Introduction to Elliptic Curves

Alexandra Sklyarova

Math 4480: Spring 2025

Abstract

Elliptic curves are among the most elegant and rich structures in mathematics, with deep connections to geometry, algebra, number theory, and cryptography. This paper aims to provide a comprehensive introduction to elliptic curves, highlighting both their intrinsic mathematical beauty and their wide-ranging applications. Beginning with a historical overview and motivation rooted in Diophantine equations, the project introduces the fundamental definitions and explores the origin of the term "elliptic." Then we will cover the basics of projective geometry, which lays the foundation for all of the later arithmetic. We then delve into the group structure of rational points, including the Weierstrass normal form and the formulas for point addition and duplication. A significant portion of the paper is dedicated to the study of torsion points, and gives the full proof of the Nagell - Lutz Theorem as well as the statement of Mazur's Theorem. Additionally, the structure of the group of rational points is explored further with a discussion of Mordell's Theorem. From there, we transition to the behavior of elliptic curves over finite fields, particularly $\mathbb{F}_p$ and its extension $\mathbb{F}_q$, which sets the stage for a discussion of elliptic curve cryptography (ECC). The final sections describe the ECC protocol, highlight its real-world implementation by major companies, and present interactive exercises to illustrate the encryption and decryption process. The project serves as an extended exploration of "Rational Points on Elliptic Curves" by Silverman and Tate, whose insights guide much of the paper.

1 Introduction

1.1 Brief History of Diophantine Equations

In $\sim$ 250AD, Diophantus published his book titled "Arithemtika" which introduced very basic algebraic equations and outlined methods for extracting their solutions. The equations, later referred to as Diophantine, serve as a gateway to the study of number theory and algebraic geometry. They are algebraic equations (or systems) with integer coefficients, where solutions are sought in integers or rational numbers.

Important questions:

Are there rational or integer solutions?
How many solutions are there? It could be none, finite, or infinite.
Is there a structure to solutions? How does this vary depending on different parameters?

We can look at a few examples to illustrate how we can approach finding solutions.

Example 1 : let $a_i \in \mathbb{Z}$ for $0 \leq i \leq n$

$$a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x_a + 0$$

This is one of the simplest Diophantine equations since it is in one variable. Gauss' lemma says that that if $\frac{u}{v}$ is an initial solution then $v|a_0$ and we can get a list of candidate solutions and subsequently check them all to determine an actual list of solutions.

Example 2 : suppose we have

$$ax + by = 1, \ \gcd(a, b) = 1$$

To solve for x, y we can use the Euclidean algorithm to get initial solutions x_0 and y_0, then we can generate infinite solutions

$$x = x_0 + bn, \quad y = y_0 - an, \quad n \in \mathbb{N}$$

Example 3: consider

$$x^2 + y^2 = z^2$$

This is commonly referred to as a Pythagorean triple. Similarly to the first equation, it is possible to generate infinite solutions as long as they satisfy

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2, \quad \gcd(m, n) = 1$$

While seemingly simple, their solutions (or lack thereof) require some of the most powerful and cutting edge tools that math has to offer. In particular, mathematicians such as Bachet, Fermat, Euler, Lagrange, and Gauss have greatly expanded on this study. Perhaps most famously, Fermat's Last Theorem, states that for $n > 2$ that

$$a^n + b^n = c^n$$

cannot be solved with $a, b, c \in \mathbb{Z}^+$. This theorem went unproven for centuries and it was only recently solved using modular forms, Iwasawa theory, category theory, and more. This unexpectedly difficult proof further shows how nuanced and complex Diophantine equations are, which is why it is important to study them with care and precision. Elliptic curves are perhaps among the most subtle and intricate Diophantine equations, so it is worth exploring them thoroughly.

1.2 What is an Elliptic Curve?

We will start by giving the most general form of an elliptic curve:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

With coefficients in some field (we will mainly examine the curve over $\mathbb{Q}$ and $\mathbb{F}_p$).

Our **main objective** will be to study elements of $\underline{\mathbf{C}(\mathbb{Q})}$, which we will use to refer to rational points on our elliptic curve. Note, in general $C(\mathbb{F})$, where $\mathbb{F}$ is some field, just refers to points in the given field that are on our curve C.

We will also look at different forms of the equation (later sections). Additionally, there are several perspective that we can approach the curve:

Algebraic: we will use polynomial equations to define rational points, torsion structures, and more.

Geometric: we will utilize it to study the shape and structure of the curve, especially to visualize its group law and to understand how points interact on the curve in projective space.

Analytic: we will use it to understand elliptic curves as quotients of the complex plane by lattices, using Weierstrass $\wp$-functions. This view connects elliptic curves to complex analysis, allowing us to study them as complex tori.

1.3 Why we call them "Elliptic" Curves

After seeing the equation, it is reasonable to question the name since it is clearly not an ellipse. While initially misleading, the name actually **is** related to ellipses since these equations were used in the computation of ellipse arc length. Recall, if your ellipse is of the form

$$\frac{x^2}{a} + \frac{y^2}{b} = 1$$

Then we get the following integral

$$\int_{-a}^{a} \sqrt{\frac{a^2 - (1 - b^2/a^2)x^2}{a^2 - x^2}} dx$$

Then if you let $k = 1 - b^2/a^2$ and perform the substitution $x \mapsto ax$ out integral becomes

$$\int_{-1}^{1} \frac{1 - k^2x^2}{\sqrt{(1 - x^2)(1 - k^2x^2)}}$$

and if you let

$$y = \sqrt{(1 - x^2)(1 - k^2x^2)} \Rightarrow y^2 = (1 - x^2)(1 - k^2x^2)$$

You get a quartic elliptic curve!
So, it is clear that their study has far reaching applications as well as a deep history in mathematics in general.

2 Projective Geometry

2.1 Projective Plane

Let $\mathbb{P}^2$ denote the projective plane. We will give two constructions of $\mathbb{P}^2$, one algebraic and the other geometric.

Algebraic: Consider two equations,

$$x^n + y^n = 1 \text{ and } X^n + Y^n = Z^n$$

We can ask, how do we relate the two equations. To do this, first suppose that $(a, b, c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ is a solution to $f(X, Y, Z)$. We see that $(\lambda a, \lambda b, \lambda c)$ for $\lambda \in \mathbb{Z}$ is also a solution. Interestingly, we also see that the second equation contains points that the first one doesn't have, namely $(1, -1, 0)$ and $(-1, 1, 0)$. So we can create a sequence

$$(a_i, b_i, c_i) \to (1, -1, 0) \text{ as } i \to \infty$$

So our solutions

$$\left(\frac{a_i}{c_i}, \frac{b_i}{c_i}\right) \to (\infty, \infty) \text{ as } (a_i, b_i, c_i) \to (1, -1, 0)$$

We see that our extra solutions correspond to points at infinity.
Now we can actually construct $\mathbb{P}^2$. Define an equivalence relation where

$$[a, b, c] \sim [a', b', c'] \text{ if } a = \lambda a', a = \lambda b', c = \lambda c'$$

Then we have

$$\mathbb{P}^2 = \{[a, b, c] : a, b, c \neq 0\}/\sim$$

Geometric : We can begin by describing the Euclidean Affine plane

$$\mathbb{A}^2 = \{(x, y) : x, y \text{ any numbers}\}$$

Then we can describe lines in the projective plane. It consists of a line in $\mathbb{A}^2$ along with the point at infinity, and it is determined by the direction. A direction in $\mathbb{A}^2$ refers to the set of line going through the origin defined by

$$Ax = By$$

With some $A, B \neq 0$ (not unique). We can also consider directions as an equivalence relation, where two lines are in the same equivalence class if they are parallel. Then we can define the projective plane using those directions

