Universiteit Utrecht

Faculteit Bètawetenschappen

Elliptic curves: an Introduction and Their Group Structure Over $\mathbb{Z}/N\mathbb{Z}$

Bachelor Thesis

Ward Jousma

Mathematics

Supervisor:

Dr. Stefano Marseglia
Utrecht University

June 13, 2021

Abstract

In this thesis we will introduce the concept of elliptic curves and discuss the group structure and classification of the group of points on elliptic curves over finite fields. In the main section we will introduce elliptic curves over $\mathbb{Z}/N\mathbb{Z}$ and derive the group structure of the group of points on such elliptic curves. Finally, as a consequence of this result we will present an isomorphism attack on the ECDLP in the group of points on an elliptic curve over $\mathbb{F}_p$ that only works when this curve is anomalous.

Contents

1 Introduction

An elliptic curve is a non-singular, projective curve defined over a field K and consists of solutions to the Weierstrass equation

$$y^2z = x^3 + Axz^2 + Bz^3,$$

when the characteristic of the field is not equal to 2 or 3. What makes elliptic curves interesting is that the set of points on an elliptic curve forms a group. This group can be used as the basis for the discrete logarithm problem, which lies at the foundation of many cryptographic systems. This is the reason elliptic curves are important in modern day cryptography.

When elliptic curves are defined over finite fields, a full classification of the group of points on these elliptic curves has been reached. However, elliptic curves can also be defined over rings, for example over $\mathbb{Z}/N\mathbb{Z}$. The goal of this thesis is to reach a description of the group structure of the group of points on elliptic curves over $\mathbb{Z}/N\mathbb{Z}$. When E is an elliptic curve over $\mathbb{Z}/N\mathbb{Z}$, we will see that

$$E(\mathbb{Z}/N\mathbb{Z}) \simeq \bigoplus_{\substack{p|N \\ |E(\mathbb{F}_p)| \neq p}} E(\mathbb{F}_p) \oplus \mathbb{Z}/p^{v_p(N)-1}\mathbb{Z} \oplus \bigoplus_{\substack{p|N \\ |E(\mathbb{F}_p)| = p}} G_p,$$

where p is a prime integer, $v_p(N)$ is the p-adic valuation of N and $E(\mathbb{F}_p)$ is an elliptic curve defined over $\mathbb{F}_p$. Also, every G_p is either equal to $\mathbb{F}_p \oplus \mathbb{Z}/p^{v_p(N)-1}\mathbb{Z}$ or to $\mathbb{Z}/p^{v_p(N)}\mathbb{Z}$.

Finally, we will discuss an interesting consequence of this group structure: an isomorphism attack on the elliptic curve discrete logarithm problem (the discrete logarithm problem where the underlying group is the group of points on an elliptic curve). The attack will run in polynomial time, however it only works for special cases of the underlying elliptic curve.

In Section 2 of this thesis we go over the basics of the discrete logarithm problem and elliptic curves over general fields. In Section 3 we discuss elliptic curves over finite fields. In Section 4 we move on to elliptic curves over $\mathbb{Z}/N\mathbb{Z}$ and prove the main result, Theorem 4.15. In Section 5 we discuss the elliptic curve discrete logarithm problem and derive the aforementioned attack. Finally, in Section 6 we provide some further reading and discuss open problems.

2 Basic Theory

First, we will define the discrete logarithm problem (DLP) and see why it is important to consider elliptic curves. Next, we will discuss elliptic curves over a general field and show how they can be represented. After that we will show how a group that we can use for the DLP arrises from elliptic curves.

2.1 Discrete Logarithm Problem

Definition 2.1. Let G be a finite, abelian group. The DLP in G is: given $g, h \in G$, find a positive integer k, if it exists, such that $g^k = h$.

Notice that the DLP has a solution if and only if h is an element of the subgroup of G generated by g. If h is not an element of such a subgroup, then the DLP has no solution. Because of this property, in practice the DLP is often used on cyclic groups. One of the simplest groups to consider the DLP on is $(\mathbb{Z}/p\mathbb{Z})^*$, the group of integers modulo a prime p under multiplication without 0.

Example 2.2. Consider the group $(\mathbb{Z}/23\mathbb{Z})^*$. Now given 3 and 12, we want to solve

$$3^k \equiv 12 \bmod 23$$

for k, this is a DLP. To solve this we can go through every possibility for k and we would find that $3^4 = 81 \equiv 12 \bmod 23$, so 4 is a solution to this DLP. △

Because the DLP was thought to be a hard problem for computers, there are some interesting real-world applications of the DLP using $(\mathbb{Z}/p\mathbb{Z})^*$ as the underlying group. Some examples are the Diffie-Hellman key exchange [1] and the ElGamal encryption system [2]. There are also some known methods to solve the DLP in $(\mathbb{Z}/p\mathbb{Z})^*$, such as the Pohlig-Hellman algorithm or Shanks' baby-step giant-step algorithm [3], these methods are both fully exponential and they do not pose a threat to the security of the DLP. However, some methods like the index calculus method [4], which can run in sub-exponential time, and a method described by Kleinjung and Wesolowski [5], which can run in expected quasi-polynomial time, cause the DLP over $(\mathbb{Z}/p\mathbb{Z})^*$ to be less secure than desired. This means that we should for look for other underlying groups for the DLP.

Luckily, there are other groups we can use for the DLP, one such set of groups uses elliptic curves. The only known algorithms to break the DLP with the points on an elliptic curve as the underlying group are fully exponential.

2.2 Elliptic Curves

Definition 2.3. An elliptic curve over a field K is a smooth or non-singular, projective curve of genus 1 over K together with a specified point $\mathcal{O}$ on the curve.

An elliptic curve over a field K describes points in K^2 and consists of solutions (x, y) of the long Weierstrass equation

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

where $a_1, ..., a_6 \in K$ are constants. This equation can always be used to represent an elliptic curve.

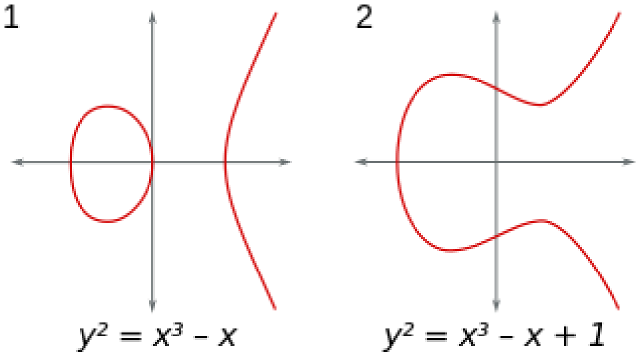

Figure 1: Two elliptic curves over the real numbers, from [6].

However, when the characteristic of the field is not 2, we can simplify this equation by replacing y with $\frac{1}{2}(y - a_1x - a_3)$, applying this change of variable we get

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

with $b_2, b_4, b_6 \in K$ constants. This is the most general equation for an elliptic curve over any field with characteristic not equal to 2. We can apply another change of variable when the characteristic of the field K is not equal to 3. This time we can replace x with $\frac{x-3b_2}{36}$ and y with $\frac{y}{108}$, the resulting equation is

$$y^2 = x^3 - 27c_4x - 54c_6$$

again with $c_4, c_6 \in K$ constants. Now denote $A = -27c_4$ and $B = -54c_6$ (note that these are constants in K), this results in the short Weierstrass equation

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

The elliptic curve is non-singular if and only if the discriminant of the curve $\Delta = -16(4A^3 + 27B^2)$ is non-zero. We will now assume that the field K has a characteristic not equal to 2 and that we can represent an elliptic curve over K by the short Weierstrass equation. We define the set of K-rational points of an elliptic curve E over a field K to be

$$E_{A,B}(K) = \{(x, y) \in K^2 \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}.$$

The inclusion of the point $\mathcal{O}$, which we will call the point at infinity, might seem strange. However, this point will be paramount to the definition of the group structure of an elliptic curve. Intuitively, we can consider the point at infinity a point that sits at the top and at the bottom of the y-axis, such that every vertical line passes through the point. This notion will be further expanded on when we introduce elliptic curves in projective space.

Now that we know what the group of points on an elliptic curve is, we will introduce the group operation, i.e. the concept of adding two points on an elliptic curve. Let $P_1, P_2 \in E_{A,B}(K)$ be two points on an elliptic curve E and denote the line through P_1 and P_2 by L. Since E is non-singular, L intersects $E_{A,B}(K)$ in a third point, which we will call P_3. Now reflect P_3 across the x-axis to get a point P_3'. This point is the sum of P_1 and P_2, or $P_1 + P_2 = P_3'$.

This process of addition is quite natural and has a beautiful geometric interpretation when the underlying field is $\mathbb{R}$ as seen in Figure 2, however the formulas carry over to other fields. We will now discuss a few different cases to make this notion more rigorous.

Firstly, assume that $P_1 \neq P_2$ with $x_1 \neq x_2$. Denote $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ and the line L through P_1 and P_2 by the equation $y = cx + d$. Then $c = \frac{y_1 - y_2}{x_1 - x_2}$. We can now find all intersections of L and E by substituting to get

$$(cx + d)^2 = x^3 + Ax + B.$$

By rewriting this, we get

$$x^3 - c^2x^2 + (A - 2cd)x + (b - d^2) = 0.$$

We know this equation has three roots in the algebraic closure of K, $\overline{K}$, with multiplicity. However, we already know what two of them are, namely x_1 and x_2, denote the final root by x_3. Since x_1 and x_2 are both points in K, we know that x_3 also lies in K. We get

$$x^3 - c^2x^2 + (A - 2cd)x + (b - d^2) = (x - x_1)(x - x_2)(x - x_3), \tag{2.1}$$

from this equation we get $x_3 = c^2 - x_1 - x_2$. This is the x-coordinate of the sum $P_1 + P_2$. Now we can find the y-coordinate y_3 by using the equation of L and reflecting across the x-axis, so $y_3 = c(x_1 - x_3) - y_1$. We get $P_1 + P_2 = (x_3, y_3)$.

