DISCRETE LOGARITHM PROBLEM ON ELLIPTIC CURVES OVER FINITE FIELDS

by
SALIHA TOKAT

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of Master of Science

Sabancı University
July 2022

ABSTRACT

DISCRETE LOGARITHM PROBLEM ON ELLIPTIC CURVES OVER FINITE FIELDS

SALIHA TOKAT

MATHEMATICS M.S. THESIS, JULY 2022

Thesis Supervisor: Assoc. Prof. Mohammad Sadek

Keywords: elliptic curves, discrete logarithm problem, elliptic curve discrete logarithm problem, elliptic curves over rings

The main focus of this thesis is the so-called elliptic curve discrete logarithm problem. The statement of the problem is that given a point P and a k-multiple of P on an elliptic curve defined over a finite field, can we recover k? There has been no general algorithm that solves this problem in subexponential time. For this reason, the problem has been conjectured to be hard, and it is used to provide the security of many cryptosystems for classical computers. In this thesis, we study several algorithms, and the theory behind them, that are used to solve the problem under certain conditions. We also provide a relatively new algorithm that can be implemented to solve the discrete logarithm problem for specific elliptic curves. Additionally, we discuss the fundamental theory of elliptic curves defined over a commutative ring with unity, as they provide a useful tool for the solution of the discrete logarithm problem for a certain family of elliptic curves over finite fields.

ÖZET

SONLU CİSİMLER ÜZERİNDE TANIMLANAN ELİPTİK EĞRİLERDE AYRIK LOGARİTMA PROBLEMİ

SALİHA TOKAT

MATEMATİK YÜKSEK LİSANS TEZİ, TEMMUZ 2022

Tez Danışmanı: Doç. Dr. Mohammad Sadek

Anahtar Kelimeler: eliptik eğriler, ayrık logaritma problemi, eliptik eğri ayrık logaritma problemi, halkalar üzerinde tanımlı eliptik eğriler

Bu tezin ana konusu eliptik eğri ayrık logaritma problemidir. Problemin ifadesi şöyledir: Sonlu cisim üzerinde tanımlı bir eliptik eğrinin bir P noktası ve P noktasının k-katı olan nokta verildiğinde, k değerini bulabilir miyiz? Bu problemi alt üstel zamanda çözen genel bir algoritma bulunamamıştır. Bu sebepten dolayı problemin zor olduğu sanısı yapılmıştır ve klasik bilgisayarlarda kullanılan birçok kriptografi sisteminin güvenliğini sağlamak için kullanılmıştır. Bu tezde, belirli koşullar altında bu problemi çözen bazı algoritmalar ve onların arkasındaki teoriyi çalıştık. Ayrıca, ayrık logaritma problemini belirli eliptik eğrilerde çözmek için uygulanabilecek nispeten yeni bir algoritma sunduk. Bunlara ek olarak, ayrık logaritma probleminin bazı eliptik eğrilerdeki çözümü için faydalı bir araç sağladığından dolayı birimli ve değişmeli halkalar üzerinde tanımlı eliptik eğrilerin temel teorisini işledik.

ACKNOWLEDGEMENTS

First of all, I would like to thank my advisor for providing guidance and feedback throughout this thesis and being patient with me constantly. He is a genuinely kind-hearted person and cares for his students as much as his own children. In addition, I want to thank the thesis jury members for devoting their time to review my thesis. Also, I extend my thanks to friends and family for their unending support.

Finally, I am thankful to Sabancı University and Scientific and Technological Research Council of Turkey (TÜBİTAK) for supporting me with scholarships.

"Life is like mathematics; nobody can describe it in the way that one can understand it without adequately experiencing it."

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS NOTATIONS

ECDLP	elliptic curve discrete logarithm problem
DLP	discrete logarithm problem
EDS	elliptic divisibility sequence
K	a perfect field
E/K	an elliptic curve defined over K
R	a commutative ring with unity
q	a power of a prime p, i.e., $q = p^r$
$\mathbb{F}_q$	a finite field of size q
P	a point on an elliptic curve
$x(P), (P)_x$	the x-coordinate of a point P
(x, y)	the affine coordinates of a point P
$(X : Y : Z)$	the projective coordinates of a point P
$\mathrm{Aut}(G)$	the automorphism group of G
$\mathrm{Gal}(\bar{K}/K)$	the automorphism group of $\bar{K}$ fixing K
I_n	the identity matrix of size $n \times n$
(W_n)	an elliptic divisibility sequence
(ψ_n)	a sequence of division polynomials

1. INTRODUCTION

In this thesis, we are mainly concerned with the fundamental theory of elliptic curves and the theory behind some of the attacks on the discrete logarithm problem defined on elliptic curves over finite fields, as well as, the description of the attacks themselves.

Many arithmetic questions on elliptic curves are subject to the research of number theorists, geometers and cryptographers. Finding rational points on elliptic curves is equivalent to finding nontrivial integer solutions to homogeneous cubic Diophantine equations in three variables. In fact, the arithmetic of curves defined by polynomials of degree less than 3 is completely understood. For example, if one considers the integer solutions to the equation

$$X^2 + Y^2 = Z^2,$$

then it is clear that these solutions correspond to rational points on the unit circle. Moreover, by finding one rational point P on the unit circle, one can give an explicit description of all other points on this circle. This can be achieved by finding the intersection points of a line with rational slope through P with the circle. In fact, the latter method provides a birational map from the unit circle to the rational line. This approach is useful in general; in order to find integer or rational solutions of given equations, we study the arithmetic of the algebraic variety defined by these equations. In particular, one may answer algebraic questions using geometric tools and ideas.

An elliptic curve is an abelian variety of dimension 1. Namely, an elliptic curve is a smooth projective curve of genus 1 with a specified rational point. Such a curve can be embedded in the projective plane, hence can be described by a planar equation of the form

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{1.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$. The equation (1.1) is called a Weierstrass equation.

One of the main reasons why mathematicians have been fascinated by elliptic curves is that its points form an abelian group under a group law defined by a tangent-chord method. Therefore, by finding one solution of the equation, we can get some other solutions. Moreover, due to the celebrated Mordell-Weil Theorem, the rational points of an elliptic curve defined over a number field can be generated using a finite set of such points. In fact, Mordell-Weil Theorem states that the group of rational points of an elliptic curve defined over a number field K is a finitely generated abelian group, in particular,

$$E(K) \cong \mathbb{Z}^r \oplus E_{tors}(K).$$

Also, due to Mazur, if the underlying field is $\mathbb{Q}$, we know all the possible arising torsion subgroups

$$E_{tors}(\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} \text{ with } 1 \leq n \leq 10 \text{ or } n = 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} \text{ with } 1 \leq n \leq 4. \end{cases}$$

When elliptic curves are defined over a finite field $\mathbb{F}_q$, the number of points with coordinates in $\mathbb{F}_q$ are necessarily finite. Due to Hasse, we have a bound on the number of these points that depends on the size of the field, namely,

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

Moreover, the group structure of an elliptic curve over a finite field is of the form

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}, \quad \text{or} \quad \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \text{ with } n_1 \mid n_2.$$

Besides their theoretic richness, elliptic curves have many applications in cryptography. The security of most cryptosystems relies on computationally hard mathematics problems, meaning that there is no general algorithm solving the problem in subexponential time using the classical computers. One of the most commonly used such problem is called the *discrete logarithm problem (DLP)* and it is stated as below.

Given $b \in \langle g \rangle$ where g is an element of the group $(G, *)$, find x such that $b = g^x \in G$.

In general, the group G is taken to be a finite field. When G is taken to be the group of rational points of an elliptic curve over a finite field, the problem is called the *elliptic curve discrete logarithm problem (ECDLP)*, and there is still no general subexponential algorithm that solves the problem. In fact, the elliptic curve version

of the problem is more commonly used since it is believed to be much harder as it provides higher security level by requiring smaller key, consequently becomes more efficient. The statement of the ECDLP is as follows.

Given $Q \in \langle P \rangle$ and a point P in $(E(\mathbb{F}_q), +)$, find x such that $Q = xP \in E(\mathbb{F}_q)$.

Although the discrete logarithm problem on elliptic curves over finite fields is conjectured to be hard, for particular curves with a certain number of rational points the problem can be solved or reduced to an easier problem by utilizing the theory of elliptic curves. The method of solving a problem or reducing to an easier problem is called an attack. In this thesis, we are mainly concerned with surveying some of the important attacks on the ECDLP. The attacks are primarily classified according to the trace t of the given elliptic curve over $\mathbb{F}_q$, that is an integer determined solely by the number of points on the elliptic curve. To be more specific,

$$t = q + 1 - \#E(\mathbb{F}_q).$$

1.1 Thesis Outline

In Chapter 2, we both cover the fundamental theory of elliptic curves and the necessary material to understand the surveyed attacks that will be presented in Chapter 3. More precisely, Section 2.5 is intended to explain the theory behind the attack presented in Section 3.1 which is for elliptic curves whose trace t is congruent to 0 modulo the characteristic of the field, i.e., supersingular elliptic curves. Similarly, Section 2.6 is meant for the attack given in Section 3.2 which is for elliptic curves with trace 1, and Sections 2.8 and 2.9.3 are meant for the attack given in Section 3.4 which is for elliptic curves with trace 2.

The attack that is covered in Section 3.5 is relatively new. We use our observation about why the attack due to (Shipsey & Swart, 2008) works which is given in Section 3.4. Then, we apply the idea for elliptic curves with trace values that have not been considered in literature. We find that if the elliptic curve $E/\mathbb{F}_q$ has a trace $1 \pm \sqrt{q}$, which implicitly requires q to be an even power of a prime, then the attack that we suggest would be successful with a conjectural probability similar to the one in Section 3.4.

Finally, in Chapter 4, we study the elliptic curves defined over a commutative ring R with unity satisfying a certain condition. The group of points $E(R)$ forms an abelian group, as well, with a slightly different defined addition law. Moreover, if R is set to be the ring $\mathbb{Z}/p^e\mathbb{Z}$, then there exist a new attack on the discrete logarithm problem on elliptic curves $E/\mathbb{F}_p$ with trace 1. This attack makes use of $E(\mathbb{Z}/p^e\mathbb{Z})$ as an intermediate object between $E(\mathbb{F}_p)$ and $\mathbb{F}_p$ when $e \geq 2$ and $E(\mathbb{Z}/p^e\mathbb{Z})$ is cyclic.

2. ELLIPTIC CURVES

In this chapter, we study the fundamental theory of elliptic curves and the theory behind some of the attacks on the discrete logarithm problem defined over elliptic curves over finite fields, which will be described in the next chapter.

An elliptic curve can be introduced in many ways. It is essentially a projective variety, also, one can consider it as an affine variety with a distinguished point denoted as O. I will define it in this order.

Note that throughout this thesis K denotes a perfect field, i.e., every algebraic extension of K is separable.

2.1 Projective Plane Curves

The *projective plane* over K, denoted as $\mathbb{P}^2(K)$, is the set of all triples (X, Y, Z) in $K \times K \times K$, excluding $(0, 0, 0)$, under the equivalence relation

$$(X_1, Y_1, Z_1) \sim (X_2, Y_2, Z_2) \iff \exists \lambda \in K^* \text{ such that } (X_1, Y_1, Z_1) = \lambda(X_2, Y_2, Z_2).$$

A *projective point* $P = (X : Y : Z)$ is the equivalence class of the triple (X, Y, Z) under the aforementioned equivalence relation. Note that for a homogeneous polynomial $F(X, Y, Z)$, if (X, Y, Z) is a zero of the polynomial then so is $(\lambda X, \lambda Y, \lambda Z)$.

An *projective set* $V \subseteq \mathbb{P}^2(K)$ is the zero-locus of homogeneous polynomials in three variables. It is called *irreducible* if V cannot be written as the union $V = V_1 \cup V_2$ where V_1 and V_2 are projective sets which are proper subsets of V.

A *projective plane curve* C_F defined over K is an irreducible projective set defined

by an homogeneous polynomial $F \in K[X,Y,Z]$, i.e.,

$$C_F = \{(X:Y:Z) \in \mathbb{P}(\bar{K}^2) : F(X,Y,Z) = 0\}.$$

It is called *smooth*, or *nonsingular*, if there is no point $P = (X:Y:Z) \in C_F$ such that

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0. \tag{2.1}$$

A point P satisfying (2.1) is called a *singular point* for C_F.

Definition 2.1.1. An *elliptic curve* E defined over K is a smooth projective plane curve defined by a homogeneous Weierstrass polynomial

$$F(X,Y,Z) : Y^2Z + a_1XYZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3), \tag{2.2}$$

with $a_1, a_2, a_3, a_4, a_6 \in K$.

The equation $F(X,Y,Z) = 0$ is called a *homogeneous Weierstrass equation*.

Remark. Elliptic curve is an irreducible projective set: Reducible cubic curves either consists of three lines or a conic and a line; every point of intersection of components is singuar, hence reducible cubics have at least two singular points.

In the first remark of Section 2.2, it is explained that irreducibility property turns an elliptic curve into a projective variety.

Whether an elliptic curve satisfies the smoothness criteria can be determined by the fact that a homogeneous Weierstrass polynomial, or equation, defines a smooth curve if and only if its discriminant Δ given in (2.11) is nonzero (Enge, 1999, Proposition 2.25).

The point $P = (0:1:0)$ is on any elliptic curve E. Moreover, due to the following sequence of implications

$$P = (X:Y:Z) \in E \text{ and } Z = 0 \Rightarrow X^3 = 0 \Rightarrow X = 0 \Rightarrow Y \neq 0 \text{ since } (0,0,0) \notin \mathbb{P}^2(K),$$

we conclude that the only point P with $Z = 0$ of an elliptic curve is $P = (0:1:0)$.

Let's dehomogenize the Weierstrass polynomial by setting $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ given in Definition 2.1.1, the polynomial becomes

$$f(x,y) : y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6). \tag{2.3}$$

This is called the *nonhomogeneous Weierstrass polynomial* or simply *Weierstrass polynomial*. Let's look at what happens to the points on the curve E during that process. They became of the form $(\frac{X}{Z} : \frac{Y}{Z} : \frac{Z}{Z})$. There are two distinct cases depending on the Z-coordinate of the point. If $Z \neq 0$, then the point becomes $(\frac{X}{Z} : \frac{Y}{Z} : 1)$ and this can be realized as (x, y) on the curve defined by $f(x, y)$. If $Z = 0$, then the point is $(0 : 1 : 0)$. For this point, dehomogenizing by the Z-coordinate requires division by 0, so we are missing this point during this process. Let's denote this point by O, and call it the *base point* or *point at infinity* of the elliptic curve.

So, an elliptic curve can also be defined on the affine plane as the following.

Definition 2.1.2. An *elliptic curve* E defined over K is the set of points satisfying the Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.4}$$

with nonzero discriminant Δ, which is defined in (2.11), together with the base point O. Moreover, the set of *K-rational points* of E is

$$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}. \tag{2.5}$$

Remark. We write E/K, and we say that E *is an elliptic curve defined over* K when the coefficients of the defining Weierstrass equation are from K. Also, it is worth to note that $E = E(\bar{K})$.

By linear transformations, we can simplify the equation of E as described below.

If $\mathrm{char}(K) \neq 2$, then the substitution $y \mapsto \frac{1}{2}(y - a_1x - a_3)$ gives

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6, \tag{2.6}$$

where

$$b_2 = a_1^2 + 4a_2 \tag{2.7}$$

$$b_4 = 2a_4 + a_1a_3 \tag{2.8}$$

$$b_6 = a_3^2 + 4a_6 \tag{2.9}$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \text{ and} \tag{2.10}$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \tag{2.11}$$

If $\text{char}(K) \neq 2,3$, then the substitution $(x, y) \mapsto (\frac{x-3b_2}{36}, \frac{y}{108})$ gives

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

where

$$c_4 = b_2^2 - 24b_4, \tag{2.12}$$

$$c_6 = -b_3^2 + 36b_2b_4 - 216b_6, \tag{2.13}$$

$$j = \frac{c_4^3}{\Delta}. \tag{2.14}$$

The simplified versions of the Weierstrass equations and other results for elliptic curves defined over K when $\text{char}(K) = 2$ and 3 can be found in (Silverman, 2009, Appendix A).

Definition 2.1.3. The quantity Δ given in (2.11) is called the *discriminant* of the Weierstrass equation (2.4) and Weierstrass polynomial (2.2). The quantity j given in (2.14) is the *j-invariant* of the elliptic curve.

Remark. The value of the discriminant Δ is not unique for the curve; it changes as one applies linear transformation on the initial defining equation of E. However, the value of the j-invariant is independent of the linear transformations applied on the defining equation of E.

Definition 2.1.4. If $\text{char}(K) \neq 2,3$, every elliptic curve E defined over K can be expressed by an equation of the form

$$E_{A,B} : y^2 = x^3 + Ax + B \text{ where } A, B \in K. \tag{2.15}$$

The equation (2.15) is called *short Weierstrass equation* and its associated discriminant is $\Delta = -16(4A^3 + 27B^2)$.

A group law can be defined on elliptic curves with the point O being the identity element. In what follows, we describe this group operation denoted as "+" and named as addition so that $(E, +)$ becomes a group.

The next theorem is a special case of the Bezout's Theorem and it is essential to mention before introducing the group law for an elliptic curve E/K.

Theorem 2.1.1. *Suppose that X and Y are two plane projective curves defined over a field K with no common component, i.e., greatest common divisor of defining polynomials of X, Y is a constant. Then the number of intersection points of X and Y with coordinates in the algebraic closure of K, counted with multiplicity, is*

equal to the product of the degrees of X and Y.

According to this theorem, if we take X to be an elliptic curve E/K as a projective plane curve and Y to be any projective line, then they don't have a common component since elliptic curve is irreducible and does not contain any line. Therefore, their number of intersection points counted with multiplicity is equal to $3 \cdot 1 = 3$. As it will become clear after description of the group law, in essence, it says that three points on a line sum to zero, which is the identity element of the group. We will see that if the points P, Q, R are on E and there is a line passing through all of them, then there is no other intersection of E and the line, and addition of any two is equal to the inverse of the other.

Geometrically, the group law "+" is defined by the tangent and chord method. Let's suppose, we want to add two distinct points $P + Q \in E$. We first take the chord passing through P and Q. This chord intersects the curve at a third point R counting with multiplicities due to Theorem 2.1.1. Then $P + Q$ corresponds to the point which is the reflection of R across the x-axis when the curve is defined by a short Weierstrass equation in which case curve is symmetric with respect to x-axis as picture in Figure 2.1. In general, $P + Q$ corresponds to the intersection point of the vertical line through R and the curve, that is different than the point R. If we want to add a point to itself, then we take the tangent at the point and continue similarly. An instance of the group law is illustrated in Figure 2.1.

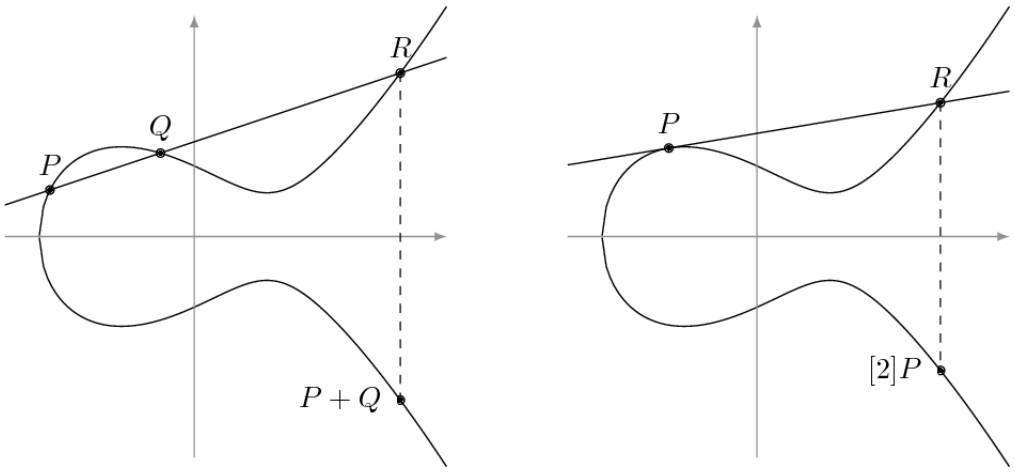

Figure 2.1 An elliptic curve defined over $\mathbb{R}$, and the geometric representation of its group law (Feo, 2017)

Remark. The addition of two points that is geometrically defined above, namely $P + Q$ or $2P$, is called the *inverse of* R and denoted as $-R$. Algebraically, the inverse of any point $R = (x, y) \in E$ where E is given by (2.4) corresponds to

$$-R = (x, -y - a_1 x - a_3). \tag{2.16}$$

Note that in terms of projective coordinates, the last coordinate is kept fixed just like the first one.

