \mathrm{Res}(F, F'), \tag{3.5}$$

where n is the degree of $F(x)$ and a_n the leading coefficient. In our case, $a_n = 1$ since $F(x)$ is monic, and $n = 3$, thus $\Delta = -\mathrm{Res}(F, F')$. It is a standard fact that the resultant of two polynomials belongs to the ideal generated by them. Therefore, there must be a way to write Δ as a combination of F and F'.

$$H(x)F(x) + S(x)F'(x) = \Delta. \tag{3.6}$$

It is not difficult to find explicit formulas for $H(x)$ and $S(x)$. To understand the calculations better, it's a good idea to write $F(x), F'(x)$ as general polynomials. Let

$$\begin{array}{rcl|rcl} F'(x) & = & q_2x^2 + q_1x + q_0, & H(x) & = & h_1x + h_0, \\ F(x) & = & p_3x^3 + p_2x^2 + p_1x + p_0, & S(x) & = & s_2x^2 + s_1x + s_0. \end{array}$$

The equality $H(x)F(x) + S(x)F'(x) = \Delta$ translates to a linear system on the coefficients.

$$\overbrace{\begin{bmatrix} p_0 & 0 & q_0 & 0 & 0 \\ p_1 & p_0 & q_1 & q_0 & 0 \\ p_2 & p_1 & q_2 & q_1 & q_0 \\ p_3 & p_2 & 0 & q_2 & q_1 \\ 0 & p_3 & 0 & 0 & q_2 \end{bmatrix}}^{S^t} \overbrace{\begin{bmatrix} h_0 \\ h_1 \\ v_0 \\ v_1 \\ v_2 \end{bmatrix}}^{\omega} = \begin{bmatrix} \Delta \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \Delta e_1,$$

where e_1 is the canonical base vector. The matrix S^t on the left-hand side is precisely the transpose of the Sylvester matrix S of F and F'. By definition, $\mathrm{Res}(F, F') = \det(S)$. We can then multiply by the cofactor matrix $\mathrm{cof}(S)$ to obtain

$$\mathrm{Res}(F, F')\omega = \mathrm{cof}(S)S^t\omega = \mathrm{cof}(S)\Delta e_1 = -\mathrm{Res}(F, F')\mathrm{cof}(S)e_1. \tag{3.7}$$

Since $\mathbb{Z}$ is a domain, we may cancel $\mathrm{Res}(F, F')$ on both sides to obtain $\omega = -\mathrm{cof}(S)e_1$. So the coefficients of $H(x)$ and $S(x)$ are precisely given by minus the first column of the cofactor matrix of S. By calculating this term we obtain the following.

Proposition 3.0.6. There are $H(x), S(x) \in \mathbb{Z}[x]$ such that

(i) $H(x) = (18B - 6A^2)x + (15AB - 27C - 4A^3)$,

(ii) $S(x) = (2A^2 - 6B)x^2 + (9C + 2A^3 - 7AB)x + (A^2B + 3AC - 4B^2)$,

(iii) $H(x)F(x) + S(x)F'(x) = \Delta$.

The last topic in this section is *reductions*. Let $E : y^2 = x^3 + Ax^3 + Bx^2 + C$ be an elliptic curve, p a prime number and $q = p^r$ for some $r \geq 1$. Since A, B, C are integers, we can define the set

$$E(\mathbb{F}_q) := \{(x, y) \in \mathbb{F}_q \ : \ y^2 = x^3 + Ax^3 + Bx^2 + C\} \cup \{\mathcal{O}\}, \tag{3.8}$$

where $\mathbb{F}_q$ is the finite field of q elements, and the coefficients A, B, C are taken modulo p. This set is known as the *reduction of E to the finite field $\mathbb{F}_q$*. This defines a new algebraic curve, now over the field $\mathbb{F}_q$, which can have singular points or not. If it is singular, we call the prime p a *bad prime*, if not, we call it a *good prime*. It is not difficult to prove that a prime is bad if and only if it divides Δ.

We'll sometimes consider the set

$$E(\mathbb{F}_q)_{\text{ns}} := \{P \in E(\mathbb{F}_q) \ : \ P \text{ is non-singular}\}. \tag{3.9}$$

This set will always be an abelian group, regarless if the underlying curve is singular or not. Its group law can be calculated in the same way as in Proposition 3.0.2. If the curve is non-singular, then $E(\mathbb{F}_q) = E(\mathbb{F}_q)_{\text{ns}}$ is a group and is called an *elliptic curve over $\mathbb{F}_q$*.

3.1 Elliptic functions

Elliptic curves are closely related to the notion of elliptic functions. In this section, we define them and investigate some of their properties. From now on, we call a set Λ a *lattice* if it is any set of the form

$$\lambda_1\mathbb{Z} + \lambda_2\mathbb{Z} \subseteq \mathbb{C}, \tag{3.10}$$

where $\lambda_1, \lambda_2 \in \mathbb{C}$ are linearly independent over $\mathbb{R}$.

Definition 3.1.1. An elliptic function $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ with respect to a lattice Λ is a meromophic function that is *doubly periodic*, that is, $f(z+\lambda_i) = f(z)$ for $i = 1, 2$.

The doubly periodic property is clearly equivalent to $f(z + \lambda) = f(z)$ for all $\lambda \in \Lambda$. From now on, we will not mention the lattice Λ unless there is potential for confusion. The following result shows why we require the function to be meromorphic.

Proposition 3.1.2. Any holomorphic elliptic function is constant.

Proof. Let f be such a function. It must attain a maximum at the compact parallelogram $P := \{a\lambda_1 + b\lambda_2 \ : \ 0 \leq a, b \leq 1\}$, i.e. there is some constant $M > 0$ with $|f(z)| < M$ for all $z \in P$. But since f is invariant under translation by λ_1, λ_2, the constant M is a global bound. Hence f a bounded holomorphic function and thus constant by Liouville's Theorem. □

There are no simple examples of elliptic functions. The simplest ones are expressed as infinite sums of the form

$$f_n(z) := \sum_{\lambda \in \Lambda} \frac{1}{(z+\lambda)^n}, \quad n \geq 3. \tag{3.11}$$

These functions are clearly doubly-periodic and can be shown to converge uniformly in compact sets outside Λ, and thus define a holomorphic function in $\mathbb{C} \setminus \Lambda$. It becomes a meromorphic function upon checking the points in Λ are poles (and not essential singularities). The same formula doesn't work for $n = 1, 2$, since the corresponding function is not convergent. However, it is possible to include correction terms to ensure convergence. We arrive at

$$\wp(z) := \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}, \quad \zeta(z) := \frac{1}{z} + \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{z+\lambda} - \frac{1}{\lambda} + \frac{z}{\lambda^2}. \tag{3.12}$$

These are called, respectively, the Weierstrass $\wp$ function and the Weierestrass zeta function. The function $\wp(z)$ is the most important example of elliptic function. In fact, although we'll not need this result, any elliptic function can be written as a rational function in $\wp(z)$ and $\wp'(z)$. The proof of convergence of $\wp$ is very similar to some calculations we'll do in the last chapter, so it was included below. The function $\zeta(z)$ is not an elliptic function, for it is not doubly periodic. However, it satisfies the property

$$\zeta(z+\lambda) - \zeta(z) = 2\zeta(\lambda/2), \quad \forall \lambda \notin 2\Lambda. \tag{3.13}$$

In other words, it is doubly periodic up to a term that depends only on the lattice points.

Lemma 3.1.3. The series

$$\sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^k}$$

converges absolutely for $k > 2$.

Proof. Here, we separate the sum into two parts. We have

$$\begin{aligned} \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{|\lambda|^k} &= \sum_{(m,n) \neq (0,0)} \frac{1}{|m\lambda_1 + n\lambda_2|^k} \\ &= \sum_{\substack{(m,n) \neq (0,0) \\ |m| \geq |n|}} (...) + \sum_{|m|<|n|} (...). \end{aligned}$$

We'll show the first term converges. The convergence of the second term is analogous. Let $L \subseteq \mathbb{C}$ be the compact line segment connecting λ_1 and $\lambda_1 + \lambda_2$.

$$\sum_{\substack{(m,n) \neq (0,0) \\ |m| \geq |n|}} \frac{1}{|m\lambda_1 + n\lambda_2|^k}$$

$$\begin{aligned}
&= \sum_{m\in\mathbb{Z}\setminus\{0\}} \sum_{\substack{|n|\leq|m| \\ (m,n)\neq(0,0)}} \frac{1}{|m\lambda_1+n\lambda_2|^k} && \text{(Change indexing)} \\
&= \sum_{m\in\mathbb{Z}\setminus\{0\}} \sum_{\substack{|n|\leq|m| \\ (m,n)\neq(0,0)}} \frac{1}{m^k}\frac{1}{|\lambda_1+(n/m)\lambda_2|^k} && \text{(Extract } m\text{)} \\
&\leq \sum_{m\in\mathbb{Z}\setminus\{0\}} \sum_{\substack{|n|\leq|m| \\ (m,n)\neq(0,0)}} \frac{\max|L|^{-k}}{m^k} && (n/m<1, \text{ so } \lambda_1+(n/m)\lambda_2\in L) \\
&\leq \sum_{m\in\mathbb{Z}\setminus\{0\}} \frac{(\max|L|^{-k})(2m+1)}{m^k} && \text{(Inner sum does not depend on } n\text{).}
\end{aligned}$$

The summand is $\mathcal{O}(m^{k-1})$ with $k>2$, so it converges. □

Proposition 3.1.4. The Weierstrass $\wp$ function is meromorphic with poles of order 2 at each point in Λ.

Proof. We first show the sum converges uniformly on compact sets outside Λ. Let $K\subseteq\mathbb{C}$ be some compact set with $K\cap\Lambda=\varnothing$. Let $R=\sup|K|$. We have the following bound for $\lambda\in\Lambda\setminus\{0\}$ and $z\in K$.

$$\left|\frac{\lambda}{z-\lambda}\right| = \frac{|\lambda|}{|\lambda||z/\lambda-1|} = \frac{1}{|z/\lambda-1|},$$

which goes uniformly to one as $|\lambda|\to\infty$ (since K is bounded), so there must be some constant $M>0$ with $|z-\lambda|\geq|\lambda|/M$. With this, we can bound the summand on $\wp$.

$$\left|\frac{1}{(z-\lambda)^2}-\frac{1}{\lambda^2}\right| = \left|\frac{z(2\lambda-z)}{\lambda^2(z-\lambda)^2}\right| \leq \frac{RM(2|\lambda|+R)}{|\lambda|^4} = \frac{RM(2+R/|\lambda|)}{|\lambda|^3}.$$

This term is of order 3 on λ. Convergence is thus a consequence of Lemma 3.1.3. This ensures $\wp$ is holomorphic on $\mathbb{C}\setminus\Lambda$. To show Λ consists of poles of order two, simply note that inside any region A containing a single lattice point λ, we may remove the term $1/(z-\lambda)^2$ from the summation to obtain a holomorphic function f on $A\setminus\{\lambda\}$. Then we have $\wp|_A = f+1/(z-\lambda)^2$ which is meromorphic with a pole of order two at $z=\lambda$. □

Proposition 3.1.5. The Weierstrass $\wp$ function has the following Taylor expansion at $z=0$, with radius of convergence $r=\min\{|\lambda|\ :\ \lambda\in\Lambda\}$.

$$\wp(z) = \frac{1}{z^2}+\sum_{n\geq1}(2n+1)G_{2n+2}z^{2n}, \quad G_n := \sum_{\lambda\in\Lambda\setminus\{0\}}\frac{1}{\lambda^n}.$$

Proof. For $|z| < r$, we have $|z/\lambda| < 1$ for all $\lambda \in \Lambda$. We use the Taylor series

$$\frac{1}{(1-x)^2} = \sum_{n=1}^{\infty} nx^{n-1} \quad (|x| < 1) \tag{3.14}$$

to arrive at

$$\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} = \frac{1}{\lambda^2}\left(\frac{1}{(1-z/\lambda)^2} - 1\right) = \sum_{n=1}^{\infty}(n+1)(z/\lambda)^n.$$

We then get

$$\wp(z) = \sum_{\lambda \in \Lambda \setminus \{0\}} \sum_{n=1}^{\infty}(n+1)(z/\lambda)^n = \sum_{n=1}^{\infty}(n+1)G_n z^n.$$

Here we exchanged the order of summation, which is allowed since everything converges absolutely. Notice that $G_n = 0$ for odd n by symmetry of the lattice. Thus we only need to consider $n \geq 2$ even. This completes the proof. □

Note that elliptic functions form a vector space. Moreover, if f is some elliptic function, then f' also is. Using this and the Taylor series we've just calculated, we arrive at the connection between $\wp(z)$ and elliptic curves.

Proposition 3.1.6. The function $\wp(z)$ satisfies the functional equation

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

Proof. Around $z = 0$, we expand the constant term and the non-holomorphic part of the following Taylor expansions.

$$\wp(z) = z^{-2} + (...), \tag{3.15}$$

$$\wp(z)^3 = z^{-6} + 9G_4z^{-2} + 15G_4 + (...), \tag{3.16}$$

$$\wp'(z)^2 = 4z^{-6} - 24G_4z^{-2} - 80G_4 + (...). \tag{3.17}$$

From this, we can see that $\wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z)$ has no poles, and hence is a holomorphic elliptic function. By Proposition 3.1.2, it must be constant and thus equal to the constant term of its Taylor expansion, which is $-140G_6$. This completes the proof. □

An important consequence of Proposition 3.1.6 is that it gives us a mapping ϕ_Λ from the torus $\mathbb{C}/\Lambda$ to the elliptic curve $E_\Lambda : y^2z = x^3 - 15G_4xz^2 - 35G_6z^3$ defined by

$$\phi_\Lambda([z]) := \begin{cases} [\wp(z) : 2\wp'(z) : 1] & \text{if } z \notin \Lambda, \\ [0 : 1 : 0] & \text{if } z \in \Lambda. \end{cases} \tag{3.18}$$

It is also possible to construct a map in the other direction, first consider any elliptic curve $E \subseteq \mathbb{C}$. Choose any basis $\{\delta_1, \delta_2\}$ of $H_1(E, \mathbb{Z})$ and define the lattice $\Lambda_E := \mathbb{Z} \int_{\delta_1} 2dx/y + \mathbb{Z} \int_{\delta_2} 2dx/y$. Then, we have a (well-defined) map $\psi_E : E \to \mathbb{C}/\Lambda$ given by

$$\psi_E(P) := \int_{\mathcal{O}}^{P} 2dx/y. \tag{3.19}$$

The surprising fact is that these two maps admit a lot of strucutre and are inverses of each other. This establishes a correspondence between complex tori and elliptic curves and is known as the Weierstrass Uniformization Theorem.

Theorem 3.1.7 (Weierstrass Uniformization Theorem)**.** Given any lattice Λ and any elliptic curve E, the maps ϕ_Λ and ψ_E are an isomorphism of Riemann surfaces and also group isomorphisms (when considering the natural structure of $\mathbb{C}/\Lambda$ as an additive group) with inverses

$$(\phi_\Lambda)^{-1} = \psi_{E_\Lambda}, \quad (\psi_E)^{-1} = \phi_{\Lambda_E}.$$

3.2 The Hasse-Weil $L-$function

L-functions (sometimes called zeta functions) are meromorphic functions that appear in a plethora of different contexts in mathematics. The simplest example is the Riemann zeta function $\zeta(s)$. In Section 2.4.6 we saw the zeta function $\zeta_K(s)$ associated to a number field K. Given a additive character $\chi : \mathbb{F}_p \to \mathbb{C}$, there is a way to build a L-function $L(\chi, s)$ (which, in particular, was used by Dirichlet to prove there are infinitely many primes in any arithmetic progression $an + b$, where $\gcd(a, b) = 1$). There are also L-functions associated to modular forms, elliptic curves, and many more mathematical objects. Some of these functions are related to very important unsolved problems including the Langlands Program, the Riemann Hypothesis, and the BSD Conjecture. There isn't a formal, all-embracing definition of L-functions, although there are works which try to come up one [14].

One remarkable property of L-functions, at least for those associated to algebraic objects, is that their Laurent expansions are often closely related to important algebraic invariants of the original object. The simplest case is that of $\zeta_K(S)$. We saw that $\zeta_{\mathbb{Q}(i)}(s)$ has a pole at $s = 1$, but it turns out this is the case for any number field K, and the residue at that point can be expressed as product of various important invariants of K, including its class number. More explicitly,

$$\lim_{s \to 1} (s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} R_K h_K}{\omega_K \sqrt{|d_K|}}. \tag{3.20}$$

This formula is known as the *analytic class number formula*, because it relates the class number h_K, an algebraic quantity, to the residue of a meromorphic function, an analytic quantity. We won't delve into what these symbols mean, but rather use this equation as an example of how one can recover algebraic information by analyzing the corresponding L-function. Given an elliptic curve E, we'll later properly define $L(E,s)$. There is an analogous (conjectural) analytic class number formula for $L(E,s)$, known as the BSD Formula. The validity of this formula is one of the stronger versions of the BSD conjecture, which we won't discuss further in this work. In Chapter 6 we'll see how $L(E,s)$ is related to a very important invariant of $E(\mathbb{Q})$ known as its *rank*.

In this section we simply aim to define $L(E,s)$. Informally, we want to clump together information about $E(F)$ for each finite field F into one big meromorphic function. As pointed out by John Baez in a great blog post [2], often in expository works $L(E,s)$ is defined in a confusing and obscure way. To avoid this, we'll first build a series of different L-functions which get more and more refined.

Definition 3.2.1. Given a sequence $N = \{N_r\}_{r\geq 1}$ of complex numbers, define its associated zeta function as the formal power series

$$\zeta(N,T) := \exp\left(\sum_{r=1}^{\infty} \frac{N_r}{r} T^r\right), \quad \text{where } \exp(u) := \sum_{n=1}^{\infty} \frac{u^n}{n!}.$$

From the definition it is clear that if M, N are sequences of complex numbers,

$$\zeta(M+N,T) = \zeta(M,T)\zeta(N,T). \tag{3.21}$$

Proposition 3.2.2. Let $A = \{\gamma\alpha^r\}_{r\geq 1}$, where $\alpha \in \mathbb{C}$, $\gamma \in \mathbb{Z}$. Then, $\zeta(A,T)$ converges to $(1-\alpha T)^{-\gamma}$ with radius of convergence $\geq |\alpha|^{-1}$.

Proof. Here we simply use the Taylor series $\sum x^r/r = -\log(1-x)$. We have

$$\zeta(A,T) = \exp\left(\gamma \sum_{r=1}^{\infty} (\alpha T)^r/r\right) = \exp(-\gamma \log(1-\alpha T)) = (1-\alpha T)^{-\gamma}.$$

The radius of convergence for the Taylor series is 1. Therefore this equality holds for $|T| < |\alpha|^{-1}$. This completes the proof. □

Corollary 3.2.3. For all $\alpha, \beta, z \in \mathbb{C}$ with $|z| < \min(|\alpha|^{-1}, |\beta|^{-1})$,

$$\zeta(\{\alpha^r - \beta^r\}_{r\geq 1}, z) = (1-\beta z)/(1-\alpha z).$$

Proof. Simply apply Equation (3.21) followed by Proposition 3.2.2. □

Let E be an elliptic curve. The first step is to construct what is called the Hasse-Weil zeta function $\zeta(E,s)$. It is built by taking the product over *local* zeta functions $\zeta_p(E,s)$ for each prime p, which in turn are built by packaging information about $E(\mathbb{F}_{p^r})$ for each $r \geq 1$. Therefore, $\zeta(E,s)$ contains information about $E(F)$ for every single finite field F.

Definition 3.2.4. Let p a prime number. Define the *local* (Hasse-Weil) zeta function associated to (E,p) as

$$\zeta_p(E,s) := \zeta(\{\#E(\mathbb{F}_{p^r})\}_{r\geq 1}, p^{-s}) = \exp\left(\sum_{r=1}^{\infty} \frac{\#E(\mathbb{F}_{p^r})}{r} p^{-sr}\right).$$

Definition 3.2.5. Define the Hasse-Weil zeta function associated to E as

$$\zeta(E,s) := \prod_{p \text{ prime}} \zeta_p(E,s).$$

The function $\zeta(E,s)$ is almost the $L-$function of E. To motivate the last upcoming modification, consider the following table of point counts for the curve $E : y^2 + y = x^3 + x$ (which, even though it is not presented in Weierstrass form, is still a smooth curve of genus 1 and thus an elliptic curve).

r	1	2	3	4	5	6	7	8	9	10	11	12
2^r	2	4	8	16	32	64	128	256	512	1024	2048	4096
$\#E(\mathbb{F}_{2^r})$	5	5	5	25	25	65	145	225	545	1025	1985	4225

Table 3.1: Point counts for $E : y^2 + y = x^3 + x$, taken from [2].

Notice that the point counts for finite fields $\mathbb{F}_{2^r}$ seem to be almost equal to 2^r minus a "correction term". This pattern in fact occurs when counting the number of points of any elliptic curve over any finite field (i.e. $\#E(\mathbb{F}_{p^r})$ is p^r minus a small correction term). It would then be a good idea to extract out the "predictable" part and keep only the correction. That is essentially $L(E,s)$. The only difference is that, for abstract reasons, it will be better to extract the term $p^r + 1$ instead of p^r. Let's actually calculate it. We define the correction term as

$$c_p(E,r) := p^r + 1 - \#E(\mathbb{F}_{p^r}). \tag{3.22}$$

We have

$$\begin{aligned} & \zeta(E,s) \\ = \quad & \prod_p \zeta_p(E,s) && \text{(Definition of } \zeta(E,s)\text{)} \\ = \quad & \prod_p \zeta(\{\#E(\mathbb{F}_{p^r})\}, p^{-s}) && \text{(Definition of } \zeta_p(E,s)\text{)} \end{aligned}$$

$$
\begin{aligned}
&= \prod_p \zeta(\{p^r + 1 + c_p(E,r)\}, p^{-s}) && \text{(Definition of } c_p(E,r)\text{)}\\
&= \prod_p \zeta(\{p^r\}, p^{-s}) \cdot \zeta(\{1\}, p^{-s}) \cdot \zeta(\{c_p(E,r)\}, p^{-s}) && \text{(Equation (3.21))}\\
&= \prod_p (1-p^{1-s})^{-1}(1-p^{-s})^{-1}\zeta(\{c_p(E,r)\}, p^{-s}) && \text{(Proposition 3.2.2)}\\
&= \zeta(s-1)\zeta(s)\prod_p \zeta(\{c_p(E,r)\}, p^{-s}) && \text{(Euler Product (2.32)).}
\end{aligned}
$$

The remaining terms on the product will be taken (for historical reasons) to be the reciprocal of the *local* $L-$function $L_p(E,s)$.

Definition 3.2.6. Let p be a prime number. Define the *local* (Hasse-Weil) $L-$function associated to it as

$$L_p(E,s) = 1/\zeta(\{c_p(E,r)\}_{r\geq 1}, p^{-s}) = \exp\left(-\sum_{r=1}^{\infty}\frac{c_p(E,r)}{r}p^{-sr}\right).$$

Definition 3.2.7. Define the Hasse-Weil $L-$function associated to E as

$$L(E,s) = \prod_{p \text{ prime}} L_p(E,s).$$

We then get the correspondence between the zeta function and $L-$function of E.

$$\zeta(E,s) = \frac{\zeta(s-1)\zeta(s)}{L(E,s)}. \tag{3.23}$$

The function $L(E,s)$ can be shown to converge for $\mathrm{Re}(s) > 3/2$, thus (since it is a power series on p^{-s}) defining a holomorphic function on the corresponding domain. It turns out that $L(E,s)$ admits a meromorphic continuation to the whole complex plane. This was proven by Deuring [11] for curves that admit what is called "complex multiplication". The general case is due to the Arithmetic Modularity Theorem [12]. Thus, it makes sense to talk about the order of vanishing of $L(E,s)$ at $s=1$. As we'll discuss in future chapters, this number turns out to be closely related to important invariants of the elliptic curve, and understanding this relation is what the BSD Conjecture entails.

To construct explicitly the meromorphic continuation is not an easy task. In Chapter 6 we'll build a continuation to $\mathrm{Re}(s) > 1/2$ for a specific family of elliptic curves. This will allow us to explicitly compute $L(E,1)$ and produce tangible, numerical evidence for the BSD Conjecture.