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \{\text{set of directions in } \mathbb{A}^2\}$$

Correspondence Between Constructions: We can relate the algebraic and geometric perspectives via

$$\{[a, b, c] : a, b, c \neq 0\}/\sim \;\longleftrightarrow\; \mathbb{A}^2 \cup \{\text{set of directions in } \mathbb{A}^2\}$$

$$[a, b, c] \to \begin{cases} (\frac{a}{c}, \frac{b}{c}) \in \mathbb{A}^2, & c \neq 0 \\ (a, b) \in \mathbb{P}^1, & c = 0 \end{cases}$$

$$[x, y, 1] \leftarrow (a, b) \in \mathbb{A}^2$$

2.2 Curves

An Algebraic curve in $\mathbb{A}^2$ is the set of solutions to a polynomial $f(x, y) = 0$. To write a curve in $\mathbb{P}^2$, we can use three variable X, Y, Z and define
Homogeneous Polynomial: $F(X, Y, Z)$ of degree d which satisfies

$$F(tX, tY, tZ) = t^d F(X, Y, Z)$$

Projective Curve is $C : F(X, Y, Z) = 0$. Then if we define $f(x, y) = F(X, Y, 1)$, we can create the following map

$$\{[a, b, c] \in C : c \neq 0\} \to \{(x, y) \in \mathbb{A}^2 : f(x, y) = 0\}$$
$$[a, b, c] \mapsto \left(\frac{a}{c}, \frac{b}{c}\right)$$

Tying back to our study, suppose we have $C : F(X, Y, Z) = 0$ with coefficients in $\mathbb{Q}$. Then we can see that the rational points on C are

$$C(\mathbb{Q}) = \{[a, b, c] \in \mathbb{P}^2 : f(a, b, c) = 0,\ a, b, c \in \mathbb{Q}\}$$

Versus, if we have affine rational curve $C_0 : f(x, y)$ then we see that $C(\mathbb{Q})$ consists of points in $C_0(\mathbb{Q})$ along with the points at infinity.

2.3 Singular Curves

We call a curve at a point P $\mathbf{non-singular}$ if at least one partial derivative doesn't vanish at P. this means

$$\text{either } \frac{\delta f}{\delta x} \neq 0 \text{ or } \frac{\delta f}{\delta y} \neq 0$$

Similarly, a point is **singular** if both partial derivatives vanish.
If every point on our curve C is non-singular then we say C itself is non-singular. For our purposes, we will be working exclusively with non-singular elliptic curves.

3 Structure of Elliptic Curves

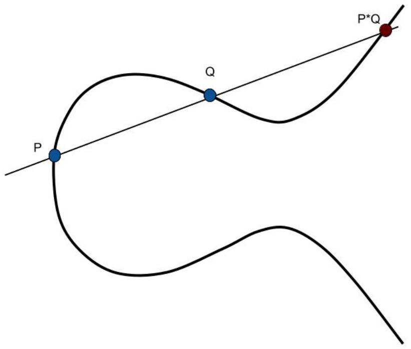
3.1 Group Law

Our goal in this section is to establish a group law in our set of rational points on an elliptic curve. Recall the general form of a cubic is

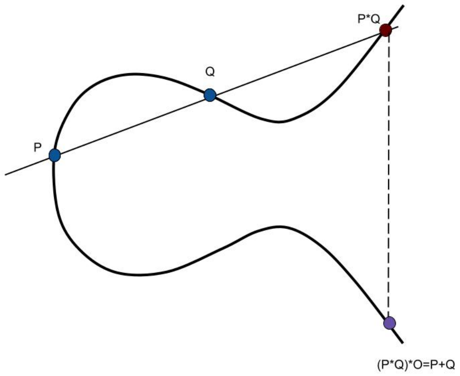
$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

and suppose all of the coefficients are rational. We want to study the rational points on some arbitrary rational elliptic curve. To begin, we need to be able to show that if we take two rational points $P, Q \in C(\mathbb{Q})$, we can compose them in some way that will get us another point on the curve. Generally, if we do have those two points then we typically can find a third.

Composition: the first step to establishing a group law is deciding what the operation will be. We begin by describing composition, which refers to the act of drawing a line through two points $P, Q \in C(\mathbb{Q})$ and the re-intersection with the curve is the point $P * Q$



Group Operation: the composition is a good start, but it doesn't quite work for a group. So we can recall our point at infinity from the projective geometry section. If we use this point, call it $\mathcal{O}$, and compose it with our $P * Q$, we get another point on the curve. We will call the operation $(P * Q) * \mathcal{O} = P + Q$

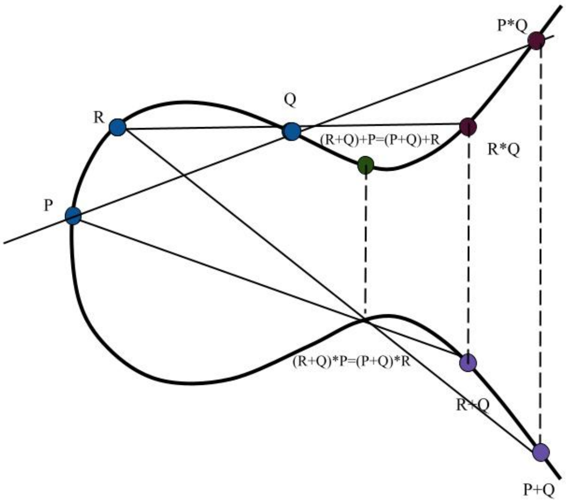


Now we just need to verify that this is a valid group operation.

Identity verification: claim that $P + \mathcal{O} = P$. This is clear since if we join $P * \mathcal{O}$ and then draw out $(P * \mathcal{O}) * \mathcal{O}$, it re-intersects the curve precisely at P.

Inverses verification: based on how we defined $\mathcal{O}$, it is easy to see that if P is on the curve then the reflection of P, which is $-P$, is also on the curve since (as we will prove rigorously later) the standard form of a cubic is symmetric around the x-axis.

Associativity: this is best demonstrated using a picture



Remark 1: if the line through P and Q is tangent to P then the third point of intersection is either P or Q.
Remark 2: if P is an inflection point then the tangent line meets the curve three times at P, i.e. $P * P = P$
Remark 3: our point at identity is not unique, in fact if we have identities $\mathcal{O}$ and $\mathcal{O}'$ then there exists an isomorphism between groups **C with identity** $\mathcal{O}$ and **C with identity** $\mathcal{O}'$ via

$$P \mapsto P + (\mathcal{O}' - \mathcal{O})$$

3.2 Weierstrass Normal Form

Our goal is to transform our cubic into a standard form called Weierstrass normal form

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

We will show that we can reconstruct our generalized equation using birational transformations, thus preserving our set of rational points.
We begin with some cubic in $\mathbb{P}^2$, the idea is to choose specific axes that allow our curve to take a particular form.

We give the following steps:

1. Given $\mathcal{O} = [1, 0, 0]$ we take a tangent line to that, call it $Z = 0$.
2. The point where $Z = 0$ intersects the curve is at $[0, 1, 0]$ and then we take a tangent line to that, call it $X = 0$.
3. Choose any other line through $\mathcal{O}$ and call in $Y = 0$

4. Now let

$$x = \frac{X}{Z} \text{ and } y = \frac{Y}{Z}$$

This gives us linear conditions on the form of the equation we need. Note that this is called a projective transformation.

