RATIONAL POINTS ON ELLIPTIC CURVES

TAN TZE HENG

Abstract. The subject of elliptic curves is widely regarded in the mathematics community as a fascinating and actively researched topic that spans multiple branches of mathematics. This paper explores rational points of elliptic curves defined over the real and complex plane. Key results regarding the algebraic structures of rational points on elliptic curves, in particular the Mordell's theorem, are discussed, some of which are supplied with proofs. The applications of these results in the study of certain important mathematical problems are then presented.

This capstone project report is submitted in partial fulfilment of the requirements of the degree of Bachelor of Science (Honours) in Mathematics of the National University of Singapore.

Contents

1. Introduction 2
1.1. Defining an Elliptic Curve 2
1.2. Group Structure of Elliptic Curves 3
2. Analysing Real and Complex Points 7
2.1. Group of Real Points 8
2.2. Group of Complex Points 8
2.3. Torsion Points and Nagell-Lutz Theorem 15
3. Group of Rational Points is Finitely Generated 24
3.1. Height Function 25
3.2. Finiteness of $E(\mathbb{Q})/2E(\mathbb{Q})$ 29
3.3. Descent Theorem and Mordell's Theorem 33
3.4. Application of Mordell's Theorem 34
4. Conclusion 38
References 38

1. Introduction

The study of elliptic curves can be traced back to the era of ancient Greeks. Elliptic curves form a special case of Diophantine equations, which concern solutions of two-variable polynomial equations with integer coefficients. They also exhibit connection with the 'congruent number problem', which asks whether it is possible to find integers n such that n is the area of a right-angled triangle with rational side lengths. Elliptic curves also emerge in the study of elliptic integrals, which is initiated by mathematicians such as Euler when attempting to obtain a closed-form formula of the arc length of an ellipse. Despite its long history, modern research on elliptic curves remains active and spans multiple branches of mathematics, including abstract algebra, algebraic geometry, number theory, and complex analysis.

The discussion of the main subject in this paper is largely based on [ST15], which influences the choice and sequence of topics and results presented in this paper.

1.1. Defining an Elliptic Curve.

There are two main directions to define an elliptic curve. The first of the two arises from the study of *cubic curves*, which is defined as follows.

Definition 1.1. *A cubic curve is a collection of points in the real plane, $\mathbb{R}^2$, or in the complex plane, $\mathbb{C}^2$, that satisfies equations of the following general form,*

$$c_1y^3 + c_2xy^2 + c_3x^2y + c_4y^3 + c_5x^2 + c_6xy + c_7y^2 + c_8x + c_9y + c_{10} = 0.$$

If the coefficients c_i are rational, we call the resulting curve a rational cubic curve.

Using projective transformation, one can show that if a cubic curve C passes through a rational point, i.e. a point with rational numbers as coordinates, then it can be equivalently defined using a particular form of equation of cubic curves, called the *Weierstrass normal form*, which is a standard way of defining elliptic curves over familiar number fields like $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$.

Lemma 1.2. *A cubic curve that passes through a rational point has a birationally equivalent Weierstrass normal form given by*

$$y^2 = ax^3 + bx^2 + cx + d,$$

where a, b, c, d are rational coefficients.

Proof. See [Mat16]. □

The second way of defining an elliptic curve generalises from real or complex numbers to arbitrary fields and involves some concepts in algebraic geometry. This definition states that an elliptic curve is a smooth, algebraic, projective curve of genus one with a specific base point $\mathcal{O}$. See, for example, [Mil20, Chapter 2], for more details on such treatment of defining elliptic curves.

Throughout most of this paper, we restrict our attention to elliptic curves that are defined over the real or complex numbers with at least one rational point and no repeated roots (so that it is non-singular, see Definition 1.3) that admit the short Weierstrass form, $y^2 = x^3 + ax + b$, which is obtained through a linear change of variable from the Weierstrass normal form by $x = x' - \frac{a}{3}$.

1.2. **Group Structure of Elliptic Curves.** In this chapter, we discuss the key observations and methods that give rise to the group structure of the set of rational points on elliptic curves, denoted here as $E(\mathbb{Q})$. For relevant definitions, particularly of a group and a field, one may consult a textbook on abstract algebra, such as [DF03]. The discovery of such structure is helpful in answering a key question regarding the number of rational points on elliptic curves: are there finitely or infinitely many of them? If there are infinitely many such rational points, is there a way to classify them meaningfully?

If we equip a suitable binary operation, we can see that $E(\mathbb{Q})$ is an abelian group. This binary operation is known as *chord-tangent addition* and is denoted here by $+$. In fact, this binary operation does not only form an abelian group on $E(\mathbb{Q})$; the abelian group structure remains if we extend to $E(\mathbb{C})$, i.e. we allow the coordinates to be complex numbers. In other words, $E(\mathbb{Q})$ is a subgroup of $E(\mathbb{C})$. Although this binary operation mainly involves elementary geometric construction, it is not at all obvious that this gives us a commutative group; this discovery is the collective effort of mathematicians across generations, see [Bro00, Section 4] for a historical overview.

However, we cannot form an abelian group using + solely with the points in $E(\mathbb{Q})$ on the complex plane, as we lack the identity element, and the origin $(0, 0)$ does not necessarily lie in $E(\mathbb{Q})$. To resolve this, it is necessary to introduce an additional point of infinity, denoted here by $\mathcal{O}$, and consider it to be an element of $E(\mathbb{Q})$ as well. The existence of such an infinity point is due to the fact that an elliptic curve is an affine algebraic plane curve, which is the restriction of the projective plane curve C, defined in $\mathbb{P}^2(\mathbb{C})$, on a two-dimensional subspace of $\mathbb{C}^3$. In $\mathbb{P}^2(\mathbb{C})$, it is defined by the equation below, which is obtained by homogenising the original equation of the elliptic curve with the multiplication of the variable z of suitable powers:

$$C : y^2z = x^3 + axz^2 + bz^3.$$

Note that substituting $z = 1$ recovers the short Weierstrass form of the elliptic curve equation in $\mathbb{C}^2$. The addition of the third variable z is due to the definition of a projective plane in which a point on a projective plane (over complex numbers), $\mathbb{P}^2(\mathbb{C})$, is viewed as a certain equivalence class of points in $\mathbb{C}^3$. It follows that this curve C intersects the line at infinity, which is the line defined by points of intersection of parallel lines on the usual two-dimensional plane, at the point $[(0, 1, 0)]$ on $\mathbb{P}^2(\mathbb{C})$. This is the point we are taking as the point of infinity, and explains why the line connecting a point on an elliptic curve and the point of infinity on the usual complex plane is a vertical line passing through the said point. For a more detailed explanation of this treatment, see, for example, [Mil20, Chapter 1].

Introducing this point of infinity into the set of points on a non-singular elliptic curve does not affect its non-singular nature, as we see below:

Definition 1.3. *A projective plane curve C_f/k is a homogeneous polynomial $f(x, y, z)$ with coefficients in a field k. For any field K containing k, the K-rational points of C_f form the set*

$$C_f(K) = \{[(x, y, z)] \in \mathbb{P}^2(K) : f(x, y, z) = 0\}.$$

A point $P \in C_f(K)$ is singular if $\frac{\partial f}{\partial x}$, $\frac{\partial f}{\partial y}$ and $\frac{\partial f}{\partial z}$ all vanish at P.

Lemma 1.4. *Let C be a projective plane curve defined by the homogeneous equation*

$$C : y^2z = x^3 + axz^2 + bz^3,$$

then the point $[(0, 1, 0)]$ at infinity is a non-singular point of C.

Proof. Note that $\frac{\partial}{\partial z} f(x, y, z)$, where $f(x, y, z) = x^3 + axz^2 + bz^3 - y^2z$, evaluates to -1 at the point at infinity $[(0, 1, 0)]$. Since the partial derivatives of f do not all vanish at the point, it is a non-singular point of C. □

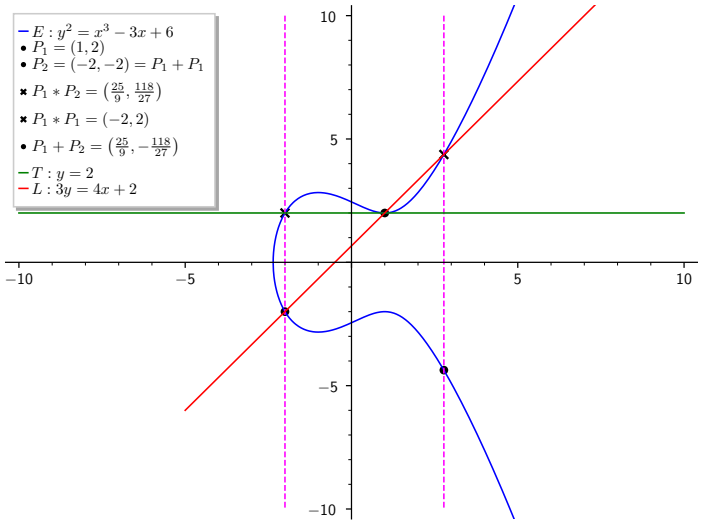

FIGURE 1. A plot that illustrates chord-tangent addition, produced using Sage [The24].

We outline the procedure of $+$ over $E(\mathbb{Q})$ as follows. Suppose that we have two rational points $P_1, P_2 \in E(\mathbb{Q})$. If we construct a straight line that passes through both of these points and obtain the third point of intersection, denoted by $P_1 * P_2$, between the line and the elliptic curve E, we define $P_1 + P_2$ to be the third point of intersection of the curve and the line connecting $P_1 * P_2$ and the point of infinity $\mathcal{O}$, which is equivalent to reflecting $P_1 * P_2$ on the x-axis. An illustration of this binary operation is given in Figure 1.

If one of the two rational points happens to be the point of infinity, that is we have $\mathcal{O}$ and another point $\mathcal{O} \neq P \in E(\mathbb{Q})$. We define $\mathcal{O} + P$ to be the point of intersection between the vertical line that passes through P and the elliptic curve.

If we only have one rational point, say, $P' \in E(\mathbb{Q})$, to start with, we construct a tangent line that passes through P' and define $P' + P' = 2P'$ to be the other point of intersection between the tangent line and the elliptic curve. If $P' = \mathcal{O}$, we define $\mathcal{O} + \mathcal{O}$ as the point of intersection between the vertical line that passes through $\mathcal{O}$ and the elliptic curve.

It is also worth noting that from the definition, if P_1, P_2, P_3 are points on an elliptic curve such that $P_1 + P_2 + P_3 = \mathcal{O}$, then P_1, P_2, P_3 are collinear.

Theorem 1.5 (See [ST15] for a discussion of this fact)**.** *The set of rational points on an elliptic curves, $E(\mathbb{Q})$, endowed with the binary operation $+$ as described in this section (1.2), forms an abelian group.*

Proof. Let P_1 and P_2 be rational points on an elliptic curve E with the equation in short Weierstrass form, i.e. $y^2 = x^3 + ax + b$, with a and b being rational. We first show that $P_1 + P_2$ is also a rational

point on E. By definition, we see that $P_1 + P_2$ must lie on E, so it suffices to show that it is rational. Observe that the procedure of $+$ requires the construction of the line connecting P_1 and P_2, which have rational coordinates, so this implies that the resulting line equation, say, $y = cx + d$, must have rational coefficients. Thus, since obtaining $P_1 + P_2$ amounts to solving $(cx + d)^2 = x^3 + ax + b \iff x^3 - c^2x^2 + (a - 2cd)x + (b - d^2) = 0$ for its x-coordinate, which is rational due to the fact that the sum of the x-coordinates of $P_1 + P_2$, P_1 and P_2 is given by c^2, a rational number, it follows that the y-coordinate of $P_1 + P_2$ must also be rational, thus $P_1 + P_2$ is rational, as desired.

Next, we show that the point of infinity $\mathcal{O}$ is the identity element, so that for any point P in $E(\mathbb{Q})$, we have that $\mathcal{O} + P = P + \mathcal{O} = P$. Note that both $\mathcal{O} + P$ and $P + \mathcal{O}$ are obtained by drawing a vertical line through P, identifying its third point of intersection (other than P and $\mathcal{O}$) with the curve, which is the reflection of P about the x-axis, and then obtaining the third point of intersection of the curve and the vertical line passing through the reflection (other than the reflection and $\mathcal{O}$), which is precisely P itself.

Next, we show the existence of the inverse element $-P$ of any point P in $E(\mathbb{Q})$, so that $P + (-P) = (-P) + P = \mathcal{O}$. In fact, we see that the point $-P$ is given by the reflection of the point P about the x-axis. The argument is then similar to the proof of the existence of the identity element, with the main difference being the initial two points to connect with a line are given by P and $-P$. We then see that the third point of intersection is $\mathcal{O}$, and the third point of intersection of the line connecting $\mathcal{O}$ and $\mathcal{O}$ and the curve is indeed still $\mathcal{O}$, as desired.

We leave the proof of associativity for the last here, as it is particularly more difficult compared to the proof of the other criteria. To show associativity, we apply the Bezout's theorem and the Cayley-Bacharach theorem, which is a consequence of the Bezout's theorem. The statement of both theorems are given below.

Theorem 1.6 (Bezout's theorem)**.** *If X is a projective plane curve defined by a polynomial of degree m, and Y is a projective plane curve defined by a polynomial of degree n, then the total number of points of intersections of X and Y, counted with their multiplicities, is mn.*

Proof of Theorem 1.6. See [Ha10]. □

From Theorem 1.6, we see that two cubic curves intersect at nine points. From this, one can obtain a result known as the Cayley-Bacharach theorem, as follows.

