



ELLIPTIC CURVES OVER $\mathbb{Q}(i)$

Thotsaphon Thongjunthug

Supervisor: Peter G. Brown

School of Mathematics,
The University of New South Wales.

November 2006

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF THE DEGREE OF
BACHELOR OF SCIENCE WITH HONOURS

Acknowledgements

I would like to thank my supervisor Peter Brown for his time and devotion throughout this year. Without his useful suggestions (for both mathematics and English), this thesis certainly could not have come this far.

I also wish to thank all of my fellow Honours students for their direct and indirect support during the year. Their busy lifestyles always make me ashamed, but encourage me to take my responsibility seriously.

My family also deserves some thanks for their support during my (hard) time overseas. Although they might not have much idea what sort of science I am majoring in, I hope to make them aware of it in a very near future.

Last but not least, I heartily thank the Development and Promotion of Science and Technology (DPST) Project, Ministry of Education of Thailand, who has been my sponsor-body over the last eight years.

Thotsaphon Thongjunthug
Sydney, 2 November 2006.

Introduction

The study of elliptic curves is one of many active research areas in mathematics nowadays. Although it has been significantly developed over the last three decades, some aspects of elliptic curves were studied much earlier. Elliptic curves have a number of applications in number theory and related fields, such as cryptography, and solutions of many Diophantine problems. In particular, they are well-known as the main tools in the proof of *Fermat's Last Theorem*, which was eventually proven in 1994 by Wiles.

There are a number of Diophantine equations which can be transformed to elliptic curves. The integer solutions of the original equation also correspond to rational points on the elliptic curve. Some Diophantine problems can be transformed into elliptic curves over $\mathbb{Q}(i)$, where

$$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}.$$

Thus it becomes an interesting question whether there are some connections between elliptic curves over \mathbb{Q} , and elliptic curves over $\mathbb{Q}(i)$. In particular, is it possible to extend some well-known results for elliptic curves over \mathbb{Q} , in order to be applicable to elliptic curves over $\mathbb{Q}(i)$?

This thesis is an introductory investigation of this question. It covers the basic theory on elliptic curves, and then extends these from \mathbb{Q} to $\mathbb{Q}(i)$. Rather than using sophisticated mathematics, the approach in this thesis is mainly based on modifying certain basic concepts in the original proofs in an elementary way.

In Chapter 1, we begin with some motivative examples, the formal definition of an elliptic curve over a field K , as well as the concept of the point at infinity, using the notion of projective space.

Chapter 2 aims to introduce the concept of addition on elliptic curves. In this chapter, we will start with the geometrical construction of such addition as well as its corresponding algebraic interpretation. At the end, we shall deduce the fact that this addition makes the set of all points on an elliptic curve into an abelian group — this is essential to the study of other algebraic properties in Chapter 3, 4, and 5.

As a consequence of addition on elliptic curves, the notion of torsion subgroups and their group structures then becomes the subject of Chapter 3. In this chapter, we will first focus on determining the torsion subgroup of $E(\mathbb{Q})$ — the set of all rational points on the elliptic curve E , using the Lutz-Nagell theorem. Mazur's

theorem then tells us which groups actually occur. In particular, the generalisation of Lutz-Nagell theorem from $E(\mathbb{Q})$ to $E(\mathbb{Q}(i))$ will be the centrepiece of this chapter.

In Chapter 4, we will move our attention to elliptic curves defined over a finite field. For this type of elliptic curve, the same concept of addition and order of points is still valid and will be considered via a number of examples. At the end, we will also study one particular family of elliptic curves over \mathbb{Z}_p , when $p \equiv 3 \pmod{4}$. This includes the result on determining the number of points on this curve, and the extended version over

$$\mathbb{Z}_p(i) = \{a + bi : a, b \in \mathbb{Z}_p\},$$

where $p \equiv 3 \pmod{4}$.

Chapter 5 will concentrate on Mordell-Weil theorem on $E(\mathbb{Q})$, which is a fundamental for the study of rank and the zeta function in Chapter 6. In this chapter, we will be interested in the theoretical development of this theorem during 1920s, and more importantly, how to derive the analogous result for the case $E(\mathbb{Q}(i))$ by some elementary modifications of the original proof.

Further concepts on the rank and zeta function then follow from Mordell-Weil theorem, and will be described in deeper detail in Chapter 6. This chapter will give some overview of the zeta function and L -function associate with an elliptic curve, which was the motivation behind a number of famous conjectures on the relationship between the (algebraic) rank of $E(\mathbb{Q})$, and the analytic rank.

The last chapter of this thesis looks briefly at the study of integral points on elliptic curves. Unlike the problem of finding rational points on elliptic curves, determining the set of all integer points is computationally more difficult. In this chapter, we will first study some well-known results on integral points on elliptic curves over \mathbb{Q} and $\mathbb{Q}(i)$. In addition, we will focus on determining all Gaussian integer points on a particular elliptic curve over $\mathbb{Q}(i)$, which is motivated by the recently published paper by Draziotis [12] in 2006.

In this thesis, a number of examples on elliptic curves over $\mathbb{Q}(i)$ are computed by `Maple` mathematical package. All `Maple` scripts used for calculating addition on elliptic curves, torsion subgroups (based on extended Lutz-Nagell theorem), and some Gaussian integer solutions to the equation $ic^2 = a^2 + b^2$, are given in Appendix A.

Contents

Chapter 1	Introduction	1
1.1	History	1
1.2	Motivative Example	1
1.3	The Weierstrass Equation	2
1.4	Formal Definition	3
1.5	Projective Space and the Point at Infinity	4
1.6	Motivation to Elliptic Curves over $\mathbb{Q}(i)$	5
Chapter 2	Basic Theory	7
2.1	Visualising Elliptic Curves	7
2.2	Additive Law on the Curve	8
2.3	Torsion Points	9
Chapter 3	Lutz-Nagell Theorem	11
3.1	Original Version	11
3.2	Extended Lutz-Nagell Theorem	13
3.2.1	Preliminaries	14
3.2.2	Birational Map	15
3.2.3	Geometrical Interpretation	17
3.2.4	Obtaining the Contradiction	18
3.3	Boundedness of Torsion Subgroups	20
3.3.1	Mazur's Theorem	20
3.3.2	Boundedness Conjecture	22
3.3.3	Torsion subgroups of $E(\mathbb{Q}(i))$	22
Chapter 4	Elliptic Curves over Finite Fields	24
4.1	Overview	24
4.2	Order of Points	26
4.3	Elliptic Curves over $\mathbb{Z}_p(i)$	27
4.3.1	A Particular Family of Elliptic Curves	28
4.3.2	Supersingular Curves	31
4.3.3	The Frobenius Endomorphism	32
Chapter 5	Mordell-Weil Theorem	34
5.1	Original Theorem	34

5.2	Height Function	35
5.2.1	Modification of Height Function	36
5.2.2	Further Duplication Formula	39
5.3	Weak Mordell-Weil Theorem	43
5.3.1	Analog of the Original Theorem	43
5.4	Examples	50
Chapter 6 Rank and Zeta Function		55
6.1	History	55
6.2	Elliptic Curves over Finite Fields	55
6.3	L -Functions and Elliptic Curves over \mathbb{Q}	58
6.4	Rank of Elliptic Curves	61
6.4.1	Birch and Swinnerton-Dyer Conjecture	62
6.4.2	Average Rank of Elliptic Curves	63
6.4.3	Complex Multiplication	64
Chapter 7 Integer Points on Elliptic Curves		66
7.1	Diophantine Equations and Hilbert's Problems	66
7.2	Integer Points on Elliptic Curves over \mathbb{Q}	66
7.3	Gaussian Integer Points on Elliptic Curves over $\mathbb{Q}(i)$	69
7.3.1	Analog of Mordell's Theorem	69
7.4	A Particular Family of Elliptic Curves over $\mathbb{Q}(i)$	71
Appendix A Maple Scripts used in the Thesis		78
A.1	Addition on Elliptic Curves: <code>addition.mpl</code>	78
A.2	Extended Lutz-Nagell Theorem	79
A.2.1	<code>eqntrans.mpl</code>	80
A.2.2	<code>listposy.mpl</code>	82
A.2.3	<code>torsion.mpl</code>	83
A.3	On the Equation $ic^2 = a^2 + b^2$: <code>triple.mpl</code>	86
References		89

CHAPTER 1

Introduction

1.1 History

The study of elliptic curves is currently an active area of mathematical research, which has been significantly developed over the last three decades. During 1980s–1990s, applications of elliptic curves significantly contributed to a large number of mathematical breakthroughs in number theory and related fields, such as cryptography, factorisation techniques, and primality testing. In particular, Wiles’ paper *Modular elliptic curves and Fermat’s Last Theorem* in 1994 used elliptic curves and modular forms to prove Fermat’s Last Theorem. They are also closely related to a number of famous problems from the ancient Greeks.

1.2 Motivative Example

The following example comes from Diophantus *Arithmetica* (around 250 A.D.) [42]:

Is there a right triangle with rational sides with area equal to 5? Firstly let the triangle we are looking for have sides $a, b, c \in \mathbb{Q}$. Since the area is $ab/2 = 5$, the problem is now transformed into looking for a, b, c satisfying

$$a^2 + b^2 = c^2, \quad ab = 10$$

simultaneously. Observe that

$$\left(\frac{a+b}{2}\right)^2 = \frac{a^2 + 2ab + b^2}{4} = \left(\frac{c}{2}\right)^2 + 5,$$

and

$$\left(\frac{a-b}{2}\right)^2 = \frac{a^2 - 2ab + b^2}{4} = \left(\frac{c}{2}\right)^2 - 5.$$

Writing $x = (c/2)^2$, the given problem is equivalent to finding x such that

$$x - 5, \quad x, \quad x + 5$$

are simultaneously the squares of rational numbers. If such an x exists, then the product $x(x-5)(x+5) = x^3 - 25x$ must also be the square of some rational number.

Thus we seek $x, y \in \mathbb{Q}$ such that

$$y^2 = x^3 - 25x.$$

An equation of this type represents an *elliptic curve*, which we shall formally define later. The above equation has $(0, 0), (\pm 5, 0)$ as trivial solutions. A little experiment yields the solution $(-4, 6)$. If we take the tangent line to the elliptic curve at the point $(-4, 6)$, i.e.

$$y = \frac{23}{12}x + \frac{41}{3},$$

and substitute back to our elliptic curve, we find the point of intersection is

$$(1681/144, 62279/1278).$$

Since $x = (c/2)^2$, we obtain $c = 41/6$. Thus

$$y = \frac{62279}{1278} = \frac{(a+b)c(a-b)}{8} = \frac{41(a^2 - b^2)}{48}.$$

This gives us $a^2 - b^2 = 1519/36$. But we already know that $a^2 + b^2 = c^2 = (41/6)^2$, so eventually we have

$$a = \frac{20}{3}, \quad b = \frac{3}{2}, \quad c = \frac{41}{6}.$$

Clearly a triangle with these sides has area 5 as desired. ■

In this example, the Diophantine problem can be transformed into finding a rational point on an elliptic curve with *rational coefficients*.

Before proceeding to the formal definition of an elliptic curve, we recall:

Definition 1.2.1. *Let K be a field. The characteristic of K , denoted by $\text{char}(K)$ is the smallest positive integer n such that*

$$n \cdot 1_K = \underbrace{1_K + 1_K + \dots + 1_K}_{n \text{ times}} = 0_K,$$

where 0_K and 1_K are the additive and multiplicative identity elements of K , respectively. If such n does not exist, then K is said to have characteristic 0.

It can be shown that $n = \text{char}(K)$ is either 0 or a prime number.

1.3 The Weierstrass Equation

We have seen, in Section 1.2, an example of an elliptic curve of the form $y^2 = f(x)$, where $f(x)$ is some cubic polynomial. The general form of an elliptic curve over a field K is given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6; \quad a_i \in K.$$

This is called the *generalised Weierstrass equation*. If $\text{char}(K) \neq 2$, then we can divide by 2 and complete the square to get

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right).$$

By substituting $y_1 = y + a_1x/2 + a_3/2$, we can write this as

$$y_1^2 = x^3 + a'_2x^2 + a'_4x + a'_6; \quad \text{where } a'_i \in K.$$

Moreover if $\text{char}(K)$ is also not equal to 3, we can even simplify above equation further. Let $x_1 = x + a'_2/3$. Then we obtain an equation of the form

$$y_1^2 = x_1^3 + Ax_1 + B; \quad \text{where } A, B \in K. \quad (1.1)$$

Thus any elliptic curve over a field K , where the characteristic is neither 2 nor 3, can be written in the form (1.1), which will be referred to as the *Weierstrass equation*.

1.4 Formal Definition

Definition 1.4.1. *An elliptic curve E over a field K is a graph of the form*

$$y^2 = f(x) = x^3 + Ax + B,$$

where $A, B \in K$ and all roots of $f(x)$ are distinct. We define $E(L)$ to be the set of ordered pairs

$$\{(x, y) \in L \times L : y^2 = f(x)\} \cup \{\infty\}$$

where $L \supseteq K$ is a field. The extra point ∞ is called the point at infinity.

Points in $E(L)$ are called *L -points* of the elliptic curve E . In the example in Section 1.2, we have $K = L = \mathbb{Q}$. Inclusion of the point at infinity will be explained in more detail in Section 1.5.

Now the question as to whether all roots of $f(x)$ are distinct can be checked using the following theorem

Theorem 1.4.2. *The following statements are equivalent:*

1. *All roots of $f(x)$ are distinct.*
2. *Let $F(x, y) = y^2 - f(x)$. There is no point on E at which*

$$\frac{\partial F}{\partial x} = -f'(x) \text{ and } \frac{\partial F}{\partial y} = 2y$$

vanish simultaneously, (in which case we say that E is non-singular).

3. *The discriminant of $f(x)$, defined by $D = -(4A^3 + 27B^2)$, is non-zero.*

Proof: Suppose that there is a point $(x_0, y_0) \in E$ where both partial derivatives are zero. Then we have $f'(x_0) = 0$ and $2y_0 = 0$. It follows that $f(x_0) = y_0^2 = 0$. Since $f(x_0) = f'(x_0) = 0$, $f(x)$ must have a repeated root.

Conversely, suppose $f(x)$ has a repeated root x_0 , i.e.

$$y^2 = f(x) = (x - x_0)^2(x - \alpha)$$

for some α . Then for $F(x) = y^2 - f(x)$, we have

$$\frac{\partial F}{\partial x} = -((x - x_0)^2 + 2(x - x_0)(x - \alpha)), \quad \frac{\partial F}{\partial y} = 2y_0,$$

which will both vanish at $(x_0, y_0) = (x_0, 0)$. Hence (1) is equivalent to (2).

If we factor $f(x)$ over the complex numbers as

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3), \quad \alpha_i \in \mathbb{C},$$

it can be checked using properties of coefficients and roots of polynomials that

$$D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2.$$

Thus $f(x)$ has a repeated root if $D = 0$, and vice versa, i.e., (2) is equivalent to (3).

■

1.5 Projective Space and the Point at Infinity

Let K be a field. The *projective space over K* , denoted by \mathbf{P}_K^2 , is the set of all equivalence classes of $(x, y, z) \in K^3 - \{(0, 0, 0)\}$ arising from the equivalence relation

$$(x_1, y_1, z_1) \sim (x_2, y_2, z_2) \iff (x_1, y_1, z_1) = \lambda(x_2, y_2, z_2), \quad \text{for some } \lambda \neq 0_K \in K.$$

The equivalence class of (x, y, z) is denoted by $(x : y : z)$, since it only depends the ratio of x to y to z .

We say that a polynomial is *homogeneous* of degree n if it is a sum of terms of the form $ax^i y^j z^k$ with $a \in K$ and $i + j + k = n$. For example, the polynomial $x^3 + 2x^2y + 7z^3$ is homogeneous of degree 3 whereas $x^3 + y$ is not. Clearly if $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ and F is homogeneous, then $F(x_1, y_1, z_1) = 0$ if and only if $F(x_2, y_2, z_2) = 0$. Thus we will only work with homogeneous polynomials.

Now consider an elliptic curve E with Weierstrass equation $y^2 = x^3 + Ax + B$. Its homogeneous form is $y^2z = x^3 + Axz^2 + Bz^3$. If $z \neq 0$, we can divide both sides by z^3 to get

$$\left(\frac{y}{z}\right)^2 = \left(\frac{x}{z}\right)^3 + A\left(\frac{x}{z}\right) + B \implies Y^2 = X^3 + AX + B.$$

where $X = x/z, Y = y/z$. The projective points on the curve correspond to the equivalence class $(x : y : 1)$, i.e. all points (x, y) on the original curve. Suppose now $z = 0$. It follows from the homogeneous form that $0 = x^3$, i.e. $x = 0$. Thus y can be any non-zero (as x, y, z cannot be all zero from the definition). This case corresponds to the equivalence class $(0 : 1 : 0)$, and we refer this as *the point at infinity* of E .

The last case implies that any vertical lines intersect E at infinity. Also, since $(0 : 1 : 0) = (0 : -1 : 0)$, the point at infinity is unique, as there is no difference between the top and the bottom of y -axis. This explains the inclusion of ∞ in the definition of an elliptic curve.

1.6 Motivation to Elliptic Curves over $\mathbb{Q}(i)$

The study of Diophantine problems is closely related to elliptic curves in several aspects. In particular, many Diophantine problems can be transformed into elliptic curves, and thus finding solutions to the original problem is equivalent to solving for rational points on the corresponding elliptic curve.

Yet the information on rational points on a particular elliptic curve is often insufficient to give a complete answer to some certain types of Diophantine problems. This situation normally arises after introducing a change of variable which involves complex numbers. The following example was introduced by Peter Brown:

Consider the Diophantine equation

$$v^2 = 2u^4 - 1.$$

It is well-known that the only integer solutions (u, v) to this equation are $(1, 1)$ and $(13, 239)$, as proved by Ljunggren in 1942. With the change of variable

$$x = \frac{2iv - 2}{u^2}, \quad y = \frac{-4(v + i)}{u^3},$$

the Diophantine equation can be transformed into the elliptic curve

$$y^2 = x^3 + 8x, \tag{1.2}$$

where clearly $x, y \in \mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$. It can be checked that

$$(u, v) = (1, 1) \iff (x, y) = (-2 + 2i, -4 - 4i),$$

and also

$$(u, v) = (13, 239) \iff (x, y) = \left(\frac{2(-1 + 239i)}{13^2}, \frac{-4(239 + i)}{13^3} \right).$$

After multiplying (1.2) both sides with 13^6 , and letting $X = 13^2x$ and $Y = 13^3y$, we obtain a new elliptic curve

$$Y^2 = X^3 + 8 \times 13^4 X, \tag{1.3}$$

and thus it follows that

$$\begin{aligned} (u, v) = (1, 1) &\iff (X, Y) = (2 \times 13^2(-1 + i), 4 \times 13^3(-1 - i)) \\ (u, v) = (13, 239) &\iff (X, Y) = (2(-1 + 239i), -4(239 + i)). \end{aligned}$$

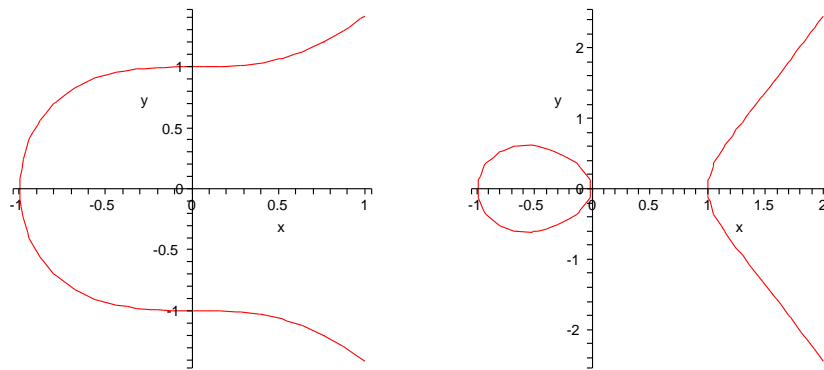
Clearly the solutions to the original Diophantine problem now correspond to two Gaussian integer points on the elliptic curve (1.3), rather than just rational (or integer) points.

CHAPTER 2

Basic Theory

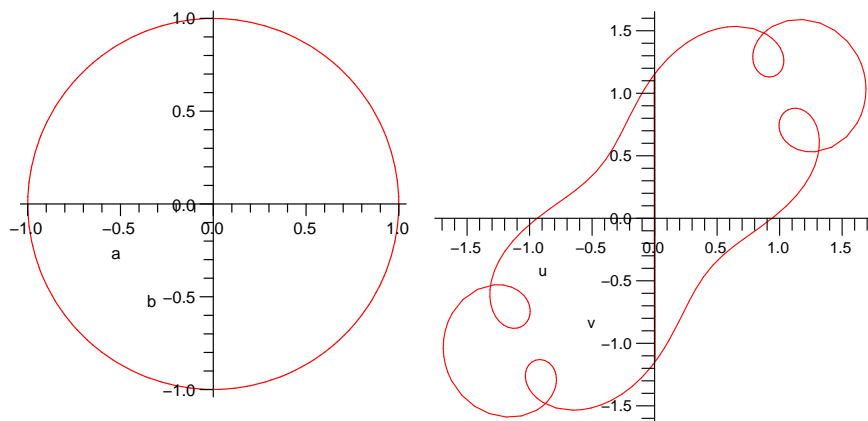
2.1 Visualising Elliptic Curves

Visualising the curve defined over an arbitrary number field K is not always possible. In the case when $L = \mathbb{R}$, it is quite easy to draw a meaningful graph and observe some geometric properties from the equation. Consider 2 elliptic curves defined by $y^2 = x^3 + x$ (left) and $y^2 = x^3 - x$ (right):



The first fact we may observe is the symmetry about x -axis due to the presence of the y^2 term. Also the graph has either only 1 component or 2 components, according as the cubic has 1 or 3 real roots.

For $K = \mathbb{Q}(i)$, we may regard the equation as a map from \mathbb{C} to \mathbb{C} . Consider an elliptic curve $y^2 = x^3 + (1 + i)x + 2i$ where $x, y \in \mathbb{C}$



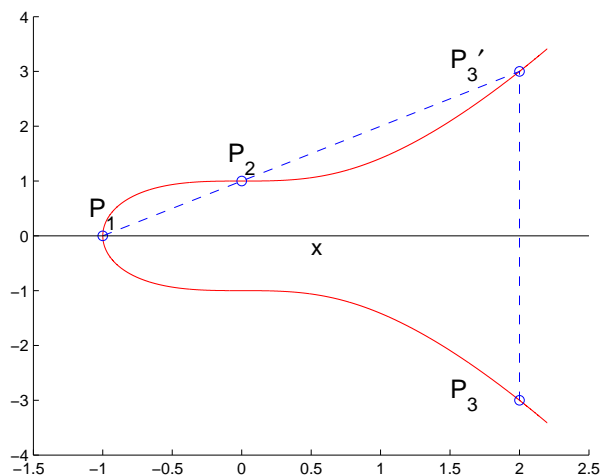
By substituting all points $x = a + bi \in \mathbb{C}$ with modulus 1 (in the left) into the elliptic curve, we obtain the curve $y = u + iv$ on the right.

2.2 Additive Law on the Curve

We will now show how to define the addition of any 2 points on an elliptic curve, in such a way that the points on our elliptic curve form an additive abelian group. Although the arithmetic in this section is geometrically motivated for the real numbers, it extends to elliptic curves over any number field K with $\text{char}(K) \neq 2$.

Consider an elliptic curve E over the real numbers. It is obvious that a line passing through any 2 points P_1, P_2 on E will always intersect the curve at a third point on E . If we know only one point P_1 on E , the tangent line at P_1 will also intersect the curve at another point on E . (Note that if a tangent line is vertical, we say that it intersects the curve at ∞). We denote such a point of intersection as P'_3 , and define $P_3 = P_1 + P_2$ by $-P'_3$, the point obtained by reflecting P'_3 about x -axis.

For instance, $(0, 1)$ and $(-1, 0)$ are on the curve $y^2 = x^3 + 1$. The line passing through these 2 points intersects the curve again at $(2, 3)$, so $(0, 1) + (-1, 0) = (2, -3)$.



To be more precise, let us start with 2 points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on an elliptic curve E given by $y^2 = x^3 + Ax + B$.

1. Suppose $P_1 \neq P_2$ and neither point is ∞ . Let L be a straight line through P_1 and P_2 , then its slope is $m = (y_2 - y_1)/(x_2 - x_1)$.
 - If $x_1 = x_2$, then L is a vertical line, which thus intersects E at ∞ . Reflecting ∞ will give ∞ . Hence we have $P_3 = \infty$.

- Otherwise, L has equation $y = m(x - x_1) + y_1$. Substituting this into E gives

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B.$$

By rearranging the terms, we get

$$0 = x^3 - m^2x^2 + \dots$$

Since we know that $m^2 = x_1 + x_2 + x_3$ and x_1, x_2 are already given, thus we have $x_3 = m^2 - x_1 - x_2$. Substituting x_3 we get $y'_3 = -y_3$.

2. If $P_1 = P_2 = (x_1, y_1)$, take L to be a tangent line at that point. Implicit differentiation gives us

$$2y \frac{dy}{dx} = 3x^2 + A \implies m = \frac{dy}{dx} = \frac{3x^2 + A}{2y}$$

i.e. the equation of L is $y = m(x - x_1) + y_1$. Now proceed as in the previous case. Since $x_1 = x_2$, we now have $x_3 = m^2 - 2x_1$, and y_3 will follow.

3. If $P_2 = \infty$, then the line through P_1 and ∞ is a vertical line intersecting the curve at $(x_1, -y_1)$. Reflecting this will give $P_3 = (x_1, y_1) = P_1$. Hence $P_1 + \infty = P_1$, and also $\infty + \infty = \infty$.

At this point, we see that ∞ can be thought as an identity element for our additive operation on E . Also the fact that $P_1 + P_2 = P_2 + P_1$ for any points P_1, P_2 on E is obvious. If we need a point Q on E such that $P + Q = \infty$, it can be checked that $Q = (x, -y)$ will work, and therefore the inverse of P exists. A surprising fact is that E also satisfies the associative law:

$$(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3).$$

The proof of associativity is straightforward but consists of several cases. Please refer to Section 2.4 of [42] for the complete proof. Finally we can conclude that the points on E form an additive abelian group, when equipped with the operation of addition defined above, and ∞ as the identity element.

It is clear from the above algebra that if $P_1, P_2 \in E(K)$, then $P_3 \in E(K)$. This means that $E(K)$ is closed under addition. This is also true when $L = \mathbb{Q}(i)$.

2.3 Torsion Points

Definition 2.3.1. *Let E be an elliptic curve and P be a point on E . The order of P , denoted by $\text{ord}(P)$ is the smallest positive integer n , if such an integer exists, such that*

$$nP = \underbrace{P + P + \dots + P}_n = \infty.$$

If n is finite, P is said to be a torsion point on E .

We denote by

$$E[n] = \{P \in E \mid nP = \infty\}$$

the set of all points of order *dividing* n . It is easy to see that ∞ is always in $E[n]$ for any $n \in \mathbb{Z}^+$. If $P, Q \in E[n]$, then so is $-P$ and $P + Q$. Hence $E[n]$ is in fact a subgroup of E .

It is easy to find all points of order 2. Suppose that $P = (x_0, y_0)$ is a point on an elliptic curve $E : y^2 = f(x)$, such that $\text{ord}(P) = 2$, i.e. $2P = \infty$. Then we must have $P = (x_0, y_0) = -P = (x_0, -y_0)$. Hence this means $y_0 = 0$, and points of order 2 are $(x_0, 0)$ when x_0 is a root of $f(x)$. Together with ∞ , there are exactly 4 points of order dividing 2.