By applying this geometric method on the equation of the curve, we can derive explicit formulas for the group law "+". Let P and Q be points on the elliptic curve E given by the equation (2.4). We will separate the addition formula into the following distinct cases.

Case 1: If both of P and Q are O, then

$$P+Q=O+O=O$$

and the explanation goes as follows: Both P and Q don't appear on the affine plane. Hence, we consider E as a projective plane curve as given in Definition 2.1.1. Since $P=Q$, we look at the tangent at P. We find that its equation is $Z=0$. We know that the only point on E whose Z-coordinate is 0 is the point O, so O has multiplicity 3 and it is the only intersection point of the tangent and the curve. Next, we have to find the inverse of O. This is again the point itself, namely O.

Case 2: If exactly one of P or Q is the point O, then

$$P+Q \text{ is the point that is different than } O$$

and the explanation goes as follows: Assume $P\neq O$, so it is of the form $P=(x_P:y_P:1)$. The line passing through P and Q has the equation $X-x_PZ=0$. The intersection points are $(0:1:0),(x_P:y_P:1),(x_P:-y_P-a_1x_P-a_3:1)$, namely $O,P,-P$. Therefore, the third intersection point is $-P$, and the inverse of $-P$ is P itself.

For the the rest of the cases, assume that neither P nor Q is the point O, i.e., both P and Q are affine points of E. So, we can write $P=(x_P,y_P)$ and $Q=(x_Q,y_Q)$.

Case 3: Assume that $x_P\neq x_Q$. Then, the line passing through P and Q has slope $\lambda=\frac{y_Q-y_P}{x_Q-x_P}$ and its equation is $y=\lambda x+\nu$ where $\nu=\frac{y_Px_Q-y_Qx_P}{x_Q-x_P}$, found by plugging P to the line equation. The coordinates of the point $P+Q$ is determined by intersecting the curve with the line which is achieved by plugging this y into the curve equation. This results in a degree 3 polynomial in variable x. The roots are the x-coordinates of the intersection points, and we already know that two of the roots are x_P and x_Q, so the other root is the x-coordinate of the third intersection point which can be easily found by the fact that sum of the roots of a monic polynomial is equal to minus the coefficient of the second-to-highest power term. Also, its y-coordinate can be simply find by plugging this value into the line equation. Then, we take inverse

of this point to find $P+Q$, hence

$$P+Q=(\lambda^2-a_1\lambda-a_2-x_P-x_Q,-(\lambda+a_1)(\lambda^2-a_1\lambda-a_2-x_P-x_Q)-\nu-a_3).$$

Case 4: Assume that $x_P=x_Q$ and $y_P=y_Q$. This means $Q=P$. So, we need to determine the equation of the tangent line at P. The tangent has slope $\lambda=\frac{3x_P^2+2a_2x_P+a_4-a_1y_P}{2y_P+a_3+a_1x_P}$, which is found by implicit differentiation of equation (2.4), and its equation is $y=\lambda x+\nu$ where $\nu=\frac{-x_P^3+a_4x_P+2a_6-a_3y_P}{2y_P+a_1x_P+a_3}$, found by plugging P to the tangent equation. The coordinates of the point $P+Q=2P$ is found with the same technique described in Case 3 but notice that in this case x_P is a repeated root with multiplicity 2. Then, the equation given for $P+Q$ in Case 3 is reduced to

$$P+Q=2P=\left(\frac{x_P^4-b_4x_P^2-2b_6x_P-b_8}{4x_P^3+b_2x_P^2+2b_4x_P+b_6},-(\lambda+a_1)\frac{x_P^4-b_4x_P^2-2b_6x_P-b_8}{4x_P^3+b_2x_P^2+2b_4x_P+b_6}-\nu-a_3\right)$$

where b_i's are as in (2.6).

Case 5: Assume that $x_P=x_Q$ and $y_P\neq y_Q$. This means $Q=-P$. The line passing through P and Q has infinite slope, i.e., it is vertical to the x-axis. Therefore, we cannot intersect it with the curve at a third point on the affine plane. However, if we examine it in the projective plane by using the equation (2.2) and setting $P=(x_P:y_P:1)$, we see that the line passing through P and Q has the equation $X-x_PZ=0$. As in Case 2, the intersection points are $P,-P,O$. Therefore, the third intersection point is O, and its inverse is itself. Hence,

$$P+Q=P-P=O.$$

Theorem 2.1.2. *(Silverman, 2009, III, Proposition 2.2) Let E be an elliptic curve defined over K. Then, $(E,+)$ is an abelian group under addition as defined earlier. Furthermore, $E(K)$ becomes its subgroup.*

Note that the closedness of the group follows from Theorem 2.1.1. The commutativity of the group follows from the geometric description of the group law as the line passing through the points P and Q is the same with the line passing through Q and P. The identity being O follows from the results of Case 1 and Case 2 describing the group law above. The existence of inverse element basically follows from Case 5. The proof of associativity is lengthy, it can be verified by both geometric and algebraic methods.

2.2 Maps Between Elliptic Curves

As we have learnt that elliptic curves are defined as projective sets with extra properties. In the next remark, we explain that they are projective varieties, hence we can talk about maps between them such as morphisms. Moreover, since they form a group, we can define a special type of a morphism between them which is called an isogeny.

For projective varieties, polynomials cannot define a function on it since they will violate homogeneity. For this reason, we have to adjust the notion of a function for curves defined as projective varieties. In what follows, we consider projective varieties in $\mathbb{P}^2$ but it can be generalized to $\mathbb{P}^n$ in the obvious way.

Let $V \subseteq \mathbb{P}^2$ be any *projective variety* defined over K, i.e., the zero-locus of some finite family of homogeneous polynomials in 3 variables with coefficients in K whose *homogeneous ideal* $I(V)$ defined as

$$I(V) = \{f \in K[X,Y,Z] : f \text{ is homogeneous and } f(P) = 0 \text{ for any } P \in V\}$$

is a prime ideal in $\bar{K}[X,Y,Z]$.

Remark. We mentioned that an elliptic curve is a projective variety, we will explain the reason behind it. It is known that a homogeneous ideal is a prime ideal if and only if it is irreducible. As explained in the previous chapter, elliptic curves are irreducible, hence the homogeneous ideal of E is a prime ideal. This makes an elliptic curve a projective variety.

The *homogeneous coordinate ring of* V is the ring $K[V] = K[X,Y,Z]/I(V)$. Since it is a quotient of a commutative ring with unity and a prime ideal, in particular, it is an integral domain. Hence, we can define its field of fractions.

Definition 2.2.1. The *function field of* V, or *the field of rational functions of* $K[V]$, is

$$\bar{K}(V) = \left\{ \frac{g}{h} : g,h \in K[X,Y,Z] \text{ are homogeneous of the same degree, } h \notin I(V) \right\}$$

under the equivalence relation

$$\frac{g_1}{h_1} \sim \frac{g_2}{h_2} \iff g_1h_2 - g_2h_1 \in I(V).$$

A *rational function* on V is an element of $\bar{K}(V)$.

By definition of a rational function $\frac{g}{h} \in \bar{K}(V)$, we know that h is not identically zero on V, therefore there are only finitely many points $P \in V$ such that the function $\frac{g}{h}$ is not defined for. We say P is a *regular* point of a rational function or rational function is *regular* at P, if P is not one of these points.

Using the notion of rational functions on projective varieties, we can construct maps between varieties.

Definition 2.2.2. Let $V_1, V_2 \subseteq \mathbb{P}^2$ be projective varieties. A *rational map* from V_1 to V_2 is a map of the form

$$\phi \colon V_1 \to V_2, \quad \phi = (f_0, f_1, f_2)$$

where the functions $f_0, f_1, f_2 \in \bar{K}(V_1)$ have the property that if $P \in V_1$ at which f_0, f_1, f_2 are regular at P, then $\phi(P) = (f_0(P), f_1(P), f_2(P)) \in V_2$.

A rational map ϕ is defined through rational functions f_i's. As we observed, there are finitely many points of V_1 such that the rational function f_i is not defined, namely f_i is not regular at these points. However, it might be still possible to evaluate the map ϕ at these points if we can find an appropriate $g \in \bar{K}(V_1)$ so that gf_i becomes regular at P.

Definition 2.2.3. A rational map ϕ as given in Definition 2.2.2 is said to be *regular* at $P \in V_1$ if there is $g \in \bar{K}(V_1)$ satisfying

(i) each gf_i is regular at P,

(ii) there is some i for which $gf_i(P) \neq 0$.

If such g exists, then $\phi(P) = ((gf_0)(P), (gf_1)(P), (gf_2)(P))$.

Note that g is specific to the point $P \in V_1$.

Definition 2.2.4. If a rational map is regular at every point of the domain, then it is called a *morphism*, or a *regular map*.

Theorem 2.2.1. *(Silverman, 2009, III.2.1) Let ϕ be a rational map $\phi \colon C \to V$ where C is a curve, namely a projective variety of dimension one, and V is a projective variety. If $P \in C$ is a smooth point, then ϕ is regular at P.*

As an immediate consequence, since an elliptic curve is a smooth curve, a rational map defined on it is regular at every point. Hence, it is, in fact, a morphism.

Example. The group law of elliptic curves

$$\begin{aligned} +\colon E \times E &\to E \\ (P_1, P_2) &\mapsto P_1 + P_2 \end{aligned}$$

is a morphism. (Silverman, 2009, III.Theorem 3.6)

Theorem 2.2.2. *(Silverman, 2009, III.Theorem 2.3) Let $\phi\colon C_1 \to C_2$ be a morphism of curves. Then ϕ is either constant or surjective.*

Elliptic curve has a more sophisticated structure than a projective variety since it forms a group with identity element O as stated in Theorem 2.1.2. We examine the morphisms between elliptic curves respecting this point.

Definition 2.2.5. Let $\phi\colon E_1 \to E_2$ be a morphism of elliptic curves. It is called an *isogeny* if $\phi(O) = O$.

The set of isogenies from E_1 to E_2 form a group, since E_1 and E_2 are abelian varieties, and it is denoted by $\mathrm{Hom}(E_1, E_2)$ whose group operation is defined as $(\phi + \psi)(P) = \phi(P) + \psi(P)$ for $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$.

Moreover, if $E_1 = E_2$, then $\mathrm{Hom}(E_1, E_2)$ becomes the group of *endomorphisms* of E and denoted by $\mathrm{End}(E)$. In fact, $\mathrm{End}(E)$ forms a ring (Silverman, 2009, III.4.8) where multiplication is defined as composition $(\phi\psi)(P) = \phi(\psi(P))$ for $\phi, \psi \in \mathrm{End}(E)$.

Example. Let E/K be an elliptic curve. For each $n \in \mathbb{Z}$, an obvious example of an endomorphism of E is *multiplication-by-n* map which is defined as

$$\begin{aligned} [n]\colon E &\to E \\ P &\mapsto nP = \underbrace{P + P + \cdots + P}_{\text{n terms}} && \text{if } n > 0, \\ P &\mapsto O && \text{if } n = 0, \\ P &\mapsto nP = \underbrace{-P - P - \cdots - P}_{\text{n terms}} && \text{if } n < 0. \end{aligned}$$

By this example, we can say that $\mathbb{Z}$ is contained in the ring $\mathrm{End}(E)$.

Furthermore, we can deduce that if n is not the order of the group, then image of P is not O for some $P \in E$. Moreover, we know that O is sent to O. Hence, the map $[n]$ is not constant in that case. By Theorem 2.2.2, it means $[n]$ is surjective when n is not the order of the group E. It is constant, otherwise. In fact, the map that sends everything to O is the only constant isogeny.

We will end this section by stating another important result about the multiplication-by-n map.

Theorem 2.2.3. *(Silverman, 2009, III.6.2(d)) For all* $n \in \mathbb{Z}$, $\deg[n] = n^2$.

This result can also be observed with a different approach than the one presented in the referred book. Recall that when describing the algebraic description of the addition law, the coordinates of $P+Q$ are given by rational functions of the coordinates of points P and Q on the curve (since the rational functions for affine varieties are just quotients of polynomials without any assumption on their degrees). Repeating the addition formula yields rational functions (considering it for affine varieties) for each coordinate of the image of P under the multiplication-by-n map which are given in the Theorem 2.8.5. As a corollary of this theorem, (Washington, 2008, Corollary 3.7) proves that the map $[n]$ has degree n^2 by showing that the numerator and the denominator of the rational function defining the x-coordinate is relatively prime and has degree n^2.

2.3 Torsion Points

Now, let's investigate the structure of the group $(E,+)$. The elements, whose order is finite, of a group are called torsion elements. Torsion elements form a subgroup when the group is abelian.

Definition 2.3.1. Let E/K be an elliptic curve and $n \in \mathbb{Z}$ with $n \geq 1$. The *n-torsion subgroup of E*, denoted as $E[n]$, is the set of points of E of order n, i.e.,

$$E[n] = \{P \in E : [n]P = O\}.$$

The *torsion subgroup of E*, denoted by E_{tors}, is the set of all points of E of finite order, i.e.,

$$E_{tors} = \bigcup_{n=1}^{\infty} E[n].$$

The subgroup $E_{tors}(K)$ denotes the points with finite order in the group $E(K)$.

Remark. Notice that by definition $E[n]$ corresponds to $\mathrm{Ker}[n]$ where $[n]$ is the multiplication-by-n map. By (Washington, 2008, Proposition 2.28), the map $[n]$ is separable if and only if $\gcd(n, \mathrm{char}(K)) = 1$ and n is nonzero. Hence, for values of n satisfying these conditions, we have $\#\mathrm{Ker}[n] = \deg[n]$ by Proposition 2.9.2.

Moreover, we can say that $\deg[n] = n^2$ by Theorem 2.2.3. Therefore,

$$\#E[n] = \#\mathrm{Ker}[n] = \deg[n] = n^2.$$

Further, for every integer d dividing n, we similarly have $\#E[d] = d^2$. Using the Structure Theorem for Finite Abelian Groups, we see that there is only one possible way of writing it, namely the product of two cyclic groups of size n. This explains the first case of the following theorem.

Theorem 2.3.1. *(Silverman, 2009, Corollary 6.4) Let E/K be an elliptic curve, and $n \in \mathbb{Z}$ with $n \neq 0$.*
If either $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) = p > 0$ and $p \nmid n$, then

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

If $\mathrm{char}(K) = p > 0$, then either

$$E[p^e] \cong \{O\} \text{ for all } e = 1, 2, 3, \ldots \text{ or } E[p^e] \cong \{\mathbb{Z}/p^e\mathbb{Z}\} \text{ for all } e = 1, 2, 3, \ldots.$$

Consequently, if $\mathrm{char}(K) = p > 0$ and $n = p^e n'$ where $\gcd(p, n') = 1$, then either

$$E[n] \cong \mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z} \text{ or } E[n] \cong \mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Suppose E/K is an elliptic curve with $\mathrm{char}(K) = p > 0$. If $E[p^e] \cong \{O\}$, then E is called *supersingular* elliptic curve. Otherwise, E is called *ordinary* elliptic curve.

Obviously, if the underlying field K is a finite field, then all points on E lies in its torsion subgroup E_{tors}. Moreover, if order of $E(K)$ is n, then it is a subgroup of $E[n]$ which immediately implies that it is isomorphic to a direct product of at most two cyclic groups. This argument will be used to prove the structure of $E(K)$ in Section 2.9.

2.4 The Group $E(\mathbb{Q})$

Let E/K be an elliptic curve. If the underlying field K is $\mathbb{Q}$, then we have the following celebrated theorems giving the group structure of $E(\mathbb{Q})$. Moreover, possible torsion subgroups of $E(\mathbb{Q})$ are completely classified.

Theorem 2.4.1 (Mordell, 1922)**.** *Let E be defined over $\mathbb{Q}$. $E(\mathbb{Q})$ is a finitely generated abelian group.*

By the Fundamental Theorem of Finitely Generated Abelian Groups, the following corollary is immediate.

Corollary 2.4.1.1.

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E_{tors}(\mathbb{Q})$$

where r is the rank of $E(\mathbb{Q})$.

In fact, the above result of Mordell is true for any abelian variety defined over a number field. This is known as Mordell-Weil Theorem (1929). It was conjectured by Poincaré(1901).

Due to Mazur, we know all possible groups that can occur as $E_{tors}(\mathbb{Q})$.

Theorem 2.4.2 (Mazur, 1977)**.** *Let E be defined over $\mathbb{Q}$. Then $E_{tors}(\mathbb{Q})$ is one of the following:*

$$\mathbb{Z}_n \text{ with } 1 \leq n \leq 10 \text{ or } n = 12,$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_{2n} \text{ with } 1 \leq n \leq 4.$$

2.5 Weil Pairing

The Weil pairing defined on the n-torsion points of the elliptic curve is a useful tool in the study of elliptic curves. As an example, it is used to attack the elliptic curve discrete logarithm problem for supersingular curves.

For the rest of the section, let E/K be an elliptic curve and n be an integer that is relatively prime to $\text{char}(K)$ if $\text{char}(K) > 0$. Consequently, $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by Theorem 2.3.1. Also, let μ_n to denote the n^{th} roots of unity, i.e.,

$$\mu_n = \{x \in \bar{K} : x^n = 1\}.$$

The group μ_n lies in $\bar{K}$. Any generator of the group μ_n is called a *primitive n^{th} root of unity.*

Theorem 2.5.1. *(Washington, 2008, Theorem 3.9) There is a pairing*

$$e_n \colon E[n] \times E[n] \to \mu_n,$$

called the Weil pairing, that satisfies the following properties:

Bilinearity:

$$e_n(P_1 + P_2, Q) = e_n(P_1, Q)e_n(P_2, Q),$$
$$e_n(P, Q_1 + Q_2) = e_n(P, Q_1)e_n(P, Q_2) \text{ for all } P_1, P_2, Q_1, Q_2 \in E[n].$$

Nondegeneracy:

$$e_n(P, Q) = 1 \text{ for all } Q \in E[n] \implies P = O,$$
$$e_n(P, Q) = 1 \text{ for all } P \in E[n] \implies Q = O.$$

Identity:

$$e_n(P, P) = 1 \text{ for all } P \in E[n].$$

Alternation:

$$e_n(P, Q) = e_n(Q, P)^{-1} \text{ for all } P, Q \in E[n].$$

Corollary 2.5.1.1 (Theorem 3.10 (Washington, 2008))**.** *Let $\{P, Q\}$ be a basis of $E[n]$. Then $e_n(P, Q)$ is a primitive n^{th} root of unity, i.e., generator for the group μ_n.*

Proof. Assume that the order of $e_n(P, Q)$ is d. Then $e_n(P, dQ) = e_n(P, Q)^d = 1$ by the bilinearity property and the assumption, respectively. Also, $e_n(Q, dQ) = e_n(Q, Q)^d = 1$ by the bilinearity and identity properties. For any $R \in E[n]$, $R = k_1P + k_2Q$ for some integers k_1, k_2. Therefore,

$$e_n(R, dQ) = e_n(P, dQ)^{k_1} e_n(Q, dQ)^{k_2} = 1$$

by the bilinearity property and the assumption, respectively. Since this is true for any R, the nondegeneracy property implies that dQ must be O. Since Q is a basis its order is n, hence $dQ = O$ implies that n must be a divisor of d. So, it follows that $d = n$ and consequently $e_n(P, Q)$ is a primitive n^{th} root of unity. □

So, we can say that if $P \in E(K)$ is a point of order n where n satisfies $\gcd(n, \text{char}(K)) = 1$ if $\text{char}(K) > 0$, then there exists a point $Q \in K$ so that $e_n(P, Q)$

is a primitive n^{th} root of unity. Moreover, if we denote a primitive n^{th} root of unity by ζ_n, then by the bilinearity of the Weil pairing

$$e_n(kP,Q) = e_n(P,Q)^k = \zeta_n^k$$

for all $k \in \mathbb{Z}$. Hence, we conclude that $\mu_n = \mathrm{Im}(e_n)$.