Theorem 1.7 (Cayley-Bacharach theorem)**.** *Let C, C_1 and C_2 be cubic curves. If C passes through eight of the nine points of intersections of C_1 and C_2, then C must pass through the ninth point of intersection.*

Proof of Theorem 1.7. See [Mil20, Chapter 1, Proposition 3.2]. □

Applying Theorems 1.6 and 1.7, one can obtain a geometric proof of the associativity of +; see [Ful08, Chapter 5.6, Proposition 4]. In fact, a sketch of this proof is also described in [ST15, pp. 13-15]. □

Now, with the group law established, we can derive explicit formulae for the binary operation +, which are useful in computing the addition of two points efficiently.

Fact 1.8 (Explicit formulae of group law)**.** *Let $P = (x, y)$ be a rational point on the elliptic curve $E : y^2 = x^3 + ax + b$ that is not the point at infinity, then its inverse $-P$ is equal to $(x, -y)$.*

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be distinct points on $E(\mathbb{Q})$, both of which are not the point at infinity. Let $y = \lambda x + \nu$ be the line connecting P_1 and P_2. Let $P_1 + P_2 = (x_3, -y_3)$, then the following hold:

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda x_3 + \nu.$$

For adding two equal points $P = (x, y)$ that are not the point at infinity, the following duplication formulae hold:

$$x\text{-coordinate of } P + P = \frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)}.$$

$$y\text{-coordinate of } P+P = \frac{x^6 + 5ax^4 + 20bx^3 - a^3 - 5a^2x^2 - 8b^2 - 4abx}{4\,(x^3 + ax + b)y}.$$

Proof. See [ST15, Section 1.4]. □

Example 1.9. *Let C be an elliptic curve defined by*

$$C : y^2 = x^3 + 17.$$

C has two rational points $Q_1 = (-2, 3)$ and $Q_2 = (2, 5)$. We use the explicit formulae to compute $Q_3 := Q_1 + Q_2$. Let $Q_3 = (x_3, -y_3)$.

Let $y = \lambda x + \nu$ be the line through Q_1 and Q_2, then $\lambda = \frac{5-3}{2+2} = \frac{1}{2}$ and $\nu = 4$.

From the explicit formulae, we then have that

$$x_3 = \lambda^2 - (-2) - 2 = \frac{1}{4}, \quad y_3 = \frac{1}{2} \cdot \frac{1}{4} + 4 = \frac{33}{8}.$$

Therefore, we find that

$$Q_3 = (x_3, -y_3) = \left(\frac{1}{4}, -\frac{33}{8}\right).$$

2. Analysing Real and Complex Points

In this section, we seek to explore the algebraic structure of complex points in an elliptic curve, denoted here as $E(\mathbb{C})$, and real points in an elliptic curve, denoted here as $E(\mathbb{R})$.

It is worth noting that since $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, we have the following chain of subgroups:

$$E(\mathbb{Q}) \subset E(\mathbb{R}) \subset E(\mathbb{C}).$$

2.1. **Group of Real Points.** The binary operation (group addition) on the group of real points $E(\mathbb{R})$ on an elliptic curve E is continuous. This implies that $E(\mathbb{R})$ is a compact one-dimensional Lie group, thus if $E(\mathbb{R})$ is connected, i.e. has only one connected component, which occurs when the corresponding elliptic curve has only one real root, then $E(\mathbb{R}) \simeq \{z \in \mathbb{C} : |z| = 1\} := \mathbb{T}$; in other words, $E(\mathbb{R})$ is isomorphic to the circle group.

If $E(\mathbb{R})$ has instead two connected components, which occurs when the corresponding elliptic curve has three real roots, then $E(\mathbb{R}) \simeq \mathbb{T} \oplus G$, where $G \simeq \mathbb{Z}/2\mathbb{Z}$, whose points correspond to the additional two real roots that lie on the part of the curve that gives rise to the second connected component.

2.2. **Group of Complex Points.** Now, we move on to the discussion of the algebraic structure of $E(\mathbb{C})$, the group of complex points on an elliptic curve E.

Without loss of generality (with a suitable change of variable), we focus on elliptic curves in the classic Weierstrass form, i.e. elliptic curves defined by the following equation:

$$y^2 = 4x^3 - g_2x - g_3,$$

where g_2 and g_3 are complex numbers.

Here, we assume that $4x^3 - g_2x - g_3$ has distinct roots, so that the resulting curve is non-singular. In the Weierstrass theory of elliptic functions, it can be shown that if we have complex numbers g_2 and g_3 such that the polynomial $4x^3 - g_2x - g_3$ has distinct roots, then we can obtain two complex numbers ω_1 and ω_2, which are known as periods, in the complex plane which are linearly independent over $\mathbb{R}$. For a proof of this fact, which is established by evaluating elliptic integrals, see [Tak23, Chapter 11].

This gives rise to the following interesting group consisting of the linear combinations of ω_1 and ω_2 over $\mathbb{Z}$:

$$L = \{n_1\omega_1 + n_2\omega_2 : n_1, n_2 \in \mathbb{Z}\}.$$

One can immediately see that L is a subgroup of the complex plane, and we call the points in L lattice points, due to the even, lattice-like distribution of such points over the complex plane. Although the choice of ω_1 and ω_2 that generate L is not unique, it turns out that the coefficients g_2 and g_3 uniquely determines L. Conversely, g_2 and g_3 can be uniquely determined via the following formulae:

$$g_2 = 60 \sum_{\substack{\omega \in L \\ \omega \neq 0}} \frac{1}{\omega^4}, \quad g_3 = 140 \sum_{\substack{\omega \in L \\ \omega \neq 0}} \frac{1}{\omega^6}.$$

The reason of the validity of these formulae, as well as the seemingly odd naming choice of the variables g_2 and g_3, will be explained in Fact 2.5.

We can then utilise L to define an elliptic function which is important in the study of complex analysis, and is called the Weierstrass $\wp$-function. This function satisfies a number of pleasant properties, and exhibits a fascinating connection with elliptic curves.

Definition 2.1. *A function $f : \mathbb{C} \to \mathbb{C}$ is called elliptic if it is meromorphic and doubly periodic, i.e. there exists two $\mathbb{R}$-linearly independent numbers $\omega_1, \omega_2 \in \mathbb{C}$ such that*

$$f(x + \omega_1) = f(x), \quad f(x + \omega_2) = f(x) \quad \text{for all } x \in \mathbb{C}.$$

Theorem 2.2 (cf. Exercise 2.3 in [ST15])**.** *Define the Weierstrass $\wp$-function $\wp : \mathbb{C} \to \mathbb{C}$ as follows:*

$$\wp(u) = \frac{1}{u^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left(\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2} \right).$$

$\wp$ satisfies the following:

(a) $\wp$ is absolutely and uniformly convergent on any compact subset of the complex u-plane that does not contain any of the points of L.

(b) $\wp$ is a meromorphic function with a double pole at each point of L and no other poles.

(c) $\wp$ is an even function, i.e. $\wp(-u) = \wp(u)$ for all $u \in \mathbb{C}$, whereas its derivative $\wp'$ is an odd function, i.e. $\wp'(-u) = -\wp'(u)$ for all $u \in \mathbb{C}$.

(d) $\wp$ and $\wp'$ are doubly periodic, i.e. they are periodic with respect to every point in L.

Due to (b) and (d), we see that $\wp$ is an elliptic function.

Proof.

(a) We state the following lemma which will be applied in the proof of this part.

Lemma 2.3. *Let L be the group of lattice points. The series*

$$\sum_{\substack{\omega \in L \\ \omega \neq 0}} \frac{1}{|\omega|^r}$$

converges if $r > 2$.

Proof. See [SS03, Lemma 9.1.5]. □

Let U be a compact subset of $\mathbb{C}$ that does not contain any lattice point, then U is bounded by some positive real constant B, so that $|u| \leqslant B$ for all $u \in U$. Let $u \in U$ and suppose that $|\omega| \geqslant 2B \geqslant 2|u|$. Note that we have

$$\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2} = \frac{\omega^2 - (u-\omega)^2}{(u-\omega)^2 \cdot \omega^2} = \frac{u(2\omega - u)}{(u-\omega)^2 \cdot \omega^2}.$$

Meanwhile, by the triangle inequality, we have the following bounds: $|2\omega - u| \leqslant \frac{5}{2}|\omega|$ and $|u - \omega| \geqslant |\omega| - |u| \geqslant \frac{1}{2}|\omega|$.

It follows that

$$\left|\frac{u(2\omega - u)}{(u-\omega)^2 \cdot \omega^2}\right| \leqslant \frac{\frac{5}{2}|\omega||u|}{\left(\frac{1}{2}|\omega|\right)^2 |\omega|^2} = \frac{10|u|}{|\omega|^3} \leqslant \frac{10B}{|\omega|^3}.$$

Therefore, for $u \in U$,

$$\begin{aligned}
&\wp(u) \\
&= \frac{1}{u^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0 \\ |\omega| < 2B}} \left(\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2}\right) + \sum_{\substack{\omega \in L \\ \omega \neq 0 \\ |\omega| \geqslant 2B}} \left(\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2}\right) \\
&\leqslant \frac{1}{u^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0 \\ |\omega| < 2B}} \left(\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2}\right) + \sum_{\substack{\omega \in L \\ \omega \neq 0 \\ |\omega| \geqslant 2B}} \left(\frac{10B}{|\omega|^3}\right).
\end{aligned}$$

Due to Lemma 2.3, as well as the fact that U is bounded and the rate of convergence does not depend on the choice of $u \in U$, it follows that $\wp$ converges absolutely and uniformly on U.

(b) From part (a), we see that on the closed disk $\{u \in \mathbb{C} : |u| \leqslant B\}$, the sum $\sum_{\substack{\omega \in L \\ \omega \neq 0 \\ |\omega| \geqslant 2B}} \left(\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2}\right)$ converges uniformly to an analytic function, whereas the sum $\sum_{\substack{\omega \in L \\ \omega \neq 0 \\ |\omega| < 2B}} \left(\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2}\right)$ is meromorphic with a double pole at $\omega \in L$ and no other poles (since the sum has order two), as long as $|\omega| < 2B$. Since the choice of B is arbitrary, it follows that $\wp$ is meromorphic on $\mathbb{C}$ with a double pole at each point of L and no other poles.

(c) Since $\wp$ is defined in terms of sums of reciprocals of terms with even powers, and in particular the summation of $1/(u-\omega)^2$ across $\omega \in L$ is symmetric, i.e. if $1/(u-\omega)^2$ is present in the sum then so does $1/(-u+\omega)^2$, it follows that $\wp$ is an even function as desired. Due to the absolute and uniform convergence of $\wp$ established in (a), we can obtain the derivative $\wp'$ of $\wp$ via term-by-term differentiation, so that

$$\wp'(u) = -\frac{2}{u^3} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left(-\frac{2}{(u-\omega)^3}\right) = \sum_{\omega \in L} \frac{-2}{(u-\omega)^3}. \tag{1}$$

Note that the series expansion (1) of $\wp'$ exhibits a similar symmetric nature as seen in $\wp$, and each term in the series is an odd function, so $\wp'$ is an odd function.

(d) We need to show that for all $u \in \mathbb{C}$ and $\omega \in L$, we have that

$$\wp(u + \omega) = \wp(u), \quad \wp'(u + \omega) = \wp'(u).$$

The double periodicity of $\wp'$ is straightforward from (1), as the summation in (1) ranges over all $\omega \in L$. Integrating both sides with respect to u yields $\wp(u+\omega) = \wp(u)+C(\omega)$, where $C(\omega) \in \mathbb{C}$ does not depend on u. Setting $u = -\omega/2$, we see that $C(\omega) \equiv 0$ since we know from (c) that $\wp$ is even. Thus, $\wp$ is doubly periodic as desired. □

Definition 2.4. *Let L be the group of lattice points with periods ω_1, ω_2. We define a period parallelogram for L to be any set of the form*

$$\mathcal{F}_\alpha = \{\alpha + t_1\omega_1 + t_2\omega_2 : \alpha \in \mathbb{C},\ t_1, t_2 \in [0,1)\}.$$

From Definition 2.4, we see that we can identify the points in $\mathcal{F}_\alpha$ with the points in the quotient group $\mathbb{C}/L$, viewing a point in $\mathcal{F}_\alpha$ as a representative of a point in $\mathbb{C}/L$; in this regard, the period parallelogram with $\alpha = 0$ is usually used. Where convenient, we may refer to the period parallelogram directly as $\mathbb{C}/L$.

Fact 2.5. *Let $E(\mathbb{C})$ be the group of complex points on an elliptic curve E defined by the equation $y^2 = 4x^3 - g_2x - g_3$. Define a mapping $P : \mathbb{C} \to E(\mathbb{C})$ given by*

$$P(u) = \begin{cases} (\wp(u), \wp'(u)) & \text{if } x \notin L, \\ \mathcal{O}, & \text{if } x \in L. \end{cases}$$

This map is well-defined and satisfies the following:

(a) P is a homomorphism, i.e. $P(u+v) = P(u) + P(v)$, where $u, v \in \mathbb{C}$. The kernel of P is L.

(b) P is surjective but not injective. However, the restriction $P|_{\mathbb{C}/L}$ of P to the period parallelogram $\mathbb{C}/L$ is injective. Hence, $P|_{\mathbb{C}/L}$ is a group isomorphism.