For all points $P = (x_0, y_0)$ of order 3, we have $3P = \infty$ or in other words $2P = -P$. By a straightforward calculation, equating the x -coordinate of $2P$ and $-P$ we have

$$\left(\frac{3x_0^2 + A}{2y_0}\right)^2 - 2x_0 = x_0.$$

Using $y^2 = x^3 + Ax + b$ and some manipulation, x_0 must be a root of

$$\psi_3(x) = 3x^4 + 6Ax^2 + 12Bx - A^2.$$

Note that $y_0 \neq 0$, since otherwise $\text{ord}(P) = 2$ as seen before. Due to symmetry about x -axis, each zero of ψ_3 gives two points. It can be easily checked that $\psi_3'(x)$ and $\psi_3(x)$ have no common factor, and thus there are 8 finite points of order 3. Including ∞ , there are 9 points of order dividing 3. In general,

Theorem 2.3.2. *Let E be an elliptic curve over a field K where $\text{char}(K) = 0$. For any positive integer n ,*

$$|E[n]| = n^2.$$

In fact, $E[n]$ is a subgroup isomorphic to $\mathbb{Z}_n \oplus \mathbb{Z}_n$.

Proof: See Section 3.2 of [42] for the proof. ■

CHAPTER 3

Lutz-Nagell Theorem

In the previous section we have seen how to find all points of order 2 or 3 on an elliptic curve E . The problem of finding the torsion subgroup $E[n]$ for $E(\mathbb{Q})$, when $n > 3$, is more difficult. The problem was eventually solved independently by Trygve Nagell [30] in 1935, and Elisabeth Lutz [25] in 1937.

In this chapter, I will outline their proof over \mathbb{Q} and show how to generalise it to find the torsion subgroup for $E(\mathbb{Q}(i))$. The proofs are moderately technical and will be followed by some examples.

3.1 Original Version

Let E be an elliptic curve defined by

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Q}.$$

Suppose that $A = a_1/a_2$ and $B = b_1/b_2$ (with $a_i, b_i \in \mathbb{Z}$ and $a_2, b_2 \neq 0$). Thus,

$$y^2 = x^3 + \frac{a_1}{a_2}x + \frac{b_1}{b_2}.$$

Now let $d = a_2b_2$. Multiplying both sides by d^6 yields

$$(d^3y)^2 = (d^2x)^3 + d^3a_1b_2(d^2x) + d^5a_2b_1.$$

By substitution with $X = d^2x$, $Y = d^3y$, $A' = d^3a_1b_2$, and $B' = d^5a_2b_1$, it turns our equation into $Y^2 = X^3 + A'X + B'$ where $A', B' \in \mathbb{Z}$. In other words, each elliptic curve over \mathbb{Q} can be written with integer coefficients. Thus we will assume that all elliptic curves have integer coefficients.

Theorem 3.1.1. (Lutz-Nagell) *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve with $A, B \in \mathbb{Z}$, and let $P = (x, y) \in E(\mathbb{Q})$. If P has finite order, then*

1. Both x and y are integers, and
2. Either $y = 0$ or $y^2 \mid 4A^3 + 27B^2$.

Remark 3.1.2. The proof of this theorem consists of 2 parts — proving that any point in $E(\mathbb{Q})$ of finite order must have integer coordinates, and some direct

calculations to prove part (2). The first part is however much harder, see Chapter 8 of [42] or Section 20.2 of [17] for the full proof. ■

The Lutz-Nagell Theorem provides necessary conditions for (x, y) being a torsion point in $E(\mathbb{Q})$ and also gives a complete list of possible such points. Consider two examples:

Example 3.1.3. Find all torsion points in $E(\mathbb{Q})$ when E is the elliptic curve $y^2 = x^3 + 4$.

Solution: Suppose that $P = (x, y) \in E(\mathbb{Q})$ has finite order. By Lutz-Nagell Theorem, we know that either $y = 0$, or y^2 divides $4A^3 + 27B^2 = 3^3 \cdot 2^4$, i.e. such torsion points must have y in the following list:

$$0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12.$$

It can be seen that only $y = \pm 2$, gives x to be an integer. Hence the only possibilities here that need to be checked are $(0, \pm 2)$. Since $(0, -2) = -(0, 2)$ and both must have the same order if it is finite, it suffices to check only one point, say, $P = (0, 2)$. Using duplication formula in Section 2.3, we obtain

$$2P = (0, -2) = -(0, 2) = -P$$

which means $3P = \infty$, i.e. P (and also $-P$) has order 3. Therefore the torsion subgroup of $E(\mathbb{Q})$ is

$$\{\infty, (0, 2), (0, -2)\}$$

which is isomorphic to \mathbb{Z}_3 via the obvious map $\infty \mapsto 0$, $(0, 2) \mapsto 1$, $(0, -2) \mapsto 2$. ■

Example 3.1.4. Find all torsion points in $E(\mathbb{Q})$ when E is an elliptic curve $y^2 = x^3 + 2$.

Solution: Here we have $4A^3 + 27B^2 = 3^3 \cdot 2^2$. From the Lutz-Nagell Theorem we know that if $P = (x, y) \in E(\mathbb{Q})$ is a torsion point, y must be one of:

$$0, \pm 1, \pm 2, \pm 3, \pm 6.$$

Now only $y = \pm 1$ give us an integer x , i.e. $x = -1$. Thus $(-1, \pm 1)$ are only possibilities here. Again, it suffices to check only $P = (-1, 1)$. But

$$2P = \left(\frac{17}{4}, \frac{-71}{8} \right),$$

which does not have integer coordinates. Then Lutz-Nagell Theorem implies that $2P$ has infinite order, and so have P and $-P$.

Hence the torsion subgroup of $E(\mathbb{Q})$ is just $\{\infty\}$, the trivial subgroup. ■

3.2 Extended Lutz-Nagell Theorem

Let $P = (x, y) \in E(\mathbb{Q}(i))$ be a torsion point. As mentioned before, the crucial part of the Lutz-Nagell theorem is to show that both $x, y \in \mathbb{Z}$. Roughly speaking, this can be shown as followed: Suppose the contrary, i.e x or y is rational but not integer. Then clearly one of both denominators is not equal to ± 1 , and thus there exists a prime p dividing it. For each prime p , a series of proof will lead to the conclusion that

$$E_p = \{(x, y) \in E(\mathbb{Q}) : p \mid \text{den}(x) \text{ or } p \mid \text{den}(y)\},$$

cannot contain any torsion point. This thus yields a contradiction, since P is a torsion point but $P \in E_p$. Hence both x, y are integers.

In this section, we will focus on how to extend the Lutz-Nagell theorem for torsion points in $E(\mathbb{Q})$, to torsion points in $E(\mathbb{Q}(i))$. Before continuing, first we need the following definitions:

Definition 3.2.1. *A Gaussian integer is a complex number of the form $a + bi$ where $a, b \in \mathbb{Z}$. The set of all Gaussian integers is denoted by $\mathbb{Z}(i)$.*

Definition 3.2.2. *Let $\alpha, \beta \in \mathbb{Z}(i)$. We say that α is divisible by β , denoted by $\beta \mid \alpha$, if $\beta \neq 0$ and there exists $\gamma \in \mathbb{Z}(i)$ such that $\alpha = \beta\gamma$. Otherwise, we say that α is not divisible by β , denoted by $\beta \nmid \alpha$.*

The Gaussian integers behave in many respects similarly to the integers. This includes:

1. For every $\alpha = a + bi \in \mathbb{Z}(i)$, the Gaussian norm of α is defined by

$$N(\alpha) = |\alpha|^2 = a^2 + b^2,$$

which is always a non-negative integer.

2. All units of $\mathbb{Z}(i)$ are $\pm 1, \pm i$.
3. A number $\pi \in \mathbb{Z}(i)$ is said to be a *Gaussian prime* if and only if π is only divisible by $\pm 1, \pm i, \pm \pi$, and $\pm i\pi$.
4. A prime number $p \in \mathbb{Z}$ is also a Gaussian prime if and only if $p \equiv 3 \pmod{4}$.
5. A number $\pi \in \mathbb{Z}(i)$ is a Gaussian prime if and only if
 - $N(\pi)$ is a prime integer, or
 - $\pi = \epsilon p$, for some unit ϵ , and a Gaussian prime p .

Let $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Q}(i)$. Now we write A and B as $A = A_1/A_2$ and $B = B_1/B_2$, where $A_j, B_j \in \mathbb{Z}(i)$ and $A_2, B_2 \neq 0$. Thus,

$$y^2 = x^3 + \frac{A_1}{A_2}x + \frac{B_1}{B_2}.$$

Let $D = A_2B_2$. Multiplying both sides by D^6 gives us

$$(D^3y)^2 = (D^2x)^3 + D^3A_1B_2(D^2x) + D^5A_2B_1.$$

With the substitution $X = D^2x$, $Y = D^3y$, $A' = D^3A_1B_2$, and $B' = D^5A_2B_1$, we have turned our equation into $Y^2 = X^3 + A'X + B'$ with $A', B' \in \mathbb{Z}(i)$. Thus we can assume that our elliptic curve has Gaussian integer coefficients.

For an elliptic curve $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}(i)$, we hope to show the following analogy of Lutz-Nagell Theorem:

Any torsion points (x, y) of $E(\mathbb{Q}(i))$ must have $x, y \in \mathbb{Z}(i)$.

We shall prove this later. Now assume that it is true, we can prove the following:

Proposition 3.2.3. *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve with $A, B \in \mathbb{Z}(i)$, and let $P = (x, y)$ where $x, y \in \mathbb{Z}(i)$. If P is a torsion point of $E(\mathbb{Q}(i))$, then either $y = 0$ or $y^2 \mid 4A^3 + 27B^2$.*

Proof: Clearly $y = 0$ if and only if P has order 2. Suppose now that $y \neq 0$. Then we have $2P = (x_2, y_2) \neq \infty$. Since $2P$ also has finite order, then by assumption $x_2, y_2 \in \mathbb{Z}(i)$. By duplication formula,

$$x_2 = \left(\frac{3x^2 + A}{2y} \right)^2 - 2x.$$

Using $y^2 = x^3 + Ax + B$ and the fact that $y \neq 0$, we have

$$x_2 = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4y^2} := \frac{g(x)}{4y^2}.$$

Note that $x_2 \in \mathbb{Z}(i)$ and so are x, y, A, B . Thus $y^2 \mid g(x)$. A straightforward calculation [42] shows that

$$(3x^2 + 4A)g(x) - (3x^3 - 5Ax - 27B)(x^3 + Ax + B) = 4A^3 + 27B^2.$$

But $y^2 = x^3 + Ax + B$. Therefore $y^2 \mid 4A^3 + 27B^2$. ■

It still remains to show that our previous assumption is valid. We shall achieve this goal by generalising the original proof, and modifying certain concepts as we go along. To make this clearer, we shall break the proof into a number of steps.

3.2.1 Preliminaries

We begin with the fact that any $x \in \mathbb{Q}(i)$ can be always written as g/h , where $g, h \in \mathbb{Z}(i)$, i.e. a quotient of Gaussian integers. Assume that g/h is in the lowest form, i.e. g and h have no common Gaussian factors apart from $1, -1, i, -i$, which are the *units* of $\mathbb{Z}(i)$.

If $x \notin \mathbb{Z}(i)$, then h cannot be a unit. Thus there is a Gaussian prime p that divides h . (A Gaussian prime p is a non-unit Gaussian integer, such that no other Gaussian integers can divide p except the units.)

From this point, we will denote the numerator of x by $\text{num}(x)$, and the denominator of x by $\text{den}(x)$. Now we have

Lemma 3.2.4. *Let $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}(i)$. For any $(x, y) \in E(\mathbb{Q}(i))$, $p \mid \text{den}(x)$ if and only if $p \mid \text{den}(y)$.*

Proof: Write

$$x = \frac{x_1}{p^r x_2}, \quad y = \frac{y_1}{p^s y_2},$$

where $x_i, y_i \in \mathbb{Z}(i)$, $p \nmid x_1 x_2$, and $p \nmid y_1 y_2$. If $p \mid \text{den}(x)$, then $r > 0$. Substituting x, y in the equation for the curve gives

$$\frac{y_1^2}{p^{2s} y_2^2} = \left(\frac{x_1}{p^r x_2} \right)^3 + A \left(\frac{x_1}{p^r x_2} \right) + B = \frac{x_1^3 + A p^{2r} x_1 x_2^2 + B p^{3r} x_2^3}{p^{3r} x_2^3}.$$

Since $p \nmid x_1$, then p does not divide the numerator of the right-hand side, i.e. p^{3r} is the exact power dividing the denominator of the right-hand side. But

$$\text{den}(y^2) = \text{den}(x^3 + Ax + B)$$

so $2s = 3r > 0$, i.e. $s > 0$ which means that $p \mid \text{den}(y)$. The converse is also true by a similar argument.

As $2s = 3r$ is an integer, there exists $q \in \mathbb{Z}$ such that $s = 3q$ and $r = 2q$. ■

As mentioned before, any number in $\mathbb{Q}(i)$ can be written as a quotient of Gaussian integers.

3.2.2 Birational Map

Let $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}(i)$. If $y \neq 0$, we can divide this by y^3 and get

$$\frac{1}{y} = \left(\frac{x}{y} \right)^3 + A \left(\frac{x}{y} \right) \left(\frac{1}{y} \right)^2 + B \left(\frac{1}{y} \right)^3.$$

i.e. $E \setminus \{(x, 0)\}$ is transformed into $E' : s = t^3 + At s^2 + Bs^3$ when $s = 1/y$ and $t = x/y$. Thus we can define a map $\phi : E \setminus \{(x, 0)\} \rightarrow E'$ by

$$(x, y) \mapsto (t, s), \quad \infty \mapsto (0, 0).$$

Note that ϕ is injective. To see this, suppose $(t_1, s_1) = (t_2, s_2)$ when $(t_i, s_i) = \phi(x_i, y_i)$, then

$$s_1 = s_2 \implies \frac{1}{y_1} = \frac{1}{y_2} \implies y_1 = y_2,$$

and

$$t_1 = t_2 \implies \frac{x_1}{y_1} = \frac{x_2}{y_2}.$$

Thus $y_1 = y_2$ and $x_1 = x_2$, so $(x_1, y_1) = (x_2, y_2)$.

The case when $y = 0$ is dealt with by:

Lemma 3.2.5. *Let $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}(i)$. Any torsion point $(x, y) \in E(\mathbb{Q}(i))$ of order 2 has $x \in \mathbb{Z}(i)$ and $y = 0$.*

Proof: If a point $P = (x, y)$ has order 2, we have $2P = \infty$, or in other words, $P = -P$. This gives us $(x, y) = (x, -y)$, i.e. $y = 0$. Thus x is a root of $x^3 + Ax + B = 0$ with $A, B \in \mathbb{Z}(i)$, i.e. a monic polynomial of degree 3 with Gaussian integer coefficients.

Since $P \in E(\mathbb{Q}(i))$ we have $x \in \mathbb{Q}(i)$, which can be written as a fraction of Gaussian integers, says, a/b . Let $x = a/b$ be written in the lowest form, substituting x in the above equation gives

$$0 = \left(\frac{a}{b}\right)^3 + \frac{Aa}{b} + B.$$

Multiplying both sides by b^3 yields

$$0 = a^3 + Aab^2 + Bb^3.$$

Note that $b \neq 0$ so that $b \mid a^3$, and so $b \mid a$. As a/b is in the lowest form, b must be a unit. Therefore $x = a/b \in \mathbb{Z}(i)$. ■

Note we have symmetry about the x -axis in E (i.e. if $(x, y) \in E$, then so is $(x, -y)$). Then in E' we always have *symmetry about zero*, i.e. if $(t, s) \in E'$, then so is $(-t, -s)$.

From this point forward, we write $a \mid q$ as the notation for $a \mid \text{num}(q)$, when $a \neq 0 \in \mathbb{Z}(i)$ and $q \in \mathbb{Q}(i)$ written as a quotient of Gaussian integers. Similarly we write $q \equiv 0 \pmod{a}$ for the same meaning. Note that these extended notations still satisfy properties similar to those for the usual notions.

Definition 3.2.6. *For any $x \neq 0 \in \mathbb{Q}(i)$, the Gaussian p -adic value of x is*

$$g_p(x) = g_p\left(\frac{a}{b}\right) = r, \quad \text{such that } \frac{a}{b} = p^r \frac{a_1}{b_1}$$

where $a, b, a_1, b_1 \in \mathbb{Z}(i)$ and $p \nmid a_1 b_1$.

Hence from Lemma 3.2.4, we have $g_p(x) = -2q$ and $g_p(y) = -3q$ (as we factor p out of the denominators). We now introduce

$$E_r = \{(x, y) \in E(\mathbb{Q}(i)) : g_p(x) \leq -2r, g_p(y) \leq -3r\} \cup \{\infty\}.$$

Clearly $E(\mathbb{Q}(i)) \supseteq E_1 \supseteq E_2 \supseteq \dots$

The set E_r allows us some control on the “size” of the Gaussian rational points on the elliptic curve.

Lemma 3.2.7. *$(x, y) \in E_r$ if and only if $p^{3r} \mid s$. If $p^{3r} \mid s$, then $p^r \mid t$.*

Proof: If $(x, y) \in E_r$, then by definition we have $g_p(y) \leq -3r$, i.e. $y = y_1/(p^{3r}y_2)$ with $p \nmid y_1$. Then

$$s = \frac{1}{y} = \frac{p^{3r}y_2}{y_1},$$

i.e. $p^{3r}|s$. Conversely, suppose $p^{3r}|s$. Then p^{3r} divides $\text{den}(y)$. By Lemma 3.2.4, p^{2r} divides $\text{den}(x)$. Thus $(x, y) \in E_r$.

If $p^{3r}|s$, then we know that $(x, y) \in E_r$ and so the exact power of p dividing $\text{den}(y)$ is p^{3k} , for some $k \geq r$. By Lemma 3.2.4, this implies that p^{2k} is the exact power of p dividing $\text{den}(x)$. Since $t = x/y$, then $p^k|t$. Thus $p^r|t$ since $k \geq r$. ■

3.2.3 Geometrical Interpretation

Suppose we have a line in x - y coordinates, say, $\alpha x + \beta y + \gamma = 0$. Dividing by y gives us $\alpha t + \gamma s + \beta = 0$, which is a line in t - s coordinates. It therefore follows that the definition of addition on E carries across E' . In E' , we can find $P_3 = P_1 + P_2$ by taking a line passing through P_1 and P_2 (if $P_1 = P_2$ then take the tangent line at that point). One can check that this line must intersect the curve at another point $(t'_3, s'_3) \in E'$. Note that E' has symmetry about zero. Hence we let $P_3 = (t_3, s_3) = (-t'_3, -s'_3)$. Similarly for any $(t, s) \in E'$, we now have $-(t, s) = (-t, -s)$.

In particular, the line $\alpha x + \beta y + \gamma = 0$ is tangent to the curve E at a point (x, y) if and only if the line $\alpha t + \gamma s + \beta = 0$ is tangent to E' at the point $(t, s) = (x/y, 1/y)$ [42]. Also if a point $P \in E$ is of finite order, then $\phi(P)$ is also of finite order in E' . (Note: we have ∞ as the identity in E , whilst we have $(0, 0)$ as the identity in E').

Lemma 3.2.8. (Washington [42]) *Any vertical line $t = k$, where k is a constant such that $p|k$, intersects E' in at most one point (t, s) with $p|s$. This line is not tangent at such point of intersection.*

Proof: Suppose the line intersects E' at two points $(t, s_1), (t, s_2) \in E'$, such that $p|s_i$. Write $s_i = ps'_i$ and suppose $p^k|s_1 - s_2$ for some $k \geq 1$. Then

$$p^{k-1}|s'_1 - s'_2 \quad \text{and so} \quad p^{k-1}|(s'_1)^2 - (s'_2)^2.$$

Thus we have $s_1^2 = (ps'_1)^2 \equiv (ps'_2)^2 = s_2^2 \pmod{p^{k+1}}$. Similarly, we have $s_1^3 \equiv s_2^3 \pmod{p^{k+2}}$. Therefore

$$s_1 = k^3 + Aks_1^2 + Bs_1^3 \equiv k^3 + Aks_2^2 + Bs_2^3 \equiv s_2 \pmod{p^{k+1}}.$$

Hence by induction, $s_1 \equiv s_2 \pmod{p}$ for all $n \geq 1$, thus $s_1 = s_2$.

By implicit differentiation, we get the slope of the tangent line as:

$$\frac{ds}{dt} = \frac{3t^2 + As^2}{1 - 2Ast - 3Bs^2}.$$

If the line $t = k$ is tangent to the curve at (t, s) , then $1 - 2Ast - 3Bs^2 = 0$ and hence is divisible by any Gaussian prime. But since $p|s$ and $p|t$, this denominator must be congruent to 1. Hence this line is not tangent to the curve. \blacksquare

For a line $\alpha t + \gamma s + \beta = 0$, if $\gamma = 0$ then this line is of the form in Lemma 3.2.8. Suppose that the line intersects the points $(t_1, s_1) = \phi(P_1)$ and $(t_2, s_2) = \phi(P_2)$, then Lemma 3.2.8 says that both points are identical.

As ϕ is injective, this gives $P_1 = P_2$ in $E \setminus \{(x, 0)\}$ with the tangent line $\alpha x + \beta y + \gamma = 0$ at that points. Hence $\alpha t + \gamma s + \beta = 0$ is the tangent line at (t_1, s_1) , which contradicts Lemma 3.2.8. Hence $\gamma \neq 0$, and then we can divide by γ to get $s = \alpha't + \beta'$ as the equation of the line, with $\alpha', \beta' \in \mathbb{Q}(i)$.

Finally, we need an alternative formula for α :

Lemma 3.2.9. *Suppose the line $s = \alpha t + \beta$ intersects the curve at the points (t_1, s_1) and (t_2, s_2) in E' . Then*

$$\alpha = \frac{t_2^2 + t_1 t_2 + t_1^2 + As_2^2}{1 - A(s_1 + s_2)t_1 - B(s_2^2 + s_1 s_2 + s_1^2)}.$$

Proof: Suppose $t_1 \neq t_2$, then $\alpha = (s_2 - s_1)/(t_2 - t_1)$. Using the fact that $s_i = t_i^3 + At_i s_i^2 + Bs_i^3$, we have

$$\begin{aligned} & (s_2 - s_1) (1 - A(s_1 + s_2)t_1 - B(s_2^2 + s_1 s_2 + s_1^2)) \\ &= (s_2 - s_1) - A(s_2^2 - s_1^2)t_1 - B(s_2^3 - s_1^3) \\ &= (s_2 - As_2^2 t_2 - Bs_2^3) - (s_1 - As_1^2 t_1 - Bs_1^3) + As_2^2(t_2 - t_1) \\ &= t_2^3 - t_1^3 + As_2^2(t_2 - t_1) \\ &= (t_2 - t_1)(t_2^2 + t_1 t_2 + t_1^2 + As_2^2). \end{aligned}$$

which is the same expression in the lemma after rearranging. Now if $t_1 = t_2$, Lemma 8 implies that both points are identical. By implicit differentiation we obtain the slope of tangent line as

$$\frac{ds}{dt} = \frac{3t^2 + As^2}{1 - 2Ast - 3Bs^2},$$

which is the same as our expression when $t = t_1 = t_2$ and $s = s_1 = s_2$. \blacksquare

3.2.4 Obtaining the Contradiction

Lemma 3.2.10. (Adapted from Goldman [17]) *Let $E'_r = \phi(E_r)$ and $E'(\mathbb{Q}(i)) = \phi(E(\mathbb{Q}(i)))$. Then E'_r is a subgroup of $E'(\mathbb{Q}(i))$.*

Proof: Let $(x, y) \in E_r$ and $\phi(x, y) = (t, s)$. Then by Lemma 3.2.7 we have $p^{3r}|s$ and $p^r|t$. By Lemma 3.2.9, it follows that $p^{2r}|\alpha$ (note that p does not divide the denominator). Also since $\beta = s - \alpha t$, this implies $p^{3r}|\beta$.

Now for $P_1, P_2 \in E'_r$ and $P_1 + P_2 = P_3$, let $s = \alpha t + \beta$ be the line passing through P_1 and P_2 . Substituting in the equation for E' yields:

$$\alpha t + \beta = t^3 + At(\alpha t + \beta)^2 + B(\alpha t + \beta)^3$$

i.e.

$$0 = t^3(1 + \alpha^2 A + \alpha^3 B) + t^2(2A\alpha\beta + 3\alpha^2\beta B) + \dots$$

Let $P^* = (t^*, s^*)$ be the new point of intersection. By addition in E' , $P_3 = (t_3, s_3) = -P^*$, and thus

$$t_1 + t_2 - t_3 = t_1 + t_2 + t^* = -\frac{2\alpha\beta A + 3\alpha^2\beta B}{1 + \alpha^2 A + \alpha^3 B} \equiv 0 \pmod{p^{5r}}. \quad (3.1)$$

Since $p^r | t_i$ for $i = 1, 2$, then $p^r | \pm t_3$. Also $s_3 = \alpha t_3 + \beta \equiv 0 \pmod{p^{3r}}$. Hence by Lemma 3.2.7, $\pm P_3 \in E'_r$. Hence E'_r is a subgroup of $E'(\mathbb{Q}(i))$. ■

For $P = (t, s) \in E'_r$, we write $t(P) = t$. Then from (3.1) we have

$$t(P_1) + t(P_2) = t(P_3) \pmod{p^{5r}}.$$

Suppose $P \in E'_1$ has order m . We can assume that $p \nmid n$ (otherwise, we can let $m = np^k$ with $p \nmid n$. Then we let $P' = p^k P$. This will give a point in E_1 of order n where $p \nmid n$). Since an arbitrarily large power of p cannot divide a fixed Gaussian integer, there exists $r > 0$ such that $P \in E_r$ but $P \notin E_{r+1}$.

If $p \nmid m$, then by above equation $t(mP) = m \cdot t(P) \pmod{p^{5r}}$. Since $mP = \infty$ and $t(\infty) = 0$, then $p^{5r} | t(P)$. This is a contradiction since $5r > r$. Hence E'_1 has no point of finite order.

Now if $(x, y) \in E(\mathbb{Q}(i))$ is a torsion point in $E_p(1)$, then $\phi((x, y))$ must have finite order in E'_1 , which contradicts the last result. Hence we have shown that

Proposition 3.2.11. *If $(x, y) \in E(\mathbb{Q}(i))$ is of finite order, then both $x, y \in \mathbb{Z}(i)$.*

Remark 3.2.12. The case when $(x, y) \in E(\mathbb{Q}(i))$ having order two clearly satisfies this proposition. ■

We summarise Proposition 3.2.3 and Proposition 3.2.11 into:

Theorem 3.2.13. (Extended Lutz-Nagell Theorem) *Let $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}(i)$. If a point $(x, y) \in E(\mathbb{Q}(i))$ has finite order, then*

1. Both $x, y \in \mathbb{Z}(i)$, and
2. Either $y = 0$ or $y^2 \mid 4A^3 + 27B^2$.

Here are some examples:

Example 3.2.14. Find the torsion subgroup of $E(\mathbb{Q}(i))$ for the elliptic curve $y^2 = x^3 + 32ix$.

