The Mathematics Behind Blockchain

Ilinca Radulescu

Supervised by Tim Dokchitser
Level 7
20 Credit Points

This project complies with the guidelines stated in the Project Handbook.

April 28, 2024

Acknowledgement of Sources

For all ideas taken from other sources (books, articles, internet), the source of the ideas is mentioned in the main text and fully referenced at the end of the report.

All material which is quoted essentially word-for-word from other sources is given in quotation marks and referenced.

Pictures and diagrams copied from the internet or other sources are labelled with a reference to the web page or book, article etc.

Signed

Date 18/03/2024

Contents

1 Introduction **4**

2 Preliminaries **5**
2.1 Finite Fields 5
2.2 Algebraic Closure 7
2.3 Projective Varieties 7

3 Elliptic Curves **8**
3.1 Weierstrass Equations 8
3.2 Point Addition 9
3.3 The j-invariant 15
3.4 Legendre Form 19
3.5 Endomorphisms 21
3.6 Isogenies 27

4 Elliptic Curves Over Finite Fields **33**
4.1 Hasse's Theorem 33
4.2 The Weil Conjectures 36
4.3 Supersingular Curves 40

5 Applications to Cryptography **51**
5.1 Elliptic Curve Discrete Logarithm Problem 52
5.2 Elliptic Curve Diffie-Hellman Key Exchange 57

6 Appendix A **61**

Bibliography **63**

1 Introduction

Probably most well known for being the crux in Andrew Wiles' proof of Fermat's Last Theorem, elliptic curves are fascinating mathematical objects. They have intrigued mathematicians since the third century, and continue to do so today. While their uses in cryptography are much more recent, being first introduced in 1985 by Victor Miller and Neal Koblitz, they have been rapidly progressing. Today, they are widely used by several companies, including very large corporations, such as Meta. Not only do elliptic curve cryptosystems provide enhanced security, being able to withstand most attacks against their classical counterparts, but they also require a much smaller encryption key size, and facilitate more time efficient computations.

The aim of this project is not to answer any specific questions, but rather to showcase the connection between these abstract mathematical objects and cryptography, a very applied domain of mathematics. Moreover, with cryptography being a fundamental part of contemporary society, the link between these two mathematical areas becomes even more intriguing. Since we are specifically interested in understanding and showcasing the applications of elliptic curves to cryptography, we study elliptic curves over finite fields, which are introduced in Section 2. In the same section, we also introduce projective and affine varieties, as well as various concepts from number theory, which will be key in proving results later on in the project. In Section 3, we define what an elliptic curve is, and introduce some fundamental results about the properties of elliptic curves. We show that the points on an elliptic curve form an abelian group under addition. We also discuss how to detect isomorphic elliptic curves using the j-invariant, as well as looking at particular maps between elliptic curves, namely endomorphisms and isogenies. In Section 4, we focus on elliptic curves over finite fields. We prove Hasse's Theorem, relating to the the number of points on an elliptic curve over a finite field, and discuss the Weil Conjectures. To end this section, we introduce a special category of elliptic curves, known as supersingular elliptic curves. In Section 5, a short introduction to cryptography is provided to emphasise the advantages of elliptic curve cryptography over its classical counterparts. We conclude the project by showcasing how the Elliptic Curve Diffie-Hellman Key Exchange works, and subsequently explore one of its particular applications to WhatsApp.

2 Preliminaries

We begin by defining what a finite field is, [1]. We then look at some of the properties of finite fields which are involved in the study of elliptic curves in Section 4.

2.1 Finite Fields

Definition 2.1.1: Let p be a prime, such that $p \in \mathbb{Z}$. We define the finite field with p elements as

$$\mathbb{Z}/p\mathbb{Z} = \{0, 1, ..., p-1\}.$$

In general, this finite field is denoted by $\mathbb{F}_p$.

Remark: The operations in $\mathbb{F}_p$ are addition and multiplication mod p.

Definition 2.1.2: We can extend this to define

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, ..., n-1\},$$

for n a composite integer. Similarly, addition and multiplication are also defined mod n.

Example 1: We consider some examples to illustrate how to work in $\mathbb{F}_p$:

- $\mathbb{F}_7 = \{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6\}$, and we obtain $4 \times 5 = 20 \equiv 6 \pmod 7$ and $4 + 5 = 9 \equiv 2 \pmod 7$.
- Say we are interested in finding the roots of $f(x) = x^3 - x + 3$ in $\mathbb{F}_{13}$. We obtain a unique solution for $x = 8$ because $8^3 - 8 + 3 = 512 - 8 + 3 = 507 = 39 \times 13 \equiv 0 \pmod{13}$, and there is no other $x \in \{0, 1, \cdots, 12\}$ for which this holds.

Definition 2.1.3: The characteristic of a field K, $\text{char}(K)$ is the smallest $n \in \mathbb{N}$ such that $\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$. If no such n exists, we say that K is a field of characteristic 0.

Example 2: Appealing to one of the previous examples, we see that $\mathbb{F}_7$ has characteristic 7 because $\underbrace{1 + 1 + \cdots + 1}_{7 \text{ times}} = 7 \equiv 0 \pmod 7$, and there is no smaller $n \in \mathbb{N}$, such that this holds. On the other hand, $\mathbb{Q}$ has characteristic 0, because no matter how many times we add 1 to itself we never obtain 0.

Theorem 2.1.4 (Fermat's Little Theorem): Let p be a prime, and a an integer not divisible by p. Then

$$a^{p-1} \equiv 1 \pmod p.$$

Proof: As the proof is not essential to our project, the interested reader is directed to [2, Chapter 28].

Theorem 2.1.5 (Lagrange's Theorem): Let G be a finite group and H a subgroup of G. Then, the order of H, $|H|$ divides the order of G, $|G|$.

Proof: While the result is fascinating in itself, we direct the curious reader to [3, Section 1.9], as we are interested in the following corollary:

Corollary 2.1.6 : Let G be a finite group and take $x \in G$. Then, the order of x, $|x|$ divides the order of G, $|G|$. In particular, $x^{|G|} = e$, the identity element.

A second key result is Theorem 8.1(ii) of [4]:

Theorem 2.1.7: Let $K = \mathbb{F}_q$ be a finite field, where q is a prime power, or in other words, $q = p^n$ for p prime and $n \in \mathbb{Z}$. Then, $K^* = \mathbb{F}_q^*$ is a cyclic group of order $q - 1 = p^n - 1$.

Proof: We begin by showing that if $f \in K[X]$ is a polynomial of degree $n \geq 1$, then f has at most n distinct roots in K. Let $\{\alpha_1, \cdots, \alpha_m\}$ be the set of distinct roots of f in K. Then, $x - \alpha_i$ is a factor of f for all i's. But $K[X]$ is a unique factorisation domain, and $\alpha_1, \cdots, \alpha_m$ are non-associate irreducible elements in $K[X]$, so their product also divides f. In other words, for some $g \in K[X]$,

$$f = (x - \alpha_1) \cdots (x - \alpha_m)g.$$

By comparing degrees, we note that $m \leq n$, and we are done.

We now appeal to the following result from Group Theory: "Let A be a finite abelian group. Then A is isomorphic to a direct product of cyclic groups of the form: $C_{m_1} \times C_{m_2} \times \cdots \times C_{m_t}$, where $m_t | m_{t-1} | \cdots | m_2 | m_1$". Since it's not relevant to the project we omit the proof, but direct the reader to [3]. We show that every finite subgroup of K^* is cyclic. Suppose that H is a subgroup of K^*, and hence finite, since K^* is also finite. As K^* is abelian, then H is also abelian. Therefore, by the fact above, $H \cong C_{m_1} \times C_{m_2} \times \cdots \times C_{m_t}$ such that $m_t | m_{t-1} | \cdots | m_2 | m_1$.

For the sake of contradiction, suppose H is not cyclic, and hence $t \geq 2$. Then, for all $a \in H$, $a^{m_1} = 1$ and observe that $|H| = m_1 m_2 \cdots m_t > m_1$. This implies that $x^{m_1} - 1 \in K^*$ has more than m_1 distinct roots in K, contradicting the first half of our proof. Therefore, H is cyclic. Putting everything together, we obtain the desired result.

Combining Corollary 2.1.6 and Theorem 2.1.7 we obtain the following theorem, which will be fundamental for proving results in Sections 3 and 4:

Theorem 2.1.8: Let $\mathbb{F}_q$ be a finite field such that q is a prime power, that is

$q = p^n$ for p prime and $n \in \mathbb{Z}$. Take $x \in \mathbb{F}_q^*$. Then,

$$x^{p^n-1} = x^{q-1} = 1 \quad \text{in} \quad \mathbb{F}_q^*.$$

Definition 2.1.9 (Legendre Symbol): Let p be an odd prime, and x an integer. Then, $\left(\frac{x}{p}\right) \in \{-1, 0, 1\}$, where $\left(\frac{x}{p}\right) \equiv x^{(p-1)/2} \pmod{p}$.

2.2 Algebraic Closure

We introduce the concept of an *algebraic closure* of a field K, which is key in understanding results in the later sections. The interested reader is directed to [5, Chapter 10] for an in depth discussion of this topic.

Definition 2.2.1: If L and K are fields we say that L is a *field extension* of K, denoted L/K, if $K \subseteq L$.

Example 1: Take $\mathbb{Q}(\sqrt{7}) = \{a + b\sqrt{7} : a, b \in \mathbb{Q}\}$. One can see that for $b = 0$ we obtain $\{a + 0(\sqrt{7}) : a \in \mathbb{Q}\} = \{a : a \in \mathbb{Q}\} = \mathbb{Q}$. Therefore, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{7})$, and we conclude that $\mathbb{Q}(\sqrt{7})$ is a field extension of $\mathbb{Q}$.

Definition 2.2.2: Let K be a field. The *algebraic closure* of K, denoted $\overline{K}$, is an algebraic field extension $\overline{K}/K$ such that every polynomial in $K[X]$ splits in $\overline{K}$, or, in other words, every polynomial in $K[X]$ has roots in $\overline{K}$.

Definition 2.2.3 : The algebraic closure of a finite field $\mathbb{F}_q$ is defined as

$$\overline{\mathbb{F}}_q = \bigcup_{n \geq 1} \mathbb{F}_{q^n}.$$

Example 2: The field $\mathbb{C}$ of complex numbers is algebraically closed. By the fundamental theorem of algebra, we can see that every polynomial in $\mathbb{C}[X]$ has a root in $\mathbb{C}$. For a detailed proof of this result see [6, Section 1.4].

2.3 Projective Varieties

The concept of a *projective variety* will be key when looking at Section 4.2, The Weil Conjectures. We begin by defining an *affine n-space*. The interested reader is directed to [7, Sections 1.1 and 1.2] for an in depth discussion of the following results.

Definition 2.3.1: *Affine n-space* over K, is the set of n-tuples

$$\mathbb{A}^n = \mathbb{A}^n(\overline{K}) = \{P = (x_1, \cdots, x_n) : x_i \in \overline{K}\}.$$

Definition 2.3.2: *Projective n-space* over K, denoted by $\mathbb{P}^n$ or $\mathbb{P}^n(\overline{K})$, is the set of all $(n+1)$-tuples $(x_0, \cdots, x_n) \in \mathbb{A}^{n+1}$, such that at least one x_i is non-zero, modulo the equivalence relation

$$(x_0, \cdots, x_n) \sim (y_0, \cdots, y_n)$$

if there exists a $\lambda \in \overline{K}^*$ such that $x_i = \lambda y_i$ for all i. An equivalence class $\{(\lambda x_0, \cdots, \lambda x_n) : \lambda \in \overline{K}^*\}$ is denoted by $[x_0, \cdots, x_n]$, and the individual $x_0, \cdots, x_n$ are called *homogeneous coordinates* for the corresponding point in $\mathbb{P}^n$.

The following result, Definition 2.4 of [8, Section 2.4], is fundamental to defining elliptic curves:

Definition 2.3.3: A curve C in $\mathbb{P}^2(\overline{K})$ defined by $F(x, y, z) = 0$ is said to be *nonsingular* at a point P if at least one of the partial derivatives F_x, F_y, F_z is nonzero at P.

3 Elliptic Curves

We now introduce the concept of an elliptic curve and assume that, by definition, all elliptic curves are nonsingular. This is equivalent to assuming that all points on an elliptic curve are nonsingular in $\overline{K}$.

3.1 Weierstrass Equations

The following results were taken from [8, Section 2.1]:

Definition 3.1.1: Let K be a field, not necessarily finite. We define an *elliptic curve*, E over K, as the set of points $(x, y) \in K^2$, such that x and y satisfy the following *generalised Weierstrass* equation:

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

where $a_i \in K$, together with the point at infinity, O.

Remark 1: This generalised form is used when working with fields of characteristic 2 or 3.

If $\text{char}(K) \neq 2$, we can divide by 2 and complete the square:

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

which can further be simplified as

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6',$$

where $y_1 = y + \frac{a_1 x}{2} + \frac{a_3}{2}$ and $a_2' = a_2 + \frac{a_1^2}{4}$, $a_4' = a_4 + \frac{a_1 a_3}{2}$, $a_6' = \frac{a_3^2}{4} + a_6$ are constants. Moreover, if $\text{char}(K) \neq 3$ also, then let $x_1 = x + \frac{a_2'}{3}$ and substitute $x_1 - \frac{a_2'}{3}$ for x in the above equation. We obtain:

$$y_1^2 = \left(x_1 - \frac{a_2'}{3}\right)^3 + a_2'\left(x_1 - \frac{a_2'}{3}\right)^2 + a_4'\left(x_1 - \frac{a_2'}{3}\right) + a_6'.$$

Opening up the brackets and rearranging the terms, we obtain the following result:

$$y_1^2 = x_1^3 + \left(a_4' - \frac{a_2'^2}{3}\right)x_1 + \left(a_6' - \frac{2a_2'^3}{27} - \frac{a_2'a_4'}{3}\right).$$

Note that by doing this substitution we have eliminated the x^2 term from our equation, and obtain the following simplified version:

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

where $A = a_4' - \frac{a_2'^2}{3}$ and $B = a_6' - \frac{2a_2'^3}{27} - \frac{a_2'a_4'}{3}$ are some constants. Hence, putting everything together, we obtain:

Definition 3.1.2: Let K be a field such that $\text{char}(K) \neq 2, 3$. Then, the *simplified Weierstrass equation* of an elliptic curve E over K is:

$$y^2 = x^3 + Ax + B,$$

where $A, B \in K$.

Remark 2: In most cryptographic applications, elliptic curves are defined over finite fields of the form $\mathbb{F}_q$, where q is a very large prime, or a power of a large prime. Therefore, we will use the simplified Weierstrass equation when proving most of our results, as the finite fields which interest us will have characteristic greater than 3.

3.2 Point Addition

Although we will be mainly working with elliptic curves over a finite field $\mathbb{F}_q$, we will appeal to graphs in $\mathbb{R}^2$ to illustrate point addition, as they are easier to visualise. Moreover, as the procedures used to find numerical values are identical in both cases, we can directly apply the same method, remembering to always work $\mod p$.

Composition Law: Let $P_1, P_2 \in E$, let L be a line through P_1 and P_2 (if $P_1 = P_2$, let L be the tangent line to E at P_1), and let P_3' be the third point

of intersection of L with E. Let L' be the line through P_3' and O, the point at infinity. Then L' intersects E at P_3', O and a third point, denoted $P_1 + P_2$.

The nature of the *Composition Law* is highly geometric, and examples of how it's performed are illustrated in the following diagrams (generated using GeoGebra and the elliptic curve, $E : y^2 = x^3 - x + 5$):

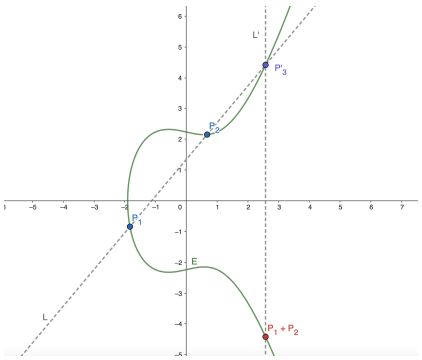

Figure 1: Case 1: $P_1 + P_2 = P_3$

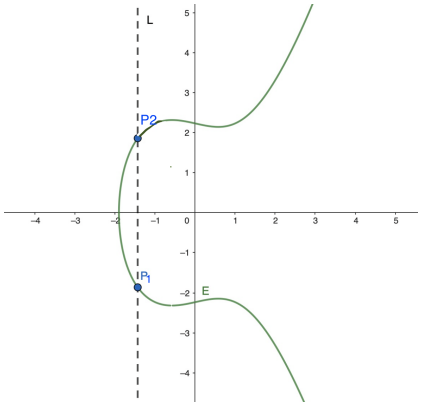

Figure 2: Case 2: $P_1 + P_2 = O$

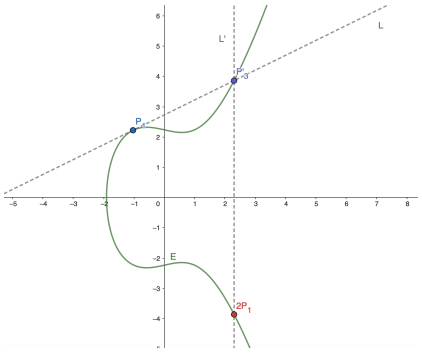

Figure 3: Case 3: $2P_1$

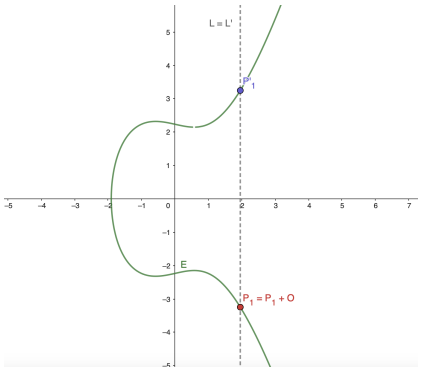

Figure 4: Case 4: $P_1 + O = P_1$

We now examine this process in more detail, as directed by [8, Section 2.2]. As previously discussed, we can assume that an elliptic curve, E, is given by the equation $y^2 = x^3 + Ax + B$.

Start with two points

$$P_1 = (x_1, y_1), \quad P_2 = (x_2, y_2),$$

such that $P_1, P_2 \in E$.

Case 1: Assume that $P_1 \neq P_2$, and also that neither is the point at infinity, O. Draw the line L through P_1 and P_2. Its gradient is

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

If $x_1 = x_2$, then L is vertical, as we are diving by 0. As we look at this particular case later, Case 2, we can assume that $x_1 \neq x_2$. Then, the equation of L as it passes through P_1 is

$$y = m(x - x_1) + y_1.$$

To find where L intersects E, we substitute $m(x-x_1)+y_1$ for y, in the simplified Weierstrass equation of E, $y^2 = x^3 + Ax + B$. We obtain:

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

Open up the brackets and rearrange to arrive at the following:

$$0 = x^3 - m^2x^2 + x(A + 2x_1m^2 - 2my_1) + (B - y_1^2 - m^2x_1^2 + 2mx_1y_1) \quad (1)$$

The three roots of this cubic polynomial correspond to the three points of intersection of L with E. Furthermore, we can specify each cubic polynomial in terms of its roots, say r, s, t , as follows:

$$x^3 + ax^2 + bx + c = (x - r)(x - s)(x - t).$$

By expanding the right hand side, we obtain:

$$x^3 + ax^2 + bx + c = x^3 - x^2(r + s + t) + x(rs + rt + st) - rst. \quad (2)$$

In our case, we already know two of the roots, x_1, x_2, as they follow directly from the intersection of L with E at P_1 and P_2 respectively. From (1), we deduce that x is a third root of the cubic polynomial. By comparing the coefficients of (1) and (2), we obtain:

$$m^2 = x + x_1 + x_2 \quad \text{and hence,} \quad x = m^2 - x_1 - x_2$$

and

$$y = m(x - x_1) + y_1,$$

which we already know from the equation of L. Lastly, to obtain $P_1 + P_2 = P_3$, with $P_3 = (x_3, y_3)$, we reflect in the x- axis:

$$x_3 = m^2 - x_1 - x_2 \quad \text{and} \quad y_3 = m(x_1 - x_3) - y_1.$$

Case 2: Following from the above case, we look at what happens when $x_1 = x_2$ and $y_1 \neq y_2$. We have already noted that the line passing through P_1 and P_2 is a vertical line, and hence intersects E at O, the point at infinity, as illustrated in Figure 2. Reflecting the point at infinity across the x-axis yields the same point O (by convention, the point at infinity is both at the top and at the bottom of the y-axis). Hence, we obtain $P_1 + P_2 = O$.

