ELLIPTIC CURVES
AND
THEIR APPLICATION IN KEY-EXCHANGE
CRYPTOGRAPHY

SARAH-TANJA HESS

AT THE

Universität
Konstanz

BACHELOR THESIS UNDER THE SUPERVISION OF
PROF. DR. SALMA KUHLMANN

KONSTANZ, 2018
Sarah-Tanja Hess
78467 Konstanz
Germany

Sarah.Hess@uni-konstanz.de
## Contents

1 Preface ............................................. 1
2 Acknowledgment ..................................... 3
3 Basic Theory ........................................ 5
  3.1 The set of an elliptic curve ..................... 5
  3.2 The element $\infty$ ............................ 9
  3.3 Inducing a group structure .................... 12
4 Endomorphisms of elliptic curves .................... 21
  4.1 Introduction to endomorphisms of elliptic curves ... 21
  4.2 Excursus on Division Polynomials ............... 28
  4.3 The Frobenius map of elliptic curves ............ 35
5 Torsion points ........................................ 39
  5.1 The group of $n$-torsion points of an elliptic curve ... 39
  5.2 Weil-Pairing ................................... 43
6 Elliptic curves over finite fields ..................... 47
  6.1 Order of an elliptic curve restricted on a finite field ... 47
  6.2 Order of a point in an elliptic curve restricted on a finite field ... 52
7 Calculating efficiently over elliptic curves ............ 55
  7.1 Method of successive doubling .................. 55
  7.2 Determining the order of a point in a restricted elliptic curve .... 58
  7.3 Determining the order of a restricted elliptic curve .... 60
8 The discrete logarithm problem .......................... 61
  8.1 Types of discrete logarithm problems ............. 61
  8.2 Attacks on the discrete logarithm problem .......... 62
9 Introduction to the principles of crypto-systems ........... 75
10 Diffie-Hellman-Key-Exchange ........................... 77
  10.1 The classical Diffie-Hellman-Key-Exchange ......... 77
  10.2 Diffie-Hellman-Key-Exchange in elliptic curve cryptography ... 78
11 The Massey-Omura Encryption .......................... 81
12 The Crypto-System of ElGamal ......................... 83
13 Deutschsprachige Zusammenfassung ...................... 85
14 Appendix ............................................ 89
  14.1 Elliptic Curves restricted on $\mathbb{R}$ ............ 89
  14.2 Elliptic Curves restricted on finite fields ......... 90
  14.3 Addition over elliptic curves restricted on $\mathbb{R}$ ... 91
  14.4 Addition over elliptic curves restricted on finite fields ... 92
References ............................................ 95
Cyberwar, crypto-currencies and leaking affairs. In the twenty-first century smart devices and the world wide web are more important than ever. These inventions connect people from all around the world and everybody seems to be just a mouse click away. Communication is incredibly prompt nowadays due to online communication systems as mail or social media platforms. Together with this gain in speed, another valuable good gained importance. Information. Today everybody is transparent to anyone and so, unnoticed at first, the problem of securing privacy evolved.

How to secure a message being transmitted in secret in this transparent world?

An answer can be given using the beautiful methods of algebraic geometry which yield the concept of key-exchange crypto-systems based on elliptic curves. Privacy can be secured!

After chapter 1 shortly introduces the topic of this thesis and chapter 2 includes the acknowledgment, the theoretical part of this thesis starts, consisting of chapter 3 to chapter 6. First off chapter 3 will introduce the set of an elliptic curve and induce a group structure on that set. Next chapter 4 will use this group of an elliptic curve to adapt the principles of endomorphisms to this special group. Then chapter 5 will translate the algebraic concept of torsion elements into the language of elliptic curves. Furthermore an important pairing will be defined. Lastly chapter 6 focuses on elliptic curves restricted on finite fields and examine the order of such curves as well as the orders of subgroups generated by single elements in restricted elliptic curves. The main source for this theoretical first part is [19].

The second part of this thesis is more related to practice, applying the introduced mathematical concepts in informatics. This will be done in chapter 7 to 12. Starting off chapter 7 will introduce methods with which calculations can be done efficiently over elliptic curves using the theory of chapter 3 and chapter 6. Then chapter 8 introduces the so called discrete logarithm problem which secures a high level of safety for elliptic curve crypto-systems as will be pointed out in chapter 10, chapter 11 and chapter 12. These chapters will introduce three different key-exchange crypto-systems. However, first off chapter 9 will carefully define the most important terms of informatics and explain the systematic of crypto-systems. Having understood the way crypto-systems work, chapter 10 will then introduce the most famous elliptic curve key-exchange crypto-system. Lastly chapter 11 and chapter 12 will introduce two alternatives to this key-exchange crypto-system. The main sources of this second part are [19], [4], [6], [15] and [11].

Closing this thesis a detailed german summary will be given in chapter 13. Moreover several calculations over elliptic curves will be done in this thesis. Those calculations were either done by hand or using Matlab. Furthermore figures visualizing (restricted) elliptic curves as well as additions over such curves, will be given. These mathematical figures were also generated using Matlab. The corresponding codes for these needs were written entirely by myself and can be found in the appendix in chapter 14.

Throughout this thesis the reader is assumed to have a fundamental knowledge of algebra. If not mentioned otherwise $K$ and $F$ will always be assumed to be fields and $\overline{K}$ will denote the algebraic closure of $K$. As always $\mathbb{R}$ will denote the field of real numbers, $\mathbb{C}$ the field of complex numbers, $\mathbb{Q}$ the field of rational numbers and $\mathbb{Z}$ the ring of integers. Furthermore $\mathbb{N}$ will be the set of positive integers endowed with the natural $+$ and $\cdot$. If 0 shall be included in $\mathbb{N}$, $\mathbb{N}_0$ will be written. In general the element 1 will always denote the neutral element of multiplication and 0 the neutral element of addition (if possible). Analogously $x^{-1}$ will denote the multiplicative inverse of $x$ and $-x$ the additive inverse of $x$ (if possible). If necessary $\mathbb{R}$ will be understood to be endowed with the euclidean norm.

Moreover in this thesis finite fields will be of great interest and be denoted as $\mathbb{F}_q$ with $q$ being the power of a prime $p$. 

1. Preface
The cardinality of a set $S$ will be denoted as $\#S$ and $\langle S \rangle$ defines the subgroup generated by $S$ in a corresponding considered group. As always $gcd$ will denote the greatest common divisor and $lcm$ the least common multiple of several elements. In terms of mappings $id$ will denote the identity mapping. Furthermore fractions of polynomials will be called rational functions and $\text{char}(K)$ denotes the characteristic of a field $K$. For a polynomial $f$ $LC(f)$ will denote the coefficient of the leading term of $f$. 
I would like to thank all my supporters for all the time and patience they invested in me, while I elaborated this thesis.
I would especially thank Prof. Dr. Salma Kuhlmann, who arouse the passion for algebra in me. I am very grateful for her encouraging me to chose this very interesting topic and always being there for questions and suggestions.
Furthermore I would like to thank my mother, who was there for me throughout my life and did her best in supporting me while I wrote this thesis.
Thank you all so much, I really appreciated it.
3. Basic Theory

This thesis aims to apply elliptic curves in key-exchange cryptography. Therefore the basic theory of elliptic curves needs to be introduced first. This chapter aims to establish this fundamental knowledge of elliptic curves which will be needed to understand all following chapters and finally the application of elliptic curves in cryptography.

Firstly in subsection 3.1 the set of an elliptic curve will be introduced using a non-generalized Weierstrass equation. Furthermore it will be pointed out, how this set can be understood as an affine variety of a cubic equation in two variables. In general an elliptic curve has coordinates in an algebraically closed field. Nevertheless, it is possible to restrict an elliptic curve onto a general field and to maintain some properties. This will also be pointed out in this subsection. Moreover it will be emphasized that there are more general definitions for elliptic curves existing. However, since this thesis focuses on the application of elliptic curves in cryptography, most of the time a field of a large prime characteristic will be considered. Therefore it will be proven that the definition introduced in the first subsection is enough to define any elliptic curve in the context of this thesis.

Moreover in the set of an elliptic curve the element $1$ has to be included. Since an elliptic curve can be understood as an affine variety, it is hence possible to embed an elliptic curve (excluding $1$) into a projective plane. This motivates the inclusion of the element $1$ as the meeting point of vertical parallels in a projective plane. In subsection 3.2 this idea will be carefully explained.

Lastly in subsection 3.3 a binary operation over elliptic curves will be introduced. The set of an elliptic curve together with this operation will be proven to form an additive abelian group. Especially it will be emphasized how the definition of this operation is geometrically motivated. Hence from that point on, elliptic curves will implicitly be assumed to be endowed with this operation.

3.1. The set of an elliptic curve.

In order to be able to talk about elliptic curves, it must be firstly carefully defined what exactly elliptic curves are. In general they can be defined in various ways, depending on the main purpose of the research done. However, all existing definitions can be easily transferred into one another. Since this is a thesis from an algebraic point of view, aiming to use elliptic curves in cryptography over finite fields, the following definition of elliptic curves is appropriate.

**Definition 3.1.** Let $K$ be a field, $A, B \in K$, then the graph of the equation

$$Y^2 = X^3 + AX + B$$

together with $\infty$ is called an elliptic curve $E$ over $K$. In order to emphasize that the coordinates of the graph lay in the algebraic closure $\overline{K}$ of $K$, $E$ is often denoted as $E(\overline{K})$ i.e.

$$E := E(\overline{K}) := \{(x, y) \in \overline{K} \times \overline{K} \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

**Remark 3.2.** The equation describing $E$ is called a non-generalized Weierstrass equation.

**Remark 3.3.** Obviously an elliptic curve (excluding $\infty$) can be understood as a variety over $\overline{K} \times \overline{K}$ given by $\mathcal{V}(Y^2 - X^3 - AX - B)$.

In definition 3.1 the element $\infty$ is introduced as part of an elliptic curve. It is very important to carefully define this element. Therefore subsection 3.2 will focus on the definition, characteristics and applications of $\infty$. This will be done using the theory of projective planes. However, in this subsection it is enough to just accept $\infty$ as a special element of an elliptic curve.

Recalling definition 3.1 it is obvious that the non-generalized Weierstrass equation has coefficients in the field $K$. Yet the elliptic curve, which was defined as the graph over the corresponding non-generalized Weierstrass equation, is a set of pairs with coordinates in the algebraic closure $\overline{K}$ of the field $K$. So an elliptic curve can now be restricted to pairs over $K$ only, since $K \subseteq \overline{K}$ holds trivially.
**Definition 3.4.** Let $L$ and $K$ be fields such that $K \subseteq L \subseteq \overline{K}$. Furthermore let $E := E(\overline{K})$ be a fixed elliptic curve over $K$. The restriction of $E$ onto $L \times \overline{L}$ is denoted as $E(L)$. More precisely

$$E(L) := E(\overline{K})\big|_{L \times \overline{L}} \cup \{\infty\}.$$

**Remark 3.5.** The aim of this thesis is to apply the subset $E(K)$ of a given elliptic curve $E(\overline{K})$ in cryptography. Therefore such subsets will be of a high interest. From now on a subset $E(K)$ of $E(\overline{K})$ will be called an *elliptic curve restricted on $K$.*

Aiming to understand the set of an elliptic curve restricted on a field $K$ better, examining some examples is indispensable.

**Example 3.6.** Example of an elliptic curve restricted on $\mathbb{R}$

In this example the field $\mathbb{R}$ and the non-generalized Weierstrass equation $Y^2 = X^3 - 3.5X + 3$ will be considered. The algebraic closure of $\mathbb{R}$ is given by $\mathbb{C}$ and hence the elliptic curve over $\mathbb{R}$ described by the given non-generalized Weierstrass equation is the set

$$E(\mathbb{R}) = E(\mathbb{C}) = \{(x, y) \in \mathbb{C} \times \mathbb{C} \mid y^2 = x^3 - 3.5x + 3\} \cup \{\infty\}.$$

The corresponding restricted elliptic curve $E(\mathbb{R})$ on $\mathbb{R}$ is a proper subset of $E(\overline{\mathbb{R}})$.

This can be seen by setting $x = (-4)$, which yields

$$y^2 = x^3 - 3.5x + 3 = (-4)^3 - 3.5 * (-4) + 3 = (-47).$$

Thus $y$ must either be $\sqrt{47}i$ or $-\sqrt{47}i$ and so $(-4, \sqrt{47}i)$ and $(-4, -\sqrt{47}i)$ are elements of the elliptic curve $E(\mathbb{C}) = E(\overline{\mathbb{R}})$ but not of the restricted elliptic curve $E(\mathbb{R})$.

Visualizing $E(\mathbb{R})$ in the plane $\mathbb{R}^2$ points out this behavior as well as another important property of elliptic curves.

![Figure 1. Visualization of $E(\mathbb{R})$ given by $Y^2 = X^3 - 3.5X + 3$ in $\mathbb{R}^2$](image)

As it can be seen in figure 1 the elliptic curve $E(\mathbb{R})$ is actually not an adhesive line but a set of (isolated) points. This is due to $\mathbb{R}$ not being algebraically closed. As already pointed out, there exist $X$-coordinates such that the possible corresponding $Y$-coordinates are not elements in $\mathbb{R}$. Hence the visualization of the proper subset $E(\mathbb{R})$ of $E(\mathbb{C})$ in figure 1 excludes points of such a behavior.

Another general property of elliptic curves can also be observed in figure 1. Obviously an elliptic curve $E(K)$ in a field $K$ must always be symmetric with respect to a parallel line of the $X$-axis. In a field $K$

$$(-1) * (-1) = 1$$

always holds. Hence if $(x, y)$ solves a given non-generalized Weierstrass equation $Y^2 = X^3 + AX + B$, then $(x, -y)$ does as well, because of

$$(-y)^2 = (-1)^2 y^2 = y^2 = x^3 + Ax + B.$$
In this example the field $\mathbb{R}$ is considered and hence the axis of symmetry is the $X$-axis itself. Therefore in figure 1 it can be easily seen that the restricted elliptic curve is indeed symmetric with respect to the $X$-axis.

It was just pointed out that the axis of symmetry for an elliptic curve restricted on $\mathbb{R}$ is the $X$-axis. In general the axis of symmetry might be shifted along the $Y$-axis.

**Example 3.7. Example of an elliptic curve restricted on $\mathbb{F}_{71}$**

In this example the field $\mathbb{F}_{71}$ for the prime number 71 will be considered. Furthermore the defining non-generalized Weierstrass equation will be given by

$$Y^2 = X^3 + 17X + 12 \mod 71.$$

Analogously to example 3.6 the restricted elliptic curve $E(\mathbb{F}_{71})$ can be visualized in the plane $\mathbb{F}_{71}^2$.

![Figure 2](image.png)

**Figure 2. Visualization of $E(\mathbb{F}_{71})$ given by $Y^2 = X^3 + 17X + 12 \mod 71$ in $\mathbb{F}_{71}^2$.**

Obviously figure 2 emphasizes the symmetric property of $E(\mathbb{F}_{71})$, where it can be seen that the axis of symmetry is parallel to the $X$-axis. Moreover the axis of symmetry is horizontal and intersects the $Y$-axis in the height of 35.5 (when interpreting in $\mathbb{Q}$). This is due to $(-1) = 70 \mod 71$ and an analogous argumentation as done in example 3.6.

Moreover the finite field $\mathbb{F}_{71}$ is not algebraically closed and so $E(\mathbb{F}_{71}) \subseteq E(\overline{\mathbb{F}_{71}})$ can be easily proven. For example setting $x = 10 \mod 71$ yields

$$y^2 = x^3 + 17x + 12 = 46 \mod 71.$$

This is only solvable in the algebraic closure $\overline{\mathbb{F}_{71}}$, but not in $\mathbb{F}_{71}$. This reflects in the absence of points with a $X$-coordinate equal 10 in figure 2.

Those two examples already give a good first glimpse into the wide range of properties, which can be observed for elliptic curves. However, it should not be forgotten that the point $\infty$ is an element of an elliptic curve as well. Therefore the plotted graphs in figure 1 of example 3.6 and figure 2 of example 3.7 do not visualize the whole restricted elliptic curves, but only the main parts. For reasons of completeness it should be always kept in mind that there is an additional element existing which can not be easily visualized.
Furthermore elliptic curves can be defined in a more general way than it was done in definition 3.1.

**Definition 3.8.** Let $K$ be a field, $a_1, \ldots, a_5 \in K$, then the graph of the equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_5$$

together with the $\infty$ is called an **elliptic curve** $E$ over $K$. Emphasizing that the pairs solving this equation have coordinates in the algebraic closure $\overline{K}$ of $K$, $E$ is often denoted as $E(\overline{K})$ i.e.

$$E(\overline{K}) := E := \{(x, y) \in \overline{K} \times \overline{K} \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5 \} \cup \{\infty\}.$$

**Remark 3.9.** The equation describing $E$ is called a **generalized Weierstrass equation**. All definitions given and observations made so far for elliptic curves described by a non-generalized Weierstrass equation can be directly transferred to elliptic curves described by a generalized Weierstrass equation.

**Fact 1.** This more general definition of elliptic curves sometimes yields more sets which are called elliptic curves than definition 3.1 does. However, when working over a field $K$ with $\text{char}(K) \not\in \{2, 3\}$ a generalized Weierstrass equation can always be reformulated into a non-generalized Weierstrass equation.

**Proof.** Let $K$ be a field with $\text{char}(K) \not\in \{2, 3\}$ and let $a_1, \ldots, a_5 \in K$ be fixed coefficients for the generalized Weierstrass equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_5$$

describing $E(\overline{K})$.

First off, the inverse of 2 is well-defined and especially non-zero, since the characteristic of the underlying field $K$ is not equal 2. Therefore the given generalized Weierstrass can be reformulated into

$$(Y + 2^{-1}(a_1X) + 2^{-1}a_3)^2 = X^3 + (a_2 + (2^{-1})^2a_2^2)X^2 + (a_4 + 2^{-1}a_1a_3)X + ((2^{-1})^2a_2^2 + a_5).$$

Setting $\overline{a}_2 := a_2 + (2^{-1})^2a_2^2$, $\overline{a}_4 := a_4 + 2^{-1}a_1a_3$ and $\overline{a}_5 := (2^{-1})^2a_2^2 + a_5$ and defining a new variable $\overline{Y} := Y + 2^{-1}a_1X + 2^{-1}a_3$ yields a new equivalent generalized Weierstrass equation with coefficients $\overline{a}_2$, $\overline{a}_4$ and $\overline{a}_5$ in $K$. This equation is given by

$$\overline{Y}^2 = \overline{X}^3 + \overline{a}_2\overline{X}^2 + \overline{a}_4\overline{X} + \overline{a}_5.$$

Furthermore the inverse of 3 is well-defined and especially non-zero, since the characteristic of the field $K$ is not equal 3. Therefore the just derived generalized Weierstrass equation can be reformulated into

$$\overline{Y}^2 = (X + 3^{-1}\overline{a}_2)^3 + (\overline{a}_4 - (3^{-1})^2\overline{a}_2^2)(X + 3^{-1}\overline{a}_2) + (\overline{a}_5 - 3^{-1}\overline{a}_2\overline{a}_4 + (3^{-1})^2\overline{a}_4^2 - (3^{-1})^3\overline{a}_2^3).$$

Setting $A := \overline{a}_4 - (3^{-1})^2\overline{a}_2^2$ and $B := \overline{a}_5 - 3^{-1}\overline{a}_2\overline{a}_4 + (3^{-1})^2\overline{a}_4^2 - (3^{-1})^3\overline{a}_2^3$ and defining a new variable $\overline{X} := X + 3^{-1}\overline{a}_2$ yields

$$\overline{Y}^2 = \overline{X}^3 + A\overline{X} + B.$$ 

Thus an equivalent non-generalized Weierstrass equation with coefficients $A$ and $B$ in $K$ was found. It is important to emphasize, that the original generalized Weierstrass equation and the lastly found non-generalized Weierstrass equation yield the same set under an appropriate variable transformation. Let $(\overline{x}, \overline{y})$ be a pair solving the lastly found non-generalized Weierstrass equation. Setting $x = \overline{x} - 3^{-1}\overline{a}_2$ and $y = \overline{y} - 2^{-1}a_1x - 2^{-1}a_3$ yields another pair $(x, y)$ which solves the original generalized Weierstrass equation and vice versa.

This thesis aims to apply elliptic curves in cryptography. For reasons of efficiency and security such applications are only done for elliptic curves over fields of characteristic 0 or of a characteristic divisible by at least one large prime. Thence according to fact 1 it is enough in this context to work with definition 3.1 only.

**Fact 2.** Recalling definition 3.1 it seems as having a normed coefficient for both $Y^2$ and $X^3$ might be an unnecessary restriction of a general cubic equation in two variables. However, it is not.

**Proof.** Let $a$, $b$, $c$ and $d$ be elements of a field $K$ such that $c \neq 0$ and $d \neq 0$. The general equation

$$cY^2 = dX^3 + aX + b$$
will be considered.
Firstly multiplying with \( c^1d^2 \) yields
\[
(c^2dY)^2 = c^1d^2Y^2 = c^1d^2(cY^2) = c^1d^2(dX^2 + aX + b) = c^1d^2X^2 + ac^2d^2X + c^2d^2b = (cdX)^3 + (ac^2d)(cdX) + (c^2d^2b),
\]
Setting \( A := ac^2d \) and \( B := c^2d^2b \) and introducing new variables \( \overline{X} := cdX \) and \( \overline{Y} = c^2dY \) yields the equivalent normed(!) equation
\[
\overline{Y}^2 = \overline{X}^3 + AX + B.
\]
Obviously the original equation is solved by a pair \((x, y)\) if and only if the corresponding (normed) non-generalized Weierstrass equation is solved by a pair \((\overline{x}, \overline{y})\) under the variable transformations \( \overline{x} = cdx \) and \( \overline{y} = c^2dy \) respectively \( x = (cd)^{-1}\overline{x} \) and \( y = (c^2d)^{-1}\overline{y} \). In this context all inverse do exist, since \( K \) is a field and \( c \) and \( d \) were chosen to be unequal zero.

Wanting to dive deeper into the theory of elliptic curves, a first step is to induce a group structure on an elliptic curve. This will be done in subsection 1.3. In order to be able to do that efficiently a restriction for the from now on used elliptic curves needs to be established.

**Remark 3.10.** Starting from now, only elliptic curves over a field \( K \), whose corresponding non-generalized Weierstrass equation \( Y^2 = X^3 + AX + B \) with \( A \) and \( B \) in \( K \) has a non-trivial discriminant, will be considered. In this context
\[
4A^3 + 27B^2 \neq 0
\]
needs to hold, which obviously implies the corresponding non-generalized Weierstrass equation having three distinct roots.

All in all so far the set of an elliptic curve over a field \( K \) was introduced and then restricted on \( K \). Furthermore some basic properties of such sets were examined.

### 3.2. The element \( \infty \).

In definition 3.1 the element \( \infty \) was firstly mentioned. This element will be defined carefully and its properties will be explained now. The element \( \infty \) is closely linked to the theory of projective spaces, which evolved as a subfield of algebraic geometry. For example in the plane \( \mathbb{R}^2 \) it is known that two parallel lines do not intersect one another. The main idea of a projective space over \( \mathbb{R}^2 \) is now to introduce elements in which parallel lines do intersect each other.

Most of this subsection is just a repetition of [13][Chapter 12] whereas projective planes are introduced independently from elliptic curves. In order to not stress the notations of this thesis, all fields in the general setting independent from elliptic curves of this subsection will be called \( F \) respectively \( \overline{F} \), if the field is algebraically closed.

In the end of this subsection the general theory of projective spaces will be applied to the theory of elliptic curves. In this context the notation \( K \) and \( \overline{K} \) will be used again to emphasize the setting of an elliptic curve.

**Definition 3.11.** Let \( F \) be a field and \( n \) a positive integer. For any fixed \((x_0, \ldots, x_n)\) and \((y_0, \ldots, y_n)\) in \( F^{n+1}\setminus\{0\} \), the relation \( \sim \) over \( F^{n+1}\setminus\{0\} \) is defined as
\[
(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)
\]
if and only if there exists a non-zero scalar \( \lambda \in F^\times \) such that \((x_0, \ldots, x_n) = \lambda(y_0, \ldots, y_n)\).

**Remark 3.12.** A straight forward calculation proves that \( \sim \) is an equivalence relation on \( F^{n+1}\setminus\{0\} \).

**Definition 3.13.** Let \( F \) be a field, \( n \) a positive integer and \( \sim \) be defined as in definition 3.11, then
\[
P_n(F) := (F^{n+1}\setminus\{0\}) / \sim
\]
is called the **n-dimensional projective space over** \( F \).

**Remark 3.14.** Let \((x_0, \ldots, x_n)\) be an element of \( F^{n+1}\setminus\{0\} \). The equivalence class of this element with respect to \( \sim \) is an element of \( P_n(F) \) and is called the **homogeneous coordinate** \((x_0 : \ldots : x_n)\) of the element \((x_0, \ldots, x_n)\).
In order to apply this concept to a fixed elliptic curves, pairs which solve the corresponding non-generalized Weierstrass equation will be considered. As mentioned in remark 3.3 an elliptic curve (excluding $\infty$) over a field $K$ can be understood as an affine variety in $\mathbb{P} \times \mathbb{P}$. Thus being able to embed $\mathbb{P}$ in the $n$-dimensional projective space $\mathbb{P}^n(\mathbb{K})$ is admirable.

**Proposition 3.15.** Let $F$ be a field, $n$ a positive integer and set
\[ U_0 := \{(x_0 : \ldots : x_n) \in \mathbb{P}^n(F) \mid x_0 \neq 0\}, \]
then the map
\[ \phi : \quad F^n \to U_0 \]
\[ (x_1, \ldots, x_n) \mapsto (1 : x_1 : \ldots : x_n) \]
is bijective.

**Proof.** [13][Subsection 12.1, Proposition 12.6, pp.80]

**Remark 3.16.** This proposition yields that $F^n$ can be embedded in $\mathbb{P}^n(F)$. More precisely it yields the isomorphic correspondence $\mathbb{P}^n(F) \cong F^n \cup \mathbb{P}^{n-1}(F)$. In this context the set $\mathbb{P}^{n-1}(F)$ is referred to as the set of points in infinity.

Now it needs to be understood, how affine varieties can be transferred into projective spaces. Therefore the definition of homogeneous polynomials needs to be recalled.

**Definition 3.17.** Let $F$ be a field, $n$ a positive integer and $f$ a polynomial in $F[X_0, \ldots, X_n]$. Then the polynomial $f$ is said to be **homogeneous**, if all monomials are of the same total degree $d$ for an appropriate $d \in \mathbb{N}$.

**Definition 3.18.** Let $F$ be a field and $n, s$ be positive integers. Furthermore let $f_1, \ldots, f_s$ be homogeneous polynomials in $F[X_0, \ldots, X_n]$. Then the **projective variety** $V_p(f_1, \ldots, f_s)$ over $f_1, \ldots, f_s$ is given by
\[ V_p(f_1, \ldots, f_s) := \{(a_0 : \ldots : a_n) \in \mathbb{P}^n(F) \mid \forall i \in \{1, \ldots, s\} : f_i(a_0, \ldots, a_n) = 0\}. \]

It is possible to observe a correspondence between affine varieties and projective varieties. In the context of this thesis only the 2-dimensional projective space over $\mathbb{K}$ for a given field $K$ will be of interest. This 2-dimensional projective space over $\mathbb{K}$ is called the **projective plane over $\mathbb{K}$**.

Moreover when interpreting an elliptic curve (excluding $\infty$) as an affine variety, then it is known that this variety is obviously generated by a single polynomial. Hence, the results of [13][Chapter 12] can be adapted to the just explained simplified relevant setting.

For the next proposition it is assumed that the reader is familiar with the concept of homogenizing a given polynomial, else [13] should be completely recapitulated.

**Proposition 3.19.** Let $\mathcal{F}$ be an algebraically closed field, $\preceq$ a fixed graduated monomial ordering on $\mathcal{F}[X_1, X_2]$, $f$ a polynomial in $\mathcal{F}[X_1, X_2]$ and $f^h \in K[X_0, X_1, X_2]$ the homogenization of $f$. Furthermore let $V_a(f)$ denote the affine variety generated by $f$ and $V_p(f^h)$ the projective variety generated by $f^h$. Set $U_0 := \{(x_0 : \ldots : x_n) \in \mathbb{P}^n(\mathcal{F}) \mid x_0 \neq 0\}$, then
\[ V_p(f^h) \cap U_0 = V_a(f). \]

**Proof.** Homogenizing the ideal generated by $f$ can easily be done by considering the ideal generated by the homogenized polynomial $f^h$ of $f$, since $\{f\}$ is obviously a Gröbner basis for $\langle f \rangle$ with respect to the graduated monomial ordering $\preceq$ on $\mathcal{F}[X_1, X_2]$.

Recalling that the affine variety given is generated by one polynomial $f$ only and using the just made observations yields $V_a(f) = V_p(f^h)$ using [13][Subsection 12.4, Theorem 12.40, pp.90] whereas $\overline{V_a(f)}$ is the projective closure of $V_a(f)$ in terms of varieties.

Finally the first bullet point of [13][Subsection 12.4, Proposition 12.44, pp.92] with $n = 2$ proves the claim.

Altogether proposition 3.19 proves that elliptic curves (excluding $\infty$) can be embedded into projective planes. In particular an elliptic curve without $\infty$ can even be understood as a projective variety in a projective plane. Therefore the theory of projective varieties can be applied to elliptic curves (excluding $\infty$) which makes including $\infty$ as an element in an elliptic curve intuitive at last.
Example 3.20. Understanding points in infinity
In this example it will be explained how intersection points of parallel lines can be understood as points in infinity. Therefore let $\mathcal{F}$ denote an algebraically closed field.
Firstly two non-vertical parallel lines described by

$$Z = mY + b_1$$

and

$$Z = mY + b_2$$

over $\mathcal{F}[Y, Z]$ with $m \neq 0$ will be considered. Furthermore $\succeq$ is a fixed graduated monomial ordering on $\mathcal{F}[Y, Z]$. Aiming to apply the results of this chapter, setting

$$f_1(Y, Z) := mY + b_1 - Z$$

and

$$f_2(Y, Z) := mY + b_2 - Z$$

is necessary.

Examining $V_\alpha(f_1, f_2)$ is indispensable, when wanting to find intersection points of the two considered parallels in $\mathcal{F}$. Unsurprisingly this is the empty set.

Thence the theory of projective spaces needs to be applied in order to may observe intersection points. A Gröbner basis of $(f_1, f_2)$ is given by $\{f_1, f_2\}$. Determining the homogenized polynomials $f_1^h$ of $f_1$ and $f_2^h$ of $f_2$ in $\mathcal{F}[X, Y, Z]$ yields $f_1^h(X, Y, Z) = mY + b_1X - Z$ and $f_2^h(X, Y, Z) = mY + b_2X - Z$.

Therefore $\{f_1^h, f_2^h\}$ is known to be a Gröbner basis for the homogenization ideal of $(f_1, f_2)$ according to [13][Subtitle 12.4, Theorem 12.40, pp.90]. The corresponding projective closure variety is given by

$$V_p(f_1^h, f_2^h) := \{(x : y : z) \in \mathbb{P}^2(\mathcal{F}) \mid my + b_1x - z = 0 \land my + b_2x - z = 0\}$$

$$= \{x : y : z \in \mathbb{P}^2(\mathcal{F}) \mid my - z = (-b_1)x \land my + b_2x - z = 0\}$$

$$= \{x : y : z \in \mathbb{P}^2(\mathcal{F}) \mid my - z = (-b_1)x \land (-b_1)x + b_2x = x(b_2 - b_1) = 0\}$$

$$= \{(0 : y : z) \in \mathbb{P}^2(\mathcal{F}) \mid my = z\} = \{(0 : y : my) \mid y \in \mathcal{F}\{0\}\}$$

where definition 3.11 and $\mathcal{F}$ being a field was used. Moreover setting $y = 1$ yields $(0, 1, m)$ as a representer of the equivalence class $(0 : y : my)$.

Altogether

$$V_p(f_1^h, f_2^h) = \{(0 : 1 : m)\}$$

was observed.

Now let $U_0$ be defined as in proposition 3.19, then obviously $(0 : 1 : m) \notin U_0$.

Furthermore

$$\mathbb{P}^2(\mathcal{F}) \simeq \mathbb{P}^2 \cup \mathbb{P}^1(\mathcal{F})$$

holds according to remark 3.16. Thus by the disjointness of $\mathbb{P}^2$ and $\mathbb{P}^1(\mathcal{F})$ under embedding, it is known that $V_p(f_1^h, f_2^h)$ can be understood as a subset of $\mathbb{P}^1(\mathcal{F})$ under embedding.

Recalling remark 3.16 yields $\mathbb{P}^1(\mathcal{F})$ being a set consisting of points in infinity in this context. So the only existing intersection point of two arbitrary but fixed non-vertical parallels was found to be a point in infinity.

Now the case for two vertical parallels will be considered. Therefore let $c_1$ and $c_2$ be two distinct elements in $\mathcal{F}$ describing the two vertical parallels $Y = c_1$ and $Y = c_2$ in $\mathcal{F}[Y, Z]$.

The set of intersection points of these two vertical parallels over $\mathcal{F}$ can be again understood as the affine variety $V_\alpha(Y - c_1, Y - c_2)$ in $\mathcal{F} \times \mathcal{F}$, which is obviously the empty set.

The corresponding projective closure variety is given by

$$V_p(Y - c_1X, Y - c_1X) := \{(x : y : z) \in \mathbb{P}^2(\mathcal{F}) \mid y = c_1x \land y = c_2x\}$$

$$= \{(x : y : z) \in \mathbb{P}^2(\mathcal{F}) \mid x(c_1 - c_2) = 0 \land y = c_1x\}$$

$$= \{(0 : 0 : z) \mid z \in \mathcal{F}\{0\}\}.$$

Without loss of generality $z = 1$ can be set.
So the only intersection point of two vertical parallels is therefore given by \((0 : 0 : 1)\) in the projective plane over \(\overline{F}\). This is analogously to the non-vertical case in this context a point in infinity.

**Example 3.21. The case of elliptic curves**

The element \(\infty\) in the context of this thesis needs to be understood as the unique meeting point of vertical parallels in a projective plane, as will now be explained.

As proven in example 3.20 parallels over an algebraically closed field in general only meet in points in infinity. However, they do not all meet in the same point in infinity. Nevertheless, in the case of vertical parallels in example 3.20 it was proven that all vertical parallels meet in the unique point \((0 : 0 : 1)\) in the projective plane over the considered algebraically closed field.

Moreover another observation can be made.

Considering an arbitrary but fixed field \(K\) and an elliptic curve \(E\) over \(K\) described by the non-generalized Weierstrass equation \(Z^2 = Y^3 + aX + B\) for some \(a\) and \(B\) in \(K\) and letting \(\prec\) be a fixed graduated monomial ordering on \(K[X, Y]\), then \(E \setminus \{\infty\}\) can be understood as the affine variety

\(V_{\prec}(Z^2 - Y^3 - aY - B)\)

in \(\overline{K} \times \overline{K}\). Furthermore the corresponding projective closure variety over \(\overline{K}\) is given by

\(V_{\prec}(Z^2X - Y^3 - aYX^2 - BX^3)\).

Recalling remark 3.16 yields the isomorphic correspondence \(\mathbb{P}^2(\overline{K}) \simeq \overline{K}^2 \cup \mathbb{P}^1(\overline{K})\) under embedding and every element in \(\mathbb{P}^1(\overline{K})\) is in this context referred to as a point in infinity. Furthermore proposition 3.19 showed that \(\overline{K}\) can be embedded in \(U_0 := \{(x : y : z) \in \mathbb{P}^2(\overline{K}) \mid x \neq 0\}\). Therefore any point in infinity must be trivial in the first coordinate i.e. all points in infinity are of the form

\((0 : y : z)\)

for appropriate elements \(y\) and \(z\) in \(\overline{K}\). Thence when wanting to find points in infinity lying on the elliptic curve \(E\) in the projective plane \(\mathbb{P}^2(\overline{K})\), appropriate \(y\) and \(z\) in \(\overline{K}\) such that \((0 : y : z) \in V_{\prec}(Z^2X - Y^3 - aYX^2 - BX^3)\) need to be determined. Since \(x = 0\) implies \(y^3 = 0\), it is obvious that \(y = 0\) needs to hold as well. Thus a point in infinity lying on \(E\) in the projective plane \(\mathbb{P}^2(\overline{K})\) is always of the form

\((0 : 0 : z)\)

for an appropriate \(z \in \overline{K}\). Without loss of generality \(z = 1\) can be set according to definition 3.11.