5. Using that substitution, C takes the form

$$xy^2 + (ax + b)y = cx^2 + dx + e$$

6. Multiply by x

$$(xy)^2 + (ax + b)xy = cx^3 + dx^2 + ex$$

7. Rename xy to y

$$y^2 + (ax + b)y = \text{cubic in x}$$

8. Replace $y \mapsto y - \frac{1}{2}(ax + b)$

$$y^2 = \text{cubic in x}$$

This transformation is rational, which is exactly what we needed.

3.3 Addition Formula

Now that we can put all of our cubics into one nice form

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

We can now use algebraic methods to compute point addition (thus making our group law more explicit)

1. First let

$$\mathbf{P_1} = (\mathbf{x_1}, \mathbf{x_2}) \text{ and } \mathbf{P_2} = (\mathbf{x_2}, \mathbf{y_2})$$

The goal is to compute

$$\mathbf{P_1} * \mathbf{P_2} = (\mathbf{x_3}, \mathbf{y_3}) \text{ and } \mathbf{P_1} + \mathbf{P_2} = (\mathbf{x_3}, -\mathbf{y_3})$$

2. Now, recall we want to draw a line through P_1 and P_2, call this line

$$y = \lambda x + \nu$$

Where

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

3. Then substitute

$$y^2 = (\lambda x + \nu)^2 = x^3 + ax^2 + bx + c$$
$$\Rightarrow x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = (x - x_1)(x - x_2)(x - x_3) = 0$$

4. So our x_3 is the desired coordinate since the three roots of this cubic correspond to the three points of intersection with the curve. Rearranging we would get the relation

$$x_1 + x_2 + x_3 = \lambda^2 - a$$

From there, we get the following formulas

$$\mathbf{x_3} = \lambda^\mathbf{2} - \mathbf{a} - \mathbf{x_1} - \mathbf{x_2} \qquad \mathbf{y_3} = \lambda \mathbf{x_3} + \nu$$

3.4 Duplication Formula

Now suppose we want to add a point $P = (x, y)$ to itself. We can't use the formula above since that would mean $\lambda = \frac{0}{0}$. So we can reformulate to use slope in a different sense i.e.

$$\lambda = \frac{f'(x)}{2y}$$

We can also substitute this λ into the equation for our curve as we did above and get the following formula for the x coordinate of $2P$:

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

4 Analytic Perspective

4.1 Weierstrass Theory

Recall, we described a method for deriving Weierstrass for for an elliptic curve, specifically we have

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

We can also put it into a different form (more suited for our analytic perspective) using the transformation

$$x - \frac{1}{3}a = x \quad \text{and} \quad x \mapsto 4x, \ y \mapsto 4y$$

To get

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

Weierstrass theory of elliptic functions says that if those $g_1, g_2 \in \mathbb{C}$ s.t. y^2 has distinct roots, then you can find

$$\omega_1, \omega_2 \in \mathbb{C}$$

by evaluating specific integrals (we will refer to the ωs as periods). These periods are in fact $\mathbb{R}$ linearly independent and we can look at their $\mathbb{Z}$ linear combinations i.e. the following lattice

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

Using our periods, we can also define the **Weierstrass $\wp$ function**:

$$\wp(u) = \frac{1}{u^2} + \sum_{\omega \in \mathcal{L}, \omega \neq 0} \left(\frac{1}{(u - \omega)^2} - \frac{1}{\omega^2} \right), \quad u \in \mathbb{C}$$

This is a meromorphic function that has poles exclusively at lattice points and nowhere else in the complex plane. Note also that $\wp$ is doubly periodic, meaning

$$\wp(u + \omega) = p(u) \quad \forall u \in \mathbb{C}, \omega \in \mathcal{L}$$

4.2 A Useful Mapping

Now we can ask, how is this related to the study of points on our curve?
First, we see that $\wp(u)$ satisfies the differential equation

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

So for every $u \in \mathbb{C}$ we get a point

$$P(u) = (\wp(u), \wp'(u))$$

Which means $\wp$ function allows us to create a map

$$P : \text{complex plane} \to C(\mathbb{C})$$

this map sends points on the lattice (poles) to $\mathcal{O}$, so the kernel is $\mathcal{L}$. Additionally, this map is surjective since every (x, y) is determined by some u in the preimage. This map also has the property

$$P(u_1 + u_2) = P(u_1) + P(u_2)$$

Where the LHS is addition in $\mathbb{C}$ and the RHS is our point addition formula for C. It follows that P is homomorphism.
Additionally, we see that

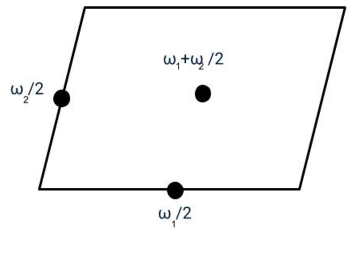
$$\text{complex plane}\big/_{\mathcal{L}} \simeq C(\mathbb{C})$$

which means that the group of complex points is a torus, i.e. $S^1 \times S^1$.

4.3 Period Parallelogram

This construction can be useful when discussing points of finite order. It allows us to use the **period parallelogram** to determine points of finite order. The period parallelogram is essentially a fundamental region that defines a lattice within the complex plane.
Suppose we want to find points of order dividing n. Then we would simply look at points in the period parallelogram s.t. $nu \in \mathcal{L}$.

We demonstrate the case for order $n = 2$ below.



5 Introduction to Torsion Points

We say an element of $C(\mathbb{Q})$ has order n if we have that n is the smallest integer s.t.

$$nP = \underbrace{P + P + ... + P}_{n-times} = \mathcal{O}$$

In this section, we will outline how to compute points of order 2 and 3. In later sections, we will cover how to study general points of finite order.

5.1 Order 2

Proposition: Let C be a non singular cubic $y^2 = x^3 + ax^2 + bx + c$. Then we have:
(i) a point $P = (x, y) \neq \mathcal{O}$ on C has order 2 if $y = 0$
(ii) C has exactly four point of order dividing 2. Those points form a group which is isomorphic to $C_2 \times C_2$.

proof: We see that

$$2P = \mathcal{O} \Rightarrow P = -P$$

Then since $-(x, y) = (x, -y)$, we see that points of order two are precisely where $\mathbf{y} = \mathbf{0}$.

$$P_1 = (\alpha_1, 0),\ P_2 = (\alpha_2, 0),\ P_3 = (\alpha_3, 0)$$

Where each α_i is a root of our cubic $x^3 + ax^2 + bx + c$. If we allow complex coordinates, then there are always precisely 3 points of order 2, and since we have the non-singular requirement we know that these roots are distinct.
We can write down all of the points of order dividing 2:

$$\{\mathcal{O}, P_1, P_2, P_3\}$$

Since every element has order 1 or 2, we see that the only possibility is that this group is $C_2 \times C_2$.
Note, if we work exclusively in $C(\mathbb{Q})$ then we get three possibilities for this group:

$$C_2 \times C_2,\ C_2,\ \{\mathcal{O}\}$$

Recall, we demonstrated what order 2 points look using the period parallelogram in the previous section. This algebraic construction is a verification that different perspectives of elliptic curves give the same results.

