TECHNISCHE
UNIVERSITÄT
WIEN

VIENNA
UNIVERSITY OF
TECHNOLOGY

D I P L O M A R B E I T

Mathematical Foundations of Elliptic Curve Cryptography

Ausgeführt am Institut für
Diskrete Mathematik und Geometrie
der Technischen Universität Wien

unter Anleitung von
Univ.Prof. Dipl.-Ing. Dr. techn. Michael Drmota

durch
Clemens Koppensteiner
Bertolt Brecht Gasse 6
2353 Guntramsdorf

_____   _____
Datum   Unterschrift

This diploma thesis was submitted on May 11, 2009. The contents of this document are identical to the submitted and graded version.

For updated versions see `http://www.caramdir.at/diplomarbeit`.

Contents

Introduction

If one drew a map of mathematical theories, the theory of elliptic curves would lie very much near the center of that map. It draws from and connects several integral parts of mathematics: analysis and the theory of functions, abstract algebra and algebraic geometry as well as number theory. In the last twenty-five years elliptic curves have been both used to solve long-outstanding problems of pure mathematics and to derive fast algorithms for practical use.

The central role of elliptic curves is made possible by them simultaneously being very simple and having a deep theory. Indeed from the standpoint of algebraic geometry they are the simplest non-trivial objects; but their theory is far from trivial. This is prominently shown by the modularity theorem (also known as Taniyama–Shimura–Weil conjecture): Even the precise statement of the theorem needs an astonishing amount of interesting mathematics [Dar99]. However here again elliptic curves are just a "simple" case: The modularity theorem can been considered to be a special case of the (mostly unproven) Langlands program.

Since 1985 a very unlikely group of people has become increasingly interested in elliptic curves: cryptographers. The first practical public key cryptosystems were published by Diffie and Hellman in 1976 [DH76] and Rivest, Shamir and Adleman in 1977 [RSA78][1]. Variants of these systems are still in use today. They rely on the difficulty of computing discrete logarithms in $\mathbb{Z}/p\mathbb{Z}$ (p prime) and factoring integers respectively. For both problems no polynomial time algorithms are known (on classical computers). However, subexponential algorithms were developed for both problems during the 1980s. Therefore the minimal bit size needed to guarantee secure communications had to be increased so much that it became impractical for some implementations. As a solution to this problem cryptography schemes based on the discrete logarithm problem on elliptic curves were proposed. Nowadays many encryption schemes are based on this idea.

The introduction of elliptic curves to cryptography lead to the interesting situation that many theorems which once belonged to the purest parts of pure mathematics are now used for practical cryptoanalysis. Therefore in order to analyze elliptic curve cryptography (ECC) it is necessary to have a thorough background in the theory of elliptic curves. The goal of this diploma thesis is to provide such a background.

This document consists of two parts: The first part, consisting of chapters 1–4 is a purely mathematical introduction to elliptic curves. Since it is impossible to reproduce the whole theory in the restricted space of a diploma thesis, many theorems will not be proven here. Instead the focus is on the theorems of particular interest to ECC. To the author's knowledge there is no such collection of these theorems available.

The second part – consisting of chapters 5–7 – shows how the theory can be used for cryptographical purposes and cryptoanalysis. While this is the more "practical" part, the focus will still be on the theory and no complete implementations are given.

The idea behind this thesis to form a bridge between the abstract texts on elliptic curves (such as [Sil92]) and concrete texts for cryptographers (such as [BSS99] and [BSS05]). It should provide enough background to read and work on current research on ECC.

---

[1]These were the first publicly published efficient public key cryptosystems. As is now known, similar systems had been developed by Ellis, Cocks and Williamson at the GCHQ (a UK intelligence agency) in the early 1970s.

Chapter 1

Algebraic Curves

It is possible to prove many theorems about elliptic curves using elementary (ad-hoc) methods. For example this is done in [ST92]. However in order to really understand the theory of elliptic curves, the framework provided by algebraic geometry is necessary. Even for "simple" theorems the language of algebraic geometry often greatly simplifies the notation and makes proofs more transparent. Therefore we will dedicate the present chapter to an introduction of the theory of algebraic curves. However in order to keep this chapter as short as possible, we have to make two concessions: First, we will only consider curves embedded into a surrounding space, and second, we will skip (nearly) all proofs.

We will follow the first two chapters of [Sil92] quite closely. When not stated otherwise, proofs (or at least references to them) can be found there. Naturally this chapter introduces only a small part of the concepts found in algebraic geometry. A very readable introductory text to algebraic geometry is the two books by Shafarevich [Sha94a, Sha94b]. A good and rather elementary introduction to algebraic curves is the classic [Ful89]. In particular Fulton covers the important concepts of intersection numbers and normalization (i.e. removing of singularities) which we will not discuss here. Of course no list of reference works on algebraic geometry is complete without [Har77], but it is not recommended to read Hartshorne's book without having had any prior exposure to the subject.

First we will fix some notation that is used throughout this thesis: When not defined otherwise, K is always a *perfect* field, i.e. every algebraic extension of K is separable. This is no real restriction as all fields that are cryptographically interesting have this property. The algebraic closure of a field K is denoted $\bar{K}$. If $L|K$ is a Galois extension then the Galois group of this extension is denoted $\mathrm{Gal}(L|K)$.

1.1 Basics of Algebraic Geometry

We will begin with a lot of definitions.

Definition 1.1. The *affine n-space over K* is the set

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \left\{ (x_1, \ldots, x_n) : x_i \in \bar{K} \right\}.$$

The set of *K-rational points in $\mathbb{A}^n$* is

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

The group $\mathrm{Gal}(\bar{K}|K)$ acts on $\mathbb{A}^n$ by $P^\sigma = (\sigma(x_1), \ldots, \sigma(x_n))$ for $\sigma \in \mathrm{Gal}(\bar{K}|K)$ and $P = (x_1, \ldots, x_n)$. Obviously the K-rational points of $\mathbb{A}^n(K)$ are exactly the points fixed under this action.

Let $K[X] = K[X_1, \ldots, X_n]$ be the polynomial ring in n variables over K.

Definition 1.2. To every subset $S \subseteq \bar{K}[X]$ associate its *zero set*

$$Z(S) = \{ P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in S \}.$$

A set $Y \subseteq \mathbb{A}^n$ is called an *(affine) algebraic set* if there exists $S \subseteq K[X]$ with $Y = Z(S)$.

Definition 1.3. Let $Y \subseteq \mathbb{A}^n$. Then the *ideal associated to* Y is

$$I(Y) = \left\{ f \in \bar{K}[X] : f(P) = 0 \text{ for all } P \in Y \right\}.$$

An algebraic set Y is *defined over* K if $I(Y)$ can be generated by polynomials in K[X]. This is denoted by Y/K. If Y is defined over K, the set of *K-rational points of* Y is the set

$$Y(K) = Y \cap \mathbb{A}^n(K).$$

One easily checks that $I(Y)$ is indeed an ideal. Note that by the Hilbert basis theorem [AM69, theorem 7.5], $\bar{K}[X]$ is a Noetherian ring and thus $I(Y)$ is always finitely generated. The K-rational points can also be characterized by

$$Y(K) = \left\{ P \in Y : P^\sigma = P \text{ for all } \sigma \in \mathrm{Gal}(\bar{K}|K) \right\}.$$

Theorem 1.4. *The union of two algebraic sets is an algebraic set. The intersection of an arbitrary family of algebraic sets is an algebraic set. The empty set $\emptyset$ and the whole space $\mathbb{A}^n$ are algebraic sets.*

Proof. [Har77, proposition I.1.1] $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ □

Definition 1.5. The topology on $\mathbb{A}^n$ with closed sets exactly the algebraic sets is called *Zariski topology*. By the last theorem it is indeed a topology.

Definition 1.6. A closed subset of a topological space is called *irreducible*, if it cannot be expressed as the union of two closed proper subsets. The empty set is not considered to be irreducible.

An algebraic set $V \subseteq \mathbb{A}^n$ that is irreducible with respect to the Zariski topology is called *(affine) variety*.

Theorem 1.7. *The functions $I : \mathfrak{P}(\mathbb{A}^n) \to \mathfrak{P}(\bar{K}[x])$ and $V : \mathfrak{P}(\bar{K}[x]) \to \mathfrak{P}(\mathbb{A}^n)$ are compatible with the inclusion of sets. For an ideal $\mathfrak{a} \subseteq \bar{K}[X]$,*

$$I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}} = \left\{ f \in \bar{K}[X] : \exists n \in \mathbb{N} : f^n \in \mathfrak{a} \right\}.$$

For any subset $Y \subseteq \mathbb{A}^n$,

$$Z(I(Y)) = \bar{Y},$$

the topological closure of Y. Therefore there is a one-to-one inclusion-reversing correspondence between algebraic set in $\mathbb{A}^n$ and radical ideals of $\bar{K}[X]$. An algebraic set is irreducible if and only if its ideal is prime.

Proof. [Har77, proposition I.1.2 and corollary I.1.4]. Note that the only hard part is $I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}$, which is Hilbert's Nullstellensatz [Mat80, (14.L)] and depends on the fact that $\bar{K}$ is algebraically closed. $\qquad$ □

Definition 1.8. Let V/K be an affine variety. The *affine coordinate ring of* V/K is

$$K[V] = K[X]/\left(I(V) \cap K[X] \right).$$

By the last theorem it is an integral domain. Its field of fractions is called the *function field of* V/K, denoted $K(V)$.

Every element $f \in \bar{K}[V]$ induces a well defined function on V: Choose $F \in \bar{K}[X]$ such that $f = F \bmod I(V)$ and set $f(P) = F(P)$. The Galois group $\mathrm{Gal}(\bar{K}|K)$ acts on $F \in \bar{K}[X]$ by acting on its coefficients. If V is defined over K, then $\mathrm{Gal}(\bar{K}|K)$ takes $I(V)$ to itself and we obtain actions on $\bar{K}[V]$ and $\bar{K}(X)$. The sets $K[V]$ resp. $K(V)$ are exactly the fixed points of this action. For every $f \in \bar{K}[V]$, $\sigma \in \mathrm{Gal}(\bar{K}|K)$ and $P \in V(\bar{K})$ we have $(f(P))^\sigma = f^\sigma(P^\sigma)$.

Definition and Proposition 1.9. *Let V be an affine variety. Then the following numbers are finite and equal:*

1. *The supremum of all integers n such that there exists a chain $Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n$ of distinct irreducible closed subsets of V.*

2. *The Krull dimension of $\bar{K}[V]$, i.e. the supremum of all integers n such that there exists a chain $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ of distinct prime ideals of $\bar{K}[V]$.*

3. *The transcendence degree of $\bar{K}(V)$ over $\bar{K}$.*

This number is called the dimension of V, *denoted* $\dim(V)$.

Proof. The equivalence of the topological dimension of V and the Krull dimension of $\bar{K}[V]$ is easy. See also [Har77, proposition I.1.7]. The equality to $\operatorname{trdeg}_{\bar{K}} K(V)$ follows from the Noether normalization theorem [Mat80, (14.G)]. □

For an affine variety V and any point $P \in V$ define an ideal $\mathfrak{m}_P$ of $\bar{K}[V]$ by

$$\mathfrak{m}_P = \left\{ f \in \bar{K}[V] : f(P) = 0 \text{ for all } P \in V \right\}.$$

Since $\bar{K}[V]/\mathfrak{m}_P = \bar{K}$, $\mathfrak{m}_P$ is a maximal ideal. Also note that $\mathfrak{m}_P/\mathfrak{m}_P^2$ is a $\bar{K}$-vector space.

Definition 1.10. Let V be an affine variety and let $P \in V$. Then the *local ring of V at P*, denoted $\bar{K}[V]_P$, is the localization[1] $\bar{K}[V]_{\mathfrak{m}_P}$ of $\bar{K}[V]$ at $\mathfrak{m}_P$. An element $f \in \bar{K}(V)$ is *regular* (or *defined*) at P, if it is in $\bar{K}[V]_P$. If $f = \frac{g}{h}$ this is equivalent to $h(P) \neq 0$ and hence $f(P) = \frac{g(P)}{h(P)} \in \bar{K}$ is well-defined.

Proposition 1.11. *If $f \in \bar{K}(V)$ is regular at every point of V, then $f \in \bar{K}[V]$.*

Proof. [Har77, thm. I.3.2] □

Definition and Proposition 1.12. *Let V be a variety in $\mathbb{A}^n$ and $P \in V$. Then the following statements are equivalent:*

1. *Let $f_1, \ldots, f_m \in \bar{K}[V]$ be a set of generators of $I(V)$. Then the rank of the Jacobian matrix*

$$\left(\frac{\partial f_i}{\partial X_j}(P) \right)_{\substack{1 \le i \le m \\ 1 \le j \le n}}$$

   is $n - \dim(V)$.

2. *The local ring $\bar{K}[V]_P$ is a regular local ring, i.e. the minimal number of generators of $\mathfrak{m}_P$ is equal to the Krull dimension of $\bar{K}[V]_P$.*

3. $\dim(V) = \dim_{\bar{K}}(\mathfrak{m}_P/\mathfrak{m}_P^2)$, *where $\dim_{\bar{K}}$ denotes the dimension as a $\bar{K}$-vector space.*

It this case V is non-singular *(or* smooth*) at P. Otherwise P is a* singular point *of V. A variety that is non-singular at every point is called* non-singular *(or* smooth*).*

Proof. For the equivalence of (2) and (3) note that $\dim(V) = \dim \bar{K}[V]$ and use [AM69, cor. 3.13] and [AM69, thm. 11.22]. For the equivalence of (1) and (3) see [Har77, thm. I.5.1]. □

An interesting corollary is that one can intrinsically define the tangent space of a variety V at point P to be $(\mathfrak{m}_P/\mathfrak{m}_P^2)^*$. By Taylor expansion this is equivalent to the "usual" definition using the surrounding space.

For several reasons (some of them will become apparent later) the natural setting for algebraic geometry is not affine, but projective space:

Definition 1.13. The *projective n-space over K* is given by

$$\mathbb{P}^n = \mathbb{P}^n(\bar{K}) = (\mathbb{A}^{n+1} \setminus \{0\})/\bar{K}^*.$$

In other words, $\mathbb{P}^n$ is the set of non-zero $(n+1)$-tuples over $\bar{K}$ where two tuples are identified when they are multiples of each other. A point of $\mathbb{P}^n$ is given by *homogeneous* (or *projective*) *coordinates* $[x_0 : x_1 : \cdots : x_n]$. The set of *$K$-rational points of $\mathbb{P}^n$* is given by

$$\mathbb{P}^n(K) = \left\{ [x_0 : \cdots : x_n] \in \mathbb{P}^n : \text{all } x_i \in K \right\}.$$

(Note that this only needs to be true for one representation of the point.)