Solution: By Theorem 3.2.13, we know that if $(x, y) \neq \infty \in E(\mathbb{Q}(i))$ is a torsion point, then both x and y are Gaussian integers. Moreover, either $y = 0$ or $y^2 | 4A^3 + 27B^2$, i.e. $|y^2 - 131072i| = -(1+i)^{34}$ in this example. It can be checked that y must be one of the following:

$$0, \quad \epsilon, \quad (1+i)\epsilon, \quad (1+i)^2\epsilon, \quad \dots, \quad (1+i)^{17}\epsilon,$$

where ϵ is $1, -1, i,$ and $-i$ respectively. By solving directly for $x \in \mathbb{Z}(i)$ (with some help from mathematical software, perhaps) we obtain all “possible” torsion points as

$$(4 - 4i, 0), \quad (-4 + 4i, 0), \quad (0, 0).$$

In general we still need to verify the order of such points. However, we do not need to do this here since all points we have just obtained clearly have order two. Hence the torsion subgroup of $E(\mathbb{Q}(i))$ in this case is

$$\{\infty, (4 - 4i, 0), (-4 + 4i, 0), (0, 0)\},$$

which is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. ■

Example 3.2.15. Find the torsion subgroup of $E(\mathbb{Q}(i))$ for the elliptic curve $y^2 = x^3 - 1$.

Solution: Here we have $4A^3 + 27B^2 = 27$. Then for any torsion point $(x, y) \neq \infty \in E(\mathbb{Q}(i))$, the possibilities for y are

$$0, \quad \pm 1, \quad \pm i, \quad \pm 3, \quad \pm 3i.$$

Substituting each y into the equation, we obtain the “possible” torsion points as

$$(1, 0), \quad (0, \pm i), \quad (-2, \pm 3i).$$

Clearly $(1, 0)$ has order 2. Also it can be checked that $(0, \pm i)$ each has order 3, and $(-2, \pm 3i)$ each has order 6. Thus the torsion subgroup of $E(\mathbb{Q}(i))$ in this case is

$$\{\infty, (1, 0), (0, \pm i), (-2, \pm 3i)\},$$

which is indeed a cyclic group of order 6. ■

3.3 Boundedness of Torsion Subgroups

3.3.1 Mazur’s Theorem

Even though the Lutz-Nagell theorem and its extended version can give a complete list of possible torsion points, it still remains to check whether such points indeed have finite order. Nevertheless, finding the order of a certain point may be quite

time-consuming if that point happens to have a very large order. It was until 1977 when Barry Mazur [27] has proven the following deep result:

Theorem 3.3.1. (Mazur) *If E is an elliptic curve over \mathbb{Q} , then the torsion subgroup of $E(\mathbb{Q})$ is isomorphic to one of the following 15 groups:*

$$\begin{aligned} & \mathbb{Z}/n\mathbb{Z}, \quad \text{for } 1 \leq n \leq 12, n \neq 11 \\ & (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2n\mathbb{Z}), \quad \text{for } 1 \leq n \leq 4. \end{aligned}$$

Thus Mazur has shown that the order of any torsion points of $E(\mathbb{Q})$ is at most 12. What will happen if we instead consider the torsion subgroup of $E(F)$, where $F \supset \mathbb{Q}$? One particular result is due to Fujita [16] from Tohoku University in 2005:

Theorem 3.3.2. (Fujita) *Let E be an elliptic curve over \mathbb{Q} . Let $F = \mathbb{Q}(\{\sqrt{m} : m \in \mathbb{Z}\})$. Then the torsion subgroup of $E(F)$ is isomorphic to one of the following 20 groups:*

$$\begin{aligned} & \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \quad \text{for } n = 1, 2, 3, 4, 5, 6, 8, \\ & \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, \quad \text{for } n = 1, 2, 3, 4, \\ & \mathbb{Z}/2n\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \quad \text{for } n = 3, 4 \end{aligned}$$

or $\{\infty\}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z}$. Moreover, there exists an elliptic curve over \mathbb{Q} which realises each group listed above as the torsion subgroup of $E(F)$.

It is clear that the order of any torsion point of $E(\mathbb{Q})$ is unchanged once we consider it as a torsion point of $E(\mathbb{Q}(i))$. For an elliptic curve E , let T_1 be the torsion subgroup of $E(\mathbb{Q})$ and T_2 be the torsion subgroup of $E(\mathbb{Q}(i))$. It is then obvious that $|T_1| \leq |T_2|$. We have seen that Mazur's theorem provides us with the set of all possible torsion subgroups (up to isomorphism) of $E(\mathbb{Q})$.

Usually we can find an elliptic curve over $\mathbb{Q}(i)$ that realises one of the groups listed in Mazur's theorem as its torsion subgroup. Since $|T_1| \leq |T_2|$, then we hope that it might be possible to find a torsion subgroup of $E(\mathbb{Q}(i))$ which does not occur as the one in such list. For example, consider the elliptic curve

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

which can be transformed into the Weierstrass equation as

$$y^2 = x^3 - 12987x - 263466. \tag{3.2}$$

It can be checked that the torsion subgroup of $E(\mathbb{Q})$ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ [14]. Now once we consider the torsion subgroup of $E(\mathbb{Q}(i))$, we obtain the following:

Order	Points
1	∞
2	$(-21, 0), (-102, 0), (123, 0)$
4	$(-57, \pm 540), (-21 - 108i, \pm(1296 + 972i)), (33, \pm 810i),$ $(-237, \pm 3240i), (-21 + 108i, \pm(1296 - 972i)), (303, \pm 4860)$

as the torsion points of $E(\mathbb{Q}(i))$ of (3.2). It can be checked that the torsion subgroup of $E(\mathbb{Q}(i))$ in this case is $\mathbb{Z}_4 \oplus \mathbb{Z}_4$, which does not fit in any form given by Mazur.

3.3.2 Boundedness Conjecture

We have already seen two examples of boundedness of torsion subgroups: Mazur's theorem and Fujita's theorem which say that the order of torsion points of $E(\mathbb{Q})$ and $\mathbb{Q}(\{\sqrt{m} : m \in \mathbb{Z}\})$ is bounded. Yet one remaining question is whether, for any elliptic curve E over an algebraic number field F , the order of any torsion points of $E(F)$ is also bounded.

The answer of this question is known as *Boundedness Conjecture*: There is a constant $B = B(F)$, depending only on the field degree $[F : \mathbb{Q}]$, such that the cardinality of torsion subgroup of every elliptic curve E over F is at most B (See [31]).

Definition 3.3.3. *Let $F \supseteq K$ be a field. The field degree of F , denoted by $[F : K]$, is the dimension of F viewed as a vector space over K .*

For example, $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ via the basis $\{1, i\}$ and $[\mathbb{Q} : \mathbb{Q}]$ is clearly 1. The boundedness conjecture has been significantly strengthened by Kamienny and Mazur [21] in 1992 for all algebraic number fields of degree up to 8, and then up to degree 14 by Abramovich [1] in 1993.

3.3.3 Torsion subgroups of $E(\mathbb{Q}(i))$

In Section 3.3.1 we found that $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ is one possible torsion subgroup of $E(\mathbb{Q}(i))$ which does not occur as a torsion subgroup over \mathbb{Q} . In fact, for each one of 15 groups given by Mazur's theorem, there exists a corresponding elliptic curve over $\mathbb{Q}(i)$ whose torsion subgroup of $E(\mathbb{Q}(i))$ is isomorphic to it. Together with $\mathbb{Z}_4 \oplus \mathbb{Z}_4$, there are at least 16 groups which can be torsion subgroups of $E(\mathbb{Q}(i))$.

Note that $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. The following analogy of Mazur's theorem is due to Kenku and Momose [22] in 1988:

Theorem 3.3.4. (Kenku-Momose) *Let F be a field of degree 2, and E be an elliptic curve over F . Then the torsion subgroup of $E(F)$ is isomorphic to one of*

the following:

$$\begin{aligned} & \mathbb{Z}/n\mathbb{Z} \quad \text{for } 1 \leq n \leq 18, n \neq 17 \\ & (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2n\mathbb{Z}) \quad \text{for } 1 \leq n \leq 6 \\ & (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/3n\mathbb{Z}) \quad \text{for } n = 1, 2 \\ & \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \end{aligned}$$

In addition, the theorem also says that $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ occur as a torsion subgroup of $E(F)$ when $F = \mathbb{Q}(i)$ only. With this generalised result, the number of possible groups which can occur as a torsion subgroup of $E(\mathbb{Q}(i))$ is between 16 and 26. Now if we only consider $E(F)$ when $F = \mathbb{Q}(i)$, it is still unknown whether every group given in Theorem 3.3.4 does in fact occur as a torsion subgroup of $E(\mathbb{Q}(i))$.

CHAPTER 4

Elliptic Curves over Finite Fields

As mentioned earlier, elliptic curves can be defined over any number field, thus we can define such a curve over a finite field. Elliptic curves over finite fields play an important role in many modern applications, particularly cryptography and factorisation techniques. In this chapter, we shall discuss some basic ideas of elliptic curves over finite fields, and then consider particular examples over $\mathbb{Z}_p(i)$.

4.1 Overview

Let \mathbb{F}_q be a finite field of q elements, so that q is a power of a prime number, and let E be an elliptic curve defined over \mathbb{F}_q . Since there are only finitely many pairs $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$, the set of \mathbb{F}_q -points lying on E , denoted by $E(\mathbb{F}_q)$, is finite. First let us consider an example:

Example 4.1.1. Determine $E(\mathbb{F}_5)$ where E is the elliptic curve $y^2 = x^3 + x + 1$ over \mathbb{F}_5 .

Solution: First we make a list of all possible values of x , and then the value of y such that $y^2 \equiv x^3 + x + 1 \pmod{5}$. This gives

x	$x^3 + x + 1 \pmod{5}$	y
0	1	1, 4
1	3	None
2	1	1, 4
3	1	1, 4
4	4	2, 3

Together with the point at infinity ∞ , we obtain $E(\mathbb{F}_5)$ as

$$\{\infty, (1, 1), (1, 4), (2, 1), (2, 4), (3, 1), (3, 4), (4, 2), (4, 3)\}$$

i.e. $|E(\mathbb{F}_5)| = 9$. ■

The usual addition of elliptic curves that we introduced before is still valid over \mathbb{F}_q provided $q \neq 2$ or 3 . To illustrate this, we compute $(3, 1) + (2, 4)$ in the above

example. First let (x, y) be the sum. The “slope” of the “line” joining these two points is

$$m = \frac{4 - 1}{2 - 3} = \frac{3}{-1} \equiv 2 \pmod{5}.$$

Using the addition formula we introduced earlier, we have

$$x = m^2 - 3 - 2 \equiv 4 \pmod{5}, \quad y = -(m(x - 3) + 1) \equiv 2 \pmod{5}.$$

i.e. $(3, 1) + (2, 4) = (4, 2)$. In the above example, a straightforward calculation will show that $(0, 1)$ has order 9, and thus $E(\mathbb{F}_5)$ is a cyclic group of order 9.

In general,

Theorem 4.1.2. *Let E be an elliptic curve over the finite field \mathbb{F}_q . Then $E(\mathbb{F}_q)$ is isomorphic to either*

$$\mathbb{Z}_n \quad \text{or} \quad \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

for some integer $n \geq 1$, or for some integers $n_1, n_2 \geq 1$ such that $n_1 | n_2$.

Proof: The proof uses basic results from the fundamental theorem of abelian groups. See page 91 in [42]. ■

To find what group $E(\mathbb{F}_q)$ is isomorphic to, we first need to know $|E(\mathbb{F}_q)|$. Even when this is known, it is still not easy to classify the group $E(\mathbb{F}_q)$, especially when q is very large.

Suppose E is an elliptic curve over \mathbb{F}_q . Clearly each $x \in \mathbb{F}_q$ yields at most two values of y , so trivially $|E(\mathbb{F}_q)| \leq 2q + 1$, after including the point at infinity. To minimise this bound further, first we recall the generalised Weierstrass equation:

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

If $x \in \mathbb{F}_q$ is substituted, the problem is reduced into solving a quadratic equation $g(y)$. Intuitively, there is roughly a 50% chance that $g(y)$ is solvable over \mathbb{F}_q . Thus we ought to be able to reduce the previous bound to about $q + 1$. The order of $E(\mathbb{F}_q)$ now should be

$$|E(\mathbb{F}_q)| = q + 1 + \text{error term}.$$

The above discussion is, in fact, the intuition behind the following theorem, which was firstly conjectured by E. Artin in his thesis, and eventually proved by Hasse [18] in 1933.

Theorem 4.1.3. (Hasse) *Let E be an elliptic curve over the finite field \mathbb{F}_q . Then the order of $E(\mathbb{F}_q)$ satisfies*

$$\left| q + 1 - |E(\mathbb{F}_q)| \right| \leq 2\sqrt{q}.$$

i.e. $q + 1 - 2\sqrt{q} \leq |E(\mathbb{F}_q)| \leq q + 1 + 2\sqrt{q}$.

Proof: See Section 5.1 of [37], or Section 4.2 of [42]. ■

There are several methods presently known that can quickly determine the order of $E(\mathbb{F}_q)$. Unfortunately none of them is effective once q is very large. An alternative approach is to use the order of certain points in $E(\mathbb{F}_q)$. Since $E(\mathbb{F}_q)$ is a group, then the order of any point in $E(\mathbb{F}_q)$ must divide $|E(\mathbb{F}_q)|$, by Lagrange's theorem. In Hasse's theorem, we know that $|E(\mathbb{F}_q)|$ is bounded in an interval of length $4\sqrt{q}$. If we can find a point in $E(\mathbb{F}_q)$ of order $m > 4\sqrt{q}$, then there will be only one multiple of m lying in that interval, which must be $|E(\mathbb{F}_q)|$. For example,

Example 4.1.4. Let E be the elliptic curve $y^2 = x^3 - 10x + 21$ over \mathbb{F}_{557} . It can be shown later that the point $(2, 3)$ has order 189. Hasse's theorem says that

$$557 + 1 - 2\sqrt{557} \leq |E(\mathbb{F}_{557})| \leq 557 + 1 + 2\sqrt{557},$$

i.e. $511 \leq |E(\mathbb{F}_{557})| \leq 605$. But the only multiple of 189 in this interval is $3(189) = 567$. Hence $|E(\mathbb{F}_{557})| = 567$. ■

4.2 Order of Points

Now the crucial step in determining the order of $E(\mathbb{F}_q)$ is to find a point of order greater than $4\sqrt{q}$. Rather than using successive additions to find the order, a smarter way is the so-called *Baby Step, Giant Step* algorithm [42], which can quickly determine the order of a given point within $4q^{1/4}$ steps (rather than \sqrt{q} steps). Let $P \in E(\mathbb{F}_q)$ be a point.

1. Compute $Q = (q + 1)P$.
2. (Baby Step) Choose an $m \in \mathbb{Z}$ such that $m > q^{1/4}$. Compute and store the points jP , for $j = 0, 1, 2, \dots, m$.
3. (Giant Step) Compute the points

$$Q + k(2mP) \text{ for } k = -m, -m + 1, \dots, m.$$

until there is a match $Q + k(2mP) = \pm jP$ on the stored list in Step 2.

4. Conclude that $(q + 1 + 2mk \mp j)P = \infty$. Let $M = q + 1 + 2mk \mp j$.
5. Find all distinct prime factors p_1, p_2, \dots, p_r of M .
6. Compute $(M/p_i)P$ for $i = 1, 2, \dots, r$. If $(M/p_i)P = \infty$ for some i , replace M with M/p_i and redo Step 5. Otherwise, M is the order of P

For the analysis of this algorithm, please refer to Section 4.3.4 of [42].

Example 4.2.1. Let E be the elliptic curve as in Example 4.1.4 defined over \mathbb{F}_{557} , and let $P = (2, 3)$. Now we want to find the order of P using Baby Step, Giant Step algorithm:

1. Let $Q = (557 + 1)P = (418, 33)$.

2. Choose $m = 5$, which is greater than $557^{1/4}$. The list of jP for $j = 0, 1, \dots, 5$ is then

$$\infty, (2, 3), (58, 164), (44, 294), (56, 339), (132, 364).$$

3. When $k = 1$, we have $Q + k(2mP) = (2, 3)$, which match the point jP when $j = 1$.
4. We now conclude that $(q + 1 + 2mk - j)P = \infty$, i.e. $567P = \infty$.
5. Here $567 = 3^4 \cdot 7$. It can be checked that $(567/3)P = 189P = \infty$. Then we let $M = 567/3 = 189$ be a new candidate for the order of P .
6. Apply the previous step again. Now $189 = 3^3 \cdot 7$ and we compute $(189/3)P$ and $(189/7)P$. Then it can be checked that $(189/3)P = (35, 535) \neq \infty$ and $(189/7)P = (136, 360) \neq \infty$. Hence the process terminates.

The order of P is therefore 189. ■

Remark 4.2.2. Calculation of nP can be done effectively by writing n as the sum of powers of 2. For example, we want to find $Q = 558P$. We write

$$558 = 512 + 32 + 8 + 4 + 2 = 2^9 + 2^5 + 2^3 + 2^2 + 2^1$$

and then we only need to find 2^jP for $j = 1, 2, \dots, 9$, which can be done by successive duplication. After that we add appropriate points to obtain the result. In general, the process finishes in $O(\lfloor \log_2 n \rfloor)$ time. ■

4.3 Elliptic Curves over $\mathbb{Z}_p(i)$

We will now consider elliptic curves over the field $\mathbb{Z}_p(i) = \{a + bi : a, b \in \mathbb{Z}_p\}$, when $p \equiv 3 \pmod{4}$. (The case when $p \equiv 1 \pmod{4}$ is trivial, since $\mathbb{Z}_p(i) \cong \mathbb{Z}_p$.)

Firstly, we consider an example:

Example 4.3.1. Let E be the elliptic curve $y^2 = x^3 + x^2 + x + 1$ over $\mathbb{Z}_3(i)$. By direct calculation, we obtain the following result:

x	$x^3 + x^2 + x + 1$	y	Points
0	1	± 1	$(0, 1), (0, 2)$
i	0	0	$(i, 0)$
$2i$	0	0	$(2i, 0)$
1	1	± 1	$(1, 1), (1, 2)$
$1 + i$	$2i$	$\pm(1 + i)$	$(1 + i, 1 + i), (1 + i, 2 + 2i)$
$1 + 2i$	i	$\pm(2 + i)$	$(1 + 2i, 2 + i), (1 + 2i, 1 + 2i)$
2	0	0	$(2, 0)$
$2 + i$	$2 + i$	—	—
$2 + 2i$	$2 + 2i$	—	—
∞			∞

i.e. $|E(\mathbb{Z}_3(i))| = 12$. We can perform addition between any two points on this curve as usual (under arithmetic modulo p in both real and imaginary parts). For example,

to find $(x_3, y_3) = (0, 1) + (0, 1)$ we proceed as follows using “formal differentiation”. The “slope of the tangent line” to the “curve” at $(0, 1)$ is

$$m = \frac{dy}{dx} = \frac{3x^2 + 2x + 1}{2y} = \frac{1}{2y} = \frac{1}{2} = 2 \pmod{3}.$$

It then follows that

$$\begin{aligned} x_3 &= m^2 - 1 - 2(0) = 0 \pmod{3} \\ y_3 &= -(m(x_3 - 0) + 1) = 2 \pmod{3}, \end{aligned}$$

i.e. $2(0, 1) = (0, 2) = -(0, 1)$. Thus $(0, 1)$ must have order 3. With this method, it can be checked that all points of order 2 are those having $y = 0$. The points $(0, \pm 1)$ have order 3, and the rest, apart from ∞ have order 6. Therefore $E(\mathbb{Z}_3(i))$ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_6$. ■

To find $|E(\mathbb{Z}_p(i))|$, we use Hasse’s theorem to determine the interval in which the order lies. For $p \equiv 1 \pmod{4}$, trivially we have

$$(\sqrt{p} - 1)^2 \leq |E(\mathbb{Z}_p(i))| \leq (\sqrt{p} + 1)^2$$

since $\mathbb{Z}_p(i)$ is indeed \mathbb{Z}_p . In contrast, the order of $E(\mathbb{Z}_p(i))$ when $p \equiv 3 \pmod{4}$ becomes

$$(p - 1)^2 \leq |E(\mathbb{Z}_p(i))| \leq (p + 1)^2,$$

since $\mathbb{Z}_p(i)$ is isomorphic to \mathbb{F}_{p^2} , the field of order p^2 .

In the following section I will illustrate a family of elliptic curves over $\mathbb{Z}_p(i)$ whose order attains the upper bound $(p + 1)^2$. Note that not every elliptic curve over $\mathbb{Z}_p(i)$ has the order equal to the upper bound, as we have seen before in Example 4.3.1.

4.3.1 A Particular Family of Elliptic Curves

In this section, we will look at a particular family of elliptic curves E , given by

$$y^2 = x^3 + kx, \quad \text{where } p \nmid k.$$

The study of determining the order of $E(\mathbb{F}_p)$ has a long history. The original but surprisingly complicated result is due to Gauss:

Theorem 4.3.2. *Let $p \neq 2$ be a prime and $p \nmid k$. Let E be the elliptic curve of the form*

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

1. *If $p \equiv 3 \pmod{4}$, then $|E(\mathbb{F}_p)| = p + 1$.*

2. If $p \equiv 1 \pmod{4}$, write $p = a^2 + b^2$, where $a, b \in \mathbb{Z}$ with b even and $a + b \equiv 1 \pmod{4}$. Then

$$|E(\mathbb{F}_p)| = \begin{cases} p + 1 - 2a & \text{if } k \text{ is a fourth power mod } p \\ p + 1 + 2a & \text{if } k \text{ is a square but not a fourth power mod } p \\ p + 1 \pm 2b & \text{if } k \text{ is not a square mod } p. \end{cases}$$

Proof: The case when $p \equiv 3 \pmod{4}$ is somewhat simpler. If $x = 0$, then clearly $y = 0$ which gives one point $(0, 0)$. Suppose now that $x \neq 0$. If the point (x, y) is on the curve, then $x^3 + kx$ is a square mod p . Since

$$(-x)^3 + k(-x) = -(x^3 + kx)$$

and the fact the -1 is not a square mod p , then $-(x^3 + kx)$ is not a square, and vice versa.

Thus each pair $\{x, -x\}$ where $x \neq 0$ contributes 2 points. Since there are $(p - 1)/2$ such pairs, we get $p - 1$ points. Together with $(0, 0)$ and ∞ , this yields $p + 1$ points.

See Section 4.4 of [42] for the proof when $p \equiv 1 \pmod{4}$, which covers the rest of that section! ■

Now we want to explore this further by allowing the solution $(x, y) \in \mathbb{Z}_p(i) \times \mathbb{Z}_p(i)$, with $p \equiv 3 \pmod{4}$, instead of $\mathbb{Z}_p \times \mathbb{Z}_p$. To illustrate this, consider the elliptic curve $y^2 = x^3 + x$ over $\mathbb{Z}_3(i)$. A direct calculation gives:

x	$x^3 + x$	y	Points	Order
0	0	0	$(0, 0)$	2
i	0	0	$(i, 0)$	2
$2i$	0	0	$(2i, 0)$	2
1	2	$\pm i$	$(1, i), (1, 2i)$	4
$1 + i$	2	$\pm i$	$(1 + i, i), (1 + i, 2i)$	4
$1 + 2i$	2	$\pm i$	$(1 + 2i, i), (1 + 2i, 2i)$	4
2	1	± 1	$(2, 1), (2, 2)$	4
$2 + i$	1	± 1	$(2 + i, 1), (2 + i, 2)$	4
$2 + 2i$	1	± 1	$(2 + 2i, 1), (2 + 2i, 2)$	4
∞			∞	1

and thus $|E(\mathbb{Z}_3(i))| = 16 = (3 + 1)^2$. Experimentation with Maple suggested the following conjecture:

Conjecture 4.3.3. *The order of $E(\mathbb{Z}_p(i))$ where E is the elliptic curve*

$$y^2 = x^3 + kx, \quad k \in \mathbb{Z}_p \setminus \{0\}$$

defined over $\mathbb{Z}_p(i)$ with $p \equiv 3 \pmod{4}$, is $(p + 1)^2$.

To prove this conjecture, one may use different approaches to count the number of points on $E(\mathbb{Z}_p(i))$. The first method, as initially suggested by Dr Yager from Macquarie University, is to note the following:

Let E be an elliptic curve of the form given in Conjecture 4.3.3. If $k \in \mathbb{Z}$, then k has a square root in $\mathbb{Z}_p(i)$, when $p \equiv 3 \pmod{4}$. To prove this, note that either k or $-k$ is a square mod p . Suppose k is not a square mod p . Then $-k = \alpha^2$, i.e. $k = (i\alpha)^2$. So k is a square in $\mathbb{Z}_p(i)$. Hence the square roots of k are either α or $i\alpha$, $\alpha \in \mathbb{Z}$.

By writing $x = bX$ and $k = b^2$, we get

$$y^2 = (bX)^3 + k(bX) = b^3(X^3 + X).$$

This implies that any elliptic curve of the form above is isomorphic to the curve $y^2 = x^3 + x$ provided that b^3 is a square in $\mathbb{Z}_p(i)$. If $b \in \mathbb{Z}$, then by the above comments, it is always a square in $\mathbb{Z}_p(i)$ (and so is b^3). Otherwise $b = ci$ for some $c \in \mathbb{Z}$. As before, c is a square in $\mathbb{Z}_p(i)$. Then it suffices to check that i is also a square in $\mathbb{Z}_p(i)$.

If we write $i = (u + iv)^2$ where $u, v \in \mathbb{Z}_p$, then we have

$$u^2 - v^2 \equiv 0 \pmod{p} \quad \text{and} \quad 2uv \equiv 1 \pmod{p}.$$

The first equation implies that either $u \equiv v \pmod{p}$ or $u \equiv -v \pmod{p}$. Thus by the second part, we have either $2u^2 \equiv 1 \pmod{p}$ or $-2u^2 \equiv 1 \pmod{p}$. Since p is prime, then 2 has an inverse $t \in \mathbb{Z}_p \setminus \{0\}$. Hence either $u^2 \equiv t \pmod{p}$ or $u^2 \equiv -t \pmod{p}$, which is always true when $p \equiv 3 \pmod{4}$.

Thus Conjecture 4.3.3 will be proved if the number of points on the curve $y^2 = x^3 + x$ over $\mathbb{Z}_p(i)$ is $(p+1)^2$. This can be shown by computing the zeta function for the curve over the field \mathbb{Z}_{p^n} , and extract the coefficient for $n = 2$. This is beyond the scope of the thesis.

An alternative approach, which we shall consider in more detail here, is to use the following generalised result due to Washington [42]. This approach was suggested by P. Brown.

Theorem 4.3.4. *Let $|E(\mathbb{F}_p)| = p + 1 - a$. Write $X^2 - aX + p = (X - \alpha)(X - \beta)$. Then*

$$|E(\mathbb{F}_{p^n})| = p^n + 1 - (\alpha^n + \beta^n)$$

for all $n \geq 1$.

We shall prove this later in Section 4.3.3, but we will apply it here to prove Conjecture 4.3.3. Suppose E is the elliptic curve as in the conjecture. Here $p \equiv 3 \pmod{4}$, so that $|E(\mathbb{F}_p)| = p + 1$ by Theorem 4.3.2. Thus in Theorem 4.3.4, $a = 0$ and then

$$X^2 - aX + p = X^2 + p = (X - i\sqrt{p})(X + i\sqrt{p}),$$

i.e. $\alpha = i\sqrt{p}$ and $\beta = -i\sqrt{p}$. Since $\mathbb{Z}_p(i) \cong \mathbb{F}_{p^2}$, by letting $n = 2$ we have

$$|E(\mathbb{Z}_p(i))| = |E(\mathbb{F}_{p^2})| = p^2 + 1 - (\alpha^2 + \beta^2) = p^2 + 1 + 2p = (p + 1)^2$$

as desired.