Corollary 2.5.1.2. *(Washington, 2008, Theorem 3.11) If $E[n] \subseteq E(K)$, then $\mu_n \subset K$.*

Theorem 2.5.2. *Let $E/\mathbb{F}_q$ be an elliptic curve such that $E[n] \subseteq E(\mathbb{F}_q)$, and $\gcd(n,q) = 1$. Let $P \in E[n]$ be a point of order n. Then for all $Q_1, Q_2 \in E[n]$, the points Q_1, Q_2 are in the same coset of $\langle P \rangle$ within $E[n]$ if and only if $e_n(P,Q_1) = e_n(P,Q_2)$.*

Proof. Assume that Q_1 and Q_2 are in the same coset, then $Q_1 = Q_2 + kP$ for some integer k. So, we get

$$\begin{aligned} e_n(P,Q_1) &= e_n(P,Q_2+kP) && \text{as } Q_1 = Q_2 + kP \\ &= e_n(P,Q_2)e_n(P,P)^k && \text{by bilinearity} \\ &= e_n(P,Q_2) && \text{by identity.} \end{aligned}$$

Conversely, assume that $e_n(P,Q_1) = e_n(P,Q_2)$. Also, assume for a contradiction that Q_1 and Q_2 are not in the same coset. Then $Q_1 - Q_2 = k_1P + k_2Q$ for some integers k_1, k_2 with $k_2Q \neq O$, where P,Q is a basis for $E[n]$. If $s_1P + s_2Q$ is any point for some integers s_1, s_2, then

$$\begin{aligned} e_n(k_2Q, s_1P + s_2Q) &= e_n(k_2Q,P)^{s_1} e_n(Q,Q)^{k_2 s_2} && \text{by bilinearity} \\ &= e_n(P,k_2Q)^{-s_1} && \text{by identity.} \end{aligned}$$

Since $s_1P + s_2Q$ is any point and $k_2Q \neq O$, the quantity $e_n(P,k_2Q)$ cannot be 1 due to (2.5.1,2). Therefore,

$$\begin{aligned} e_n(P,Q_1) &= e_n(P,Q_2 + k_1P + k_2Q) && \text{as } Q_1 = Q_2 + k_1P + k_2Q \\ &= e_n(P,Q_2)e_n(P,P)^{k_1} e_n(P,k_2Q) && \text{by bilinearity} \\ &= e_n(P,Q_2) && \text{by identity and } e_n(P,k_2Q) \neq 1. \end{aligned}$$

□

We end this section by the following theorem which is essentially important for the

attack presented in Section 3.1 to be understood. Its proof clearly follows from bilinearity of the Weil pairing and the assumptions of the theorem.

Theorem 2.5.3. *(Menezes, Okamoto & Vanstone, 1993, Theorem 10) Suppose that $Q \in E[n]$ and $e_n(P,Q)$ is a primitive n^{th} root of unity. Then*

$$\begin{aligned} f\colon \langle P\rangle &\to \mu_n \\ R &\mapsto e_n(R,Q) \end{aligned}$$

is a group isomorphism.

2.6 The Group $E(\mathbb{Q}_p)$

Let p be a prime, then

$$\mathbb{Q}_p = \left\{ \sum_{i=m}^{\infty} a_i p^i : m \in \mathbb{Z}, a_i \in \mathbb{Z}, 0 \leq a_i < p \right\}$$

is a local field, i.e., it is a complete field with respect to a norm induced by a discrete valuation and its residue field is finite. The respective discrete valuation and the norm it induces is defined as follows.

Definition 2.6.1. For a fixed prime number p, we define the *p-adic valuation*

$$\begin{aligned} v_p\colon \mathbb{Q} &\to \mathbb{Z} \cup \{\infty\} \\ p^r \frac{a}{b} &\mapsto r \\ 0 &\mapsto \infty \end{aligned}$$

where $a, b \in \mathbb{Z}$ such that $\gcd(a,p) = \gcd(b,p) = 1$.

Also, we define the *p-adic norm*

$$\begin{aligned} ||.||_p\colon \mathbb{Q} &\to \mathbb{R}_{\geq 0} \\ q &\mapsto p^{v_p(q)} \\ 0 &\mapsto 0. \end{aligned}$$

Remark. Properties of v_p implies that $||.||_p$ is a norm on $\mathbb{Q}_p$.

Its ring of integers is the p-adic integers $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : ||x||_p \leq 1\}$, and its maximal ideal is $p\mathbb{Z}_p = \{x \in \mathbb{Z}_p : ||x||_p < 1\}$, and its residue field is $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$. Moreover, p is a uniformizer for the ring $\mathbb{Z}_p$ since $v_p(p) = 1$.

For the theory of elliptic curves over a general local field K and the corresponding generalizations of the results presented in this section, see (Silverman, 2009, Chapter VII). Here, I set the local field $K = \mathbb{Q}_p$ and provide the necessary preliminaries that will be useful in describing the attack presented in Section 3.2. Also, for a detailed explanation of these results when $K = \mathbb{Q}_p$ see (Leprévost, Monnerat, Varrette & Vaudenay, 2005) and (Kosters & Pannekoek, 2017).

Now, we will define the *reduction modulo p* map, p can be replaced by a uniformizer in general. Let's denote the map by r, then

$$\begin{aligned} r \colon \mathbb{Z}_p &\to \mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p \\ x &\mapsto \tilde{x} \end{aligned}$$

where $\tilde{x}$ is given by $x \pmod p$.

Let $E/\mathbb{Q}_p$ be an elliptic curve defined by the homogenous Weierstrass equation

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

because when we apply the reduction map the points with nonzero Z-coordinate may have zero Z-coordinate. The curve $\tilde{E}/\mathbb{F}_p$, possibly singular, is called the *reduction of E modulo p* and defined as

$$\tilde{E} : Y^2Z + \tilde{a_1}XYZ + \tilde{a_3}YZ^2 = X^3 + \tilde{a_2}X^2Z + \tilde{a_4}XZ^2 + \tilde{a_6}Z^3.$$

The reduction of coefficients and points of the curve can be calculated by the map r since elliptic curve defined over $\mathbb{Q}_p$ can be written with coefficients in $\mathbb{Z}_p$ by transformations. Therefore, in a similar fashion, we can consider the map r between the curves $E/\mathbb{Q}_p$ and $\tilde{E}/\mathbb{F}_p$:

$$\begin{aligned} r \colon E(\mathbb{Q}_p) &\to \tilde{E}(\mathbb{F}_p) \\ P = (X : Y : Z) &\mapsto \tilde{P} = (\tilde{X} : \tilde{Y} : \tilde{Z}) \end{aligned}$$

Denote the set of nonsingular points of $\tilde{E}(\mathbb{F}_p)$ by $\tilde{E}_{ns}(\mathbb{F}_p)$. Let's define

$$E_0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : \tilde{P} \in \tilde{E}_{ns}(\mathbb{F}_p)\}.$$

This is the points of $E(\mathbb{Q}_p)$ that reduce to a nonsingular point of the reduction curve $\tilde{E}/\mathbb{F}_p$, in fact $E_0(\mathbb{Q}_p)$ is a subgroup of $E(\mathbb{Q}_p)$ under addition.

Next, define the set of points of $E(\mathbb{Q}_p)$ that is reduced to the base point (identity),

$$E_1(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : \tilde{P} = O\}, \text{ more precisely}$$

$$E_1(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : v_p(x(P)) \leq -2, v_p(y(P)) \leq -3\} \cup \{O\}.$$

The following sequence becomes an exact sequence

$$0 \to E_1(\mathbb{Q}_p) \overset{\iota}{\hookrightarrow} E_0(\mathbb{Q}_p) \overset{r}{\to} \tilde{E}_{ns}(\mathbb{F}_p) \to 0.$$

since $E_1(\mathbb{Q}_p) = \mathrm{Im}(\iota) = \mathrm{Ker}(r) = E(\mathbb{Q}_p)$, hence we get

$$E_0(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) \cong \tilde{E}_{ns}(\mathbb{F}_p). \tag{2.17}$$

If we suppose that the reduced curve $\tilde{E}(\mathbb{F}_p)$ has no singular points, i.e., $\tilde{E}_{ns}(\mathbb{F}_p) = \tilde{E}(\mathbb{F}_p)$ and also $E_0(\mathbb{Q}_p) = E(\mathbb{Q}_p)$. Then,

$$E_0(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) \cong \tilde{E}(\mathbb{F}_p). \tag{2.18}$$

Similarly, for $n \geq 1$ we can define $E_n(\mathbb{Q}_p)$ as

$$E_n(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : v_p(x(P)) \leq -2n, v_p(y(P)) \leq -3n\} \cup \{O\}.$$

Due to (Silverman, 2009), we have the following "filtration" admitted by $E_0(\mathbb{Q}_p)$,

$$E_0(\mathbb{Q}_p) \supset E_1(\mathbb{Q}_p) \supset E_2(\mathbb{Q}_p) \supset \ldots,$$

where for each $n \geq 1$, $E_n(\mathbb{Q}_p)$ is isomorphic to $p^n\mathbb{Z}_p$. Hence, the quotient $E_n(\mathbb{Q}_p)/E_{n+1}(\mathbb{Q}_p)$ is isomorphic to $p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p$ which is the residue field of $\mathbb{Z}_p$, namely $\mathbb{F}_p$. So, we get

$$E_n(\mathbb{Q}_p)/E_{n+1}(\mathbb{Q}_p) \cong \mathbb{F}_p. \tag{2.19}$$

In fact, we have a chain of isomorphisms

$$E_n(\mathbb{Q}_p) \cong \hat{E}(p^n\mathbb{Z}_p) \cong p^n\mathbb{Z}_p$$

for $n \geq 1$ where the middle object is the group of $p\mathbb{Z}_p$-valued points of the one-parameter formal group associated to E. (For the theory of formal groups, see

(Silverman, 2009, Chapter IV)). The isomorphism map from $E_n(\mathbb{Q}_p)$ to $p^n\mathbb{Z}_p$ is explicitly given in (Leprévost et al., 2005) and (Blake, Seroussi & Smart, 1999) as

$$\log_{\mathcal{F}} \circ \vartheta_p^{-1} \colon E_n(\mathbb{Q}_p) \to p^n\mathbb{Z}_p$$

where

$$\begin{aligned} \vartheta_p \colon \hat{E}(p^n\mathbb{Z}_p) &\to E_n(\mathbb{Q}_p) \\ z &\mapsto \begin{cases} O & \text{if } z = 0 \\ \left(\frac{z}{w(z)}, \frac{-1}{w(z)}\right) & \text{otherwise, i.e., } z = -x/y \end{cases} \end{aligned}$$

with $w(z)$ is the power series in z, and

$$\log_{\mathcal{F}} \colon \hat{E}(p^n\mathbb{Z}_p) \to p^n\mathbb{Z}_p$$

with $\log_{\mathcal{F}}$ is an isomorphism satisfying $\log_{\mathcal{F}} F(z_1, z_2) = \log_{\mathcal{F}} F(z_1) + \log_{\mathcal{F}} F(z_2)$.

2.7 Elliptic Divisibility Sequences

Elliptic divisibility sequences are special class of divisibility sequences. They are the first example of divisibility sequences that are defined by a nonlinear recurrence relation. Moreover, they are closely related to elliptic curves.

Let R be an integral domain.

Definition 2.7.1. A *divisibility sequence* (*DS*) is a recurrence sequence $a : \mathbb{Z} \to R$ satisfying the property that a_n divides a_m whenever $n \mid m$ for all $n, m \in \mathbb{Z}$ where $a_n = a(n)$.

A full characterisation of divisibility sequences can be found in (Bézivin, Pethö & van der Poorten, 1990).

Example. The Fibonacci sequence $f : \mathbb{Z} \to \mathbb{Z}$ is defined by the recurrence relation $f_{n+2} = f_{n+1} + f_n$ and the initial conditions $f_0 = 0$, $f_1 = 1$ is a DS.

Recall from linear algebra that the closed form for the n^{th} term of the Fibonacci sequence is that

$$f_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

Assume that $n \mid m$ such that $nk = m$, and let $a = \frac{1+\sqrt{5}}{2}$ and $b = \frac{1-\sqrt{5}}{2}$. Then

$$f_m = \frac{a^m - b^m}{\sqrt{5}} = \frac{a^n - b^n}{\sqrt{5}} \left(a^{n(k-1)} + a^{n(k-2)} b^n \cdots + a^n b^{n(k-2)} + b^{n(k-1)} \right)$$
$$f_m = f_n \left(a^{n(k-1)} + a^{n(k-2)} b^n \cdots + a^n b^{n(k-2)} + b^{n(k-1)} \right).$$

The quantity $f_m / f_n = a^{n(k-1)} + a^{n(k-2)} b^n \cdots + a^n b^{n(k-2)} + b^{n(k-1)}$ is an integer since a and b are conjugates of each other, therefore $f_n \mid f_m$.

Definition 2.7.2. An *elliptic divisibility sequence* (*EDS*) is a DS satisfying the recurrence relation

$$W_{m+n} W_{m-n} = W_{m+1} W_{m-1} W_{n^2} - W_{n+1} W_{n-1} W_{m^2} \text{ for all } m, n \in \mathbb{Z}.$$

The study of EDS was introduced by (Ward, 1948). In his context, R is taken to be $\mathbb{Z}$, namely he studied integer elliptic divisibility sequences.

Remark. All integer EDSs have the property that $W_0 = 0, W_1 = \pm 1, W_{-n} = -W_n$ for all $n \in \mathbb{Z}$.

Example. The sequence $A : \mathbb{Z} \to \mathbb{Z}$ defined by $A_n = n$ is an EDS, since

$$A_{m+n} A_{m-n} = (m+n)(m-n) = m^2 - n^2$$

and

$$\begin{aligned} A_{m+1} A_{m-1} A_{n^2} - A_{n+1} A_{n-1} A_{m^2} &= (m+1)(m-1)n^2 - (n+1)(n-1)m^2 \\ &= m^2 n^2 - n^2 - n^2 m^2 + m^2 \\ &= m^2 - n^2 \end{aligned}$$

are equal, and it is clear that $n \mid m$ implies $A_n \mid A_m$.

Example. The Fibonacci sequence (f_n) is an EDS as well.

Another example of an EDS is that division polynomials of elliptic curves evaluated at a point P on the curve. In fact, almost all EDSs are of this form. An EDS is called *proper* if it satisfies $W_0 = 0$, $W_1 = 1$ and $W_2 W_3 \neq 0$. Ward proves that a proper EDS is associated to a pair of elliptic curve, possibly singular, and a point on the curve. Additionally, (Shipsey, 2000, Theorem 4.3.1) fromalize the relationship between the elliptic curves and EDSs. More information on division polynomials will be given after stating some important results regarding the integer EDSs.

In an integer EDS, multiples of most primes are regularly spaced; the length of this

space is denoted by N and it is called the gap of p. More precisely, *gap of* p is the integer satisfying the assumptions of the following theorem.

Theorem 2.7.1. *(Ward, 1948, Theorem 5.2) Let* (W_n) *be an integer EDS, and let* p *be a prime dividing a term of the sequence with positive index and not dividing* W_2 *or* W_3*. Let* N *be the smallest positive integer among the indices of the terms that are divisible by* p*. If* $W_{N+1} \not\equiv 0 \pmod{p}$*, then*

$$W_n = 0 \pmod{p} \iff n \equiv 0 \pmod{N}.$$

The below result is called a *symmetry formula*; it expresses the term of an EDS modulo a prime p in terms of some constants and a term whose index is the index of the original term reduced modulo the gap of p.

Theorem 2.7.2. *(Shipsey & Swart, 2008, Theorem 2) Let* (W_n) *be an integer EDS, and let* p *be a prime not dividing* W_2 *or* W_3*, and let* p *have gap* N *in* (W_n)*. Then there exist two integers* c *and* d *such that* $d^2 \equiv c^N \pmod{p}$*, and for all* $s,t \in \mathbb{Z}$*,*

$$W_{t+sN} \equiv c^{st} d^{s^2} W_t \pmod{p}.$$

Moreover, the integers c, d *are given as* $c \equiv \frac{W_{-2}W_{N-1}}{W_{-1}W_{N-2}} \pmod{p}$ *and* $d \equiv \frac{W_2 (W_{N-1})^2}{(W_{-1})^2 W_{N-2}} \pmod{p}$.

Considering Theorem 2.7.1 and 2.7.2, it is natural to expect that an EDS is a periodic sequence. So, we define a condition to determine the period of (W_n) in the next theorem for completeness of the subject.

Corollary 2.7.2.1. *(Ward, 1948, Theorem 10.1) Let* $(W_n), p, N, c, d$ *be as in Theorem 2.7.2. Let* τ *be the smallest positive integer such that*

$$d^{\tau^2} \equiv c^{\tau} \equiv 1 \pmod{p}.$$

Then (W_n) *is purely periodic with period* τN*.*

2.8 Division Polynomials

Now, we will introduce an important family of elliptic divisibility sequences, namely the sequence of division polynomials (ψ_n) that is defined through an elliptic curve

E/K. As explained in the previous section, almost all EDSs (W_n) can be associated to a pair of an elliptic curve E/K and a point P on the curve so that $W_n = \psi_n(P)$ for all n.

Definition 2.8.1. Let E/K be an elliptic curve described by

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

where $a_i \in K$. For a positive integer $n \neq 0$, the n^{th} *division polynomial* $\psi_n \in \mathbb{Z}[x, y, a_1, a_2, a_3, a_4, a_6]$ is given by initial conditions and recurrence relations as follows

$$\begin{aligned}
\psi_1 &= 1, \\
\psi_2 &= 2y + a_1x + a_3, \\
\psi_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8, \\
\psi_4 &= \psi_2 \cdot (2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)),
\end{aligned}$$

where b_i's are defined as in Section 2.1, and

$$\psi_{2n+1} = \psi_n^3\psi_{n+2} - \psi_{n-1}\psi_{n+1}^3 \text{ for } n \geq 2, \tag{2.20}$$

$$\psi_2\psi_{2n} = \psi_{n-1}^2\psi_n\psi_{n+2} - \psi_{n-2}\psi_n\psi_{n+1}^2 \text{ for } n \geq 3. \tag{2.21}$$

For convention ψ_0 is taken to be 0.

The sequence of division polynomials (ψ_n) arises from the multiplication-by-n map for elliptic curves. The following theorem summarizes the fundamental results about division polynomials.

Theorem 2.8.1. *(Enge, 1999, Proposition 3.51) The following identities are valid for $m, n > 0$*

$$\psi_{-n} = -\psi_n, \tag{2.22}$$

$$\psi_n^2 = n^2 \sum_{P \in E[n] \setminus \{O\}} x - x(P), \tag{2.23}$$

$$\psi_n \in \begin{cases} K[x] & \text{if } n \text{ is odd} \\ (2y + a_1x + a_3)K[x] & \text{if } n \text{ is even} \end{cases} \tag{2.24}$$

$$\psi_m\psi_n \in K[x] \text{ if } m \text{ and } n \text{ has the same parity.} \tag{2.25}$$

The result (2.22) enables us to extend the index of ψ_n to all integers. The result

(2.23) means that $P \neq O$ is an n-torsion point if and only if ψ_n vanishes at P, i.e.,

$$nP = O \iff \psi_n(P) = 0. \tag{2.26}$$

Theorem 2.8.2. *(Enge, 1999, Proposition 3.53) Division polynomials satisfy the following recurrence relation*

$$\psi_{m+n}\psi_{m-n} = \psi_{m+1}\psi_{m-1}\psi_{n^2} - \psi_{n+1}\psi_{n-1}\psi_{m^2} \text{ for all } m, n \in \mathbb{Z}.$$

Notice that by definition of torsion points, if $n \mid m$ then $E[n] \subseteq E[m]$. The result (2.23) implies that if $n \mid m$ then $\psi_n \mid \psi_m$, therefore (ψ_n) is a divisibility sequence. Furthermore, Theorem 2.8.2 means that it is in fact an elliptic divisibility sequence.

Consider that the sequence of division polynomials arising from an elliptic curve E/K is evaluated at a point $P \in E$ so that $\psi_n(P) \in K$ for all n. This sequence $(\psi_n(P))$ does not necessarily form an integer EDS since R in Definition 2.7.2 can be replaced by a finite field of size q, namely $\mathbb{F}_q$. The analogous versions of the theorems given for integer EDSs in Section 2.7 will be given for EDSs obtained by the division polynomials of elliptic curves defined over a finite field and evaluated at a point in Section 2.9.3.