5.2 Order 3

Proposition: As before, let C be a non singular cubic $y^2 = x^3 + ax^2 + bx + c$. Then we have:
(i) a point $P = (x, y) \neq \mathcal{O}$ on C has order 3 if x is a root of the polynomial

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

(ii) C has exactly nine points of order dividing 3. They form a group isomorphic to $C_3 \times C_3$

proof: Similarly to our order 2 points, we see

$$3P = \mathcal{O} \Rightarrow 2P = -P$$

So if we take $P \neq \mathcal{O}$ then we can use the duplication formula

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

Multiplying the denominator and rewriting we get

$$x^4 - 2bx^2 - 8cx + b^2 - 4ac = 4x^4 + 4ax^3 + 4bx^2 + 4cx \;\Rightarrow\; 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2 = 0$$

So we do in fact see that x has order 3 if it is a root of the polynomial above.
Next, we see that since the x coordinate of

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

we can rewrite $\psi_3(x)$ as

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

We claim that it has 4 distinct roots. Note that $\psi_3'(x) = 2f(x)f'''(x) = 12f(x)$, so if ψ_3 had common roots then so would $2f(x)f'''(x)$ and $12f(x)$, which would contradict the non singular assumption. So let $\beta_1, \beta_2, \beta_3, \beta_4$ be those four distinct complex roots. Then define

$$\gamma_i = \sqrt{f(\beta_i}$$

From the previous part of the proof, we get the set

$$\{(\beta_1, \pm\gamma_1),\ (\beta_2, \pm\gamma_2),\ (\beta_3, \pm\gamma_3),\ (\beta_4, \pm\gamma_4)\}$$

Which is now the full set of order 3 points on C. Note also that no $\gamma_i = 0$ since that would make it an order 2 point. Further, we know that the corresponding group for points of order dividing 3 must be $C_3 \times C_3$. If we restrict to $C(\mathbb{Q})$, get the following possibilities

$$C_3 \text{ or } \{\mathcal{O}\}$$

6 Nagell-Lutz Theorem

The goal of this section is to give a proof of the Nagell-Lutz Theorem. In the previous part, we classified points of order 2 and 3, it is now natural to ask what points of general order look like. This theorem gives insight on how to find desired points.
Brief History : This theorem comes as a result of the world of Elisabeth Lutz and Trygve Nagell. Lutz was known for her work on p-adic Diophantine approximation. Similarly, Nagell also primarily worked on Diophantine equations. Interestingly, the two proved it independently, Nagell in 1935 and Lutz in 1937. It is then necessary to note how extraordinary it was for a women to be credited with such a contribution considering the historical period during which the proofs were published.

We will now state the theorem and break this section into several subsections, which each give an essential part of the proof. Note that this proof is directly from the book Rational Points on Elliptic Curves, so credit goes to Silverman and Tate as well as its original provers.

Theorem (**Nagell – Lutz**) Let

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

be a non-singular cubic curve with integer coefficients. Let

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

be the discriminant of $f(x)$. Then let $P = (x, y)$ be a rational point of finite order, then $x, y \in \mathbb{Z}$. Also, we have two cases, either $y = 0$, which means P has order 2, or $y|D$.

6.1 Understanding Integer Coordinates

Proposition: let p be a prime, R be the ring of rational numbers having a denominator prime to p, and take $C(p^v)$ be the set of rational points (x, y) on the curve C for which x has the denominator divisible by p^{2v} (include $\mathcal{O}$). Then we have:
(i) $C(p)$ consists of rational point (x, y) s.t. the denominator of either x or y is divisible by p.
(ii) For all $v \geq 1$, the set $C(p^v)$ is a subgroup of $C(\mathbb{Q})$
(iii) The map

$$\frac{C(p^v)}{C(p^{3v})} \to \frac{p^vR}{p^{3v}R}, \quad P = (x, y) \mapsto t(P) = \frac{x}{y}$$

is an injective homomorphism.

proof: the idea here is to show that a coordinate is an integer by proving that no primes divide its denominator. We will use the following notation for any arbitrary non zero rational number:

$$\frac{m}{n}p^v, \quad \gcd(m, p) = 1, \ \gcd(n, p) = 1$$

We will also refer to the order of a rational number as

$$\text{ord}(\frac{m}{n}p^v) = v$$

Now take $P = (x, y)$ and let

$$x = \frac{m}{np^\mu}, \quad y = \frac{u}{wp^\sigma} \quad \text{with } \mu > 0, \ p \nmid m, n, u, w$$

We can plug this into our Weierstrass form of the cubic and get

$$\frac{u^2}{w^2p^{2\sigma}} = \frac{m^3 + am^2np^\mu + bmn^2p^{2\mu} + cn^3p^{3\mu}}{n^3p^{3\mu}}$$

We know $p \nmid u^2, w^2$ so $\text{ord}(\frac{u^2}{w^2p^{2\sigma}}) = -2\sigma$. then since $\mu > 0$ and $p \nmid m$, we get that $p \nmid m^3 + am^2np^\mu + bmn^2p^{2\mu} + cn^3p^{3\mu}$, so the order of the RHS is -3μ.

So, we get

$$2\sigma = 3\mu$$

Then $p|$(denominator of y) and $2|\mu$, $3|\sigma$, so

$$\mu = 2v \quad \sigma = 3v$$

So let

$$C(p^v) = \{(x, y) \in C(\mathbb{Q}) : \text{ord}(x) \leq -2v,\ \text{ord}(y) \leq -3v\}$$

Which means that a point of finite order cannot lie in $C(p)$.

Now we want to show that each $C(p^v)$ is a subgroup of $C(\mathbb{Q})$. Let

$$t = \frac{x}{y} \quad s = \frac{1}{y}$$

Which transforms

$$y^2 = x^3 + ax^2 + bx + c \ \Rightarrow\ s = t^2 + at^2s + bts^2 + cs^3$$

Note that $\mathcal{O}$ now lines at $(0, 0)$ and a line $y = \lambda x + \nu$ in the (x, y)-plane no corresponds to a line $s = \frac{-\lambda}{\nu}t + \frac{1}{\nu}$ in the (t, s)-plane.

Now define R_p to be the ring with no p in the denominator of rational numbers. Let $(x, y) \in C(p^v)$. Then

$$x = \frac{m}{np^{2(v+i)}} \quad y = \frac{u}{wp^{3(v+i)}}$$

transform into

$$t = \frac{x}{y} = \frac{mw}{nu}p^{v+i} \quad s = \frac{1}{y} = \frac{w}{u}p^{3(v+i)}$$

So we get that $(t, s) \in C(p^v)$ if and only if $t \in p^vR$ and $s \in p^{3v}R$. Now to show that $C(p^v)$s are subgroups, we need to check if they are closed under point addition. So, let

$$P_1 = (t_1, s_1) \quad P_2 = (t_2, s_2)$$

If we have $t_1 = t_2$ then we get $P_1 = -P_2$, so $P_1 + P_2 \in C(p^v)$. Now suppose the points are distinct. Let $s = \alpha t + \beta$ be the line through the points, with usual slope. This means $P_1 = (t_1, s_1)$ and $P_2 = (t_2, s_2)$ satisfy

$$s = t^3 + at^2s + bts^2 + cs^3$$

We get the relation

$$s_2 - s_1 = b((t_2 - t_1)s_2^2 + t_1(s_2^2 - s_1^2)) + c(s_2^3 - s_1^3)$$

Then we get

$$\alpha = \frac{t_2^2 + t_1t_2 + t_1^2 + (at_2 + at_1)s_2 + bs_2^2}{1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1s_2 + s_1^2)}$$

Since there is a 1 in the denominator, it is clear that α is a unit in R.

Now, let $P_3 = (t_3, s_3)$ be the third point of intersection of the line $s = \alpha t + \beta$ with the cubic. We want to construct an equation whose roots are t_1, t_2, t_3. So we substitute $s = \alpha t + \beta$ into $s = t^3 + at^2s + bts^2 + cs^3$ and get

$$\alpha t + \beta = t^3 + at^2(\alpha t + \beta) + bt(\alpha t + \beta)^2 + c(\alpha t + \beta)^3 = \text{constant} \cdot (t - t_1)(t - t_2)(t - t_3)$$

Then we get the relation

$$t_1 + t_2 + t_3 = -\frac{\alpha\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + b\alpha^2 + c\alpha^3}$$

This gives us a formula for t_3, so we can draw a line through P_3 and $(0, 0)$. We know that if (s, t) in on our curve then so is $(-t, -s)$, so we get that our third point of intersection is $(-t_3, -s_3)$ i.e. our $P_1 + P_2$. Now we just need to verify that it is indeed in $C(p^v)$.