Secondly, the case where $P_1 \neq P_2$, but $x_1 = x_2$. In this case the line L is vertical and will intersect at most two points on the curve. However, as we have seen every vertical line also passes through the point at infinity and the point at infinity reflected across the x-axis is itself, so in this case $P_1 + P_2 = \mathcal{O}$.

Next, assume $P_1 = P_2 = (x_1, y_1)$. Let L be the tangent line at P_1. The slope of L can now be found by differentiation at P_1:

$$c = \frac{3x_1 + A}{2y_1}.$$

If $y_1 = 0$, the tangent line is vertical, thus it intersects the point at infinity and we get $P_1 + P_2 = \mathcal{O}$.

Now we may assume $y_1 \neq 0$, we can then proceed in a similar way we did in the first case. However, we only know one root of equation (2.1), namely x_1. Because this is a root for both P_1 and P_2, it is a double root and we find $x_3 = c^2 - 2x_1$ and $y_3 = c(x_1 - x_3) - y_1$. Which also gives us $P_1 + P_2 = (x_3, y_3)$.

Finally, when $P_1 = \mathcal{O}$, then the line L through P_1 and P_2 will be vertical. The third point of intersection is the reflection of P_2 across the x-axis. In order to find the result of $P_1 + P_2$ we must reflect this point back across the x-axis, this results in P_2. To conclude, this means that $\mathcal{O} + P_2 = P_2$ and analogously $P_1 + \mathcal{O} = P_1$.

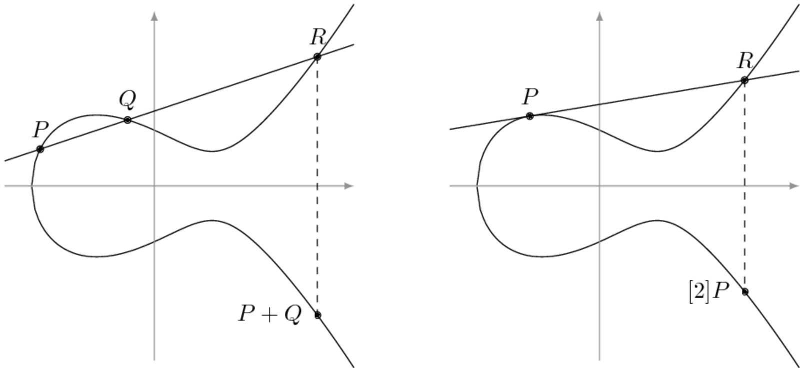

Figure 2: Geometric interpretation of the group law of an elliptic curve, from [7].

The group operation is as follows

1. For each $P \in E_{A,B}(K)$ holds $\mathcal{O} + P = P + \mathcal{O} = P$.
2. If $P_1 = P_2 = (x_1, 0)$, then $P_1 + P_2 = \mathcal{O}$.
3. If $P_1 = P_2 = (x_1, y_1)$ with $y_1 \neq 0$, then $P_1 + P_2 = (x_3, y_3)$, where
$$x_3 = c^2 - 2x_1, \qquad y_3 = c(x_1 - x_3) - y_1, \qquad \text{with } c = \frac{3x_1 + A}{2y_1}.$$
4. If $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ with $x_1 = x_2$ and $y_1 \neq y_2$, then $P_1 + P_2 = \mathcal{O}$.
5. If $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ with $x_1 \neq x_2$, then $P_1 + P_2 = (x_3, y_3)$, where
$$x_3 = c^2 - x_1 - x_2, \qquad y_3 = c(x_1 - x_3) - y_1, \qquad \text{with } c = \frac{y_1 - y_2}{x_1 - x_2}.$$

Example 2.4. Let E be an elliptic curve over the real numbers defined by the equation $y^2 = x^3 - 7x + 10$. Let $P_1 = (x_1, y_1) = (1, 2)$ and $P_2 = (x_2, y_2) = (3, 4)$, now we want to compute $P_3 = P_1 + P_2 = (x_3, y_3)$. We see that $P_1 \neq P_2$ and $x_1 = 1 \neq 3 = x_2$, this means that
$$x_3 = c^2 - x_1 - x_2, \qquad \text{with } c = \frac{y_1 - y_2}{x_1 - x_2}.$$
We calculate $c = \frac{2-4}{1-3} = \frac{-2}{-2} = 1$, now we can calculate x_3, we get
$x_3 = 1^2 - 1 - 3 = -3$. Finally we can calculate y_3 using
$$y_3 = c(x_1 - x_3) - y_1,$$
we get $y_3 = 1(1 + 3) - 2 = 2$. So we have $P_1 + P_2 = (-3, 2)$. △

Now we will prove that the points on an elliptic curve form a group.

Theorem 2.5. *Let E be an elliptic curve defined over a field K. The points on E with group operation as defined above form an abelian group with $\mathcal{O}$ as the identity element.*

Proof. By definition of the group operation $\mathcal{O}$ is the identity element, so the group does contain an identity element. Now let P_1 be a point on the elliptic curve not equal to $\mathcal{O}$, then let P_2 be the reflection of P_1 across the x-axis. From the fourth point of the group operation we see that P_1 and P_2 are each others inverse. This proves the existence of inverses. It is clear from the formulas that commutativity holds in this group, but we can also deduce commutativity from the geometric interpretation of the group operation. Obviously, a line through two points P_1 and P_2 is the same as a line through P_2 and P_1.

Finally, we have to prove that the group operation is associative. We can do this by calculating $P_1 + (P_2 + P_3)$ and $(P_1 + P_2) + P_3$ with P_1, P_2, P_3 points on the curve. Because of the amount of cases, this is a long, arduous and messy calculation. There are different approaches to the proof of associativity in almost every source on elliptic curves. These proofs are definitely not easy and instead of writing out a proof, I would encourage you to look into the references ([8], [9]) for a proof. □

We now know what elliptic curves are, how the points on an elliptic curve form a group and what the group operation for this group is. However, we have only looked at elliptic curves defined over a general field, this means that this field could be infinite. In the field of cryptography we work with computers and since computers cannot handle infinite computations, we can only work with finite groups. To ensure that the group of points on an elliptic curve is finite, we also take a finite field over which the elliptic curve is defined. In the next section we will discuss elliptic curves over finite fields and their properties and see some useful theorems about these curves.

3 Elliptic Curves over Finite Fields

Now that we have a little bit of background in cryptography and elliptic curves, we can dive deeper into the theory of elliptic curves. In cryptography we can only make use of finite groups and so far we have studied the group of points on an elliptic curve over general fields, meaning the group is not necessarily finite. So in this section we will focus on elliptic curves over finite fields $\mathbb{F}_q$, these are fields of order q where q is a power of a prime integer. Since there are only finitely many pairs $(x, y) \in \mathbb{F}_q^2$, the group $E_{A,B}(\mathbb{F}_q)$ is also finite. There are a couple of natural questions about these groups. How many elements does $E_{A,B}(\mathbb{F}_q)$ contain? What is the group structure of $E_{A,B}(\mathbb{F}_q)$? What groups can occur as groups $E_{A,B}(\mathbb{F}_q)$? The goal of this section is to answer these questions. However, before we can do this, there are some definitions we need to discuss.

Definition 3.1. Let K be any field and E an elliptic curve defined over K. Denote the algebraic closure of K by $\overline{K}$. An endomorphism of E is a homomorphism

$$f : E_{A,B}(\overline{K}) \to E_{A,B}(\overline{K})$$

given by rational functions, functions that are quotients of polynomials. This means we have

$$f(x, y) = (g(x, y), h(x, y))$$

for all $(x, y) \in E_{A,B}(\overline{K})$, where g, h are rational functions with coefficients in $\overline{K}$. When f is not defined for a certain point (x, y) we define $f(x, y) = \mathcal{O}$.

Example 3.2. Let E be an elliptic curve given by $y^2 = x^3 + Ax + B$, then $\phi(P) = 2P$ for $P \in E$ is a group homomorphism. However, we also have $\phi(x, y) = (g(x, y), h(x, y))$ with

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

and

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

We can see that both g and h are rational functions, this means that ϕ is an endomorphism. △

For the coming discussion it will be useful to have a standard form for the rational functions in an endomorphism. We will now assume, for simplicity, that an elliptic curve is given by the short Weierstrass equation. Let E be an elliptic curve and let $g(x, y)$ be a rational function. Since every point (x, y) on E satisfies

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

we can replace any even power of y in $g(x, y)$ by a polynomial of x and any odd power of y by y times a polynomial of x. So we can write

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

where every p_i is a polynomial of x. Now we can multiply this by $\frac{p_3(x)-p_4(x)}{p_3(x)-p_4(x)}$ to get

$$g(x, y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}\frac{p_3(x) - p_4(x)}{p_3(x) - p_4(x)} = \frac{q_1(x) + q_2(x)y}{q_3(x) + q_4(x)y^2} = \frac{q_1(x) + q_2(x)y}{q_5(x)},$$

where every q_i is a polynomial and we again replaced y^2 by a polynomial of x. Now let

$$f(x,y) = (g_1(x,y), g_2(x,y))$$

be an endomorphism. This means that $f(x,y)$ is also a homomorphism, it now follows that

$$f(x,-y) = f(-(x,y)) = -f(x,y).$$

So we have

$$g_1(x,-y) = g_1(x,y), \quad g_2(x,-y) = -g_2(x,y).$$

If we now write $g_1(x,y) = \frac{q_1(x)+q_2(x)y}{q_5(x)}$, then it now follows that $q_2(x) = 0$. Next, write $g_2(x,y) = \frac{q_1(x)+q_2(x)y}{q_5(x)}$, now we have that $q_1(x) = 0$. So therefore

$$f(x,y) = (\alpha(x), \beta(x)y)$$

where α, β are rational functions.

Now we have a standard form for an endomorphism f. Assume f is nontrivial. We define the *degree* of f by

$$\deg(f) = \max(\deg(\alpha), \deg(\beta)).$$

We call f *separable* if the derivative of α is not equal to zero.