Proof. To show that the map P is well-defined, it suffices to show that for all $u \in \mathbb{C}$, the following differential equation holds:

$$\wp'(u)^2 = 4\wp(u)^3 - g_2\wp(u) - g_3.$$

The following proof can also be found in [SS03, Theorem 9.2.2]. We reproduce the proof here with added explanations where appropriate.

We start from the definition of $\wp$ and investigate its Laurent expansion near $u = 0$. The geometric series formula implies that

$$\frac{1}{u-\omega} = -\frac{1}{\omega}\left(\frac{1}{1-\frac{u}{\omega}}\right) = -\frac{1}{\omega}\sum_{k=0}^{\infty}\left(\frac{u}{\omega}\right)^k, \quad \text{for } \left|\frac{u}{\omega}\right| < 1. \tag{2}$$

Differentiating with respect to u on both sides of (2) before taking negatives yields

$$\frac{1}{(u-\omega)^2} = \frac{1}{\omega^2}\sum_{k=0}^{\infty}(k+1)\left(\frac{u}{\omega}\right)^k = \frac{1}{\omega^2} + \frac{1}{\omega^2}\sum_{k=1}^{\infty}(k+1)\left(\frac{u}{\omega}\right)^k. \tag{3}$$

Equation (3) implies that when u is close to 0, we have that

$$\begin{aligned}\wp(u) &= \frac{1}{u^2} + \sum_{\substack{\omega\in L\\ \omega\neq 0}} \frac{1}{\omega^2}\sum_{k=1}^{\infty}(k+1)\left(\frac{u}{\omega}\right)^k \\ &= \frac{1}{u^2} + \sum_{k=1}^{\infty}(k+1)\left(\sum_{\substack{\omega\in L\\ \omega\neq 0}} \frac{1}{\omega^{k+2}}\right)u^k \\ &= \frac{1}{u^2} + \sum_{k=1}^{\infty}(k+1)E_{k+2}u^k \\ &= \frac{1}{u^2} + \sum_{j=1}^{\infty}(2j+1)E_{2j+2}u^{2j}\end{aligned}$$

Here, $E_k := \sum_{\substack{\omega\in L\\ \omega\neq 0}} \frac{1}{\omega^k}$ denotes the Eisenstein series of order k and note that $E_{k+2} \equiv 0$ whenever k is odd due to symmetry: if $n\omega_1 + m\omega_2 \in L$ for some integers n and m, then $-n\omega_1 - m\omega_2 \in L$ as well.

It follows that

$$\wp'(u) = -\frac{2}{u^3} + \sum_{k=1}^{\infty}(2k)(2k+1)E_{2k+2}u^{2k-1}.$$

We can then obtain the following three expansions for u near 0:

$$\wp'(u) = -\frac{2}{u^3} + 6E_4u + 20E_6u^3 + 42E_8u^5 + \cdots,$$

$$\wp'(u)^2 = \frac{4}{u^6} - \frac{24E_4}{u^2} - 80E_6 + \cdots,$$

$$\wp(u)^3 = \frac{1}{u^6} + \frac{9E_4}{u^2} + 15E_6 + \cdots$$

After some manipulations, one can find that

$$\wp'(u)^2 - 4\wp(u)^3 + 60E_4\wp(u) + 140E_6$$

is holomorphic near zero and is equal to zero at the origin. Since as a $\mathbb{Z}$-linear combination of doubly periodic functions $\wp$ and $\wp'$, it is also doubly periodic, it follows that it is constant due to its consequent boundedness and Liouville's theorem, thus $\wp'(u)^2 = 4\wp(u)^3 - 60E_4\wp(u) - 140E_6$ for all $u \in \mathbb{C}$. The desired result then follows by setting $g_2 = 60E_4$ and $g_3 = 140E_6$, as previously alluded. This also explains the choice of variables g_2 and g_3 when one considers the alternative notation $G_k := E_{2k}$ for Eisenstein series of even order.

Part (a) can be proved in several manners. For a proof that applies some results in complex analysis without delving too deep into algebraic number theory, see [Sut23, Theorem 15.1]. Alternative proofs that involve more algebraic number theory include [Hus03, Theorem 4.3] and [Sil09, Proposition VI.3.6]. The kernel of P is immediate from the definition.

For part (b), since $\wp$ has a double pole at all points in the group of lattice points L and no other poles, it follows that $\wp$ has order two. Let $(x_0, y_0) \in E(\mathbb{C})$ and define $f(u) = \wp(u) - x_0$. It follows by [SS03, Theorem 9.1.4] that f has two roots in $\mathbb{C}/L$. Neither of such roots is 0, since f has a pole at 0. Let $u_0 \neq 0$ be one of such roots. This implies that $P(u_0) = (x_0, \pm y_0)$, thus $(x_0, y_0) = P(\pm u_0)$, implying that $P : \mathbb{C} \to E(\mathbb{C})$ is surjective, but, due to the double periodicity of $\wp$ as well, not injective.

To prove that $P|_{\mathbb{C}/L}$ is injective, we need to show that if $\wp(u_1) = \wp(u_2) \mod L$, then $u_1 = u_2 \mod L$, where $u_1, u_2 \in \mathbb{C}$. Note that $u_1 = u_2 \mod L$ if and only if $u_1 - u_2 \in L$. By part (a), this implies that $\wp(u_1) - \wp(u_2) = \mathcal{O} \implies \wp(u_1) = \wp(u_2)$. □

Corollary 2.6. *The addition formulae for the Weierstrass $\wp$-function are given as follows:*

$$\wp(u+v) = -\wp(u) - \wp(v) + \frac{1}{4}\left[\frac{\wp'(v) - \wp'(u)}{\wp(v) - \wp(u)}\right]^2,$$

$$\wp(2u) = -2\wp(u) + \frac{1}{4}\left(\frac{\wp''(u)}{\wp'(u)}\right)^2,$$

where $\wp''(u) = 6\wp(u)^2 - \frac{1}{2}g_2$.

Proof. From Fact 2.5, we know that $\wp'(u)^2 = 4\wp(u)^3 - g_2\wp(u) - g_3$ for all $u \in \mathbb{C}$. Differentiating both sides with respect to u yields $2\wp'(u)\wp''(u) = 12\wp(u)^2\wp'(u) - g_2\wp'(u) \implies \wp''(u) = 6\wp(u)^2 - g_2$, applying the fact that $\wp'(u) \neq 0$ for all $u \in \mathbb{C}$ due to (1).

Let $y = \lambda x + \nu$ be the line passing through the points $P_u = (\wp(u), \wp'(u))$ and $P_v = (\wp(v), \wp'(v))$, obtained from the mapping P described in Fact 2.5. We know from Fact 2.5 as well that these two points lie on the elliptic curve $y^2 = x^3 - 4g_2x - 16g_3$ and the point $P_u + P_v = (\wp(u+v), \wp'(u+v))$ also lies on the curve. It follows that

$$\lambda = \frac{\wp'(v) - \wp'(u)}{\wp(v) - \wp(u)}.$$

Substituting $y = \lambda x + \nu$ into the elliptic curve equation which gives

$$(\lambda x + \nu)^2 = 4x^3 - g_2x - g_3,$$

it follows by Vieta's formula that

$$\wp(u+v) + \wp(u) + \wp(v) = \frac{\lambda^2}{4}$$

$$\implies \wp(u+v) = -\wp(u) - \wp(v) + \frac{1}{4}\left[\frac{\wp'(v) - \wp'(u)}{\wp(v) - \wp(u)}\right]^2.$$

The addition formula for $\wp(2u)$ is then derived from that of $\wp(u+v)$ by observing that

$$\frac{\wp'(v)-\wp'(u)}{\wp(v)-\wp(u)} = \frac{\wp'(v)-\wp'(u)}{v-u} \cdot \frac{v-u}{\wp(v)-\wp(u)},$$

and taking limits on both sides such that $v \to u$, which yields $\wp''(u)/\wp'(u)$. □

The significance of Fact 2.5 is that it tells us the algebraic structure of the group of complex points $E(\mathbb{C})$ on an elliptic curve, i.e. it is isomorphic to the quotient group $\mathbb{C}/L$. In other words, $E(\mathbb{C})$ is isomorphic to the complex torus, or the direct product $\mathbb{T} \times \mathbb{T}$ of two circle groups. This is a special case of the Abel-Jacobi theorem. In fact, the mapping P in Fact 2.5 is the inverse of the Abel-Jacobi map that comes from said theorem. For more details, see [Tak23, Chapter 10].

Before we move on to the next section, it would be remiss if we do not mention some other interesting facts about the Weierstrass $\wp$-function. In particular, Lemma 2.7 gives us a clear picture of what the points in $E(\mathbb{C})$ of order two are, with reasons that will be clearer when we discuss the Nagell-Lutz theorem in the next section.

Lemma 2.7. *Let $\wp$ and $\wp'$ be the Weierstrass $\wp$-function with double periods ω_1 and ω_2 and its derivative respectively, then the following hold:*

(a) $\wp'(\omega_i/2) = 0$, where $i = 1, 2, 3$ with $\omega_3 := \omega_1 + \omega_2$.

(b) Let $e_i = \wp(\omega_i/2)$, where $i = 1, 2, 3$ with $\omega_3 = \omega_1 + \omega_2$, then

$$e_1 + e_2 + e_3 = 0,$$

$$e_1e_2 + e_2e_3 + e_3e_1 = -\frac{g_2}{4},$$

$$e_1e_2e_3 = \frac{g_3}{4}.$$

(c) The e_i's ($i = 1, 2, 3$) defined in (b) are distinct from each other.

Proof.

(a) From Theorem 2.2, we know that $\wp'$ is an odd function with periods ω_1, ω_2 and $\omega_3 = \omega_1+\omega_2$. This implies that for $i = 1, 2, 3$, we have

$$\begin{aligned} &\wp'(\omega_i/2) = -\wp'(-\omega_i/2) = -\wp'(\omega_i/2) \\ \implies\ &2\wp'(\omega_i/2) = 0 \implies \wp'(\omega_i/2) = 0. \end{aligned}$$

(b) By part (a) and Fact 2.5, it follows that the equation $4x^3 - g_2x - g_3 = 0 \iff x^3 - \frac{g_2}{4} - \frac{g_3}{4} = 0$ has three roots at $\wp(\omega_i/2) = e_i$, where $i = 1, 2, 3$. The desired result then follows from Vieta's formula.

(c) Since $\wp$ has order two, the equation $\wp(u) - e_i$, where $i = 1, 2, 3$, has two roots with multiplicity in $\mathbb{C}/L$. Note that by part (a), the equation $\wp(u) - e_i$ has a double root at $u = \omega_i$. If each e_i is not distinct from each other, then $\wp$ would have at least four roots in $\mathbb{C}/L$, contradicting the fact that $\wp$ has order two, thus each e_i must be distinct. □

Remark 2.8. *Lemma 2.7 implies two key results:*

(1) We can construct a non-singular elliptic curve using the Weierstrass $\wp$-function as the starting point.
(2) The complex numbers $\omega_1/2$, $\omega_2/2$ and $(\omega_1 + \omega_2)/2$ give us the three remaining points of order two in $E(\mathbb{C})$ other than $\mathcal{O}$.

2.3. **Torsion Points and Nagell-Lutz Theorem.** A torsion point P of an abelian group is a point that has finite order, i.e. there exists a positive integer m such that $mP = e$, where e denotes the identity element; in the case of the group of rational points $E(\mathbb{Q})$ on an elliptic curve E, we have that $e = \mathcal{O}$. The subgroup that consists of only torsion points is then known as the torsion subgroup. In this section, we investigate the structures of the torsion subgroup in $E(\mathbb{R})$, $E(\mathbb{C})$, and finally $E(\mathbb{Q})$, in which case the Nagell-Lutz theorem is introduced.

The torsion subgroup in $E(\mathbb{R})$ exhibits the following algebraic structure: since $E(\mathbb{R})$ is isomorphic to the circle group, it follows that the torsion subgroup containing points of order dividing a positive integer m is a cyclic group of order m that is isomorphic to the group of m-th roots of unity.

As for the torsion subgroup in $E(\mathbb{C})$, to obtain complex points of order dividing m, it follows from applying the map P described in Fact 2.5 that it suffices to determine complex numbers $u \in \mathbb{C}/L$ such that $mu \in L$. It turns out that there are m^2 of them (since L is in some sense two-dimensional), so the group of complex points of order dividing m has order m^2, and is a direct product of two cyclic groups of order m.

Now, one may wonder why in the previous section, we can conclude that the numbers $\omega_1/2$, $\omega_2/2$ and $(\omega_1 + \omega_2)/2$ correspond to points of order two in $E(\mathbb{C})$. We provide the reason by presenting the following key result regarding points of order two and three on an elliptic curve.

Theorem 2.9 (cf. Theorem 2.1 and Exercise 2.2 in [ST15])**.** *Let E be a non-singular elliptic curve defined by*

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c.$$

(a) A point $P = (x, y) \neq \mathcal{O}$ on E has order two if and only if $y = 0$, or equivalently, P
(b) The curve E has exactly four points of order dividing two. These four points form a group that is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(c) *A point $P = (x, y) \neq \mathcal{O}$ on E has order three if and only if x is a root of the polynomial*

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2.$$

(d) *The curve E has exactly nine points of order dividing three. These nine points form a group that is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.*

(e) *$P = (x, y) \in E$ is a point of order three if and only if $P \neq \mathcal{O}$ and P is a point of inflection on the curve E.*

Proof.