---

[1] The localization of an integral domain A at a prime ideal $\mathfrak{p} \subset A$ is

$$A_{\mathfrak{p}} = \left\{ \frac{a}{b} : a \in A, b \in A \setminus \mathfrak{p} \right\} \subseteq \operatorname{Quot}(A)$$

with the usual sum and product of fractions.

Again the Galois group acts on $\mathbb{P}^n$ by acting on the coordinates and the K-rational points are exactly the points fixed by $\mathrm{Gal}(\bar{K}|K)$.

Definition 1.14. A polynomial $f \in \bar{K}[X_0, \ldots, X_n]$ is *homogeneous of degree d* if $f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n)$ for all $\lambda \in \bar{K}$. An ideal of $\bar{K}[X]$ is called *homogeneous* if it is generated by homogeneous polynomials.

While in general it is not possible to evaluate a polynomial f at a point P of projective space, if f is homogeneous it makes sense to ask whether $f(P) = 0$.

Definition 1.15. To every homogeneous ideal $\mathfrak{h} \subseteq \bar{K}[X_0, \ldots, X_n]$ associate its *zero set*

$$Z(\mathfrak{h}) = \{P \in \mathbb{A}^n : f(P) = 0 \text{ for all homogeneous } f \in \mathfrak{h}\} \subseteq \mathbb{P}^n.$$

Every set $Y \subseteq \mathbb{A}^n$ such that there exists $\mathfrak{h} \subseteq K[X]$ with $Y = Z(\mathfrak{h})$ is called a *(projective) algebraic set*.

Let $Y \subseteq \mathbb{P}^n$. Then the *(homogeneous) ideal $I(Y)$ associated to Y* is the homogeneous ideal generated by all homogeneous polynomials of $\bar{K}[X]$ that vanish at all points of Y. The *homogeneous coordinate ring of Y* is $\bar{K}[X]/I(Y)$. An algebraic set Y is *defined over K* if $I(Y)$ can be generated by homogeneous polynomials $f \in K[X]$. This is denoted by V/K. If V is defined over K, the set of *K-rational points of V* is the set

$$Y(K) = Y \cap \mathbb{P}^n(K).$$

The topology on $\mathbb{P}^n$ with closed sets exactly the algebraic sets is called *Zariski topology*. Again one easily checks that it is indeed a topology. An algebraic set is called a *(projective) variety* if it is irreducible or equivalently if its associated ideal is prime.

For each $0 \le i \le n$ there is an inclusion $\phi_i \colon \mathbb{A}^n \hookrightarrow \mathbb{P}^n$, given by

$$\phi_i(x_1, \ldots, x_n) = [x_1 : \cdots : x_{i-1} : 1 : x_i : \cdots : x_n].$$

The set $\mathbb{P}^n \setminus \phi_i(\mathbb{A}^n) = V(\langle X_i \rangle)$ is closed. Thus $\mathbb{P}^n$ is covered by the open sets $U_i = \phi_i(\mathbb{A}^n)$. One can easily show that all ϕ_is are homeomorphisms [Har77, proposition I.2.2]. In other words every point of $\mathbb{P}^n$ has an open affine neighborhood. The sets U_i are called *affine pieces of $\mathbb{P}^n$*.

To each polynomial $f \in \bar{K}[X_1, \ldots, X_n]$ of degree d one can associate its *homogenization with respect to X_i*. This is the homogeneous polynomial $f^h \in \bar{K}[Y_0, \ldots, Y_n]$ given by

$$f^h(Y_0, \ldots, Y_n) = Y_i^d f\left(\frac{Y_0}{Y_i}, \ldots, \frac{Y_{i-1}}{Y_i}, \frac{Y_{i+1}}{Y_i}, \ldots, \frac{Y_n}{Y_i}\right).$$

This process can be reversed by associating to every homogeneous polynomial $f \in \bar{K}[Y]$ of degree d its *dehomogenization with respect to Y_i* which is

$$f^d(X_1, \ldots, X_n) = f(X_1, \ldots, X_{i-1}, 1, X_{i+1}, \ldots, X_n).$$

Fix an affine piece U_i of $\mathbb{P}^n$ and identify it with $\mathbb{A}_i$. Let $Y \subseteq \mathbb{A}_i$ be an algebraic set. Its *projective closure* $\bar{V} \subseteq \mathbb{P}^n$ is just the topological closure of V in $\mathbb{P}^n$ with respect to the Zariski topology. Its ideal is given by

$$I(\bar{V}) = \langle f^h : f \in I(V) \rangle$$

Proposition 1.16. *If V is an affine variety, then $\bar{V}$ is a projective variety and $\bar{V} \cap \mathbb{A}^n = V$.*

If V is a projective variety, then $V \cap \mathbb{A}^n$ is an affine variety and $V \cap \mathbb{A}^n = \emptyset$ or $\overline{V \cap \mathbb{A}^n} = V$.

If an affine (resp. projective) variety V is defined over K, then $\bar{V}$ (resp. $V \cap \mathbb{A}^n$) is also defined over K.

We will usually give a variety by its equations in affine space with the understanding that its projective closure is considered. The points in $\bar{V} \setminus V$ are called *points at infinity*.

Definition 1.17. Let V be a projective variety. The *function field* of V, denoted $\bar{K}(V)$, consists of equivalence classes of fractions $\frac{f}{g}$, with f and g homogeneous polynomials of the same degree and $g \notin I(V)$ where two frations $\frac{f}{g}$ and $\frac{f'}{g'}$ are considered equal if $fg' - f'g \in I(V)$. (In other words it is the degree zero part of the localization of $\bar{K}[V]$ with respect to the multiplicative system of non-zero homogeneous polynomials.) The *local ring of V at $P \in V$*, denoted $\bar{K}[V]_P$, is the ring of all elements $\frac{f}{g} \in \bar{K}(V)$ with $g(P) \neq 0$. These elements are called *regular* (or *defined*) *at P*.

If $F = \frac{f}{g} \in \bar{K}(V)$ is regular at $P \in V$, then $F(P) = \frac{f(P)}{g(P)}$ is a well-defined element of $\bar{K}$. When we speak of a *(rational) function* F on V, we always mean an element of $\bar{K}(V)$ even though F might not be defined at every point of V. Indeed all functions that are regular at all points of V are trivial:

Proposition 1.18. *Let V be a projective variety. The only functions that are regular at all points of V are the constant functions.*

Let $\mathbb{A}^n$ be an affine piece of projective space such that $\mathbb{A}^n \cap V \neq \emptyset$. Then $\bar{K}(V) \cong \bar{K}(V \cap \mathbb{A}^n)$. If $P \in V \cap \mathbb{A}^n$, then $\bar{K}[V]_P \cong \bar{K}[V \cap \mathbb{A}^n]_P$.

Proof. [Har77, theorem 3.2] and Hartshorne's definition of the function field and local rings.   □

The preceding proposition implies that in many cases it sufficient to prove theorems for affine varieties and the projective case will follow automatically. This will always work when the property in question is local.

Definition 1.19. Let V be a projective variety, $P \in V$ and $\mathbb{A}^n$ an affine piece with $P \in V \cap \mathbb{A}^n$. Then the *dimension* $\dim V$ *of* V is the dimension of $V \cap \mathbb{A}^n$. The variety V is *non-singular* (or *smooth*) at P if $V \cap \mathbb{A}^n$ is non-singular at P.

To complete the category of projective varieties, we need to define what the morphisms are:

Definition 1.20. Let V_1 and V_2 be projective varieties with $V_2 \subseteq \mathbb{P}^n$. A *rational map from V_1 to V_2* is a collection of functions $f_0, \ldots, f_n \in \bar{K}(V_1)$ such that $[f_0(P) : \cdots : f_n(P)] \in V_2$ for all points $P \in V_1$ where the expression is well-defined. Even though a rational map ϕ might not be defined on all of V_1, we write

$$\phi \colon V_1 \to V_2, \, \phi = [f_0 : \cdots : f_n].$$

A rational map $\phi = [f_0 : \cdots : f_n]$ is *regular* or *(defined)* at $P \in V_1$ if there exists $g \in \bar{K}(V_1)$ such that each $g f_i$ is regular at P and there exists an index i with $g f_i(P) \neq 0$. A *morphism* is a rational map which is regular at every point of V_1. A morphism is an *isomorphism*, if it has an inverse that is again a morphism.

Definition 1.21. A rational map $\phi = [f_0 : \cdots : f_n]$ is *defined over K* if there exists an element $\lambda \in \bar{K}^*$ such that all $\lambda f_i \in K(V_1)$. Two varieties are *isomorphic over K* if there exists an isomorphism ϕ between them such that both ϕ and its inverse are defined over K.

The Galois group $\mathrm{Gal}(\bar{K}|K)$ acts on a rational map $\phi = [f_0 : \cdots : f_n]$ by acting on the f_i. Note that ϕ is defined over K if and only if $\phi^\sigma = \phi$ for all $\sigma \in \mathrm{Gal}(\bar{K}|K)$.

Definition 1.22. Let $\phi \colon V_1 \to V_2$ be a rational map. The *pull-back of $f \in \bar{K}(V_2)$ by ϕ* is

$$\phi^* f = f \circ \phi \in \bar{K}(V_1).$$

The function $\phi^* \colon \bar{K}(V_2) \to \bar{K}(V_a)$ is a homomorphism of fields. If the image of V_1 under ϕ is dense in V_2, then ϕ^* is injective [Sha94a, p. 51]. A rational map ϕ is regular if and only if ϕ^* maps regular functions to regular functions.

1.2 Curves

Even in classical algebraic geometry there are several different notions of a "curve" [Har77, section I.6] and of course modern algebraic geometry has vastly generalized the concept [Har77, definition II.6.7]. For the purpose of this text the word *curve* will always mean a one-dimensional projective variety. A curve in $\mathbb{P}^2$ is uniquely determined by a single equation. We will usually give the dehomogenized version of this equation. When we speak of *models* of a curve C, we mean curves with the same function field (i.e. curves which are birational to C, see [Sha94a, sections I.4.3 and II.4.5]). Note that by proposition 1.27 below two non-singular curves are birationally equivalent if and only if they are isomorphic. Also compare theorem 1.29.

Proposition 1.23. *Let P be a non-singular point of a curve C. Then $\bar{K}[C]_P$ is a discrete valuation ring (see definition 3.59).*

Definition 1.24. Let P be a non-singular point of a curve C and $f \in \bar{K}[C]_P$. The *order of f at P* is

$$\mathrm{ord}_P(f) = \max \left\{ d \in \mathbb{Z} : f \in \mathfrak{m}_P^d \right\} \in \{0, 1, 2, \dots\} \cup \{\infty\}.$$

By $\mathrm{ord}_P(\frac{f}{g}) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$ this can be extended to

$$\mathrm{ord}_P \colon \bar{K}(C) \to \mathbb{Z} \cup \{\infty\}.$$

Let $f \in \bar{K}(C)$. If $\mathrm{ord}_P(f) > 0$, then f has a *zero* at P. If $\mathrm{ord}_P(f) < 0$, then f has a *pole* at P. If $\mathrm{ord}_P(f) \geq 0$ then f is regular at P and $f(P) \in \bar{K}$ is well-defined. Otherwise we write $f(P) = \infty$. If $\mathrm{ord}_P(f) = 1$, then f is a *uniformizer at P*.

Proposition 1.25. *Let $f \in \bar{K}(C)$, where C is smooth curve. Then f has only finitely many poles and zeros. Further if f has no poles or no zeros, then it is constant.*

Proposition 1.26. *Let C/K be a curve and let $t \in K(C)$ be a uniformizer. Then $K(C)$ is a finite separable extension of $K(t)$.*

Proposition 1.27. *Let C be a curve, $P \in C$ a non-singular point, V a (projective) variety and $\phi \colon C \to V$ a rational map. Then ϕ is regular at P. In particular, if C is smooth then ϕ is a morphism.*

Note that there is a natural one-to-one correspondence between functions in $K(C)$ and rational maps $C \to \mathbb{P}^1$ defined over K: A function $f \in K(C)$ defines a rational map (also denoted f) by

$$f \colon C \to \mathbb{P}^1, \ P \mapsto \begin{cases} [f(P) : 1] & \text{if } f \text{ is regular at } P \\ [1 : 0] & \text{if } f \text{ has a pole at } P \end{cases}.$$

The next two theorems are central to the study of algebraic curves:

Theorem 1.28. *A morphism between two curves is either constant or surjective.*

Theorem 1.29. *Let C_1/K and C_2/K be smooth curves.*

1. *Let $\phi \colon C_1 \to C_2$ be a non-constant morphism. Then $K(C_1)$ is a finite field extension of $\phi^* K(C_2)$.*

2. *Let $\iota \colon K(C_1) \to K(C_2)$ be an injective homomorphism fixing K. Then there exists a unique non-constant morphism $\phi \colon C_1 \to C_2$ such that $\phi^* = \iota$.*

3. *Let $L \subseteq \bar{K}(C_1)$ be a subfield of finite index containing K. Then there exists a smooth curve C'/K and a non-constant map $\phi \colon C_1 \to C'$ defined over K such that $\phi^* K(C') = L$. The curve C' is unique up to K-isomorphism.*

Definition 1.30. Let $\phi \colon C_1 \to C_2$ be a rational map of curves defined over K. If ϕ is constant, then the *degree* of ϕ is 0. Otherwise we define the degree of ϕ by

$$\deg \phi = [K(C_1) : \phi^* K(C_2)].$$

The rational map ϕ is called *separable*, *inseparable* or *purely inseparable* if the field extension $K(C_1)|\phi^* K(C_2)$ has the corresponding property. The separable and inseparable degrees of the extension are denoted $\deg_s \phi$ resp. $\deg_i \phi$ (see [Lan02, chapter V] for definitions of the field extension properties.).

Corollary 1.31. *A map of degree one between smooth curves is an isomorphism.*

Definition 1.32. Let $\phi \colon C_1 \to C_2$ be a non-constant morphism of smooth curves defined over K. Define the *push-forward by ϕ*,

$$\phi_* \colon K(C_1) \to K(C_2),$$

by

$$\phi_* = (\phi^*)^{-1} \circ N_{K(C_1)|\phi^* K(C_2)},$$

where $N_{K(C_1)|\phi^* K(C_2)}$ denotes the usual norm map for field extensions ([Lan02, section VI.5]).