4.3.2 Supersingular Curves

We now complete the analysis by finding the structure of the group. Recall that $E[n]$ is the set of points (whose coordinates are allowed to be in the algebraic closure) having the order dividing n .

Definition 4.3.5. Let E be an elliptic curve over a field \mathbb{F}_q , where $q = p^k$ and p is prime. E is said to be supersingular if $E[p] = \{\infty\}$.

Lemma 4.3.6. Let α, β be defined as in Theorem 4.3.4. Then $\alpha^n + \beta^n$ is always an integer, for any $n \geq 0$.

Proof: The cases when $n = 0, 1$ are clearly true. Suppose the result holds when $n = k - 1$ and $n = k$, for some $k \geq 1$. Since $\alpha^2 - a\alpha + p = 0$ and $\beta^2 - a\beta + p = 0$, this implies that

$$\alpha^{k+1} + \beta^{k+1} = \alpha^2\alpha^{k-1} + \beta^2\beta^{k-1} = a(\alpha^k + \beta^k) - p(\alpha^{k-1} + \beta^{k-1})$$

i.e. the case when $n = k + 1$ is also true. Thus the result follows by induction. ■

Theorem 4.3.7. If $|E(\mathbb{F}_p)| \equiv 1 \pmod{p}$, then E is supersingular.

Proof: First we write $|E(\mathbb{F}_p)| = p + 1 - a$. If $|E(\mathbb{F}_p)| \equiv 1 \pmod{p}$, then $a \equiv 0 \pmod{p}$. Let α, β be defined as in Theorem 4.3.4. By Lemma 4.3.6,

$$\alpha^{k+1} + \beta^{k+1} = a(\alpha^k + \beta^k) - p(\alpha^{k-1} + \beta^{k-1})$$

for $k \geq 1$. Since $a \equiv 0 \pmod{p}$, it follows that $\alpha^n + \beta^n \equiv 0 \pmod{p}$ for every $n \geq 1$. Hence by Theorem 4.3.4, we have

$$|E(\mathbb{F}_{p^n})| = p^n + 1 - (\alpha^n + \beta^n) \equiv 1 \pmod{p},$$

for every $n \geq 1$. This implies that there is no point of order p in $E(\mathbb{F}_{p^n})$, for any $n \geq 1$. Note that the algebraic closure of \mathbb{F}_p is the field $\overline{\mathbb{F}}_p = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$. Thus $E[p] = \{\infty\}$, and so E is supersingular. ■

By Theorem 4.3.2, any elliptic curve of the form $y^2 = x^3 + kx$, $p \nmid k$ over \mathbb{Z}_p has its group of points of order $p + 1$ when $p \equiv 3 \pmod{4}$. Therefore $E(\mathbb{Z}_p)$ is supersingular by Theorem 4.3.7. We can now classify the group structure of $E(\mathbb{Z}_p(i))$, using the following theorem due to Wittmann [44] in 2001:

Theorem 4.3.8. (Wittmann) *Let E be a supersingular elliptic curve over \mathbb{F}_p . Then*

$$E(\mathbb{F}_{p^{2k}}) \simeq \mathbb{Z}/((-p)^k - 1)\mathbb{Z} \oplus \mathbb{Z}/((-p)^k - 1)\mathbb{Z}.$$

Since $\mathbb{Z}_p(i) \simeq \mathbb{F}_{p^2}$, substituting $k = 1$ into Theorem 4.3.8 above, we obtain

$$E(\mathbb{Z}_p(i)) \simeq E(\mathbb{F}_{p^2}) \simeq \mathbb{Z}/(p+1)\mathbb{Z} \oplus \mathbb{Z}/(p+1)\mathbb{Z}.$$

This agrees with our earlier example.

4.3.3 The Frobenius Endomorphism

The aim of this section is to introduce the concept of the Frobenius endomorphism, which will provide enough information to prove Theorem 4.3.4.

Definition 4.3.9. *Let \mathbb{F}_p be a finite field with algebraic closure $\overline{\mathbb{F}_p}$. The Frobenius map ϕ_p for \mathbb{F}_p is defined by:*

$$\begin{aligned} \phi_p : \overline{\mathbb{F}_p} &\longrightarrow \overline{\mathbb{F}_p} \\ x &\longmapsto x^p \end{aligned}$$

and then ϕ_p acts on the coordinates of points in $E(\overline{\mathbb{F}_p})$ by

$$\phi_p(x, y) = (\phi_p(x), \phi_p(y)) = (x^p, y^p), \quad \phi_p(\infty) = \infty.$$

The map ϕ_p is an example of an *endomorphism*. By this, we mean a homomorphism which is given by rational functions. Clearly ϕ_p is given by rational functions (in fact, by polynomials of degree p). It remains to confirm that ϕ_p is a homomorphism.

Lemma 4.3.10. *Let E be an elliptic curve over \mathbb{F}_p where $p \neq 2, 3$. Then ϕ_p is a homomorphism of E .*

Proof: Suppose we have two points $(x_1, y_1), (x_2, y_2) \in E(\overline{\mathbb{F}_p})$, and let (x_3, y_3) be the sum of these two points. Then we need to show that

$$\phi_p(x_3, y_3) = \phi_p((x_1, y_1) + (x_2, y_2)) = \phi_p(x_1, y_1) + \phi_p(x_2, y_2).$$

Assume that E is in the Weierstrass form. The first case to consider is when $x_1 \neq x_2$. We obtain the sum (x_3, y_3) by the usual formula:

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{where } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

Note that $(a + b)^p = a^p + b^p$ in \mathbb{F}_p . By raising x_3, y_3 to the p -th power:

$$x_3^p = (m')^2 - x_1^p - x_2^p, \quad y_3^p = m'(x_1^p - x_2^p) - y_1^p, \quad \text{where } m' = m^p = \frac{y_2^p - y_1^p}{x_2^p - x_1^p}.$$

i.e. $(x_3^p, y_3^p) = (x_1^p, y_1^p) + (x_2^p, y_2^p)$. In other words, we have just proved that

$$\phi_p(x_3, y_3) = \phi_p(x_1, y_1) + \phi_p(x_2, y_2).$$

The case when $x_1 = x_2$ or one of these points is ∞ can be checked similarly. \blacksquare

Now let us return to Theorem 4.3.4. First, let α, β be as in the theorem. Then by Lemma 4.3.6, $\alpha^n + \beta^n \in \mathbb{Z}$ for any $n \geq 0$. Now we let

$$f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + p^n.$$

Note that all coefficients are integers. Clearly $f(X)$ is divisible by $(X - \alpha)(X - \beta) = X^2 - aX + p$, i.e.

$$f(X) = (X^n - \alpha^n)(X^n - \beta^n) = Q(X)(X^2 - aX + p) \quad (4.1)$$

for some polynomial $Q(X)$ of integer coefficients. The next point is to note that

Theorem 4.3.11. *Let $a = p + 1 - |E(\mathbb{F}_p)|$ and ϕ_p be the Frobenius map. Then $\phi_p^2 - k\phi_p + p = 0$ if and only if $k = a$.*

Proof: The proof aims to show that the kernel of the endomorphism $\phi_p^2 - a\phi_p + p$ is infinite, which will imply that the endomorphism is indeed zero. To prove the uniqueness of a , let $a' \in \mathbb{Z}$ be another integer satisfying $\phi_p^2 - a'\phi_p + p = 0$. Then

$$0 = (\phi_p^2 - a\phi_p + p) - (\phi_p^2 - a'\phi_p + p) = (a' - a)\phi_p.$$

Using the fact that ϕ_p is surjective, this implies $a' = a$.

The entire proof is long and technical, and will be omitted. Please refer to Theorem 4.10 of [42] for more detail. \blacksquare

We will now finish off the proof of Theorem 4.3.4. From (4.1), we have

$$(\phi_p^n)^2 - (\alpha^n + \beta^n)\phi_p^n + p^n = f(\phi_p) = Q(\phi_p)(\phi_p^2 - a\phi_p + p) = 0$$

by Theorem 4.3.11. Note that $\phi_p^n = \phi_{p^n}$. Then by Theorem 4.3.11, there is a unique integer k such that

$$(\phi_{p^n})^2 - k\phi_{p^n} + p^n = 0,$$

and in fact, $k = p^n + 1 - |E(\mathbb{F}_{p^n})|$. Therefore $|E(\mathbb{F}_{p^n})| = p^n + 1 - (\alpha^n + \beta^n)$. This completes the proof of Theorem 4.3.4. \blacksquare

CHAPTER 5

Mordell-Weil Theorem

We already know that $E(\mathbb{Q})$, the set of all rational points on an elliptic curve E , is an abelian group under addition, but what else do we know about it? One of many interesting questions is whether $E(\mathbb{Q})$ is finitely generated. The answer “yes” to this question has a long history, from Poincaré’s hypothesis in 1901 until it becomes a theorem proved by Mordell in 1922. It was then significantly generalised by Weil in 1928, when the theorem was extended from $E(\mathbb{Q})$ to any algebraic variety, i.e. a higher-dimensional analog of elliptic curves.

This chapter aims to follow the classical proof, and modify it to the case $E(\mathbb{Q}(i))$. Finally, we hope to briefly discuss how Weil generalised the original theorem. The proof shown here is based on a modified version by Weil in 1930 [43], and is somewhat technical.

5.1 Original Theorem

First we state the original version of the theorem.

Theorem 5.1.1. (Mordell-Weil) *Let E be an elliptic curve over \mathbb{Q} . The group $E(\mathbb{Q})$ is finitely generated.*

The theorem was initially proved by Mordell using rather different approach from what we will consider here. The more refined version was firstly introduced by Weil in his thesis, where the proof consists of proving the following two important lemmas:

- $E(\mathbb{Q})/2E(\mathbb{Q}) = \{R_i + 2E(\mathbb{Q}) : R_i \in E(\mathbb{Q})\}$ is finite, where R_i is the representative of each coset of $E(\mathbb{Q})$ relative to $2E(\mathbb{Q})$. The result is normally referred as the *weak Mordell-Weil theorem*. This is the hardest part of the proof, so we will postpone this for the time being.
- “Infinite descent”. This idea was mainly motivated by *method of descent* introduced by Fermat.

Now let us return to the proof of Theorem 5.1.1. Assume that the first lemma is true. It then follows that $E(\mathbb{Q})$ is a finite disjoint union of those cosets. Thus any point $P \in E(\mathbb{Q})$ must be in some coset, say,

$$P = R_{n_1} + 2P_1$$

for some $n_1 \in \mathbb{Z}$, and $P_1 \in E(\mathbb{Q})$. Then $P_1 \in E(\mathbb{Q})$ implies that $P_1 = R_{n_2} + 2P_2$ for some $n_2 \in \mathbb{Z}$ and $P_2 \in E(\mathbb{Q})$. Thus we can repeat the process and get

$$\begin{aligned} P &= R_{n_1} + 2P_1 \\ &= R_{n_1} + 2R_{n_2} + 4P_2 \\ &= R_{n_1} + 2R_{n_2} + 4R_{n_3} + 8P_3 \\ &\vdots \\ &= \sum_{j=1}^{\ell} 2^{j-1}R_{n_j} + 2^{\ell}P_{\ell} \end{aligned}$$

after ℓ iterations. If we can show that the process terminates, i.e. if there is a finite set S such that for every $P \in E(\mathbb{Q})$, $P_{\ell} \in S$ for some ℓ , then the set $\{R_{n_j} : 1 \leq j \leq \ell\} \cup S$ generates P , and we are done. This is known as the *method of descent*. The first problem is how to construct such an S , which requires the following concept:

5.2 Height Function

We wish to define a function $H : \mathbb{Q} \rightarrow \mathbb{Z}^+$ in such a way that it measures how “complex” the given rational number is. A simple definition of H is

$$H(x) = \begin{cases} \max\{|a|, |b|\} & \text{if } x \neq 0 \text{ and } x = a/b, \gcd(a, b) = 1, \\ 1 & \text{if } x = 0. \end{cases}$$

Such a function H is called the *height function*. For example, 1 and 997/998 are roughly the same value. But $H(1) = 1$ whereas $H(997/998) = 998$, and the definition of H intuitively makes sense. With this definition, we can extend H to measure the complexity of a rational point $P = (x, y) \in E(\mathbb{Q})$ by

$$H(P) = H((x, y)) = \begin{cases} H(x) & \text{if } P \neq \infty, \\ 1 & \text{otherwise.} \end{cases}$$

This extended notion is not so surprising. Clearly y is determined once we know x , and thus it suffices to only “measure” x as a “height” of the point.

Some remarkable properties of H that enables us to construct S are as follows: (these lemmas are adapted from the version given by Goldman [17]):

Lemma 5.2.1. *For any constant $K > 0$, the set $\{P \in E(\mathbb{Q}) : H(P) < K\}$ is finite.*

Lemma 5.2.2. *Let $R \in E(\mathbb{Q})$ be a fixed point. Then there is a constant $c \geq 1$, depending only on R and E , such that*

$$H(P + R) \leq c(H(P))^2.$$

for all $P \in E(\mathbb{Q})$, provided that $P \neq \infty, \pm R$.

Lemma 5.2.3. *There is a constant $d \geq 1$, depending only on E , such that*

$$(H(P))^4 \leq dH(2P).$$

for all $P \in E(\mathbb{Q})$.

Proof of Infinite Descent:

We now show how to get the Mordell-Weil theorem using the method of descent. Lemma 5.2.1 is obviously true, and we shall prove Lemma 5.2.2 and 5.2.3 later. Let R_1, R_2, \dots, R_n be the representatives of each of the coset in $E(\mathbb{Q})/2E(\mathbb{Q})$. Let c_j be the constant in Lemma 5.2.2 that depends only on $-R_j$ and E . Let d be the constant as given by Lemma 5.2.3 (depending on E only). Now we let

$$\rho = d \cdot \max_{1 \leq j \leq n} c_j,$$

and we define

$$S = \{P \in E(\mathbb{Q}) : H(P) \leq \rho^2\}.$$

Then S is finite by Lemma 5.2.1. We will show that S is the desired set, i.e. $P_\ell \in S$ when P_ℓ is as defined above. Suppose the contrary, i.e. there exists $P \in E(\mathbb{Q})$ such that $P_j \notin S$ for all $j \geq 1$. Note that $P_{j-1} = R_{n_j} + 2P_j$ for $j \geq 1$ and $P = P_0$. Then we have

$$\begin{aligned} (H(P_j))^4 &\leq dH(2P_j) \\ &= dH(P_{j-1} - R_{n_j}) \\ &\leq dc_{n_j} (H(P_{j-1}))^2 \\ &\leq \rho (H(P_{j-1}))^2, \end{aligned}$$

and thus $H(P_j) \leq \rho^{1/4} \sqrt{H(P_{j-1})} \leq \rho \sqrt{H(P_{j-1})}$. But $P_{j-1} \notin S$, i.e. $H(P_{j-1}) > \rho^2$. Hence we have

$$H(P_j) \leq \rho \sqrt{H(P_{j-1})} < H(P_{j-1}),$$

in other words, $H(P_j) \leq H(P_{j-1}) - 1$ since H is a positive integer. It follows that

$$H(P_\ell) \leq H(P_{\ell-1}) - 1 \leq H(P_{\ell-2}) - 2 \leq \dots \leq H(P_1) - (\ell - 1) \leq H(P) - \ell.$$

Choose $\ell > H(P)$ will make $H(P_\ell)$ negative, which contradicts the positiveness of H . This completes the proof of infinite descent. ■

5.2.1 Modification of Height Function

We are now interested in extending the Mordell-Weil theorem in order to show that $E(\mathbb{Q}(i))$ is also finitely generated. A possible approach to this goal is to modify the notion of the height function, generalise the weak Mordell-Weil theorem to handle

$\mathbb{Q}(i)$, and follow the same track! First, we will establish the new version of height function, which is still compatible with the original definition, and which (hopefully) also satisfies Lemma 5.2.1, 5.2.2, and 5.2.3.

Let E be an elliptic curve over $\mathbb{Q}(i)$. Without loss of generality, we may assume that E is in the Weierstrass form $y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Z}(i)$. We define the *extended height function* $H' : \mathbb{Z}(i) \rightarrow \mathbb{Z}^+$ by

$$H'(z) = \max\{|z_1|^2, |z_2|^2\}$$

for $z \neq 0$ and $z = z_1/z_2$, a quotient of co-prime Gaussian integers. For $z = 0$, let $H'(z) = 1$. Again, we can define the extended height function for a point $P = (x, y) \in E(\mathbb{Q}(i))$ in the similar way by

$$H'(P) = \begin{cases} H(x) & \text{for } P \neq \infty, \\ 1 & \text{otherwise.} \end{cases}$$

Note that $H'(x) = (H(x))^2$ if x is just a rational number. We will now show that the definition of H' does satisfy Lemma 5.2.1, 5.2.2, and 5.2.3 (after replacing H by H'). The following proofs will be done by using H' rather than H . The proof of Lemma 5.2.2 and 5.2.3 can be deduced easily since the general argument is essentially unchanged when H is replaced by H' .

Lemma 5.2.4. (c.f. Lemma 5.2.1) *For any constant $K > 0$, the set $\{P \in E(\mathbb{Q}(i)) : H'(P) < K\}$ is finite.*

Proof: Let $P = (x, y) \in E(\mathbb{Q}(i))$. By definition of H' , we have $H'(P) = H'(x)$. Since each $x \in \mathbb{Q}(i)$ contributes at most 2 values of y , it then remains to show that the number of such $x \in \mathbb{Q}(i)$, with $H'(x) < K$, is finite.

Recall the definition of H' . The problem is now equivalent to counting the number of integer points in a “4-dimensional hypercube of side \sqrt{K} ”, which is clearly finite. This completes the proof. ■

Before we prove the analog of Lemma 5.2.2, we need the following results:

Lemma 5.2.5. *For $P = (x, y) \in E(\mathbb{Q}(i))$, there exist $x_1, y_1, z \in \mathbb{Z}(i)$, where x_1, y_1 are relatively prime to z as Gaussian integers, such that*

$$x = \frac{x_1}{z^2}, \quad y = \frac{y_1}{z^3}.$$

Proof: First we write $x = x_1/z_1$ and $y = y_1/z_2$ as a quotient of Gaussian integers in lowest terms, that is, $\gcd(x_1, z_1)$ and $\gcd(y_1, z_2)$ are units. Substituting x, y into the equation for E gives:

$$\left(\frac{y_1}{z_2}\right)^2 = \left(\frac{x_1}{z_1}\right)^3 + \frac{Ax_1}{z_1} + B,$$

i.e.

$$y_1^2 z_1^3 = x_1^3 z_2^2 + Ax_1 z_1^2 z_2^2 + Bz_1^3 z_2^2.$$

Note that all numbers here are Gaussian integers. Then first we have $z_2^2 | z_1^3$, and also $z_1^2 | z_2^2$. The last result then implies that $z_1^3 | x_1^3 z_2^2$, and so $z_1^3 | z_2^2$. Hence we have $z_1^3 = z_2^2$.

Let $z = z_2/z_1 \in \mathbb{Z}(i)$. Then

$$z^2 = \frac{z_2^2}{z_1^2} = z_1, \quad z^3 = \frac{z_2^3}{z_1^3} = z_2,$$

and this proves the lemma. ■

Lemma 5.2.6. *There exists a constant $K \geq 1$, depending only on E , such that*

$$|y| \leq K (H'(P))^{3/4}$$

for every point $P = (x, y) \in E(\mathbb{Q}(i))$.

Proof: We can write $P = (x_1/z^2, y_1/z^3)$ as in Lemma 5.2.5. Substituting into the equation for E , and multiplying both sides by z^6 yields

$$y_1^2 = x_1^3 + Ax_1 z^4 + Bz^6.$$

Note that $H'(P) = H'(x) = \max\{|x_1|^2, |z^2|^2\}$. By the triangle inequality, we have

$$\begin{aligned} |y_1|^2 &\leq |x_1|^{2 \cdot 3/2} + |A| \cdot |x_1|^{2 \cdot 1/2} |z^2|^2 + |B| \cdot |z^2|^{2 \cdot 3/2} \\ &\leq (H'(P))^{3/2} (1 + |A| + |B|), \end{aligned}$$

i.e

$$|y| \leq \frac{(H'(P))^{3/4} \sqrt{1 + |A| + |B|}}{|z^3|} \leq (H'(P))^{3/4} \sqrt{1 + |A| + |B|} := K (H'(P))^{3/4}$$

since $z \neq 0 \in \mathbb{Z}(i)$ and so $|z| \geq 1$. The fact that $K \geq 1$ and depends only on E is now apparent. ■

Suppose we have two points $P = (x_1, y_1), R = (x_2, y_2) \in E(\mathbb{Q}(i))$, such that neither is ∞ , and $P \neq \pm R$. Let $x(P + R)$ denote the first component of $P + R$. From the addition formula, we have

$$x(P + R) = \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - (x_1 + x_2).$$

Using the fact that $y_1^2 = x_1^3 + Ax_1 + B$ and $y_2^2 = x_2^3 + Ax_2 + B$, we can rewrite this as

$$x(P + R) = \frac{(A + x_1 x_2)(x_1 + x_2) + 2B - 2y_1 y_2}{(x_2 - x_1)^2} \tag{5.1}$$

Now we are ready to state:

Lemma 5.2.7. (c.f. Lemma 5.2.2) *Let $R = (x_0, y_0) \in E(\mathbb{Q}(i))$ be a fixed point. There exists a constant $c \geq 1$, depending only on R and E , such that*

$$H'(P + R) \leq c(H'(P))^2$$

for every $P \in E(\mathbb{Q}(i))$, where $P \neq \infty, \pm R$.

Proof: The result is trivial if $R = \infty$. Let $P = (x, y) = (x_1/z^2, y_1/z^3)$, with $x_1, y_1, z \in \mathbb{Z}(i)$ as before. Then from (5.1), we have

$$\begin{aligned} x(P + R) &= \frac{\left(A + \frac{x_0 x_1}{z^2}\right) \left(x_0 + \frac{x_1}{z^2}\right) + 2B - \frac{2y_0 y_1}{z^3}}{\left(x_0 - \frac{x_1}{z^2}\right)^2} \\ &:= \frac{\alpha_1 z^4 + \alpha_2 x_1 z^2 + \alpha_3 x_1^2 + \alpha_4 y_1 z}{\alpha_5 z^4 + \alpha_6 x_1 z^2 + x_1^2} \end{aligned}$$

after multiplying both numerator and denominator by z^4 . Here $\alpha_1, \alpha_2, \dots, \alpha_6$ are some constants depending only on R (in terms of x_0, y_0), and E (in terms of A, B). Note that

$$|x_1| \leq \sqrt{H'(P)}, \quad |z^2|^2 \leq H'(P), \quad |y_1| \leq K(H'(P))^{3/4}$$

by the definition of $H'(P)$ and Lemma 5.2.6. It then follows that

$$|\alpha_1 z^4 + \alpha_2 x_1 z^2 + \alpha_3 x_1^2 + \alpha_4 y_1 z| \leq (|\alpha_1| + |\alpha_2| + |\alpha_3| + K|\alpha_4|) H'(P),$$

and

$$|\alpha_5 z^4 + \alpha_6 x_1 z^2 + x_1^2| \leq (|\alpha_5| + |\alpha_6| + 1) H'(P).$$

Therefore we can conclude that

$$H'(P + R) = H'(x(P + R)) \leq c(H'(P))^2$$

where $c = \max\{(|\alpha_1| + |\alpha_2| + |\alpha_3| + K|\alpha_4|)^2, (|\alpha_5| + |\alpha_6| + 1)^2\}$. Clearly $c \geq 1$ and depends only on R and E . ■

5.2.2 Further Duplication Formula

In order to prove the extended version of Lemma 5.2.3, we first need another formula for doubling a point. Let

$$y^2 = f(x) = x^3 + Ax + B \quad \text{with } A, B \in \mathbb{Z}(i)$$

be an elliptic curve over $\mathbb{Q}(i)$. Also we let r_1, r_2, r_3 be the roots of $f(x)$, with a further assumption that $r_j \in \mathbb{Z}(i)$ for all $j = 1, 2, 3$. We shall write r for any one of these roots.

Let $P = (x_1, y_1) \in E(\mathbb{Q}(i))$, such that $P \neq \infty, (r, 0)$. Since the tangent line to the curve at P intersects the curve at the point $-2P$, then the points satisfying

$$[m(x - x_1) + y_1]^2 = x^3 + Ax + B, \quad \text{where } m = \frac{3x_1^2 + A}{2y_1}, \quad (5.2)$$

are P and $\pm 2P$. For a fixed root $r = r_j$, we write

$$X_1 = x_1 - r \quad \text{and} \quad X = x - r.$$

Hence (5.2) becomes

$$[m(X - X_1) + y_1]^2 = [m(x - x_1) + y_1]^2 = x^3 + Ax + B = f(X + r).$$

But we can rewrite this as

$$\begin{aligned} f(X + r) &= x^3 + Ax + B \\ &= (x - r)^3 + 3x^2r + x(A - 3r^2) + r^3 + B \\ &= (x - r)^3 + 3r(x - r)^2 + x(A + 3r^2) - 2r^3 + B \\ &= (x - r)^3 + 3r(x - r)^2 + (A + 3r^2)(x - r) + (r^3 + Ar + B) \\ &= X^3 + 3rX^2 + (A + 3r^2)X \quad (\text{since } f(r) = 0). \end{aligned}$$

This implies that $X = 0$ is a root of $f(X + r)$.

Since x_1 and $x(2P)$ satisfy (5.2), we have $x_1 - r$ and $x(2P) - r$ as the roots of $f(X + r)$. The product (with multiplicity 2, for $x_1 - r$) of these roots must be the constant term of above equation, i.e.

$$\begin{aligned} (x(2P) - r)(x_1 - r)^2 &= (y_1 - mX_1)^2 \\ &= \left[y_1 - \frac{(3x_1^2 + A)(x_1 - r)}{2y_1} \right]^2 \\ &= \left[\frac{2y_1^2 - (x_1 - r)(3x_1^2 + A)}{2y_1} \right]^2. \end{aligned} \quad (5.3)$$

Since $f(r) = 0$, we can divide $x^3 + Ax + B$ by $x - r$, using $r^3 + Ar + B = 0$ to obtain

$$y^2 = x^3 + AX + B = (x - r)(x^2 + rx + A + r^2).$$

Thus the numerator of (5.3) becomes

$$2y_1^2 - (x_1 - r)(3x_1^2 + A) = (x_1 - r)(-x_1^2 + 2rx_1 + A + 2r^2).$$

After simplifying the expression, we eventually obtain

$$x(2P) - r = \left[\frac{-x_1^2 + 2rx_1 + A + 2r^2}{2y_1} \right]^2 \quad (5.4)$$

for each $r = r_1, r_2, r_3$.

We can now prove the analog of Lemma 5.2.3

Lemma 5.2.8. (c.f. Lemma 5.2.3) *There exists a constant $d \geq 1$, depending only on E , such that*

$$(H'(P))^4 \leq dH'(2P)$$

for all $P \in E(\mathbb{Q}(i))$.

Proof: The proof is trivial when $P = \infty$. If $P = (r_j, 0)$ where r_j is the j -th root of $x^3 + Ax + B$, then $2P = \infty$ and so $H'(2P) = 1$. In this case, we can increase d if necessary to make the inequality holds. Thus we assume that P is none of those points.