So we now list all of the important results that will lead to the conclusion:
numerator$(\alpha) \in p^{2v}R$, $t_1, t_2, s_1, s_2 \in p^vR$, $-at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1s_2 + s_1^2) \in p^{2v}R$:

The denominator is a unit of R

$s_1 \in p^{3v}R$, $\alpha \in p^{2v}R$, $\beta \in p^{3v}R$, $1 + a\alpha + b\alpha^2 + c\alpha^3$ is a unit in R:

$$t_1 + t_2 + t_3 \in p^{3v}R$$

$t_3 \in p^vR$ and $-t_3 \in p^vR$:

$C(p^vR)$ is closed under addition and under taking negatives

Then we conclude that

$\mathbf{C(p^v)}$ is a subgroup of $\mathbf{C}(\mathbb{Q})$

We see that

$$t(P_1 + P_2) \equiv t(P_1) + t(P_2) \mod p^{3v}R$$

Which means it is almost a homomorphism. To ensure it preserves structure fully, we construct the map

$$\frac{C(p^v)}{C(p^{3v})} \to \frac{p^vR}{p^{3v}R}, \quad P = (x, y) \mapsto t(P) = \frac{x}{y}$$

Where the kernel is $t(P) \in p^{3v}R$ i.e. $C(p^{3v})$.

Corollary : For all primes p, the subgroup $C(p)$ contains no points of finite order. Also, if $P = (x, y) \neq \mathcal{O}$ is a rational point of finite order, then $x, y \in \mathbb{Z}$

proof: let m be the order of P. Take any prime p. We will show $P \notin C(p)$. Suppose for a contradiction that it is contained in $C(p)$. It may be contained in some smaller $C(p^v)$, but it can't be contained in all powers of p. So there exists some $v > 0$ s.t. $P \in C(p^v)$ but $P \notin C(p^{v+1})$.

Case 1: $p \nmid m$. Writing $t(P_1 + P_2) \equiv t(P_1) + t(P_2) \mod p^{3v}R$ repeatedly gives formula $t(mP) \equiv mt(P) \mod p^{3v}R$. Some $mP = \mathcal{O}$, we have $t(mP) = \mathcal{O}$. On the other hand, since m is coprime to p, it must be a unit in R, hence $0 \equiv t(P) \mod p^{3v}R$, which means $P \in C(p^{3v})$ contradicting $P \notin C(p^{v+1})$.

Case 2: $p|m$. First, write $m = pn$ and look at $P' = nP$. Since P has order m, we know that P' has order p. Also since $P \in C(p)$ we see that $P' \in C(P)$ (since it is a subgroup). So we can again find

$v > 0$ s.t. $P' \in C(p^v)$ but $P' \notin C(p^{v+1})$. Then we write $0 \equiv t(\mathcal{O}) = t(pP') \equiv pt(P') \mod p^{3v}R$. This means that $t(P') \equiv 0 \mod p^{3v}R$. But since $3v - 1 \geq v + 1$, we get a contradiction.

Lastly, if $P = (x, y)$ is a point of finite order then $P \notin C(p)$ for all primes p. This means that no prime divides the denominator of x and y hence they are integers.

6.2 The Discriminant

Recall that a discriminant for a cubic polynomial is

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

To find rational points of finite order, we can find all divisors y of D and substitute them into the equation

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

$f(x)$ has integer coefficients with leading coefficient 1. So if it has an integer root, it will divide the constant term. Therefore, we have a finite amount of possibilities to check to find all of the points of finite order.
Lemma : let $P = (x, y) \in C$ s.t. P and $2P$ have integer coordinates. Then either $y = 0$ or $y|D$.

proof: assume $y \neq 0$ since this would imply that our point has order 2. So we will prove that $y|D$. Write $2P = (X, Y)$. By assumption $x, y, X, Y \in \mathbb{Z}$. The duplication formula gives

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

it is clear that $\lambda \in \mathbb{Z}$ as well. Then since $2y, f'(x) \in \mathbb{Z}$, we have $2y|f'(x)$, and since $y^2 = f(x)$, we have that $y|f(x)$. Now we can use the relation

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

Where

$$r(x) = (18b - 6a^2)x - (4a^3 - 15ab + 27c)$$

And

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

When evaluating at integer x, it is clear that all of the components of D will be integers. It then follows that $y|D$.

6.3 Restatement and Conclusion

Recall, the Nagell-Lutz Theorem states that if $P = (x, y)$ be a rational point of finite order, then $x, y \in \mathbb{Z}$. Also, we have two cases, either $y = 0$, which means P has order 2, or $y|D$.

From **6.2**, the Corollary states that $P = (x, y)$ be a rational point of finite order, then $x, y \in \mathbb{Z}$. From **6.3**, the Lemma states that if $P = (x, y) \in C$ s.t. P and $2P$ have integer coordinates, then either $y = 0$ or $y|D$.

So we have addressed all parts of the theorem and can now use it to get a list of points of finite order on our curve.

Warning 1: The theorem is not an if and only if statement. This means that you can have point $P = (x, y)$ where $x, y \in \mathbb{Z}$ and $y|D$ but it is not a point of finite order.
Warning 2: You cannot use the theorem to show that any one specific point has finite order. To do this, you still have to find $n \in \mathbb{Z}$ s.t. $nP = \mathcal{O}$. However, you can use it to show that a point has infinite order by duplicating the point until you get a point whose coordinates are not integers.

7 Mazur's Theorem

Now that we have found a way to list all of the points of finite order for a cubic, we can ask which orders are possible. Additionally, we can try to see what subgroup the set of points of finite order forms in $C(\mathbb{Q})$. These are very complicated and nuanced questions, and the answer was initially conjectured by **Beppo Levi** in the early 1900s. The ideas were then reformulated by **Andrew Ogg** in 1971, and the conjecture was subsequently named after him. However, it wasn't until 1977 that **Barry Mazur** gave the full proof of the theorem. We give the full statement below.

Mazur′s Theorem: Let C be a non-singular rational cubic curve, and suppose that $C(\mathbb{Q})$ contains a point of finite order m. Then either

$$1 \leq m \leq 10 \quad \text{or} \quad m = 12$$

Additionally, the set of all points of finite order in $C(\mathbb{Q})$ forms a subgroup which has one of the following forms:
(i) A cyclic group C_N with $1 \leq N \leq 10$ or $N = 12$.
(ii) The product of a cyclic group of order two and a cyclic group of order N, $C_2 \times C_N$ of order $2N$ with $1 \leq N \leq 4$.

8 Mordell's Theorem

This elegant theorem was initially proposed by Poincare in 1901 and was finally proven in 1922 by Louis Mordell. An important generalization of it states that if you have an abelian variety A over a number field K then the group $A(K)$ (with points in K being consider "rational") is a finitely-generated abelian group, it is often called the Mordell Weil group. This is a bit too general (and complicated) for our case so we state our version of the theorem below.

