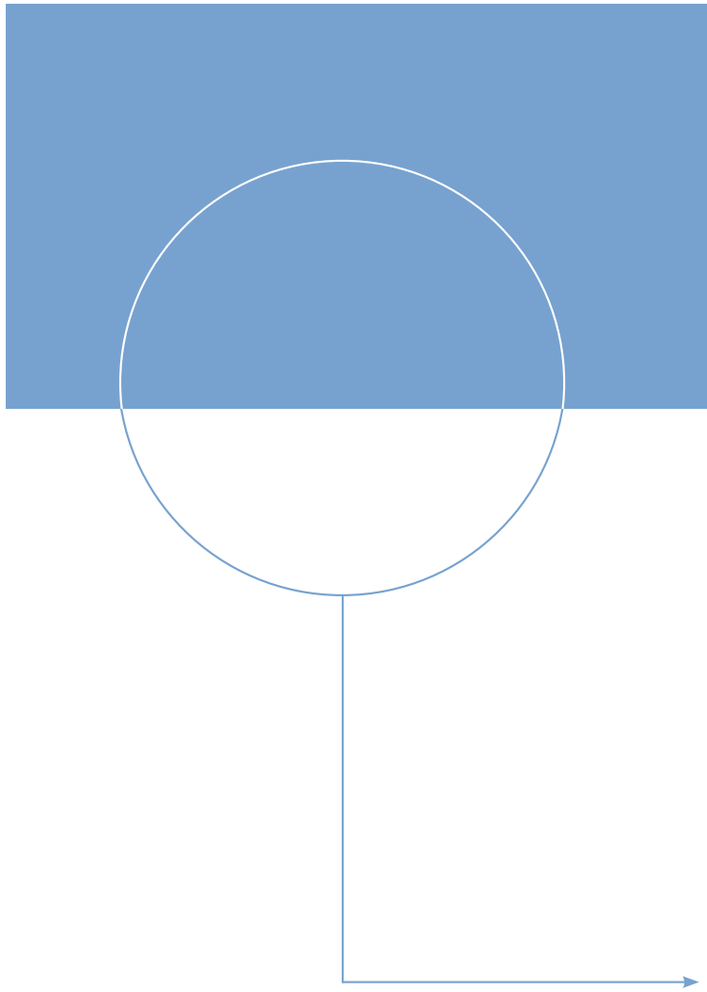


Master's thesis

2019

Jenny Kvamme Høvik

NTNU
Norwegian University of
Science and Technology
Faculty of Information Technology and Electrical
Engineering
Department of Mathematical Sciences

Jenny Kvamme Høvik

Bilinear Pairings on Elliptic Curves

June 2019

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of
Science and Technology

NTNU

Norwegian University of
Science and Technology

Bilinear Pairings on Elliptic Curves

Lektorutdanning i realfag
Submission date: June 2019
Supervisor: Kristian Gjøsteen

Norwegian University of Science and Technology
Department of Mathematical Sciences

Summary

In this thesis we consider bilinear pairings on elliptic curves. First, we give an introduction to algebraic geometry and in particular the concept of divisors. Further, we consider elliptic curves and their arithmetic. We study two different pairings on elliptic curves, the Weil pairing and the Tate pairing. We state the Weil pairing in to versions and prove the relation between them. Further, we describe the Tate pairing in details and show the properties of both pairings. We also explain how to calculate them. Finally, we describe the MOV-attack and the tripartite Diffie-Hellman key agreement, as an example of the use of pairings in cryptography.

Samandrag

I denne oppgåva studerer vi bilineære parringer på elliptiske kurver. Først gir vi ein introduksjon til algebraisk geometri og spesielt omgrepet divisorar. Vidare ser vi på elliptiske kurver og deira aritmetikk. Vi ser på to ulike parringer på elliptiske kurver, Weilparringa og Tateparringa. Vi skildrar Weilparringa på to ulike måtar og viser provet for relasjonen mellom dei. Vidare skildrar vi Tateparringa i detalj og syner eigenskapane til begge parringane. Vi syner òg korleis dei kan reknast ut. Til slutt skildrar vi MOV-angrepet og den tredelte nøkkelavtala til Diffie-Hellman som døme på bruk av parringar i kryptografi.

Preface

This thesis completes my studies at the Norwegian University of Science and Technology, where I have studied to become a teacher in mathematics and chemistry. Through the work on this thesis, I have worked independently, embarked on a difficult topic and had the goal of conveying it in an easier way. I will bring these experiences into my work as a teacher.

My master's thesis was carried out under the supervision of Professor Kristian Gjøsteen. I would like to thank you for providing helpful and encouraging supervision. I could not have done this without your help.

I would like to thank my family and Kristian for always supporting me. Thank you for reminding me that my value does not depend on my master's thesis.

These wonderful five years as a student would not have been the same without good friends. Thank you for filling my life with much more that studies. Tora and Elisabeth, thank you for making "Matteland" a better place to be.

Trondheim, 31.05.2019

Jenny Kvamme Høvik

Contents

List of Figures

Chapter 1

Introduction

The theme of this thesis is bilinear pairings on elliptic curves. We discuss the topic with the assumption that the reader has basic knowledge of groups, rings, fields, number theory and cryptography. Two different bilinear pairings, the Weil pairing and the Tate pairing, are presented. To do this, we need algebraic geometry and the arithmetic of elliptic curves.

We describe the structure of the thesis. Chapter 2 deals with algebraic geometry and lays the foundation for us to talk about elliptic curves. In Chapter 3 we describe elliptic curves and how we can do calculations with points on such curves. After these chapters we are ready to study bilinear pairings. We do this in Chapters 4 and 5. First, we look at the Weil pairing and its properties. Then, we look at the Tate pairing. Finally, we use the pairings in two examples from cryptography in Chapter 6.

Notation: We let the symbols

$$\mathbb{Z},\ \mathbb{Q},\ \mathbb{R},\ \mathbb{C},\ \mathbb{F}_q \text{ and } \mathbb{Z}/n\mathbb{Z},$$

denote the integers, rational, real and complex numbers, a finite field with q elements and n-adic numbers, respectively. Further, we let $A[n]$ denote the elements of order dividing n, given that A is an abelian group.

References: Bibliographical references are given in squared brackets, e.g. [8, p. 55]. Cross-references to equations are given in parentheses, e.g. (2.2). Cross-references to figures, theorems, sections etc. are given with reference to chapter, e.g. Lemma 1.1, Theorem 3.4.

Chapter 2

Algebraic Geometry

Algebraic geometry is the study of geometries that can be described algebraically. In this chapter we will define some concepts that will be used throughout this thesis. In Section 2.1 we introduce affine and projective n-spaces. This lays the basis for working with elliptic curves. Further, we describe divisors of curves in Section 2.2.

The definitions in this thesis are based on the assumption that we work in a perfect field K. A field is said to be *perfect* if every algebraic extension of it is separable [1, p. 316]. Note that in a perfect field $K = \{x^q \mid x \in K\}$. The field of rational numbers is an example of a perfect field with characteristic 0. The characteristic of a field K is denoted $n = \mathrm{char}(K)$. By that, we mean the smallest integer n such that

$$\underbrace{(1 + 1 + ... + 1)}_{n \text{ times}} = 0$$

where 1 and 0 are the multiplicative and additive identity, respectively. Other examples of perfect fields are all finite fields, $\mathbb{F}_{p^k} = \mathbb{F}_p[X]/\langle f(X)\rangle$, where k is a positive integer, p a prime number and $\langle f(X)\rangle$ an irreducible polynomial.

We finish the introduction to perfect fields by showing an example of a non perfect field. Consider $\mathbb{F}(X) = \left\{\frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{F}[X]\right\}$. It has characteristic $p > 0$ and there exists a map given by $f(x) \mapsto f(x)^p$. If $\mathbb{F}(X)$ is perfect, then there exist an element $\frac{f(x)}{g(x)}$ such that $x = \frac{f(x)^p}{g(x)^p}$. We write out the equation for $xg(x)^p = f(x)^p$ to see if there is such an element and get that

$$x(g_0^p + g_1^p x^p + ... + g_n^p (x^p)^n) = f_0^p + f_1^p x^p + ... + f_m^p (x^p)^m. \tag{2.1}$$

From (2.1), we find that $f(x) = g(x) = 0$, but that gives us a problem since our plan was to find an x such that $x = \frac{f(x)^p}{g(x)^p}$. We cannot find such an x, hence $\mathbb{F}(X)$ is not perfect.

Finally, some remarks on notation. A perfect field will always be denoted K. By $\overline{K}$, we

denote a fixed algebraic closure of K and the Galois group of $K/\overline{K}$ is denoted $G_{K/\overline{K}}$.

2.1 Affine and Projective n-spaces

Throughout this thesis, we work with affine and projective n-spaces. They are described in detail in Fulton [2], and this introduction follows his book. Both affine and projective n-spaces are sets of n-tuples. We start by looking at affine n-spaces. An affine space, $\mathbb{A}^n$, is a cartesian product of K with itself n times.

Definition 2.1. An *affine n-space* over K is a set of n-tuples of elements of K. We call its elements *points* and denote them by

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

In particular, an affine 1-space is a line given by $\mathbb{A}^1 = \left\{P = (x_1) \mid x_1 \in \overline{K}\right\}$ and an affine 2-space is a plane consisting of all points (x_1, x_2) such that $x_1, x_2 \in \overline{K}$. Further, we let S be a set of polynomials with coefficients in K such that $S \subseteq K[X_1, ..., X_n]$. Let $V(S) = \{P \in \mathbb{A}^n \mid F(P) = 0 \text{ for all } F \in S\}$. That is, $V(S)$ is the set of all points P in $\mathbb{A}^n$ that gives $F(P) = 0$ for all $F \in S$. Given these assumptions, we define an affine algebraic set,

Definition 2.2. A subset $X \subset \mathbb{A}^n(K)$ is an *affine algebraic set* if $X = V(S)$ for some S.

Imagine that you want to find all the intersections between two curves. For example, consider the line $Y = \frac{1}{a}X$ and the curve $Y^2 = X^2 - 4$. They intersects in two points for $a \notin [-1, 1]$ given that we restrict ourselves to real values of X and Y. If we allow $X, Y \in \mathbb{C}$, the curves intersect when $Y = \pm\sqrt{X^2 - 4}$. This gives intersections as long as $a \neq \pm 1$.