Definition 1.33. Let $\phi \colon C_1 \to C_2$ be a non-constant morphism of smooth curves and let $P \in C_1$. Further let $t_{\phi(P)}$ be a uniformizer of C_2 at $\phi(P)$. The *ramification index of ϕ at P* is

$$e_\phi(P) = \mathrm{ord}_P(\phi^* t_{\phi(P)}).$$

The ramification index is always a positive integer. If $e_\phi(P) = 1$, then ϕ is *unramified at P*. If ϕ is unramified at all points of C_1, then it is *unramified*.

Theorem 1.34. *Let $\phi\colon C_1 \to C_2$ be a non-constant morphism of smooth curves.*

1. For every $Q \in C_2$,

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi.$$

2. For all but finitely many $Q \in C_2$,

$$\#\phi^{-1}(Q) = \deg_s(\phi).$$

3. Let $\psi\colon C_2 \to C_3$ be another non-constant morphism of smooth curves. Then for all $P \in C_1$,

$$e_{\psi\circ\phi}(P) = e_\phi(P)e_\psi(\phi(P)).$$

In particular ϕ is unramified if and only if $\#\phi^{-1}(Q) = \deg(\phi)$ for all $Q \in C_2$.

We will now introduce the most important family of morphisms for the study of varieties over fields of positive characteristic. Let K be a field with char $K = p > 0$ and let $q = p^r$ for some positive integer r. For any polynomial $f \in K[x]$ let $f^{(q)}$ be the polynomial obtained from f by raising each coefficient to the qth power. If V is a projective variety we define $V^{(q)}$ to be the variety given by the homogeneous ideal

$$I\left(V^{(q)}\right) = \left\langle f^{(q)} : f \in I(V) \right\rangle.$$

Definition 1.35. *The qth-power Frobenius morphism of a variety V is*

$$\phi_q\colon \begin{cases} V & \to & V^{(q)} \\ [x_0 : \cdots : x_n] & \mapsto & [x_0^q : \cdots : x_n^q] \end{cases}$$

Theorem 1.36. *Let K be a field with characteristic p, C/K a curve, $q = p^r$ and $\phi_q\colon C \to C^{(q)}$ the qth-power Frobenius morphism. Then the following statements hold (remember that K is assumed to be perfect):*

1. $\phi_q^* K(C^{(q)}) = K(C)^q$.
2. ϕ_q is purely inseparable.
3. $\deg \phi_q = q$.

Theorem 1.37. *Let $\psi\colon C_1 \to C_2$ be a morphism of smooth curves defined over a field of characteristic $p > 0$. Further let $q = \deg_i \psi$ and let ϕ_q be the qth-power Frobenius morphism. Then ψ factors as*

$$C_1 \overset{\phi_q}{\to} C_1^{(q)} \overset{\lambda}{\to} C_2,$$

where λ is separable.

Note that by [Lan02, corollary V.6.2], $q = \deg_i \psi$ is indeed a power of p.

1.3 Divisors

(Weil) divisors of curves are in several respects a very good concept: They are essentially trivial, provide a very concise language that makes some difficult theorems more accessible and they give rise to several interesting mathematical objects.

Definition 1.38. *The divisor group of a curve C, denoted $\mathrm{Div}(C)$, is the free Abelian group generated by the points of C. Its elements are called divisors and are usually written as a formal sum*

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

with $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many points P. The order of a divisor D at a point P, denoted $\mathrm{ord}_P D$, is n_P. The degree of D is

$$\deg D = \sum_{P \in C} n_P \in \mathbb{Z}.$$

The *divisors of degree* 0 form a subgroup, denoted

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) : \deg D = 0\}.$$

The set $\{P \in C : \mathrm{ord}_P D \neq 0\}$ is called the *support* of the divisor D, denoted $\mathrm{supp}\, D$.

The concept can be generalized to arbitrary varieties (as Weil divisors, see [Sha94a, chapter III]) and even to schemes (as Cartier divisors, see [Har77, section II.6]).

If C is defined over K, then $\mathrm{Gal}(\bar{K}|K)$ acts on $\mathrm{Div}(C)$ by

$$D^\sigma = \sum_{P \in C} n_P (P^\sigma).$$

This action obviously takes $\mathrm{Div}^0(C)$ to itself.

Definition 1.39. A divisor $D \in \mathrm{Div}(C)$ is *defined over* K if $D = D^\sigma$. The divisors defined over K form a group, denoted $\mathrm{Div}_K(C)$. In the same way, $\mathrm{Div}_K^0(C)$ is the group of divisors of degree 0 defined over K.

Note that $D = n_1(P_1) + \cdots + n_r(P_r)$ with $n_i \neq 0$ and D defined over K does not necessarily mean that all $P_i \in C(K)$. It is sufficient that $\mathrm{Gal}(\bar{K}|K)$ permutes the P_is in an appropriate way.

Definition 1.40. Let C be a smooth curve and let $f \in \bar{K}(C)^*$. Then the *divisor of* f is

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

This is well-defined by proposition 1.25. If C is defined over K and $\sigma \in \mathrm{Gal}(\bar{K}|K)$, then $\mathrm{div}(f^\sigma) = \mathrm{div}(f)^\sigma$. In particular if $f \in K(C)$, then $\mathrm{div}(f) \in \mathrm{Div}_K(C)$. The map $\mathrm{div} \colon \bar{K}(C)^* \to \mathrm{Div}(C)$ is a homomorphism of Abelian groups.

Proposition 1.41. *Let C be a smooth curve and $f \in \bar{K}(C)^*$. Then $\deg(\mathrm{div}(f)) = 0$. Further $\mathrm{div}(f) = 0$ if and only if $f \in \bar{K}^*$.*

Definition 1.42. A divisor $D \in \mathrm{Div}(C)$ is called *principal* if it is of the form $D = \mathrm{div}(f)$ for some $f \in \bar{K}(C)$. The principal divisors form a subgroup of $\mathrm{Div}(C)$. The quotient of $\mathrm{Div}(C)$ ($\mathrm{Div}^0(C)$) by this subgroup is called (*the degree zero part of*) the *divisor class group* or *Picard group* of C and is denoted $\mathrm{Pic}(C)$ ($\mathrm{Pic}^0(C)$). Two divisors D_1, D_2 are called *linearly equivalent*, denoted $D_1 \sim D_2$, if $D_1 - D_2$ is a principal divisor. In other words, $\mathrm{Pic}(C)$ is the divisor group of C modulo linear equivalence. Further if C is defined over K then $\mathrm{Pic}_K(C)$ ($\mathrm{Pic}_K^0(C)$) denotes the subgroup of $\mathrm{Pic}(C)$ ($\mathrm{Pic}^0(C)$) fixed by $\mathrm{Gal}(\bar{K}|K)$.

The definitions and the last proposition are summarized by the following exact sequence:

$$0 \to \bar{K}^* \to \bar{K}(C)^* \xrightarrow{\mathrm{div}} \mathrm{Div}^0(C) \to \mathrm{Pic}^0(C) \to 0.$$

In section 3.1 we will prove an analogous sequence in an analytic context.

Definition 1.43. Let $\phi \colon C_1 \to C_2$ be a non-constant morphism of smooth curves. We define the *pull-back* and *push-forward*

$$\phi^* \colon \mathrm{Div}(C_2) \to \mathrm{Div}(C_1) \qquad\qquad \phi_* \colon \mathrm{Div}(C_1) \to \mathrm{Div}(C_2)$$
$$\phi^*(Q) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P) \qquad\qquad \phi_*(P) = (\phi(P))$$

for $P \in C_1$, $Q \in C_2$ and extending $\mathbb{Z}$-linearly.

Note that for a smooth curve C and a function $f \in \bar{K}(C)^*$ (identified with the corresponding map $f \colon C \to \mathbb{P}^1$) we have

$$\mathrm{div}(f) = f^* \left((0) - (\infty)\right).$$

Definition 1.44. For a function f on a curve C and a divisor $D = \sum_P n_p(P) \in \mathrm{Div}^0(C)$ such that the support of D is disjoint from the support of $\mathrm{div}(f)$ we define

$$f(D) = \prod_P f(P)^{n_p} \in \bar{K}^*.$$

If g is another rational function on C with $g = cf$ for some constant $c \in \bar{K}^*$ then $f(D) = g(D)$. Thus $f(D)$ only depends on the divisors D and $\mathrm{div}(f)$. If C, f and D are all defined over K, then $f(D) \in K^*$.

The next proposition shows the all definitions we have so far perfectly fit together.

Proposition 1.45. *Let $\phi\colon C_1 \to C_2$ be a non-constant morphism of smooth curves. Let $D_i \in \mathrm{Div}(C_i)$ and $f_i \in \bar{K}(C_i)^*$.*

1. $\deg(\phi_* D_1) = \deg D_1$

2. $\deg(\phi^* D_2) = (\deg \phi)(\deg D_2)$

3. $\phi_*(\mathrm{div}\, f_1) = \mathrm{div}(\phi_* f_1)$

4. $\phi^*(\mathrm{div}\, f_2) = \mathrm{div}(\phi^* f_2)$

5. $\phi_* \circ \phi^*$ *acts as multiplication by* $\deg \phi$ *on* $\mathrm{Div}(C_2)$.

6. $f_1(\phi^* D_2) = (\phi_* f_1)(D_2)$

7. $f_2(\phi_* D_1) = (\phi^* f_2)(D_1)$

8. *If $\psi\colon C_2 \to C_3$ is another morphism of smooth curves then*

$$(\psi \circ \phi)^* = \phi^* \circ \psi^* \qquad and \qquad (\psi \circ \phi)_* = \psi_* \circ \phi_*.$$

Theorem 1.46 (Weil Reciprocity)**.** *Let f and g be two disjoint non-zero rational functions on a curve C such that the supports of $\mathrm{div}(f)$ and $\mathrm{div}(g)$ are disjoint. Then $f(\mathrm{div}(g)) = g(\mathrm{div}(f))$.*

Proof. If $C = \mathbb{P}^1$ one can easily write the functions g and f in terms of their divisors (if $\infty \notin \mathrm{supp}\,\mathrm{div}(f)$ and $\mathbb{P}_1$ is identified with $\bar{K} \cup \{\infty\}$, then $f = c \prod_{a \in \bar{K}} (x - a)^{\mathrm{ord}_a(f)}$). Then it is easy to check that Weil reciprocity holds.

Let C be an arbitrary curve. Let i be the identity map on $\mathbb{P}^1$. Then $\mathrm{div}(i) = (0) - (\infty)$ and $\mathrm{div}(g) = g^* \mathrm{div}(i)$. Also $g_* f$ is a function on $\mathbb{P}^1$ and hence by the first paragraph $(g_* f)(\mathrm{div}(i)) = i(\mathrm{div}(g_* f)) = i(g_* \mathrm{div}(f))$. Now the theorem follows by manipulating symbols:

$$f(\mathrm{div}(g)) = f(g^* \mathrm{div}(i)) = (g_* f)(\mathrm{div}(i)) = i(g_* \mathrm{div}(f)) = (g^* i)(\mathrm{div}(f)) = i \circ g(\mathrm{div}(f)) = g(\mathrm{div}(f)).$$

$\square$

1.4 Differentials

We need one last ingredient of the theory of algebraic curves: the space of differential forms. We will give a functorial definition which could be generalized to higher dimensions.

Definition 1.47. Let A be a commutative ring with identity, B an A-algebra and M a B-module. An *A-derivation from B into M* is a map $\mathrm{d}\colon B \to M$ with

1. $\mathrm{d}(b + b') = \mathrm{d}b + \mathrm{d}b'$ for all $b, b' \in B$;
2. $\mathrm{d}(bb') = b\,\mathrm{d}b' + b'\,\mathrm{d}b$ for all $b, b' \in B$;
3. $\mathrm{d}a = 0$ for all $a \in A$.

The *module of relative differential forms of B over A* is a B-module $\Omega_{B|A}$ together with an A-derivation $\mathrm{d}\colon B \to \Omega_{B|A}$ such that for any B-module M and A-derivation $\mathrm{d}'\colon B \to M$ there exists a unique B-module homomorphism $f\colon \Omega_{B|A} \to M$ such that the following diagram commutes:

$$
\begin{array}{ccc}
B & \xrightarrow{\ \mathrm{d}\ } & \Omega_{B|A} \\
& \mathllap{\mathrm{d}'}\searrow & \downarrow{\scriptstyle \exists! f} \\
& & M
\end{array}
$$

Definition 1.48. Let C be a curve. The *space of differential forms on C* is $\Omega_C = \Omega_{\bar{K}(C)|\bar{K}}$.

Proposition 1.49. *The pair* $(\Omega_{B|A}, \mathrm{d})$ *exists and is unique up to unique isomorphism. In particular,* Ω_C *can be constructed in the following way:* Ω_C *is the* $\bar{K}(C)$*-vector space generated by symbols of the form* $\mathrm{d}f$, $f \in \bar{K}(C)$, *modulo the relations*

1. $\mathrm{d}(f + g) = \mathrm{d}f + \mathrm{d}g$ *for all* $f, g \in \bar{K}(C)$;
2. $\mathrm{d}(fg) = g \,\mathrm{d}f + f \,\mathrm{d}g$ *for all* $f, g \in \bar{K}(C)$;
3. $\mathrm{d}a = 0$ *for all* $a \in \bar{K}$.

Proposition 1.50. *Let* C *be a curve. Then* Ω_C *is a one-dimensional* $\bar{K}(C)$*-vector space. An element* $\mathrm{d}x$, $x \in \bar{K}(C)$, *is non-zero if and only if* $\bar{K}(C)|\bar{K}(x)$ *is a finite separable extension.*

Definition 1.51. Let $\phi \colon C_1 \to C_2$ be a non-constant map of curves. Then ϕ induces a *pull-back*

$$\phi^* \colon \left\{ \begin{array}{ccc} \Omega_{C_2} & \to & \Omega_{C_1} \\ \sum_i f_i \,\mathrm{d}x_i & \mapsto & \sum_i (\phi^* f_i) \,\mathrm{d}(\phi^* x_i) \end{array} \right. .$$

Proposition 1.52. *Let* $\phi \colon C_1 \to C_2$ *be a non-constant map of curves. Then* ϕ *is separable if and only if* $\phi^* \colon \Omega_{C_2} \to \Omega_{C_1}$ *is injective.*

Proposition 1.53. *Let* C *be a curve, let* $P \in C$, *let* $t \in \bar{K}(C)$ *be a uniformizer at* P *and let* $\omega \in \Omega_C$.