Mordell′s Theorem : Let C be a non-singular cubic give with the equation

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

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

8.1 Height and Descent

Height : we define the height of some rational number $x = \frac{m}{n} \in \mathbb{Q}$ in lowest terms to be

$$H(x) = H\left(\frac{m}{n}\right) = \max\{\ |m|, |n|\}$$

Small Height : we define this to be

$$h(x) = h\left(\frac{m}{n}\right) = \log\left(H\left(\frac{m}{n}\right)\right)$$

We can then apply height to our study of cubic curves. Suppose we have $P = (x, y) \in C(\mathbb{Q})$, then we define the height of P as the height of the x coordinate

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

Note that $H(\mathcal{O}) = 1$.
We will also see that $C(\mathbb{Q})$ points have a finiteness property. More specifically for some given M,

$$\{P \in C(\mathbb{Q}) : H(P) \leq M\} \text{ is finite}$$

This also holds for small height, in which case the given M is a real number.

8.2 Descent Theorem

We will now introduce a theorem, which is more general than Mordell's, but leads to the same outcome. So, we will show this for some arbitrary abelian group Γ
Note, for any such abelian group Γ, the multiplication by m map is a homomorphism and the image is a subgroup in Γ

$$\Gamma \to \Gamma, \quad P \mapsto \underbrace{P + ... + P}_{m-times} = mP$$

Now define the height function of Γ,

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

Descent Theorem : Let Γ be an abelian group with the height function as described above. Suppose it satisfies:
1) For all $M \in \mathbb{R}$, the set $\{P \in \Gamma : h(P) \leq M\}$ is finite.
2) For all $P_0 \in \Gamma$, there exists a constant κ_0 such that $h(P + P_0) \leq 2h(P) + \kappa$.
3) There exists a constant κ such that $h(2P) \geq 4h(P) - \kappa$ for all $P \in \Gamma$.
4) $[\Gamma : 2\Gamma]$ is finite.
Then Γ is finitely generated.

proof: take a representative from each coset of 2Γ in Γ. There are only a finite number of such cosets, suppose that there are n. Let the representatives be

$$Q_1 ... Q_n$$

Now since for any $P \in \Gamma$, P has to be in one of the cosets, so we can write

$$P - Q_{i_1} = 2P_1, \quad \text{for some } P_1 \in \Gamma$$

So for any $P \in \Gamma$, there is index ξ_i s.t.

$$P - Q_i \in 2\Gamma$$

Now do the same with P i.e.

$$P_1 - Q_{i_2} = 2P_2, \; P_2 - Q_{i_3} = 2P_3, \; ..., P_{m-1} - Q_{i_m} = 2P_m$$

where $Q_1...Q_m$ are chosen from the n coset representatives. Now, since P_i is approximately equal to $2P_{i+1}$, then the height of P_{i+1} is more or less 1/4 of the height of P_i. So the sequence of points $P_1, P_2, ...$ should have decreasing height and eventually we will end up in a set of points with bounded height. From 1) we know that this set is finite. Now take the first equation again that says $P = Q_{i_1} + 2P_1$. Then substitute that into the next equation and repeat that process until you get

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + ... + 2^m P_m$$

This means that P is in the subgroup of Γ that is generated by the Q_is and P_m. We will now show that we can choose a large enough M that will allow us to force P_m to have height less than a certain fixed bound which doesn't rely on the initial choice of P. Then the finite set of points with heights less than this bound, along with the Q_is, will generate Γ.

So take one P_j and P_{j-1} and examine their heights. We will show that the height of P_j is significantly smaller than the height of P_{j-1}. So, using 2) with $-Q_i$ in place of P_0, we get a κ_i s.t.

$$h(P - Q_i) \leq 2h(P) + \kappa_i, \quad \forall P \in \Gamma$$

We can do this with any Q because there are a finite number of them, so we have

$$h(P - Q_i) \leq 2h(P) + \kappa'$$

Now, let κ be the constant from 3) and compute

$$4h(P_j) \leq h(2P_j) + \kappa = h(P_{j-1} - Q_{i_j}) + \kappa \leq 2h(P_{j-1}) = \kappa' + \kappa$$

Then we have

$$h(P_j) \leq \frac{1}{2}h(P_{j-1}) + \frac{\kappa' + \kappa}{4} = \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1}) - (\kappa' - \kappa))$$

So if $h(P_{j-1}) \geq \kappa' + \kappa$ then $h(P_j) \leq \frac{3}{4}h(P_{j-1})$. So as long as P_j satisfies $h(P_{j-1}) \geq \kappa' + \kappa$, the next points has much smaller height, which would eventually approach 0. So we will find some index m where $h(P_m) \leq \kappa' + \kappa$.

So every

$$P = a_1Q_1 + a_2Q_2 + ... + a_nQ_n + 2^m R \quad \text{for } a_1...a_n \in \mathbb{Z}, \; R \in \Gamma \text{ s.t. } h(R) \leq \kappa' + \kappa$$

Therefore the set

$$\{Q_1, Q_2, ..., Q_n\} \cup \{R \in \Gamma : h(R) \leq \kappa' + \kappa\}$$

generated Γ and it follows from 4) that it is indeed finite.

This is a truly genius argument that allows us to reach the conclusion that our abelian group $C(\mathbb{Q})$ is also finitely generated, which is incredible!

8.3 Crucial Lemmas

In our section about the Descent Theorem, we supposed that our group Γ satisfied **4** sets of criteria in order for it to be finitely generated. In this section, we will refer to each of them as Lemma (1-4) and will give a sketch for the proof of each, but using our usual group $C(\mathbb{Q})$ instead of Γ and for the elliptic curve

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

Lemma 1 : For all $M \in \mathbb{R}$, the set $\{P \in C(\mathbb{Q}) : h(P) \leq M\}$ is finite.
proof: this is the simplest of the lemmas. Just take any rational $P = \frac{m}{n} < M$. Then $|m|, |n| < M$ so there is a finite number of possibilities for m, n, which means the set of all Ps satisfying the height requirement is finite.

Lemma 2 : For all $P_0 \in C(\mathbb{Q})$, there exists a constant κ_0 such that $h(P + P_0) \leq 2h(P) + \kappa$.
proof: We will only give a sketch of this proof. So let $P = (\frac{m}{e^2}, \frac{n}{e^3})$. Suppose that $|m| \leq H(P)$ and $e^2 \leq H(P)$, then we claim that there is a constant $K > 0$ s.t. $|n| \leq KH(P)^{3/2}$. Plugging in P into Weierstrass form and using triangle inequality we will end up with

$$K = \sqrt{1 + |a| + |b| + |c|}$$

with a, b, c coefficients of the curve. Next, we will use our normal point addition formula for

$$P + P_0 = (\xi, \eta)$$

We will end up with the following form

$$\xi = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G}$$

with $A, B, C, D, E, F, G \in \mathbb{Q}$ which can be expressed in terms of $a, b, c, (x_0, y_0)$. Then plugging in $(\frac{m}{e^2}, \frac{n}{e^3})$, we find that

$$H(\xi) \leq \max\{|Ane + Bm^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|\}$$

Then using the fact that $e \leq H(P)^{1/2}$, $|n| \leq KH(P)^{3/2}$, and $m \leq H(P)$ along with triangle inequality, we get

$$H(P + P_0) = H(\xi) \leq \max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\}H(P)^2$$

Taking the logarithm we get that our desired constant is

$$\kappa_0 = \log \max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\}$$

Lemma 3 : There exists a constant κ such that $h(2P) \geq 4h(P) - \kappa$ for all $P \in C(\mathbb{Q})$.
proof: We will only give a sketch of this proof. Let $P = (x, y)$ and $2P = (\xi, \eta)$. Using our normal duplication formula we get

$$\xi = \frac{(f'(x))^2 - (8x + 4a)f(x)}{4f(x)}$$

We will now use a sub-lemma (the proof of which we will omit) to conclude.