Altogether the only element solving the given homogenized non-generalized Weierstrass equation in the projective plane is given by

\((0 : 0 : 1)\).

So the elliptic curve \(E\) needs to be understood as the union of an affine variety generated by a non-generalized Weierstrass equation and the set only containing the homogeneous coordinate \((0 : 0 : 1)\) under embedding. This unique point in infinity will from now on be denoted as the point \(\infty\) and will be treated in that manner.

Altogether in this subsection it was pointed out, how the extra element \(\infty\) of an elliptic curve has to be understood and also why in the context of this thesis the element \(\infty\) is uniquely defined.

### 3.3. Inducing a group structure.

One of the most common structure in algebra is the one of a (abelian) group. Therefore the aim of this subsection is to introduce a binary operation \(+\) on an elliptic curve. This operation can be proven to be associative and commutative. More precisely it will be proven that an elliptic curve endowed with this operation forms an abelian group. Fortunately this concept can even be applied to the case of restricted elliptic curves.
Definition 3.22. Rules of addition

Let $E$ be an elliptic curve over a field $K$ which is given by a non-generalized Weierstrass equation $Y^2 = X^3 + AX + B$ with $A$ and $B$ in $K$. Furthermore let $P := (x_1, y_1)$ and $Q := (x_2, y_2)$ be elements in $E\setminus\{\infty\}$. Then the addition $P + Q := Z := (x_3, y_3)$ is defined by the following.

1. **Case I** $x_1 \neq x_2$:
   
   Set $m := (y_2 - y_1)(x_2 - x_1)^{-1}$ and define
   
   $x_3 := m^2 - x_1 - x_2$
   
   $y_3 := m(x_1 - x_3) - y_1$.

2. **Case II** $x_1 = x_2, y_1 \neq y_2$:
   
   Define $Z := \infty$.

3. **Case III** $P = Q, y_1 \neq 0$:
   
   Set $m := (3x_1^2 + A)(2y_1)^{-1}$ and define
   
   $x_3 := m^2 - 2x_1$
   
   $y_3 := m(x_1 - x_3) - y_1$.

4. **Case IV** $P = Q, y_1 = 0$:
   
   Define $Z := \infty$.

Additionally for any $V \in E$, $V + \infty := V =: \infty + V$ is set.

Remark 3.23. The addition is well-defined.

Proof. Let $K$ be a field and $Y^2 = X^3 + AX + B$ be a non-generalized Weierstrass equation with coefficients $A$ and $B$ in $K$ describing the elliptic curve $E$. Obviously the case of adding $\infty$ to an element in an elliptic curve is well-defined. Therefore only elements $(x_1, y_1)$ and $(x_2, y_2)$ in $E\setminus\{\infty\}$ need to be considered.

If Case II or Case IV need to be applied, then the claim holds trivially. Thus only Case I and Case III need to be examined.

Since the field $K$ is closed under addition and multiplication, $(x_1, y_1) + (x_2, y_2) := (x_3, y_3)$ is an element of $K \times K$. Therefore it only needs to be examined whether $(x_3, y_3)$ is an element of the non-generalized Weierstrass equation.

Considering Case I yields $m := (y_2 - y_1)(x_2 - x_1)^{-1}$, $x_3 := m^2 - x_1 - x_2$ and $y_3 := m(x_1 - x_3) - y_1$.

Proving $(x_3, y_3)$ solving the given non-generalized Weierstrass equation is not difficult and can be done easily by a straightforward approach. Yet a lengthy calculation is needed and the proof will just shortly be sketched.

Firstly the equation $y_3^2 = (m(x_1 - x_3) - y_1)^2$ needs to be considered. Then $x_3$ can be replaced with $m^2 - x_1 - x_2$. This yields a term only controlled by $x_1$, $x_2$ and $m$. Next substituting $m$ with $(y_2 - y_1)(x_2 - x_1)^{-1}$ and recalling $y_1^2 = x_1^3 + Ax_1 + B$ and $y_2^2 = x_2^3 + Ax_2 + B$ yields an equation only controlled by $x_1$ and $x_2$. Lastly reordering and substituting $(y_2 - y_1)(x_2 - x_1)^{-1}$ with $m$ in reverse proves

\[ y_3^2 = x_3^3 + Ax_3 + B. \]

The proof of Case III can be done by an analogous straightforward approach.

Altogether $P + Q$ is an element in the elliptic curve $E$ for all cases, so the addition is well-defined. ■

Proposition 3.24. Let $E$ be an elliptic curve over a field $K$ described by a non-generalized Weierstrass equation, then $(E, +, \infty)$ is an abelian group with neutral element $\infty$ and for any $(x, y) \in E\setminus\{\infty\}$ the additive inverse is given by $(x, -y)$.

Proof. Let $K$ be a field and $Y^2 = X^3 + AX + B$ be a non-generalized Weierstrass equation with coefficients $A$ and $B$ in $K$ describing the elliptic curve $E$. As already pointed out in remark 3.23 the addition is well-defined. Furthermore $\infty$ is obviously the neutral element of $+$ by definition.

In order to prove the existence of inverse elements, arbitrary but fixed elements $(x, y) \in E\setminus\{\infty\}$ need to be considered. As already pointed out in example 3.6 $(x, -y) \in E\setminus\{\infty\}$ immediately holds as well, due to the symmetrical property of $E$. Obviously when adding $(x, -y)$ to $(x, y)$ Case II or Case IV need to be applied which yield $(x, y) + (x, -y) = \infty$. Hence $-(x, y) = (x, -y)$.

Moreover $-\infty = \infty$ holds trivially.

When aiming to prove commutativity, the case of adding $\infty$ to an arbitrary element in $E$, can be excluded, since for all $V \in E\setminus\{\infty\}$ immediately holds as well, due to the symmetrical property of $E$. Obviously when adding $(x, -y)$ to $(x, y)$ Case II or Case IV need to be applied which yield $(x, y) + (x, -y) = \infty$. Hence $-(x, y) = (x, -y)$.

Moreover $-\infty = \infty$ holds trivially.
Firstly the setting of Case I will be considered. According to definition 3.22 it is known that 
\((x_1, y_1) + (x_2, y_2) =: (x_3, y_3)\) with 
\[ m := (y_2 - y_1)(x_2 - x_1)^{-1} \]
\[ x_3 := m^2 - x_1 - x_2 \]
\[ y_3 := m(x_1 - x_3) - y_1. \]

Analogously \((x_2, y_2) + (x_1, y_1) =: (\overline{x}_3, \overline{y}_3)\) with 
\[ m := (y_1 - y_2)(x_1 - x_2)^{-1}, \quad \overline{x}_3 := m^2 - x_2 - x_1 \]
and 
\[ \overline{y}_3 := m(x_2 - \overline{x}_3) - y_2 \] can be derived. Obviously 
\[ m := (y_2 - y_1)(x_2 - x_1)^{-1} = (-1)(y_1 - y_2)(-1)^{-1}(x_1 - x_2)^{-1} \]
\[ = (y_1 - y_2)(x_1 - x_2)^{-1} := \overline{m} \] (3.1)
which implies 
\[ x_3 := m^2 - x_1 - x_2 = \overline{m}^2 - x_2 - x_1 =: \overline{x}_3. \] (3.2)

Hence 
\[ y_3 := m(x_1 - x_3) - y_1 = (3.1),(3.2) \quad \overline{m}(x_1 - \overline{x}_3) - y_1. \] (3.3)
Moreover \(x_3 := m^2 - x_1 - x_2\) yields 
\[ x_1 = m^2 - x_2 - x_3 = (3.1),(3.2) \quad \overline{m}^2 - x_2 - \overline{x}_3 \] (3.4)
and so 
\[ y_3 = (3.3) \quad \overline{m}(x_1 - \overline{x}_3) - y_1 = (3.4) \quad \overline{m}(m^2 - x_2 - \overline{x}_3 - \overline{x}_3) - y_1 \] (3.5)
can be observed. Furthermore using 
\[ m := (y_2 - y_1)(x_2 - x_1)^{-1} \] shows 
\[ y_1 = (3.1),(3.4) \quad y_2 - \overline{m}(x_2 - m^2 + x_2 + \overline{x}_3) \]
\[ = y_2 - \overline{m}(2x_2 - \overline{m}^2 + \overline{x}_3). \] (3.6)
Finally 
\[ y_3 = (3.5) \quad \overline{m}(m^2 - x_2 - \overline{x}_3 - \overline{x}_3) - y_1 \]
\[ = (3.6) \quad \overline{m}(m^2 - x_2 - \overline{x}_3 - \overline{x}_3) - y_2 + \overline{m}(2x_2 - \overline{m}^2 + \overline{x}_3) \]
\[ = \overline{m}^4 - \overline{m}x_2 - 2\overline{m}x_3 - y_2 + 2\overline{m}x_2 - \overline{m}^3 + \overline{m}x_3 \]
\[ = \overline{m}(x_2 - \overline{x}_3) - y_2 = \overline{y}_3 \]
concludes the proof of commutativity for the first case.

Altogether 
\((x_1, y_1) + (x_2, y_2) = (x_3, y_3) = (\overline{x}_3, \overline{y}_3) = (x_2, y_2) + (x_1, y_1)\)
was proven.
The commutativity for Case III can be proven analogously.
Altogether commutativity was proven.

It finally remains to prove associativity.

One way of proving associativity is using a straight forward approach considering all possible cases whereas the case of adding \(\infty\) to two other points is trivial and hence can be excluded. Nevertheless the addition of three points would still resolve in examining several different cases. Therefore this approach is stylistically unattractive.

In a more beautiful approach the theory of projective spaces could be used. However, this proof needs a lot more sophisticated theory than so far introduced and would furthermore outrage the scope of this thesis. Nevertheless a full proof of associativity can be found in [19][Subsection 2.4].

All in all \((E, +, \infty)\) was proven to be a well-defined abelian group. Hence from now on when talking of an elliptic curve \(E\) implicitly the set of \(E\) endowed with + as an abelian group will be meant. Moreover the abelian group \((E, +, \infty)\) can once again be restricted onto the underlying field.
Corollary 3.25. Let $K$ and $L$ be fields such that $K \subseteq L \subseteq \overline{K}$. Furthermore let $+$ be defined as in definition 3.22 over the elliptic curve $E(L)$ described by a non-generalized Weierstrass equation, then $(E(L), +, \infty)$ is a well-defined abelian group with neutral element $\infty$ and for any $(x, y) \in E(L) \setminus \{\infty\}$ the inverse is given by $(x, -y)$.

Proof. Since $L$ as a subfield of $\overline{K}$ is closed under addition and multiplication, the corollary can be proven analogously to proposition 3.24. □

At a first glance definition 3.22 might seem unreasonable. However, the definition is geometrically motivated. Following up a very detailed explanation of how the addition can be interpreted geometrically using two examples will be given. The first example will be done over the commonly known field $\mathbb{R}$. Then the second example will use the same geometrical motivation as the first example, but focuses on elliptic curves restricted on finite fields.

Example 3.26. Geometrical motivation over $\mathbb{R}$

For reasons of simplicity an arbitrary elliptic curve $E(\mathbb{R})$ restricted on $\mathbb{R}$ given by a non-generalized Weierstrass equation $Y^2 = X^3 + AX + B$ with coefficients $A$ and $B$ in $\mathbb{R}$ will be considered. Well known according to example 3.6 such a curve is symmetric with respect to the $X$-axis.

Firstly the case of two elements $P$ and $Q$ in $E(\mathbb{R}) \setminus \{\infty\}$ with distinct $X$-coordinates will be considered. The geometrical motivation of the addition of such two elements is visualized in figure 3.

![Figure 3. Addition of two points with distinct X-coordinates.](image)

The idea which motivates the addition of $P$ and $Q$ is to firstly connect $P$ and $Q$. This is visualized as Step 1 in figure 3. Next a third point $S'$ is determined which is the intersection point of the restricted elliptic curve $E(\mathbb{R})$ and the connection line of $P$ and $Q$. This is the point found in Step 2 in figure 3. Lastly $S'$ is reflected with respect to the $X$-axis which yields another point $S$ on the restricted elliptic curve $E(\mathbb{R})$, due to the symmetrical property. This found point $S$ shall be the sum of $P$ and $Q$. So Step 3 in figure 3 visualizes how lastly the supposed sum $S$ of $P$ and $Q$ is determined.

The just explained geometrical motivation indeed coincides with Case I of definition 3.22.

The first step of connecting $P := (x_1, y_1)$ and $Q := (x_2, y_2)$ yields a straight line with slope

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$
More precisely the connection line is given by $Y = m(X - x_1) + y_1$. An intersection point of that connection line and the considered restricted elliptic curve $E(\mathbb{R})$, if existing, is given by $S' := (x'_3, y'_3)$ with

$$(y'_3)^2 = (x'_3)^3 + Ax'_3 + B$$

and

$$y'_3 = m(x'_3 - x_1) + y_1.$$

Therefore the equation

$$(m(x'_3 - x_1) + y_1)^2 \neq (x'_3)^3 + Ax'_3 + B \tag{3.7}$$

needs to be examined in the manner of finding an appropriate $X$-coordinate for $S'$. However, firstly a very general observation needs to be made which can then be adapted to this special case.

Let $\alpha, \beta$ and $\gamma$ be coefficients in $\mathbb{R}$ for a term $X^3 + \alpha X^2 + \beta X + \gamma$. When working over the algebraic closure of $\mathbb{R}$ i.e. working over $\mathbb{C}$, this term can be factored into a product

$$X^3 + \alpha X^2 + \beta X + \gamma = (X - r_1)(X - r_2)(X - r_3)$$

for unique roots $r_1, r_2$ and $r_3$ in $\mathbb{C}$, due to the fundamental theorem of algebra. Therefore

$$X^3 + \alpha X^2 + \beta X + \gamma = (X - r_1)(X - r_2)(X - r_3) = X^3 - X^2(r_1 + r_2 + r_3) + X(r_1r_2 + r_1r_3 + r_2r_3) - r_1r_2r_3.$$

By comparison of coefficients this yields

$$\alpha = -(r_1 + r_2 + r_3).$$

The just made observation can be applied to the currently observed example.

Firstly factoring equation (3.7) yields

$$0 = X^3 - m^2 X^2 + X(A + 2m^2 x_1 - 2my_1) + B - m^2 x_1^2 + 2my_1x_1 - y_1^2 = (X - r_1)(X - r_2)(X - r_3)$$

for three unique appropriate roots $r_1, r_2$ and $r_3$ in $\mathbb{C}$. Obviously $x_1$ and $x_2$ are roots of that equation by construction, hence without loss of generality $r_1 := x_1$ and $r_2 := x_2$ can be set.

Applying the just made general observation to this example with $\alpha = -m^2$ hence yields

$$m^2 = x_1 + x_2 + r_3.$$

Therefore the third root $r_3$ is given by

$$r_3 = m^2 - x_1 - x_2$$

which is obviously an element in $\mathbb{R}$. Hence the only possible existing $X$-coordinate for $S'$ was found to be

$$x'_3 = r_3 = m^2 - x_1 - x_2.$$

Inserting $x'_3$ into the formula of the connection line yields the $Y$-coordinate of $S'$ given by

$$y'_3 = m(x'_3 - x_1) + y_1.$$

Altogether the first step of the geometrical motivation was translated into the terms of definition 3.22. The second step of the geometric motivation can be translated easily. Let $S := (x_3, y_3)$ be the mirrored point of $S' := (x'_3, y'_3)$ with respect to the $X$-axis, so

$$x_3 = x'_3 = m^2 - x_1 - x_2$$

and

$$y_3 = -y'_3 = -m(x'_3 - x_1) + y_1 = m(x_3 - x_3) - y_1.$$

To put it all in a nutshell, the geometrical motivation indeed coincides with Case I of definition 3.22.

Wanting to geometrically motivate Case II of the addition, two distinct elements $P$ and $Q$ in $E(\mathbb{R}) \setminus \{\infty\}$ having the same $X$-coordinate but distinct $Y$-coordinates will be considered. The geometrical motivation for the second case is analogous to the geometrical motivation of the first case.

Firstly the connection line of $P$ and $Q$ needs to be determined. Since the two points have the same $X$-coordinate and both are element of the underlying restricted elliptic curve, it is known that $P$ and $Q$ are each others mirror points with respect to the $X$-axis. Therefore the connection line is obviously
vertical and thus parallel to the $Y$-axis.

Recalling example 3.21, in general vertical parallels intersect a (restricted) elliptic curve in the uniquely defined point $\infty$. Thus it is natural to set $S' := \infty$. Moreover according to definition 3.11 $-\infty = \infty$ and thus the step of mirroring $S'$ with respect to the $X$-axis yields $S := -S' = -\infty = \infty$. Therefore this geometrical motivation coincides with Case II of definition 3.22.

Aiming to examine Case III, a point $P \neq \infty$ with a $Y$-coordinate unequal zero needs to be considered and added to itself. The procedure for adding $P$ to itself can again be visualized as done in figure 4.

![Figure 4. Addition of a point with a $Y$-coordinate unequal 0 to itself](image)

Analogously to the just explained two cases the idea of the geometrical motivation is to firstly determine the connection line of the two points, which shall be added. In this case this resolves in determining the tangential line in $P$ with respect to the restricted elliptic curve $E(\mathbb{R})$ which was done in Step 1 of figure 4. The next steps follow the same geometrical procedure as done in the first case. These steps are visualized as Step 2 and Step 3 in figure 4.

This geometrical procedure can now be translated into terms of formula. Firstly the tangential line in $P$ with respect to the restricted elliptic curve $E(\mathbb{R})$ can be derived by an implicit derivation of $Y^2 = X^3 + AX + B$ which yields $2Y = 3X^2 + A$. Thus the slope $m$ of the tangential line in $P := (x_1, y_1)$ with respect to $E(\mathbb{R})$ is given by

$$m := \frac{3x_1^2 + A}{2y_1}.$$  

At this point it is important to emphasize that $y_1$ as the $Y$-coordinate of $P$ was explicitly assumed to be unequal zero. Therefore the division by $2y_1 \neq 0$ is permitted and the tangential line is given by

$$Y = m(X - x_1) + y_1.$$  

Wanting to find an intersection point $S' := (x'_2, y'_2)$ of this tangential line and the restricted elliptic curve given, the same observation as before can be used, proving

$$0 = X^3 - m^2X^2 + X(A + 2m^2x_1 - 2my_1) + B - m^2x_1^2 + 2my_1x_1 - y_2^2 = (X - r_1)(X - r_2)(X - r_3)$$  

for three unique roots $r_1, r_2$ and $r_3$ in $\mathbb{C}$. Recalling that $P$ is added to itself yields $x_1$ being a double root of this equation. Hence $r_1 = x_1 = r_2$ can be set without loss of generality. Therefore the third
root is found to be
\[ r_3 = m^2 - 2x_1 \]
and so
\[ x_2' = m^2 - x_1 - x_1 = m^2 - 2x_1 \]
is immediately derived as the only possible \( X \)-coordinate of \( S' \). This is obviously an existing element in \( \mathbb{R} \). Inserting \( x_2' \) as the \( X \)-coordinate in \( Y = m(X - x_1) + y_1 \) yields the \( Y \)-coordinate
\[ y_2' = m(x_2' - x_1) + y_1 \]
of \( S' \).
Lastly mirroring \( S' \) with respect to the \( X \)-axis delivers \( S := (x_2, y_2) \) with
\[ x_2 = x_2' = m^2 - 2x_1 \]
and
\[ y_2 = -y_2' = m(x_1 - x_2) - y_1. \]

Altogether it was shown that the geometrical motivation in this case coincides with Case III of definition 3.22.

For Case IV \( P \) must be set as an arbitrary but fixed element in \( E(\mathbb{R}) \setminus \{\infty\} \) with a \( Y \)-coordinate being equal zero. Using the same idea as before, the tangential line in \( P \) with respect to \( E(\mathbb{R}) \) must firstly be determined. Since an elliptic curve restricted on \( \mathbb{R} \) is symmetric with respect to the \( X \)-axis, it is obvious that the slope of the tangential line of a point with respect to a restricted elliptic curve gets steeper, the closer the \( Y \)-coordinate of the boundary point gets to zero. Hence if the \( Y \)-coordinate of the boundary point is equal zero the tangential line is vertical i.e. parallel to the \( Y \)-axis. This is the case for \( P \). Just as in the second case it is known that a vertical line intersects the restricted elliptic curve \( E(\mathbb{R}) \) uniquely in \( \infty \). Thus \( P + P = -\infty = \infty \) analogously to Case II.

**Example 3.27. Geometrical motivation over finite fields**

In this example a finite field \( \mathbb{F}_p \) for a prime \( p \) and a restricted elliptic curve \( E(\mathbb{F}_p) \) given by the non-generalized Weierstrass equation \( Y^2 = X^3 + AX + B \) with coefficients \( A \) and \( B \) in \( \mathbb{F}_p \) will be considered. Furthermore two fixed non-trivial elements \( P \) and \( Q \) in \( E(\mathbb{F}_p) \) shall be added.
Firstly the connection line of \( P \) and \( Q \) needs to be determined and then a third intersection point \( S' \) of the connection line of \( P \) and \( Q \) with the restricted elliptic curve given, needs to be found.

In this setting it might occur that the connection line of two points reaches a boundary of the plane \( \mathbb{F}_p^2 \) before intersecting the considered restricted elliptic curve. In that case the connection line would be geometrically continued from the corresponding opposite boundary with the same slope.
If for example the connection line has a slope of 3 and reaches the top boundary at coordinate \((x, p)\) for a fixed \( x \in \{1, \ldots, p-1\} \), then the connection line needs to be continued with the same slope of 3 in \((x, 0)\). Such a procedure is to be continued until the connection line intersects the restricted elliptic curve for the first time.
Hence the intersection point \( S' \) of a connection line of two to-be-added points with a given restricted elliptic curve can be geometrically determined.
Lastly mirroring \( S' \) with respect to the horizontale line running through \((0, \frac{p}{2})\) (to be interpreted over \( \mathbb{Q} \)), yields the sum \( S \) of \( P \) and \( Q \).

To clarify this geometrical interpretation for an elliptic curve restricted on a finite field, another example will be pointed out. Therefore the prime \( p := 7 \) and the coefficients \( A := 3 \) and \( B := 1 \) for a non-generalized Weierstrass equation will be considered. Moreover \( P := (2, 1) \) and \( Q := (3, 3) \) which are elements in the corresponding restricted elliptic curve \( E(\mathbb{F}_7) \), shall be added as visualized in figure 5.
Following the just described geometrical procedure in Step 1 of figure 5 the connection line of $P$ and $Q$ is determined. Then the intersection point of this connection line with the considered restricted elliptic curve is found to be $S' := (6, 2)$ in Step 2. Mirroring $S'$ with respect to the horizontal axis running through $(0, 3.5)$ yields $S := (6, 5)$ in Step 3 of figure 5.

Wanting to verify that the geometrical motivation coincides with the rules of addition, they need to be applied carefully. Since the X-coordinates of $(2, 1)$ and $(3, 3)$ are distinct, Case I needs to be applied. An easy calculation shows

\[
\begin{align*}
    m &= 2 \cdot 1^{-1} = 2 \mod 7 \\
    x &= 2^2 - 2 - 3 = 4 - 2 - 3 = -1 = 6 \mod 7 \\
    y &= 2 * (2 - 6) - 1 = 2 * (-4) - 1 = 2 * 3 - 1 = 5 \mod 7.
\end{align*}
\]

So

\[
P + Q = (x, y) = (6, 5) = S
\]

was determined according to the rules of addition.

Summing up, it was pointed out, how the geometrical motivation of the first case of the rules of addition can be reasonably applied to elliptic curves restricted on finite fields. Of course all other cases of the rules of addition can be applied analogously.

At this point it is important to emphasize that in example 3.26 and example 3.27 it was implicitly assumed, that an unique intersection point in the plane can always be founded. This can indeed be mathematically proven, but would outrange the scope and aim of this thesis.

The concept of adding a point a fixed integer times to itself will later be important for efficiently implementing elliptic curves in crypto-systems.

**Definition 3.28.** Let $E$ be an elliptic curve over a field $K$, $P \in E$ and $k \in \mathbb{Z}$. Then

\[
*_{k}(P) := kP := \begin{cases} 
    P + \ldots + P & \text{if } k \geq 0 \\
    (-P) + \ldots + (-P) & \text{if } k < 0.
\end{cases}
\]

Remark 3.29. The above multiplication by $k$ is well-defined by repeatedly applying remark 3.23 a finite $\#k$-times.

It is important to emphasize $0P := \infty$.

Obviously this concept can be applied to any restricted elliptic curve $E(L)$ for any field $L$ with $K \subseteq L \subseteq \overline{K}$.

Altogether this subsection firstly induced an additive operation $+$ on elliptic curves. Secondly it was proven that the set of an elliptic curve together with this operation forms a well-defined abelian group. Lastly it was pointed out, how this addition is geometrically motivated and a short notation for adding a point an integer times to itself was introduced.
4. Endomorphisms of elliptic curves

After chapter 3 introduced the set of an elliptic curve and proved that a set of an elliptic curve $E$ can be endowed with an addition $+$ such that $(E, +, \infty)$ forms an abelian group, this chapter aims to adapt the algebraic concept of endomorphisms to elliptic curves. This concept will be extremely important in proving Hasse’s Theorem in chapter 6.

Therefore subsection 4.1 firstly defines the term of an endomorphism of an elliptic curve. This definition will be explained using the important example of the Frobenius map of a fixed elliptic curve. Furthermore this subsection will emphasize how an endomorphism can be uniquely (up to association) be represented by rational functions. Such a standardized representation yields a way of uniquely defining the degree of an endomorphism as well as the property of being separable respectively inseparable. Especially for the class of separable endomorphisms a correspondence between the degree and the kernel of a considered endomorphism will be proven.

Furthermore in subsection 4.2 a short excursus on division polynomials will be made. This special family of polynomials will then be used to point out a standardized representation for the multiplication by a fixed integer over elliptic curves as an endomorphism. Having obtained this standardized representation further properties of the multiplication by a fixed integer will be proven.

Lastly in subsection 4.3 a closer look onto the Frobenius map of an elliptic curve will be taken. It will be proven that this map can be understood as an inseparable endomorphism of an elliptic curve and thus the degree of a Frobenius map can be determined using the observations of the first subsection. Furthermore the Frobenius map of an elliptic curve induces another endomorphism over the same elliptic curve which is separable. This endomorphism will be useful in a to-be-stated theorem which will among others be used in proving Hasse’s Theorem. Moreover this theorem motivates the definition of supersingular curves which will be given in the very end of this subsection.

4.1. Introduction to endomorphisms of elliptic curves.

Having made the observation that an elliptic curve can be understood as an abelian group, further algebraic concepts on the (additive) abelian group of an elliptic curve can be induced. One of these concepts, which shall be adapted to elliptic curves in this subsection, is the concept of endomorphisms.

**Definition 4.1.** Let $E$ be an elliptic curve over a field $K$, then an endomorphism $\alpha$ of $E$ is a homomorphism

$$\alpha : E \to E$$

which is representable as two rational functions $R_1$ and $R_2$ in $\overline{K}(X, Y)$.

Moreover if $\alpha \neq \infty$, then the representing rational functions shall be simultaneously defined in at least one element in $E \setminus \{\infty\}$ i.e. it exists at least one element $(x, y) \in E \setminus \{\infty\}$ such that $R_1(x, y)$ and $R_2(x, y)$ are simultaneously defined.

**Remark 4.2.** In this context $\alpha$ being a homomorphism means that for all $P, Q \in E$ it holds

$$\alpha(P + Q) = \alpha(P) + \alpha(Q).$$

Furthermore being representable as rational functions $R_1, R_2 \in \overline{K}(X, Y)$ means that for all $(x, y) \in E \setminus \{\infty\}$, in which $R_1$ and $R_2$ are simultaneously defined, it holds

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

**Remark 4.3.** Since $\alpha$ is a homomorphism $\alpha(\infty) = \infty$.

**Notation 4.4.** If $\alpha \equiv \infty$, then $\alpha$ is denoted as the trivial endomorphism $0$ of $E$.

Aiming to clarify the term of endomorphisms of elliptic curves, an easy to understand, yet very important example of an endomorphism is given next.
Putting it all together and moreover appropriate polynomials and curve
Firstly an arbitrary but fixed rational function endomorphism of
over Weierstrass equation be transformed into a standardized pair of representing rational functions.
Obviously closely related to the commonly-known Frobenius map over
All in all the map and is well-defined.
Moreover the homomorphic property of and This proves \( \phi_q(x, y) \in E \) and so the map \( \phi_q \) is well-defined.
Furthermore the homomorphic property of \( \phi_q \) can be proven easily by a straight forward, yet lengthy calculation, where all possible cases of the rules of addition on elliptic curves need to be considered and \((a + b)^q = a^q + b^q\) for elements \( a \) and \( b \) in \( \mathbb{F}_q \) and \( c^q = c \) for elements \( c \in \mathbb{F}_q \) need to be used. A detailed proof of the homomorphic property of \( \phi_q \) will be given in the means of proving proposition 4.24 in subsection 4.3.

All in all the map \( \phi_q \) defined in this example is an easy to understand example of an endomorphism of an elliptic curve over a finite field. This map is called the Frobenius map of \( E \) over \( \mathbb{F}_q \) and is obviously closely related to the commonly-known Frobenius map over \( \mathbb{F}_q \).

The Frobenius map introduced in example 4.5 on an elliptic curve will be more closely examined in subsection 4.3.

Moreover it is important to emphasize that the rational functions representing an endomorphism \( \alpha \) of an elliptic curve do not have to be unique. However, every representing pair of rational functions can be transformed into a standardized pair of representing rational functions.

In order to explain this procedure a field \( K \) and an elliptic curve \( E \) over \( K \) given by the non-generalized Weierstrass equation \( Y^2 = X^3 + AX + B \) with coefficients \( A \) and \( B \) in \( K \) need to be considered. Moreover \( p(X) := X^3 + AX + B \) is set to be a polynomial in \( K[X] \subseteq \overline{K}[X] \) and \( \alpha \) is set to be a fixed endomorphism of \( E \).

Firstly an arbitrary but fixed rational function \( R(X, Y) \in \overline{K}(X, Y) \) over the setting of the elliptic curve \( E \) will be considered. Thence by the definition of rational functions, there exist polynomials \( r_1 \) and \( r_2 \) in \( \overline{K}[X, Y] \) such that
\[
R = \frac{r_1}{r_2}. \tag{4.2}
\]
Moreover appropriate polynomials \( p_1, p_2, q_1 \) and \( q_2 \) in \( \overline{K}[X] \) can be found such that
\[
r_1(X, Y) = p_1(X) + Yp_2(X) \tag{4.3}
\]
and
\[
r_2(X, Y) = q_1(X) + Yq_2(X). \tag{4.4}
\]

Putting it all together \( R \) can be written as
\[
R(X, Y) = \frac{r_1(X, Y)}{r_2(X, Y)} \xlongequal{(4.2)} \frac{p_1(X) + Yp_2(X)}{(4.3, 4.4) q_1(X) + Yq_2(X)} = \frac{(p_1(X) + Yp_2(X))(q_1(X) - Yq_2(X))}{(q_1(X) + Yq_2(X))(q_1(X) - Yq_2(X))} \xlongequal{(4.5)} \frac{(p_1(X) + Yp_2(X))(q_1(X) - Yq_2(X))}{q_1^2(X) + Y^2q_2^2(X)}.
\]
 Obviously substitute $Y^2$ with $p(X)$ in the denominator of (4.5) is possible in the setting of the elliptic curve $E$. This yields the denominator
\[ \bar{q}(X) := q_1^2(X) - q_2^2(X)p(X) \]
in $K[X]$. Furthermore $\tilde{p}_1$ and $\tilde{p}_2$ in $K[X]$ can be defined as
\[ \tilde{p}_1(X) := p_1(X)q_1(X) - p(X)p_2(X)q_2(X) \] (4.6)
and
\[ \tilde{p}_2(X) := p_2(X)q_1(X) - p_1(X)q_2(X) \] (4.7)
Analogously as done for the denominator, the numerator of (4.5) can be rewritten using the setting of the elliptic curve $E$ which shows
\[ (p_1(X) + Yp_2(X))(q_1(X) - Yq_2(X)) = p_1(X)q_1(X) - Y^2p_2(X)q_2(X) - Yp_1(X)q_2(X) + Yp_2(X)q_1(X) \]
\[ = p_1(X)q_1(X) - p(X)p_2(X)q_2(X) + Y(p_2(X)q_1(X) - p_1(X)q_2(X)) \]
\[ = \tilde{p}_1(X) + Y\tilde{p}_2(X). \]
Altogether a simplified representation for a general rational function $R$ was derived to be given by
\[ R(X, Y) = \frac{\tilde{p}_1(X) + Y\tilde{p}_2(X)}{\bar{q}(X)}. \] (4.8)

Coming back to the setting of the endomorphism $\alpha$, the representing rational functions $R_1$ and $R_2$ in $K(X, Y)$ with $\alpha = (R_1, R_2)$ are now to be considered. Moreover $P := (x, y)$ is set to be an element in $E \setminus \{\infty\}$ such that $R_1$ and $R_2$ are simultaneously defined in $P$. Obviously $R_1$ and $R_2$ are then also simultaneously defined in $-P = (x, -y)$ because of $\alpha(P) = -\alpha(-P)$ for the endomorphism $\alpha$.

The just made observation (4.8) for a general rational function over the setting of the elliptic curve $E$ can now be applied to $R_1$. Therefore the existence of polynomials $\overline{p}_1$, $\overline{p}_2$ and $\bar{q}$ in $K[X]$ is known such that
\[ R_1(P) = R_1(x, y) = \frac{\overline{p}_1(x) + y\overline{p}_2(x)}{\bar{q}(x)}. \] (4.9)
Calculating $R_1(x, -y)$ in the same manner as $R_1(x, y)$ was calculated, yields
\[ R_1(x, -y) = \frac{\overline{p}_1(x) - y\overline{p}_2(x)}{\bar{q}(x)}. \] (4.10)
Furthermore $\alpha$ especially being a homomorphism of $E$ proves
\[ (R_1(x, -y), R_2(x, -y)) = \alpha(-P) = -\alpha(P) = -(R_1(x, y), R_2(x, y)) = (R_1(x, y), -R_2(x, y)) \]
and so
\[ R_1(x, y) = R_1(x, -y). \]
Together with (4.9) and (4.10) this yields
\[ y\overline{p}_2(x) = -y\overline{p}_2(x). \] (4.11)
Since $P := (x, y)$ was arbitrarily chosen in $E \setminus \{\infty\}$ observation (4.11) holds for infinitely many $(x, y) \in E \setminus \{\infty\}$ and so
\[ \overline{p}_2 \equiv 0 \]
which proves
\[ R_1(X, Y) = \frac{\overline{p}_1(X) + Y\overline{p}_2(X)}{\bar{q}(X)} = \frac{\overline{p}_1(X)}{\bar{q}(X)}. \] (4.12)
Moreover
\[ R_2(x, -y) = -R_2(x, y) \]
can be proven analogously. Furthermore due to the general observation (4.8) the existence of polynomials $\tilde{p}_1$, $\tilde{p}_2$ and $\bar{q}$ in $K[X]$ is known such that
\[ R_2(X, Y) = \frac{\tilde{p}_1(X) + Y\tilde{p}_2(X)}{\bar{q}(X)}. \]
Thence
\[ \frac{\hat{p}_1(x) - y\hat{p}_2(x)}{q(x)} = R_2(x, -y) = -R_2(x, y) = -\frac{\hat{p}_1(x) + y\hat{p}_2(x)}{q(x)} \]
which shows
\[ \hat{p}_1(x) = -\hat{p}_1(x). \]
Again since \( P := (x, y) \) was arbitrarily chosen in \( E \setminus \{ \infty \} \), the equation especially holds for all \( x \in \mathbb{K} \) and thus
\[ \hat{p}_1 \equiv 0 \]
which shows
\[ R_2(X, Y) = \frac{\hat{p}_1(X) + Y\hat{p}_2(X)}{q(X)} = \frac{Y\hat{p}_2(X)}{q(X)}. \]  
(4.13)

Altogether setting
\[ r_1(X) := \frac{p_1(X)}{q(X)} \]
and
\[ r_2(X) := \frac{p_2(X)}{q(X)} \]
as rational functions in \( \mathbb{K}(X) \) simplifies the representation of the endomorphism \( \alpha \) into
\[ \alpha(X, Y) = (R_1(X, Y), R_2(X, Y)) = (r_1(X), Yr_2(X)). \]  
(4.14)
These rational functions \( r_1(X) \) and \( Yr_2(X) \) can be further standardized.