We are now ready to move on to elliptic curves over finite fields.

Example 3.3. Let E be an elliptic curve over $\mathbb{F}_{13}$ given by $y^2 = x^3 + 3x + 8$. We can find every point on E by going through the elements of $\mathbb{F}_{13}$ and substituting it for x in the equation of the elliptic curve. If the substitution results in a square modulo 13, then we have found two points on the elliptic curve, since every square has two roots. If not, then the element of $\mathbb{F}_{13}$ does not result in a point on the curve. For example, taking $x = 0$ gives us $x^3 + 3x + 8 = 8$, since 8 is not a square modulo 13, $x = 0$ does not result in points on E. Next, taking $x = 1$ gives us $x^3 + 3x + 8 = 12$, since we have

$$5^2 \equiv 12 \bmod 13, \quad \text{and} \quad 8^2 \equiv 12 \bmod 13,$$

it follows that $(1,5)$ and $(1,8)$ are both points on E. Continuing over every element in $\mathbb{F}_{13}$, we eventually get the entire list of points on E:

$$E = \{\mathcal{O}, (1,5), (1,8), (2,3), (2,10), (9,6), (9,7), (12,2), (12,11)\}.$$

We can of course also add these point according to the group law explained in Section 2, keeping in mind that we have to perform each calculation modulo 13. Let $P = (x_1, y_1) = (1,5)$ and $Q = (x_2, y_2) = (12, 11)$, we will now compute $P + Q = (x_3, y_3)$. First we compute

$$c = \frac{y_1 - y_2}{x_1 - x_2} = \frac{5 - 11}{1 - 12} = \frac{-6}{-11} = \frac{7}{2} \equiv 10 \bmod 13.$$

Then we get

$$x_3 = c^2 - x_1 - x_2 = 10^2 - 1 - 12 = 87 \equiv 9 \bmod 13$$

and

$$y_3 = c(x_1 - x_3) - y_1 = 10(1 - 9) - 5 = -85 \equiv 6 \bmod 13.$$

So we have $(1,5) + (12,11) = (9,6)$ in E. △

We are now ready to look at one the most important endomorphisms in the study of elliptic curves over finite fields. Let $\mathbb{F}_q$ be a finite field with algebraic closure $\overline{\mathbb{F}}_q$. The Frobenius map over $\mathbb{F}_q$ is the ring homomorphism $\phi_q : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q$ given by

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

Let $E_{A,B}(\mathbb{F}_q)$ be an elliptic curve, the Frobenius map also works for points $E_{A,B}(\overline{\mathbb{F}}_q)$ as follows

$$\phi_q(x,y) = (x^q, y^q), \quad \phi_q(\mathcal{O}) = \mathcal{O}.$$

This map is critical in the proof of Hasse's theorem, which we will discuss next.

3.1 Hasse Bound

Before we can give the proof of Hasse's theorem, we have to proof some properties of the Frobenius map for points in $E_{A,B}(\mathbb{F}_q)$. In the following let E be an elliptic curve over $\mathbb{F}_q$.

We will first prove that ϕ_q actually maps points onto $E_{A,B}(\overline{\mathbb{F}}_q)$ and that points in $E_{A,B}(\overline{\mathbb{F}}_q)$ are in $E_{A,B}(\mathbb{F}_q)$ precisely when they are fixed by ϕ_q.

Lemma 3.4. *Let $(x,y) \in E_{A,B}(\overline{\mathbb{F}}_q)$. Then $\phi_q(x,y) \in E_{A,B}(\overline{\mathbb{F}}_q)$. Also $(x,y) \in E_{A,B}(\mathbb{F}_q)$ if and only if $\phi_q(x,y) = (x,y)$.*

Proof. We will proof the first part of the lemma for the long Weierstrass equation, since it is not different from the proof for the short Weierstrass equation. Let $(x,y) \in E_(\mathbb{F}_q)$, the group of points on the elliptic curve over $\mathbb{F}_q$ defined by the long Weierstrass equation. We know the following holds

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

with $a_1, ..., a_6 \in \mathbb{F}_q$. Since $\mathbb{F}_q$ is a field of order q, we know that $g^q = g$ and since q is a power of the characteristic of $\mathbb{F}_q$, we know that $(g+h)^q = g^q + h^q$ for all $g, h \in \mathbb{F}_q$. This means that if we take the long Weierstrass equation to the qth power, we get

$$(y^q)^2 + a_1x^qy^q + a_3y^q = (x^q)^3 + a_2(x^q)^2 + a_4x^q + a_6.$$

We see that $\phi_q(x,y) = (x^q, y^q)$ also satisfies the long Weierstrass equation, so we have
$\phi_q(x,y) \in E_{A,B}(\overline{\mathbb{F}}_q)$. This proves the first part.
To prove the second part, take $(x,y) \in E_{A,B}(\mathbb{F}_q)$. Then we have $x, y \in \mathbb{F}_q$. However, by definition $x \in \mathbb{F}_q$ if and only if $\phi_q(x) = x$ for any element of $\overline{\mathbb{F}}_q$. This means that we have $\phi_q(x,y) = (\phi_q(x), \phi_q(y)) = (x,y)$. Now notice that if $\phi_q(x,y) = (x,y)$, then $x, y \in \mathbb{F}_q$, but (x,y) also satisfies the long Weierstrass equation. So we can conclude that $(x,y) \in E_{A,B}(\mathbb{F}_q)$. This proves the second part. □

Now we will prove that ϕ_q is an endomorphism of E.

Lemma 3.5. *Let E be an elliptic curve over $\mathbb{F}_{||}$. Then the Frobenius map ϕ_q is a non-separable endomorphism of E of degree q.*

Proof. Clearly, the map ϕ_q is given by rational functions, so to prove that ϕ_q is an endomorphism, we just have to check that it is a homomorphism. So we have to prove that $\phi_q(P_1) + \phi_q(P_2) = \phi_q(P_1 + P_2)$. This can be done by writing down the formulas defining $P_1 + P_2$ for every case of addition over elliptic curves and raising every formula to the qth power. One fact needed in this calculation is that $(x+y)^q = x^q + y^q$ for all $x, y \in \mathbb{F}_q$, since q is a power of the characteristic of the field. We will not perform these calculations here, an interested reader can find them in the proof of Lemma 2.20 in Washington's book [8]. It is clear that the degree of ϕ_q is q, since the degree of x^q is q. Also we know that $q = 0$ in $\mathbb{F}_q$. This means that $(x^q)' = qx^{q-1} = 0$, so ϕ_q is not separable. □

Lemma 3.6. *Let E be an elliptic curve over $\mathbb{F}_q$, then Ker$(\phi_q - 1) = E_{A,B}(\mathbb{F}_q)$.*

Proof. Since ϕ_q is an endomorphism, $\phi_q - 1$ is also an endomorphism. Now by Lemma 3.4 we know that the points on $E_{A,B}(\mathbb{F}_q)$ are exactly equal to the points fixed by ϕ_q. Let P be an element of $E_{A,B}(\mathbb{F}_q)$, then $\phi_q(P) = P$, or $\phi_q(P) - P = 0$. So the elements of $E_{A,B}(\mathbb{F}_q)$ are precisely the solutions to $(\phi_q - 1)(P) = 0$, this is the same as the kernel of $\phi_q - 1$. □

Lemma 3.7 ([8], Proposition 2.21)**.** *Let f be a non-trivial, separable endomorphism of an elliptic curve E over a field K, then deg$(f) = \#$Ker(f), with Ker(f) the kernel of the homomorphism $f : E_{A,B}(\overline{K}) \to E_{A,B}(\overline{K})$.*

The endomorphism $\phi_q - 1$ is separable as shown in Proposition 2.29 in Washington's book [8]. We can now relate the elliptic curve $E_{A,B}(\mathbb{F}_q)$ to the kernel Ker$(\phi_q - 1)$ and this kernel to the degree of $\phi_q - 1$, we know that the size of $E_{A,B}(\mathbb{F}_q)$ is equal to the degree of $\phi_q - 1$. Now we will find an expression for the degree of $\phi_q - 1$.

Lemma 3.8. *Let $a = q + 1 -$ deg$(\phi_q - 1)$ and let r, s be integers. Then deg$(r\phi_q - s) = r^2 q + s^2 - rsa$.*

Proof. In Proposition 3.16 in Washington's book [8] it is shown that

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

We know that $\deg(\phi_q) = q$ and $\deg(-1) = 1$, so we get

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

as desired. □

Now we are ready to prove Hasse's theorem.

Theorem 3.9 (Hasse's Theorem)**.** *Let E be an elliptic curve over $\mathbb{F}_q$. Then*

$$|q + 1 - \#E_{A,B}(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

Proof. Let a be as defined in Lemma 2.6. We know that $\deg(r\phi_q - s) \geq 0$, because by definition a degree is at least 0. So $r^2 q + s^2 - rsa \geq 0$ for all integers r, s by Lemma 2.6. Let $s \neq 0$, dividing by s^2 gives

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

The set $\left\{\frac{r}{s} \mid r, s \in \mathbb{Z}\right\}$ is dense in $\mathbb{R}$. It now follows that

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

for all $x \in \mathbb{R}$. So the discriminant of this equation, $a^2 - 4q$, is non-positive. It follows that $|a| \leq 2\sqrt{q}$. Applying this to $\phi_q - 1$, this is a separable, non-trivial endomorphism. So $\deg(\phi_q - 1) = \#\text{Ker}(\phi_q - 1) = \#E_{A,B}(\mathbb{F}_q)$ follows from Lemma 3.6 and Lemma 3.7. So we can also use Lemma 3.8, now it follows that $a = q + 1 - \#E_{A,B}(\mathbb{F}_q)$. The desired inequality follows. □

The quantity

$$q - 1 + \#E_{A,B}(\mathbb{F}_q)$$

that we bounded with Hasse's theorem is called the trace or trace of Frobenius of an elliptic curve over $\mathbb{F}_q$.
Hasse's Theorem provides a very useful bound on the size of an elliptic curve over finite fields. In the next section we will discuss the group structure of elliptic curves over a finite field and the groups that can occur as groups $E_{A,B}(\mathbb{F}_q)$.