Let $n \in \mathbb{Z}$, and define

$$\begin{aligned} \phi_n &= x\psi_n^2 - \psi_{n+1}\psi_{n-1}, \\ 4y\omega_n &= \psi_{n-1}^2\psi_{n+2} - \psi_{n+1}^2\psi_{n-2}. \end{aligned}$$

Lemma 2.8.3. *(Washington, 2008, Lemma 3.5) The leading term of ϕ_n and ψ_n are x^{n^2} and $n^2x^{n^2-1}$, respectively.*

Lemma 2.8.4. *ϕ_n and ψ_n have no common root, i.e., they are relatively prime.*

This result is shown in the proof of (Washington, 2008, Corollary 3.6)

Recall that for any point $P = (x_P, y_P)$ on any elliptic curve, the x-coordinate of $2P$ is given by $\frac{x_P^4 - b_4x_P^2 - 2b_6x_P - b_8}{4x_P^3 + b_2x_P^2 + 2b_4x_P + b_6} = \frac{x_P^4 - b_4x_P^2 - 2b_6x_P - b_8}{(2y + a_1x_P + a_3)^2}$. Observe that P is a 2-torsion

point if and only $P+P=O$, i.e.,

$$\begin{aligned} P \in E[2] &\iff 2P = (0:1:0) \\ &\iff x(2P) \text{ is undefined in affine coordinates} \\ &\iff P \text{ is a root of the denominator of } x(2P) \\ &\iff P \text{ is a root of } (2y + a_1 x_P + a_3)^2 = \psi_2^2. \end{aligned}$$

The following theorem is derived by generalizing this idea and is useful in calculating nP for $n \in \mathbb{Z}$.

Theorem 2.8.5. *(Washington, 2008, Theorem 3.6) Let E/K be an elliptic curve, and $P = (x, y) \in E$. For positive integer $n \geq 2$,*

$$nP = \left(\frac{\phi_n(P)}{\psi_n(P)^2}, \frac{\omega_n(P)}{\psi_n(P)^3} \right)$$

where $\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}$, and $4y\omega_n = \psi_{n-1}^2\psi_{n+2} - \psi_{n+1}^2\psi_{n-2}$, in particular,

$$x(nP) = x - \frac{\psi_{n+1}(P)\psi_{n-1}(P)}{\psi_n(P)^2}.$$

An immediate corollary of this theorem is that multiplication-by-n map has degree n^2 since the polynomials defining the numerator and the denominator of the x-coordinate of nP has no common roots and maximum of their degree is n^2. This is one way to see Theorem 2.2.3.

The property of division polynomials given in the next theorem is called chain rule. Similar results are valid for ϕ_n and ω_n since they are defined in terms of ψ_n's.

Theorem 2.8.6. *(Ayad, 1992, (2.3)) Let E/K be an elliptic curve. If $P \in E$, then the division polynomials satisfy*

$$\psi_{nk}(P) = \psi_k(P)^{n^2} \psi_n(kP) \text{ for all } n, k \in \mathbb{Z},$$

as long as $kP \neq O$.

2.9 Elliptic Curves over Finite Fields

Let p be a prime and $q = p^r$ for some positive integer r, then $\mathbb{F}_q$ is a *finite field* of size q with characteristic p. The $\mathbb{F}_q$-rational points of an elliptic curve defined over $E/\mathbb{F}_q$ is

$$E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}.$$

Obviously, the number of points of $E(\mathbb{F}_q)$, denoted as $\#E(\mathbb{F}_q)$, is bounded from above by $2q+1$ since there are q many x candidates, and for each x there are two many y candidates, also there is the base point O. However, due to Hasse there is a better bound for $\#E(\mathbb{F}_q)$.

Theorem 2.9.1 (Hasse Bound)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve. Then*

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

Generalization of the above result for any absolutely irreducible smooth projective curve C defined over $\mathbb{F}_q$ with genus g is called *Hasse-Weil bound*; $|\#C(\mathbb{F}_q) - q - 1| \leq 2g\sqrt{q}$. Note that genus g of the elliptic curve is 1.

2.9.1 Trace of the Frobenius Endomorphism

We will introduce an important endomorphism between elliptic curves defined over a finite field, namely the Frobenius endomorphism ϕ_q. Then we will derive an equality to express the size of $E(\mathbb{F}_q)$ depending on the trace of this map when considered as a linear transformation of n-torsion points.

Definition 2.9.1. Let K be a finite field of characteristic p, and q be a power of p. The *q^{th}-power Frobenius map*, or *q^{th}-power map*, is

$$\begin{aligned} \phi_q \colon K &\to K \\ x &\mapsto x^q. \end{aligned}$$

It is an endomorphism of K, it is also called the *Frobenius endomorphism*. Moreover,

if K has size q then ϕ_q is the identity.

Let E/K be an elliptic curve, then ϕ_q acts on the coordinates of points on E as

$$\begin{aligned} \phi_q \colon E &\to E^{(q)} \\ (x, y) &\mapsto (x^q, y^q) \\ O &\mapsto O \end{aligned}$$

where $E^{(q)}$ is defined by the Weierstrass equation of E whose coefficients are raised to the power q, clearly the coefficients are still in K, therefore $E^{(q)}$ is defined over K as well. Moreover, the discriminant of $E^{(q)}$, namely $\Delta(E^{(q)})$, is equal to $(\Delta(E))^q$ since discriminant is a formula depending on the coefficients of the Weierstrass equation of the curve which are in K and ϕ_q is a homomorphism of K. Therefore, the discriminant of $E^{(q)}$ is not zero, and $E^{(q)}/K$ is an elliptic curve as well.

Now, if we suppose that $K = \mathbb{F}_q$, then $E^{(q)} = E$ (because ϕ_q is the identity on K) and ϕ_q becomes an endomorphism of E, in particular it is called the *Frobenius endomorphism of E*.

Observe that the set of elements in K that is fixed by ϕ_q must satisfy the equation $x^q = x$, i.e., $x(x^{q-1} - 1) = 0$. Also, there are $q-1$ many nonzero elements of $\mathbb{F}_q$, consequently their order is divisible by $q-1$, i.e., they satisfy $x^{q-1} - 1$. The number of possible roots of $x^{q-1} - 1$ is $q-1$ as well. Therefore, elements of K fixed by ϕ_q are exactly the elements of $\mathbb{F}_q$. Similarly, points of E fixed by ϕ_q is exactly $E(\mathbb{F}_q)$. Therefore, we deduce the following results

$$\phi_q(x) = x \iff x \in \mathbb{F}_q, \tag{2.27}$$

$$\phi_q(P) = P \iff P \in E(\mathbb{F}_q). \tag{2.28}$$

Remark. The statement given in (2.28) implies that $\phi_q(P) - P = O$ if and only if $P \in E(\mathbb{F}_q)$. In other words,

$$Ker(\phi_q - 1) = E(\mathbb{F}_q). \tag{2.29}$$

By the above results, if $E/\mathbb{F}_q$ is an elliptic curve, then $E^{(q)} = E$ and $\phi_q \in \mathrm{Gal}\,(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. Furthermore, any element σ in $\mathrm{Gal}\,(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ acts on $E[l]$ because

$$P \in E[l] \Rightarrow lP = O \Rightarrow l(P^\sigma) = (lP)^\sigma = O^\sigma = O.$$

Therefore, considering that $E[l] \cong \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$ for l such that $\gcd(l, p) = 1$, we can

write the following representation

$$\mathrm{Gal}\,(\bar{\mathbb{F}}_q/\mathbb{F}_q) \to \mathrm{Aut}(E[l]) \cong \mathrm{Aut}(\mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z}).$$

This implies that the image of $\sigma \in \mathrm{Gal}\,(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ can be represented by a 2×2 matrix with entries from $\mathbb{Z}/l\mathbb{Z}$ where the matrix depends on the basis chosen for the $E[l]$. Let's denote the matrix representative of the image of $\phi_q \in \mathrm{Gal}\,(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ by $(\phi_q)_l$, then we can associate a determinant and trace to $(\phi_q)_l$.

The general idea is that for an elliptic curve defined over $\mathbb{F}_q$ and for l such that $\gcd(l,p) = 1$ if $\alpha : E(\bar{K}) \to E(\bar{K})$ is an endomorphism, then α necessarily maps $E[l]$ to $E[l]$. Hence, due to Theorem 2.3.1, it can be represented by a 2×2 matrix, call it α_l with entries $a, b, c, d \in \mathbb{Z}/l\mathbb{Z}$ as

$$\alpha_l = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{2.30}$$

This matrix describes the action of α on a basis $\{B_1, B_2\}$ of $E[l]$.

Now, several propositions will be given in order to define the relation between the trace t of ϕ_q and size of $E(\mathbb{F}_q)$.

Proposition 2.9.1. *(Washington, 2008, Lemma 2.20) Let $E/\mathbb{F}_q$ be an elliptic curve. Then ϕ_q is an endomorphism of E of degree q, and ϕ_q is not separable.*

Proposition 2.9.2. *(Washington, 2008, Proposition 2.21) Let $\alpha \neq 0$ be a separable endomorphism of an elliptic curve E. Then*

$$deg(\alpha) = \#Ker(\alpha),$$

where $Ker(\alpha)$ is the kernel of the homomorphism $\alpha : E(\bar{K}) \to E(\bar{K})$.

By Proposition 2.9.2, we can conclude that since degree of an endomorphism by definition is a finite number, then so does the kernel of the nonzero separable endomorphism.

Proposition 2.9.3 (Proposition 2.29, (Washington, 2008))**.** *Let $E/\mathbb{F}_q$ be an elliptic curve. Let r and s be integers, not both 0. The endomorphism $r\phi_q + s$ separable if and only if $p \nmid s$.*

Proposition 2.9.4 (Proposition 3.15, (Washington, 2008))**.** *Let α be an endomorphism of an elliptic curve E/K. Let n be a positive integer not divisible by the* $\mathrm{char}(K)$*. Then $det(\alpha_l) \equiv deg(\alpha) \pmod{l}$ where α_l is given by (2.30).*

Theorem 2.9.2. *Let $E/\mathbb{F}_q$ be an elliptic curve. Let $t = q+1-\#E(\mathbb{F}_q)$. Then*

$$\phi_q^2 - t\phi_q + q = 0 \tag{2.31}$$

as endomorphisms of E, and t is the unique integer k such that

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

In other words, if $(x,y) \in E(\bar{\mathbb{F}}_q)$,then

$$(x^{q^2}, y^{q^2}) - t(x^q, y^q) + q(x,y) = O,$$

and t is the unique integer such that this relation holds for all $(x,y) \in E(\bar{\mathbb{F}}_q)$. Moreover, t is the unique integer satisfying

$$t \equiv Trace((\phi_q)_l) \pmod{l}$$

for all l with gcd(l,q)=*1.*

Proof. Proposition 2.9.2 implies that if the kernel of a separable homorphism is not finite then it is the zero endomorphism. Therefore, to prove (2.31), it is enough to show that kernel of $\phi_q^2 - t\phi_q + q$ is infinite.

Let l be an integer such that $\gcd(l,q) = 1$. Recalling (2.30), we can represent the action of ϕ_q on $E[l]$ by a matrix $(\phi_q)_l$ given as

$$(\phi_q)_l = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

By the following sequence of equailities and congruences

$$\begin{aligned}
q+1-t &= \#E(\mathbb{F}_q) && \text{(by the hypothesis)} \\
&= \#Ker(\phi_q - 1) && \text{(by the equality 2.29)} \\
&= deg(\phi_q - 1) && \text{(by the Propositions 2.9.3 and 2.9.2)} \\
&\equiv det((\phi_q)_l - I_2) \pmod{l} && \text{(by the Proposition 2.9.4)} \\
&\equiv ad - bc - (a+d) + 1 \pmod{l} \\
&\equiv det((\phi_q)_l) - (a+b) + 1 \pmod{l} \\
&\equiv q - (a+b) + 1 \pmod{l} && \text{(by the Proposition 2.9.4)} \\
&\equiv q - Trace((\phi_q)_l) + 1 \pmod{l},
\end{aligned}$$

we single out that

$$t \equiv Trace((\phi_q)_l) \pmod{l}$$

which proves the moreover part of the theorem. By the Cayley-Hamilton Theorem, a square matrix A over a commutative ring satisfies its own characteristic equation which for a 2×2 matrix is that $x^2 - Trace(A)x - det(A) = 0$, we have

$$(\phi_q)_l^2 - t(\phi_q)_l + qI_2 \pmod{l}.$$

This means that $\phi_q^2 - t\phi_q + q$ is identically zero on $E[l]$. Obviously, there are infinitely many choice for l, therefore kernel of $\phi_q^2 - t\phi_q + q$ is infinite. Hence, it is the zero endomorphism.

To prove uniqueness of t over the integers, assume for a contradiction that there exists another integer t' satisfying $\phi_q^2 - t'\phi_q + q = 0$. Then

$$(t - t')\phi_q = (\phi_q^2 - t'\phi_q + q) - (\phi_q^2 - t\phi_q + q) = 0.$$

Since ϕ_q is a nonconstant endomorphism, it is surjective on the elliptic curve by Theorem 2.2.2. Hence, ϕ_q is an automorphism of $E(\bar{\mathbb{F}}_q)$, so $(t - t')$ annihilates $E(\bar{\mathbb{F}}_q)$, in particular, it annihilates $E[l]$ for for every $l \geq 1$. If gcd(l, q)=1, then $E[l]$ contains points of order l. So $(t - t') \equiv 0 \pmod{l}$. Therefore by Chinese Remainder Theorem, $t - t' = 0$ which proves the uniqueness of t. □

Definition 2.9.2. The quantity t where $t = q + 1 - \#E(\mathbb{F}_q)$ is called the *trace of the Frobenius endomorphism.*

The quantity t depends on q which is the size of the field that the elliptic curve E is defined over. Therefore, sometimes this quantity is denoted as t_q. It provides a tool to calculate the number of $\mathbb{F}_q$-rational points on an elliptic curve defined over $\mathbb{F}_q$. Furthermore, trace t enables us to calculate the size of an elliptic curve in the extension field of $\mathbb{F}_q$.

Theorem 2.9.3. *(Washington, 2008, Theorem 4.12) Let $t = q + 1 - \#E(\mathbb{F}_q)$, then*

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

where α, β are complex numbers determined from the factorization of $X^2 - tX + q = (1 - \alpha X)(1 - \beta X)$, for all $k \geq 1$.

Remark. (Schoof, 1985) Schoof's algorithm uses Theorem 2.9.2 to calculate $\#E(\mathbb{F}_q)$; it is a deterministic polynomial time algorithm. He computes the value of the trace modulo distinct primes l_i (i.e. the value τ satisfying $\phi_{l_i}^2 - \tau\phi_{l_i} + q = 0$ where $\tau \in$

$\mathbb{Z}/l\mathbb{Z}$) whose product ($\prod_i l_i$) is greater than the length of the interval for the value of the trace ($4\sqrt{q}$) that is attained by the Hasse's Theorem, hence finds the correct value of the trace over integers using the Chinese Remainder Theorem which immediately gives $\#E(\mathbb{F}_q)$. As a side note, Elkies and Atkin made Schoof's algorithm more efficient but probabilistic; so it is now called the SEA Algorithm.

2.9.2 Classification of the Group Structure

The aim of this section is to present the theorems that will enable us to determine whether an elliptic curve over a finite field with certain order exist or not. Moreover, if it exists, we can find its corresponding group structure.

We start by stating the group structure of $E(\mathbb{F}_q)$ in general.

Theorem 2.9.4. *Let $E/\mathbb{F}_q$ be an elliptic curve. Then*

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}, \text{ or}$$
$$E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \text{ with } n_1 \mid n_2.$$

Proof. Since $E(\mathbb{F}_q)$ is a finite abelian group, by the Structure Theorem for Finite Abelian Groups, we can write

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \text{ with } n_i \mid n_{i+1} \text{ for } i \geq 1.$$

This implies that $E(\mathbb{F}_q)$ contains n_1^r points of order dividing n_1. Due to Theorem 2.3.1 we know that $\#E[n_1] \leq n_1^2$, so we conclude that $r \leq 2$. Hence, the result follows: If $n_1 = 1$, then we write $E(\mathbb{F}_q) \cong \mathbb{Z}/n_2\mathbb{Z}$. If $n_1 \neq 1$, we write $E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$. □

Now, we will state a theorem to determine whether a group $E(\mathbb{F}_q)$ of certain order exists.

Theorem 2.9.5 (Waterhouse (1969))**.** *Let p be a prime and $q = p^r$. There is an elliptic curve $E/\mathbb{F}_q$ such that $\#E(\mathbb{F}_q) = q + 1 - t$ if and only if $|t| \leq 2\sqrt{q}$ and t satisfies one of the followings*

(1) $\gcd(t, p) = 1$

(2) $t^2 = 4q$ *and r is even*

(3) $t^2 = q$, $p \not\equiv 1 \pmod 3$ *and* r *is even*

(4) $t^2 = pq$, $p \in \{2,3\}$ *and* r *is odd*

(5) $t = 0$ *and either* r *is odd or* $p \not\equiv 1 \pmod 4$.

The next theorem defines the group structure of each case in the above theorem.

Note that by the notion of trace t associated to an elliptic curve E defined over a finite field $\mathbb{F}_q$, we can give an alternative condition to determine whether an elliptic curve is supersingular or ordinary.

Elliptic curves corresponding to the case (1) in the above theorem are called *ordinary*, and the result about their group structure is proved by both (Voloch, 1988) and (Rück, 1987), separately. Elliptic curves corresponding to the other cases, simply the ones with $p \mid t$, are called *supersingular*, and the results about their group structure is proved by (Schoof, 1987).

Theorem 2.9.6. *Let* p,q,r,t *be as in Theorem 2.9.5, and let* $n = \#E(\mathbb{F}_q)$. *The corresponding group structure of each case is as follows:*

(1) Let $n = \prod_{\substack{l \mid n \\ l \text{ prime}}} l^{v_l(n)}$ *be the prime factorization of* n. *There are integers* $0 \le a_l \le min\{v_l(q-1), \lfloor \frac{v_l(n)}{2} \rfloor\}$ *such that the group is*

$$\mathbb{Z}/p^{v_p(n)}\mathbb{Z} \oplus \bigoplus_{l \neq p} (\mathbb{Z}/l^{a_l}\mathbb{Z} \oplus \mathbb{Z}/l^{v_l(n)-a_l}\mathbb{Z})$$

(2) Either $\mathbb{Z}/(\sqrt{q}+1)\mathbb{Z} \oplus \mathbb{Z}/(\sqrt{q}+1)\mathbb{Z}$ *or* $\mathbb{Z}/(\sqrt{q}-1)\mathbb{Z} \oplus \mathbb{Z}/(\sqrt{q}-1)\mathbb{Z}$, *depending on whether* $t = 2\sqrt{q}$ *or* $t = -2\sqrt{q}$

(3) Cyclic

(4) Cyclic

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

As a final result, for future reference, we state a necessary and sufficient condition for $E(\mathbb{F}_q)$ to contain $E[n]$.

Theorem 2.9.7. *(Schoof, 1987, 3.7) Let* $E/\mathbb{F}_q$ *be an elliptic curve. If* $\gcd(n,q) = 1$, *then* $E[n] \subset E(\mathbb{F}_q)$ *if and only if the followings are satisfied:*

(i) $n^2 \mid \#E(\mathbb{F}_q)$

(ii) $n \mid q-1$

(iii) Either $\phi \in \mathbb{Z}$ *or* $\mathcal{O}\left(\frac{t^2-4q}{n^2}\right) \subset End_{\mathbb{F}_q(E)}$*, where* ϕ *is the Frobenius endomorphism and* t *is its trace.*

2.9.3 Elliptic Divisibility Sequences and Division Polynomials

As we mentioned in Section 2.8, the sequence of division polynomials of elliptic curves when evaluated at a point, namely $(\psi_n(P))$, form an elliptic divisibility sequence. If E is defined over a finite field $\mathbb{F}_q$, the aforementioned EDS is not necessarily an integer EDS. However, they satisfy the analogous results of theorems that are satisfied by integer EDSs as given in Section 2.7.

Recall the result (2.26). This implies that the order of a point $P \in E$ for the sequence $(\psi_n(P))$ acts as the gap of a prime p for an integer EDS (W_n).

The following theorem is analogous for Theorem 2.7.2

Theorem 2.9.8. *(Silverman, 2005, Theorem 8) Let* $E/\mathbb{F}_q$ *be an elliptic curve, and let* $P \in E$ *be a point of order* $N \geq 3$*. Then there exists constants* $c, d \in \mathbb{F}_q$ *such that* $d^2 = c^N$ *and for all* $s, t \in \mathbb{Z}$*,*

$$\psi_{t+sN}(P) = c^{st} d^{s^2} \psi_t(P) \text{ in } \mathbb{F}_q.$$

Similarly, the following is analogous for Corollary 2.7.2.1.

Corollary 2.9.8.1. *(Silverman, 2005, Corollary 9) Let* $E, P, (\psi_n(P), N, c, d$ *be as in Theorem 2.7.2. Let* τ *be the smallest positive integer such that*

$$d^{\tau^2} = c^\tau = 1 \text{ in } \mathbb{F}_q.$$

Then $(\psi_n(P))$ *is purely periodic with period* τN*.*

3. DISCRETE LOGARITHM PROBLEM ON ELLIPTIC CURVES OVER FINITE FIELDS

Elliptic curves have been introduced to cryptography by (Miller, 1985) and (Koblitz, 1987) independently, and they have many applications in cryptography. The security of most cryptosystems relies on computationally hard mathematics problems, meaning that there is no general algorithm solving the problem in subexponential time using the classical computers. One of the most commonly used such problem is called the *discrete logarithm problem (DLP)* and it is stated as below.