Case 3: We consider the case when $P_1 = P_2 = (x_1, y_1)$. We have previously discussed that when this happens, and the two points coincide, we take L to be the tangent line at the point (x_1, y_1). By using implicit differentiation on the equation of E, $y^2 = x^3 + Ax + B$, and then substituting in the point (x_1, y_1), we find the gradient of L:

$$2y\frac{dy}{dx} = 3x^2 + A \quad \text{and hence,} \quad m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}.$$

Note that if $y_1 = 0$, then we are dividing by $2y_1 = 2 \times 0 = 0$, and hence, as in Case 2, L is vertical. As before, we obtain $P_1 + P_2 = O$, the point at infinity. Therefore, we can assume that $y_1 \neq 0$. As before, the equation of L is

$$y = m(x - x_1) + y_1,$$

where m is as above. Applying the same reasoning and method as in Case 1, we obtain the same cubic equation:

$$0 = x^3 - m^2x^2 + x(A + 2x_1m^2 - 2my_1) + (B - y_1^2 - m^2x_1^2 + 2mx_1y_1).$$

This time however, we know that x_1 is a double root, because L is a tangent to E at P_1. Then, using the same method as before, we obtain:

$$x_3 = m^2 - x_1 - x_1 = m^2 - 2x_1 \quad \text{and} \quad y_3 = m(x_1 - x_3) - y_1.$$

Case 4: Suppose that $P_2 = O$, the point at infinity, and let P_1 be any point on the curve E. The line passing through P_1 and P_2 is a vertical line that intersects E at the point P_1', which is just the reflection of P_1 in the x-axis as illustrated in Figure 4. However, when we reflect P_1' across the x-axis to obtain $P_1 + P_2$, we end up back at P_1. Hence,

$$P_1 + O = P_1,$$

for all points on the elliptic curve E. We extend this to include $O + O = O$.

Remark 1: Following Case 4, we define $P + O = P$ for all points P on the elliptic curve E.

The reader interested in a proof of these results for the generalised Weierstrass equation is directed to [7, Section 3.2].

Example 1: Define $E(\mathbb{F}_{17}) = \{(x, y) \in \mathbb{F}_{17} \times \mathbb{F}_{17} : y^2 = x^3 + 11x + 3\} \cup \{O\}$. We want to compute $(2, 13) + (5, 8)$ on $E(\mathbb{F}_{17})$.

Firstly, we check that $(2, 13), (5, 8) \in E(\mathbb{F}_{17})$: $2^3 + 11(2) + 3 = 33 = 17 \times 2 - 1 \equiv -1 \pmod{17} \equiv 16 \pmod{17}$ and $13^2 = 169 = 17 \times 10 - 1 \equiv -1 \pmod{17} \equiv 16 \pmod{17}$, also. Secondly, $5^3 + 11(5) + 3 = 183 = 17 \times 10 + 13 \equiv 13 \pmod{17}$ and $8^2 = 64 = 17 \times 4 - 4 \equiv -4 \pmod{17} \equiv 13 \pmod{17}$ also, and we are done.

Therefore, points $P_1 = (2, 13), P_2 = (5, 8) \in E(\mathbb{F}_{17})$. Since $P_1 \neq P_2$ and the two points have distinct x-coordinates (since $2 \neq 5$ in $\mathbb{F}_{17}$), we use Case 1, remembering to work mod 17. Start by calculating $m = \frac{8-13}{5-2} = \frac{-5}{3} \equiv -5 \times 3^{-1} \pmod{17}$, where 3^{-1} is the inverse of 3 in $\mathbb{F}_{17}$. We find that $3 \times 6 = 18 \equiv 1 \pmod{17}$. Hence, $3^{-1} \equiv 6 \pmod{17}$. Putting everything together, we obtain $m = -5 \times 6 = -30 = 4$ in $\mathbb{F}_{17}$, yielding the following coordinates:

$$\begin{aligned} x_3 &= 4^2 - 2 - 5 = 9 \equiv 9 \pmod{17} \\ y_3 &= 4(2 - 9) - 13 = -41 \equiv 10 \pmod{17}. \end{aligned}$$

Therefore, $(2, 13) + (5, 8) = (9, 10)$ on $E(\mathbb{F}_{17})$.

In the following example, we look at how to approach larger computations. We use the method of *consecutive doubling* as a tool, since it's efficient in finding large multiples of a point on $E(K)$.

Example 2: Define $E(\mathbb{F}_{23}) = \{(x, y) \in \mathbb{F}_{23} \times \mathbb{F}_{23} : y^2 = x^3 + 7x + 9\} \cup \{O\}$. We want to compute $17(4, 3)$ on $E(\mathbb{F}_{23})$, where $17(4, 3)$ is just $\underbrace{(4, 3) + \cdots + (4, 3)}_{17 \text{ times}}$. Again, we check that $(4, 3) \in E(\mathbb{F}_{23})$: $4^3 + 7(4) + 9 = 101 = 4 \times 23 + 9 \equiv 9 \pmod{23}$ and $3^2 = 9 \equiv 9 \pmod{23}$ also, and we are done.

Note that since $17 = 2^4 + 1$, we can double $(4, 3)$ four times, and then add $(4, 3)$ once. Hence, we use Case 3 four times, followed by Case 1. We start by calculating the gradient, $m = \frac{3(4)^2+7}{2(3)} = \frac{55}{6} \equiv \frac{9}{6} \equiv \frac{3}{2} \pmod{23}$. Since 2^{-1} is the inverse of 2 in $\mathbb{F}_{23}$, and $2 \times 12 = 24 \equiv 1 \pmod{23}$, then $2^{-1} = 12$ in $\mathbb{F}_{23}$. Hence, $m = 3 \times 12 = 36 = 23 + 13 \equiv 13 \pmod{23}$. Therefore, we obtain the following coordinates:

$$\begin{aligned} x_3 &= 13^2 - 2(4) = 161 = 7 \times 23 \equiv 0 \pmod{23} \\ y_3 &= 13(4 - 0) - 3 = 49 = 2 \times 23 + 3 \equiv 3 \pmod{23}. \end{aligned}$$

Hence, $2(4, 3) = (0, 3)$ on $E(\mathbb{F}_{23})$. Using similar computations, we can show that:

$$\begin{aligned} 4(4, 3) &= 2(0, 3) = (2, 10) \\ 8(4, 3) &= 4(0, 3) = 2(2, 10) = (8, 5) \\ 16(4, 3) &= 8(0, 3) = 4(2, 10) = 2(8, 5) = (15, 19) \\ 17(4, 3) &= 16(4, 3) + (4, 3) = (15, 19) + (4, 3) = (16, 13), \end{aligned}$$

on $E(\mathbb{F}_{23})$. The interested reader can refer to [9], which is useful in computing these point multiplications and additions.

This method allows us to compute kP for very large k, say several hundreds of digits in a very short time. For a more in depth discussion of this approach and its applications, see [8, end of Section 2.2]. Moreover, the associative law,

stated below in Theorem 3.2.1, allows us to make these computations without worrying about the order the points are added in.

Remark 2: Note that when P_1 and P_2 have coordinates in a field K which also contains A and B, then $P_1 + P_2$ also has coordinates in K. Therefore, $E(K)$ is closed under the composition law, yielding the following result:

Theorem 3.2.1: The composition law makes E into an abelian group with O as the identity element. In other words, the addition of points on E satisfies the following properties:

1. (commutativity) $P_1 + P_2 = P_2 + P_1$ for all $P_1, P_2 \in E$.
2. (existence of identity) $P + O = P$ for all points $P \in E$.
3. (existence of inverses) Given P on E, there exists P' on E with $P + P' = O$. This point P' will be generally be denoted as $-P$.
4. (associativity) $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ for all $P_1, P_2, P_3 \in E$.

Proof:

1. (commutativity) Trivial, since the line through P_1 and P_2 is the same as the line through P_2 and P_1.
2. (existence of identity) The identity property of O holds by definition and from Remark 1.
3. (existence of inverses) Let P' be the reflection of P across the x-axis. Then $P + P' = O$. This is illustrated in Case 2.
4. (associativity) The proof is not central to the rest of the project, so we only give a brief overview. The interested reader can find a detailed account in [8, Section 2.4]. Take an elliptic curve E, and points $P_1, P_2, P_3 \in E$. To compute $-((P_1 + P_2) + P_3)$ we need to take the lines $l_1 = \overline{P_1 P_2}, m_2 = \overline{O, P_1 + P_2}$ and $l_3 = \overline{P_3, P_1 + P_2}$, and look at where they intersect E. To compute $-(P_1 + (P_2 + P_3))$ we need to take the lines $m_1 = \overline{P_2 P_3}, l_2 = \overline{O, P_2 + P_3}$ and $m_3 = \overline{P_1, P_2 + P_3}$. We observe that the points $P_{1(ij)} = l_i \cap m_j$ lie on E, except possibly for $P_{1(33)}$. It can be shown that having the eight points $P_{1(ij)} \neq P_{1(33)}$ on E forces $P_{1(33)}$ to be on E. As l_3 intersects E at the points $P_3, P_1 + P_2$ and $-((P_1 + P_2) + P_3)$, we must have that $-((P_1 + P_2) + P_3) = P_{1(33)}$. Similar reasoning shows that $-(P_1 + (P_2 + P_3)) = P_{1(33)}$ also, so

$$-((P_1 + P_2) + P_3) = -(P_1 + (P_2 + P_3)),$$

obtaining the desired associativity.

Remark 3: For the simplified Weierstrass equation, if $P = (x, y)$, then $-P = (x, -y)$. However, for the generalised form presented in Definition 3.1.1, this is not the case. If we have a point $P = (x, y)$ on $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, it can shown that $-P = (x, -a_1x - a_3 - y)$. A detailed account is given in [8, pp.15].

We have established what an elliptic curve is and looked at one of its main structural features. We proceed by analysing further properties of elliptic curves, which will provide us with a deeper understanding of these mathematical objects, and in subsequent sections, their uses in cryptography.

3.3 The j-invariant

Let E be an elliptic curve given by $y^2 = x^3 + Ax + B$, where $A, B \in K$, such that K is a field and $\text{char}(K) \neq 2, 3$. Let

$$x_1 = \mu^2 x \quad \text{and} \quad y_1 = \mu^3 y,$$

where $\mu \in \overline{K}^{\times}$. Substituting, we obtain:

$$\frac{y_1^2}{\mu^6} = \frac{x_1^3}{\mu^6} + A\frac{x_1}{\mu^2} + B.$$

Multiplying by μ^6, we get:

$$y_1^2 = x_1^3 + A_1x_1 + B_1,$$

where $A_1 = A\mu^4$ and $B_1 = B\mu^6$.

Remark: This can be viewed as a transformation, taking an elliptic curve $E : y^2 = x^3 + Ax + B$, to a second elliptic curve $E' : y_1^2 = x_1^3 + A_1x_1 + B_1$. This result will be used in the proof of Theorem 3.3.2.

Definition 3.3.1 : Define the *j-invariant* to be:

$$j = j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}$$

Remark 1: The denominator is the negative of the discriminant of the cubic polynomial, $x^3 + Ax + B$, and hence, by assumption, is nonzero.

Example 1: Let $E : y^2 = x^3 + 5x + 2$. The j-invariant of E is

$$j(E) = 1728\frac{4 \times 5^3}{4 \times 5^3 + 27 \times 2^2} = \frac{27000}{19}.$$

Note that if we are considering the elliptic curve over a finite field $\mathbb{F}_p$, then we would compute the j-invariant $\mod p$. For example, if we take E over $\mathbb{F}_7$, since

$27000/19 \equiv 1/5 \pmod 7$, then $j(E) = \frac{1}{5} = 1 \times 5^{-1} = 3$ in $\mathbb{F}_7$ (as 3 is the inverse of 5 in $\mathbb{F}_7$, because $3 \times 5 = 15 = 14 + 1 \equiv 1 \pmod 7$).

We proceed by introducing the main result of this subsection, Proposition 1.4(b) of [7, Section 3.1]:

Theorem 3.3.2: Two elliptic curves are isomorphic over $\overline{K}$ if and only if they both have the same j-invariant.

Proof: Assume that there exist two elliptic curves, E_1, E_2 with equations $y_1^2 = x_1^3 + A_1x_1 + B_1$, and $y_2^2 = x_2^3 + A_2x_2 + B_2$, respectively. If they are isomorphic, then there exists a transformation $A_2 = A_1\mu^4, B_2 = B_1\mu^6$, taking E_1 to E_2, as previously shown. We now show these two curves have the same j-invariant:

$$\begin{aligned} j(E_2) &= 1728\frac{4A_2^3}{4A_2^3 + 27B_2^2} \\ &= 1728\frac{4(A_1\mu^4)^3}{4(A_1\mu^4)^3 + 27(B_1\mu^6)^2} \\ &= 1728\frac{4A_1^3\mu^{12}}{4A_1^3\mu^{12} + 27B_1^2\mu^{12}} \\ &= 1728\frac{4A_1^3}{4A_1^3 + 27B_1^2} \\ &= j(E_1), \end{aligned}$$

and we are done.

For the converse, let E_1, E_2 be two elliptic curves with the same j-invariant, and with the following Weierstrass equations:

$$E_1 : y_1^2 = x_1^3 + A_1x_1 + B_1$$

$$E_2 : y_2^2 = x_2^3 + A_2x_2 + B_2.$$

Assuming $j(E_1) = j(E_2)$, we obtain:

$$1728\frac{4A_1^3}{4A_1^3 + 27B_1^2} = 1728\frac{4A_2^3}{4A_2^3 + 27B_2^2}.$$

Cancelling 1728 on both sides (note that $1728 = 2^6 \times 3^3$, and since we have assumed that $\text{char}(K) \neq 2, 3$, we are not dividing by 0), and cross multiplying we obtain:

$$4A_1^3(4A_2^3 + 27B_2^2) = 4A_2^3(4A_1^3 + 27B_1^2).$$

Opening up the brackets, we have:

$$16A_1^3A_2^3 + 108A_1^3B_2^2 = 16A_1^3A_2^3 + 108A_2^3B_1^2.$$

Subtracting $16A_1^3A_2^3$, from both sides and dividing by 108 (again $108 = 2^2 \times 3^3$, so by our assumption, we are not dividing by 0), yields:

$$A_1^3B_2^2 = A_2^3B_1^2. \tag{3}$$

We now look for an isomorphism of the form $(x_1, y_1) = (\mu^2 x_2, \mu^3 y_2)$ and consider three cases:

Case 1: $A_1 = 0$, and hence $j = 0$. We have already seen that the denominator is the negative of the discriminant of a cubic, hence nonzero, and so $B_1 \neq 0$. This further implies that $A_2 = 0$ (for (3) to hold), and we obtain an isomorphism using $\mu = (\frac{B_1}{B_2})^{\frac{1}{6}}$. It's clear that if we substitute $x_2(\frac{B_1}{B_2})^{\frac{1}{3}}$ and $y_2(\frac{B_1}{B_2})^{\frac{1}{2}}$, for x_1 and y_1 respectively in E_1, then we obtain E_2, and we are done.

Case 2: $B_1 = 0$, and hence $j = 1728$. By the same reasoning as in Case 1, $A_1 \neq 0$, and $B_2 = 0$. Take $\mu = (\frac{A_1}{A_2})^{\frac{1}{4}}$. Substituting $x_2(\frac{A_1}{A_2})^{\frac{1}{2}}$ and $y_2(\frac{A_1}{A_2})^{\frac{3}{4}}$ in E_1 for x_1 and y_1 respectively, we obtain E_2, and we are done.

Case 3: $A_1B_1 \neq 0$, and so $j \neq 0, 1728$. Then $A_2B_2 \neq 0$, since if one of them was 0, then both of them would be 0, contradicting the fact that the discriminant is nonzero. Take $\mu = (\frac{A_1}{A_2})^{\frac{1}{4}} = (\frac{B_1}{B_2})^{\frac{1}{6}}$ to obtain the desired isomorphism. We have already discussed, in the previous two cases, the required change of variables to obtain E_2 from E_1.

From the proof we deduce that there are two special categories of elliptic curves, corresponding to $j = 0$ and $j = 1728$, respectively. We conclude that:

- $j = 0$: from *Case 1*, we infer that this corresponds to the elliptic curve, E, of the form $x^3 + B$ (since $A_1 = A_2 = 0$).
- $j = 1728$: from *Case 2*, we deduce that this correspond to the elliptic curve E, of the form $x^3 + Ax$ (since $B_1 = B_2 = 0$).

Appealing to an example, we illustrate how we can detect isomorphic elliptic curves using the j-invariant.

Example 2: Let $E_1(\mathbb{F}_{13}) = \{(x_1, y_1) \in \mathbb{F}_{13} \times \mathbb{F}_{13} : y_1^2 = x_1^3 + 2x_1 + 5\} \cup \{O\}$, $E_2(\mathbb{F}_{13}) = \{(x_2, y_2) \in \mathbb{F}_{13} \times \mathbb{F}_{13} : y_2^2 = x_2^3 + 5x_2 + 8\} \cup \{O\}$ and $E_3(\mathbb{F}_{13}) = \{(x_3, y_3) \in \mathbb{F}_{13} \times \mathbb{F}_{13} : y_3^2 = x_3^3 + 8x_3 + 1\} \cup \{O\}$ be three elliptic curves defined over $\mathbb{F}_{13}$. We show that while all three elliptic curves have the same j-invariant in $\mathbb{F}_{13}$, only the first two are isomorphic.

Remark: This emphasizes the central concept that the j-invariant only tells us when curves are isomorphic over an algebraically closed field (for example, in $\overline{\mathbb{F}}_{13}$, we would have $E_1 \cong E_2 \cong E_3$). On the other hand, in a non-algebraically closed field, such as any field of the form $\mathbb{F}_q$, it's possible to have have two curves with the same j-invariant, that are not isomorphic. Therefore, further

inspection is required to ensure that two elliptic curves are isomorphic over a finite filed $\mathbb{F}_q$.

We begin by calculating the j-invariant of each elliptic curve in $\mathbb{F}_{13}$. Note that $1728 = 1729 - 1 = 13 \times 133 - 1 \equiv -1 \pmod{13}$ and also that $27 = 26 + 1 = 2 \times 13 + 1 \equiv 1 \pmod{13}$. Hence, for ease of calculation, let

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2} = -\frac{4A^3}{4A^3 + B^2}$$

in $\mathbb{F}_{13}$. We obtain:

$$j(E_1) \equiv -\frac{4(2)^3}{4(2)^3 + 5^2} \equiv -\frac{32}{32 + 25} \equiv -\frac{6}{5} \pmod{13}.$$

We know that $5^{-1} \equiv 8 \pmod{13}$ (since $5 \times 8 = 40 = 3 \times 13 + 1 \equiv 1 \pmod{13}$). Therefore, $j(E_1) = -6 \times 8 = -48 = 4$ in $\mathbb{F}_{13}$. Similarly, we obtain

$$j(E_2) \equiv -\frac{4(5)^3}{4(5)^3 + 8^2} \equiv -\frac{500}{500 + 64} \equiv -\frac{6}{5} \pmod{13}.$$

We have already seen that this is equivalent to $j(E_2) = 4$ in $\mathbb{F}_{13}$. Lastly,

$$j(E_3) \equiv -\frac{4(8)^3}{4(8)^3 + 1^2} \equiv -\frac{2048}{2048 + 1} \equiv -\frac{7}{8} \pmod{13}.$$

We have previously shown that $5 \times 8 \equiv 1 \pmod{13}$. Hence, $8^{-1} \equiv 5 \pmod{13}$. Therefore, $j(E_3) = -7 \times 5 = -35 = 4$ in $\mathbb{F}_{13}$. We conclude that in $\mathbb{F}_{13}$, $j(E_1) = j(E_2) = j(E_3) = 4$.

Secondly, we show that $E_1 \cong E_2$. Appealing to the proof of Theorem 3.3.2, it's enough to show that there exists μ, such that $5 = 2\mu^4$ and $8 = 5\mu^6$ in $\mathbb{F}_{13}$. We claim that $\mu = 6$ works. We compute

$$2\mu^4 = 2(6)^4 = 2592 = 199 \times 13 + 5 \equiv 5 \pmod{13} \quad \text{and}$$
$$5\mu^6 = 5(6)^6 = 233280 = 17944 \times 13 + 8 \equiv 8 \pmod{13},$$

finishing the second part of the exercise.