Firstly \( r_1 \) is considered and \( q \) and \( p \) are set to be polynomials in \( \mathbb{K}[X] \) such that \( q \) and \( p \) do not share a common root and
\[ r_1 = \frac{p}{q}. \]
In case that \( q(x_0) = 0 \) for a \( x_0 \in \mathbb{K} \) and so \( \frac{p}{q} \) not being defined in \( x_0 \), it is then known for all \( y \in \mathbb{K} \) with \( (x_0, y) \in E \) that \( \alpha(x_0, y) = \infty \) due to \( \alpha \) being an endomorphism. Therefore only \( P := (x, y) \) in \( E \setminus \{ \infty \} \) with \( q(x) \neq 0 \) will be considered.

Next \( r_2 \) is to be considered. Analogously as done for \( r_1 \), two polynomials \( s \) and \( t \) in \( \mathbb{K}[X] \) can be found such that \( s \) and \( t \) do not share a common root and
\[ r_2 = \frac{s}{t}. \]

Claim The endomorphism \( \alpha \) is representable as \( \alpha(X, Y) = \left( \frac{p(X)}{q(X)}, \frac{Ys(X)}{t(X)} \right) \).
Firstly set \( P := (x, y) \in E \setminus \{ \infty \} \) with \( q(x) \neq 0 \) arbitrary but fixed. Then
\[ \alpha(P) = \alpha(x, y) = (R_1(x, y), R_2(x, y)) = (r_1(x), yr_2(x)) = \left( \frac{p(x)}{q(x)}, \frac{ys(x)}{t(x)} \right) \]
can easily be observed.
Moreover \( \alpha(P) = (r_1(x), yr_2(x)) \) being an element in \( E \) yields
\[ \left( \frac{ys(x)}{t(x)} \right)^2 = (yr_2(x))^2 = r_1^2(x) + A r_1(x) + B \]
\[ = \left( \frac{p(x)}{q(x)} \right)^3 + A \left( \frac{p(x)}{q(x)} \right) + B = \frac{p^3(x) + Ap(x)q^2(x) + Bq^3(x)}{q^3(x)}. \]  
(4.15)
Hence setting \( u(X) := p^3(X) + Ap(X)q^2(X) + Bq^3(X) \) as a polynomial in \( \mathbb{K}[X] \) yields
\[ \frac{y^2s^3(x)}{t^2(x)} = \left( \frac{ys(x)}{t(x)} \right)^2 = \frac{u(x)}{q^3(x)}. \]  
(4.15)

Subclaim For any \( x \in \mathbb{K} \) with \( q(x) \neq 0 \) the fraction \( \frac{ys(x)}{t(x)} \) is well-defined.

Aspect 1 The polynomials \( u \) and \( q \) do not share a common root.
As for a contradiction it is assumed that there exists a \( x_0 \in \mathbb{K} \) such that \( x_0 \) is a common root of \( u \)
and \( q \) meaning \( u(x_0) = 0 = q(x_0) \). Hence adding zero and using the definition of \( u \) shows
\[
p^3(x_0) = p^3(x_0) + Ap(x_0)q^2(x_0) + Bq^3(x_0) =: u(x_0) = 0
\]
and so
\[p(x_0) = 0.
\]
Therefore \( x_0 \) is a common root of \( p \) and \( q \) which contradicts the choice of \( p \) and \( q \).

Aspect 2 For all \( x \in \overline{K} \) with \( q(x) \neq 0 \) it holds \( t(x) \neq 0 \).

Again for a contradiction it is assumed that there exists a \( x_0 \in \overline{K} \) with \( q(x_0) \neq 0 \) and \( t(x_0) = 0 \).

Moreover \( y \) is set to be an appropriate element in \( \overline{K} \) such that \( (x_0, y) \) is in \( E \). Hence
\[
y^2 = \frac{y^2 s^2}{t^2} \cdot \frac{t^2}{s^2} = \frac{u(x_0)t^2(x_0)}{q^3(x_0)s^2(x_0)}
\tag{4.16}
\]
Recalling \( s \) and \( t \) not sharing a common root and \( t(x_0) = 0 \) by choice of \( x_0 \), obviously \( s(x_0) \neq 0 \) needs to hold. Thus together with Aspect 1 and (4.16) \( x_0 \) is known to be a \( X \)-coordinate of a double root of the considered non-generalized Weierstrass equation.

This contradicts the choice of the considered non-generalized Weierstrass equation which was implicitly assumed to have a non-trivial discriminant as stated in remark 3.10.

Altogether \( t \) being defined in any element in which \( q \) is defined, was proven.

To put it all in a nutshell, the endomorphism \( \alpha \) is representable as
\[
\alpha(X, Y) = \left( \frac{p(X)}{q(X)}, \frac{Y_s(X)}{t(X)} \right)
\]
for appropriate polynomials \( p, q, s \) and \( t \) in \( \overline{K}[X] \) such that \( p \) and \( q \) as well as \( s \) and \( t \) do not share a common root. This representation is simultaneously well-defined in any \( x \in \overline{K} \) in which \( q(x) \neq 0 \).

Moreover if \( q(x) = 0 \) for some \( x \in \overline{K} \) the endomorphism is reasonably evaluated to be equal \( \infty \).

Obviously all representations of \( \alpha \) yield some \( p, q, s \) and \( t \)'s. All such found polynomials need to be associated to the other \( p, q, s \) and \( t \)'s, due to being chosen as reducing the describing fraction as far as possible and \( \overline{K} \) being algebraically closed. Therefore such a representation is unique up to association and will from now on be called a **standardized representation of the endomorphism** \( \alpha \).

Being able to talk of a standardized representation for an endomorphism, defining further properties of an endomorphism is possible.

**Definition 4.6.** Let \( \alpha \) be a non-trivial endomorphism of an elliptic curve \( E \) over \( K \) and \( p, q, s \) and \( t \) be polynomials in \( \overline{K}[X] \) as in a standardized representation given by \( \left( \frac{p}{q}, \frac{Y_s}{t} \right) \). Then the **degree** of \( \alpha \) is defined as
\[
\deg(\alpha) := \max\{\deg(p), \deg(q)\}.
\]

**Remark 4.7.** The degree of the trivial endomorphism 0 is set to be equal zero so \( \deg(0) := 0 \).

**Remark 4.8.** This definition yields an unique degree for any endomorphism \( \alpha \) of an elliptic curve \( E \), since all \( p \) and \( q \)'s of a standardized representation for \( \alpha \) are unique up to association. Thus the degrees of all possible \( p \)'s respectively \( q \)'s are the same and hence the degree of the endomorphism \( \alpha \) is unaffected by the chosen standardized representation.

Another characteristic of endomorphism can be defined using a standardized representation. This property will divide endomorphisms into two distinct classes.

**Definition 4.9.** Let \( \alpha \) be a non-trivial endomorphism of an elliptic curve \( E \) over a field \( K \) and \( p, q, s \) and \( t \) be polynomials in \( \overline{K}[X] \) as in a standardized representation given by \( \left( \frac{p}{q}, \frac{Y_s}{t} \right) \). Moreover \( r_1 \in \overline{K}(X) \) is defined as \( r_1 := \frac{p}{q} \). If \( r_1 \) as the derivative of \( r_1 \) is not identically zero, then \( \alpha \) is called **separable**. Else \( \alpha \) is called **inseparable**.
Remark 4.10. Obviously the property of being separable is equivalent to at least one of $p'$ and $q'$ not being identically zero.

On the one hand when working over a field $K$ with characteristic 0, this means that at least one of $p$ and $q$ is not a constant polynomial.

On the other hand for an underlying field of characteristic $p > 0$ this means that at least one of $p$ and $q$ can not be of the form $g(X^p)$ for any polynomial $g \in \overline{K}[X]$.

In the context of this thesis separable endomorphisms are of a great interest. Therefore an important property of separable endomorphism is observed next.

**Proposition 4.11.** Let $\alpha$ be a non-trivial separable endomorphism of an elliptic curve $E$ over a field $K$, then

$$\deg(\alpha) = \# \ker(\alpha).$$

**Proof.** Firstly a non-trivial separable endomorphism $\alpha$ of $E$ will be considered.

As shown in (4.14), it is known that for all $(x, y) \in E$ it holds $\alpha(x, y) = (r_1(x), yr_2(x))$ for some fixed appropriate rational functions $r_1$ and $r_2$ over the algebraic closure $\overline{K}$ of $K$.

Furthermore let $p$, $q$, $s$ and $t$ be polynomials in $\overline{K}[X]$ with $q \neq 0$ as in a standardized representation $\left(\frac{a}{q}, \frac{b}{t}\right)$ of $\alpha$.

According to definition 4.9 $r_1' \neq 0$, since $\alpha$ is not separable and so $\frac{wp' - pq'}{a} = r_1' \neq 0$ yields $qp' - pq' \neq 0$.

Furthermore

$$S := \{x \in \overline{K} \mid (qp' - pq')(x)q(x) = 0\}$$

can be defined.

**Claim** It exists $(a, b) \in E$ such that

1) $a, b \neq 0$ and $(a, b) \neq \infty$

2) $\deg(p - aq) = \deg(\alpha)$

3) $a \notin r_1(S)$

4) $(a, b) \in \alpha(E)$.

Obviously $S$ is a finite set, since assuming $S$ being infinite implies the existence of infinitely many $x$ solving either $(qp' - pq')(x) = 0$ or $q(x) = 0$. This yields either $qp' - pq' \equiv 0$ or $q \equiv 0$ and hence a contradiction to $\alpha$ being a non-trivial separable endomorphism was found.

Furthermore the set

$$\mathcal{A} := \{r_1(x) \mid x \in \overline{K}\}$$

can be defined. Assuming $\mathcal{A}$ to be a finite set yields $r_1$ having finitely many distinct values when evaluated in infinitely many $x$. Since $r_1$ is a rational function over the infinite algebraic closure $\overline{K}$, this proves $r_1$ being constant. So $r_1' \equiv 0$ needs to hold. This contradicts the preconditions of $\alpha$ being separable. Therefore the set $\mathcal{A}$ is proven infinite.

Due to the definition of an algebraic closure it is known that for all $x \in \overline{K}$ exists a $y \in \overline{K}$ such that $(x, y)$ is an element in the elliptic curve $E$. Together with $r_1' \equiv 0$, $\alpha(E)$ being a infinite set is obvious. Therefore removing finitely many elements of this set resolves in yet another infinite set.

Hence an appropriate element $(a, b) \in E$ can be constructed by firstly fixing an $a \in \overline{K}$ with $a \neq 0$.

Since $S$ is finite, the image of $\mathcal{S}$ under $r_1$ given by $r_1(S)$ needs to be a finite subset of the infinite set $\mathcal{A}$. Thence there exist infinitely many elements $a$ which are not in $r_1(S)$. Therefore $a \notin r_1(S)$ can be tested and after testing finitely many $a$'s an appropriate

$$0 \neq a \notin r_1(S)$$

can be found. For such an $a$ property 3) is met.

At this point it is important to emphasize that $\deg p \neq \deg q$ immediately yields property 2) being fulfilled for any fixed $a$. If this is not the case

$$a \neq \frac{LC(p)}{LC(q)}$$

needs to be tested. In case that this inequality is not given, another $a$ from the remaining infinite set of $a$'s fulfilling property 3) needs to be chosen and again tested until an appropriate $a$ fulfilling 2) and 3) is found after testing finitely many $a$'s.

Moreover not more than three pairs of the form $(a, 0)$ solve the cubic non-generalized Weierstrass
equation defining $E$. Hence an appropriate $a$ satisfying $2)$ and $3)$ such that

$$(a,0) \notin E$$

can easily be chosen.

Lastly $a,b \in \overline{K}\backslash\{0\}$ can obviously be chosen such that $(a,b)$ is in $\alpha(E)$. Altogether the constructed $(a,b)$ fulfills property $1)$ to $4)$.

Such an arbitrary $(a,b)$ in $E$ fulfilling the properties of the just proven claim is now fixed.

**Claim** It holds $\#\{(x,y) \in E \mid \alpha(x,y) = (a,b)\} = \deg \alpha$.

Firstly $P_{a,b} := \{(x,y) \in E \mid \alpha(x,y) = (a,b)\}$ can be defined, which is by property $4)$ not the empty set. Hence let $(x,y) \in P_{a,b}$ be arbitrary but fixed, so

$$(a,b) = \alpha(x,y) = (r_1(x), yr_2(x)).$$

Obviously $q(x) \neq 0$ holds, due to $(a,b) \neq \infty$ and $r_1(x) = \frac{p(x)}{q(x)}$. Moreover it is important to recall that $q(x) \neq 0$ implies $r_2$ being well-defined in $x$. Furthermore $0 \neq b = yr_2(x)$ yields $y = \frac{b}{r_2(x)}$. Hence $y$ being completely defined via $x$ can be observed, meaning that $x$ appearing as the $X$-coordinate of an element in $P_{a,b}$ belongs to exactly one $y$ such that $(x,y)$ is an element in $P_{a,b}$.

Therefore only the number of all possible $X$-coordinates appearing in elements in $P_{a,b}$ needs to be determined.

Due to $(a,b)$ fulfilling property $2)$ $p - aq$ having exactly $\deg \alpha$ many roots is obvious. However, some roots might appear to a power greater than $1$. Consequently

$$\#P_{a,b} \leq \deg \alpha$$

needs to hold. Especially

$$\#P_{a,b} = \deg \alpha$$

if and only if only distinct roots of $p - aq$ exist.

For a contradiction it is assumed that there exists a $(\bar{x},\bar{y})$ in $P_{a,b}$ such that $\bar{x}$ is a multiple root of $p - aq$. Hence

$$(p - aq)(\bar{x}) = 0$$

and

$$0 = (p - aq)'(\bar{x}) = (p' - aq')(\bar{x})$$

which is equivalent to

$$p'(\bar{x}) = aq'(\bar{x}) \quad (4.17)$$

and

$$p(\bar{x}) = aq(\bar{x}). \quad (4.18)$$

Multiplying $(4.18)$ with $p'(\bar{x})$ yields

$$aq(\bar{x})p'(\bar{x}) = p(\bar{x})p'(\bar{x}) = \frac{p(\bar{x})aq'(\bar{x})}{p(\bar{x})} \quad (4.17)$$

which is equivalent to

$$a((qp' - q'p)(\bar{x})) = 0.$$ 

Thus since $a \neq 0$, 

$$(qp' - q'p)(\bar{x}) = 0$$

is proven.

Altogether $\bar{x}$ is an element in $S$ and so $a = r_1(\bar{x})$ is an element in $r_1(S)$ which contradicts $(a,b)$ fulfilling property $3)$.

All in all the assumption must have been wrong and thus no multiple roots for $p - aq$ exist. This proves

$$\#P_{a,b} = \deg \alpha.$$ 

Lastly having a closer look onto the elements in the kernel of $\alpha$ is indispensable for concluding this proof.
For a fixed \((a, b)\) fulfilling property 1) to 4) and \(u, v \in \mathcal{P}_{a,b}\), 
\[(a, b) = \alpha(u) = \alpha(v)\]
by definition of \(\mathcal{P}_{a,b}\). This is equivalent to \(\infty = \alpha(u) - \alpha(v) = \alpha(u - v)\) which proves \(u - v \in \ker \alpha\).

Now an arbitrary but fixed \(u_1 \in \mathcal{P}_{a,b}\) is considered and 
\[\mathcal{M} := \{(u_1, v) \mid v \in \mathcal{P}_{a,b}\}\]
is defined.
Having observed \(\#\mathcal{P}_{a,b} = \deg\alpha\) immediately shows 
\[\#\mathcal{M} \geq \#\mathcal{P}_{a,b}\tag{4.19}\]
Furthermore for any \((u_1, v) \in \mathcal{M}, u_1 - v \in \ker \alpha\) is already known. Hence
\[\# \ker \alpha \geq \#\mathcal{M} \geq \#\mathcal{P}_{a,b} = \deg\alpha\]
For a contradiction
\[\# \ker \alpha > \deg\alpha =: n \in \mathbb{N}\]
is now assumed which yields the existence of at least \(n + 1\) distinct elements in the kernel of \(\alpha\). Therefore appropriate distinct \(a_1, \ldots, a_{n+1}\) in \(K \times K\) exist such that 
\[\{a_1, \ldots, a_{n+1}, \ldots\} \subseteq \ker \alpha\]
Moreover let \((a, b)\) be fixed fulfilling the properties 1) to 4). Then \(\mathcal{P}_{a,b}\) provenly consists of exactly \(n\) elements i.e.
\[\mathcal{P}_{a,b} := \{u_1, \ldots, u_n\}\]
According to the definition of a kernel and \(\mathcal{P}_{a,b}\), for any \(j \in \{1, \ldots, n + 1\}\)
\[(a, b) = \alpha(u_1) = \alpha(u_1 + a_j) = \alpha(u_1 + a_j)\]
is known. Hence \(u_1 + a_j \in \mathcal{P}_{a,b}\) for any \(j \in \{1, \ldots, n + 1\}\). So for any \(j \in \{1, \ldots, n + 1\}\) exists a \(k \in \{1, \ldots, n\}\) such that 
\[u_1 + a_j = u_k\]
This clearly contradicts \(a_1, \ldots, a_{n+1}\) being \(n + 1\) distinct elements, since only \(n\) distinct \(u_k\)'s exist.
The assumption must have been wrong and so altogether
\[\ker \alpha = \deg\alpha\]
was proven. 

\textbf{Remark 4.12.} Let \(\alpha\) be a non-trivial inseparable endomorphism of an elliptic curve \(E\) over a field \(K\), then 
\[\deg(\alpha) > \# \ker(\alpha)\]

\textbf{Proof.} [19][Section 2.8, Proposition 2.20, pp.50]

All in all in this chapter the term of an endomorphism of an elliptic curve was introduced. Then a standardized representation for an endomorphism was derived which is found to be unique up to association. Having made this observation, the degree of an endomorphism and the class of separable endomorphism, was defined. Furthermore an important endomorphism, called the Frobenius map of an elliptic curve, was introduced.

4.2. Excursus on Division Polynomials.

In order to prove that the multiplication by a fixed integer over an elliptic curve is an endomorphism, it will be essential to find representing rational functions. Therefore special polynomials will firstly be introduced. It is important to emphasize that in this chapter the setting of an elliptic curve is assumed to hold implicitly meaning that a field \(K\) is fixed as well as an elliptic curve \(E\) over \(K\) given by a non-generalized Weierstrass equation \(Y^2 = X^3 + AX + B\) for fixed coefficients \(A\) and \(B\) in \(K\). Those coefficients however will not be specified in more detail and hence will be treated as variables.
**Definition 4.13.** The division polynomials are a family of polynomials \( \{\psi_m\}_{m \in \mathbb{N}_0} \subseteq \mathbb{Z}[X,Y,A,B] \) recursively defined by

\[
\psi_0 := 0 \\
\psi_1 := 1 \\
\psi_2 := 2Y \\
\psi_3 := 3X^4 + 6AX^2 + 12BX - A^2 \\
\psi_4 := 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3).
\]

Furthermore for any \( m \geq 2 \)
\[
\psi_{2m} := (2Y)^{-1}\psi_m(\psi_{m+2}\psi_{m-1} - \psi_m^2\psi_{m+1}) \\
\psi_{2m+1} := \psi_{m+2}\psi_{m} - \psi_{m-1}\psi_{m+1}.
\]

**Remark 4.14.** It holds \( \psi_m \in \mathbb{Z}[X,Y^2,A,B] \), while \( m = 1 \) mod 2.
It holds \( \psi_m \in 2Y\mathbb{Z}[X,Y^2,A,B] \), while \( m = 0 \) mod 2.

**Proof.** The proof can easily be done by induction over \( \mathbb{N}_0 \).

**Start of induction for \( m \in \{0, \ldots , 4\} \)** The claim obviously holds according to definition 4.13.

**Claim of induction for all \( n \in \mathbb{N}_0 \leq m \)** It holds \( \psi_n \in \mathbb{Z}[X,Y^2,A,B] \), while \( n = 1 \) mod 2
\( \psi_n \in 2Y\mathbb{Z}[X,Y^2,A,B] \), while \( n = 0 \) mod 2.

**Step of induction for \( m \geq 4, m \mapsto m + 1 \)** Firstly \( m + 1 = 1 \) mod 2 is assumed.
Since \( m \) was chosen greater than 3, it exists a \( n \geq 2 \) such that \( m + 1 = 2n + 1 \), so \( n - 1, n, n + 1 \) and \( n + 2 \) are non-negative integers not larger than \( m \). Hence the claim of induction already holds for those indices.

As a first subcase \( n = 1 \) mod 2 is assumed to be true. Thus \( n + 2 = 1 \) mod 2 and
\( m - 1 = m + 1 = 0 \) mod 2. The claim of induction yields
\[
\psi_{m+1} = \psi_{2n+1} := \underbrace{\psi_{n+2}}_{\subseteq \mathbb{Z}[X,Y^2,A,B]} \star \underbrace{\psi_3}_{\subseteq \mathbb{Z}[X,Y^2,A,B]} - \underbrace{\psi_{n-1}}_{\subseteq 2Y\mathbb{Z}[X,Y^2,A,B]} \star \underbrace{\psi_{n+1}}_{\subseteq 2Y^3\mathbb{Z}[X,Y^2,A,B]} \in \mathbb{Z}[X,Y^2,A,B].
\]

The subcase of \( n = 0 \) mod 2 can be proven analogously.
Furthermore the case of \( m + 1 = 0 \) mod 2 can be shown by an alike argumentation as done for the first case.

**Another two families of polynomials,** which are also essential for the representation of the multiplication by a fixed integer as rational functions, can be defined using these division polynomials. Those two families must be carefully examined, in order to understand their most useful properties.

**Definition 4.15.** Using \( \{\psi_m\}_{m \in \mathbb{N}_0} \) of definition 4.13 two families of polynomials \( \{\phi_m\}_{m \in \mathbb{N}} \) and \( \{\omega_m\}_{m \geq 2} \) in \( \mathbb{Z}[X,Y,A,B] \) can be recursively defined by
\[
\phi_m := X\psi_m^2 - \psi_{m+1}\psi_{m-1}
\]
and
\[
\omega_m := (4Y)^{-1}(\psi_{m+2}\psi_{m-1} - \psi_m^2\psi_{m+1}).
\]

**Remark 4.16.** It holds \( \omega_m \in Y\mathbb{Z}[X,Y^2,A,B] \), while \( m = 1 \) mod 2.
It holds \( \omega_m \in \mathbb{Z}[X,Y^2,A,B] \), while \( m = 0 \) mod 2.
Moreover \( \{\phi_m\}_{m \in \mathbb{N}} \subseteq \mathbb{Z}[X,Y^2,A,B] \).

**Proof.** The claim for \( \{\omega_m\}_{m \geq 2} \) will be proven first.

Therefore firstly a \( m \in \mathbb{N}_{\geq 2} \) such that \( m = 1 \) mod 2 will be considered.
Hence \( m + 2 = m - 2 = 1 \) mod 2 and \( m + 1 = m - 1 = 0 \) mod 2.

According to definition 4.15 and remark 4.14
\[
\omega_m := (4Y)^{-1} \left( \psi_{m+2} \ast \psi_{m-1}^{2} - \psi_{m-2} \ast \psi_{m+1}^{2} \right) \in YZ[Y^2, A, B]
\]
can be observed.
Moreover the case of a $m \in \mathbb{N}_{\geq 2}$ such that $m = 0 \mod 2$, can be proven analogously.

Now the claim for $\{\phi_m\}_{m \in \mathbb{N}}$ will be proven.
Therefore firstly any $m \in \mathbb{N}$ such that $m = 1 \mod 2$ will be considered. Hence $m+1 = m - 1 = 0 \mod 2$.
According to definition 4.15 and remark 4.14
\[
\phi_m := X \ast \psi_m^{2} - \psi_{m+1} \ast \psi_{m-1}^{2} \in Z[Y^2, A, B]
\]
can be observed.
Moreover the case of any $m \in \mathbb{N}$ such that $m = 0 \mod 2$, can be proven analogously.

**Remark 4.17.** Since $Y^2 = X^3 + AX + B$ in the setting of an elliptic curve over a field, the polynomials of definition 4.13 and definition 4.15 can be interpreted in $Z[A, B][X]$ according to remark 4.14 and remark 4.16. Especially
\[
\phi_m(X) = X^{m^2} + \text{(lower degree terms)}
\]
and
\[
\psi_m^{2}(X) = m^{2}X^{m^2-1} + \text{(lower degree terms)}
\]
can be proven.

**Proof.** This structural behavior of $\phi_m$ and $\psi_m^{2}$ can be proven using the structure of $\psi_m$. Therefore firstly $\psi_m$ will be interpreted in $Z[A, B][X, Y]$ and
\[
\psi_m(X, Y) = \begin{cases} 
Y(mX^{m^2-4} + l_{m}^{(e)}(X)), & \text{if } m \text{ is even} \\
(mX^{m^2-4} + l_{m}^{(m)}(X)), & \text{if } m \text{ is odd}
\end{cases}
\]
is claimed whereas $l_{m}^{(m)}$ and $l_{m}^{(e)}$ denote appropriate polynomials in $Z[A, B][X]$ with $\deg l_{m}^{(m)} < \frac{m^2-4}{2}$ and $\deg l_{m}^{(e)} < \frac{m^2-1}{2}$. This claim will be proven by induction over $\mathbb{N}$.

Start of induction for $m \in \{1, \ldots, 4\}$ Firstly $m = 1$ will be considered.
Definition 4.13 yields $\psi_1 \equiv 1$. Furthermore $m(X^{\frac{m^2-1}{2}} + l_{m}^{(m)}(X)) = 1(X^0 + l_{1}^{(1)}(X)) \equiv 1$ holds, since $\deg l_{1}^{(1)} < 0$ yields $l_{1}^{(1)} \equiv 0$.

Altogether
\[
\psi_1 = 1(X^{\frac{1^2-1}{2}} + l_{1}^{(1)}).
\]
Secondly $m = 3$ will be considered. An analogous argumentation immediately yields
\[
\psi_{3} = 3(X^{\frac{3^2-1}{2}} + l_{3}^{(3)}).
\]
Therefore the start of induction for the case of an odd $m \in \{1, 3\}$ was proven.

For the case of an even $m$ firstly $m = 2$ will be considered.
Definition 4.13 yields $\psi_2(X, Y) = 2Y$. Furthermore
\[
Y(mX^{\frac{m^2-4}{4}} + l_{m}^{(e)}(X)) = Y(2X^0 + l_{2}^{(2)}(X)) = 2Y
\]
holds according to an alike argumentation as was done for the odd cases. So
\[
\psi_2(X, Y) = Y(2X^{\frac{2^2-4}{4}} + l_{2}^{(2)}(X))
\]
was proven.
Secondly \( m = 4 \) is considered. Again an analogous argumentation yields
\[
\psi_4(X, Y) = Y(4X^{\frac{2^2-1}{2}} + l_e^{(4)}(X)).
\]
Therefore the start of induction for the case of an even \( m \in \{2, 4\} \) was proven.

**Claim of induction** For all \( s \in \mathbb{N}_{\leq m} \)
\[
\psi_n(X, Y) = \begin{cases} 
Y(sX^{\frac{s^2-1}{2}} + l_{o}^{(s)}(X)), & \text{if } s \text{ is even} \\
(sX^{\frac{s^2-1}{2}} + l_{o}^{(s)}(X)), & \text{if } s \text{ is odd}
\end{cases}
\]

whereas \( l_{o}^{(s)} \) and \( l_{e}^{(s)} \) denote appropriate polynomials in \( \mathbb{Z}[A, B][X] \) such that \( \deg l_{e}^{(s)} < \frac{s^2-2}{2} \) and \( \deg l_{o}^{(s)} < \frac{s^2-1}{2} \).

**Step of induction: \( m \mapsto m + 1 \)** First off the case of \( m > 4 \) being even will be considered. Hence \( m + 1 \) is odd and \( n \) can be set as the unique integer greater than 2 such that \( m = 2n \).

Definition 4.13 yields \( \psi_{m+1} = \psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_n^3 + \psi_{n+1} \). Therefore the structures of \( \psi_n, \psi_{n+2} \) and \( \psi_{n-1}, \psi_{n+1} \) need to be carefully examined.

Since \( 2n = m \) for an appropriate \( m > 4, n-1, n+1 \) and \( n+2 \) being smaller than \( m \) is given. Thus the claim of induction can be applied to \( n-1, n, n+1 \) and \( n+2 \).

As a first subcase \( n \) is assumed to be odd. Therefore \( n+2 \) is odd as well.

The claim of induction yields
\[
\psi_n(X, Y) = n(X^{\frac{n^2-1}{2}} + n_2^{(n)}(X))
\]
and
\[
\psi_{n+2}(X, Y) = (n+2)(X^{\frac{(n+2)^2-1}{2}} + n_2^{(n+2)}(X)).
\]
Furthermore \( n-1 \) and \( n+1 \) need to be even and hence
\[
\psi_{n-1}(X, Y) = Y((n-1)X^{\frac{(n-1)^2-4}{2}} + l_{o}^{(n-1)}(X))
\]
and
\[
\psi_{n+1}(X, Y) = Y((n+1)X^{\frac{(n+1)^2-4}{2}} + l_{o}^{(n+1)}(X)).
\]

Altogether
\[
\psi_{n+2}(X, Y)\psi_n^3(X, Y) = (n+2)n^3(X^{\frac{(n+2)^2-1}{2}}X^{\frac{3(n^2-1)}{2}} + l(X)) = n^3(n+2)(X^{\frac{4n^2+4n}{2}} + l(X)) = (n^3 + 2n^3)(X^{\frac{(2n+1)^2-1}{2}} + l(X))
\]

whereas \( l \) denotes an appropriate polynomial in \( \mathbb{Z}[A, B][X] \) with \( \deg l < \frac{(2n+1)^2-1}{2} \).

Analogously
\[
\psi_{n-1}(X, Y)\psi_n^3(X, Y) = Y^4((n-1)(n+1)X^{\frac{(n-1)^2-4k(n+1)^2-12}{2}} + h(X)) = Y^4((n^3 + 2n^3 - 2n - 2)X^{\frac{4n^2+4n-12}{2}} + h(X))
\]

with \( h \) being an appropriate polynomial in \( \mathbb{Z}[A, B][X] \) with \( \deg h < \frac{4n^2+4n-12}{2} \) can be observed.

Recalling the correspondence \( Y^2 = X^3 + AX + B \) in the setting of an elliptic curve over a field described by a non-generalized Weierstrass equation with coefficients \( A \) and \( B \) shows
\[
Y^4 = (Y^2)^2 = (X^3 + AX + B)^2 = X^6 + k(X)
\]
for an appropriate polynomial \( k \) in \( \mathbb{Z}[A, B][X] \) with \( \deg k < 6 \).

Hence
\[
\psi_{n-1}(X, Y)\psi_{n+1}^3(X, Y) = (4.21)
\]
\[
= Y^4((n^4 + 2n^3 - 2n - 1)X^{\frac{4n^2+4n-12}{2}} + h(X))
\]
\[
= (4.22)
\]
\[
= (n^4 + 2n^3 - 2n - 1)(X^{\frac{4n^2+4n}{2}} + X^{\frac{4n^2+4n-12}{2}}k(X)) + (X^6 + k(X))h(X)
\]
\[
= (4.23)
\]
\[
(n^4 + 2n^3 - 2n - 1)X^{\frac{(2n+1)^2-1}{2}} + h(X)
\]
for an appropriate \( h \) in \( \mathbb{Z}[A,B][X] \) with \( \deg h < \frac{(2n+1)^2-1}{2} \).

Altogether

\[
\psi_{m+1}(X,Y) := \psi_{n+2}(X,Y)\psi_n^3(X,Y) - \psi_{n-1}(X,Y)\psi_{n+1}(X,Y)
\]

\[
\leq (n^4 + 2n^3)X\frac{(2n+1)^2-1}{2} + l(X) - ((n^4 + 2n^3 - 2n - 1)X\frac{(2n+1)^2-1}{2} + h(X))
\]

\[
= (2n + 1)X\frac{(2n+1)^2-1}{2} + g(X)
\]

\[
\leq 2n = m + 1)X\frac{m^2-1}{2} + g(X)
\]

with \( g \) being an appropriate polynomial in \( \mathbb{Z}[A,B][X] \) of a degree lower than \( \frac{(m+1)^2-1}{2} \) was proven.

The other subcase for an even \( m \) can be shown analogously.

Moreover the case for an odd \( m \) can be proven alike.

Altogether the structural behavior of \( \psi_m \) was proven for any \( m \in \mathbb{N} \) and can now be used to derive the structural behavior of \( \psi_m^2 \) and \( \phi_m \) for an arbitrary but fixed \( m \in \mathbb{N} \).

The just proven structure of \( \psi_m \) immediately yields

\[
\psi_m^2 = \begin{cases} 
Y^2(m^2X^{m^2-4} + \text{(lower degree terms)}), & \text{if } m \text{ is even} \\
m^2(X^{m^2-1} + \text{(lower degree terms)}), & \text{if } m \text{ is odd} 
\end{cases}
\]

Since the setting of an elliptic curve is assumed, \( Y^2 \) can be substituted by \( X^3 + AX + B \), which shows

\[
\psi_m^2 = m^2X^{m^2-1} + \text{(lower degree terms)}.
\]

Furthermore definition 4.15 yields

\[
\phi_m = X\psi_m^2 - \psi_{m+1}\psi_{m-1}.
\]

Together with the just proven structures of the polynomials in the family \( \{\psi_m\}_{m \in \mathbb{N}_0} \), the structural behavior

\[
\phi_m = X^{m^2} + \text{(lower degree terms)}
\]

can finally be observed.

Still being in the setting of an elliptic curve, these families can be used to find rational functions representing the multiplication by a fixed integer over an elliptic curve.

**Proposition 4.18.** Let \( E \) be an elliptic curve over a field \( K \) with \( \text{char}(K) \neq 2 \) represented by \( Y^2 = X^3 + AX + B \) for fixed \( A \) and \( B \) in \( K \). Furthermore let \( m \in \mathbb{N} \) and \( (x,y) \in E\setminus\{\infty\} \) be given. Then the multiplication of \( (x,y) \) by the integer \( m \) on \( E \) is representable by

\[
*(x,y) = \left( \frac{\phi_m(x)}{\psi_m^2(x)}, \frac{\omega_m(x,y)}{\psi_m^2(x)} \right)
\]

in the case of simultaneously well-defined rational functions in \( (x,y) \).

**Proof.** [19][Subsection 9.5, Theorem 9.31, pp.288f]

From the just stated proposition 4.18 it is obvious that the multiplication by a fixed integer over an elliptic curve can be represented by a pair of rational functions. Moreover according to remark 3.29 \( *_m \) is well-defined.

In order to prove the homomorphic property of the multiplication by a fixed integer, two elements \( P \) and \( Q \) in the elliptic curve \( E \) need to be considered according to remark 4.2. Moreover let \( m \) be a fixed integer by which shall be multiplied.

Firstly \( m \geq 0 \) will be assumed. Hence

\[
m(P + Q) = (P + Q + \ldots + (P + Q)) = (P + \ldots + P) + (Q + \ldots + Q) = mP + mQ
\]

whereas for the second equation commutativity and associativity for the addition on elliptic curves was used.
Secondly the case of $m < 0$ can be proven analogously.