Chapter 4

The rank and the Mordell-Weil Theorem

Notation 4.0.1. In what follows, we let $E : y^2 = F(x)$, with $F(x) = x^3 + Ax^2 + Bx + C$, be an elliptic curve with $A, B, C \in \mathbb{Z}$ and e_1, e_2, e_3 the roots of $F(x)$. We write Δ for the discriminant of E. Define $Q := \mathbb{Q}(e_1, e_2, e_3)$, i.e. the splitting field of $F(x)$ over $\mathbb{Q}$.

We begin our study of the group $E(\mathbb{Q})$ with the fundamental result by Mordell, which was later generalized by Weil to $E(K)$, where K is an arbitrary number field [44].

Theorem 4.0.2 (Mordell-Weil)**.** The group $E(\mathbb{Q})$ is finitely generated.

Our proof will be based on the book by Knapp [21] and is essentially elementary, requiring some algebraic number theory only at the last step. For a sketch of the original proof by Mordell, see [30]. The theorem still holds when considering the group $E(K)$, where K is a number field [35]. In this case, the argument requires a more refined knowledge of the theory of heights.

As a consequence of the Fundamental Theorem of Finitely Generated Abelian Groups, Theorem 4.0.2 implies that $E(\mathbb{Q})$ is of the form

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}. \tag{4.1}$$

The term $E(\mathbb{Q})_{\text{tors}}$ is a finite group called the *torsion subgroup of* $E(\mathbb{Q})$. Surprisingly, there are only 15 possibilities for $E(\mathbb{Q})_{\text{tors}}$ and it can be computed explicitly in finite time. A complete description of such an algorithm will be given in Chapter 5. The value r is much more elusive and is called the (Mordell-Weil) *rank of the curve E*. Currently, there is no general algorithm for computing r, and many simple questions about its nature remain unanswered. For example, we do not know which values of r can exist, or whether or not there are elliptic curves of arbitrarily high rank. Much research is done on finding elliptic curves of high ranks. Currently, the largest known rank is ≥ 29 and was discovered by Elkies (see [13] for an extensive list of rank records). The rank r is also related to the famous BSD Conjecture, which will be discussed in Chapter 6. In Section 4.3, we'll see an algorithm called *descent by* $2-$*isogeny* that calculates lower and upper bounds for r, i.e. numbers a, b such that $r \in [a, b]$, provided $E(\mathbb{Q})$ has a point of order 2. When $a = b$, which is not uncommon, this pinpoints the exact value of r. There are also other more sophisticated methods of descent [40, 24].

Proving Mordell-Weil is an extensive task, so it is fruitful to give a quick sketch before we proceed. The main tool is the Descent Theorem (for a proof, see Section 7.2 of the Appendix), which relies on the notion of a *height* on an abelian group.

Definition 4.0.3 (Height)**.** Let G be an abelian group. A height of G is a tuple (h, s, k), where $h, s : G \to \mathbb{R}_+$ and $k \geq 0$, satisfying

1. $h(x + y) \leq 2h(x) + s(y)$,
2. $4h(x) \leq h(2x) + k$,
3. $|\{x \; : \; h(x) \leq M\}| < \infty$ for all $M \geq 0$.

Theorem 4.0.4. (Descent Theorem) Let Γ be an abelian group. Then, the following are equivalent.

1. Γ is finitely generated,
2. Γ admits a height and $|\Gamma/2\Gamma| < \infty$.

The problem is reduced to (i) finding a height for $E(\mathbb{Q})$ and (ii) proving $|E(\mathbb{Q})/2E(\mathbb{Q})| < \infty$, which turns out to be much easier than finding actual generators for $E(\mathbb{Q})$. Item (ii) is known as the Weak Mordell-Weil Theorem. Currently, the only known proofs of the Mordell-Weil Theorem are through this method. We now give a rough sketch of the next steps.

(I) Construct a height (h, s, k) for the group $E(\mathbb{Q})$. This is the only step that cannot be easily generalized to an arbitrary number field.

(II) Show that the finiteness of $E(\mathbb{Q})/2E(\mathbb{Q})$ follows from the finiteness of $E(Q)/2E(Q)$ (where Q was defined above as the splitting field of $F(x)$).

(III) Construct a group homomorphim $\phi : E(Q) \to G$ for some group G, such that ϕ has finite image and $\text{Ker}(\phi) = 2E(Q)$.

4.1 Contructing a height for $E(\mathbb{Q})$

Theorem 4.1.1. *$E(\mathbb{Q})$ admits a height (h, s, k) where*

$$h(P) := \begin{cases} \log H(x) & \text{if } P = (x, y); \\ 0 & \text{if } P = \mathcal{O}. \end{cases} \qquad H(a/b) := \max(|a|, |b|),$$

where $\gcd(a, b) = 1$.

Proof. We show h satisfies the three properties in Definition 4.0.3. First, property 3 is evident: given a constant $K \geq 1$, there are only finitely many rational numbers $x = a/b$, $\gcd(a, b) = 1$ where $H(x) = \max(|a|, |b|) < K$. Moreover, for each possibility of x, there are only two possibilities for y, namely $\pm\sqrt{F(x)}$.

We now show property 1. Pick points $P_i = (x_i, y_i)$ for $i = 1, 2, 3$ such that $P_1 \oplus P_2 = P_3$. Write $(x_i, y_i) = (a_i/c_i^2, b_i/c_i^3)$ with $\gcd(a_i, c_i) = \gcd(b_i, c_i) = 1$. Assume first $P_1 \neq \pm P_2$. By the addition formula

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 - A. \tag{4.2}$$

We expand this expression in terms of a_i, b_i, c_i obtaining

$$x_3 = \frac{(a_1a_2 + Bc_1^2c_2^2)(a_1c_2^2 + a_2c_1^2) + 2Cc_1^4c_2^4 - 2b_1c_1b_2c_2 - A(a_1c_2^2 - a_2c_1^2)^2}{(a_1c_2^2 - a_2c_1^2)^2}. \tag{4.3}$$

The denominator and numerator may not be in lowest terms, but at least this is an upper bound on the height. We therefore have

$$H(x_3) \leq K_1 \max(|a_1^2|, |c_1^4|, |b_1c_1|), \tag{4.4}$$

where K_1 is the expression depending on P_2 and the coefficients of $F(x)$ that appears after we extract the terms a_1, b_1, c_1. The only remaining issue is the term $|b_1c_1|$. We use the equation of the elliptic curve to get

$$b_1^2 = a_1^3 + Aa_1^2c_1^2 + Ba_1c_1^4 + Cc_1^6. \tag{4.5}$$

Therefore, by the same logic as before, for some constant K_2 we have

$$|b_1| \leq K_2 \max(|a_1|^{3/2}, |c_1|^3). \tag{4.6}$$

We now put together Equations (4.4) and (4.5) to get

$$\begin{aligned} H(x_3) &\leq K_1 \max(|a_1|^2, |c_1|^4, |c_1|K_2 \max(|a_1|^{3/2}, |c_1|^3)) && (4.7)\\ &\leq K_1K_2 \max(|a_1|^2, |c_1|^4, |c_1a_1^{3/2}|) && (4.8)\\ &= K_1K_2 \max(|a_1|^2, |c_1|^4) = K_1K_2H(x_1)^2. && (4.9) \end{aligned}$$

Define $K(P_2) := \log K_1 + \log K_2$. By taking log on both sides we get $h(P_3) \leq 2h(P_1) + K(P_2)$. We assumed $P_1 \neq \pm P_2$ for this bound. If $P_2 = -P_1$ the bound is automatically true. Let $P_2 = P_1$, we clearly have $h(2P_1) \leq 2h(P_1) + h(2P_1)$. Therefore, we get the desired bound for any P_2 by setting $s(P_2) := \max(K(P_2), h(2P_2))$.

The last step is to show property 2. This is the hardest part. Fix $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2) = 2P_1$. By the duplication formula we have

$$x_2 = \frac{x_1^4 - 2Bx_1^2 - 8Cx_1 + B^2 - 4AC}{4(x_1^3 + Ax_1^2 + Bx_1 + C)}. \tag{4.10}$$

We define $H(x,z), S(x,z)$ as the homogenization of this ratio, i.e.

$$H(x,z) := x^4 - 2Bx^2z^2 - 8Cxz^3 - 4ACz^4, \quad S(x,z) := 4(x^3z + Ax^2z^2 + Bxz^3 + Cz^4). \tag{4.11}$$

Let $x_1 = a/b$ in lowest terms. We have that $x_2 = H(a,b)/S(a,b)$. The cancellation between numerator and denominator of this expression is precisely the greatest common divisor $\delta := \gcd(H(a,b), S(a,b))$. It turns out that, in $\mathbb{Q}[x,z]$, H and S are relatively prime. Therefore, we must have f_1, f_2, g_1, g_2 such that

$$f_1 H - g_1 S = 4\Delta z^7, \quad f_2 H - g_2 S = 4\Delta x^7. \tag{4.12}$$

Evaluating formulas for these polynomials using the Euclidean algorithm we see that they all have degree at most 3 in each monomial (see [35, page 222]). By (4.12), we see that δ divides $4\Delta \gcd(a^7, b^7) = 4\Delta$. Hence,

$$H(x_2) = \frac{\max(|H(a,b)|, |S(a,b)|)}{|\delta|} \geq \frac{\max(|H(a,b)|, |S(a,b)|)}{4|\Delta|}. \tag{4.13}$$

Now we do a series of inequalities.

$$\begin{aligned} & 4|\Delta b^7| \\ \leq\ & |f_1(a,b)H(a,b)| + |g_1(a,b)S(a,b)| && \text{(Equation (4.12))} \\ \leq\ & 2\max(|f_1(a,b)|, |g_1(a,b)|)\max(|H(a,b)|, |S(a,b)|) && \text{(Bound by the maximum)} \\ \leq\ & 2K_1 \max(|a|^3, |b|^3)\max(|H(a,b)|, |S(a,b)|) && \text{(All monomials have deg} \leq 3 \text{ in } f_1, g_1\text{).} \end{aligned}$$

The constant K_1 depends only on the coefficients of f_1, g_1. By the same argument we get an analogous inequality for $4|\Delta a^7|$, now involving a constant K_2. Define $K := \max(K_1, K_2)$. Joining both inequalities we have

$$4|\Delta| \max(|a|^7, |b|^7) \leq 2K \max(|a|^3, |b|^3)\max(|H(a,b)|, |S(a,b)|). \tag{4.14}$$

Therefore, using expression (4.12) for $H(x_2)$ we get

$$H(x_2) \geq (2K)^{-1}\max(|a|^4, |b|^4) = (2K)^{-1} H(x_1)^4. \tag{4.15}$$

Define $k := \log 2K$. By taking log on both sides we finally get $h(x_2) + k \geq 4h(x_1)$. □

4.2 The Weak Mordell-Weil Theorem

The goal of this section is to prove the Weak Mordell-Weil Theorem.

Theorem 4.2.1 (Weak Mordell-Weil)**.** $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

The proof will proceed in a series of steps. First, we reduce the problem to the group $E(Q)$.

Proposition 4.2.2. If $E(Q)/2E(Q)$ is finite, so is $E(\mathbb{Q})/2E(\mathbb{Q})$.

Proof. The inclusion $E(\mathbb{Q}) \hookrightarrow E(Q)$ induces a map

$$\frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \xrightarrow{\phi} \frac{E(Q)}{2E(Q)}, \quad \operatorname{Ker}(\phi) = \frac{E(\mathbb{Q}) \cap 2E(Q)}{2E(\mathbb{Q})}.$$

Then, for each class $h \in \operatorname{Ker}(\phi)$ choose $P_h \in E(\mathbb{Q})$ and $Q_h \in E(Q)$ in that class such that $2Q_h = P_h$. Now, the extension $Q/\mathbb{Q}$ is Galois (since it is the splitting field of a polynomial in $\mathbb{Q}$) and its Galois group $G := \operatorname{Gal}(Q/\mathbb{Q})$ acts on $E(Q)$ by $\sigma \cdot (x, y) := (\sigma x, \sigma y)$. We then have a map of sets (not a group homomorphism!) $\lambda : \operatorname{Ker}(\phi) \times G \to E(\mathbb{Q})[2]$ given by

$$\lambda(h, \sigma) := \sigma Q_h - Q_h.$$

Notice the image is indeed in $E(\mathbb{Q})[2]$ since $2\lambda(h, \sigma) = 2(\sigma Q_h) - 2Q_h = \sigma(2Q_h) - P_h = \sigma P_h - P_h = P_h - P_h = \mathcal{O}$. As a side note, notice that $\lambda_h(\sigma) := \lambda(h, \sigma)$ satisfies $\lambda_h(\sigma\beta) = \sigma\lambda_h(\beta) + \lambda_h(\sigma)$, which is "almost" a group homomorphism. Maps with this property are called twisted homomorphisms, and are precisely the $1-$cocycles in group cohomology.

Now, suppose $\lambda(h, \cdot) = \lambda(f, \cdot)$ as maps. This implies $\sigma(Q_h - Q_f) = Q_h - Q_f$ for all $\sigma \in G$, but then $Q_h - Q_f$ must be in $E(\mathbb{Q})$. But then $P_h - P_f = 2(Q_h - Q_f) \in 2E(\mathbb{Q})$, so h and f must be the same class. This shows that $\lambda(h, \cdot) : \operatorname{Ker}(\phi) \to \operatorname{Hom}_{\mathrm{Set}}(G, E(\mathbb{Q})[2])$ is injective. But G is finite and $E(\mathbb{Q})[2] = \{\mathcal{O}, (e_1, 0), (e_2, 0), (e_3, 0)\}$, so $\operatorname{Ker}(\phi)$ is finite. But since $\operatorname{Img}(\phi) \subseteq E(Q)/2E(Q)$ is also finite, it follows that the domain $E(\mathbb{Q})/2E(\mathbb{Q})$ must be finite as well. □

Theorem 4.2.3. The map $\pi_{e_1} : E(Q) \to Q^*/(Q^*)^2$ defined as

$$\pi_{e_1}(\mathcal{O}) := 1, \quad \pi_{e_1}(x, y) := \begin{cases} x - e_1 & \text{if } x \neq e_1, \\ (e_3 - e_1)(e_2 - e_1) & \text{if } x = e_1, \end{cases}$$

is a group homomorphism.

Proof. Let $\pi := \pi_{e_1}$. We write $\equiv$ for equality in $Q^*/(Q^*)^2$. Clearly, π preserves inverses and the identity element. Let $P_i = (x_i, y_i)$, for $i = 1, 2, 3$. It remains to show that if

$P_1 \oplus P_2 \oplus P_3 = \mathcal{O}$, then $\pi(P_1)\pi(P_2)\pi(P_3) \equiv 1$. This is clear if some $P_i = \mathcal{O}$. Assuming all $P_i \neq \mathcal{O}$, we have three cases to check without loss of generality.

Case 1: $P_1 \neq P_2$, and $P_i \neq (e_1, 0)$ for all $i = 1, 2, 3$

First, it will be useful to derive an expression for x_3 in terms of e_1. Let L be the line passing through P_1 and P_2. Its equation is given by

$$L : y = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x - x_1) + y_1. \tag{4.16}$$

We plug this into the equation for E to get the expression (whose roots must be x_1, x_2, x_3)

$$\left(\left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x - x_1) + y_1\right)^2 = x^3 + Ax^2 + Bx + C. \tag{4.17}$$

Now we do the substitution $x_i = X_i + e_1$ for $i = 2, 3$ and $x = X + e_1$.

$$\left(\left(\frac{y_2 - y_1}{X_2 - X_1}\right)(X - X_1) + y_1\right)^2 = X^3 + (3e_1 + A)X^2 + (3e_1^2 + 2Ae_1 + B)X \tag{4.18}$$

$$+ (e_1^3 + Ae_1^2 + Be_1 + C). \tag{4.19}$$

The last term cancels out since e_1 is a root of $F(x)$. Therefore, the constant term of this expression is contained in the left-hand side. We expand and simplify.

$$\text{LHS} = (\ldots) \cdot X + \left(\frac{X_2 y_1 - X_1 y_2}{X_2 - X_1}\right)^2 = (\ldots) \cdot X + \left(\frac{(x_2 - e_1)y_1 - (x_1 - e_1)y_2}{x_2 - x_1}\right)^2. \tag{4.20}$$

This constant term must be equal to the product of the roots of the polynomial in (4.19). The roots are $x_1 - e_1, x_2 - e_1, x_3 - e_1$. Hence, we get the final formula

$$x_3 - e_1 = \frac{1}{(x_1 - e_1)(x_2 - e_1)}\left(\frac{(x_2 - e_1)y_1 - (x_1 - e_1)y_2}{x_2 - x_1}\right)^2. \tag{4.21}$$

By using Equation (4.21) we have $\pi(P_1)\pi(P_2)\pi(P_3) = (x_1 - e_1)(x_2 - e_1)(x_3 - e_1) \equiv 1$.

Case 2: $P_1 = (e_1, 0)$

Here, we have $P_2, P_3 \neq (e_1, 0)$ or else one would have to be equal to $\mathcal{O}$. We use the addition formula to get

$$x_3 - e_1 = \left(\frac{y_2}{x_2 - e_1}\right)^2 - (x_2 + 2e_1 + A). \tag{4.22}$$

We now do a series of calculations.

$$\begin{aligned} & x_3 - e_1 \\ \equiv\ & (x_3 - e_1)(x_2 - e_1)^2 && \text{(Equality in } Q/Q^2) \end{aligned}$$

$$\begin{aligned}
&= \quad y_2^2 - (x_2 + 2e_1 + A)(x_2 - e_1)^2 && \text{(Equation (4.22))}\\
&= \quad (x_2 - e_1)(x_2 - e_2)(x_2 - e_3) - (x_2 + 2e_1 + A)(x_2 - e_1)^2 && (y_2^2 = P(x_2))\\
&= \quad (x_2 - e_1)(e_2e_3 + Ae_1 + 2e_1^2 - (e_1 + e_2 + e_3 + A)x_2) && \text{(Simplify)}\\
&= \quad (x_2 - e_1)(e_2e_3 + Ae_1 + 2e_1^2) && (e_1 + e_2 + e_3 = -A)\\
&= \quad (x_2 - e_1)((e_2 - e_1 + e_1)(e_3 - e_1 + e_1) + Ae_1 + 2e_1^2) && \text{(Add and subtract } e_1\text{)}\\
&= \quad (x_2 - e_1)((e_2 - e_1)(e_3 - e_1) + e_1(e_1 + e_2 + e_3 + A)) && \text{(Simplify)}\\
&= \quad (x_2 - e_1)(e_2 - e_1)(e_3 - e_1) && (e_1 + e_2 + e_3 = -A).
\end{aligned}$$

Thus, $\pi(P_1)\pi(P_2)\pi(P_3) = (x_2 - e_1)^2(e_2 - e_1)^2(e_3 - e_1)^2 \equiv 1$.

Case 3: $P_1 = P_2 = P_3$

In this case, we have $P_i \neq (e_1, 0)$. We take the limit $x_1 \to x_2$ in Equation (4.21).

$$\begin{aligned}
& \quad x_3 - e_1 \\
&= \quad \lim_{x_1\to x_2} \frac{1}{(x_1 - e_1)(x_2 - e_1)} \left(\frac{(x_2 - e_1)y_1 - (x_1 - e_1)y_2}{x_2 - x_1}\right)^2 && \text{(Equation (4.21))}\\
&= \quad \lim_{x_1\to x_2} \frac{(x_2 - e_1)^2}{(x_1 - e_1)(x_2 - e_1)} \left(\frac{y_1 - \left(\frac{x_1 - e_1}{x_2 - e_1}\right) y_2}{x_2 - x_1}\right)^2 && \text{(Extract } x_2 - e_1\text{)}\\
&= \quad \lim_{x_1\to x_2} \left(\frac{y_1 - \left(\frac{x_1 - e_1}{x_2 - e_1}\right) y_2}{x_2 - x_1}\right)^2 && \text{(Left term converges to 1)}\\
&= \quad \lim_{x_1\to x2} \left[\left(y_1' - \frac{y_2}{x_2 - e_1}\right)^2 + \left(y_1 - \left(\frac{x_1 - e_1}{x_2 - e_1}\right) y_2\right) y_1''\right] && \text{(L'Hopital's rule 2 times)}\\
&= \quad \lim_{x_1\to x2} \left(y_1' - \frac{y_2}{x_2 - e_1}\right)^2 && \text{(Right term goes to zero)}\\
&= \quad \left[\lim_{x_1\to x2} \left(y_1' - \frac{y_2}{x_2 - e_1}\right)\right]^2 && \text{(Push the limit inside)}\\
&= \quad \left(y_2' - \frac{y_2}{x_2 - e_1}\right)^2 && \text{(Evaluate).}
\end{aligned}$$

Therefore, $x_3 - e_1 \in (Q^*)^2$. We conclude that $\pi(P_1)\pi(P_2)\pi(P_3) \equiv 1$. □

The map π_{e_1} induces an isomorphism $E(Q)/\mathrm{Ker}(\pi_{e_1}) \cong \mathrm{Img}(\pi_{e_1})$. The map π_{e_1} has finite image, but unfortunately $\mathrm{Ker}(\pi_{e_1})$ is, in general, bigger than $2E(Q)$. However, it turns out that $\mathrm{Ker}(\pi_{e_1}) \cap \mathrm{Ker}(\pi_{e_2}) = 2E(Q)$. So, we can instead consider the map $\phi := \pi_{e_1} \times \pi_{e_2}$, i.e. $\phi(P) = (\pi_{e_1}(P), \pi_{e_2}(P))$. The last two steps of the proof will be showing that $\mathrm{Ker}(\phi) = 2E(Q)$ and that $\mathrm{Img}(\phi)$ is finite. We begin with a Lemma.

Lemma 4.2.4. Pick a point $P_1 = (x_1, y_1) \in E(K)$. Define $\epsilon_i := \sqrt{x_1 - e_i} \in \overline{Q}$. Then, there are exactly four solutions (counting multiplicity) $P_2 = (x_2, y_2) \in E(\overline{Q})$ to the equation $2P_2 = P_1$. They are given by

$$x_2 = \frac{1}{2}(u^2 - x_1 - A), \quad y_2 = ux_2 + (y_1 - ux_1),$$

where

$$u \in \left\{ \begin{matrix} \epsilon_1 + \epsilon_2 - \epsilon_3, & -\epsilon_1 + \epsilon_2 + \epsilon_3, \\ \epsilon_1 - \epsilon_2 + \epsilon_3, & -\epsilon_1 - \epsilon_2 - \epsilon_3 \end{matrix} \right\}.$$

Proof. Let $L : y = ux + v$ be the line tangent to P_2 passing through P_1. We substitute it in the equation for E to obtain

$$x^3 + (A - u^2)x^2 + (B - 2uv)x + (C - v^2) = 0. \tag{4.23}$$

We divide it by the trivial root $x = x_1$, and apply the identity $v = y_1 - ux_1$ to get

$$x^2 + (A + x_1 - u^2)x + (B - 2uy_1 + (A + x_1 + u^2)x_1) = 0. \tag{4.24}$$

This equation should have a double root at $x = x_2$, so the discriminant should be zero. Thus, we have

$$(A + x_1 - u^2)^2 = 4(B - 2uy_1 + (A + x_1 + u^2)x_1). \tag{4.25}$$

Equation (4.25) is a quartic polynomial in u. Here comes a trick that turns a problem of solving quartics into a problem of solving cubics. The idea is to introduce a new variable λ so as to make the right-hand side a square. We have

$$(A + x_1 - u^2 + \lambda)^2 = (4x_1 - 2\lambda)u^2 - (8y_1)u + (4B + 4Ax_1 + 4x_1^2 + 2\lambda(A + x_1) + \lambda^2). \tag{4.26}$$

In order for the right-hand side to be a square, the discriminant of the quadratic polynomial in the right-hand side should be zero. After simplifying the expression we have

$$0 = 8\lambda^3 + 16A\lambda^2 + 32B\lambda + 64(y_1^2 - x_1^3 - Ax_1^2 - Bx_1). \tag{4.27}$$

Since (x_1, y_1) is a point in the curve, the constant term is equal to $64C$. We make the substitution $2\eta = \lambda$ and divide the equation by 64 to get

$$0 = \eta^3 + A\eta^2 + B\eta + C. \tag{4.28}$$

Clearly, the three solutions to this equation are $\lambda = 2e_1, 2e_2, 2e_3$. Let's fix $\lambda = 2e_1$ (if $x_1 = e_1$, we choose $\lambda = 2e_3$ instead). Using the quadratic formula, we conclude that the double root of the right-hand side of Equation (4.26) is $u = y_1/(x_1 - e_1)$. We can then write it as a square.

$$(A - u^2 + x_1 + 2e_1)^2 = 4(x_1 - e_1)(u - y_1/(x_1 - e_1))^2 \tag{4.29}$$

$$= 4(\epsilon_1 u - y_1/\epsilon_1)^2 \tag{4.30}$$

$$= 4(\epsilon_1 u - \epsilon_2\epsilon_3)^2. \tag{4.31}$$

In the last equation we used the identity $y_1 = \epsilon_1\epsilon_2\epsilon_3$. Now we take the square root on both sides, denoting the varying sign by ±.

$$A - u^2 + x_1 + 2e_1 = \pm 2(\epsilon_1 u - \epsilon_2\epsilon_3). \tag{4.32}$$

We rearrange terms and use the identity $A = -e_1 - e_2 - e_3$ to get

$$(u \pm \epsilon_1)^2 = (\epsilon_2 \pm \epsilon_3)^2. \tag{4.33}$$

We take the square roots again and arrive at the desired solutions for the slope u of the tangent line. The expression for (x_2, y_2) then follows by the duplication formula on elliptic curves. □

Proposition 4.2.5. $\mathrm{Ker}(\pi_{e_1} \times \pi_{e_2}) = 2E(Q)$.