Lastly, we show that E_3 is not isomorphic to either E_1 or E_2, despite having the same j-invariant. Note that the isomorphism relation is an equivalence relation, and hence transitive (the interested reader can find a proof of this result in [3, Section 1]), meaning that it suffices to show that either $E_3 \ncong E_1$ or $E_3 \ncong E_2$, as we have already shown that $E_1 \cong E_2$. We claim that there is no μ' in $\mathbb{F}_{13}$ such that $8 = 2\mu'^4$ and $1 = 5\mu'^6$, taking E_1 to E_3. For the sake of contradiction, assume that such a μ' exists. Then, $1 \equiv 5\mu'^6 \pmod{13}$. We have previously seen that $5 \times 8 \equiv 1 \pmod{13}$, implying that $8 \equiv \mu'^6 \pmod{13}$. We can rewrite this as $8 = (\mu'^3)^2$ in $\mathbb{F}_{13}$. But the set of squares, S, in $\mathbb{F}_{13}$ is $S = \{0, 1, 3, 4, 9, 10, 12\}$.

As $8 \notin S$, this leads to a contradiction. Therefore, no such μ' exists and we are done.

Remark: An alternative method would be to calculate the number of points on $E_1(\mathbb{F}_{13})$, $E_2(\mathbb{F}_{13})$ and $E_3(\mathbb{F}_{13})$. The reader will find that $E_1(\mathbb{F}_{13})$ and $E_2(\mathbb{F}_{13})$ both have 12 points, while $E_3(\mathbb{F}_{13})$ has 16 points. By definition, an isomorphism is a bijective map. As one cannot have a bijective map between finite sets of different cardinalities (for a proof of this result the reader is directed to [10]), this also shows that $E_3 \ncong E_1$, and further, that $E_3 \ncong E_2$. An in depth discussion on how to calculate the number of points on an elliptic curve over a finite field can be found in the examples provided in Section 3.6 and Section 4.1.

Remark 2: One can now see where the j-invariant gets its name from. It's an invariant of the isomorphism class of an elliptic curve, E, and it's independent of our choice of the particular equation of E.

Remark 3: As stated in [8, Section 2.7], if two different elliptic curves defined over a field K have the same j-invariant, then the two curves are *twists* of each other. In our example, Example 2, we say that E_1 is a *twist* of E_3.

3.4 Legendre Form

As seen in [7, Section 3.1], there is another way of expressing elliptic curves, which will be key in understanding and proving results in Section 4.3, Supersingular Curves.

Definition 3.4.1: A Weierstrass equation is in *Legendre form* if it can be written as

$$y^2 = x(x-1)(x-\lambda).$$

Proposition 3.4.2 : Assume that $\mathrm{char}(K) \neq 2$.

(a) Every elliptic curve is isomorphic, over $\overline{K}$, to an elliptic curve in Legendre form

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

for some $\lambda \in \overline{K}$, with $\lambda \neq 0, 1$.

(b) The j-invariant of E_λ is

$$j(E_\lambda) = 2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}.$$

(c) The association

$$\overline{K}\backslash\{0,1\} \to \overline{K}, \quad \lambda \mapsto j(E_\lambda),$$

is surjective and exactly six-to-one, except for $j = 0$ and $j = 1728$, where it's two-to-one and three-to-one, respectively.

Remark: (c) is not true for $\text{char}(K) = 3$, but we are not interested in this case. As previously mentioned, the finite fields we are interested in have characteristic a very large prime.

Proof: (a) Since $\text{char}(K) \neq 2$, we know E has a Weierstrass equation of the form

$$y^2 = x^3 + a_2'x^2 + a_4'x + a_6'.$$

Factorise the cube as,

$$y^2 = x^3 + a_2'x^2 + a_4'x + a_6' = (x - e_1)(x - e_2)(x - e_3),$$

with $e_1, e_2, e_3 \in \overline{K}$. Moreover, since the discriminant of the polynomial is

$$\Delta = 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2 \neq 0,$$

we note that the e_i's are distinct. The substitution

$$x = (e_2 - e_1)x' + e_1 \quad \text{and} \quad y = (e_2 - e_1)^{3/2}y',$$

results in an equation in Legendre form with

$$\lambda = \frac{e_3 - e_1}{e_2 - e_1} \in \overline{K}.$$

As the e_i's are distinct, $\lambda \neq 0, 1$.

(b) From (a), we know that every elliptic curve is isomorphic, over $\overline{K}$, to an elliptic curve in Legendre form. Hence, the goal is to find a suitable change of variables that will transform the elliptic curve $E_\lambda : y^2 = x(x - 1)(x - \lambda)$ into $E' : y'^2 = x'^3 + Ax' + B$ (as previously discussed we can further assume that $\text{char}(K) \neq 3$). By Theorem 3.3.2, isomorphic elliptic curves over $\overline{K}$ have the same j-invariant. Therefore, $j(E_\lambda) = j(E')$ and it suffices to calculate $j(E') = \frac{4A^3}{4A^3 - 27B^2}$. We claim that

$$y = y' \quad \text{and} \quad x = x' - \frac{-\lambda - 1}{3}$$

works (since by assumption $\text{char}(K) \neq 3$, we are not dividing by 0). Substituting in the original equation, we obtain:

$$y'^2 = \left(x' - \frac{-\lambda - 1}{3}\right)\left(\left(x' - \frac{-\lambda - 1}{3}\right) - 1\right)\left(\left(x' - \frac{-\lambda - 1}{3}\right) - \lambda\right).$$

Opening up the brackets and rearranging, we get:

$$y'^2 = x'^3 + \left(-\frac{1}{3}(\lambda + 1)^2 + \lambda\right)x' + \frac{4(\lambda + 1)^3 + 9\lambda(\lambda + 1)}{27}.$$

(essentially cancelling the terms in x'^2, as when we open the brackets we obtain $-3\left(\frac{-\lambda-1}{3}\right)x'^2 + -(\lambda+1)x'^2 = (\lambda+1)x'^2 - (\lambda+1)x'^2 = 0$). Substituting in the values we obtained for A and B, we get:

$$j(E') = \frac{4\left(-\frac{1}{3}(\lambda+1)^2+\lambda\right)^3}{4\left(-\frac{1}{3}(\lambda+1)^2+\lambda\right)^3 - 27\left(\frac{4(\lambda+1)^3+9\lambda(\lambda+1)}{27}\right)^2}.$$

A computationally laborious process of rearranging and expanding the brackets gives the desired result.

(c) Recall that the j-invariant classifies elliptic curves up to isomorphism. Hence, suppose that $E_\lambda$and E_μ have the same j-invariant, or in other words, they are isomorphic over $\overline{K}$. In the previous section, we noted that a change of variables relates the two elliptic curves: $x = u^2x' + r$ and $y = u^3y'$. Writing the two elliptic curves in Legendre form, we obtain:

$$x(x-1)(x-\mu) = \left(x + \frac{r}{u^2}\right)\left(x + \frac{r-1}{u^2}\right)\left(x + \frac{r-\lambda}{u^2}\right).$$

This implies there are six ways of assigning the linear terms to one another. In particular, this yields six particular values of μ in terms of λ, as shown below:

$$\mu \in \left\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}\right\}.$$

Therefore, $\lambda \mapsto j(E_\lambda)$ is six to one, unless two or more values of μ are the same. By equating the pairs, we note that this is the case if and only if $\lambda \in \{-1, 2, \frac{1}{2}\}$, corresponding to a three-to-one association and $j = 1728$ or if and only if $\lambda^2 - \lambda + 1 = 0$, corresponding to a two-to-one association and $j = 0$.

3.5 Endomorphisms

This section introduces and proves some results which are key in the proof of Hasse's Theorem in Section 4.1. A similar approach can be found in [8, Section 2.9].

Definition 3.5.1: An *endomorpshism* of an elliptic curve E, is a homomorphism $\alpha : E(\overline{K}) \to E(\overline{K})$ that is given by rational functions. A *rational function* is a function that can be expressed as the quotient of two polynomial functions. More specifically, $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$, and there are rational functions $R_1(x, y), R_2(x, y)$ with coefficients in $\overline{K}$ such that:

$$\alpha(x, y) = (R_1(x, y), R_2(x, y))$$

for all $(x, y) \in E(\overline{K})$.

As one of the properties of a homomorphism is that it maps the identity element of the domain to the identity element of the codomain, one can easily deduce that $\alpha(O) = O$. Secondly, we assume that α is nontrivial, or, in other words, that there exits some (x, y) such that $\alpha(x, y) \neq O$. The *trivial endomorphism* is the endomorphism that maps every point $(x, y) \in E(\overline{K})$ to O and is denoted by 0.

Example: Let $E : y^2 = x^3 + 2x + 5$ be an elliptic curve, and let $\alpha(P) = 3P$, for any point $P = (x, y) \in E$. It's clear that α is a homomorphism. We want to show that α is an endomorphism. Hence, we need to show that

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)).$$

Note that $3P = 2P + P$. From Section 3.2, we know that addition of points on elliptic curves is both associative and commutative. Hence, we can apply Case 3, followed by Case 1, from Point Addition to obtain our result. From Case 3, we obtain: $2P = \left(\left(\frac{3x^2+2}{2y}\right)^2 - 2x, \quad \left(\frac{3x^2+2}{2y}\right)\left(3x - \left(\frac{3x^2+2}{2y}\right)^2\right) - y\right)$. Applying Case 1, we obtain: $\alpha(P) = 3P = (R_1(x, y), R_2(x, y))$, where

$$R_1(x, y) = m^2 + x - \left(\frac{3x^2 + 2}{2y}\right)^2$$
$$R_2(x, y) = m\left(x - R_1\left(x, y\right)\right) - y,$$

and $m = \frac{2y((3x^2+2)^2-12xy^2)}{12xy^2(3x^2+2)-(3x^2+2)^3-16y^2}$. Hence, as α is a homomorphism given by rational functions, it's an endomorphism of E.

Remark: We can generalise this result for any elliptic curve of the form $E : y^2 = x^3 + Ax + B$, as we obtain the same result if we substitute A for 2 and B for 5, respectively.

For convenience, it will be useful to have a standard form for the rational functions characterizing an endomorphism. We continue with our assumption that E is an elliptic curve given in simplified Weierstrass form. Take $R(x, y)$ to be an arbitrary rational function. Since $y^2 = x^3 + Ax + B$ for all $(x, y) \in E(\overline{K})$, we can replace every even power of y by a polynomial in x, and replace any odd power of y by y times a polynomial in x. This yields a rational function which gives the same function as $R(x, y)$ on points in $E(\overline{K})$. Hence, assume that:

$$R(x, y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}.$$

Furthermore, we can rationalise the denominator by multiplying the numerator and denominator by $p_3(x) - p_4(x)y$, and then replacing y^2 by $x^3 + Ax + B$. We obtain:

$$R(x, y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}, \tag{4}$$

where $q_1(x) = p_1(x)p_3(x) - p_2(x)p_4(x)(x^3 + Ax + B)$, $q_2(x) = p_2(x)p_3(x) - p_1(x)p_4(x)$ and $q_3(x) = p_3^2(x) - p_4^2(x)(x^3 + Ax + B)$.

Consider an endomorphism of the form:

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)),$$

as before. Since α is a homomorphism, one of its properties is that:

$$\alpha(x, -y) = \alpha(-(x, y)) = -\alpha(x, y).$$

This implies that

$$R_1(x, -y) = R_1(x, y) \quad \text{and} \quad R_2(x, -y) = -R_2(x, y).$$

Hence, if R_1 is written in the same form as (4), then the corresponding $q_2(x) = 0$. Similarly, if we write R_2 in the same form as (4), then the corresponding $q_1(x) = 0$. Therefore, we can simply this further by having

$$\alpha(x, y) = (r_1(x), yr_2(x)),$$

with rational functions $r_1(x) = \frac{q_1(x)}{q_3(x)}$ and $r_2(x) = \frac{q_2(x)}{q_3(x)}$.

Remark: A technical point we have omitted, as it's not central to the project, is to consider the case when one of the rational functions is not defined at a point. Write $r_1(x) = \frac{p(x)}{q(x)}$, such that the polynomials $p(x), q(x)$ don't have a common factor. If $q(x) = 0$, for some point (x, y), then we assume that $\alpha(x, y) = O$. For the case when $q(x) \neq 0$, $r_2(x)$ is defined. The interested reader can find a detailed account in [8, Exercise 2.19]. Therefore, the rational functions defining α are defined.

Definition 3.5.2: Define the *degree* of α to be

$$\deg(\alpha) = \max\{\deg p(x), \deg q(x)\}$$

if α is nontrivial (where $p(x), q(x)$ are as above). When $\alpha = 0$, let $\deg(0) = 0$.

Definition 3.5.3 We say that α, $\alpha \neq 0$, is a *separable endomorphism* if the derivative $r_1'(x) \neq 0$.

Remark 1: As we are interested in finite fields, we note that in characteristic $p > 0$, the polynomials with zero derivatives are exactly those of the form $g(x^p)$.

Definition 3.5.4: Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, where q is a prime power or, in other words, $q = p^n$, p prime and $n \in \mathbb{Z}$. The *Frobenius map* is:

$$\phi_q(x, y) = (x^q, y^q).$$

The Frobenius map, $\phi_q(x, y)$, plays a fundamental role in the study of elliptic curves over finite fields $\mathbb{F}_q$.

Lemma 3.5.5: Let E be defined over $\mathbb{F}_q$, and let $(x, y) \in E(\overline{\mathbb{F}}_q)$. Then,

1. $\phi_q(x, y) \in E(\overline{\mathbb{F}}_q)$
2. $(x, y) \in E(\mathbb{F}_q)$ if and only if $\phi_q(x, y) = (x, y)$

Proof: We begin by appealing to the following result: $(a + b)^q = a^q + b^q$ in $\mathbb{F}_q$ (to see why this is the case, note that $(a + b)^q = \sum_{i=1}^{q} \binom{q}{i} a^{q-i}b^i = \sum_{i=1}^{q} \frac{q!}{i!(q-i)!} a^{q-i}b^i$. If $i \neq 0, q$, then we obtain $q \times Aa^{q-i}b^i \equiv 0 \pmod{q}$. One can see that when $i = 0$, we obtain a^q and, similarly, for $i = q$ we get b^q. Putting everything together, $(a + b)^q = a^q + 0 + \cdots + 0 + b^q = a^q + b^q$ in $\mathbb{F}_q$). Secondly, by Theorem 2.1.8, $a^q = a$ for all $a \in \mathbb{F}_q$. Hence, $(a+b)^q = a^q + b^q = a + b$ in $\mathbb{F}_q$.

As the proof is the same for the simplified and the generalised Weierstrass equation, we work with the generalised form. We have:

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

with $a_i \in \mathbb{F}_q$. Raising the equation to the qth power, and appealing to the fact that $(a + b)^q = a^q + b^q = a + b$ in $\mathbb{F}_q$, we obtain:

$$(y^q)^2 + a_1(x^q y^q) + a_3(y^q) = (x^q)^3 + a_2(x^q)^2 + a_4(x^q) + a_6.$$

This entails that (x^q, y^q) lies on E, proving (1).

For (2), we need the following fact: $x \in \mathbb{F}_q$ if and only if $\phi_q(x) = x$ (for a proof see [8, Appendix C]), and the same holds for y. Hence, we have that:

$$\begin{aligned}(x, y) \in \mathbb{F}_q &\Leftrightarrow x, y \in \mathbb{F}_q \\ &\Leftrightarrow \phi_q(x) = x \quad \text{and} \quad \phi_q(y) = y \\ &\Leftrightarrow \phi_q(x, y) = (x, y),\end{aligned}$$

and we are done.

Lemma 3.5.6: Let $E : y^2 = x^3 + Ax + B$ be defined over $\mathbb{F}_q$. Then, the Frobenius map, $\phi_q(x, y)$, is an endomorphism of E of degree q, and $\phi_q(x, y)$ is not separable.

Proof: Since the Frobenius map is defined as $\phi_q(x, y) = (x^q, y^q)$, it's clear that the map is specified by rational functions of degree q. The key idea is that $\phi_q(x, y) : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)$ is a homomorphism. Take $(x_1, y_1), (x_2, y_2) \in E(\overline{\mathbb{F}}_q)$ with $x_1 \neq x_2$. Let $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$. By Case 1 in Section 3.2, Point Addition, we obtain:

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

Raising everything to the qth power, and again, using the fact that $(a + b)^q = a^q + b^q$ in $\mathbb{F}_q$, we obtain:

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

This implies that

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

showing that $\phi_q(x, y)$ is a homomorphism. One can use Cases 2 and 4, respectively, from the same section, to check the cases when $x_1 = x_2$, or when one of the points is the point at infinity, O. However, there is one subtlety that arises when adding a point to itself (Case 3). The result for point addition states that $2(x_1, y_1) = (x_3, y_3)$, with

$$x_3 = m^2 - 2x_1 \quad \text{and} \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{where } m = \frac{3x_1^2 + A}{2y_1}.$$

By the same reasoning as before, raising this to the qth power, we obtain:

$$x_3^q = m'^2 - 2x_1^q \quad \text{and} \quad y_3^q = m'(x_1^q - x_3^q) - y_1^q, \quad \text{where } m' = \frac{3^q(x_1^q)^2 + A^q}{2^q y_1^q}.$$

We have previously assumed that $A \in \mathbb{F}_q$. A further assumption is that q is a large prime or the power of a large prime, so $2, 3 \in \mathbb{F}_q$ also. Hence, by Theorem 2.1.8, $2^q = 2, 3^q = 3$ and $A^q = A$ in $\mathbb{F}_q$. This shows that we obtain the desired formula for doubling the point (x_1^q, y_1^q) on E. Note that if $A^q \neq A$, then we would be working on a new elliptic curve with A^q instead of A.

Therefore, we have shown that $\phi_q(x, y)$ is a homomorphism given by rational functions and hence, an endomorphism of E.

Lastly, we show that $\phi_q(x, y)$ is not separable. We appeal to Definition 3.5.3. As $q = 0$ in $\mathbb{F}_q$, the derivative of x^q is $qx^{q-1} = 0$ in $\mathbb{F}_q$, and we are done.

The following result, Proposition 2.21 of [8], is fundamental to the proof of Hasse's Theorem, Theorem 4.1.1:

Proposition 3.5.7: Let $\alpha \neq 0$ be a separable endomorphism of an elliptic curve E. Then

$$\deg \alpha = \#\mathrm{Ker}(\alpha),$$

where $\mathrm{Ker}(\alpha)$ is the kernel of the homomorphism $\alpha : E(\overline{K}) \to E(\overline{K})$.
If $\alpha \neq 0$ is not separable, then

$$\deg \alpha > \#\mathrm{Ker}(\alpha).$$

Proof: As before, let $\alpha(x, y) = (r_1(x), yr_2(x))$, such that $r_1(x) = \frac{p(x)}{q(x)}$.
Case 1: Assume that α is separable. By Definition 3.5.3, it follows that $r_1'(x) \neq 0$. Therefore, $r_1'(x) = p'(x)q(x) - p(x)q'(x)$ is not the zero polynomial.
Let S be the set of $x \in \overline{K}$ such that $(p'q - pq')(x)q(x) = 0$. Let $(a, b) \in E(\overline{K})$ be such that:

1. $a, b \neq 0, (a, b) \neq O$,

2. $\deg(p(x) - aq(x)) = \max\{\deg(p), \deg(q)\} = \deg(\alpha)$,

3. $a \notin r_1(S)$, and

4. $(a, b) \in \alpha(E(\overline{K}))$.

As $p'(x)q(x) - p(x)q'(x)$ is not the zero polynomial, S is a finite set and therefore, its image under α is finite. One can easily see that the function $r_1(x)$ takes infinitely many distinct values as x varies through $\overline{K}$. As for each x there exists a point $(x, y) \in E(\overline{K})$, $\alpha(E(\overline{K}))$ is an infinite set. Hence, there exists an $(a, b) \in E(\overline{K})$ satisfying $(1) - (4)$.

Claim: There are exactly $\deg(\alpha)$ points $(x_1, y_1) \in E(\overline{K})$ such that $\alpha(x_1, y_1) = (a, b)$. For such a point, we have:

$$a = \frac{p(x_1)}{q(x_1)}, \quad b = y_1 r_2(x_1).$$

Recall (1): $(a, b) \neq O$. It follows that $q(x_1) \neq 0$ also. We have previously showed that $r_2(x_1)$ is defined. As $b \neq 0$ and $b = y_1 r_2(x_1)$, we obtain that $y_1 = \frac{b}{r_2(x_1)}$. This shows that y_1 is determined by x_1. Hence, we only need to count the values of x_1.

By assumption (2), $p(x) - aq(x) = 0$ has $\deg(\alpha)$ roots, counting multiplicity. Hence, we need to show that $p(x) - aq(x)$ has no multiple roots. Assume, for the sake of contradiction, that x_0 is a multiple root. Then

$$p(x_0) - aq(x_0) = 0 \quad \text{and} \quad p'(x_0) - aq'(x_0) = 0.$$

Multiplying the two equations $p(x_0) = aq(x_0)$ and $aq'(x_0) = p'(x_0)$, we obtain:

$$ap(x_0)q'(x_0) = ap'(x_0)q(x_0).$$

As $a \neq 0$ from assumption (1), this implies that x_0 is a root of $p(x)q'(x) - p'(x)q(x)$, and so $x_0 \in S$. Hence, $a = r_1(x_0) \in r_1(S)$, contradicting assumption (3). It follows that $p(x)q'(x) - p'(x)q(x)$ has no multiple roots. Therefore, $p(x)q'(x) - p'(x)q(x)$ has $\deg(\alpha)$ distinct roots.