Given $b \in \langle g \rangle$ where g is an element of the group $(G, *)$, find x such that $b = g^x \in G$.

In general, the group G is taken to be a finite field. So, when we say DLP, unless otherwise mentioned, it must be understood that $G = \mathbb{F}_q$. When G is taken to be the group of rational points of an elliptic curve over a finite field, the problem is called the *elliptic curve discrete logarithm problem (ECDLP)*, and there is still no general subexponential algorithm that solves the problem. In fact, the elliptic curve version of the problem is more commonly used since it is believed to be much harder as it provides higher security level by requiring smaller key that is used in the encryption or decryption. Consequently, using the ECDLP becomes more efficient. The statement of the ECDLP is as follows.

Given $Q \in \langle P \rangle$ and a point P in $(E(\mathbb{F}_q), +)$, find x such that $Q = xP \in E(\mathbb{F}_q)$.

The smallest positive x which is a solution of the DLP and ECDLP is called the logarithm of b and Q, respectively.

Although the discrete logarithm problem on elliptic curves over finite fields is conjectured to be hard, for particular curves with a certain number of rational points the problem can be solved or reduced to an easier problem by utilizing the theory of elliptic curves. The method of solving a problem or reducing to an easier problem is called an attack. In this chapter, we describe some of the important attacks for the ECDLP. The attacks are primarily classified according to the trace t of the given

elliptic curve over $\mathbb{F}_q$, that is an integer determined solely by the number of points on the elliptic curve. To be more specific,

$$t = q + 1 - \#E(\mathbb{F}_q).$$

In general, the order of the point P that is used in the ECDLP is assumed to be a large prime number. If the order of P is a product of distinct primes, namely $p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$, the logarithm of Q can be solved modulo each $p_i^{k_i}$ and then result can be calculated modulo $p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$ by Chinese Remainder Theorem. This method is known as Pohlig Hellman algorithm. In fact, bare minimum condition for an elliptic curve to be used in cryptography is that the order of $E(\mathbb{F}_q)$ to have a large prime divisor.

Each attack to be described in this chapter and in Section 4.3.1 solves the ECDLP or reduces to a DLP in a finite field, for which there exists a subexponential time attack called as index calculus method.

3.1 Attack For Supersingular Curves

This section is based on (Menezes et al., 1993).

The algorithm to be explained uses a bilinear mapping, namely Weil pairing, to reduce the ECDLP, the problem of finding k when given P and kP on $E/\mathbb{F}_q$, to the DLP in an extension $\mathbb{F}_{q^s}$. The importance of the algorithm is that if we assume that the curve is supersingular, then this reduction takes probabilistic polynomial time. Moreover, if q is a prime or $q = p^r$ where p is small, then the algorithm to be proposed can solve for k in probabilistic subexponential time as proven in (Theorem 11 and Corollary 12,(Menezes et al., 1993)).

The key idea of the algorithm is establishing an isomorphism between the subgroup of E generated by P, with order N, and the subgroup of N^{th} roots of unity in $\mathbb{F}_{q^s}$ where s is the smallest integer such that $\mathbb{F}_{q^s}$ contains the N^{th} roots of unity. This isomorphism is given by Theorem 2.5.3.

Let $E/\mathbb{F}_q$ be an elliptic curve, with group structure $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ with $n_1 \mid n_2$, and let N to denote the order of P. Assume that $\gcd(\#E(\mathbb{F}_q), q) = 1$ which implies that for any point $P \in E(\mathbb{F}_q)$ with order N, we can conclude that $P \in E[n] \cong$

$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Moreover, we will assume that the curve is supersingular for the reason that is explained in the next remark.

The reduction process is described as follows. First, one needs to determine the smallest integer s such that $E[N]$ is contained in $E(\mathbb{F}_{q^s})$ which implies that $\mathrm{Im}(e_N) \subseteq \mathbb{F}_{q^s}$ by the property of the Weil pairing (Theorem 2.5.1). The necessary and sufficient condition for $E(\mathbb{F}_q)$ to contain all N-torsion points in $E(\mathbb{F}_q)$ is given by Theorem 2.9.7. The integer s when E is supersingular can be found in the Table 3.1 which classifies the supersingular curves according to their trace t and gives the corresponding value of such s for each possible case. Moreover, if the curve is supersingular, then the group $E(\mathbb{F}_{q^s})$ has a certain structure given as $\mathbb{Z}/cn_2\mathbb{Z} \times \mathbb{Z}/cn_2\mathbb{Z}$. The corresponding value of s is calculated by applying the Weil conjecture and using Theorem 2.9.6. One can find the values of s and c from Table 3.1.

Remark. In the case that E is not assumed to be supersingular, there is still an algorithm in (Menezes et al., 1993, Algorithm 2) to reduce the ECDLP to DLP but it takes exponential time in general as s can be exponentially large in general. The calculation of s in the general case can be achieved by (Van Tuyl, Van Tuyl).

	t	Structure of $E(\mathbb{F}_q)$	$\mathbf{n_2}$	$\mathbf{c}$	s
I	0	cyclic	$q+1$	1	2
II	0	$\mathbb{Z}/(q+1)/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$(q+1)/2$	2	2
III	$\pm\sqrt{q}$	cyclic	$q+1\mp\sqrt{q}$	$\sqrt{q}\pm 1$	3
IV	$\pm\sqrt{2q}$	cyclic	$q+1\mp\sqrt{2q}$	$q\pm\sqrt{2q}+1$	4
V	$\pm\sqrt{3q}$	cyclic	$q+1\mp\sqrt{3q}$	$(q+1)(q\pm\sqrt{3q}+1)$	6
VI	$\pm 2\sqrt{q}$	$\mathbb{Z}/\sqrt{q}\mp 1\mathbb{Z} \times \mathbb{Z}/\sqrt{q}\mp 1\mathbb{Z}$	$\sqrt{q}\mp 1$	1	1

Table 3.1 Some information about supersingular curves

Next, one needs to find $R \in E[N]$ such that $\alpha = e_N(P,R)$ has order N. The existence of a point R satisfying this condition is provided by Corollary 2.5.1.1. The selection of such a point can be done as first picking a random point $R' \in E(\mathbb{F}_{q^s}) \cong \mathbb{Z}/cn_2\mathbb{Z} \times \mathbb{Z}/cn_2\mathbb{Z}$ and setting $R = (cn_2/N)R'$ which guarantees the order of R to be a divisor of N. So, $R \in E[N]$ is achieved, hence $\alpha = e_N(P,R)$ is defined. Later on, we will check whether α is of order N, if not we should come back to this step and take another random point R. The necessity of the condition on the order of α will become clear in the next step. (Note that $\alpha \in \mu_N$ by definition, so its order is necessarily a divisor of N.) Let m denote the order of α.

Afterwards, one can compute $\alpha = e_N(P,R)$ and $\beta = e_N(Q,R)$. By the fact that

$Q = kP$ and the bilinearity of the Weil pairing, we have

$$\beta = e_N(Q,R) = e_N(\underbrace{P+\cdots+P}_{k\text{-many}},R) = \underbrace{e_N(P,R)\ldots e_N(P,R)}_{k\text{-many}} = e_N(P,R)^k = \alpha^k.$$

This implies that

$$k' = \log_\alpha \beta \equiv k \pmod{m},$$

Because of the isomorphism given in Theorem 2.5.3, if R satisfies the desired condition on it, then α has the same order with P, namely $m = N$, and β has same order with Q. Hence, k' is equal to k modulo N which is what we are looking for. One method to check whether $k' = k$ is computing $k'P$. If $k'P = Q$, then the ECDLP is reduced to a DLP, hence we are done. Otherwise, $m < N$, and we should repeat the process by selecting another random point R.

Last but not least, we will comment on the probability of randomly selected R to satisfy that $\alpha = e_N(P,R)$ to have order N, i.e., α to be a primitive N^{th} root of unity. It will be concluded that this probability is $\phi(N)/N$ where ϕ is the Euler's totient function.

My first claim is that R is a random point in $E[N]$. We choose R' uniformly and randomly from $E(\mathbb{F}_{q^s})$ by first selecting an element $x \in \mathbb{F}_{q^s}$, plugging to the equation of the curve E and then solving for y. If there is a solution, then x is the x-coordinate of some point P, which is the case with probability $1/2 - 1/\sqrt{q}$ due to Hasse's Theorem (2.9.1), and we can select P or $-P.$, which are easily derived from one another. Recall that $E(\mathbb{F}_{q^s}) \cong \mathbb{Z}/cn_2\mathbb{Z} \times \mathbb{Z}/cn_2\mathbb{Z}$. Then by (Menezes et al., 1993, Lemma 7) , we conclude that $R = (cn_2/N)R'$ is uniformly distributed about the elements of the subgroup $E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

My second claim is that for a random $R \in E[N]$ the probability of $e_N(P,R) \in \mu_N$ to have order N is equal to the probability of a random element in μ_N to be a primitive N^{th} root of unity which is $\phi(N)/N$. by Theorem 2.5.2, for all $P_1, P_2 \in E[N]$

$$P_1, P_2 \text{ are in the same coset of } {}^{E[N]}/_{\langle P\rangle} \iff e_N(P,P_1) = e_N(P,P_2).$$

There are N distinct cosets in ${}^{E[N]}/_{\langle P\rangle}$. Let $R_i + \langle P\rangle$ denote the distinct cosets for $i = 1,2,\ldots,N$, and by abusing the notation let $e_N = (P, R_i + \langle P\rangle)$ denote the $e_N = (P,R_i)$. Observe that each $e_N = (P, R_i + \langle P\rangle)$ has a distinct value for each distinct i, and they are all in μ_N. So, there is a bijection between ${}^{E[N]}/_{\langle P\rangle}$ and μ_N. The argument above justifies the following isomorphism

$${}^{E[N]}/_{\langle P\rangle} \cong {}^{\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}}/_{\mathbb{Z}/N\mathbb{Z}} \cong \mathbb{Z}/N\mathbb{Z} \cong \mu_N.$$

Since R is uniformly distributed in $E[N]$, it is uniformly distributed in the quotient group ${}^{E[N]}/_{\langle P \rangle}$. Due to the relation between ${}^{E[N]}/_{\langle P \rangle}$ and μ_N, our claim follows.

3.2 Attack For Anomalous Curves

This section is based on (Smart, 1999).

The algorithm to be explained uses the theory of elliptic curves defined over $\mathbb{Q}_p$, in particular it lifts the points of the elliptic curve defined over a finite field to $E(\mathbb{Q}_p)$ in order to solve the ECDLP under the assumption that $\#E(\mathbb{F}_p) = p$, such curves are called *anomalous*.

The key idea of the algorithm is that $\#E(\mathbb{F}_p)$ and $\#\mathbb{F}_p$ are same and it is a prime number, so they are isomorphic.

We shall assume that our elliptic curve E is defined over $\mathbb{F}_p$, and let P and $Q = kP$ be points on $E(\mathbb{F}_q)$ where k is a positive integer.

First compute an arbitrary lift of P and Q to points $P^{\uparrow}$ and $Q^{\uparrow}$, respectively, on the same elliptic curve considered over $\mathbb{Q}_p$. Write $P = (x, y)$, then $P^{\uparrow} = (x, y^{\uparrow})$ where $y^{\uparrow}$ is computed via Hensel's Lemma since it is not a point of order 2, its y-coordinate is not 0. Same argument applies for Q, since neither P nor Q are points of order 2.

Lemma 3.2.1 (Hensel' Lemma)**.** *Let p be a prime number. Also, let $f(x)$ be a polynomial with integer coefficients, $k \in \mathbb{Z}^+$ and $r \in \mathbb{Z}$ such that $f(r) \equiv \pmod{p^k}$. Suppose $k \in \mathbb{Z}^+$ with $m \leq k$. Then if $f'(r) \not\equiv \pmod{p}$, there is an integer s such that $f(s) \equiv 0 \pmod{p^{k+m}}$ and $s \equiv r \pmod{p^k}$. So, s is a "lifting" of r to a root modulo p^{k+m}. Moreover, s is unique modulo p^{k+m}.*

Recall the definition of $E_n(\mathbb{Q}_p)$ and the results about the quotients $E_n(\mathbb{Q}_p)/E_{n+1}(\mathbb{Q}_p)$ from Section 2.6.

Notice that $Q - kP = O \in \mathbb{F}_q$. Therefore,

$$Q^{\uparrow} - kP^{\uparrow} = R^{\uparrow} \in E_1(\mathbb{Q}_p).$$

Also,

$$E_0(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) \cong \tilde{E}_{ns}(\mathbb{F}_p) = E(\mathbb{F}_p)$$

where the first isomorphism follows from (2.17) and the latter equality follows from the following reasoning. We have started with an elliptic curve $E/\mathbb{F}_p$, then considered the curve E over $\mathbb{Q}_p$. So, we can say that E has a good reduction at p and consequently $\tilde{E}_{ns}(\mathbb{F}_p) = E(\mathbb{F}_p)$ where $\tilde{E}_{ns}(\mathbb{F}_p)$ is as defined in Section 2.6. Moreover,

$$E_1(\mathbb{Q}_p)/E_2(\mathbb{Q}_p) \cong \mathbb{F}_q$$

as given in (2.19).

The key point is that $E(\mathbb{F}_p)$ and $\mathbb{F}_p$ have the same order, namely p, because of the assumption on the size of $E(\mathbb{F}_p)$. So,

$$pQ^{\uparrow} - k(pP^{\uparrow}) = pR^{\uparrow} \in E_2(\mathbb{Q}_p).$$

Apply p-adic logarithm ψ_p which is given as $\psi_p(x,y) \equiv \frac{-x}{y} \pmod{p^2}$ when $(x,y) \in E_1(\mathbb{Q}_p)$, since it is a homomorphism we can apply it termwise and obtain

$$\psi(pQ^{\uparrow}) - k\psi(pP^{\uparrow}) = \psi(pR^{\uparrow}) \equiv 0 \pmod{p^2}.$$

The p-adic logarithm ψ is defined for these points since for any point $P^{\uparrow} \in \mathbb{Q}_p$, we have $pP^{\uparrow} = O \in E_1(\mathbb{Q}_p)$ due to the assumption. Then the value k is calucalted as

$$k \equiv \frac{\psi(pQ^{\uparrow})}{\psi(pP^{\uparrow})} \pmod{p}.$$

3.3 Xedni Attack

In this section, a brief description of the xedni attack based on (Silverman, 2000) will be given. The importance of this attack is that it adapts the idea of the index calculus attack which is the most efficient method known for solving the DLP; it has subexponential time complexity. However, the xedni attack, although it is a subexponential algorithm, fails to solve ECDLP in general.

Let us first summarize the index calculus method. The DLP is to recover k when given $b \equiv a^k \pmod{p}$. The aim of the method is to find a "rank" r which is an

upper bound for the prime divisors of numbers of the form a^j, namely "liftings" of a, i.e., $a^j = \prod_{i=1}^{r} p_i^{e_i} \pmod{p}$. This equality can also be expressed by $j = \sum_{i=1}^{r} e_i \log_a p_i \pmod{p-1}$. If such a selection of "rank" r is achieved, then by taking r-many linearly independent equations of the latter form, we can solve for the unknowns $\log_a p_i$, hence consequently for k. (If we take $4r$-many equations, r-many of them will be linearly independent with high probability.)

One way to express the ECDLP is as finding a linear dependence relation between points $P, Q \in E(\mathbb{F}_q)$, i.e., finding the coefficients $a, b \in \mathbb{F}_q$ such that

$$aP + bQ = O.$$

This is the key idea of the xedni attack.

The ECDLP is to recover k when given $Q = kP$ on $E/\mathbb{F}_p$. In the xedni attack, we aim to find a small rank r which is the rank of the elliptic curve $\tilde{E}/\mathbb{Q}$, a lifting of $E/\mathbb{F}_p$. If r is small enough, then we can find a linear dependence relation between the lifted points and since they are selected to be the liftings of the points formed as the linear combinations of P, Q, by reducing them modulo p we can solve for k.

We can elaborate the xedni attack more. We are given $P, Q \in E(\mathbb{F}_p)$. First step is choosing points of the form $P_i = a_i P + b_i Q \in E(\mathbb{F}_p)$ where $a_i, b_i \in \mathbb{F}_p$. (At most 9 points should be chosen because 9 points determine a unique cubic curve, and if we choose more points we may not force them to be on the same cubic curve.) Then choose a lifting $\tilde{P}_i$ with integer coefficients for each point. Next, find a cubic curve $\tilde{E}$ over $\mathbb{Q}$ containing these liftings as follows: Since points lie on the curve, for each point $\tilde{P}_i = (x, y)$, replacing the variables of a general cubic equation with the coordinates of the points gives a linear equation where coefficients are the unknowns. Then solve for the coefficients. Afterwards, convert the general cubic equation to a Weierstrass form. Last but not least step is finding a linear dependence relation between the points on $\tilde{E}(\mathbb{Q})$, i.e., find the coefficients s_i's in

$$\sum s_i \tilde{P}_i = O.$$

This is the crucial step in this algorithm and it is the reason of why we are considering the liftings of the points $P_i's$. There is no method to find a linear dependence in $\mathbb{F}_q$. If solution for s_i's can be found, then the value of k can be computed by reducing the relation modulo p, hence solving the ECDLP. However, even though most curves over $\mathbb{Q}$ tend to have at most rank 2, the curves obtained by this algorithm tend to have a larger rank, hence it is hard or impossible to find a linear dependence relation among the chosen points. Therefore, the algorithm is concluded to be practically

unsuccessful for the ECDLP.

3.4 Attack For Trace 2 Curves

This section is based on (Shipsey & Swart, 2008).

The algorithm to be explained reduces the ECDLP, finding k when given P and $kP = Q$ on $E/\mathbb{F}_q$, to a DLP. In order to do this, it uses properties of division polynomials and elliptic divisibility sequences, as the former is an EDS in particular. The reduction is achieved under the assumptions that $\#E(\mathbb{F}_q) = q-1$ and the order of P is a large prime factor of $\#E(\mathbb{F}_q)$. Let N denote the order of P, then write $\#E(\mathbb{F}_q) = q-1 = \ell N$ with ℓ being small. The assumption on the size of ℓ is required to form Conjecture 1 which explains the the success probability of the algorithm. In addition to these, ℓ is assumed to be even which only requires q to be a power of an odd prime, i.e., q to be not a power of 2. This is also assumed for the sake of the argument about success probability of the algorithm.

The key idea of the algorithm relies on that the order of the group $E(\mathbb{F}_q)$ is $q-1$. Therefore, we have $P = qP$ in $E(\mathbb{F}_q)$ which allows us to use P and qP interchangeably. So, we can write $\psi_n(P)$ in place of $\psi_n(qP)$ for all n. However, 1 and q cannot be used interchangeably in the indices of $\psi(P)$ terms in general.

Due to this observation, the algorithm provided by (Shipsey & Swart, 2008) will be simplified in the following representation. To be more specific, Theorem 2.8.6 will be enough to construct the algorithm and Theorem 2.9.8 will only be used to explain the aforementioned Conjecture 1 that is about the success probability of the algorithm in reducing ECDLP to DLP.

Now, consider the sequence of division polynomials evaluated at P, i.e., $(\psi_n(P))$. By Theorem 2.8.6, since $\psi_{kq}(P) = \psi_{qk}(P)$, we can write

$$\psi_q(P)^{k^2}\psi_k(qP) = \psi_k(P)^{q^2}\psi_q(kP). \tag{3.1}$$

Similarly, since $\psi_{(k+1)q}(P) = \psi_{q(k+1)}(P)$, we write

$$\psi_q(P)^{(k+1)^2}\psi_{(k+1)}(qP) = \psi_{(k+1)}(P)^{q^2}\psi_q((k+1)P). \tag{3.2}$$

Due to the assumption $\#E(\mathbb{F}_q) = q-1$, we can replace qP with P. Also, obviously

kP can be replaced with Q. Hence, the equations (3.1) and (3.2) become

$$\psi_q(P)^{k^2}\psi_k(P) = \psi_k(P)^{q^2}\psi_q(Q), \tag{3.3}$$

$$\psi_q(P)^{(k+1)^2}\psi_{(k+1)}(P) = \psi_{(k+1)}(P)^{q^2}\psi_q(Q+P). \tag{3.4}$$

Dividing the equations (3.3) and (3.4) side by side, we get

$$\psi_q(P)^{2k+1} = \left(\frac{\psi_{k+1}(P)}{\psi_k(P)}\right)^{q^2-1} \cdot \frac{\psi_q(Q+P)}{\psi_q(Q)}. \tag{3.5}$$

Note that the quantity $\frac{\psi_{k+1}(P)}{\psi_k(P)}$ is both defined and nonzero. It is defined because $\psi_k(P) = 0$ if and only if $kP = O$ as explained in (2.26), and kP being O means $N \mid k$ which contradicts with the nature of the ECDLP. It is also not zero since this would imply $(k+1)P = O$, and then k can be easily solved. Similarly, $\psi_q(P)$ and $\psi_q(Q)$ are nonzero elements of $\mathbb{F}_q$.