3.2 Group structure and classification

The goal of this section is to discuss four theorems, the first of which describes the group structure of $E_{A,B}(\mathbb{F}_q)$. And the latter three describe the possible groups that can occur as $E_{A,B}(\mathbb{F}_q)$. Before discussing the first theorem, we will again need some new theory.

Definition 3.10. Let E be an elliptic curve defined over a field K, with algebraic closure $\overline{K}$ and let n be a positive integer. Then the n-torsion points are defined as

$$E[n] = \{P \in E_{A,B}(\overline{K}) \mid nP = \mathcal{O}\}.$$

Notice that if $K = \mathbb{F}_q$, every point on E is a torsion point for some positive integer n.

Theorem 3.11 ([8], Theorem 3.2)**.** *Let E be an elliptic curve defined over $\mathbb{F}_q$ and let n be a positive integer. Then $E[n]$ is either cyclic of isomorphic to the direct sum of two cyclic groups.*

This result will be crucial in the following theorem.

Theorem 3.12. *Let E be an elliptic curve defined over $\mathbb{F}_q$. Then the group of points on E is either cyclic or isomorphic to the direct sum of two cyclic groups.*

Proof. Since $\mathbb{F}_q$ is a finite field, the group of points $E_{A,B}(\mathbb{F}_q)$ is also finite. Let $n := \#E_{A,B}(\mathbb{F}_q)$, now since n is the order of the group, for every $P \in E_{A,B}(\mathbb{F}_q)$ we have $nP = \mathcal{O}$, so

$$E_{A,B}(\mathbb{F}_q) \subseteq E[n].$$

However, we know that $E[n]$ is also finite and either cyclic or isomorphic to the direct sum of two cyclic groups by Theorem 3.11. We can conclude that $E_{A,B}(\mathbb{F}_q)$ is either cyclic itself or is isomorphic to the direct sum of two cyclic groups. □

In the following three theorems we will see what groups can occur. The proofs of these theorems are not in the scope of this thesis, but the theorems themselves are crucial results in the study of elliptic curves over finite fields and they are definitely worth mentioning. In the first one we define the traces for which an elliptic is defined.

Theorem 3.13 ([10], Theorem 4.1)**.** *Let p be a prime and let $q = p^k$ be a power of p for a positive integer k. An elliptic curve E defined over $\mathbb{F}_q$ of trace t is defined for every integer $|t| \leq 2\sqrt{q}$ if and only if t satisfies one of the following:*

1. *$gcd(t, p) = 1$*

2. *k is even and $t = \pm 2\sqrt{q}$*

3. *k is even, $p \not\equiv 1$ mod 3, and $t = \pm\sqrt{q}$*

4. *k is odd, $p = 2$ or 3, and $t = \pm q^{\frac{k+1}{2}}$*

5. *Either p is odd or p is even and $p \not\equiv 1$ mod 4, and $t = 0$.*

From this theorem follows a classification of all possible groups of points on elliptic curves over finite fields. For each of the cases in Theorem 3.13 a group structure has been discovered. Since these cases make up all of the possible pointgroups on elliptic curves over finite fields, this results in a classification of all possible pointgroups. Schoof discovered the classification for cases 2-5. Then Voloch discovered the possible groups for the first case.

Theorem 3.14 ([11], Lemma 4.8)**.** *Let p be a prime and let $q = p^k$ be a power of p for a positive integer k. Let $|t| \leq 2\sqrt{q}$ be a trace satisfying one of the conditions 2-5 from theorem 2.10. Then a list of possible elliptic curves over $\mathbb{F}_q$ with trace t is as follows, where each case is corresponding to the same case in theorem 2.10:*

2. $\mathbb{Z}/(\sqrt{q} \pm 1)\mathbb{Z} \oplus \mathbb{Z}(\sqrt{q} \pm 1)\mathbb{Z}$

3. *Cyclic*

4. *Cyclic*

5. *If $q \equiv 3$ mod 4, then $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/\frac{q+1}{2}\mathbb{Z}$ or cyclic, otherwise cyclic.*

Theorem 3.15 ([12])**.** *Let $q = p^k$ be the power of a prime p for a positive integer k. Let t be the trace of an elliptic curve E over $\mathbb{F}_q$, with $|t| \leq 2\sqrt{q}$ and $gcd(t, p) = 1$. The possible groups of points on $E_{A,B}(\mathbb{F}_q)$ are*

$$\mathbb{Z}/p^{v_p(N)}\mathbb{Z} \bigoplus_{l \neq p} \left(\mathbb{Z}/l^{r_l}\mathbb{Z} \bigoplus \mathbb{Z}/l^{s_l}\mathbb{Z}\right)$$

with N the order of $E_{A,B}(\mathbb{F}_q)$, $v_p(N)$ the largest integer such that $p^{v_p(N)} \mid N$ for any prime p, l a prime, $r_l + s_l = v_l(N)$ and $min(r_l, s_l) \leq v_l(q-1)$.

Combining these last two theorems we have achieved a full classification of possible groups of points on elliptic curves over finite fields. Now our discussion about elliptic curves over finite fields is finished, in the next section we will move on to elliptic curves over $\mathbb{Z}/N\mathbb{Z}$.

4 Elliptic curves over $\mathbb{Z}/N\mathbb{Z}$

This section is based on Section 3 of a paper by Sala and Taufer [13], we will mostly discuss the same theorems that are discussed in that section, building up to the group structure of the group of points on an elliptic curve over $\mathbb{Z}/N\mathbb{Z}$, where $N \geq 2$ is an integer. Also, in this section we will only work with elliptic curves that may be defined by the short Weierstrass equation. Finally, we denote the group of integers modulo an integer $N \geq 2$ consisting of elements which have a multiplicative inverse by $(\mathbb{Z}/N\mathbb{Z})^*$.

We will first introduce a new space in which we can view elliptic curves, the two-dimensional projective space $\mathbb{P}^2$.

Definition 4.1. A tuple of coefficients $(x_1, x_2, ..., x_n)$ with $x_i \in \mathbb{Z}/N\mathbb{Z}$ is called primitive if

$$\gcd(N, x_1, x_2, ..., x_n) = 1.$$

The two-dimensional projective space over $\mathbb{Z}/N\mathbb{Z}$, $\mathbb{P}^2_{\mathbb{Z}/N\mathbb{Z}}$ consists of the equivalence classes of triples (x, y, z) with $x, y, z \in \mathbb{Z}/N\mathbb{Z}$, such that (x, y, z) is primitive. Two triples (x_1, y_1, z_1) and (x_2, y_2, z_2) in $\mathbb{P}^2_{\mathbb{Z}/N\mathbb{Z}}$ are equivalent if there exists a $\lambda \in (\mathbb{Z}/N\mathbb{Z})^*$ such that

$$(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_3).$$

Notice that equivalence classes in $\mathbb{P}^2_{\mathbb{Z}/N\mathbb{Z}}$ only depend on the ratio between x, y and z, so we denote the equivalence class of (x, y, z) by $(x : y : z)$. We can divide $\mathbb{P}^2_{\mathbb{Z}/N\mathbb{Z}}$ into two groups of points, the finite or affine points and the points at infinity. Let $(x : y : z) \in \mathbb{P}^2_K$ be a point, if $\gcd(N, z) \neq 1$, $(x : y : z)$ is a point at infinity. If $\gcd(N, z) = 1$, then $(x : y : z)$ is an affine point.

We also impose the condition that $6 \in (\mathbb{Z}/N\mathbb{Z})^*$, this way the characteristic of the ring is not equal to 2 or 3. This means that working with the short Weierstrass equation is not restrictive as shown in Section 2. We are now ready to define an elliptic curve over $\mathbb{Z}/N\mathbb{Z}$.

Definition 4.2. Let $A, B \in \mathbb{Z}/N\mathbb{Z}$, such that $-(4A^3 + 27B^2) \in (\mathbb{Z}/N\mathbb{Z})^*$. An elliptic curve E over $\mathbb{Z}/N\mathbb{Z}$ is the set of solutions in $\mathbb{P}^2_{\mathbb{Z}/N\mathbb{Z}}$ to the equation

$$y^2z = x^3 + Axz^2 + Bz^3.$$

The group of points on E is the set

$$E_{A,B}(\mathbb{Z}/N\mathbb{Z}) = \left\{(x : y : z) \in \mathbb{P}^2_{\mathbb{Z}/N\mathbb{Z}} \mid y^2z = x^3 + Axz^2 + Bz^3\right\}.$$

The unity element or point at infinity $\mathcal{O}$ is the point $(0 : 1 : 0)$. Denote the affine points on the curve by E^a and the points at infinity by E^∞.

Example 4.3. Let E be an elliptic curve over $\mathbb{Z}/8\mathbb{Z}$ given by $y^2z = x^3 + xz^2 + z^3$. Consider the points at infinity, these are points such that $\gcd(N, z) \neq 1$. There are several elements $z \in \mathbb{Z}/8\mathbb{Z}$ such that z is not coprime with 8, namely 0, 2, 4 and 6. This shows that there are several points at infinity on this curve. So there can be multiple points at infinity when we consider elliptic curves over commutative rings instead of fields. △

The formulas used in the group law of an elliptic curve over $\mathbb{Z}/N\mathbb{Z}$ reduce down to the formulas used in the group law when working with fields, we saw these formulas in Section 2. The identity element is still $\mathcal{O}$ and inverses are defined as $-(x : y : z) = (x : -y : z)$. However, adding two points now requires complicated formulas, for a detailed discussion of the group law see Section 2.11 of the book by Washington [8].

In the next theorem we will see that to give the group structure of the group of points on elliptic curves over $\mathbb{Z}/N\mathbb{Z}$, we will only need to consider the point group of elliptic curves over $\mathbb{Z}/p^e\mathbb{Z}$, with p a prime and e a positive integer.