As there are exactly $\deg(\alpha)$ points (x_1, y_1) such that $\alpha(x_1, y_1) = (a, b)$, the kernel of α has $\deg(\alpha)$ elements.

As α is a homomorphism, for each $(a, b) \in \alpha(E(\overline{K}))$, there are exactly $\deg(\alpha)$ points (x_1, y_1) with $\alpha(x_1, y_1) = (a, b)$.
Remark: The assumptions $(1) - (4)$ were required during the proof to ensure that this result holds for at least one point, which suffices.

Case 2: Assume that α is not separable. If α is not separable, the steps in the proof above hold. The only difference is that $p'(x) - aq'(x)$ is always the zero

polynomial. Hence, $p(x) - aq(x) = 0$ always has multiple roots and therefore, has fewer than $\deg(\alpha)$ solutions.

Remark 2: From this result, we can infer that the kernel of the Frobenius map, ϕ_q, is trivial. We have previously shown, Lemma 3.5.6, that ϕ_q is not separable and has degree q. Therefore, $q > \#\text{Ker}(\phi_q)$. But as q is a prime power, $q \geq 2$, and hence, $\#\text{Ker}(\phi_q) < 2$. Therefore, $\#\text{Ker}(\phi_q) = 1$. The only point in $\text{Ker}(\phi_q)$ is O, the point at infinity.

The next result is key to counting points on elliptic curves over finite fields. Since ϕ_q is an endomorphism of E, then so are $\phi_q^2 = \phi_q \circ \phi_q$, and $\phi_q^n = \underbrace{\phi_q \circ \phi_q \circ \cdots \circ \phi_q}_{n \text{ times}}$ for all $n \geq 1$. As multiplication by -1 is also an endomorphism, the sum $\phi_q^n - 1$ is an endomorphism of E.

Proposition 3.5.8: Let E be defined over $\mathbb{F}_q$ and let $n \geq 1$. Then,

1. $\text{Ker}(\phi_q^n - 1) = E(\mathbb{F}_{q^n})$.
2. $\phi_q^n - 1$ is a separable endomorphism, so $\#E(\mathbb{F}_{q^n}) = \deg(\phi_q^n - 1)$.

Proof: As ϕ_q^n is the Frobenius map for the finite field $\mathbb{F}_{q^n}$, part (1) is just a restatement of Lemma 3.5.5. As it's beyond the scope of this project, we omit the proof for the separability of $\phi_q^n - 1$. However, the interested reader is directed to Proposition 2.29 of [8]. We conclude that (2) follows from Proposition 3.5.7.

3.6 Isogenies

Isogenies play a central role in understanding elliptic curves, as they allow us to relate two elliptic curves to one another. The main goal of this subsection is to illustrate how isogenies can be used to count points on elliptic curves over finite fields. The main results are taken from [7, Section 3.4] and [8, Section 12.1].

Definition 3.6.1: Let $E_1 : y_1^2 = x_1^3 + A_1 x_1 + B_1$, $E_2 : y_2^2 = x_2^3 + A_2 x_2 + B_2$ be two elliptic curves over a field K. An *isogeny* from E_1 to E_2 is a nonconstant homomorphism $\alpha : E_1(\overline{K}) \to E_2(\overline{K})$ that is given by rational functions.

This implies that $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$ for all $P_1, P_2 \in E_1(\overline{K})$, and that there exist rational functions R_1, R_2 such that if $\alpha(x_1, y_1) = (x_2, y_2)$ then

$$x_2 = R_1(x_1, y_1), \quad y_2 = R_2(x_1, y_1)$$

for all but finitely many $(x_1, y_1) \in E_1(\overline{K})$. The technicalities for the points where R_1 and R_2 are not defined are dealt with in a similar manner to the analogue case for endomorphisms, in the previous section, Section 3.5.

Remark 1: When $E_1 = E_2$, an isogeny is a nonzero endomorphism.

As in the previous section, we can write α in the following way:

$$(x_2, y_2) = \alpha(x_1, y_1) = (r_1(x_1), y_1 r_2(x_1)),$$

with r_1, r_2 rational functions. If the coefficients of r_1, r_2 are in K, we say that α is *defined over* K. Let

$$r_1(x) = \frac{p(x)}{q(x)}$$

with polynomials $p(x), q(x)$ that don't have a a common factor.

Definition 3.6.2: The *degree* of α is defined as:

$$\deg(\alpha) = \max\{\deg p(x), \deg q(x)\}.$$

Definition 3.6.3: We say that α is *separable* if the derivative $r_1'(x)$ is not identically zero.

In the following example, we illustrate how to apply these results. Note that we consider two elliptic curves E_1, E_2 defined over a finite field $\mathbb{F}_p$, and therefore restrict our attention to an isogeny defined over $\mathbb{F}_p$.

Example 1: Let E_1, E_2 be two elliptic curves defined over the finite field $\mathbb{F}_{17}$, such that $E_1(\mathbb{F}_{17}) = \{(x_1, y_1) \in \mathbb{F}_{17} \times \mathbb{F}_{17} : y_1^2 = x_1^3 + 11x_1 + 13\} \cup \{O\}$ and $E_2(\mathbb{F}_{17}) = \{(x_2, y_2) \in \mathbb{F}_{17} \times \mathbb{F}_{17} : y_2^2 = x_2^3 + 15x_2 + 12\} \cup \{O\}$. Find an isogeny, α, such that $\alpha : E_1(\mathbb{F}_{17}) \to E_2(\mathbb{F}_{17})$.

First, we check whether the two elliptic curves are isomorphic. If $E_1 \cong E_2$, then we can simply use the transformation for the change of variables discussed in Section 3.3. Recall that for two elliptic curves over a finite field to be isomorphic, they must have the same j-invariant and the same number of points, $\#E_1(\mathbb{F}_{17}) = \#E_2(\mathbb{F}_{17})$. Hence, we begin by computing $j(E_1)$ and $j(E_2)$, remembering to work mod 17. Note that $1728 = 101 \times 17 + 11 \equiv 11 \pmod{17}$ and $27 = 17 + 10 \equiv 10 \pmod{17}$. We can now rewrite Definition 3.3.1 as:

$$j(E) = 11\frac{4A^3}{4A^3 + 10B^2} \quad \text{in} \quad \mathbb{F}_{17}.$$

Therefore, we obtain:

$$j(E_1) = 11 \times \frac{4(11)^3}{4(11)^3 + 10(13)^2} = 11 \times \frac{5324}{7014} = 11 \times \frac{3}{10} \quad \text{in} \quad \mathbb{F}_{17}.$$

Note that $12 \times 10 = 120 = 17 \times 7 + 1 \equiv 1 \pmod{17}$, and hence, $10^{-1} = 12$ in $\mathbb{F}_{17}$. Therefore $j(E_1) = 11 \times 3 \times 12 = 396 = 17 \times 23 + 5 \equiv 5 \pmod{17}$. Similarly,

$$j(E_2) = 11 \times \frac{4(15)^3}{4(15)^3 + 10(12)^2} = 11 \times \frac{75}{83} = 11 \times \frac{7}{15} \quad \text{in} \quad \mathbb{F}_{17}.$$

Note that $15 \times 8 = 120 \equiv 1 \pmod{17}$ (as previously seen), and hence, $15^{-1} = 8$ in $\mathbb{F}_{17}$. Therefore, $j(E_2) = 11 \times 7 \times 8 = 616 = 17 \times 36 + 4 \equiv 4 \pmod{17}$. Hence,

$$j(E_1) = 5 \quad \text{and} \quad j(E_2) = 4 \quad \text{in} \quad \mathbb{F}_{17}.$$

Since $4 \neq 5$ in $\mathbb{F}_{17}$, the two elliptic curves are not isomorphic, $E_1 \ncong E_2$. Therefore, a change of variables transformation won't work.

Claim: The following map, $\alpha : E_1(\mathbb{F}_{17}) \to E_2(\mathbb{F}_{17})$, gives the desired isogeny:

$$\alpha(x_1, y_1) = \left(\frac{x_1^2 + 2x_1 + 6}{x_1 + 2}, \quad y_1 \left(\frac{x_1^2 + 4x_1 - 2}{x_1^2 + 4x_1 + 4} \right) \right),$$

with

$$r_1(x_1) = \frac{x_1^2 + 2x_1 + 6}{x_1 + 2} \quad \text{and} \quad y_1 r_2(x_1) = y_1 \left(\frac{x_1^2 + 4x_1 - 2}{x_1^2 + 4x_1 + 4} \right)$$

(in Appendix A, we provide a SageMath code for finding an isogeny, α, between an elliptic curve $E_1 : y_1^2 = x_1^3 + A_1 x_1 + B_1$ over a finite field $\mathbb{F}_p$ and a second elliptic curve, $E_2 : y_2^2 = x_2^3 + A_2 x_2 + B_2$ over the same finite field).

It's evident that r_1 and r_2 are rational functions, and that their coefficients are members of $\mathbb{F}_{17}$. Hence, we can say that α is defined over $\mathbb{F}_{17}$. To prove that α is the desired isogeny, it remains to show that α maps points of $E_1(\mathbb{F}_{17})$ to points of $E_2(\mathbb{F}_{17})$ and that α is a homomorphism.

To show that α maps points of $E_1(\mathbb{F}_{17})$ to points of $E_2(\mathbb{F}_{17})$, we substitute $r_1(x_1, y_1)$ and $y_1 r_2(x_1, y_1)$ in $E_2(\mathbb{F}_{17})$ and show that the equation is satisfied:

$$\left(y_1 \left(\frac{x_1^2 + 4x_1 - 2}{x_1^2 + 4x_1 + 4} \right) \right)^2 = \left(\frac{x_1^2 + 2x_1 + 6}{x_1 + 2} \right)^3 + 15 \left(\frac{x_1^2 + 2x_1 + 6}{x_1 + 2} \right) + 12.$$

Noting that $x_1^2 + 4x_1 + 4 = (x_1 + 2)^2$, we can now rewrite the equation as:

$$y_1^2 \frac{(x_1^2 + 4x_1 - 2)^2}{(x_1 + 2)^4} = \frac{(x_1^2 + 2x_1 + 6)^3}{(x_1 + 2)^3} + 15 \frac{(x_1^2 + 2x_1 + 6)}{(x_1 + 2)} + 12.$$

Multiplying both sides by $(x_1 + 2)^4$, we obtain:

$$y_1^2 (x_1^2 + 4x_1 - 2)^2 = (x_1^2 + 2x_1 + 6)^3 (x_1 + 2) + 15 (x_1^2 + 2x_1 + 6)(x_1 + 2)^3 + 12 (x_1 + 2)^4.$$

Opening up the brackets and reducing mod 17, we obtain:

$$y_1^2 (x_1^2 + 4x_1 - 2)^2 = x_1^7 + 8x_1^6 + 6x_1^5 + 2x_1^3 + 14x_1^2 + 6x_1 + 1.$$

Dividing both sides by $(x_1^2 + 4x_1 - 2)^2$, we obtain:

$$y_1^2 = x_1^3 + 11x_1 + 13.$$

This finishes this first part of our proof.
(from the definition of $E_1(\mathbb{F}_{17})$ we know that x_1 and y_1 satisfy this relation)

To prove that α is a homomorphism, we have to show that for all $P_1, P_2 \in E_1(\mathbb{F}_{17})$,

$$\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2).$$

We first illustrate how this works with two points $P_1, P_2 \in E_1(\mathbb{F}_{17})$. Let $P_1 = (1, 5)$ and $P_2 = (7, 12)$. We begin by showing that indeed, $P_1, P_2 \in E_1(\mathbb{F}_{17})$: $1^3 + 11(1) + 13 = 25 \equiv 8 \pmod{17}$ and $5^2 = 25 \equiv 8 \pmod{17}$, also, and secondly, $7^3 + 11(7) + 13 = 433 \equiv 8 \pmod{17}$, and $12^2 = 144 \equiv 8 \pmod{17}$, also, and we are done. Since neither P_1 nor P_2 is the point at infinity, O, and they have distinct x-coordinates ($1 \neq 7$ in $\mathbb{F}_{17}$), to compute $P_1 + P_2$, we appeal to Case 1, from Point Addition, Section 3.2. We first find the value of m, remembering to work $\pmod{17}$: $m = \frac{12-5}{7-1} = \frac{7}{6}$ in $\mathbb{F}_{17}$. Note that $6 \times 3 = 18 \equiv 1 \pmod{17}$, and hence $6^{-1} = 3$ in $\mathbb{F}_{17}$. Therefore, $m \equiv 7 \times 3 \equiv 21 \equiv 4 \pmod{17}$. We can now compute the coordinates (x_3, y_3) of $P_1 + P_2$:

$$x_3 = 4^2 - 1 - 7 = 8 \quad \text{and} \quad y_3 = 4(1 - 8) - 5 = -33 = 1 \quad \text{in} \quad \mathbb{F}_{17}.$$

Hence, we obtain: $P_1 + P_2 = (8, 1)$ on $E(\mathbb{F}_{17})$. We apply α to $P_1 + P_2$:

$$\begin{aligned}
\alpha(P_1 + P_2) &= \alpha((8, 1)) \\
&= \left(\frac{8^2 + 2(8) + 6}{8 + 2}, \quad 1 \times \frac{8^2 + 4(8) - 2}{8^2 + 4(8) + 4}\right) \\
&= \left(\frac{86}{10}, \frac{94}{100}\right) \\
&= \left(\frac{1}{10}, \frac{9}{15}\right) \quad \text{in} \quad \mathbb{F}_{17}.
\end{aligned}$$

Note that $10 \times 12 = 15 \times 8 = 120 \equiv 1 \pmod{17}$, and hence, $10^{-1} = 12$ and $15^{-1} = 8$ in $\mathbb{F}_{17}$. Therefore, $\frac{1}{10} = 1 \times 12 = 12$ and $\frac{9}{15} = 9 \times 8 = 72 = 4$ in $\mathbb{F}_{17}$. Hence,

$$\alpha(P_1 + P_2) = (12, 4) \quad \text{on} \quad E_2(\mathbb{F}_{17}).$$

(note that indeed, $(12, 4) \in E_2(\mathbb{F}_{17})$: $12^3 + 15(12) + 12 = 1920 \equiv 16 \pmod{17}$ and $4^2 = 16 \equiv 16 \pmod{17}$, also).

We similarly compute $\alpha(P_1)$ and $\alpha(P_2)$, and obtain:

$$\alpha(P_1) = (3, 13) \quad \text{and} \quad \alpha(P_2) = (2, 13) \quad \text{on} \quad E_2(\mathbb{F}_{17})$$

(we omit the details, as the calculations are identical to the ones showcased above). Note that indeed, $(3, 13), (2, 13) \in E_2(\mathbb{F}_{17})$, since $3^3 + 15(3) + 12 = 84 \equiv 16 \pmod{17}$, and $13^2 = 169 \equiv 16 \pmod{17}$, also, and lastly, $2^3 + 15(2) + 12 = 50 \equiv 16 \pmod{17}$, also.

Lastly, we compute $\alpha(P_1) + \alpha(P_2) = (3, 13) + (2, 13)$ on $E_2(\mathbb{F}_{17})$. As $P_1 \neq P_2$, neither of them is the point at infinity O, and they have distinct x-coordinates ($3 \neq 2$ in $\mathbb{F}_{17}$), we use Case 1 of Section 3.2. We begin by computing m: $m = \frac{13-13}{2-3} = 0$. Hence,

$$x_3 = 0^2 - 2 - 3 = -5 = 12 \quad \text{and} \quad y_3 = 0(3 - 12) - 13 = -13 = 4 \quad \text{in} \quad \mathbb{F}_{17}.$$

Therefore, $\alpha(P_1) + \alpha(P_2) = (12, 4)$ on $E_2(\mathbb{F}_{17})$. Since $(12, 4) = (12, 4)$, it's evident that:

$$\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2).$$

To prove that α is a homomorphism, we would have to show that this holds for all points $P_1, P_2 \in E_1(\mathbb{F}_{17})$. As illustrated, this approach is computationally laborious, so often, an alternative method is used, namely Theorem 3.6.4.

However, before discussing this alternative approach, note that we are ineterested in determining the degree of α and whether it's a separable iosgeny. By Definition 3.6.2, to determine the degree of α, we look at

$$r_1(x_1) = \frac{x_1^2 + 2x_1 + 6}{x_1 + 2}.$$

It's clear that $p(x_1) = x_1^2+2x_1+6$ and $q(x_1) = x_1+2$ are coprime (if $q(x_1)|p(x_1)$, then $p(-2) = 0$ in $\mathbb{F}_{17}$; but $p(-2) = 6 \neq 0$ in $\mathbb{F}_{17}$, so $q(x_1) \nmid p(x_1)$). Therefore,

$$\deg(\alpha) = \max\{\deg p(x_1), \deg q(x_1)\} = \max\{2, 1\} = 2.$$

By Definition 3.6.3, to determine whether α is separable, we compute $r'(x_1)$:

$$r'(x_1) = \frac{x_1^2 + 4x_1 - 2}{(x_1 + 2)^2}.$$

Hence, $r'(x_1)$ is zero in $\mathbb{F}_{17}$ if and only if $x_1^2 + 4x_1 - 2 = 0$ in $\mathbb{F}_{17}$. Note that $x_1^2+4x_1-2 = (x_1+2)^2-6$. If there exists an $x_1 \in \mathbb{F}_{17}$ such that $x_1^2+4x_1-2 = 0$, then $(x_1 + 2)^2 - 6 = 0$, also, and hence, $(x_1 + 2)^2 = 6$ in $\mathbb{F}_{17}$. But 6 is not a square in $\mathbb{F}_{17}$, and hence the equation $x_1^2 + 4x_1 - 2 = 0$ has no solutions in $\mathbb{F}_{17}$, or, in other words $x_1^2 + 4x_1 - 2 \neq 0$ in $\mathbb{F}_{17}$. Therefore, $r'(x_1) \neq 0$ in $\mathbb{F}_{17}$ and hence, α is separable. Putting everything together, we conclude that α is a separable isogeny of degree 2.

Remark: While not discussed in this example, as it's beyond the scope of this project, note that for an isogeny to exist between two elliptic curves E_1, E_2 over a finite field $\mathbb{F}_p$, the two curves must have the same number of points. An in depth discussion of why this is necessary can be found in [11]. In our example, $\#E_1(\mathbb{F}_{17}) = \#E_2(\mathbb{F}_{17}) = 22$. A discussion on how to calculate the number of points on an elliptic curve, E over a finite field $\mathbb{F}_p$, can be found in the second example provided in this section, Example 2.

Theorem 3.6.4: Let E_1, E_2 be two elliptic curves over a field K. Let $\alpha : E_1(\overline{K}) \to E_2(\overline{K})$ be a nonconstant map given by rational functions. If

$$\alpha(O) = O,$$

then α is a homomorphism, and therefore, an isogney.

Proof: The proof and application of this result are beyond the scope of this project, so we omit them. The interested reader is directed to [8, Theorem 12.10].

The theory of understanding and constructing isogenies between two elliptic curves is very rich in itself. A detailed account extends far beyond the scope of this project, but the interested reader is directed to [7, Setion 3.4] and [8, Chapter 12]. For an in depth discussion on how to construct an isogeny between two elliptic curves E_1, E_2, over $\mathbb{F}_p$, where $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$, we point the reader to [11]. This article is particularly fascinating, as it provides a general algorithm for the construction.

Definition 3.6.5: Let E be an elliptic curve and let $m \in \mathbb{Z}$ with $m \geq 1$. The *m-torsion subgroup of E*, denoted by $E[m]$, is the set of points of order m,

$$E[m] = \{P \in E : [m]P = 0\}.$$

Example 2: Let E be the following elliptic curve defined over $\mathbb{F}_5$, $E(\mathbb{F}_5) = \{(x, y) \in \mathbb{F}_5 \times \mathbb{F}_5 : y^2 = x^3 + x + 3\} \cup \{O\}$. We want to find $E[2]$.