Write P as $(x_1/z_1^2, y_1/z_1^3)$, and $2P$ as $(x_2/z_2^2, y_2/z_2^3)$, where $x_i, y_i, z_i \in \mathbb{Z}(i)$. We replace x_1 with x_1/z_1^2 , and y_1 with y_1/z_1^3 in (5.4). After simplification we obtain

$$x_2 - r_j z_2^2 = z_2^2 \left[\frac{-x_1^2 + 2r_j x_1 z_1^2 + (A + 2r_j^2) z_1^4}{2y_1 z_1} \right]^2$$

and then we write

$$\alpha_j := \left(\frac{z_2}{2y_1 z_1} \right) [-x_1^2 + 2r_j x_1 z_1^2 + (A + 2r_j^2) z_1^4]. \quad (5.5)$$

Clearly $\alpha_j \in \mathbb{Q}(i)$. Also $\alpha_j^2 = x_2 - r_j z_2^2 \in \mathbb{Z}(i)$, since $r_j \in \mathbb{Z}(i)$ by assumption. Thus $\alpha_j \in \mathbb{Z}(i)$. Now we have

$$\begin{aligned} |\alpha_j|^2 = |x_2 - r_j z_2^2| &\leq |x_2| + |r_j| \cdot |z_2^2| \\ &\leq |r_j| (|x_2| + |z_2^2|) \quad (\text{as } r_j \in \mathbb{Z}(i), \text{ so } |r_j| \geq 1) \\ &\leq 2|r_j| \cdot \left(\max\{|x_2|^2, |z_2^2|^2\} \right)^{1/2} \\ &= 2|r_j| \sqrt{H'(2P)}. \end{aligned}$$

Hence $|\alpha_j| \leq c(H'(2P))^{1/4}$, where $c = \sqrt{\max\{2|r_1|, 2|r_2|, 2|r_3|\}} \geq 1$ depends only on E .

Now we wish to estimate $H'(P)$. From (5.5), we can rearrange terms to get

$$\alpha_j = \mu_1 + \mu_2 r_j + \mu_3 r_j^2,$$

where

$$\mu_1 = \frac{z_2(-x_1^2 + Az_1^4)}{2y_1z_1}, \quad \mu_2 = \frac{x_1z_1z_2}{y_1}, \quad \mu_3 = \frac{z_2z_1^4}{y_1z_1}.$$

We can write the system of equations ($j = 1, 2, 3$) in matrix form as

$$\begin{pmatrix} 1 & r_1 & r_1^2 \\ 1 & r_2 & r_2^2 \\ 1 & r_3 & r_3^2 \end{pmatrix} \begin{pmatrix} \mu_1 \\ \mu_2 \\ \mu_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} \quad \implies \quad \mathcal{R}\boldsymbol{\mu} = \boldsymbol{\alpha}.$$

In fact, \mathcal{R} is the well-known *van der Monde matrix*, and its determinant is

$$\det \mathcal{R} = \prod_{i>j} (r_i - r_j).$$

Clearly $\det \mathcal{R} \in \mathbb{Z}(i)$ and is non-zero since all roots are distinct. Then $\boldsymbol{\mu}$ is uniquely determined by Cramer's rule. To be precise, for $j = 1, 2, 3$,

$$\mu_j = \frac{D_j}{D} := \frac{\det \mathcal{R}_j}{\det \mathcal{R}},$$

where \mathcal{R}_j is obtained by replacing the j -th column of \mathcal{R} with $\boldsymbol{\alpha}$. In other words, $D\mu_j$ is a linear combination of $\alpha_1, \alpha_2, \alpha_3$ with Gaussian integer coefficients. Thus $D\mu_j \in \mathbb{Z}(i)$ for all $j = 1, 2, 3$. A direct calculation shows that

$$D(A\mu_3 - 2\mu_1) = D \left[\frac{Az_2z_1^4 - z_2(-x_1^2 + Az_1^4)}{y_1z_1} \right] = \left(\frac{Dz_2}{y_1z_1} \right) x_1^2$$

and also

$$D\mu_3 = \left(\frac{Dz_2}{y_1z_1} \right) z_1^4$$

Since x_1 and z_1 have no common non-unit factor, this implies that $z_1 | Dz_2$. Similarly, since y_1 and z_1 has no common non-unit factor, then $y_1 | Dz_2$ as well. Hence we conclude that $y_1z_1 | Dz_2$, i.e.

$$\frac{Dz_2}{y_1z_1} \in \mathbb{Z}(i)$$

which then implies that

$$x_1^2 | D(A\mu_3 - 2\mu_1) \quad \text{and} \quad z_1^4 | D\mu_3,$$

and thus

$$|x_1|^2 \leq |D(A\mu_3 - 2\mu_1)| \quad \text{and} \quad |z_2|^2 \leq |D\mu_3|.$$

But we already show that $D\mu_j$ is a linear combination of α_j with Gaussian integer coefficients, and also

$$|\alpha_j| \leq c(H'(2P))^{1/4}$$

for $j = 1, 2, 3$. Therefore,

$$|x_1|^2 \leq c_1 (H'(2P))^{1/4}, \quad |z_2^2|^2 \leq c_2 (H'(2P))^{1/4}$$

for some appropriate constants $c_1, c_2 \geq 1$, (which still depend only on E). Hence

$$H'(P) = \max\{|x_1|^2, |z_2^2|^2\} \leq d (H'(2P))^{1/4}, \quad \text{where } d = \max\{c_1, c_2\}.$$

Raising both sides to the fourth power will yield our result. ■

It can be seen immediately that the method of descent is still valid once we replace the height function with the extended height function. It now remains to show that the analog of the weak Mordell-Weil theorem is valid.

5.3 Weak Mordell-Weil Theorem

In Section 5.1, we have seen the original Weak Mordell-Weil theorem, that is, $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. Although this seems to be a local property depending on the field, it turns out that this is still true for any extension of \mathbb{Q} , including $\mathbb{Q}(i)$.

In this section, we will prove that $E(\mathbb{Q}(i))/2E(\mathbb{Q}(i))$ is also finite. Rather than dealing with advanced group theory, we shall construct the result via an elementary extension of the original proof. To keep the discussion simple, we will only prove this result for all elliptic curves of the form

$$y^2 = f(x) = x^3 + Ax + B, \quad A, B \in \mathbb{Z}(i)$$

with a further assumption that $f(x) = (x - r_1)(x - r_2)(x - r_3)$, where $r_j \in \mathbb{Z}(i)$ for all $j = 1, 2, 3$. For the proof without any restriction on $f(x)$, please refer to Section 4.4 in Knapp [23].

5.3.1 Analog of the Original Theorem

The aim of this section is to prove:

Theorem 5.3.1. (c.f. Weak Mordell-Weil Theorem) *The quotient group $E(\mathbb{Q}(i))/2E(\mathbb{Q}(i))$ is finite.*

We first introduce some notation: let $\mathbb{Q}^*(i) = \mathbb{Q}(i) \setminus \{0\}$ denotes the multiplicative group of $\mathbb{Q}(i)$. Also we let $\mathbb{Q}^*(i)/(\mathbb{Q}^*(i))^2$ denote the subgroup of square free elements in $\mathbb{Q}^*(i)$.

To prove this theorem, we start by constructing a homomorphism $\phi : E(\mathbb{Q}(i)) \rightarrow \mathbb{Q}^*(i)/(\mathbb{Q}^*(i))^2 \times \mathbb{Q}^*(i)/(\mathbb{Q}^*(i))^2 \times \mathbb{Q}^*(i)/(\mathbb{Q}^*(i))^2$, in such a way that

$$\ker \phi = 2E(\mathbb{Q}(i)) := \{P \in E(\mathbb{Q}(i)) : P = 2Q \text{ for some } Q \in E(\mathbb{Q}(i))\},$$

and the image of ϕ is finite. Then it will follow that ϕ gives an injection from $E(\mathbb{Q}(i))/2E(\mathbb{Q}(i))$ to the image of ϕ , and thus $E(\mathbb{Q}(i))/2E(\mathbb{Q}(i))$ is finite. This

will complete the proof of Theorem 5.3.1, for which follows the analog of Mordell-Weil theorem.

For each j , we define a map $\phi_j : E(\mathbb{Q}(i)) \rightarrow \mathbb{Q}^*(i)/(\mathbb{Q}^*(i))^2$ by

$$\phi_j(P) = \phi_j((x, y)) = [\rho_j(x)](\mathbb{Q}^*(i))^2$$

where

$$\rho_j(x) = \begin{cases} 1 & \text{if } P = \infty \\ (x - r_i)(x - r_k), & (i \neq j \neq k) \\ x - r_j & \text{otherwise.} \end{cases}$$

and then we simply let

$$\phi(P) = (\phi_1(P), \phi_2(P), \phi_3(P)).$$

The following lemmas are adapted from the original versions given by Goldman [17], Knapp [23], Rose [33], and Washington [42]:

Lemma 5.3.2. *ϕ is a homomorphism.*

Proof: It suffices to show that for each j ,

$$\phi_j(P + Q) = \phi_j(P)\phi_j(Q) \tag{5.6}$$

for any $P, Q \in E(\mathbb{Q}(i))$. The proof is trivial if one of these points is ∞ . Thus, we can assume that neither point is ∞ .

It is easy to see that $\phi(P) = \phi(-P)$ for any $P \in E(\mathbb{Q}(i))$ (since ϕ is independent of y -coordinate). Also

$$(\phi_j(P))^2 = (x(P) - r_j)^2(\mathbb{Q}^*(i))^2 = (\mathbb{Q}^*(i))^2.$$

Hence proving (5.6) is equivalent to proving that

$$\phi_j(P + Q)\phi_j(P)\phi_j(Q) = (\mathbb{Q}^*(i))^2. \tag{5.7}$$

Let $y = mx + b$ be the “line” intersecting P , Q , and $-(P + Q)$. Then $x(P)$, $x(Q)$, and $x(P + Q)$ must satisfy

$$y^2 = (mx + b)^2 = (x - r_1)(x - r_2)(x - r_3).$$

Hence $(x - r_1)(x - r_2)(x - r_3) - (mx + b)^2 = 0$ when $x = x(P), x(Q), x(P + Q)$, and thus

$$\prod_{j=1}^3 (x - r_j) - (mx + b)^2 = (x - x(P))(x - x(Q))(x - x(P + Q)). \tag{5.8}$$

Consider the following cases:

- Neither point is $(r_j, 0)$ where $j = 1, 2$, or, 3 . If we let $x = r_j$ (for $j = 1, 2, 3$) in (5.8), we obtain

$$(mr_j + b)^2 = (x(P) - r_j)(x(Q) - r_j)(x(P + Q) - r_j)$$

which implies (5.7).

- Exactly one point is of the form $(r_j, 0)$, say, $P = (r_1, 0)$ (relabelling if necessary). From (5.8), we have

$$(x - r_1)(x - r_2)(x - r_3) - (mx + b)^2 = (x - r_1)(x - x(Q))(x - x(P + Q)). \quad (5.9)$$

If we let $x = r_2, r_3$, then this implies (5.7) for the case when $j = 2, 3$. For $j = 1$, first note that the line $y = mx + b$ intersects the point $P = (r_1, 0)$. Thus we have $0 = mr_1 + b$, i.e. $b = -mr_1$, so that

$$y = mx + b = m(x - r_1). \quad (5.10)$$

We shall take the limit as $x \rightarrow r_1$ in (5.9) in order to get the result. By substituting (5.10) into (5.9), we obtain

$$(x - r_1)(x - r_2)(x - r_3) - m^2(x - r_1)^2 = (x - r_1)(x - x(Q))(x - x(P + Q)).$$

Cancelling $(x - r_1)$ from both sides gives us

$$(x - r_2)(x - r_3) - m^2(x - r_1) = (x - x(Q))(x - x(P + Q)).$$

Let $x = r_1$, we eventually obtain

$$(r_1 - r_2)(r_1 - r_3) = (x(Q) - r_1)(x(P + Q) - r_1),$$

which implies that $\phi_1(P) = \phi_1(x(Q))\phi_1(x(P + Q))$, and thus (5.7) is true for $j = 1$.

- If both points are of the form $(r_j, 0)$, say, $P = (r_1, 0)$ and $Q = (r_2, 0)$. It is easy to see (from the geometrical construction of the addition) that $P + Q = (r_3, 0)$. Hence for any $j = 1, 2, 3$, we have

$$\phi_j(P + Q)\phi_j(P)\phi_j(Q) = (r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2(\mathbb{Q}^*(i))^2 = (\mathbb{Q}^*(i))^2.$$

This completes the proof. ■

Lemma 5.3.3. *Let $P \in E(\mathbb{Q}(i))$, with $P \notin \{\infty, (r_1, 0), (r_2, 0), (r_3, 0)\}$. If $P \in \ker \phi$, then $P = 2Q$ for some $Q \in E(\mathbb{Q}(i))$.*

Proof: Suppose $P = (x, y) \in \ker \phi$, where P satisfies the assumption. If there is such a point $Q = (x_1, y_1)$, then x_1 must satisfy the duplication formula (see (5.4) in Section 5.2.2):

$$x - r_j = x(P) - r_j = x(2Q) - r_j = \left[\frac{-x_1^2 + 2r_j x_1 + A + 2r_j^2}{2y_1} \right]^2 \quad (5.11)$$

for all $j = 1, 2, 3$. Since $P \in \ker \phi$, the definition of ϕ implies that $\phi_j(P) = (x - r_j)(\mathbb{Q}^*(i))^2 = (\mathbb{Q}^*(i)^2)$, i.e. $x - r_j$ is the square of a number in $\mathbb{Q}(i)$, and thus we set $\lambda_j := \sqrt{x - r_j} \in \mathbb{Q}(i)$.

After rearranging terms in (5.11) with respect to powers of r_j , we obtain

$$\lambda_j = \mu_1 + \mu_2 r_j + \mu_3 r_j^2, \quad (5.12)$$

where

$$\mu_1 = \frac{-x_1^2 + A}{2y_1}, \quad \mu_2 = \frac{x_1}{y_1}, \quad \mu_3 = \frac{1}{y_1}. \quad (5.13)$$

It can be seen that the corresponding system of equations is

$$\begin{pmatrix} 1 & r_1 & r_1^2 \\ 1 & r_2 & r_2^2 \\ 1 & r_3 & r_3^2 \end{pmatrix} \begin{pmatrix} \mu_1 \\ \mu_2 \\ \mu_3 \end{pmatrix} = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} \quad \implies \quad \mathcal{R}\boldsymbol{\mu} = \boldsymbol{\lambda},$$

where \mathcal{R} is the van der Monde matrix as seen earlier. Since $\det \mathcal{R} \neq 0$, $\boldsymbol{\mu} \in (\mathbb{Q}(i))^3$ and is unique by Cramer's rule. By (5.13), it follows that $Q = (x_1, y_1) \in (\mathbb{Q}(i))^2$. Hence we have just shown that $P = 2Q$ for some $Q \in (\mathbb{Q}(i))^2$. It now remains to confirm that $Q \in E(\mathbb{Q}(i))$.

Note that $\lambda_j^2 = x - r_j$. Then from (5.12), we obtain

$$(\mu_1^2 - 2B\mu_2\mu_3 - x)\mathbf{v}_0 + (1 + 2\mu_1\mu_2 - 2A\mu_2\mu_3 - B\mu_3^2)\mathbf{v}_1 + (\mu_2^2 + 2\mu_1\mu_3 - A\mu_3^2)\mathbf{v}_2 = 0$$

(using the fact that $r_j^3 = -Ar_j - B$ to eliminate the terms r_j^3, r_j^4), where \mathbf{v}_j is the j -th column of \mathcal{R} . Since $\det \mathcal{R} \neq 0$, all columns of \mathcal{R} are linearly independent, and thus each scalar is zero. In particular,

$$2\mu_1\mu_2 - 2A\mu_2\mu_3 - B\mu_3^2 = -1 \quad (5.14)$$

$$\mu_2^2 + 2\mu_1\mu_3 - A\mu_3^2 = 0. \quad (5.15)$$

Since $\mu_3 = 1/y_1 \neq 0$, we can solve for μ_1 in (5.15). Substituting μ_1 into (5.14) gives

$$\mu_2^3 + A\mu_2\mu_3^2 + B\mu_3^3 = \mu_3.$$

Divide both sides by μ_3^3 yields

$$\left(\frac{\mu_2}{\mu_3}\right)^3 + A \left(\frac{\mu_2}{\mu_3}\right) + B = \left(\frac{1}{\mu_3}\right)^2,$$

i.e. $x_1^3 + Ax_1 + B = y_1^2$ by (5.13). Hence $Q \in E(\mathbb{Q}(i))$ and we are done. \blacksquare

It is easy to see that the approach used in Lemma 5.3.3 will fail once P is of order dividing two, and thus such points need to be treated separately. The following lemmas are adapted from Rose [33]:

Lemma 5.3.4. *Let $E : y^2 = f(x) = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}(i)$, with $A, B \in \mathbb{Z}(i)$ and $r_1, r_2, r_3 \in \mathbb{Z}(i)$ be the zeros of $f(x)$. Then*

$$(r_j - r_\ell)(r_j - r_k) = 3r_j^2 + A$$

where $j, k, \ell \in \{1, 2, 3\}$ and $k \neq j \neq \ell$.

Proof: Using sum and products of the roots, we see that

$$r_1 + r_2 + r_3 = 0 \quad \text{and} \quad r_1r_2 + r_2r_3 + r_1r_3 = A.$$

Thus,

$$\begin{aligned} (r_j - r_\ell)(r_j - r_k) &= r_j^2 - r_jr_k - r_jr_\ell + r_\ell r_k \\ &= r_j^2 + (r_jr_k + r_jr_\ell + r_\ell r_k) - 2r_j(r_k + r_\ell) \\ &= 3r_j^2 + A - 2r_j(r_j + r_k + r_\ell) \\ &= 3r_j^2 + A - 2r_j(0) = 3r_j^2 + A. \end{aligned}$$

\blacksquare

Lemma 5.3.5. *Let $P \in E(\mathbb{Q}(i))$ with $P \in \{\infty\} \cup \{(r_j, 0) : j = 1, 2, 3\}$. If $P \in \ker \phi$, then $P = 2Q$ for some $Q \in E(\mathbb{Q}(i))$.*

Proof: The case when $P = \infty$ is trivial, since clearly $P \in \ker \phi$ and $P = 2Q$, when $Q = \infty$, $(r_j, 0) \in E(\mathbb{Q}(i))$ for $j = 1, 2, 3$ by assumption. Thus we may assume that $Q \neq \infty$ and $y(Q) \neq 0$.

Suppose that $P = (r_j, 0)$ and $P \in \ker \phi$. For simplicity, we take $P = (r_1, 0)$ (the cases when $j = 2, 3$ are treated similarly). By the definition of ϕ ,

$$\begin{aligned} \phi_1(P) &= (r_1 - r_2)(r_2 - r_3)(\mathbb{Q}^*(i))^2, \\ \phi_2(P) &= (r_1 - r_2)(\mathbb{Q}^*(i))^2, \end{aligned}$$

$$\phi_3(P) = (r_1 - r_3)(\mathbb{Q}^*(i))^2.$$

Since $P \in \ker \phi$, then each component is the square of a number in $\mathbb{Q}(i)$. That is,

$$r_1 - r_2 = s^2, \text{ and, } r_1 - r_3 = t^2, \quad (5.16)$$

for some $s, t \in \mathbb{Q}(i)$. If there is such a point $Q = (x_1, y_1)$ such that $P = 2Q$, the tangent line to the curve at the point Q is

$$y - y_1 = m(x - x_1), \quad \text{where } m = \frac{3x_1^2 + A}{2y_1},$$

which can be rearranged into

$$2y_1y = (3x_1^2 + A)x + (2B - x_1^3 + Ax_1). \quad (5.17)$$

If $P = 2Q$, then $-P = P$ is on this line. Substituting $P = (r_1, 0)$ into (5.17) yields

$$x_1^3 - 3r_1x_1^2 - Ax_1 - (Ar_1 + 2B) = 0.$$

Clearly $x_1 - r_1$ is a factor of this polynomial. Dividing by $x_1 - r_1$ gives us

$$x_1^2 - 2r_1x_1 - (A + 2r_1^2) = 0,$$

and thus

$$\begin{aligned} x_1 &= \frac{2r_1 \pm \sqrt{4r_1^2 + 4(A + 2r_1^2)}}{2} = r_1 \pm \sqrt{3r_1^2 + A} \\ &= r_1 + \sqrt{(r_1 - r_2)(r_1 - r_3)} \\ &= r_1 \pm st \in \mathbb{Q}(i), \end{aligned}$$

by Lemma 5.3.4 and (5.16). After substituting $(x, y) = Q = (x_1, y_1)$ into (5.17), it follows that

$$y_1^2 = x_1^3 + Ax_1 + B,$$

i.e. $Q = (x_1, y_1)$ is on E , and hence $y_1^2 = (x_1 - r_1)(x_1 - r_2)(x_1 - r_3)$. A direct calculation shows that

$$y_1^2 = \begin{cases} s^2t^2(s+t)^2, & \text{if } x_1 = r_1 + st \\ s^2t^2(s-t)^2, & \text{if } x_1 = r_1 - st. \end{cases}$$

Since $s, t \in \mathbb{Q}(i)$, we then have $y_1 \in \mathbb{Q}(i)$. Therefore $P = 2Q$ for some $Q \in E(\mathbb{Q}(i))$. This completes the proof. ■

We are now ready to state:

Proposition 5.3.6. $\ker \phi = 2E(\mathbb{Q}(i))$.

Proof: First we claim that $2E(\mathbb{Q}(i)) \subseteq \ker \phi$. To see this, let $P \in E(\mathbb{Q}(i))$. Then

$$\phi_j(2P) = \phi_j(P)\phi_j(P) = (\phi_j(P))^2 = (\mathbb{Q}^*(i))^2$$

for all $j = 1, 2, 3$, and the claim follows. The converse follows immediately from Lemma 5.3.3 and Lemma 5.3.5. \blacksquare

The last step is to ensure that the image of ϕ is finite. Before proving this, first note that we can always write

$$x - r_1 = au^2, \quad x - r_2 = bv^2, \quad x - r_3 = cw^2,$$

for some $u, v, w \in \mathbb{Q}(i)$, with a, b, c square-free Gaussian integers, that is, Gaussian integers which have no square factor.

Proposition 5.3.7. *Let*

$$S = \{p : p \text{ is Gaussian prime, and } p \mid (r_1 - r_2)(r_1 - r_3)(r_2 - r_3)\}.$$

If p is a Gaussian prime such that $p \mid abc$, then $p \in S$.

Proof: Suppose p be a Gaussian prime that divides abc . Let

$$k = w_p(x - r_1), \quad \ell = w_p(x - r_2), \quad m = w_p(x - r_3),$$

where w_p is the extended p -adic valuation as defined in Chapter 3.

Since $p \mid abc$, p divides at least one of a, b, c , say, $p \mid a$. Thus p^k is the largest power of p dividing $x - r_1$. Since $x - r_1 = au^2$ and $a \in \mathbb{Z}(i)$ is square free, it follows that k is odd.

Suppose $k < 0$. Then $p^{|k|}$ is the largest power of p dividing the denominator of $x - r_1$. But $r_1 \in \mathbb{Z}(i)$, $p^{|k|}$ must divide the denominator of x . Since $r_2, r_3 \in \mathbb{Z}(i)$, it then follows that $p^{|k|}$ is the largest power of p dividing the denominator of $x - r_2$ and $x - r_3$, i.e.

$$k = \ell = m.$$

Hence $p^{|3k|}$ is the largest power of p dividing $y^2 = (x - r_1)(x - r_2)(x - r_3)$, which is impossible (since $k + \ell + m$ must be even). Therefore $k > 0$.

We use the notation $a \mid b$, where $a \in \mathbb{Z}(i)$ and $b \in \mathbb{Q}(i)$ written as a quotient of Gaussian integers in lowest form, to denote that a divides the numerator of b . Since $k > 0$, we must have

$$p^k \mid x - r_1 \implies x \equiv r_1 \pmod{p},$$

and hence

$$x - r_2 \equiv r_1 - r_2 \pmod{p}, \quad \text{and,} \quad x - r_3 \equiv r_1 - r_3 \pmod{p}.$$

If $p \notin S$, i.e. $p \nmid (r_1 - r_2)(r_1 - r_3)(r_2 - r_3)$, then we have

$$\begin{aligned} p \nmid r_1 - r_2 &\implies p \nmid x - r_2, & \text{and} \\ p \nmid r_1 - r_3 &\implies p \nmid x - r_3, \end{aligned}$$

i.e. $\ell = m = 0$. Thus the largest power of p dividing

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

is $p^{k+\ell+m} = p^k$. But k is odd, this is impossible. Therefore $p \in S$. ■

We can now conclude the following:

Lemma 5.3.8. *The image of ϕ is finite*

Proof: Suppose (α, β, γ) is the triple representing $\phi(P)$, for some $P \in E(\mathbb{Q}(i))$. Without loss of generality, we may assume that $\alpha, \beta, \gamma \in \mathbb{Z}(i)$ are square free.

Proposition 5.3.7 says that each α, β, γ is a product of some Gaussian primes in S , as defined in the proposition. Since S is finite, there are only finitely many possibilities of (α, β, γ) . Thus the image of ϕ is finite. ■

Recall that ϕ gives an injection from $E(\mathbb{Q}(i))/2E(\mathbb{Q}(i))$ to the image of ϕ . Then Lemma 5.3.8 implies that $E(\mathbb{Q}(i))/2E(\mathbb{Q}(i))$ is finite, and this completes the proof of Theorem 5.3.1.

5.4 Examples

So far, we have proven that $E(\mathbb{Q}(i))$ is a finitely generated abelian group. It then follows from the structure theorem that

$$E(\mathbb{Q}(i)) \cong T \oplus \mathbb{Z}^r,$$

where T is the torsion subgroup of $E(\mathbb{Q}(i))$, and r is a non-negative integer called the *rank* of $E(\mathbb{Q}(i))$. While T can be found easily by the application of extended Lutz-Nagell theorem, computing r is difficult, and is a famous topic of on-going research in the study of elliptic curves. We will discuss this in more detail in the next chapter.

Clearly $E(\mathbb{Q}(i))$ is finite if and only if $r = 0$. In this section, we will show the group classification of some elliptic curves over $\mathbb{Q}(i)$. Note that this is just one of several ways to find the rank, which should reveal the difficulty in such computation.

Example 5.4.1. Let E be the elliptic curve

$$y^2 = x(x - 2)(x + 2).$$

If we regard E as an elliptic curve over \mathbb{Q} , it can be proved that

$$E(\mathbb{Q}) = \{\infty, (0, 0), (-2, 0), (2, 0)\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

(see Section 8.4 in Washington [42]). This implies that every $\mathbb{Q}(i)$ -rational point in E has finite order, and thus the rank $r = 0$. We will show that this is also true when E is defined over $\mathbb{Q}(i)$.

Since $x \in \mathbb{Q}(i)$, we can always write

$$x = au^2, \quad x - 2 = bv^2, \quad x + 2 = cw^2,$$

for some $u, v, w \in \mathbb{Q}(i)$, and $a, b, c \in \mathbb{Z}(i)$ as square free integers. In fact, (a, b, c) is the image of the homomorphism ϕ as defined in Section 5.3.1.

Lemma 5.4.2. $a, b, c \in \{1, i, 1 + i, i(1 + i)\}$.