Theorem 4.4. *Let N_1 and N_2 be coprime integers and let E be an elliptic curve defined over $\mathbb{Z}/N_1N_2\mathbb{Z}$. Then there exists a group isomorphism*

$$E_{A,B}(\mathbb{Z}/N_1N_2\mathbb{Z}) \simeq E_{A,B}(\mathbb{Z}/N_1\mathbb{Z}) \oplus E_{A,B}(\mathbb{Z}/N_2\mathbb{Z}).$$

Proof. According to the Chinese Remainder Theorem there is a bijection

$$\mathbb{Z}/N_1N_2\mathbb{Z} \simeq \mathbb{Z}/N_1\mathbb{Z} \oplus \mathbb{Z}/N_2\mathbb{Z}$$

such that

$$x \bmod N_1N_2 \longleftrightarrow (x \bmod N_1, x \bmod N_2).$$

This means that there is a bijection between triples in $\mathbb{Z}/N_1N_2\mathbb{Z}$ and pairs of triples in $\mathbb{Z}/N_1\mathbb{Z}$ and $\mathbb{Z}/N_2\mathbb{Z}$. If a triple (x, y, z) in $\mathbb{Z}/N_1N_2\mathbb{Z}$ is primitive, then $\texttt{gcd}(N_1N_2, x, y, z) = 1$. Then we also have $\texttt{gcd}(N_1, x, y, z) = 1$ and $\texttt{gcd}(N_2, x, y, z)$. This means that primitive triples in $\mathbb{Z}/N_1N_2\mathbb{Z}$ correspond to pairs of primitive triples in $\mathbb{Z}/N_1\mathbb{Z}$ and $\mathbb{Z}/N_2\mathbb{Z}$. Finally, we know that

$$y^2z \equiv x^3 + Axz^2 + Bz^3 \bmod N_1N_2$$

if and only if

$$y^2z \equiv x^3 + Axz^2 + Bz^3 \bmod N_1, \quad y^2z \equiv x^3 + Axz^2 + Bz^3 \bmod N_2.$$

We can now conclude that there is a bijection

$$\phi : E_{A,B}(\mathbb{Z}/N_1N_2\mathbb{Z}) \to \mathbb{Z}/N_1\mathbb{Z} \oplus \mathbb{Z}/N_2\mathbb{Z}.$$

Now to prove the theorem, we just have to prove that ϕ is a group homomorphism. Let $P, Q \in E_{A,B}(\mathbb{Z}/N_1N_2\mathbb{Z})$ and $P + Q = R$. The calculations done to get R are modulo N_1N_2, now when reducing the calculations to modulo N_1 and modulo N_2 we do have to watch out. Since reducing a calculation modulo N_1N_2 can lead to differences in the calculations modulo N_1 and the calculations modulo N_2. However, when we write down the calculations modulo N_1 and modulo N_2 we do always get the same result. We now have $P \bmod N_1 + Q \bmod N_1 = R \bmod N_1$ and $P \bmod N_2 + Q \bmod N_2 = R \bmod N_2$. We conclude that $\phi(P + Q) = \phi(P) + \phi(Q)$, so ϕ is a group homomorphism and thus ϕ is group isomorphism. □

In the remainder of this section, we will focus on the group of points of elliptic curves over $\mathbb{Z}/p^e\mathbb{Z}$, since we can now write the group of points on an elliptic curve over $\mathbb{Z}/N\mathbb{Z}$ as the direct sum of groups of points on elliptic curves over $\mathbb{Z}/p^e\mathbb{Z}$, where p ranges over the prime divisors of N and e is the maximum integer such that p^e divides into N.

In [14] Lange and Rupert define a sum operation such that for every proper ideal I of $\mathbb{Z}/N\mathbb{Z}$ there is a well-defined group homomorphism

$$\pi : E_{A,B}(\mathbb{Z}/N\mathbb{Z}) \to E_{A',B'}((\mathbb{Z}/N\mathbb{Z})/I). \tag{4.1}$$

We will use this group homomorphism in the next lemma, where we will see that affine points and points at infinity on such elliptic curves have prescribed representatives.

Lemma 4.5. *Let $P \in E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$, now there are two cases*

1. *If $P \in E^a$, then there are $x, y \in \mathbb{Z}/p^e\mathbb{Z}$ such that*
$$P = (x : y : 1).$$
2. *If $P \in E^\infty$, then there are $x, z \in p(\mathbb{Z}/p^e\mathbb{Z})$ such that*
$$P = (x : 1 : z)$$
where $p(\mathbb{Z}/p^e\mathbb{Z})$ is the principal ideal generated by p.

Proof. First set $P = (x' : y' : z')$. If $P \in E^a$, then $\gcd(p^e, z') = 1$. This is the case when z' and p are coprime. Now we can divide by z' to get $P = (\frac{x'}{z'} : \frac{y'}{z'} : 1)$ with $\frac{x'}{z'}, \frac{y'}{z'} \in \mathbb{Z}/p^e\mathbb{Z}$. If $P \in E^\infty$, then $\gcd(p^e, z') \neq 1$ and since p is a prime number, this means that $p \mid z'$. So $\pi(z') = \mathcal{O} = (0 : 1 : 0)$ with π as discussed above. We see that $p \mid x'$ while $p \nmid y'$. Therefore we can divide by y' to get $P = (\frac{x'}{y'} : 1 : \frac{z'}{y'})$ with $\frac{x'}{y'}, \frac{z'}{y'} \in p(\mathbb{Z}/p^e\mathbb{Z})$. □

Lenstra determined the size of elliptic curves $E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ in [15] as described in the following lemma for which we will omit the proof.

Lemma 4.6. *Let*
$$\pi : E_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \to E_{A,B}(\mathbb{F}_p)$$
be the canonical projection. Now for every point $P \in E_{A,B}(\mathbb{F}_p)$ we have
$$|\pi^{-1}(P)| = p^{e-1}.$$
This has two consequences

1. *The size of $E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ can be expressed in the size of $E_{A,B}(\mathbb{F}_p)$ as follows, $|E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})| = p^{e-1}|E_{A,B}(\mathbb{F}_p)|$.*
2. *The kernel of π is a subgroup of $E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ and we have $|Ker(\pi)| = p^{e-1}$.*

In the next lemma we will establish a relation that the coordinates of the points at infinity satisfy. We will use this relation later on to get an approximation of the sum of two points at infinity.

Lemma 4.7. *Let E be an elliptic curve over $\mathbb{Z}/p^e\mathbb{Z}$. Then there exists a polynomial $f \in \mathbb{Z}[x]$ of degree at most $e - 1$ such that for every $P \in E^\infty$ there is an $x' \in p(\mathbb{Z}/p^e\mathbb{Z})$ which satisfies*
$$P = (x' : 1 : f(x')).$$

Proof. We know from Lemma 4.5 that points in E^∞ have $(x' : 1 : z')$ as their representative, with $x', z' \in p(\mathbb{Z}/p^e\mathbb{Z})$, so x' and z' are divisible by p. As these points are elements of $E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$, they satisfy
$$z' \equiv x'^3 + Ax'z'^2 + Bz'^3 \bmod p^e.$$
Now we will use the above equation to recursively define a sequence of polynomials in $\mathbb{Z}[x, z]$ as follows
$$F_0(x, z) = x^3 + Axz^2 + Bz^3, \quad F_i(x, z) = F_{i-1}(x, F_0(x, z))$$

for all $i \in \mathbb{Z}_{\geq 1}$. We will now prove by induction that

$$z' \equiv F_i(x', z') \bmod p^e$$

for all $i \in \mathbb{Z}_{\geq 0}$. We have already seen that by definition this statement is true for $i = 0$. Now assume that $z' \equiv F_i(x', z') \bmod p^e$ for an $i \in \mathbb{Z}_{\geq 1}$. We have $F_{i+1}(x', z') = F_i(x', F_0(x', z'))$, however $z' \equiv F_0(x', z') \bmod p^e$. So we have

$$F_{i+1}(x', z') = F_i(x', F_0(x', z')) \equiv F_i(x', z') \bmod p^e.$$

Therefore $z' \equiv F_{i+1}(x', z') \bmod p^e$ and the induction is complete, we conclude that

$$z' \equiv F_i(x', z') \bmod p^e$$

for every $i \in \mathbb{Z}_{\geq 0}$. Since we obtain every F_i for $i \geq 1$ by substituting every z in F_{i-1} with $F_0(x, z)$, in which all terms have a degree of 3, the total degree of the terms involving z in strictly increasing in the sequence $\{F_i\}_{i \in \mathbb{Z}_{\geq 0}}$. Also notice that every F_i has at least one term that is independent of z, so we can write every $F_i(x, z)$ as $F_i(x, z) = f_i(x) + g_i(x, z)$, where f_i and g_i are polynomials. While the degree of g_i is strictly increasing with increasing i, the degree of f_i is not. This means that there is an $M \in \mathbb{Z}_{\geq 0}$ such that

$$F_M(x, z) = f_M(x) + g_M(x, z)$$

with $\deg(g_M) \geq e$ and $\deg(f_M) < e$. Because both x' and z' are divisible by p and $\deg(g) \geq e$ it follows that

$$z' \equiv F_M(x', z') \bmod p^e \equiv f(x') + g(x', z') \bmod p^e \equiv f(x') \bmod p^e.$$

This means that f is a polynomial such that

$$P = (x' : 1 : z') = (x' : 1 : f(x')),$$

so $f_M \in \mathbb{Z}[x]$ is the required polynomial. □

In the next Lemma we will describe the first-order approximation of the sum of two points at infinity.