Furthermore, $\left(\frac{\psi_{k+1}(P)}{\psi_k(P)}\right)^{q^2-1}$ is equal to 1 because it is an element of $\mathbb{F}_q^*$ and the power q^2-1 is divisible by the order of $\mathbb{F}_q^*$, namely $q-1$. Hence, the equality (3.5) becomes

$$\left(\psi_q(P)^2\right)^k = \frac{\psi_q(Q+P)}{\psi_q(P)\psi_q(Q)}. \tag{3.6}$$

Therefore, if $\psi_q(P)^2$ is not equal to 1 in $\mathbb{F}_q$, then the problem is reduced to a DLP which can be solved for k modulo the order of $\psi_q(P)^2$ in $\mathbb{F}_q$. In particular, if the order of $\psi_q(P)^2$ is N, which is the order of the point P, then k can be solved modulo N as desired and hence the reduction becomes successful. In what follows, we explain why this algorithm is successful in reducing the ECDLP to a DLP with high probability.

First, we will deduce that the order of $\psi_k(P)$ and $\psi_k(P)^2$ are same in $\mathbb{F}_q$ and it is either 1 or N. After explaining that algorithm fails only in the former case, we will conclude that the probability of failure is equivalent to the probability of $\psi_k(P)$ being 1. Next, we will conjecture that their order is N with high probability. So, if the conjecture is assumed, then k can be solved correctly.

Recall that $q-1 = \ell N$ and ℓ is even when q is assumed to be not a power of 2. Then by using assumptions and Theorem 2.9.8, we deduce the following sequence

of equalities.

$$\begin{aligned}
\psi_q(P) &= \psi_{1+\ell N}(P) && (q-1=\ell N)\\
&= d^{\ell^2} c^{\ell} && \text{(Theorem 2.9.8)}\\
&= c^{(\ell N)\frac{\ell}{2}} c^{\ell} && (d^2 = c^N \text{ and } \ell \text{ is even})\\
&= (c^{q-1})^{\frac{\ell}{2}} c^{\ell} && (q-1=\ell N)\\
&= c^{\ell} && (c \in \mathbb{F}_q^* \text{ and } |\mathbb{F}_q^*| = q-1).
\end{aligned}$$

Observe that since $c^{\ell N} = c^{q-1} = 1$ in $\mathbb{F}_q$, the order of $c^{\ell} = \psi_q(P)$ is a divisor of N. Considering that N is a large prime, order of $\psi_q(P)$ is either 1 or N. In both cases, the order of $\psi_k(P)$ and $\psi_k(P)^2$ are same since $2 \nmid 1$ and $2 \nmid N$. In the former case, the order of $\psi_k(P)$ and $\psi_k(P)^2$ being 1 means that $\psi_k(P) = \psi_k(P)^2 = 1$ in $\mathbb{F}_q$, therefore the algorithm fails. However, in the latter case, the order of $\psi_k(P)^2$ being N means that algorithm succeeds. So, for the probability of failure, it is enough to investigate the probability of $c^{\ell} = \psi_q(P)$ being 1. Also, keep in mind that $\psi_q(P) \neq 0$ as explained before, hence $c \in \mathbb{F}_q^*$.

Elements of $\mathbb{F}_q^*$ whose l^{th} power is 1 are exactly the roots of $x^{\ell} - 1$, whereas, all elements of $\mathbb{F}_q^*$ are exactly the roots of $x^{q-1} - 1$. So, for a random element c of $\mathbb{F}_q^*$ the probability of this element to satisfy $c^{\ell} = 1$ is $\frac{\ell}{q-1} = \frac{1}{N}$. Therefore, we form the following conjecture as stated in (Shipsey & Swart, 2008, Conjecture 1).

Conjecture 1. *If P is a point of order N on an elliptic curve $E/\mathbb{F}_q$ and $\#E(\mathbb{F}_q) = q-1 = \ell N$ where ℓ is even, then*

$$\psi_q(P) = 1 \text{ in } \mathbb{F}_q$$

with probability $\frac{1}{N}$.

Remark. To have $\psi_q(P) = \psi_{1+\ell N}(P) = \psi_1(P) = 1$, the period of the sequence $\psi_n(P)$ must divide ℓN, which is not the case in general.

If this conjecture is assumed to be true, then $\psi_q(P)^2$ has order N with high probability. Hence, using the equation (3.6) we can solve for k modulo N in $\mathbb{F}_q$ with the index calculus method.

3.5 Attack For Trace $1+\sqrt{q}$ Curves

We will develop a similar attack to the one presented in the previous section in order to reduce the ECDLP to a DLP by using division polynomials which form an elliptic divisibility sequences in particular. Let $E/\mathbb{F}_q$ be an elliptic curve where $\text{char}(\mathbb{F}_q) = p$, and we are given the points $P, Q = kP$ on $E(\mathbb{F}_q)$ with $k \in \mathbb{Z}^+$ and asked to recover k. Assume that the order of P is a large prime, denoted as N, so that $E(\mathbb{F}_q) = \ell N$ with ℓ being small. The assumption on the size of ℓ is required for the Conjecture 2 which explains the success probability of the algorithm. We will set $\#E(\mathbb{F}_q) = q - r$ and find out for which values of r the attack might be successful. Additionally, we assume $p \neq 2$ to make ℓ even. This is also assumed for the sake of the argument about success probability of the algorithm.

The key idea of the algorithm to be presented relies on the following

$$\#E(\mathbb{F}_q) = q - r \implies qP = rP \implies \psi_n(qP) = \psi_n(rP) \text{ for all } n \in \mathbb{Z}.$$

So, q and r can be used interchangeably in the coefficients of elements of the group $E(\mathbb{F}_q)$, however, they cannot be used interchangeably in the indices of $\psi(P)$ terms in general.

Consider the sequence of division polynomials evaluated at P, i.e., $\psi_n(P)$. As in the previous section by Theorem 2.8.6, since $\psi_{kq} = \psi_{qk}$, we can write

$$\psi_q(P)^{k^2}\psi_k(qP) = \psi_k(P)^{q^2}\psi_q(kP). \tag{3.7}$$

Similarly, since $\psi_{(k+1)q}(P) = \psi_{q(k+1)}(P)$, we write

$$\psi_q(P)^{(k+1)^2}\psi_{(k+1)}(qP) = \psi_{(k+1)}(P)^{q^2}\psi_q((k+1)P). \tag{3.8}$$

Here comes the trick, apply the same idea for $\psi_{kr} = \psi_{rk}$ which is given in the first line below and compare it with the equation (3.7) which is repeated in the second line below. Then, arrange both as given on the right hand sides of the implication symbols.

$$\psi_r(P)^{k^2}\psi_k(rP) = \psi_k(P)^{r^2}\psi_r(kP) \implies \psi_k(rP) = \frac{\psi_k(P)^{r^2}\psi_r(kP)}{\psi_r(P)^{k^2}},$$
$$\psi_q(P)^{k^2}\psi_k(qP) = \psi_k(P)^{q^2}\psi_q(kP) \implies \psi_k(qP) = \frac{\psi_k(P)^{q^2}\psi_q(kP)}{\psi_q(P)^{k^2}}.$$

Note 1. While choosing the value of r for our purposes, we should keep in mind that $\psi_r(P)$ and $\psi_q(P)$ should not be zero for above fractional terms to be defined. By the result (2.26), this condition reduces to $N \nmid r$ and $N \nmid q$. In fact, satisfying one

of these will be enough since $q - r = \ell N$. Moreover, $N \nmid q$ is equivalent to saying $N \neq \text{char}(\mathbb{F}_q)$. Therefore, from now on we are assuming that $N \neq \text{char}(\mathbb{F}_q)$ for the algorithm to work.

As observed previously, we know $qP = rP$ and consequently $\psi_k(rP) = \psi_k(qP)$, i.e.,

$$\frac{\psi_k(P)^{r^2}\psi_r(kP)}{\psi_r(P)^{k^2}} = \frac{\psi_k(P)^{q^2}\psi_q(kP)}{\psi_q(P)^{k^2}}. \tag{3.9}$$

Remark. Notice that even though $\psi_k(rP) = \psi_k(qP)$, this does not necessarily imply that $\psi_{kr} = \psi_{kq}$. Since satisfying $\psi_{kr} = \psi_{kq}$ would require $\psi_q = \psi_{r+\ell N} = \psi_r$, i.e., period of $\psi_n(P)$ to divide ℓN, which is not the case in general.

Next, replace $\psi_k(qP)$ in the equation (3.7) with the left hand side of the equation (3.9). (If, instead, we were to do this with the right hand side, we would get a tautology 1=1). Do the same trick for the quantity $\psi_{k+1}(qP)$ in the equation (3.8). Hence, after substituting kP with Q, write (3.7) and (3.8) as

$$\psi_q(P)^{k^2}\frac{\psi_k(P)^{r^2}\psi_r(Q)}{\psi_r(P)^{k^2}} = \psi_k(P)^{q^2}\psi_q(Q) \tag{3.10}$$

$$\psi_q(P)^{(k+1)^2}\frac{\psi_{(k+1)}(P)^{r^2}\psi_r(Q+P)}{\psi_r(P)^{(k+1)^2}} = \psi_{(k+1)}(P)^{q^2}\psi_q(Q+P). \tag{3.11}$$

Dividing the equations (3.10) and (3.11) side by side, we get

$$\left(\frac{\psi_q(P)}{\psi_r(P)}\right)^{2k+1} = \left(\frac{\psi_{k+1}(P)}{\psi_k(P)}\right)^{q^2-r^2} \cdot \frac{\psi_q(Q+P)\psi_r(Q)}{\psi_q(Q)\psi_r(Q+P)}. \tag{3.12}$$

Recall that in Note 1 by assuming $N \neq \text{char}(K)$, we ensured that $\psi_r(P)$ and, consequently, $\psi_r(Q+P)$ are nonzero. Now, there are four requirements to be satisfied by r for the algorithm to be successful in reducing the ECDLP to a DLP, namely,

Requirement 1. r must satisfy the Hasse Bound (Theorem 2.9.1).

Requirement 2. $q-1 \mid q^2-r^2$ so that $\left(\frac{\psi_{k+1}(P)}{\psi_k(P)}\right)^{q^2-r^2} = 1$.

Requirement 3. Elliptic curves of order $q-r$ must exist (Theorem 2.9.5).

Requirement 4. Order of $\left(\frac{\psi_q(P)}{\psi_r(P)}\right)^2$ must be N with high probability.

Requirement 1. Note that trace of an elliptic curve with $\#E(\mathbb{F}_q) = q - r$ is $r+1$.

Hence, due to Theorem 2.9.5, it must satisfy

$$-2\sqrt{q}-1 \leq r \leq 2\sqrt{q}-1. \tag{3.13}$$

Requirement 2. In the following discussion, we investigate the possible values for r so that $q-1 \mid q^2-r^2$. Also, we assume that $q^2-r^2>0$ because $q^2-r^2=0$ means $r=q$ and $\frac{\psi_q(P)}{\psi_r(P)}=1$, which immediately results in failure of the algorithm. Obviously, the remainders must be 0 in all cases below since we aim $q-1 \mid q^2-r^2$. This is how we decide the possible values for r in each case. All possible cases are given in Table 3.2 where n is a positive integer such that the quotient and remainder will be positive, quotient is greater than the remainder, and corresponding r should satisfy (3.13). (So, in Case 3 the value of $r=\pm\sqrt{(n+1)q-n}$ is not valid for all n as it needs to satisfy further conditions.)

	q^2-r^2	=	divisor	·	quotient	+	remainder	r
Case 1	q^2-r^2	=	$(q-1)$	·	$(q+1)$	+	$(1-r^2)$	± 1
Case 2	q^2-r^2	=	$(q-1)$	·	q	+	$(q-r^2)$	$\pm\sqrt{q}$
Case 3	q^2-r^2	=	$(q-1)$	·	$(q-n)$	+	$(n+1)q-r^2-n$	$\pm\sqrt{(n+1)q-n}$

Table 3.2 Possible values for r such that $q-1 \mid q^2-r^2$

In Case 1, the possible values for r satisfy the bounds given in (3.13). When $r=1$, the equation (3.12) becomes same with (3.5) since $\psi_1=1$. Hence, this subcase corresponds to the attack presented in the previous section. When $r=-1$, the term $\psi_q(P)^2$ becomes 1. Hence, the algorithm fails.

In Case 3, the possible values for r are of the form $\pm\sqrt{(n+1)q-n}$. We know that r must be an integer, so this condition becomes very restrictive. Additionally, as n grows the bounds (3.13) are not satisfied, more precisely, when $n=1,2,3$ it is satisfied but when $n=4$ they are not satisfied for the positive value of r. For these reasons, we will not investigate this case in more detail. We continue by elaborating the Case 2.

In Case 2, the values for r are $\pm\sqrt{q}$. Both $\sqrt{q}$ and $-\sqrt{q}$ satisfy the bounds (3.13). From now on, we will investigate whether the algorithm can be successful for $r=\sqrt{q}$.

Note 2. As r must be an integer, in the rest we are assuming that q is an even power of a prime.

By setting $r = \sqrt{q}$, we rewrite the equation (3.12) as follows

$$\left(\frac{\psi_q(P)}{\psi_{\sqrt{q}}(P)}\right)^{2k+1} = \frac{\psi_q(Q+P)\psi_{\sqrt{q}}(Q)}{\psi_q(Q)\psi_{\sqrt{q}}(Q+P)}. \tag{3.14}$$

Notice that by Theorem 2.8.6, we can write

$$\frac{\psi_q(P)}{\psi_{\sqrt{q}}(P)} = \frac{\psi_{\sqrt{q}\sqrt{q}}(P)}{\psi_{\sqrt{q}}(P)} = \frac{\psi_{\sqrt{q}}(P)^q \cdot \psi_{\sqrt{q}}(\sqrt{q}P)}{\psi_{\sqrt{q}}(P)} = \psi_{\sqrt{q}}(P)^{q-1} \cdot \psi_{\sqrt{q}}(\sqrt{q}P) = \psi_{\sqrt{q}}(\sqrt{q}P).$$

Therefore, the equation (3.14) becomes

$$\left(\psi_{\sqrt{q}}(\sqrt{q}P)^2\right)^k = \frac{\psi_{\sqrt{q}}\left(\sqrt{q}(Q+P)\right)}{\psi_{\sqrt{q}}(\sqrt{q}P) \cdot \psi_{\sqrt{q}}(\sqrt{q}Q)}. \tag{3.15}$$

The quantities on the right hand side can be calculated in $O(\log q)$ operations in $\mathbb{F}_q$. So, we have a discrete logarithm problem $\alpha^k = \beta$ in $\mathbb{F}_q$, which can be solved for k modulo the order of $\psi_{\sqrt{q}}(\sqrt{q}P)^2$ in $\mathbb{F}_q$.

Requirement 3. When r is set to be $\sqrt{q}$, there exist an elliptic curve of size $q - r = q - \sqrt{q}$ by Theorem 2.9.5 since trace t of the curve becomes $\sqrt{q}+1$ and $\gcd(t, \mathrm{char}(\mathbb{F}_q)) = 1$.

Requirement 4. We will investigate the probability of order of $\left(\frac{\psi_q(P)}{\psi_r(P)}\right)^2$ being N, i.e., the success probability of the algorithm. As we set $r = \sqrt{q}$, it is equivalent to investigating the probability of order of $\psi_{\sqrt{q}}(\sqrt{q}P)^2$ being N. We will do this by first observing that the order of $\psi_{\sqrt{q}}(\sqrt{q}P)^2$ is a divisor of N, and then we will conclude by Conjecture 2 that it is not 1, which means it is N, with high probability.

In general, recall that $q - r = \ell N$ and ℓ is even when q is assumed to be not a power of 2. Then by using assumptions and Theorem 2.9.8, we deduce the following sequence of equalities.

$$\begin{aligned}
\frac{\psi_q(P)}{\psi_r(P)} &= \frac{\psi_{r+\ell N}(P)}{\psi_r(P)} && (q - r = \ell N) \\
&= c^{r\ell} d^{\ell^2} && (\text{Theorem 2.9.8}) \\
&= c^{r\ell} c^{\frac{N\ell^2}{2}} && (d^2 = c^N \text{ and } \ell \text{ is even}) \\
&= c^{\ell(r + \frac{N\ell}{2})} \\
&= c^{\frac{\ell}{2}(q+r)} && (q - r = \ell N).
\end{aligned}$$

Therefore, we get $\left(\frac{\psi_q(P)}{\psi_r(P)}\right)^2 = c^{\ell(q+r)}$. When this quantity is raised to the power N,

$$c^{\ell N(q+r)} = c^{(q-r)(q+r)} = c^{q^2-r^2}.$$

Moreover, if Requirement 2 is satisfied, then $c^{q^2-r^2} = 1$ which implies that the order of $\left(\frac{\psi_q(P)}{\psi_r(P)}\right)^2$ is a divisor of N. If it is not 1, then it must be N since N is a prime.

Let g denote the $\gcd(\ell(q+r), q-1)$. The elements of $\mathbb{F}_q^*$ which becomes 1 when raised to the power $\ell(q+r)$ are the ones whose order is a divisor of g. These are exactly the roots of $x^g - 1$, whereas, all elements of $\mathbb{F}_q^*$ are exactly the roots of $x^{q-1} - 1$. So, for a random element c of $\mathbb{F}_q^*$, the probability of $c^{\ell(q+r)} = 1$ is $\frac{g}{q-1}$. If r is set to be $\sqrt{q}$, then $\ell(q+r) = \frac{q(q-1)}{N}$ and the respective probability is

$$\frac{g}{q-1} \text{ where } g = \begin{cases} \frac{q-1}{N} & \text{if } N \neq \text{char}(\mathbb{F}_q) \\ q-1 & \text{otherwise.} \end{cases}$$

Hence, we form the following conjecture by including the assumptions given by Note 1 and Note 2 to satisfy all the requirements for the case that $r = \sqrt{q}$.

Conjecture 2. *Let $E/\mathbb{F}_q$ be an elliptic curve of size $q - \sqrt{q}$ where $\text{char}(\mathbb{F}_q) \neq 2$. Also, let $P \in E$ be a point of order N where N is a large prime. If we suppose that q is an even power of a prime and $N \neq \text{char}(\mathbb{F}_q)$, then*

$$\psi_{\sqrt{q}}(\sqrt{q}P)^2 = 1 \in \mathbb{F}_q$$

with probability $\frac{1}{N}$.

If this conjecture is assumed to be true, then $\psi_{\sqrt{q}}(\sqrt{q}P)^2$ has order N with high probability. Hence, using the equation (3.15) we can solve for k modulo N in $\mathbb{F}_q$ by using the index calculus method. Therefore, the algorithm would be successful with high probability for elliptic curves satisfying the assumptions of Conjecture 2.

Example. Let E be an elliptic curve

$$y^2 = x^3 + x + w^{125}$$

defined over the field $\mathbb{F}_{23}(w)$ where $w^2 - 2w + 5 = 0$, and P be the point (w^{41}, w^{486}). Then $\#E(\mathbb{F}_{23}(w)) = 23^2 - 23$ and P has order 11, which is different than $\text{char}(\mathbb{F}_{23})$ and is a divisor of $\#E(\mathbb{F}_{23}(w))$. Let $Q = kP = (w^{435}, w^{215}) \in E(\mathbb{F}_{23}(w))$. We want to find k. Since the setup satisfies all the assumptions of the algorithm when $\left(\frac{\psi_q(P)}{\psi_r(P)}\right)^2$

is not 1, the value of k is equivalent to the smallest value of k satisfying

$$\left(\frac{\psi_q(P)}{\psi_r(P)}\right)^{2k+1} = \left(\frac{\psi_{k+1}(P)}{\psi_k(P)}\right)^{q^2-r^2} \cdot \frac{\psi_q(Q+P)\psi_r(Q)}{\psi_q(Q)\psi_r(Q+P)} \tag{3.16}$$

where $r = 23$ and $q = 23^2$.