Proof. ($\supseteq$) Pick $P_1 = 2P_2$ in $E(Q)$. Then, $\pi_{e_i}(P_1) = \pi_{e_i}(2P_2) = \pi_{e_i}^2(P_2) = 1$. ($\subseteq$) Pick $P_1 = (x_1, y_1)$ in the kernel of the map, i.e. $\pi_{e_1}(P_1) = 1$, $\pi_{e_2}(P_1) = 1$. Assume first that $P_1 \notin \{(e_1, 0), (e_2, 0)\}$. Then, $\pi_{e_1}(P_1) = x_1 - e_1$ and $\pi_{e_2}(P_1) = x_1 - e_2$ are squares. But then

$$x_1 - e_3 = \frac{y_1^2}{(x_1 - e_1)(x_1 - e_2)} \tag{4.34}$$

is also a square, so for $i = 1, 2, 3$, $\epsilon_i := \sqrt{x_1 - e_i} \in Q$. So by Lemma 4.2.4 there exists a $P_2 \in E(Q)$ with $2P_2 = P_1$. Lastly, assume without loss of generality that $P_1 = (e_1, 0)$. Then, $\pi_{e_1}(P_1) = (e_1 - e_2)(e_1 - e_3)$ and $\pi_{e_2}(P_1) = e_1 - e_2$ are squares. But then $e_1 - e_3$ is also a square. The result follows again by Lemma 4.2.4. □

The last part of the Theorem is to prove that the image of π_{e_1} is finite, which immediately implies that the image of ϕ is finite. For this, we need a result in algebraic number theory, namely Proposition 2.4.32, which says there is a principal ideal domain (hence a unique factorization domain) R_Q with $\mathcal{O}_Q \subseteq R_Q \subseteq Q$, where $R_Q^\times$ is a finitely generated group. Notice that $Q = \mathrm{Frac}(\mathcal{O}_Q) = \mathrm{Frac}(R_Q)$.

Proposition 4.2.6. $\mathrm{Img}(\pi_{e_1})$ is a finite set.

Proof. Let $P_1 = (x_1, y_1) \in E(Q)$. We may suppose $x_1 \neq e_1$. We want to show that, up to squares, there is only a finite amount of possible values for $\pi_{e_1}(P_1) = x_1 - e_1$. Pick a prime $p \in R_Q$. Write $v_p : R_Q \to \mathbb{Z} \cup \{\infty\}$ for the $p-$adic valuation on p. We'll show that either $v_p(x_1 - e_1)$ is even, or $p \mid \Delta$.

Suppose $p \nmid \Delta$. This implies $v_p(e_1 - e_i) = 0$ for $i = 2, 3$. We have the equation for E, namely $y^2 = (x_1 - e_1)(x_1 - e_2)(x_1 - e_3)$. Applying v_p to both sides we obtain

$$v_p(x_1 - e_1) + v_p(x_1 - e_2) + v_p(x_1 - e_3) \equiv 0 \mod 2. \tag{4.35}$$

If $v_p(x_1 - e_1) = 0$, we're done. Suppose it is $\neq 0$. Then, for $i = 2, 3$ we have

$$v_p(x_1 - e_i) = v_p((x_1 - e_1) + (e_1 - e_i)) = \begin{cases} 0 & \text{if } v_p(x_1 - e_1) > 0 \\ v_p(x_1 - e_1) & \text{if } v_p(x_1 - e_1) < 0. \end{cases}$$

Here we used the property of v_p that says $v_p(a+b) = \min(v_p(a), v_p(b))$ when $v_p(a) \neq v_p(b)$. But then, by substituting these values in Equation (4.35) we obtain $v_p(x_1 - e_1) \equiv 0 \mod 2$ in all cases. We conclude that

$$x_1 - e_1 = \alpha^2 d \epsilon_1^{r_1} \ldots \epsilon_n^{r_n},$$

where $\alpha \in Q$, $d \mid \Delta$, $\{\epsilon_1, \ldots, \epsilon_n\}$ are generators of $R_Q^\times$ and $r_i \in \{0, 1\}$. Therefore there are only finitely many possibilities for $x_1 - e_1$ up to squares. □

Using Propositions 4.2.5 and 4.2.6, we conclude that $E(Q)/2E(Q) = E(Q)/\text{Ker}(\phi) \cong \text{Img}(\phi)$ is finite. By Proposition 4.2.2, $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite, which proves the Weak Mordell-Weil Theorem.

4.3 Calculating the rank

The goal of this section is to present an algorithm for finding upper and lower bounds for the rank r of the group $E(\mathbb{Q})$, provided the group has a point of order two $P_0 = (x_0, 0)$. This method is known as *descent by* $2-$*isogeny*. We can always do a change of variables $x \leftarrow x - x_0$, which ensures $P_0 = (0, 0)$, hence E may be assumed to have equation

$$E : y^2 = x^3 + Ax^2 + Bx. \tag{4.36}$$

The key idea is that we can find an explicit isogeny $\phi : E \to E/\langle P_0 \rangle =: \overline{E}$ of degree two. Then, if $\psi : \overline{E} \to E$ is the dual isogeny of ϕ, we have that the maps $\phi \circ \psi$ and $\psi \circ \phi$ are the multiplication-by-two maps $P \mapsto 2P$. Given P_0, the maps ϕ, ψ and the curve $\overline{E}$ can be calculated explicitly [42], giving rise to the following.

Theorem 4.3.1. The following hold.

(i) The curve $\overline{E}$ has equation $\overline{E} : y^2 = x^3 + \overline{A}x^2 + \overline{B}x$, where we define $\overline{A} := -2A$ and $\overline{B} := A^2 - 4B$;

(ii) $\phi(p) := \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-B)}{x^2}\right) & \text{if } p \notin \{(0,0), \mathcal{O}\}, \\ \mathcal{O} & \text{else;} \end{cases}$

(iii) $\psi(p) := \begin{cases} \left(\frac{y^2}{4x^2}, \frac{y(x^2-B)}{8x^2}\right) & \text{if } p \notin \{(0,0), \mathcal{O}\}, \\ \mathcal{O} & \text{else.} \end{cases}$

Notice that $\operatorname{Ker}(\phi) = \{(0,0), \mathcal{O}\} = \operatorname{Ker}(\psi)$. Our next goal is to derive expressions for their image. First, we must return to the homomorphism π_{e_1} defined in Theorem 4.2.3. Since we're assuming $e_1 = 0$, we have a map $\alpha := \pi_0$. We claim that α can be viewed as a map from $E(\mathbb{Q})$ to $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. This is clear since $\alpha(P_0) = e_2e_3 = B \in \mathbb{Q}^*$, so

$$\alpha(\mathcal{O}) = 1, \quad \alpha(x,y) = \begin{cases} x & \text{if } x \neq 0, \\ B & \text{if } x = 0. \end{cases} \tag{4.37}$$

We define $\overline{\alpha} : \overline{E}(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ as the corresponding map on $\overline{E}$. We have

Proposition 4.3.2. The following hold.

$$\begin{array}{llll} \text{(i)} & \operatorname{Ker}(\phi) = \{(0,0), \mathcal{O}\}, & \text{(iii)} & \operatorname{Img}(\phi) = \operatorname{Ker}(\overline{\alpha}), \\ \text{(ii)} & \operatorname{Ker}(\psi) = \{(0,0), \mathcal{O}\}, & \text{(iv)} & \operatorname{Img}(\psi) = \operatorname{Ker}(\alpha). \end{array}$$

Proof. Items (i) and (ii) are clear. We prove only item (iii), as item (iv) is identical. ($\subseteq$) By the definition, $\phi(P)$ either is $\mathcal{O}$ or has $x-$coordinate in $(\mathbb{Q}^*)^2$, so the statement is clear. ($\supseteq$) Pick $P = (x,y) \in \operatorname{Ker}(\overline{\alpha})$. We have two cases to consider. First, assume $P = (0,0)$, thus $\overline{\alpha}(P) = \overline{B} = A^2 - 4B$ is a rational square. But this is the discriminant of $x^2 + Ax + B$, so it must admit a rational root r. But then $(r,0)$ is a point in $E(\mathbb{Q})$ with $\phi(r,0) = (0,0) = P$. Now assume $P \neq (0,0)$, so x must be a square, say, w^2. We must now construct a point $P_1 = (x_1, y_1)$ such that $\phi(x_1, y_1) = (w^2, y)$. From the definition of ϕ we get a system of equations

$$y_1^2 = w^2x_1^2, \quad y_1(x_1^2 - B) = yx_1^2. \tag{4.38}$$

By the first equation we have $y_1 = \pm wx_1$. We substitute it on the second equation and solve for x_1 (using the fact that $y^2 = x^3 + \overline{A}x^2 + \overline{B}x$) obtaining solutions

$$y_1 = wx_1, \quad x_1 = \frac{1}{2}(\pm y/w + w^2 - A). \tag{4.39}$$

It remains to check if this point belongs to $E(\mathbb{Q})$. We want (x_1, y_1) to satisfy the equation

$$y_1^2 = x_1^3 + Ax_1^2 + Bx_1. \tag{4.40}$$

By substituting $y_1^2 = w^2 x_1^2$ and solving for x_1 we obtain $x_1 = \frac{1}{2}(\pm y/w + w^2 - A)$. □

Corollary 4.3.3. We have

$$[\overline{E}(\mathbb{Q}) : \mathrm{Img}(\phi)] = \#\mathrm{Img}(\overline{\alpha}), \quad [E(\mathbb{Q}) : \mathrm{Img}(\psi)] = \#\mathrm{Img}(\alpha).$$

Proof. This is a consequence of the First Isomorphism Theorem. We have $\mathrm{Img}(\overline{\alpha}) \cong \overline{E}(\mathbb{Q})/\mathrm{Ker}(\overline{\alpha}) = \overline{E}(\mathbb{Q})/\mathrm{Img}(\phi)$. The same argument works for ψ. □

Before we proceed, we need a basic Lemma in group theory.

Lemma 4.3.4. Let $A \subseteq B$ be abelian groups and $[B : A] < \infty$. Let $f : B \to C$ be a group homomorphism. Then,

$$[f(B) : f(A)] = \frac{[B : A]}{[\mathrm{Ker}(f) : \mathrm{Ker}(f) \cap A]}.$$

Proof. Using the isomorphism theorems we have

$$\frac{f(B)}{f(A)} \cong \frac{B}{A + \mathrm{Ker}(f)} \cong \frac{B/A}{(A + \mathrm{Ker}(f))/A} \cong \frac{B/A}{\mathrm{Ker}(f)/(\mathrm{Ker}(f) \cap A)}.$$

□

With this, we are able to express the index $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ in terms of α and $\overline{\alpha}$.

$$\begin{aligned}
& [E(\mathbb{Q}) : 2E(\mathbb{Q})] \\
= \; & [E(\mathbb{Q}) : \mathrm{Img}(\psi \circ \phi)] && (\psi \circ \phi \text{ is the multiplication-by-two map}) \\
= \; & [E(\mathbb{Q}) : \mathrm{Img}(\psi)][\mathrm{Img}(\psi) : \mathrm{Img}(\psi \circ \phi)] && ([A : C] = [A : B][B : C] \text{ when } A \supseteq B \supseteq C) \\
= \; & \frac{[E(\mathbb{Q}) : \mathrm{Img}(\psi)][\overline{E}(\mathbb{Q}) : \mathrm{Img}(\phi)]}{[\mathrm{Ker}(\psi) : \mathrm{Ker}(\psi) \cap \mathrm{Img}(\phi)]} && (\text{Lemma 4.3.4}) \\
= \; & \frac{\#\mathrm{Img}(\alpha)\#\mathrm{Img}(\overline{\alpha})}{[\mathrm{Ker}(\psi) : \mathrm{Ker}(\psi) \cap \mathrm{Img}(\phi)]} && (\text{Corollary 4.3.3})
\end{aligned}$$

Since $\mathrm{Ker}(\psi) = \{(0,0), \mathcal{O}\}$, the index in the denominator is equal to 1 if $(0,0) \in \mathrm{Img}(\phi)$, otherwise it is equal to 2. But $(0,0) \in \mathrm{Img}(\phi)$ if and only if $x^2 + Ax + B$ has a rational root, which happens if and only if $A^2 - 4B$ is a perfect square. We thus have

$$[E(\mathbb{Q}) : 2E(\mathbb{Q})] = \begin{cases} \#\mathrm{Img}(\alpha)\#\mathrm{Img}(\overline{\alpha}) & \text{if } A^2 - 4B \text{ is a perfect square,} \\ \#\mathrm{Img}(\alpha)\#\mathrm{Img}(\overline{\alpha})/2 & \text{otherwise.} \end{cases} \tag{4.41}$$

We are now ready to express the rank r in terms of α and $\overline{\alpha}$. Write $E(\mathbb{Q})$ as

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T \oplus \bigoplus_{i=1}^{N} \mathbb{Z}_{p_i}, \tag{4.42}$$

where T is a finite group with order relatively prime to 2 and each p_i is a power of 2. Again, this form follows by the Fundamental Theorem of Finitely Generated Abelian Groups. We then have

$$\begin{aligned}
&E(\mathbb{Q})/2E(\mathbb{Q}) \\
\cong\ & \mathbb{Z}^r/2\mathbb{Z}^2 \oplus T/2T \oplus \bigoplus_{i=1}^{N} \mathbb{Z}_{p_i}/2\mathbb{Z}_{p_i} && \text{(Equation (4.42))} \\
\cong\ & \mathbb{Z}^2/2\mathbb{Z}^r \oplus T/2T \oplus \bigoplus_{i=1}^{N} \mathbb{Z}_2 && (\mathbb{Z}_p/2\mathbb{Z}_{p_i} \cong \mathbb{Z}_2 \text{ since } p_i \text{ is a power of two}) \\
\cong\ & \mathbb{Z}^2/2\mathbb{Z}^r \oplus \bigoplus_{i=1}^{N} \mathbb{Z}_2 && (T/2T \cong \{0\} \text{ since } T \text{ has order relatively prime to 2}) \\
\cong\ & \mathbb{Z}_2^{r+N} && \text{(Simplify).}
\end{aligned}$$

Notice that $2^N = \#E(\mathbb{Q})[2]$, i.e., the number of elements of order 2. These are the rational roots of $x^3 + Ax^2 + Bx$ plus the element $\mathcal{O}$ at infinity. Thus, there are 4 points if $A^2 - 4B$ is a perfect square, otherwise 2 points. We conclude

$$[E(\mathbb{Q}) : 2E(\mathbb{Q})] = \begin{cases} 2^{r+2} & \text{if } A^2 - 4B \text{ is a perfect square,} \\ 2^{r+1} & \text{otherwise.} \end{cases} \tag{4.43}$$

We join equations (4.41) and (4.43) and take $\log_2$ on both sides, arriving at the final identity

$$r = \log_2 \#\mathrm{Img}(\alpha) + \log_2 \#\mathrm{Img}(\overline{\alpha}) - 2. \tag{4.44}$$

We have thus reduced the problem of bounding the rank r to finding elements in the images of α and $\overline{\alpha}$. In what follows we'll derive a necessary and sufficient condition that will reduce this problem to determining whether or not a finite number of Diophantine equations admit an integer solution. This will immediately lead to an algorithm.

Proposition 4.3.5. A class $\gamma \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ is in the image of α if and only if one of the following hold.

(i) $\gamma \equiv 1$;

(ii) $\gamma \equiv b_1$ for some divisor $\neq 1$ of B such that the affine curve $y^2 = b_1x^4 + Ax^2 + B/b_1$ admits a rational solution.

Proof. ($\Leftarrow$) If $\gamma \equiv 1$, then $\gamma = \alpha(\mathcal{O})$. Suppose $\gamma \equiv b_1$ satisfying (ii). Let (x_0, y_0) be such a rational solution. Then, we have the morphism of curves

$$\{y^2 = b_1 x^4 + Ax^2 + B/b_1\} \to \{y^2 = x^3 + Ax^2 + Bx\}, \quad (x, y) \mapsto (b_1 x^2, b_1 xy). \tag{4.45}$$

Thus, the rational point $P_0 := (b_1 x_0^2, b_1 x_0 y_0)$ is in $E(\mathbb{Q})$ and $\alpha(P_0) = b_1 \equiv \gamma$. ($\Rightarrow$) Suppose $\gamma \in \mathrm{Img}(\alpha)$ with $\gamma \not\equiv 1$. If $\gamma \equiv B$, then the curve in (ii) becomes $y^2 = Bx^4 + Ax^2 + 1$, which admits the rational solutions $(0, \pm 1)$. Suppose then $\gamma \not\equiv B$. Therefore, there must exist a point $P = (x, y) \in E(\mathbb{Q})$, with $x \neq 0$, such that $\alpha(P) = \gamma$.

Write $x = m/e^2$ and $y = n/e^3$ with $\gcd(m, e) = \gcd(n, e) = 1$ and $m, e \neq 0$. Let $b_1 := \gcd(m, B)$. Then, we can write $m = b_1 m_1$ and $B = b_1 b_2$ with $\gcd(m_1, b_2) = 1$. Substituting it in the equation for the elliptic curve we get

$$n^2 = b_1^2 m_1 (b_1 m_1^2 + Am_1 e^2 + b_2 e^4). \tag{4.46}$$

Hence, $b_1^2 | n^2$, which implies $b_1 | n$. Let $n = b_1 n_1$, so

$$n_1^2 = m_1 (b_1 m_1^2 + am_1 e^2 + b_2 e^4). \tag{4.47}$$

Since $\gcd(m_1, b_2) = \gcd(m_1, e) = 1$, m_1 is relatively prime with $b_1 m_1^2 + am_1 e^2 + b_2 e^4$. Since their product is a square, both terms must be squares. So, there are M, N integers such that

$$M^2 = m_1, \quad N^2 = b_1 m_1^2 + am_1 e^2 + b_2 e^4. \tag{4.48}$$

By plugging in the first equation on the second we arrive at

$$N^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4. \tag{4.49}$$

Therefore, $(N/e^2, M/e)$ is a rational point in the curve. □

Remark 4.3.6. The curve in (ii), although it has degree 4, defines an elliptic curve (together with a point $\mathcal{O}$ at infinity), i.e. a smooth projective curve of genus one.

We can always write a rational point (x_0, y_0) in this curve as $(x/z, y/z^2)$ with $x, y, z \in \mathbb{Z}$ and $z \neq 0$. Therefore, to determine if this curve has rational points or not, it suffices to determine if the Diophantine equation

$$y^2 = b_1 x^4 + Ax^2 z^2 + b_2 z^4 \tag{4.50}$$

has an integer solution (x, y, z) with $z \neq 0$. And such a solution exists if and only if $b_1 \in \mathrm{Img}(\alpha)$. This gives us a method of approximating the size of $\#\mathrm{Img}(\alpha)$. Let d_B be the number of square-free divisors (which may be negative or positive) of B. Notice that $\#\mathrm{Img}(\alpha) \in [1, d_B]$. Each time we determine if Equation (4.50) has a solution or not for a given square-free divisor b_1, we can sharpen that interval. This is described in Algorithm 1.

Algorithm 1 image_of_alpha

```
    Input: $E : y^2 = x^3 + Ax^2 + Bx$ an elliptic curve
    Output: Integers $L, U$ such that $L \leq \#\mathrm{Img}(\alpha) \leq U$
UnknownEquations ← #{square-free divisors of $B$}
PointsOnImage ← {1}
for $b_1$ square-free factor of $B$ do
    $b_2 \leftarrow B/b_1$
    if found a solution $(x, y, z)$, with $z \neq 0$, of $y^2 = b_1x^4 + Ax^2z^2 + b_2z^4$ then
        PointsOnImage ← PointsOnImage ∪ $\{b_1 \mod (\mathbb{Q}^*)^2\}$
        UnknownEquations ← UnknownEquations−1
    else if there exist no solutions in the integers then
        UnknownEquations ← UnknownEquations−1
    end if
end for
$L$ ← #PointsOnImage
$U$ ← $L$ + UnknownEquations
return $L, U$
```

There are some slightly more clever ways of checking for solutions instead of simply testing for all possible triplets (x, y, z). Below are some useful considerations.

(I) We may assume the solution (x, y, z) is pairwise coprime, since if a prime p divides any two variables, it also must divide the third one, and so the solution can be reduced to $(x/p, y/p^2, z/p)$.

(II) If $A, b_1, b_2 \leq 0$, then there are not even real solutions to the equation, so there is no need to perform a check.

(III) It is a good idea to check for solutions in $\mathbb{Z}_p$ for a large number of primes. If at least one $\mathbb{Z}_p$ fails to have solutions, then there must be no solutions in the integers. In $\mathbb{Z}_p$, the condition that (x, y, z) are pairwise coprime implies that at most one variable is $= 0$.

With this, we use Equation (4.44) to construct an algorithm for finding lower and upper bounds for the rank r, shown in Algorithm 2. This algorithm was executed for a total of 10000 inputs (all elliptic curves $E : y^2 = x^3 + Ax^2 + Bx$ for $-40 \leq A, B < 60$). Unfortunately, it managed to pinpoint the exact rank for only 22.39% of these curves, totalling 2214. There were 139 of rank 0, 1577 of rank 1, 488 of rank 2 and 10 of rank 3. Table 4.2 shows some of the conclusive results and Table 4.3 some of the inconclusive results, i.e. where only lower and upper bounds for the rank were found.

Algorithm 2 rank_of_elliptic_curve

```
    **Input:** $E : y^2 = x^3 + Ax^2 + Bx$ an elliptic curve
    **Output:** Integers $L, U$ such that $L \leq$ rank of $E \leq U$
$\overline{E} \leftarrow$ Elliptic curve given by $y^2 = x^3 - 2Ax^2 + (A^2 - 4B)x$
$L_1, U_1 \leftarrow$ image_of_alpha($E$)
$L_2, U_2 \leftarrow$ image_of_alpha($\overline{E}$)
$L \leftarrow \lceil \log_2(L_1) + \log_2(L_2) \rceil - 2$
$U \leftarrow \lfloor \log_2(U_1) + \log_2(U_2) \rfloor - 2$
**return** $L, U$
```

It is possible to use this data to visualize how the rank behaves when we vary the coefficients A and B. For each point $(A, B) \in \mathbb{Z}^2$, consider the curve $E : y^2 = x^3 + Ax^2 + Bx$ and compute and interval $[a, b]$ bounding its rank. Then, generate two images. In the first image, each coordinate is painted a color based on the value of a. The color starts at black and gets greener the higher the value of a (for example, a value of $a = 0$ would yield a black pixel, whereas a value of $a = 5$ would yield a completely green pixel). Singular curves are painted white. After this, do the same, but considering the value of b instead, generating a second picture. The result is shown in Table 4.1. In contrast to the images corresponding to the torsion subgroup, which we'll construct in Chapter 5, this one looks like just a chaotic arrengement of pixels. This goes to show how unpredictable the behavior of the rank is.