Lemma 4.8. *Let E be an elliptic curve over $\mathbb{Z}/p^e\mathbb{Z}$ with point group $E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ and $f \in \mathbb{Z}[x]$ be the polynomial as in Lemma 4.7. Also let $P, Q \in E^\infty$ with*

$$P = (x_1 : 1 : f(x_1)), \quad Q = (x_2 : 1 : f(x_2))$$

and let $e_1 = v_p(x_1)$ and $e_2 = v_p(x_2)$. Denote

$$P + Q = (x_3 : 1 : f(x_3)),$$

then

$$x_3 \equiv x_1 + x_2 \bmod p^{5min(e_1, e_2)}.$$

Proof. Let π be the group homomorphism defined in (4.1). Since π is a group homomorphism, we have $\pi(P + Q) = \pi(P) + \pi(Q)$. Because $P, Q \in E^\infty$, we have $\pi(P) = \pi(Q) = \mathcal{O}$, so $\pi(P + Q) = \mathcal{O} + \mathcal{O} = \mathcal{O}$. This means that $P + Q$ is also a point at infinity. Bosma and Lenstra proved that we can use the addition law corresponding to $(0 : 1 : 0)$ to compute $P + Q$ [[16], Theorem 2]. The formulas for this addition law are described in Section 2.3 of the paper by

Sala and Taufer [13]. Using these formulas to compute $P+Q$ modulo $p^{5\min(e_1,e_2)}$, so modulo monomials in x_1 and x_2 of total degree at least 5, gives us

$$P+Q=(x_1+x_2:1+3Ax_1^2x_2^2:(x_1+x_2)^3).$$

We won't write down the entire computation here, since it is quite long. Now consider $1-3Ax_1^2x_2^2 \in \mathbb{Z}/p^{5\min(e_1,e_2)}\mathbb{Z}$, then $P+Q$ is equal to $(1-3Ax_1^2x_2^2)(P+Q)$. Performing this computation, again modulo monomials in x_1 and x_2 of total degree at least 5, gives us

$$(1-3Ax_1^2x_2^2)(P+Q)=(x_1+x_2:1:(x_1+x_2)^3) \bmod p^{5\min(e_1,e_2)}.$$

This concludes the proof. □

Before moving on to the next theorem, we need some theory.

Definition 4.9. A short exact sequence of groups

$$0 \to G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} G_3 \to 0,$$

where 0 is the trivial group, is a collection of three groups G, H, K together with two group homomorphisms ϕ_1, ϕ_2, such that

1. The group homomorphism ϕ_1 is an injection.
2. The group homomorphism ϕ_2 is a surjection.
3. The kernel of ϕ_2 is equal to the image of ϕ_1.

A short exact sequence is called split if it is isomorphic to the sequence where the middle term is the direct sum of the outer terms. Meaning that there is a group isomorphism $\psi: G_2 \to G_1 \oplus G_3$ such that $\psi \circ \phi_1$ is the canonical inclusion and there is a function $f: G_1 \oplus G_3 \to G_3$ such that $f \circ \psi$ is equal to ϕ_2.

We can now move on to the next theorem where we provide a structure for elliptic curves over $\mathbb{Z}/p^e\mathbb{Z}$.

Theorem 4.10. *Let $f \in \mathbb{Z}[x]$ be the polynomial derived from $E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ as in Lemma 3.6. Then*

$$0 \to \langle (p:1:f(p)) \rangle \overset{\iota}{\hookrightarrow} E_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \xrightarrow{\pi} E_{A,B}(\mathbb{F}_p) \to 0,$$

where ι is the inclusion and π is the canonical projection, is a short exact sequence of groups.

Proof. By definition the inclusion ι is injective. Since π is the canonical projection, we know that π is a surjective group homomorphism and $|\mathrm{Ker}(\pi)| = p^{e-1}$ by Lemma 4.6. So to prove the sequence is a short exact sequence, it suffices to show that the kernel of π is equal to the image of ι. Let $P=(p:1:f(p))$. Then, because $P \in \mathrm{Ker}(\pi)$, we only have to show that the order of P is p^{e-1}. Using Lemma 4.7 we see that P lies over $\mathcal{O} \in \mathbb{F}_p$ and since $\mathrm{Ker}(\pi)$ is a p-group, the order of P is a power of p. We will now prove that

$$p^\epsilon P = (x':1:f(x')), \quad \text{and} \quad v_p(x') = \epsilon + 1$$

by induction on $0 \le \epsilon \le e-1$. This would mean that the minimal ϵ such that $x' \equiv 0 \bmod p^e$ is $\epsilon = e-1$, thus proving the theorem. First consider the case $\epsilon = 0$. This gives

$$p^0P = P = (p:1:f(p)), \quad \text{and} \quad v_p(p) = 1 = \epsilon + 1,$$

so the statement holds for $\epsilon = 1$. We now assume the statement is true for ϵ. Then we have to prove it is true for $\epsilon + 1$. The case $\epsilon + 1$ with the induction hypothesis gives us

$$p^{\epsilon+1}P = p(p^{\epsilon}P) = p(x' : 1 : f(x')), \quad \text{and} \quad v_p(x') = \epsilon + 1.$$

We need to prove that the p-adic valuation of the first component of $p(x' : 1 : f(x'))$ is $v_p(x')+1$. To prove this we will use Lemma 3.7. With induction on $1 \leq n \leq p-1$ and Lemma 3.7 we have

$$(x' : 1 : f(x')) + (nx' : 1 : f(nx')) = (x_2 : 1 : f(x_2)),$$

such that

$$x_2 \equiv (n+1)x' \bmod p^{5(\epsilon+1)}.$$

We see that the case $n = p-1$ gives us the same point as in the case $\epsilon + 1$ in the original induction, and now

$$x_2 \equiv px' \bmod p^{5(\epsilon+1)}.$$

So we can conclude that the p-adic valuation of the first coordinate of $p(x' : 1 : f(x'))$ is $v_p(x') + 1$ and that proves the original induction and thus the theorem. □

Definition 4.11. We call an elliptic curve E over the field $\mathbb{F}_p$ anomalous when the order of the group of points on E is equal to p, so $|E_{A,B}(\mathbb{F}_p)| = p$.

From the above proof together with Lemma 4.6 we can conclude that the set of points at infinity of any elliptic curve over $\mathbb{Z}/p^e\mathbb{Z}$ is a $\mathbb{Z}/p^e\mathbb{Z}$-torsor according to the action of standard multiplication. This means that $\langle (p : 1 : f(p)) \rangle \simeq \mathbb{Z}/p^{e-1}\mathbb{Z}$. We can use this to figure out the group structure of elliptic curves over $\mathbb{Z}/p^e\mathbb{Z}$ when the canonical projection of these curves is not anomalous. However, we do need the following lemma.

Lemma 4.12 ([17], Section 2.2). *Let*

$$0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$$

be a short exact sequence of abelian groups. Then this sequence is split if there exists a group homomorphism $p : B \to A$ such that $p \circ i = id_A$.

Now we are ready to prove the group structure of the group of points on elliptic curves over $\mathbb{Z}/p^e\mathbb{Z}$ when the canonical projection of these curves is not anomalous.

Corollary 4.13. *Let E be an elliptic curve defined over $\mathbb{Z}/p^e\mathbb{Z}$ such that the projection of these curves in not anomalous, i.e. $|E_{A,B}(\mathbb{F}_p)| \neq p$. Then we have the following group isomorphism*

$$E_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \simeq E_{A,B}(\mathbb{F}_p) \oplus \mathbb{Z}/p^{e-1}\mathbb{Z}.$$

Proof. To prove this, we just have to prove that the short exact sequence from Theorem 3.9 is split. By Lemma 4.12 we just have to prove that there exists a group homomorphism $\phi : E_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \to \langle (p : 1 : f(p)) \rangle$ such that $\phi \circ \iota$ is the identity on $\langle (p : 1 : f(p)) \rangle$. Denote $q = |E_{A,B}(\mathbb{F}_p)|$, then $q \neq p$ is inside the Hasse bound of p, so $\gcd(p, q) = 1$. This means that there exists a $k \in \mathbb{Z}$ such that

$$k \equiv 0 \bmod q, \quad \text{and} \quad k \equiv 1 \bmod p^{e-1}.$$

It follows from Theorem 4.10 that $E^{\infty}_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) = \pi^{-1}(\mathcal{O}) = \langle (p : 1 : f(p)) \rangle$. Combining this fact with the fact that $k \equiv 0 \bmod q$ we get that the map of multiplication by k

$$\phi : E_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \xrightarrow{\cdot k} \langle (p : 1 : f(p)) \rangle$$

is a well-defined group homomorphism. Now we just have to prove that $\phi \circ \iota$, where ι is the canonical inclusion, is equal to the identity on $\langle(p:1:f(p))\rangle$. Since ι is the canonical inclusion, it suffices to prove that $\langle(p:1:f(p))\rangle$ is fixed under ϕ. However, since $k \equiv 1 \bmod p^{e-1}$ we can directly conclude that $\langle(p:1:f(p))\rangle$ is fixed under ϕ. This concludes the proof. □

We now have the group structure of $E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ when the group $E_{A,B}(\mathbb{F}_p)$ is not anomalous. However to attain the group structure of the group of points on elliptic curves over $\mathbb{Z}/N\mathbb{Z}$ we also need to know the group structure when $E_{A,B}(\mathbb{F}_p)$ is anomalous. By Theorem 4.10 we know that $E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ contains a cyclic subgroup of order p^{e-1}. This means that either the group itself is cyclic, so

$$E_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \simeq \mathbb{Z}/p^e\mathbb{Z}$$

or the sequence from Theorem 4.10 is split, then we have

$$E_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \simeq \mathbb{F}_p \oplus \mathbb{Z}/p^{e-1}\mathbb{Z}.$$

Note that both cases do occur as seen in the following example.

Example 4.14 ([13], page 14)**.** Let E be an elliptic curve defined over $\mathbb{Z}/13^2\mathbb{Z}$. When E is given by $y^2z = x^3 + 7xz^2 + 3z^3$ we have

$$E_{7,3}(\mathbb{Z}/13^2\mathbb{Z}) \simeq \langle(0:61:1)\rangle.$$

However, when E is given by $y^2z = x^3 + xz^2 + 6z^3$ we have

$$E_{1,6}(\mathbb{Z}/13^2\mathbb{Z}) \simeq \langle(2:4:1)\rangle \oplus \langle(13:1:0)\rangle.$$

Thus we see that both cases occur. △

Now we are ready to prove the group structure theorem.