Proof: Clearly a, b, c can be either $\pm 1, \pm i$, i.e. a unit of $\mathbb{Q}(i)$. If p is a Gaussian prime such that $p|a, p|b$, or $p|c$, Proposition 5.3.7 implies that p must divide

$$(0 - 2)(0 + 2)(2 + 2) = -16,$$

and thus $p = 1 \pm i$. The result then follows after noting that $1 - i = -i(1 + i)$, and -1 is a square in $\mathbb{Q}(i)$. ■

Since $y^2 = x(x - 2)(x + 2) = (abc)(uvw)^2$, abc is a square of some Gaussian integer. By Lemma 5.4.2, c is determined by (a, b) and there are 16 possibilities for such pairs. Thus there are 16 possibilities of (a, b, c) .

By the extended Lutz-Nagell theorem, the torsion subgroup of $E(\mathbb{Q}(i))$ is again

$$T = \{\infty, (0, 0), (2, 0), (-2, 0)\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

It is easy to check that

$$\phi(\infty) = (1, 1, 1), \quad \phi((0, 0)) = (1, i, i), \quad \phi((-2, 0)) = (i, 1, i), \quad \phi((2, 0)) = (i, i, 1),$$

which correspond to our four known points in $E(\mathbb{Q}(i))$. Thus we have to show that the remaining twelve triples (a, b, c) do not appear in the image of ϕ .

Here we show how to eliminate three of such triples:

Lemma 5.4.3. *The triple $(1, 1 + i, 1 + i)$ does not appear in the image of ϕ .*

Proof: Suppose $\phi(P) = (a, b, c) := (1, 1 + i, 1 + i)$ for some point $P \in E(\mathbb{Q}(i))$. Then we have

$$x = u^2, \quad x - 2 = (1 + i)v^2, \quad x + 2 = (1 + i)w^2, \tag{5.18}$$

i.e.

$$2 = u^2 - (1 + i)v^2, \quad -2 = u^2 - (1 + i)w^2, \quad -4 = (1 + i)(v^2 - w^2). \tag{5.19}$$

If v has $1 + i$ as a factor of its denominator (assuming that v is written as a quotient of Gaussian integers in the lowest form), then $(1 + i)v^2$ has an odd power of $1 + i$

in its denominator. Since u^2 always has an even power of $1+i$ in its denominator, this says that $2 = u^2 - (1+i)v_2 \notin \mathbb{Z}(i)$ which is a contradiction. Thus there is no $1+i$ in the denominator of v , and also not in the denominator of w by a similar argument.

Note that $-4 = (1+i)^4$. Then the third equality in (5.19) can be written as

$$(1+i)^3 = (v+w)(v-w).$$

It then follows that one of the following cases holds:

$$\begin{aligned} v+w &= k(1+i) & \text{and} & & v-w &= (1+i)^2/k, & \text{or} \\ v+w &= k(1+i)^2 & \text{and} & & v-w &= (1+i)/k, & \text{or} \\ v+w &= k & \text{and} & & v-w &= (1+i)^3/k, & \text{or} \\ v+w &= k(1+i)^3 & \text{and} & & v-w &= 1/k, \end{aligned} \tag{5.20}$$

for some $k \in \mathbb{Q}(i)$.

Since $1+i$ is not a factor of the denominator of v and w , then the denominators of both $v+w$ and $v-w$ do not have $1+i$ as a factor. Then (5.20) implies that $w_{1+i}(k) = 0$, i.e. k does not have $1+i$ as a factor in either numerator or denominator.

It turns out that each case in (5.20) always gives a contradiction, which will complete the proof. For example, suppose that the first case holds, i.e.

$$v+w = k(1+i) \quad \text{and} \quad v-w = (1+i)^2/k.$$

Then we have

$$2v = k(1+i) + (1+i)^2/k.$$

Since $(1+i)^2|2v$, this implies that $(1+i)^2|k(1+i)$, and thus $(1+i)|k$. But this is impossible since $w_{1+i}(k) = 0$. The other remaining cases can be done similarly. ■

Lemma 5.4.4. *The triples $(1+i, 1+i, 1)$ and $(1+i, 1, 1+i)$ do not appear in the image of ϕ .*

Proof: We will show how to deal with $(1+i, 1+i, 1)$. The second triple can be dealt with in a similar way.

Suppose $(a, b, c) = (1+i, 1+i, 1)$. Then we have

$$x = (1+i)u^2, \quad x-2 = (1+i)v^2, \quad x+2 = w^2,$$

and thus

$$2 = (1+i)(u^2 - v^2), \quad -4 = (1+i)v^2 - w^2, \quad -2 = (1+i)u^2 - w^2. \tag{5.21}$$

Suppose that the denominator of v has $1+i$ as a factor (assume that all numbers in $\mathbb{Q}(i)$ are written as a quotient of Gaussian integers in the lowest term). It then follows that $(1+i)v^2$ has an odd power of $1+i$ in its denominator, while w^2 has an

even power of $1+i$ in its denominator. This implies that $(1+i)v^2 - w^2 = -4 \notin \mathbb{Z}(i)$, a contradiction.

Hence there is no factor of $1+i$ in the denominators of v, w . By a similar argument, the denominator of u also has no $1+i$ in its denominator. Therefore we can perform arithmetic modulo $1+i$.

The last two equations in (5.21) imply that $(1+i)|w$, which then implies that $(1+i)|v$ and $(1+i)|u$. But the first equation in (5.21) will imply that $(1+i)^3|2$ which is impossible. Thus $(1+i, 1+i, 1)$ does not appear in the image of ϕ . ■

We are now able to eliminate the remaining nine triples. Recall that

$$\phi((0, 0)) = (1, i, i), \quad \phi((-2, 0)) = (i, 1, i), \quad \phi((2, 0)) = (i, i, 1).$$

Suppose there exists a point $P \in E(\mathbb{Q}(i))$ such that $\phi(P)$ is one of those nine triples, and $Q \in \{(0, 0), (2, 0), (-2, 0)\}$. Then we have $\phi(P+Q) = \phi(P)\phi(Q)$ since ϕ is a homomorphism. It can be seen that

$\phi(P)$	$\phi(Q)$	$\phi(P+Q)$
$(1, i(1+i), i(1+i))$	$(1, i, i)$	
$(i, 1+i, i(1+i))$	$(i, 1, i)$	$(1, 1+i, 1+i)$
$(i, i(1+i), 1+i)$	$(i, i, 1)$	
$(1+i, i, i(1+i))$	$(1, i, i)$	
$(i(1+i), 1, i(1+i))$	$(i, 1, i)$	$(1+i, 1, 1+i)$
$(i(1+i), i, 1+i)$	$(i, i, 1)$	
$(1+i, i(1+i), i)$	$(1, i, i)$	
$(i(1+i), 1+i, i)$	$(i, 1, i)$	$(1+i, 1+i, 1)$
$(i(1+i), i(1+i), 1)$	$(i, i, 1)$	

whereas Lemma 5.4.3 and 5.4.4 imply that these three values of $\phi(P+Q)$ do not occur. Hence there is no such point $P \in E(\mathbb{Q}(i))$.

We already know that T is the set of all points of order dividing 2. Then $2T = \{\infty\}$, and thus $T/2T = T$. It can be seen that

$$E(\mathbb{Q}(i))/2E(\mathbb{Q}(i)) \cong [T \oplus \mathbb{Z}^r]/[2T \oplus (2\mathbb{Z})^r] \cong (T/2T) \oplus \mathbb{Z}_2^r \cong T \oplus \mathbb{Z}_2^r.$$

Since ϕ is an isomorphism between $E(\mathbb{Q}(i))/2E(\mathbb{Q}(i))$ and the set of all possible triples, $|E(\mathbb{Q}(i))/2E(\mathbb{Q}(i))| = 4$. But $|T| = |\mathbb{Z}_2 \oplus \mathbb{Z}_2| = 4$, then $r = 0$. Therefore the set of all $\mathbb{Q}(i)$ -points on E is

$$E(\mathbb{Q}(i)) = \{\infty, (0, 0), (-2, 0), (2, 0)\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2,$$

which is the same as $E(\mathbb{Q})$. Note that $\text{rank}(E(\mathbb{Q}(i))) \geq \text{rank}(E(\mathbb{Q}))$ in general, so this immediately implies that $\text{rank}(E(\mathbb{Q})) = 0$ as seen earlier. ■

Example 5.4.5. Consider the elliptic curve

$$y^2 = x^3 - 9.$$

If we regard this as an elliptic curve over \mathbb{Q} , it can be checked that it has a trivial torsion subgroup $\{\infty\}$, and the rank of $E(\mathbb{Q})$ is zero [8]. Thus we have $E(\mathbb{Q}) = \{\infty\}$, i.e. there is no rational point (x, y) on this curve.

On the other hand, the structure of $E(\mathbb{Q}(i))$ is rather surprising. If we regard this as an elliptic curve over $\mathbb{Q}(i)$, the extended Lutz-Nagell theorem says that the torsion subgroup of $E(\mathbb{Q}(i))$ is

$$T = \{\infty, (0, 3i), (0, -3i)\} \cong \mathbb{Z}_3.$$

It is easy to see that $(2, \pm i) \in E(\mathbb{Q}(i))$. Since $(2, \pm i) \notin T$, they cannot have finite order. Hence we can conclude that

$$E(\mathbb{Q}(i)) \cong \mathbb{Z}_3 \oplus \mathbb{Z}^r,$$

for some integer $r \geq 1$. In other words, there are infinitely many $\mathbb{Q}(i)$ -points on this curve. In fact, it can be checked that, for example,

$$\begin{aligned} 2(2, i) &= (-40, -253i), \\ 3(2, i) &= \left(\frac{629}{441}, \frac{22870i}{9261} \right), \\ 4(2, i) &= \left(\frac{-639280}{64009}, \frac{-513439919i}{16194277} \right), \end{aligned}$$

and so on.

CHAPTER 6

Rank and Zeta Function

6.1 History

The zeta function has become dominant in the study of elliptic curves after its applications in analysis were introduced by Euler. It may be thought of as a way to encode information regarding points on elliptic curves, especially over finite fields or \mathbb{Q} , into one function.

Whereas several famous conjectures have been proposed regarding the zeta function, only a few of them are currently proven. A number of unsolved conjectures related to the zeta function are nowadays regarded as among the most difficult problems in mathematics. In particular, the relation between zeta function and the rank of the corresponding elliptic curve over \mathbb{Q} , known as *Birch and Swinnerton-Dyer Conjecture*, is one of seven million-dollar prize problems, as announced by the Clay Mathematics Institute in 2000.

6.2 Elliptic Curves over Finite Fields

In this section, we aim to introduce the zeta function for an elliptic curve defined over a finite field, and its relation to the number of points on such a curve.

Definition 6.2.1. *Let E be an elliptic curve defined over a finite field \mathbb{F}_p , where p is a prime. The zeta function of E is defined by*

$$Z_E(T) = \exp\left(\sum_{n=1}^{\infty} \frac{N_n}{n} T^n\right),$$

where $N_n = |E(\mathbb{F}_{p^n})|$.

Note that N_n can be determined for every $n \geq 1$, if $Z_E(T)$ is known. From Definition 6.2.1, we have

$$\log Z_E(T) = \sum_{n=1}^{\infty} \frac{N_n}{n} T^n = N_1 T + \frac{N_2 T^2}{2} + \frac{N_3 T^3}{3} + \dots,$$

and thus

$$N_n = \frac{1}{(n-1)!} \frac{d^n}{dT^n} \log Z_E(T) \Big|_{T=0}. \quad (6.1)$$

In fact, we can obtain the entire expression of the zeta function of E once only N_1 is known, as shown by the following theorem:

Theorem 6.2.2. *Let E be an elliptic curve over \mathbb{F}_p , and write $N_1 = p + 1 - a$. Then*

$$Z_E(T) = \frac{pT^2 - aT + 1}{(1 - T)(1 - pT)}.$$

Proof: From Theorem 4.3.4, we have

$$N_n = p^n + 1 - (\alpha^n + \beta^n),$$

where α, β are such that $X^2 - aX + p = (X - \alpha)(X - \beta)$. By Definition 6.2.1 and the fact that $-\log(1 - t) = \sum_{n=1}^{\infty} \frac{t^n}{n}$, we have

$$\begin{aligned} \log Z_E(T) &= \sum_{n=1}^{\infty} \frac{N_n}{n} T^n \\ &= \sum_{n=1}^{\infty} (p^n + 1 - \alpha^n - \beta^n) \frac{T^n}{n} \\ &= \sum_{n=1}^{\infty} \frac{(pT)^n}{n} + \sum_{n=1}^{\infty} \frac{T^n}{n} - \sum_{n=1}^{\infty} \frac{(\alpha T)^n}{n} - \sum_{n=1}^{\infty} \frac{(\beta T)^n}{n} \\ &= -\log(1 - pT) - \log(1 - T) + \log(1 - \alpha T) + \log(1 - \beta T), \end{aligned}$$

which yields the result after taking exponential. ■

In Section 4.3.1 we have used Theorem 4.3.4 to determine the order of $E(\mathbb{Z}_p(i))$, when $p \equiv 3 \pmod{4}$ and E is an elliptic curve of the form

$$y^2 = x^3 + kx, \quad \text{where } p \nmid k.$$

Equivalently, we can use the zeta function to determine such order. Recall that

$$N_1 = |E(\mathbb{F}_p)| = p + 1$$

as proved by Gauss. Then by Theorem 6.2.2, we have $a = 0$ and thus

$$Z_E(T) = \frac{pT^2 + 1}{(1 - T)(1 - pT)}.$$

Since $E(\mathbb{Z}_p(i)) \cong E(\mathbb{F}_{p^2})$, then $|E(\mathbb{Z}_p(i))| = N_2$. By (6.1), it can be checked that

$$N_2 = \left. \frac{d^2}{dT^2} \log Z_E(T) \right|_{T=0} = (p + 1)^2,$$

as we proved earlier.

Recall that the classical Riemann zeta function is defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

where the domain is $\{s \in \mathbb{C} : \Re(s) > 1\}$. This can be extended to $\mathbb{C} \setminus \{1\}$ by analytic continuation. There are a number of remarkable properties of ζ , including:

- *Riemann's functional equation.* For any $s \in \mathbb{C}$ with $s \notin \{0, 1, 2, \dots\}$, we have

$$\zeta(s) = 2(2\pi)^{s-1} \sin(\pi s/2) \Gamma(1-s) \zeta(1-s).$$

- *Riemann hypothesis.* If $\zeta(s) = 0$ with $0 < \Re(s) < 1$, then it is conjectured that $\Re(s) = 1/2$.

It turns out that the zeta function of elliptic curves is strongly analogous to the classical Riemann zeta function in these particular aspects. To make this clearer, first we introduce

$$\zeta_E(s) = Z_E(p^{-s}),$$

where s is a complex variable.

Theorem 6.2.3. *Let E be an elliptic curve over a finite field. Then the following properties are true:*

1. $\zeta_E(s) = \zeta_E(1-s)$.
2. If $\zeta_E(s) = 0$, then $\Re(s) = 1/2$.

Proof: From Theorem 6.2.2, we have

$$\begin{aligned} \zeta_E(s) = Z_E(p^{-s}) &= \frac{p^{1-2s} - ap^{-s} + 1}{(1-p^{-s})(1-p^{1-s})} \\ &= \frac{p^{2s-1}}{p^{2s-1}} \cdot \frac{p^{1-2s} - ap^{-s} + 1}{(1-p^{-s})(1-p^{1-s})} \\ &= \frac{1 - ap^{s-1} + p^{2s-1}}{(p^s - 1)(p^{s-1} - 1)} \\ &= \zeta_E(1-s), \end{aligned}$$

which yields (1). To prove (2), first recall that α, β in Theorem 4.3.4 satisfy

$$\alpha + \beta = a \quad \text{and} \quad \alpha\beta = p.$$

Then the numerator of $\zeta_E(s)$ becomes

$$p^{1-2s} - ap^{-s} + 1 = (\alpha\beta)^{1-2s} - (\alpha + \beta)p^{-s} + 1 = (1 - \alpha p^{-s})(1 - \beta p^{-s}).$$

Suppose $\zeta_E(s) = 0$. This implies that $p^s = \alpha$ or $p^s = \beta$. Now it can be seen that

$$\begin{aligned} p^{1-2s} - ap^{-s} + 1 = 0 &\iff p^{2s} - ap^s + p = 0 \\ &\iff p^s = \frac{a \pm \sqrt{a^2 - 4p}}{2} \\ &\iff \alpha, \beta = \frac{a \pm \sqrt{a^2 - 4p}}{2}. \end{aligned}$$

By Hasse's theorem, we have

$$|a| = |p + 1 - N_1| \leq 2\sqrt{p}.$$

It then follows that $a^2 - 4p < 0$, which implies that α and β are complex conjugates. In particular,

$$p^{\Re(s)} = |p^s| = |\alpha| = |\beta| = \sqrt{\frac{a^2 + (4p - a^2)}{4}} = \sqrt{p},$$

and hence $\Re(s) = 1/2$. ■

Although Theorem 6.2.2 suggests that the zeta function (and thus N_n for any $n > 1$) can be computed once N_1 is known, this is not always convenient in practice. In several cases, N_1 may be very large with no effective way to find it. There are currently a number of algorithms which can compute the zeta function without any prior knowledge to N_1 . For example, Satoh's algorithm provides an efficient computation for elliptic curves over finite fields of small characteristic $p \geq 5$ [34]. Fouquet, Gaudry, and Harley [15] have dealt with the cases $p = 2$ and $p = 3$.

6.3 L -Functions and Elliptic Curves over \mathbb{Q}

The definition of the zeta function of elliptic curves over finite fields can be extended to elliptic curves over \mathbb{Q} . A number of remarkable results and conjectures in the theory of elliptic curves have appeared.

Let E be an elliptic curve over \mathbb{Q} . Throughout this section, we assume that E is of the form

$$y^2 = f(x) = x^3 + Ax + B, \quad \text{where } A, B \in \mathbb{Z},$$

and let $D = 4A^3 + 27B^2$ be the discriminant of $f(x)$.

For each prime p , we can reduce all coefficients of E by modulo p to obtain the curve

$$E_p : y^2 = f(x) \bmod p = x^3 + (A \bmod p)x + (B \bmod p).$$

Definition 6.3.1. *We say that E has good reduction mod p if E_p is still an elliptic curve, that is, if $p \nmid D$. Otherwise, E is said to have bad reduction mod p .*

From the definition of an elliptic curve, E has bad reduction mod p if and only if $f(x)$ has repeated roots mod p .

Definition 6.3.2. If E has bad reduction mod p , then E is said to have one of the following properties:

- **Additive reduction mod p** , if $f(x)$ has a triple root mod p .
- **Split multiplicative reduction mod p** , if $f(x)$ has a double root mod p (say, at x_0), and the slope of the tangent lines to the curve E_p at $(x_0, 0)$ are in \mathbb{F}_p . The point $(x_0, 0)$ is called a singular point.
- **Non-split multiplicative reduction mod p** , otherwise.

Recall that for every prime p with $p \nmid D$, the zeta function of E_p is given by

$$\zeta_{E_p}(s) = Z_{E_p}(p^{-s}) = \frac{p^{1-2s} - a_p p^{-s} + 1}{(1 - p^{-s})(1 - p^{1-s})}.$$

For convenience, when $p \mid D$, we define

$$Z_{E_p}(T) = \frac{1}{(1 - T)(1 - pT)}.$$

The functions $Z_{E_p}(p^{-s})$, for each prime p , is called the *local zeta function* of E at p . The *global zeta function* for E is simply the product of all local zeta functions, that is,

$$\zeta_E(s) = \prod_p Z_{E_p}(p^{-s}).$$

A direct calculations shows that

$$\begin{aligned} \zeta_E(s) &= \prod_p \frac{1}{1 - p^{-s}} \prod_p \frac{1}{1 - p^{1-s}} \prod_{p \nmid D} (p^{1-2s - a_p p^{-s} + 1}) \\ &= \zeta(s) \zeta(s - 1) \prod_{p \nmid D} (p^{1-2s - a_p p^{-s} + 1}) \\ &= \frac{\zeta(s) \zeta(s - 1)}{L_E(s)}, \end{aligned}$$

where $L_E(s) = \prod_{p \nmid D} (p^{1-2s - a_p p^{-s} + 1})^{-1}$. We can now state the definition of an L -function:

Definition 6.3.3. Let E be an elliptic curve over \mathbb{Q} . The L -function of E is defined as

$$L_E(s) = \prod_{p \nmid D} (1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p \mid D} (1 - a_p p^{-s})^{-1},$$

where s is a complex variable, and

$$a_p = \begin{cases} p + 1 - |E(\mathbb{F}_p)| & \text{if } E \text{ has good reduction mod } p \\ 0 & \text{if } E \text{ has additive reduction mod } p \\ 1 & \text{if } E \text{ has split multiplicative reduction mod } p \\ -1 & \text{otherwise.} \end{cases}$$

Since $|a_p| \leq 2\sqrt{p}$ by Hasse's theorem, it can be shown that

Theorem 6.3.4. $L_E(s)$ converges for every $s \in \mathbb{C}$ such that $\Re(s) > 3/2$.

Proof: Note that there are only finitely many primes p such that $p|D$, and thus the second product always converges for any $s \in \mathbb{C}$. We will show that the first infinite product converges when $\Re(s) > 3/2$.

In particular, it suffices to show that

$$\prod_{p \nmid D} (1 - a_p p^{-s} + p^{1-2s})$$

is convergent. Note that $\prod (1 + b_n)$ converges when $\sum |b_n|$ converges. So our problem is now equivalent to showing that $\sum_{p \nmid D} |p^{1-2s} - a_p p^{-s}|$ is convergent.

From Hasse's theorem, we have $|a_p| \leq 2\sqrt{p}$. It then follows that

$$\begin{aligned} \sum_{p \nmid D} |p^{1-2s} - a_p p^{-s}| &\leq \sum_{p \nmid D} (|p^{1-2s}| + |a_p| \cdot |p^{-s}|) \\ &\leq \sum_{p \nmid D} p^{1-2\Re(s)} + 2 \sum_{p \nmid D} p^{\frac{1}{2}-\Re(s)} \\ &\leq \sum_{n=1}^{\infty} n^{1-2\Re(s)} + 2 \sum_{n=1}^{\infty} n^{\frac{1}{2}-\Re(s)}. \end{aligned}$$

But the sum $\sum_{n=1}^{\infty} n^{1-2\Re(s)}$ converges only when $1 - 2\Re(s) < -1$, i.e. $\Re(s) > 1$. Similarly, the second sum will converge only when $1/2 - \Re(s) < -1$, i.e. $\Re(s) > 3/2$. Hence

$$\sum_{p \nmid D} |p^{1-2s} - a_p p^{-s}|$$

converges when $\Re(s) > 3/2$, and so does the infinite product. ■

In general, one prefers to work with an elliptic curve over \mathbb{Q} which has good reduction at p , for as many p as possible. This can be done by means of changes of variables. Such an elliptic curve with the “best” reduction is called the *minimal Weierstrass equation*.

Example 6.3.5. Consider an elliptic curve E given by

$$y^2 = f(x) = x^3 + 10^6 x + 10^6.$$

It can be checked that the discriminant of $f(x)$ is $2^{12} \cdot 5^{12} \cdot 1777 \cdot 2251$. Thus E has good reduction modulo any prime apart from 2, 5, 1777, and 2251. By dividing

both sides by 10^6 , we obtain a new curve

$$E_1 : y_1^2 = f_1(x_1) = x_1^3 + 100x_1 + 1,$$

where $x_1 = x/100$ and $y_1 = y/1000$.

It is easy to show that the discriminant of $f_1(x_1)$ is $(1777)(2251)$. Thus E_1 now has bad reduction only at 1777 and 2251, and this is the furthest we can go. Hence the minimal Weierstrass equation for E is

$$y^2 = x^3 + 100x + 1.$$

We can now classify the type of bad reduction on E . It can be checked that

$$f_1(x_1) \equiv \begin{cases} (x_1 + 693)(x_1 + 542)^2 & (\text{mod } 1777) \\ (x_1 + 1193)(x_1 + 529)^2 & (\text{mod } 2251). \end{cases}$$

Thus by Definition 6.3.2, E has multiplicative reduction at 1777 and 2251. To decide whether E has a split multiplicative reduction at, for example, $p = 1777$, we need to consider the tangent line to E_p at its singular point, namely $(-542, 0)$.

By writing $X = x_1 + 542$ and $Y = y_1$, we can translate $f_1(x_1)$ into

$$Y^2 = X^2(X + 151) \implies \left(\frac{Y}{X}\right)^2 = X + 151.$$

If $X \rightarrow 0$, the right side of this equation approaches to 151, and thus E_p is approximated by $(Y/X)^2 = 151$. In fact, it can be checked that

$$151 \equiv (\pm 611)^2 \pmod{p}.$$

Thus the slope of two tangent lines at the singular point are ± 611 , which are in \mathbb{F}_p . Hence E has split multiplicative reduction at 1777. By a similar argument, it can be shown that E also has split multiplicative reduction at 2251. ■

6.4 Rank of Elliptic Curves

Recall that the rank of $E(\mathbb{Q})$ is the integer $r \geq 0$ such that

$$E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r,$$

where T is the torsion subgroup of $E(\mathbb{Q})$. As mentioned earlier, we can calculate T easily by using the Lutz-Nagell theorem. It is also known that the number of possible group classifications of T is finite (Mazur's theorem). Nevertheless, finding r is much more difficult and there is still no efficient algorithm known for its computation.

One of many unanswered questions is whether the rank could be arbitrarily large, or whether there exists an integer K such that the rank of any elliptic curve over \mathbb{Q} is at most K . In contrast to the boundedness of the torsion subgroup, it is widely believed that the rank of elliptic curves is unbounded. This is known as the *folklore conjecture*.

One supporting piece of evidence of this conjecture is a work due to Mestre [28] in 1982, where he claimed that the elliptic curve E given by

$$y^2 + y = x^3 - 6349808647x + 193146346911036$$

has $E(\mathbb{Q})$ of rank at least 12. The construction of this curve was quite explicit, and thus it is possible to construct a new elliptic curve of even higher rank based on his method. Unfortunately, it turns out that this idea is not so easy to put into practice. At this moment, the elliptic curve currently known to have the highest rank is that found by Elkies [13] in 2006, where $E(\mathbb{Q})$ has rank at least 28. The equation of this curve is of the form

$$y^2 + xy + y = x^3 - x^2 - ax + b,$$

where $a \approx 2.007 \times 10^{55}$ and $b \approx 3.448 \times 10^{82}$, which is clearly far more complicated than any of our previous examples.

For any elliptic curve E ,

$$\text{rank}(E(\mathbb{Q}(i))) \geq \text{rank}(E(\mathbb{Q})).$$

If the folklore conjecture is indeed true, then the rank of $E(\mathbb{Q}(i))$ could be also arbitrarily large. On the other hand, the failure of the conjecture would tell us nothing about the behaviour of the rank of $E(\mathbb{Q}(i))$. As shown in Example 5.4.5, the number of $\mathbb{Q}(i)$ -points becomes infinite whilst $E(\mathbb{Q})$ is a trivial group. Thus the rank of $E(\mathbb{Q}(i))$ may not be bounded even though the rank of $E(\mathbb{Q})$ is.

6.4.1 Birch and Swinnerton-Dyer Conjecture

Let E be an elliptic curve $y^2 = x^3 - Cx$, for some fixed constant C . During 1958–1960, Birch and Swinnerton-Dyer studied the behaviour of the product

$$\prod_{p \leq N} \frac{N_p}{p},$$

as $N \rightarrow \infty$, where p is a prime, and N_p is the number of rational points on E_p (provided that E has good reduction mod p).