By calculating $Q + P = (w^{418}, w^{231})$ and replacing values of P, Q, r, q, the equation (3.16) is becomes

$$\left(\frac{\psi_{23^2}(w^{41}, w^{486})}{\psi_{23}(w^{41}, w^{486})}\right)^{2k+1} = \frac{\psi_{23^2}(w^{418}, w^{231})\psi_{23}(w^{435}, w^{215})}{\psi_{23^2}(w^{435}, w^{215})\psi_{23}(w^{418}, w^{231})}$$

which reduces to

$$4^{2k+1} = 3 \text{ in } \mathbb{F}_{23}(w), \text{ i.e.,} \tag{3.17}$$

$$16^k = 18 \text{ in } \mathbb{F}_{23}(w). \tag{3.18}$$

When the DLP in (3.18) is solved, the smallest value of k is found to be 7 as expected.

4. ELLIPTIC CURVES OVER $\mathbb{Z}/N\mathbb{Z}$

Elliptic curves modulo large integers have also been proposed for cryptography with the motivation that the security of the cryptosystems might be improved by adding another hard problem, namely the integer factorization problem. Therefore, it is natural to develop the theory of elliptic curves over $\mathbb{Z}/N\mathbb{Z}$ for $N \in \mathbb{Z}$.

Throughout this chapter, R denotes a commutative ring with unity. We will introduce some preliminaries to define an elliptic curve E over the ring R. Under certain conditions, the group $E(R)$ where E is an elliptic curve defined over R forms an abelian group with a slightly different addition operation because of the existence of the points whose Z-coordinate is a nonunit element in R. Later, we will fix the ring R to be $\mathbb{Z}/N\mathbb{Z}$ and study $E(\mathbb{Z}/N\mathbb{Z})$, in particular $E(\mathbb{Z}/p^e\mathbb{Z})$ where p is a prime and e is a positive integer.

This chapter is based on (Sala & Taufer, 2020).

4.1 Preliminaries

Definition 4.1.1. A finite collection $(a_i)_{i\in I}$ of elements of R is called *primitive* if it generates R as an R-ideal, i.e.,

$$\text{if there exists } r_i \in R \text{ such that } \sum_{i\in I} r_i a_i = 1.$$

Remark. In the case that $R = \mathbb{Z}/N\mathbb{Z}$, the condition for primitivity boils down to $\gcd(N, a_1, a_2, \ldots, a_{|I|}) = 1$.

We will introduce the definitions of *minor ideal* and *strong rank* of a matrix in order to give an equivalence of statements in Theorem 4.1.1 that will be used in creating

a condition on R to define an elliptic curve over R. In particular, we need to make sure that the points of the elliptic curve are unique under the projective equivalence relation, and moreover $P_1 + P_2$ defines a unique point under the projective equivalence relation. For a nonnegative integer n, a *projective n-space over R*, denoted as $\mathbb{P}^n(R)$, is the set of all primitive tuples in R^{n+1}. We say any two tuples P_1, P_2 is *projectively equivalent* if there exist $r \in R^*$ such that $P_1 = rP_2$.

Definition 4.1.2. Let $n, m \in \mathbb{Z}_{\geq 1}$ and $A \in M_{n,m}(R)$. For every integer $1 \leq t \leq \min\{n, m\}$, we define the *t-minor ideal* $I_t(A)$ as the ideal generated by the $t \times t$ minors of A. We also define by convention $I_0(A) = R$ and for every $t > \min\{n, m\}$ we set $I_t(A) = (0)$.

Definition 4.1.3. Let $n, m \in \mathbb{Z}_{\geq 1}$ and $A \in M_{n,m}(R)$. We define the *strong rank* of A as

$$\mathrm{rk}(A) = \max\{t \in \mathbb{Z}_{\geq 0} : I_t(A) \neq (0)\}.$$

Remark. The strong rank of a matrix is never lower than the usual notion of a rank of a matrix over a ring.

Theorem 4.1.1. *(Sala & Taufer, 2020, Lemma 6) Let $n, m \in \mathbb{Z}_{\geq 1}$ and $A \in M_{n,m}(R)$ be a matrix whose entries are primitive, then the followings are equivalent:*

(i) rk(A)=1.

(ii) The 2×2 minors of A vanish.

(iii) All the primitive vectors of R^n that may be obtained from an R-linear combination among the rows of A are equal up to R^*-multiples.

Condition 4.1.1. For every pair $n, m \in \mathbb{Z}_{\geq 1}$ and every matrix

$$A = (a_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \in M_{n,m}(R)$$

with strong rank $\mathrm{rk}(A)$=1 and primitive entries, there exists an R-linear combination of the rows of A whose entries are primitive.

Note that the condition of strong rank can be replaced by any other equivalent statement in Theorem 4.1.1.

Remark. As it can be found in (Lenstra, 1986, p.2), this condition can be expressed in terms of R-module or Picard group of R, as well.

Now we are ready to introduce the definition of an elliptic curve over R.

Definition 4.1.4. Let R be a commutative ring with unity satisfying the Condition 4.1.1, and let E be given by the homogeneous Weierstrass equation

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

with $a_i \in R$ and $\Delta(E) \in R^*$. Then the *elliptic curve E(R)* is the set

$$\{(X : Y : Z) \in \mathbb{P}^2(R) : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\}.$$

The point $(0 : 1 : 0) \in E(R)$ is called the base point and acts as the identity element of $E(R)$ which is going to be a group under the addition law that is to be define in the next section. The points in the intersection $E(R) \cap \mathbb{P}^2_{aff}(R)$, i.e., the ones whose Z-coordinate is in R^*, are called the *affine points* of $E(R)$ and denoted by E^a. The rest of the points in $E(R)$ are called *points at the infinity* of $E(R)$ and denoted by E^∞.

Remark. For the rest of the chapter, we will assume that $6 \in R^*$, then equation of E can be transformed into homogeneous short Weierstrass equation, i.e.,

$$E : Y^2Z = X^3 + AXZ^2 + BZ^3.$$

This is assumed only to simplify the exposition; results are valid when $6 \notin R^*$.

4.2 Addition Laws On $E(R)$

Let E be an elliptic curve defined over R, in this section we will introduce a group law, namely addition, on $E(R)$ so that it becomes an abelian group.

In (Lange & Ruppert, 1987), they explicitly exhibited a complete system of addition laws on elliptic curves defined over a field. By an *addition law* on elliptic curve E, we roughly mean a formula that calculates $P_1 + P_2$ for some points $P_1, P_2 \in E$. It is called a *complete system* if for any P_1 and P_2 on the curve, there is at least one addition law among a collection of addition laws that calculates $P_1 + P_2$. Each addition law that they described consists of polynomials of bidegree (2,2).

Definition 4.2.1. Let $u, v \in \mathbb{Z}^+$. An *addition law of bidegree (u,v)* on elliptic curve E/K means a triple of polynomials $X_3, Y_3, Z_3 \in K[X_1, Y_1, Z_1, X_2, Y_2, Z_2]$ satisfying

(i) Each polynomial is bihomogeneous of bidegree (u,v), that is, homogeneous of degree u in variables X_1, Y_1, Z_1 and homogeneous of degree v in variables X_2, Y_2, Z_2,

(ii) Whenever K' is an extension field of K and $P_1 = (x_1 : y_1 : z_1)$, $P_2 = (x_2 : y_2 : z_2)$ are in $E(K')$, then the elements $x_3 = X_3(x_1, y_1, z_1, x_2, y_2, z_2)$, $y_3 = Y_3(x_1, y_1, z_1, x_2, y_2, z_2)$, and $z_3 = Z_3(x_1, y_1, z_1, x_2, y_2, z_2)$ of K' either satisfy $(x_3 : y_3 : z_3) \notin \mathbb{P}^2(K')$, or the point $P_3 = (x_3 : y_3 : z_3) \in E(K')$ with $P_3 = P_1 + P_2$.

More explicitly, the aforementioned complete system of addition laws, consisting of polynomials of bidegree (2,2), for E/K that is exhibited by (Lange & Ruppert, 1987) are the followings.

Addition Law I.

$$\begin{aligned}
X_3' =& (X_1Y_2 - X_2Y_1)(Y_1Z_2 + Y_2Z_1) + (X_1Z_2 - X_2Z_1)Y_1Y_2 \\
& - A(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) - 3B(X_1Z_2 - X_2Z_1)Z_1Z_2 \\
Y_3' =& -3X_1X_2(X_1Y_2 - X_2Y_1) - Y_1Y_2(Y_1Z_2 - Y_2Z_1) - A(X_1Y_2 - X_2Y_1)Z_1Z_2 \\
& + A(X_1Z_2 + X_2Z_1)(Y_1Z_2 - Y_2Z_1) + 3B(Y_1Z_2 - Y_2Z_1)Z_1Z_2 \\
Z_3' =& 3X_1X_2(X_1Z_2 - X_2Z_1) - (Y_1Z_2 + Y_2Z_1)(Y_1Z_2 - Y_2Z_1) \\
& + A(X_1Z_2 - X_2Z_1)Z_1Z_2
\end{aligned}$$

Addition Law II.

$$\begin{aligned}
X_3'' =& Y_1Y_2(X_1Y_2 + X_2Y_1) - AX_1X_2(Y_1Z_2 + Y_2Z_1) \\
& - A(X_1Y_2 + X_2Y_1)(X_1Z_2 + X_2Z_1) - 3B(X_1Y_2 + X_2Y_1)Z_1Z_2 \\
& - 3B(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1) + A^2(Y_1Z_2 + Y_2Z_1)Z_1Z_2 \\
Y_3'' =& Y_1^2Y_2^2 + 3AX_1^2X_2^2 + 9BX_1X_2(X_1Z_2 + X_2Z_1) - A^2X_1Z_2(X_1Z_2 + 2X_2Z_1) \\
& - A^2X_2Z_1(2X_1Z_2 + X_2Z_1) - 3ABZ_1Z_2(X_1Z_2 + X_2Z_1) - (A^3 + 9B^2)Z_1^2Z_2^2 \\
Z_3'' =& 3X_1X_2(X_1Y_2 + X_2Y_1) + Y_1Y_2(Y_1Z_2 + Y_2Z_1) + A(X_1Y_2 + X_2Y_1)Z_1Z_2 \\
& + A(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1) + 3B(Y_1Z_2 + Y_2Z_1)Z_1Z_2
\end{aligned}$$

Addition Law III.

$$\begin{aligned}
X_3''' =&(X_1Y_2+X_2Y_1)(X_1Y_2-X_2Y_1)+AX_1X_2(X_1Z_2-X_2Z_1)\\
&+3B(X_1Z_2+X_2Z_1)(X_1Z_2-X_2Z_1)-A^2(X_1Z_2-X_2Z_1)Z_1Z_2\\
Y_3''' =&(X_1Y_2-X_2Y_1)Y_1Y_2-3AX_1X_2(Y_1Z_2-Y_2Z_1)\\
&+A(X_1Y_2+X_2Y_1)(X_1Z_2-X_2Z_1)+3B(X_1Y_2-X_2Y_1)Z_1Z_2\\
&-3B(X_1Z_2+X_2Z_1)(Y_1Z_2-Y_2Z_1)+A^2(Y_1Z_2-Y_2Z_1)Z_1Z_2\\
Z_3''' =&-(X_1Y_2+X_2Y_1)(Y_1Z_2-Y_2Z_1)-(X_1Z_2-X_2Z_1)Y_1Y_2\\
&-A(X_1Z_2+X_2Z_1)(X_1Z_2-X_2Z_1)-3B(X_1Z_2-X_2Z_1)Z_1Z_2
\end{aligned}$$

Addition Law I is derived from the algebraic formula for addition corresponding to Case 3 in Section 2.1. It is done as follows: Replace x-coordinate and y-coordinate with x/z and y/z, respectively. Then, clear the denominators, and replace x^3 with $y^2z-axz^2-bz^3$ whenever necessary. Other addition laws are formed similarly for other cases.

Remark. When E is defined by long Weierstrass equation, the corresponding polynomials can be found in (Bosma & Lenstra, 1995, Section 5). Also, they explicitly describe which addition laws are valid for which type of point pairs P_1, P_2. They conclude that if $B \neq 0$ then Addition Laws II, III are enough to form a complete system for E/K.

In (Bosma & Lenstra, 1995), they pointed out that coefficients of Weierstrass equation, namely A and B, enter polynomially into addition laws, hence the same laws can be used to perform the addition on elliptic curves defined over commutative rings, namely $E(R)$. In particular, (Lenstra, 1986) showed that how a complete system of addition laws leads to an efficient algorithm for adding two points on an elliptic curves defined over a finite ring.

Therefore, for points $P_1 = (x_1 : y_1 : z_1)$ and $P_2 = (x_2 : y_2 : z_2)$ on $E(R)$ at least one of these three addition laws will give the point $P_1 + P_2 \in E(R)$. Hence, $E(R)$ will become an abelian group. In fact, since R is assumed to satisfy Condition 4.1.1 (to define an elliptic curve) and the matrix (4.1) has the property that all 2×2 minors vanishes (which is equivalent to saying its strong rank is 1 by Theorem 4.1.1), the assumptions of the Condition 4.1.1 is satisfied. Consequently, there exists a primitive R-linear combination of the rows of the matrix (4.1) giving $P_1 + P_2$.

$$\begin{pmatrix} X_3' & Y_3' & Z_3' \\ X_3'' & Y_3'' & Z_3'' \\ X_3''' & Y_3''' & Z_3''' \end{pmatrix} \tag{4.1}$$

Example. Let $N = 13 \cdot 17 = 221$ and set $R = \mathbb{Z}/N\mathbb{Z}$, also let

$$E : Y^2Z = X^3 + XZ^2 + 4Z^3.$$

Then $E(R)$ forms an elliptic curve since its corresponding discriminant is $6 \in R^*$.

Take $P_1 = (21 : 15 : 1), P_2 = (31 : 80 : 1) \in E(R)$. Applying Addition Law I for P_1 and P_2 results in $P_3 = (X_3' : Y_3' : Z_3') = (195 : 119 : 116)$ which is a point in $\mathbb{P}^2(R)$, hence consequently in $E(R)$ by the property of the addition law employed. So, we conclude that $P_3 = P_1 + P_2$.

Moreover, applying Addition Law II for P_1 and P_2 results in $(X_3'' : Y_3'' : Z_3'') = (52 : 119 : 142) = 66(195 : 119 : 116)$, so the point $(52 : 119 : 142)$ corresponds to P_3 in $\mathbb{P}^2(R)$. However, applying Addition Law III for P_1 and P_2 results in $(X_3''' : Y_3''' : Z_3''') = (0 : 187 : 17)$ which is not in $\mathbb{P}^2(R)$. So, Addition Law III is not valid for P_1 and P_2.

4.3 Elliptic Curves Over $\mathbb{Z}/N\mathbb{Z}$

From now on, we set $R = \mathbb{Z}/N\mathbb{Z}$.

Theorem 4.3.1. *Let $N \in \mathbb{Z}_{\geq 2}$ be an integer and A be a matrix over $\mathbb{Z}/N\mathbb{Z}$ whose entries are primitive, then there exists a linear combination of the rows of A that is primitive. In particular, $\mathbb{Z}/N\mathbb{Z}$ satisfies Condition* 4.1.1.

Proof. Let $r_1, r_2, \ldots, r_n$ denote the rows of the matrix A with entries in $\mathbb{Z}/N\mathbb{Z}$, and assume that A is primitive. Since A is primitive, for every prime p dividing N there are scalars $\alpha_1^{(p)}, \alpha_2^{(p)}, \ldots, \alpha_n^{(p)} \in \mathbb{Z}/N\mathbb{Z}$ such that

$$v^{(p)} = \sum_{i=1}^{n} \alpha_i^{(p)} r_i$$

is primitive over $\mathbb{Z}/p\mathbb{Z}$. By the Chinese Remainder Theorem we can find integers $\beta_1, \beta_2, \ldots, \beta_n \in \mathbb{Z}$ solving, for every prime p dividing N, the congruence system

$$\beta_i \equiv \alpha_i^{(p)} \text{ for all } i = 1, 2, \ldots, n.$$

Hence, $\sum_{i=1}^{n} \beta_i r_i$ becomes a primitive linear combination of rows of A.

□

Therefore, we can define elliptic curves defined over $\mathbb{Z}/N\mathbb{Z}$, and study their properties. Moreover, due to the Proposition 4.3.1, it is enough to study elliptic curves over $\mathbb{Z}/p^{v_p(N)}\mathbb{Z}$ where p is a prime divisor of N. We can simply denote this type of a group by $\mathbb{Z}/p^e\mathbb{Z}$ where p is any prime and e is any positive integer.

Proposition 4.3.1. *(Washington, 2008, Corollary 2.32) Let N_1, N_2 be integers such that $\gcd(N_1, N_2) = 1$, and let E be an elliptic curve defined over $\mathbb{Z}/N_1N_2\mathbb{Z}$. Then the canonical projections induce a group isomorphism*

$$E(\mathbb{Z}/N_1N_2\mathbb{Z}) \cong E(\mathbb{Z}/N_1\mathbb{Z}) \times E(\mathbb{Z}/N_2\mathbb{Z})$$

since

$$\begin{aligned} & Y^2Z \equiv X^3 + AXZ^2 + BZ^3 \pmod{N_1N_2} \\ \iff & \begin{cases} Y^2Z \equiv X^3 + AXZ^2 + BZ^3 \pmod{N_1} \\ Y^2Z \equiv X^3 + AXZ^2 + BZ^3 \pmod{N_2} \end{cases} \end{aligned}$$

The points of the group $E(\mathbb{Z}/p^e\mathbb{Z})$ has distinct type of representatives for the ones belonging to E^a and for the others belonging to E^∞. Corresponding representatives for each set is given in the next theorem.

Lemma 4.3.2. *Let p be a prime and $e \in \mathbb{Z}^+$. For $P = (X : Y : Z) \in E(\mathbb{Z}/N\mathbb{Z})$,*

$$\begin{cases} \text{there are } X, Y \in \mathbb{Z}/p^e\mathbb{Z} \text{ such that } P = (X : Y : 1) & \text{if } P \in E^a, \\ \text{there are } X, Z \in p(\mathbb{Z}/p^e\mathbb{Z}) \text{ such that } P = (X : 1 : Z) & \text{if } P \in E^\infty. \end{cases}$$

Proof. Let $P = (X' : Y' : Z') \in E(\mathbb{Z}/p^e\mathbb{Z})$. If $P \in E^a$, then by definition of E^∞ we have $\gcd(Z', p) = 1$. So, we can normalize the point P by the Z-coordinate as $P = \left(\frac{X'}{Z'} : \frac{Y'}{Z'} : 1\right) = (X : Y : 1)$. On the other hand, if $P \in E^\infty$ then by definition of E^∞ we have $\gcd(Z', p) \neq 1$ which is equivalent to saying $p \mid Z'$. Observe the following implications

$$\begin{aligned} p \mid Z' &\implies Y'^2Z' - AX'Z'^2 - BZ'^3 \equiv 0 \pmod{p}, \\ P \in E(\mathbb{Z}/p^e\mathbb{Z}) &\implies Y'^2Z' - X'^3 - AX'Z'^2 - BZ'^3 \equiv 0 \pmod{p}. \end{aligned}$$

Combining these two observations yields that $X'^3 \equiv 0 \pmod{p}$, consequently

$X' \equiv 0 \pmod{p}$. Hence, we conclude that $X', Z' \in p(\mathbb{Z}/p^e\mathbb{Z})$. Moreover,

$$P \in E(\mathbb{Z}/p^e\mathbb{Z}) \implies P \text{ is primitive} \implies \gcd(p, X', Y', Z') = 1 \implies p \nmid Y'.$$

Therefore, we can normalize the point P by the Y-coordinate as $P = \left(\frac{X'}{Y'} : 1 : \frac{Z'}{Y'}\right) = (X : 1 : Z)$. □

Computing the size of the group $E(\mathbb{Z}/p^e\mathbb{Z})$ reduces to computing the size of $E(\mathbb{F}_p)$ as stated in the next lemma. This reduction happens by means of the canonical projection map.

Lemma 4.3.3. *(Lenstra, 1986, Section 4) Let p be a prime, e be a positive integer and*

$$\pi \colon E(\mathbb{Z}/p^e\mathbb{Z}) \to E(\mathbb{F}_p) \tag{4.2}$$

be the canonical projection, that reduces the coordinates of points in $E(\mathbb{Z}/p^e\mathbb{Z})$ modulo p. Then for each point $P \in E(\mathbb{Z}/p^e\mathbb{Z})$, we have

$$|\pi^{-1}(P)| = p^{e-1}.$$

In particular,

(i) $|E(\mathbb{Z}/p^e\mathbb{Z})| = p^{e-1}|E(\mathbb{F}_p)|$,

(ii) $\operatorname{Ker}\pi$ *is a subgroup of* $E(\mathbb{Z}/p^e\mathbb{Z})$ *with size* p^{e-1}.