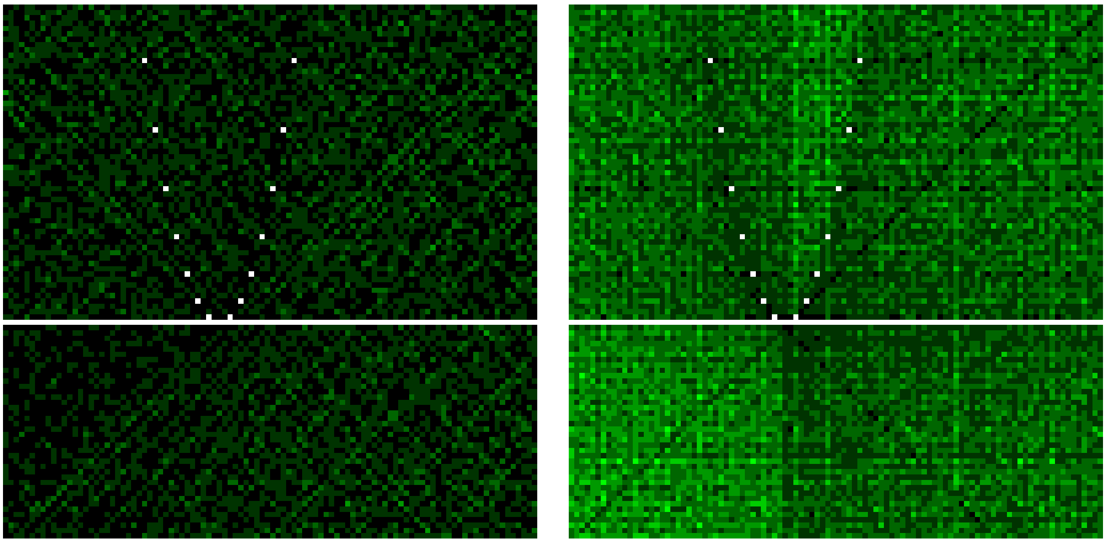


Table 4.1: Colorings of the lower bound a (left image) and the upper bound b (right image) on the rank of the elliptic curve $E : y^2 = x^3 + Ax^2 + Bx$. The parameter A corresponds to the $x-$axis, while B corresponds to the $y-$axis. Both vary from -40 to 60.

A	B	Rank	A	B	Rank	A	B	Rank	A	B	Rank
-37	37	3	24	-34	3	39	-39	3	34	56	3
40	14	3	40	23	3	47	30	3	52	47	3
56	46	3	59	42	3	-9	-39	2	-9	-30	2
-7	-33	2	-3	-38	2	-20	5	2	-19	13	2
-18	2	2	-19	19	2	-17	17	2	-16	9	2
-12	17	2	-10	10	2	-10	18	2	-3	10	2
-20	23	2	-19	22	2	-19	26	2	-17	20	2
-17	32	2	-15	34	2	-15	39	2	-14	26	2
-13	37	2	-11	26	2	-10	34	2	-5	20	2
-5	29	2	-4	37	2	-3	34	2	-20	54	2
-18	50	2	-18	57	2	-16	49	2	-15	58	2
-14	56	2	-13	52	2	-12	41	2	-11	50	2
-11	53	2	-8	41	2	-7	42	2	-6	50	2
-5	53	2	-3	58	2	-2	50	2	-1	49	2
-35	-35	2	-33	-35	2	-29	-31	2	-23	-33	2
-20	-7	1	-17	-18	1	-15	-15	1	-15	-3	1
-14	-7	1	-13	-7	1	-12	-7	1	-11	-9	1
-11	-3	1	-9	-11	1	-7	-11	1	-7	-7	1
-5	-15	1	-5	-9	1	-5	-7	1	-5	-6	1
-3	-3	1	-20	-21	1	-19	-23	1	-17	-27	1
-17	-23	1	-15	-25	1	-14	-23	1	-13	-32	1
-12	-39	1	-11	-31	1	-11	-33	1	-7	-23	1
-6	-35	1	-5	-36	1	-5	-35	1	-3	-39	1
-3	-28	1	-3	-31	1	-3	-21	1	-20	3	1
-19	2	1	-19	18	1	-18	19	1	-17	7	1
-17	14	1	-16	1	1	-16	5	1	-15	1	1
-15	3	1	-15	6	1	-15	9	1	-15	13	1
-15	10	1	-15	15	1	-19	9	0	-19	16	0
-11	10	0	-11	18	0	-10	9	0	-8	9	0
-7	1	0	-7	9	0	-6	1	0	-6	5	0
-5	4	0	-5	6	0	-5	9	0	-3	1	0
-3	2	0	-3	3	0	-2	9	0	-1	1	0
-14	25	0	-13	22	0	-13	36	0	-11	24	0
-11	25	0	-11	27	0	-6	25	0	-18	49	0
-17	42	0	-15	49	0	-14	45	0	-13	49	0
-11	49	0	-34	1	0	-31	9	0	-39	25	0
-37	25	0	-35	25	0	-27	26	0	-26	25	0
-39	49	0	-29	54	0	-22	49	0	0	-1	0
1	-20	0	1	-2	0	1	-1	0	3	-4	0
4	-5	0	6	-3	0	7	-8	0	12	-13	0

Table 4.2: Calculated ranks (part 1). For each pair (A, B), shows the exact rank of the elliptic curve $y^2 = x^3 + Ax^2 + Bx$.

A	B	Bound	A	B	Bound	A	B	Bound	A	B	Bound
-19	-19	$[0,1]$	-19	-11	$[0,1]$	-19	-9	$[0,1]$	-19	-7	$[0,1]$
-19	-5	$[0,1]$	-18	-17	$[0,1]$	-18	-11	$[0,1]$	-17	-13	$[0,1]$
-17	-11	$[0,1]$	-17	-9	$[0,1]$	-17	-7	$[0,1]$	-17	-1	$[0,1]$
-15	-19	$[0,1]$	-15	-5	$[0,1]$	-15	-1	$[0,1]$	-14	-15	$[0,1]$
-14	-13	$[0,1]$	-14	-9	$[0,1]$	-14	-5	$[0,1]$	-14	-1	$[0,1]$
-13	-19	$[0,1]$	-13	-17	$[0,1]$	-13	-14	$[0,1]$	-13	-1	$[0,1]$
-12	-13	$[0,1]$	-11	-12	$[0,1]$	-11	-5	$[0,1]$	-11	-1	$[0,1]$
-10	-19	$[0,1]$	-10	-13	$[0,1]$	-10	-11	$[0,1]$	-10	-7	$[0,1]$
-9	-15	$[0,1]$	-9	-13	$[0,1]$	-9	-3	$[0,1]$	-8	-11	$[0,1]$
-8	-9	$[0,1]$	-8	-3	$[0,1]$	-7	-18	$[0,1]$	-7	-8	$[0,1]$
-7	-1	$[0,1]$	-6	-15	$[0,1]$	-6	-7	$[0,1]$	-6	-3	$[0,1]$
-5	-14	$[0,1]$	-5	-5	$[0,1]$	-5	-3	$[0,1]$	-5	-1	$[0,1]$
-4	-5	$[0,1]$	-3	-7	$[0,1]$	-3	-4	$[0,1]$	-3	-1	$[0,1]$
-20	-15	$[1,2]$	-20	-6	$[1,2]$	-20	-4	$[1,2]$	-19	-17	$[1,2]$
-19	-4	$[1,2]$	-19	-1	$[1,2]$	-18	-19	$[1,2]$	-18	-6	$[1,2]$
-17	-16	$[1,2]$	-17	-15	$[1,2]$	-17	-8	$[1,2]$	-17	-4	$[1,2]$
-16	-17	$[1,2]$	-16	-13	$[1,2]$	-15	-17	$[1,2]$	-15	-12	$[1,2]$
-15	-8	$[1,2]$	-15	-4	$[1,2]$	-14	-19	$[1,2]$	-13	-18	$[1,2]$
-13	-16	$[1,2]$	-13	-11	$[1,2]$	-13	-9	$[1,2]$	-13	-4	$[1,2]$
-12	-14	$[1,2]$	-12	-3	$[1,2]$	-12	-1	$[1,2]$	-11	-18	$[1,2]$
-11	-15	$[1,2]$	-11	-13	$[1,2]$	-11	-2	$[1,2]$	-10	-20	$[1,2]$
-10	-15	$[1,2]$	-10	-9	$[1,2]$	-10	-4	$[1,2]$	-10	-1	$[1,2]$
-9	-19	$[1,2]$	-9	-12	$[1,2]$	-9	-10	$[1,2]$	-9	-9	$[1,2]$
-9	-5	$[1,2]$	-9	-2	$[1,2]$	-9	-1	$[1,2]$	-8	-18	$[1,2]$
-8	-19	$[1,2]$	-8	-8	$[1,2]$	-8	-7	$[1,2]$	-8	-6	$[1,2]$
-7	-17	$[1,2]$	-7	-13	$[1,2]$	-7	-14	$[1,2]$	-7	-9	$[1,2]$
-17	-19	$[2,3]$	-16	-18	$[2,3]$	-13	-15	$[2,3]$	-12	-17	$[2,3]$
-9	-14	$[2,3]$	-4	-14	$[2,3]$	-19	-24	$[2,3]$	-18	-28	$[2,3]$
-18	-23	$[2,3]$	-14	-40	$[2,3]$	-14	-34	$[2,3]$	-11	-28	$[2,3]$
-5	-22	$[2,3]$	-4	-30	$[2,3]$	-2	-28	$[2,3]$	-1	-38	$[2,3]$
-1	-24	$[2,3]$	-20	13	$[2,3]$	-14	14	$[2,3]$	-4	19	$[2,3]$
-20	38	$[2,3]$	-18	26	$[2,3]$	-16	31	$[2,3]$	-12	22	$[2,3]$
-6	26	$[2,3]$	-20	44	$[2,3]$	-16	51	$[2,3]$	-12	57	$[2,3]$
-10	48	$[2,3]$	-10	51	$[2,3]$	-10	58	$[2,3]$	-6	44	$[2,3]$
-6	54	$[2,3]$	-4	51	$[2,3]$	-1	42	$[2,3]$	-2	58	$[2,3]$
-31	-11	$[2,3]$	-39	-38	$[2,3]$	-37	-21	$[2,3]$	-36	-31	$[2,3]$
-32	-34	$[2,3]$	-32	-23	$[2,3]$	-31	-33	$[2,3]$	-30	-32	$[2,3]$
-29	-34	$[2,3]$	-27	-35	$[2,3]$	-26	-28	$[2,3]$	-25	-21	$[2,3]$
-40	10	$[2,3]$	-38	11	$[2,3]$	-34	3	$[2,3]$	-25	4	$[2,3]$
-40	43	$[3,4]$	34	-34	$[3,4]$	26	46	$[3,4]$	50	-2	$[3,4]$

Table 4.3: Calculated ranks (part 2). For each pair (A, B), shows an interval bounding the of the elliptic curve $y^2 = x^3 + Ax^2 + Bx$.

Chapter 5

The Torsion and the Nagell-Lutz Theorem

As we've seen in the previous chapter, the Mordell-Weil Theorem tells us that if E is an elliptic curve defined over $\mathbb{Q}$, then the group $E(\mathbb{Q})$ is finitely generated. By the classification of finitely generated abelian groups, we can thus write it as

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}. \tag{5.1}$$

The value r is called the *rank* of E. The term $E(\mathbb{Q})_{\text{tors}}$ is a finite group and is called the *torsion subgroup of* E. However, the theorem provides no insight into how to actually calculate these objects. This chapter will address the issue of calculating the torsion subgroup. As we shall see, in contrast to the previous chapter, where we only had partial methods for calculating the rank, the torsion is much more well-behaved and can be fully calculated in all cases. There are two important arithmetic results: the Mazur Theorem and the Nagell-Lutz theorem. The first classifies all possible torsion subgroups. The second shows a simple finite set containing all points of finite order, and thus reduces the problem of calculating $E(\mathbb{Q})_{\text{tors}}$ to a finite number of checks, which can be performed by a computer.

Theorem 5.0.1 (Mazur [26, 27])**.** Let E be an elliptic curve defined over $\mathbb{Q}$. Then, the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ is one of the following fifteen groups:

$$\mathbb{Z}_n,\ 1 \leq n \leq 10 \text{ or } n = 12; \quad \mathbb{Z}_2 \times \mathbb{Z}_n,\ 1 \leq n \leq 4.$$

Since the Mordell-Weil Theorem extends to elliptic curves defined over a number field K, it is natural to ask if $\#E(K)_{\text{tors}}$ is also bounded by a constant which depends only on K. It turns out that this bound exists and depends only on the degree $[K : \mathbb{Q}]$. This was proved in [20] for all quadratic fields and in [28] for all number fields. Moreover, there are various classification theorems for these torsion subgroups [25].

For the remainder of this section, let E be an elliptic curve given by the Weierstrass equation $y^2 = F(x)$ with $F(x) := x^3 + Ax^2 + Bx + C$, where $A, B, C \in \mathbb{Z}$. Its discriminant is given by

$$\Delta = -4B^3 - 27C^2 - 4A^3C - 27C^2 + 18ABC + A^2B^2. \tag{5.2}$$

Our goal in this section is to prove the Nagell-Lutz Theorem, stated below.

Theorem 5.0.2 (Nagell-Lutz)**.** Let (x, y) be a point of finite order in $E(\mathbb{Q})$, then

1. x and y are integers,
2. either $y = 0$, in this case the order is 2, or y^2 divides Δ.

The proof of this theorem is long, but achievable by elementary methods. Some proofs can be found in [38, page 56], [43]. The first, however, omits a necessary technical result (namely 5.1.4). Another book by the same author [37, page 221] provides a different proof using the notion of formal groups. Lastly, a quick proof can be achieved by finding a clever inductive formula for adding a point to itself n times [1]. It is important to note that Nagell-Lutz can't be generalized much further beyond Weierstrass equations (i.e. equations of the form $y^2 = x^3 + Ax^2 + Bx + C$). More concretely, Silverman points that $(-1/4, 1/8)$ is a point of order two of the curve

$$y^2 + xy = x^3 + 4x + 1,$$

which is not in Weierstrass form. It will be useful to first give a rough sketch of the proof.

(I) Given a prime p, exhibit a chain of subgroups $E(\mathbb{Q}) \supseteq E_p^1 \supseteq E_p^2 \supseteq ...$ that contains points with higher and higher powers of p in the denominator.

(II) Show that E_p^1 is torsion-free, which implies any point with p in the denominator must have infinite order. As this is true for any prime p, any torsion point must have integer coordinates.

(III) Show that $y^2 \mid \Delta$ by using the well-known formula for the discriminant in terms of the resultant. In our case, $\Delta = -\text{Res}(F, F')$.

The first thing we do is to change coordinates. Given a point $P = [a : b : c] \in E(\mathbb{Q})$ with $b \neq 0$, we let its $ts-$coordinates be

$$t(P) = a/b, \quad s(P) = c/b. \tag{5.3}$$

Notice that $\mathcal{O} = (0, 0)$ in $ts-$coordinates, and the "points at infinity" in this coordinate system are precisely the points of order two, i.e. points $[x : 0 : 1]$. This transformation is simply a change of charts, so it maps lines to lines and preserves the multiplicities of intersections. So, we can add points in the $ts-$plane just as we add points in the $xy-$plane. The curve E can be rewriten in terms of the $ts-$coordinates, yielding a new curve $\tilde{E}$ isomorphic to E given by

$$\tilde{E} : s = t^3 + At^2s + Bts^2 + Cs^3. \tag{5.4}$$

Remark 5.0.3. Recall that the inverse operation $P \mapsto -P$ is done by tracing a line through $P, \mathcal{O}$ and picking the third point of intersection. In $ts-$coordinates, $\mathcal{O} = (0,0)$, so inverse is simply taking the negative of a point (i.e. $-(t,s) = (-t,-s)$).

Notation 5.0.4. Given a point $P_i \in E(\mathbb{Q})$, $P_i \neq \mathcal{O}$, we'll denote its $xy-$coordinates by (x_i, y_i). If we also have $y_i \neq 0$, we'll denote its $ts-$coordinates as (t_i, s_i). The $ts-$coordinates of $\mathcal{O}$ are, of course, $(0,0)$. If we write P for a point in $E(\mathbb{Q})$ (now without subscript) given the appropriate conditions mentioned above, its coordinates will respectively be x, y, t, s.

5.1 Points of finite order have integer coordinates

We'll start with the hardest part of the proof, namely showing that torsion points have integer $xy-$coordinates. Let $P \in E(\mathbb{Q})$, $P \neq \mathcal{O}$. Notice that, if $x = 0$, then $y = \sqrt{C}$, which must be an integer (since $y \in \mathbb{Q}$ and $C \in \mathbb{Z}$). If, on the other hand, $y = 0$, then x must be a root of $x^3 + Ax^2 + Bx + C$. Since this is a monic polynomial with integer coefficients, its roots must be integers also, so x is an integer. Therefore, the case where one of the $xy-$coordinates is zero is trivial. Our strategy for the case where $x \neq 0 \neq y$ is to tackle the problem "one prime at a time", showing that no prime divides the denominator of x or y.

Let v_p be the standard $p-$adic valuation in $\mathbb{Z}$ defined in 2.4.33. Our goal is then to show that if P has finite order then for all primes p we have $v_p(x) \geq 0$ and $v_p(y) \geq 0$. It is a good idea to examine the case where this doesn't hold, namely $v_p(x) < 0$ or $v_p(y) < 0$. This case is solved by Proposition 3.0.4, which motivates the introduction of the following set.

Definition 5.1.1. Given a prime p and an integer $r \geq 1$, define

$$E_p^r := \{(x,y) \in E(\mathbb{Q}) \; : \; v_p(x) \leq -2r, v_p(y) \leq -3r\} \cup \{\mathcal{O}\}.$$

These sets are what is called a "filtration", in the sense that they belong to a chain of inclusions. In the near future, we'll see this is not only a chain of subsets, but also a chain of subgroups.

$$E(\mathbb{Q}) \supseteq E_p^1 \supseteq E_p^2 \supseteq E_p^3 \supseteq ... \tag{5.5}$$

We now state a Proposition which allows us to represent E_p^r in terms of $ts-$coordinates.

Proposition 5.1.2. The following hold.

(i) $(x,y) \in E_p^r \iff v_p(s) \geq 3r$ and $v_p(t) \geq r$.

(ii) $(x,y) \in E_p^r$ and $(x,y) \notin E_p^{r+1} \iff v_p(s) = 3r$ and $v_p(t) = r$

Proof. (i $\Rightarrow$) By Proposition 3.0.4, we know there is $l \geq 1$ such that $v_p(x) = -2l$ and $v_p(y) = -3l$. The hypothesis guaratees to us that $l \geq r$. So, we have $v_p(s) = -v_p(y) = 3l \geq 3r$ and $v_p(t) = v_p(x) - v_p(y) = -2l + 3l = l \geq r$. (i $\Leftarrow$) We have $v_p(y) = -v_p(s) \leq -3r$ and so by Proposition 3.0.4 there must be $l \geq r$ such that $v_p(x) \leq -2l$ and $v_p(y) \leq -3l$. (ii $\Rightarrow$) In this case, $v_p(x) = -2r$ and $v_p(y) = -3r$. Hence, $v_p(s) = -v_p(y) = 3r$ and $v_p(t) = v_p(x) - v_p(y) = r$. (ii $\Leftarrow$) Conversely, if these two equalities hold, we have that $v_p(y) = -v_p(s) = -3r$ and $v_p(x) = v_p(t) + v_p(y) = r - 3r = -2r$. □

Notation 5.1.3. Given a prime p, we write R_p for the localization of $\mathbb{Q}$ at the ideal generated by p, i.e. $R_p := \{x \in \mathbb{Q} \,:\, v_p(x) \geq 0\}$ (see Proposition 2.4.35). Given two rational numbers $a, b \in \mathbb{Q}$, we say $a \equiv b \mod p^r$ if $a - b \in p^r R_p$.

The first main step of the proof is showing that E_p^r is a subgroup of $E(\mathbb{Q})$. For that, we'll first derive a formula for a line in $ts-$coordinates passing through two points in E_p^r. First, we need the following technical Lemma that excludes a degenerate case.

Lemma 5.1.4. Let L be a line given by the equation $t = c$ in the $ts-$plane with $c \equiv 0 \mod p$. Suppose L intersects $\tilde{E}(\mathbb{Q})$ at a point (t, s) with $s \equiv 0 \mod p$. Then,

(i) (t, s) is the only point in $L \cap \tilde{E}(\mathbb{Q})$ with $s \equiv 0 \mod p$,

(ii) the line L is not tangent to (t, s).

Proof. (i) First, we'll show uniqueness. Suppose (t_1, s_1) and (t_2, s_2) are two points of intersection such that $s_1 \equiv 0 \equiv s_2 \mod p$. We'll prove they are equal by showing, by induction, that $s_1 \equiv s_2 \mod p^k$ for all $k \geq 1$. The base case is the hypothesis. Suppose, then, by induction, that $s_1 \equiv s_2 \mod p^k$ for some $k \geq 1$. Then, by methods of number theory (Proposition 7.0.1 in the Appendix), we know that $s_1^2 \equiv s_2^2 \mod p^{k+1}$ and $s_1^3 \equiv s_2^3 \mod p^{k+2}$. Therefore, by plugging $t = c$ in the Weierstrass equation we have

$$s_1 = c^3 + Ac^2 s_1 + Bcs_1^2 + Cs_1^3 \equiv c^3 + Ac^2 s_2 + Bcs_2^2 + Cs_2^3 = s_2 \mod p^{k+1}.$$

Hence, $s_1 = s_2$. And so, since $t_1 = c = t_2$, the points are equal. (ii) For the second part, we have to calculate the slope of the tangent line at (t_1, s_1). By doing implicit differentiation and isolating ds/dt we have

$$ds/dt = \frac{3t_1^2 + 2Ats_1 + Bs_1^2}{1 - At_1^2 - 2Bs_1t_1 - 3Cs_1^2}. \tag{5.6}$$

Suppose by contradiction that the line L is the tangent line. Then, ds/dt must be ∞, so the denominator of ds/dt must be zero. But since $t_1 = c \equiv s_1 \equiv 0 \mod p$,

$$0 = 1 - At_1^2 - 2Bs_1t_1 - 3Cs_1^2 \equiv 1 \mod p,$$

which is a contradiction since no prime divides 1. Thus, L cannot be the tangent line, and this concludes the proof. □

Lemma 5.1.5. Let $P_1, P_2 \in E_p^r \setminus \{\mathcal{O}\}$. Then, the line L in the $ts-$plane passing through P_1 and P_2 (the tangent line if $P_1 = P_2$) has the form $s = \alpha t + \beta$ with

$$\alpha = \frac{t_2^2 + t_1 t_2 + t_1^2 + A(t_2 + t_1)s_2 + Bs_2^2}{1 - At_1^2 - B(s_1 + s_2)t_1 - C(s_2^2 + s_1 s_2 + s_1^2)}.$$

Proof. (Case 1: $t_1 = t_2$ and $s_1 \neq s_2$) In this case, L is given by $t = t_1$. Proposition 5.1.2 tells us that $v_p(t_1) > 0$, and thus $t_1 \equiv 0 \mod p$. We therefore fit into the conditions of Lemma 5.1.4, and hence $P_1 = P_2$, which is a contradiction. So this case doesn't happen.

(Case 2: $P_1 = P_2$) In this case, we have to calculate the tangent line L through P_1. Suppose the line has infinite slope (i.e. given by $t = t_1$). Then, Lemma 5.1.4 tells us that L cannot be the tangent line. So the slope of L must be finite, and hence L must be of the form $s = \alpha t + \beta$. By doing implicit differentiation and isolating the term ds/dt, we arrive at (5.6), which is equal the desired expression by setting $t_1 = t_2$ and $s_1 = s_2$.

(Case 3: $t_1 \neq t_2$) In this case, the line L must be of the form $s = \alpha t + \beta$ with $\alpha = (s_2 - s_1)/(t_2 - t_1)$. If we subtract the equation of $\tilde{E}$ at P_2 from the one at P_1 we get

$$s_2 - s_1 = (t_2^3 - t_1^3) + A(t_2^2 s_2 - t_1^2 s_1) + B(t_2 s_2^2 - t_1 s_1^2) + C(s_2^3 - s_1^3).$$

But each of the three terms on the right can be decomposed into multiples of $t_2 - t_1$ and $s_2 - s_1$. More concretely,

$$\begin{aligned} t_2^3 - t_1^2 &= (t_2 - t_1)(t_2^2 + t_1 t_2 + t_1^2), \\ A(t_2^2 s_2 - t_1^2 s_1) &= A(t_2 - t_1)(t_2 + t_1)s_1 + A(s_2 - s_1)t_2^2, \\ B(t_2 s_2^2 - t_1 s_1^2) &= B(s_2 - s_1)(s_2 + s_1)t_1 + B(t_2 - t_1)s_2^2, \\ C(s_2^3 - s_1^3) &= C(s_2 - s_1)(s_2^2 + s_2 s_1 + s_1^2). \end{aligned}$$

By isolating the term $(s_2 - s_1)/(t_2 - t_1)$ we arrive at the desired expression. And this concludes the proof. □

The following is a key step to showing that E_p^r is a subgroup of $E(\mathbb{Q})$.