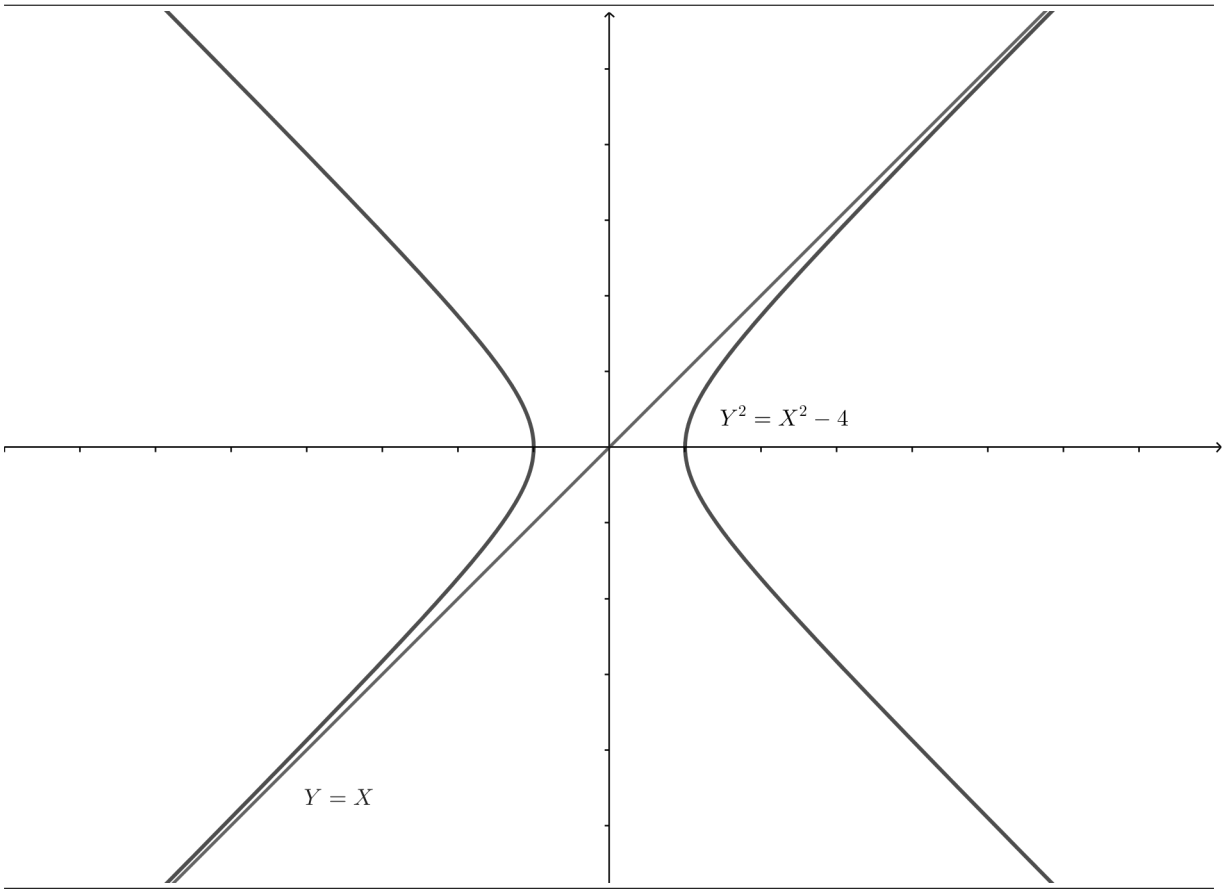
The curve is asymptotic to the line when $a = \pm 1$, as shown for $a = 1$ in Figure 2.1. We would like them to intersect at infinity, so we let $(x, y) \in \mathbb{A}^2$ correspond to $(x, y, 1) \in \mathbb{A}^3$. We do this by letting $(x, y, 1)$ determine a line through $(0, 0, 0)$ and $(x, y, 1)$. Further, we let the lines through $(0, 0, 0)$ in the xy-plane correspond to $\mathcal{O}$, the point at infinity. This way, we may define all lines through $(0, 0, ..., 0)$ in $\mathbb{A}^{n+1}$ as the projective n-space over K.

In order to define a projective n-space over K, we need to know when two points are equivalent. The equivalence of points is based on the fact that any point $x = (x_1, ..., x_{n+1}) \neq (0, 0, ..., 0)$ determine a unique line. We say that x and y determine the same line if and only if there exists a $\lambda \neq 0$ in K such that $y_i = \lambda x_i$ for all $i = 1, ..., n + 1$. If x and y determine the same line, we say that they are equivalent. The projective n-space, $\mathbb{P}^n$, can be considered as the set of divisor classes of points in $\mathbb{A}^{n+1} \setminus (0, 0, ..., 0)$.

Definition 2.3. A *projective n-space* over K is a set of n-tuples

$$\mathbb{P}^n = \mathbb{P}^n(\overline{K}) = \{(x_0, ..., x_n) \in \mathbb{A}^n \mid (x_0, ..., x_n) \neq (0, ..., 0) \mod (x_0, ..., x_n) \sim (y_0, ..., y_n)\},$$

Figure 2.1 Intersection of $Y^2 = X^2 - 4$ and $Y = X$



where $(x_0, ..., x_n) \sim (y_0, ..., y_n)$ denotes that the points are equivalent.

Let $P \in \mathbb{P}^n$ be a zero of a polynomial $F \in \overline{K}[X_1, ..., X_{n+1}]$. That is, $F(x_1, ..., x_{n+1}) = 0$ for all homogeneous coordinates $(x_1, ..., x_{n+1})$ for P. If P is a zero for F, we write $F(P) = 0$. Let S be a set of polynomials in $\overline{K}[X_1, ..., X_{n+1}]$ and let

$$V(S) = \{P \in \mathbb{P}^n \mid F(P) = 0 \text{ for all } F \in S\}.$$

Consider the ideal generated by S, and denote it by I. The ideal is homogeneous if it is generated by homogeneous polynomials. $F = \sum a_i X^i$ is *homogeneous of degree* d if all coefficients are zero except for a_d. If I is homogeneous we associate it with a subset of $\mathbb{P}^n$,

Definition 2.4. A *projective algebraic set* is a set V_I on the form

$$V_I = \{P \in \mathbb{P}^n \mid F(P) = 0 \text{ for all homogeneous } F \in I\},$$

where I is a homogeneous ideal.

We finish this section with the definition of a function field from [4] and the definition of the

order of a function at a point. Let $I_K(C)$ be the ideal generated by homogeneous polynomials,

$$I_K(C) = (\{f \in K[C] \mid f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in C\}).$$

Then a function field is given by Definition 2.5.

Definition 2.5. Let C be a curve defined over K. Then the *function field* $K(C)$ is the set

$$K(C) = \{f_1/f_2 \mid f_1, f_2 \in K[C] \text{ homogeneous of the same degree }, f_2 \notin I_K(C)\}$$

of classes under the equivalence relation $f_1/f_2 \equiv f_3/f_4$ if and only if $f_1 f_4 - f_2 f_3 \in I_K(C)$.

Let C be a curve and $P \in C$ be a smooth point. We define the *order* of $f \in \overline{K}(C)$ at P as the smallest integer m such that $mP = \mathcal{O}$ and denote it $\mathrm{ord}_P(f)$. We say that f has a *zero* at P if $\mathrm{ord}_P(f) > 0$ and if $\mathrm{ord}_P(f) < 0$, f has a *pole* at P [11, p. 18].

2.2 Divisors

The study of elliptic curves requires work with functions on curves. These functions have poles and zeroes, which will be of great importance. We need a tool to keep track of the poles and zeroes, and divisors are suitable for this purpose. First, we take a look at the divisor of a curve. We will follow [10] and [11] and use notation as in the latter.

Definition 2.6. Let P be a point on the curve, C. The divisor of C is a formal sum,

$$\mathfrak{D} = \sum_{P \in C} n_P(P),$$

of the points on the curve, with only a finite number of nonzero coefficients $n_P \in \mathbb{Z}$.

We write divisors with the points in round brackets and place the multiplicity of the points in front. We will focus on some types of divisors, based on what we call the *degree of a divisor*.

Definition 2.7. Let $\mathfrak{D} = \sum_{P \in C} n_P(P)$ be a divisor on a curve C. The *degree of* $\mathfrak{D}$ is denoted

$$\deg(\mathfrak{D}) = \sum_{P \in C} n_P.$$

In this thesis we shall mostly work with divisors of degree zero. The degree of the divisor is the sum of what we call the valuation at each point P. We define the *valuation* $v_P(\mathfrak{D})$ at a point P of a divisor $\mathfrak{D}$ to be the the coefficient of (P) in $\mathfrak{D}$, where $\mathfrak{D} = \sum_{P \in C} n_P(P)$. The set of points with nonzero valuation is called *the support of* $\mathfrak{D}$. In [10], Miller gives the following definition of support,

Definition 2.8. Let C be a curve and $\mathfrak{D} = \sum_{P \in C} n_P(P)$ be a divisor on C. The *support* of $\mathfrak{D}$ is

$$\mathrm{Supp}(\mathfrak{D}) = \{P \in C \mid v_P(\mathfrak{D}) \neq 0\}.$$

We will now look at divisors of functions. Consider a smooth curve C and a function $f \in \overline{K}(C)$. Then, f has poles or zeroes in finitely many points of C. These points give rise to the definition of a divisor associated with the function,

Definition 2.9. Let C and f be as described above and P be a point on the curve C. Then,

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P).$$

Further, this definition is used to define an expression for a function $f(\mathfrak{D})$. In Chapter 4, we describe the Weil pairing in terms of this function and use the notation for proving some of the properties of the Weil pairing.

Definition 2.10. Let C be a curve, $\mathfrak{D}$ a divisor and $P \in C$ a point. Let $v_P(\mathfrak{D})$ be the valuation of f at P and $f \in K(C)$ be a function such that $\mathrm{Supp}(\mathfrak{D}) \cap \mathrm{Supp}(\mathrm{div}(f)) = \emptyset$. Then, we define

$$f(\mathfrak{D}) := \prod_{P \in C} f(P)^{v_P(\mathfrak{D})}.$$

2.2.1 Properties

The properties of divisors are of great interest in the following chapters. They allow us to compare divisors, make calculations and simplify expressions. Therefore, we present the properties in this subsection. The first property is a very interesting result, namely the Weil reciprocity law [10].

Proposition 2.11 (The Weil Reciprocity Law)**.** *Let C be a curve and $f, g \neq 0$ be functions in the function field $K(C)$ with disjoint supports. Then,*

$$f(\mathrm{div}(g)) = g(\mathrm{div}(f)).$$

The proof of Proposition 2.11 is out of scope for this thesis, but a proof can be found in [11, p. 39].

Definition 2.12. A divisor $\mathfrak{D} \in \mathrm{Div}(C)$ is said to be *principal* if it can be written as $\mathfrak{D} = \mathrm{div}(f)$ for some $f \in \overline{K}(C)^*$.

Thus, if a divisor represents the zeroes and poles of a rational function, then the divisor is principal. In order to know whether a divisor is principal or not, we may calculate two sums,

Proposition 2.13. *Let E be an elliptic curve and $\mathfrak{D} = \sum_{P \in C} n_P(P)$ a divisor. Then $\mathfrak{D}$ is a principal divisor if and only if*

$$\sum_{P \in E} n_P = 0 \qquad \textit{and} \qquad \sum_{P \in E} n_P P = \mathcal{O}.$$

The first sum is a sum of integers, while the latter is the addition of the points on E.

A proof of this proposition can be found in [11, p. 63], but is out of scope for this thesis.