(a) If $P = (x, y) \neq \mathcal{O}$ has order two, then $2P = \mathcal{O} \iff P = -P \iff (x, y) = (x, -y) \iff y = 0$.

(b) From (a), it suffices to determine points on E with $y = 0$. These are exactly the points $(\alpha_i, 0)$, where α_i, $i = 1, 2, 3$ are the three complex roots of the cubic polynomial that defines E. Together with $\mathcal{O}$, they form a subgroup with four elements, and since each of them has order either one or two, this subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(c) The point $P = (x, y) \neq \mathcal{O}$ has order three if and only if $2P = -P$. Note that by the duplication formula, we have that

$$x\text{-coordinate of } 2P = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4(x^3 + ax^2 + bx + c)},$$

whereas the x-coordinate of $-P$ is still x. Equating the two and simplifying yields $3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2 = 0$. This implies that P has order three if and only if the x-coordinate is a root of ψ_3.

(d) By the explicit formulae of the group law, we have that

$$x\text{-coordinate of } 2P = \frac{f'(x)^2}{4f(x)} - a - 2x.$$

Equating this with x and performing the simplification procedure that is similar to how we derive ψ_3 in part (c) yields

$$(12x + 4a)f(x) - f'(x)^2 = 0.$$

Since $f''(x) = 6x + 2a$, it follows that ψ_3 has an alternative expression given by

$$\psi_3(x) = 2f(x)f''(x) - f'(x)^2.$$

We claim that ψ_3 has four distinct complex roots. To verify the claim, it suffices to check that $\psi_3(x)$ and $\psi_3'(x)$ have no common roots. Note that

$$\psi_3'(x) = 2f(x)f'''(x) = 12f(x),$$

thus a common root of $\psi_3(x)$ and $\psi_3'(x)$ would be a common root of

$$2f(x)f''(x) - f'(x)^2 \quad \text{and} \quad 12f(x).$$

This would give us a common root of $f(x)$ and $f'(x)$, contradicting the assumption that E is non-singular, and this proves the claim.

Let $\beta_1, \beta_2, \beta_3, \beta_4$ be the four complex roots of $\psi_3(x)$, and for each β_i, let δ_i be one of the square roots of $f(\beta_i)$. From (c), it follows that the set

$$\{(\beta_i, \pm\delta_i) : i = 1, 2, 3, 4\}$$

is the complete set of points of order three on E. In addition, since none of the δ_i's can be zero, as it would give a point of order two instead of three, it follows that this set gives us eight distinct points, so E contains eight points of order three. The only other point on E with order dividing three is the point of order one, namely $\mathcal{O}$, so E has exactly nine points of order dividing three.

Finally, every abelian group with nine elements such that each element has order dividing three is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

(e) We provide an analytic proof of this statement. Specifically, it suffices to show that

$$\frac{d^2y}{dx^2} = \frac{2f''(x)f(x) - f'(x)^2}{4yf(x)} = \frac{\psi_3(x)}{4yf(x)}. \tag{*}$$

Performing implicit differentiation twice on both sides of $y^2 = f(x)$ with respect to x gives us

$$2y\frac{d^2y}{dx^2} + 2\left(\frac{dy}{dx}\right)^2 = f''(x).$$

Substituting $\dfrac{dy}{dx} = \dfrac{f'(x)}{2y}$ yields

$$2y\frac{d^2y}{dx^2} + \frac{f'(x)^2}{2y} = f''(x)$$

$$\implies \frac{d^2y}{dx^2} = \frac{f''(x)}{2y} - \frac{f'(x)}{4y^2}.$$

Substituting $y^2 = f(x)$ and simplifying further, we have that

$$\frac{d^2y}{dx^2} = \frac{2f''(x)f(x) - f'(x)^2}{4yf(x)} = \frac{\psi_3(x)}{4yf(x)}$$

as desired.

Now, by part (c), a point $P = (x_0, y_0) \in E$ has order three if and only if $P \neq \mathcal{O}$ and is such that x_0 is a root of the polynomial

$\psi_3(x)$, thus by substituting x_0 to (*), it follows that $\dfrac{d^2y}{dx^2} = 0$, which happens if and only if P is an inflection point (in the algebraic geometry sense). □

Remark 2.10. *The polynomial ψ_3 described in Theorem 2.9 belongs to a special family of polynomials known as division polynomials, which are used to calculate multiples of points on an elliptic curve. For more details, see [Sil09, Exercise 3.7].*

Remark 2.11. *Let us briefly return to the context in Remark 2.8. We know that the numbers $\omega_1/2$, $\omega_2/2$ and $(\omega_1 + \omega_2)/2$ are sent via the mapping P as described in Fact 2.5 to points in $E(\mathbb{C})$ such that the y-coordinates are zero, due to Lemma 2.7. Therefore, by Theorem 2.9, they correspond to points of order two on $E(\mathbb{C})$.*

Now, we introduce the notion of p-adic numbers and p-adic topology, defined on the rational numbers. This is helpful in proving a part of the statement of the Nagell-Lutz Theorem, specifically the part that asserts that rational points of finite order have integer coordinates, considering that integers are essentially rational numbers with denominator 1, and 1 is not divisible by p for any prime p.

We first establish the definitions. Let r be a non-zero rational number, then due to the Fundamental Theorem of Arithmetic, r can be uniquely expressed in the form $\dfrac{m}{n}p^\nu$, where m and n are integers that are prime to p, $n \geqslant 1$ and the fraction m/n is in its simplest form. In other words, we fix a prime p and 'extract' the maximum possible power of p from the numerator and denominator of the initial expression of r.

Based on the unique expression as discussed above, we then define the *order* of r as $\operatorname{ord}(r) = \nu$. If $r = 0$, we then define $\operatorname{ord}(0) = \infty$.

It is not difficult to show that ord is a discrete valuation. In fact, ord is also called the p-adic valuation.

Definition 2.12. *A discrete valuation on a field K is a function $v : K^* \to \mathbb{Z}$ such that*

(a) v is surjective.
(b) $v(xy) = v(x) + v(y)$ for all $x, y \in K^*$.
(c) $v(x + y) \geqslant \min\{v(x), v(y)\}$ for all $x, y \in K^*$ with $x + y \neq 0$.

Fact 2.13 (cf. Exercise 2.6 in [ST15])**.** ord *is a discrete valuation defined on $\mathbb{Q}^* = \mathbb{Q} - \{0\}$. Moreover, if $\operatorname{ord}(r_1) \neq \operatorname{ord}(r_2)$, where $r_1, r_2 \in \mathbb{Q}$, then $\operatorname{ord}(r_1 + r_2) = \min\{\operatorname{ord}(r_1), \operatorname{ord}(r_2)\}$.*

Proof. The surjectivity of ord is straightforward, as $\mathbb{Q} \supset \mathbb{Z}$ and $\operatorname{ord}(x) = x$ for all $x \in \mathbb{Z}$.

Now, let $r_1, r_2 \in \mathbb{Q}$ and $r_1 = \frac{m_1}{n_1}p^{\nu_1}$ and $r_2 = \frac{m_2}{n_2}p^{\nu_2}$ where p is a prime, with $\frac{m_1}{n_1}$ and $\frac{m_2}{n_2}$ not containing p as a factor. It follows that $\operatorname{ord}(r_1 r_2) = \nu_1\nu_2 = \operatorname{ord}(r_1)\operatorname{ord}(r_2)$. Next, we have that $r_1 + r_2 =$

$p^\nu \left(\frac{m_1}{n_1} p^{\nu_1-\nu} + \frac{m_2}{n_2} p^{\nu_2-\nu}\right)$, where $\nu = \min\{\nu_1, \nu_2\}$, so that exactly one of $\nu_1 - \nu$ and $\nu_2 - \nu$ is zero if $r_1 \neq r_2$, implying that $\operatorname{ord}(r_1 + r_2) = \min\{\operatorname{ord}(r_1), \operatorname{ord}(r_2)\}$, or both of $\nu_1 - \nu$ and $\nu_2 - \nu$ are zero if $r_1 = r_2$, but $\frac{m_1}{n_1} + \frac{m_2}{n_2}$ may contain some power of p as a factor, implying that $\operatorname{ord}(r_1 + r_2) \geqslant \min\{\operatorname{ord}(r_1), \operatorname{ord}(r_2)\}$. □

We can then define a norm and subsequently a topology in terms of p-adic numbers based on ord.

Definition 2.14. *Let r be a rational number and p a prime. The p-adic norm, $\|r\|_p$, of r, is defined as follows:*

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

where ord *represents the order of r (as previously discussed). This induces the p-adic metric, denoted here as d_p, in the standard way, i.e. $d_p(x, y) = \|x - y\|$, where x and y are rational numbers.*

The topology induced by the p-adic metric is then called the p-adic topology.

Lemma 2.15 (cf. Exercise 2.6 in [ST15])**.** *The p-adic norm $\|\cdot\|_p$ satisfies the following properties:*

(i) $\|\cdot\|_p$ is positive-definite, i.e. if r is a rational number, then $\|r\|_p \geqslant 0$, and $\|r\|_p = 0$ if and only if $r = 0$.
(ii) $\|r_1 r_2\|_p = \|r_1\|_p \cdot \|r_2\|_p$, where r_1, r_2 are rational numbers.
(iii) $\|\cdot\|_p$ satisfies the strong triangle inequality, i.e. if r_1, r_2 are rational numbers, then $\|r_1 + r_2\|_p \leqslant \max\{\|r_1\|_p, \|r_2\|_p\}$.

Proof.

(i) This is straightforward from the definition.
(ii) Let r_1, r_2 be rational numbers. If at least one of them is zero, then we are done. Suppose that both of them are nonzero, then the result follows by Fact 2.13.
(iii) Let r_1, r_2 be rational numbers, then by Fact 2.13, we have $\|r_1 + r_2\|_p = \frac{1}{p^{\operatorname{ord}(r_1+r_2)}} \leqslant \frac{1}{p^{\min\{\operatorname{ord}(r_1), \operatorname{ord}(r_2)\}}} = \max\{\|r_1\|_p, \|r_2\|_p\}$. □

Definition 2.16. *Let p be a prime and ν a positive integer. We define $E(p^\nu)$ to be the set of rational points (x, y) of an elliptic curve E such that $p^{2\nu}$ divides the denominator of x and $p^{3\nu}$ divides the denominator of y. In other words,*

$$E(p^\nu) = \{(x, y) \in E(\mathbb{Q}) : \operatorname{ord}(x) \leqslant -2\nu \text{ and } \operatorname{ord}(y) \leqslant -3\nu\}.$$

The motivation of Definition 2.16 comes from the fact that if $P = (x, y)$ is a point on the elliptic curve $y^2 = x^3 + ax^2 + bx + c$, then we can write

$$x = \frac{m}{e^2} \quad \text{and} \quad y = \frac{n}{e^3},$$

where m, n and e are integers with $e > 0$ and $\gcd(m, e) = \gcd(n, e) = 1$. A derivation of this fact can be found in [ST15, pp. 48-49] or [ST15, pp. 71-72].

Definition 2.17. *Define the subring R_p of the field of rational numbers as the set of all rational numbers such that the denominator of each of them does not have p in its prime factorisation. Equivalently,*

$$R_p = \{\alpha \in \mathbb{Q} : \operatorname{ord}(\alpha) \geqslant 0\} = \{x \in \mathbb{Q} : \|x\|_p \leqslant 1\}.$$

If the choice of p is clear or does not matter, we simply denote the subring as R.

More formally, R is a discrete valuation ring for the rationals with respect to the discrete valuation ord. This type of ring is helpful for our purpose as it is a unique factorisation domain with exactly one maximal ideal; for the case of R, the maximal ideal is the one generated by p. We also see that R is analogous to a closed disk centred at the origin on a complex plane, but with respect to the p-adic topology.

For more details on the topic of discrete valuation rings, one may consult [DF03, Chapter 16].

Lemma 2.18 (Proposition 2.3 in [ST15])**.** *Let p be a prime, let R be the ring of rational numbers with denominator prime to p, and let $E(p^\nu)$ be the set of rational points (x, y) on E for which x has denominator divisible by $p^{2\nu}$, together with the point $\mathcal{O}$, then the following hold:*

(a) $E(p)$ consists of all rational points (x, y) for which the denominator of either x or y is divisible by p.
(b) For every $\nu \geqslant 1$, the set $E(p^\nu)$ is a subgroup of the group of rational points $E(\mathbb{Q})$.
(c) The map $t : E(p^\nu)/E(p^{3\nu}) \to p^\nu R/p^{3\nu}R$ defined by

$$P = (x, y) \mapsto t(P) = \frac{x}{y}, \quad t(\mathcal{O}) = 0$$

is an injective homomorphism.

Proof. See [ST15, pp. 48-54]. □

Note that Lemma 2.18 gives rise to the descending chain of subgroups of $E(\mathbb{Q})$ as follows:

$$E(\mathbb{Q}) \supset E(p) \supset E(p^2) \supset E(p^3) \supset \cdots$$

In fact, we can see from Definition 2.16 that each of the subgroups $E(p^\nu)$ is a neighbourhood of the point of infinity $\mathcal{O}$ with respect to the p-adic topology. This descending chain is useful later in proving that the only point of finite order in $E(p)$ for each prime p is $\mathcal{O}$ itself, by applying a technique known as proof by infinite descent. For a glimpse of the utility of this method, see [Con07].