Proposition 5.1.6. Let $P_1, P_2, P_3 \in E(\mathbb{Q})$ with $P_1, P_2 \in E_p^r$. Then,

$$P_1 \oplus P_2 \oplus P_3 = \mathcal{O} \implies \begin{cases} t_1 + t_2 + t_3 \equiv 0 \mod p^{3r}, \\ s_3 \equiv 0 \mod p^{3r}. \end{cases}$$

Proof. Since the points P_1 and P_2 are in E_p^r, by Proposition 5.1.2 we have that

$$t_1 \equiv t_2 \equiv 0 \mod p^r, \quad s_2 \equiv s_1 \equiv 0 \mod p^{3r}. \tag{5.7}$$

First, assume some point is equal to $\mathcal{O}$, say, $P_1 = \mathcal{O}$. In this case, we have that $P_2 = -P_3$. And so $t_2 = -t_3$ and $s_2 = -s_3$. Therefore, $t_1 + t_2 + t_3 = 0 - t_3 + t_3 = 0$ and $s_3 = -s_2 \equiv 0 \mod p^{3r}$. So this case is trivial. Assume then that $P_i \neq \mathcal{O}$ for all i. In this case, P_1 and P_2 fit into the requirements of Lemma 5.1.5, and so the line passing through them is $L : s = \alpha t + \beta$ and we have an expression for α. We'll first analyze the valuation of α and β. The numerator and denominator of α have the following valuations.

$$v_p(t_2^2 + t_1t_2 + t_1^2 + A(t_2 + t_1)s_2 + Bs_2^2) \geq \min(2r, v_p(A) + 4r, v_p(B) + 6r) = 2r, \tag{5.8}$$

$$v_p(1 - At_1^2 - B(s_1 + s_2)t_1 - C(s_2^2 + s_1s_2 + s_1^2)) = 0. \tag{5.9}$$

The latter equation is true because we're calculating the valuation of 1+ (something with strictly positive valuation), therefore, it must be *equal* to the minimum, which is zero. Therefore, $v_p(\alpha) \geq 2r$. Now, since $\beta = s_1 - \alpha t_1$ we have

$$v_p(\beta) = v_p(s_1 - \alpha t_1) \geq \min(v_p(s_1), v_p(\alpha) + v_p(t_1)) \geq \min(3r, 2r + r) = 3r. \tag{5.10}$$

Hence, in the end, we conclude the following.

$$v_p(\alpha) \geq 2r, \quad v_p(\beta) \geq 3r. \tag{5.11}$$

Now we plug the equation for L into the equation for $\tilde{E}$ and collect terms. The result is a polynomial on t which has the following form.

$$0 = t^3(1 + A\alpha + B\alpha^2 + C\alpha^3) + t^2(A\beta + 2B\alpha\beta + 3C\alpha^2\beta) + (\text{terms or order } \leq 1). \tag{5.12}$$

By Equation (5.11), α has strictly positive valuation, and so the coefficient of t^3 can't be zero. This equation then must have three roots t_1, t_2, t_3. Using the relations between roots and coefficients of a polynomial we get

$$t_1 + t_2 + t_3 = \frac{A\beta + 2B\alpha\beta + 3C\alpha^2\beta}{1 + A\alpha + B\alpha^2 + C\alpha^3}. \tag{5.13}$$

We'll show that the right-hand size is equivalent to zero mod p^{3r}, which will prove the first part of the Lemma. The valuations of the numerator and denominator are

$$\begin{aligned} v_p(A\beta + 2B\alpha\beta + 3C\alpha^2\beta) &\geq \min(v_p(A\beta), v_p(2B\alpha\beta), v_p(3C\alpha^2\beta)) && (5.14)\\ &\geq \min(v_p(A) + 3r, v_p(2B) + 5r, v_p(3C) + 7r) \geq 3r. && (5.15)\\ v_p(1 + A\alpha + B\alpha^2 + C\alpha^3) &= \min(0, v_p(A\alpha + B\alpha^2 + C\alpha^3)) = 0. && (5.16) \end{aligned}$$

And so indeed $t_1 + t_2 + t_3 \equiv 0 \mod p^{3r}$. From this, we know that $t_3 = cp^{3r} + t_1 + t_2$ for some c and so $v_p(t_3) \geq r$. Then, $v_p(s_3) = v_p(\alpha t_3 + \beta) \geq \min(3r, 3r) = 3r$. And this concludes the proof. □

Corollary 5.1.7. E_p^r is a subgroup of $E(\mathbb{Q})$.

Proof. By Proposition 5.1.2, $P = (t, s) \in E_p^r$ is equivalent to $t \equiv 0 \mod p$ and $s \equiv 0 \mod p^{3r}$. Let $P_1, P_2 \in E_p^r$. First, E_p^r is closed by inverses since $-P_1$ has $ts-$coordinates $(-t_1, -s_1)$, which clearly satisfy the congruence conditions. Now, let $(t_3, s_3) = P_3 := P_1 \oplus P_2$. Then, $P_1 \oplus P_2 \oplus (-P_3) = \mathcal{O}$, and so by Proposition 5.1.6 we have that $s_3 \equiv 0 \mod p^{3r}$ and $t_1 + t_2 - t_3 \equiv 0 \mod p^{3r}$, which means $t_3 \equiv t_1 + t_2 \equiv 0 \mod p$. □

Now, we would like to define a map from E_p^r to a simpler group.

Proposition 5.1.8. Consider the map $\lambda_r : E_p^r \to p^r R_p / p^{3r} R_p$ given by $\lambda(P) := t$. Then, λ_r is a group homomorphism with $\text{Ker}(\lambda_r) = E_p^{3r}$.

Proof. Let $P_1 \oplus P_2 = P_3$. λ_r is well-defined since the $t-$coordinate of any point $P \in E_p^r$ has $v_p(t) \geq r$, and hence $t \in p^r R_p$. Notice that $\lambda_r(\mathcal{O}) = 0$ and $\lambda_r(P_1 + P_2) = t_3 \equiv t_1 + t_2 = \lambda_r(P_1) + \lambda_r(P_2) \mod p^{3r}$ by Proposition 5.1.6. So it is a group homomorphism.

Now, clearly $E_p^{3r} \subseteq \text{Ker}(\lambda_r)$. To show the other inclusion, pick $P \in \text{Ker}(\lambda_r)$. So $v_p(t), v_p(s) \geq 3r$ and $v_p(y) = -v_p(s) < 0$. By Proposition 3.0.4, $v_p(y) = -3u, v_p(x) = -2u$ for some integer $u \geq 1$. We have

$$-2u - 3r = v_p(x) - 3r = v_p(t) + v_p(y) - 3r \geq v_p(y) = -3u. \tag{5.17}$$

So $u \geq 3r$. This means $P \in E_p^{3r}$. □

By the First Isomorphism Theorem, we have an injective map $\lambda_r : E_p^r / E_p^{3r} \to p^r R_p / p^{3r} R_p$.

Proposition 5.1.9. The group E_p^1 is torsion-free.

Proof. Suppose there is a point $P \in E_p^1$ with order $m > 1$. We have two cases to consider. (Case 1: $p \nmid m$) Let r be such that $P \in E_p^r$ but $P \notin E_p^{r+1}$. So, by Proposition 5.1.2, $v_p(t) = r$. But then

$$0 \not\equiv m\lambda_r(P) \equiv \lambda_r(mP) = \lambda_r(\mathcal{O}) = 0 \mod p^{r+1}.$$

Which is a contradiction. (Case 2: $p \mid m$) In this case, $(t', s') = P' := (m/p)P$ has order p. Let r be such that $P' \in E_p^r$ but $P' \notin E_p^{r+1}$. So, $v_p(t') = r$ and $0 \not\equiv \lambda_r(P') \mod p^{r+1}$. But we also have

$$p\lambda_r(P') \equiv \lambda_r(pP') = 0 \mod p^{3r},$$

and so $\lambda_r(P') \equiv 0 \mod p^{3r-1}$. Since $3r - 1 \geq r + 1$, we have a contradiction. □

5.2 Proving Nagell-Lutz

We are now ready to give a proof of Theorem 5.0.2.

Proof of Theorem 5.0.2. Let $P_1 = (x_1, y_1) \in E(\mathbb{Q})$. First of all, if $x_1 = 0$ or $y_1 = 0$, we know that the point must have order 2 and integer coordinates by the argument at the beginning of the previous section. Assume then $x_1 \neq 0 \neq y_1$. To prove the first part, assume P_1 does not have integer coordinates. Then, there must be a prime p such that $v_p(x_1) < 0$ or $v_p(y_1) < 0$. By Proposition 3.0.4, $P_1 \in E_p^1$ which has no torsion points by Proposition 5.1.9.

To prove the second part, we use the first part. Let $F(x) := x^3 + Ax^2 + Bx + C$. Since P_1 has finite order, $P_2 := 2P_1 = (x_2, y_2)$ must have as well, and $P_2 \neq \mathcal{O}$ since we're assuming $y_1 \neq 0$. So, P_2 has integer coordinates and thus by the duplication formula

$$2x_1 + x_2 = \left(\frac{P'(x_1)}{2y_1}\right)^2 \in \mathbb{Z}. \tag{5.18}$$

Now, the formula for the discriminant in terms of the resultant says $\Delta = -\text{Res}(F, F')$. It is a standard fact that the resultant of two polynomials belongs to the ideal generated by them. Therefore, there must be a way to write Δ as a combination of F and F'.

$$H(x)F(x) + S(x)F'(x) = \Delta. \tag{5.19}$$

By the equation of the elliptic curve we know that $y_1^2 = F(x_1)$, and since the term in Equation (5.18) is an integer, it follows that $F(x_1) \mid (F'(x_1))^2$. Therefore, we conclude that $y_1^2 \mid \Delta$, which completes the proof of the Nagell-Lutz Theorem. □

5.3 Calculating the torsion

The main application of Nagell-Lutz Theorem is the calculation of $E(\mathbb{Q})_{\text{tors}}$. Given a torsion point $P = (x, y)$, we know that either $y = 0$ or y^2 divides Δ and so there are only a finite number of possibilities to check. For each possibility of y, say, y_0, we must find all integer roots of the equation

$$x^3 + Ax^2 + Bx + (C - y_0^2) = 0. \tag{5.20}$$

This is a monic polynomial in $\mathbb{Z}[x]$ and so any integer root x_0 must divide the constant term. This leaves a finite number of possibilities for x_0 also. After compiling a set $L := \{(x_0, y_0), ..., (x_N, y_N)\}$ of all possible torsion points, it remains to calculate the order of each of them. To that end, if $P_i = (x_i, y_i)$, it suffices to compute mP_i until we either (1) reach $\mathcal{O}$, in this case the order is m, or (2) reach a point outside L, in this case the order is ∞. From there, we collect all points of finite order and determine which group it must be. One quick way of doing this is using Mazur's Theorem 5.0.1 which reduces the number of possibilities to 15. This whole process is layed out in Algorithm 3.

Thanks to Mazur's classification Theorem there is a nice way of visualizing the patterns among torsions of different elliptic curves. This First of all, any point $v := (A, B, C) \in \mathbb{Z}^3$

Algorithm 3 calculate_torsion_subgroup

```
Input: $E : y^2 = x^3 + Ax^2 + Bx + C$ elliptic curve
Output: $G$ the torsion subgroup of $E$
$G \leftarrow \{\mathcal{O}\}$
for $y \in \mathbb{Z}$ such that $y = 0$ or $y^2 | \Delta$ do
    for $x \in \mathbb{Z}$ such that $x^3 + Ax^2 + Bx + (C - y^2) = 0$ do
        if $R :=$ "order of $(x, y)$" is not infinite then
            $G \leftarrow G \cup \{(x, y)\}$
        end if
    end for
end for
return $G$
```

can be thought of as a curve $E_v : y^2 = x^3 + Ax^2 + Bx + C$, which may be either singular or an elliptic curve. By assigning a different color for each of the 15 torsion possibilities in Theorem 5.0.1 (plus an additional 16th color for singular curves) we obtain a coloring of $\mathbb{Z}^3$. By examining different cross-sections of this coloring we get a geometric visualization of how the torsion behaves as we change the parameters A, B, C.

Group	Color	Group	Color	Group	Color	Group	Color
Singular	□	$\mathbb{Z}_4$	🟩	$\mathbb{Z}_8$	🟪	$\mathbb{Z}_2 \times \mathbb{Z}_2$	🟥
$\mathbb{Z}_1$	■	$\mathbb{Z}_5$	🟥	$\mathbb{Z}_9$	■	$\mathbb{Z}_2 \times \mathbb{Z}_4$	🟨
$\mathbb{Z}_2$	🟦	$\mathbb{Z}_6$	🟪	$\mathbb{Z}_{10}$	■	$\mathbb{Z}_2 \times \mathbb{Z}_6$	🟧
$\mathbb{Z}_3$	🟦	$\mathbb{Z}_7$	🟩	$\mathbb{Z}_{12}$	□	$\mathbb{Z}_2 \times \mathbb{Z}_8$	🟧

Table 5.1: Assigning colors to each torsion subgroup.

Some cross-sections of this $\mathbb{Z}^3$ coloring are shown in Table 5.2. The image at position (i, j) corresponds to fixing the $j-$th coordinate (the coordinates are, respectively, A, B, C) equal to $i - 3$, and then letting the other two coordinates vary in the interval $[-50, 49]$. For example, let $I_{i,j}$ be the points appearing in the image at line i, row j of the table. Then,

$$I_{2,3} = \{(A, B, C) \ : \ C = -1, -50 \leq A, B \leq 49\}. \tag{5.21}$$

Just from these 15 small sections of the coloring, one can already see vastly different patterns. For example, $I_{3,3}$ (i.e. fixing $C = 0$) contains no elliptic curve with trivial torsion. This is clear from its equation $y^2 = x^3 + Ax^2 + Bx$: the point $(0, 0)$ is always a point of order two. Another observation is that, at points where two colored pieces cross, the corresponding torsion seems to be the product of the torsion in each piece. For example, two blue lines (corresponding to torsion $\mathbb{Z}_2$) usually meet at a pink point (torsion $\mathbb{Z}_2 \times \mathbb{Z}_2$). The reader can play with these cross-sections by themselves by cloning the repository by the author [32], where currently more than 100 million torsion subgroups were calculated, and therefore the generated images are much bigger.

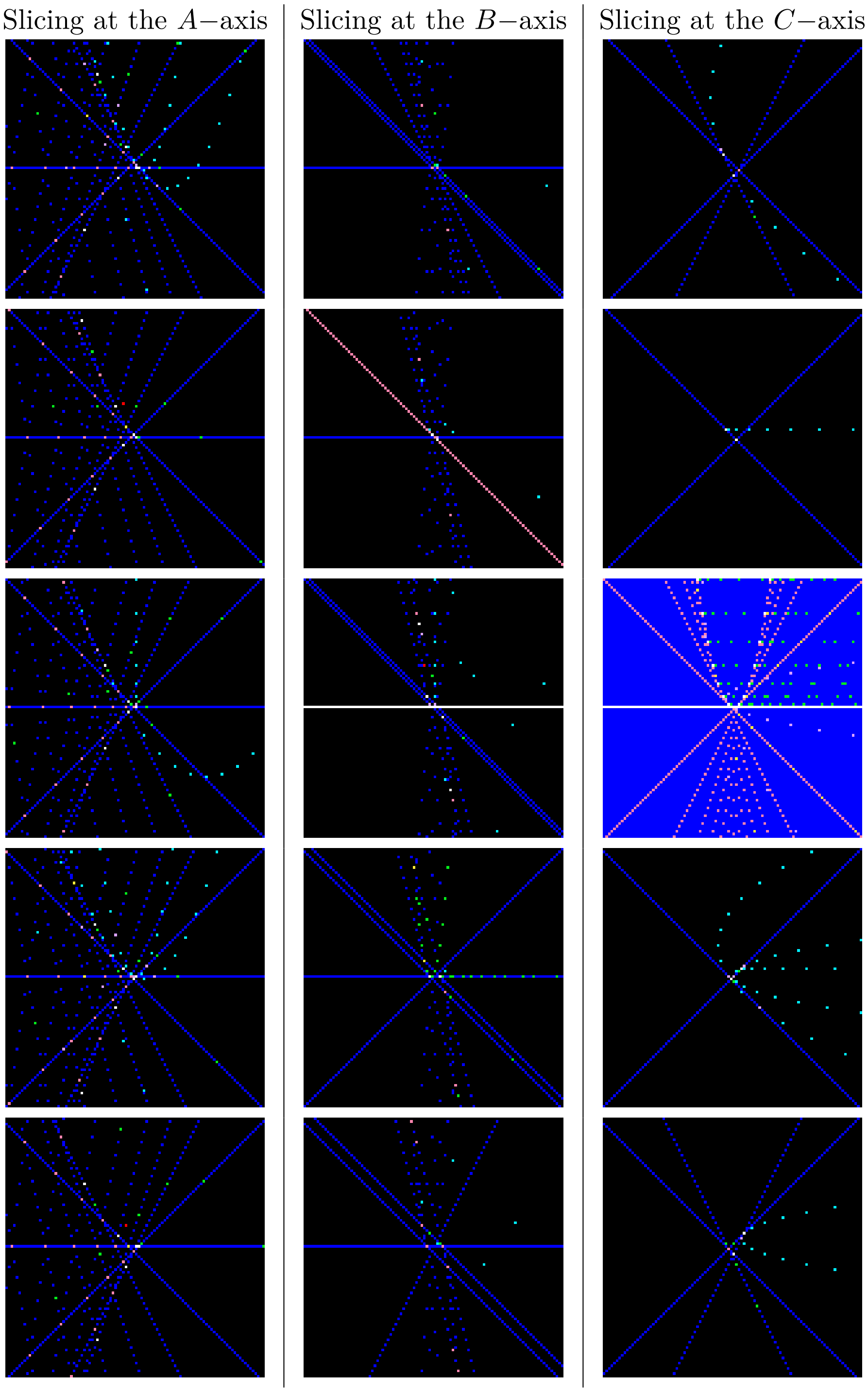


Table 5.2: Each image displays a cross-section of the $\mathbb{Z}^3$ coloring centered at the origin. The entry (i, j) of the image corresponds to slicing at the $j-$th coordinate equal to $i - 3$.

Besides the aesthetic aspect of this visualization, one can also use them to construct families of elliptic curves with fixed torsion (or fixed subgroup of the torsion). This seems to be a rather non-trivial task without the visual aid. Here, it is simply a matter of observing patterns in the images and trying to prove them. Below we show two examples, corresponding to the light-blue parabola and a blue line in image $(3, 1)$. Since this visualization was conceived by the author, these examples serve as contributions of this work.

Proposition 5.3.1. Let n be an integer and E_n be the elliptic curve given by

$$E_n : y^2 = x^3 + (3 + 6n)x + (n^2 - 8n - 11).$$

Then, $\mathbb{Z}_3$ is a subgroup of $E_n(\mathbb{Q})_{\text{tors}}$.

Proof. This parametrizes the light-blue parabola in image (3, 1) in Table 5.2. The proposition says E_n always has a rational point of order three. To prove this, suppose $P = (p, q)$ is a rational point of order three. Then, $2P = -P$. Assume $q \neq 0$ and let $ux + v$ be the tangent line to P. By the duplication formula, we know that the $x-$coordinate of $2P$ is equal to $u^2 - 2p$. But the $x-$coordinate of $2P = -P$ is p. Therefore, $3p = u^2$. If we expand this expression (by using the fact that $u = (3p^2 + 3 + 6n)/2q$) we get

$$0 = 12pq^2 - (3p^2 + 3 + 6n)^2.$$

If we eliminate q^2 by using the equation for E_n, we arrive at a polynomial on p and n. This polynomial always has a root at $p = 3$. It remains to check if this yields a point in $E(\mathbb{Q})$ or not. By substituting $p = 3$ in the equation for the elliptic curve we get

$$\begin{aligned} q^2 &= 3^3 + (3 + 6n) \cdot 3 + (n^2 - 8n - 11) \\ &= n^2 + 10n + 25 \\ &= (n + 5)^2. \end{aligned}$$

So, the points $(3, \pm(n + 5))$ are always rational points of order three in E_n. And this completes the proof. □

Proposition 5.3.2. Let a, n be integers such that $4(3 - a) = (n^3 + 3)^2$. Consider the elliptic curve E_a given by

$$E_a : y^2 = x^3 - ax - a + 1.$$

Then, $\mathbb{Z}_4$ is a subgroup of $E(\mathbb{Q})_{\text{tors}}$.

Proof. This parametrizes one of the blue diagonal lines in image (3, 1) in Table 5.2. We aim to show that E_a always has a rational point of order 4. Suppose that $P = (p, p')$ is a rational point of order 4. Notice that $(-1, 0)$ is always a rational point of order 2 of E_a. Suppose then that $2P = (-1, 0)$. Let $ux + v$ be the tangent line to P. Substituting in the equation for E_a and dividing by the root representing the point $(-1, 0)$ (i.e., $x + 1 = 0$) we get the quadratic

$$x^2 - (u^2 + 1)x + 1 - a - u^2 = 0.$$

This should have a double root at p. Therefore, the discriminant should be equal to zero. So, $0 = (u^2 + 1)^2 - 4(1 - a - u^2)$. By simplifying some things we get the following equation.

$$-(4a - 3) = u^4 + 6u^2. \tag{5.22}$$

Now, by the duplication formula,

$$-1 = u^2 - 2p. \tag{5.23}$$

By using this equality, we can remove the term u from equation (5.22) in the following way.

$$-(4a - 3) = u^4 + 6u^2 = u^2(u^2 + 6) = (-1 + 2p)(5 + 2p).$$

By simplifying things a bit we arrive at the polynomial

$$4p^2 + 8p + 4a - 8 = 0. \tag{5.24}$$

Solving this for p we get that

$$p = -1 \pm \sqrt{3 - a}. \tag{5.25}$$

So any point $P = (p, p')$ such that $2P = (-1, 0)$ must have p in this form. If you plug this expression for p in equation (5.23) you'll see the equality holds only for the + term. The remaining question is: when does this expression for p gives a rational point in the elliptic curve? First of all, p is an integer if and only if $3 - a$ is a square number. Now, there are two possibilities for p', namely

$$\pm\sqrt{p^3 - ap - a + 1} = \pm\sqrt{(3 - a)(2\sqrt{3 - a} - 3)}.$$

Since $(3 - a)$ is a square number, it follows that p' is an integer if and only if $2\sqrt{3 - a} - 3$ is also a square number. Call it n^2. In other words, $4(3 - a) = (n^2 + 3)^2$, which is true by assumption. Hence, the point

$$P = \left(-1 + \sqrt{3 - a}, \pm\sqrt{(3 - a)(2\sqrt{3 - a} - 3)}\right)$$

is always a point of order 4 in E_a. And this completes the proof. □

Proposition 5.3.3 ([17])**.** Let a be a fourth-power free integer and E_a be the ellptic curve given by the equation

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

Then, the torsion subgroup of $E(\mathbb{Q})$ is classified as follows

$$E_a(\mathbb{Q})_{\text{tors}} = \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}_2 & \text{if } -a \text{ is a square,} \\ \mathbb{Z}_4 & \text{if } a = 4, \\ \mathbb{Z}_2 & \text{otherwise.} \end{cases}$$

Proof. This parametrizes the horizontal blue line in image (3, 1) in Table 5.2. This proof will consist of six parts. We'll classify, respectively, the points of order 2, 4, 2^k, 3 and 5. Lastly, we'll use Theorem 5.0.1, which classifies all possible torsion subgroups, to conclude the proof. Here we denote the set of points with exact order m by $E[m]$.

Part 1: $2-$**torsion points**

First of all, let $P = (p, p')$ be a $2-$torsion points. In this case, p' must be zero so we have $x^3 + ax = x(x^2 + a) = 0$. This equation has 3 rational roots $\{(0,0), (\pm\sqrt{-a}, 0)\}$ if and only if $-a$ is a square. If not, the only rational root is $(0,0)$. So, we have the following.