Theorem 4.15. *Let N be a positive integer and A, B integers such that $\Delta_{A,B}$ is coprime to N. Then $E_{A,B}(\mathbb{Z}/N\mathbb{Z})$ has the following group structure*

$$E_{A,B}(\mathbb{Z}/N\mathbb{Z}) \simeq \bigoplus_{\substack{p|N \\ |E_{A,B}(\mathbb{F}_p)|\neq p}} E_{A,B}(\mathbb{F}_p) \oplus \mathbb{Z}/p^{v_p(N)-1}\mathbb{Z} \oplus \bigoplus_{\substack{p|N \\ |E_{A,B}(\mathbb{F}_p)|=p}} G_p.$$

Every G_p is either $\mathbb{Z}/p^{v_p(N)}$ or $\mathbb{F}_p \oplus \mathbb{Z}/p^{v_p(N)-1}\mathbb{Z}$.

Proof. Firstly, we know from Theorem 4.4 that

$$E_{A,B}(\mathbb{Z}/N\mathbb{Z}) \simeq \bigoplus_{p|N} E_{A,B}(\mathbb{Z}/p^{v_p(N)}\mathbb{Z}).$$

For every p such that $|E_{A,B}(\mathbb{F}_p)| \neq p$, we saw in Corollary 3.11 that

$$E_{A,B}(\mathbb{Z}/e^{v_p(N)}\mathbb{Z}) \simeq E_{A,B}(\mathbb{F}_p) \oplus \mathbb{Z}/p^{v_p(N)-1}\mathbb{Z}.$$

For every p such that $E_{A,B}(\mathbb{F}_p)$ is anomalous, we saw in the above discussion that

$$E_{A,B}(\mathbb{Z}/p^{v_p(N)}\mathbb{Z}) \simeq \mathbb{F}_p \oplus \mathbb{Z}/p^{v_p(N)-1}\mathbb{Z}, \quad \text{or} \quad E_{A,B}(\mathbb{Z}/p^{v_p(N)}\mathbb{Z}) \simeq \mathbb{Z}/p^{v_p(N)}\mathbb{Z},$$

so we have

$$G_p \simeq \mathbb{F}_p \oplus \mathbb{Z}/p^{v_p(N)-1}\mathbb{Z}, \quad \text{or} \quad G_p \simeq \mathbb{Z}/p^{v_p(N)}\mathbb{Z}.$$

Now we have considered all cases and the prove is complete. □

With Theorem 4.15 we have accomplished the goal of this section, giving the group structure of the group of points on elliptic curves over $\mathbb{Z}/N\mathbb{Z}$. In the next section we will discuss an attack on the elliptic curve DLP in the case where the underlying elliptic curve is anomalous, based on the group structure in this section.

5 An attack on anomalous ECDLP

In this final section we will discus the elliptic curve discrete logarithm problem (ECDLP) and an attack on the ECDLP when the underlying elliptic curve is anomalous 4.11.

5.1 Elliptic Curve Discrete Logarithm Problem

The ECDLP is the same as the general DLP, but now the underlying group is the group of points on an elliptic curve. There are cases where the ECDLP is computationally easy to solve, but in general the fastest known algorithms to solve the ECDLP are fully exponential. An example of such an algorithm when the underlying curve is defined over the field $\mathbb{F}_p$ for a prime p, is Pollard's Rho algorithm [18] with a running time of $\mathcal{O}(\sqrt{p})$. Since the ECDLP is a computationally hard problem, there are a number of cryptographic systems based on this problem. Examples are the elliptic curve Diffie-Hellman key exchange, the elliptic curve integrated encryption scheme and the elliptic curve digital signature algorithm. Currently elliptic curve cryptography is widely used. We will take a look at an example of the ECDLP before moving on to the attack.

Example 5.1. Let E be an elliptic curve defined over $\mathbb{Z}/7\mathbb{Z}$ given by $A = 1$ and $B = 1$. Then one can check that $P = (2 : 2 : 1)$ and $Q = (0 : 6 : 1)$ are points on the curve. Now we want to find an integer k such that $Q = kP$. By adding P to itself repeatedly and checking if the result equals Q we see that $Q = 3P$. So the solution to this DLP is 3. △

5.2 An isomorphism attack

This section will follow Section 5 of the paper by Sala and Taufer [13]. In this section we will discuss an isomorphism attack on the ECDLP when the underlying elliptic curve is anomalous based on the group structure developed in Section 4. We will first introduce an explicit group homomorphism in the next theorem.

Theorem 5.2. *Let E be an elliptic curve over $\mathbb{Z}/p^e\mathbb{Z}$ with p a prime and $e \geq 2$ an integer such that the group of points $E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ is cyclic and has order p^e. Then there is a well-defined surjective group homomorphism*

$$\phi : E_{A,B}(\mathbb{Z}/p^e\mathbb{Z}) \to \mathbb{F}_p,$$

given by

$$\phi : P \mapsto \frac{1}{p^{e-1}} \frac{(p^{e-1}P)_x}{(p^{e-1}P)_y},$$

where $(p^{e-1}P)_x$ and $(p^{e-1}P)_y$ are the first and second coordinates of $p^{e-1}P$ respectively. Moreover the kernel of ϕ is

$$Ker(\phi) = \langle (p : 1 : f(p)) \rangle,$$

where f is the function defined in Lemma 4.7.

Proof. Let $P \in E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be a point on the elliptic curve, since the order of $E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ is p^e, the order of every point is a divisor of p^e. So $p^eP = \mathcal{O}$ for every $P \in E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$. This means that the point $p^{e-1}P$ is a p-torsion point of $E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$. Since $p(p^{e-1}P) = \mathcal{O}$ we have

$$p^{e-1}P = (x : 1 : f(x)), \quad v_p(x) \geq e - 1$$

by the proof of Theorem 4.10. This means that

$$\phi(P) = \frac{1}{p^{e-1}} \frac{(p^{e-1}P)_x}{(p^{e-1}P)_y} = \frac{1}{p^{e-1}} \frac{x}{1} = \frac{x}{p^{e-1}}$$

is well-defined since $v_p(x) \geq e-1$. Let $G \in E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ be a generator of the group of points on E and denote $p^{e-1}G = (x' : 1 : f(x'))$. Also, let $k \in \mathbb{Z}$ be an integer. Then we have

$$kp^{e-1}G = k(x' : 1 : f(x')).$$

Furthermore by induction on 4.8 we have

$$k(x' : 1 : f(x')) = (x'' : 1 : f(x'')), \quad x'' \equiv kx' \bmod p^{5(e-1)}.$$

Also since G is a generator it follows that for every $e \geq 2$, $p^{e-1}G \in \langle (p^{e-1} : 1 : 0) \rangle$, this means that

$$(x'' : 1 : f(x'')) = (kx' : 1 : f(kx')).$$

Now because $kp^{e-1}G = (kx' : 1 : f(kx'))$ the following equality follows

$$\phi(kG) = \frac{kx'}{p^{e-1}} = k\frac{x'}{p^{e-1}} = k\phi(G).$$

This means that ϕ is a group homomorphism. Now it also follows that $\phi(P) = 0$ exactly when $P = pkG$ for every integer k, so

$$\text{Ker}(\phi) = \{pkG \mid k \in \mathbb{Z}\}.$$

Since G is a generator for the group of points on E it follows that

$$\{pkG \mid k \in \mathbb{Z}\} = \langle (p : 1 : f(p)) \rangle.$$

Now we just have to prove that ϕ is surjective. We know that the image of ϕ is a subgroup of $\mathbb{F}_p$. However, since the order of $\mathbb{F}_p$ is p, which is a prime, the order of every subgroup of $\mathbb{F}_p$ is either 1 or p. This means that the only subgroups of $\mathbb{F}_p$ are the trivial subgroup and the entire group. However, since the kernel of ϕ is not equal to $E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$, the image of ϕ is not the trivial subgroup. So the image of ϕ is $\mathbb{F}_p$, thus ϕ is surjective. □

From the group homomorphism in Theorem 4.1 we can derive a group isomorphism.

Corollary 5.3. *Let E be an elliptic curve over $\mathbb{Z}/p^e\mathbb{Z}$ with p a prime and $e \geq 2$ an integer such that the group of points $E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})$ is cyclic and has order p^e. Then there is a well-defined group isomorphism as follows*

$$\phi' \circ \pi'^{-1} : E_{A',B'}(\mathbb{F}_p) \to \mathbb{F}_p,$$

where ϕ' is a group isomorphism induced from the group homomorphism from Theorem 4.1 and π' is a group isomorphism induced from the canonical projection. Also $A', B' \in \mathbb{F}_p$ are elements equivalent to $A, B \in \mathbb{Z}/p^e\mathbb{Z}$.

Proof. Both the canonical projection and ϕ induce a group isomorphism as we will see. Since π is surjective, applying the First Isomorphism Theorem to Theorem 4.10 gives us the group isomorphism

$$\pi' : E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})/\langle (p : 1 : f(p)) \rangle \simeq E_{A,B}(\mathbb{F}_p).$$

Similarly, we know that ϕ is surjective, so applying the First Isomorphism Theorem to Theorem 5.2 gives us the group isomorphism

$$\phi' : E_{A,B}(\mathbb{Z}/p^e\mathbb{Z})/\langle(p : 1 : f(p))\rangle \simeq \mathbb{F}_p.$$

Now we can compose ϕ' with π'^{-1} to get

$$\phi' \circ \pi'^{-1} : E_{A',B'}(\mathbb{F}_p) \to \mathbb{F}_p,$$

which is also a group isomorphism since it is a composition of group isomorphisms. □

Definition 5.4. Let P be a point on an elliptic curve E defined over $\mathbb{F}_p$. Let E' be an elliptic curve such that the group of points on E' reduces to the group of points on E modulo p. This is for example the case when E' is defined over $\mathbb{Z}/p^e\mathbb{Z}$ with $e \geq 2$. A point $P^\uparrow$ on E' is called the lift of P when $P^\uparrow$ reduces to P modulo p. Note that a point can have multiple lifts.