Chapter 3

Elliptic curves

The study of bilinear pairings on elliptic curves is based on the arithmetic of elliptic curves which will be described in Section 3.2. It is of great interest, as knowledge about the arithmetic is required in order to understand the rest of this thesis. Elliptic curves are examples of projective groups and can be defined in the following way. Given a nonsingular cubic curve E and an identity element $\mathcal{O} \in E$, an elliptic curve can be given by the pair $(E, \mathcal{O})$. Often, we denote it E. If the curve E is defined over K and $\mathcal{O} \in E(K)$, we say that the elliptic curve is defined over K, written E/K. It can be shown that an elliptic curve has an abelian group structure. This is best explained for Weierstrass form, a form which will be described in Section 3.1.

3.1 Weierstrass form

We would like to study the arithmetic of elliptic curves. The first step is to look at how to present them. Silverman [11, p. 42] writes an elliptic curve as a homogeneous equation,

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

where E is defined over K if $a_1, ..., a_6 \in K$. In addition, he includes a point at infinity denoted $\mathcal{O}$. The infinity point is given in projective coordinates by $\mathcal{O} = [0, 1, 0]$. By substituting $x = X/Z$ and $y = Y/Z$ into the equation we get the nonhomogeneous equation,

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

As before, if $a_1, ..., a_6 \in K$ we say that E is defined over K. This representation is called the *Weierstrass form* for an elliptic curve. We can simplify the expression in the cases where the characteristic of K is different from 2 and 3. That gives us a new expression for an elliptic curve, $E : y^2 = x^3 + ax + b$. This is called the *Weierstrass normal form* of an elliptic curve and is what we mostly will use throughout this thesis.

3.2 The Arithmetic of Elliptic Curves

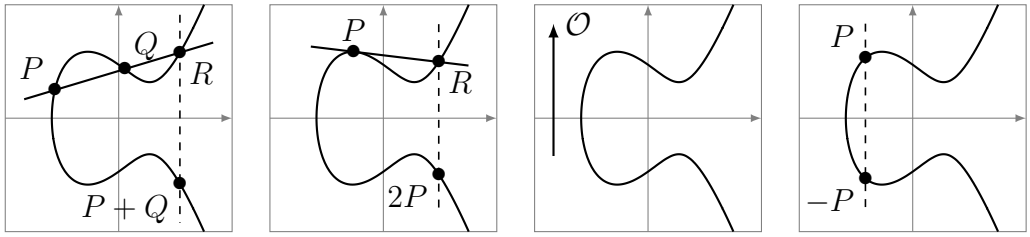
In this section, we describe how to do arithmetic of elliptic curves. First, we describe the group operations in detail in a composition law and show it in figures. Then, we state and prove the properties of the composition law (except for associativity) and we show an example of arithmetic on an elliptic curve. The presentation follows Silverman [11].

It can be shown that any line in the projective plane intersects an elliptic curve in exactly three points if we count multiplicity [11, p. 51]. This gives rise to the definition of the composition law.

Definition 3.1 (Composition Law)**.** Let L be a line that intersects E in the two points P, Q. If $P = Q$, let L be the tangent line of E in P. L will intersect the line in a third point, denoted R. The line L' intersects E in $R, \mathcal{O}$ and a third point. We denote this point $P + Q$.

The group operation is shown in Figure 3.1, where the first figure shows how to find $P + Q$ when P and Q are distinct. The second shows it when they are equal and the third and fourth figures illustrates the neutral element and the inverse element, respectively.

Figure 3.1 The composition law on elliptic curves



Addition $P + Q$ "Chord rule" | Doubling $P + P$ "Tangent rule" | Neutral element $\mathcal{O}$ | Inverse element $-P$

Based on the composition law, we can show that the group law has five useful properties. These properties are essential for the usage of arithmetic of elliptic curves.

Proposition 3.2. *The properties of the composition law are given by,*

1. *For a line L that intersects E at points, P, Q, R, we have $(P + Q) + R = \mathcal{O}$.*
2. *$P + \mathcal{O} = P$ for all $P \in E$.*
3. *$P + Q = Q + P$ for all $P, Q \in E$.*
4. *Let $P \in E$. Then there exists a point of E, denoted $-P$, such that $P + (-P) = \mathcal{O}$.*
5. *Let $P, Q, R \in E$. Then $(P + Q) + R = P + (Q + R)$.*

Proof. 1. Let the line L intersect E at the points, P, Q, R. By the composition law, the line L' intersects E in $(P + Q)$ and by definition L' is the line through R and $\mathcal{O}$. It follows that $(P + Q) + R = \mathcal{O}$.

2. Insert $Q = \mathcal{O}$ into the composition law. Then L will intersect E in $P, \mathcal{O}, R$ and L' will intersect E in $R, \mathcal{O}, P$, but the latter point is defined as $P+Q$. Thus $P = P+Q = P+\mathcal{O}$ for all $P \in E$.

3. Let $P, Q \in E$. Further, let L and L^* be the lines passing through P, Q and Q, P, respectively. By the composition law, L and L^* will intersect E in the same point R. Since both $(P + Q)$ and $(Q + P)$ are constructed by letting the line L' through R and $\mathcal{O}$ intersect E, we get the desired result. $P + Q = Q + P$ for all $P, Q \in E$.

4. Let $P \in E$ and let L be the line through P and $\mathcal{O}$. Then L also intersects E in R. By 3.2.1 and by 3.2.2 we know that

$$\mathcal{O} = (P + \mathcal{O}) + R = P + R.$$

   Define $(-P) := R$ and we get $P + (-P) = \mathcal{O}$.

5. The proof of associativity is difficult, but a geometric proof can be found in Fulton [2, p. 63].

□

The collection of these five properties provides us with a set of rules that can be used for calculations. These calculations are required for the two types of bilinear pairings that we will present in the next chapters. In addition, the properties give us that E is an abelian group with $\mathcal{O}$ as identity element [11, p. 52].

Example 3.3. Let $E/\mathbb{Q}$ be the elliptic curve $E : y^2 = x^3 + 37$. By using the software system SageMath, we easily find the points on the curves with integer coordinates (in Appendix). These are: $P = (-1, 6), Q = (3, 8), R = (234, 3788)$. We find that

$$P + Q = (-7/4, -45/8) \text{ and } P + R = (-7/4, 45/8),$$

which gives us that $P + Q = -(P + R)$.

We have discussed the properties of the composition law. Finally, we will define n-torsion points and show how equality of two points on an elliptic curve affects the relation of their divisors.

Definition 3.4. Let P be a point on an elliptic curve. P is called an *n-torsion point* if there exists a nonzero integer n such that $nP = \mathcal{O}$.

A torsion subgroup $E[n]$ consists of all n-torsion points on an elliptic curve, E.

Lemma 3.5. *Let C be a curve with genus one and $P, Q \in C$. Then,*

$$(P) \sim (Q) \text{ if and only if } P = Q.$$

The proof of the lemma is out of scope for this thesis, but a proof can be read in [11, p. 61].

Chapter 4

The Weil Pairing

In this chapter, we present the Weil pairing on an elliptic curve. We do the presentation of the Weil pairing in two different ways in Section 4.1 and show the relation between them. Further, we state and prove the properties of the Weil pairing in Section 4.2. The proofs are based on the introduction given in Section 4.1 and equip us with tools to continue our work on the Weil pairing.

The study of the Weil pairing is a study of algebraic maps between elliptic curves. It is important for the utility of the Weil pairing that the calculations can be done effectively. We explain how to compute the pairing in Section 4.3, using Miller's algorithm. The properties of the Weil pairing make us able to use the pairing in cryptography. This will be done in Chapter 6.

4.1 Introduction

4.1.1 Version I

Silverman [11] gives a description of the Weil pairing. Consider the isomorphism

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

where $E[n]$ is the group of n-torsion points and E/K is an elliptic curve. The Weil pairing is a bilinear map from $E[n]$ to the nth roots of unity. We construct it by letting n be an integer which is relatively prime to p, the characteristics of K, and such that it fulfills the requirement that $n \geq 2$. Next, we choose points on the elliptic curve that we want to pair. Choose Q to be an n-torsion point and let $Q' \in E$ be chosen such that $[n]Q' = Q$. Then, it exists functions $f, g \in \overline{K}(E)$ that have divisors given by (4.1) and (4.2), respectively.

$$\operatorname{div}(f) = n(Q) - n(\mathcal{O}), \tag{4.1}$$

$$\operatorname{div}(g) = [n]^*(Q) - [n]^*(\mathcal{O}) = \sum_{R \in E[n]} ((Q' + R) - R). \tag{4.2}$$

Here, $[n]^*$ maps the divisor (Q) to the divisor $(R_1) + (R_2) + ... + (R_n)$ where $nR_i = Q$ for all $i \in \{1, ..., n\}$. We know that $[n](Q' + R) = [n]Q' + [n]R = Q + \mathcal{O} = Q$ for all $i \in \{1, ..., n\}$. From Corollary 6.4 in [11], we know that the number of elements in the group $E[n]$ is n^2. Hence, we sum over n^2 terms. By the group law for points on an elliptic curve, we have that

$$(Q' + R) - R = Q' + (R + (-R)) = Q' + \mathcal{O} = Q'.$$

Our sum is reduced to a sum over Q', which gives us $\operatorname{div}(g) = [n^2]Q' = [n]Q = \mathcal{O}$.

We show that $f \circ [n]$ and g^n have the same divisor by observing that

$$\operatorname{div}(f \circ [n]) = \operatorname{div}([n]^* f) = [n]^* \operatorname{div}(f) = [m]^*(n(P) - n(\mathcal{O})) = \operatorname{div}(g^n).$$

We may therefore assume that $f \circ [n] = g^n$. Further, we choose a new n-torsion point P on the elliptic curve and let X be any point on E. P might be equal to Q. We get that

$$g(X + P)^n = f([n]X + [n]P) = f([n]X + \mathcal{O}) = f([n]X) = f \circ [n](X) = g(X)^n.$$

Thus, $g(X + P)/g(X)$ has an nth root of unity for all $X \in E$, and takes finitely many values. We define the Weil pairing in terms of our newly created function g,

Definition 4.1. Let E, g, P, Q be as above and let $\boldsymbol{\mu}_n = \{x \in \overline{K} \mid x^n = 1\}$. Then, the Weil pairing is given by

$$e_n : E[n] \times E[n] \to \boldsymbol{\mu}_n,$$
$$e_n(P, Q) = \frac{g(X + P)}{g(X)}.$$

4.1.2 Version II

Miller gives a different approach to the Weil pairing in [10]. Like Silverman, he defines functions, but he works more directly with divisors on elliptic curves. Miller suggests that we choose an integer $n > 1$ and divisors $\mathfrak{D}_1, \mathfrak{D}_2$ of the curve such that both $n\mathfrak{D}_1$ and $n\mathfrak{D}_2$ are equivalent to $\mathcal{O}$. He uses Weil functions when he defines the Weil pairing. These functions are constructed by first looking at their divisors.

Assume that the elliptic curve is on Weierstrass form and start by fixing uniformizers $u_\mathcal{O}, u_P$ to the point at infinity and to the point P, respectively,

$$u_\mathcal{O} := -y/x,$$

$$u_P := \begin{cases} x - x(P), & \text{ord}(P) \neq 2 \\ y - y(P), & \text{ord}(P) = 2 \end{cases}$$

This allow us to use the Laurent series.