Firstly, we determine the points on $E(\mathbb{F}_5)$. As we are working with a small finite field, we can list the solutions $x^3 + x + 3 \pmod 5$ for $x \in \mathbb{F}_5$, and compare them with the squares $\mod 5$, which are $0, 1$ and 4. We obtain the following:

x	$x^3 + x + 3$	y	(x, y)
0	3	no solutions	no solutions
1	0	0	$(1, 0)$
2	3	no solutions	no solutions
3	3	no solutions	no solutions
4	1	$\pm 1 = (1, 4)$	$(4, 1), (4, 4)$
O	O	O	O

From the table we conclude that, $|E(\mathbb{F}_5)| = 4$. By Corollary 2.1.6, we know that the order of an element divides the order of the group. Hence, the four points on $E(\mathbb{F}_5)$ can have order $1, 2$ or 4. The point at infinity, O, is the only element of order 1, as it's the identity element. Hence, the remaining three points can have order 2 or 4. It suffices to calculate $2P$ for each point $P \in E(\mathbb{F}_5)$ to determine its order, $|P|$: if we obtain O, the identity element, the respective point has order 2. If we obtain any other point on the curve, then the respective point

has order 4. Therefore, using Case 3 in Section 3.2, we obtain:

$$2(1,0) = O, \quad 2(4,1) = (1,0) \quad \text{and} \quad 2(4,4) = (1,0).$$

We conclude that $E[2] = \{(1,0)\}$. Furthermore, we can also deduce that $E[4] = \{(4,1),(4,4)\}$.

Remark 2: The central property of the multiplication-by-m map is that it has degree m^2, from which we can deduce the structure of the finite group $E[m]$.

4 Elliptic Curves Over Finite Fields

The focus of this section is to study elliptic curves defined over a finite field $\mathbb{F}_q$, where q is a prime power. As $\mathbb{F}_q$ is finite, there are only finitely many pairs of points (x,y) with $x,y \in \mathbb{F}_q$. Hence, the group $E(\mathbb{F}_q)$ is finite. The various properties of $E(\mathbb{F}_q)$ are the foundation of the cryptographic applications discussed in the next section.

4.1 Hasse's Theorem

We begin by stating the main result of this section, *Hasse's Theorem*, Theorem 4.2 of [8]. We then examine various results that play a key role in its proof.

Theorem 4.1.1 (Hasse's Theorem): Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. The order of $E(\mathbb{F}_q)$, $\#E(\mathbb{F}_q)$, satisfies

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

Example: Before we prove Hasse's Theorem, we illustrate how it works. Define $E(\mathbb{F}_7) = \{(x,y) \in \mathbb{F}_7 \times \mathbb{F}_7 : y^2 = x^3 + 3x + 1\} \cup \{O\}$. We want to find $\#E(\mathbb{F}_7)$.

As we are working with a small finite field, we can use the same method as in the previous example. We start by listing all the solutions to $x^3 + 3x + 1 \pmod 7$ for $x \in \mathbb{F}_7$, and compare them with the squares (mod 7), which are $0, 1, 2, 4$. We obtain the following result:

x	x^3+3x+1	y	(x,y)
0	1	$\pm 1 = \{1,6\}$	$(0,1),(0,6)$
1	5	no solutions	no solutions
2	1	$\pm 1 = \{1,6\}$	$(2,1),(2,6)$
3	2	$\pm 3 = \{3,4\}$	$(3,3),(3,4)$
4	0	0	$(4,0)$
5	1	$\pm 1 = \{1,6\}$	$(5,1),(5,6)$
6	4	$\pm 2 = \{2,5\}$	$(6,2),(6,5)$
O	O	O	O

Using the table, we count that $\#E(\mathbb{F}_7) = 12$, and we obtain:

$$|7+1-\#E(\mathbb{F}_7)| = |8-12| = |-4| = 4 \quad \text{and} \quad 2\sqrt{7} \approx 5.3.$$

As $4 \leq 5.3$, it's evident that the result holds.

Proof of Hasse's Theorem:
Using Proposition 3.5.8 (2), let

$$a = q+1-\#E(\mathbb{F}_q) = q+1-\deg(\phi_q - 1). \tag{5}$$

We want to prove that $|a| \leq 2\sqrt{q}$. We require the following:

Lemma 4.1.2: Let r, s be integers such that $\gcd(s,q) = 1$. Then

$$\deg(r\phi_q - s) = r^2 q + s^2 - rsa.$$

Proof: We need the following result:

$$\deg(a\alpha + b\beta) = a^2 \deg\alpha + b^2 \deg\beta + ab(\deg(\alpha+\beta) - \deg\alpha - \deg\beta)$$

(for a proof, the reader is directed to Proposition 3.16 of [8]).

Substituting r, ϕ_q, s and -1 for a, α, b and β respectively, we obtain:

$$\deg(r\phi_q - s) = r^2 \deg(\phi_q) + s^2 \deg(-1) + rs(\deg(\phi_q - 1) - \deg(\phi_q) - \deg(-1)).$$

As $\deg(\phi_q) = q$ and $\deg(-1) = 1$, the result follows from (5).

We can now finish the proof of Hasse's Theorem. As $\deg(r\phi_q - s) \geq 0$, Lemma 4.1.2 implies that

$$q\left(\frac{r}{s}\right)^2 - a\left(\frac{r}{s}\right) + 1 \geq 0$$

for all r, s such that $\gcd(s,q) = 1$.

Claim: The set of rational numbers $\frac{r}{s}$ such that $\gcd(s,q) = 1$ is dense in $\mathbb{R}$.
Proof: Take s to be a power of 2 or a power of 3, one of which must be relatively

prime with q. It's easy to see that the rationals of the form $\frac{r}{2^m}$ and of the form $\frac{r}{3^m}$ are dense in $\mathbb{R}$. Therefore,

$$qx^2 - ax + 1 \geq 0,$$

for all $x \in \mathbb{R}$. Hence, the discriminant of the polynomial is negative or zero. This implies that $a^2 - 4q \leq 0$, and hence that $|a| \leq 2\sqrt{q}$. The proof of Hasse's Theorem is now complete.

While Hasse's Theorem gives us both an upper and a lower bound for the number of points on an elliptic curve over a finite field $\mathbb{F}_q$, we now explore a method which allows us to calculate the exact order, $\#E(\mathbb{F}_q)$, for a small finite field $\mathbb{F}_q$, [8, Section 4.3.1]. As we have seen in previous examples, we determine the number of points on $E(\mathbb{F}_q)$ by enumerating the points. Unexpectedly, this can be used to calculate the number of points on $E(\mathbb{F}_{q^n})$ for all n.

Theorem 4.1.3: Let $\#E(\mathbb{F}_q) = q + 1 - a$. Write $x^2 - ax + q = (x - \alpha)(x - \beta)$. Then, for all $n \geq 1$,

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n).$$

Lemma 4.1.4: Let $s_n = \alpha^n + \beta^n$. Then, $s_0 = 2$, $s_1 = a$, and $s_{n+1} = as_n - qs_{n-1}$, for all $n \geq 1$.

Proof: To obtain this result, we multiply $\alpha^2 - a\alpha + q = 0$ by α^{n-1}, and we obtain $\alpha^{n+1} = a\alpha^n - q\alpha^{n-1}$. Similarly for β, and by adding the two relations we are done.

Proof of Theorem 4.1.3: As the finite fields used in cryptography are extremely large, these results, while interesting, and needed for Section 4.3, are not applicable to cryptography. Therefore, we give an overview of the proof and direct the interested reader to [8, Section 4.3.1] for a detailed account. From Lemma 4.1.4, it follows that $\alpha^n + \beta^n$ is an integer for all $n \geq 0$. Then, letting

$$f(x) = (x^n - \alpha^n)(x^n - \beta^n) = x^{2n} - (\alpha^n + \beta^n)x^n + q^n,$$

we note that $(x - \alpha)(x - \beta)|f(x)$ (this is because for all $n \geq 1$, $r^n - t^n = (r - t)B(r, t)$, where $B(r, t)$ is a polynomial in terms of r and t). From the standard algorithm for dividing polynomials we infer that the quotient is a polynomial, $Q(x)$, with integer coefficients. Hence, we obtain an endomorphism of E,

$$(\phi_q^n)^2 - (\alpha^n + \beta^n)\phi_q^n + q^n = f(\phi_q) = Q(\phi_q)(\phi_q^2 - a\phi_q + q) = 0.$$

Then, as $\phi_q^n = \phi_{q^n}$ and since it can be shown (Theorem 4.10 of [8, Section 4.3]) that there exists a unique $k \in \mathbb{Z}$ such that $\phi_{q^n}^2 - k\phi_{q^n} + q^n = 0$, and that such a k is determined by $k = q^n + 1 - \#E(\mathbb{F}_{q^n})$, we obtain that $\alpha^n + \beta^n = q^n + 1 - \#E(\mathbb{F}_{q^n})$, and we are done.

4.2 The Weil Conjectures

These are a series of conjectures made by André Weil, [7, Section 5.2], about the number of points on varieties defined over finite fields. In this subsection we state the Weil conjectures and show that they hold for elliptic curves.

For all integers $n \geq 1$, let $\mathbb{F}_{q^n}$ be the extension of $\mathbb{F}_q$ of degree n. Hence, $\#\mathbb{F}_{q^n} = q^n$. Let $V/\mathbb{F}_q$ be a projective variety, say V is the set of solutions to

$$f_1(x_0, \ldots, x_N) = \cdots = f_m(x_0, \ldots, x_N) = 0,$$

where $f_1, \ldots, f_m$ are homogeneous polynomials with coefficients in $\mathbb{F}_q$. Hence, $V(\mathbb{F}_{q^n})$ is the set of points of V with coordinates in $\mathbb{F}_{q^n}$. We now encode the number of points in $V(\mathbb{F}_{q^n})$ for all $n \geq 1$ into a generating function.

Definition 4.2.1: The *zeta function* of $V/\mathbb{F}_q$ is the power series

$$Z(V/\mathbb{F}_q; T) = \exp\left(\sum_{n=1}^{\infty} \left(\#V(\mathbb{F}_{q^n})\right) \frac{T^n}{n}\right).$$

For any power series $F(T) \in \mathbb{Q}[[T]]$ with no constant term, we define the power series $\exp(F(T))$ to be the series $\sum_{k\geq 0} \frac{F(T)^k}{k!}$.

Example: We illustrate how the definition works. Let $V = \mathbb{P}^1 = \mathbb{H}^1 \cup \{\infty\}$, where $\mathbb{H}^1 = \mathbb{F}_p$. We know that $\#V(\mathbb{F}_p) = p+1$ and $\#V(\mathbb{F}_{p^n}) = p^n + 1$. Hence, we obtain:

$$\begin{aligned} Z(V/\mathbb{F}_p; T) &= \exp\left(\sum_{n=1}^{\infty} \frac{\#V(\mathbb{F}_{p^n})}{n} T^n\right) \\ &= \exp\left(\sum_{n=1}^{\infty} \frac{p^n + 1}{n} T^n\right) \\ &= \exp\left(\sum_{n=1}^{\infty} \frac{p^n}{n} T^n + \sum_{n=1}^{\infty} \frac{1}{n} T^n\right) \\ &= \exp\left(\sum_{n=1}^{\infty} \frac{p^n}{n} T^n\right) \exp\left(\sum_{n=1}^{\infty} \frac{1}{n} T^n\right) \end{aligned}$$

Note that

$$\log(1 - T) = -T - \frac{T^2}{2} - \frac{T^3}{3} - \cdots.$$

Hence, we can easily see that

$$\sum_{n=1}^{\infty} \frac{1}{n} T^n = -\log(1 - T).$$

Similarly, by noting that $\frac{p^n}{n}T^n = \frac{1}{n}(pT)^n$, we obtain that

$$\sum_{n=1}^{\infty} \frac{p^n}{n} T^n = -\log(1-pT).$$

Therefore, putting everything together we obtain:

$$\begin{aligned} Z(V/\mathbb{F}_p;T) &= \exp(-\log(1-pT))\exp(-\log(1-T)) \\ &= \exp\left(\log\left(\frac{1}{1-pT}\right)\right)\exp\left(\log\left(\frac{1}{1-T}\right)\right) \\ &= \frac{1}{(1-pT)(1-T)}, \end{aligned}$$

and we are done.

Theorem 4.2.2 (Weil Conjectures): Let $V/\mathbb{F}_q$ be a smooth projective variety of dimension N.

1. *Rationality*:
$$Z(V/\mathbb{F}_q;T) \in \mathbb{Q}(T).$$

2. *Functional Equation* :
There is an integer ϵ, called the *Euler characteristic of* V, such that
$$Z(V/\mathbb{F}_q;\frac{1}{q^N}T) = \pm q^{\frac{N\epsilon}{2}} T^{\epsilon} Z(V/\mathbb{F}_q;T).$$

3. *Riemann Hypothesis*:
The zeta function factors as
$$Z(V/\mathbb{F}_q;T) = \frac{P_1(T)\cdots P_{2N-1}(T)}{P_0(T)P_2(T)\cdots P_{2N}(T)}$$
with each $P_i(T) \in \mathbb{Z}[T]$, with
$$P_0(T) = 1-T \quad \text{and} \quad P_{2N}(T) = 1-q^N T,$$
and such that for every $0 \leq i \leq 2N$, the polynomial $P_i(T)$ factors over $\mathbb{C}$ as
$$P_i(T) = \prod_{j=1}^{b_i}(1-\alpha_{ij}T) \quad \text{with} \quad |\alpha_{ij}| = q^{\frac{i}{2}}.$$
The quantity b_i, in other words the degree of $P_i(T)$, is called the ith Betti number of V.

We will prove the Weil conjectures for elliptic curves. We begin by introducing some general results that will aid us in the proof.

Definition 4.2.3: Let E be an elliptic curve and let $l \in \mathbb{Z}$ be a prime, different from $p = \text{char}(\mathbb{F}_q)$. The *($l$-adic) Tate module of E* is the group

$$T_l(E) = \lim_{\leftarrow n} E[l^n],$$

where $E[l^n]$ is the l^n-torsion subgroup of E, and the inverse limit is being taken with respect to the natural map

$$[l] : E[l^{n+1}] \to E[l^n].$$

This map takes points in the subgroup $E[l^{n+1}]$ and maps them to their corresponding points in $E[l^n]$ by scalar multiplication by l.

The following result is key to proving the Weil conjectures for elliptic curves: "Let $\phi : E_1 \to E_2$ be an isogeny. Then ϕ induces maps $\phi : E_1[l^n] \to E_2[l^n]$, and $\phi_l : T_l(E_1) \to T_l(E_2)$. Hence, the following natural homomorphism is obtained: $\text{Hom}(E_1, E_2) \to \text{Hom}(T_l(E_1), T_l(E_2))$. Moreover, if $E_1 = E_2 = E$, then the map

$$\text{End}(E) \to \text{End}(T_l(E)), \quad \psi \to \psi_l,$$

is a homomorphism of rings. We can also write ψ_l as a 2×2 matrix and compute its determinant and trace, $\det(\psi_l)$ and $\text{tr}(\psi_l)$". For a more detailed discussion of this result, see [7, Section 3.7 and Section 5.2].

Proposition 4.2.4: Let $\psi \in \text{End}(E)$. Then

$$\det(\psi_l) = \deg(\psi) \quad \text{and} \quad \text{tr}(\psi_l) = 1 + \deg(\psi) - \deg(1 - \psi).$$

More specifically, $\det(\psi_l)$ and $\text{tr}(\psi_l)$ are in $\mathbb{Z}$ and are independent of l.

Proof: While the proof is omitted as it's beyond the scope of this project, the interested reader is directed to [7, Section 3.8].

We apply this result to an elliptic curve over a finite field. This allows us to compute the number of points and to infer a fundamental property of the Frobenius endomorphism.

Theorem 4.2.5: Let $E(\mathbb{F}_q)$ be an elliptic curve over a finite field $\mathbb{F}_q$, and let ϕ_q be the qth-power Frobenius endomorphism. As before, let $a = q + 1 - \#E(\mathbb{F}_q)$. Let $\alpha, \beta \in \mathbb{C}$ be the roots of the polynomial $T^2 - aT + q$. Then, α, β are complex conjugates satisfying $|\alpha| = |\beta| = \sqrt{q}$, and for every $n \geq 1$,

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n.$$

Proof: The results in Section 3.5 imply that $\#E(\mathbb{F}_q) = \deg(1-\phi)$. We use Proposition 4.2.4 to compute:

$$\begin{aligned}\det(\phi_l) &= \deg(\phi) = q,\\ tr(\phi_l) &= 1 + \deg(\phi) - \deg(1-\phi) = 1 + q - \#E(\mathbb{F}_q) = a.\end{aligned}$$

Therefore, the characteristic polynomial of ϕ_l is

$$\det(T - \phi_l) = T^2 - \mathrm{tr}(\phi_l)T + \det(\phi_l) = T^2 - aT + q.$$

Note that the characteristic polynomial of ϕ_l has integer coefficients (since $a, q \in \mathbb{Z}$), so we can factor over $\mathbb{C}$ as

$$\det(T - \phi_l) = T^2 - aT + q = (T-\alpha)(T-\beta).$$

For every rational number $\frac{m}{n} \in \mathbb{Q}$, we obtain:

$$\det\left(\frac{m}{n} - \phi_l\right) = \frac{\det(m - n\phi_l)}{n^2} = \frac{\deg(m - n\phi_l)}{n^2} \geq 0.$$

Therefore, the quadratic polynomial $\det(T - \phi_l) = T^2 - aT + q \in \mathbb{Z}[T]$ is nonnegative for all $T \in \mathbb{R}$. Hence, it either has a double root or complex conjugate roots. In both cases, however, we obtain that $|\alpha| = |\beta|$, and from

$$\alpha\beta = \det \phi_l = \deg \phi = q$$

we infer that

$$|\alpha| = |\beta| = \sqrt{q},$$

finishing the first part.

Similarly, the (q^n)th-power Frobenius endomorphism, satisfies

$$\#E(\mathbb{F}_{q^n}) = \deg(1 - \phi^n),$$

for all integers $n \geq 1$. Hence, the characteristic polynomial of ϕ_l^n is given by

$$\det(T - \phi_l^n) = (T - \alpha^n)(T - \beta^n).$$

More specifically,

$$\begin{aligned}\#E(\mathbb{F}_{q^n}) &= \deg(1-\phi^n)\\ &= \det(1-\phi_l^n), \quad \text{Proposition 4.2.4}\\ &= 1 - \alpha^n - \beta^n + q^n.\end{aligned}$$

Using this result, it's now straightforward to verify that the Weil conjectures hold for elliptic curves.

Theorem 4.2.6: Let $E(\mathbb{F}_q)$ be an elliptic curve over a finite field $\mathbb{F}_q$. Then, there exists $a \in \mathbb{Z}$ such that

$$Z(E/\mathbb{F}_q; T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}.$$

Moreover,

$$Z(E/\mathbb{F}_q; 1/qT) = Z(E/\mathbb{F}_q; T),$$

and

$$1 - aT + qT^2 = (1 - \alpha T)(1 - \beta T) \quad \text{with} \quad |\alpha| = |\beta| = \sqrt{q}.$$

Proof: Using Definition 4.2.1, we have:

$$\log Z(E/\mathbb{F}_q; T) = \sum_{n=1}^{\infty} \frac{\#E(\mathbb{F}_{q^n})}{n} T^n.$$

Applying the result of Theorem 4.2.5, we obtain:

$$\log Z(E/\mathbb{F}_q; T) = \sum_{n=1}^{\infty} \frac{(1 - \alpha^n - \beta^n + q^n)T^n}{n}.$$

As before, using the power series definition of the log function, we obtain:

$$\log Z(E/\mathbb{F}_q; T) = -\log(1 - T) + \log(1 - \alpha T) + \log(1 - \beta T) - \log(1 - qT).$$

Hence,

$$\log Z(E/\mathbb{F}_q; T) = \log\left(\frac{(1 - \alpha T)(1 - \beta T)}{(1 - T)(1 - qT)}\right).$$

Therefore, we conclude:

$$Z(E/\mathbb{F}_q; T) = \frac{(1 - \alpha T)(1 - \beta T)}{(1 - T)(1 - qT)}.$$

This is the desired result, as Theorem 4.2.5 states that α and β are complex conjugates of absolute value $\sqrt{q}$ and that they satisfy

$$a = \alpha + \beta = \mathrm{tr}(\phi_l) = 1 + q - \deg(1 - \phi) \in \mathbb{Z}.$$

The equation is now immediate, with $\epsilon = 0$.

4.3 Supersingular Curves

Let E be an elliptic curve over $\mathbb{F}_q$, where q is a prime power, $q = p^n$, and $n \in \mathbb{Z}$ (it's clear that $\mathbb{F}_q$ is a field of characteristic p). We call E *supersingular* if $E[p] = \{O\}$. Equivalently, we say that there are no points of order p, not even with coordinates in $\overline{\mathbb{F}}_q$. Therefore, it's a property of an elliptic curve over an algebraically closed field.