Corollary 2.19 (Corollary 2.4 in [ST15])**.**

(a) *For every prime p, the only point of finite order in the group $E(p)$ is the point of infinity $\mathcal{O}$.*
(b) *Let $P = (x, y) \in E(\mathbb{Q})$ be a rational point of finite order, then x and y are integers.*

Proof.

(a) We prove this statement by descent. Let $P \in E(\mathbb{Q})$ be a point of order m with $m \geqslant 2$. Let p be any prime. We need to show that $P \notin E(p)$.

Assume that the point $P \in E(p)$, then P may be contained in $E(p^\nu)$ for some $\nu > 0$. We separate the proof into two cases based on whether p divides the order m.

Case I: $p \nmid m$. By Lemma 2.18, it follows that

$$t(mP) \equiv mt(P) \mod p^{3\nu}R.$$

Since $mP = \mathcal{O}$, we have that $t(mP) = 0$. Meanwhile, since m is prime to p, it is a unit in R. Thus,

$$0 \equiv t(P) \mod p^{3\nu}R,$$

which implies that $P \in E(p^{3\nu})$. However, note that this process can be repeated infinitely many times, implying that $P \in E(p^\mu)$ where $\mu > 0$ is arbitrarily large. In other words, the denominator of x is divisible by arbitrarily high powers of p, which is impossible.

Case II: $p \mid m$, then $m = pn$ for some integer n. Consider the point $P' = nP$. Since P has order m, we see that P' has order p. In addition, since $P \in E(p)$ and $E(p)$ is a subgroup of $E(\mathbb{Q})$, we have that $P' \in E(p)$. Now, we know that $P' \in E(p^\nu)$ for some $\nu > 0$, then similarly, we obtain

$$0 = t(\mathcal{O}) = t(pP') \equiv pt(P') \mod p^{3\nu}R.$$

This implies that

$$t(P') \equiv 0 \mod p^{3\nu-1}R.$$

Thus, $P' \in E(p^{3\nu-1})$. By a similar argument as Case I, we reach a contradiction, which completes the proof of this part.

(b) If $P = (x, y)$ is a point of finite order, then it follows from (a) that $P \notin E(p)$ for all primes p. This means that no prime can divide the denominators of x and y, so they must be 1. Thus, x and y are integers. □

Now, we proceed to prove the remaining part of the Nagell-Lutz theorem, which concerns the possible values of the y-coordinate of a rational point on an elliptic curve if it is of finite order.

Fact 2.20 (cf. Lemma 2.2 in [ST15])**.** *Let $P = (x, y)$ be a point on an elliptic curve $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ such that both P and $2P$ have integer coordinates, then either $y = 0$ or $y \mid D$, where*

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

is the discriminant of $f(x)$.

Proof. We know from Theorem 2.9 that if $y = 0$, then P has order two, so we are done for this case.

Now, suppose that $y \neq 0$ and we need to show that $y \mid D$. Since $y \neq 0$, we know that $2P \neq \mathcal{O}$, so we may write $2P = (X, Y)$. By assumption, x, y, X, Y are integers. By the duplication formula, we have that

$$2x + X = \lambda^2 - a, \quad \text{where } \lambda = \frac{f'(x)}{2y}.$$

Since x, X and a are all integers and λ is rational, it follows that λ must be an integer. Along with the fact that $2y$ and $f'(x)$ are integers, we see that $2y \mid f'(x)$, in particular $y \mid f'(x)$. Since $y^2 = f(x)$.

Now, note that

$$D = r(x)f(x) + s(x)f'(x)$$

where

$$r(x) = \left((18b - 6a^2)x - (4a^3 - 15ab + 27c)\right), \quad \text{and}$$

$$s(x) = \left((2a^2 - 6b)x^2 + (2a^3 - 7ab + 9c)x + (a^2b + 3ac - 4b^2)\right).$$

The coefficients of r and s are integers, so $r(x)$ and $s(x)$ take on integer values when evaluated at the integer x. Thus, y divides D. □

Theorem 2.21 (Nagell-Lutz Theorem)**.** *Let*

$$y^2 = x^3 + ax^2 + bx + c$$

be a non-singular cubic curve with integer coefficients a, b, and let D be the discriminant of the cublic polynomial, given by

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

Let $P = (x, y)$ be a rational point of finite order, then x and y are integers, and either $y = 0$, in which case P has order two, or else $y \mid D$.

Proof. This follows from Corollary 2.19 and Fact 2.20. □

In fact, a stronger version of Nagell-Lutz Theorem also holds.

Theorem 2.22 (Nagell-Lutz Theorem, strong version)**.** *Let*

$$y^2 = x^3 + ax^2 + bx + c$$

be a non-singular cubic curve with integer coefficients a, b, and let D be the discriminant of the cubic polynomial, given by

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

If $P = (x, y)$ is a rational point of finite order, then either $2P = \mathcal{O}$ or $y^2 \mid D$.

Proof. The idea of this proof is based on [ST15, Exercise 2.11].

It suffices to prove that if $y \neq 0$, then $y^2 \mid D$. We know that if $P = (x, y)$ is a point on E, then by duplication formula, we have that

$$x\text{-coordinate of } 2P = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4(x^3 + ax^2 + bx + c)}.$$

Let $\phi(x) = x^4 - 2bx^2 - 8cx + b^2 - 4ac$. By algebraic manipulation or invoking the theory of resultants (see [Mil20, Chapter I]), we see that there exists polynomials $F(X)$ and $\Phi(X)$ such that

$$F(X)f(X) + \Phi(X)\phi(X) = D. \tag{4}$$

For the specific $F(x)$ and $\Phi(x)$ in the case of elliptic curves in short Weierstrass form, i.e. $y^2 = x^3 + ax + b$, see [Sil09, Corollary VIII.7.2].

Since $y^2 = x^3 + ax^2 + bx + c$, the duplication formula implies that y^2 divides $\phi(x)$ because the x-coordinate of $2P$ is an integer if P is a point of finite order, as seen in Corollary 2.19. The equality (4) indicates that y^2 divides D. □

For elliptic curves that have a rational point of order two, one can also derive a variant of the Nagell-Lutz Theorem.

Theorem 2.23 (Variant of Nagell-Lutz Theorem, cf. Exercise 3.7 in [Sil09])**.** *Let C be defined in Weierstrass form by $y^2 = x^3 + ax^2 + bx$, where a and b are integers. If $P = (x, y)$ is a rational point of finite order, then P has integer coordinates with either $y = 0$, or if $y \neq 0$, then x divides b and $x + a + \frac{b}{x}$ is a perfect square.*

Proof. We defer to Chapter 3 for the proof of this version of the Nagell-Lutz theorem. □

Example 2.24 (cf. Exercise 2.10 and Exercise 3.7 in [ST15])**.** *Let p be a prime, and let C be the cubic curve*

$$C : y^2 = x^3 + px.$$

Denote the group of rational points on C by $C(\mathbb{Q})$, then all points of finite order in $C(\mathbb{Q})$ are the point of infinity $\mathcal{O}$ and the origin $T = (0, 0)$. In other words, the torsion subgroup of $C(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Two versions of the proof of Example 2.24 are presented here, one applying the strong Nagell-Lutz Theorem (Theorem 2.22), whereas the other makes use of the variant (Theorem 2.23).

Proof 1 (via Theorem 2.22). Let $P = (x, y) \neq \mathcal{O}$ be a point on C. By Theorem 2.22, it follows that if$P$ has finite order, then has integer coordinates with $y = 0$, or if $y \neq 0$, then y^2 divides $D = -4p^3$. From

the equation of C, we see that the only point on C such that the y-coordinate is zero is $(0, 0)$.

Now, we move on to those with $y \neq 0$. We then see that we only need to consider the case when $y = \pm 1$ or $y = \pm p$. However, both $x^3 + px - 1 = 0$ and $x^3 + px - p^2 = 0$ have no integer solutions. Therefore, the only points of finite order are $\mathcal{O}$ and $(0, 0)$. □

Proof 2 (via Theorem 2.23). Let $P = (x, y) \neq \mathcal{O}$ be a point on C. The case when $y = 0$ is the same as in Proof 1, which gives us the point $(0, 0)$.

By Theorem 2.23, if $y \neq 0$, then x must divide p and $x + \frac{p}{x}$ is a perfect square. Since x must divide p, it follows that either $x = 1$ or $x = p$. In either case, we see that $p + 1$ is a perfect square.

If $p+1$ is a perfect square, then $p+1 = m^2$ for some integer m. This gives $p = m^2-1 = (m+1)(m-1)$. Since p is prime and $m+1 > m-1$, it follows that $m + 1 = p$ and $m - 1 = 1$ necessarily, so that $m = 2$ and $p = 3$. This eliminates the existence of a point of finite order with nonzero y-coordinate for the cases of all primes such that $p \neq 3$.

It remains to check the case when $p = 3$. By Theorem 2.23, it suffices to check the cases when $x = 1$ and $x = 3$, i.e. the points $P_1 = (1, \pm 2)$ and $P_2 = (3, \pm 6)$. However, by duplication formula, we have that $2P_1 = \left(\frac{1}{4}, \mp\frac{7}{8}\right)$ and $2P_2 = \left(\frac{1}{4}, \pm\frac{7}{8}\right)$, implying that P_1 and P_2 have infinite order. Thus, the only points of finite order are $\mathcal{O}$ and $(0, 0)$. □

An overview of further developments of the Nagell-Lutz theorem, such as determining the possible orders of points of finite order in an elliptic curve over number fields of degree d, including the famous Mazur's theorem that classifies such points for the group of rational points, can be found in [Dan+17]. In particular, Mazur's theorem is stated as follows.

Theorem 2.25 (Mazur's Theorem)**.** *Let E be an elliptic curve, then the subgroup of points of finite order $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following:*

$$E(\mathbb{Q})_{tors} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } 1 \leqslant M \leqslant 10 \text{ or } M = 12, \text{or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 1 \leqslant M \leqslant 4. \end{cases}$$

3. Group of Rational Points is Finitely Generated

An important result regarding the group $E(\mathbb{Q})$ of rational points on an elliptic curve E is that $E(\mathbb{Q})$ is finitely generated, i.e. every element in $E(\mathbb{Q})$ can be expressed as a linear combination of finitely many distinct elements in $E(\mathbb{Q})$ with integer coefficients (scalars), which was proven by Louis Mordell in 1922.

This chapter provides a more detailed walk-through of the proof of Mordell's theorem for a family of elliptic curves with a point of order two that is presented in [ST15] which utilises the technique of proof by infinite descent via a mathematical tool known as height functions. A number of important consequences and applications of this theorem are also discussed.

3.1. **Height Function.** A height function provides a method of quantitatively measuring the complexity of a mathematical object. There are several types of height functions (see [Sil06] for some examples). However, in this section, we focus on a simple type of height function known as the naive height function, applied on the field of rational numbers, and see how this tool plays a key role in proving the Mordell's theorem.

Definition 3.1 (Height Function)**.** *Let $x = m/n$ be a rational number in its simplest form, i.e. m and n are coprime, then the height H of x is defined as the maximum of the absolute values of m and n, i.e.*

$$H(x) = \max\{|m|, |n|\}.$$

We then define the 'small height function' h of x as the natural logarithm of H evaluated at x, i.e. $h(x) = \log H(x)$.

Definition 3.2 (Height of a Rational Point)**.** *Let $E(\mathbb{Q})$ be the group of rational points of an elliptic curve and $P = (x, y)$ be a point in $E(\mathbb{Q})$. We define the 'small height function' h on $E(\mathbb{Q})$ to be the 'small h height' of the x-coordinate of P, i.e.*

$$h(P) = h(x).$$

We will later see that the height function H, and thus the 'small height function' h, satisfy the four conditions for the Descent Theorem.

We restate the four conditions, applied on the 'small height function' h, here and list each of them as a lemma.

Lemma 3.3 (Finiteness Property, Lemma 3.1 in [ST15])**.** *For every real number M, the set*

$$\{P \in C(\mathbb{Q}) : h(P) \leqslant M\}$$

is finite.

Proof. This is relatively straightforward to see from the definition of h. The 'small h height' of a rational number is the natural logarithm of the maximum of the absolute value of its numerator and denominator, and since the numerator and denominator are integers, there are finitely many possible integers whose absolute value is less than or equal to e^M (note that this is applied to both the numerator and the denominator), so there are finitely many possible rational numbers whose 'small h height' is less than M.

This implies that there are finitely many possible x-coordinates of a rational point in $E(\mathbb{Q})$, and since for each x-coordinate, there are only two possibilities for the y-coordinate, it follows that there are finitely many possible rational points whose 'small h height' is not more than M. □

Lemma 3.4 (Lemma 3.2 in [ST15]). *Let P_0 be a fixed rational point of an elliptic curve E. There then exists a constant κ_0 that depends on P_0 and the non-leading coefficients of the equation of E, such that*

$$h(P + P_0) \leqslant 2h(P) + \kappa_0 \quad \text{for all } P \in E(\mathbb{Q}).$$

Proof. See [ST15, pp. 73-75]. □

Lemma 3.5 (Lemma 3.6 in [ST15]). *Let $\phi(X)$ and $\psi(X)$ be polynomials with integer coefficients and no common complex roots. Let d be the maximum of the degrees of ϕ and ψ.*

(a) There is an integer $R \geqslant 1$, depending on ϕ and ψ, such that for all rational numbers m/n, $\gcd\left(n^d\phi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)\right)$ divides R.