In fact, this is equivalent to studying $L_E(s)$ at $s = 1$. From Definition 6.3.3, the infinite product over all “good” primes at $s = 1$ yields

$$\prod_{p \nmid D} (1 - a_p p^{-1} + p^{-1})^{-1} = \prod_{p \nmid D} \frac{p}{p + 1 - a_p} = \prod_{p \nmid D} \frac{p}{N_p},$$

where D is the discriminant of E . Note that in this case we ignore the fact that the product, $L_E(s)$, only converges when $\Re(s) > 3/2$.

Based on extensive numerical computation on EDSAC II computer at the University of Cambridge, Birch and Swinnerton-Dyer [4] eventually proposed the following remarkable conjectures:

Conjecture 6.4.1. (Weak Birch and Swinnerton-Dyer Conjecture) $E(\mathbb{Q})$ is infinite if and only if $L_E(1) = 0$.

Conjecture 6.4.2. (Strong Birch and Swinnerton-Dyer Conjecture) let r be the rank of $E(\mathbb{Q})$. Then

$$L_E(s) = (s - 1)^r g(s),$$

with $g(1) \neq 0, \infty$. In other words, the rank of $E(\mathbb{Q})$ is the order of the zero of $L_E(s)$ at $s = 1$.

The Birch and Swinnerton-Dyer conjecture is a rather amazing result in the study of elliptic curves. In particular, it is an example of where algebraic and analytic properties of elliptic curves coincide.

6.4.2 Average Rank of Elliptic Curves

One of many challenges in the study of elliptic curves nowadays is to construct elliptic curves of high rank. Since there are infinitely many elliptic curves over \mathbb{Q} , one might expect that the number of elliptic curves of high rank is also significantly large. However, the fact that the highest rank currently known is merely (at least) 28, may also convince us that such curves are considerably rare. In particular, the rank of all elliptic curves *on average* should be small if the latter is true.

In this section, we shall call the rank defined by the structure theorem as *algebraic rank*, and the order of zero of $L_E(s)$ at $s = 1$ as *analytic rank*. This is based on the assumption that Birch and Swinnerton-Dyer Conjecture is true.

Theorem 6.4.3. (Tate [41]) *The algebraic rank is bounded by the analytic rank.*

Hence the algebraic rank on average is also bounded by the average analytic rank. In fact, the analytic rank on average is rather small, as shown by Brumer in 1992 [5]:

Theorem 6.4.4. (Brumer) *The average of the analytic ranks of all elliptic curves over \mathbb{Q} is bounded by 2.3.*

As we can see from the theorem, this implies that most elliptic curves over \mathbb{Q} have very small rank. In particular, more can be said once we also assume that Riemann hypothesis is true. The following theorem is due to Heath-Brown in 2004 [19], and improves Brumer's result:

Theorem 6.4.5. (Heath-Brown) *The average of the analytic ranks of all elliptic curves over \mathbb{Q} is bounded by 2. Moreover, the density of elliptic curves with analytic rank at least r decreases faster than exponentially as r grows.*

Thus it is clear that finding an elliptic curve of high rank is extremely difficult, and the rate of difficulty is even worse than exponential rate!

6.4.3 Complex Multiplication

For every elliptic curve E , one natural homomorphism on $E(\mathbb{C})$ to itself is the *multiplication-by- n* map, that is

$$\phi_n : P \mapsto nP, \quad n \in \mathbb{Z}.$$

In particular, ϕ_n is given by rational functions. This can be seen directly from the algebraic definition of addition on the curve.

In general, a homomorphism $\phi : E(\mathbb{C}) \rightarrow E(\mathbb{C})$ defined by rational functions, i.e.

$$\phi(P) = \phi(x, y) = \left(\frac{f_1(x, y)}{f_2(x, y)}, \frac{f_3(x, y)}{f_4(x, y)} \right),$$

where $f_i(x, y)$ are polynomials in terms of x and y , is called an *endomorphism*. Thus ϕ_n is also an endomorphism.

For most elliptic curves, ϕ_n is the only endomorphism. Nonetheless, some elliptic curves may also have additional endomorphisms apart from ϕ_n . For this family of such elliptic curves, we say that

Definition 6.4.6. *An elliptic curve E is said to have complex multiplication if there exists an endomorphism apart from the multiplication-by- n map.*

For example, the elliptic curve

$$E : y^2 = x^3 + kx, \quad \text{for some constant } k$$

has complex multiplication, via the endomorphism

$$\phi(x, y) = (-x, iy).$$

Note that $\phi(x, y) \in E(\mathbb{C})$ since

$$(iy)^2 = -y^2 = -x^3 - kx = (-x)^3 + k(-x).$$

Clearly ϕ is defined by rational functions. To confirm that ϕ is an endomorphism, we need to show that it is a homomorphism, which can be done directly from the definition. However, this is not necessary, as suggested by the following theorem:

Theorem 6.4.7. *Let E be an elliptic curve, and $\phi : E(\mathbb{C}) \rightarrow E(\mathbb{C})$ be a map given by rational functions. If $\phi(\infty) = \infty$, then ϕ is automatically a homomorphism.*

Proof: The proof is rather deep. See Section III.4.8 in Silverman [37]. ■

The set of all endomorphisms of E also forms a ring, where the operations of addition and multiplication are defined by

$$\begin{aligned}(\phi_1 + \phi_2)(P) &= \phi_1(P) + \phi_2(P), \\ (\phi_1\phi_2)(P) &= \phi_1(\phi_2(P)),\end{aligned}$$

for ϕ_1, ϕ_2 endomorphisms of E . If E has no complex multiplication, the only endomorphisms of E are $\{\phi_n : n \in \mathbb{Z}\}$ and thus the ring is merely isomorphic to \mathbb{Z} . Otherwise, the ring of endomorphisms must be strictly larger than \mathbb{Z} . It is still unknown what sort of ring it is isomorphic to.

The concept of complex multiplication is very useful in proving many interesting results. In particular, this leads to some progress in proving Birch and Swinnerton-Dyer conjecture. In 1977, Coates and Wiles [7] proved that

Theorem 6.4.8. (Coates-Wiles) *Let E be an elliptic curve over \mathbb{Q} with complex multiplication. If $L_E(1) \neq 0$, then $E(\mathbb{Q})$ is finite.*

For more discussions on complex multiplication, see Chapter VI in Silverman and Tate [38], and Chapter 10 in Washington [42].

CHAPTER 7

Integer Points on Elliptic Curves

7.1 Diophantine Equations and Hilbert's Problems

The study of many Diophantine problems is closely related to finding rational solutions on a particular elliptic curve. In many cases, it is even more natural to focus on integer solutions on such a curve. The nature of the integer solutions of Diophantine equations has been widely studied by a number of mathematicians since late 19th century, including Hilbert, Thue, Siegel and Baker.

One of many obvious questions is whether there exists an integer solution for a particular Diophantine problem. In 1900, this became known as the *Hilbert's Tenth Problem*, which is one of 23 challenging problems addressed by Hilbert to the International Congress of Mathematicians in Paris (See [20] for the entire address). Hilbert asked:

10. Determination of the solvability of a Diophantine equation.

Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *to devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

Unfortunately, the general answer to this problem is “no”, as later proposed by Davis, Putnam, and Robinson [11] in 1961, and eventually proved by Matijasevič [26] in 1970. In other words, there is no general algorithm which can decide the existence of integer solutions for an arbitrary Diophantine equation. Hence this is also true for elliptic curves.

For more discussion on the Hilbert's Tenth Problem, see Poonen [32].

7.2 Integer Points on Elliptic Curves over \mathbb{Q}

Let E be an elliptic curve over \mathbb{Q} . If the rank of $E(\mathbb{Q})$ is zero, then trivially the number of all integer points on E is finite since $E(\mathbb{Q})$ is finite. Nonetheless, the

fact that $E(\mathbb{Q})$ is infinite does not necessarily imply that the set of integer points is also infinite. For example, the elliptic curve E given by

$$y^2 = x^3 - 2$$

has infinitely many rational points, as proved by Bachet in 1621. But the only integer points on E are $(3, \pm 5)$, as shown by Fermat. More examples can be seen in Chapter 26 of Mordell [29].

It turns out that this is always the case for every elliptic curve over \mathbb{Q} , as initially proved by Mordell [29] in 1922:

Theorem 7.2.1. (Mordell) *The equation*

$$y^2 = f(x) = ax^3 + bx^2 + cx + d, \quad a \neq 0,$$

where all coefficients are integers and $f(x)$ has no repeated root, has only a finite number of integer solutions.

A more generalised version of Theorem 7.2.1 for the case when $\deg(f(x)) \geq 4$ was later introduced by Siegel in 1926 [36]. Consequently, this implies that the number of integer points on any elliptic curve E over \mathbb{Q} is always finite. Based on Siegel's method, the analogous result has been obtained for any arbitrary number field K , (see Sprindžuk [40] for more details).

An immediate consequence of Theorem 7.2.1 is that the possibilities of $x, y \in \mathbb{Z}$ to be an integer point on E must be subject to some bound. In 1968, an explicit bound for such x, y was firstly introduced by Baker [2]:

Theorem 7.2.2. (Baker) *Let E be a Diophantine equation of the form*

$$y^2 = ax^3 + bx^2 + cx + d,$$

with $a, b, c, d \in \mathbb{Z}$ and $a \neq 0$. Then every integer solution (x, y) of E satisfies

$$\max(|x|, |y|) < \exp\{(10^6 H)^{10^6}\},$$

where $H = \max\{|a|, |b|, |c|\}$.

Although Baker's bound can be computationally achievable in some certain families of elliptic curves, some additional techniques are still required in order to make such computation even more practical. In many cases, the set of all integer points can be easily determined by an elementary approach rather than using Baker's bound. Consider the following example:

Example 7.2.3. The only integer point on the elliptic curve $y^2 = x^3 - 1$ is $(1, 0)$.

Proof: First we rewrite the equation as

$$x^3 = 1 + y^2 = (1 + iy)(1 - iy).$$

Note that $x, y \in \mathbb{Z}$. Suppose y is odd, i.e. $y = 2k + 1$ for some $k \in \mathbb{Z}$. Then we have

$$x^3 = 1 + (4k^2 + 4k + 1) \equiv 2 \pmod{4},$$

which can be easily verified to be impossible. Thus y must be even.

Let $d = \gcd(1 + iy, 1 - iy)$. Then it follows that d divides $(1 + iy) + (1 - iy) = 2$. Clearly $d \neq 2$. Since $2 = -i(1 + i)^2$, then either $d = 1$ or $d = 1 + i$.

Suppose there exist $a, b \in \mathbb{Z}$, such that $1 + iy = (1 + i)(a + bi)$. By considering both real and imaginary parts, we have

$$1 = a - b, \quad y = a + b,$$

and thus $2a = y + 1$, which is impossible since y is even. Hence $d = 1$, and this implies that

$$1 + iy = i^r(u + iv)^3,$$

for some $r \in \{0, 1, 2, 3\}$, and $u, v \in \mathbb{Z}$.

Note that

$$i = (-i)^3, \quad i^2 = -1 = (-1)^3,$$

so it can be absorbed in the third power. Hence it suffices to consider only the case $r = 0$. Thus we have

$$1 + iy = (u + iv)^3.$$

By considering the real part of both sides, we obtain

$$1 = u^3 + 3u(iv)^2 = u(u^2 - 3v^2).$$

This implies that either

$$u = u^2 - 3v^2 = 1 \quad \text{or} \quad u = u^2 - 3v^2 = -1.$$

It is easy to see that the second case is impossible; since otherwise we will have $v^2 = 2/3$ whereas $v \in \mathbb{Z}$. The first case yields

$$u = 1, \quad v = 0,$$

and thus $1 + iy = 1$, i.e. $y = 0$ and then $x = 1$.

In fact, it can be shown by a similar argument that $(1, 0)$ is the only integer point on the curve $y^2 + 1 = x^p$, for every odd prime p . See Cassels [6] for the generalised version of the proof.

Note that Baker's bound in this case is $\max(|x|, |y|) < \exp\{(10^6)^{10^6}\}$. ■

Reducing Baker's bound is an active topic in the theory of elliptic curves. In some certain families of elliptic curves over \mathbb{Q} , the bound for the maximum magnitude of integer points on such curve can be significantly reduced into more computable level. For example, a result due to Draziotis [12] in 2006 said that

Theorem 7.2.4. (Draziotis) *Let E be an elliptic curve over \mathbb{Q} of the form*

$$y^2 = f(x) = (x - \rho)h(x),$$

with $\rho \in \mathbb{Z}$, and $h(x)$ is a quadratic with integer coefficients such that $h(\rho) = \pm 1$. Then any integer point (x, y) on E satisfies

$$|x| < 11H^2 + 5,$$

where $H = \max\{|a_i| : a_i \text{ is a coefficient of } f(x)\}$.

Several studies also focus on generalising such a bound for any arbitrary number field. One of several such results is due to Bugeaud [3] in 1998, where an optimised bound for the magnitude of "integer points" on elliptic curves over a number field K has been established. Moreover, this bound is only polynomial in terms of H (as defined in Theorem 7.2.2), rather than exponential as in Baker's result.

7.3 Gaussian Integer Points on Elliptic Curves over $\mathbb{Q}(i)$

7.3.1 Analog of Mordell's Theorem

As mentioned before, the analogous result of Theorem 7.2.1 has been generalised for any number field K . Thus there are only a finite number of Gaussian integer points on any elliptic curves over $\mathbb{Q}(i)$. For simplicity, we shall only illustrate a special case when the elliptic curve E is given by

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

where $r_j \in \mathbb{Z}(i)$ for all $j = 1, 2, 3$, and $r_i \neq r_j$ when $i \neq j$. The following proof is adapted from Lang [24]:

First note that we are only interested in $x \in \mathbb{Z}(i)$. Assume that $x \neq r_j$ for any $j = 1, 2, 3$. Then for each j , we have $x - r_j \in \mathbb{Z}(i)$. Moreover, we can always write these as

$$x - r_j = a_j u_j^2,$$

for some $u_j \in \mathbb{Z}(i)$, and $a_j \in \mathbb{Z}(i)$ is square-free. By Proposition 5.3.7, it follows that a_1, a_2, a_3 belong to a finite set.

Consider the set of all points (x, y) which yield the same triple (a_1, a_2, a_3) . Now we write $a_j = t_j^2$. Note that since a_j is square free, then $t_j \notin \mathbb{Z}(i)$ unless $a_j = 1$. Thus we have

$$x - r_j = t_j^2 u_j^2.$$

After eliminating x , we obtain the system of equations

$$r_i - r_j = t_j^2 u_j^2 - t_i^2 u_i^2 = (t_j u_j + t_i u_i)(t_j u_j - t_i u_i), \quad (7.1)$$

where $i, j \in \{1, 2, 3\}$ and $i \neq j$. This implies that the factors on the right divide the constant $r_i - r_j$, once we consider this over the field $K := \mathbb{Q}(i, t_1, t_2, t_3)$. Hence there exists a finite number of $\lambda_{ij} \in K$ such that

$$t_j u_j - t_i u_i = \epsilon_{ij} \lambda_{ij},$$

for some units $\epsilon_{ij} \in K$.

If we again restrict ourselves to those x having the same system $(\lambda_{12}, \lambda_{23}, \lambda_{13})$, it can be seen that (u_1, u_2, u_3) satisfies

$$\begin{aligned} u_1 t_1 - u_2 t_2 &= \epsilon_1 \lambda_1 \\ u_2 t_2 - u_3 t_3 &= \epsilon_2 \lambda_2 \\ u_3 t_3 - u_1 t_1 &= \epsilon_3 \lambda_3, \end{aligned} \quad (7.2)$$

where $(\lambda_1, \lambda_2, \lambda_3)$ is fixed, and $\epsilon_1, \epsilon_2, \epsilon_3$ are units. By summing all these three equations, we have

$$0 = \epsilon_1 \lambda_1 + \epsilon_2 \lambda_2 + \epsilon_3 \lambda_3.$$

Since $r_i \neq r_j$, we have $\epsilon_3 \lambda_3 \neq 0$. Dividing the above equation by $\epsilon_3 \lambda_3$ yields

$$\frac{\lambda_1}{\lambda_3} \left(\frac{\epsilon_1}{\epsilon_3} \right) + \frac{\lambda_2}{\lambda_3} \left(\frac{\epsilon_2}{\epsilon_3} \right) = -1.$$

By Siegel's result [35], there are only a finite number of the solutions $(\epsilon_1, \epsilon_2, \epsilon_3)$. Now we fix all t_j, λ_j , and ϵ_j , for $j = 1, 2, 3$. Then by (7.2), $t_j u_j - t_i u_i$ are also fixed for all $i \neq j$.

Hence it follows from (7.1) that $t_j u_j + t_i u_i$ are also fixed (since $r_i - r_j$ are fixed). This gives us another system of equations

$$\left(\begin{array}{ccc|c} t_1 & t_2 & 0 & \alpha_{21} \\ 0 & t_2 & t_3 & \alpha_{32} \\ t_1 & 0 & t_3 & \alpha_{13} \end{array} \right) \implies \left(\begin{array}{ccc|c} t_1 & t_2 & 0 & \alpha_{21} \\ 0 & t_2 & t_3 & \alpha_{32} \\ 0 & 0 & 2t_3 & \alpha_{13} + \alpha_{32} - \alpha_{21} \end{array} \right),$$

where $\alpha_{ji} = (r_j - r_i)/(\epsilon_i \lambda_i)$. Thus (u_1, u_2, u_3) is uniquely determined.

Therefore the equations $x - r_j = a_j u_j^2$ have only a finite number of solutions in $\mathbb{Z}(i)$, for all $j = 1, 2, 3$, and so does E . ■

7.4 A Particular Family of Elliptic Curves over $\mathbb{Q}(i)$

In general, there is no “best” algorithm which can determine all Gaussian integer points on an elliptic curve over $\mathbb{Q}(i)$ in general. Many of the well-known techniques for finding all integer points still fail for certain elliptic curves, and most require a significant amount of information about the elliptic curve a priori.

One of many popular approaches nowadays is the *Elliptic Logarithm Method (ELM)*, which was originally developed by Lang and Zagier during 1980s. In 1997, Smart and Stephens [39] generalised this method to find all integral points on elliptic curves over any number field K (Here, integral point refers to one whose coordinates x, y are in the ring of integers of the field K). Although this method works for most elliptic curves, its preliminary requirement is the knowledge of the rank and the set of all independent points on that particular curve. As mentioned before, this is rather expensive and there is still no effective way known for such computation.

In this section, we will concentrate on determining all Gaussian integer points on elliptic curves E of the form

$$y^2 = xh(x) := x(x^2 \pm p^k),$$

where $k \in \mathbb{Z}^+$, and p is a Gaussian prime. The method we shall study here is modified from the work of Draziotis [12] in 2006.

We shall introduce some notation before continuing to the main results. First, let E' be the curve defined by

$$E' : y'^2 = x'^4 \pm p^k.$$

For each point (x', y') on E' , there is a corresponding point (x, y) on E via the map

$$\begin{aligned} \psi : E' &\rightarrow E \\ (x', y') &\mapsto (x'^2, x'y'). \end{aligned}$$

It can be verified that $\psi : E' \rightarrow E \setminus (0, 0)$ is also surjective. In fact, any point $(x, y) \neq (0, 0)$ on E corresponds to a point on E' via the map

$$\begin{aligned} \psi^{-1} : E \setminus \{(0, 0)\} &\rightarrow E' \\ (x, y) &\mapsto \left(\sqrt{x}, \frac{y}{\sqrt{x}} \right). \end{aligned}$$

Let $d \in \mathbb{Z}(i)$ be a divisor of $\pm p^k$. Then for each d , we define the curve W_d as

$$W_d : dY^2 = d^2X^4 \pm p^k.$$

The notations

$$E(\mathbb{Z}(i)), \quad E'(\mathbb{Z}(i)), \quad W_d(\mathbb{Z}(i)),$$

denote the set of all Gaussian integer points on the curve E , E' , and W_d respectively. Finally we introduce

$$\Pi_d = \{(\epsilon_1 A\sqrt{d}, \epsilon_2 B\sqrt{d}) : (A, B) \in W_d(\mathbb{Z}(i)), \epsilon_1 = \pm 1, \pm i, \epsilon_2 = \pm 1\},$$

and

$$T = \{(x, 0) \in E(\mathbb{Z}(i))\}.$$

Proposition 7.4.1.

$$E(\mathbb{Z}(i)) = T \cup \psi \left(E'(\mathbb{Z}(i)) \cup \bigcup_{d \in S} \Pi_d \right),$$

where $S = \{1, i, p, pi\}$.

Proof: Suppose a point $P = (x, y) \in E(\mathbb{Z}(i))$. If $y = 0$, then clearly $P \in T$ and vice versa. Thus we can now assume that $y \neq 0$, and also $P \neq (0, 0)$.

Since $\psi : E' \rightarrow E \setminus \{(0, 0)\}$ is surjective, then there exists a point (x', y') on E' (allowing $x', y' \in \mathbb{C}$ if necessary) such that $\psi(x', y') = (x, y)$. Let $K = \mathbb{Q}(i, x', y')$. Recall that $x'^2 = x \in \mathbb{Z}(i)$ and $x'y' = y \in \mathbb{Z}(i)$. Thus we can conclude that $[K : \mathbb{Q}(i)] \leq 2$, and both x', y' are $\mathbb{Q}(i)$ -algebraic integers.

Suppose $x' \in \mathbb{Z}(i)$. Since $y \in \mathbb{Z}(i)$, we must have $y' = y/x' \in \mathbb{Q}(i)$, and thus $y' \in \mathbb{Z}(i)$ (as y' is $\mathbb{Q}(i)$ -algebraic). The converse is also true by a similar argument. Hence $x' \in \mathbb{Z}(i)$ if and only if $y' \in \mathbb{Z}(i)$, i.e. $(x', y') \in E'(\mathbb{Z}(i))$. In this case, we have $P \in \psi(E(\mathbb{Z}(i)))$.

If both $x', y' \notin \mathbb{Z}(i)$, we have $[K : \mathbb{Q}(i)] = 2$ and thus there exists a square-free $d \in \mathbb{Z}(i)$ with $d \neq 0, 1$, such that $K = \mathbb{Q}(i, \sqrt{d})$. Let \mathcal{O}_K be the ring of integers of K . Since $x'^2 = x \in \mathbb{Z}(i)$ but $x' \notin \mathbb{Z}(i)$, this implies that $x' = A\sqrt{d}$ for some $A \in \mathbb{Z}(i)$. It then follows from $y = x'y'$ that $y' = B\sqrt{d}$ for some $B \in \mathbb{Z}(i)$.

Substituting $x' = A\sqrt{d}$ and $y' = B\sqrt{d}$ into the equation of E' yields

$$dB^2 = d^2A^4 \pm p^k.$$

Thus we have $d \mid \pm p^k$, i.e. $d \in S := \{1, i, p, pi\}$ (Note that d is square-free). Also it can be verified that (A, B) is indeed on W_d . Hence by definition, $(x', y') \in \Pi_d$ and thus $P \in \psi(\Pi_d)$ with $d \in S$. This completes the proof. \blacksquare

In Draziotis's result, the set of all integer points on $y^2 = x(x^2 \pm p^k)$ has been completely deduced for every k . For simplicity, we shall only consider a special

case when $k = 4\beta$, for some $\beta \in \mathbb{Z}^+$, and p a Gaussian prime. That is, we aim to determine all Gaussian integer points on the elliptic curve

$$E : y^2 = x(x^2 \pm p^{4\beta}), \quad \beta \in \mathbb{Z}^+.$$

The corresponding curve E' is now

$$E' : y'^2 = x'^4 \pm p^k,$$

which can be transformed into E via the map ψ defined earlier. We will now use Proposition 7.4.1 to find all Gaussian integer points on E . Let $d \in \mathbb{Z}(i)$ be a square-free divisor of $\pm p^k$. Since p is a Gaussian prime, then we have $d \in \{1, i, p, ip\}$.

We first examine the case where E is given by $y^2 = x(x^2 + p^{4\beta})$. To proceed further, the next step is to determine the sets $W_d(\mathbb{Z}(i))$ and Π_d . Now consider the equations

$$\begin{aligned} W_1 : Y^2 &= X^4 + p^{4\beta} \\ W_i : Y^2 &= i(X^4 - p^{4\beta}) \\ W_p : Y^2 &= pX^4 + p^{4\beta-1} \\ W_{ip} : Y^2 &= i(pX^4 - p^{4\beta-1}). \end{aligned}$$

We wish to find all Gaussian integer points on each of these W_d .

Lemma 7.4.2. *There is no pair $(X, Y) \in \mathbb{Z}(i) \times \mathbb{Z}(i)$ such that*

$$Y^2 = pX^4 \pm p^{4\beta-1},$$

where $\beta \in \mathbb{Z}^+$.

Proof: Let $X = p^\alpha X_0$ and $Y = p^\gamma Y_0$, where $\alpha, \gamma \geq 0$ and $p \nmid X_0 Y_0$. Then the above equation becomes

$$p^{2\gamma} Y_0^2 = p^{4\alpha+1} X_0^4 \pm p^{4\beta-1}.$$

By comparing the exponent of p in every term, it is easy to see that all these three exponents cannot be identical. Also if all of them are distinct, we can divide the equation by p^k , where $k = \min\{2\gamma, 4\alpha + 1, 4\beta - 1\}$. But this will imply that either $p|1$, or $p|X_0$, or $p|Y_0$, which is impossible. Hence the only possible case is that exactly 2 of these exponents are equal.

Considering all these exponents modulo 4 shows that this case is also impossible. Therefore, such a pair (X, Y) does not exist. ■

Note that for W_{ip} , we have

$$Y^2 = i(pX^4 - p^{4\beta-1}) = (ip)X^4 + (ip)^{4\beta-1},$$

since $\beta \in \mathbb{Z}^+$. It then follows from Lemma 7.4.2 that

$$W_p(\mathbb{Z}(i)) = W_{ip}(\mathbb{Z}(i)) = \emptyset.$$

It now still remains to determine W_1 and W_i . In the case $d = 1$, $W_1(\mathbb{Z}(i)) = E'(\mathbb{Z}(i))$. We can quickly obtain $W_1(\mathbb{Z}(i))$ by using the following result:

Theorem 7.4.3. *There exists no triple (a, b, c) of non-zero Gaussian integers with $\gcd(a, b) = 1$, $b \equiv 0 \pmod{1+i}$, and $a, c \equiv 1 \pmod{1+i}$, such that*

$$a^4 \pm b^4 = c^2.$$

Proof: The general argument of this proof was commonly known as the *infinite descent*, as initially introduced by Fermat. This proof is adapted from the version given by Cross [10] in 1993.

Let $a, b, c \in \mathbb{Z}(i)$ and $abc \neq 0$. Suppose that (a, b, c) satisfies the above equation and $d \in \mathbb{Z}(i)$ is the greatest common divisor of any two of a, b, c . Then it is easy to see that d^4 divides every term in the equation. Thus we can assume that $d = 1$. Moreover, we can assume that (a, b, c) is chosen so that c has the smallest modulus $|c| = \sqrt{\Re(c)^2 + \Im(c)^2}$.