	$-a$ is a square	$a = 4$	else
$E[2]$	$\{(0,0), (\pm\sqrt{-a}, 0)\}$	$\{(0,0)\}$	$\{(0,0)\}$

Part 2: $4-$**torsion points**

Let $P = (p, p')$ be a $4-$torsion point. Then, $(q, q') = Q := 2P$ is a $2-$torsion point. From the previous case, there are two possibilities for Q.

(Case 2.1: $Q = (0,0)$) In this case, let $y = ux + v$ be the line tangent to P. Since it must pass through $Q = (0,0)$, we have that $v = 0$. If we substitute it in the equation for the elliptic curve and divide by x, which is a trivial root, we get $x^2 - u^2x + a = 0$. This should have a double root at $x = p$. So, that means the discriminant is zero, which happens if and only if $4a = u^4$. Since a has no fourth-power factors, it follows that $a = 4$ and $u = \pm 2$. Hence, $x = 2$ and $y = \pm 4$. So we get two $4-$torsion points: $(2, \pm 4)$.

(Case 2.2: $Q = (\gamma\sqrt{-a}, 0)$ with $\gamma = \pm 1$) In this case, again, let $ux+v$ be the tangent line to P. Substituting in the equation for the elliptic curve we get $x^3 - u^2x^2 + (a - 2uv)x - v^2 = 0$. This should have a double root at p and a simple root at $\gamma\sqrt{-a}$. The product of the roots must be equal to v^2, so $\gamma\sqrt{-a} = (v/p)^2$. We can divide by p since $p = 0$ would imply $P = (0,0)$ which has order 2, not 4. Then, squaring both sides we get $-a = (v/p)^4$, which contradicts the fact that a is a fourth-power free integer. So, we get the following table for $4-$torsion points.

	$-a$ is a square	$a = 4$	else
$E[4]$	$\varnothing$	$\{(2, \pm 4)\}$	$\varnothing$

Part 3: 2^k-torsion points for $k \geq 3$

Let $P = (p, p')$ be a 2^k-torsion point for $k \geq 3$. Let $(q, q') = Q := 2^{k-3}P$. We have that $2Q$ is a $4-$torsion point, so $2Q = (2, \gamma 4)$ for $\gamma = \pm 1$. Let $ux + v$ be the tangent line to Q. Substituting it in the equation for the elliptic curve we get, as usual, $x^3 - u^2x^2 + (a - 2uv)x - v^2 = 0$. This should have a double root at q and a simple root at $x = 2$. So, using the identity for the product of the roots we get $2q^2 = v^2$, which has no solutions in the rational numbers. So there are no 2^k-torsion points for $k \geq 3$, independently of the value of a.

Part 4: $3-$torsion points

Let $P = (p, p')$ be a $3-$torsion point. Then, $2P = -P$. Let $ux + v$ be the tangent line to P. Substitute it in the equation for the elliptic curve and get $x^3 - u^2x^2 + (a - 2uv)x - v^2 = 0$. This should have a triple root at p. So, by the relations of roots and coefficients of a polynomial, we have the three identities

$$p^3 = v^2, \quad 3p^2 = a - 2uv, \quad 3p = u^2.$$

From the first and the third equations we get $27v^2 = u^6$. This means $v = \pm u^3/(3\sqrt{3})$. So, substituting this in the second equation we get

$$\frac{u^2}{3} = a \pm 2\frac{u^4}{3\sqrt{3}}.$$

The only way this can be true for a and u rationals is if $u = 0$. But then $a = 0$, which makes the curve singular. So this case is impossible. Hence, there are no $3-$torsion points.

Part 5: $5-$torsion points

This is by far the hardest part of this proof. The strategy will be analogous to part 4, but there will be a lot more calculations to be done. Let $(p, p') = P$ be a $5-$torsion point. Let $(q, q') = Q := 2P$. Then, we have $2Q = -P$. Let $ux + v$ be the tangent line to P and $\alpha x + \beta$ be the tangent line to Q. Substituting both in the equation for the elliptic curve yields the two equations

$$\begin{cases} x^3 - u^2x^2 + (a - 2uv)x - v^2 = 0, \\ x^3 - \alpha^2x^2 + (a - 2\alpha\beta)x - \beta^2 = 0. \end{cases}$$

The first polynomial has roots p, p, q. The second has roots p, q, q. Using the relations between roots and coefficients we arrive at the following six equations.

$$p^2q = v^2, \tag{5.26}$$
$$p^2 + 2pq = a - 2uv, \tag{5.27}$$
$$2p + q = u^2, \tag{5.28}$$
$$q^2p = \beta^2, \tag{5.29}$$
$$q^2 + 2pq = a - 2\alpha\beta, \tag{5.30}$$
$$2q + p = \alpha^2. \tag{5.31}$$

From (5.27) and (5.30) we arrive at

$$p^2 - q^2 = 2(\alpha\beta - uv).$$

Square both sides to obtain

$$(p^2 - q^2)^2 = 4(\alpha^2\beta^2 - 2\alpha\beta uv + u^2v^2).$$

Now using equations (5.26), (5.28), (5.29) and (5.31) we get

$$(p^2 - q^2)^2 - 8(p^3q + p^2q^2 + pq^3) = -8\alpha\beta uv.$$

Finally, square both sides one last time and use the same identities again to arrive at a polynomial involving only p and q.

$$((p^2 - q^2)^2 - 8(p^3q + p^2q^2 + pq^3))^2 = 64p^3q^3(2p + q)(2q + p).$$

Expanding this yields

$$0 = p^8 - 16p^7q + 44p^6q^2 + 16p^5q^3 - 90p^4q^4 + 16p^3q^5 + 44p^2q^6 - 16pq^7 + q^8.$$

Now, the key observation is that the coefficients of this polynomial are symmetric. That means we can write it in terms of the new variables $x := p + q$ and $y := pq$. After some very long computation, we get that this polynomial can be written as

$$0 = x^8 - 24yx^6 + 160y^2x^4 - 320y^3x^2.$$

Now, we have two cases to consider.

(Case 5.1: $x = 0$) In this case, $p = -q$. By plugging this in equations (5.28) and (5.31) we get $\alpha^2 = q = -u^2$. So $\alpha = u = q = p = 0$. But then $P = (0, 0)$, which has order 2, not 5, so this case is impossible.

(Case 5.2: $x \neq 0$) In this case, we set $z = y/x^2$ and divide both sides by x^8 to get the following polynomial in z.

$$0 = 1 - 24z + 160z^2 - 320z^3.$$

Now, this is a polynomial in one variable with integer coefficients, so we can use Gauss' Lemma to check for all the rational solutions. There is, in fact, only one rational solution $z = 1/4$. But that means $x^2 = 4y$. Substituting the definitions of x and y we get $(p+q)^2 = 4pq$. After a bit of simplification we arrive at $(p-q)^2 = 0$. So $p = q$. But then, that means either $2P = P$ or $2P = -P$. In either case, the order of P is less than 5, so this case is impossible as well. Hence, there are no $5-$torsion points.

Part 6: putting it all together

By joining all the results from previous cases, we have the following table.

	$-a$ is a square	$a = 4$	else
$\#E[2]$	3	1	1
$\#E[4]$	0	2	0
$\#E[2^k]$ for $k \geq 3$	0	0	0
$\#E[3]$	0	0	0
$\#E[5]$	0	0	0

By pure inspection we conclude that there is only one possible group for each case. Namely, $\mathbb{Z}_2 \times \mathbb{Z}_2$ if $-a$ is a square, $\mathbb{Z}_4$ if $a = 4$ and $\mathbb{Z}_2$ otherwise. □

Chapter 6

The Birch and Swinnerton-Dyer Conjecture

As we've seen, given an elliptic curve E, we can define its $L-$function via the correction terms $c_p(E, r) := q + 1 - \#E(\mathbb{F}_q)$, where $q = p^r$. The Arithmetic Modularity Theorem tells us that $L(E, s)$ has an analytic continuation to the whole complex plane. Therefore, it makes sense to talk about its value on $s = 1$. Birch and Swinnerton-Dyer [4] have developed a method to compute $L(E, 1)$ explicitly for the following family of elliptic curves

$$E : y^2 = x^3 - Dx, \quad D \in \mathbb{Z}. \tag{6.1}$$

Their observations suggested a connection between this particular value and the rank of E. This led to the following.

Conjecture 6.0.1 (BSD Conjecture)**.** Let E be an elliptic curve of rank r. Then,

$$\text{ord}_{s=1} L(E, s) = r.$$

The quantity on the left is often referred to as the *analytic rank* of E. The goal of this chapter is to explain the original calculations that led to the conjecture. More concretely, we will provide a method of computing $L(E, 1)$ for elliptic curves in (6.1). By combining this with the rank calculation from 4.3, it will be possible to verify for a number of cases the following weakened version of the BSD conjecture.

Conjecture 6.0.2 (Weak BSD Conjecture)**.** Let E be an elliptic curve of rank r. Then,

$$r > 0 \iff L(E, 1) = 0.$$

In other words, this weakened statements says that $E(\mathbb{Q})$ is infinite if and only if the $L-$function vanishes at $s = 1$. Under the assumption that the analytic rank is $= 1$, Gross and Zagier showed that $E(\mathbb{Q})$ admits a point of infinite order [15], which remains to this day one of the strongest results we have concerning BSD.

In Section 6.1 we'll calculate explicitly the numbers $\#E(\mathbb{F}_q)$. In Section 6.2 we derive a formula for $L(E,1)$ in terms of the Weierstrass $\wp$−function. Lastly, in Section 6.3 we give a pseudo-code for computing this value and a table comparing it with the rank of E.

6.1 Counting points on $E : y^2 = x^3 - Dx$

In order to calculate the L−function of an elliptic curve with integer coefficients, we first must find the number of points in each reduction $E(\mathbb{F}_q)$. In this section, we are interested in counting the number of rational points in the (possibly singular) curve $E(\mathbb{F}_q)$ where q is a prime power and $E : y^2 = x^3 - Dx$. The discriminant of E is $\Delta = 4D^3$. Our ultimate goal is to prove the following.

Theorem 6.1.1. Let $q = p^r$. We have

$$\#E(\mathbb{F}_q) = \begin{cases} q+1 & \text{if } p \mid \Delta, \\ q+1-\tau_p^r - \overline{\tau}_p^r & \text{if } p \nmid \Delta. \end{cases} \qquad \tau_p = \begin{cases} i\sqrt{p} & \text{if } p \overset{4}{\equiv} 3, \\ [\frac{D}{\pi}]\overline{\pi} & \text{if } p \overset{4}{\equiv} 1. \end{cases}$$

In the last case, we assume $p = \pi\overline{\pi}$, with π primary.

First, we'll consider primes that divide the discriminant.

Proposition 6.1.2. Let $E : y^2 = x^3$. Then $(E(\mathbb{F}_q)_{\text{ns}}, \oplus) \cong (\mathbb{F}_q, +)$ as an additive group and thus $\#E(\mathbb{F}_q) = q+1$.

Proof. Here, $E(\mathbb{F}_q)_{\text{ns}} = E(\mathbb{F}_q) - \{(0,0)\}$. Let $t := x/y$. Then, $1/t^3 = y^3/x^3 = y$ and $1/t^2 = y^2/x^2 = x$. Therefore, the following map $\phi : E(\mathbb{F}_q) - \{(0,0)\} \to \mathbb{F}_q$ is a bijection of sets

$$\phi(\mathcal{O}) := 0, \quad \phi(x,y) := x/y = t. \tag{6.2}$$

It thus suffices to prove that given points $(x_1,y_1) \oplus (x_2,y_2) = (x_3,y_3)$ we have $t_1 + t_2 = t_3$ where $t_i = x_i/y_i$. Here, we'll assume $x_1 \neq x_2$. The other cases can be checked similarly. By the addition formula

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \quad -y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_3 - x_1) + y_1. \tag{6.3}$$

We substitute $x_i, y_i \leftarrow 1/t^2, 1/t^3$ and simplify to get

$$\frac{1}{t_3^2} = \frac{1}{(t_1+t_2)^2}, \quad \frac{1}{t_3^3} = \frac{1}{(t_1+t_2)^3}. \tag{6.4}$$

We divide one equation by the other to arrive at $t_1 + t_2 = t_3$. □

Corollary 6.1.3. Let $p \mid \Delta$, then $\#E(\mathbb{F}_q) = q + 1$.

Proof. If $p \mid D$, the result follows from Proposition 6.1.2. Assume then $p = 2$ and Δ is odd. The reduced curve becomes $y^2 = x^3 - x$. But then we do the (invertible) transformation $y \leftarrow y + x$ to get $y^2 = x^3$ and we reduce the problem to the previous case. □

With this, the case of bad primes is completely understood. We now move to good primes.

Proposition 6.1.4. Let $p \nmid \Delta$ and $q \overset{4}{\equiv} 3$. Then, $\#E(\mathbb{F}_q) = q + 1$.

Proof. We have two obvious points $\{\infty, (0, 0)\}$ in $E(\mathbb{F}_q)$. For $x \neq 0$, we have $x \neq -x$ (since $p \neq 2$). Hence we can arrange the $q - 1$ remaining possibilities for x in pairs $\{x, -x\}$.

Let $f(x) = x^3 - Dx$. If $f(x) = 0$ for some $x \neq 0$, then the pair $\{x, -x\}$ yields two solutions $\{(x, 0), (-x, 0)\}$. Suppose $f(x) \neq 0$. By Corollary 2.3.10, -1 is *not* a square in $\mathbb{F}_q$. Since the squares of $\mathbb{F}_q^*$ form a subgroup of index 2, it follows that one, and only one, of the two (non-zero) elements $f(x)$ and $f(-x) = -f(x)$ is a square. Therefore, the pair $\{x, -x\}$ gives us two solutions $\left(\alpha, \pm\sqrt{f(\alpha)}\right)$, where $\alpha = \pm x$ is such that $f(\alpha)$ is a square. Therefore, each one of the $(q-1)/2$ pairs $\{x, -x\}$ gives us two points in $\#E(\mathbb{F}_q)$. Summing up all of the solutions we have a total of $2 + (q - 1) = q + 1$. □

Proposition 6.1.5. Let $p \nmid \Delta$ and $q \overset{4}{\equiv} 1$. Let χ_2, χ_4 be multiplicative characters of $\mathbb{F}_q$ of order 2 and 4 respectively. Then,

$$\#E(\mathbb{F}_q) = q + 1 - \alpha_q - \overline{\alpha}_q,$$

where $\alpha_q = -\overline{\chi}_4(D) J(\chi_2, \chi_4)$.

Proof. This is the hardest case. Here we use the full extent of Gauss and Jacobi sums' results proven in Section 2.3. To use them, we first need to put the equation for E in diagonal form. Consider the set

$$\tilde{E}(\mathbb{F}_q) := \{(u, v) \in \mathbb{F}_q^2 \ : \ u^2 = v^4 + 4D\}.$$

We have a bijection of sets $F : E(\mathbb{F}_q) - \{(0, 0), \infty\} \to \tilde{E}(\mathbb{F}_q)$.

$$F(x, y) := (2x - y^2/x^2, y/x), \quad F^{-1}(u, v) := \left(\frac{1}{2}(u + v^2), \frac{1}{2}v(u + v^2)\right).$$

Therefore, $\#E(\mathbb{F}_q) = \#\tilde{E}(\mathbb{F}_q) + 2$. So we've reduced the problem to counting the solutions of an equation in diagonal form. Notice that, by Corollary 2.3.10,-1 *is* a square in $\mathbb{F}_q$. Let ξ be such that $\xi^2 = -1$. We tackle the counting of $\#\tilde{E}(\mathbb{F}_q)$ by considering respectively the cases where (1) $u = 0$, (2) $v = 0$ and (3) $u, v \neq 0$.

Case 1: $u = 0$

Since $p \nmid D$, $-4D$ is non-zero in $\mathbb{F}_q$. Also, by hypothesis, 4 divides $q-1$. So, by Proposition 2.3.18, we have

$$\begin{aligned}\#\{v^4 = -4D\} &= \sum_{j=1}^{4} \chi_4^j(-4D) = \sum_{j=1}^{4} \chi_4^j(D) \\ &= 1 + \chi_2(D) + \chi_4(D) + \overline{\chi}_4(D).\end{aligned}$$

In the second equality we used the fact that $\chi_4(-4) = \chi_2(2\xi) = 1$. This calculation already was done in Example 2.3.17.

Case 2: $v = 0$

Similarly to the previous case, we have

$$\#\{u^2 = 4D\} = \sum_{i=1}^{2} \chi_2^i(4D) = \sum_{i=1}^{2} \chi_2^i(D) = 1 + \chi_2(D).$$

Case 3: $u, v \in \mathbb{F}_q^*$

This is the hardest part. Here, we'll finally use Jacobi sums.

$$\begin{aligned}
& \#\{u, v \in \mathbb{F}_q \ : \ u^2 - v^4 = 4D\} \\
= \ & \sum_{\substack{a,b \in \mathbb{F}_q \\ a+b=4D}} \#\{u^2 = a\}\#\{v^4 = -b\} && \text{(Counting)} \\
= \ & \sum_{\substack{a,b \in \mathbb{F}_q \\ a+b=4D}} \sum_{i=1}^{2}\sum_{j=1}^{4} \chi_2^i(a)\chi_4^j(-b) && \text{(Proposition 2.3.18)} \\
= \ & \sum_{\substack{a,b \in \mathbb{F}_q \\ a+b=1}} \sum_{i=1}^{2}\sum_{j=1}^{4} \chi_2^i(4Da)\chi_4^j(-4Db) && \left(\text{Substitution} \begin{cases} a \leftarrow 4Da, \\ b \leftarrow 4Db \end{cases}\right) \\
= \ & \sum_{\substack{a,b \in \mathbb{F}_q \\ a+b=1}} \sum_{i=1}^{2}\sum_{j=1}^{4} \chi_2^i(D)\chi_4^j(D)\chi_2^i(a)\chi_4^j(b) && \left(\begin{cases} \chi_2(4D) = \chi_2(D), \\ \chi_4(-4D) = \chi_2(2\xi)\chi_4(D) = \chi_4(D) \end{cases}\right) \\
= \ & \sum_{i=1}^{2}\sum_{j=1}^{4} \chi_2^i(D)\chi_4^j(D)\chi_2^j(2\xi)J(\chi_2^i, \chi_4^j) && \text{(Definition 2.3.20: Jacobi sum).}
\end{aligned}$$

Then, by using the properties in Proposition 2.3.21, we arrive at the expression

$$q - 3 - \chi_4(D) - \overline{\chi}_4(D) - 2\chi_2(D) + \overline{\chi}_4(D)J(\chi_2, \chi_4) + \chi_4(D)\overline{J(\chi_2, \chi_4)}.$$

Now we sum all the cases together and simplify, obtaining

$$\begin{aligned} \#E_n(\mathbb{F}_q) &= \#\tilde{E}_n(\mathbb{F}_q) + 2 \\ &= q + 1 + \overline{\chi}_4(D)J(\chi_2, \chi_4) + \chi_4(D)\overline{J(\chi_2, \chi_4)}. \end{aligned}$$

We set $\alpha_q := -\overline{\chi_4}(D)J(\chi_2, \chi_4)$ and we're done. □

The next step is to pinpoint the exact value of α_q. We already know it is a Gaussian integer (because it involves only sums and products of characters of order 2 and 4). Moreover, Proposition 2.3.21 tells us that $|\alpha_q|^2 = q^2$. So the possibilities for α_q are severely limited. The next Proposition allows us to fully determine its value when $q = p$, or $q = p^2$ with $p \overset{4}{\equiv} 3$.

Proposition 6.1.6. Let χ_2, χ_4 be multiplicative characters in $\mathbb{F}_q$ of order 2 and 4, respectively, with $q \overset{4}{\equiv} 1$. Then,

(i) $-J(\chi_2, \chi_4)$ is primary;

(ii) If $p \overset{4}{\equiv} 3$, $q = p^2$, then $\alpha_q = -p$;

(iii) Assume $q = p \overset{4}{\equiv} 1$ and $p = \pi\overline{\pi}$ with π primary. Fix $\overline{\chi}_4 = [\frac{\cdot}{\pi}]$.
Then, $-J(\chi_2, \chi_4) = \overline{\pi}$ and $\alpha_p = [\frac{D}{\pi}]\overline{\pi}$.

Proof. (i) Here we do

$$\begin{aligned} & J(\chi_2, \chi_4) \\ = \quad & \sum_{\substack{a \in \mathbb{F}_q^* \\ a \neq 1}} \chi_2(1-a)\chi_4(a) && \text{(Definition 2.3.20: Jacobi sum)} \\ = \quad & \sum_{\substack{a \in \mathbb{F}_q^* \\ a \neq 1}} \chi_2(1-a)\chi_4(a) + 1 + \sum_{\substack{a \in \mathbb{F}_q^* \\ a \neq 1}} \chi_4(a) && \text{(Proposition 2.3.13: summing over } \chi_4) \\ = \quad & 1 + \sum_{\substack{a \in \mathbb{F}_q^* \\ a \neq 1}} (\chi_2(1-a) + 1)\chi_4(a) && \text{(Simplifying).} \end{aligned}$$

Now, the term $\chi_2(1-a) + 1$ is always equal to 0 or 2. Since $\chi_4(a)$ is a unit, it follows that

$$(\chi(1-a) + 1)\chi_4(a) \overset{2+2i}{\cong} \chi(1-a) + 1. \tag{6.5}$$

So we have

$$J(\chi_2,\chi_4) = 1 + \sum_{\substack{a\in\mathbb{F}_q^*\\ a\neq 1}} (\chi_2(1-a)+1) = 1 - 1 + q - 2 \overset{2+2i}{\cong} -1.$$

Therefore $-J(\chi_2,\chi_4)$ is primary. (ii) By Proposition 2.3.21, we know $|J(\chi_2,\chi_4)|^2 = p^2$. Since $p \overset{4}{\equiv} 3$, the only Gaussian integers satisfying this property are $\pm p$, $\pm ip$. From these, the only primary is $-p$. So $J(\chi_2,\chi_4) = p$. So $\alpha_q = -\overline{\chi}_4(D)p$. It suffices to show that $\chi_4(D) = 1$. We know $p = 4k+3$. Let $\alpha \in \mathbb{F}_q^*$ be a generator. Then, we have that $\mathbb{N}\alpha = \alpha^{1+p} = \alpha^{4(k+1)}$ is a generator of $\mathbb{F}_p^*$. So there is some η such that $\chi_4(D) = \chi_4(\alpha^{4\eta(k+1)}) = \chi_4^4(\alpha^{\eta(k+1)}) = 1$. (iii) Here, we already know $-J(\chi_2,\chi_4) \in \{\pi,\overline{\pi}\}$. To determine which one it is, we prove $J(\chi_2,\chi_4) \overset{\overline{\pi}}{\cong} 0$. Let $k = (p-1)/4$. We have

$$J(\chi_2,\chi_4) = J\left(\left(\frac{\cdot}{p}\right),\left[\frac{\cdot}{\overline{\pi}}\right]\right) = \sum_{\substack{a\in\mathbb{F}_p^*\\ a\neq 1}} \left(\frac{a}{p}\right)\left[\frac{1-a}{\overline{\pi}}\right] \overset{\overline{\pi}}{\cong} \sum_{\substack{a\in\mathbb{F}_p^*\\ a\neq 1}} a^{2k}(1-a)^k.$$

In the last equality we used Euler's criterion and the definition of the quartic symbol. Now we use Newton's binomial identity to get

$$\sum_{\substack{a\in\mathbb{F}_p^*\\ a\neq 1}} \sum_{j=0}^{k} \binom{k}{j} a^{2k}(-a)^j = \sum_{j=0}^{k} \binom{k}{j} (-1)^j \sum_{\substack{a\in\mathbb{F}_p^*\\ a\neq 1}} a^{2k+j} \overset{p}{\equiv} \sum_{j=0}^{k} \binom{k}{j} (-1)^j \cdot (-1) = 0.$$

In the second equality we used the well-known fact in number theory that $\sum_{a\in\mathbb{F}_p} a^n = 0$ provided $(p-1) \nmid n$ (see Proposition 7.0.3 in the Appendix). In the last equality, we have the alternating sum of binomial coefficients, which is zero. □

We are now ready to provide a proof of Theorem 6.1.1.