We can use the group homomorphism ϕ from Theorem 4.1 to perform an attack on the ECDLP based on the isomorphism from Corollary 5.3. To compute the discrete logarithm of two points P and Q with this attack, we first have to compute lifts of P and Q, then apply ϕ to the lifts and finally divide the results. The computational complexity of the first and the last step is negligible and the total complexity depends on the cost of computing ϕ. Since computing ϕ can be done in polynomial time, the attack also has a polynomial running time.

Example 5.5 ([13], Example 28)**.** Let E be an elliptic curve defined over $\mathbb{F}_p$ given by

$$p = 730750818665451459112596905638433048232067471723,$$

$$A = 425706413842211054102700238164133538302169176474,$$

$$B = 203362936548826936673264444982866339953265530166.$$

Now let $P, Q \in E_{A,B}(\mathbb{F}_p)$ be

$$P = (1 : 203362936548826936673264444982866339953265530166 : 1),$$

$$Q = (3 : 38292783053156441019740319553956376819943854515 : 1).$$

We want to compute the discrete logarithm $Q = kP$. Now we need to compute any lifts $P^\uparrow, Q^\uparrow \in E_{A,B}(\mathbb{Z}/p^2\mathbb{Z})$, let these lifts be

$$P^\uparrow = (1 : P_y + p\frac{1 + A + B - P_y^2}{2pP_y} : 1),$$

$$Q^\uparrow = (1 : Q_y + p\frac{27 + 3A + B - Q_y^2}{2pQ_y} : 1).$$

One can check that the group of points on E is cyclic. We can now apply the group homomorphism ϕ from Theorem 5.2 to these lifts to get

$$\phi(P^\uparrow) = 343088892565802863386490109374548044078624360215,$$

$$\phi(Q^\uparrow) = 470974712001084540433398653921983741661987449793.$$

Now since $\phi(p^\uparrow)$ and $\phi(Q^\uparrow)$ live in $\mathbb{F}_p$ and there is a group isomorphism between $E_{A,B}(\mathbb{F}_p)$ and $\mathbb{F}_p$ as seen in Corollary 5.3, dividing $\phi(Q^\uparrow)$ by $\phi(P^\uparrow)$ modulo p gives us k:

$$k = \frac{\phi(Q^\uparrow)}{\phi(P^\uparrow)} \bmod p = 113690975836469390483838646646828917131453128585.$$

So we have now solved the discrete logarithm problem for P and Q. △

6 Further reading and open problems

In this section we will first provide some pointers to further reading for readers who are interested in elliptic curves and want to study them in more detail. After that we will discuss some open problems relating to this thesis.

Further reading

The research area of elliptic curves is vast and very actively studied. Readers interested in elliptic curve cryptography might find it interesting to study algorithms like Lenstra's elliptic curve factorisation algorithm [19]. This is an algorithm that uses elliptic curves over $\mathbb{Z}/N\mathbb{Z}$ for the prime-factorisation of integers. Other interesting cryptographic uses of elliptic curves are public key cryptosystems, these may make use of elliptic curves over $\mathbb{Z}/N\mathbb{Z}$, like proposed by Vanstone et al. [20], or of elliptic curves over finite fields, like proposed by Koblitz [21] and Miller [22].

Readers interested in more general elliptic curve theory may find it interesting to study elliptic curves defined over fields other than the ones discussed in this thesis, like the rational numbers or the complex numbers. Both of these areas open up a whole new world of concepts and theorems. References readers could look at are Chapters 8 and 9 of [8] or [23].

Open problems

A natural open problem arising from this thesis would be the complete classification of the group of points on elliptic curves over $\mathbb{Z}/N\mathbb{Z}$. Such a classification has been achieved for the group of points on elliptic curves over finite fields as we discussed with Theorems 3.14 and 3.15. In this thesis we described the group structure of the group of points on elliptic curves over $\mathbb{Z}/N\mathbb{Z}$, but a complete classification of such groups is still an open problem.

Another interesting open problem is the existence of an efficient algorithm to solve the ECDLP. Currently, it is not proven that there is no efficient algorithm to solve the ECDLP. The open problem is either finding an efficient algorithm to solve the ECDLP or proving that there exists no such algorithm.

References

[1] Nan Li. "Research on Diffie-Hellman key exchange protocol". In: vol. 4. May 2010, pp. V4–634. DOI: 10.1109/ICCET.2010.5485276.

[2] Yiannis Tsiounis and Moti Yung. "On the security of ElGamal based encryption". In: *International Workshop on Public Key Cryptography*. Springer. 1998, pp. 117–134.

[3] A Uma Maheswari and Prabha Durairaj. "MODIFIED SHANKS'BABY-STEP GIANT-STEP ALGORITHM AND POHLIG-HELLMAN ALGORITHM". In: *International Journal of Pure and Applied Mathematics* 118.10 (2018), pp. 47–56.

[4] R Padmavathy and Chakravarthy Bhagvati. "Discrete logarithm problem using index calculus method". In: *Mathematical and computer modelling* 55.1-2 (2012), pp. 161–169.

[5] Thorsten Kleinjung and Benjamin Wesolowski. "Discrete logarithms in quasi-polynomial time in finite fields of fixed characteristic". In: *arXiv preprint arXiv:1906.10668* (2019).

[6] Wikipedia, the free encyclopedia. *Elliptic curve*. [Online; accessed May 5, 2021]. 2021. URL: https://en.wikipedia.org/wiki/Elliptic_curve#/media/File:ECClines-3.svg.

[7] L. D. Feo. *Mathematics of Isogeny Based Cryptography*. [Online; accessed June 13, 2021]. 2017. URL: https://www.semanticscholar.org/paper/Mathematics-of-Isogeny-Based-Cryptography-Feo/261bd07d53502b5d4a53888e01c3b05ba0c532e5/figure/0.

[8] L.C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition*. Discrete Mathematics and Its Applications. CRC Press, 2008. ISBN: 9781420071474. URL: https://books.google.nl/books?id=nBfCEqpYKW0C.

[9] J. Silverman. "The arithmetic of elliptic curves". In: *Graduate texts in mathematics*. 1986.

[10] William C. Waterhouse. "Abelian varieties over finite fields". In: *Ann. Sci. École Norm. Sup. (4)* 2 (1969), pp. 521–560. ISSN: 0012-9593. URL: http://www.numdam.org/item?id=ASENS_1969_4_2_4_521_0.

[11] René Schoof. "Nonsingular plane cubic curves over finite fields". In: *J. Combin. Theory Ser. A* 46.2 (1987), pp. 183–211. ISSN: 0097-3165. DOI: 10.1016/0097-3165(87)90003-3. URL: https://doi.org/10.1016/0097-3165(87)90003-3.

[12] J. F. Voloch. "A note on elliptic curves over finite fields". In: *Bull. Soc. Math. France* 116.4 (1988), 455–458 (1989). ISSN: 0037-9484. URL: http://www.numdam.org/item?id=BSMF_1988__116_4_455_0.

[13] Massimiliano Sala and Daniele Taufer. *The group structure of elliptic curves over Z/NZ*. 2020. arXiv: 2010.15543 [math.NT].

[14] H. Lange and W. Ruppert. "Complete systems of addition laws on abelian varieties". In: *Invent. Math.* 79.3 (1985), pp. 603–610. ISSN: 0020-9910. DOI: 10.1007/BF01388526. URL: https://doi.org/10.1007/BF01388526.

[15] H. W. Lenstra Jr. "Elliptic curves and number-theoretic algorithms". In: *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Berkeley, Calif., 1986)*. Amer. Math. Soc., Providence, RI, 1987, pp. 99–120.

[16] W. Bosma and H. W. Lenstra Jr. "Complete systems of two addition laws for elliptic curves". In: *J. Number Theory* 53.2 (1995), pp. 229–240. ISSN: 0022-314X. DOI: 10.1006/jnth.1995.1088. URL: https://doi.org/10.1006/jnth.1995.1088.

[17] A. Hatcher, Cambridge University Press, and Cornell University. Department of Mathematics. *Algebraic Topology*. Algebraic Topology. Cambridge University Press, 2002. ISBN: 9780521795401. URL: `https://books.google.nl/books?id=BjKs86kosqgC`.

[18] J. M. Pollard. "Monte Carlo methods for index computation (mod p)". In: *Math. Comp.* 32.143 (1978), pp. 918–924. ISSN: 0025-5718. DOI: `10.2307/2006496`. URL: `https://doi.org/10.2307/2006496`.

[19] H. W. Lenstra Jr. "Factoring integers with elliptic curves". In: *Ann. of Math. (2)* 126.3 (1987), pp. 649–673. ISSN: 0003-486X. DOI: `10.2307/1971363`. URL: `https://doi.org/10.2307/1971363`.

[20] Kenji Koyama et al. "New public-key schemes based on elliptic curves over the ring Z_n". In: *Advances in cryptology—CRYPTO '91 (Santa Barbara, CA, 1991)*. Vol. 576. Lecture Notes in Comput. Sci. Springer, Berlin, 1992, pp. 252–266. DOI: `10.1007/3-540-46766-1\_20`. URL: `https://doi.org/10.1007/3-540-46766-1_20`.

[21] Neal Koblitz. "Elliptic curve cryptosystems". In: *Math. Comp.* 48.177 (1987), pp. 203–209. ISSN: 0025-5718. DOI: `10.2307/2007884`. URL: `https://doi.org/10.2307/2007884`.

[22] Victor S. Miller. "Use of elliptic curves in cryptography". In: *Advances in cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985)*. Vol. 218. Lecture Notes in Comput. Sci. Springer, Berlin, 1986, pp. 417–426. DOI: `10.1007/3-540-39799-X\_31`. URL: `https://doi.org/10.1007/3-540-39799-X_31`.

[23] Joseph Silverman. *The Arithmetic of Elliptic Curves*. Vol. 106. Jan. 2009. ISBN: 978-0-387-09493-9. DOI: `10.1007/978-0-387-09494-6`.