Definition 4.2. A *Laurent series* is a power series with a finite number of terms with negative exponents in x. The *leading term*, $\text{lt}_x(f) = \text{lt}(f)$, of a Laurent series is the term in which the smallest exponent of x occurs. The smallest exponent is called the *degree* of the Laurent series. For $f(x) = ax^n + bx^{n+1} + ...$, we have $\deg(f) = n$ and $\text{lt}(f) = ax^n$.

We construct Weil functions inductively. Our goal is to build them such that $\text{div}(f) = n((P) - (\mathcal{O}))$, and we do this by constructing a function $f_{m,P}$ which meets the requirement that for a suitable $m < n$,

$$\text{div}(f_{m,P}) = m(P) - (mP) - (m-1)(\mathcal{O}).$$

Let f be a nonzero function on E. f is *normalized* if 1 is the leading coefficient of f as a Laurent series in $u_{\mathcal{O}}$. We let $L_{P,Q}$ be the normalized function where the line through the points P, Q is given by $L_{P,Q} = 0$. If $P = Q$, it is the tangent line through P. Given the normalized function, we may define a function $g_{P,Q}$.

Definition 4.3. Let $P, Q \in E$. We define

$$g_{P,Q} := \frac{L_{P,Q}}{L_{P+Q,-(P+Q)}}.$$

We would like find the divisor of this function. That requires knowledge about $\text{div}(L_{P,Q})$ which is found directly from the definition of addition on elliptic curves. Given a normalized function $L_{P,Q}$ as described above,

$$\text{div}(L_{P,Q}) = (P) + (Q) + (-(P+Q)) - 3(\mathcal{O}).$$

This can be used to calculate the divisor of $g_{P,Q}$,

$$\begin{aligned} \text{div}(g_{P,Q}) &= \text{div}(L_{P,Q}) - \text{div}(L_{P+Q,-(P+Q)}) \\ &= (P) + (Q) + (-(P+Q)) - 3(\mathcal{O}) \\ &\quad - ((P+Q) + (-(P+Q)) + (-((P+Q) - (P+Q))) - 3(\mathcal{O})) \\ &= (P) + (Q) - (P+Q) - (\mathcal{O}). \end{aligned} \tag{4.3}$$

We are now ready to define our Weil functions, $f_{n,P}$. First, we define the functions for the base cases where $n \in \{0, 1\}$. Define constant functions $f_{0,P} = f_{1,P} = 1$. The induction step is given by the following definition.

Definition 4.4. Let $P \in E$ and $f_{0,P} = f_{1,P} = 1$. Then for $n > 0$, define,

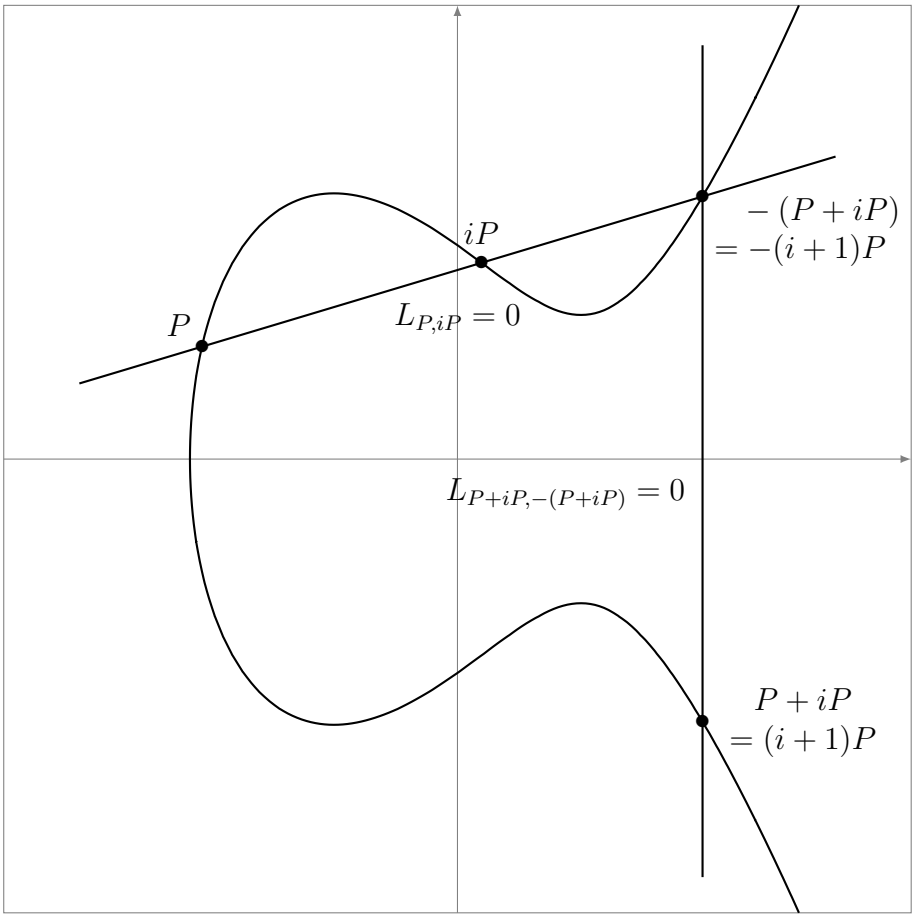
$$f_{n+1,P} := f_{n,P} g_{P,nP},$$
$$f_{-n,P} := \frac{1}{f_{n,P} g_{nP,-nP}}.$$

To increase the speed of the computations, the following lemma might be useful,

Lemma 4.5. *Let $P, Q \in E$ and let m, n be integers. Then*

$$f_{m+n,P} := f_{m,P} f_{n,P} g_{mP,nP}$$
$$f_{mn,P} := f_{m,P}^n f_{n,mP} = f_{n,P}^m f_{m,nP}$$
$$\mathrm{div}(f_{n,P}) = n(P) - (n-1)(\mathcal{O}) - (nP).$$

Figure 4.1 Addition of points



Example 4.6. Assume that $f_{0,P} = f_{1,P} = 1$. We know that $f_{i,P}$ should be built such that $\mathrm{div}(f_{i,P}) = i(P) - (iP) - (i-1)(\mathcal{O})$. Further, we look at the divisor of $f_{i+1,P}$. By definition,

$\mathrm{div}(f_{i+1,P}) = (i+1)(P) - ((i+1)P) - i(\mathcal{O})$. We notice the following relation,

$$\begin{aligned}\mathrm{div}(f_{i+1,P}) &= (i+1)(P) - ((i+1)P) - i(\mathcal{O}) \\ &= \underbrace{i(P) - (iP) - (i-1)(\mathcal{O})}_{\mathrm{div}(f_{i,P})} + \underbrace{(P) + (iP) - ((i+1)P) - (\mathcal{O})}_{\mathrm{div}(L_{P,iP}) - \mathrm{div}(L_{P+iP,-(P+iP)})} \\ &= \mathrm{div}(f_{i,P}) + \mathrm{div}(g_{P,iP}).\end{aligned}$$

The last equality is due to (4.3) and Lemma 4.5. In Figure 4.1, we see the lines $L_{P,iP} = 0$ and $L_{P+iP,-(P+iP)} = 0$. We observe that $f_{i+1,P}$ will get the desired divisor if we let $f_{i+1,P} := f_{i,P} g_{P,iP}$.

Definition 4.7. The *Weil pairing* on an elliptic curve E uses Weil functions and provides a family of maps $\tilde{e}_n : E[n] \times E[n] \to \boldsymbol{\mu}_n$, where $\boldsymbol{\mu}_n$ is the algebraic group of *n*th roots of unity. The maps are defined over K and there is one for each positive integer n relatively prime to $p = \mathrm{char}(K)$.

$$\tilde{e}_n(\mathfrak{D}_1, \mathfrak{D}_2) = \frac{f_1(\mathfrak{D}_2)}{f_2(\mathfrak{D}_1)} \tag{4.4}$$

It is useful to express the Weil pairing in the following way.

Proposition 4.8. *Let $T \in E$ be a point different from $P, Q, Q-P$, and $\mathcal{O}$. Then $(P) - (\mathcal{O}) \sim (P+T) - (T)$. In addition, $(Q) - (\mathcal{O})$ and $(P+Q) - (T)$ have disjoint supports. We get that*

$$\tilde{e}_n(P, Q) = \frac{f_{n,Q}(T)}{f_{n,P}(-T)} \frac{f_{n,P}(Q-T)}{f_{n,Q}(P+T)}. \tag{4.5}$$

Proof. By the definition of the Weil pairing, there is a function f_1 such that $\mathrm{div}(f_1) = n(P+T) - n(T)$ and

$$\tilde{e}_n(P, Q) = \frac{f_1(Q)/f_1(\mathcal{O})}{f_{n,Q}(P+T)/f_{n,Q}(T)}. \tag{4.6}$$

Observe that $\mathrm{div}(f_1) = \mathrm{div}(f_{n,P} \circ \tau_{-T})$. If we insert it to (4.6), we get the desired result. □

4.1.3 Proof of the Relation Between Version I and II.

The proof of the relation between the two versions of the Weil pairing in Sections 4.1.1 and 4.1.2 follows [8]. First, we look at the assumptions made in the two approaches to the Weil pairing. Both approaches choose an integer $n > 1$ relatively prime to $p = \mathrm{char}(K)$. The formulas for

version I and II of the Weil pairing are given in (4.7) and (4.8), respectively.

$$e_n(P,Q) = \frac{g(X+P)}{g(X)}, \tag{4.7}$$

$$\tilde{e}_n(\mathfrak{D}_1,\mathfrak{D}_2) = \frac{f_1(\mathfrak{D}_2)}{f_2(\mathfrak{D}_1)}. \tag{4.8}$$

Theorem 4.9. *Let $P,Q \in E[n]$. Then*

$$e_n(P,Q) = \frac{1}{\tilde{e}_n(P,Q)}.$$

Proof. Assume that $\mathfrak{D}_1 = (P) - (\mathcal{O}), \mathfrak{D}_2 = (Q) - (\mathcal{O})$, where $P,Q \in E[n]$. The divisors $n\mathfrak{D}_1$ and $n\mathfrak{D}_2$ are principal since P and Q are n-torsion points. Therefore, it exists functions $f_1, f_2 \in \overline{K}(E)$ with divisors $\mathrm{div}(f_1) = n\mathfrak{D}_1$ and $\mathrm{div}(f_2) = n\mathfrak{D}_2$.

Let us assume that Q' and P' are such that $[n]Q' = Q$ and $[n]P' = P$. Observe that, by the same argument as for (4.2), it exists a function g_1 such that $\mathrm{div}(g_1) = \sum_{R\in E[n]} ((P'+R) - R)$ and $g_1^n = f_1 \circ [n]$. We choose $X \in E$ such that

$$\mathfrak{D} = (n-1)(P'+X) + (P'-P+X) - n(X)$$

is a divisor with $\mathrm{Supp}(\mathfrak{D}) \cap \mathrm{Supp}(\mathrm{div}(g)) = \emptyset$ and let $h \in \overline{K}(E)$ be a function with $\mathrm{div}(h) = \mathfrak{D}$.