Now we rewrite the equation as

$$c^2 = (a^2)^2 + (\epsilon b^2)^2,$$

where $\epsilon = 1$ or i , according as $c^2 = a^4 + b^4$ or $c^2 = a^4 - b^4$. Using the Pythagorean triple formula for Gaussian integers (see Cross [9]), there exist $u, v \in \mathbb{Z}(i)$ with $\gcd(u, v) = 1$, both u, v have odd real parts, and both $u, v \equiv 1 \pmod{1+i}$, such that

$$a^2 = \frac{u^2 + v^2}{2}, \quad \epsilon b^2 = \frac{u^2 - v^2}{2i}, \quad c = uv. \quad (7.3)$$

By assumption, $b \equiv 0 \pmod{1+i}$. Thus $-(1+i)^2 = -2i$ divides ϵb^2 , and we obtain

$$-\frac{\epsilon b^2}{2i} = \frac{u^2 - v^2}{4} = \frac{(u+v)(u-v)}{2 \cdot 2}.$$

Suppose that $u = u_1 + u_2i$ and $v = v_1 + v_2i$, then since both u_1, v_1 are odd, then it is clear from above equation that $\Re(u \pm v)/2 \in \mathbb{Z}$. Now note that $\Im(u^2 - v^2) = 2(u_1u_2 - v_1v_2)$ is divisible by 4 (since $-\epsilon b^2/(2i) \in \mathbb{Z}(i)$). Thus we have

$$u_1u_2 - v_1v_2 \equiv u_2 - v_2 \equiv 0 \pmod{2},$$

since both u_1, v_1 are odd. Hence both u_2, v_2 are either odd or even. In any case, this makes both $(u \pm v)/2 \in \mathbb{Z}(i)$.

The numbers $(u + v)/2$ and $(u - v)/2$ are coprime. To see this, suppose that d is a common Gaussian prime factor of both. Then it follows that d also divides both u and v , which is impossible since $\gcd(u, v) = 1$. Consequently, we have

$$\frac{u + v}{2} = \eta_1 s^2, \quad \frac{u - v}{2} = \eta_2 t^2,$$

for some $\eta_1, \eta_2 \in \{1, -1, i, -i\}$. Then s and t are also coprime. Now we have

$$\left(\frac{u + v}{2}\right)^2 + \left(\frac{u - v}{2}\right)^2 = (\eta_1 s^2)^2 + (\eta_2 t^2)^2 = \frac{u^2 + v^2}{2} = a^2.$$

Note that $\eta_1^2, \eta_2^2 = \pm 1$. Multiplying this (if necessary) by -1 yields the form

$$s^4 \pm t^4 = a^2.$$

Recall that by early assumption, $a \equiv 1 \pmod{1 + i}$. Thus exactly one of s and t is not divisible by $1 + i$, say

$$s \equiv 1 \pmod{1 + i} \quad \text{and} \quad t \equiv 0 \pmod{1 + i}.$$

Thus this is exactly the same type of equation we have considered here. By calculating moduli, it can be seen that

$$|a^2| = \frac{|u^2 + v^2|}{2} \quad \text{and} \quad |c^2| = |u^2 v^2| = |u^2| |v^2|.$$

But the Triangle Inequality says that

$$|a^2| = \frac{|u^2 + v^2|}{2} \leq \frac{|u^2| + |v^2|}{2} \leq \frac{2|u^2| |v^2|}{2} = |c^2|, \tag{7.4}$$

using the fact that $m + n \leq 2mn$ for any $m, n \in \mathbb{Z}^+$. Moreover, it is easy to see that the equality only holds when $m = n = 1$.

If the equality holds in (7.4), then we will have $|u| = |v| = 1$, i.e. $u, v \in \{\pm 1, \pm i\}$. By considering all 16 possibilities of the pairs (u, v) in (7.3), it turns out that in each case, either $a^2 = 0$ or $b^2 = 0$. Since we have already excluded all cases when $abc = 0$ from the beginning, this is thus impossible.

Hence from (7.4), we have $|a^2| < |c^2|$, and thus $|a| < |c|$. But this contradicts the minimality of $|c|$. This completes the proof. ■

Thus by Theorem 7.4.3, $W_1(\mathbb{Z}(i))$ only contains all points (X, Y) such that $XY = 0$. It can be checked that

$$E'(\mathbb{Z}(i)) = W_1(\mathbb{Z}(i)) = \{(0, \pm p^{2\beta})\},$$

and thus the corresponding Gaussian integer point on E obtained from this case is $\psi(0, \pm p^{2\beta}) = (0^2, \pm 0 \cdot p^{2\beta}) = (0, 0)$.

It still remains to consider all other possible points in W_i . Recall that the equation of W_i is

$$Y^2 = i(X^4 - p^{4\beta}),$$

which can be rewritten as $iY^2 = p^{4\beta} - X^4$. Now it is easy to see that there is no point in W_i with $X = 0$. For $Y = 0$, we quickly obtain $X = \epsilon p^\beta$, where $\epsilon \in \{\pm 1, \pm i\}$. Then the corresponding points in Π_i given by these points in $E'(\mathbb{Z}(i))$ are

$$\{(\epsilon_1 \epsilon p^\beta \sqrt{i}, 0) : \epsilon_1 = \pm 1, \pm i\} = \{(\epsilon p^\beta \sqrt{i}, 0)\}.$$

Finally by using the map ψ , the corresponding points in $E(\mathbb{Z}(i))$ are therefore

$$\psi(\epsilon p^\beta \sqrt{i}, 0) = (i\epsilon^2 p^{2\beta}, 0 \cdot \epsilon p^\beta) = (\pm p^{2\beta} i, 0),$$

which are other trivial points in $E(\mathbb{Z}(i))$.

One obvious question at this point is whether there exists some non-trivial points (X, Y) in $E(\mathbb{Z}(i))$, i.e. the ones with $XY \neq 0$. Since we have already seen that the cases W_1, W_p yield nothing, and the case W_1 only yields the point $(0, 0)$, any non-trivial points in $E(\mathbb{Z}(i))$ must arise from the non-trivial points in W_i .

The equation of W_i can be written as

$$iY^2 = (p^{2\beta})^2 + (iX^2)^2,$$

which is of the form $ic^2 = a^2 + b^2$, where $a, b, c \in \mathbb{Z}(i)$. Unlike the Pythagorean triple for Gaussian integers (see Cross [9]), the general solution to this type of equation is still unknown at this moment. Even though it is possible to generate (perhaps) infinitely many of such triples (a, b, c) , experiment with `Maple` currently shows that none of them seems to allow us to obtain other non-trivial points in $E(\mathbb{Z}(i))$. Although this convinces me that there are no other non-trivial Gaussian integer points in $E(\mathbb{Z}(i))$, I have been unable to deal with the case $ic^2 = a^2 + b^2$.

The `Maple` script for generating triples (a, b, c) can be seen in Appendix A.

For the elliptic curve E given by $y^2 = x(x^2 - p^{4\beta})$, the calculation is very similar to the previous case. Let d be a square-free divisor of $-p^{4\beta}$. Then again we have $d \in \{1, i, p, pi\}$, and thus we have to consider all points in each W_d , where

$$\begin{aligned} W_1 : Y^2 &= X^4 - p^{4\beta} \\ W_i : Y^2 &= i(X^4 + p^{4\beta}) \\ W_p : Y^2 &= pX^4 - p^{4\beta-1} \\ W_{ip} : Y^2 &= i(pX^4 + p^{4\beta-1}). \end{aligned}$$

Similarly to the previous case, Lemma 7.4.2 implies that $W_p(\mathbb{Z}(i)) = W_{pi}(\mathbb{Z}(i)) = \emptyset$, and thus there is no point in $E(\mathbb{Z}(i))$ which can be obtained from these two curves.

The set $W_1(\mathbb{Z}(i))$ is again a consequence of Theorem 7.4.3, which gives us

$$E'(\mathbb{Z}(i)) = W_1(\mathbb{Z}(i)) = \{(0, \pm ip^{2\beta}), (\epsilon p^\beta, 0) : \epsilon = \pm 1, \pm i\}.$$

Thus the corresponding points in $E(\mathbb{Z}(i))$ obtained from W_1 are

$$\psi(E'(\mathbb{Z}(i))) = \{(0, 0), (\pm p^{2\beta}, 0)\}.$$

Now we consider W_i . Again, it is easy to see that there is no point $(X, Y) \in W_i(\mathbb{Z}(i))$ with $X = 0$. Moreover, there is no point (X, Y) with $Y = 0$; since otherwise -1 is a fourth power over Gaussian integer, a contradiction. Now the equation of W_i can be written as

$$i(iY)^2 = (X^2)^2 + (p^{2\beta})^2,$$

which is still of the form $ic^2 = a^2 + b^2$, where $a, b, c \in \mathbb{Z}(i)$. As mentioned before, any non-trivial points in $E(\mathbb{Z}(i))$, if there exists, must be obtained from some non-trivial points in $W_i(\mathbb{Z}(i))$.

APPENDIX A

Maple Scripts used in the Thesis

In this thesis, a number of scripts for Maple mathematics package have been written and used in calculating some general properties of elliptic curves over $\mathbb{Q}(i)$. All scripts used in this thesis are included below, according to its main function.

A.1 Addition on Elliptic Curves: `addition.mpl`

```
# Maple script for addition on elliptic curve
# by T.Thongjunthug
# last modified: 3 Apr, 2006
# don't change unless you know what you doing

# std package loaded - none
# external .mpl loaded - none

##### Addition of Points on Curve #####
# add 2 points on the curve
# usage: addPts([x1,y1],[x2,y2],a,b)
# where [x1,y1],[x2,y2] = points on curves
# of the form  $y^2 = x^3 + ax + b$  ONLY!
addPts:= proc(P1,P2::list, a,b::complexcons)
    local x1,x2,y1,y2,x3,y3,m;

    x1:= op(1,P1);
    x2:= op(1,P2);
    y1:= op(2,P1);
    y2:= op(2,P2);

    # case 0: x1 = infty or x2 = infty
    if (x1 = infinity) then
        x3:= x2;
        y3:= y2;

    elif (x2 = infinity) then
        x3:= x1;
```

```

y3:= y1;

# case 1: x1 != x2
elif (x1 <> x2) then
  m:= (y2-y1)/(x2-x1);
  x3:= m^2 - x1 - x2;
  y3:= -1 * (m*(x3-x1) + y1);

# case 2: x1 = x2 but y1 != y2
elif (y1 <> y2) then
  x3:= infinity;
  y3:= infinity;

# case 3: both point identical
elif (y1 = 0) then
  x3:= infinity;
  y3:= infinity;

else
  m:= (3*(x1^2) + a)/(2*y1);
  x3:= m^2 - 2*x1;
  y3:= -1 * (m*(x3-x1) + y1);
end if;

return([x3,y3]);
end proc;

# point duplication = 2P = P+P
# usage: dupPt([x,y],a,b)
# where [x,y] = point
# and y^2 = x^3 + ax + b
dupPt:= proc(P::list, a,b::complexcons)
  return(addPts(P,P,a,b));
end proc;

```

A.2 Extended Lutz-Nagell Theorem

The scripts for calculating all torsion points in $E(\mathbb{Q}(i))$ using the extended Lutz-Nagell theorem consist of 3 files:

- `eqntrans.mpl` - for transforming equations given in the generalised Weierstrass form into the Weierstrass form $y^2 = x^3 + Ax + B$.
- `listposy.mpl` - for determining all possible values of y which satisfy the extended Lutz-Nagell theorem.

- `torsion.mpl` - the top-level interface to users.

A.2.1 `eqntrans.mpl`

```

# eqntrans.mpl
# transform generalised Weierstrass eqn into std version
# only for field K, with char(K) <> 2,3 only
# by T.Thongjunthug
# last update on 8 apr, 2006
# DON'T change unless you know what you doin'

# std package loaded
# with(GaussInt):

# external .mpl loaded - none

##### Equation Transformer #####

# complete the square
# provided char(K) <> 2
# usage: nonChar2Transfrm(a1,a3,a5,a2,a4,a6)
# such that in the generalised Weierstrass equation
#  $y^2 + a1(xy) + a3(y) = x^3 + a2(x^2) + a4(x) + a6$ 
# return: (a,b,c) where the simplify version is
#  $y^2 = x^3 + ax^2 + bx + c$ 
completeSqr:= proc(a1,a3,a2,a4,a6:: complexcons)
  local a,b,c;
  a:= a2 + (a1^2)/4;
  b:= a4 + a1*a3/2;
  c:= a6 + (a3^2)/4;

  return((a,b,c));
end proc;

# made into std Weierstrass eqn
# provided char(K) <> 3
# usage: nonChar3Transfrm(a,b,c)
# where  $y^2 = x^3 + ax^2 + bx + c$ 
# return: (a1,b1) for  $y^2 = x^3 + a1x + b1$ 
nonChar3Transfrm:= proc(a,b,c :: complexcons)
  local a1,b1;
  a1:= b - (a^2)/3;
  b1:= c + 2*(a^3)/27 - a*b/3;

```

```

    return((a1,b1));
end proc;

# top-level proc -- user should access only from this proc
# tidy up given std Weierstrass form into of GI coeff
# usage: makeGICoeff(a,b)
# where  $y^2 = x^3 + ax + b$ 
# return (a1,b1) in Gi coord
makeGICoeff:= proc(a,b::complexcons)
    #local a1, b1, d;
    #d:= lcm(denom(a), denom(b));
    #a1:= d^4 * a;
    #b1:= d^6 * b;

    local cmmDen, cdenFac,
          i, j, numFac,
          fac, base, orgPow, scaleMul;

    cmmDen:= lcm(denom(a), denom(b));
    cdenFac:= op(2, ifactors(cmmDen));

    numFac:= nops(cdenFac);
    scaleMul:= 1;
    for i from 1 to numFac do
        fac:= op(i, cdenFac);
        base:= op(1, fac);
        j:= op(2, fac);

        while (j mod 6 <> 0) do
            j:= j+1;
        end do;

        scaleMul:= scaleMul * (base ^ j);
    end do;

    return((a*root(scaleMul, 3)^2, scaleMul*b));
end proc;

# top-level
# simplify any Generalised Weierstrass eqn over Q(i) into
# std one of GI coeff!

```

```

simplifyEqn:= proc(a1,a3,a2,a4,a6::complexcons)
  local p1, p2;
  p1:= completeSqr(a1,a3,a2,a4,a6);
  p2:= nonChar3Transfrm(p1);

  return(makeGICoeff(p2));
end proc;

```

A.2.2 *listposy.mpl*

```

# listposy.mpl
# maple script for elliptic curve over Q(i)
# by T.Thongjunthug
# last update on 7 Apr, 2006
# don't change unless you know what u doing

# std package loaded
with(GaussInt):

# external .mpl loaded - none

##### begin implementation #####

# generate all possible y in ext. LN theorem
# usage : listY(a,b :: complexcons); y^2 = x^3 + ax + b
# return: K=[y1,y2,...] a list of all possible y's
newlistY:= proc(a,b :: complexcons)
  local L, K, Fac, NewY,      # list
        num_fac,num_y,      # parameter value
        base,pow,          # temp varying value
        i,j,k;              # index counter

  K:= [1,I];
  L:= op(2, GIfactors(4*a^3 + 27*b^2));
  num_fac:= nops(L);
  for i from 1 to num_fac do
    Fac:= op(i,L);
    base:= op(1,Fac);
    pow:= op(2,Fac);

    # assign y where y^2 divides discriminant
    j:= 1;
    NewY:= [];

```

```

while (2*j <= pow) do
  num_y:= nops(K);
  for k from 1 to num_y do
    NewY:= [op(NewY), (base^j) * op(k,K)];
  end do;

  j:= j+1;
end do;

K:= [op(K), op(NewY)];
end do;

K:= [0, op(K)];
return(K);
end proc;

```

A.2.3 torsion.mpl

```

# Maple script for elliptic arithmetic
# by T.Thongjunthug
# last modified on 3 Apr 2006
# don't change unless you know what you doing

# std package loaded
with(GaussInt):

# external .mpl loaded
read "addition.mpl":
read "listposy.mpl":

##### Lutz-Nagell related #####
# decide whether a number is Gaussian int
# usage: isGI(x), where x is complex number
isGI:= proc(x::complexcons)
  local a,b;
  a:= Re(x);
  b:= Im(x);
  return (type(a,integer) and type(b,integer));
end proc;

# check whether coeffs are in GI
# usage: chkCoeff(a,b), where  $y^2 = x^3 + ax + b$ 
chkCoeff:= proc(a,b::complexcons)

```

```

# check if a,b are GI
if not(isGI(a) and isGI(b)) then
  error("a and b must be Gaussian integers");
end if;
end proc;

# return a list of all possible y (from discriminant)
# usage: listY(a,b) where  $y^2 = x^3 + ax + b$ 
# and both a,b are GI
listY:= proc(a,b::complexcons)
# local i, e, root_e, L, K;
  chkCoeff(a,b); # check if coeff in GI
#
# K:= [0];
# L:= GIdivisor(4*a^3 + 27*b^2);
# convert(L, list);
# for i from 1 to nops(L) do
#   e:= op(i, L);
#   if (GIissqr(e)) then
#     root_e:= GIsqrt(e);
#     # append possible y
#     K:= [op(K), root_e, I*root_e];
#   end if;
# end do;
#
# return(K);
  return(newlistY(a,b));
end proc;

# find possible points (x,y) from the theorem
# usage: findPosXY(a,b), where  $y^2 = x^3 + ax + b$ 
# where a,b are GI
findPosXY:= proc(a,b::complexcons)
  local i,j,t,y,Sol, L, K;
  chkCoeff(a,b);

  L:= listY(a,b);
  K:= [];
  for i from 1 to nops(L) do
    y:= op(i, L);
    Sol:= GIroots(x^3 + a*x + b - y^2);

```

```

    # if there is such x, extract it and make
    # the ordered pair
    if (nops(Sol) <> 0) then
        for j from 1 to nops(Sol) do
t:= op(1, op(j, Sol));
K:= [op(K), [t,y]];
            end do;
        end if;
    end do;

    return(K);
end proc;

# top-level proc -- user should execute only from this proc
# find the order of a given point
# usage: ptOrder([x,y],a,b)
# where [x,y] = point
# on the curve  $y^2 = x^3 + ax + b$ 
# return: order of points as integer
# if infinite order -- return 0;
# require: addition.mpl
ptOrder:= proc(P::list, a,b::complexcons)
    local Q, x, y, ord;
    ord:= 1;
    Q:= P;

    while (op(1,Q) <> infinity) do
        Q:= addPts(Q,P,a,b);
        x:= op(1,Q);
        y:= op(2,Q);
        if (not(isGI(x) and isGI(y)) and (x <> infinity)) then
            return(0);
        else
            ord:= ord + 1;
        end if;
    end do;

    return(ord);
end proc;

# top-level proc - user shall execute only from this proc!
# find all torsion pts of  $E(Q(i))$  from given  $f(x)$ 

```

```

# usage: torsionPts(a,b), where  $y^2 = x^3 + ax + b$ 
torsionPts:= proc(a,b::complexcons)
  local L, pt, i, x, y, ord, totalTors;
  chkCoeff(a,b);

  totalTors:= 1;
  print(infinity, "has order", 1);

  L:= findPosXY(a,b);
  for i from 1 to nops(L) do
    pt:= op(i, L); # get the point to be checked
    ord:= ptOrder(pt, a, b);
    if (ord <> 0) then
      print(pt, "has order", ord);

      x:= op(1,pt);
      y:= op(2,pt);
      if (y <> 0) then
print ([x,-1*y], "has order", ord);
totalTors:= totalTors + 2;
      else
totalTors:= totalTors + 1;
      end if;

    end if;
  end do;

  print("Total torsion pts in  $E(Q(i)) =$ ", totalTors);
end proc;

```

A.3 On the Equation $ic^2 = a^2 + b^2$: triple.mpl

This script illustrates how to generate some triples (a, b, c) where $a, b, c \in \mathbb{Z}(i)$ and $\gcd(a, b, c) = 1$, which satisfy the equation $ic^2 = a^2 + b^2$.

```

# Maple script for generating triplet (a, b, c)
# in Gaussian integers satisfying  $a^2 + b^2 = ic^2$ 
# By T. Thongjunthug
# Last modified 19 Oct 2006, 23:40

```

```
restart:
```

```
# need GaussInt package for finding square root
```

```

with(GaussInt):

# seed: initial (non-trivial) triplet (a,b,c) = (1, 1, 1-i)
# note that a is fixed here
# Other seeds can be obtained from the previously generated ones.
# Say, if the process yields (a,b,c), then we can take (b,a,c)
# as a new seed
a:= 1:  b:= -1:  c:= 1-I:

# need to track c
C:= [c]:

# try a finite number of iterations
numItr:= 30:
for n from 1 to numItr do
  # show the current valid triple
  print(a, b, c);

  # calculate new c
  # proceed if c is new
  c:= -I*(c - (1-I)*b):
  if member(c, C) = true then
    printf("Process terminates - triplet repeated\n");
    break;
  end if;

  # 2 values of new b
  # since c is new, so are b's
  # and both define a separate triplet
  C:= [op(C), c]:
  tmp:= I*c^2 - a^2:

  # GUARD1: check whether tmp is a square
  if GIissqr(tmp) = false then
    printf("Process terminates - no further move possible\n");
    break;
  end;
  tmp:= GIsqrt(tmp):

  # only choose b so that a new iteration is not what we have before
  # this can be done by checking a new c

```

```

c1:= -I*(c - (1-I)*tmp):
c2:= -I*(c + (1-I)*tmp):

if member(c1, C) = true then
  if member(c2, C) = true then
    printf("Process terminates - triplet repeated\n");
    break;
  else
    b:= -tmp:
  end if;
else
  b:= tmp:
end if;

# GUARD2: verification - may be deleted later
valDif:= a^2 + b^2 -I*c^2:
if valDif <> 0 then
  printf("Verification failed. (a, b, c) is\n");
  print(a, b, c);
  printf("and a^2 + b^2 - I*c^2 = \n");
  print(valDif);
  break;
end if;
end do:

printf("-----\n");
printf("Remark: After experiment, starting with seeds\n");
printf("with the same a gives the same sets of triples,\n");
printf("up to some units\n");
printf("-----\n");

```

References

- [1] D. Abramovich. Formal finiteness and the uniform boundedness conjecture. *Astérisque*. 228:5–17, 1995.
- [2] A. Baker. The Diophantine equation $y^2 = ax^3 + bx^2 + cx + d$. *J. London Math. Soc.* 43:1–9, 1968.
- [3] Y. Bugeaud. On the size of integer solutions of elliptic equations. *Bull. Austral. Math. Soc.* 57:199–206, 1998.
- [4] B. J. Birch and H. P. F. Swinnerton-Dyer. Note on elliptic curves II. *J. Reine. Angew. Math.* 218:79–108, 1965.
- [5] A. Brumer. The average rank of elliptic curves I. With an appendix by O. McGuinness. *Invent. Math.* 109:445–472, 1992.
- [6] J. W. S. Cassels. On the equation $a^x - b^y = 1$. *Amer. J. Math.* 75(1): 159–162, January 1953.
- [7] J. Coates and A. Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.* 39:223–251, 1977.
- [8] J. E. Cremona. Elliptic curve data. Access on July 27, 2006.
<http://www.maths.nottingham.ac.uk/personal/jec/ftp/data/>.
- [9] J. T. Cross. Primitive Pythagorean triples of Gaussian integers. *Math. Mag.* 59(2):106–110, April 1986.
- [10] J. T. Cross. In the Gaussian integers, $\alpha^4 + \beta^4 \neq \gamma^4$. *Math. Mag.* 66(2):105–108, April 1993.
- [11] M. Davis, H. Putnam, and J. Robinson. The decision problem for exponential Diophantine equations. *Ann. of Math. (2)* 74:425–436, 1961.
- [12] K. A. Draziotis. Integer points on the curve $Y^2 = X^3 \pm p^k X$. *Math. Comp.* 75(255):1493–1505, July 2006.
- [13] N. D. Elkies. \mathbb{Z}^{28} in $E(\mathbb{Q})$, etc. in Number Theory Listserver and Archives, May 2006. Access on August 24, 2006.
<http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0605&L=nmbthrtry>.
- [14] J. Fernandez. Some data on torsion subgroups of elliptic curves. Access on April 9, 2006.
<http://www.math.utah.edu/~jfernand/elliptic/docs/torsion/torsion.pdf>.
- [15] M. Fouquet, P. Gaudry, and R. Harley. On Satoh’s algorithm and its implementation. *J. Ramanujan Math. Soc.* 15:281–318, 2000.
- [16] Y. Fujita. Torsion subgroups of elliptic curves in elementary abelian 2-extension of \mathbb{Q} . *J. Number Theory.* 114(1):124–134, September 2005.

- [17] J. R. Goldman. *The Queen of Mathematics: A Historically Motivated Guide to Number Theory*. A K Peters, Massachusetts, 1998.
- [18] H. Hasse. Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzetafunktionen in gewissen elliptischen Fällen. *Nachr. Ges. Wiss. Göttingen, Math.-Phys. K.* 253–262, 1933.
- [19] D. R. Heath-Brown. The average analytic rank of elliptic curves. *Duke Math. J.* 122(3):591–623, 2004.
- [20] D. E. Joyce. Hilbert’s mathematical problems. Access on September 9, 2006. <http://aleph0.clarku.edu/~djoyce/hilbert/toc.html>.
- [21] S. Kamienny and B. Mazur. Rational torsion of prime order in elliptic curves over number fields. With an appendix by A. Granville. *Astérisque*. 228:81–100, 1995.
- [22] M. A. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Math. J.* 109:125–149, 1988.
- [23] A. W. Knap. *Elliptic Curves*. Princeton University Press, New Jersey, 1992.
- [24] S. Lang. *Elliptic Curves: Diophantine Analysis*. Springer-Verlag, Berlin, 1978.
- [25] E. Lutz. Sur l’équation $y^2 = x^3 - Ax - B$ dans les corps p -adic. *J. Reine Angew. Math.* 177:431–466, 1937.
- [26] J. V. Matijasevič. The Diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR*. 191:279–282, 1970.
- [27] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.* 47:33–186, 1977.
- [28] J. F. Mestre. Construction d’une courbe elliptique de rang ≥ 12 . *C. R. Acad. Sc. Paris. Série I*, 295:643–644, December 1982.
- [29] L. J. Mordell. *Diophantine Equations*. Academic Press, London, 1969.
- [30] T. Nagell. Solution de quelque problemes dans la theorie arithmetique des cubiques planes du premier genre. *Wid. Akad. Skrifter Oslo I*. Nr.1, 1935.
- [31] M. Pfeifer. A boundedness theorem for the torsion of a class of elliptic curves over algebraic number fields. *Arch. Math.* 62(6):519–527, June 1994.
- [32] B. Poonen. *Hilbert’s Tenth Problem over Rings of Number-Theoretic Interest*. Note from the lecture at the Arizona Winter School on “Number Theory and Logic”, March 15–19, 2003.
- [33] H. E. Rose. *A Course in Number Theory*. Clarendon Press, Oxford, 1988.
- [34] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.* 15:247–270, 2000.
- [35] C. L. Siegel. Approximation algebraischer Zahlen. *Math. Zeitschrift*. 10:173–213, 1921.
- [36] C. L. Siegel. The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \dots + k$. *J. London Math. Soc.* 1:66–68, 1926.
- [37] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.

- [38] J. H. Silverman and J. Tate. *Rational Points on Elliptic Curves*. Springer-Verlag, New York, 1992.
- [39] N. P. Smart and N. M. Stephens. Integral points on elliptic curves over number fields. *Math. Proc. Camb. Phil. Soc.* 122(1):9–16, July 1997.
- [40] V. G. Sprindžuk. *Classical Diophantine Equations*. Lecture Notes in Mathematics vol. 1559, Springer-Verlag, Berlin, 1993.
- [41] J. Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. *Séminaire Bourbaki Exposé.* 306, 1966.
- [42] L. C. Washington. *Elliptic Curves: Number Theory and Cryptography*. Chapman & Hall/CRC, Florida, 2003.
- [43] A. Weil. Sur un théorème de Mordell. *Bull. Sci. Math.* 54:182–191, 1930.
- [44] C. Wittmann. Group structure of elliptic curves over finite fields. *J. Number Theory.* 88(2):335–344, June 2001.