1. *There exists a unique function* $g \in \bar{K}(C)$ *(depending on* ω *and* t*) such that* $\omega = g \,\mathrm{d}t$. *It is denoted* $\frac{\omega}{\mathrm{d}t}$.

2. *Let* $f \in \bar{K}(C)$ *be regular at* P. *Then* $\frac{\mathrm{d}f}{\mathrm{d}t}$ *is also regular at* P.

3. *The order* $\mathrm{ord}_P\left(\frac{\omega}{\mathrm{d}t}\right)$ *is independent of the choice of the uniformizer* t. *It is denoted* $\mathrm{ord}_P(\omega)$ *and called the* order *of* ω *at* P.

4. *Let* $x, f \in \bar{K}(C)$ *with* $x(P) = 0$. *Then:*

$$\begin{array}{ll} \mathrm{ord}_P(f \,\mathrm{d}x) = \mathrm{ord}_P(f) + \mathrm{ord}_P(x) - 1, & \text{if } \mathrm{char}\, K = 0 \text{ or } \mathrm{char}\, K \nmid \mathrm{ord}_P(x) \\ \mathrm{ord}_P(f \,\mathrm{d}x) \geq \mathrm{ord}_P(f) + \mathrm{ord}_P(x), & \text{if } \mathrm{char}\, K > 0 \text{ and } \mathrm{char}\, K \mid \mathrm{ord}_P(x) \end{array}$$

5. *For all but finitely many* $P \in C$, $\mathrm{ord}_P(\omega) = 0$.

Definition 1.54. The *divisor associated to* $\omega \in \Omega_C$ is

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

Definition 1.55. A differential $\omega \in \Omega_C$ is *regular* (or *holomorphic*) if $\mathrm{ord}_P(\omega) \geq 0$ for all $P \in C$. It is *non-vanishing* if $\mathrm{ord}_P(\omega) \leq 0$ for all $P \in C$.

If ω_1, ω_2 are two non-zero differentials on C, then there exists a function $f \in \bar{K}(C)^*$ such that $\omega_1 = f\omega_2$. In terms of divisors this implies $\mathrm{div}(\omega_1) = \mathrm{div}(f) + \mathrm{div}(\omega_2)$. Therefore the following definition is independent of the chosen differential form ω.

Definition 1.56. Let ω be a non-zero differential form on C. The *canonical divisor class on* C is the image of $\mathrm{div}(\omega)$ in $\mathrm{Pic}(C)$. Any divisor in this class is called a *canonical divisor* and often denoted K_C.

1.5 The Riemann-Roch Theorem

We will finish this introductory chapter with one of the most fundamental results of the theory of algebraic curves. It will allow us to describe the space of functions on C having prescribed zeros and poles. Before we can state the theorem we need to introduce some additional notation.

Definition 1.57. A divisor $D = \sum_P n_P(P)$ is called *effective* (or *positive*), denoted $D \geq 0$, if $n_P \geq 0$ for all $P \in C$. This extends to a partial order $\geq$ on $\mathrm{Div}(C)$ by setting $D_1 \leq D_2$ if $D_2 - D_1 \geq 0$.

Definition 1.58. Let $D \in \mathrm{Div}(C)$. The *associated vector space* or *Riemann-Roch space of* D is the set of functions

$$\mathscr{L}(D) = \left\{ f \in \bar{K}(C)^* : \mathrm{div}(f) \geq -D \right\} \cup \{0\}.$$

It is a finite dimensional $\bar{K}$-vector space (see the next proposition) and its dimension is denoted $\ell(D)$.

Proposition 1.59. *Let $D \in \mathrm{Div}(C)$. Then $\mathscr{L}(D)$ is a finite dimensional $\bar{K}$-vector space. If $\deg D < 0$, then $\mathscr{L}(D) = 0$. Let $D' \in \mathrm{Div}(C)$ with $D' \sim D$. Then $\mathscr{L}(D') \cong \mathscr{L}(D)$. In particular $\ell\colon \mathrm{Div}(D) \to \mathbb{Z}$ descends to a well defined function $\ell\colon \mathrm{Pic}(C) \to \mathbb{Z}$.*

Proposition 1.60. *Let K_C be a canonical divisor of C. Then*

$$\mathscr{L}(K_C) \cong \{\omega \in \Omega_C : \omega \text{ is holomorphic}\} .$$

Theorem 1.61 (Riemann-Roch)**.** *Let C be a smooth curve and K_C a canonical divisor of C. There exists a number $g \geq 0$, called the* genus *of C, such that for every divisor $D \in \mathrm{Div}(C)$,*

$$\ell(D) - \ell(K_C - D) = \deg D - g + 1.$$

A proof of the Riemann-Roch theorem would definitely be beyond the scope of this text. However it is interesting to see that there are many different ways to prove the theorem: An elegant and short proof is given in [Har77, theorem IV.1.3] but it uses the language sheaves and Serre duality. A more elementary proof is given in [Lan82, I.2]. Lang's proof goes back to a proof by Weil [Wei48]. Both use a definition of differentials that is different from the one we are using and then show that the definitions are in fact equivalent (which is a nontrivial part of the proof). Also both proofs use the definition of an abstract curve we have skipped in section 1.2 (see [Har77, section I.6]). The most accessible proof is probably the classic proof of Noether and Brill for embedded curves as given in [Ful89]. It only needs normalization (or one could restrict oneself to non-singular plane curves) and Bézout's theorem. Restricting even further to non-singular plane cubic curves (and this is what we will need) the proof gets much shorter and is given in [Sha94a, theorem III.3.2].

Corollary 1.62. *Some simple – but important – consequences of the Riemann-Roch theorem are:*

1. $\ell(K_C) = g$.
2. $\deg K_C = 2g - 2$.
3. If $\deg D > 2g - 2$, then $\ell(D) = \deg D - g + 1$.

Proposition 1.63. *Let C/K be a smooth curve and let $D \in \mathrm{Div}_K(C)$. Then $\mathscr{L}(D)$ has a basis consisting of functions in $K(C)$.*

Chapter 2

Elliptic Curves

The mathematical objects used in elliptic curve cryptography are – of course – elliptic curves. For cryptographic purposes we are mainly interested in curves over finite fields. In this chapter we will however study elliptic curves over arbitrary (perfect) fields. This has two reasons: First, most of the theory presented here is not harder to study in a general setting that it is over finite fields – it might even become clearer. Second, we will need to make use of elliptic curves over $\mathbb{C}$ and over extensions of the p-adic numbers $\mathbb{Q}_p$ to derive information about curves over finite fields. Therefore in this section K will again be an arbitrary perfect field and $\bar{K}$ a (fixed) algebraic closure of K.

There as several books that cover many of the topics of this and the next chapter. In the author's opinion, the work by Silverman [Sil92] is still the best written "standard book" on elliptic curves. Other books we will occasionally refer to include [Hus04] and [Was08]. The book by Washington deserves special notice because it covers some material of particular importance to elliptic curve cryptography. Also introductory books on algebraic geometry often contain a section dedicated to elliptic curves. Further the book [ST92] should be mentioned. It is a very gentle introduction to elliptic curves over the rationals and is useful for gaining intuition.

2.1 Curves of Genus One

We begin by defining the main object of our study.

Definition 2.1. An *elliptic curve* is a pair $(E, \mathcal{O})$, where E is a smooth curve of genus 1 and $\mathcal{O} \in E$. The point $\mathcal{O}$ is called the *base point*. The elliptic curve E is defined over K, denoted E/K, if E is defined over K as a curve and $\mathcal{O} \in E(K)$.

Theorem 2.2. *Let $(E, \mathcal{O})$ be an elliptic curve defined over K.*

1. *There exist functions $x, y \in K(E)$ such that the map*

$$\phi \colon \left\{ \begin{array}{c} E \to \mathbb{P}^2 \\ \phi = [x,\, y,\, 1] \end{array} \right.$$

   gives an isomorphism of E/K onto a curve given by an equation of the form

$$C \colon Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6 \tag{2.1}$$

   with $a_1, \ldots, a_6 \in K$ and $\phi(\mathcal{O}) = [0 : 1 : 0]$.

2. *Any two equations of the form (2.1) for E are related by a linear change of variables of the form*

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} u^2 & 0 \\ s & u^3 \end{pmatrix} \begin{pmatrix} X' \\ Y' \end{pmatrix} + \begin{pmatrix} r \\ t \end{pmatrix}, \tag{2.2}$$

   where $r, s, t \in K$ and $u \in K^*$.

3. *Conversely every smooth cubic curve C given by a equation of the form (2.1) is an elliptic curve defined over K with base point $\mathcal{O} = [0 : 1 : 0]$.*

Proof.

1. We will use the Riemann-Roch theorem to show the existence of x and y and their relationship. Consider the divisors $n(\mathcal{O})$ ($n = 1, 2, \dots$). Corollary 1.62 with $g = 1$ implies $\ell(n(\mathcal{O})) = \dim \mathscr{L}(n(\mathcal{O})) = n$. By definition, $\mathscr{L}((\mathcal{O})) \subseteq \mathscr{L}(2(\mathcal{O})) \subseteq \mathscr{L}(3(\mathcal{O})) \subseteq \cdots$. Hence there are functions $x, y \in \bar{K}(C)$ such that $\{1, x\}$ is a basis of $\mathscr{L}(2(\mathcal{O}))$ and $\{1, x, y\}$ is one of $\mathscr{L}(3(\mathcal{O}))$. By theorem 1.63 we can even choose x, y to be defined over K. We note that x must have exact pole order 2 in $\mathcal{O}$, because otherwise it would already be in $\mathscr{L}((\mathcal{O}))$ which is one dimensional. Similarly y must have exact pole order 3 at $\mathcal{O}$.

   The functions $1, x, y, x^2, xy, y^2, x^3$ are all in $\mathscr{L}(6(\mathcal{O}))$ which is 6-dimensional. Therefore there exists a relation

   $$A_1 + A_2 x + A_3 y + A_4 x^2 + A_5 xy + A_6 y^2 + A_7 x^3 = 0.$$

   The coefficients A_6 and A_7 cannot be 0 since otherwise every term would have a different pole order at $\mathcal{O}$ and thus all coefficients would vanish. Replacing x by $-A_6 A_7 x$ and y by $A_6 A_7^2 y$ we get the desired map

   $$\phi \colon E \to \mathbb{P}^2, \phi = [x : y : 1]$$

   with image in the locus of a curve C described by an equation of type (2.1). By 1.27, ϕ is a morphism and by 1.28 it is onto. Also because y has higher pole order than x, $\phi(\mathcal{O}) = [0 : 1 : 0]$.

   Next we will show that $\phi \colon E \to C$ has degree 1, or equivalently that $K(E) = K(x, y)$. The function x has a double pole at $\mathcal{O}$ and no other poles. Hence theorem 1.34.1 with $Q = [1 : 0]$ implies that the map $[x : 1] \colon E \to \mathbb{P}^1$ has degree 2. In other words $[K(E) : K(x)] = 2$. Similarly $[K(E) : K(y)] = 3$. But then $[K(E) : K(x, y)] = 1$ because it has to divide both 2 and 3.

   Now suppose that C was singular. Then by lemma 2.3 below there exists a rational map $\psi \colon C \to \mathbb{P}^1$ of degree 1. Therefore the composition $\psi \circ \phi$ is a map of degree 1 of smooth curves and hence an isomorphism (1.31). This is a contradiction to the fact that $\mathbb{P}^1$ has genus 0 but E has genus 1. Therefore C is smooth and 1.31 shows that ϕ is an isomorphism.

2. Let C, C' be curves of the type (2.1) isomorphic to E via x, y resp. x', y'. Then x and x' have poles of order 2 at $\mathcal{O}$, so both $\{1, x\}$ and $\{1, x'\}$ are bases of $\mathscr{L}(2(\mathcal{O}))$. Therefore there exist scalars u_1 and r in K such that $x = u_1 x' + r$. By analogous reasoning in $\mathscr{L}(3(\mathcal{O}))$ there exists scalars $u_2, s, t \in K$ such that $y = sx + u_2 y' + t$. Both (x, y) and (x', y') satisfy equations of the form (2.1) where the coefficients of x^3 and y^2 are 1. Thus $u_1^3 = u_2^2$. Let $u = u_2 / u_1$ to obtain the coordinate change given in the theorem.

3. We will see in 2.9 that the differential

   $$\omega = \frac{\mathrm{d}x}{2y + a_1 x + a_3} \in \Omega_C$$

   has neither zeros nor poles. In other words $\mathrm{div}(\omega) = 0$. Hence the Riemann-Roch theorem (1.62.2) implies

   $$2g - 2 = \deg(\mathrm{div}(\omega)) = 0,$$

   where g is the genus of C. Thus $g = 1$ and C together with the point $[0 : 1 : 0]$ is an elliptic curve. $\qquad\square$

Lemma 2.3. *Let C be a singular plane curve with equation* (2.1). *Then there exists a rational map $\phi \colon E \to \mathbb{P}^1$ of degree 1.*

Proof. [Sil92, proposition III.1.6] $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Definition 2.4. Let E be an elliptic curve. Then by theorem 2.2 there exists a curve isomorphic to E with equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6. \tag{2.3}$$

Every equation of this form is called a called a *Weierstraß equation* for E with Weierstraß coordinate functions x, y. When not stated otherwise we will always assume that E is given by a Weierstraß equation and $\mathcal{O} = [0 : 1 : 0]$. A change of coordinates of type (2.2) is called a *Weierstraß change of coordinates* over K.

Let E be an elliptic curve given by a Weierstraß equation (2.3). We will make use of the following quantities:

$$
\begin{aligned}
b_2 &= a_1^2 + 4a_2, \\
b_4 &= 2a_4 + a_1 a_3, \\
b_6 &= a_3^2 + 4a_6, \\
b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2, \\
c_4 &= b_2^2 - 24b_4, \\
c_6 &= -b_2^3 + 36b_2 b_4 - 216b_6.
\end{aligned}
\tag{2.4}
$$

Definition 2.5. The *discriminant* of an elliptic curve E in Weierstraß form (2.3) is

$$
\Delta = \Delta(a_1, \ldots, a_6) = -b_2^2 b_8 - 8b_4 b^3 - 27b_6^2 + 9b_2 b_4 b_6.
$$

Its *j-invariant* is

$$
j = j(a_1, \ldots, a_6) = \frac{c_4^6}{\Delta}.
$$

Its *invariant differential* is

$$
\omega = \frac{\mathrm{d}x}{2y + a_1 x + a_3} = \frac{\mathrm{d}y}{3x^2 + 2a_2 x + a_4 - a_1 y}.
$$

Proposition 2.6. *A Weierstraß change of coordinates (2.2) of elliptic curves changes the quantities of the previous definition in the following way:*

$$
\begin{aligned}
\Delta' &= u^{-12} \Delta, \\
j' &= j, \\
\omega' &= u\omega.
\end{aligned}
$$

In particular j depends only on the isomorphism class and hence is well defined for an arbitrary elliptic curve (not necessarily in Weierstraß from).