All in all it was shown that the multiplication by a fixed integer over an elliptic curve can be understood as an endomorphism of that elliptic curve.

**Corollary 4.19.** Let $E$ be an elliptic curve over a field $K$ and $m \in \mathbb{Z}$. Then the endomorphism $*_m$ of $E$ has degree $m^2$.

**Proof.** Firstly recalling proposition 4.18 yields that the multiplication by an integer $m$ is an endomorphism of $E$ representable as $*_m(x, y) := m(x, y) = \left( \frac{\phi_m(x)}{\psi_m(x)}, \frac{\psi_m(x)}{\psi_m(x)} \right)$ for any element $(x, y) \neq \infty$ in $E$ in which both rational functions are defined simultaneously.

Furthermore let $Y^2 = X^3 + AX + B$ be the non-generalized Weierstrass equation representing $E$ over $K$ for fixed coefficients $A$ and $B$ in $K$.

In order to determine the degree of $*_m$ a standardized representation of $*_m$ needs to be found.

Claim $\phi_m$ and $\psi_m^2$ do not share a common root.

For a contradiction it will be assumed that there exists a common root of $\phi_m$ and $\psi_m^2$. Furthermore $m_0$ is set to be the smallest positive integer existing such that $\phi_{m_0}$ and $\psi_{m_0}^2$ share a common root.

First off $m_0$ is assumed to be even. So it exists a positive integer $n$ such that $m_0 = 2n$.

An easy calculation yields

$$\phi_2(X) = X\psi_2^2(X) - \psi_3(X, Y)\psi_1(X, Y)$$

$$= X(4Y^2) - (3X^4 + 6AX^2 + 12BX - A^2) = 0.$$ (4.24)

Moreover

$$\psi_2^2(x) = 4y^2 = 4x^3 + 4Ax + 4B.$$ (4.25)

Therefore $*_m$ can be rewritten into

$$*_m(X, Y) := m_0(X, Y) \quad m_0 = 2n \quad 2(n(X, Y)) = \frac{\phi_n(X)}{\psi_n^2(X)} \cdot \frac{\omega_n(X)}{\psi_n^3(X)} = \left( \frac{\phi_2 \left( \frac{\phi_n(X)}{\psi_n^2(X)} \right)}{\psi_2 \left( \frac{\phi_n(X)}{\psi_n^2(X)} \right)}, \frac{\omega_2 \left( \frac{\phi_n(X)}{\psi_n^2(X)} \right)}{\psi_2 \left( \frac{\phi_n(X)}{\psi_n^2(X)} \right)} \right).$$

Furthermore

$$*_m(X, Y) = \left( \frac{\phi_m(X)}{\psi_m^2(X)}, \frac{\omega_m(X, Y)}{\psi_m^3(X)} \right) = \left( \frac{\phi_{2n}(X)}{\psi_{2n}(X)}, \frac{\omega_{2n}(X, Y)}{\psi_{2n}^3(X)} \right).$$

according to proposition 4.18. Comparing the first components of both representations of $*_m$ yields

$$\phi_{2n}(X) = \frac{\phi_2 \left( \frac{\phi_n(X)}{\psi_n^2(X)} \right)}{\psi_2 \left( \frac{\phi_n(X)}{\psi_n^2(X)} \right)}$$

$$= \frac{\phi_2 \left( \frac{\phi_n(X)}{\psi_n^2(X)} \right)}{\psi_2 \left( \frac{\phi_n(X)}{\psi_n^2(X)} \right)} = \frac{\phi_n(X)}{\psi_n^2(X)}.$$ (4.26)

From now $N$ will denote the numerator and $D$ the denominator of this fraction i.e.

$$N := \phi_n^4(X) - 2A\phi_n^2(X)\psi_n^4(X) - 8B\psi_n^6(X) + A^2\psi_n^8(X).$$
and
\[ D := (4\psi_n^2(X))(\phi_n(X) + A\phi_n(X)\psi_n^4(X) + B\psi_n^6(X)). \]

Moreover
\[
\Delta := 4A^3 + 27B^2 \\
f_1(X, Z) := 12X^2Z + 16AZ^3 \\
f_2(X, Z) := 4\Delta X^3 - 4A^2BX^2Z + 4A(3A^3 + 22B^2)XZ^2 + 12B(A^3 + 8B^2)Z^3 \\
g_1(X, Z) := 3X^3 - 5AXZ^2 - 27BZ^3 \\
g_2(X, zZ) := A^2BX^3 + A(5A^3 + 32B^2)XZ^2 + 2B(13A^3 + 96B^2)XZ^2 - 3A^2(A^3 + 8B^2)Z^3 \\
F(X, Z) := X^4 - 2AX^2Z^2 - 8BZ^3 + A^2Z^4 \\
G(X, Z) := 4Z(3X^3 + AXZ^2 + BZ^3)
\]

are defined.

A straightforward, yet lengthy calculation as done in [19][Subsection 3.2, Lemma 3.8, pp.80] proves
\[ F(X, Z)f_1(X, Z) - G(X, Z)g_1(X, Z) = 4\Delta Z^7 \]
and
\[ F(X, Z)f_2(X, Z) + G(X, Z)g_2(X, Z) = 4\Delta X^7. \]

Setting the $X$-component of the equation as $\psi_n(X)$ and the $Z$-component as $\psi_n^2(X)$ hence proves
\[ Nf_1(\phi_n(X), \psi_n^2(X)) - Dg_1(\phi_n(X), \psi_n^2(X)) = 2\psi_n^{14}(X)\Delta \quad (4.27) \]
and
\[ Nf_2(\phi_n(X), \psi_n^2(X)) + Gg_2(\phi_n(X), \psi_n^2(X)) = 4\phi_n^7(X)\Delta. \quad (4.28) \]

Now it is moreover assumed that a common root of $N$ and $D$ exists.

Therefore according to (4.27) and (4.28) it exists a common root of $\psi_n^2$ and $\phi_n$. This however immediately contradicts the choice of $m_0$ being chosen as the smallest positive integer such that $\phi_{m_0}$ and $\psi_{m_0}^2$ share a common root, as $m_0$ is obviously greater than the positive integer $n$.

Altogether $N$ and $D$ cannot share a common root.

Moreover since $\frac{\phi_{2n}}{\psi_{2n}^2} = \frac{N}{D}$ was observed, it is hence obvious that $\phi_{2n}$ is a multiple of $N$ and $\psi_{2n}^2$ is a multiple of $D$.

Furthermore remark 4.17 yields $X^{(2n)^2} = X^{4n^2}$ being the leading term of both $N$ and $\phi_{2n}$. Hence $N = \phi_{2n}$ needs to hold and $D = \psi_{2n}^2$ immediately follows.

Finally recalling $N$ and $D$ not sharing a common root lastly proves $\phi_{2n} = \phi_{m_0}$ and $\psi_{2n}^2 = \psi_{m_0}^2$ not sharing a common root.

This contradicts the choice of $m_0$.

Altogether the case for an even $m_0$ led to a contradiction and therefore cannot have been true.

Now $m_0$ is assumed to be odd. So there exists a non-negative integer $n$ such that $m_0 = 2n + 1$.

Again for a contradiction it is assumed that there exists a common root $r$ of $\phi_{m_0}$ and $\psi_{m_0}^2$. Therefore
\[ 0 = \phi_{m_0}(r) = X\psi_{m_0}^2(r) - \psi_{m_0-1}(r)\psi_{m_0-1}(r) = \psi_{m_0-1}(r)\psi_{m_0+1}(r) \]
is known. Hence either
\[ \psi_{m_0-1}(r) = 0 \]
or
\[ \psi_{m_0+1}(r) = 0. \]

Therefore the smallest $k \in \{1, -1\}$ can be chosen such that
\[ \psi_{m_0+k}(r) = 0. \]

Recalling remark 4.14 it is known that for any odd integer $s$ over the setting of an elliptic curve, $\psi_s$ can be understood as a polynomial in $\mathbb{Z}[A, B][X]$ and so $\psi_{m_0}$ and $\psi_{m_0+2k}$ are obviously polynomials in $\mathbb{Z}[A, B][X]$. 

34
Again using the property of $r$ being a root of $\psi_{m_0}^2$ yields
\[ 0 = \psi_{m_0}^2(r) \psi_{m_0+2k}^2(r) = (\psi_{m_0}(r)\psi_{m_0+2k}(r))^2 \]
and therefore
\[ \psi_{m_0}(r)\psi_{m_0+2k}(r) = 0. \] (4.29)

Hence
\[ \phi_{m_0+k}(r) = (X\psi_{m_0+k}^2 - \psi_{m_0}\psi_{m_0+2k})(r) = r \psi_{m_0+k}^2(r) - \psi_{m_0}(r)\psi_{m_0+2k}(r) = 0 \]
was proven.

Altogether $r$ is a common root of $\phi_{m_0+k}$ and $\psi_{m_0+k}^2$.

Now let $n_0$ be the unique integer such that $2n_0 = m_0 + k$ so $n_0 = \frac{m_0 + k}{2}$. Since $\phi_{m_0}$ and $\psi_{m_0}$ share the common root $r$ and $n_0$ was chosen as the smallest positive integer such that $\phi_{m_0}$ and $\psi_{m_0}^2$ share a common root, $\frac{m_0 + k}{2} = n_0 \geq m_0$ needs to be given. Hence $m_0 = 1$ holds.

Therefore
\[ \phi_{m_0} = \phi_1 := X \]
and
\[ \psi_{m_0}^2 \psi_1^2 := 1 \]
share a common root which is obviously impossible.

All in all $\phi_{m_0}$ and $\psi_{m_0}^2$ not sharing a common root was also proven for the odd case of $m_0$.

Summing up it was proven that proposition 4.18 especially yields a standardized representation for $*_m$ and so definition 4.6 yields
\[ \deg(*_m) = \max\{\deg\phi_m, \deg\psi_m^2\} = \max\{m^2, m^2 - 1\} = m^2. \]

To put it all in a nutshell, this chapter aimed to find a representation of rational functions for the multiplication by a fixed integer over an elliptic curve. In order to do that, division polynomials and two other families of polynomials were firstly introduced and their main properties were examined. Having understood these polynomials and their properties, appropriate representing rational functions were found. Moreover it was proven that the found representation of rational functions is a standardized representation and so the degree of the multiplication by a fixed integer was determined.

### 4.3. The Frobenius map of elliptic curves.

In subsection 4.1 the Frobenius map of an elliptic curve over a finite field was introduced. Moreover it was pointed out, how this map can be understood as an endomorphism of an elliptic curve. The Frobenius map of an elliptic curve over a finite field is essential for chapter 6. Hence it is indispensable to observe this map in more detail and to prove some essential properties.

Starting from scratch, the definition of the Frobenius map over a finite field will be firstly recalled.

**Definition 4.20.** Let $q$ be a power of a prime $p$, then the map
\[ \phi_q: \mathbb{F}_q \rightarrow \mathbb{F}_q \text{ with } \phi_q(x) := x^q \]
is called the **Frobenius map over** $\mathbb{F}_q$.

The idea of the Frobenius map over a finite field can be adapted to the case of elliptic curves. From now on, when talking of the Frobenius map, the Frobenius map of an elliptic curve over a finite field will be meant, if not said otherwise.

**Definition 4.21.** Let $q$ be the power of a prime $p$ and $E$ be an elliptic curve over the finite field $\mathbb{F}_q$. Then the map
\[ \phi_q: E \times E \rightarrow E \text{ with } \phi_q(x, y) := \begin{cases} (x^q, y^q), & \text{if } (x, y) \neq \infty \\ \infty, & \text{if } (x, y) = \infty \end{cases} \]
is called the **Frobenius map of** $E$ over $\mathbb{F}_q$.

**Remark 4.22.** The Frobenius map of $E$ over $\mathbb{F}_q$ is well-defined according to example 4.5.
Remark 4.23. For any \((x, y)\) in \(E \setminus \{\infty\}\) it holds
\[(x, y) \in E(\mathbb{F}_q)\) if and only if \(\phi_q(x, y) = (x, y)\).

Proof. It is obvious that for any \((x, y)\) in \(E \setminus \{\infty\}\)
\[(x, y) \in E(\mathbb{F}_q)\) if and only if \(x\) and \(y\) are elements in \(\mathbb{F}_q\).
Furthermore \(x\) and \(y\) are elements in \(\mathbb{F}_q\) if and only if \(x = x^q = \phi_q(x)\) and \(y = y^q = \phi_q(y)\).
Altogether \((x, y) \in E \setminus \{\infty\}\) is an element in \(E(\mathbb{F}_q)\) if and only if \(\phi_q(x, y) := (x^q, y^q) = (x, y)\). □

Recalling subsection 4.1, it is important to examine whether the Frobenius map belongs to the class of separable endomorphism or not. Furthermore it is important to determine the degree of the Frobenius map as an endomorphism.

Proposition 4.24. Let \(q\) be the power of a prime \(p \not\equiv \{2, 3\}\) and \(E\) be an elliptic curve over \(\mathbb{F}_q\). Furthermore let \(\phi_q\) be the Frobenius map of \(E\) over \(\mathbb{F}_q\), then \(\phi_q\) is an inseparable endomorphism of degree \(q\).

Proof. The well-defined Frobenius map of \(E\) over \(\mathbb{F}_q\) is obviously representable as two (rational) functions which are defined in at least one point \((x, y)\) in \(E\) simultaneously according to definition 4.21. Therefore only the homomorphic property needs to be examined.

Let \(P := (x, y)\) be an arbitrary but fixed element in \(E \setminus \{\infty\}\) over \(\mathbb{F}_q\) with \(y \neq 0\). More precisely let the elliptic curve \(E\) be defined by the non-generalized Weierstrass equation \(Y^2 = X^3 + AX + B\) for fixed coefficients \(A\) and \(B\) in \(\mathbb{F}_q\). Hence
\[
\phi_q(P + P) = \phi_q(2P) = \phi_q(m^2 - 2x, m(x - (m^2 - 2x))) - y)
\]
with \(m := (3x^2 + A)(2y)^{-1}\) according to the rules of addition of definition 3.22. Now evaluating using the Frobenius map yields
\[
\phi_q(m^2 - 2x, m(x - (m^2 - 2x))) - y)
= ((m^2 - 2x)^q, (m(x - (m^2 - 2x))) - y)^q)
= ((m^2)^q - 2^qx^q, m^q(x^q - ((m^2)^2 - 2^qx^q)) - y^q)
= ((m^2)^q - 2^qx^q, m^2(x^q - ((m^2)^2 - 2^qx^q)) - y^q),
\]
where it was used that the characteristic of the underlying field divides \(q\) as well as 2 and 3 being elements in \(\mathbb{F}_q\) since \(p \not\equiv \{2, 3\}\).

Analogously
\[
m^q := ((3x^2 + A)(2y)^{-1})^q = (3^q(x^q)^2 + A^q)(2^qy^q)^{-1}
\]
because of 2, 3 and \(A\) being elements in \(\mathbb{F}_q\) since \(p \not\equiv \{2, 3\}\).

This observation together with definition 3.22 yields
\[
((m^2)^q - 2^qx^q, m^q(x^q - ((m^2)^2 - 2^qx^q)) - y^q) = 2(x^q, y^q) = 2\phi_q(x, y) = \phi_q(x, y) + \phi_q(x, y).
\]
All other cases can be proven analogously.

Hence it was proven that the Frobenius map is indeed an endomorphism of \(E\) over \(\mathbb{F}_q\).
Observe the degree of the Frobenius map of \(E\) over \(\mathbb{F}_q\) definition 4.21 needs to be recalled which obviously yields a standardized representation given by \(\phi_q(X, Y) = (X^q, Y^q)\). Both representing polynomials are of degree \(q\) hence
\[
\deg \phi_q = q
\]
holds trivially.
In terms of inseparability the derivative of \(X^q\) is given by
\[
(X^q)' = qX^{q-1} \equiv 0
\]
which is constantly equal zero, since \(q = 0\) in \(\mathbb{F}_q \subseteq \mathbb{F}_q\). Thus \(\phi_q\) is inseparable according to definition 4.9. □

It was just shown that the Frobenius map of an elliptic curve over a finite field is inseparable. Nevertheless, this map can be used to derive an important separable endomorphism.
Proposition 4.25. Let \( q \) be the power of a prime \( p \not\in \{2,3\} \) and \( E \) be an elliptic curve over \( \mathbb{F}_q \). Furthermore let \( \phi_q \) be the Frobenius map of \( E \) over \( \mathbb{F}_q \) and \( n \in \mathbb{N} \), then
\[
\ker(\phi_q^n - \text{id}) = E(\mathbb{F}_q^n)
\]
and \( \phi_q^n - \text{id} \) is a separable endomorphism of \( \deg(\phi_q^n - \text{id}) = \#E(\mathbb{F}_q^n) \).

Proof. Obviously \( \phi_q^n - \text{id} \) as a linear composition of endomorphisms is an endomorphism itself. So firstly \( \ker(\phi_q^n - \text{id}) = E(\mathbb{F}_q^n) \) needs to be proven.

Therefore let \((x, y)\) be an arbitrary but fixed element in the kernel of \( \phi_q^n - \text{id} \). So
\[
\infty = (\phi_q^n - \text{id})(x, y) = \phi_q^n(x, y) - (x, y)
\]
which is equivalent to \( \phi_q^n(x, y) = (x, y) \). Moreover an easy calculation shows \( \phi_q^n(x, y) = \phi_q^n(x, y) \).

Altogether
\[
\phi_q^n(x, y) = (x, y).
\]

According to remark 4.23 this holds if and only if \((x, y)\) is in \( E(\mathbb{F}_q^n) \). Due to the equivalence of all statements
\[
\ker(\phi_q^n - \text{id}) = E(\mathbb{F}_q^n)
\]
was proven.

Proving \( \phi_q^n - \text{id} \) being a separable endomorphism is rather technical and can be found in detail in [19][Subsection 2.8, Proposition 2.28, pp.54].

Finally knowing \( \phi_q^n - \text{id} \) being a non-trivial separable endomorphism proposition 4.11 can be used which yields
\[
\deg(\phi_q^n - \text{id}) = \# \ker(\phi_q^n - \text{id}) = \#E(\mathbb{F}_q^n).
\]

In order to secure a high safety level for elliptic curve crypto-systems it is very important to be able to determine the cardinal number of an elliptic curve \( E(K) \) restricted on a field \( K \). Therefore the next theorem yields a way of determining the cardinal number of an elliptic curve restricted on a finite field, using the Frobenius map. This idea will be examined and explained in more detail in chapter 6 and chapter 7.

Theorem 4.26. Let \( q \) be the power of a prime \( p \not\in \{2,3\} \) and let \( E \) be an elliptic curve over \( \mathbb{F}_q \). Moreover set \( a := q + 1 - \#E(\mathbb{F}_q) \), then
\[
\phi_q^2 - a\phi_q + q \equiv 0
\]
holds in the manner of endomorphisms of \( E \).

Furthermore the integer \( a \) is uniquely defined by this property i.e. for any integer \( k \) with \( \phi_q^k - k\phi_q + q \equiv 0 \) it immediately holds \( a = k \).

Proof. [19][Subsection 4.2, Proposition 4.10, pp.95f]

Remark 4.27. Evaluating the endomorphism of theorem 4.26 in elements of a considered elliptic curve, \( (x^2, y^2) - a(x, y) + q(x, y) = \infty \) is known for any \((x, y)\) in \( E \setminus \{\infty\}\).

Especially \( a \) is the unique integer for which this equation holds for all elements in \( E \) simultaneously.

The just stated theorem 4.26 is very important for a later in paragraph 8.2.4 introduced algorithm called the MOV-Attack. Furthermore this theorem can be used to define a special class of elliptic curves.

Definition 4.28. Let \( q \) be a power of a prime \( p \not\in \{2,3\} \) and \( E \) be an elliptic curve over \( \mathbb{F}_q \), then according to theorem 4.26 there exists an unique integer \( a \) such that \( \#E(\mathbb{F}_q) = q + 1 - a \). Furthermore if \( a = 0 \mod p \), then the elliptic curve \( E \) is called supersingular.

All in all this chapter carefully observed the Frobenius map of elliptic curves over finite fields. Then it was pointed out how the inseparable Frobenius map induces an important separable endomorphism. This endomorphism was used to observe a correspondence between the endomorphism’s degree and the cardinal number of an elliptic curve restricted on a finite field. This correspondence will be useful chapter 8 in order to determine the level of security for a considered elliptic curve crypto-system.
5. TORSION POINTS

Just as chapter 4 did before, this chapter aims to adapt a well known algebraic concept - the one of torsion elements - to the case of elliptic curves.

First of subsection 5.1 will define the subset of $n$-torsion points for a $n \in \mathbb{N}$ in an elliptic curve. Then it will be proven that this subset endowed with the addition $+$ of an elliptic curve, especially forms a subgroup of that elliptic curve. Hence the structural behavior of this group will be examined in more detail whereas the structure theorem for abelian groups will be used as well as the knowledge of the multiplication by a fixed integer being an endomorphism according to the previous chapter. Lastly the concept of a basis for this subgroup will be introduced.

Secondly subsection 5.2 will firstly recall the definition of (primitiv) $n^{th}$ roots of unity for a $n \in \mathbb{N}$ as well as some basic properties of such elements. Then a pairing will be introduced which maps $n$-torsion points into the group of $n^{th}$ roots of unity having six important properties. Such a pairing helps to prove many important properties of $n$-torsion points and endomorphisms by simply evaluating elements with such a paring and using the broad knowledge of the properties of the group of $n^{th}$ roots of unity. Various properties will therefore be proven using this strategy at the end of subsection 5.2. All in all such a pairing will be very important in the application of elliptic curves in cryptography in paragraph 8.2.4.

5.1. The group of $n$-torsion points of an elliptic curve.

All observations made so far can be used to introduce an important subgroup of an elliptic curve. This subgroup translates the commonly known algebraic concept of torsion points into the language of elliptic curves. Interestingly an isomorphic correspondence between this group and well known cyclic groups over $\mathbb{Z}$ can be observed. Therefore many properties of this group can be derived by this isomorphic correspondence.

The group itself will be very important in the next chapter as well as for the application of elliptic curves in cryptography in the second part of this thesis.

**Definition 5.1.** Let $E$ be an elliptic curve over a field $K$ and $n \in \mathbb{N}$, then the set

$$E[n] := \{ P \in E \mid nP = \infty \}$$

is called the set of $n$-torsion points in $E$.

**Remark 5.2.** Obviously $\infty$ is a $n$-torsion point for any integer $n$.

Furthermore if $P$ is a $n$-torsion point for a fixed integer $n$, then any multiple of $P$ is a $n$-torsion point as well.

**Proof.** Let $Q$ be a $n$-torsion point in an elliptic curve $E$ over a field $K$ for a fixed integer $n$. Furthermore let $k$ be an arbitrary but fixed integer. Then

$$n(kQ) = (nk)Q = (kn)Q = k(nQ) = k\infty = \infty$$

proves $kQ \in E[n]$.

It is important to observe that the set of $n$-torsion points in $E$ is not just an arbitrary set.

**Proposition 5.3.** Let $E$ be an elliptic curve over a field $K$ and $n \in \mathbb{N}$, then $E[n]$ is a subgroup of $E$.

**Proof.** According to definition 5.1 the set of $n$-torsion points in $E$ is obviously a subset of $E$, which according to remark 5.2 includes the neutral element $\infty$ of the abelian group $(E, +, \infty)$. So especially $E[n]$ is not the empty set.

Hence it remains to show that $E[n]$ is closed under addition.

Therefore, let $P$ and $Q$ be arbitrary but fixed $n$-torsion points in $E$. Obviously

$$n(P + Q) = nP + nQ = \infty + \infty = \infty,$$
due to the homomorphic property of the endomorphism $*_n$. Hence $P + Q$ is also a $n$-torsion point in $E$. Moreover, since $P$ and $Q$ have been chosen arbitrarily, this concludes the proof.

Hence from now on $E[n]$ will be referred to as the group of $n$-torsion points in $E$.

In order to understand $n$-torsion points better, an example needs to be observed.

**Example 5.4.** In this example the elliptic curve $E$ over the finite field $\mathbb{F}_5$ defined by the non-generalized Weierstrass equation $Y^2 = X^3 + X + 1 \mod 5$ will be considered. The aim of this example is to determine a non-trivial 4-torsion point in $E$. Therefore the point $P := (3,1)$ in $E(\mathbb{F}_5) \subseteq E$ will be considered.

Since $1 \neq 0 \mod 5$ the third case of the rules of addition needs to be applied in order to determine $2P$ which yields $S := 2P = (0, 1)$. Furthermore $4P$ needs to be determined in order to be able to decide, whether $P$ is a 4-torsion point or not. This can be done using the correspondence $4P = 2P + 2P = S + S$. Again the third case of the rules of addition needs to be applied when wanting to determine $S + S$. This finally shows $4P = S + S = (0, 1) + (0, 1) = \infty$. Altogether $P \in E[4]$ was proven.

Since the group of $n$-torsion points is essential for later in subsection 5.2 introducing a map called Weil-Pairing, further properties of this group need to be observed.

Fortunately it can be proven that the group of $n$-torsion points is isomorphic to a direct sum of two well understood cyclic groups over $\mathbb{Z}$. In order to prove this isomorphic correspondence the structure theorem for abelian groups firstly needs to be recalled.

**Theorem 5.5. Structure theorem for abelian groups**

Let $M$ be a finitely generated abelian group, then there exist unique $d$ and $s$ in $\mathbb{N}_0$, unique pairwise distinct prime numbers $p_1, \ldots, p_s$ and furthermore for any $i \in \{1, \ldots, s\}$ there exists a unique $t_i \in \mathbb{N}$, so that there exist unique $\nu_i t_i \geq \ldots \geq \nu_1 t_1 \geq 1$ such that altogether

$$M \cong \mathbb{Z}^d \bigoplus_{i=1}^s \mathbb{Z}/(p_i^{\nu_i} t_i).$$

Having recalled this important theorem a structural behavior of $n$-torsion groups can be proven.

**Theorem 5.6.** Let $E$ be an elliptic curve over a field $K$ with $\text{char}(K) \neq 2$ and $n \in \mathbb{N}$. If $\text{char}(K)$ does not divide $n$ or if $\text{char}(K) = 0$, then

$$E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

Else if $\text{char}(K) =: p > 0$ and $p$ divides $n$ with $n = p^r n'$ for an appropriate positive integer $r$ and an appropriate $n' \in \mathbb{N}$ such that $p$ does not divide $n'$, then either

$$E[n] \cong \mathbb{Z}_{p^r} \oplus \mathbb{Z}_{n'},$$

or

$$E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_{n'}.$$

**Proof.** Let $E$ be an elliptic curve over a field $K$ with $\text{char}(K) \neq 2$ and $n \in \mathbb{N}$. Firstly the case of $\text{char}(K) \nmid n$ or $\text{char}(K) = 0$ will be considered.

First off proposition 4.18 yields the multiplication $*_n$ being representable as $*_n = (\phi_n, \psi_n, \phi_n \psi_n)$.

Furthermore remark 4.17 proves the structural behaviors $\phi_n(X) = X^{n^2} + (\text{lower degree terms})$ and $\psi_n(X) = n^2 X^{n^2 - 1} + (\text{lower degree terms})$.

Setting $R(X) := \frac{2n(X)}{2X^2} - \frac{X}{2}$ as the rational function describing the $X$-coordinate of $*_n$, the polynomial $N$ representing the numerator of the derivative $R'$ can be easily determined. According to the just made observations $N$ is obviously given by

$$N(X) = n^2 X^{2n^2 - 2} - n^4 X^{2n^2 - 2} + n^2 X^{2n^2 - 2} + l(X) = n^2 X^{2n^2 - 2} + l(X)$$

whereas $l$ is a polynomial in $\mathbb{Z}[A, B][X]$ with $\deg l < 2n^2 - 2$.

Obviously $n^2 X^{2n^2 - 2} \neq 0$ over $K$ since either $\text{char}(K) \nmid n$ or $\text{char}(K) = 0$. Thence the numerator $N$ of the derivative of $R'$ is not the zero polynomial. Especially this proves $R'$ not being identically zero. Therefore according to definition 4.9 $*_n$ is separable.

Furthermore proposition 4.11 can be applied to the non-trivial separable endomorphism $*_n$ which yields

$$\deg(*_n) = \# \ker(*_n) = \# E[n].$$
Moreover corollary 4.19 states  
\[ \deg(\ast_n) = n^2. \]

Altogether  
\[ \#E[n] = n^2 \quad \text{(5.1)} \]

was proven.

Recalling the structure theorem for abelian groups  
\[ E[n] \simeq \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k} \quad \text{(5.2)} \]

holds for an appropriate positive integer \( k \) and \( n_1, \ldots, n_k \in \mathbb{N} \) such that for all \( i \in \{1, \ldots, k\} \) \( n_i \) divides \( n_{i+1} \).

Now let \( p \) be a prime dividing \( n_1 \) then for all \( i \in \{1, \ldots, k\} \) \( p \) does immediately divide \( n_i \). Therefore, according to (5.2) and \( E[p] \subseteq E[n] \)

\[ \#E[p] = p^k \quad \text{(5.3)} \]

is known.

Altogether (5.1) and (5.3) yields \( k = 2 \) and so

\[ E[n] \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}. \quad \text{(5.4)} \]

According to the structure theorem for abelian groups it is furthermore given that \( n_1 \) divides \( n_2 \) and \( n_2 \) divides \( n \). Together with

\[ n^2 = \#E[n] = n_1 n_2 \quad \text{(5.1)} \]

this proves

\[ n_1 = n = n_2. \]

So

\[ E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n \]

can be concluded.

Secondly the case for \( \text{char}(K) \) dividing \( n \) will be considered. Therefore starting off \( p := \text{char}(K) \) is set.

Now \( \ast_p \) being an inseparable endomorphism can be proven. A proof of this claim can be found in [19][Subsection 2.8, Proposition 2.27, pp.54].

Hence together with remark 4.12 and corollary 4.19 this proves

\[ \#E[p] = \#\ker(\ast_p) < \deg(\ast_p) = p^2. \quad \text{(5.5)} \]

Now an arbitrary but fixed \( P \in E[p] \) has to be considered.

Let \( k_P \) denote the smallest positive integer such that \( k_P P = 1 \). So \( k_P \) divides the prime \( p \). So \( k_P \in \{1, p\} \) needs to be given.

Furthermore \( P \) was chosen arbitrarily and so \( k_P \in \{1, p\} \) holds for all \( P \in E[p] \). Thence

\[ \#E[p] = p^k \]

for an appropriate \( k \in \mathbb{N}_0 \). Moreover recalling (5.5) finally shows \( k \in \{0, 1\} \).

First off \( k = 0 \) will be assumed. It can be shown by induction over \( \mathbb{N} \) that for all \( m \in \mathbb{N} \)

\[ E[p^m] = \{\infty\}. \quad \text{(5.6)} \]

**Start of induction for \( m = 1 \)** It holds \( \#E[p^m] = \#E[p] = \#E[p^k] = p^k \quad \text{(5.3)} \)

Moreover according to remark 5.2 \( \infty \) is known to be an element of every torsion group, so altogether \( E[p^m] = \{\infty\} \).

**Claim of induction** For all \( s \in \mathbb{N} \leq m \) it holds \( E[p^s] = \{\infty\} \).

**Step of induction** \( m \mapsto m + 1 \) According to remark 5.2 \( E[p^{m+1}] \) is a non-empty set. Hence an arbitrary, but fixed \( P \in E[p^{m+1}] \) can be chosen. Together with definition 5.1 this yields

\[ p \ast (p^m P) = p^{m+1} P = \infty. \]

Thence \( p^m P \) is an element in \( E[p] \).

41
Therefore the claim of induction can be applied to \( p^m P \in E[p] \) showing
\[
p^m P = \infty.
\]
This is equivalent to \( P \in E[p^m] \).

Hence the claim of induction can also be applied to \( P \in E[p^m] \) proving
\[
P = \infty.
\]

Recalling \( P \) being chosen arbitrarily in \( E[p^{m+1}] \) concludes the induction.

Altogether it was just shown that for all positive integers \( m \), \( E[p^m] = \{ \infty \} \). Therefore the isomorphic correspondence between trivial abelian groups holds in the case of \( k = 0 \). Thus for all \( m \in \mathbb{N} \)
\[
E[p^m] = \{ \infty \} \simeq \{ z \}.
\]

Furthermore the case of \( k = 1 \) needs to be observed. Just like in the case of \( k = 0 \), an isomorphic correspondence given by
\[
E[p^m] \simeq \mathbb{Z}_{p^m}
\]
can be proven by induction over \( m \in \mathbb{N} \).

Firstly \( E[p^m] \) being a finite cyclic group is obvious. However, the cardinality of \( E[p^m] \) being equal \( p^m \) and not being equal to a smaller power of the prime \( p \) is not as obvious. Therefore it will be proven by induction over \( m \in \mathbb{N} \) that it exists an element \( P \in E[p^m] \) such that the smallest positive integer \( k_P \) with \( k_PP = \infty \) is equal \( p^m \). Then
\[
E[p^m] \simeq \mathbb{Z}_{p^m} \tag{5.7}
\]
needs to hold immediately.

**Start of induction for \( m = 1 \)** It holds \( E[p^m] = E[p] \simeq \mathbb{Z}_p = \mathbb{Z}_{p^m} \) due to \( \#E[p] = \#E[p^m] = p^m = p \) and \( p \) being prime.

**Claim of induction** For all \( s \in \mathbb{N}_{\leq m} \) it holds \( E[p^s] \simeq \mathbb{Z}_{p^s} \).

Step of induction \( m \mapsto m + 1 \) Firstly the claim of induction yields the existence of a \( P \in E[p^m] \) such that the smallest positive integer \( k_P \) with \( k_PP = \infty \) is equal \( p^m \). Furthermore the multiplication \( *_p \) is obviously surjective over \( E \), due to \( E \) being defined over the algebraic closure \( K \) of \( K \). Therefore especially a \( Q \) in \( E \) exists such that
\[
P = *_p(Q) = pQ \tag{5.8}
\]
Hence \( \infty = p^mP = p^m * (pQ) = p^{m+1}Q \) can be observed, which proves \( Q \in E[p^{m+1}] \).

Since (5.8) holds and \( k_P = p^m \) was observed, \( Q \) cannot be the neutral element \( \infty \). Furthermore for any arbitrary \( l \in \{ 1, \ldots, m \} \) the inequality
\[
\infty \neq p^{l-1}P = p^{l-1} * (pQ) = p^lQ \tag{5.8}
\]
needs to be true, due to the choice of \( P \).

To put it all in a nutshell, there exists a point \( Q \) in \( E[p^{m+1}] \) such that the smallest positive integer \( k_Q \) with \( k_QQ = \infty \) is equal \( m + 1 \).

As already explained this immediately proves
\[
E[p^{m+1}] \simeq \mathbb{Z}_{p^{m+1}}.
\]

In order to conclude this proof \( p \) needs to be divided out of \( n \) to the highest power possible i.e. \( n = p^r n' \) for an appropriate \( r \in \mathbb{N} \) such that \( p \nmid n' \), so
\[
E[n] = E[p^r n'] \simeq E[p^r] \oplus E[n'] \tag{5.9}
\]
Recalling \( p \) being defined as the characteristic of \( K \), the already proven first case can be applied to \( E[n'] \) showing
\[
E[n'] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \tag{5.10}
\]
Furthermore (5.6) or (5.7) can be applied to $E[p^r]$ showing $E[p^r] \simeq \{0\}$ or $E[p^r] \simeq \mathbb{Z}_p$. Putting it all together finally proves either

$$E[n] \simeq (5.9) E[p^r] \oplus E[n'] \simeq (5.10) \mathbb{Z}_p \oplus \mathbb{Z}_n \oplus \mathbb{Z}_n' \simeq \mathbb{Z}_p \oplus \mathbb{Z}_n \oplus \mathbb{Z}_n'$$

or

$$E[n] \simeq (5.6, 5.10) \{0\} \oplus \mathbb{Z}_n' \oplus \mathbb{Z}_n' \simeq \mathbb{Z}_n' \oplus \mathbb{Z}_n'. $$

\[\square\]

Having derived this structural representation under isomorphisms for the group of $n$-torsion points, the term of a basis of $E[n]$ can be introduced.