We begin with a useful result, Proposition 4.31 of [8], which gives a straightforward method for determining whether an elliptic curve over a finite field is supersingular:

Proposition 4.3.1: Let E be an elliptic curve over $\mathbb{F}_q$, as above. Let $a = q + 1 - \#E(\mathbb{F}_q)$. Then, E is supersingular if and only if $a \equiv 0 \pmod{p}$, which is if and only if $\#E(\mathbb{F}_q) \equiv 1 \pmod{p}$.

Proof: Take $x^2 - ax + q = (x - \alpha)(x - \beta)$. By Theorem 4.1.3, we know that $\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$, and by Lemma 4.1.4, we know that $s_n = \alpha^n + \beta^n$ satisfies the following recurrence relation: $s_0 = 2, s_1 = a$ and $s_{n+1} = as_n - qs_{n-1}$.

Case 1: Assume that $a \equiv 0 \pmod{p}$. Then, $s_1 = a \equiv 0 \pmod{p}$, and $s_{n+1} \equiv 0 \pmod{p}$ also, since, by assumption, $p|q$. By recurrence, this holds for all $n \geq 1$. Hence,

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - s_n \equiv 1 \pmod{p}.$$

Moreover, we infer that for all $n \geq 1$, there are no point of order p in $E(\mathbb{F}_{q^n})$ (recall that by Corollary 2.1.6, the order of an element divides the order of the group; hence, the order of any point $P \in E(\mathbb{F}_{q^n})$, divides $\#E(\mathbb{F}_{q^n}) = kp + 1$, and it's evident that $p \nmid kp + 1$). By Definition 2.2.3, $\overline{\mathbb{F}}_q = \bigcup_{n \geq 1} \mathbb{F}_{q^n}$. Putting everything together, we conclude there are no points of order p in $\overline{\mathbb{F}}_q$, and hence, by definition, E is supersingular.

Case 2: Assume that $a \not\equiv 0 \pmod{p}$. From the recurrence relation, we infer that $s_{n+1} \equiv as_n \pmod{p}$ for all $n \geq 1$, as again, by assumption, $p|q$. Moreover, since $s_1 = a$, then $s_n \equiv a^n \pmod{p}$, for all $n \geq 1$. Hence,

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - s_n \equiv 1 - a^n \pmod{p}.$$

By Theorem 2.1.4, $a^{p-1} \equiv 1 \pmod{p}$. Hence, $\#E(\mathbb{F}_{q^{p-1}}) \equiv 1 - a^{p-1} \equiv 0 \pmod{p}$, or in other words, the order of $E(\mathbb{F}_{q^{p-1}})$ is divisible by p. Cauchy's Theorem for abelian groups states that for a prime p' and G a finite abelian group such that p' divides the order of G, then G contains an element of order p' (a proof of this result can be found in [3, Section 2.2]). In Section 3.2 and in the introduction of Section 4, we have established that $E(\mathbb{F}_{q^{p-1}})$ is a finite abelian group. Therefore, we conclude that $E(\mathbb{F}_{q^{p-1}})$ contains a point of order p, making E not supersingular.

Lastly, remark that

$$\#E(\mathbb{F}_q) \equiv q + 1 - a \equiv 1 - a \pmod{p},$$

(again, since by assumption, $p|q$), and hence, $a \equiv 0 \pmod{p} \Leftrightarrow \#E(\mathbb{F}_q) \equiv 1 \pmod{p}$, finishing the proof.

Example 1: In the Example provided in Section 4.1, we computed $\#E(\mathbb{F}_7) = 12$, where $E(\mathbb{F}_7) = \{(x, y) \in \mathbb{F}_7 \times \mathbb{F}_7 : y^2 = x^3 + 3x + 1\} \cup \{O\}$. Hence, we obtain that $a = 7 + 1 - 12 = -4$. But $-4 \equiv 3 \not\equiv 0 \pmod{7}$. Therefore, $E(\mathbb{F}_7)$ is not supersingular.

On the other hand, take the following curve, $E(\mathbb{F}_{25}) = \{(x, y) \in \mathbb{F}_{25} \times \mathbb{F}_{25} : y^2 = x^3 + 3x + 7\} \cup \{O\}$ (note that $25 = 5^2$, where 5 is prime). A computationally laborious process shows that $\#E(\mathbb{F}_{25}) = 21$ (we omit the process as it's identical to the method previously illustrated in the two examples provided in Section 4.1 and Section 3.6). Then, we compute $a = 25 + 1 - 21 = 5$. Since $5 \equiv 0 \pmod 5$, we conclude that $E(\mathbb{F}_{25})$ is supersingular. Note also that $\#E(\mathbb{F}_{25}) = 21 \equiv 1 \pmod 5$, since $21 = 5 \times 4 + 1$.

As it's evident from the above example, the first criterion is computationally inefficient, as one would have to calculate the number of points, $\#E(\mathbb{F}_q)$, on the elliptic curve $E(\mathbb{F}_q)$. Although Hasse's Theorem, Theorem 4.1.1, provides an upper and a lower bound for this value, when working with very large primes or very large prime powers, we still have a vast amount of possibilities to consider. Therefore, the following result, Theorem 4.1 of [7, Section 5.4], gives an alternative criteria for establishing whether an elliptic curve is supersingular, for $p > 2$.

Theorem 4.3.2: Let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 3$.
(a) Let $E(\mathbb{F}_q)$ be an elliptic curve given by a Weierstrass equation

$$E : y^2 = f(x),$$

where $f(x) \in \mathbb{F}_q[x]$ is a cubic polynomial with distinct roots in $\overline{\mathbb{F}}_q$. Then E is supersingular if and only if the coefficient of x^{p-1} in $f(x)^{p-1/2}$ is zero.

(b) Let $m = \frac{(p-1)}{2}$, and define a polynomial

$$H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i.$$

Let $\lambda \in \overline{\mathbb{F}}_q$ with $\lambda \neq 0, 1$. Then the elliptic curve

$$E : y^2 = x(x-1)(x-\lambda)$$

is supersingular if and only if $H_p(\lambda) = 0$.

Proof: Let

$$\chi : \mathbb{F}_q^* \to \{\pm 1\}$$

be the unique nontrivial character of order 2, and extend χ to $\mathbb{F}_q$ by setting $\chi(0) = 0$. Note that we can use the character χ to count the number of points on E, where $E : y^2 = f(x)$. As $0 \notin \mathbb{F}_q^*$, we have two cases:

Case 1: The equation has a solution, or, in other words, $f(x)$ is a square in $\mathbb{F}_q$. Therefore, for the respective $x \in \mathbb{F}_q$, we obtain two points on $E(\mathbb{F}_q)$, $(x, y = \sqrt{f(x)})$ and $(x, y = -\sqrt{f(x)})$. Moreover, by the definition of the character function, we have $\chi(f(x)) = 1$.

Case 2: The equation has no solutions, or, in other words, $f(x)$ is not a square in $\mathbb{F}_q$. Therefore, for this particular value of $x \in \mathbb{F}_q$, there are no points lying on $E(\mathbb{F}_q)$. Again, by the definition of the character function, we obtain that $\chi(f(x)) = -1$.

Note that in both cases, for each $x \in \mathbb{F}_q$, we can determine the number of points it generates on $E(\mathbb{F}_q)$ by adding 1 to the value of $\chi(f(x))$. Remembering the point at infinity, we can calculate the total number of points on $E(\mathbb{F}_q)$ as follows:

$$\#E(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q} 1 + \chi\left(f(x)\right)$$

Lastly, since $\mathbb{F}_q$ has q elements, we obtain:

$$\#E(\mathbb{F}_q) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi\left(f(x)\right).$$

By Theorem 2.1.7, $\mathbb{F}_q^*$ is cyclic of order $q-1$. Appealing to the Legendre symbol, Definition 2.1.9, we have that for any $z \in \mathbb{F}_q$, $\chi(z) = z^{(q-1)/2}$ in $\mathbb{F}_q$. Hence, we can rewrite our result as:

$$\#E(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q} f(x)^{(q-1)/2} \quad \text{as an equality in } \mathbb{F}_q,$$

where $q \equiv 0 \pmod{q}$.
Due to the cyclic nature of $\mathbb{F}_q^*$, we have:

$$\sum_{x \in \mathbb{F}_q} x^i = \begin{cases} -1 & \text{if} \quad q-1 | i \\ 0 & \text{if} \quad q-1 \nmid i. \end{cases}$$

Note that by Theorem 2.1.8, for all $x \in \mathbb{F}_q^*$, $x^{q-1} = 1$ in $\mathbb{F}_q$.
Case 1: Let $i = r(q-1)$. We know that there are $q-1$ elements in $\mathbb{F}_q$, excluding 0, and further that 0 to any power is 0. Hence, we obtain

$$\sum_{x \in \mathbb{F}_q} x^i = \sum_{x \in \mathbb{F}_q} (x^{q-1})^r = 0 + \underbrace{1 + 1 + \cdots + 1}_{q-1 \text{ times}} = q - 1 = -1 \quad \text{in } \mathbb{F}_q.$$

Case 2: $q - 1 \nmid i$. Let g be a generator. As $\mathbb{F}_q^*$ is a cyclic group of order $q-1$, then every nonzero element of $\mathbb{F}_q$ can be expressed as g^j, where $0 \leq j \leq q-2$. Hence,

$$\sum_{x \in \mathbb{F}_q} x^i = 0 + \sum_{x \in \mathbb{F}_q^*} x^i = \sum_{j=0}^{q-2} (g^j)^i = \sum_{j=0}^{q-2} (g^i)^j = 1 + (g^i) + \cdots + (g^i)^{q-2}.$$

Note that this is a geometric series, and can therefore be rewritten as:

$$1 + (g^i) + \cdots + (g^i)^{q-2} = \frac{(g^i)^{q-1} - 1}{g^i - 1} = \frac{(g^{q-1})^i - 1}{g^i - 1} = 0 \quad \text{in } \mathbb{F}_q,$$

since by Theorem 2.1.8 , $g^{q-1} = 1$ in $\mathbb{F}_q$.

Now, since $f(x)$ is a polynomial of degree 3, if we expand $f(x)^{(q-1)/2}$, we notice that the expansion has terms of the form x^n for $0 \leq n \leq \frac{3}{2}(q-1)$. Note that $q-1$ the unique element in the specified interval such that $q-1|q-1$. Therefore, from the above fact, when we sum over $x \in \mathbb{F}_q$, the only nonzero element comes from x^{q-1}. Let

$$A_q = \text{coefficient of } x^{q-1} \text{ in } f(x)^{(q-1)/2}.$$

Then,

$$\#E(\mathbb{F}_q) = 1 - A_q.$$

Remark: This result only holds in $\mathbb{F}_q$, so it's in fact only a formula for the number of points on $E(\mathbb{F}_q)$ modulo p, the characteristic of the field $\mathbb{F}_q$.

Conversely, let $\phi : E \to E$ be the qth-power Frobenius endomorphism. Using the same results as in the previous section, Section 4.2, and (5) from Section 4.1, we have:

$$\#E(\mathbb{F}_q) = \deg(1 - \phi) = 1 - a + q,$$

where $a = 1 - \deg(1 - \phi) + \deg(\phi)$. Equating our two results for $\#E(\mathbb{F}_q)$, we obtain that $1 - A_q = 1 - a + q$, which can be simplified as:

$$a = A_q \quad \text{in } \mathbb{F}_q.$$

As a is an integer, this shows that

$$A_q = 0 \Leftrightarrow a \equiv 0 \pmod{p}.$$

From Proposition 4.3.1, we also know that $a \equiv 0 \pmod{p} \Leftrightarrow E$ is supersingular. This shows that

$$A_q = 0 \Leftrightarrow E \quad \text{is supersingular.}$$

All we have left to prove now is that $A_q = 0$ if and only if $A_p = 0$. Writing

$$f(x)^{(p^{r+1}-1)/2} = f(x)^{(p^r-1)/2}(f(x)^{(p-1)/2})^{p^r}$$

and equating coefficients, keeping in mind that f is a cubic, we obtain

$$A_{p^{r+1}} = A_{p^r} A_p^{p^r}.$$

A simple induction on r gives the desired result.

(b) This is a special case of (a). We need the coefficient of x^{p-1} in the expression $(x(x-1)(x-\lambda))^m$. In other words, we need the coefficient of x^m in $(x-1)^m(x-\lambda)^m$, which is

$$\sum_{i=0}^{m} \binom{m}{i} (-\lambda)^i \binom{m}{m-i} (-1)^{m-i}.$$

This only differs from $H_p(\lambda)$ by a factor of $(-1)^m$, and we are done.

Example 2: We illustrate how to apply (a) to determine whether an elliptic curve is supersingular. Define $E(\mathbb{F}_{11}) = \{(x, y) \in \mathbb{F}_{11} \times \mathbb{F}_{11} : y^2 = x^3 + 3x + 3\} \cup \{O\}$. We want to find the coefficient of x^{10} in $(x^3 + 3x + 3)^5$. Expanding and opening up the brackets, we obtain:

$$(x^3 + 3x + 3)^5 = x^{15} + 15x^{13} + \cdots 180x^{10} + \cdots .$$

This shows that $E(\mathbb{F}_{11})$ is not supersingular, as the coefficient of x^{10} is $180 \neq 0$ in $\mathbb{F}_{11}$.

The following result, Proposition 4.37 of [8], gives a criterion for determining whether an elliptic curve is supersingular over $\mathbb{F}_p$, for specific classes of elliptic curves:

Proposition 4.3.3: Let $p \geq 5$ be prime. Then, the elliptic curve $y^2 = x^3 + 1$ over $\mathbb{F}_p$ is supersingular if and only if $p \equiv 2 \pmod 3$, and the elliptic curve $y^2 = x^3 + x$ over $\mathbb{F}_p$ is supersingular if and only if $p \equiv 3 \pmod 4$.

Proof: By Theorem 4.3.2 (a), we are looking for the coefficient of x^{p-1} in $(x^3 + 1)^{(p-1)/2}$ to be zero. Note that as p is prime and $p \geq 5$, $p \not\equiv 0 \pmod 3$. Hence, we have two cases to explore:

Case 1: $p \equiv 2 \pmod 3$. It follows that $p - 1 \equiv 1 \pmod 3$, and as p is odd, $(p-1)/2$ is an integer. The binomial expansion contains terms of the form x^{3k}, for $k = 0, 1, 2, \cdots, \frac{p-1}{2}$. But since $3 \not| p - 1$ (as $p - 1 \equiv 1 \pmod 3$), none of the exponents $3k$ will equal $p - 1$, so there will be no term x^{p-1} in the expansion, or in other words, the coefficient of x^{p-1} is zero, finishing the first case.

Case 2: $p \equiv 1 \pmod 3$. It follows that $p - 1 \equiv 0 \pmod 3$, so, from *Case 1*, we deduce that there is a term x^{p-1} in the expansion. Its binomial coefficient is $\binom{(p-1)/2}{(p-1)/3}$. As it contains no factors p, $\binom{(p-1)/2}{(p-1)/3} \not\equiv 0 \pmod p$, or, in other words, it's not zero.
This proves the first part.

Similarly, we are looking for the coefficient of x^{p-1} in $(x^3 + x)^{(p-1)/2}$ to be zero. Note that this is equivalent to the coefficient of $x^{(p-1)/2}$ in $(x^2 + 1)^{(p-1)/2}$ (this is because $(x^3 + x)^{(p-1)/2} = (x(x^2 + 1))^{(p-1)/2} = x^{(p-1)/2}(x^2 + 1)^{(p-1)/2} = x^{(p-1)/2}(x^{(p-1)} + \cdots Ax^{(p-1)/2} + \cdots + 1) = x^{3(p-1)/2} + \cdots + Ax^{(p-1)} + \cdots + 1)$. The binomial expansion contains terms of the form x^{2k}, where $k = 0, 1, \cdots, \frac{p-1}{2}$. Hence, all the exponents are even. When $p \equiv 3 \pmod 4$, $\frac{p-1}{2}$ is odd, so $x^{(p-1)/2}$ doesn't appear, or in other words, it has coefficient zero. On the other hand, when $p \equiv 1 \pmod 4$, $\frac{p-1}{2}$ is even, and the coefficient of $x^{(p-1)/2}$ is $\binom{(p-1)/2}{(p-1)/4}$. Again, as it contains no factors p, $\binom{(p-1)/2}{(p-1)/4} \not\equiv 0 \pmod p$, or in other words, the coefficient of $x^{(p-1)/2}$ is not zero. As p is prime and $p \geq 5$, $p \not\equiv 0, 2 \pmod 4$. This proves the second part of the result.

We now fix p and aim to determine the number of supersingular elliptic curves

over $\overline{\mathbb{F}}_p$. As seen in [8, Section 4.6], this boils down to counting the distinct zeros of $H_p(T)$. Note that the values $\lambda = 0, 1$ cannot be used in the Legendre form of an elliptic curve. Furthermore, they are also not zeros of $H_p(t)$. One can see that $H_p(0) = 1$. For, $H_p(1)$, note that the coefficient of $x^{(p-1)/2}$ in

$$(x+1)^{p-1} = (x+1)^{(p-1)/2}(x+1)^{(p-1)/2}$$

is

$$\binom{p-1}{(p-1)/2} = \sum_k \binom{(p-1)/2}{k}\binom{(p-1)/2}{(p-1)/2-k} = H_p(1),$$

by using the identity $\binom{n}{k} = \binom{n}{n-k}$. As $\binom{p-1}{(p-1)/2}$ contains no factors p, it's nonzero mod p. Hence, $H_p(1) \neq 0$.

Proposition 4.3.4: $H_p(t)$ has $(p-1)/2$ distinct roots in $\overline{\mathbb{F}}_p$.

Proof: We claim that

$$4t(1-t)H_p^{''}(t) + 4(1-2t)H_p'(t) - H_p(t) \equiv 0 \pmod{p}. \tag{6}$$

Write $H_p(t) = \sum_k b_k t^k$. The coefficient of t^k on the left hand side of (6) is

$$4(k+1)kb_{k+1} - 4k(k-1)b_k + 4(k+1)b_{k+1} - 8kb_k - b_k = 4(k+1)^2 b_{k+1} - (2k+1)^2 b_k.$$

From Theorem 4.3.2 (b) we know that

$$\begin{aligned} b_{k+1} &= \binom{(p-1)/2}{k+1}^2 \\ &= \left(\frac{((p-1)/2)!}{(k+1)!(((p-1)/2)-k-1)!}\right)^2. \end{aligned}$$

Simplifying the denominator we obtain:

$$(k+1)!(((p-1)/2)-k-1)! = \frac{(k+1)!((p-1)/2)!}{(((p-1)/2)-(k+1))!}.$$

This leads to

$$\begin{aligned} b_{k+1} &= \left(\frac{((p-1)/2)!(((p-1)/2)-(k+1))!}{(k+1)!((p-1)/2)!}\right)^2 \\ &= \left(\frac{((p-1)/2)-k}{k+1}\right)^2 b_k, \end{aligned}$$

where $b_k = \binom{(p-1)/2}{k}$. We find that the coefficient of t^k is:

$$\left(4(((p-1)/2)-k)^2 - (2k+1)^2\right) b_k = p(p-2-4k)b_k \equiv 0 \pmod{p},$$

proving the claim.

Now, assume that $H_p(\lambda) = 0$, where $\lambda \in \overline{\mathbb{F}}_p$. As we have seen, $H_p(0), H_p(1) \neq 0$, so $\lambda \neq 0, 1$. Write $H_p(t) = (t-\lambda)^r G(t)$, for some polynomial $G(t)$ such that $G(\lambda) \neq 0$. Assume that $r \geq 2$. In (6), we have $(t-\lambda)^{r-1}$ dividing the middle term and the last term. However, only $(t-\lambda)^{r-2}$ divides the term $4t(1-t)H_p^{''}(t)$. As the sum of the three terms is zero, this is impossible. Therefore, we must have $r = 1$. Hence, λ is a simple root.
Remark: A technical point to consider is that since the degree of $H_p(t)$ is less than p, we have $r < p$, so the first term of the derivative

$$H_p^{''}(t) = r(r-1)(t-\lambda)^{r-2}G(t) + 2r(t-\lambda)^{r-1}G'(t) + (t-\lambda)^r G^{''}(t)$$

does not vanish in characteristic p. Therefore, $(t-\lambda)^{r-1}$ doesn't divide the first term of (6).

Corollary 4.3.5: Let $p \geq 5$ be a prime. The number of $j \in \overline{\mathbb{F}}_p$ that occur as j-invariants of supersingular elliptic curves is

$$\left[\frac{p}{12}\right] + \epsilon_p,$$

where $\epsilon_p = 0, 1, 1, 2$ if $p \equiv 1, 5, 7, 11 \pmod{12}$, respectively.