(b) There are constants κ_1 and κ_2, depending on ϕ and ψ, so that for all rational numbers m/n that are not roots of ψ, $dh\left(\frac{m}{n}\right) - \kappa_1 \leqslant h\left(\frac{\phi(m/n)}{\psi(m/n)}\right) \leqslant dh\left(\frac{m}{n}\right) + \kappa_2$.

Proof. A partial proof is provided in [ST15], which is reproduced here with the omitted parts filled in.

(a) To ease the notation, let $\Phi(m,n) = n^d\phi(m/n)$ and $\Psi(m,n) = n^d\psi(m/n)$. Since $\phi(X)$ and $\psi(X)$ have no common roots, they are relatively prime in $\mathbb{Q}[X]$, so we can find polynomials $F(X)$ and $G(X)$ in $\mathbb{Q}[X]$ such that $F(X)\phi(X) + G(X)\psi(X) = 1$.

Without loss of generality, we assume that $\deg\phi = d$ and $\deg\psi = e \leqslant d$. We can then write

$$n^d\phi(m/n) = a_0m^d + a_1m^{d-1}n + \cdots + a_dn^d,$$
$$n^d\psi(m/n) = b_0m^en^{d-e} + b_1m^{e-1}n^{d-e+1} + \cdots + b_en^d.$$

Let A be a sufficiently large integer so that $AF(X)$ and $AG(X)$ have integer coefficients. Let $D = \max\{\deg F, \deg G\}$. Evaluating the identity above at m/n and multiplying both sides by An^{D+d} yields

$$\underbrace{n^DAF(m/n)}_{\text{integer}}\cdot n^d\phi(m/n) + \underbrace{n^DAG(m/n)}_{\text{integer}}\cdot n^d\psi(m/n) = An^{D+d}.$$

Note that if we write $n^d\phi(m/n) = a_0m^d + a_1m^{d-1}n + \cdots + a_dn^d$, where $d = \max\{\deg\phi, \deg\psi\}$, we see that

$$Aa_0^in^{D+d-1-i}\Phi(m,n) = Aa_0^{i+1}m^dn^{D+d-1-i} + Aa_1a_0^im^{d-1}n^{D+d-i} + \cdots + Aa_0^ia_dn^{D+2d-1-i}$$

where $i = 0, 1, \ldots, D + d - 1$.

Let $\gamma = \gcd(\Phi(m,n), \Psi(m,n))$. We see from the previous equality that γ divides An^{D+d}, due to Bezout's identity. To show that γ divides a constant that is independent of n, we show that γ divides Aa_0^{D+d}, where a_0 is the leading coefficient of $\phi(X)$. This is done by showing that for $i = 0, \ldots, D+d-1$, γ divides $Aa_0^i n^{D+d-1-i}\Phi(m,n)$, so that γ divides $Aa_0^{i+1}n^{D+d-i-1}$, since γ divides $\gcd(An^{D+d}, Aa_0m^dn^{D+d-i})$ and m and n are relatively prime.

(b) Let m/n be a rational number that is not a root of ϕ or ψ. Without loss of generality, suppose again that $\deg\phi = d$ and $\deg\psi = e \leqslant d$.

The proof of the upper bound is omitted in [ST15]; we provide one here. Note that after some manipulation, we have that $\dfrac{\phi(m/n)}{\psi(m/n)} = \dfrac{a_0m^d + \cdots}{b_0m^en^{d-e} + \cdots}$ with $a_0, b_0, \ldots$ being integers. Observe that $a_0, b_0, \ldots$ do not depend on m nor n. It follows that

$$\begin{aligned} h\left(\frac{\phi(m/n)}{\psi(m/n)}\right) &= \log\max\{|a_0m^d + \cdots|, |b_0m^en^{d-e} + \cdots|\} \\ &\leqslant \log\left(\max\{|m|,|n|\}^d \max\{|a_0|,|b_0|,\ldots\}\right) \\ &\leqslant dh\left(\frac{m}{n}\right) + \kappa_2 \quad \text{where } \kappa_2 = \log\max\{|a_0|,|b_0|,\ldots\}. \end{aligned}$$

We now prove the lower bound. Continuing with the notation from (a), let $\xi = \dfrac{\Phi(m,n)}{\Psi(m,n)}$. Note that this is equal to $\dfrac{\phi(m/n)}{\psi(m/n)}$.

We know from (a) that there exists some integer $R \geqslant 1$ that does not depend on m and n such that $\gcd(\Phi(m,n), \Psi(m,n))$ divides R. It follows that

$$\begin{aligned} H(\xi) &\geqslant \frac{1}{R}\max\{|\Phi(m,n)|, |\Psi(m,n)|\} \\ &\geqslant \frac{1}{2R}\left(\left|n^d\phi(m/n)\right| + \left|n^d\psi(m/n)\right|\right). \end{aligned}$$

The last inequality above applies the fact that for real numbers a and b, we have that $\max\{a,b\} \geqslant \frac{1}{2}(a+b)$.

Now, consider the quotient

$$\frac{H(\xi)}{(H(m/n))^d} \geqslant \frac{1}{2R} \cdot \frac{|\phi(m/n)| + |\psi(m/n)|}{\max\{|m/n|^d, 1\}}.$$

Let $p(t) = \dfrac{|\phi(t)| + |\psi(t)|}{\max\{|t|^d, 1\}}$ where $t \in \mathbb{R}$. Note that

$$\lim_{|t|\to\infty} p(t) = \begin{cases} |a_0| & \text{if } \deg\psi < d, \\ |a_0| + |b_0| & \text{if } \deg\psi = d. \end{cases}$$

This implies that $p(t)$ is bounded away from zero outside of some closed interval I.

As for values inside the closed interval I, by the Extreme Value Theorem, since I is compact, $p(t)$ assumes its minimum value in I, which is positive since $p(t)$ is never equal to zero. This implies that there is a constant $C_1 > 0$ such that $p(t) \geqslant C_1$ for all real numbers t. Previously, we have shown that

$$\frac{H(\xi)}{(H(m/n))^d} \geqslant \frac{1}{2R} \cdot p(m/n).$$

It follows that

$$H(\xi) \geqslant \frac{C_1}{2R} \cdot (H(m/n))^d.$$

Taking logarithms yields the desired lower bound

$$h(\xi) \geqslant dh(m/n) - \kappa_1$$

with $\kappa_1 = \log(2R/C_1)$. □

Lemma 3.5 is useful in showing that 'small height function' h satisfies the third condition of the Descent Theorem (Lemma 3.17).

Corollary 3.6 (Lemma 3.3 in [ST15])**.** *Let $E(\mathbb{Q})$ be the group of rational points on an elliptic curve E. There exists a constant κ, which depends on the non-leading coefficients of the equation of E, such that*

$$h(2P) \geqslant 4h(P) - \kappa \quad \text{for all } P \in E(\mathbb{Q}).$$

Proof. The explicit formulae for the group law implies that

$$\xi + 2x = \lambda^2 \text{ with } \lambda = \frac{f'(x)}{2y}.$$

Simplifying the above and substituting $y^2 = f(x) = x^3 + ax + b$ yields

$$\xi = \frac{(f'(x))^2 - (8x)f(x)}{4f(x)} = \frac{x^4 - 2ax^2 + \cdots}{4x^3 + 4ax + \cdots}.$$

This implies that ξ is the quotient of two polynomials in x with integer coefficients, and the polynomials in the numerator and denominator have no common complex roots (since $f(x)$ is non-singular).

We then see that the desired statement follows from Lemma 3.5. Note that from the polynomial quotient expression of ξ above, we can apply Lemma 3.5 to prove the inequality above with ϕ being the numerator of the quotient, ψ being the denominator of the quotient, and $m/n = x$, so that $d = 4$ and $\frac{\phi(m/n)}{\psi(m/n)} = \xi$. The existence of the constant κ follows by taking the lower bound of the inequality in Lemma 3.5(b). □

Note that the upper bound in Lemma 3.5(b) also gives rise to the following fact related to Lemma 3.4.

Fact 3.7 (Extension of Lemma 3.4)**.** *Let Γ be the group of rational points on an elliptic curve E. There is a constant κ_0, depending on the non-leading coefficients of the equation of E, such that*

$$h(2P) \leqslant 4h(P) + \kappa_0$$

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

Lemma 3.8 (Lemma 3.4 in [ST15])**.** *Let $E(\mathbb{Q})$ be the group of rational points on an elliptic curve E, then the index $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ of $2E(\mathbb{Q})$ in $E(\mathbb{Q})$ is finite.*

Lemma 3.8 will be the main focus of discussion in the next section.

3.2. **Finiteness of $E(\mathbb{Q})/2E(\mathbb{Q})$.** In this section, we prove that the group of rational points $E(\mathbb{Q})$ on an elliptic curve E with a point of order two satisfies the fourth and last condition for invoking the Descent Theorem. In other words, we show that the index of $2E(\mathbb{Q})$ in $E(\mathbb{Q})$ is finite.

Now, for reasons that will be stated at the end of this section, we assume that the elliptic curve that we are interested in has at least one rational root x_0. In this case, by performing a linear change of variable that shifts x_0 to the origin where necessary, we focus on the following family of elliptic curves C defined by

$$C : y^2 = x^3 + ax^2 + bx,$$

where a and b are integers. For simplicity, we may refer to the corresponding group of rational points $C(\mathbb{Q})$ as Γ.

Next, we introduce the correspondence of curves $C \mapsto \bar{C}$, where the family of elliptic curves $\bar{C}$ is defined by

$$\bar{C} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x,$$

where

$$\bar{a} = -2a, \quad \bar{b} = a^2 - 4b.$$

This correspondence is helpful because it behaves like a dual mapping that is often seen in linear algebra, in the sense that the double dual is isomorphic to the original space: if we apply the correspondence once again on $\bar{C}$ to obtain $\bar{\bar{C}}$, we then see that the resulting non-leading coefficients $\bar{\bar{a}}$ and $\bar{\bar{b}}$ of $\bar{\bar{C}}$ becomes

$$\bar{\bar{a}} = 4a, \quad \bar{\bar{b}} = (-2a)^2 - 4(a^2 - 4b) = 16b.$$

Observe that $\bar{\bar{a}}$ (resp. $\bar{\bar{b}}$) is just a scalar multiple of a (resp. b). This gives rise to an isomorphism from C to $\bar{\bar{C}}$, specifically $(x, y) \mapsto (4x, 8y)$. Indeed, this is also an isomorphism from Γ to the group of rational points $\bar{\bar{\Gamma}}$ on $\bar{\bar{C}}$.

It is also worth noting that the definition of $\bar{b}$ is a factor of the discriminant of C, which is $b^2(a^2 - 4b)$.

In view of this, we introduce two useful homomorphisms ϕ and ψ that will be described in Fact 3.9. These two homomorphisms play a role in 'separating' the multiplication by two map into two simpler operations. In particular, we are interested in $\phi(\Gamma)$ and $\psi(\bar{\Gamma})$, the images of Γ by ϕ and $\bar{\Gamma} := \bar{C}(\mathbb{Q})$ by ψ respectively. This is because we will see later that the indices of $\phi(\Gamma)$ in $\bar{\Gamma}$ and $\psi(\bar{\Gamma})$ in Γ, along with the fact that the composition of ϕ and ψ gives the multiplication by two map, are helpful in showing the finiteness of the index of 2Γ in Γ that we need.

Fact 3.9 (cf. Proposition 3.7 in [ST15])**.** *Let C and $\bar{C}$ be elliptic curves given by the equations*

$$C : y^2 = x^3 + ax^2 + bx \quad \text{and} \quad \bar{C} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$$

where

$$\bar{a} = -2a \quad \text{and} \quad \bar{b} = a^2 - 4b.$$

Denote the origin $(0,0) \in C$ and $(0,0) \in \bar{C}$ by T and $\bar{T}$ respectively.

(a) There is a homomorphism $\phi : C \to \bar{C}$ defined by

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

The kernel of ϕ is $\{\mathcal{O}, T\}$.

(b) There is a homomorphism $\psi : \bar{C} \to C$ defined by

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

(c) The composition $\psi \circ \phi : C \to C$ is the multiplication by two map,

$$(\psi \circ \phi)(P) = 2P.$$

Proof. See [ST15, pp. 85-88]. □

To those who are familiar with algebraic number theory, one may see that the homomorphisms ϕ and ψ is a special case of isogenies; more precisely, ϕ and ψ are dual isogenies, i.e. an isogeny of degree two. For a more detailed treatment of isogenies, one may consult [Sil09, in particular Sections III.4 and III.6].

It turns out that ϕ is also helpful in proving the aforementioned variant of Nagell-Lutz Theorem (Theorem 2.23).

Proof of Theorem 2.23. By Fact 3.9, we know that ϕ is a homomorphism, so if $P = (x, y)$ has finite order, then $\phi(P)$ must also have finite order (since if $mP = \mathcal{O}$ for some integer m, then $m\phi(P) = \phi(mP) = \phi(\mathcal{O}) = \bar{\mathcal{O}}$). By Corollary 2.19, we know that P must have integer coordinates, so $\frac{y^2}{x^2} = x + a + \frac{b}{x}$ is an integer, implying that x divides b and $x + a + \frac{b}{x}$ is a perfect square. □

Now, we investigate the nature of the points in $\phi(\Gamma)$.

Lemma 3.10. *Let ϕ be the homomorphism described in Fact 3.9, and Γ be the group of rational points on the curve $C : y^2 = x^3 + ax^2 + bx$, where a and b are integers, then the following hold:*

(a) $\bar{\mathcal{O}} \in \phi(\Gamma)$.
(b) $\bar{T} := (0,0) \in \phi(\Gamma)$ if and only if $\bar{b} := a^2 - 4b$ is a perfect square.
(c) Let $\bar{P} := (\bar{x}, \bar{y}) \in \bar{\Gamma}$ with $\bar{x} \neq 0$, then $\bar{P} \in \phi(\bar{\Gamma})$ if and only if $\bar{x}$ is the square of a rational number.