To prove the relation between Silverman's and Miller's version of the Weil pairing, we look at the divisors of h and g, where g is given in (4.2). First, we express $g(\mathrm{div}(h))$ in terms of $e_n(P,Q)$.

$$\begin{aligned}
g(\mathrm{div}(h)) &= g(\mathfrak{D}) \\
&= \frac{g(P'+X)^{n-1} g(P'-P+X)}{g(X)^n} \\
&= \frac{g(P'+X)^n}{g(X)^n} \frac{g(P'-P+X)}{g(P'+X)} && \text{Let } P'' = P'-P+X \\
&= \frac{f\circ[n](P'+X)}{f\circ[n](X)} \frac{g(P'')}{g(P''+P)} && \text{Given } e_n(P,Q) \text{ as in Definition } 4.1 \\
&= \frac{f(P'+[n]X)}{f([n]X)} \frac{1}{e_n(P,Q)}.
\end{aligned}$$

Next, we look at $h(\mathrm{div}(g))$ and observe that

$$h(\mathrm{div}(g)) = h\left(\sum_{R\in E[n]} (Q'+R) - (R)\right) = \prod_{R\in E[n]} \frac{h(Q'+R)}{h(R)}.$$

Based on that, we define a new function $H \in \overline{K}(E)$ as

$$H(S) = \prod_{R \in E[n]} h(S+R) = \prod_{R \in E[n]} h \circ \tau_R(S)$$

with divisor given by

$$\begin{aligned}
\operatorname{div}(H) &= \sum_{R \in E[n]} \operatorname{div}(h \circ \tau_R) \\
&= \sum_{R \in E[n]} ((n-1)(P'+X-R) + (P'-P+X-R) - n(X-R)) \\
&= \sum_{R \in E[n]} ((n-1)(P'+X+R) + (P'+X+R) - n(X+R)) \\
&= n \sum_{R \in E[n]} ((P'+X+R) - (X+R)) \\
&= n \ \operatorname{div}(g_1 \circ \tau_{-X}) \\
&= \operatorname{div}(g_1^n \circ \tau_{-X}).
\end{aligned}$$

It follows that $H = g_1^n \circ \tau_{-X} = f_1 \circ [n] \circ \tau_{-X}$. We express $h(\operatorname{div}(g))$ in terms of f_1,

$$\begin{aligned}
h(\operatorname{div}(g)) &= \prod_{R \in E[n]} \frac{h(Q'+R)}{h(R)} = \frac{H(Q')}{H(\mathcal{O})} = \frac{f_1 \circ [n] \circ \tau_{-X}(Q')}{f_1 \circ [n] \circ \tau_{-X}(\mathcal{O})} \\
&= \frac{f_1 \circ [n](Q'-X)}{f_1 \circ [n] \circ \tau_{-X}(\mathcal{O})} = \frac{f_1(Q-[n]X)}{f_1(-[n]X)}.
\end{aligned}$$

Finally, we use that $h(\operatorname{div}(g)) = g(\operatorname{div}(h))$ by Weil reciprocity law and that $f = f_2$ to complete the proof. As we insert the expressions for both $h(\operatorname{div}(g))$ and $g(\operatorname{div}(h))$, we get

$$\frac{f_1(Q-[n]X)}{f_1(-[n]X)} = \frac{f_2(P'+[n]X)}{f_2([n]X)} \frac{1}{e_n(P,Q)}.$$

We reformulate the equation to

$$e_n(P,Q) = \frac{f_1(-[n]X)}{f_1(Q-[n]X)} \frac{f_2(P'+[n]X)}{f_2([n]X)} \frac{1}{e_n(P,Q)} = \frac{f_2(\mathfrak{D}_1)}{f_1(\mathfrak{D}_2)} = \frac{1}{\tilde{e}_n(P,Q)},$$

which proves the relation $e_n(P,Q) = \frac{1}{\tilde{e}_n(P,Q)} = \tilde{e}_n(Q,P)$. □

4.2 Properties of the Weil Pairing

We have shown that Miller and Silverman describe two closely related pairings . Our next step is to prove that the Weil pairing is bilinear, alternating, nondegenerate and compatible. We state

the properties in the following lemmas.

Lemma 4.10 (Bilinearity)**.** *If $P, Q, R \in E[n]$, then*

$$e_n(P+Q,R) = e_n(P,R)e_n(Q,R),$$
$$e_n(P,Q+R) = e_n(P,Q)e_n(P,R).$$

Proof. The proof of bilinearity follows Miller [10]. Let $\mathfrak{D}_1, \mathfrak{D}_2, \mathfrak{D}_3$ be divisors on the elliptic curve E, with disjoint supports. First, we prove linearity in the first factor. By Definition 4.7, given that $f_1 f_2(\mathfrak{D}_3) := f_1(\mathfrak{D}_3) f_2(\mathfrak{D}_3)$,

$$e_n(\mathfrak{D}_1 + \mathfrak{D}_2, \mathfrak{D}_3) = \frac{f_1 f_2(\mathfrak{D}_3)}{f_3(\mathfrak{D}_1 + \mathfrak{D}_2)}.$$

Observe that by Definition 2.10 the denominator can be written as follows,

$$\begin{aligned} f_3(\mathfrak{D}_1 + \mathfrak{D}_2) &= \prod_{P \in E} f_3(P)^{v(\mathfrak{D}_1 + \mathfrak{D}_2)} \\ &= \prod_{P \in E} f_3(P)^{v(\mathfrak{D}_1) + v(\mathfrak{D}_2)} \\ &= \prod_{P \in E} f_3(P)^{v(\mathfrak{D}_1)} \prod_{P \in E} f_3(P)^{v(\mathfrak{D}_2)} \\ &= f_3(\mathfrak{D}_1) f_3(\mathfrak{D}_2). \end{aligned}$$

Further, we see that the numerator is given by $f_1 f_2(\mathfrak{D}_3) = f_1(\mathfrak{D}_3) f_2(\mathfrak{D}_3)$ which gives us the desired result,

$$e_n(\mathfrak{D}_1 + \mathfrak{D}_2, \mathfrak{D}_3) = \frac{f_1 f_2(\mathfrak{D}_3)}{f_3(\mathfrak{D}_1 + \mathfrak{D}_2)} = \frac{f_1(\mathfrak{D}_3) f_2(\mathfrak{D}_3)}{f_3(\mathfrak{D}_1) f_3(\mathfrak{D}_2)} = e_n(\mathfrak{D}_1, \mathfrak{D}_3) e_n(\mathfrak{D}_2, \mathfrak{D}_3).$$

In the same way, it can be shown that linearity holds for the second factor. □

Lemma 4.11 (Alternating)**.** *If $P \in E[n]$, then $e_n(P,P) = 1$. Together with linearity, we get that if $P, Q \in E[n]$, then*

$$e_n(P,Q) = e_n(Q,P)^{-1}$$

Proof. The proof follows Miller [10]. Suppose that T is a point different from $\mathcal{O}$ and $\pm P$, then

$$e_n(P,P) = \frac{f_{n,P}(T)}{f_{n,P}(-T)} \frac{f_{n,P}(P-T)}{f_{n,P}(P+T)}. \tag{4.9}$$

We consider two cases. Let T be of order 2, giving us $T = -T$. Inserted in (4.9) we get,

$$e_n(P,P) = \frac{f_{n,P}(T)}{f_{n,P}(-T)}\frac{f_{n,P}(P-T)}{f_{n,P}(P+T)} = \frac{f_{n,P}(T)}{f_{n,P}(T)}\frac{f_{n,P}(P+T)}{f_{n,P}(P+T)} = 1.$$

We check that T meets the requirement stated in the beginning of the proof, namely that $T \notin \{\mathcal{O}, \pm P\}$. Case 1: n is odd. Since P is an n-torsion point and T a point of order 2, it follows that $T \neq \pm P$. Further, T cannot be $\mathcal{O}$ because $\mathcal{O}$ is not of order 2. Case 2: n is even. Since n is defined to be relatively prime to $p = \mathrm{char}(K)$, we need the characteristics to be odd. There are three points of order 2 in $E[2]$. We know that $\mathcal{O}$ is not one of them and at most two of them are $\pm P$. Therefore, we may choose the last point as T. □

Lemma 4.12 (Non-degeneracy)**.** *If $e_n(P,Q) = 1$ for all $Q \in E[n]$, then $P = \mathcal{O}$ and if $e_n(P,Q) = 1$ for all $P \in E[n]$, then $Q = \mathcal{O}$.*

Proof. The proof of nondegeneracy follows Silverman [11]. Assume that $Q \in E[n]$ is such that $e_n(P,Q) = 1$ for all $P \in E[n]$. Then, $g(X+P) = g(X)$ for all $P \in E[n]$.

By Proposition 9.34 in [15], it exists a function $h \in \overline{K}(E)$ such that $g = h \circ [n]$. This gives us the relation between the functions h and f,

$$(h \circ [n])^n = g^n = f \circ [n].$$

Since $(h \circ [n])^n = (h^n) \circ [n]$, we get that $h^n = f$. Thus,

$$n \,\mathrm{div}(h) = \mathrm{div}(h^n) = \mathrm{div}(f) = n(Q) - n(\mathcal{O}),$$

where the last equality is due to (4.1). Hence, $\mathrm{div}(h) = (Q) - (\mathcal{O})$. We know that $\mathrm{div}(h) = 0$ and therefore $(Q) \sim (\mathcal{O})$.