Remark. Observe that by definition E^∞ corresponds to the $\operatorname{Ker}\pi$. Hence, E^∞ forms a subgroup of $E(\mathbb{Z}/p^e\mathbb{Z})$.

The next result admits a certain form of a point that represents the points at infinity of $E(\mathbb{Z}/p^e\mathbb{Z})$, namely E^∞. The idea of creating this form of a point relies on the theory of formal groups (Silverman, 2009, Chapter IV) which studies the structure of an elliptic curve around O.

Proposition 4.3.2. *Let p be a prime, e be a positive integer and $E/\mathbb{Z}/p^e\mathbb{Z}$ be an elliptic curve. Then there is a polynomial $f \in \mathbb{Z}[x]$ of degree at most $e-1$ such that for every $P \in E^\infty$ there is $X \in p(\mathbb{Z}/p^e\mathbb{Z})$ satisfying*

$$P = (X : 1 : f(X)).$$

Moreover, the polynomial f satisfies

$$f(X) \equiv X^3 + AX^7 + BX^9 \pmod{p^{10}}.$$

Proof. By Lemma 4.3.2, we know that $P \in E^\infty$ is of the form $(X : 1 : Z)$ with $X, Z \in p(\mathbb{Z}/p^e\mathbb{Z})$. Define a sequence (F_i) by the initial condition $F_0(x, z) = x^3 + Axz^2 + Bz^3$ and recurrence relation $F_i(x, z) = F_{i-1}(x, F_0(x, z))$ for $i \geq 1$. By induction, we will prove that

$$Z \equiv F_i(X, Z) \pmod{p^e} \text{ for all } i \geq 0.$$

For the basis step, set $i = 0$ and observe that $P \in E(\mathbb{Z}/p^e\mathbb{Z})$ implies that

$$Z \equiv X^3 + AXZ^2 + BZ^3 \pmod{p^e} \equiv F_0(X, Z) \pmod{p^e}.$$

For the induction step, suppose that $Z \equiv F_k(X, Z) \pmod{p^e}$ for some $k \geq 1$, then

$$F_{k+1}(X, Z) = F_k(X, F_0(X, Z)) \equiv F_k(X, Z) \pmod{p^e} \equiv Z \pmod{p^e}.$$

Now, notice that by the definition of the recurrence relation each F_i is obtained from F_{i-1} by replacing all z's with $F_0(x, z) = x^3 + Axz^2 + bz^3$, which consists of terms of degree 3 only. Hence, the total degree of the terms involving z in F_i is strictly increasing. This means that there exists an integer $N \geq 0$ and a polynomial $g \in \mathbb{Z}[x, z]$ such that we can write

$$F_N(x, z) = f(x) + g(x, z) \text{ with } \deg g \geq e \text{ and } \deg f < e.$$

Since $X, Z \in p(\mathbb{Z}/p^e\mathbb{Z})$, we get $g(X, Z) \equiv 0 \pmod{p^e}$ and consequently

$$Z \equiv F_N(X, Z) \pmod{p^e} \equiv f(X) \pmod{p^e}.$$

Hence, we have shown that $P = (X : 1 : f(X))$ for some $X \in p(\mathbb{Z}/p^e\mathbb{Z})$ and $f \in \mathbb{Z}[x]$ of degree at most $e - 1$.

$$
\begin{aligned}
F_2(X,Z) =& F_1(X,F_0(X,Z)) = F_0(X,F_0(X,F_0(X,Z))) \\
=& F_0(X,F_0(X,X^3+AXZ^2+Z^3)) \\
=& F_0(X,X^3+AX(X^3+AXZ^2+Z^3)^2+(X^3+AXZ^2+Z^3)^3) \\
=& X^3+AX\left(X^3+AX(X^3+AXZ^2+Z^3)^2+(X^3+AXZ^2+Z^3)^3\right)^2 \\
&+\left(X^3+AX(X^3+AXZ^2+Z^3)^2+(X^3+AXZ^2+Z^3)^3\right)^3 \\
=& X^3+AX^7+BX^9+ \text{ (terms of degree } \geq 11)
\end{aligned}
$$

and the fact that $X, Z \in p(\mathbb{Z}/p^e\mathbb{Z})$. □

By using the polynomial $f \in \mathbb{Z}[x]$ in Proposition 4.3.2, we will derive an approximation for the sum of two points at infinity.

Proposition 4.3.3. *(Sala & Taufer, 2020, Proposition 16) Let p be a prime, e be a positive integer and $E(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic curve. Also, let f be the polynomial in the Proposition* 4.3.2 *for the respective $E(\mathbb{Z}/p^e\mathbb{Z})$. If*

$$P_1 = (X_1 : 1 : f(X_1)), P_2 = (X_2 : 1 : f(X_2)) \in E^\infty$$

with $e_1 = v_p(X_1)$ and $e_2 = v_p(X_2)$, then

$$P_1 + P_2 = (X_3 : 1 : f(X_3)) \text{ where } X_3 \equiv X_1 + X_2 \pmod{p^{5\min\{e_1,e_2\}}}.$$

The key ingredient of the attack for ECDLP described in Section 4.3.1 is the short exact sequence defined in the next theorem.

Theorem 4.3.4. *Let p be a prime, e be a positive integer and $E(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic curve. Also, let f be the polynomial defined in Proposition* 4.3.2 *corresponding to $E(\mathbb{Z}/p^e\mathbb{Z})$. Then*

$$0 \to \langle (p : 1 : f(P)) \rangle \overset{\iota}{\hookrightarrow} E(\mathbb{Z}/p^e\mathbb{Z}) \overset{\pi}{\to} E(\mathbb{F}_p) \to 0$$

is a short exact sequence of groups.

Proof. Clearly, ι is an injective group homomorphism. Also, π in (4.2) is the canonical projection, in particular it is a surjective group homomorphism. Therefore, we only need to show that $\operatorname{Im}\iota = \operatorname{Ker}\pi$, i.e., $\langle (p : 1 : f(P)) \rangle = \operatorname{Ker}\pi$. In fact, we know that $|\operatorname{Ker}\pi| = p^{e-1}$ by Lemma 4.3.3 and $P = (p : 1 : f(p)) \in \operatorname{Ker}\pi$ by Proposition

4.3.2. Therefore, it is enough to prove that P has order p^{e-1}, i.e., it is the generator of $\operatorname{Ker}\pi$.

We will prove by induction that

$$p^k P = (X : 1 : f(X)) \text{ and } v_p(X) = k+1 \text{ for } 0 \leq k-1 \leq e-1.$$

For the basis step, set $k = 0$, then $p^k P = P = (p : 1 : f(P))$ and $v_p(p) = 1 = k+1$. For the induction step, suppose that $p^k P = (X : 1 : f(X))$ and $v_p(X) = k+1$ for some $k \in \{0, 1, \ldots, e-1\}$. Now, observe that by Proposition 4.3.3 and induction on $\alpha \in \{1, 2, \ldots, p-1\}$, we get

$$\begin{aligned} P = (X : 1 : f(X)) &\implies \alpha P = (X_\alpha : 1 : f(X_\alpha)) \text{ where } X_\alpha \equiv \alpha X \pmod{p^{5v_p(X)}} \\ &\implies v_p(X_\alpha) = v_p(X). \end{aligned}$$

Then,

$$\begin{aligned} p^{k+1}P &= p(p^k P) \\ &= p(X : 1 : f(X)) \text{ and } v_p(X) = k \\ &= (X : 1 : f(X)) + (p-1)(X : 1 : f(X)) \\ &= (X : 1 : f(X)) + (X' : 1 : f(X')) \text{ where } X' \equiv (p-1)X \pmod{p^{5k}} \\ &= (X'' : 1 : f(X'')) \text{ where } X'' \equiv X + X' \pmod{p^{5k}} \equiv pX \pmod{p^{5k}} \end{aligned}$$

where the second equality follows from the inductive hypothesis, fourth one follows from the observation, and last one follows from Proposition 4.3.3 and the fact that $k = \min\{v_p(X), v_p(X')\}$. By this chain of equalities, we conclude that $v_p(X'') = k+1$. This concludes the induction step. Hence, the result follows. □

This result implies that $E(\mathbb{Z}/p^e\mathbb{Z}) \cong E(\mathbb{F}_p) \oplus \mathbb{Z}/p^e\mathbb{Z}$ when $|E(F_p)| \neq p$ as shown in (Sala & Taufer, 2020, Corollary 18). Hence, they classified the group structure of $E(\mathbb{Z}/p^e\mathbb{Z})$ when $E(\mathbb{F}_p)$ is not anomalous, and they also provided the possible group structures of $E(\mathbb{Z}/p^e\mathbb{Z})$ when $E(\mathbb{F}_p)$ is anomalous. Due to the Proposition 4.3.1, they stated the group structure of $E(\mathbb{Z}/N\mathbb{Z})$ as given in the next result.

Theorem 4.3.5. *(Sala & Taufer, 2020, Theorem 20) Let N be a positive integer and E be an elliptic curve defined over $\mathbb{Z}/N\mathbb{Z}$. Then*

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

In particular,

$$E(\mathbb{Z}/p^e\mathbb{Z}) \cong \begin{cases} E(\mathbb{F}_p) \oplus \mathbb{Z}/p^{e-1}\mathbb{Z} & \text{if } |E(\mathbb{F}_p)| \neq p \\ \mathbb{F}_p \oplus p^{e-1}\mathbb{Z} \text{ or } \mathbb{Z}/p^e\mathbb{Z} & \text{if } |E(\mathbb{F}_p)| = p. \end{cases}$$

4.3.1 Attack For Anomalous Curves

As we have seen $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ with $n_1 \mid n_2$ by Theorem 2.9.4. So, one way to solve the ECDLP, computing k when given $P, Q = kP \in E(\mathbb{F}_q)$, is finding an explicit isomorphism map f between $E(\mathbb{F}_q)$ and $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ since the problem might be solved by computing $f(kP)/f(P) = k$.

In Chapter 3, we presented some of the attacks to solve the ECDLP under certain conditions. In particular, in Section 3.2 we presented an attack for the elliptic curve $E/\mathbb{F}_p$ satisfying $\#E(\mathbb{F}_p) = p$. In this section, we will present another attack for the ECDLP resulted by this type of curves. The attack is due to (Sala & Taufer, 2020). This attack is worth to mention since it provides an explicit isomorphism map between $E(\mathbb{F}_p)$ and $\mathbb{F}_p$ by using the group $E(\mathbb{Z}/p^e\mathbb{Z})$ as an intermediate object in the case that $E(\mathbb{Z}/p^e\mathbb{Z}) \cong \mathbb{Z}/p^e\mathbb{Z}$. So, in order to solve the ECDLP, we assume that $\#E(\mathbb{F}_p) = p$ and $E(\mathbb{Z}/p^e\mathbb{Z}) \cong \mathbb{Z}/p^e\mathbb{Z}$.

The key idea of the algorithm is that the cyclic group $E(\mathbb{Z}/p^e\mathbb{Z})$ projects on $E(\mathbb{F}_p)$ by a nontrivial map as given in the next theorem.

Theorem 4.3.6. *Let p be a prime and $e \geq 2$ be an integer. Also, let $E(\mathbb{Z}/p^e\mathbb{Z})$ be an elliptic curve such that $E(\mathbb{Z}/p^e\mathbb{Z}) \cong \mathbb{Z}/p^e\mathbb{Z}$. Then the map*

$$\begin{aligned} \Theta \colon E(\mathbb{Z}/p^e\mathbb{Z}) &\to \mathbb{F}_p \\ P &\mapsto \frac{1}{p^{e-1}} \frac{(p^{e-1}P)_x}{(p^{e-1}P)_y} \end{aligned}$$

is a well-defined surjective group homomorphism whose kernel is

$$\mathrm{Ker}\Theta = \langle (p : 1 : f(P)) \rangle$$

where $f \in \mathbb{Z}[x]$ is the polynomial defined in Proposition 4.3.2.

Proof. For any $P \in E(\mathbb{Z}/p^e\mathbb{Z})$, we have $p^eP = O$. This implies $p^{e-1}P$ is a p-torsion point of $E(\mathbb{Z}/p^e\mathbb{Z})$, in particular it is in $E^\infty = \mathrm{Ker}\,\pi$. By the observation done in

the proof of Proposition 4.3.4, we conclude that

$$p^{e-1}P = (X : 1 : f(X)) \text{ with } v_p(X) \geq e-1.$$

Therefore, for the chosen representative of P, we get $p^{e-1} \mid (p^{e-1}P)_x$ and $(p^{e-1}P)_y = 1$. Hence, Θ is well-defined.

$E(\mathbb{Z}/p^e\mathbb{Z})$ is a cyclic group, let G be a generator for the group. Then $p^{e-1}G = (X' : 1 : f(X'))$ by the same reasoning as above, in particular $p^{e-1}G \in \langle (p^{e-1} : 1 : 0) \rangle$. Then by Proposition 4.3.2 and applying induction, we conclude that for any $m \in \mathbb{Z}$, $mp^{e-1}G = m(X' : 1 : f(X')) = (mX' : 1 : f(mX'))$. Therefore,

$$\Theta(mG) = \frac{1}{p^{e-1}} \frac{(mX')_x}{1} = m \frac{1}{p^{e-1}} \frac{(X')_x}{1} = m\Theta(G).$$

So, Θ is a group homomorphism.

$E(\mathbb{Z}/p^e\mathbb{Z})$ is a cyclic group of size p^e, hence it has a unique subgroup of size p^{e-1}, namely $\langle pG \rangle$. Observe that

$$P \in \mathrm{Ker}\Theta \iff p^{e-1}P = O \iff P \in \langle pG \rangle.$$

Therefore, $\mathrm{Ker}\,\Theta$ has size p^{e-1} and is cyclic. Since by Proposition 4.3.4 we know that $\langle (p : 1 : f(P)) \rangle$ generates a subgroup of order p^{e-1} and is cyclic, these two subgroups coincide. Hence, $\mathrm{Ker}\Theta = \langle (p : 1 : f(P)) \rangle$.

By first isomorphism theorem, since Θ is a group homomorphism

$$E(\mathbb{Z}/p^e\mathbb{Z}) \big/ \langle (p:1:f(P)) \rangle \cong \mathbb{Z}/p^e\mathbb{Z} \big/ \mathbb{Z}/p^{e-1}\mathbb{Z} \cong \mathbb{F}_p \cong \mathrm{Im}\,\Theta.$$

So, we can say that Θ is surjective. □

Theorem 4.3.6 has an important consequence. Let $P, Q(= kP)$ be points in $E(\mathbb{F}_p)$, lift them to $E(\mathbb{Z}/p^e\mathbb{Z})$. If $E(\mathbb{Z}/p^e\mathbb{Z})$ satisfies the assumptions of Theorem 4.3.6, then apply the map Θ on these liftings. Dividing image of the latter by the image of the former will solve for k, consequently the ECDLP will be solved. The process defined works due to the isomorphism between $E(\mathbb{F}_p)$ and $\mathbb{F}_p$, for which the explicit map is given in the next theorem.

Corollary 4.3.6.1. *Let p be a prime and $e \geq 2$ be an integer such that the elliptic curve $E/\mathbb{Z}/p^e\mathbb{Z}$ satisfies $E(\mathbb{Z}/p^e\mathbb{Z}) \cong \mathbb{Z}/p^e\mathbb{Z}$. Then the map*

$$\Theta \circ \pi^{-1} \colon E(\mathbb{F}_p) \to \mathbb{F}_p$$

is a well-defined group isomorphism.

Proof. The short exact sequence given in Proposition 4.3.4 induces an isomorphism ${}^{E(\mathbb{Z}/p^e\mathbb{Z})}/_{\langle(p:1:f(P))\rangle} \overset{\pi}{\cong} E(\mathbb{F}_p)$. Also, as we observed in the proof of Theorem 4.3.6, the map Θ induces an isomorphism ${}^{E(\mathbb{Z}/p^e\mathbb{Z})}/_{\langle(p:1:f(P))\rangle} \overset{\Theta}{\cong} \mathbb{F}_p$. By composing Θ and π^{-1}, the result follows. □

The key assumption in constructing this isomorphism, in particular in constructing the map Θ given in Theorem 4.3.6 was that $E(\mathbb{Z}/p^e\mathbb{Z}) \cong \mathbb{Z}/p^e\mathbb{Z}$. This observation suggests that for achieving strong ECDLP, one should consider elliptic curves violating this assumption, i.e., $E(\mathbb{Z}/p^e\mathbb{Z})$ being isomorphic to direct sum of two nontrivial groups.

BIBLIOGRAPHY

Ayad, M. (1992). Points s-entiers des courbes elliptiques. *Manuscripta mathematica*, *76*(1), 305–324.

Blake, I., Seroussi, G., & Smart, N. (1999). *Elliptic curves and their applications to cryptography: an introduction*. Cambridge University press.

Bosma, W. & Lenstra, H. W. (1995). Complete systems of two addition laws for elliptic curves. *Journal of Number theory*, *53*(2), 229–240.

Bézivin, J.-P., Pethö, A., & van der Poorten, A. J. (1990). A full characterisation of divisibility sequences. *American Journal of Mathematics*, *112*(6), 985–1001.

Enge, A. (1999). *Elliptic curves and their applications to cryptography: an introduction*. Springer.

Feo, L. D. (2017). Mathematics of isogeny based cryptography. *ArXiv*, *abs/1711.04062*.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, *48*(177), 203–209.

Kosters, M. & Pannekoek, R. (2017). On the structure of elliptic curves over finite extensions of $\mathbb{Q}_p$ with additive reduction. *arXiv preprint arXiv:1703.07888*.

Lange, H. & Ruppert, W. (1987). Addition laws on elliptic curves in arbitrary characteristics. *Journal of Algebra*, *107*(1), 106–116.

Lenstra, H. W. (1986). Elliptic curves and number-theoretic algorithms.

Leprévost, F., Monnerat, J., Varrette, S., & Vaudenay, S. (2005). Generating anomalous elliptic curves. *Information processing letters*, *93*(5), 225–230.

Menezes, A. J., Okamoto, T., & Vanstone, S. A. (1993). Reducing elliptic curve logarithms to logarithms in a finite field. *iEEE Transactions on information Theory*, *39*(5), 1639–1646.

Miller, V. S. (1985). Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques*, (pp. 417–426). Springer.

Rück, H.-G. (1987). A note on elliptic curves over finite fields. *Mathematics of Computation*, *49*(179), 301–304.

Sala, M. & Taufer, D. (2020). The group structure of elliptic curves over $\mathbb{Z}/n\mathbb{Z}$. *arXiv preprint arXiv:2010.15543*.

Schoof, R. (1985). Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of computation*, *44*(170), 483–494.

Schoof, R. (1987). Nonsingular plane cubic curves over finite fields. *Journal of combinatorial theory, Series A*, *46*(2), 183–211.

Shipsey, R. & Swart, C. (2008). Elliptic divisibility sequences and the elliptic curve discrete logarithm problem. *Cryptology ePrint Archive*.

Shipsey, R. E. (2000). *Elliptic divisibility sequences*. PhD thesis, Goldsmiths College (University of London).

Silverman, J. H. (2000). The xedni calculus and the elliptic curve discrete logarithm problem. *Designs, Codes and Cryptography*, *20*(1), 5–40.

Silverman, J. H. (2005). p-adic properties of division polynomials and elliptic divisibility sequences. *Mathematische Annalen*, *332*(2), 443–471.

Silverman, J. H. (2009). *The arithmetic of elliptic curves*, volume 106. Springer.

Smart, N. P. (1999). The discrete logarithm problem on elliptic curves of trace one.

Journal of cryptology, *12*(3), 193–196.

Van Tuyl, A. Computing the degree of the field of n-torsion points.

Voloch, J. F. (1988). A note on elliptic curves over finite fields. *Bulletin de la Société mathématique de France*, *116*(4), 455–458.

Ward, M. (1948). Memoir on elliptic divisibility sequences. *American Journal of Mathematics*, *70*(1), 31–74.

Washington, L. C. (2008). *Elliptic curves: number theory and cryptography*. Chapman and Hall/CRC.

Waterhouse, W. C. (1969). Abelian varieties over finite fields. In *Annales scientifiques de l'École normale supérieure*, volume 2, (pp. 521–560).