**Definition 5.7.** Let $K$ be a field of char($K$) $\neq 2$ and $n \in \mathbb{N}$ such that char($K$) $\nmid n$ and $E$ be an elliptic curve over $K$, then according to proposition 5.6 $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$.

Hence a set

$$\{\beta_1, \beta_2\} \subseteq E[n]$$

can be chosen such that for all $P \in E[n]$ integers $m_1$ and $m_2$ with $P = m_1\beta_1 + m_2\beta_2$ can be found. Moreover $m_1$ and $m_2$ are uniquely defined modulo $n$ as can easily be seen. Such a set $\{\beta_1, \beta_2\}$ is called a basis of $E[n]$.

Altogether this chapter introduced the group of $n$-torsion points in an elliptic curve and proved a structural theorem for this group. Furthermore the definition of a basis of the group of $n$-torsion points was given. Now a pairing can be defined in the next chapter which maps $n$-torsion points onto $n^\text{th}$ roots of unity.

### 5.2. Weil-Pairing.

An important tool for implementing elliptic curves efficiently in crypto-systems is a so called Weil-Pairing. Such a pairing maps the group of $n$-torsion points in an elliptic curve into the group of $n^\text{th}$ roots of unity in the corresponding field. Many properties of torsion points can therefore be derived by evaluating in a Weil-Pairing and using the already known properties of the group of $n^\text{th}$ roots of unity. Hence the definition of the group of $n^\text{th}$ roots of unity should be recalled and observed first.

**Definition 5.8.** Let $K$ be a field, $n \in \mathbb{Z}$ and $\overline{K}$ be the algebraic closure of $K$. The set

$$\mu_n := \{x \in \overline{K} \mid x^n = 1\}$$

is called the group of $n^\text{th}$ roots of unity in $\overline{K}$.

**Remark 5.9.** The set $\mu_n$ is well known a cyclic group of order $n$.

Moreover generating elements of the group of $n^\text{th}$ roots of unity can be defined and examined in more detail.

**Definition 5.10.** Let $\overline{K}$ be the algebraic closure of the field $K$. Any element $\zeta \in \overline{K}$ such that

$$\langle \zeta \rangle = \mu_n$$

is called a primitiv $n^\text{th}$ root of unity.

**Remark 5.11.** Let $K$ be a field with char($K$) = $n$ and $\zeta$ be a primitiv $n^\text{th}$ root of unity, then the above definition is equivalent to the condition

$$\zeta^k = 1 \text{ if and only if } n \text{ divides } k.$$
However, since \( p \in \{0, \ldots, n - 1\} \) and \( \langle \zeta \rangle = \mu_n \), \( p = 0 \). Hence \( k = m \ast n \) which is equivalent to \( n \mid k \).

Vice versa let \( k \) divide \( n \) with factor \( m \), then obviously
\[
\zeta^k = \zeta^{n \ast m} = \left( \zeta^n \right)^m = 1.
\]

\( \Leftarrow \)

Let \( \zeta^k = 1 \) hold if and only if \( n \) divides \( k \), be assumed.

Hence the contraposition shows that for all \( k \) smaller than \( n \), \( \zeta^k \neq 1 \). So \( \# \langle \zeta \rangle \geq n \) needs to hold.

However, since \( n \) divides \( k \), \( \zeta^n = 1 \) is known and hence \( \# \langle \zeta \rangle \leq n \) needs to hold as well.

Altogether \( \# \langle \zeta \rangle = n \). Finally using \( \langle \zeta \rangle \subseteq \mu_n \) and \( \# \mu_n = n \) shows
\[
\langle \zeta \rangle = \mu_n.
\]

Having recalled these two basic definitions, a Weil-Pairing can be defined via its characteristic properties.

**Theorem 5.12.** Let \( K \) be a field, \( n \in \mathbb{N} \) such that \( \text{char}(K) \nmid n \) and let \( E \) be an elliptic curve over \( K \), then there exists a pairing
\[
e_n: E[n] \times E[n] \rightarrow \mu_n
\]
such that

1. \( e_n \) is bilinear
2. \( e_n \) is non-degenerate in each variable i.e. if for some \( S \in E[n] \) and for all \( T \in E[n] \)
\[
e_n(S, T) = 1, \text{then immediately } S = \infty \text{ and analogues is true in the second component.}
\]
3. For all \( T \in E[n] \) it holds \( e_n(T, T) = 1 \)
4. For all \( S, T \in E[n] \) it holds \( e_n(T, S) = e_n(S, T)^{-1} \)
5. For all automorphism \( \sigma \) of \( \overline{K} \) fixing the coefficients of the corresponding non-generalized Weierstrass equation and for all \( S, T \in E[n] \) it holds
\[
e_n(\sigma(S), \sigma(T)) = \sigma(e_n(S, T)).
\]
6. For all endomorphism \( \alpha \) of \( E \) and for all \( S, T \in E[n] \) it holds
\[
e_n(\alpha(S), \alpha(T)) = e_n(S, T)^{\deg(\alpha)}.
\]

Such a pairing \( e_n \) is called **Weil-Pairing**.

**Remark 5.13.** It is important to have a closer look onto bullet points (5.) and (6.).

In order to examine bullet point (5.) in detail, setting \( \sigma \) to be an automorphism of \( \overline{K} \) fixing the coefficients of the corresponding non-generalized Weierstrass equation \( Y^2 = X^3 + AX + B \) is indispensable. Hence \( \sigma(A) = A \) and \( \sigma(B) = B \) is assumed to be given.

Such an automorphism \( \sigma \) of \( \overline{K} \) can naturally be expanded onto points \((x, y)\) in \( E[n]\backslash\{\infty\} \) by setting
\[
\sigma(x, y) := (\sigma(x), \sigma(y))
\]
and
\[
\sigma(\infty) := \infty.
\]

Furthermore for any arbitrary but fixed \( S \) in \( E[n]\backslash\{\infty\} \) \( \sigma(S) \) is a \( n \)-torsion point as well. This can be proven using the linearity of the automorphism \( \sigma \) which yields
\[
n\sigma(S) = \sigma(nS) = \sigma(\infty) = \infty.
\]

Therefore \( \sigma(S) \) is an element in \( E[n] \) and so the expression of (5.) is permitted and well-defined.

An analogous observation can be done for bullet point (6.).

To put it all in a nutshell, all expressions used in the definition of a Weil-Pairing are permitted, well-defined and to be understood in the just explained manner.

**Proof.** [19][Subsection 11.2, Theorem 11.7, pp.335ff]

In this subsection the numerations (1.) to (6.) will from now on denote the corresponding characteristic of a Weil-Pairing.

These characteristics can be used to observe an important property of basis elements of the \( n \)-torsion group.
Corollary 5.14. Let $E$ be an elliptic curve over a field $K$ and $n \in \mathbb{N}$ with $\text{char}(K) \nmid n$. Furthermore let $\{T_1, T_2\}$ be a basis of $E[n]$, then $e_n(T_1, T_2)$ is a primitive $n$th root of unity.

Proof. Let $\{T_1, T_2\}$ be a basis of $E[n]$. When evaluating the basis elements $T_1$ and $T_2$ in a Weil-Pairing $e_n$ then $e_n(T_1, T_2) = \zeta$ for an appropriate $\zeta \in \mu_n$ is known. Thus it exists a $k \in \mathbb{N}$ such that $\zeta^k = 1$.

This immediately shows

$$1 = \zeta^k = e_n(T_1, T_2)^k = e_n(T_1, kT_2).$$

Furthermore characteristic (3.) of a Weil-Pairing yields

$$e_n(T_2, T_2) = 1.$$ 

Now let $S$ be arbitrary but fixed in $E[n]$, then according to definition 5.7 integers $m_1$ and $m_2$ (unique modulo $n$) exist such that $S = m_1T_1 + m_2T_2$. Therefore

$$e_n(S, kT_2) = e_n(m_1T_1 + m_2T_2, kT_2) = e_n(m_1T_1, kT_2)e_n(m_2T_2, kT_2) = (e_n(T_1, T_2))^{km_1}(e_n(T_2, T_2))^{km_2} = 1.$$ 

Moreover since $S$ was chosen arbitrarily in $E[n]$ and due to a Weil-Pairing being non-degenerate in each variable, $kT_2$ needs to be equal $\infty$.

Recalling $T_2$ being a basis element of $E[n]$ thus yields $n \mid k$. Altogether $\zeta^k = 1$ implied $n/\mid k$. Obviously $n/k$ yields $\zeta^k = 1$ vice versa. Therefore remark 5.11 proves $e_n(T_1, T_2) = \zeta$ being a primitive $n$th root of unity.

Yet another property of the group of $n$-torsion points can also be proven using a Weil-Pairing. In this proof however some basic knowledge of Galois theory is needed. If not being familiar with this theory [12] should be completely recapitulated.

Corollary 5.15. Let $E$ be an elliptic curve over a field $K$ and $n \in \mathbb{N}$ with $\text{char}(K) \nmid n$. Furthermore let $E[n] \subseteq E(K)$, then $\mu_n \subseteq K$.

Proof. Let $\sigma \in \text{Gal}(\overline{K}/K)$ be arbitrary but fixed and $\{T_1, T_2\}$ be a basis of $E[n]$. Since $E[n] \subseteq E(K)$ is given, especially the basis $\{T_1, T_2\}$ needs to have $X$- and $Y$-coordinates in $K$. Therefore any element of the Galois group fixes the basis $\{T_1, T_2\}$ so

$$\sigma(T_1) = T_1$$

and

$$\sigma(T_2) = T_2.$$ 

Hence corollary 5.14 yields

$$\sigma(e_n(T_1, T_2)) = e_n(\sigma(T_1), \sigma(T_2)) = e_n(T_1, T_2) = \zeta$$

being a primitive $n$th root of unity with $\sigma(\zeta) = \zeta$. So $\zeta \in \text{Inv}(\text{Gal}(\overline{K}/K))$ and hence

$$\zeta \in K$$

can easily be observed using the fundamental theorem of Galois theory.

Altogether $\mu_n = \{\zeta\} \subseteq K$ was proven.

Fact 3. Recalling definition 5.7 it can be shown that an endomorphism of an elliptic curve restricted onto the group of $n$-torsion points is completely defined by an representing matrix.

Proof. To verify that a field $K$ and an elliptic curve $E$ over $K$ need to be considered. Furthermore $\alpha$ is set to be an endomorphism of $E$ and $n$ is set to be a positive integer such that $\text{char}(K)$ does not divide $n$.

As already pointed out in remark 5.13

$$\alpha(E[n]) \subseteq E[n].$$

Moreover let $\{\beta_1, \beta_2\}$ be a basis for $E[n]$. According to definition 5.7 there exist (unique modulo $n$) integers $a_{11}$, $a_{12}$, $a_{21}$ and $a_{22}$ such that

$$\alpha(\beta_1) = a_{11}\beta_1 + a_{21}\beta_2$$

45
and
\[ \alpha(\beta_2) = a_{12}\beta_1 + a_{22}\beta_2. \]
Thus
\[ [\alpha]_{\{\beta_1, \beta_2\}} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} =: \alpha_n \]
is a matrix representing the actions of the endomorphism \( \alpha \) restricted on \( E[n] \) completely.

Such a representing matrix can be used to easily determine the degree of a given endomorphism of an elliptic curve.

**Proposition 5.16.** Let \( E \) be an elliptic curve over a field \( K \), \( \alpha \) be an endomorphism of \( E \) and \( n \in \mathbb{N} \) such that \( \text{char}(K) \nmid n \), then
\[ \det(\alpha_n) = \deg(\alpha) \mod n. \]

**Proof.** In the same setting as before \( \{T_1, T_2\} \) is set to be a basis of \( E[n] \) and \( \alpha \) is set to be an endomorphism of \( E \). Furthermore \( \alpha_n := \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \) is the matrix representing the actions of the endomorphism \( \alpha \) on \( E[n] \) with respect to the basis \( \{T_1, T_2\} \).

According to corollary 5.14 \( e_n(T_1, T_2) := \zeta \) is a primitive \( n^{th} \) root of unity. Hence according to fact 3
\[ \zeta^{\deg(\alpha)} = e_n(T_1, T_2)^{\deg(\alpha)} = e_n(\alpha(T_1), \alpha(T_2)) = e_n(a_{11}T_1 + a_{21}T_2, a_{12}T_1 + a_{22}T_2) \]
\[ = \begin{array}{c} e_n(T_1, T_2)^{a_{11}a_{12}} \\ = 1 \end{array} = e_n(T_2, T_2)^{a_{21}a_{22}} = e_n(T_2, T_2)^{a_{21}a_{22}}. \]

So all in all \( \deg \alpha = a_{11}a_{22} - a_{21}a_{12} = \det(\alpha_n) \mod n \) due to \( \zeta \) being a primitive \( n^{th} \) root of unity.

This proposition can be used to derive a formula for determining the degree of a linear composition of endomorphisms of elliptic curves.

**Corollary 5.17.** Let \( E \) be an elliptic curve over a field \( K \), \( \alpha \) and \( \beta \) be endomorphisms of \( E \) and \( a \) and \( b \) be in \( \mathbb{Z} \). Furthermore for all \( P \in E \) define the endomorphism \( a\alpha + b\beta \) of \( E \) by
\[ (a\alpha + b\beta)(P) := a\alpha(P) + b\beta(P) \]
as a linear composition of endomorphisms. Then
\[ \deg(a\alpha + b\beta) = a^2 \deg(\alpha) + b^2 \deg(\beta) + ab(\deg(\alpha + \beta) - \deg(\alpha) - \deg(\beta)). \]

**Proof.** Let \( n \) be an integer such that \( \text{char}(K) \) does not divide \( n \) and let \( \{T_1, T_2\} \) be a basis of \( E[n] \). Furthermore let \( \alpha_n \) and \( \beta_n \) be the matrices defining the endomorphisms \( \alpha \) and \( \beta \) on \( E[n] \) with respect to the fixed basis. Hence the endomorphism \( \gamma := a\alpha + b\beta \) restricted on \( E[n] \) is uniquely defined by the matrix
\[ \gamma_n := a\alpha_n + b\beta_n. \]

Moreover some basic calculations prove
\[ \det \gamma_n := \det(a\alpha_n + b\beta_n) = a^2 \det(\alpha_n) + b^2 \det(\beta_n) + ab(\det(\alpha_n + \beta_n) - \det \alpha_n - \det \beta_n). \]

Together with proposition 5.16 this yields
\[ \deg(\gamma) = \det \gamma_n = a^2 \deg(\alpha_n) + b^2 \deg(\beta_n) + ab(\deg(\alpha_n + \beta_n) - \deg \alpha_n - \deg \beta_n) \mod n. \]

By the choice of \( n \) it is known that (5.11) holds for infinitely many \( n \)’s, so especially
\[ \deg \gamma = \deg(a\alpha + b\beta) = a^2 \deg(\alpha) + b^2 \deg(\beta) + ab(\deg(\alpha + \beta) - \deg(\alpha) - \deg(\beta)) \]
needs to hold.

To put it all in a nutshell, this subsection introduced the concept of a Weil-Pairing. Using the characteristics of such a pairing various properties of the group of \( n \)-torsion points were derived. Furthermore properties for endomorphisms of elliptic curves were observed. Especially a formula for the degree of a linear composition of endomorphisms of an elliptic curve was observed.
6. Elliptic curves over finite fields

The aim of this thesis is to apply elliptic curves in key exchange cryptography. Therefore it is necessary to have a closer look onto elliptic curves restricted on finite fields.

In the application of elliptic curves in cryptography the underlying field is almost always finite with at least one large prime number dividing the characteristic of the underlying field. This secures a high level of safety as will be explained in chapter 8. Moreover working over finite fields simplifies the addition over an elliptic curve and thus makes the implementation of such curves in crypto-systems very efficient. Hence it is of a high importance to prove the most important properties of elliptic curves restricted on finite fields.

Therefore subsection 6.1 will firstly introduce the term of the order of a restricted elliptic curve. Then a naive approach on determining the order of a restricted elliptic curve will be given and explained using some examples. Next a more abstract approach on determining the order of a given restricted elliptic curve will be pointed out. This approach uses a structural behavior of a restricted elliptic curve which will be proven in detail. Furthermore subsection 6.1 will determine an interval in which the order of a given restricted elliptic curve lays using Hasse’s Theorem. Of course Hasse’s Theorem will therefore be proven first. Being able to determine the order of a restricted elliptic curve $E(\mathbb{F}_q)$ for a power $q$ of a prime, the order of $E(\mathbb{F}_{q^n})$ can easily be derived for any non-negative integer $n$. This will be explained in detail in the subsection.

Furthermore subsection 6.2 will focus on the order of a subgroup generated by a single element over a restricted elliptic curve which yields the term of the order of the generating point. Being able to determine the order $N$ of such an element, a restricted elliptic curve can be found, in which the group of $N$-torsion points lays.

6.1. Order of an elliptic curve restricted on a finite field.

Implementing an elliptic curve of an order which factors into a product of primes including at least one very large prime number, is indispensable for securing a high safety level of the corresponding elliptic curve crypto-system. In order to be able to determine the order of an elliptic curve, this term needs to be defined first.

**Definition 6.1.** Let $E(\mathbb{F}_q)$ be an elliptic curve restricted on $\mathbb{F}_q$ with $q$ being a power of a prime $p$, then the **order of the elliptic curve** $E(\mathbb{F}_q)$ **restricted on** $\mathbb{F}_q$ is defined as $\#E(\mathbb{F}_q)$.

If the underlying finite field has a rather small characteristic, then the points laying in an elliptic curve restricted on that field, can be counted without great effort. In such a case the order of a considered elliptic curve can be determined easily which yields a naive approach on determining the order of a restricted elliptic curve.

**Example 6.2.** Recalling example 3.27 it is obvious that the restricted elliptic curve $E(\mathbb{F}_7)$ given by $Y^2 = X^3 + 3X + 1$ only consists of very few elements.

A straightforward approach on determining the order of this curve can either be done by simply counting the points in figure 5 or testing all possible $X$-coordinates in $\mathbb{F}_7$ for corresponding $Y$-coordinates in $\mathbb{F}_7$ over $E(\mathbb{F}_7)$. These two approaches lead to a total of 11 non-trivial elements in $E(\mathbb{F}_7)$. Hence adding 1 for $\infty$ shows $\#E(\mathbb{F}_7) = 12$.

Obviously when considering a restricted elliptic curve $E(\mathbb{F}_p)$ for a prime $p \geq 2$, all $X$-coordinates in the set $\{0, \ldots, p-1\}$ can straightforward be tested for corresponding $Y$-coordinates in $\mathbb{F}_p$ over $E(\mathbb{F}_p)$. This yields the number of non-trivial elements existing on the considered restricted elliptic curve. Not forgetting $\infty$ being an element of any (restricted) elliptic curve determines the order $\#E(\mathbb{F}_p)$ in finitely many steps.
Recalling example 3.7 the naive approach yields the order 77 of the restricted elliptic curve $E(\mathbb{F}_{71})$ given by $Y^2 = X^3 + 17X + 12$. In this example it gets obvious that the naive approach on determining the order of a restricted elliptic curve gets impractical quickly with an increasing prime characteristics $p$ of the underlying finite field. This is due to the fact that $p$ possible $X$-coordinates need to be tested for corresponding $Y$-coordinates in a naive approach. This is in terms of implementation very inefficient.

Altogether the naive approach can not be used for dealing with underlying fields of a characteristics divisible by at least one large prime.

The idea of the naive approach however can be generalized using the Legendre Symbol.

**Definition 6.3.** Let $\mathbb{F}_p$ be a finite field for a prime $p > 2$, then the **Legendre Symbol** for $x \in \mathbb{F}_p$ is defined as

$$\left(\frac{x}{\mathbb{F}_p}\right) := \begin{cases} +1, & \text{if } t^2 = x \text{ has a solution } t \in \mathbb{F}_p^\times \\ -1, & \text{if } t^2 = x \text{ has no solution } t \in \mathbb{F}_p^\times \\ 0, & \text{if } x = 0. \end{cases}$$

The next proposition yields a formula motivated by the naive approach of example 6.2, which determines the order of a restricted elliptic curve.

**Proposition 6.4.** Let $E(\mathbb{F}_p)$ be an elliptic curve restricted on $\mathbb{F}_p$ for a prime $p > 2$ given by the non-generalized Weierstrass equation $Y^2 = X^3 + AX + B$ with coefficients $A$ and $B$ in $\mathbb{F}_p$. Then

$$\#E(\mathbb{F}_p) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + Ax + B}{\mathbb{F}_p}\right).$$

**Proof.** The proof can be done straightforward by simply counting all elements in $E(\mathbb{F}_p)$ as in the naive approach.

Therefore let $x_0 \in \mathbb{F}_p$ be arbitrary but fixed. Now the number of elements in $E(\mathbb{F}_p)$ having $x_0$ as $X$-coordinate needs to be determined.

To do that efficiently $x_0^3 + Ax_0 + B = y^2$ having exactly one solution in $\mathbb{F}_p$ if and only if $x_0^3 + Ax_0 + B = 0$ in $\mathbb{F}_p$ should be recalled.

Furthermore $x_0^3 + Ax + B = y^2$ has exactly two solutions in $\mathbb{F}_p$ if and only if $x_0^3 + Ax + B$ is a square in $\mathbb{F}_p$.

Moreover $x_0^3 + Ax + B = y^2$ has no solution in $\mathbb{F}_p$ if and only if $x_0^3 + Ax + B$ is not a square in $\mathbb{F}_p$.

Altogether considering the fixed $x_0$ again

$$1 + \left(\frac{x_0^3 + Ax_0 + B}{\mathbb{F}_p}\right)$$

elements in $E(\mathbb{F}_p)$, having $x_0$ as $X$-coordinate, exist.

Repeating this for all $p$ elements of $\mathbb{F}_p$ and not forgetting $\infty$ thus yields

$$\#E(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{x^3 + Ax + B}{\mathbb{F}_p}\right)\right) = 1 + p + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + Ax + B}{\mathbb{F}_p}\right).$$

In the search for a more efficient way of determining the order of a restricted elliptic curve, the structure of the underlying restricted elliptic curve needs to be understood better.

Alike as done for the case of the group of $n$-torsion points in theorem 5.6, an isomorphic correspondence between an elliptic curve restricted on a finite field and a finite group respectively a direct sum of two finite groups over $\mathbb{Z}$, can be proven. This reveals a clearer insight on the structure of an elliptic curve restricted on a finite field, since the corresponding finite groups are broadly understood.

**Theorem 6.5.** Let $E(\mathbb{F}_p)$ be an elliptic curve restricted on $\mathbb{F}_q$ with $q$ being a power of a prime $p$. Then it either exists a $n \in \mathbb{N}$ such that $E(\mathbb{F}_q) \simeq \mathbb{Z}_n$

or it exists $n_1, n_2 \in \mathbb{N}$ such that $n_1 \mid n_2$ and $E(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$.
Two basic results of group theory need to be recalled first, in order to prove this structural theorem.

**Proposition 6.6.** A finite abelian group $G$ is isomorphic to a direct sum of cyclic groups i.e.

$$G \simeq \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k}$$

whereas for all $i \in \{1, \ldots, k - 1\}$ it holds $n_i \mid n_{i+1}$ and all $n_i$’s are uniquely defined.

**Proposition 6.7.** Let $G$ be a finite cyclic group of order $n$ and let $d$ divide $n$, then there exist exactly $d$ elements in $G$ with an order dividing $d$ i.e.

$$\#\{g \in G \mid \text{ord}(g) \mid d\} = d.$$

Now the proof of theorem 6.5 can be given.

**Proof.** First of all $E(F_q)$ is known to be a finite abelian group, hence according to proposition 6.6 there exist $n_1, \ldots, n_k$ such that $n_i \mid n_{i+1}$ for all $i \in \{1, \ldots, k - 1\}$ and

$$E(F_q) \simeq \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k}.$$  

If $k = 1$ then the claim holds immediately, therefore $k > 1$ is assumed.

At this point it needs to be emphasized that $\#\mathbb{Z}_{n_i} = n_i$ and by induction $n_1$ divides all $n_i$’s. Furthermore according to proposition 6.7

$$\#\{g \in \mathbb{Z}_{n_i} \mid \text{ord}(g) \mid n_1\} = n_1$$

for all $i = 1, \ldots, k$. Since $E(F_q)$ is isomorphic to the direct sum of all $\mathbb{Z}_{n_i}$’s especially

$$\#\{g \in E(F_q) \mid \text{ord}(g) \mid n_1\} \geq n_1^k > n_1$$

is known.

Moreover $k > 1$ yields $\text{char}(F_q)$ not dividing $n_1$ and so theorem 5.6 proves

$$\#E[n_1] \leq n_1^2.$$  

Altogether $n_1^2 \geq \#E[n_1] = \#\{g \in G \mid \text{ord}(g) \mid n_1\} \geq n_1^k > n_1$ was proven which yields $k = 2$. So $k \in \{1, 2\}$ was overall proven and hence the claim holds.  

**Remark 6.8.** Especially if $E(F_q) \simeq \mathbb{Z}_1 = \{0\}$, then $E(F_q)$ is the trivial elliptic curve $\{\infty\}$. Furthermore if there exists a $n \in \mathbb{N}$ such that $E(F_q) \simeq \mathbb{Z}_n$, then

$$\#E(F_q) = \#\mathbb{Z}_n = n$$

can immediately be observed.

Analogously if there exist $n_1$ and $n_2 \in \mathbb{N}$ with $n_1 \mid n_2$ such that $E(F_q) \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, then

$$\#E(F_q) = \#(\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}) = n_1 n_2$$

determines the order of the restricted elliptic curve $E(F_q)$.

As proposed in remark 6.8 the structural theorem 6.5 yields a way of determining the order of a restricted elliptic curve. Unfortunately the appropriate $n_i$’s of this theorem can not be easily determined in most cases. Therefore other methods need to be found for determining the order of a restricted elliptic curve.

For example a rather accurate interval in which the order of a restricted elliptic curve lays is given by Hasse’s Theorem.

**Theorem 6.9.** Hasse’s Theorem

Let $E(F_q)$ be an elliptic curve restricted on $F_q$ with $q$ being a power of a prime $p \not\in \{2, 3\}$, then

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

**Proof.** Firstly according to proposition 4.25 and theorem 4.26 $a := q + 1 - \#E(F_q) = q + 1 - \text{deg}(\phi_q - \text{id})$ can be defined.

Furthermore let $r$ and $s$ be integers with $\text{gcd}(r, s) = 1$, then according to corollary 5.17

$$0 \leq \text{deg}(r\phi_q - \text{id}) = r^2 \text{deg}(\phi_q) + s^2 \text{deg}(-\text{id}) + rs(\text{deg}(\phi_q - \text{id}) - \text{deg}(\phi_q) - \text{deg}(-\text{id})) \begin{array}{c} \text{at } q \\ \text{at } -q \end{array}$$

$$= r^2 q + s^2 - rsa.$$
Thence dividing by \( r \) and \( s \) and then multiplying with \( \frac{r}{s} \) proves
\[
0 \leq q(\frac{r}{s})^2 - a(\frac{r}{s}) + 1. \tag{6.1}
\]

Secondly \( \mathcal{A} := \{ \frac{r}{s} \in \mathbb{R} \mid \gcd(s, q) = 1 \} \subseteq \mathbb{R} \) needs to be examined.
Since \( q \) is a power of a prime \( p \not\in \{2, 3\} \) it is obvious that for at least one \( i \in \{2, 3\} \) the set
\[
B_i := \{ \frac{T}{im} \mid m \in \mathbb{Z} \}
\]
is a subset of \( \mathcal{A} \).
Moreover both \( B_i \)'s are obviously dense in \( \mathbb{Q} \). Since \( \mathbb{Q} \) is known to be dense in \( \mathbb{R} \), both \( B_i \)'s being dense in \( \mathbb{R} \) can be concluded.
Altogether \( \mathcal{A} \), containing at least one \( B_i \), is dense in \( \mathbb{R} \).

Thirdly using the density of \( \mathcal{A} \) in \( \mathbb{R} \) and (6.1), for all \( x \in \mathbb{R} \)
\[
0 \leq qx^2 - ax + 1
\]
is known. Therefore setting \( f(X) := X^2 - \frac{a}{q}X + \frac{1}{q} \) in \( \mathbb{R}[X] \) yields
\[
0 \leq f
\]
pointwise.
This immediately shows the discriminate \( \Delta(f) \) of the (quadratic) polynomial \( f \) not being positive i.e.
\[
0 \geq \Delta(f) = \left( -\frac{a}{q} \right)^2 - 4\left( \frac{1}{q} \right).
\]
Multiplying by \( q^2 \) finally proves \( a^2 - 4q \leq 0 \) and thence \( |a| \leq 2\sqrt{q} \).

Remark 6.10. Hasse’s Theorem determines an upper bound for the order of an elliptic curve restricted on a finite field given by
\[
\#E(\mathbb{F}_q) \leq |q + 1 - \#E(\mathbb{F}_q)| + |-(q + 1)| \leq 2\sqrt{q} + q + 1.
\]
This will be useful in subsection 7.3 and paragraph 8.2.1.

In the context of this thesis it is enough to know an upper bound for the order of a restricted elliptic curve. The upper bound given by Hasse’s Theorem can easily be determined, hence it is really efficient in terms of implementation.
Moreover Hasse’s Theorem yields a property of supersingular curves.

Remark 6.11. In the setting of Hasse’s Theorem let \( q = p \geq 5 \) and \( a := q + 1 - \#E(\mathbb{F}_q) \) as in theorem 4.26. Then it is known that the corresponding unrestricted elliptic curve \( E \) to \( E(\mathbb{F}_q) \) over \( \mathbb{F}_p \) is supersingular if and only if \( a = 0 \).

Proof.
\( \Leftarrow \) Let \( a = 0 \) be given. This immediately yields \( E \) being supersingular according to definition 4.28.
\( \Rightarrow \) Let \( E \) be supersingular so \( a = 0 \) mod \( p \).
For a contradiction \( a \neq 0 \) will be assumed. Hence \( a \geq p \) holds.
Hasse’s Theorem states \( |a| \leq 2\sqrt{p} \) and so
\[
p \leq |a| \leq 2\sqrt{p}.
\]
However, this is only true for \( p \leq 4 \) which contradicts the precondition \( p \geq 5 \).
Altogether the assumption \( a \neq 0 \) was wrong and \( a = 0 \) was proven.

To put it all in a nutshell, remark 6.11 yields
\[
\#E(\mathbb{F}_p) = p + 1
\]
in terms of corresponding unrestricted supersingular elliptic curves \( E \) over \( \mathbb{F}_p \) with \( p \geq 5 \).

The next goal is to find a way of easily determining \( \#E(\mathbb{F}_{q^n}) \) for any arbitrary but fixed integer \( n \), when \( \#E(\mathbb{F}_q) \) is already known.
Therefore let \( q \) be a power of a prime \( p \not\in \{2, 3\} \) and let \( \#E(\mathbb{F}_q) \) be already determined. As in theorem 4.26 set \( a \) to be the unique integer such that \( \#E(\mathbb{F}_q) = q + 1 - a \). Working in the algebraic closure of \( \mathbb{F}_q \) appropriate \( \alpha \) and \( \beta \) can be found such that
\[
X^2 - aX + q = (X - \alpha)(X - \beta)
\]
(6.2)
over \( \mathbb{F}_q \).

Hence for any \( n \in \mathbb{N}_0 \)
\[
s_n := \alpha^n + \beta^n
\]
can be defined. Now \( s_n \) being an integer for any \( n \in \mathbb{N}_0 \) can be proven by induction over \( \mathbb{N}_0 \).

**Start of induction for \( n \in \{0, 1\} \)**
First set \( n = 0 \), hence
\[
s_0 := \alpha^0 + \beta^0 = 1 + 1 = 2 \in \mathbb{Z}.
\]
Second set \( n = 1 \) and so
\[
s_1 := \alpha + \beta = a \in \mathbb{Z}
\]
whereas the last equation holds by comparison of coefficients in
\[
X^2 - aX + q = (X - \alpha)(X - \beta) = X^2 - (\alpha + \beta)X + \alpha\beta.
\]
At this point it is important to emphasize that also
\[
\alpha\beta = q
\]
(6.3)
can be observed.

**Claim of induction**
For all \( m \in \mathbb{N}_{\leq n} \cup \{0\} \) it holds that \( s_m \) is an integer.

**Step of induction** \( n \mapsto n + 1 \) It is \( s_{n+1} = \alpha^{n+1} + \beta^{n+1} \) to be considered. Evaluating \( X^2 - aX + q \) once in \( \alpha \) and once in \( \beta \) implies
\[
\alpha^2 - a\alpha + q = (\alpha - \alpha)(\alpha - \beta) = 0
\]
and
\[
\beta^2 - a\beta + q = (\beta - \alpha)(\beta - \beta) = 0.
\]
Hence multiplying by \( \alpha^{n-1} \) respectively \( \beta^{n-1} \) shows
\[
\alpha^{n+1} = a\alpha^n - q\alpha^{n-1}
\]
(6.4)
and
\[
\beta^{n+1} = a\beta^n - q\beta^{n-1}.
\]
(6.5)
Therefore
\[
s_{n+1} = \alpha^{n+1} + \beta^{n+1} = a(\alpha^n + \beta^n) - q(\alpha^{n-1} + \beta^{n-1}) = (\text{coi}) \sum_{n \in \mathbb{Z}} a \ast s_n = q \ast s_{n-1} \in \mathbb{Z}
\]
whereas (coi) emphasized the usage of the claim of induction for \( s_{n-1} \) and \( s_n \).

Obviously the just done induction also proves \( s_n \) being recursively given by \( s_0 = 2, s_1 = a \) and
\[
s_{n+1} = as_n - qsn-1.
\]
Furthermore \( s_n \) can be used to determine the order of \( E(\mathbb{F}_q^\ell) \).

**Theorem 6.12.** Let \( E(\mathbb{F}_q) \) be an elliptic curve restricted on \( \mathbb{F}_q \) with \( q \) being a power of a prime \( p \not\in \{2, 3\}, a := q + 1 - \#E(\mathbb{F}_q) \) as in theorem 4.26 and set \( X^2 - aX + q = (X - \alpha)(X - \beta) \) as in (6.2). Then for all \( n \in \mathbb{N} \) it holds
\[
\#E(\mathbb{F}_q^\ell) = q^n + 1 - (\alpha^n + \beta^n).
\]
**Proof.** It needs to be recalled that \( s_n := \alpha^n + \beta^n \) is provenly recursively given by \( s_0 = 2, s_1 = a \) and \( s_{n+1} = as_n - qsn-1 \) and all \( s_n \)’s are integers.