E is an elliptic curve and thus has genus 1. From Lemma 3.5, it implies that $Q = \mathcal{O}$. The Weil pairing is therefore nondegenerate in P, and by Lemma 4.11 it is also nondegenerate in Q. □

Lemma 4.13 (Compatibility)**.** *Let $P \in E[mn]$ and $Q \in E[n]$. Then*

$$e_{mn}(P,Q) = e_n(mP,Q)$$

Proof. The proof of compatibility follows Miller [10]. To prove the compatibility property, we write out the expression for both $e_{mn}(P,Q)$ and $e_n(mP,Q)$. We show that the first expression can be reformulated to be equal to the latter. First, assume that $P \in E[mn]$ and $Q \in E[n]$. Suppose further that there are functions f_1, f_2, f_3 such that,

$$\mathrm{div}(f_1) = mn((P) - (\mathcal{O})),$$

$$\begin{aligned}\operatorname{div}(f_2) &= n((Q+T)-(T)),\\ \operatorname{div}(f_3) &= n((mP)-(\mathcal{O})).\end{aligned}$$

The divisors of the functions are used in the definition of the Weil pairing. We insert them in (4.5), giving the expressions of the desired Weil pairings,

$$\begin{aligned}e_{mn}(P,Q) &= \frac{f_1((Q+T)-(T))}{f_2^m((P)-(\mathcal{O}))},\\ e_n(mP,Q) &= \frac{f_3((Q+T)-(T))}{f_2((P)-(\mathcal{O}))}.\end{aligned}$$

We would like to show that they are equal. To do that, we first express $\operatorname{div}(f_3)$ in terms of $\operatorname{div}(f_1)$. This is done by adding and subtracting the same element in the equation, allowing us to extract $\operatorname{div}(f_1)$ from the expression. We get

$$\begin{aligned}\operatorname{div}(f_3) &= n((mP)-(\mathcal{O}))\\ &= n((mP)-(\mathcal{O})+m(P)-m(P)+m(\mathcal{O})-m(\mathcal{O}))\\ &= n((mP)-(m-1)(\mathcal{O})-m(P))+mn((P)-(\mathcal{O}))\\ &= \operatorname{div}(f_4^n)+\operatorname{div}(f_1)\\ &= \operatorname{div}(f_4^n f_1),\end{aligned}$$

where $\operatorname{div}(f_4) = (mP)-(m-1)(\mathcal{O})-m(P)$. Further, we use the relationship between the divisors of f_3 and f_1 to express $e_{mn}(P,Q)$. Let

$$\begin{aligned}e_{mn}(P,Q) &= \frac{f_1((Q+T)-(T))}{f_2^m((P)-(\mathcal{O}))} && f_1 = f_3 f_4^{-n}\\ &= \frac{f_3 f_4^{-n}((Q+T)-(T))}{f_2^m((P)-(\mathcal{O}))}\\ &= \frac{f_3((Q+T)-(T))f_4^{-n}((Q+T)-(T))}{f_2^m((P)-(\mathcal{O}))}\\ &= \frac{f_3((Q+T)-(T))}{f_4^n((Q+T)-(T))f_2^m((P)-(\mathcal{O}))}\\ &= \frac{f_3((Q+T)-(T))}{f_4(n((Q+T)-(T)))f_2^m((P)-(\mathcal{O}))} && n((Q+T)-(T)) = \operatorname{div}(f_2)\\ &= \frac{f_3((Q+T)-(T))}{f_4(\operatorname{div}(f_2))f_2^m((P)-(\mathcal{O}))} && \text{Weil reciprocity law}\\ &= \frac{f_3((Q+T)-(T))}{f_2(\operatorname{div}(f_4))f_2^m((P)-(\mathcal{O}))}\\ &= \frac{f_3((Q+T)-(T))}{f_2(\operatorname{div}(f_4)+m((P)-(\mathcal{O})))}\end{aligned}$$

$$= \frac{f_3((Q+T)-(T))}{f_2((mP)+(m-1)(\mathcal{O})-m(P)+m(P)-m(\mathcal{O}))}$$
$$= \frac{f_3((Q+T)-(T))}{f_2((mP)-(\mathcal{O}))}$$
$$= e_n(mP, Q).$$

We have shown compatibility for the Weil pairing. □

Proposition 4.14. *The Weil pairing has the following properties:*

1. Bilinearity: $e_n(P+Q, R) = e_n(P, R)e_n(Q, R)$,
   $e_n(P, Q+R) = e_n(P, Q)e_n(P, R)$.

2. Alternating: *If* $P \in E[n]$, *then* $e_n(P, P) = 1$. *Together with linearity, we get that if* $P, Q \in E[n]$, *then* $e_n(Q, P) = e_n(Q, P)^{-1}$

3. Non-degeneracy: *If* $e_n(P, Q) = 1$ *for all* $Q \in E[n]$, *then* $P = \mathcal{O}$.
   If $e_n(P, Q) = 1$ *for all* $P \in E[n]$, *then* $Q = \mathcal{O}$.

4. Compatibility: *Let* $P \in E[mn]$ *and* $Q \in E[n]$. *Then* $e_{mn}(P, Q) = e_n(mP, Q)$.

Proof. The proof of Proposition 4.14 follows immediately Lemma 4.10, 4.11, 4.12 and 4.13. □

4.3 Calculations

The Weil pairing can be calculated using Miller's algorithm. The algorithm allows us to efficiently find functions f_P and f_Q such that we can calculate the Weil pairing using Proposition 4.8. We will describe how to do calculations on an elliptic curve given by $E : y^2 = x^3 + ax + b$. The calculations follow Section XI.8 in Silverman [11].

First, choose an integer n and write the binary expansion,

$$n = \epsilon_0 + \epsilon_1 \cdot 2 + \epsilon_2 \cdot 2^2 + ... + \epsilon_t \cdot 2^t,$$

where $\epsilon_t \neq 0$ and $\epsilon_i \in \{0, 1\}$ for $i = 0, 1, ..., t$. Further, choose two n-torsion points $P = (x_P, y_P), Q = (x_Q, y_Q)$ from the elliptic curve such that they span $E[n]$. In addition, we need a point on the elliptic curve with order different from n, denoted T. As described in Section 4.1.2, we need a function depending on $L_{P,Q}$ and $L_{P+Q,-(P+Q)}$. We consider the line through P and Q. This line is given by $L_{P,Q} : y = \lambda x + \nu$, where the values of λ and ν depend on whether the x-coordinates of P and Q are equal or not. We have that

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}, \qquad x_P \neq x_Q,$$

$$\lambda = \frac{3x_P^2 + a}{2y_P}, \qquad x_P = x_Q,$$
$$\nu = \frac{y_P x_Q - y_Q x_P}{x_Q - w_P}, \qquad x_P \neq x_Q,$$
$$\nu = \frac{-x_P^3 + 2b}{2y_P}, \qquad x_P = x_Q.$$

Given λ and a point, P, on the line the equation for the line is $L_{P,Q} : y = y_P + \lambda(x - x_P)$. The line through $P + Q$ and $-(P + Q)$ is vertical and thus given by $x = x_{P+Q}$. By the addition formula, we get that $x_{P+Q} = \lambda^2 - x_P - x_Q$. It follows that $L_{P+Q,-(P+Q)} : x = \lambda^2 - x_P - x_Q$. The function $g_{P,Q}$ in Definition 4.3 is therefore given by

$$g_{P,Q} = \frac{y - y_P - \lambda(x - x_P)}{x + x_P + x_Q - \lambda^2}.$$

We use Miller's algorithm to find the Weil functions, as shown in Algorithm 1. We evaluate f_P at $-T$ and $Q - T$ and evaluate f_Q at T and $P + T$. By inserting the results into (4.5), we get the desired result.

Algorithm 1 Miller's algorithm

Input: $P \in E[n]$, $T \in E$, $n = (1\epsilon_{t-1}...\epsilon_1\epsilon_0)_2$
Output: $f_{n,P}(T)$

$S \leftarrow P$
$f \leftarrow 1$
for $i = t - 1$ down to 0 **do**
  $f \leftarrow f^2 \cdot g_{S,S}(T)$
  $S \leftarrow 2S$
  if $\epsilon_i = 1$ **then**
    $f \leftarrow f \cdot g_{S,P}(T)$
    $S = S + P$
  end if
end for
return f

Chapter 5

The Tate Pairing

The Tate pairing is based on the work of John Tate [12, 13] and extended by Stephen Lichtenbaum [7]. It is therefore also referred to as the Tate-Lichtenbaum pairing. We describe the pairing in Section 5.1. Further, we state and prove the properties of the Tate pairing in Section 5.2 and show how to calculate the pairing in Section 5.3. The Tate pairing is closely related to the Weil pairing, but we shall see that it requires less computations [11].

5.1 Introduction

In order to define the Tate pairing, we make some assumptions as done in Galbraith, Harrison and Soldera [5]. We consider an elliptic curve E over a finite field $\mathbb{F}_q$ and let n be such that $\gcd(q, n) = 1$ and $n|\#E(\mathbb{F}_q)$, where $\#E(\mathbb{F}_q)$ is the number of points on the elliptic curve over $\mathbb{F}_q$. The presentation of the Tate pairing follows Galbraith [4].

Definition 5.1. Let E and n be as described above and $\boldsymbol{\mu}_n = \{x \in \mathbb{F}_q \mid x^n = 1\}$. Then there are two families of maps, τ_n and t_n, given by

$$\tau_n : E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \to \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^n,$$
$$t_n : E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \to \boldsymbol{\mu}_n.$$

The first is called the Tate pairing and the second is called the modified Tate pairing.

Let us clarify the notation. $E(\mathbb{F}_q)[n]$ denotes the n-torsion points on the elliptic curve. Further, $E(\mathbb{F}_q)/nE(\mathbb{F}_q)$ is a quotient group. $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^n$ can be considered as the set of equivalence classes of $\mathbb{F}_{q^k}^*$, where $a \equiv b$ if and only if there exists a $c \in \mathbb{F}_{q^k}^*$ such that $a = bc^n$.

We define the Tate pairing by choosing $P \in E(\mathbb{F}_q)[n]$ and $Q \in E(\mathbb{F}_q)$. The divisor $n(P) - n(\mathcal{O})$ is principal, and thus there exist a function $f \in \mathbb{F}_q(E)$ such that $\mathrm{div}(f) = n(P) - n(\mathcal{O})$. In addition, we want $\mathfrak{D} \sim (Q) - (\mathcal{O})$ to have support disjoint from $\mathrm{Supp}(\mathrm{div}(f))$ and be a

divisor on E. The Tate pairing is given by

$$\tau_n(P, Q) = f(\mathfrak{D}).$$

We would like the Tate pairing to be well defined, but this is not necessarily the case for the first pairing since it is a map into a quotient group. To fulfill this requirement, we exponentiate the result in $(q^k - 1)/n$, where $k \in \mathbb{N}$ is the smallest nonzero integer such that $n|(q^k - 1)$. This will eliminate all multiples of order n, giving what we call the modified Tate pairing.

Proposition 5.2. *The modified Tate pairing,*

$$t_n(P, Q) = \tau(P, Q)^{(q^k-1)/n},$$

is well defined.

Proof. To prove that the modified Tate pairing is well defined, we first show that the Tate pairing is well defined up to nth powers. This is shown by proving the two following lemmas.