Proof. Tedious but simple calculations. $\hfill\square$

Proposition 2.7. *Let E/K be an elliptic curve. Then, under the assumptions below, there is a Weierstraß change of coordinates that takes E into the indicated form.*

1. char $K \neq 2, 3$:

$$
y^2 = x^3 + a_4 x + a_6 \qquad \Delta = -16(4a_4^3 + 27a_6^2) \qquad j = 1728\frac{4a_4^3}{4a_4^3 + 27a_6^2}
$$

The only change of coordinates preserving this form of equation is $x = u^2 x'$, $y = u^3 y'$ for some $u \in K^*$.

2. char $K = 3$ and $j(E) \neq 0$:

$$
y^2 = x^3 + a_2 x^2 + a_6 \qquad \Delta = -a_2^4 a_6 \qquad j = -\frac{a_2^3}{a_6}
$$

char $K = 3$ and $j(E) = 0$:

$$
y^2 = x^3 + a_4 x + a_6 \qquad \Delta = -a_4^3 \qquad j = 0
$$

3. char $K = 2$ and $j(E) \neq 0$:

$$
y^2 + xy = x^3 + a_2 x^2 + a_6 \qquad \Delta = a_6 \qquad j = \frac{1}{a_6}
$$

char $K = 2$ and $j(E) = 0$:

$$
y^2 + a_3 y = x^3 + a_4 x + a_6 \qquad \Delta = a_4^3 \qquad j = 0
$$

Proof. See [Sil92, proposition A.1.1]. Explicit calculations for characteristic 0 and a geometric interpretation can be found in [ST92]. □

Proposition 2.8.

1. *A curve given by a Weierstraß equation (2.3) is non-singular if and only if $\Delta \neq 0$.*
2. *Two elliptic curves are isomorphic (over $\bar{K}$) if and only if they have the same j-invariant.*
3. *Let $j_0 \in \bar{K}$. Then there exists an elliptic curve defined over $K(j_0)$ with j-invariant equal to j_0.*

Proof. See [Sil92, proposition III.1.4]. For convenience we will state the equation of a curve for a given j-invariant. If $j_0 \neq 0, 1728$ then

$$E\colon y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}$$

has j-invariant j_0. If $j_0 = 0$ then

$$E\colon y^2 + y = x^3 \qquad (\Delta = -27)$$

is such a curve and for $j_0 = 1728$ we can use

$$E\colon y^2 = x^3 + x \qquad (\Delta = -64).$$

Note that for char $K = 2, 3$ we have $1728 = 0$ and exactly one of the two curves is nonsingular. □

Proposition 2.9. *Let E be an elliptic curve in Weierstraß form. Then the invariant differential associated to the Weierstraß equation of E is holomorphic and non-vanishing (i.e. $\mathrm{div}(\omega) = 0$).*

Proof. [Sil92, proposition III.1.5] □

To every curve we already associated a group: the divisor group. However, while divisors are a very useful tool, the group itself is rather uninteresting – it is just a free Abelian group. A much more interesting group is the Picard group. As we will see in a moment, elliptic curves have the remarkable property that there is a natural bijection between the degree zero part of the Picard group and the curve.

Lemma 2.10. *Let C be a smooth curve of genus one and let $P, Q \in C$. Then $(P) \sim (Q)$ if and only if $P = Q$.*

Proof. [Sil92, lemma III.3.3] □

Theorem 2.11. *Let $(E, \mathcal{O})$ be an elliptic curve. For each divisor $D \in \mathrm{Div}^0(E)$ there exists a unique point $P \in E$ such that $D \sim (P) - (O)$. This induces a surjective map $\sigma\colon \mathrm{Div}^0(E) \to E$. The map is invariant under linear equivalence and descends to a bijection*

$$\sigma\colon \mathrm{Pic}^0(E) \to E.$$

Proof. [Sil92, proposition III.3.4 (a)-(c)] □

The map σ of the last theorem can be used to define a group law on E. Another remarkable property of elliptic curves is that this group law can also be defined geometrically and can be computed in a very simple way.

Note that if $L \subseteq \mathbb{P}^2(\bar{K})$ is a line and E is an elliptic curve in Weierstraß equation, then L and E will have exactly three points of intersection (when counted with multiplicity). This is a special case of Bézout's theorem [Har77, theorem I.7.8] or can be calculated explicitly (see [ST92]).

Definition 2.12 (Tangent-Chord Law)**.** Let P, Q be two points of an elliptic curve E given in Weierstraß equation. We will define their sum $P + Q \in E$. Let L_1 be the line connecting P and Q (or the tangent at P if $P = Q$). Let R be the third point of intersection of L_1 with E. Let L_2 be the line connecting R and $\mathcal{O}$. Then $P + Q$ is the third point of intersection of L_2 with E.

Theorem 2.13. *Let E be an elliptic curve in Weierstraß form and let $\sigma\colon \operatorname{Pic}^0(E) \to E$ be the map of theorem 2.11. Let $D_1, D_2 \in \operatorname{Pic}^0(E)$. Then*

$$\sigma(D_1 + D_2) = \sigma(D_1) + \sigma(D_2),$$

where addition on the right side is according to the preceding definition. In particular, the tangent-chord law makes E into an Abelian group. The neutral element of this group is $\mathcal{O}$. If E is defined over K, then the set of K-rational points $E(K)$ forms a subgroup.

Proof. Because we will need similar constructions later on, we will give a full proof of the theorem. Let κ be the inverse of σ. To every point $P \in E$, κ assigns the class of $(P) - (\mathcal{O})$. It is sufficient to show that for any two points $P, Q \in E$,

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

Let $l_{P,Q}(X, Y, Z) = 0$ be an equation of the line through P and Q. Let R be its third point of intersection with E and let $l_{R,\mathcal{O}}(X, Y, Z) = 0$ be the line through R and $\mathcal{O}$. By definition its third point of intersection with E is $P + Q$. The line $Z = 0$ intersects E at $\mathcal{O}$ with multiplicity 3. Dividing the equations by Z gives functions on E with

$$\operatorname{div}\left(\frac{l_{P,Q}}{Z}\right) = (P) + (Q) + (R) - 3(\mathcal{O})$$

$$\operatorname{div}\left(\frac{l_{R,\mathcal{O}}}{Z}\right) = (R) + (P + Q) - 2(\mathcal{O})$$

Therefore

$$(P + Q) - (P) - (Q) + (\mathcal{O}) = \operatorname{div}\left(\frac{l_{R,\mathcal{O}}}{l_{P,Q}}\right) \sim 0,$$

which implies

$$\kappa(P + Q) - \kappa(P) - \kappa(Q) = 0.$$

If two solutions of a cubic equations with coefficients in K lie in K, then the third solution is also in K. Therefore $E(K)$ forms a subgroup of E. See also theorem 2.15 for explicit formulas. $\square$

Of course it can also be directly verified that that the tangent-chord law gives a group structure on E. See [Sil92, proposition III.3.4 (a) - (e)] and [ST92].

Definition 2.14. Let E be an elliptic curve, $P \in E$ and $m \in \mathbb{Z}$. Then $[m]P$ is defined by

$$[0]P = \mathcal{O}, \qquad [m + 1]P = [m]P + P, \qquad [m - 1]P = [m]P - P.$$

We call $[m]\colon E \to E$ the *multiplication-by-m map*.

Theorem 2.15 (Group Law Algorithm). *Let E be an elliptic curve in Weierstraß form*

$$E\colon y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Let $P_i = (x_i, y_i)$ be points on E.

1. *$-P_0 = (x_0, -y_0 - a_1 x_0 - a_3)$.*
2. *If $x_1 = x_2$ and $y_1 + y_2 + a_1 x_2 + a_3 = 0$, then $P_1 + P_2 = 0$.*
3. *Assume $P_1 \neq -P_2$. If $x_1 \neq x_2$ let*

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad and \qquad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$

If $x_1 = x_2$ (i.e. $P_1 = P_2$) let

$$\lambda = \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3} \qquad and \qquad \nu = \frac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3}.$$

Then $P_3 = P_1 + P_2$ is given by

$$x_3 = \lambda^2 + a_1 \lambda - a_2 - x_1 - x_2$$
$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3$$

These equations define morphisms

$$+\colon E \times E \to E\colon (P_1,\, P_2) \mapsto P_1 + P_2$$

$$-\colon E \to E\colon P \mapsto -P.$$

Proof. The formulas can be derived by direct calculations using the tangent-chord group law, see [Sil92, section III.2] or [ST92]. That the group operations are morphism is proved in [Sil92, theorem III.3.6]. □

Theorem 2.16. *Let E be an elliptic curve and $D = \sum n_P(P)$ a divisor on E. Then D is principal if and only if $\deg D = 0$ and $\sum [n_P]P = \mathcal{O}$.*

Proof. [Sil92, corollary III.3.5] □

We will finish this section with a brief look at singular curves in Weierstraß equation.

Definition 2.17. Let E be a (possibly singular) curve given by a Weierstraß equation. The *non-singular part of E*, denoted E_{ns}, is the set of non-singular points of E. If E is defined over K, then $E_{ns}(K)$ is the set of non-singular points in $E(K)$.

Theorem 2.18. *Let E be a curve given by a Weierstraß equation with discriminant $\Delta = 0$. Then E has exactly one singular point. The tangent-chord law makes E_{ns} into an Abelian group.*

If $c_4 \neq 0$, then E has a node (i.e. a point with two different tangent lines) and there exists an isomorphism $E_{ns} \to \bar{K}^*$. If $c_4 = 0$, then E has a cusp (i.e. a singular point with exactly one tangent line) and there exists an isomorphism $E_{ns} \to \bar{K}^+$. In both cases the isomorphism can be explicitly given by a (simple) rational function in the coordinates.

Proof. [Sil92, proposition III.1.4a and III.2.5] □

2.2   Isogenies

Definition 2.19. An *isogeny* between two elliptic curves E_1, E_2 is a morphism $\phi\colon E_1 \to E_2$ with $\phi(\mathcal{O}) = \mathcal{O}$. Two elliptic curves E_1 and E_2 are *isogenous* if there exists an isogeny ϕ between them with $\phi(E_1) \supsetneq \{\mathcal{O}\}$.

Note that by theorem 1.28 an isogeny is either constant or surjective. Obviously the composition of two isogenies is an isogeny. Hence "being isogenous" is a transitive relation. We will later see that it is also symmetric and therefore defines an equivalence relation on the set of elliptic curves over a fixed field.

Theorem 2.20. *Every isogeny is also a homomorphism of the Abelian groups defined on the elliptic curves: For $P, Q \in E_1$ we have*

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

The kernel of a non-constant isogeny is always a finite subgroup.

Proof. [Sil92, theorem III.4.8] □

Definition 2.21. Let E_1, E_2 be elliptic curves. We let[1]

$$\mathrm{Hom}(E_1,\ E_2) = \{\text{isogenies } E_1 \to E_2\}.$$

This is an Abelian group under the usual addition of functions

$$(\phi + \psi)(P) = \phi(P) + \psi(P).$$

The *endomorphism ring* of an elliptic curve E is

$$\mathrm{End}(E) = \mathrm{Hom}(E, E).$$

The invertible elements of $\mathrm{End}(E)$ form the *automorphism group* $\mathrm{Aut}(E)$.

---

[1]Some authors use $\mathrm{Isog}(E_1,\ E_2)$ instead of $\mathrm{Hom}(E_1,\ E_2)$.

Proposition 2.22.

1. *Let E be an elliptic curve and $m \in \mathbb{Z}$, $m \neq 0$. Then the multiplication-by-m map $[m] \colon E \to E$ is a surjective isogeny.*
2. *Let E_1, E_2 be elliptic curves. Then $\mathrm{Hom}(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module.*

Proof. [Sil92, proposition III.4.2] $\square$

Definition 2.23. The kernel of $[m] \colon E \to E$ $(m > 0)$ is called the *m-torsion subgroup* of E and is denoted $E[m]$. The *torsion subgroup of E* is the union of all m-torsion subgroups, $\bigcup\limits_{m>0} E[m]$.

Lemma 2.24. *Let E/K be an elliptic curve over a field of positive characteristic p given by a Weierstraß equation and let $\phi_q \colon E \to E^{(q)}$ be the qth-power Frobenius morphism. Then $E^{(q)}$ is an elliptic curve with $j(E^{(q)}) = j(E)^q$ and $\Delta(E^{(q)}) = \Delta(E)^q$.*

Definition 2.25. Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Then $E^{(q)} = E$ and ϕ_q is called the *Frobenius endomorphism* of E.

Definition 2.26. Let E be an elliptic curve and $Q \in E$. The *translation-by-Q map* on E is the map $P \to P + Q$. It is an isomorphism (but no isogeny) and denoted τ_Q.

Proposition 2.27. *Let ω be the invariant differential of an elliptic curve. Then $\tau_Q^* \omega = \omega$.*

Proof. [Sil92, corollary III.5.1] $\square$

Theorem 2.28. *Let $\phi \colon E_1 \to E_2$ be a non-constant isogeny. Then the map*

$$\begin{aligned} \ker \phi & \rightarrow \mathrm{Aut}\left(\bar{K}(E_1)/\phi^*\bar{K}(E_2)\right) \\ T & \mapsto \tau_T^* \end{aligned}$$

is an isomorphism. (τ_T is the translation-by-T map and τ_T^* the automorphism it induces on $\bar{K}(E_1)$.) If ϕ is separable, then it is unramified (hence $\#\ker\phi = \deg\phi$) and $\bar{K}(E_1)|\phi^*\bar{K}(E_2)$ is a Galois extension.