Furthermore the polynomial \( f(X) := (X^n - \alpha^n)(X^n - \beta^n) \) needs to be considered. Obviously \( f \) is divisible by the polynomial \( g(X) := (X - \alpha)(X - \beta) \).
Moreover \( f \) and \( g \) can be expanded into
\[
f(X) := (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - X^n \beta^n - \alpha^n X^n + \alpha^n \beta^n =
\]
\[
= X^{2n} - (\alpha^n + \beta^n)X^n + (\alpha \beta)^n\quad \text{with} \quad \alpha^n + \beta^n = s_n, \quad (6.3)
\]
and
\[
g(X) := (X - \alpha)(X - \beta) = X^2 - \alpha X - \beta X + \alpha \beta = X^2 - (\alpha + \beta)X + q
\]
\[
= \alpha + \beta = s_1 X + q \equiv X^2 - aX + q.
\]
Since \( f \) and \( g \) are both normed and only have integers as coefficients and \( g \) divides \( f \), according to the euclidean algorithm for polynomials, a polynomial \( l \) with coefficients being integers exists such that
\[
f(X) = l(X)g(X) = l(X)(X - \alpha)(X - \beta).
\]
Evaluating \( f \) in the Frobenius endomorphism thus yields
\[
f(\phi_q) = (\phi_q)^{2n} - s_n \phi_q^n + q^n \text{id} \quad (6.6)
\]
on the one hand and
\[
f(\phi_q) = l(\phi_q)(\phi_q - \alpha \text{id})(\phi_q - \beta \text{id}) = l(\phi_q)(\phi_q - \alpha \phi_q + q \text{id}) \quad (6.7)
\]
on the other hand.
Since theorem 4.26 yields \( \phi_q^2 - a \phi_q + q \text{id} \equiv 0 \)
\[
0 \equiv l(\phi_q)(\phi_q - \alpha \phi_q + q \text{id}) = f(\phi_q) = (\phi_q)^{2n} - s_n \phi_q^n + q^n \text{id} = \phi_q^{2n} - s_n \phi_q^n + q^n \text{id}
\]
is known. Moreover, according to theorem 4.26, \( s_n \) is the unique integer solving this equation. More precisely theorem 4.26 states \( s_n \) being given by \( q^n + 1 - \#E(F_{q^n}). \)
All in all \( (\alpha^n + \beta^n) =: s_n = q^n + 1 - \#E(F_{q^n}) \) proves
\[
\#E(F_{q^n}) = q^n + 1 - (\alpha^n + \beta^n).
\]

In this subsection a close look onto the order of elliptic curves restricted on finite fields was taken. Firstly a naive approach using the Legendre Symbol was introduced, then Hasse’s Theorem stated a quite accurate interval in which the order of a restricted elliptic curve can be found. Lastly a method was introduced, with which the order of a restricted elliptic curve \( E(F_{q^n}) \) can be determined for any \( n \in \mathbb{N} \), when \( \#E(F_q) \) is already known.
This correspondence is very useful, if \( q \) is a large power of a small prime \( p \not\in \{2, 3\} \). In such a case only the order of \( E(F_{p}) \) needs to be determined, which can easily be done using the naive approach. This observation is very important in terms of efficiency in cryptography as will later be emphasized.

### 6.2. Order of a point in an elliptic curve restricted on a finite field.

Immediately linked to the order of an elliptic curve restricted on a finite field is the order of a subgroup of a restricted elliptic curve generated by a single element. Therefore the term of an order of a point in an elliptic curve restricted on a finite field needs to be carefully defined and examined.
Just like the order of a restricted elliptic curve, the order of a point in a restricted elliptic curve plays an important role for the safety level of an elliptic curve in key exchange cryptography.

**Definition 6.13.** Let \( P \) be an element in an elliptic curve \( E(F_q) \) restricted on \( F_q \) with \( q \) being a power of a prime \( p \). Then the **order** of \( P \) is defined to be the smallest positive integer \( k_P \) such that
\[
k_PP = \infty
\]
and is denoted as \( \text{ord}(P) := k_P \).

**Remark 6.14.** Lagrange’s Theorem immediately yields \( kP = \infty \) if and only if \( \text{ord}(P) \mid k \). Especially \( \text{ord}(P) \mid \#E(F_q) \) is known. Moreover if \( \text{ord}(P) = \#E(F_q) \) then \( \langle P \rangle = E(F_q) \).
Being able to determine the order of a point in an elliptic curve restricted on a finite field, a structural behavior for a group of torsion points can be specified. This is very useful when aiming to apply corollary 5.15.
**Proposition 6.15.** Let $E$ be an elliptic curve over $\mathbb{F}_q$ with $q$ being the power of a prime $p \notin \{2, 3\}$ and let $a := q + 1 - \#E(\mathbb{F}_q)$ be as proposed in theorem 4.26. Furthermore $a$ is assumed to be equal zero and $N \in \mathbb{N}$ is set. If there exists a $P$ in the corresponding restricted elliptic curve $E(\mathbb{F}_q)$ with $\text{ord}(P) = N$, then $E[N] \subseteq E(\mathbb{F}_{q^2})$.

**Proof.** Recalling theorem 4.26 for the Frobenius map of the elliptic curve $E$ over $\mathbb{F}_q$ $\phi_q^2 - a\phi_q + qid \equiv 0$ is known. Since $a = 0$ is assumed, this shows $\phi_q^2 + qid \equiv 0$ and $\#E(\mathbb{F}_q) = q + 1$. Furthermore $\text{ord}(P)$ dividing $\#E(\mathbb{F}_q)$ yields $N = \text{ord}(P)$ dividing $\#E(\mathbb{F}_q) = q + 1$ and so $q = (-1) \mod N$.

Now an arbitrary but fixed $N$-torsion point $S$ is considered.

**Claim** $S$ is an element in $E(\mathbb{F}_{q^2})$.

It is enough to prove $\phi_{q^2}(S) = S$ according to remark 4.23 in order to verify the claim. However, this is trivial due to

$$0 = \phi_q^2(S) + qid(S) = \phi_{q^2}(S) + qid(S) = \phi_{q^2}(S) - \text{id}(S) = \phi_{q^2}(S) - S \mod N.$$ 

All in all this subsection introduced the term of an order of a point in an elliptic curve restricted on a finite field and some properties were shortly observed.
Aiming to be able to use elliptic curves in cryptography, it is important to firstly understand how algorithms concentrating on basic calculations can be efficiently implemented over elliptic curves. In terms of efficiency it is appropriate to use elliptic curves restricted on finite fields.

The first subsection 7.1 will introduce a method, with which a point can efficiently be added to itself a fixed integer times. Therefore a pseudo-code will be given and explained using an example. Furthermore it will be pointed out that this method is more efficient than the naive approach of simply straight forward repeatedly adding the point to itself.

Moreover subsection 7.2 will introduce a method with which the order of a point in a restricted elliptic curve can be efficiently determined. Therefore again a pseudo-code will be given and it will be proven that this method terminates in finite time. Moreover it will be shown that this method indeed determines the order of the given point.

Fortunately the method introduced in subsection 7.2 together with Hasse’s Theorem of chapter 6 can be used to determine the order of a restricted elliptic curve. Being able to determine the order of a considered restricted elliptic curve will be very important in chapter 8 in terms of security. Hence this procedure will be carefully explained using an example in subsection 7.3. Furthermore it will be pointed out that this method can only be applied in some special cases.

7.1. Method of successive doubling.

First off it is very important to understand how a point $P$ in an elliptic curve can be efficiently multiplied with a fixed integer $k$. The naive approach would be to recursively add the point $P$ $k$-times to itself using definition 3.22. However, this naive approach is really time consuming and therefore impractical. The effort needed to determine $kP$ using the naive method increases exponentially with increasing $k$.

Fortunately there exists another method called successive doubling which is more efficient. The effort needed to determine $kP$ using this method only increases linearly with increasing $k$.

The idea of this method is to firstly rewrite the integer $k$ as

$$k = \sum_{j=0}^{m} k_j 2^j$$

for an appropriate $m \in \mathbb{N}_0$ whereas each $k_j$ is either equal zero or one. Obviously this is always possible. The multiplication of $P$ with $k$ can thus be reformulated into

$$kP = \left( \sum_{j=0}^{m} k_j 2^j \right) P = \sum_{j=0}^{m} (k_j 2^j P).$$

Therefore the knowledge of an already determined summand $k_j 2^j P$ can be used to determine another summand. Hence many calculations to be done in the naive approach can be avoided. This motivates the algorithm given next.
Successive Doubling Algorithm

1. **INPUT** \((E, +, \infty)\) additive group of an elliptic curve, \(P \in E, k \in \mathbb{N}\)
2. Set \(a = k\);
3. Set \(B = \infty\);
4. Set \(C = P\);
5. **While** \(a \neq 0\)
   6. If \(a = 0 \mod 2\)
      7. Set \(a = a/2\);
      8. Set \(C = 2 \times C\);
   9. Else
      10. Set \(a = a - 1\);
      11. Set \(B = B + C\);
12. **End**
13. **End**
14. **OUTPUT** \(B\)

This algorithm does exactly what was explained in the beginning whereas the reformulation of \(k\) as a sum and the determinations of the \(k; 2^j P\)'s are done simultaneously. In order to understand this algorithm better, it is best to test it on an example.

**Example 7.1.** Let \((E, +, \infty)\) be a fixed additive group of an elliptic curve. Set \(P\) as a fixed point in \(E\) and set \(k = 27\) so \(27P\) shall be determined.

Applying the just introduced algorithm firstly resolves in setting \(a = 27\), \(B = \infty\) and \(C = P\).

Obviously \(0 \neq 27 = a\) and so the While-loop starts. The equations denoted as \(\div\) which will be stated next, need to be understood from an informatics point of view, where for example an "old" \(a\) is used to define a "new" \(a\) via "\(\div\)".

Since \(a = 27 = 1 \mod 2\) the steps nine to twelve need to be applied. Hence

\[
a \div a = 27 - 1 = 26
\]

and

\[
B \div B + C = \infty + P = P
\]

need to be set and since \(0 \neq 26 = a\) the While-loop continues.

Observing \(a = 26 = 0 \mod 2\) shows that step six to eight need to be applied stating

\[
a \div a/2 = 26/2 = 13
\]

and

\[
C \div 2 \times C = 2 \times P.
\]

Moreover the While-loop continues, since \(0 \neq 13 = a\).

Due to \(a = 13 = 1 \mod 2\)

\[
a \div a = 13 - 1 = 12
\]

and

\[
B \div B + C = P + 2 \times P
\]

need to be set. Still \(0 \neq 12 = a\) and so the While-loop continues.

Now \(a = 0 \mod 2\) is observable. Hence

\[
a \div a/2 = 12/2 = 6
\]

and

\[
C \div 2 \times C = 2 \times 2 \times P
\]

are determined. Moreover \(0 \neq 6 = a\) and so the While-loop does not terminate yet.

Again \(a = 6 = 0 \mod 2\) holds, implying

\[
a \div a/2 = 6/2 = 3
\]

and

\[
C \div 2 \times C = 2 \times 2 \times 2 \times P.
\]

Still \(a = 3 \neq 0\) and thus the While-loop continues.

Observing \(a = 3 = 1 \mod 2\) yields

\[
a \div a = 3 - 1 = 3 - 1 = 2
\]
and 
\[ B = B + C = P + 2 \cdot P + 2 \cdot 2 \cdot 2 \cdot P. \]
Again the While-loop continues.
Since \( a = 2 \mod 2 \)
\[ a \doteq a/2 = 1 \]
and
\[ C = 2 \cdot C = 2 \cdot 2 \cdot 2 \cdot 2 \cdot P \]
need to be set. Now the While-loop starts its last loop.
Due to \( a = 1 \mod 2 \)
\[ a \doteq a - 1 = 0 \]
and
\[ B = B + C = P + 2 \cdot P + 2 \cdot 2 \cdot 2 \cdot P + 2 \cdot 2 \cdot 2 \cdot 2 \cdot P \]
can be determined. The While-loop terminates.
The solution was found as being
\[ kP = B = P + 2 \cdot P + 2 \cdot 2 \cdot 2 \cdot P + 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot P. \]

What was done, was to rewriting \( k \) uniquely as
\[ k = 27 = 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 \]
as proposed in the very beginning of this subsection. This was translated into
\[ kP = (1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4)P = P + 2P + 2^3P + 2^4P \]
by the algorithm. Having a closer look onto all calculations done, it gets obvious that
\[ 2 \cdot P = P + P \]
was firstly calculated. Then
\[ P + 2P \]
was derived using \( P \) and \( 2P \). Following up \( 2^2P \) was determined by using the already calculated \( 2P \) by
\[ 2^2P = 2 \cdot (2P) = 2P + 2P. \]
This then yielded \( 2^3P \) using \( 2^2P \) via
\[ 2^3P = 2 \cdot (2^2P) = 2^2P + 2^2P \]
and so
\[ P + 2P + 2^2P \]
was derived together with the already determined \( P + 2P \). Lastly \( 2^4P \) was calculated using the known value of \( 2^3P \) in
\[ 2^4P = 2 \cdot (2^3P) = 2^3P + 2^3P. \]
Taking the sum over all already calculated points finally delivered
\[ 27P = P + 2P + 2^3P + 2^4P. \]

All in all in order to determine \( 27P \) seven additions were needed to be done. The naive approach would have needed nearly four times as many additions namely \( 26 \) in order to calculate \( 27P \).
This example emphasizes that the successive doubling method is already more efficient for rather small integers than the naive approach. This gap in efficiency obviously widens with increasing integers, since the naive approach has an exponential effort growth whereas the successive doubling method only grows linearly in effort.
To put it all in a nutshell, the successive doubling method is an easy to implement algorithm which is very efficient for multiplying points in an elliptic curve by a fixed integer. Thus elliptic curve cryptosystems based on this method for the multiplication by a fixed integer are commonly used nowadays.
7.2. Determining the order of a point in a restricted elliptic curve.

Being able to determine the order of a point in a restricted elliptic curve is another very important milestone on the way of implementing an efficient elliptic curve crypto-system. A naive approach would be to randomly test appropriate integers on whether they are a possible candidate for the order or not. In order to explain this approach in more detail a restricted elliptic curve $E(\mathbb{F}_q)$ with $q$ being a power of a prime $p$ will be considered. Furthermore $N := \#E(\mathbb{F}_q)$ is set and $P$ is a fixed element in $E(\mathbb{F}_q)$ whose order shall be determined.

Lagrange’s Theorem yields $M := \text{ord}(P)$ dividing $N$. The naive approach now proposes to start determining $mP$ for increasing positive integers $m$ dividing $N$. The smallest $m$ for which $mP = 1$ is the order of $P$.

This method is obviously quite inefficient and an appropriate $4\sqrt{q}$ steps are needed in order to determine the order of $P$. Fortunately there are various more efficient algorithms existing. One of such algorithms will be introduced next which determines the order of a point $P$ in a restricted elliptic curve $E(\mathbb{F}_q)$ in an appropriate $2\sqrt{q}$ steps.

**Baby Step - Giant Step**

1. **INPUT** $(E(\mathbb{F}_q), +, \infty)$ additive group of a restricted elliptic curve, $q$ power of a prime $p \notin \{2, 3\}$, $P \in E(\mathbb{F}_q)$
2. Set $Q = (q + 1) \cdot P$;
3. Set $m = \lceil q^{1/4} \rceil$
4. For $j = 0 : m$
5. Calc and Save $j \cdot P$;
6. For $k = m + 1 : m$
7. If $Q + k \cdot (2 \cdot m \cdot P) = j \cdot P$
8. Set $M = q + 1 + 2 \cdot m \cdot k - j$;
9. Break;
10. Goto 19.;
11. Elseif $Q + k \cdot (2 \cdot m \cdot P) = -j \cdot P$
12. Set $M = q + 1 + 2 \cdot m \cdot k + j$;
13. Break;
14. Goto 19.;
15. End
16. End
17. End
18. Factorize $M$ in distinct power of primes i.e. $M = p_1^{\varepsilon_1} \cdots p_r^{\varepsilon_r}$ for an appropriate $r \in \mathbb{N}$, $p_1, \ldots, p_r$ distinct primes, $\varepsilon_1, \ldots, \varepsilon_r \in \mathbb{N}$
19. Set $i = 1$
20. While $i <= r$
21. While $(M/p_i) \cdot P \neq \infty$
22. Set $M = M/p_i$;
23. End
24. Set $i = i + 1$
25. End
26. **OUTPUT** $M$

This algorithm might seem a little confusing at a first glance. However, observing it in more detail clarifies the idea of this algorithm.

Firstly it needs to be observed why step four to step seventeen really determine two appropriate existing(!) integers $j_0$ and $k_0$.

**Lemma 7.2.** Let $a$ be an integer such that $|a| \leq 2m^2$ for a fixed integer $m$, then there exist two integers $a_0$ and $a_1$ such that

$$a = a_0 + 2ma_1$$

with $-m < a_0 \leq m$ and $-m \leq a_1 < m$. 

58
Proof. Constructively $a_0$ is set as the unique integer in \{-m + 1, \ldots , m\} such that
\[ a_0 = a \mod 2m. \]
Furthermore
\[ a_1 := \frac{a - a_0}{2m} \]
is set which is trivially an integer in \{-m, \ldots , m - 1\} by the choice of $a_0$. Obviously
\[ a_0 + 2ma_1 = a_0 + 2m\frac{a - a_0}{2m} = a_0 + a - a_0 = a \]
and hence the claim was proven.

This lemma can now be applied to the Baby Step - Giant Step.

Therefore $a := q + 1 - \#E(\mathbb{F}_q)$ is set as in theorem 4.26 and applying Hasse’s Theorem yields $|a| \leq 2\sqrt{q}$. Hence setting $m = \lceil q^{1/4} \rceil$ as in step three yields $|a| \leq 2\sqrt{q} \leq 2m^2$. Thus lemma 7.2 claims that there exist two integers $a_1$ and $a_2$ such that $a = a_0 + 2ma_1$ with $-m < a_0 \leq m$ and $-m \leq a_1 < m$.

Now the loops of step four and step six will succeed in finding a pair $(j_0, k_0)$ satisfying either the If-condition of step seven or the Elseif-condition of step eleven. This is due to if $j_0 = |a_0|$ and $k_0 = -a_1$ are set, then
\[
Q + k_0(2mP) = (q + 1)P + k_0(2m)P = (q + 1)P + (-a_1)(2mP)
\]
\[= (q + 1 - 2a_1m)P = (q + 1 - a + a_0)P = \#E(\mathbb{F}_q) + a_0)P
\]
\[= \infty + a_0P = a_0P = \pm j_0P.\]

So this pair always satisfies the If-or the Elseif-condition of the considered section and thus determines an integer $M$ as in the algorithm.

It is important to emphasize that other appropriate pairs might exist as well and could also be found first by this algorithm.

 Altogether it was proven that up to step seventeen the algorithm really compiles with determining an integer $M$.

Step eighteen and nineteen are then of no mathematical trouble at all. Obviously the While-loop of step twenty will terminate after finitely many steps. Moreover step twenty-two can successfully be executed.

Now the last remaining questions left to answer are why the While-loop of step twenty-one terminates in finitely many steps and why the finally calculated $M$ really determines the order of $P$. These questions are answered in the next lemma.

\textbf{Lemma 7.3.} Let $(G, +, 0)$ be an additive group and $g \in G$ be fixed. Furthermore let $M \in \mathbb{N}$ be such that $Mg = 0$. If for all primes $p$ dividing $M$ it simultaneously holds $\frac{M}{p}g \neq 0$, then

\[ M = \text{ord}(g). \]

\textbf{Proof.} This proof will be done by contraposition, so let $M$ be unequal the order of $g$.

Nevertheless since $Mg = 0$, $\text{ord}(g)$ dividing $M$ is known. Thus it exists a unique positive integer $k$ greater than one such that $\text{ord}(g) = k$.

Moreover it exists a prime $p$ dividing $k$ and hence such a $p$ especially divides $M$ with

\[ \frac{M}{p}g = \underbrace{\frac{\text{ord}(g)}{p}g}_{p \in \mathbb{Z}, a_0} = 0. \]

In the setting of the Baby Step - Giant Step this translates into

\[ (G, +, 0) = (E(\mathbb{F}_q), +, \infty) \]

and $M$ is the integer found in step eight respectively step twelve. Furthermore $(j_0, k_0)$ is the pair found in step four and step six with

\[ MP = (q + 1 + 2mk_0 \neq j_0)P = (q + 1)P + 2mk_0P \neq j_0P = Q + 2mk_0P \neq j_0P = \pm j_0P \neq j_0P = \infty. \]
Thus the While-loop started in step twenty-one starts with dividing all unnecessary (power) of primes out of \( M \) so that lemma 7.3 can be applied which finally determines the order of \( P \). The process of dividing unnecessary primes out surely can be enclosed after finitely many steps.

All in all it was therefore proven that the Baby Step - Giant Step proposed in this subsection terminates after finitely many steps and determines the order of a fixed point.

### 7.3. Determining the order of a restricted elliptic curve.

To conclude this chapter it will be explained how the order of a restricted elliptic curve can be efficiently determined. Obviously in some cases it might be possible to use the formula of proposition 6.4 and the Legendre Symbol of definition 6.3 to determine the order of a considered restricted elliptic curve. However, this might not always be possible.

Fortunately the just introduced Baby Step - Giant Step of the previous subsection can be used to determine the order of a restricted elliptic curve as well. Hence a restricted elliptic curve \( E(\mathbb{F}_q) \) for a power \( q \) of a prime \( p \not\in \{2, 3\} \) will be considered.

According to Hasse’s Theorem it is known that the order \( N \) of the restricted elliptic curve \( E(\mathbb{F}_q) \) needs to lay in the interval \( [-2\sqrt{q} + q + 1, 2\sqrt{q} + q + 1] \). Furthermore the order of randomly fixed points \( P \) in the restricted elliptic curve \( E(\mathbb{F}_q) \) can be determined by the Baby Step - Giant Step. Moreover Lagrange’s Theorem yields all \( \text{ord}(P) \)'s dividing the order of the restricted elliptic curve \( E(\mathbb{F}_q) \). Together with the interval proposed by Hasse’s Theorem the order of the considered restricted elliptic curve can hence be uniquely determined.

**Example 7.4.** In this example the elliptic curve \( E(\mathbb{F}_{71}) \) given by the non-generalized Weierstrass equation \( Y^2 = X^3 + 17X + 12 \) in \( \mathbb{F}_{71} \) as introduced in example 3.7 will be considered.

Firstly Hasse’s Theorem yields

\[
54 = 71 + 1 - 2 \times 9 < 71 + 1 - 2\sqrt{71} \leq E \leq 71 + 1 + 2\sqrt{71} \leq 71 + 1 + 2 \times 9 = 90
\]

according to remark 6.10. Moreover randomly fixing the point \( P = (7, 30) \in E(\mathbb{F}_{71}) \) and determining the order of \( P \) using the Baby Step - Giant Step yields

\[
\text{ord}(P) = 7.
\]

Therefore 7 needs to divide the order of the restricted elliptic curve given.

Together with the interval proposed by Hasse’s Theorem

\[
#E(\mathbb{F}_{71}) \in \{56, 63, 70, 77, 84\}
\]

was proven.

Furthermore again randomly fixing \( Q = (21, 51) \in E(\mathbb{F}_{71}) \) yields

\[
\text{ord}(Q) = 11.
\]

Hence 11 needs to divide \( #E(\mathbb{F}_{71}) \in \{56, 63, 70, 77, 84\} \). This immediately proves

\[
#E(\mathbb{F}_{71}) = 77
\]

which coincides with the order determined in example 6.2.

All in all this subsection introduced a method using the Baby Step - Giant Step of the previous subsection in order to determine the order of a given restricted elliptic curve. This method is more efficient than just using the formula of proposition 6.4.

It is known that the method introduced in this subsection can be efficiently used for elliptic curves restricted on finite fields \( \mathbb{F}_q \) for integers \( q \) as large as \( 10^{24} \). However, in cryptography it might happen that elliptic curves restricted on finite fields over even larger integers \( q \) are considered.
8. THE DISCRETE LOGARITHM PROBLEM

Independently of the theory of elliptic curves, there is another well-known problem in informatics existing which is named the discrete logarithm problem and from a huge interest in the theory of applied mathematics and informatics. All security levels of the crypto-systems which will be introduced in chapter 10, chapter 11 and chapter 12 are based on the difficulty of solving a given discrete logarithm problem.

There are various ways of formulating this problem existing. The most popular versions of this problem will be introduced in subsection 8.1 and explained in more detail. Moreover it is possible to transfer some versions into one another. This will also be done in the first subsection.

In subsection 8.2 four possible attacks on this problem will be introduced in four paragraphs. Firstly the setting of the considered problem will be fixed and then a pseudo-code on attacking the problem will be given. Furthermore it will be examined why each attack terminates in finite time with a solution of the considered problem. Moreover in some cases simplifications in the setting of an elliptic curve can be made. This will also be pointed out and explained if possible. Ideas used in those attacks are the concept of a Weil-Pairing, the Chinese Remainder Theorem and the concept of logarithms. Each attack will only be efficiently applicable in certain cases. Hence in order to be secure a high safety level for an elliptic curve crypto-system, those cases should be avoided. All in all subsection 8.2 clarifies criteria which shall be met by an elliptic curve in order to secure a safe elliptic curve crypto-system.

8.1. Types of discrete logarithm problems.

There are various ways of formulating a discrete logarithm problem existing. The most three important versions will be given in this subsection.

Therefore firstly the classical version of this problem will be introduced, because the theory used is well-known and so this version is best to get to know this problem.

Definition 8.1. Let \( p \) be a prime in \( \mathbb{N} \) and \( a, b \) be positive integers. Knowing that there exists an integer \( k \) such that multiplying \( a \) \( k \)-times to itself equals \( b \) modulo \( p \) i.e.
\[
a^k = b \mod p,
\]
but not knowing the value of \( k \), yields the classical discrete logarithm problem which is to determine a \( k \) solving this equation.

Example 8.2. For example a riddle can be considered, where it is known that the prime \( 7 \) in \( \mathbb{N} \) and the positive integers \( 6 \) and \( 1 \) were chosen. Moreover \( 6 \) was multiplied a secret times \( k \) to itself and thus \( 1 \) modulo \( 7 \) was derived. The task now is to determine an integer \( k \) such that \( k \) solves
\[
6^k \equiv 1 \mod 7.
\]
Such a solving \( k \) would be \( k = 4 \), because
\[
6^4 = 1296 = 7 \times 185 + 1 = 1 \mod 7.
\]

Therefore the integer \( 4 \) solves the given classical discrete logarithm problem. However, due to \( \mathbb{F}_7 \) being a finite cyclic field, there are other solving integers existing as well.

Remark 8.3. Obviously if \( k \) is a solution to a given classical discrete logarithm problem, then so is \( k + p - 1 \). That is because
\[
a^{k+p-1} = a^{k+(p-1)} = a^k \ast a^{p-1} = a^k \equiv b \mod p.
\]
Hence every element of the equivalence class of \( k \) modulo \( p-1 \) is also a solution for that given classical discrete logarithm problem. The integer \( k \) therefore has to be understood as a representing element of that equivalence class and it needs to be kept in mind that \( k \) is not unique.
As already mentioned, the just introduced problem is called the classical discrete logarithm problem. Having understood the idea of this problem, the general discrete logarithm problem can be formulated.

**Definition 8.4.** Let \((G, *, 1)\) be a multiplicative group and \(a, b\) be elements in \(G\). Knowing that there exists an integer \(k\) such that
\[ a^k = b \]
over \(G\), but not knowing the value of \(k\), yields the **general discrete logarithm problem** which is to determine a \(k\) solving this equation.

Of course the general discrete logarithm problem can be adapted to the additive group of an elliptic curve.

**Definition 8.5.** Let \(p\) be a prime in \(\mathbb{N}\) and \(q\) be a power of \(p\). Set \((E, +, \infty)\) as the additive group of an elliptic curve as introduced in subsection 3.3. Let \(P_1\) and \(P_2\) be fixed elements in this elliptic curve. Knowing that there exists a secret integer \(k\) such that
\[ kP_1 = P_2 \]
over \(E\), but not knowing the value of \(k\), yields the **elliptic curve discrete logarithm problem** which is to determine a \(k\) solving this equation.

**Remark 8.6.** Obviously the elliptic curve discrete logarithm problem is a special case of the general discrete logarithm problem. The multiplicative group \((G, *, 1)\) in definition 8.4 is just replaced by the additive group \((E, +, \infty)\) and the elements \(a\) and \(b\) by the elements \(P_1\) and \(P_2\) in the elliptic curve. In the elliptic curve problem an additive group instead of a multiplicative group is considered, so the \(k^{\text{th}}\) power of \(a\) is reformulated into \(k\)-times \(P_1\). Therefore \(a^k = b\) over \(G\) yields \(kP_1 = P_2\) over \(E\).

As mentioned before most crypto-systems’ safety level in general relies on the hardness of a to-be-solved discrete logarithm problem. Hence it should nearly be infeasible to solve such a given problem. However, a straight forward attack would be to just randomly test integers \(k\) on whether they solve the problem or not. Therefore neither the groups’ order nor the integer \(k\) should be of a too small value. They should both be at least several hundreds of digits long. Regarding nowadays’ crypto-systems based on elliptic curves, most integers \(k\) consist of at least \(2^{160}\) to \(2^{1024}\) digits. The just stated naiv approach is therefore very impractical and of no use at all. Therefore other methods on attacking an elliptic discrete logarithm problem need to be considered, in order to be able to ensure that an implemented elliptic curve is safe against such possible attacks.

### 8.2. Attacks on the discrete logarithm problem.

Nowadays there are four commonly known attacks on discrete logarithm problems existing. Most of those attacks can only be efficiently applied if certain criteria of the underlying group, respectively in the context of this thesis, of the underlying elliptic curve are met. Thus in order to secure a high level of security, it has to be ensured that those criteria are not met. In the following four paragraphs each of those four commonly known attacks will be firstly introduced and then carefully examined.

#### 8.2.1. Baby Step - Giant Step.

The first attack on a general discrete logarithm problem to be discussed, is the **Baby Step - Giant Step**. This method was developed by D. Shanks and aims to solve a given general discrete logarithm problem over an arbitrary finite additive group \((G, +, 0)\) of an group order \(\#G\). So for given elements \(P\) and \(Q\) in \(G\) such that \(kP = Q\) for an existing, yet unknown integer \(k\), the method tries to find at least one appropriate integer \(k\) solving this problem.
Baby Step - Giant Step

1. INPUT \((G, +, 0)\) finite additive group, \(P \in G, Q \in G, \#G =: N \in \mathbb{N}\)
2. \(m = \lceil \sqrt{N} \rceil\)
3. For \(i = 0 : (m - 1)\)
   4. Calc \(iP = (i - 1) * P + P\);
   5. Save \(iP\);
   6. For \(j = 0 : (m - 1)\)
      7. Calc \(Q - j * m * P = Q - (j - 1) * m * P - m * P\);
      8. Save \(Q - j * m * P\);
      9. If \(iP = Q - j * m * P\) Save \(i, j\) and \(m\);
      10. Break;
     11. Goto 16.;
   12. End
13. End
14. End
15. End
16. \(k = i + j * m\);
17. OUTPUT \(k\)

Remark 8.7. Step four is called a Baby Step, since \(iP\) is derived by adding \(P\) to \((i - 1)P\), hence a rather small step is taken.
Moreover step seven is called a Giant Step, because \(Q - jmP\) is calculated by subtracting \(mP\) from \(Q - (j - 1)mP\). Thus a rather huge step is done.
In step sixteen \(k\) could be furthermore simplified by being taken modulo the group order \(N\).
Step seventeen yields the output element \(k\) which solves the given general discrete logarithm problem i.e. \(kP = Q\) over \(G\).
Having understood the algorithm of the Baby Step - Giant Step for general discrete logarithm problems, it is now of a mathematical interest to understand, why that algorithm delivers a solution \(k\) for an inserted general discrete logarithm problem in finite time.

Proposition 8.8. The Baby Step - Giant Step of this paragraphs terminates in finitely many steps with a solution of a given general discrete logarithm problem.

Proof. In step two \(m\) is set to be \(m = \lceil \sqrt{N} \rceil\). Hence \(m \geq \sqrt{N}\) and therefore \(m^2 \geq N\) whereas the integer \(N\) was set as the group order of \(G\).
Obviously the general discrete logarithm states the existence of a solving integer \(k\). Moreover since \((G, +, 0)\) is a finite abelian group of order \(N\) and a solution \(k\) of the general discrete logarithm problem for fixed \(P\) and \(Q\) in \(G\) exists, especially a solution \(k\) can be found such that
\[
0 \leq k < N^2 \leq m^2
\]
according to remark 8.3. Hence an existing(!) integer \(k_0 \in \{0, \ldots, m - 1\}\) is uniquely defined by
\[
k_0 \equiv k \mod m
\]
which yields
\[
k = k_0 + mk_1
\]
for an appropriate existing(!) integer \(k_1\). Since \(0 \leq k < m^2\) and \(0 \leq k_0 < m\),
\[
0 \leq k_1 < m
\]
holds obviously.
Moreover observing
\[
Q - k_1mP = Q - (k - k_0)P = Q = kP - (k - k_0)P = k_0P
\]
yields at least one pair \((k_0, k_1)\) fulfilling the If-condition of step nine.
Furthermore any pair \((i, j)\) solving the If-condition of step nine yields
\[
i + jm
\]
being a solving integer of the given discrete logarithm problem, because

$$Q = iP + jmP = (i + jm)P.$$  \hfill (8.1)

Hence determining such an existing pair \((i, j)\) solves the given discrete logarithm problem.

The hard part is to determine such a provenly(!) existing pair \((i, j)\). This is done by the naive approach of testing all possible integer pair combinations in \(\{0, \ldots, m - 1\} \times \{0, \ldots, m - 1\}\), since the pair \((k_0, k_1)\) can be found for sure in this set.

In step three the to-be-tested integer \(i\) is set and in step six the to-be-tested integer \(j\) is set. Next the algorithm starts testing whether the currently observed pair \((i, j)\) determines a solution for the given general discrete logarithm problem or not. This is done by testing the criterion

$$iP = Q - jmP$$

in step nine which is enough for \(i + jm\) being a solving integer due to (8.1).

If such a solving pair is found, the algorithm jumps to step sixteen and determines

$$k = i + jm$$

which is the output in step seventeen. As already proven in (8.1) such a \(k\) solves a given general discrete logarithm problem.

Since it is enough to let \(i\) and \(j\) run from 0 to \(m - 1\) the algorithm terminates in finitely many steps with a solution \(k\) of the given general discrete logarithm problem.

Implicitly it was shown that the running time of the algorithm is closely connected to the given group order. Carefully observing the Baby Step - Giant Step, it gets obvious that the group order \(N\) is only needed as an upper bound for finding an appropriate integer \(m\). This \(m\) acts as an upper bound for the to-be-tested integers \(i\) and \(j\) in step three and step six.

Idealistically speaking the \(m\) defined in step two is the best upper bound possible, so the exact group order \(N\) is only needed in order to determine that best \(m\).

When considering the case of \((G, +, 0)\) being the additive abelian group of a restricted elliptic curves, it was pointed out in subsection 7.2 and subsection 7.3 that determining the group order of a restricted elliptic curve is a hard problem to solve. Fortunately Hasse’s Theorem introduced in subsection 6.1 yields another easy to calculate, yet quite accurate upper bound for the group order of a restricted elliptic curve.

Remark 8.9. Recalling remark 6.10 for elliptic curves restricted on finite fields, it is known that for a power \(q\) of a prime \(p \notin \{2, 3\}\) and a restricted elliptic curve \(E(\mathbb{F}_q)\)

$$\#E(\mathbb{F}_q) := N \leq 2\sqrt{q} + q + 1.$$  \hfill (8.2)

Hence instead of choosing \(m := \lceil \sqrt{\{N\}} \rceil\) as an upper bound as done in step two, it is enough to chose a positive integer \(\overline{m}\) as small as possible such that \(\overline{m}^2 \geq 2\sqrt{q} + q + 1\). For such a \(\overline{m}\) obviously \(\overline{m}^2 \geq N\) according to (8.2) and so the Baby Step - Giant Step can be applied using \(\overline{m}\) by the same argumentation as done in the proof of proposition 8.8.

Moreover since the boundary provided by Hasse’s Theorem is rather accurate, it is more efficient to maybe test a few more integers \(i\) and \(j\) by using not the smallest possible upper bound \(m\) but the upper bound \(\overline{m}\) derived by Hasse’s Theorem, than to expensively calculate the group order \(N\).

When implementing the Baby Step - Giant Step for elliptic curves the command of step two can therefore be replaced with the command

$$m = \lceil \sqrt{2\sqrt{q} + q + 1} \rceil.$$  

Furthermore the Baby Step - Giant Step can be even more simplified in the case of restricted elliptic curves.

Remark 8.10. Working with the group of an elliptic curve restricted on a finite field, it is known that the curve is symmetric with respect to a parallel of the \(X\)-axis. This property can be used to simplify the introduced Baby Step - Giant Step.