Proof. See [ST15, pp. 89-91]. □

As for the case of $\psi(\bar{\Gamma})$, we have an almost identical result to Lemma 3.10, which is stated as follows.

Lemma 3.11. *Let ψ be the homomorphism, and $\bar{\Gamma}$ be the group of rational points on the curve $\bar{C} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$ described in Fact 3.9, then the following hold:*

(a) $\mathcal{O} \in \psi(\bar{\Gamma})$.
(b) $T := (0,0) \in \psi(\bar{\Gamma})$ if and only if b is a perfect square.
(c) Let $P := (x, y) \in \bar{\Gamma}$ with $x \neq 0$, then $\bar{P} \in \psi(\Gamma)$ if and only if x is the square of a rational number.

Proof. Similar to the proof for Lemma 3.10. □

Note that Lemma 3.11 implies that the image $\psi(\bar{\Gamma})$ is a subgroup of the rational points Γ in C, where the points in the subgroup are $\mathcal{O}$, together with points $(x, y) \in \Gamma$ where x to be a nonzero rational square; if b is a perfect square, then T is also in the subgroup.

Definition 3.12. *Let $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ denote the multiplicative group of rational numbers and $(\mathbb{Q}^*)^2$ be the group of squares of elements in $\mathbb{Q}^*$, i.e. $(\mathbb{Q}^*)^2 := \{x^2 : x \in \mathbb{Q}^*\}$.*

Fact 3.13 (cf. Proposition 3.8 in [Sil09])**.** *Define a map $\alpha : \Gamma \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ as follows:*

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

The following then hold:

(a) α is a homomorphism.
(b) The kernel of α is the image $\psi(\bar{\Gamma})$. Hence α induces an injective homomorphism from $\Gamma/\psi(\bar{\Gamma})$ to $\mathbb{Q}^*/(\mathbb{Q}^*)^2$.
(c) Let $p_1, p_2, \ldots, p_t$ be the distinct primes dividing b, then the image of α is contained in the subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ consisting of the elements

$$\{\pm p_1^{\varepsilon_i} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t} : \varepsilon_i = 0 \text{ or } 1\}.$$

(d) The index $[\Gamma : \psi(\bar{\Gamma})]$ is at most 2^{t+1}.

Proof. See [ST15, pp. 92-93] for an almost complete proof. Here, we fill in an omitted detail in the proof of part (a) that handles the edge cases when showing that if $P_1, P_2, P_3 \in \Gamma$ satisfies $P_1 + P_2 + P_3 = \mathcal{O}$, then $\alpha(P_1)\alpha(P_2)\alpha(P_3) \equiv 1 \mod (\mathbb{Q}^*)^2$, specifically when at least one of the three points is $\mathcal{O}$ or T. This corresponds to Exercise 3.5 in [ST15].

If at least one of the points, say, P_3, is $\mathcal{O}$, then $P_1 + P_2 = \mathcal{O}$, implying that P_1 and P_2 are inverses of each other. Since $\alpha(P^{-1}) \equiv (\alpha(P))^{-1} \mod (\mathbb{Q}^*)^2$, it follows that $\alpha(P_1)\alpha(P_2)\alpha(P_3) \equiv \alpha(P_1) \cdot (\alpha(P_1))^{-1} \cdot 1 \equiv 1 \mod (\mathbb{Q}^*)^2$.

If at least one of the points, say, P_3, is T, then $P_1 + P_2 = -T = T$. It is impossible that both P_1 and P_2 are either $\mathcal{O}$ or T, so we first suppose that only one of them, say, P_1 is $\mathcal{O}$, then $P_2 = -T = T$ necessarily. It follows that $\alpha(P_1)\alpha(P_2)\alpha(P_3) \equiv 1 \cdot b \cdot b \equiv b^2 \equiv 1 \mod (\mathbb{Q}^*)^2$.

If $P_1, P_2 \neq \mathcal{O}, T$, let $y = \lambda x + \nu$ be the line joining P_1, P_2 and P_3 with x-coordinates x_1, x_2 and x_3 respectively, where $x_3 = 0$ by assumption. Substituting $y = \lambda x + \nu$ into the curve equation and solving for x implies that $x_1x_2 + x_1x_3 + x_2x_3 = x_1x_2 = b - 2\lambda\nu$. Since the line passes through T, it follows that $\nu = 0$. Therefore, we have that $\alpha(P_1)\alpha(P_2)\alpha(P_3) \equiv (b - 2\lambda\nu) \cdot b = b^2 - 2\lambda\nu b = b^2 \equiv 1 \mod (\mathbb{Q}^*)^2$. □

Remark 3.14. *An analogous statement to Fact 3.13 can be made with* Γ *replaced by* $\bar{\Gamma}$ *(the corresponding homomorphism is denoted as* $\bar{\alpha}$*), and the argument being almost identical.*

Fact 3.15 (cf. Exercise 3.6 in [ST15])**.** *Let A and B be abelian groups, and $m \geqslant 2$ be an integer. Suppose that $\phi : A \to B$ and $\psi : B \to A$ are homomorphisms satisfying*

$$(\psi \circ \phi)(a) = ma \text{ for all } a \in A, \quad (\phi \circ \psi)(b) = mb \text{ for all } b \in B.$$

Suppose further that $\phi(A)$ has finite index in B and $\psi(B)$ has finite index in A, then mA has finite index in A. More precisely, the index satisfies the inequality

$$[A : mA] \leqslant [A : \psi(B)][B : \phi(A)].$$

Proof. We slightly modify the proof provided in [ST15, Lemma 3.9].

Since $\psi(B)$ has finite index in A, say, k, there are k representatives, say, $a_1, \ldots, a_k$ of its cosets. Similarly, since $\phi(A)$ has finite index in B, say, l, we can take, say, $b_1, \ldots, b_l$, as representatives of each of its l cosets.

We claim that the set

$$\{a_i + \psi(b_j) : 1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant l\}$$

contains a complete set of the representatives for the cosets of mA in A. Note that this set contains $[A : \psi(B)][B : \phi(A)]$ elements. If the claim holds, then this implies that $[A : mA]$ is at most $[A : \psi(B)][B : \phi(A)]$, as desired.

To see this, suppose that $a \in A$; our aim is to show that a can be written as a sum of an element of this set plus an element of mA. Since $a_1, \ldots, a_k$ are representatives for the cosets of $\psi(B)$ in A, we can find some a_i, with $i = 1, \ldots, k$, such that $a - a_i \in \psi(B)$. Similarly, since $b_1, \ldots, b_l$ are representatives for the cosets of $\phi(A)$ inside B, we can find some b_j, with $j = 1, \ldots, l$, such that $b - b_j \in \phi(A)$, then $b - b_j = \phi(a')$ for some $a' \in A$. It follows that

$$\begin{aligned} a = a_i + \psi(b) &= a_i + \psi(b_j + \psi(a')) \\ &= a_i + \psi(b_j) + \psi(\phi(a')) \\ &= a_i + \psi(b_j) + ma', \end{aligned}$$

and this concludes the proof. □

Corollary 3.16 (Lemma 3.4 in [ST15])**.** *Let Γ be the group of rational points on an elliptic curve $C : y^2 = x^3 + ax^2 + bx$, then 2Γ has finite index in Γ.*

Proof. This follows from Fact 3.15, with $m = 2$, because we have $\phi : \Gamma \to \bar{\Gamma}$ and $\psi : \bar{\Gamma} \to \Gamma$ are homomorphisms described in Fact 3.9. Moreover, Γ and $\bar{\Gamma}$ are abelian groups. The indices $[\Gamma : \psi(\bar{\Gamma})]$ and $[\bar{\Gamma} : \phi(\Gamma)]$ are also finite by Fact 3.13. □

3.3. **Descent Theorem and Mordell's Theorem.** We have established in the previous sections that the 'small height function' h defined on Γ satisfies four key conditions. Here, we show that with these four conditions equipped, we can then prove the crux of Mordell's theorem, which is that Γ is finitely generated.

Theorem 3.17 (Descent Theorem)**.** *Let Γ be a commutative group, and suppose that there exists a function*

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

such that

- *(a) for every real number M, the set $P \in \Gamma : h(P) \leqslant M$ is finite;*
- *(b) for every $P_0 \in \Gamma$, there exists a constant κ_0 such that $h(P + P_0) \leqslant 2h(P) + \kappa_0$ for all $P \in \Gamma$;*
- *(c) there is a constant κ where $h(2P) \geqslant 4h(P) - \kappa$ for all $P \in \Gamma$;*
- *(d) the index $[\Gamma : 2\Gamma]$ is finite,*

then Γ is finitely generated.

Proof. See [ST15, pp. 68-70]. □

Theorem 3.18 (Mordell's Theorem for Elliptic Curves with Points of Order Two)**.** *Let C be a non-singular cubic curve given by an equation*

$$C : y^2 = x^3 + ax^2 + bx$$

where a and b are integers, then the group of rational points $C(\mathbb{Q})$ is a finitely generated abelian group.

Proof. We know from the previous section that $C(\mathbb{Q})$ is an abelian group that can be equipped with a function, i.e. the 'small height function' $h : C(\mathbb{Q}) \to [0, \infty)$ previously introduced, that satisfies the conditions for Descent Theorem, thus it follows from Descent Theorem that $C(\mathbb{Q})$ is finitely generated, as desired. □

Now, if the non-leading coefficients of the equation of the elliptic curve are rational numbers that are not integers, we can still apply Theorem 3.18 by performing a suitable change of variables via scalar multiplication.

However, to extend Theorem 3.18 described here to general elliptic curves, i.e. those defined by equations in the form of $y^2 = x^3 + ax + b$, all the proofs described that lead to Theorem 3.18 still go through, except for the part that proves the finiteness of $E(\mathbb{Q})/2E(\mathbb{Q})$, as in this case we then need to take a root ζ of $x^3 + ax + b$, and work in $\mathbb{Q}(\zeta)$. Nevertheless, a more generalised form of this result exists, which is known as the weak Mordell-Weil Theorem, and is applicable for elliptic curves defined over any number field K and the corresponding quotient group $E(K)/mE(K)$ where $m \geqslant 2$ is an integer. See, for example, [Sil09, Section VIII.1], for more details.

3.4. **Application of Mordell's Theorem.** One of the applications of Mordell's theorem is the computation of ranks of groups of rational points induced by elliptic curves.

We have previously proven Mordell's theorem for the family of elliptic curves C defined by equations in the form of $y^2 = x^3 + ax^2 + bx$, where a and b are integers, which shows that the corresponding group of rational points Γ is finitely generated. Thus, by the fundamental theorem of finitely generated abelian groups, we have the following isomorphism:

$$\Gamma \simeq \mathbb{Z}^r \oplus \mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_s^{\nu_s}\mathbb{Z}, \tag{5}$$

where $p_1, \ldots, p_s$ are primes and $\nu_1, \ldots, \nu_s$ are positive integers. In other words, we can obtain generators $P_1, \ldots, P_r, Q_1, \ldots, Q_s \in \Gamma$ such that every $P \in \Gamma$ can be expressed as the following linear combination:

$$P = n_1P_1 + \cdots + n_rP_r + m_1Q_1 + \ldots + m_sQ_s,$$

where $n_1, \ldots, n_r$ are uniquely determined by P, while the integers m_j are determined modulo $p_j^{\nu_j}$, with $j = 1, \ldots, s$.

The rank of Γ is then the integer r. From (5), we also see that Γ is finite if and only if Γ contains only elements of finite order, or equivalently $r = 0$. We then see that the torsion subgroup of Γ is isomorphic to $\mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_s^{\nu_s}\mathbb{Z}$, with $|\Gamma| = p_1^{\nu_1} \cdots p_s^{\nu_s}$.

Applying this, one can then derive a formula and an algorithm for computing the rank of a given Γ; a proof is outlined in [ST15, pp. 95-98]. This algorithm is also known as the 2-descent method.

Fact 3.19 (Formula for rank computation)**.** *Let Γ and $\bar{\Gamma}$ be the group of rational points on elliptic curves C and $\bar{C}$ respectively as described in Fact 3.9. Let $\alpha : \Gamma \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ and $\bar{\alpha} : \bar{\Gamma} \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ be the homomorphisms as defined in Fact 3.13. Let r be the rank of Γ, then*

$$2^r = \frac{\#\alpha(\Gamma) \cdot \#\bar{\alpha}(\bar{\Gamma})}{4}.$$

Here, $\#\alpha(\Gamma)$ denotes the number of elements in the image of Γ under α, similarly for $\#\bar{\alpha}(\bar{\Gamma})$.