Proof. [Sil92, theorem III.4.10b and c] $\square$

Corollary 2.29. *Let $f \in \bar{K}(E)$ and m a positive integer. If $f = f \circ \tau_T$ for all $T \in E[m]$, then there exists $h \in \bar{K}(E)$ such that $f = h \circ [m]$.*

Theorem 2.30. *Let $\phi \colon E_1 \to E_2$ and $\psi \colon E_1 \to E_3$ be non-constant isogenies of elliptic curves. If ϕ is separable and $\ker\phi \subseteq \ker\psi$ there is a unique isogeny $\lambda \colon E_2 \to E_3$ such that $\psi = \lambda \circ \phi$.*

Proof. [Sil92, corollary III.4.11] $\square$

Theorem 2.31. *Let $\phi, \psi \colon E_1 \to E_2$ be two isogenies of elliptic curves and let ω be the invariant differential on ω. Then*

$$(\phi + \psi)^* \omega = \phi^* \omega + \psi^* \omega.$$

Proof. [Sil92, theorem III.5.2] $\square$

Theorem 2.32. *Let char $K = p$, let E be defined over $\mathbb{F}_q$ and let $\phi_q \colon E \to E$ be the qth-power Frobenius morphism. Then for $m, n \in \mathbb{Z}$ the map*

$$m + n\phi_q \colon E \to E$$

is separable if and only if $p \nmid m$. In particular $1 - \phi_q$ is separable.

Proof. [Sil92, corollary III.5.5] $\square$

Theorem 2.33. *Let E/K be an elliptic curve given by a Weierstraß equation*

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Let C be a finite subgroup of $E(\bar{K})$. Then there exists an elliptic curve E' and a separable isogeny $\alpha \colon E \to E'$ such that $C = \ker\alpha$. Further the Weierstraß coefficients of E' and the rational map α can be explicitly constructed from the a_i and the coordinates of the points in C.

Proof. An abstract proof of the first statement is given in [Sil92, theorem III.4.12] while a constructive proof of the whole theorem is given in [Was08, theorem 12.16]. $\qquad\square$

The formulas for E' and α are called *Vélu's formulas* and are explicitly given in [Was08, section 12.3].

While it is generally difficult to fully describe the endomorphism ring of an elliptic curve, the automorphism group $\mathrm{Aut}(E)$ is trivial for most curves:

Theorem 2.34. *Let E be an elliptic curve. Then $\mathrm{Aut}(E)$ is a finite group of order dividing* 24. *If $j(E)$ is not* 0 *or* 1728, *then $Aut(E) = \{\pm\,\mathrm{id}\}$.*

Proof. [Sil92, theorem III.10.1.] $\qquad\square$

We have already hinted that isogenies define an equivalence relation on the space of elliptic curves over a field. The following theorems says that indeed for every isogeny there exists a canonical isogeny going the other way.

Theorem 2.35. *Let $\phi\colon E_1 \to E_2$ be a non-constant isogeny of elliptic curves. Then there exists a unique isogeny $\widehat{\phi}\colon E_2 \to E_1$ satisfying $\widehat{\phi}\circ\phi = [\deg\phi]$. As a group homomorphism, $\widehat{\phi}$ equals the composition*

$$E_2 \to \mathrm{Div}^0(E_2) \overset{\phi^*}{\to} \mathrm{Div}^0(E_1) \overset{\mathrm{sum}}{\to} E_1,$$

where the first step is the embedding $Q \mapsto (Q) - (\mathcal{O})$ and $\mathrm{sum}\left(\sum n_P(P)\right) = \sum[n_P]P$.

Proof. [Sil92, theorem III.6.1] $\qquad\square$

Definition 2.36. The isogeny $\widehat{\phi}$ of the preceding theorem is called the *dual isogeny* to ϕ. The dual isogeny of $[0]$ is $[0]$.

Theorem 2.37. *Let $\phi\colon E_1 \to E_2$ be an isogeny. Then*

$$\widehat{\phi}\circ\phi = [\deg\phi] \qquad and \qquad \phi\circ\widehat{\phi} = [\deg\phi].$$

$$\deg\widehat{\phi} = \deg\phi.$$

$$\widehat{\widehat{\phi}} = \phi.$$

Let $\lambda\colon E_2 \to E_3$ be another isogeny. Then

$$\widehat{\lambda\circ\phi} = \widehat{\phi}\circ\widehat{\lambda}.$$

Let $\psi\colon E_1 \to E_2$ be another isogeny. Then

$$\widehat{\phi+\psi} = \widehat{\phi}+\widehat{\psi}.$$

For all $m \in \mathbb{Z}$,

$$\widehat{[m]} = [m] \qquad and \qquad \deg[m] = m^2.$$

Proof. [Sil92, theorem III.6.2] $\qquad\square$

2.3   Torsion Subgroups

Theorem 2.38. *Let E be an elliptic curve over K and m a non-zero integer. Then $\#E[m] < m^2$. If $\mathrm{char}\,K = 0$ or m is coprime to $\mathrm{char}(K)$, then*

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).$$

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

$$E[p^e] = 0 \qquad\quad \text{for all } e \in \mathbb{Z}^+, \text{ or}$$
$$E[p^e] = \mathbb{Z}/p^e\mathbb{Z} \qquad \text{for all } e \in \mathbb{Z}^+$$

As we have seen in theorem 2.33, every finite subgroup of $E(\bar{K})$ corresponds to a (separable) isogeny of degree equal to the order of the subgroup. If l is a prime different from $\operatorname{char} K$, the theorem above tells us that there are $l+1$ subgroups C_i of order l. Some of them might correspond to the same isogenous curve (up to isomorphism). Fortunately most of the time this is not true and the subgroups of order l correspond exactly to the isogenous curves of E with isogenies of degree l.

Theorem 2.39. *Let E/K be an elliptic curve with j-invariant not equal to 0 or 1728. Further let l be a prime different from $\operatorname{char}(K)$ and let C_i $(1 \leq i \leq l+1)$ be all subgroups of $E(\bar{K})$ of order l. Then no two of the elliptic curves E/C_i are isomorphic.*

Proof. Assume on the contrary that there exists $1 \leq r \neq s \leq l+1$ such that E/C_r and E/C_s are isomorphic. Let ϕ_r and ϕ_s be the corresponding isogenies and κ the isomorphism, so that we get the following diagram:

$$
\begin{array}{ccc}
E & \xrightarrow{\phi_r} & E/C_r \\
 & & \downarrow{\kappa} \\
E & \xrightarrow{\phi_s} & E/C_s
\end{array}
$$

The maps $\widehat{\phi}_s \circ \phi_s$ and $\widehat{\phi}_s \circ \kappa \circ \phi_r$ are both endomorphisms of E of degree l^2. Hence they both have a kernel of size l^2 which has to be $E[l]$. By theorem 2.30 they differ only by an endomorphism of degree 1, i.e. and automorphism. By theorem 2.34 this automorphism must be $\pm\operatorname{id}$. Therefore,

$$\widehat{\phi}_s \circ \kappa \circ \phi_r = \pm\widehat{\phi}_s \circ \phi_s = \pm[l]$$

and by applying ϕ_s we get

$$\phi_s \circ \widehat{\phi}_s \circ \kappa \circ \phi_r = [l] \circ \kappa \circ \phi_r = \kappa \circ \phi_r \circ [l] = \phi_s \circ [\pm l]. \tag{2.5}$$

Since $C_r \neq C_s$ and both have prime order, $C_r \cap C_s = \{\mathcal{O}\}$. Let $P \in E(\bar{K})$ with $[l]P \in C_r \setminus \{\mathcal{O}\}$. Then

$$\kappa \circ \phi_r([l]P) = \mathcal{O} \qquad \text{and} \qquad \phi_s(\pm[l]P) \neq \mathcal{O}.$$

This is a contradiction to (2.5). $\qquad\square$

2.4   Pairings

Definition 2.40. Let n be a positive integer, G_1, G_2 two Abelian groups with exponent n (written additively) and G_3 a cyclic group of order n (written multiplicatively). A *pairing* is a function

$$e\colon G_1 \times G_2 \to G_3.$$

A pairing is *bilinear* if for all $P, P' \in G_1$ and $Q, Q' \in G_2$:

$$e(P + P', Q) = e(P, Q)e(P', Q)$$

$$e(P, Q + Q') = e(P, Q)e(P, Q').$$

It is *degenerate* if there exists $P \in G_1$, $P \neq 0$ such that $e(P, Q) = 1$ for all $Q \in G_2$ or if there exists $Q \in G_2$, $Q \neq 0$ such that $e(P, Q) = 1$ for all $P \in G_1$. Otherwise it is *non-degenerate*.

We will define pairings on (subgroups of) the points of an elliptic curve E and will use them for two purposes: First we will use the existence of specific pairings to derive facts about the group structure and secondly we will use them to transfer the elliptic curve discrete logarithm problem to a DLP where more efficient algorithms are known.

Let $\boldsymbol{\mu}_n = \boldsymbol{\mu}_n(K) = \{u \in \bar{K}^* : u^n = 1\}$ be the nth *roots of unity*. Further let $(K^*)^n = \{u^n : u \in K^*\}$.

Choose a point $P \in E(K)[n]$. Then by theorem 2.16 there exists a function f_P (unique up to a multiplicative constant) with $\operatorname{div}(f_P) = n(P) - n(\mathcal{O})$. Choose a second point $Q \in E(K)$ and choose a divisor $D_Q \sim (Q) - (\mathcal{O})$ such that the support of D_Q is disjoint from the support of $\operatorname{div}(f_P)$. We can now combine f_P and D_Q and calculate $f_P(D_Q) \in K^*$ (see definition 1.44). Obviously the result will not only depend on P and Q but also on the chosen divisor D_Q. However, by factoring out the right subgroups we can make it independent of the divisor.

Definition 2.41. Let n be a positive integer such that K contains the nth roots of unity. Using the notation of the preceding paragraph and writing $\bar{Q}$ for the coset of Q, the *Tate* (or *Tate-Lichtenbaum*) *pairing*

$$\tau_n \colon E(K)[n] \times E(K)/nE(K) \to K^*/(K^*)^n$$

on the elliptic curve E/K is defined as

$$\tau_n(P, \bar{Q}) = f_P(D_Q).$$

The groups $E(K)/nE(K)$ are called the *weak Mordell-Weil groups* of E and are used to study the structure of $E(K)$. The Tate pairing is in turn used to study the weak Mordell-Weil groups. See [Sil92, chapters VIII–X] for more information. We will use it in section 7.3 to derive information about the other group, $E(K)[n]$.

Theorem 2.42. *The Tate pairing is well-defined and bilinear. Further, it is Galois invariant, i.e. if $\sigma \in \mathrm{Gal}(\bar{K}/K)$, then $\tau_n(P^\sigma, Q^\sigma) = \tau_n(P, Q)^\sigma$. If K is a finite field then it is also non-degenerate.*

Proof.

1. *Well-definedness:* Let $D \sim D' = D + \mathrm{div}(g)$ be two degree zero divisors such that the supports of D and D' are disjoint from $\mathrm{supp}\,\mathrm{div}(f_P)$. Then the supports of $\mathrm{div}(g)$ are $\mathrm{div}(f_P)$ are also disjoint and

   $$f_P(D') = f_P(D + \mathrm{div}(g)) = f_P(D)f_P(\mathrm{div}(g)).$$

   Using Weil reciprocity (theorem 1.46) we get

   $$f_P(\mathrm{div}(g)) = g(\mathrm{div}(f_P)) = g(n(P) - n(\mathcal{O})) = (g(P)/g(\mathcal{O}))^n \in (K^*)^n$$

   and thus $f_P(D) = f_P(D') \bmod (K^*)^n$.

   Let Q_1 and $Q_2 = Q_1 + [n]R$ be two representatives of $\bar{Q}$ and $D_{Q_i} \sim (Q_i) - (\mathcal{O})$. By theorem 2.16

   $$D_{Q_2} \sim (Q_1 + [n]R) - (\mathcal{O}) \sim (Q_1) - (\mathcal{O}) + n(R) - n(\mathcal{O}) \sim D_{Q_1} + n(R) - n(\mathcal{O})$$

   and, like above,

   $$f_P(D_{Q_2}) = f_P(D_{Q_1} + n(R) - n(\mathcal{O})) = f_P(D_{Q_1})f_P((R) - (\mathcal{O}))^n = f_P(D_{Q_1}) \mod (K^*)^n.$$

2. *Bilinearity:* For bilinearity in the first component we have to show that $\tau_n(P_1 + P_2, Q) = \tau_n(P_1, Q)\tau_n(P_2, Q)$. Let $P_3 = P_1 + P_2$ and let g be a rational function with $\mathrm{div}(g) = (P_3) - (P_1) - (P_2) + (\mathcal{O})$. Hence $\mathrm{div}(f_{P_3}) = \mathrm{div}(f_{P_1}f_{P_2}g^n)$. Further choose $D_Q \sim (Q) - (\mathcal{O})$ with support disjoint from $\{P_1, P_2, P_3, \mathcal{O}\}$. Then

   $$\tau_n(P_1 + P_2, Q) = \tau_n(P_3, Q) = f_{P_1}f_{P_2}g^n(D_Q)$$
   $$= f_{P_1}(D_Q)f_{P_2}(D_Q)g(D_Q)^n = \tau_n(P_1, Q)\tau_n(P_2, Q) \mod (K^*)^n.$$

   For the second component we have to show $\tau_n(P, Q_1 + Q_2) = \tau_n(P, Q_1)\tau_n(P, Q_2)$. We have $D_{Q_1 + Q_2} \sim (Q_1 + Q_2) - (\mathcal{O}) \sim (Q_1) + (Q_2) - 2(\mathcal{O}) \sim D_{Q_1} + D_{Q_2}$ and hence $\bmod(K^*)^n$,

   $$\tau_n(P, Q_1 + Q_2) = f_P(D_{Q_1} + D_{Q_2}) = f_P(D_{Q_1})f_P(D_{Q_2}) = \tau_n(P, Q_1)\tau_n(P, Q_2).$$

3. *Non-degeneracy:* see [Heß04].

4. *Galois invariance:* We have $\mathrm{div}(f_{P^\sigma}) = n(P^\sigma) - n(\mathcal{O}) = \mathrm{div}((f_P)^\sigma)$ and $D_{Q^\sigma} = (D_Q)^\sigma$. Thus modulo n^{th} powers:

   $$\tau_n(P^\sigma, Q^\sigma) = f_{P^\sigma}(D_{Q^\sigma}) = (f_P)^\sigma((D_Q)^\sigma) = (f_P(D_Q))^\sigma = \tau_n(P, Q)^\sigma. \qquad \square$$

Definition 2.43. A bilinear pairing $e \colon G \times G \to G'$ is *alternating* if $e(P, P) = 1$ for all $P \in G$.

For alternating pairings,

$$1 = e(P+Q, P+Q) = e(P,P)e(P,Q)e(Q,P)e(Q,Q) = e(P,Q)e(Q,P)$$

and hence $e(P,Q) = e(Q,P)^{-1}$.