Proof: In Section 3.4 we have shown that the j-invariant of $y^2 = x(x-1)(x-\lambda)$ is:

$$j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda-1)^2}.$$

Hence, the values of λ yielding a given j are roots of the polynomial

$$P_j(\lambda) = 2^8(\lambda^2 - \lambda + 1)^3 - j\lambda^2(\lambda-1)^2.$$

The discriminant of the polynomial is $2^{30}(j-1728)^3 j^4$, which is zero, only when $j = 0$ or $j = 1728$. Hence, as shown in Proposition 3.4.2 (c), there are six distinct values of $\lambda \in \overline{\mathbb{F}}_p$ corresponding to each value of $j \neq 0, 1728$. If one of these λ's is a root of $H_p(t)$, then all six must be roots, as the corresponding elliptic curves are all the same, up to the change of variables. Therefore, all or none are supersingular.

As the degree of $H_p(t)$ is $(p-1)/2$, we expect approximately $(p-1)/12$ supersingular j-invariants, with corrections needed for the cases when at least one of $j = 0$ or $j = 1728$ is supersingular.

When $j = 0$, the polynomial $P_j(\lambda)$ becomes $2^8(\lambda^2 - \lambda + 1)^3$, so there are two values of λ that yield $j = 0$. When $j = 1728$, the polynomial becomes $2^8(\lambda - 2)^2(\lambda - \frac{1}{2})^2(\lambda + 1)^2$, so there are three values of λ giving $j = 1728$.

We have previously seen, at the end of Section 3.3, that a curve with j-invariant 0 can be expressed as $y^2 = x^3 + 1$ over an algebraically closed field. Hence, by Theorem 4.3.2 (a), when $p \equiv 2 \pmod{3}$, the two λ's giving $j = 0$ are roots of

$H_p(t)$. Similarly, when $p \equiv 3 \pmod 4$, the three λ's giving $j = 1728$ are roots of $H_p(t)$.

Putting everything together, the total number of roots of $H_p(t)$ is

$$6 \times \#\{\text{supersingular } j \neq 0, 1728\} + 2\delta_{2(3)} + \delta_{3(4)} = \deg H_p(t) = (p-1)/2,$$

where $\delta_{i(j)} = 1$ if $p \equiv i \pmod j$, and $\delta_{i(j)} = 0$, otherwise.

Assume that $p \equiv 7 \pmod{12}$. Then $\delta_{2(3)} = 0$ and $\delta_{3(4)} = 1$ (since $7 \equiv 1 \not\equiv 2 \pmod 3$ and $7 \equiv 3 \pmod 4$). Hence, $\#\{\text{supersingular } j \neq 0, 1728\}$, the number of supersingular $j \neq 0, 1728$ is

$$\frac{1}{6}\left(\frac{p-1}{2} - 2(0) - 3(1)\right) = \frac{p-1}{12} - \frac{1}{2} = \left[\frac{p}{12}\right].$$

Adding 1 for the case when $j = 0$ gives the result stated in the proposition. The other cases for $p \pmod{12}$ are dealt with in a similar manner.

Example 3: Let $p = 151$. We know that $p = 12 \times 12 + 7 \equiv 7 \pmod{12}$. Hence, there are $[\frac{151}{12}] + 1 = 12 + 1 = 13$ j-invariants in $\overline{\mathbb{F}}_{151}$. By Theorem 3.3.2, if two elliptic curves over the same finite field, K, have the same j-invariant, then they are isomorphic in $\overline{K}$. Therefore, we deduce that there are 13 supersingular elliptic curves over $\overline{\mathbb{F}}_{151}$ up to isomorphism.

We now illustrate how to apply these results not only to determine the number of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, but also their form.

Example 4: Let $p = 11$. Then $m = 5$, and we obtain

$$\begin{aligned} H_{11}(t) &= 1 + 3t + t^2 + t^3 + 3t^4 + t^5 \\ &= (t+1)(t-2)(t+5)(t^2 + 10t + 1), \end{aligned}$$

where this is the factorisation of $H_{11}(t)$ over $\mathbb{F}_{11}$.

We have that $[\frac{11}{12}] = 0$ and, trivially, $11 \equiv 11 \pmod{12}$. Hence, by Corollary 4.3.5, there are $0 + 2 = 2$ possible values for the j-invariant in $\overline{\mathbb{F}}_{11}$. The first three factors correspond to $j = 1728$, and therefore, as previously seen, to the curve $y^2 = x^3 + x$.

Secondly, note that $t^2 + 10t + 1 \equiv t^2 - t + 1 \pmod{11}$ and let λ be a root of this second factor. Then, $\lambda^2 + 10\lambda + 1 \equiv \lambda^2 - \lambda + 1 \equiv 0 \pmod{11}$. Therefore,

$$j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2} \equiv 0 \pmod{11}.$$

As previously observed, there are two roots corresponding to $j = 0$, and to the elliptic curve $y^2 = x^3 + 1$. In this case, it's the two roots of $t^2 + 10t + 1$.

We have now found the two supersingular elliptic curves over $\overline{\mathbb{F}}_{11}$, corresponding to the two j-invariants in $\overline{\mathbb{F}}_{11}$ (by Theorem 3.3.2, elliptic curves with the same j-invariant are isomorphic over $\overline{\mathbb{F}}_{11}$). Note that over $\mathbb{F}_{11}$, one can find different forms of these curves. Take $y^2 = x^3 + 1$ and $y^2 = x^3 + 3$, which are different curves over $\mathbb{F}_{11}$, but the same over $\overline{\mathbb{F}}_{11}$.
(a similar approach can be found in [7, Section 5.4]).

Example 5: For a second example, let $p = 17$. Then, $m = 8$ and we obtain

$$\begin{aligned} H_{17}(t) &= 1 - 4t + 2t^2 + 8t^3 + 4t^4 + 8t^5 + 2t^6 - 4t^7 + t^8 \\ &= (t^2 + t + 16)(t^2 + 14t + 1)(t^2 + 16t + 1)(t^2 + 16t + 16) \end{aligned}$$

where this is the factorisation of $H_{17}(t)$ over $\mathbb{F}_{17}$ (to obtain this factorisation, we have used a code in MAGMA, which can be found in Appendix A).

Note that $[\frac{17}{12}] = 1$ and $17 \equiv 5 \pmod{12}$. Hence, as before, by Corollary 4.3.5, there are $1 + 1 = 2$ j-invariants in $\overline{\mathbb{F}}_{17}$. Furthermore, let λ be a root of $t^2 + 16t + 1 \equiv t^2 - t + 1 \pmod{17}$. Then, $\lambda^2 - \lambda + 1 \equiv 0 \pmod{17}$. As seen in the previous example,the two roots of $t^2 + 16t + 1$ correspond to $j = 0$, and therefore to the elliptic curve $y^2 = x^3 + 1$.

The remaining three factors correspond to the same j-invariant. As we have previously remarked, the six roots correspond to

$$\left\{\lambda, \frac{1}{\lambda}, 1 - \lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda - 1}, \frac{\lambda - 1}{\lambda}\right\},$$

with $\lambda = -7 + 4\sqrt{3}$, which is a root of the second factor. Therefore, the corresponding elliptic curve is $y^2 = x(x-1)(x + 7 - 4\sqrt{3})$.
We have now found the two supersingular elliptic curves over $\overline{\mathbb{F}}_{17}$.

Remark: The appearance of square roots, such as in the above example, is fairly common. It can be shown that a supersingular elliptic curve over a finite field $\mathbb{F}_q$, where $q = p^n$, p prime and $n \in \mathbb{Z}$, has its j-invariant in $\mathbb{F}_{p^2}$ (we don't prove this result as it's beyond the scope of this project, but direct the interested reader to [7, Section 5.3]). Hence, a supersingular elliptic curve over $\overline{\mathbb{F}}_q$ can always be transformed into an elliptic curve defined over $\mathbb{F}_{p^2}$, via a change of variables (the variables are defined over $\overline{\mathbb{F}}_q$).

Example 6: We show that for $p \geq 5$, E is supersingular if and only if

$$\#E(\mathbb{F}_p) = p + 1.$$

($\Longleftarrow$) Let $\#E(\mathbb{F}_p) = p + 1$. Then, $\#E(\mathbb{F}_p) \equiv 1 \pmod{p}$, and by Proposition 4.3.1, $E(\mathbb{F}_p)$ is supersingular. This finishes this first part.

($\Longrightarrow$) Assume that E is supersingular. By Hasse's Theorem, Theorem 4.1.1,

we know that $|p+1-\#E(\mathbb{F}_p)| \leq 2\sqrt{p}$. By definition of the modulus function,

$$|p+1-\#E(\mathbb{F}_p)| = \begin{cases} p+1-\#E(\mathbb{F}_p) & \text{if} \quad p+1-\#E(\mathbb{F}_p) \geq 0 \\ -(p+1-\#E(\mathbb{F}_p)) = & \\ = \#E(\mathbb{F}_p) - p - 1 & \text{if} \quad p+1-\#E(\mathbb{F}_p) < 0. \end{cases}$$

Note that $2\sqrt{p} < p$ (since we have assumed that $p \geq 5 > 4$, then $4p < p \times p = p^2$; square rooting both sides gives the desired result). Hence, we can rewrite our inequality as:

$$|p+1-\#E(\mathbb{F}_p)| < p.$$

Note that Hasse's Theorem provides both a lower and an upper bound for the number of points on an elliptic curve over a finite field. From the relation $p+1-\#E(\mathbb{F}_p) < p$, we deduce that $1 < \#E(\mathbb{F}_p)$ and from the relation $\#E(\mathbb{F}_p) - p - 1 < p$ we deduce that $\#E(\mathbb{F}_p) < 2p+1$. Putting everything together, we obtain:

$$1 < \#E(\mathbb{F}_p) < 2p+1.$$

Recall our assumption that $E(\mathbb{F}_p)$ is supersingular. By Proposition 4.3.1, if $E(\mathbb{F}_p)$ is supersingular, then $\#E(\mathbb{F}_p) \equiv 1 \pmod{p}$. Looking at our interval, $\#E(\mathbb{F}_p) \in \{2, 3, \cdots, p, p+1, p+2, \cdots, p+p = 2p\}$, we note that there is exactly one value that satisfies the condition of Proposition 4.3.1, namely

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

(to make this even more clear, note that $\{2, 3, \cdots, p, p+1, p+2, \cdots, 2p\} \equiv \{2, 3, \cdots -1, 0, 1, 2, \cdots, -1, 0\} \pmod{p}$; and there is exactly one value congruent to $1 \pmod{p}$). This finishes the proof.
Remark: The statement of this exercise is taken from [7, Exercises (5.10 (b)) in Section 5], but the solution is my own.

Remark: Let E be a supersingular elliptic curve defined over $\mathbb{F}_q$, and let $P = (x, y)$ be a point on $E(\mathbb{F}_{q^n})$, for some $n \geq 1$. Generally, n is large. Let k be a positive integer. From [8, Section 4.6], we note that an appealing feature of supersingular elliptic curves is that computations of the form kP are sometimes done in a shorter time than initially anticipated. Usually, for a time efficient computation successive doubling is used, but an even better result can be achieved when using supersingular elliptic curves . Suppose that $a = 0$. From the proofs of Proposition 4.3.1 and Theorem 4.3.2, we deduce that

$$\phi_q^2 + q = 0.$$

Hence,

$$q(x, y) = -\phi_q^2(x, y) = (x^{q^2}, -y^{q^2}).$$

To compute x^{q^2} and y^{q^2} we use finite field arithmetic, which is generally more time efficient than elliptic curve computations. This leads us onto the next section, Section 5, where we look at some particular applications of elliptic curves to cryptography.

5 Applications to Cryptography

In this final section, we look at some particular applications of elliptic curves to modern cryptography. We introduce the elliptic curve discrete logarithm problem, and illustrate the key role it plays in the validity of the Elliptic Curve Diffie-Hellman Key Exchange Algorithm, which is fundamental in blockchain development.

We begin with a short introduction to *cryptography*, the study of methods of sending messages in disguised form, so that only the intended recipients can remove the disguise and read the message, as stated in [12].

The message we want to send is called the *plaintext*. As we want to prevent Eve, the unauthorized third party - for example, a hacker trying to access the financial documents of two banks exchanging information - from accessing the message we use an *encryption key* to disguise, or *encrypt* our message. The disguised message is called the *ciphertext*. The ciphertext is then sent to the intended recipient, often called Bob in literature. To read our message, Bob now uses a *decryption key* to convert the ciphertext back to the original plaintext message.

The fundamental idea of this method is that while the encryption key is made available publicly, so that both us and Bob can use it encrypt our messages, the decryption key must be private. This ensures that the messages aren't intercepted by an unauthorized third party. The diagram below illustrates how this method works, with Alice sending Bob a message.

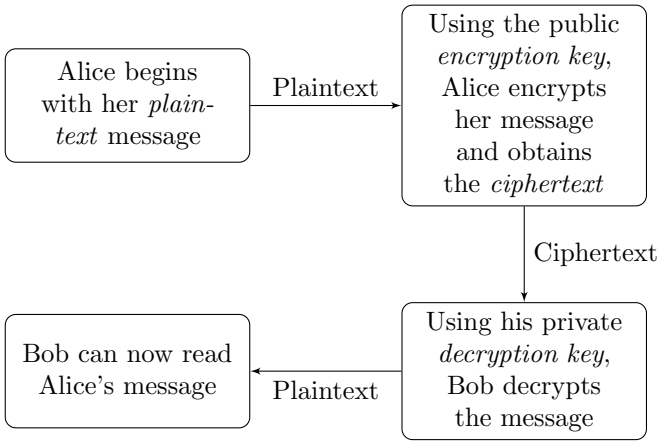

Figure 5: Flow diagram depicting public key cryptography

For a more detailed account see [12, Section 3.1].

5.1 Elliptic Curve Discrete Logarithm Problem

The aim of this subsection is to motivate the use of elliptic curves in modern cryptography. Not only why we need them for safer encryption, but also highlight their advantages over their classical counterparts. We begin by introducing the classical **Discrete Logarithm Problem** (DLP), as stated in [8, Chapter 5]:

Let p be a prime, and let $a, b \in \mathbb{Z}$ that are coprime to p. Assume we know that there exists an integer k, such that

$$a^k \equiv b \pmod{p}.$$

Find k.

Remark: We can extend the DLP to any multiplicatively written group, but classically it's taken over $\mathbb{F}_q^*$, where $q = p^n, p$ a prime and $n \in \mathbb{Z}$. Later in this section, we will see how we can extend this problem to the group $E(\mathbb{F}_q)$, for some elliptic curve E.

The *naive algorithm* for solving the DLP is to simply appeal to brute force, or in other words, to compute $a, a^2, \cdots$ until b is obtained. One can easily see that this approach is impractical, especially when k could be an integer of several hundreds of digits, which is often the case in cryptography. Hence, more efficient techniques are required.

A first technique, developed by Daniel Shanks, [13], known as the **"Baby Step, Giant Step"** algorithm is discussed. While it "square-roots" the number of steps required to solved the DLP compared to the naive approach, it requires a very large amount of storage. Hence, it can only be applied to groups of moderate size. We give an overview of this algorithm:
Let $a, b \in \mathbb{F}_q^*$, where $q = p^n$, p a prime and $n \in \mathbb{Z}$, and let m be the order of a.

1. Let M be the smallest integer that is greater than or equal to $\sqrt{m}$.
2. Make a list of elements (the babysteps):
$$a, a^2, \cdots a^M.$$
3. Take $c = (a^M)^{-1}$ and create a list of elements (the giantsteps):
$$bc, bc^2, \cdots bc^M.$$

4. Look for a match between the lists in steps (2) and (3). If there is a match, say $a^i = bc^j$, then $b = a^{i+jM}$ (since $c = (a^M)^{-1}$, and $b = a^i(c^j)^{-1} = a^i(((a^M)^{-1})^j)^{-1} = a^i a^{(-M\times -j)} = a^i a^{jM}$); otherwise, b is not a power of a.

Example 1: Let $a = 5, b = 3 \in \mathbb{F}_{23}^*$. Find k, such that $5^k = 3$.

Firstly, by Theorem 2.1.7, we know that $|\mathbb{F}_{23}^*| = 23-1 = 22$. By Corollary 2.1.6, m, the order of 5, divides 22. Therefore, $m \in \{1, 2, 11, 22\}$. We note that since 5 is not the identity element, it can't have order 1. Now, $5^2 = 25 = 23 + 2 \equiv 2 \pmod{23}$. So $m \neq 2$. Note that $5^5 = 3125 = 135\times 23+20 \equiv 20 \equiv -3 \pmod{23}$. Hence, $5^{11} = 5^5\times 5^5\times 5 \equiv -3\times -3\times 5 \equiv 45 \equiv -1 \pmod{23}$. Therefore, $m \neq 11$. As $m \neq 1, 2, 11$, we conclude that $m = 22$. We can now perform the algorithm:

1. We begin by computing $\sqrt{m} = \sqrt{22} \approx 4.69$. Hence, $M = 5$.
2. List the babysteps:
$$5, 5^2, 5^3, 5^4, 5^5 = 5, 2, 10, 4, 20 \quad \text{in} \quad \mathbb{F}_{23}.$$
3. Take $c = (5^5)^{-1} = (20)^{-1}$ in $\mathbb{F}_{23}$ (we have seen in the previous step that $5^5 \equiv 20 \pmod{23}$). Note that $20 \times 15 = 300 = 299 + 1 = 23 \times 13 + 1 \equiv 1 \pmod{23}$. Hence, $c = (20)^{-1} = 15$ in $\mathbb{F}_{23}$. We list the giantsteps:
$$3 \times 15, 3 \times 15^2, 3 \times 15^3, 3 \times 15^4, 3 \times 15^5 = 22, 8, 5, 6, 21 \quad \text{in} \quad \mathbb{F}_{23}.$$
4. We note that there is a match between steps (2) and (3), namely $5^1 = 3 \times 15^3$. Hence, $3 = 5^{1+3\times 5} = 5^{16}$ in $\mathbb{F}_{23}$, and we are done.

We have found $k = 16$.

We proceed by looking at a second alternative algorithm, due to John Pollard, [14], which takes approximately the same amount of time, but the storage space required is essentially null. Before illustrating how the algorithm works, we introduce some background results. Let G be a finite group of order N, and f a function, $f : G \to G$. Starting with an initial value $x_0 \in G$, define a sequence of points $x_0, x_1, \cdots$ by
$$x_i = f(x_{i-1}) = \underbrace{f \circ f \circ \cdots \circ f(x_0)}_{i \text{ iterations of } f}.$$
As G is a finite set, there exists some indices $i_0 < j_0$, such that $x_{i_0} = x_{j_0}$. Then
$$x_{i_0+1} = f(x_{i_0}) = f(x_{j_0}) = x_{j_0+1},$$
and, similarly, $x_{i_0+l} = x_{j_0+l}$, for all $l \geq 0$. Hence, the sequence x_i is periodic with period $j_0 - i_0$ (or it's possible that the period is a divisor of $j_0 - i_0$).

Remark: The picture describing this process, as shown below [8, Section 5.2, Figure 5.1], resembles the Greek letter ρ, which is where the method gets its name from:

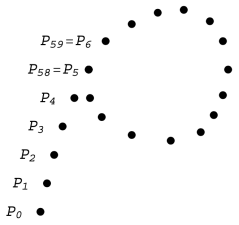

Figure 6: Pollard's ρ algorithm

Theorem 5.1.1: There exists an index i, such that $x_{2i} = x_i$.

Proof: We only give an overview, as the proof is not central to our project and direct the interested reader to [8, Section 11.5]. The main idea is that once there is a match for two indices differing by d, all subsequent indices differing by d will yield matches. This is simply due to the periodicity previously mentioned. Hence, we can compute pairs (x_i, x_{2i}) for $i = 1, 2, \cdots$, but only keep the current pair. We can calculate these by appealing to the rules:

$$x_{i+1} = f(x_i), \quad x_{2(i+1)} = f(f(x_{2i})).$$

Assume $i \geq i_0$ and i is a multiple of d. Then, the indices $2i$ and i differ by a multiple of d, and therefore, yield a match $x_i = x_{2i}$. As $d \leq j_0$, and $i_0 < j_0$, we can deduce that there is a match for $i \leq j_0$.

We are now equipped to describe **Pollard's ρ algorithm**: Let G be a finite group and $a, b \in G$. The goal is to compute an integer k such that $a^k = b$ in G. We use Theorem 5.1.1 to find integers i, j, m, l such that

$$a^i b^j = a^m b^l.$$

By rearranging, we obtain $a^{i-m} = b^{l-j}$, and supposing that $l - j$ is coprime to n, the order of a, we can solve for b as a power of a.