Proof of Theorem 6.1.1. The case where $p \mid \Delta$ was proven in Corollary 6.1.3. Suppose $p \nmid \Delta$ and define

$$h := \begin{cases} p & \text{if } p \overset{4}{\equiv} 1, \\ p^2 & \text{if } p \overset{4}{\equiv} 3. \end{cases}$$

Then, $h^n \overset{4}{\equiv} 1$ for all $n \geq 1$ and we can analyze the number α_{h^n}. We'll use the Hasse-Davenport Formula (Theorem 2.3.22) prove that $\alpha_{h^n} = \alpha_h^n$. Let χ_2, χ_4 be characters of $\mathbb{F}_h$ of order 2 and 4, respectively. Define

$$\chi_2^{(n)} := \chi_2 \circ \mathbb{N}_{h^n/h}, \quad \chi_4^{(n)} := \chi_4 \circ \mathbb{N}_{h^n/h}. \tag{6.6}$$

By Proposition 2.3.15, these are also characters of order 2 and 4. From there, we have

α_{h^n}

$$\begin{aligned}
&= -\,\overline{\chi}_4^{(n)}(D)J(\chi_2^{(n)},\chi_4^{(n)}) && \text{(Proposition 6.1.5: formula for } \alpha_{h^n}\text{)}\\
&= -\,\overline{\chi}_4^{n}(D)J(\chi_{2,n},\chi_{4,n}) && \Big(\text{Proposition 2.3.15: } \chi_4^{(n)}(D) = \chi_4^n(D) \text{ since } D \in \mathbb{F}_h\Big)\\
&= -\,\overline{\chi}_4^{n}(D)\frac{g(\chi_2^{(n)})g(\chi_4^{(n)})}{g(\chi_2^{(n)}\chi_4^{(n)})} && \text{(Proposition 2.3.21: Jacobi sums in terms of Gauss sums)}\\
&= -\,\overline{\chi}_4^{n}(D)\frac{g(\chi_2^{(n)})g(\chi_4^{(n)})}{g((\chi_2\chi_4)^{(n)})} && \Big(\chi_2^{(n)}\chi_4^{(n)} = (\chi_2\chi_4)\circ\mathbb{N}_{h^n/h} = (\chi_2\chi_4)^{(n)}\Big)\\
&= \left[-\overline{\chi}_4(D)\frac{g(\chi_2)g(\chi_4)}{g(\overline{\chi}_4)}\right]^n && \text{(Corollary 2.3.22: Hasse-Davenport Formula)}\\
&= \alpha_h^n && \text{(Proposition 6.1.5: formula for } \alpha_h\text{).}
\end{aligned}$$

If $p \overset{4}{\equiv} 1$, fix $\overline{\chi}_4 = [\frac{\cdot}{\pi}]$. We proved in Proposition 6.1.6 that $\alpha_p = [\frac{D}{\pi}]\overline{\pi}$. So we set $\pi_p = \alpha_p$ and we're done. Let $p \overset{4}{\equiv} 3$. Again, we have by Proposition 6.1.6 that $\alpha_{p^2} = -p$. Combining with Proposition 6.1.4, we have

$$\#E(\mathbb{F}_q) = \begin{cases} q+1-(-p)^r-(-p)^r & \text{if } q \overset{4}{\equiv} 1,\\ q+1 & \text{if } q \overset{4}{\equiv} 3.\end{cases} \tag{6.7}$$

By setting $\pi_p = i\sqrt{p}$ we reach the desired equality. □

6.2 Formula for $L(E,1)$

In this section, we use the calculations done in Section 6.1 to derive some formulas for the $L-$function of E at the point $s=1$. These formulas will be crafted so that a computer can easily approximate them. To allow some simplifications, we will assume that D is fourth-power free and $\neq 1,2,4,8$. Our starting point is the following product form.

Theorem 6.2.1. We have the following formula for the $L-$function of E.

$$L(E,s) = \prod_{\substack{\pi\nmid\Delta\\ \text{primary}\\ \text{prime}}} \left(1-\left[\frac{D}{\pi}\right]\frac{\overline{\pi}}{(\mathbb{N}\pi)^s}\right)^{-1}.$$

Proof. First, we calculate the local $L-$functions $L_p(E,s)$. To that end, we must know the correction terms $c_p(E,s)$ as explained in Section 3.2. We have three cases to consider, all follow by Theorem 6.1.1.

(Case 1: $p \mid \Delta$) In this case, the correction term is $c_p(E,r) = 0$, so $L_p(E,s) = 1$.

(Case 2: $p \nmid \Delta$, $p \overset{4}{\equiv} 3$) Here, the correction term is $c_p(E,r) = -\tau_p^r - \overline{\tau}_p^r$ with $\tau_p = i\sqrt{p}$. In order to put $L_p(E,s)$ in the desired form, we do

$$L_p(E,s) = \frac{1}{1-(i\sqrt{p})p^{-s}} \frac{1}{1+(i\sqrt{p})p^{-s}} = \frac{1}{1+p^{1-2s}} = \frac{1}{1-(-p)(\mathbb{N}(-p))^{-s}} \tag{6.8}$$

$$= \left(1 - \left[\frac{D}{-p}\right] \frac{-\overline{p}}{(\mathbb{N}(-p))^s}\right)^{-1}. \tag{6.9}$$

In the last step we used Proposition 2.2.6 that says $[\frac{D}{p}] = 1$.

(Case 3: $p \nmid \Delta$, $p \overset{4}{\equiv} 1$) In this case, let $p = \pi\overline{\pi}$ with π primary (which also implies that $\overline{\pi}$ is primary). The correction term is $c_p(E,r) = -\tau_p^r - \overline{\tau}_p^r$ with $\tau_p = [\frac{D}{\pi}]\overline{\pi}$. We thus have

$$L_p(E,s) = \left(1 - \left[\frac{D}{\pi}\right]\overline{\pi}p^{-s}\right)^{-1} \left(1 - \overline{\left[\frac{D}{\pi}\right]}\pi p^{-s}\right)^{-1} \tag{6.10}$$

$$= \left(1 - \left[\frac{D}{\pi}\right]\frac{\overline{\pi}}{(\mathbb{N}\pi)^s}\right)^{-1} \left(1 - \left[\frac{D}{\overline{\pi}}\right]\frac{\pi}{(\mathbb{N}\overline{\pi})^s}\right)^{-1}. \tag{6.11}$$

Notice that Equations (6.9) and (6.11) have terms corresponding to each primary Gaussian prime that does not divide Δ. Therefore, by putting all the terms together in

$$L(E,s) = \prod_{p \text{ prime}} L_p(E,s)$$

we get the desired product identity. □

In order to compute this $L-$function, it will be useful to consider instead the product of *all* primary Gaussian primes, instead of just those that don't divide Δ. Since this new object differs from the original $L-$function by a finite number of factors, we can easily recover one from the other. We therefore define

$$L_D(s) := \prod_{\substack{\pi \text{ primary} \\ \text{prime}}} \left(1 - \left[\frac{D}{\pi}\right]\frac{\overline{\pi}}{(\mathbb{N}\pi)^s}\right)^{-1} = \sum_{\sigma \text{ primary}} \left[\frac{D}{\sigma}\right]\frac{\overline{\sigma}}{(\mathbb{N}\sigma)^s}. \tag{6.12}$$

The advantage of working with $L_D(s)$ is that it can be neatly represented as a series instead of an infinite product, using Euler's product identity (which can be used in this situation because complex conjugation, norm and the quartic symbol are all multiplicative). We now derive an analytic continuation of $L_D(s)$ for $\mathrm{Re}(s) > 1/2$ which will allow us to compute $L_D(1)$. First, we define some quantities.

Let $E, F \in \mathbb{Z}$ such that $D = EF, E$ is primary with no factors of $2, F = \pm 2^k$ for some k. Let $R \in \mathbb{Z}$ be the product of all distinct primes dividing E, normalized so that R is primary.

Since D is not a power of 2 (because we assumed $D \neq 1, 2, 4, 8$ and is fourth-power-free), we have $E \neq 1$. We can rewrite the quartic symbol in (6.12) as

$$\left[\frac{D}{\sigma}\right] = \left[\frac{EF}{\sigma}\right] = \left[\frac{E}{\sigma}\right]\left[\frac{F}{\sigma}\right] = \left[\frac{\sigma}{E}\right]\left[\frac{F}{\sigma}\right]. \tag{6.13}$$

In the last equality we've used quartic reciprocity, the sign is positive by Proposition 2.2.9 since both E and σ are primary. Notice that $[\frac{\sigma}{E}]$, by multiplicativity of the quartic symbol, depends only on the class of σ in $\mathbb{Z}[i]/(R)$ and is equal to zero if σ is not coprime to R. Also, since $F = \pm 2^k \sim (1+i)^{2k}$ and σ is primary, by Proposition 2.2.11, the quartic symbol $[\frac{F}{\sigma}]$ depends only on the class of σ in $\mathbb{Z}[i]/(K)$, where $K = 4$ if $F = \pm 1$, otherwise $K = 8$. By combining everything, we conclude that $[\frac{D}{\sigma}] = [\frac{\sigma}{E}][\frac{F}{\sigma}]$ depends only on the class of σ in $\mathbb{Z}[i]/(RK)$. We then choose the following data.

1. Let $K = 4$ if $F = \pm 1$, else $K = 8$;

2. Let A be a set of representatives for the elements in $\mathbb{Z}[i]/(R)$ coprime to R;

3. Let B to be a set of *primary* representatives for the elements in $\mathbb{Z}[i]/(K)$.

Any σ primary and coprime to R can be written uniquely as $K\alpha + R\beta + RK\mu$ for some $\alpha \in A, \beta \in B, \mu \in \mathbb{Z}[i]$ (see Corollary 7.0.6 in the Appendix). So, we can replace the summation in (6.12) by a summation in α, β, μ. To ease the notation, define $\lambda := K\alpha + R\beta$.

$$\begin{aligned}
&L_D(s)\\
&= \sum_{\substack{\alpha\in A\\ \beta\in B}} \sum_{\mu\in\mathbb{Z}[i]} \left[\frac{D}{\lambda + RK\mu}\right] \frac{\overline{\lambda} + \overline{RK\mu}}{(\mathbb{N}(\lambda + RK\mu))^s} && \text{(Change summation indexes; } \sigma = \lambda + RK\mu)\\
&= \sum_{\substack{\alpha\in A\\ \beta\in B}} \left[\frac{D}{\lambda}\right] \sum_{\mu\in\mathbb{Z}[i]} \frac{\overline{\lambda} + \overline{RK\mu}}{(\mathbb{N}(\lambda + RK\mu))^s} && \left([\tfrac{D}{\sigma}] \text{ depends only on the class of } \sigma \text{ in } \frac{\mathbb{Z}[i]}{(RK)}\right)\\
&= \sum_{\substack{\alpha\in A\\ \beta\in B}} \left[\frac{D}{\lambda}\right] \sum_{\mu\in\mathbb{Z}[i]} \frac{\overline{\lambda} + \overline{RK\mu}}{|\lambda + RK\mu|^{2s}} && \text{(Rewrite } \mathbb{N}x = |x|^2).
\end{aligned}$$

Now, we would like to find an analytic continuation of the inner sum. Consider the function

$$\psi_\nu(s) := \frac{\overline{\nu}}{|\nu|^{2s}} + \sum_{\substack{\mu\in\mathbb{Z}[i]\\ \mu\neq 0}} \frac{\overline{\nu} + \overline{\mu}}{|\nu + \mu|^{2s}} - \frac{\overline{\mu}}{|\mu|^{2s}}\left(1 - \frac{s\nu}{\mu} - \frac{\overline{\nu}(s-1)}{\overline{\mu}}\right). \tag{6.14}$$

This function is similar to the original sum, but we've added a correction term similar to the definition of the Weierstrass $\wp$−function. Since the summand is $\mathcal{O}(\mu^{-2s-1})$, it follows that $\psi_\nu(s)$ is analytic on $\mathrm{Re}(s) > 1/2$ and so we can evaluate it at $s = 1$.

$$\psi_\nu(1) = \frac{1}{\nu} + \sum_{\substack{\mu\in\mathbb{Z}[i]\\ \mu\neq 0}} \frac{1}{\mu + \nu} - \frac{1}{\mu} + \frac{\nu}{\mu^2} = \xi(\nu), \tag{6.15}$$

where ξ is the Weierstrass zeta-function with periods 1 and i. Then, we have

$$\begin{aligned}
&\sum_{\mu\in\mathbb{Z}[i]} \frac{\overline{\nu}+\overline{\mu}}{|\nu+\mu|^{2s}} \\
= \quad & \psi_\nu(s) + \sum_{\substack{\mu\in\mathbb{Z}[i]\\ \mu\neq 0}} \frac{\overline{\mu}}{|\mu|^{2s}} \left(1 - \frac{s\nu}{\mu} - \frac{\overline{\nu}(s-1)}{\overline{\mu}}\right) && \text{(Equation (6.14))} \\
= \quad & \psi_\nu(s) + \sum_{\substack{\mu\in\mathbb{Z}[i]\\ \mu\neq 0}} \frac{\overline{\mu}}{|\mu|^{2s}} - \sum_{\substack{\mu\in\mathbb{Z}[i]\\ \mu\neq 0}} \frac{s\nu\overline{\mu}^2}{|\mu|^{2s+2}} - \sum_{\substack{\mu\in\mathbb{Z}[i]\\ \mu\neq 0}} \frac{\overline{\nu}(s-1)}{|\mu|^{2s}} && \text{(Distribute the product)} \\
= \quad & \psi_\nu(s) - \sum_{\substack{\mu\in\mathbb{Z}[i]\\ \mu\neq 0}} \frac{\overline{\nu}(s-1)}{|\mu|^{2s}} && \text{(First two sums vanish by symmetry)} \\
= \quad & \psi_\nu(s) - 4\overline{\nu}(s-1)\zeta_{\mathbb{Z}[i]}(s) && \Big(\text{Definition of } \zeta_{\mathbb{Z}[i]}\Big).
\end{aligned}$$

On the third equality we've canceled two sums by symmetry. On the first sum, the terms μ and $-\mu$ cancel each other; on the second sum, the terms μ and $i\mu$ cancel each other. The term $\zeta_{\mathbb{Z}[i]}(s)$ is the Gaussian zeta function (see Definition 2.4.36). We now put together everything we did so far.

$$\begin{aligned}
L_D(s) &= \sum_{\substack{\alpha\in A\\ \beta\in B}} \left[\frac{D}{\lambda}\right] \sum_{\mu\in\mathbb{Z}[i]} \frac{\overline{\lambda}+\overline{RK\mu}}{|\lambda+RK\mu|^{2s}} \\
&= \frac{\overline{RK}}{|RK|^{2s}} \sum_{\substack{\alpha\in A\\ \beta\in B}} \left[\frac{D}{\lambda}\right] \sum_{\mu\in\mathbb{Z}[i]} \frac{\overline{\lambda/RK}+\overline{\mu}}{|\lambda/RK+\mu|^{2s}} \\
&= \frac{\overline{RK}}{|RK|^{2s}} \sum_{\substack{\alpha\in A\\ \beta\in B}} \left[\frac{D}{\lambda}\right] \Big(\psi_{\lambda/RK}(s) - 4\overline{\lambda/RK}(s-1)\zeta_{\mathbb{Z}[i]}(s)\Big).
\end{aligned}$$

Finally, we take the limit $s \to 1$. By Proposition 2.4.37, $\lim_{s\to 1}(s-1)\zeta_{\mathbb{Z}[i]}(s) = \pi/4$.

$$L_D(1) = \frac{1}{RK} \sum_{\substack{\alpha\in A\\ \beta\in B}} \left[\frac{D}{\lambda}\right] \left(\xi\left(\frac{\lambda}{RK}\right) - \pi\overline{\lambda/RK}\right). \tag{6.16}$$

We could stop here, but it'll be convenient to rewrite this expression in terms of the Weierstrass $\wp-$function. We can choose $\wp$ to have periods ω and $i\omega$ in such a way that $\wp$ satisfies the functional equation

$$(\wp')^2 = 4\wp^3 - 4\wp. \tag{6.17}$$

Then, notice that $\omega^2\wp(\omega u)$ has periods 1 and i. This change of periods will simplify later computations. We can then write the standard addition formula for ξ in terms of $\wp$.

$$\xi(u+v) = \xi(u) + \xi(v) + \frac{\omega}{2}\frac{\wp'(\omega u) - \wp'(\omega v)}{\wp(\omega u) - \wp(\omega v)}. \tag{6.18}$$

If we let $u = \beta/K$ and $v = \alpha/R$, then $\lambda/RK = u+v$ and we can apply the addition formula to (6.16).

$$L_D(1) = \frac{1}{RK} \sum_{\substack{\alpha\in A\\ \beta\in B}} \left[\frac{D}{\lambda}\right] \left(\xi\left(\frac{\beta}{K}\right) + \xi\left(\frac{\alpha}{R}\right) + \frac{\omega}{2}\frac{\wp'(\omega\beta/K) - \wp'(\omega\alpha/R)}{\wp(\omega\beta/K) - \wp(\omega\alpha/R)} - \pi\overline{\lambda/RK}\right). \tag{6.19}$$

Now, we use the fact that this expression does not depend on the set of representatives. Consider another set $-A = \{-\alpha : \alpha \in A\}$ of representatives for the elements in $\mathbb{Z}[i]/(R)$. We can add the corresponding expression (6.19) for $-A$ on both sides. If we let $\lambda' = R(-\alpha)+K\beta$ notice that

$$\left[\frac{D}{\lambda}\right] = \left[\frac{\lambda}{E}\right]\left[\frac{F}{\lambda}\right] = \left[\frac{K\alpha}{E}\right]\left[\frac{F}{R\beta}\right] = \left[\frac{-1}{E}\right]\left[\frac{K\alpha}{E}\right]\left[\frac{F}{R\beta}\right] = \left[\frac{K(-\alpha)}{E}\right]\left[\frac{F}{R\beta}\right] = \left[\frac{D}{\lambda'}\right].$$

In the first and last equalities we've used (6.13). On the third equality to get $\left[\frac{-1}{E}\right] = 1$ we used Proposition 2.2.6. The conclusion is that $\left[\frac{D}{\lambda}\right]$ is not affected when changing α by $-\alpha$. Furthermore, ξ and $\wp'$ evaluated on α will cancel out since they are odd functions and $\wp$ will remain, since it is even. We then arrive at the following expression for $L_D(1)$.

$$L_D(1) = \frac{1}{RK} \sum_{\substack{\alpha\in A\\ \beta\in B}} \left[\frac{D}{\lambda}\right] \left(\xi\left(\frac{\beta}{K}\right) - \pi\overline{\beta/K}\right) + \frac{\omega}{2RK} \sum_{\substack{\alpha\in A\\ \beta\in B}} \left[\frac{D}{\lambda}\right] \frac{\wp'(\beta\omega/K)}{\wp(\beta\omega/K) - \wp(\alpha\omega/R)}. \tag{6.20}$$

The last thing we want to do is to show that the first sum on the right-hand side is equal to zero. To that end, notice the only term dependant on α is $\left[\frac{D}{\lambda}\right] = \left[\frac{K\alpha}{E}\right]\left[\frac{F}{R\beta}\right]$, so the sum on α is simply $\sum \left[\frac{\alpha}{E}\right]$. Since E is not a fourth-power (we've assumed D is fourth-power free), the function $\left[\frac{\cdot}{E}\right]$ is a non-principal character in $[\mathbb{Z}[i]/(R)]^*$, and thus the summation is zero by Proposition 2.3.13. So we are left with the final formula

$$L_D(1) = \frac{\omega}{2RK} \sum_{\substack{\alpha\in A\\ \beta\in B}} \left[\frac{D}{\lambda}\right] \frac{\wp'(\beta\omega/K)}{\wp(\beta\omega/K) - \wp(\alpha\omega/R)}. \tag{6.21}$$

6.3 Putting it all together

We are now ready to provide a pseudo-code. To calculate the values of $\wp$ and $\wp'$, one possibility is to use the Taylor series derived in Proposition 3.1.5. A clever and more efficient method can be found at [7], which makes use of the Weierstrass Uniformization Theorem to require less computation. Our goal is to calculate $L_D(1)$. After that, one can recover $L(E,1)$ simply by removing the bad prime terms in Equation (6.12). More concretely,

$$L(E,1) = L_D(1) \prod_{\substack{\pi \text{ primary prime}\\ \pi | D}} \left(1 - \left[\frac{D}{\pi}\right]\frac{\overline{\pi}}{(\mathbb{N}\pi)^s}\right). \tag{6.22}$$

As we are only interested in whether or not $L(E,1)=0$, it suffices to calculate $L_D(1)$. The best we can do with elementary tools is approximate $L_D(1)$ and show it is close to zero. The following (see Theorem 1 in [4]) gives us with a way to calculate it exactly.

Theorem 6.3.1. $(\sqrt[4]{D}/\omega)L_D(1)\in\mathbb{Z}$.

This tells us $L_D(1)$ is almost an integer: by approximating $(\sqrt[4]{D}/\omega)L_D(1)$ and observing it is close to zero, we can conclude that it is, in fact, exactly zero.

Algorithm 4 calculate_L_function

```
Input: $E : y^2 = x^3 - Dx$ an elliptic curve, where $D$ is fourth-power-free
Output: The value of $(\sqrt[4]{D}/\omega)L_D(1)$
Let $E, F \in Z$ be such that $D = EF$, $E$ primary, $\gcd(E, 2) = 1$, $F = \pm 2^k$ for some $k$
Let $K = 4$ if $F = \pm 1$, otherwise $K = 8$
Let $A \subseteq \mathbb{Z}$ be a set of representatives of $\mathbb{Z}[i]/(R)$ coprime to $R$
Let $B \subseteq \mathbb{Z}$ be a set of primary representatives of $\mathbb{Z}[i]/(K)$
Let $R \in \mathbb{Z}$ be primary and be the product of all distinct primes dividing $E$
Let $\wp$ satisfy (6.17) with periods $\omega, i\omega$ and $\omega = \sqrt{2}\pi e^{-\pi/6}\prod_{n\geq 1}\left(1-e^{-2\pi n}\right)^2 \approx 2.622$
Let $L_D(1)$ be as in Equation (6.12)
return $(\sqrt[4]{D}/\omega)L_D(1)$ truncated to the nearest integer
```

Tables 6.1 and 6.2 put together all of the main algorithms we've explained in this work. It shows the torsion, the rank (when it is not possible to pinpoint the rank, a lower-bound is provided), and the value of $(\sqrt[4]{D}/\omega)L_D(1)$ for various curves of the form $E : y^2 = x^3 - Dx$. It also shows the values of E, F, K and R to help others implement this code. In all cases where the rank can be estimated, we observe that $(\sqrt[4]{D}/\omega)L_D(1) = 0 \iff \text{rank} > 0$, which is equivalent to the statement of the weakened BSD Conjecture 6.0.2.