We will now construct an alternating pairing on $E[n]$. Let $P, Q \in E[n]$ and, like for the Tate pairing, choose divisors $D_P \sim (P) - (\mathcal{O})$ and $D_Q \sim (Q) - (\mathcal{O})$ with disjoint support. Further choose functions g_P and g_Q with $\mathrm{div}(g_P) = nD_P$ and $\mathrm{div}(g_Q) = nD_Q$ respectively.

Definition 2.44. Let n be a positive integer such that $E[n] \subseteq E(K)$. Using the notation of the preceding paragraph we define the *Weil pairing*

$$e_n \colon E[n] \times E[n] \to \boldsymbol{\mu}_n(K)$$

on the elliptic curve E/K by

$$e_n(P,Q) = \frac{g_P(D_Q)}{g_Q(D_P)}.$$

Theorem 2.45. *The Weil pairing is well-defined, bilinear, non-degenerate, alternating and Galois invariant. Further if $P \in E[mn]$ and $Q \in E[n]$, then $e_{mn}(P,Q) = e_n([m]P,Q)$.*

Proof.

1. *Well-definedness:* We have to show that the pairing does not depend on the particular choice of D_P and D_Q. We will only show the independence of the choice of D_P since the proof for D_Q is completely analogous. Let $D'_P = D_P + \mathrm{div}(f)$ for some $f \in K(E)$ and $g'_P \in K(E)$ with $\mathrm{div}(g'_P) = nD'_P = nD_P + n\,\mathrm{div}(f)$. Then $g'_P = cg_P f^n$ for some $c \in \bar{K}^*$. Also (using Weil reciprocity),

$$g_Q(D'_P) = g_Q(D_P)g_Q(\mathrm{div}(f)) = g_Q(D_P)g_Q(\mathrm{div}(f)) = g_Q(D_P)f(\mathrm{div}(g_Q))$$

   and hence

$$\frac{g'_P(D_Q)}{g_Q(D'_P)} = \frac{g_P(D_Q)f(D_Q)^n}{g_Q(D_P)f(nD_Q)} = \frac{g_P(D_Q)}{g_Q(D_P)}.$$

   Further $e(P,Q) \in \boldsymbol{\mu}_n$ because

$$\left(\frac{g_P(D_Q)}{g_Q(D_P)}\right)^n = \frac{g_P(nD_Q)}{g_Q(nD_P)} = \frac{g_Q(nD_P)}{g_Q(nD_P)} = 1.$$

2. *Bilinearity* can be checked, like for the Tate pairing, using a function h such that $D_{P_1+P_2} = D_{P_1} + D_{P_2} + \mathrm{div}(h)$.

3. *Alternating:* The pairing $e_n(P,P)$ is computed using the divisors $D_P, D'_P \sim (P) - (\mathcal{O})$ and corresponding functions g_P, g'_P. Let $f \in K(E)$ with $D'_P = D_P + \mathrm{div}(f)$. Then like above there exists $c \in \bar{K}^*$ with $g'_P = cg_P f^n$. Hence

$$g_P(D'_P) = g_P(D_P)g_P(\mathrm{div}(f)) = g_P(D_P)f(\mathrm{div}(g_P)) = g_P(D_P)f(D_P)^n = g'_P(D_P).$$

4. *Non-degeneracy:* Assume that $e_n(P,Q) = 1$ for all $Q \in E[n]$. Fix a point R in $E(\bar{K})$ with $R \notin \{\mathcal{O}, P\}$. For every point $X \in E$ let $Y_X = [n]X - [n-1]R$ and choose a function ψ_X with $\mathrm{div}(\psi_X) = n(X) - (n-1)(R) - (Y_X)$. We note that the map $X \mapsto \psi_X(D)$ is rational for any fixed $D \in \mathrm{Div}^0(E)$. In the definition of the Weil pairing we choose $D_P = (P) - (\mathcal{O})$. Then we have

$$\left(\frac{g_P(X)}{\psi_X((P) - (\mathcal{O}))}\right)^n = \frac{g_P(n(X))}{\psi_X(\mathrm{div}(g_P))} = \frac{g_P(n(X))}{g_P(\mathrm{div}(\psi_X))} = g_P(n(X) - \mathrm{div}(\psi_X))$$
$$= g_P((Y_X) + (n-1)(R)) = g_P(Y_X)g_P(R)^{n-1}.$$

   Further we choose $D_Q = (Q + X) - (X)$. Since $[n](Q+X) = [n](X)$ we see that

$$\mathrm{div}(\psi_{Q+X}) - \mathrm{div}(\psi_X) = n(Q+X) - n(X) = \mathrm{div}(g_Q).$$

Hence for all $Q \in E[n]$ (τ_Q is the translation-by-Q map),

$$\left(\frac{g_P}{\psi_\cdot(D_P)} \circ \tau_Q \right)(X) = \frac{g_P(X+Q)}{\psi_{X+Q}(D_P)} = \frac{g_P((X+Q)-(X))}{g_Q(D_P)} \frac{g_P(X)}{\psi_X(D_P)} = \underbrace{e_n(P,Q)}_{=1} \frac{g_P(X)}{\psi_X(D_P)}.$$

Using corollary 2.29 we deduce that there exists a function $h \in \bar{K}(E)$ such that

$$\frac{g_P(X)}{\psi_X(D_P)} = (h \circ [n])(X) = h(Y_X + [n-1]R).$$

Putting things together we get

$$g_P(Y_X)g_P(R)^{n-1} = \left(\frac{g_P(X)}{\psi_X(D_P)} \right)^n = (h \circ \tau_{[n-1]R})^n(Y_X).$$

Since $[m]$ is a non-zero isogeny and hence surjective, for every $Y \in E$ we can find an $X \in E$ with $Y_X = Y$. So the above equation is indeed an equation of functions on E. R is constant and thus

$$n((P) - (\mathcal{O})) = \operatorname{div}(g_P) = n\operatorname{div}(h \circ \tau_{[n-1]R}).$$

Therefore $(P) \sim (\mathcal{O})$ which is only possible if $P = \mathcal{O}$ (lemma 2.10).

5. *Galois invariance* can again be simply checked by inserting definitions.

6. *Compatibility:* In the same manner one can verify that

$$e_{mn}(P,Q) = e_n([m]P,Q). \qquad \qed$$

Theorem 2.46. *Let char $K = 0$ or n be coprime to char K. Then there exist points $P, Q \in E[n]$ such that $e_n(P,Q)$ is a primitive n^{th} root of unity. In particular the Weil pairing is surjective and if $E[n] \subseteq E(K)$ then $\boldsymbol{\mu}_n \subseteq K^*$.*

Proof. By linearity the image of e_n is a subgroup $\boldsymbol{\mu}_d$ of $\boldsymbol{\mu}_n$. Therefore for all $P, Q \in E[n]$ we have $1 = e_n(P,Q)^d = e_n([d]P,Q)$ an since the Weil pairing is non-degenerate this implies $P \in E[d]$ for all $P \in E[n]$. By theorem 2.38 this is only possible if $d = n$. Hence e_n is surjective and the image contains a primitive n^{th} root of unity.

If $E[n] \subseteq E(K)$, the Galois invariance of e_n shows that $e_n(P,Q) \in K^*$ for all $P, Q \in E[n]$ and thus $\boldsymbol{\mu}_n \subseteq K^*$. $\qed$

Our definition of the Weil pairing is not the only one possible, but it is one that is useful for our purposes because it lends itself to computation. (The same is true for the Tate-Lichtenbaum pairing.) However sometimes the following alternative definition is used:

Proposition 2.47. *Let $P, Q \in E[n]$. Chose a function g satisfying*

$$\operatorname{div}(g) = [n]^*(Q) - [n]^*(\mathcal{O}).$$

Then for any point $X \in E$ such that X and $X + P$ are disjoint from the support of $\operatorname{div}(g)$,

$$e_n(P,Q) = g((X) - (X+P)).$$

Proof. The proof is conceptually simple but rather technical and lengthy and thus we will not include it here. See [Was08, Theorem 11.12] $\qed$

Proposition 2.48. *Let $\psi \colon E \to E'$ be an isogeny with dual $\widehat{\phi} \colon E' \to E$. Then ϕ and $\widehat{\phi}$ are adjoint with respect to the Weil pairing, i.e. $e_m(\phi(P),Q) = e_m(P,\widehat{\phi}(Q))$.*

Proof. We will use our original definition of the Weil pairing. Let $D_Q = (Q) + (\mathcal{O})$, $D_{\widehat{\phi}Q} = (\widehat{\phi}Q) - (\mathcal{O})$ and $D_{\phi P} = \phi_* D_P$ (and thus $g_{\phi P} = \phi_* g_P$). Chose a function $h \in \bar{K}(E_1)$ such that

$$\phi^*(Q) - \phi^*(\mathcal{O}) = (\widehat{\phi}Q) - (\mathcal{O}) + \operatorname{div}(h).$$

This is possible by 2.35. Now

$$\text{div}\left(\frac{f \circ \phi}{h^m}\right) = \phi^* \text{div}(f) - m\,\text{div}(h) = m(\widehat{\phi}Q) - m(\mathcal{O}).$$

Hence up to multiplication with a constant $g_{\widehat{\phi}Q} = \frac{g_Q \circ \phi}{h^m}$. Using this we get

$$e_m(P, \widehat{\phi}Q) = \frac{g_P(D_{\widehat{\phi}Q})}{\frac{g_Q \circ \phi}{h^m}(D_P)} = \frac{g_P(D_{\widehat{\phi}Q}) \cdot h(mD_P)}{(g_Q \circ \phi)(D_P)} = \frac{g_P(D_{\widehat{\phi}Q}) \cdot g_P(\text{div}(h))}{(g_Q \circ \phi)(D_P)} = \frac{g_P(D_{\widehat{\phi}Q} + \text{div}(h))}{(g_Q \circ \phi)(D_P)}$$

$$= \frac{g_P(\phi^* D_Q)}{g_Q(\phi_* D_P)} = \frac{\phi_* g_P(D_Q)}{g_Q(\phi_* D_P)} = \frac{g_{\phi P}(D_Q)}{g_Q(D_{\phi P})} = e_m(\phi P, Q). \quad \square$$

2.5   The Tate Module

Definition 2.49. Let E be an elliptic curve and $\ell \in \mathbb{Z}$ be a prime. Then the (ℓ-*adic*) *Tate module* of E is the group

$$T_\ell(E) = \varprojlim_n E[\ell^n],$$

where the inverse limit is taken with respect to the multiplication-by-ℓ maps

$$[\ell] \colon E[\ell^{n+1}] \to E[\ell^n].$$

Every $E[\ell^n]$ is a $\mathbb{Z}/\ell^n\mathbb{Z}$-module and the natural maps $\mathbb{Z}/\ell^{n+1}\mathbb{Z} \to \mathbb{Z}/\ell^n\mathbb{Z}$ are obviously compatible with the inverse system used to define the Tate module. Hence $T_\ell(E)$ is a $\mathbb{Z}_\ell$-module.

From theorem 2.38 we immediately obtain the following structure of the Tate module:

Proposition 2.50. *As a $\mathbb{Z}_\ell$-module $T_\ell(E)$ has the following structure:*

1. $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ *for* $\ell \neq \text{char}(K)$;
2. $T_p(E) \cong \{0\}$ *or* $\mathbb{Z}_p$ *for* $p = \text{char}(K) > 0$.

On every torsion group $E[n]$ we defined a pairing e_n, so we can try to put them together to get a pairing on the Tate module. First we need some additional notation: Let K be a field and $\boldsymbol{\mu}_{\ell^n} \subseteq \bar{K}$ its $(\ell^n)^{\text{th}}$ roots of unity. Then raising to the ℓth power gives maps $\ell \colon \boldsymbol{\mu}_{\ell^{n+1}} \to \boldsymbol{\mu}_{\ell^n}$ and all these maps together form an inverse system $(\boldsymbol{\mu}_{\ell^n}, \ell)_{n \in \mathbb{N}}$. The inverse limit $T_\ell(\boldsymbol{\mu}) = \varprojlim_n \boldsymbol{\mu}_{\ell^n}$ of this system is called the *Tate module of K*.

Theorem 2.51. *There exists a bilinear, alternating, non-degenerate and Galois invariant pairing*

$$e \colon T_\ell(E) \times T_\ell(E) \to T_\ell(\boldsymbol{\mu}),$$

called the ℓ-adic Weil pairing. If $\phi \colon E_1 \to E_2$ is an isogeny then ϕ and $\widehat{\phi}$ are adjoints for this pairing.

Proof. We only have to show that the Weil pairing is compatible with the maps of the inverse systems defining $T_\ell(E)$ and $T_\ell(\boldsymbol{\mu})$, i.e. that

$$e_{\ell^{n+1}}(P, Q)^\ell = e_{\ell^n}([\ell]P, [\ell]Q).$$

This follows immediately from the properties of the Weil pairing (in particular linearity and compatibility):

$$e_{\ell^n}([\ell]P, [\ell]Q) = e_{\ell^n}([\ell]P, Q)^\ell = e_{\ell^n \cdot \ell}(P, Q)^\ell. \qquad \square$$

Let $\phi \colon E_1 \to E_2$ be an isogeny of elliptic curves. It induces homomorphisms

$$\phi \colon E_1[\ell^n] \to E_2[\ell^n].$$

Thus every isogeny ϕ induces a $\mathbb{Z}_\ell$-linear map

$$\phi_\ell \colon T_\ell(E_1) \to T_\ell(E_2).$$

In particular this gives a (ring) homomorphism $\text{End}(E) \to \text{End}(T_\ell(E))$. For $\ell \neq \text{char}\,K$, $\text{End}(T_\ell(E))$ is isomorphic to $M_2(\mathbb{Z}_\ell)$ (the 2×2-matrices over $\mathbb{Z}_\ell$). So we can look at the determinant and trace of endomorphisms.

Theorem 2.52. *Let ℓ be a prime not equal to $\mathrm{char}(K)$ and $\phi \in \mathrm{End}(E)$. Then*

$$\det(\phi_\ell) = \deg(\phi), \qquad \mathrm{tr}(\phi) = 1 + \deg(\phi) + \deg(1 - \phi).$$

In particular, $\det(\phi_\ell)$ and $\mathrm{tr}(\phi_\ell)$ are in $\mathbb{Z}$ and independent of ℓ.