Lemma 3′ : let $\phi(X), \psi(X) \in \mathbb{Z}[X]$ with no common complex roots. Let $d = \max\{\deg(\phi), \deg(\psi)\}$, then
a) there is an integer $R \geq 1$ depending on ϕ and ψ s.t. for all rational numbers $\frac{m}{n}$, we have

$$\gcd\left(n^d\phi\left(\frac{m}{n}\right), n^d\psi(\left(\frac{m}{n}\right)\right) \text{ divides } R$$

b) there are constant numbers κ_1 and κ_2 depending on ϕ and ψ s.t. for all rational numbers $\frac{m}{n}$ that are not roots of ψ

$$dh\left(\frac{m}{n}\right) - \kappa_1 \leq h\left(\frac{\phi(\frac{m}{n})}{\psi(\frac{m}{n})}\right) \leq dh\left(\frac{m}{n}\right) + \kappa_2$$

We see that lemma 3 is just a special case of the sub-lemma if we let $\xi = \frac{\varphi(x)}{\psi(x)}, \quad \varphi(x), \psi(x) \in \mathbb{Z}[x]$. Then since the degree $d = 2$,

$$h(\xi) = h\left(\frac{\varphi(x)}{\psi(x)}\right) \geq 2h(x) - \kappa$$

But since $h(P) = h(x(P)) + c$ (up to a bounded constant c), we can write:

$$h(2P) \geq 4h(P) - \kappa'$$

for some constant κ', as claimed in Lemma 3.

Lemma 4 : $[C(\mathbb{Q}) : 2C(\mathbb{Q})]$ is finite.
proof: We will only give a sketch of this proof. This is actually the most complicated of the lemmas so we will restrict our sketch to outlining a homomorphism between curves and another sub lemma.

Homomorphism : Let

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

where $\overline{a} = -2a$ and $\overline{b} = a^2 - 4b$. Also, let $T = (0, 0) \in C$.
a) There exists a homomorphism $\phi : C \to \overline{C}$

$$\phi(P) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right), & P = (x, y) \neq \mathcal{O}, T \\ \overline{\mathcal{O}}, \quad P = \mathcal{O}, \ P = T \end{cases} \qquad \text{With } \ker(\phi) = \{\mathcal{O}, T\}$$

b) We can also get a map $\overline{\phi} : \overline{C} \to \overline{\overline{C}}$ We see that

$$\overline{\overline{C}} \simeq C \quad \text{via map} \quad (x, y) \mapsto \left(\frac{1}{4}x, \frac{1}{8}y\right)$$

Then there exists a homomorphism $\psi : \overline{C} \to C$

$$\psi(\overline{P}) : \begin{cases} \left(\frac{\overline{y}^2}{\overline{x}^2}, \frac{\overline{y}(\overline{x}^2 - \overline{b})}{\overline{x}^2}\right), & \overline{P} = (\overline{x}, \overline{y}) \neq \overline{\mathcal{O}}, \quad \overline{T} \\ \overline{\mathcal{O}}, \overline{P} = \mathcal{O},\ \overline{P} = \overline{T} \end{cases}$$

c) The composition $\psi \circ \phi : C \to C$ is the multiplication by 2 map

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

Lemma 4′ : Let A and B be arbitrary abelian groups, and suppose $\phi : A \to B$ and $\psi : B \to A$ are homomorphisms satisfying

$$\phi \circ \psi(a) = 2a,\ \forall a \in A \qquad \psi \circ \phi(b) = 2b,\ \forall b \in B$$

Also, if we have that $\phi(A)$ has a finite index in B and $\psi(B)$ has finite index in A, then $2A$ has finite index in A i.e.

$$[A : 2A] \leq [A : \psi(B)][B : \phi(A)]$$

Since our homomorphisms satisfy the necessary property, we can conclude that $[C(\mathbb{Q}) : 2C(\mathbb{Q})]$ is finite. Note, the proof would require verification of the claim: $\phi(A)$ has a finite index in B and $\psi(B)$ has finite index in A. However, this was omitted for brevity.

8.4 Conclusion

We have now finished outlining the proof of Mordell's Theorem! This is a beautiful and elegant theorem from number theory which has broad implications for our study of elliptic curves. It allows us to examine rational points and torsion points in a brand new way. It even gives us methods to determining the generators of $C(\mathbb{Q})$, but these techniques don't necessarily work for all curves. In fact, it is still an open question if there is a procedure that will work for all elliptic curves.

9 Curves over Finite Fields

9.1 Analogue for Rational Points

We can now extend our study of elliptic curves to the field $\mathbb{F}_p$. So let

$$C : f(x) = y^2 = x^3 + ax^2 + bx + c, \quad a, b, c \in \mathbb{F}_p$$

We will refer to the **rational points** of C as

$$C(\mathbb{F}_p) = \{(x, y) : x, y \in \mathbb{F}_p,\ f(x, y) = 0\}$$

We refer to points that are not rational as those (x, y) where $x, y \in \mathbb{F}_q$ where $\mathbb{F}_q = \mathbb{F}_{p^e}$, i.e. some field extension of $\mathbb{F}_p$.

Non – Singular Curves : we will be looking exclusively at non-singular curves over finite fields. In this case, a curve is non-singular if $p \neq 2$ and the discriminant $D \not\equiv 0 \mod p$, where $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$.

How many points in $\mathbb{F}_\mathbf{p}$? Since we have spent so much time discussing $C(\mathbb{Q})$, we can ask how big is $C(\mathbb{F}_p)$. It turns out that it's computable. We can first think about it conceptually. Consider $y^2 = f(x) = x^3 + ax^2 + bx + c, \quad a, b, c \in \mathbb{F}_p$ with $p \neq 2$. In the group $\mathbb{F}_p^\times$, exactly half of the elements are **Quadratic Residues** while the other half are not. Recall that quadratic residues are the set

$$\{a \in \mathbb{F}_p : a \equiv n^2 \mod p, \quad \text{for some} \;\; 0 < n < p\}$$

Now substitute each of $0, 1, ...p - 1$ into $y^2 = f(x)$.
If $f(x) = 0$ then there is only one solution i.e. $y = 0$.
If $f(x) \neq 0$ then there are two possibilities. Either $f(x)$ is a quadratic residue, which means it would contribute two solutions for y. Or $f(x)$ is not a quadratic residue, which means it contributes 0 solutions.
So each x either corresponds to 1 solution or it has a 50 percent chance of either contributing 2 solutions or 0 i.e.

$$|C(\mathbb{F}_p)| = p + 1 + \text{error term}$$

9.2 Hasse-Weil

We can actually compute the error term from the previous section. Unfortunately, the proof of the theorem is far too complicated, but it is worth stating.
Hasse – Weil Theorem : If C is a non singular curve of genus g over $\mathbb{F}_p$, then the number of points on C with coordinates in $\mathbb{F}_p$ is

$$p + 1 + \epsilon, \quad \text{where } |\epsilon| \leq 2g\sqrt{p}$$

Here, elliptic curves have genus 1, so we see that

$$-2\sqrt{p} \leq |C(\mathbb{F}_p)| - p - 1 \leq 2\sqrt{p}$$

9.3 Points of Finite Order

We will now extend our study of torsion points to finite fields i.e. we want to know more about the subgroup

$$\Phi = \{P = (x, y) \in C(\mathbb{Q}) : P \;\; \text{has finite order}\}$$

Consider first the map

$$\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}, \qquad z \mapsto \tilde{z} \quad \text{via} \quad \tilde{z} \equiv z \mod p$$

So from $C : y^2 = x^3 + ax^2 + bx + c$ we get $\tilde{C} : y^2 = x^3 + \tilde{a}x^2 + \tilde{b}x + \tilde{c}$. We also see that as long as p does not divide the denominator, this map is well defined. Further, we see that as long as $P = (x, y)$ where $x, y \in \mathbb{Z}$, we can reduce the coordinates for all primes. Which means that $\tilde{P} = (\tilde{x}, \tilde{y})$ is a point in $\tilde{C}(\mathbb{F}_p)$. So, we get the following theorem.