Lemma 5.3. *Let $P \in E(\mathbb{F}_q)[n]$ and let $f \in \mathbb{F}_q(E)$ be such that $\operatorname{div}(f) = n(P) - n(\mathcal{O})$. Further, let $\mathfrak{D}_1, \mathfrak{D}_2$ be divisors on E defined over $\mathbb{F}_q$with disjoint support from $\{\mathcal{O}, P\}$. Suppose that $\mathfrak{D}_1 \sim \mathfrak{D}_2 \sim (Q) - (\mathcal{O})$ for $Q \in E(\mathbb{F}_q)$. Then $f(\mathfrak{D}_1)/f(\mathfrak{D}_2) \in (\mathbb{F}_q^*)^n$.*

Proof. Let $\mathfrak{D}_2 = \mathfrak{D}_1 + \operatorname{div}(h)$ for a function $h \in \mathbb{F}_q(E)$. Then $\operatorname{Supp}(\operatorname{div}(h)) \cap \{\mathcal{O}, P\} = \emptyset$ and

$$f(\mathfrak{D}_2) = f(\mathfrak{D}_1 + \operatorname{div}(h)) = f(\mathfrak{D}_1) f(\operatorname{div}(h)). \tag{5.1}$$

This gives us $f(\mathfrak{D}_2)/f(\mathfrak{D}_1) = f(\operatorname{div}(h))$ and by Weil reciprocity, we have that

$$\begin{aligned} f(\operatorname{div}(h)) &= h(\operatorname{div}(f)) = h(n(P) - n(\mathcal{O})) \\ &= h(n(P))/h(n(\mathcal{O})) = (h(P)/h(\mathcal{O}))^n \in (\mathbb{F}_q^*)^n. \end{aligned}$$

□

Lemma 5.4. *Let $P, f, \mathfrak{D}_1, \mathfrak{D}_2$ be as in Lemma 5.3, but suppose that $\mathfrak{D}_1 \sim (Q_1) - (\mathcal{O})$ and $\mathfrak{D}_2 \sim (Q_2) - (\mathcal{O})$ where $Q_1, Q_2 \in E(\mathbb{F}_q)$ are such that $Q_1 \neq Q_2$ and $Q_1 - Q_2 \in nE(\mathbb{F}_q)$. Then $f(\mathfrak{D}_1)/f(\mathfrak{D}_2) \in (\mathbb{F}_q^*)^n$.*

Proof. Let $Q_1 - Q_2 = [n]R$ for some point $R \in E(\mathbb{F}_q)$. Lemma 5.3 takes care of the case where $R = \mathcal{O}$, so we assume that $R \neq \mathcal{O}$. Further,

$$(Q_1) - (Q_2) = n((R + S) - (S)) + \operatorname{div}(h_0)$$

for some $S \in E(\mathbb{F}_q)$ with $S \notin \{\mathcal{O}, -R, P, P-R\}$ and some $h_0 \in \mathbb{F}_q(E)$. Let

$$\mathfrak{D}_1 = (Q_1) - (\mathcal{O}) + \mathrm{div}(h_1),$$
$$\mathfrak{D}_2 = (Q_2) - (\mathcal{O}) + \mathrm{div}(h_2).$$

We insert this into (5.1) and get that

$$\begin{aligned} f(\mathfrak{D}_2) &= f(\mathfrak{D}_1 - n((R+S) - (S)) + \mathrm{div}(h_2) - \mathrm{div}(h_1) - \mathrm{div}(h_0)) \\ &= f(\mathfrak{D}_1) f((R+S) - (S))^n f(\mathrm{div}((h_2/(h_0 h_1))). \end{aligned}$$

We know that $\mathrm{Supp}(\mathrm{div}(h_2/(h_0h_1))) \subseteq \mathrm{Supp}(\mathfrak{D}_1) \cup \mathrm{Supp}((\mathfrak{D}_2) \cup \{R+S, S\}$ is disjoint from $\{\mathcal{O}, P\}$. Thus, we may use Weil reciprocity to finish the proof.

$$\begin{aligned} f(\mathrm{div}(h_2/(h_0h_1))) &= (h_2/(h_0h_1))(\mathrm{div}(f)) \\ &= (h_2/(h_0h_1))(n(P) - n(\mathcal{O})) \\ &= \frac{(h_2/(h_0h_1))(n(P))}{(h_2/(h_0h_1))(n(\mathcal{O}))} \\ &= \left(\frac{(h_2/(h_0h_1))(P)}{(h_2/(h_0h_1))(\mathcal{O})}\right)^n \in (\mathbb{F}_q^*)^n. \end{aligned}$$

□

The Tate pairing is well defined up to nth powers by Lemma 5.3 and Lemma 5.4. It follows by construction that the modified Tate pairing is well defined. Thus, Proposition 5.2 is proved. □

5.2 Properties

In this section we state and prove some properties of the Tate pairing. The same properties were proved for the Weil pairing in Chapter 4.2, so we focus on the parts that differ from the proofs for the Weil pairing.

The Tate pairing is closely related to the Weil pairing [4, p. 577]. It allows us to make use of some of the same algorithms when proving the properties of the pairings. The Tate pairing is bilinear and nondegenerate and we describe these properties in the following lemmas.

Lemma 5.5 (Bilinearity)**.** *If $P, P_1, P_2 \in E[n]$ and $Q, Q_1, Q_2 \in E/nE$, then*

$$t_n(P_1 + P_2, Q) = t_n(P_1, Q) t_n(P_2, Q),$$
$$t_n(P, Q_1 + Q_2) = t_n(P, Q_1) t_n(P, Q_2).$$

Proof. The proof of bilinearity follows Galbraith [3] and we consider two cases; linearity in first and in second factor.

First, let $P_1 + P_2 = P_3$ and let g be a function such that

$$(P_3) - (\mathcal{O}) = (P_1) - (\mathcal{O}) + (P_2) - (\mathcal{O}) + (g).$$

If f_1 and f_2 are such that $(f_1) = n(P_1) - n(\mathcal{O})$ and $(f_2) = n(P_2) - n(\mathcal{O})$, then

$$\begin{aligned}(f_1 f_2 g^n) &= (f_1) + (f_2) + (g^n) \\ &= (f_1) + (f_2) + n(g) \\ &= n(P_1) - n(\mathcal{O}) + n(P_1) - n(\mathcal{O}) + n(g) \\ &= n(P_1) - n(\mathcal{O}) + n(P_1) + n(g) - n(\mathcal{O}) \\ &= n(P_3) - n(\mathcal{O}).\end{aligned}$$

We let $\mathfrak{D} \sim (Q) - (\mathcal{O})$ be such that $\mathrm{Supp}(\mathfrak{D}) \cap \mathrm{Supp}\{P_1, P_2, P_3, Q\} = \emptyset$. This gives,

$$t_n(P_1 + P_2, Q) = t_n(P_3, Q) = f_1 f_2 g^n(\mathfrak{D}) = f_1(\mathfrak{D}) f_2(\mathfrak{D}) g(\mathfrak{D})^n.$$

Since we work in $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^n$, we get that $g(\mathfrak{D})^n = 1$. It follows that

$$f_1(\mathfrak{D}) f_2(\mathfrak{D}) g(\mathfrak{D})^n = t_n(P_1, Q) t_n(P_2, Q),$$

and we have completed the proof of linearity in the first factor.

Next, let us consider linearity in second factor. First, we assume that $Q_1 + Q_2 = Q_3$. Further, we observe that if $\mathfrak{D}_1 \sim (Q_1) - (\mathcal{O})$ and $\mathfrak{D}_2 \sim (Q_2) - (\mathcal{O})$, then $\mathfrak{D}_1 + \mathfrak{D}_2 \sim (Q_3) - (\mathcal{O})$. We use this to show linearity in second factor,

$$\begin{aligned}t_n(P, Q_1 + Q_2) &= t_n(P, Q_3) \\ &= f(\mathfrak{D}_1 + \mathfrak{D}_2) \\ &= f(\mathfrak{D}_1) f(\mathfrak{D}_2) \\ &= t_n(P, Q_1) t_n(P, Q_2).\end{aligned}$$

□

Lemma 5.6 (Non-degeneracy)**.** *If $\mathcal{O} \neq P \in E[n]$, then there exists $Q \in E$ such that $t_n(P, Q) \notin (\mathbb{F}_{q^k}^*)^n$.*

Proof. The proof of nondegeneracy follows Washington [15]. Let $Q \in E(\mathbb{F}_q)$ and let $Q = nR$ for some $R \in E(\overline{\mathbb{F}_q})$. Recall that $\phi = \phi_q$ is the qth power Frobenius endomorphism. We assume

that

$$\tau_n(P,Q) = e_n(P, R - \phi R) = 1 \text{ for all } P \in E(\mathbb{F}_q)[n],$$

and want to show that this is only possible if $Q \in nE(\mathbb{F}_q)$ which proves nondegeneracy in the second factor. Next, we want to show that nondegeneracy in the first factor follows from the fact that $E(\mathbb{F}_q)[n]$ and $E(\mathbb{F}_q)/nE(\mathbb{F}_q)$ have the same order. In order to do this we have to state and prove multiple lemmas.

Let $\langle , \rangle : B \times A \to \boldsymbol{\mu}_n$ be a bilinear pairing with A, B finite abelian groups written additively. Choose the pairing such that $na = 0$ for all $a \in A$ and $nb = 0$ for all $b \in B$, $n \geq 1$. We consider the homomorphism, $\psi_n : b \mapsto \langle b, a \rangle$ for a fixed a and let the set of homomorphisms from B to $\boldsymbol{\mu}_n$ be denoted $\mathrm{Hom}(B, \boldsymbol{\mu}_n)$. We define a product for the group by letting

$$(\alpha \cdot \beta)(b) = \alpha(b) \cdot \beta(b) \text{ for all } b \in B$$

where $\alpha, \beta \in \mathrm{Hom}(B, \boldsymbol{\mu}_n)$.

We need to show that nondegeneracy in the second factor implies nondegeneracy in the first factor. To do this, we show that it holds for groups of the same order, and show that they indeed have the same order.

Lemma 5.7. *Assume $\langle , \rangle : B \times A \to \boldsymbol{\mu}_n$ is nondegenerate in A. Then,*

1. *The map from A to Hom$(B, \boldsymbol{\mu}_n)$ given by $a \mapsto \psi_n$ is injective.*
2. *If $\#A = \#B$, then $\langle , \rangle$ is nondegenerate in B.*

Proof. Suppose that $\langle b, a \rangle = \psi_a(b) = 1$ for all $b \in B$. Then, by nondegeneracy of A, we get that $a = 0$. Thus, $a \mapsto \psi_a$ is injective and we have completed the proof of (1). Further, assume that $\#A = \#B$ and let

$$B_1 = \{b \in B | \langle b, a \rangle = 1 \text{ for all } a \in A\}.$$

Then, for each $a \in A$, we have that $\beta_a : B/B_1 \to \boldsymbol{\mu}_n$ is a well defined homomorphism given by $\beta_a(b \mod B_1) = \langle b, a \rangle$. By (1) we know that the map $A \to \mathrm{Hom}(B/B_1, \boldsymbol{\mu}_n)$ is injective. By Lemma 11.26 in [15] we know that $\mathrm{Hom}(B/B_1, \boldsymbol{\mu}_n)$ has order $\#B/\#B_1$. We have already assumed that $\#A = \#B$, but then we must have $\#B_1 = 1$. It follows that $B_1 = 0$, giving us that $\langle , \rangle$ is nondegenerate in B. □

Lemma 5.8. *Let A, B and M be finite abelian groups written additively.*

1. *Suppose that $\langle , \rangle : B \times A \to \boldsymbol{\mu}_n$ is nondegenerate in both A and B. Then $\#A = \#B$, and $A \simeq \mathrm{Hom}(B, \boldsymbol{\mu}_n)$ and $B \simeq \mathrm{Hom}(A, \boldsymbol{\mu}_n)$.*

2. *Let $\alpha : M \to M$ be a homomorphism. Then $\# \operatorname{Ker} \alpha = \#M/\#\alpha(M)$.*

Proof. 1. We have an injection from A to $\operatorname{Hom}(B, \boldsymbol{\mu}_n)$ by Lemma 5.7, so

$$\#A \leq \# \operatorname{Hom}(B, \boldsymbol{\mu}_n) = \#B.$$

By the same argument, we have that

$$\#B \leq \# \operatorname{Hom}(A, \boldsymbol{\mu}_n) = \#A.$$

Thus, $\#A = \#B$, and the injections are isomorphisms.