Note that we omit the question of how to choose a suitable function f, as it's beyond the scope of the project. The interested reader is directed to [8, Section 5.2.2] and [7, Section 11.5] for an in depth discussion. We use Pollard's suggestion, [14], of splitting G into a disjoint union of three sets of approximately equal size, $G = A \cup B \cup C$, and using the function $f(c)$, where:

$$f(c) = \begin{cases} ac & \text{if} \quad c \in A \\ c^2 & \text{if} \quad c \in B \\ bc & \text{if} \quad c \in C. \end{cases}$$

We now examine what happens when we repeatedly apply f to the initial point $c_0 = 1$. After i iterations, we arrive at a point

$$c_i = \underbrace{f \circ f \circ \cdots \circ f(1)}_{i \text{ iterations of } f} = a^{\alpha_i} b^{\beta_i}$$

for some integers α_i, β_i. Predicting the values of α_i and β_i is challenging a priori. Therefore, we compute them simultaneously to $c_1, c_2, \cdots$, by starting with $\alpha_0 = \beta_0 = 0$ and using the iterative formulas

$$\alpha_{i+1} = \begin{cases} \alpha_i + 1 & \text{if} \quad c_i \in A \\ 2\alpha_i & \text{if} \quad c_i \in B \\ \alpha_i & \text{if} \quad c_i \in C, \end{cases} \quad \text{and} \quad \beta_{i+1} = \begin{cases} \beta_i & \text{if} \quad c_i \in A \\ 2\beta_i & \text{if} \quad c_i \in B \\ \beta_i + 1 & \text{if} \quad c_i \in C. \end{cases}$$

Note that we only need to keep track of α_i and β_i modulo n, the order of a, as $a^n = 1$ in G (by Corollary 2.1.6). This ensures that the values of α_i and β_i are of practical size.

Similarly, we compute the sequence of points:

$$d_0 = 1 \quad \text{and} \quad d_{i+1} = f(f(d_i)).$$

From Theorem 5.1.1 we know that:

$$d_i = c_{2i} = a^{\gamma_i} b^{\delta_i},$$

where γ_i and δ_i can be calculated from γ_{i-1} and δ_{i-1} using two repetitions of the recurrences for α_i and β_i.

For the next step, we compute $(c_1, d_1), (c_2, d_2), \cdots$, until a pair with the same coordinates is found.
Remark: As each successive (c_i, d_i) is computed only in terms of the previous (c_{i-1}, d_{i-1}) we never need to store more than a few numbers.

From $c_i = a^{\alpha_i} b^{\beta_i}$ and the equality $c_i = d_i$ we infer that

$$a^{\alpha_i - \gamma_i} = b^{\delta_i - \beta_i}.$$

If $\gcd(\delta_i - \beta_i, n) = 1$, which is generally the case when we take n prime, then

$$k \equiv (\alpha_i - \gamma_i)(\delta_i - \beta_i)^{-1} \pmod{n}.$$

This solves $a^k = b$ in G.

In short, Pollard's ρ algorithm to solve the DLP in a finite group G, uses a map $f : G \to G$ that is straightforward to compute, yet whose iterates mix up the elements of G in a random manner. We illustrate how this algorithm works with an example:

Example 2: Let $G = \mathbb{F}_{47}^*$, and $a = 3, b = 2 \in \mathbb{F}_{47}^*$. Find k such that $3^k = 2$.

We begin by splitting $\mathbb{F}_{47}^*$ into a disjoint union of three sets of approximately equal size, $\mathbb{F}_{47}^* = A \cup B \cup C$, with $A = \{1, 3, 5, 7, 8, 12, 15, 21, 29, 30, 31, 36, 41, 42, 43, 46\}$, $B = \{4, 10, 13, 14, 18, 20, 22, 23, 24, 26, 27, 28, 32, 34, 37, 43\}$ and $C = \{2, 6, 9, 11, 16, 17, 19, 25, 33, 35, 38, 39, 40, 44, 45\}$ (we obtained these sets by using a random number generator). We claim that 3 has order 23. By Theorem 2.1.7, $|\mathbb{F}_{47}^*| = 47 - 1 = 46 = 2 \times 23$. Hence, an element in $\mathbb{F}_{47}^*$ can have order $1, 2, 23$ or 46. Since 3 is not the identity element, it cannot have order 1. Note, $3^2 = 9 \equiv 9 \pmod{47}$, so it cannot have order 2 either. Remark that $3^5 = 243 = 47 \times 5 + 8 \equiv 8 \pmod{47}$. Hence, $3^{23} = 8 \times 8 \times 8 \times 8 \times 3^3 = 110592 = 47 \times 2353 + 1 \equiv 1 \pmod{47}$. This proves our claim.

Starting from $c_0 = d_0 = 1$ and $\alpha_0 = \beta_0 = 0$, we commence our iteration, following the rules discussed above:

1. $c_1 = f(c_0) = 3 \times 1 = 3$, as $1 \in A$ and $d_1 = f(f(d_0)) = f(f(1)) = f(3) = 3 \times 3 = 9$, as $3 \in A$. Since $1 \in A$, we also obtain $\alpha_1 = 1$ and $\beta_1 = 0$. We obtain the pair $(3, 9)$, so we continue the process.
2. $c_2 = f(c_1) = f(3) = 3 \times 3 = 9$, since $3 \in A$, and $d_2 = f(f(d_1)) = f(f(9)) = f(2 \times 9) = f(18) = 18^2 = 42$ in $\mathbb{F}_{47}^*$ (since $9 \in C$ and $18 \in B$). As $3 \in A$, $\alpha_2 = 2$ and $\beta_2 = 0$, also. Hence, we obtain the pair $(9, 42)$ and we continue the process.
3. $\cdots$
4. $c_9 = f(c_8) = f(12) = 3 \times 12 = 36$ in $\mathbb{F}_{47}^*$, as $12 \in A$ and $d_9 = f(f(d_8)) = f(f(8)) = f(3 \times 8) = f(24) = 24^2 = 12$ in $\mathbb{F}_{47}^*$ (since $8 \in A$ and $24 \in B$). As $12 \in A$, we also obtain $\alpha_9 = 21$ and $\beta_9 = 9$. We obtain the pair $(36, 12)$, and we continue the process.
5. $c_{10} = f(c_9) = f(36) = 3 \times 36 = 14$ in $\mathbb{F}_{47}^*$, as $36 \in A$ and $d_{10} = f(f(d_9)) = f(f(12)) = f(3 \times 12) = f(36) = 3 \times 36 = 14$ in $\mathbb{F}_{47}^*$ (since $12, 36 \in A$). As $36 \in A$, we also obtain $\alpha_{10} = 22$ and $\beta_{10} = 9$. We obtain the pair $(14, 14)$, and end the process.

We have obtained that $c_{10} = d_{10}$. From Theorem 5.1.1, we also know that $d_{10} = c_{20}$. Hence, we obtain $c_{10} = c_{20}$, and infer that:

$$3^{\alpha_{10}} 2^{\beta_{10}} = 3^{\alpha_{20}} 2^{\beta_{20}}.$$

Further computations (which we omit as they are computationally laborious and identical to the process previously illustrated; except we are only interested in the value of c_i, for $11 \leq i \leq 19$) show that $\alpha_{20} = 4$ and $\beta_{20} = 6$, working mod 23, the order of a. Therefore, we obtain:

$$3^{22} 2^9 = 3^4 2^6.$$

Lastly,

$$k \equiv (22-4)(6-9)^{-1} \equiv 18 \times (-3)^{-1} \equiv 18 \times 20^{-1} \pmod{23}.$$

Note that $20 \times 15 = 300 = 299+1 = 23 \times 13 + 1 \equiv 1 \pmod{23}$. Hence, $20^{-1} \equiv 15 \pmod{23}$. Putting everything together, we obtain

$$k \equiv 18 \times 15 \equiv 270 \equiv 17 \pmod{23},$$

and we are done. We conclude that $3^{17} = 2$ in $\mathbb{F}_{47}^*$.

These are just a few of the methods that have been developed to solve the DLP. A more detailed account of their proofs, as well as of other various techniques for attacking the DLP can be found in [8, Section 5.2] and [7, Section 11.5].

The main point of this subsection was to illustrate that the DLP is no longer a secure approach to cryptography. Therefore, a more advantageous analogous problem has been developed using elliptic curves, which can withstand the strongest attacks developed against the DLP. As described in [15, Chapter 5], it's known as the:

Elliptic Curve Discrete Logarithm Problem (ECDLP): Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Let n denote the order of the group $E(\mathbb{F}_q)$, and let $P \in E(\mathbb{F}_q)$. Given Q is an element of the subgroup generated by P, find $m \in \mathbb{Z}$, such that

$$Q = [m]P.$$

The difficulty of ECDLP lies at the heart of the Elliptic Curve Diffie-Hellman Key Exchange algorithm.

The fundamental idea for applications to cryptography, is that while $[m]P$ can be efficiently calculated, for example, we have seen in Section 3.2 the method of successive doubling, finding m from only knowing P and Q is a much more challenging and time-consuming process.

5.2 Elliptic Curve Diffie-Hellman Key Exchange

Two parties, Alice and Bob wish to exchange information, and they want to agree on a common key, [8, Section 6.2]. As an example, Alice and Bob could be two financial companies that would like to share their data. It's time-consuming and not practical to use a courier to deliver the key. Furthermore, the assumption is that Alice and Bob have had no contact previously, so they can only communicate through public channels. One way to establish a secret key is the following method, due to Whitfield Diffie and Martin Hellman, [16], which relies on the hardness of the discrete logarithm problem for elliptic curves over large finite fields:

1. Alice and Bob agree on an elliptic curve E over a finite field $\mathbb{F}_q$, where q is chosen to be a large prime order such that the discrete logarithm problem is difficult to solve on $E(\mathbb{F}_q)$. They also agree on a point $P \in E(\mathbb{F}_q)$, such that the order of P, $\text{ord}(P) = m$ is very large.

   Remark 1: If the order of P, $\text{ord}(P) = m$, is relatively small, then Eve could use a computer to calculate and list all the values $P, [2]P, \cdots, [m-1]P$ and find which one corresponds to Q. The fundamental idea is that m needs to be large enough, so that the time required to run this computations would be too long for the unauthorised party to intercept the message.

   Remark 2: In general, E and P are chosen in such a way that m is a very large prime.

2. Alice chooses a secret integer a, $a \in \{0, \cdots, m-1\}$, and calculates $P_1 = aP \in E(\mathbb{F}_q)$. She then sends P_1 to Bob.

   Remark: Usually, larger values of a are chosen to ensure that the discrete logarithm problem remains hard to solve. If a small value was to be chosen, a similar approach as in *Remark 1* could be used to find a.

3. Similarly, Bob chooses a secret integer b, $b \in \{0, \cdots, m-1\}$ and calculates $P_2 = bP \in E(\mathbb{F}_q)$. He then sends P_2 to Alice.

4. Alice computes $aP_2 = abP$.

5. Bob computes $bP_1 = baP$.

6. The private decryption key of Alice and Bob is abP (since addition of points on any elliptic curve E, is both commutative and associative, $abP = baP$, or in other words, both parties obtain the same point at the end of the algorithm). In practice, Alice and Bob use a method they privately agreed on to extract a key from abP. For example, they could take their key to be the last 512 bits of the x-coordinate of the point abP.

   Remark: When resources such as storage and bandwidth are at a premium, it's preferable to represent the points P, P_1, P_2 and abP using the minimum possible amount of bits. This is referred to as *point compression*. The interested reader is directed to [15, Section 4.4], for a detailed account of how this is achieved.

The only information that the eavesdropper, Eve, has access to is the curve E, the finite field $\mathbb{F}_q$, and the points P, aP and bP. Hence, she needs to solve the following:

Diffie-Hellman Problem: Given P, aP, and bP in $E(\mathbb{F}_q)$, compute abP.

If Eve can solve the discrete logarithm problem in $E(\mathbb{F}_q)$, she can then use P and aP to find a. She can then compute $a(bP)$ to obtain abP. As it remains

unknown whether one can calculate aP, without first finding a solution to the elliptic curve discrete logarithm problem, we conclude that this algorithm does indeed obtain a valid secret key. (If an alternative solution is presented, the validity of the algorithm may come under scrutiny).

Remark 1: Not only is the Elliptic Curve Diffie-Hellman Key Exchange more secure than its classical counterpart, by inheriting the advantages of the ECDLP over the classical DLP, but it's also faster and more efficient. It requires a smaller key size and the computations are done in a much shorter time.

Example: We illustrate how the Elliptic Curve Diffie-Hellman Key Exchange algorithm works. Let $\mathbb{F}_q = \mathbb{F}_{23}$.

1. Alice and Bob agree on the elliptic curve,

   $$E(\mathbb{F}_{23}) = \{(x, y) \in \mathbb{F}_{23} \times \mathbb{F}_{23} : y^2 = x^3 + 3x + 5\} \cup \{O\},$$

   and a point

   $$P = (1, 3).$$

   We begin by noting that indeed, $P \in E(\mathbb{F}_{23})$, as $1^3 + 3 \times 1 + 5 = 9 \equiv 9 \pmod{23}$, and $3^2 = 9 \equiv 9 \pmod{23}$, also. Appealing to Case 1 from Section 3.2, Point Addition, we obtain that $28P = O$.

   Remark: To ensure that 28 is the smallest integer such that $28P = O$, we have manually added P to itself 28 times.

   Therefore, we obtain $\text{ord}(P) = m = 28$.

2. Alice chooses $a = 7 \in \mathbb{F}_{23}$ and sends Bob:

   $$P_1 = aP = 7(1, 3) = (8, 9).$$

3. Bob chooses $b = 11 \in \mathbb{F}_{23}$ and sends Alice:

   $$P_2 = bP = 11(1, 3) = (17, 22).$$

4. Alice calculates

   $$aP_2 = 7(17, 22) = (8, 14).$$

5. Bob calculates

   $$bP_1 = 11(8, 9) = (8, 14).$$

6. We now have Alice and Bob's decryption key, $abP = (8, 14)$.

Remark: While we have used small numbers to simplify computations, in practice, to ensure the intractability of the elliptic curve discrete logarithm problem, elliptic curves would be taken over much larger finite fields.

To illustrate this point, we look at Curve25519, an elliptic curve used in the encryption of WhatsApp messages, [17]. It was introduced by Daniel Bernstein, [18], and it's considered to obtain new speed records for high-security Diffie-Hellman computations.

Curve25519 is considered over the finite field $\mathbb{F}_p$, where p is the prime

$$p = 2^{255} - 19,$$

and E is the elliptic curve

$$E : y^2 = x^3 + 486662x^2 + x.$$

Note that Curve25519 is an example of a Montgomery curve, a special type of elliptic curves, which are often preferred in cryptography, due to their efficiency. A detailed discussion of this particular choice is far beyond the scope of this project, but the interested reader is directed to [18, Section 2].

To conclude, remark how fascinating the simplicity of the curve and of the prime are, in stark contrast to the difficulty of the ECDLP.

6 Appendix A

These are the SageMath codes for finding an isogeny, α, between an elliptic curve $E_1 : y_1^2 = x_1^3 + A_1x_1 + B_1$ over a finite field $\mathbb{F}_p$ and a second elliptic curve, $E_2 : y_2^2 = x_2^3 + A_2x_2 + B_2$ over the same finite field (this is what we used for Example 1, Section 3.6).

```
// Define the finite field
k = GF(17)
// Define the elliptic curve E_1 over k, where A = 11 and B = 13
E = EllipticCurve(k, [11,13])
// Define Q, a point in the kernel of the isogney
Q = E(15,0)
phi = E.isogeny(Q)
phi.codomain()
phi.rational_maps()
```

Remark: The code can be generalised to any elliptic curve, and any finite field $\mathbb{F}_p$, as shown:

```
// Define the finite field
k = GF(F_p)
// Define the elliptic curve E_1 over k
E = EllipticCurve(k, [A,B])
// Define Q, a point in the kernel of the isogney
Q = E(q_1,q_2)
phi = E.isogeny(Q)
phi.codomain()
phi.rational_maps()
```

These are the MAGMA codes for finding the factorisation of $H_{11}(t)$,over $\mathbb{F}_{11}$ and the factorisation of $H_{17}(t)$ over $\mathbb{F}_{17}$, respectively.

```
// Define the finite field and polynomial
p := 11; // Prime characteristic
q := p^1; // Field size
Fq := GF(q); // Finite field
R<x> := PolynomialRing(Fq); // Polynomial ring

// Polynomial to factorize
f := x^5 + 3*x^4 + x^3 + x^2 + 3*x + 1;
```

```
// Factorize the polynomial
Factorization := Factorization(f);

// Print the factors
for i := 1 to #Factorization do
    print "Factor ", i, ": ", Factorization[i][1];
end for;


// Define the finite field and polynomial
p := 17; // Prime characteristic
q := p^1; // Field size
Fq := GF(q); // Finite field
R<x> := PolynomialRing(Fq); // Polynomial ring

// Polynomial to factorize
f := x^8 - 4*x^7 + 2*x^6 + 8*x^5 + 4*x^4 + 8*x^3 + 2*x^2 - 4*x + 1;

// Factorize the polynomial
Factorization := Factorization(f);

// Print the factors
for i := 1 to #Factorization do
    print "Factor ", i, ": ", Factorization[i][1];
end for;
```

A general MAGMA code, for any polynomial, is:

```
// Define the finite field and polynomial
p := p; // Prime characteristic
q := p^1; // Field size
Fq := GF(q); // Finite field
R<x> := PolynomialRing(Fq); // Polynomial ring

// Polynomial to factorize
f := f(x);

// Factorize the polynomial
Factorization := Factorization(f);

// Print the factors
for i := 1 to #Factorization do
    print "Factor ", i, ": ", Factorization[i][1];
end for;
```

Bibliography

[1] S. Kopparty, "Topics in finite fields," Fall 2019. Lecture notes, Rutgers University.

[2] U. Daepp and P. Gorkin, *Reading, writing, and proving: A closer look at mathematics*. Springer, 2011.

[3] M. Tointon, *Group Theory*. University of Bristol, 2022–2023. Physical lecture notes.

[4] T. Dokchitser, *Algebra 2*. University of Bristol, 2021–2022. Physical lecture notes.

[5] J. McKernan, "Chapter 10: Algebraic closure." Lecture Notes, 2016-2017. `https://mathweb.ucsd.edu/~jmckerna/Teaching/16-17/Winter/200B/l_10.pdf`.

[6] H. Bourlès, "Field extensions and differential field extensions," in *Fundamentals of Advanced Mathematics 2* (H. Bourlès, ed.), pp. 1–53, Elsevier, 2018. `https://www.sciencedirect.com/science/article/pii/B9781785482496500018`.

[7] J. H. Silverman, *The arithmetic of elliptic curves*. Springer, 2nd ed., 2009.

[8] L. C. Washington, *Elliptic curves: number theory and cryptography*. CRC press, 2nd ed., 2008.

[9] A. Corbellini, "Elliptic curve point addition," 2015. `https://andrea.corbellini.name/ecc/interactive/modk-add.html`.

[10] P. Bartlett, "Lecture 10: Injection, surjection, and linear maps." Lecture Notes, 2013. `https://web.math.ucsb.edu/~padraic/ucsb_2013_14/mathcs103_f2013/mathcs103_fall_2013_lecture10.pdf`.

[11] S. D. Galbraith, "Constructing isogenies between elliptic curves over finite fields," *LMS Journal of Computation and Mathematics*, vol. 2, pp. 118–138, 1999.

[12] N. Koblitz, *A course in number theory and cryptography*, vol. 114. Springer Science & Business Media, 1994.

[13] D. Shanks, "Class number, a theory of factorization, and genera," in *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, NY, 1969)*, pp. 415–440, Providence, RI: Amer. Math. Soc., 1971.

[14] J. M. Pollard, "Monte carlo methods for index computation (mod p)," *Math. Comp.*, vol. 32, no. 143, pp. 918–924, 1978.

[15] I. Blake, G. Seroussi, and N. Smart, *Elliptic curves in cryptography*, vol. 265. Cambridge university press, 1999.

[16] B. Woodberg, M. K. Madwachar, M. Swarm, N. R. Wyler, M. Albers, and R. Bonnell, "Chapter 11 - vpn theory and usage," in *Configuring Juniper Networks NetScreen & SSG Firewalls* (B. Woodberg, M. K. Madwachar, M. Swarm, N. R. Wyler, M. Albers, and R. Bonnell, eds.), pp. 551–586, Burlington: Syngress, 2007. `https://www.sciencedirect.com/science/article/pii/B9781597491181500137`.

[17] P. P. G. Neogi, "A dive into whatsapp's end-to-end encryption," *arXiv preprint arXiv:2209.11198*, 2022.

[18] D. J. Bernstein, "Curve25519: New diffie-hellman speed records," in *Public Key Cryptography - PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography*, vol. 3958 of *Lecture Notes in Computer Science*, pp. 207–228, Springer, 2006. `https://iacr.org/archive/pkc2006/39580209/39580209.pdf`.