Theorem : let $C = y^2 = x^3 + ax^2 + bx + c$ be a non-singular cubic with $a, b, c \in \mathbb{Z}$ and discriminant $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$. Take $\Phi \subset C(\mathbb{Q})$ be a subgroup of points of finite order. Then, for any prime p, let $P \to \tilde{P}$ be the reduction $\mod p$ map

$$\Phi \to \tilde{C}(\mathbb{F}_p), \quad P \mapsto \tilde{P} = \begin{cases} (\tilde{x}, \tilde{y}), & P = (x, y) \\ \tilde{\mathcal{O}}, & P = \mathcal{O} \end{cases}$$

If $p \nmid 2D$, then it is an isomorphism of Φ into a subgroup of $\tilde{C}(\mathbb{F}_p)$.

10 ECC Protocol

10.1 History

This cipher was initially proposed in 1985 by Neal Koblitz and Victor S. Miller. The idea was to extend the existing DLP (discrete log problem) to elliptic curves. In 1999, the government organization NIST gave guidelines for how to potentially implement this system. Specifically, it gave a list of elliptic curves corresponding to finite field for primes p of sizes 192, 224, 256, 384, and 521 bits. Then, in 2005 the NSA introduced Suite B which used ECC for DSG and key exchanges. Currently, ECC is widely used in digital signatures, especially in cryptocurrencies like Bitcoin and Ethereum. Its also being adopted in general web encryption standards due to its performance and efficiency advantages.

Pros : Its considered an alternative to RSA and is preferred for its smaller key size and efficiency, especially on mobile devices
Cons : It's still vulnerable to quantum attacks, so various organizations are working on new elliptic curve based protocols that will hopefully be quantum resistant in the future.

10.2 Encryption and Decryption Process

We will now describe the procedure for *ECC* as an analogue of Elgamal.

Both parties, Alice and Bob, agree on an elliptic curve in the form $y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_p$ and some point $P \in C$ with a large order.

Alice: picks some integer a and computes

$$aP = A$$

Bob: writes message $M \in C$ and some ephemeral key $k \in \mathbb{Z}$. He computes

$$c_1 = kP \qquad c_2 = m + kA$$

He then sends out (c_1, c_2)

Alice: decrypts using

$$M = -ac_1 + c_2$$

10.3 ECDLP Collision Algorithm

ECDLP: asks, given $P, Q \in C(\mathbb{F}_p)$, can you find an integer n s.t. $nP = Q$.

Collision Algorithm : let $n \approx \sqrt{p}$. Then make two lists:

$$kP \quad \text{and} \quad Q - nkP, \qquad \text{for } k = 1, 2, 3, ...$$

We will see a collision at some $k < n$. In general, for any group G, the DLP can be solved in approximately $2\sqrt{o(G)}$ steps. Currently, there is no better algorithm for trying to break the elliptic curve DLP.

10.4 Exercises

Exercise 1 : Let the elliptic curve be defined over $\mathbb{F}_{17}$ by the equation:

$$y^2 = x^3 + 2x + 2 \mod 17$$

Let the base point be $P = (5, 1)$ on the curve.

- Alice chooses $a = 7$ and computes $A = 7P$.
- Bob wants to send the message $M = (6, 3)$ and chooses ephemeral key $k = 3$.
- Bob computes $c_1 = 3P$, and $c_2 = M + 3A$.

Questions:

(a) Compute $A = 7P$

(b) Compute $c_1 = 3P$

(c) Compute $c_2 = M + 3A$

(d) Show how Alice recovers M using $M = -7c_1 + c_2$

Exercise 2 : Consider the elliptic curve $y^2 = x^3 + x + 1 \mod 19$ and base point $P = (2, 2)$.

- Alice has private key $a = 4$, so $A = 4P$.
- Bob uses ephemeral key $k = 5$ and encodes message $M = (13, 7)$.
- Bob sends $c_1 = 5P$ and $c_2 = M + 5A$.

Questions:

(a) Compute Alices public key $A = 4P$

(b) Compute $c_1 = 5P$

(c) Compute $c_2 = M + 5A$

(d) Verify that decryption recovers $M = -4c_1 + c_2$

10.5 Answers

Solution 1:

(a) $A = 7P = (0, 6)$

(b) $c_1 = 3P = (10, 6)$

(c) $3A = 3(0, 6) = (6, 14)$ then $c_2 = M + 3A = (6, 3) + (6, 14) = \mathcal{O}$ (point at infinity)

(d) Decryption: $M = -7c_1 + c_2 = -7(10, 6) + \mathcal{O} = (6, 3)$

Solution 2:

(a) $c_1 = 5P = (7, 11)$

(b) $5A = (6, 9)$

(c) $c_2 = M + 5A = (13, 7) + (6, 9) = (3, 12)$

(d) Decryption: $M = -4c_1 + c_2 = -4(7, 11) + (3, 12) \Rightarrow M = (13, 7)$

11 Useful Sage Code

Graphing Curves

```
E = EllipticCurve(RR, [0, 0, 1, -1, 0])  # y^2 + y = x^3 - x
E.plot()
```

Adding and Duplicating Points

```
E = EllipticCurve(RR, [0, 0, 1, -1, 0])
P = E(0, 0)
Q = E(1, 0)
R = P + Q
S=2*P
print(R)
print(S)
```

Listing points and Group Structure over $\mathbb{F}_p$

```
F = FiniteField(7)
E = EllipticCurve(F, [2, 3])  # y^2 = x^3 + 2x + 3 over F_7
E.points()
E.abelian_group()
```

Torsion Subgroup in $C(\mathbb{Q})$

```
E = EllipticCurve([0, 0, 1, -1, 0])
E.torsion_subgroup()
```

ECC Implementation

```
F = FiniteField(17)
E = EllipticCurve(F, [2, 2])  # y^2 = x^3 + 2x + 2 over F_17

# Choose a base point P on the curve
P = E.random_point()
print("Base point P:", P)

# Alice chooses her private key
a = 7
A = a * P
print("Alice's public key A = aP:", A)

# Bob wants to send a message M     E
M = E.random_point()
print("Original message point M:", M)

# Bob picks ephemeral key k and encrypts
k = 3
c1 = k * P
c2 = M + k * A
print("Ciphertext c1:", c1)
print("Ciphertext c2:", c2)

# Alice decrypts the message
decrypted_M = -a * c1 + c2
print("Decrypted message M:", decrypted_M)

# Confirm it matches original
print("Message recovered correctly:", decrypted_M == M)
```

References

[1] Diophantine equations. Encyclopedia of Mathematics. URL: http://encyclopediaofmath.org/index.php?title=Diophantineequationsoldid=52515

[2] Brown, Ezra, and Bruce T. Myers. ”Elliptic Curves from Mordell to Diophantus and Back.” The American Mathematical Monthly, vol. 109, no. 7, Aug.Sept. 2002, pp. 639649. JSTOR, https://www.jstor.org/stable/3072428.

[3] ”What is Elliptic Curve Cryptography? Definition FAQs.” VMware, https://www.vmware.com/topics/elliptic-curve-cryptography. Accessed 18 Apr. 2025.

Special Acknowledgment to:

[4] Silverman, Joseph H., and John T. Tate. Rational Points on Elliptic Curves. 2nd ed., Springer, 2015.