For an element \(P := (x, y)\) in a restricted elliptic curve the additive inverse \(-P\) can be easily derived by setting \(-P = (x, -y)\) with \(-y\) being the additive inverse of \(y\) in the considered finite field. Thus the command of step three can be replaced by the command

For \(i = 0 : \lfloor (m/2) \rfloor\)
The section of step nine until the end with

9. \textbf{If} \ iP == Q - j * m * P \\
10. \ \ \ \text{Save} \ i, j, m; \\
11. \ \ \ \text{Break}; \\
12. \ \ \ \text{Goto 21;} \\
13. \textbf{Elseif} \ -iP == Q - j * m * P \\
14. \ \ \ \text{Calc} \ i = -i; \\
15. \ \ \ \text{Save} \ i, j, m; \\
16. \ \ \ \text{Break}; \\
17. \ \ \ \text{Goto 21;} \\
18. \ \ \ \textbf{End} \\
19. \ \ \ \textbf{End} \\
20. \ \ \ \textbf{End} \\
21. \ k = i + j * m; \\
22. \ \ \ \textbf{OUTPUT} \ k.

This adaption does not influence the systematic of the algorithm at all. However, less loops are needed in order to terminate and so this adaption is more efficient.

For the general Baby Step - Giant Step the integers \(i\) and \(j\) run from 0 to \(m - 1\) with \(m\) being the smallest integer such that \(m^2 \geq N\). Therefore when examining the efficiency of the algorithm the worst case scenario in terms of running time should be considered. This is the case for \(m\) needed loops in order to test all possible \(i\)'s. So in a worst case scenario approximately \(\sqrt{N}\) steps are needed to terminate the algorithm. Since all the \(iP's\) and \(Q - jmP's\) need to be saved, a storage of about \(\sqrt{N}\) bytes is needed.

When working with elliptic curves restricted on finite fields the adaptions of remark 8.10 can be made. Now instead of \(m\) loops only \(\lfloor m/2 \rfloor\) loops are needed in order to test all possible \(i\)'s. Therefore in a worst case scenario approximately \(\lfloor \sqrt{N}/2 \rfloor\) steps are needed until a solution is found. Moreover the storage space needed gets halved when using this adaption by an analogous argumentation.

All in all in order to be able to efficiently apply the Baby Step - Giant Step a finite group \(G\) respectively an elliptic curve \(E\) restricted on a finite field with a rather moderate group order is needed. It is now obvious that it is very important to determine the group order of a considered restricted elliptic curve or at least to determine an interval in which the group order can be found.

When implementing a restricted elliptic curve for the purpose of key-exchange cryptography, the group order of a considered restricted elliptic curve always needs to be tested, aiming to propose a restricted elliptic curve of a rather large group order in order to secure a high safety level. For example a commonly used restricted elliptic curve nowadays is called the curve prime192v1 which has a group order of approximately eighty-octillions (\(10^{48}\)). When wanting to solve an elliptic discrete logarithm problem over this curve by using the Baby Step - Giant Step with the adaption proposed in remark 8.10 then in the worst case scenario approximately \(2.5 * 10^{30}\) bytes of memory space and steps are needed. However, the whole memory space available on earth consists of only approximately \(10^{21}\) bytes. Therefore the Baby Step - Giant Step is clearly of no use for attacking an elliptic discrete logarithm problem over the curve prime192v1. The same holds for all commonly used curves nowadays, hence they are all invulnerable to this attack.

To sum it all up, in this paragraph the Baby Step - Giant Step was introduced and it was explained why this algorithm yields a solution in finitely many steps. Furthermore some adaptions were proposed which can be made in the case of elliptic curve crypto-systems. In the end it was pointed out that the algorithm is only efficient when the given group order is rather moderate. In order to be invulnerable to that attack restricted elliptic curves of a large group order are used nowadays.

8.2.2. \textbf{Pohlig-Hellman Method}.

Another method for an attack on a general discrete logarithm problem called the \textbf{Pohlig-Hellman Method} was invented by S. Pohlig and M. Hellman. This method uses the Chinese Remainder Theorem.
Theorem 8.11. Chinese Remainder Theorem

Let $R$ be a ring and $A_1, \ldots, A_m$ be ideals in $R$ for a positive integer $m$. Then the map

$$
\varphi : \quad R \rightarrow \prod_{i=1}^{m} R / A_i
$$

$$
r \mapsto (r + A_1, \ldots, r + A_m)
$$

is a homomorphism between rings with $\ker(\varphi) = \bigcap_{i=1}^{m} A_i$.

Especially if the $A_i$’s are pairwise co-prime, then $\varphi$ is surjective and

$$
R / \bigcap_{i=1}^{m} A_i \cong \prod_{i=1}^{m} R / A_i.
$$

Just as in the previous paragraph $(G, +, 0)$ is considered to be a finite additive group. The given general algorithm problem to solve is

$$
Q = kP
$$

for an existing, yet unknown integer $k$ and fixed elements $P$ and $Q$ in $G$. Obviously the order of the point $P$ given by $\#P = : N \in \mathbb{N}$ factors into primes i.e.

$$
N = \prod_{i=1}^{t} p_i^{\varepsilon_i},
$$

whereas the $p_i$’s are appropriate distinct primes, $\varepsilon_i$’s are appropriate positive integers and $t \in \mathbb{N}$.

The idea of the Pohlig-Hellman Method is to determine the values of a solving $k$ of the general discrete logarithm problem given in modulo $p_i^{\varepsilon_i}$ for all $i \in \{1, \ldots, t\}$. Obviously the Chinese Remainder Theorem then yields the solving $k$ modulo $N$. In order to determine

$$
k \mod p_i^{\varepsilon_i}
$$

for a fixed $i \in \{1, \ldots, t\}$, the corresponding prime $p_i$ needs to be considered. Furthermore $k$ can obviously be represented as

$$
k = \sum_{j=0}^{\infty} k_j p_i^j
$$

(8.3)

for appropriate integers $k_j \in \{0, \ldots, p_i - 1\}$. Moreover $k \mod p_i^{\varepsilon_i}$ is uniquely defined by $k_0, \ldots, k_{\varepsilon_i - 1}$, because for all $n \in \mathbb{N}$ it holds

$$
p_i^{\varepsilon_i + n} = p_i^{\varepsilon_i} p_i^n = 0 \times p_i^n = 0 \mod p_i^{\varepsilon_i}.
$$

(8.4)

Hence the Pohlig-Hellman Method aims to determine $k_0, \ldots, k_{\varepsilon_i - 1}$. In an application the Pohlig-Hellman Method would be repeatedly used for all $i \in \{1, \ldots, t\}$ and then the Chinese Remainder Theorem would be applied to determine $k \mod N$. This would finally yield a solving $k$ for a given general discrete logarithm problem.

Pohlig-Hellman Method

1. **INPUT** $(G, +, 0)$ finite additive group, $P \in G$, $Q \in G$, $\#P = : N \in \mathbb{N}$, prime $p$ dividing $N$, largest integer $\varepsilon$ such that $p^\varepsilon$ divides $N$

2. Set $r = 0$;

3. Set $Q_0 = Q$;

4. **While** $r < : \varepsilon - 1$

5. Determine $k_r$ such that $(N / p^{r+1}) \ast Q_r = k_r \ast (N / p) \ast P$;

6. **If** $r < : \varepsilon - 1$

7. **Calc and Save** $Q_{r+1} = Q_r - k_r \ast p^r \ast P$;

8. **End**

9. Set $r = r + 1$;

10. **End**

11. **OUTPUT** $k_0, \ldots, k_{\varepsilon-1}$
Proposition 8.12. The Pohlig-Hellman Method yields the desired elements \( k_0, \ldots, k_{\varepsilon-1} \) in finite time with

\[ k = \sum_{j=0}^{\varepsilon-1} k_j p^j \mod p \]

as an output in step sixteen whereas for all \( j \in \{0, \ldots, \varepsilon - 1\}, 0 \leq k_i < p \) is known according to step three and step fourteen.

Proof. According to step four it is obvious that at most \( \varepsilon \) loops are needed to be considered, before the algorithm terminates. Therefore the \( k_j \)'s are calculated in finitely many steps.

However, a closer look should be taken onto the Pohlig-Hellman Method, in order to understand why the \( k_j \)'s are of the desired form.

Firstly

\[
\begin{align*}
N \quad Q & = \sum_{j=0}^{\varepsilon-1} k_j p^j \\ p & = k_0 N \quad P + N \quad \phi(P) \\ \phi(P) & = k_0 N \quad p \quad \mod \quad p^\varepsilon.
\end{align*}
\]

Therefore step five determines the desired integer \( k_0 \) for the first While-loop of \( r = 0 \).

All of the other \( k_j \)'s are then recursively determined analogously. The first step of \( j = 0 \) was already done.

Now it is assumed that for a fixed \( r \in \{0, \ldots, \varepsilon - 1\} \) the appropriate \( k_0, \ldots, k_r \) were already determined. If \( r \neq \varepsilon - 1 \) then the next step is to determine \( k_{r+1} \). In order to do that another recursive correspondence will be firstly shown.

Claim. For all \( n \in \{0, \ldots, \varepsilon - 1\} \) it holds

\[
Q_n = \left( \sum_{j=n}^{\infty} k_j p^j \right) P. \tag{8.5}
\]

For \( n = 0 \) the claim holds trivially, because step three yields

\[
Q_0 = Q = kP = \left( \sum_{k=0}^{\infty} k_j p^j \right) P = \left( \sum_{k=n}^{\infty} k_j p^j \right) P.
\]

Thence it is now assumed that for a fixed \( n \in \{0, \ldots, \varepsilon - 1\} \) the claim already holds for all \( j \in \{0, \ldots, n\} \).

If \( n \neq \varepsilon - 1 \) it needs to be proven that the claim also holds for the case of \( n + 1 \) i.e.

\[
Q_{n+1} = \left( \sum_{j=n+1}^{\infty} k_j p^j \right) P
\]

needs to be proven. Step seven of the Pohlig-Hellman Method yields

\[
Q_{n+1} := Q_n - k_n p^n P.
\]

Since the claim already holds for \( Q_n \), this proves

\[
Q_{n+1} := Q_n - k_n p^n P = \left( \sum_{j=n}^{\infty} k_j p^j \right) P - k_n p^n P = \left( \sum_{n+1}^{\infty} k_j p^j \right) P.
\]
Having proven this claim, \( k_{r+1} \) can now be determined analogously to the case of \( r = 0 \), because

\[
\frac{N}{p^{r+1}} Q_{r+1} = \left( \sum_{j=0}^{r} k_j p^j \right) P = \frac{N}{p} \left( \sum_{j=r+1}^{\infty} k_j p^{j-(r+1)} \right) P = k_{r+1} \frac{N}{p} P + \frac{\sum_{j=r+1}^{\infty} k_j p^{j-(r+1)}}{p} NP
\]

\[
= k_{r+1} \frac{N}{p} P + \left( \sum_{j=r+1}^{\infty} k_j p^{j-(r+2)} \right) \cdot \frac{Np}{p} = k_{r+1} \frac{N}{p} P \mod p^r.
\]

Altogether this shows that the desired \( k_j \)'s with \( j \in \{0, \ldots, \varepsilon-1\} \) are determined by the algorithm. ■

Concluding this paragraph it is necessary to have a brief look onto the efficiency of the Pohlig-Hellman Method.

**Remark 8.13.** As proven in proposition 8.12 the Pohlig-Hellman Method finds appropriate integers \( k_0, \ldots, k_{\varepsilon-1} \) such that \( k = \sum_{j=0}^{\varepsilon-1} k_j p^j \mod p^\varepsilon \) whereas \( p \) is a prime dividing the order of the point \( P \) given by \( N \) and \( \varepsilon \) is the largest integer such that \( p^\varepsilon \) still divides \( N \).

As already mentioned in the introduction of this paragraph, the idea of the Pohlig-Hellman Method is to determine \( k_0^{(i)}, \ldots, k_{\varepsilon-1}^{(i)} \) for all \( i \)'s such that \( p_i^r \) is a prime power in the unique prime factorization of \( N \). Setting \( k^{(i)} := \sum_{j=0}^{\varepsilon-1} k_j^{(i)} p_i^j \) then yields for all \( i \)'s

\[
k = k^{(i)} \mod p_i^{r_i}
\]

simultaneously and the Chinese Remainder Theorem finally determines a \( k \) solving the given general discrete logarithm problem.

Carefully considering step five clarifies that determining a \( k_r \) such that

\[
\frac{N}{p^{r+1}} Q_r = k_r \left( \frac{N}{p} \right) P
\]

is a matter of solving another general discrete logarithm problem. Hence the rather difficult general discrete logarithm problem over \( G \) is translated into a more easy general discrete logarithm problem over a subgroup generated by \( \frac{N}{p} P \), which is of a smaller order \( p \).

Therefore in order to be efficient, it is desirable that the points’ order \( N \) factors into rather small primes \( p_i \), so that another attack as for example the Baby Step - Giant Step, as introduced in the previous paragraph, can be applied.

Hence when implementing elliptic curve crypto-systems, restricted elliptic curves whose group order factors into rather small primes should be avoided in order to be safe against attacks by the Pohlig-Hellman Method.

Summarizing this paragraph, another method of attacking a general discrete logarithm was introduced and carefully examined. It was proven that the algorithm does what it should and terminates in finitely many steps. Obviously this general attack can easily be applied to the case of an elliptic discrete logarithm problem by specifying the general finite additive group \((G, +, 0)\) into the finite additive abelian group of a restricted elliptic curve given by \((E(F_q), +, \infty)\) with \( q \) being the power of a prime \( p \).

8.2.3. **Index Calculus.**

The attack to be introduced in this paragraph focuses on attacking a classical discrete logarithm problem. Even though this specification might seem to be a disadvantage, the attack can still be applied to very general cases.

Moreover an attack will be introduced in the next paragraph which translates an elliptic curve discrete logarithm problem into a classical discrete logarithm problem. Hence, the Index Calculus attack introduced in this paragraph can then be applied.
For the setting of the considered classical discrete logarithm problem a prime $p$ and a finite field $\mathbb{F}_p$ need to be fixed. Moreover $g$ is set to be a primitive root in modulo $p$ i.e.

$$\mathbb{F}_p^* = \langle g \rangle.$$ 

Hence for all $h \in \mathbb{F}_p^*$ it exists a $k \in \mathbb{Z}$ such that $h = g^k \mod p$ with $k$ being unique modulo $p - 1$.

**Definition 8.14.** Let $p$ be a prime, $h$ in $\mathbb{F}_p^*$ and $g$ in $\mathbb{F}_p$ be a primitive root. Furthermore let $k \in \{0, \ldots, p - 2\}$ be the unique integer solving $h = g^k \mod p$. Then $k$ is called the discrete logarithm of $h$ with respect to $g$ and $p$ and is denoted as

$$L_{g,p}(h) := k \in \{0, \ldots, p - 1\}$$

i.e.

$$g^{L_{g,p}(h)} = h \mod p.$$

**Remark 8.15.** Therefore the map

$$L_{g,p} : \mathbb{F}_p^* \to \{0, \ldots, p - 2\}$$

$$h \mapsto L_{g,p}(h)$$

can be defined. Obviously $L_{g,p}$ is well-defined and injective. Furthermore for all $h_1$ and $h_2$ in $\mathbb{F}_p^*$ it holds

$$L_{g,p}(h_1 h_2) = L_{g,p}(h_1) + L_{g,p}(h_2).$$

**Proof.** Let $h_1$ and $h_2$ be arbitrary but fixed elements in $\mathbb{F}_p^*$. According to definition 8.14

$$g^{L_{g,p}(h_1 h_2)} = h_1 h_2 \mod p$$

is known on the one hand. Moreover

$$g^{L_{g,p}(h_1 h_2)} = g^{L_{g,p}(h_1) + L_{g,p}(h_2)} = h_1 h_2 \mod p$$

is known on the other hand. Altogether $g^{L_{g,p}(h_1 h_2)} = g^{L_{g,p}(h_1) + L_{g,p}(h_2)}$ mod $p$ and hence

$$L_{g,p}(h_1 h_2) = L_{g,p}(h_1) + L_{g,p}(h_2) \mod p - 1$$

due to $L_{g,p}$ being injective. 

The idea of the next attack, called the **Index Calculus**, is to use this property of the map $L_{g,p}$. The motivation is to determine the discrete logarithm with respect to $g$ and $p$ for several primes $p$ and to then use $L_{g,p}$ for determining the discrete logarithm for a product of those primes. This then yields a solution for the corresponding classical discrete logarithm problem. Such a set of primes $B$, whose discrete logarithms with respect to $g$ and $p \in B$ will be calculated, is in informatics called a **factor base**.

A pseudo code for solving the classical discrete logarithm problem

$$g^k = m \mod p$$

for an unknown, yet existing integer $k$ and an unique $m \in \{0, \ldots, p - 1\}$, using the Index Calculus will be introduced next.
Index Calculus

1. **INPUT** \(\mathbb{F}_p\) for a prime \(p\), primitive root \(g\) in \(\mathbb{F}_p\), factor base \(B := \{b_1, \ldots, b_n\}\) with \(n \in \mathbb{N}, m \in \{0, \ldots, p - 1\}\)
2. **While** not all \(L_{p,g}(b_i)\)'s with \(i \in \{0, \ldots, n\}\) are calculated and saved
3. Choose random \(s \geq 0\);
4. Calc and Save \(g^s \mod p\);
5. **If** \(g^s \mod p\) is equivalent to a plus or minus product of \(b_i\)'s
6. Save the used \(b_i\)'s and the integers \(\varepsilon_i\)'s with \(b_i \varepsilon_i\) being the highest power of \(b_i\) dividing the product;
7. **End**
8. Use the just found \(\varepsilon_i\)'s and the found integer \(s\) and already calculated \(L(b_i)\)'s to calculate and save another \(L(b_i)\) if possible
9. **End**
10. Set \(j = 0\);
11. **While** \(g^j m \mod p\) is not a plus or minus product of elements of \(B\)
12. Choose a random \(j \geq 0\);
13. Calc \(g^j m\);
14. Save \(j\);
15. **End**
16. Determine \(\gamma_1, \ldots, \gamma_n\) such that \(g^j m = \prod_{i=1}^{n} b_i^{\gamma_i} \mod p\);
17. Calc and Save \(L_{p,g}(m)\) using the \(\gamma_i\)'s, \(L_{p,g}(b_i)\)'s and \(j\);
18. **OUTPUT** \(L_{p,g}(m)\)

**Remark 8.16.** Obviously it is very important to chose the factor base \(B\) carefully.

On the one hand if the set \(B\) is chosen too small, it will be hard to succeed in the section of step two to step nine, because the attack might not terminate in finite steps or will need a long time to break this While-loop.

On the other hand if the factor base \(B\) is chosen too large, the same section might as well not terminate or take a huge amount of time to terminate, since many \(L_{p,g}(b)\)'s need to be calculated.

Choosing an efficient factor base \(B\) is the crux of the Index Calculus.

Nevertheless if an appropriate factor base \(B\) is chosen, it can be proven that the Index Calculus has a subexponential running time with respect to the underlying prime \(p\). This is fast compared with the already introduced Baby Step - Giant Step and the Pohlig-Hellman Method which both have an exponential running time with respect to the underlying group order. If applicable the Index Calculus is therefore more efficient.

For the purpose of understanding the Index Calculus better, it is indispensable to test the algorithm on an example.

**Example 8.17.** In this example the finite field \(\mathbb{F}_p\) for the prime \(p = 1217\) with the primitive root \(g = 3\) in modulo 1217 will be considered. The classical discrete logarithm problem given, is to find an existing, yet unknown integer \(k\) such that

\[3^k = 51 \mod 1217.\]

The Index Calculus will now be applied in order to solve that problem.

Therefore firstly a factor base \(B\) needs to be carefully chosen. Thus \(B := \{2, 3, 5\}\) is set. In the notation of the Index Calculus \(m = 51\) is set. Moreover the equations denoted as \(\pm\) stated next, need to be understood from an informatics point of view, where for example an "old" \(a\) is used to define a "new" \(a\) via "\(\pm\)".

The Index Calculus suggests to firstly determine \(L_{1217,3}(b)\) for all \(b \in B\).

Hence \(\pm 1\) is set first and \(g^s \mod p\) is calculated stating \(3^1 = 3 \mod 1217\). Therefore according to definition 8.14

\[L_{1217,3}(3) = 1 \mod 1216\]

is immediately known.

Nevertheless there are still \(b \in B\) existing with \(L_{1217,3}(b)\) not calculated yet. Thus another \(s\) is randomly chosen as step three suggests.

\[70\]
For example \( s \doteq 25 \). Hence \( 3^s = 3^{25} = 125 = 5^3 \) mod 1217 is obtained. Now remark 8.15 yields
\[
25 = L_{1217,3}(5^3) = 3L_{1217,3}(5) \text{ mod } 1216
\]
which implies
\[
L_{1217,3}(5) = 819 \text{ mod } 1216. \tag{8.6}
\]
It now remains to obtain the value of \( L_{1217,3}(2) \).
This time \( s \doteq 30 \) is randomly chosen and \( 3^s = 3^{30} = 1167 = -50 = -2 \cdot 5^2 \) mod 1217 is derived. Hence
\[
30 = L_{1217,3}(-2 \cdot 5^2) = L_{1217,3}(-1 \cdot 2 \cdot 5^2) = L_{1217,3}(-1) + L_{1217,3}(2) + 2L_{1217,3}(5)
\]
is known.
At this point it is important to emphasize that when working over \( \mathbb{F}_p \) for a prime \( p \), obviously \( g^p \equiv g \mod p \) for a primitive root \( g \). In this case
\[
3^{608} = 3^{-1} \mod 1217.
\]
Thus
\[
L_{1217,3}(-1) = 608 \text{ mod } 1216.
\]
Altogether
\[
30 = L_{1217,3}(-1) + L_{1217,3}(2) + 2 \cdot 819 = 608 + L_{1217,3}(2) + 422 \text{ mod } 1216
\]
is determined and so
\[
L_{1217,3}(2) = 216 \text{ mod } 1216 \tag{8.7}
\]
is determined.

The While-loop of step two to step nine now terminates and the Index Calculus continues to step ten, setting \( j \doteq 0 \) and calculating \( g^j m = m \mod p \).
On the one hand
\[
m = 51 = 3 \cdot 17 \mod 1217
\]
is not a product of primes of the factor base. On the other hand
\[
-51 = 1166 = 2 \cdot 11 \cdot 53 \mod 1217
\]
does not factor into primes of the factor base either.
At this point it is important to emphasize that if the factor base \( B \) would have included the prime 17, then the attack would have directly continued with step sixteen. However, \( L_{1217,3}(17) \) would have been needed to be determined in the first While-loop. Hence including 17 in \( B \) would have resolved in a large extra effort. Therefore it was decided to exclude 17 and try another random \( j \) in the section of step eleven to step fifteen instead.
For example \( j \doteq 3 \) is randomly tried next which shows
\[
g^j m = 3^3 \cdot 51 = 160 = 2^5 \cdot 5 \text{ mod } 1217
\]
whereas 2 and 5 are elements in the considered factor base \( B \). So it can be continued with step seventeen of determining \( L_{1217,3}(51) \). Since \( 3^3 \cdot 51 = 2^5 \cdot 5 \text{ mod } 1217 \) and because an integer \( k \) is known to exists such that \( 3^k = 51 \text{ mod } 1217 \),
\[
2^5 \cdot 5 = 3^3 \cdot 51 = 3^3 \cdot 3^k = 3^{3+k} \text{ mod } 1217
\]
can be observed. Now remark 8.15 yields
\[
3 + k = L_{1217,3}(2^5 \cdot 5) = 5L_{1217,3}(2) + L_{1217,3}(5) \text{ mod } 1216.
\]
Hence
\[
k = 5L_{1217,3}(2) + L_{1217,3}(5) - 3 \equiv 5 \cdot 216 + 819 - 3 = 680 \text{ mod } 1216. \tag{8.7}, (8.6)
\]
Altogether
\[
L_{1217,3}(51) = k = 680 \text{ mod } 1216
\]
solves the given classical discrete logarithm problem according to the Index Calculus.

All in all this paragraph introduced a method on attacking classical discrete logarithm problems. In the usage of the Index Calculus it was emphasized that choosing an appropriate factor base \( B \) is
very important. If such a factor base is chosen appropriately, the attack is known to terminate in a subexponentially increasing timespan for increasing primes $p$. It was also emphasized that the two earlier introduced algorithms terminate only with exponentially increasing time effort for increasing group orders.

8.2.4. MOV-Attack.

Even though the Index Calculus only attacks classical discrete logarithm problems, it can still be useful for attacking general discrete logarithm problems. A well-known attack which translates elliptic discrete logarithm problems into classical discrete logarithm problems is the so-called MOV-Attack. This attack was invented and named after A. Menezes, T. Okamoto and S.A. Vanstone.

The idea of this method is to use a Weil-Pairing over elliptic curves to translate an elliptic discrete logarithm problem into a classical discrete logarithm problem. Therefore let $q$ be a power of a prime $p$ and a restricted elliptic curve $E(F_q)$ is considered. Moreover let $P$ and $Q$ be elements in $E(F_q)$ such that for $N := \text{ord}(P)$ it holds $\gcd(N, q) = 1$. So especially $\text{ord}(P) \nmid \text{char}(F_q)$.

The given elliptic discrete logarithm is to find an existing, yet unknown integer $k$ such that $kP = Q$ over $E(F_q)$.

Furthermore an appropriate positive integer $m$ such that

$$E[N] \subseteq E(F_{q^m})$$

needs to be fixed. Such a $m$ exists, because of each non-trivial $N$-torsion point having coordinates in $F_q = \bigcup_{j \in \mathbb{N}} F_{q^j}$ with $F_{q^j} \subseteq F_{q^{j+1}}$ for all $j \in \mathbb{N}$ and due to $\#E[N] < \infty$.

**MOV-Attack**

1. **INPUT** restricted elliptic curve $E(F_q)$, $P \in E(F_q)$, $Q \in E(F_q)$, $N := \text{ord}(P) \in \mathbb{N}$, $m \in \mathbb{N}_0$ such that $E[N] \subseteq E(F_{q^m})$
2. Set $d_0 = 1$
3. Set $c = 0$
4. While $\text{lcm}(d_0, \ldots, d_c) \neq N$
5. $c = c + 1$
6. Randomly fix $T \in E(F_{q^m})$
7. Calc and Save $M = \text{ord}(T)$
8. Calc and Save $d_c = \gcd(M, N)$
9. Calc and Save $S = (M/(d_c)) \ast T$
10. Calc and Save $\xi = e_N(P, S)$
11. Calc and Save $\eta = e_N(Q, S)$
12. Determine $k_c$ such that $\xi^{k_c} = \eta$ over $F_{q^m}$
13. **End**
14. Knowing $k = k_c \mod d_c$ for all $c$'s, determine $k$ modulo $N$
15. **OUTPUT** $k$
It is now important to examine what exactly the MOV-Attack does and why it terminates in finitely many steps.
The idea is to translate points in \(E[N]\) into elements in \(\mathbb{F}_{q^m}\) using a Weil-Pairing and its properties. This then yields a classical discrete logarithm problem which can be attacked by the Index Calculus.

**Proposition 8.18.** The MOV-Attack determines an integer solving the given elliptic discrete logarithm problem.

**Proof.** Firstly step six needs to be considered, which suggest randomly choosing a point \(T\) in \(E(\mathbb{F}_{q^m})\). Next in step seven

\[ M := \text{ord}(T) \]

is determined and in step eight

\[ d_c := \gcd(M, N) = \gcd(\text{ord}(T), \text{ord}(P)) \]

is set for a fixed index \(c \in \mathbb{N}_0\) of step five. Thus \(d_c\) obviously divides \(M\). Hence setting

\[ S := \frac{\text{ord}(T)}{d_c} \cdot T \quad \in \mathbb{E}(\mathbb{F}_{q^m}) \]

yields a point in \(E(\mathbb{F}_{q^m})\). Moreover

\[ NS = \frac{N \cdot \text{ord}(T)}{d_c} T = \frac{N \cdot M}{\gcd(M, N)} T = \text{lcm}(M, N) T = \infty, \]

since \(M = \text{ord}(T)\) and \(M \mid \text{lcm}(M, N)\). Thus \(S\) is a \(N\)-torsion point with \(\text{ord}(S) = d_c\) according to step eight.

Hence it is possible to apply a Weil-Pairing to \((P, S)\) and \((Q, S)\) as done in step ten and eleven which yields

\[ \xi := e_N(P, S) \]

and

\[ \eta := e_N(Q, S). \]

Obviously

\[ \xi^{d_c} = e_N(P, S)^{d_c} = e_N(P, d_c S) = e_N(P, \infty) = 1 \]

and analogously

\[ \eta^{d_c} = 1. \]

Hence \(\xi\) and \(\eta\) are elements in \(\mu_{d_c} \subseteq \mu_N \subseteq \mathbb{F}_{q^m}\) on the one hand.

On the other hand \(\xi\) and \(\eta\) are known to not be units in \(\mathbb{F}_{q^m}\), since a Weil-Pairing is non-degenerate in each variable. So together with property (1.) of a Weil-Pairing

\[ \eta := e_N(Q, S) \quad \overset{Q = kP}{=} e_N(kP, S) = e_N(P, S)^k = \xi^k \]

in \(\mu_{d_c}\).

Hence a solving integer \(k \mod d_c\) given by \(k_c\) for this classical discrete logarithm problem can be determined as done in step twelve. For example the Index Calculus could be used to determine \(k \mod d_c\) resulting in \(k_c\). This procedure is repeated for rising indices \(c\) until the least common multiple of all determined \(d_c\)’s equals \(N\). This will happen in finite time as proposition 8.19 will prove.

Lastly in step fourteen

\[ k \mod N \]

can be determined, which simultaneously solves

\[ k \equiv k_c \mod d_c \]

for all \(c\)’s, since the least common multiple of all \(d_c\)’s is assumed to be equal \(N\). Such a determination of \(k \mod N\) can for example be done using the Chinese Remainder Theorem.
Altogether the output variable $k$ in step fifteen is obviously a solving integer $k$ modulo $N$ for

$$kP = Q$$

over the given restricted elliptic curve $E(\mathbb{F}_q)$.

The question of the MOV-Attack terminating in finitely many steps, can easily be answered, by having a closer look onto the While-loop started in step four.

**Proposition 8.19.** The MOV-Attack terminates in finite time.

**Proof.** Considering step eight it is obvious that each $d_c$ will always divide $N$ and thus the least common multiple of all found $d_c$’s in a current loop needs to divide $N$.

Moreover since $E[N]$ is a subgroup of the finite restricted elliptic curve $E(\mathbb{F}_{q^m})$ and since $E[N]$ is of the group order $N := \text{ord}(P)$ for the given $P \in E[N] \subseteq E(\mathbb{F}_{q^m})$, at some point the randomly chosen $T$ of step six needs to be equal to $P$. In this case $d_c = N$ will be set and the While-loop terminates in finitely many steps.

Nevertheless, it might happen that the While-loop terminates before the random choice of $P$ is done.

All in all in this paragraph a fourth attack was introduced which aims to solve a given elliptic discrete logarithm problem. This attack translates an elliptic discrete logarithm problem into a classical discrete logarithm problem which can then be attacked by the Index Calculus introduced in paragraph 8.2.3. Since the Index Calculus is considered to be efficient, this guarantees a high level of efficiency for the MOV-Attack as well.

However, the MOV-Attack can only be usefully applied when the integer $m$ can be chosen such that $\mathbb{F}_{q^m}$ is not much larger than $\mathbb{F}_q$. Thus it was pointed out that in order to be invulnerable to the MOV-Attack, the class of supersingular elliptic curves needs to be avoided.
9. INTRODUCTION TO THE PRINCIPLES OF CRYPTO-SYSTEMS

So far the term of a crypto-system was only vaguely used. However, since this thesis aims to apply elliptic curves in key-exchange cryptography it is necessary to introduce the principles of key-exchange crypto-systems in more detail. Therefore the world of informatics needs to be scratched in order to define the most important types of crypto-systems.

Firstly a public key crypto-system is a system whose goal is to establish two distinct keys $E$ and $D$ whereas $E$ works as the encryption key and $D$ as the decryption key. Obviously it should be relatively simple to derive $E$ from $D$ so that everybody e.g. a private person wanting to transmit bank related information to the institute, can encrypt its information safely. However, deriving $D$ from $E$ should be nearly infeasible so that nobody can decrypt a secret message except the person actually having the decryption key. In our example the bank institute would be the only party having the decryption key and being able to decrypt the information transmitted. Altogether in a public key crypto-system the key $E$ should be safe enough to be made public without compromising $D$ which should be kept private. The eavesdropper’s challenge lays within solving this hard problem of actually getting the decryption key $D$.

Secondly a public key distribution system is a systems which enables two or more parties to communicate back and forth publicly, in order to establish a common key which can simultaneously be used for encryption and decryption. The main concern of such a system is to secure that the public communication between the parties does not reveal enough information for an eavesdropper to be able to derive the established key.

Thirdly a privacy system is a public system between two or more parties which prevents the extraction of information by an eavesdropper. Such a system ensures that only the intended reader is able to correctly receive the sent message.

Moreover the terms of public and private channels need to be defined.

A public channel is a channel over which two or more parties communicate. However, the channel itself is not secure enough for the intended needs.

For example a blackboard might not seem secure enough to transmit bank account information, since anybody would be able to read the pin. The blackboard would therefore be considered a public channel.

At the same time a blackboard would be considered secure enough for transmitting the date time for lunch, since it does not matter if anybody unintended reads this message. In that case the blackboard is not a public channel.

Keeping that example in mind, it is obvious that the term of a public channel depends on the involved parties, their needs and the intention of the to-be-exchanged message.

Any channel, which is not considered a public channel, is called a private channel.
As can be seen in figure 6, the aim of a crypto-system is to transmit a message, the so-called plaintext $P$, via public channels to a receiver. However, the plaintext shall be kept secret and therefore has to be encrypted by the transmitter into $S_k(P)$. This encryption $S_k$ is done in private and then send publicly to the receiver. The intended receiver is able to do the decryption $S_k^{-1}$ which is done in private and yields $S_k^{-1}(S_k(P)) = P$. Hence the receiver obtains the original plaintext $P$.

Obviously both parties need a common key $k$ which simultaneously yields the encryption $S_k$ and the decryption $S_k^{-1}$. This key must be established in a way such that $S_k$ can be made public (so that both parties can encrypt) without compromising the decryption $S_k^{-1}$.

The eavesdropper challenge is to decrypt $S_k(P)$ without actually knowing $S_k^{-1}$. In the case of $n \in \mathbb{N}_{\geq 2}$ parties, $n^2/2$ keys are needed in a systematic as proposed in figure 6. Thus let $K := \{\text{keys}\}$ be the set of keys established in a key-exchange crypto-system, then the family of maps $\{S_k\}_{k \in K}$ with

$$S_k: \{\text{plaintexts}\} \rightarrow \{\text{encrypted texts}\}$$

such that $S_k^{-1}$ does exist, is called a cryptographic system.

As for simplicity in this thesis only cryptographic systems of cardinality equal one will be considered. The aim of this thesis is to point out methods over elliptic curves for establishing a common key $k$ which can then be used in other methods to establish appropriate $S_k$’s and $S_k^{-1}$’s. Obviously it is hard secure 100% of safety, as most systems can be cracked. Hence between two types of security needs to be distinguished.

On the one hand a system is said to be computationally secure, if it relies on the fact that a huge amount of operations, steps, storage space and/or time are needed to successfully crack the system. Thus such a system is computational infeasible and so it is hoped to be secure against most attacks. However, in an idealistic world it could be compromised.

On the other hand a system can be considered unconditionally secure. Such a system is provenly secure and can not be cracked at all. Proofs of unconditional security are done by logical and mathematical argumentations. An example for a system in key-exchange cryptography which is unconditionally secure, is the one time pad system. However, it requires enormously large keys and is therefore very impractical.

Key-exchange crypto-systems using elliptic curves are not provenly secure. Nevertheless, as will be shown in the next chapter, they are assumed to belong to the class of the computational secure systems. In order to compromise an elliptic curve key-exchange crypto-system it is assumed (not proven yet!) that an elliptic discrete logarithm problem needs to be solved. This is considered (not proven yet!) to be nearly infeasible over appropriate restricted elliptic curves.
Lastly the step of establishing a key-exchange crypto-system can be made. There are different ideas of establishing such a system existing, of which three will be introduced in the next three chapters. In this chapter the most common key-exchange crypto-system will be introduced.

In subsection 10.1 the original system as introduced for the most general setting possible will be given. Therefore a pseudo-code will be given and it will be explained, why this key-exchange crypto-system is considered to be secure and efficient.