2. The result follows from Theorem B.6 in [15], where it is stated that

$$\#M = (\# \operatorname{Ker} \alpha)(\#\alpha(M)).$$

□

We have seen in Lemma 5.7 that nondegeneracy in first factor follows from nondegeneracy in second factor if the groups have the same order. To prove that they do, the next lemma is crucial.

Lemma 5.9. *Assume A and B are finite abelian groups such that $nx = 0$ for all $x \in A$ and for all $x \in B$. Suppose that $\langle , \rangle : B \times A \to \boldsymbol{\mu}_n$ is a bilinear pairing and nondegenerate in both A and B. Let C be a subgroup of B and define a mapping*

$$\psi : A \to \prod_{c \in C} \boldsymbol{\mu}_n, \qquad \text{where } a \mapsto (..., \langle c, a \rangle, ...).$$

Then $\#\psi(A) = \#C$.

Proof. By Lemma 5.8, $A \simeq \operatorname{Hom}(B, \boldsymbol{\mu}_n)$. We express the kernel of ψ, first in terms of A and then using the isomorphism.

$$\operatorname{Ker} \psi = \{a \in A \mid \langle c, a \rangle = 1, \text{ for all } c \in C\},$$
$$\operatorname{Ker} \psi = \{f \in \operatorname{Hom}(B, \boldsymbol{\mu}_n) \mid f(C) = 1\}.$$

Note that a homomorphism from B/C to $\boldsymbol{\mu}_n$ sends C to 1, but this is the same as our homomorphism does. We know that a homomorphism from B/C to $\boldsymbol{\mu}_n$ has order $\#(B/C) = \#B/\#C$. We use that $\#A = \#B$ and finish the proof by observing that

$$\#\psi(A) = \#A/\# \operatorname{Ker} \psi = \#A/\#(B/C) = \#C.$$

□

Lemma 5.10. *Let $\phi = \phi_q$ be the qth power Frobenius endomorphism of E. Then* $\operatorname{Ker}\psi = (\phi - 1)E[n]$.

The proof of Lemma 5.10 is out of scope for this thesis, but a proof can be found in [15, p. 379].

Recall our assumption that $\tau_n(P, Q) = e_n(P, R - \phi R) = 1$ for all $P \in E(\mathbb{F}_q)[n]$. Then, $R - \phi R \in \operatorname{Ker}\psi$. From Lemma 5.10 we know that $\operatorname{Ker}\psi = (\phi - 1)E[n]$, but then $R - \phi R = \phi T - T$ for some $T \in E[n]$. We get that $\phi(R + T) = R + T$ and know that $R + T$ gets coordinates in $\mathbb{F}_q$, by properties of ϕ. It follows that $R + T \in E(\mathbb{F}_q)$.

By construction, $Q = nR = nR + \mathcal{O} = nR + nT = n(R + T)$. Thus, $Q \in nE(\mathbb{F}_q)$. We have therefore shown that

$$t_n : E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \to \boldsymbol{\mu}_n.$$

is nondegenerate in the second factor. By Lemmas 5.7 and 5.8 with $\alpha = n$, $E(\mathbb{F}_q)[n]$ and $E(\mathbb{F}_q)/nE(\mathbb{F}_q)$ have the same order and the pairing is indeed nondegenerate in first factor. □

5.3 Calculations

We calculate the Tate pairing using Miller's algorithm, as described in Algorithm 1. Consider an elliptic curve $E : y^2 = x^3 + ax + b$, and let $\mathfrak{D} \sim (Q) - (\mathcal{O})$ be a divisor. Further, choose $P \in E(\mathbb{F}_q)[n]$ and $Q \in E(\mathbb{F}_q)$. By Proposition 5.2,

$$t_n(P, Q) = f(\mathfrak{D})^{(q^k-1)/n}.$$

To find function a f, we apply Miller's algorithm to $\mathfrak{D}$. The calculations are done as in Section 4.3, but we only need to use Miller's algorithm once to find the Tate pairing.

Chapter 6

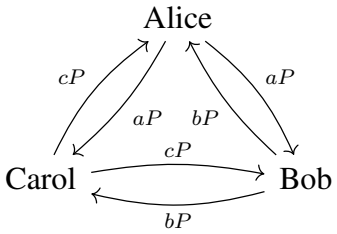
Pairings in Cryptography

6.1 Tripartite Diffie-Hellman

The tripartite Diffie-Hellman key agreement allows three persons to agree on a shared secret key using pairings on elliptic curves. The first version was given by Joux in [6] and required agreement of two independent points on an elliptic curve. Later, Verheul [14] gave a protocol using one point P and a distortion map. A distortion map Ψ is defined as follows. Let P, Q be points such that $\mathrm{ord}(P) = n$ and $\mathcal{O} \neq Q \in \langle P \rangle$. Then Ψ is an endomorphism that maps Q to a point independent of Q, denoted $\Psi(Q)$, where $\Psi(Q) \in E[n]$. Verheul suggests to use a version of the modified Tate pairing given by

$$\hat{t}_n(P, Q) = t_n(P, \Psi(Q)). \tag{6.1}$$

Figure 6.1 Tripartite Diffie-Hellman



Let Alice, Bob and Carol be three persons who want to agree on a shared key. First, they decide upon an elliptic curve E over $\mathbb{F}_q$ and a point $P \in E(\mathbb{F}_q)$ in public. Their second step is to individually choose an element at random from $\{1, \ldots, n-1\}$. They choose a, b and c, respectively. Alice computes and publishes aP, as shown in Figure 6.1. In the same way, Bob and Carol publishes bP and cP. Now, they can all compute their shared key using the pairing

given in (6.1). They get the shared key

$$\hat{t}_n(P,P)^{abc} = \hat{t}_n(bP,cP)^a = \hat{t}_n(aP,cP)^b = \hat{t}_n(aP,bP)^c.$$

The security of the tripartite Diffie-Hellman protocol relies on the difficulty of computing $\hat{t}_n(P,P)^{abc}$ if you are given (P, aP, bP, cP) where a, b, c are random numbers.

6.2 The MOV-attack

Menezes, Okamoto and Vanstone gave name to the MOV-attack when publishing [9]. The attack consists of a reduction from a discrete logarithm problem on an elliptic curve to a discrete logarithm problem in a finite field. They use the Weil pairing to reduce a problem from E($\mathbb{F}_q$) to $\mathbb{F}_{q^k}^*$.

Let $P, Q \in E(\mathbb{F}_q)$, $\mathrm{ord}(P) = n$ and assume that $\gcd(q, n) = 1$. The problem handled in the MOV-attack is to find an a such that $aP = Q$, given that such an a exists. This can be done using the Weil pairing and the following is a simple example.

Let $S \in E[n]$ and $u = e_n(P,S), v = e_n(Q,S)$. The Weil pairing is bilinear and thus

$$v = e_n(Q,S) = e_n(aP,S) = e_n(P,S)^a = u^a.$$

Since this is a discrete logarithm problem in $\mathbb{F}_{q^k}$, it can be solved there instead.

We are not guaranteed that there exists an a such that $aP = Q$, as showed in the next lemma.

Proposition 6.1. *There exists an a such that $aP = Q$ if and only if $Q \in E[n]$ and $e_n(P,Q) = 1$.*

Proof. The proof follows [15, p. 155].

Let $aP = Q$. Then $nQ = n(aP) = a(nP) = \mathcal{O}$ and thus $Q \in E[n]$. We observe that $e_n(P,Q) = e_n(P,aP) = e_n(P,P)^a = 1^a = 1$.

Now, assume that $Q \in E[n]$ and $e_n(P,Q) = 1$. We know that $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by Theorem 3.2 in [15, p. 79]. Let R be a point such that $\{P, R\}$ is a basis of $E[n]$. Thus, we can express Q as a linear combination of P and R, $Q = xP + yR$ for some integers x, y. It can be shown that $e_n(P,R) = \zeta$ is a primitive nth root of unity [15, p. 87]. By assuming $e_n(P,Q) = 1$, we get

$$1 = e_n(P,Q) = e_n(P, xP + yR) = e_n(P,P)^x e_n(P,R)^y = \zeta^y.$$

Hence, $y \equiv 0 \pmod{n}$, giving us $yR = \mathcal{O}$. It follows that $Q = xP$. □

Bibliography

[1] Bhattacharya, P. B., Jain, S. K., Nagpaul, S., 1994. Basic abstract algebra. Cambridge University Press.

[2] Fulton, W., 2008. Algebraic curves: an introduction to algebraic geometry. Addison-Wesley.

[3] Galbraith, S., 2005. Pairings. London Mathematical Society Lecture Note Series. Cambridge University Press, p. 183–214.

[4] Galbraith, S. D., 2012. Mathematics of public key cryptography. Cambridge University Press.

[5] Galbraith, S. D., Harrison, K., Soldera, D., 2002. Implementing the Tate pairing. In: International Algorithmic Number Theory Symposium. Springer, pp. 324–337.

[6] Joux, A., 2000. A one round protocol for tripartite Diffie–Hellman. In: International algorithmic number theory symposium. Springer, pp. 385–393.

[7] Lichtenbaum, S., 1969. Duality theorems for curves over p-adic fields. Inventiones mathematicae 7 (2), 120–136.

[8] Maas, M., 2004. Pairing-based cryptography. Master's thesis, Technische Universiteit Eindhoven.

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

[10] Miller, V. S., 2004. The Weil pairing, and its efficient calculation. Journal of cryptology 17 (4), 235–261.

[11] Silverman, J. H., 2009. The arithmetic of elliptic curves, 2nd Edition. Vol. 106 of Graduate texts in mathematics. Springer, Dordrecht.

[12] Tate, J., 1958. wc-groups over p-adic fields. In: Séminaire Bourbaki : années 1956/57 - 1957/58, exposés 137-168. No. 4 in Séminaire Bourbaki. Société mathématique de France, pp. 265–277, talk:156.
URL http://www.numdam.org/item/SB_1956-1958__4__265_0

[13] Tate, J., 1962. Duality theorems in galois cohomology over number fields. In: Proc. Internat. Congr. Mathematicians (Stockholm, 1962). pp. 288–295.

[14] Verheul, E. R., 2004. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. Journal of Cryptology 17 (4), 277–296.

[15] Washington, L. C., 2003. Elliptic curves: number theory and cryptography. Chapman and Hall/CRC.

Appendix A

Example 3.3:

```
A = 0
B = 37
E = EllipticCurve([A, B]); print E

points = E.integral_points()
O = E(0)

print ("The curve has these points with integer coefficients:")
print points
print ("The infinity point is given by O = " + str(O))

P = points[0]
Q = points[1]
R = points[2]

if P + Q == -(P + R):
    print "We observe that P + Q = -(P + R), where"
    print "(P+Q) = " + str(P+Q)
    print "(P+R) = " + str(P+R)
```