D	E	F	K	R	$(\sqrt[4]{D}/\omega)L_D(1)$	Rank	Torsion
3	-3	-1	4	-3	1	0	$\mathbb{Z}_2$
5	5	1	4	5	0	1	$\mathbb{Z}_2$
6	-3	-2	8	-3	0	1	$\mathbb{Z}_2$
7	-7	-1	4	-7	0	1	$\mathbb{Z}_2$
10	5	2	8	5	0	1	$\mathbb{Z}_2$
11	-11	-1	4	-11	1	0	$\mathbb{Z}_2$
12	-3	-4	8	-3	0	1	$\mathbb{Z}_2$
14	-7	-2	8	-7	0	≥ 1	$\mathbb{Z}_2$
15	-15	-1	4	-15	0	1	$\mathbb{Z}_2$
17	17	1	4	17	0	2	$\mathbb{Z}_2$
19	-19	-1	4	-19	1	0	$\mathbb{Z}_2$
20	5	4	8	5	0	1	$\mathbb{Z}_2$
21	21	1	4	21	0	1	$\mathbb{Z}_2$
22	-11	-2	8	-11	0	1	$\mathbb{Z}_2$
23	-23	-1	4	-23	0	1	$\mathbb{Z}_2$
25	25	1	4	5	0	1	$\mathbb{Z}_2 \times \mathbb{Z}_2$
26	13	2	8	13	0	1	$\mathbb{Z}_2$
30	-15	-2	8	-15	0	1	$\mathbb{Z}_2$
31	-31	-1	4	-31	0	1	$\mathbb{Z}_2$
34	17	2	8	17	0	≥ 1	$\mathbb{Z}_2$
35	-35	-1	4	-35	2	0	$\mathbb{Z}_2$
36	9	4	8	-3	0	≥ 1	$\mathbb{Z}_2 \times \mathbb{Z}_2$
37	37	1	4	37	0	1	$\mathbb{Z}_2$
38	-19	-2	8	-19	0	1	$\mathbb{Z}_2$
39	-39	-1	4	-39	0	≥ 1	$\mathbb{Z}_2$
41	41	1	4	41	0	≥ 1	$\mathbb{Z}_2$
42	21	2	8	21	0	1	$\mathbb{Z}_2$
43	-43	-1	4	-43	1	0	$\mathbb{Z}_2$
45	45	1	4	-15	0	1	$\mathbb{Z}_2$
46	-23	-2	8	-23	0	≥ 1	$\mathbb{Z}_2$
47	-47	-1	4	-47	0	1	$\mathbb{Z}_2$
49	49	1	4	-7	0	≥ 1	$\mathbb{Z}_2 \times \mathbb{Z}_2$
50	25	2	8	5	0	≥ 1	$\mathbb{Z}_2$
51	-51	-1	4	-51	2	0	$\mathbb{Z}_2$
52	13	4	8	13	0	1	$\mathbb{Z}_2$
54	-27	-2	8	-3	0	≥ 1	$\mathbb{Z}_2$
55	-55	-1	4	-55	0	≥ 1	$\mathbb{Z}_2$
56	-7	-8	8	-7	0	≥ 1	$\mathbb{Z}_2$
57	57	1	4	57	0	1	$\mathbb{Z}_2$
59	-59	-1	4	-59	1	0	$\mathbb{Z}_2$
60	-15	-4	8	-15	0	≥ 1	$\mathbb{Z}_2$

Table 6.1: Numerical evidence for BSD Conjecture (Part 1)

D	E	F	K	R	$(\sqrt[4]{D}/\omega)L_D(1)$	Rank	Torsion
62	-31	-2	8	-31	0	≥ 1	$\mathbb{Z}_2$
65	65	1	4	65	0	2	$\mathbb{Z}_2$
66	33	2	8	33	0	≥ 1	$\mathbb{Z}_2$
67	-67	-1	4	-67	1	0	$\mathbb{Z}_2$
69	69	1	4	69	0	≥ 1	$\mathbb{Z}_2$
70	-35	-2	8	-35	0	1	$\mathbb{Z}_2$
71	-71	-1	4	-71	0	1	$\mathbb{Z}_2$
72	9	8	8	-3	0	≥ 1	$\mathbb{Z}_2$
76	-19	-4	8	-19	0	1	$\mathbb{Z}_2$
77	77	1	4	77	0	2	$\mathbb{Z}_2$
78	-39	-2	8	-39	0	1	$\mathbb{Z}_2$
82	41	2	8	41	0	3	$\mathbb{Z}_2$
83	-83	-1	4	-83	1	0	$\mathbb{Z}_2$
84	21	4	8	21	0	1	$\mathbb{Z}_2$
85	85	1	4	85	0	1	$\mathbb{Z}_2$
86	-43	-2	8	-43	0	1	$\mathbb{Z}_2$
87	-87	-1	4	-87	0	1	$\mathbb{Z}_2$
90	45	2	8	-15	0	≥ 2	$\mathbb{Z}_2$
91	-91	-1	4	-91	2	0	$\mathbb{Z}_2$
95	-95	-1	4	-95	0	≥ 1	$\mathbb{Z}_2$
97	97	1	4	97	0	2	$\mathbb{Z}_2$
99	-99	-1	4	33	0	≥ 1	$\mathbb{Z}_2$
101	101	1	4	101	0	1	$\mathbb{Z}_2$
102	-51	-2	8	-51	0	1	$\mathbb{Z}_2$
105	105	1	4	105	0	1	$\mathbb{Z}_2$
106	53	2	8	53	0	1	$\mathbb{Z}_2$
107	-107	-1	4	-107	1	0	$\mathbb{Z}_2$
110	-55	-2	8	-55	0	1	$\mathbb{Z}_2$
111	-111	-1	4	-111	0	≥ 1	$\mathbb{Z}_2$
114	57	2	8	57	0	≥ 1	$\mathbb{Z}_2$
115	-115	-1	4	-115	2	0	$\mathbb{Z}_2$
116	29	4	8	29	0	1	$\mathbb{Z}_2$
117	117	1	4	-39	0	2	$\mathbb{Z}_2$
119	-119	-1	4	-119	0	1	$\mathbb{Z}_2$
122	61	2	8	61	0	1	$\mathbb{Z}_2$
123	-123	-1	4	-123	2	0	$\mathbb{Z}_2$
124	-31	-4	8	-31	0	≥ 1	$\mathbb{Z}_2$
127	-127	-1	4	-127	0	1	$\mathbb{Z}_2$
130	65	2	8	65	0	1	$\mathbb{Z}_2$
131	-131	-1	4	-131	1	0	$\mathbb{Z}_2$
132	33	4	8	33	0	2	$\mathbb{Z}_2$

Table 6.2: Numerical evidence for BSD Conjecture (Part 2)

Chapter 7

Appendix

Proposition 7.0.1. Let R be a commutative ring, $I \subseteq R$ an ideal and $s_1, s_2 \in I$. If $s_1 \equiv s_2 \mod I^k$ for some $k \geq 1$, then $s_1^n \equiv s_2^n \mod I^{k+n-1}$ for all $n \geq 1$.

Proof. We'll prove it by induction on n. The case for $n = 1$ is the hypothesis. Suppose $s_1^n \equiv s_2^n \mod I^{k+n-1}$. Then,

$$\begin{aligned} & s_1^{n+1} = s_1(s_1)^n \\ = \quad & (s_2+\alpha)(s_2^n+\beta) && \Big(\text{Where } \alpha \in I^k,\ \beta \in I^{k+n-1}\Big) \\ = \quad & s_2^{n+1} + \alpha s_2^n + s_2\beta + \alpha\beta && \text{(Expand)} \\ \equiv \quad & s_2^{n+1} \mod I^{k+n} && \Big(\text{Since every other term is in } I^{k+n-1}\Big). \end{aligned}$$

□

Proposition 7.0.2. Let R be a ring and $\mathfrak{p}, \mathfrak{h} \subseteq R$ coprime ideals (i.e. $\mathfrak{p} + \mathfrak{h} = R$). Then, $\mathfrak{p}$ is still coprime to $\mathfrak{h}^n$ for all $n \geq 1$.

Proof. Suppose by contradiction that $\mathfrak{p} + \mathfrak{h}^n$ is proper, and thus contained in some maximal ideal $\mathfrak{m}$. But then,

$$R = \sqrt{R} = \sqrt{\mathfrak{p} + \mathfrak{h}} = \sqrt{\sqrt{\mathfrak{p}} + \sqrt{\mathfrak{h}^n}} = \sqrt{\mathfrak{p} + \mathfrak{h}^n} \subseteq \mathfrak{m},$$

which is a contradiction since $\mathfrak{m}$ is maximal, and thus proper. Here, we've used the facts that the radical of an ideal I is the intersection of all prime ideals containing I and that $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$. □

Proposition 7.0.3. Let p be a prime number and $n \geq 0$. Then,

$$\sum_{a \in \mathbb{F}_p^*} a^n = \begin{cases} 0 & (p-1) \nmid n, \\ p-1 & \text{otherwise.} \end{cases}$$

Proof. Suppose $p-1$ does not divide n and let $\beta \in \mathbb{F}_p^*$ be a generator. Then, $\beta^n \neq 1$ and

$$\sum_{a \in \mathbb{F}_p^*} a^n = \sum_{i=0}^{p-2} (\beta^n)^i = \frac{(\beta^n)^{p-1} - 1}{\beta^n - 1} = \frac{1-1}{\beta^n - 1} = 0.$$

If $(p-1) \mid n$, $\sum_{a \in \mathbb{F}_p^*} a^n = \sum_{a \in \mathbb{F}_p^*} 1 = p-1$. □

Theorem 7.0.4 (Abstract Chinese Remainder Theorem)**.** Let R be a commutative ring and $I, J \subseteq$ ideals such that $I + J = R$. Then, there is a ring isomorphism $\phi : R/(I \cap J) \to R/I \times R/J$ given by

$$\phi(x) := (x + I, x + J).$$

Proof. The map $x \in R \mapsto (x + I, x + J)$ clearly has kernel $I \cap J$, so ϕ is injective by the First Isomorphism Theorem. It remains to show surjectiveness. By hypothesis, we can Write $1 = i + j$ for $i \in I$, $j \in J$. Then, $1 \mapsto (1, 1) = (j + I, i + J)$, so $i \mapsto (I, 1 + J)$ and $j \mapsto (1 + I, J)$. For any $(r + I, s + J) \in R/I \times R/J$ we have

$$is + jr = (jr + I, is + J) = (r, s).$$

Therefore, the map is surjective. □

Proposition 7.0.5. Let a, b be coprime Gaussian integers. Let A be any set of representatives of the Gaussian residues modulo a, i.e. $A = \{a_i\}_{i=1}^{a}$, where $a_i \overset{a}{\cong} i$. Similarly, let B be any set of representatives of the Gaussian residues modulo b. Then, for all $z \in \mathbb{Z}[i]$ there is a unique triplet $k \in \mathbb{Z}[i], \alpha \in A, \beta \in B$ such that

$$z = abk + b\alpha + a\beta.$$

Proof. We first show existence. Since a and b are coprime, we have $(a) \cap (b) = (ab)$ and by Bezout's Identity $(a) + (b) = \mathbb{Z}[i]$. So by the Abstract Chinese Remainder Theorem 7.0.4, the map ϕ given by $z + (ab) \mapsto (z + (a), z + (b))$ is a ring isomorphism. Let $\alpha \in A, \beta \in B$ be the unique representatives such that $\alpha \overset{a}{\cong} b^{-1}z$ and $\beta \overset{b}{\cong} a^{-1}z$. Then, we have

$$\phi(b\alpha + a\beta) = (z, z) = \phi(z).$$

Since ϕ is an isomorphism, $b\alpha+a\beta \overset{ab}{\cong} z$, so there is some $k \in \mathbb{Z}[i]$ such that $z = abk+b\alpha+a\beta$. Now we prove uniqueness. Let $\alpha_1, \alpha_2 \in A$, $\beta_1, \beta_2 \in b$ and $k_1, k_2 \in \mathbb{Z}[i]$. Assume

$$abk_1 + b\alpha_1 + a\beta_1 = z = abk_2 = b\alpha_2 + a\beta_2.$$

We consider the equations mod a and mod b, obtaining

$$b\alpha_1 \overset{a}{\cong} b\alpha_2, \quad a\beta_1 \overset{b}{\cong} a\beta_2.$$

Therefore $\alpha_1 \overset{a}{\cong} \alpha_2$ and $\beta_1 \overset{b}{\cong} \beta_2$. But A and B contain exactly one representative for each Gaussian residue, so $\alpha_1 = \alpha_2$ and $\beta_1 = \beta_2$. But then, in the original equations we are left with $abk_1 = abk_2$, so $k_1 = k_2$. □

Corollary 7.0.6. Let $K = \pm 2^k$ and R be primary. Let A be the set of representatives for the elements in $\mathbb{Z}[i]/(R)$. Let B be the set of representatives for the elements in $\mathbb{Z}[i]/(K)$. Then, for all $z \in \mathbb{Z}[i]$ be primary and coprime to R, there is a unique triplet $k \in \mathbb{Z}[i], \alpha \in A, \beta \in B$, with α coprime to R and β primary, such that

$$z = abk + b\alpha + a\beta.$$

Proof. By Proposition 7.0.5 we know there is a unique triplet (k, α, β) satisfying the equation. It thus suffices to show that α must be coprime to R and β must be primary. We have

$$z = KRk + K\alpha + R\beta = K\alpha + R(\beta + Kk).$$

Since z is coprime to R, α must also be coprime to R. Similarly,

$$1 \overset{2+2i}{\cong} z = KRk + K\alpha + R\beta \overset{2+2i}{\cong} = \beta,$$

so β must be primary. □

7.1 Power residues

Definition 7.1.1. Let p be a prime number. For $n \geq 0$, let $R_n < \mathbb{Z}_p^*$ be the subgroup of 2^n−residues. That is,

$$R_n := \{a \in \mathbb{Z}_p^* \ : \ x^{2^n} \overset{p}{\equiv} a \text{ admits solution}\}.$$

Note that $R_{n+1} < R_n$ for all n.

Proposition 7.1.2. Let p be an odd prime and pick $k \geq 1$ such that $p \overset{2^{k+1}}{\equiv} 2^k + 1$. Then, for all $a \in \mathbb{Z}$,

1. for $r \leq k$, $a \in R_r \iff a^{(p-1)/2^r} \overset{p}{\equiv} 1$; moreover $[R_{r-1} : R_r] = 2$;
2. for $r \geq k$, $R_r = R_k$.

Proof. Statement 1: we prove the first part by induction. For $r = 0$, the left side of the equivalence is trivially true and the right side becomes Fermat's Little Theorem. For $0 < r \leq k$, we have two directions to prove. ($\Rightarrow$) In this case, let $a = b^{2^r}$, then $a^{(p-1)/2^r} = b^{p-1} \overset{p}{\equiv} 1$. ($\Leftarrow$) By squaring both sides we get $a^{(p-1)/2^{r-1}} = 1$. By induction $a = b^{2^{r-1}}$ and so $b^{(p-1)/2} \overset{p}{\equiv} 1$. By Euler's criterion $b = c^2$. So $a = c^{2^r}$ and we're done. To prove the second part, define the homomorphism $\phi : R_{k-1} \to \{\pm 1\}$ given by

$$\phi(x) := x^{(p-1)/2^k} \mod p.$$

This is well-defined since for $x = y^{2^{k-1}}$, $\phi(x) = y^{(p-1)/2}$ which is congruent to ± 1 by Euler's criterion. Ker(ϕ) is equal to the subgroup of 2^k-residues, $R_k < R_{k-1}$. Also ϕ is clearly surjective since $\left(\frac{\cdot}{p}\right)$ is surjective. Therefore $[R_{k-1} : R_k] = 2$.

Statement 2: again, we'll argue by induction. For $r = k$ there is nothing to prove. For $r + 1 > k$, assume a is a 2^r-residue. We want to show that it is also a $2^{r+1}-$residue. Write $a = b^{2^r}$ and $c := b^{2^{k-1}}$, so $a = c^{2^{r+1-k}}$. If c is a 2^k-residue, we're done. Suppose it isn't. By Proposition 2.3.10, -1 is not a 2^k-residue. Since $[R_{k-1} : R_k] = 2$ by Statement 2, it follows that $-c$ is a 2^k-residue. So $c = d^{2^k}$ and $a = c^{2^{r+1-k}} = d^{2^{k+1}}$. □

7.2 Proof of the Descent Theorem

Proof of Theorem 4.0.4. ($1 \Rightarrow 2$) First, we'll show that $|\Gamma/2\Gamma| < \infty$. Let $a_1, ..., a_n$ be the generators of Γ and pick $[p] \in \Gamma/2\Gamma$. We have that

$$p = \sum_{i=1}^{n} n_i a_i \equiv \sum_{i=1}^{n} k_i a_i.$$

where $|k_i| \leq 1$. So, the set is finite.

Now we'll show that Γ admits a height. By the Fundamental Theorem of Finitely Generated Abelian Groups, we know that $\Gamma \cong \mathbb{Z}^n \oplus H$ for some finite group H. For $p = (p_1, ..., p_n, h) \in \Gamma$, define the height (h, s, k) of Γ as $h(p) := \max_i |p_i|^2$, $s(p) := 2h(p)$, $k := 0$. We need to prove the three properties established in Definition 4.0.3. Property (3) clearly holds. For property (2) we have

$$h(2p) = \max_i |2p_i|^2 = 4 \max_i |p_i|^2 = 4h(p) = 4h(p) + k.$$

Lastly, for property (1),

$$\begin{aligned} h(p+q) &= \max_i |p_i + q_i|^2 \le \max_i (|p_i| + |q_i|)^2 \le \max_i 2(|p_i|^2 + |q_i|^2) \\ &= 2\max_i |p_i|^2 + 2\max_i |q_i|^2 = 2h(p) + s(q). \end{aligned}$$

($2 \Rightarrow 1$) Let $p_0 \in \Gamma$. Let $\{q_1, ..., q_n\} = \Gamma/2\Gamma$. Then, we have that

$$\begin{aligned} p_0 &= q_{i_1} + 2p_1 \\ p_1 &= q_{i_2} + 2p_2 \\ &\vdots \\ p_{m-1} &= q_{i_m} + 2p_m. \end{aligned}$$

And so $p_0 = q_{i_1} + 2q_{i_2} + ... + 2^{m-1}q_{i_m} + 2^m p_m$. So, p can be written as a combination of $\{q_1, ..., q_n, p_m\}$. We will show that, for m large enough, p_m has only finitely many possible values. For any p_j with $j \ge 1$ we have that

$$4h(p_j) \le h(2p_j) + k = h(p_{j-1} - q_{i_j}) + k \le 2h(p_{j-1}) + s(-q_{i_j}) + k \le 2h(p_{j-1}) + k' + k.$$

Here, $k' := \max_i h(-q_i)$. And so we get

$$h(p_j) \le \frac{1}{2}h(p_{j-1}) + \frac{1}{4}(k' + k) = \frac{3}{4}h(p_{j-1}) - \frac{1}{4}(h(p_{j-1}) - (k' + k)).$$

We have two possibilities.

(Case 1: $h(p_{j-1}) - (k' + k) \le 0$) In this case, $h(p_{j-1})$ is bounded by $k' + k$.

(Case 2: $h(p_{j-1}) - (k' + k) > 0$) In this case, $h(p_j) < (3/4)h(p_{j-1})$. So the height has decreased by a factor of 3/4. We can keep decreasing the height in this fashion until we end up at case 1.

And so we conclude that there must be some m such that $h(p_m) \le k' + k$. By the third height property, we get that p_m belongs to the finite family $\{t_1, ..., t_N\} = \{x \in \Gamma \ : \ h(x) \le k' + k\}$. With this, p_0 can be written as a combination of $\{q_1, ..., q_n, t_1, ..., t_N\}$. Since p_0 was arbitrary, Γ is finitely generated. □

Bibliography

[1] Levent Alpöge. *Nagell-Lutz, quickly.* `https://people.math.harvard.edu/~alpoge/papers/nagell-lutz,quickly.pdf`.

[2] John Baez. *Counting Points on Elliptic Curves.* `https://golem.ph.utexas.edu/category/2024/03/counting_points_on_elliptic_cu.html`. 2024.

[3] Elwyn R Berlekamp. *Algebraic coding theory (revised edition).* World Scientific, 2015.

[4] Bryan John Birch and Henry Peter Francis Swinnerton-Dyer. "Notes on elliptic curves. II." In: *Journal für die reine und angewandte Mathematik* (1965).

[5] David G Cantor and Hans Zassenhaus. "A new algorithm for factoring polynomials over finite fields". In: *Mathematics of Computation* (1981), pp. 587–592.

[6] John WS Cassels. *Rational quadratic forms.* Vol. 74. Elsevier, 1982, pp. 9–26.

[7] Robert Coquereaux, Alex Grossmann, and Benny E Lautrup. "Iterative method for calculation of the Weierstrass elliptic function". In: *IMA journal of numerical analysis* 10.1 (1990), pp. 119–128.

[8] David A Cox. *Primes of the Form x2+ ny2: Fermat, Class Field Theory, and Complex Multiplication. with Solutions.* Vol. 387. American Mathematical Soc., 2022.

[9] John Cremona and David Rusin. "Efficient solution of rational conics". In: *Mathematics of Computation* 72.243 (2003), pp. 1417–1441.

[10] William D'Alessandro. "Proving quadratic reciprocity: Explanation, disagreement, transparency and depth". In: *Synthese* 198.9 (2021), pp. 8621–8664.

[11] Max Deuring. *Die Zetafunktion einer algebraischen Kurve von Geschlechte Eins.* Vol. I, II, III, IV. Nachr. Akad. Wiss. Göttingen, (1953) 85–94, (1955) 13–42, (1956) 37–76, (1957) 55–80.

[12] Fred Diamond. "On deformation rings and Hecke rings". In: *Annals of Mathematics* 144.1 (1996), pp. 137–166.

[13] Andrej Dujella. *History of elliptic curves rank records.* `https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html`.

[14] David Farmer et al. "Analytic L-functions: Definitions, theorems, and connections". In: *Bulletin of the American Mathematical Society* 56.2 (2019), pp. 261–280.

[15] Benedict H Gross and Don B Zagier. “Heegner points and derivatives of L-series”. In: *Inventiones mathematicae* 84 (1986), pp. 225–320.

[16] Xiang-dong Hou. *Lectures on finite fields.* Vol. 190. American Mathematical Soc., 2018.

[17] D. Husemöller. *Elliptic curves.* Second. Vol. 111. Graduate Texts in Mathematics. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen. New York: Springer-Verlag, 2004, pp. xxii+487. ISBN: 0-387-95490-2.

[18] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory.* Vol. 84. Springer Science & Business Media, 2013.

[19] Nathan Jacobson. *Basic Algebra II, 1989.*

[20] S. Kamienny. “Torsion points on elliptic curves and q-coefficients of modular forms”. In: *Invent. Math.* 109.2 (1992), pp. 221–229. ISSN: 0020-9910.

[21] Anthony W Knapp. *Elliptic curves.* Vol. 40. Princeton University Press, 1992.

[22] Neal Koblitz. *Introduction to elliptic curves and modular forms.* Vol. 97. Springer Science & Business Media, 1993.

[23] Franz Lemmermeyer. *Reciprocity laws: from Euler to Eisenstein.* Springer Science & Business Media, 2013.

[24] Martin Leslie. “Descent on Elliptic Curves”. PhD thesis. Citeseer, 2007.

[25] Álvaro Lozano-Robledo. *Recent progress in the classification of torsion subgroups of elliptic curves.* `https://alozano.clas.uconn.edu/wp-content/uploads/sites/490/2019/09/UNION-Torsion-survey-v1.pdf`. 2019.

[26] B. Mazur. “Modular curves and the Eisenstein ideal”. In: *Inst. Hautes Études Sci. Publ. Math.* 47 (1977), 33–186 (1978). ISSN: 0073-8301.

[27] B. Mazur. “Rational isogenies of prime degree (with an appendix by D. Goldfeld)”. In: *Invent. Math.* 44.2 (1978), pp. 129–162. ISSN: 0020-9910.

[28] Loïc Merel. “Bornes pour la torsion des courbes elliptiques sur les corps de nombres”. In: *Invent. Math.* 124.1-3 (1996), pp. 437–449. ISSN: 0020-9910.

[29] James S Milne. *Algebraic number theory.* JS Milne, 2008.

[30] Louis Joel Mordell. *Diophantine Equations: Diophantine Equations.* Academic press, 1969.

[31] Jürgen Neukirch. *Algebraic number theory.* Vol. 322. Springer Science & Business Media, 2013.

[32] Lucas Rufino. *Elliptic curve calculator, available online at: https://github.com/lucas-martelotte/elliptic_ curve_ calculator*. Github, 2025.

[33] Jean-Pierre Serre. *Local fields.* Vol. 67. Springer Science & Business Media, 2013.

[34] Jerry Shurman. *Zorotalev’s Proof of Quadratic Reciprocity.* `https://people.reed.edu/~jerry/361/lectures/qrz.pdf`.

[35] Joseph H Silverman. *The arithmetic of elliptic curves*. Vol. 106. Springer, 2009.

[36] Joseph H Silverman and John Torrence Tate. *Rational points on elliptic curves*. Vol. 9. Springer, 1992.

[37] Joseph H. Silverman. *The arithmetic of elliptic curves*. Vol. 106. Graduate Texts in Mathematics. Corrected reprint of the 1986 original. New York: Springer-Verlag, 1992, pp. xii+400. ISBN: 0-387-96203-4.

[38] Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. New York: Springer-Verlag, 1992, pp. x+281. ISBN: 0-387-97825-9.

[39] Denis Simon. "Solving quadratic equations using reduced unimodular quadratic forms". In: *Mathematics of Computation* 74.251 (2005), pp. 1531–1543.

[40] Michael Stoll. "Descent on elliptic curves". In: *arXiv preprint math/0611694* (2006).

[41] Ye Tian. "Congruent number problem". In: *Notices of the International Consortium of Chinese Mathematicians* 5.1 (2017), pp. 51–61.

[42] Jacques Vélu. "Isogenies between elliptic curves". In: *l'Académie, Sci. Paris, Sér. A* 273 (1971), pp. 1–5.

[43] Lawrence C Washington. *Elliptic curves: number theory and cryptography*. Chapman and Hall/CRC, 2008.

[44] André Weil. "L'arithmétique sur les courbes algébriques". In: *Acta mathematica* 52 (1929), pp. 281–315.