Fact 3.20 (2-descent method)**.** *Given a curve $C : y^2 = x^3 + ax^2 + bx$, one can compute the rank of its group of rational points Γ by the following steps:*

1. *Obtain all possibilities of integer pairs b_1 and b_2 such that $b = b_1 b_2$.*
2. *Write down equations of the form*

$$N^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4 \qquad (\triangle)$$

   for all pairs of b_1 and b_2, and determine whether or not each of them has a solution in integers with $M \neq 0$. Here, the variables M, n, e are pairwise coprime, due to the assumption that a point $(x, y) \in \Gamma$ is expressed in lowest terms. This helps in determining $\#\alpha(\Gamma)$ and $\#\bar{\alpha}(\bar{\Gamma})$. In particular, $\alpha(\Gamma)$ consists of $b \bmod (\mathbb{Q}^*)^2$, along with those $b_1 \bmod (\mathbb{Q}^*)^2$ such that $(\triangle)$ has a solution with $M \neq 0$.
3. *Apply the formula in Fact 3.19 to compute the rank.*

See [ST15, pp. 98-101] for a derivation of Fact 3.20. The difficulty of the 2-descent method to compute the rank of arbitrary elliptic curves lies in the fact that there is no general and efficient way to determine whether $(\triangle)$ has an integer solution.

It is also not known that whether or not it is possible to have groups of rational points on elliptic curves with arbitrarily large rank. As of 2025, the largest known rank is the following example constructed by Noam Elkies and Zev Klagsbrun in 2024 [Elk24], which has rank 29:

$$y^2 + xy = x^3 + ax + b,$$

where $a = -27\ 006\ 183\ 241\ 630\ 922\ 218\ 434\ 652\ 145\ 297\ 453\ 784\ 768\ 054\ 621\ 836\ 357\ 954\ 737\ 385$, and $b = 55\ 258\ 058\ 551\ 342\ 376\ 475\ 736\ 699\ 591\ 118\ 191\ 821\ 521\ 067\ 032\ 535\ 079\ 608\ 372\ 404\ 779\ 149\ 413\ 277\ 716\ 173\ 425\ 636\ 721\ 497$.

We have previously explored elliptic curves defined by the equation $y^2 = x^3 + ax^2 + bx$, which contains a rational point of order two. Now, we focus in particular on those with the coefficient of the x^2 term being zero, i.e. $a = 0$, so that they are defined by $y^2 = x^3 + Dx$, where D is a non-zero integer.

Example 3.21 (cf. Examples 3.11 and 3.12 in [ST15])**.** *We compute the rank of the two elliptic curves*

$$C_1 : y^2 = x^3 + x \quad \textit{and} \quad C_2 : y^2 = x^3 - x.$$

The corresponding $\bar{C}$'s are then given by

$$\bar{C_1} : y^2 = x^3 - 4x \quad \textit{and} \quad \bar{C_2} : y^2 = x^3 + 4x.$$

The respective ranks of the group of rational points on C_1, C_2, $\bar{C_1}$ and $\bar{C_2}$ are all zero.

Proof. See [ST15, pp. 101-103]. □

Example 3.22. *Define the elliptic curve C_3 and its corresponding $\bar{C_3}$ as follows:*

$$C_3 : y^2 = x^3 + 3x \quad \textit{and} \quad \bar{C_3} : y^2 = x^3 - 12x.$$

The rank of both C_3 and $\bar{C_3}$ is one.

Proof. Denote the group of rational points on C_3 and $\bar{C_3}$ by Γ and $\bar{\Gamma}$ respectively. Note that for C_3, the non-leading coefficients are given by $a = 0$ and $b = 3$, whereas for $\bar{C_3}$, we have $\bar{a} = 0$ and $\bar{b} = -12$.

Applying Fact 3.20, we calculate $\alpha(\Gamma)$ by determining all factorisations of $b = b_1 b_2$, which are given by

$$b_1 = 1, -1, 3, -3.$$

The corresponding equations for C_3 are:

$$N^2 = M^4 + 3e^4, \tag{6}$$
$$N^2 = -M^4 - 3e^4, \tag{7}$$
$$N^2 = 3M^4 + e^4, \tag{8}$$
$$N^2 = -3M^4 - e^4. \tag{9}$$

Since for Equations (7) and (9), the left-hand side is always non-negative whilst the right-hand side is strictly negative if $M \neq 0$, they have no non-zero real solutions. Equations (6) and (8) have a rational solution $(M, N, e) = (1, 2, 1)$. This implies that $\alpha(\Gamma) = \{1, 3 \pmod{(\mathbb{Q}^*)^2}\}$, which has order two.

As for $\bar{\alpha}(\bar{\Gamma})$, we determine the factorisations of $\bar{b} = \bar{b_1}\bar{b_2}$, so that we have

$$\bar{b_1} = 1, -1, 2, -2, 3, -3, 4, -4, 6, -6, 12, -12.$$

There are twelve corresponding equations for $\bar{C_3}$, which are:

$$N^2 = M^4 - 12e^4, \tag{10}$$
$$N^2 = -M^4 + 12e^4, \tag{11}$$
$$N^2 = 2M^4 - 6e^4, \tag{12}$$
$$N^2 = -2M^4 + 6e^4, \tag{13}$$
$$N^2 = 3M^4 - 4e^4, \tag{14}$$
$$N^2 = -3M^4 + 4e^4, \tag{15}$$

$$N^2 = 4M^4 - 3e^4, \tag{16}$$
$$N^2 = -4M^4 + 3e^4, \tag{17}$$
$$N^2 = 6M^4 - 2e^4, \tag{18}$$
$$N^2 = -6M^4 + 2e^4, \tag{19}$$
$$N^2 = 12M^4 - e^4, \tag{20}$$
$$N^2 = -12M^4 + e^4. \tag{21}$$

It suffices to check Equations (10) to (15) as they are equal to Equations (16) to (21) with the variables M and e swapped. It follows that Equation (10) has a rational solution $(M, N, e) = (1, 1, 0)$, Equation (13) has a solution $(M, N, e) = (1, 2, 1)$ and Equation (15) has a solution $(M, N, e) = (1, 1, 1)$, whilst Equations (11), (12) and (14) have no rational solutions with $M \neq 0$. Since $\pm 12 \equiv \pm 3 \mod (\mathbb{Q}^*)^2$ and $\pm 4 \equiv \pm 1 \mod (\mathbb{Q}^*)^2$, this implies that $\bar{\alpha}(\bar{\Gamma}) = \{1, -2, -3, 6 \pmod{(\mathbb{Q}^*)^2}\}$, which has order four.

Thus, applying Fact 3.19, the rank of both C_3 and $\bar{C}_3$ is $\log_2((2 \cdot 4)/4) = 1$. □

Example 3.23 (Congruent number problem)**.** *The congruent number problem is a classical problem in number theory, which was first stated by Persian mathematician Al-Karaji more than a thousand years ago; see [Whi18]. The first* 65 *congruent numbers can be found in [SI25]. The statement of this problem is elementary-sounding: a positive integer is called a congruent number if it is the area of a right-angled triangle with rational sides; is there an efficient algorithm that determines if any given positive integer n is a congruent number?*

As of 2025, although this problem has been solved for many special cases (see [Con08]), the ultimate goal of obtaining a general algorithm remains unresolved, though a conjectural solution exists (see [Tun83]). Here, we illustrate how this problem relates to the topic of elliptic curves, and present some relevant key results.

Theorem 3.24. *A positive rational number n is congruent if and only if the elliptic curve*

$$E_n : y^2 = x^3 - n^2 x$$

has a rational point with $y \neq 0$.

Proof. See [Con08, Section 6.4]. □

Lemma 3.25. *Let Γ_n be the group of rational points on an elliptic curve E_n described in Theorem 3.24, then the torsion subgroup T_n is either isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if n is an integer, or $\mathbb{Z}/2\mathbb{Z}$ otherwise.*

Proof. The point of infinity $\mathcal{O}$ is clearly a point of finite order. Let $P = (x, y) \in T_n$ be a rational point of finite order that is not $\mathcal{O}$. By Nagell-Lutz Theorem (Theorem 2.21), P then has integer coordinates,

where either $y = 0$, in which case P has order two, or if $y \neq 0$, then y divides the discriminant $D = -4n^6$.

We first suppose that $y = 0$. To determine the possible values of x, we obtain the roots of the polynomial $x^3 - n^2x = x(x^2 - n^2)$, which are 0 and $\pm n$. If n is not an integer, then together with Theorem 3.24, it follows that the only rational points in E_n are $\mathcal{O}$ and $(0, 0)$, so T_n is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ in this case.

If n is an integer, then the points $(\pm n, 0)$ are in T_n with order two. If n is not congruent, we can then conclude from Theorem 3.24 that $T_n = \{\mathcal{O}, (0, 0), (\pm n, 0)\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. If n is congruent, then we show that there is no rational point (x, y) with integer coordinates such that $y \neq 0$ and $y \mid D$; in fact, we can show that no such integer coordinate exists, as this would imply that the product of the integers $x-n$, x and $x+n$ is a non-zero perfect square, which is impossible. □

Corollary 3.26. 1 *and* 2 *are not congruent numbers.*

Proof. From Example 3.21, we see that the elliptic curves $y^2 = x^3 - x$ and $y^2 = x^3 - 4x$ do not have a rational point with $y \neq 0$, thus it follows from Theorem 3.24 that 1 and 2 are not congruent. □

Another key result that characterises a congruent number is the following:

Theorem 3.27. *A positive integer n is congruent if and only if the group of rational points $E_n(\mathbb{Q})$ on the elliptic curve*

$$E_n : y^2 = x^3 - n^2x$$

has positive rank.

Proof. See [Kob12, Proposition 18]. □

4. Conclusion

In this paper, we have provided an overview of the motivations and fundamental steps of the study of rational points on elliptic curves through the lens of abstract algebra, revisited Mordell's theorem which asserts that it is possible to reproduce all rational points on an elliptic curve with a finite number of generators. Some applications of this theorem, including rank computation and congruent number problem, are also discussed.

References

[Bro00] Ezra Brown. "Three Fermat trails to elliptic curves". In: *College Math. J.* 31.3 (May 2000), pp. 162–172.

[Con07] Keith Conrad. *Proofs by Descent*. 2007. URL: `https://kconrad.math.uconn.edu/blurbs/ugradnumthy/descent.pdf`.

[Con08] Keith Conrad. "The Congruent Number Problem". In: *The Harvard College Mathematics Review* 2.2 (2008). URL: https://legacy-www.math.harvard.edu/hcmr/issues/2a.pdf.

[Dan+17] Harris B. Daniels et al. "Torsion subgroups of rational elliptic curves over the compositum of all cubic fields". In: *Mathematics of Computation* 87.309 (May 2017), pp. 425–458. ISSN: 1088-6842. DOI: 10.1090/mcom/3213. URL: http://dx.doi.org/10.1090/mcom/3213.

[DF03] David S Dummit and Richard M Foote. *Abstract Algebra*. en. 3rd ed. Nashville, TN: John Wiley & Sons, June 2003.

[Elk24] Noam Elkies. *Z^{29} in $E(Q)$*. 2024. URL: https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;b9d018b1.2409&FT=&P=&H=&S=b.

[Ful08] William Fulton. *Algebraic curves*. 3rd ed. Self-published, 2008. URL: https://dept.math.lsa.umich.edu/~wfulton/CurveBook.pdf.

[Ha10] Jan Hilmar and Chris Smyth and. "Euclid Meets Bézout: Intersecting Algebraic Plane Curves with the Euclidean Algorithm". In: *The American Mathematical Monthly* 117.3 (2010), pp. 250–260. DOI: 10.4169/000298910X480090. eprint: https://www.tandfonline.com/doi/pdf/10.4169/000298910X480090. URL: https://www.tandfonline.com/doi/abs/10.4169/000298910X480090.

[Hus03] Dale Husemoller. *Elliptic Curves*. en. 2nd ed. Graduate Texts in Mathematics. New York, NY: Springer, Dec. 2003.

[Kob12] Neal I Koblitz. *Introduction to elliptic curves and modular forms*. en. 2nd ed. Graduate texts in mathematics. New York, NY: Springer, Dec. 2012.

[Mat16] Ryota Matsuura. *How to Transform a Cubic (With a Rational Point) into Weierstrass Normal Form*. 2016. URL: http://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2016/02/Matsuura-projective_transformation.pdf.

[Mil20] James S Milne. *Elliptic curves*. 2nd ed. World Scientific Publishing, Sept. 2020.

[SI25] Neil J. A. Sloane and The OEIS Foundation Inc. *A003273 - The on-line encyclopedia of integer sequences*. 2025. URL: https://oeis.org/A003273.

[Sil06] Joseph H. Silverman. *An Introduction to Height Functions*. 2006. URL: https://legacy.slmath.org/attachments/workshops/301/HtSurveyMSRIJan06.pdf.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*. en. 2nd ed. Graduate texts in mathematics. New York, NY: Springer, Dec. 2009.

[SS03] Elias M Stein and Rami Shakarchi. *Complex analysis*. en. Princeton lectures in analysis. Princeton, NJ: Princeton University Press, Apr. 2003.

[ST15] Joseph H Silverman and John T Tate. *Rational points on elliptic curves*. en. 2nd ed. Undergraduate texts in mathematics. Cham, Switzerland: Springer International Publishing, June 2015.

[Sut23] Andrew Sutherland. *Elliptic curves over C (part II)*. 2023. URL: https://math.mit.edu/classes/18.783/2023/LectureNotes15.pdf.

[Tak23] Takashi Takebe. *Elliptic integrals and elliptic functions*. en. Cham: Springer International Publishing, 2023.

[The24] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.5)*. https://www.sagemath.org. 2024.

[Tun83] J B Tunnell. "A classical Diophantine problem and modular forms of weight 3/2". en. In: *Invent. Math.* 72.2 (June 1983), pp. 323–334.

[Whi18] Debbie D White. *The Congruent Number Problem*. 2018. URL: https://math-sites.uncg.edu/sites/yasaki/publications/debbie-white-congruent-numbers-2018.pdf.