Moreover in subsection 10.2 the general Diffie-Hellman-Key-Exchange crypto-system will be adapted to the case of elliptic curves and the most important advantages respectively disadvantages of this system will be pointed out.


One of the most famous key-exchange crypto-system was introduced by W. Diffie and M. E. Hellman in the last half of the twentieth century. Together they invented a method which is today known as the Diffie-Hellman-Key-Exchange. In order to understand how their crypto-system works, the considered problem firstly needs to be introduced.

As pointed out in the previous section, the aim of a crypto-system is enabling one party to safely transmit a secret encryption key via insecure channels to another party. What was in the mid age a matter of how to get a well-trained soldier from A to B without getting murdered and the key stolen, evolved into a matter of how to avoid hackers on cracking your encryption code, when for example executing online banking.

The following method is the original one as introduced by W. Diffie and M. E. Hellman and proposes a public key distribution system over finite fields in general. It shows how two parties named Alice and Bob can establish a common private key via an insecure public channel using the advantages of a finite field.

This established common key can then be used in other methods in order to establish a public key crypto-system which induces a privacy system.

<table>
<thead>
<tr>
<th>Diffie-Hellman-Key-Exchange</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>SETTING</strong></td>
</tr>
<tr>
<td>2.</td>
</tr>
<tr>
<td>3. Alice: Randomly choose $A \in {1, \ldots, p-1}$</td>
</tr>
<tr>
<td>4. Calculate $Y_A := \alpha^A \mod p$</td>
</tr>
<tr>
<td>5. Bob: Randomly choose $B \in {1, \ldots, p-1}$</td>
</tr>
<tr>
<td>6. Calculate $Y_B := \alpha^B \mod p$</td>
</tr>
<tr>
<td>7. Alice: Send $Y_A$ to Bob</td>
</tr>
<tr>
<td>8. Bob: Send $Y_B$ to Alice</td>
</tr>
<tr>
<td>9. Alice: Calculate $Y_B^A \mod p$</td>
</tr>
<tr>
<td>10. Bob: Calculate $Y_A^B \mod p$</td>
</tr>
</tbody>
</table>

In step one and two the setting of the distribution system gets publicly defined. In the third respectively fifth step Alice respectively Bob both define their private keys which are kept secret. Next in step four respectively step six both determine elements $Y_A$ respectively $Y_B$ corresponding to their private keys which get made public in the exchange done in step seven and eight.

After the public exchange is executed, both take their partner’s element to the power of their private key modulo the prime $p$ in step nine and ten.
In the end Alice and Bob have the same common key, because
\[ Y_A^B = (\alpha^B)^A = Y_A^B = (\alpha^A)^B = Y_B^A, \]
over \( GF(p) \). Hence
\[ K := \alpha^{AB} \mod p \]
is the publicly established common private key \( K \).

However, the eavesdropper Eave only has the information \( p, \alpha, Y_A \) and \( Y_B \). In order to get the common key \( K \) Eave needs to solve
\[ K = \alpha^{AB} \mod p. \]
Since Eave does not have the information \( A \) nor \( B \), this problem translates into solving
\[ K := \alpha^{AB} = \alpha^{A \log_\alpha(Y_B)} = (\alpha^A)^{\log_\alpha(Y_B)} = Y_A^{\log_\alpha(Y_B)} \mod p. \]

Obviously this is the earlier introduced general discrete logarithm problem of chapter 8 and thus is considered to be nearly infeasible to solve. It is assumed that in a best case scenario \( \sqrt{p} \) operations are needed to solve such a general discrete logarithm problem, when it was chosen hard enough.

This is the reason, why the introduced procedure is considered to be highly secure in terms of computationally security. However, it needs to be pointed out that solving the general discrete logarithm problem was not proven to be the only way of getting \( K \). Maybe there is another way existing, which only might not have been found yet. Nevertheless this seems unlikely.

Moreover it was not proven yet that a hard general discrete logarithm problem really guarantees high security.

Furthermore being 100% sure that a chosen general discrete logarithm problem is really nearly infeasible to solve, can never be guaranteed. As was emphasized in chapter 8 there are algorithms existing which can solve a discrete logarithm problem, when the right criteria are met. Even though such cases are tried to be avoided, there might be other algorithms existing which are either not invented yet or were not made public so far. Unfortunately a criteria securing 100% infeasibility of a discrete logarithm problems was not found yet.

Moreover it is important to emphasize the huge difference in effort needed to do the calculations in step four and six by Alice and Bob versus the effort needed to solve the discrete logarithm problem by Eave.

Supposing \( p \) being a prime and \( b \) being the smallest integer such that \( 2^b \geq p \), the calculations in step four and six are known to be solvable in at most
\[ 2 \log_2(2^b) = 2b \]
steps at its worst. Meanwhile the discrete logarithm problem can at its best be solved in
\[ \sqrt{2^{2b}} \]
steps. Therefore the effort needed to do the calculations of step four and six increases linear for an increasing prime \( p \), whereas the effort needed to solve the eavesdropper challenge increases exponentially for an increasing prime \( p \). Due to that enormous difference in effort needed for increasing primes \( p \), finite fields with huge prime characteristics \( p \) are implemented nowadays. This guarantees an even higher level of computational security.

All in all this section introduced the original idea of the Diffie-Hellman-Key-Exchange over finite fields. This method is very easy to understand and seems to induce a high level of security. Moreover this method can be easily adapted to the case of restricted elliptic curves.

### 10.2. Diffie-Hellman-Key-Exchange in elliptic curve cryptography.

As already mentioned at the end of the previous section, it is possible to adapt the idea of the classical Diffie-Hellman-Key-Exchange to the case of restricted elliptic curves. It was V. S. Miller who firstly translated the Diffie-Hellman-Key-Exchange method into the language of elliptic curves. This method is nowadays known as the Elliptic-Curve-Diffie-Hellman-Key-Exchange and is currently widely used, as for example in data exchange.
**Elliptic-Curve-Diffie-Hellman-Key-Exchange**

1. **SETTING**
   Set a prime \( p \) and a restricted elliptic curve \( E(\mathbb{F}_p) \)

2. Fix \( P \in E(\mathbb{F}_p) \)

3. Alice: Choose (randomly) \( a \in \mathbb{Z} \)

4. Calculate \( P_a := aP \mod p \)

5. Bob: Choose (randomly) \( b \in \mathbb{Z} \)

6. Calculate \( P_b := bP \mod p \)

7. Alice: Send \( P_a \) to Bob

8. Bob: Send \( P_b \) to Alice

9. Alice: Calculate \( aP_b \mod p \)

10. Bob: Calculate \( bP_a \mod p \)

Analogously to the general case a private common key gets established which is hard to be derived when only knowing \( p, E(\mathbb{F}_p), P, P_a \) and \( P_b \).

Aiming to compromise this crypto-system, an eavesdropper needs to determine \( abP \), when only knowing \( P, aP, bP \) with \( a, b \) being integers and the restricted elliptic curve \( E(\mathbb{F}_p) \). This problem is referred to as the Diffie-Hellman Problem.

In order to secure an even higher level of safety the above crypto-system can be optimized by a careful choice of the input parameters \( p, E(\mathbb{F}_p) \) and \( P \). The main concern lays within guaranteeing an elliptic curve \( E(\mathbb{F}_p) \) over which the elliptic discrete logarithm problem induced by the crypto-system is as hard as possible.

Recalling chapter 8 at least a restricted elliptic curve which is not supersingular and whose group order is neither small or factors into small primes only, should be chosen. On top of that even more criteria are known which secure an even harder to solve elliptic discrete logarithm problem.

In terms of efficiency the calculations done in step four and six can be implemented using the method of successive doubling which was introduced in subsection 7.1. On top of that all observations of the general case hold for the special case of restricted elliptic curve as well. For example a huge difference in effort needed by Alice and Bob versus Eave can be secured by choosing a restricted elliptic curve of a large group order.

All in all the Elliptic-Curve-Diffie-Hellman-Key-Exchange induces public key distribution system which is assumed to be computationally secure. All calculations done in that crypto-system are rather easy to be done for the two involved parties and are extremely hard to be done by a potential eavesdropper.

Moreover there are not many people existing that have a broad enough knowledge to understand the mathematics behind this algorithm. Thus it is unlikely for some random person to compromise such an established key distribution system. Since the implementation of such a key distribution system can, however, be done efficiently very few storage space is needed.

Nevertheless, those advantages might as well evolve into disadvantages. Since most people are not able to implement such crypto-systems, they need to use crypto-systems provided by a company called NIST. This yields the danger of an abuse by experts. On top of that, this system is only assumed to be computationally secure, but the proof is still missing. Obviously the proof of the system being unconditionally secure was neither found so far.

Summing up, this subsection explained the adaption of the classical Diffie-Hellman-Key-Exchange in elliptic curve cryptography and the most important advantages and disadvantages were shortly pointed out.
11. The Massey-Omura Encryption

Independently of the classical Diffie-Hellman-Key-Exchange J. Massey and J. K. Omura introduced another public key distribution system which enables a party Alice to transmit a secret plaintext $P$ to another party Bob. This secret message $P$ will in most cases be a key which functions as a private common key for Alice and Bob.

It was N. Koblitz who applied the procedure of J. Massey and J. K. Omura in elliptic curve cryptography. This public key distribution system introduced by N. Koblitz is known as the **Massey-Omura Encryption** over restricted elliptic curves.

**Massey-Omura Encryption**

1. **SETTING**
   - Set a prime $p$ and a restricted elliptic curve $E(\mathbb{F}_p)$
2. Determine $N := \#E(\mathbb{F}_p)$
3. Alice: Fix $P \in E(\mathbb{F}_p)$
4. Calculate $P_A := m_A P$
5. Send $P_A$ to Bob
6. Bob: Choose $m_B \in \mathbb{Z}_N$ such that $\gcd(m_B, N) = 1$
7. Calculate $P_B := m_B P_A$
8. Send $P_B$ to Alice
9. Alice: Calculate $P'_A := m_A^{-1} P_B$
10. Send $P'_A$ to Bob
11. Bob: Calculate $P'_B := m_B^{-1} P'_A$

Obviously the first two steps are just specifying the setting. Those steps are done publicly, thus an eavesdropper has the knowledge of the used restricted elliptic curve $E(\mathbb{F}_p)$ over a known prime $p$ and the order $N$ of that curve.

In the third step Alice fixes her secret plaintext $P$ which she wants to transmit to Bob. This message is set to be a point in the restricted elliptic curve and will in most cases function as a common key which shall be established.

In the fourth step Alices secretly chooses her private key $m_A \in \mathbb{Z}_N$ whereas she makes sure that $\gcd(m_A, N) = 1$. This ensures the existence of $m_A^{-1}$ in $\mathbb{Z}_N$. She then encrypts $P$ by calculating

$$P_A := m_A P$$

in step five. Next she sends $P_A$ to Bob in step six. Thus only an encrypted version of $P$ is made public.

Metaphorically speaking, Alice puts her secret message $P$ into a box and seals the box with her own lock $m_A$. This locked box is publicly send to Bob.

In step seven Bob starts to do the same as Alice before. First he chooses a private key $m_B \in \mathbb{Z}_N$ such that $\gcd(m_B, N) = 1$ and then determines

$$P_B := m_B P_A.$$  \hspace{1cm} (11.2)

This $P_B$ is send back to Alice.

In the introduced example Bob takes the locked box and puts a second lock, his own lock $m_B$, on it. Then he sends the twice locked box back to Alice.

In step ten Alice takes her old lock off in private. This is done by calculating

$$P'_A := m_A^{-1} P_B,$$

because

$$P'_A := m_A^{-1} P_B = m_A^{-1} m_B m_A P = m_B P.$$  \hspace{1cm} (11.3)

Thus the secret message is now only locked by Bobs seal. Next Alice publicly sends the once locked box $P'_A$ back to Bob.
Lastly in step twelve Bob finally takes his own lock off by calculating
\[ P_B' := m_B^{-1} P_A'. \]
This leaves Bob with
\[ P_B' := m_B^{-1} P_A' = m_B^{-1} m_B P = P \]
the secret message of Alice.
Thus a common \( P \) was established via public channels. However, \( P \) was encrypted throughout the whole procedure.

The only information an eavesdropper has are \( p, E(\mathbb{F}_p), N, P_A = m_A P, P_B = m_B m_A P \) and \( P_A' = m_A^{-1} m_B m_A P \). Setting \( M := m_B m_A P \) the eavesdropper therefore knows \( p, E(\mathbb{F}_p), N, m_B^{-1} M, m_A^{-1} M \) and \( M \) and wants to determine
\[ m_A^{-1} m_B^{-1} M \]
for existing, but unknown integers \( m_A^{-1} \) and \( m_B^{-1} \). This problem is obviously the Diffie-Hellman Problem introduced in the previous chapter. Therefore this method can be assumed to be quite computationally secure by an alike argumentation as already done.

To put it all in a nutshell, this chapter showed how the idea of W. Diffie and M.E. Hellman to induce a hard Diffie-Hellman Problem over elliptic curves, was used in a completely different crypto-system introduced by J. Massey and J.K. Omura. Just like the Elliptic-Curve-Diffie-Hellman-Key-Exchange, this crypto-system is not provenly secure. However, it seems as if nobody was able to successfully attack such a crypto-system so far. Hence they are widely used nowadays.
12. The Crypto-System of ElGamal

Uninfluenced by the two already introduced crypto-systems of chapter 10 and chapter 11 T. ElGamal invented another public key distribution system. This crypto-system was proposed in a very general way and can easily be adapted to the case of restricted elliptic curves.

### Classical ElGamal

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>SETTING</strong></td>
<td>Fix a large prime $p$, a primitive root $\alpha \mod p$</td>
</tr>
<tr>
<td>2. <strong>Alice:</strong></td>
<td>Fix $X_A \in \mathbb{Z}$</td>
</tr>
<tr>
<td>3. <strong>Bob:</strong></td>
<td>Fix $X_B \in \mathbb{Z}$</td>
</tr>
<tr>
<td>4. <strong>Alice:</strong></td>
<td>Fix $P$ such that $0 \leq P &lt; p$</td>
</tr>
<tr>
<td>5. <strong>Bob:</strong></td>
<td>Calculate $Y_B = \alpha^{X_B} \mod p$</td>
</tr>
<tr>
<td>6. <strong>Alice:</strong></td>
<td>Send $Y_B$ to Alice</td>
</tr>
<tr>
<td>7. <strong>Alice:</strong></td>
<td>Randomly choose $k \in {0, \ldots, p-1}$</td>
</tr>
<tr>
<td>8. <strong>Alice:</strong></td>
<td>Calculate $K = Y_B^k \mod p$</td>
</tr>
<tr>
<td>9. <strong>Alice:</strong></td>
<td>Calculate $c_1 = \alpha^k \mod p$</td>
</tr>
<tr>
<td>10. <strong>Alice:</strong></td>
<td>Calculate $c_2 = PK \mod p$</td>
</tr>
<tr>
<td>11. <strong>Alice:</strong></td>
<td>Send $c_1$ and $c_2$ to Bob</td>
</tr>
</tbody>
</table>

Carefully examining this public key distribution system, it gets obvious that a common key is established. Firstly in step one the setting of the system is defined publicly. Then in step two Alice secretly chooses her private key $X_A \in \mathbb{Z}$ and in step three defines the secret message $P$. This could for example be a common key which she wants to transmit to Bob. Moreover Bob needs to choose a private key $X_B \in \mathbb{Z}$ himself, as he does in step four. Furthermore in step five he determines $Y_B$ in private using the public $\alpha$ and his private key $X_B$. He then send $Y_B$ publicly to Alice. In step seven Alice chooses a random $k \in \{0, \ldots, p-1\}$ which she will keep secret all the time. Using this $k$ she establishes $K$. This $K$ is used in step nine and ten to determine $c_1$ and $c_2$. Those are next publicly send to Bob. In the end Bob knows $c_1$ and $c_2$, which he can use to firstly obtain $K$ and then secondly the secret message $P$. Knowing his private key $X_B$ he can easily determine $c_1^{X_B} \mod p$.

This yields

$$c_1^{X_B} = (\alpha^k)^{X_B} = (\alpha^{X_B})^k = Y_B^k \equiv K \mod p$$

whereas the small numbers emphasize the used steps of the Classical ElGamal. Therefore Bob provenly derives $K$.

Since $\alpha$ was chosen to be a primitive root modulo $p$ it is possible to determine $K^{-1} = (\alpha^{X_B})^{-1}$. Hence Bob is able to calculate $c_2K^{-1}$ and so with step ten he derives

$$c_2K^{-1} = PKK^{-1} = P \mod p.$$ 

All in all Bob was able to get the secret message $P$.

However, an eavesdropper can not as easily derive $P$ as Bob did, since the private key $X_B$ of Bob is unknown. The only information an eavesdropper has, are those being made public given by $p$, $\alpha$, $Y_B$, $c_1$ and $c_2$.

Just like for the Massey-Omura Encryption system, it was N. Koblitz who translated the Classical ElGamal system into the language of elliptic curve.
Elliptic ElGamal

1. **SETTING**
   Select a prime $p$ and a restricted elliptic curve $E(\mathbb{F}_p)$

2. Fix $R \in E(\mathbb{F}_p)$ such that $\text{ord}(R)$ is a large prime

3. **Alice**: Randomly choose $k \in \mathbb{Z}$

4. Fix $P \in E(\mathbb{F}_p)$

5. **Bob**: Fix $s \in \mathbb{Z}$

6. Calculate $B = sR$

7. Send $B$ to Alice

8. **Alice**: Calculate $P_1 = kR$

9. Calculate $P_2 = P + kB$

10. Send $P_1$ and $P_2$ to Bob

This crypto-system works analogously to the Classical ElGamal whereas $k$ functions as Alice’s private key and $s$ as Bob’s. Again $P$ is the secret plaintext of Alice which can easily be derived by Bob. Just as before Bob uses $P_1$ and $P_2$ in order to derive $P$. To do that he uses his private key $s$ and determines

$$P_2 - sP_1$$

over the restricted elliptic curve. This yields

$$P_2 - sP_1 = P + kB - s(kR) = P + kB - k(sR) = P + kB - kB = P$$

whereas the small numbers emphasize the used steps of the Elliptic ElGamal.

However, an eavesdropper only knows the publicly established $p$, $E(\mathbb{F}_p)$, $R$, $B = sR$, $P_1 = kR$ and $P_2$. In order to derive the secret message $P$ an eavesdropper therefore needs to solve

$$P_1 = kR$$

in order to firstly obtain $k$. Solving this is a matter of solving an elliptic discrete logarithm problem which is assumed to be nearly infeasible to solve. Therefore this system is assumed to be highly computationally secure. If an eavesdropper would be able to solve this problem, according to step two

$$P_2 - kB = P + kB - kB = P$$

could easily be derived. Hence it is very important for Alice to keep $k$ secret.

Furthermore it is important that Alice and Bob use a different $k$ respectively $s$ each time. To verify that Alice is assumed to use the same private key $k$ twice for two messages $P$ and $P'$. Bob simultaneously uses his private key $s$ twice.

Unfortunately in step eight Alice derives

$$P_1' = kR = P_1$$

twice. An eavesdropper might notices that the same $P_1$ (respectively $P_1'$) is send in two different procedures. Moreover in step six

$$B' = sR = B$$

is derived by Bob and so $B$ (respectively $B'$) is also send twice. Now an eavesdropper is able to determine

$$P_2' - P_2 = P' + kB' - P - kB = P' - P$$

with step nine. If one of the two message (for example $P$) gets made public at some point (for example in the news when considering governmental transfers) an eavesdropper only needs to determine

$$P_2' - P_2 + P = P' - P + P = P'$$

in order to obtain the other secret message $P'$. To avoid such a compromise of the established system, it is necessary for both parties to each time chose another private key, because it is assumed that the two parties do not have any contact except in the crypto-system.

All in all the just introduced method uses the assumed hardness of an elliptic discrete logarithm problem to secure a high level of computational security. However, this method is not as commonly used as the Elliptic-Curve-Diffie-Hellman-Key-Exchange or the Massey-Omura Encryption, due to the need of new private keys for both parties in every usage of the established crypto-system.
Deutschsprachige Zusammenfassung


Nachdem Kapitel 1 zunächst kurze die Thematik dieser Arbeit einführt und Kapitel 2 die Danksagungen enthält, setzt sich der erste Teil dieser Arbeit aus Kapitel 3 bis Kapitel 6 zusammen und konzentriert sich auf die Einführung der mathematischen Grundlagen elliptischer Kurven. Der zweite Teil besteht aus Kapitel 7 bis Kapitel 12 und wendet die Prinzipien des ersten Teiles in der Kryptographie an.

In Kapitel 3 werden zunächst elliptisch Curven formal definiert und näher betrachtet. Dieses Kapitel setzt sich aus drei Unterkapiteln zusammen.


In der Definition einer elliptischen Kurve als Menge, wird das spezielles Element 1 verwendet. Dieses wird in Unterkapitel 3.2 näher beleuchtet. Da eine elliptische Curve (ohne 1) als eine affine Varietät verstanden werden kann, ist es möglich, diese in die entsprechende projektive Ebene als projektive Varietät einzubetten. Somit kann als Punkt im Unendlichen verstanden werden. Dies wird in Unterkapitel 3.2 detailliert erklärt.

Schlussendlich wird in Unterkapitel 3.3 eine binäre Rechenoperation auf der Menge einer elliptischen Curve eingeführt. Insbesondere wird bewiesen, dass die Menge einer elliptischen Curve zusammen mit dieser Operation eine additive abelsche Gruppe bildet. Diese Operation scheint zunächst willkürlich gewählt zu sein. Jedoch ist sie geometrisch motiviert, was anhand zweier Beispiele erläutert wird. Von diesem Moment an, werden elliptische Curven immer als additive abelsche Gruppe versehen mit ebendieser Operation aufgesetz.

Nachdem die Gruppe einer elliptischen Curve eingeführt wurde, wird in Kapitel 4 das algebraischen Konzept von Endomorphismen auf elliptische Curven übertragen. Hierfür gliedert sich Kapitel 4 in drei Unterkapiteln auf.

Dadurch ist es dann auch möglich, weitere Begriffe, wie den Grad eines Endomorphismus, einzuführen. Des Weiter ermöglicht dies die Unterscheidung in separable und inseparable Endomorphismen.


Ähnlich wie Kapitel 4 zielt auch Kapitel 5 darauf ab, ein grundlegendes mathematisches Konzept - jenes über Torsionselemente - in die Sprache elliptischer Kurven zu übersetzen. Hierfür ist dieses Kapitel zweigeteilt.

In Unterkapitel 5.1 wird hierfür zunächst die Menge der $n$-Torsionspunkte für ein $n \in \mathbb{N}$ über elliptische Kurven definiert und dann bewiesen, dass diese Menge gemeinsam mit der üblichen Addition über elliptische Kurven eine Untergruppe der betrachteten elliptischen Kurve bildet. Diese Untergruppe wird demnach auf weitere Eigenschaften untersucht. Unter Nutzung des Struktursatzes abelscher Gruppen und den Erkenntnissen aus Unterkapitel 4.2 wird ein Struktursatz für die Gruppe der $n$-Torsionspunkte einer fixierten elliptischen Kurve bewiesen. Mit diesem ist es dann möglich den Begriff einer Basis einzuführen.


Den ersten theoretischen Teil dieser Arbeit abschließend, konzentriert sich Kapitel 6 auf elliptische Kurven eingeschränkt auf endlichen Körpern. Dabei teilt sich dieses Kapitel in zwei Unterkapitel.

Eine besondere Eigenschaft von elliptischen Kurven eingeschränkt auf endlichen Körpern ist, dass diese stets endlich sind und damit eine endliche zyklische Gruppe bilden. Unterkapitel 6.1 wird daher zunächst formal den Begriff der Ordnung einer elliptischen Kurve eingeschränkt auf endlichen Körpern einführen.


Des Weiteren wird bewiesen, wie die Ordnung einer elliptischen Kurve $E(F_{q^n})$ leicht für beliebiges $n \in \mathbb{N}_0$ bestimmt werden kann, wenn die Ordnung von $E(F_q)$ für eine Primzahlpotenz $q$ bereits bekannt ist.


Nachdem in aller Ausführlichkeit die theoretischen Grundlagen in Kapitel 3 bis Kapitel 6 gelegt wurden, startet nun Kapitel 7 in den anwendungsbezogenen Teil dieser Arbeit. Hierfür befasst sich Kapitel 7 in drei Unterkapiteln zunächst mit Methoden, mit welchen fundamentale Berechnungen auf elliptischen Kurven möglichst effizient durchgeführt werden können.


Die Methode des Unterkapitels 7.2 kann glücklicherweise unter Verwendung des Satzes von Hasse aus Kapitel 4 genutzt werden, um die Ordnung einer eingeschränkten elliptischen Kurve selbst zu bestimmen. Da die Bestimmung der Ordnung einer eingeschränkten elliptischen Kurve zentral für die Gewährleistung eines sicheren elliptischen Kurven Kryptosystems ist, wird diese Methodik sehr detailliert in Unterkapitel 7.3 anhand eines Beispiels erklärt.

Mit der Sicherheitsfrage von Kryptosystemen beschäftigt sich Kapitel 8 in zwei Unterkapiteln, wobei sich das zweite erneut in vier Abschnitte untergliedert.


Da dies eine mathematische Abschlussarbeit darstellt, ist es notwendig Begriffe aus der Informatik genauestens zu definieren. Hierfür führt Kapitel 9 die wichtigsten Konzepte der Informatik - zum Beispiel das Konzept von Kryptosystemen - ein.

Nachdem Kapitel 9 somit den Weg für die schlussendliche Anwendung elliptischer Kurven in der Kryptographie geebnet hat, stellt Kapitel 10 die bekannteste Form eines elliptischen Kurven Kryptosystems vor, welches es ermöglicht einen geheimen Schlüssel zwischen zwei Parteien über öffentliche und somit unsichere Kanäle auszutauschen, ohne ebenenjenen zu komprimieren.

Anschließend wird Unterkapitel 10.2 dieses Prinzip auf den Fall elliptischer Kurven übertragen. In diesem Spezialfall ergeben sich einige Vorteile, welche erklärt werden. Natürlich werden auch nicht die Nachteile unerforscht gelassen.


Appendix

In this appendix four Matlab Codes are provided. Subsection 14.1 and subsection 14.2 suggest an easy to implement code for elliptic curves restricted on either \( \mathbb{R} \) or a finite field. Moreover subsection 14.3 and subsection 14.4 provide codes for easily adding two elements in either an elliptic curve restricted on \( \mathbb{R} \) or an elliptic curve restricted on a finite field. Those Matlab Codes were entirely written by myself and were used for all calculations in this thesis as well as for generating all used figures.

14.1. Elliptic Curves restricted on \( \mathbb{R} \).

```matlab
function [x,y1,y2]=EllipticCurveR(x,A,B)
% This function calculates the corresponding (if existing) Y-coordinate(s) to
% given X-coordinate(s) (via Input x) laying in the restricted elliptic
% curve described by \( Y^2=X^3+AX+B \) over the field of real numbers
% INPUT
% x vector (either column or row) containing all evaluation points in x
% A scalar
% B scalar
% OUTPUT
% x vector containing the X-coordinate(s)
% y1 vector containing the first possible Y-coordinate(s) corresponding to x
% y2 vector containing the second possible Y-coordinate(s) with \( y2 = -y1 \)
% due to the symmetry of elliptic curves
% Note: \( y1 = 0 = y1 \) might occure
% Calculating possible \( y^2 \)'s
testysquare = x.^3 + A.*x + B;
% Deleting all \( y^2 \)'s with negative values, since this would result in
% complex numbers with existing imaginary parts
for i = length(x):(-1):1
    if testysquare(i) < 0
        testysquare(i) = [];
    end
end
% Finding the corresponding +/- \( y \)'s to the calculated \( y^2 \)'s via x
y1 = sqrt(testysquare)';
y2 = -sqrt(testysquare)';
end
```

14.2. Elliptic Curves restricted on a finite field.

```matlab
function [x,y]=EllipticCurveF(x,A,B,p)
% This function calculates the corresponding \( y \) to
% given \( x \) laying in the elliptic curve described by
% \( Y^2=X^3+AX+B \) over the field of a finite field
% INPUT
% x column vector containing all evaluation points in x
% A scalar
% B scalar
% p prime number determining the finite field
% OUTPUT
% x vector containing the X-coordinate(s)
% y vector containing the Y-coordinate corresponding to x
% Note: \( x = y = 0 \) might occure
% Calculating possible \( y^2 \)'s
testysquare = x.^3 + A.*x + B;
% Deleting all \( y^2 \)'s with negative values, since this would result in
% complex numbers with existing imaginary parts
for i = 1:length(x)
    if testysquare(i) < 0
        testysquare(i) = [];
    end
end
% Finding the corresponding \( y \) to the calculated \( y^2 \) via x
y = sqrt(testysquare);`
14.2. Elliptic Curves restricted on finite fields.

```matlab
function [x,y1,y2] = EllipticCurveFF(x,A,B,q)

% This function calculates the corresponding (if existing) Y-coordinate(s) to
% given X-coordinate(s) (via Input x) laying in the restricted elliptic
% curve described by Y^2=X^3+AX+B over the finite field with characteristic q
% INPUT
% x  vector (either column or row) containing all evaluation points in x
% A  scalar
% B  scalar
% q  scalar
% OUTPUT
% x  vector containing possible X-coordinates
% y1 vector containing the first possible Y-coordinate corresponding to x
% y2 vector containing the second possible Y-coordinate(s) with
%     y2 = -y1 due to the symmetry of elliptic curves
% Note:  y1 = 0 = y1 might occure

% Finding the corresponding coefficients over the finite Field F_q
A = mod(A,q);
B = mod(B,q);

% Calculating possible y^-2's and generating saving spots for the later
% calculated y1 and y2
testysquare = mod(x.^3 + A.*x + B,q);
y1 = zeros(length(x),1);
y2 = zeros(length(x),1);

% Calculating all squares in the cyclic field
squares = mod([0:q].^2,q);

% Checking if there exists corresponding squares
for i = length(x):(-1):1
    j = 1;
    go = 1;
    while (j <= q+1) && (go == 1)
        % Case of a corresponding square existing
        if testysquare(i) == squares(j)
            % Saving of all relevant values
            y1(i,1) = mod(j-1,q);
            y2(i,1) = mod(-j+1,q);
            % Loop can be stopped
            go = 0;
        end
        j = j+1;
    end
end
% In case that there was no corresponding square existing the
% X-coordinate needs to be cancelled as well as the corresponding
% saving spots of y1 and y2
if go == 1
    x(i) = [];
    y1(i) = [];
    y2(i) = [];
end
end
```
14.3. Addition over elliptic curves restricted on \( \mathbb{R} \).

```matlab
function P3 = addr(P1,P2,A,B)

% This function adds two points P1 and P2 (both unequal infinity)
% laying in the restricted elliptic curve over the field of real numbers
% described by the non-generalized Weierstrass equation \( Y^2 = X^3 + AX + B \) and
% determines their sum P3
% INPUT
% P1 1x2 Vector
% P2 1x2 Vector
% A scalar
% B scalar
% OUTPUT
% P3 1x2 Vector
% Note: If necessary INFINITY will be displayed instead of a tuple

% Calculating corresponding Y-Coordinates to the given X-coordinates of P1 and P2
 [~, Test1, Test2] = EllipticCurveR(P1(1,1),A,B);
 [~, Test3, Test4] = EllipticCurveR(P2(1,1),A,B);

% Testing of P1 and P2 being elements in the considered restricted real
% elliptic curve and if so, the addition starts in the "else"-loop
if ((Test1 == P1(1,2) & Test2 == P1(1,2)) || ( (Test3 == P2(1,2)) & (Test4 == P2(1,2)))
    disp('At least one point is not an element in the elliptic curve given');
else
    % Generating a saving spot for the later calculated sum P3 of P1 and P2
    P3 = zeros(1,2);

    % Addition of two points according to the rules of addition in elliptic
    % curves (Cases!)
    if P1(1,1)==P2(1,1) & P1(1,2) ~= P2(1,2)
        % Both points having the same X-coordinate and distinct Y-coordinates
        P3 = disp('Infinity');
    elseif P1(1,1) == P2(1,1) & P1(1,2) == P2(1,2)
        % Points being identical
        if P1(1,2)==0
            % Special Case of points being identical with a
            % Y-coordinate equal 0
            P3 = disp('Infinity');
        else
            % P1 and P2 being identical with a Y-coordinate
            % unequal to 0
            m = (3*P1(1,1)^2+A)/(2*P1(1,2));
            P3(1,1) = m^2-2*P1(1,1);
            P3(1,2) = m*(P1(1,1)-P3(1,1))-P1(1,2);
        end
    else
        % Case of P1 and P2 being distinct in both coordinates
        m = (P2(1,2)-P1(1,2))/(P2(1,1)-P1(1,1));
        P3(1,1) = m^2-P1(1,1)-P2(1,1);
        P3(1,2) = m*(P1(1,1)-P3(1,1))-P1(1,2);
    end
end
end
```
14.4. Addition over elliptic curves restricted on finite fields.

function \(P3 = \text{addFF}(P1, P2, A, B, q)\)

% This function adds two points (both unequal infinity) laying in
% the restricted elliptic curve over the finite field with characteristic \(q\)
% described by the non-generalized Weierstrass equation \(Y^2 = X^3 + aX + B\)
% and determines their sum \(P3\)

% INPUT
7 \% P1 1x2 Vector
8 \% P2 1x2 Vector
9 \% A scalar
10 \% B scalar
11 \% q scalar (power of a prime)
12 % OUTPUT
13 \% P3 1x2 Vector
14 % Note: If necessary INFINITY will be displayed instead of a tupel

function Hess@uni-konstanz.de

% Calculating corresponding Y-Coordinates to the given X-coordinates of
18 \% P1 and P2
19 ['~, Test1, Test2] = EllipticCurveFF(P1(1,1),A,B,q);
20 ['~, Test3, Test4] = EllipticCurveFF(P2(1,1),A,B,q);
21
22 % Testing of P1 and P2 being elements in the considered restricted elliptic
23 % curve and if so, the addition starts in the "else"-loop
25 if ((Test1 == P1(1,2) && Test2 == P1(1,2)) || ((Test3 == P2(1,2)) && Test4 == P2(1,2)))
26 disp('At least one point is not an element in the elliptic curve given');
27 else
28 % Generating a saving spot for the later calculated sum P3 of P1 and P2
29 P3 = zeros(1,2);
30
31 % Addition of two points according to the rules of addition in elliptic
32 % curves (Cases!)
33 if P1(1,1)==P2(1,1) && P1(1,2) ~= P2(1,2)
34 \% Both points having the same X-coordinate and distinct Y-coordinates
35 P3 = disp('Infinity');
36 elseif P1(1,1) == P2(1,1) && P1(1,2) == P2(1,2)
37 \% Points being identical
38 if P1(1,2)==0
39 \% Special Case of points being identical with
40 \% a Y-coordinate equal 0
41 P3 = disp('Infinity');
42 else
43 \% P1 and P2 being identical with a Y-coordinate
44 \% unequal to 0
45 d = mod(2*P1(1,2),q);
46 invd = 1;
47 \% Determination of the multiplicative inverse of d
48 while mod(d*invd,q) ~= 1
49 invd = mod(invd+1,q);
50 end
51 \% Addition of P1 and P2
52 m = mod((3*P1(1,1)^2+a)*d,q);
53 P3(1,1) = mod(m^2-2*P1(1,1),q);
54 P3(1,2) = mod(m*(P1(1,1)-P3(1,1))-P1(1,2),q);
55 end
56 else
% Case of P1 and P2 being distinct in both coordinates

d = mod(P2(1,1)-P1(1,1),q);

% Determination of the multiplicative inverse of d

while mod(d*invd,q) ~= 1
    invd = mod(invd +1,q);
end

% Addition of P1 and P2

m = mod((P2(1,2)-P1(1,2))*invd,q);
P3(1,1) = mod(m^2-P1(1,1)-P2(1,1),q);
P3(1,2) = mod(m*(P1(1,1)-P3(1,1))-P1(1,2),q);
end

end

end
REFERENCES