Proof. Choose any basis v_1, v_2 for $\mathbb{Z}_\ell$ and write $\phi_\ell = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right)$ with respect to this basis. Using the paring e we have just defined we can calculate

$$e(v_1, v_2)^{\deg \phi} = e([\deg \phi]v_1, v_2) = e(\widehat{\phi_\ell}\phi_\ell v_1, v_2) = e(\phi_\ell v_1, \phi_\ell v_2) =$$
$$e(av_1 + cv_2, bv_1 + bv_2) = e(v_1, v_2)^{ad-bc} = e(v_1, v_2)^{\det \psi_\ell}.$$

By the non-degeneracy of e this implies $\deg \phi = \det \psi_\ell$. Further for any 2×2 matrix A we have

$$\mathrm{tr}\, A = 1 + \det A - \det(1 - A). \qquad \square$$

Definition 2.53. Let $\phi \in \mathrm{End}(E)$. Then the *determinant* $\det \phi$, the *trace* $\mathrm{tr}\, \phi$ and the *characteristic polynomial* of ϕ are defined to be the respective objects of ϕ_ℓ for any prime $\ell \neq \mathrm{char}(K)$.

In section 3.3 we will see that the trace of the Frobenius plays an important role in the theory of elliptic curves over finite fields.

Proposition 2.54. *The characteristic polynomial of the qth-power Frobenius endomorphism ϕ_q is*

$$T^2 - \mathrm{tr}(\phi_q)T + q \in \mathbb{Z}[T].$$

Proof. By linear algebra we know that the characteristic polynomial of a 2×2 matrix A is $T^2 - \mathrm{tr}(A)T + \det(A)$. For the Frobenius we have $\det \phi_q = \deg \phi_q = q$. $\qquad \square$

Theorem 2.55. *For any $\phi \in \mathrm{End}(E)$,*
$$\phi + \widehat{\phi} = [\mathrm{tr}\, \phi].$$

Further, ϕ and $\widehat{\phi}$ have the same characteristic polynomial.

Proof. First we will show that $\phi + \widehat{\phi} \in \mathbb{Z} \subseteq \mathrm{End}(E)$:

$$\deg(1 + \phi) = (1 + \phi)(1 + \widehat{\phi}) = 1 + (\phi + \widehat{\phi}) + \phi\widehat{\phi}.$$

Since $\phi\widehat{\phi} \in \mathbb{Z}$ and $\deg(1 + \phi) \in \mathbb{Z}$, also $\phi + \widehat{\phi} \in \mathbb{Z}$. Define a polynomial

$$p(T) = T^2 - (\phi + \widehat{\phi})T + \det(\phi) \in \mathbb{Z}[T].$$

Then $p(\phi) = 0$ (because $\det(\phi) = \widehat{\phi}\phi$) and hence $p(T)$ is equal to the minimal polynomial of ϕ, which is $T^2 - (\mathrm{tr}\, \phi)T + \det(\phi)$.

Also directly from theorem 2.52 we see that $\mathrm{tr}\, \phi = \mathrm{tr}\, \widehat{\phi}$ and $\det \phi = \det \widehat{\phi}$. $\qquad \square$

2.6 Hyperelliptic curves

Our interest in elliptic curves ultimately stems from the fact that they provide a means of realizing an abstract group. In particular, the abstract group $\mathrm{Pic}^0(E)$ is represented by the points of E and the group laws of section 2.1. Therefore the group operations in $\mathrm{Pic}^0(E)$ are efficiently computable. A second class of curves where the degree zero part of the Picard group has an efficiently computable group operation are the hyperelliptic curves. We will later see how they are connected to elliptic curve cryptography. Presently we will only introduce the necessary theoretic background. As we have done for the basic properties of elliptic curves, we will skip all proofs. Everything in this chapter can be proven in an elementary way. A good self-sufficient introduction is given in [MWZ98]. Another (less elementary) introduction is [Was08, chapter 13].

Definition 2.56. A *hyperelliptic curve of genus g* ($g \geq 2$) is an algebraic curve C/K given by an equation

$$C \colon y^2 + h(x)y = f(x), \tag{2.6}$$

where $h(x) \in K[x]$ is a polynomial of degree at most g and $f(x) \in K[x]$ is a monic polynomial of degree exactly $2g + 1$ and such that C is non-singular at all points of $C \cap \mathbb{A}^2$.

There is exactly one point on C that does not lie in the usual affine piece. As usual it is called the *point at infinity* and denoted ∞. Note that while a hyperelliptic curve is non-singular at every finite point, it is singular at ∞. In order to apply the results of chapter 1 to C one needs a non-singular model of the curve. The way to obtain one is a process called *normalization* [Sha94a, section II.5.3]. For hyperelliptic curves this is done explicitly in [Sil92, exercise 2.14]. Fortunately the curve one obtains by this process has the same affine piece as (2.6). The same exercise in Silverman's book also shows that the genus of the curve given by this equation is indeed g.

There is also an intrinsic way to define hyperelliptic curves: A curve X is hyperelliptic if and only if its genus is at least 2 and there exists a finite morphism $f \colon X \to \mathbb{P}^1$ of degree 2.[2] See [Har77] for the essential differences of hyperelliptic and non-hyperelliptic curves form the point of view of abstract algebraic geometry. See also [Mum84] for a through study of hyperelliptic curves over the complex numbers.

For $g = 1$, definition 2.56 also includes elliptic curves, but it is usual not to include elliptic curves under the notion of hyperelliptic curves, as there are some essential differences. Nevertheless, everything in this section does also apply in the case of $g = 1$ and yields the corresponding properties of elliptic curves.

Proposition 2.57. *Let* $\operatorname{char} K \neq 2$ *and let* C/K *be the hyperelliptic curve given by* (2.6). *Then the change of variables* $x \mapsto x$, $y \mapsto \frac{y - h(x)}{2}$ *transforms* C *to the form*

$$C \colon y^2 = f(x). \tag{2.7}$$

An equation of this form defines an hyperelliptic curve if and only if $\operatorname{char} K \neq 2$ *and* f *has no repeated roots in* $\bar{K}$.

For the rest of this section C will always denote a hyperelliptic curve of genus g given by an equation of the form (2.6) or (2.7).

Definition 2.58. For a finite point $P = (x, y) \in C(\bar{K})$ define $w(P) = (x, -y - h(x))$ and for the point at infinity define $w(\infty) = \infty$. Then $w(P)$ is called the *opposite of* P and the map w the *hyperelliptic involution*. On elliptic curves w is just multiplication by -1. If $D = \sum m_P P \in \operatorname{Div}(C)$ is a divisor then $w(D) = \sum m_P w(P)$.

Proposition 2.59. *Let* D *be a divisor of degree* 0. *Then* $D + w(D)$ *is a principal divisor.*

Definition 2.60. A divisor $D \in \operatorname{Div}(C)$ is called *semi-reduced* if it is of the form $D = \sum m_P (P) - (\sum m_P)(\infty)$ and satisfies the following conditions:

1. all $m_P \geq 0$ and $m_\infty = 0$,
2. if $P = w(P)$, then $m_P \leq 1$ and
3. if $P \neq w(P)$, then $m_P = 0$ or $m_{w(P)} = 0$.

A divisor is called *reduced* if it is semi-reduced and $\sum m_P \leq g$.

Let $J = \operatorname{Pic}^0(C)$ be the degree zero part of the divisor class group, i.e. the quotient of $\operatorname{Div}^0(C)$ by the subgroup of principal divisors. It is also called the *Jacobian variety* of C. (Strictly speaking this name is not correct, see [Sha94a, section III.4.4] and [Har77, section IV.4]). The following two theorems are crucial to the use of hyperelliptic curves for computational purposes.

Theorem 2.61. *In every class of* $\operatorname{Pic}^0(C)$ *there is a unique reduced representative.*

For every point $P \in C(\bar{K})$ the divisor $P - \infty$ is reduced. Thus the last theorem implies that the map

$$\begin{aligned} \kappa \colon C &\to J \\ P &\mapsto \text{class of } P - \infty \end{aligned}$$

is injective. In the case of elliptic curves it is an isomorphism as we have already seen in theorems 2.11 and 2.13.

---

[2]This definition is not completely equivalent to the one we gave, but a through discussion of hyperelliptic curves is beyond the scope of this section.

Definition 2.62. Let $D_1 = \sum m_P((P) - (\infty))$ and $D_2 = \sum n_P((P) - (\infty))$ be two divisors with $m_P, n_P \geq 0$ for all $P \in C$. Then the *greatest common divisor of D_1 and D_2* is

$$\gcd(D_1, D_2) = \sum_P \min\{m_P, n_P\}((P) - (\infty)).$$

Theorem 2.63. *There is a one-to-one correspondence between semi-reduced divisors $\sum m_P((P) - (\infty))$ and pairs $(U(x), V(x))$ of polynomials in $\bar{K}[x]$ satisfying*

1. *$U(x)$ is monic,*
2. *$\deg U(x) = \sum m_P$, $\deg V(x) < \deg U(x)$ and*
3. *$V(x)^2 + V(x)h(x) - f(x)$ is a multiple of $U(x)$.*

Under this correspondence, $D = \gcd(\operatorname{div}(U(x)), \operatorname{div}(y - V(x)))$.

Corollary 2.64. *There is a one-to-one correspondence between element of $\operatorname{Pic}^0(C)$ and pairs $(U(x), V(x))$ of polynomials in $\bar{K}[x]$ satisfying*

1. *$U(x)$ is monic,*
2. *$\deg V(x) < \deg U(x) \leq g$ and*
3. *$V(x)^2 + V(x)h(x) - f(x)$ is a multiple of $U(x)$.*

There is a one-to-one correspondence between element of $\operatorname{Pic}_K^0(C)$ and pairs $(U(x), V(x))$ of polynomials in $K[x]$ satisfying the above properties.

This representation of divisor classes is called *Mumford representation*. The zero divisor is represented by $(1, 0)$.

Corollary 2.65. *If K is a finite field, then $\operatorname{Pic}_K^0(C)$ is finite.*

We will later give bounds for the exact size of $\operatorname{Pic}_K^0(C)$.

The only remaining piece is an algorithm that calculates the Mumford representation of the sum of two divisors given in Mumford representation. Such an algorithm has been devised by David Cantor in [Can87] for $h(x) = 0$. It has been extended to arbitrary h by Neil Koblitz in [Kob89]. We will state the generalized algorithm. Cantor's original algorithm is obtained by setting $h(x) = 0$.

Algorithm 2.66 (Cantor's Algorithm). *Let D_1 and D_2 be two semi-reduced divisors of C with Mumford representation (U_1, V_1) and (U_2, V_2) respectively. The following algorithm returns the Mumford representation (U, V) of $D_1 + D_2$.*

1. *Using the (extended) Euclidean algorithm, calculate $d = \gcd(U_1, U_2, V_1 + V_2 + h)$ and polynomials h_1, h_2, h_3 such that $d = h_1 U_1 + h_2 U_2 + h_3(V_1 + V_2 + h)$.*
2. *Set $U = \frac{U_1 U_2}{d^2}$.*
3. *Set $V = \frac{U_1 V_2 h_1 + U_2 V_1 h_2 + (V_1 V_2 + f)h_3}{d} \bmod U$ with $\deg V < \deg U$.*
4. *Return (U, V).*

Algorithm 2.67 (Reduction Procedure). *Let D be a semi-reduced divisor with Mumford representation (U, V). The following algorithm returns the Mumford representation (U', V') of a reduced divisor $D' \sim D$.*

1. *Set $U' = \frac{f - Vh - V^2}{U}$.*
2. *Set $V' = -h - V' \bmod U$ with $\deg V' < \deg U'$.*
3. *If $\deg U' > g$, set $U = U'$ and $V = V'$ and return to step 1.*
4. *Let c be the leading coefficient of U', and set $U' \leftarrow c^{-1} U'$.*
5. *Return (U', V').*

Corollary 2.68. *Let (U, V) be the Mumford representation of a divisor class in $\operatorname{Pic}^0(C)$. Then its inverse in given by $(U, -V - h)$.*

Cartan's algorithm is not the only algorithm for the addition of two divisor classes. See [BSS05, section VII.2] for an overview of algorithms and considerations that have to be taken into account for efficient implementation.

Chapter 3

Elliptic Curves over Special Fields

So far we developed the theory of elliptic curves without assuming anything about the ground field (except that it is perfect). Ultimately we want to derive information about elliptic curves defined over finite fields. However in order to do this we have to make use of the theory of elliptic curves over the complex numbers and over local fields. Therefore we will take a look at these classes of curves. We will also define two families of polynomials which make sense over every field.

3.1 Elliptic Curves over the Complex Numbers

In many parts of the theory of elliptic curves it is helpful to have the background of elliptic curves over the complex numbers. In a sense the complex numbers are the must natural field of definition. Historically the study of elliptic curves began here. The intuition gained over the complex numbers will guide us in the next section to the right definitions.

Why are the complex numbers the "most natural" setting for elliptic curves? Firstly the GAGA principle [Har77, appendix B] allows us to use methods from complex analysis to study the a priori only algebraic variety. Secondly there exists an analytic group isomorphism to a much simpler space (namely a 2-torus) which reduces many problems on the elliptic curve to problems about elliptic functions which are a classical and well-studies domain. Historically the development was of course the other way round, starting with elliptic integrals and then elliptic function. Algebraic methods were only introduced much later. See the appendix of [Sha94b] for a short historical sketch.

Throughout this section Λ will always denote a *lattice* in $\mathbb{C}$, i.e. a discrete subgroup which contains an $\mathbb{R}$-basis of $\mathbb{C}$, or equivalently the image of the canonical lattice $\mathbb{Z}^2$ in $\mathbb{R}^2$ under an $\mathbb{R}$-linear map $\mathbb{R}^2 \to \mathbb{C}$ of rank 2. Further for $a \in \mathbb{C}$ let

$$\mathcal{P} = \mathcal{P}_a = \{a + t_1\omega_1 + t_2\omega_2 : 0 \leq t_1, t_2 < 1\}$$

be a *fundamental parallelogram* of Λ. Here and later ω_1, ω_2 are a basis of the lattice. Of course the canonical projection map $\mathbb{C} \to \mathbb{C}/\Lambda$ is bijective when restricted to $\mathcal{P}$.

Definition 3.1. An *elliptic function* with respect to a lattice Λ is a meromorphic function f such that for all $z \in \mathbb{C}$ and all $\omega \in \Lambda$,
$$f(z + \omega) = f(z).$$
The field of all elliptic functions is denoted $\mathbb{C}(\Lambda)$.

If f is elliptic and holomorphic it has to be bounded on the compact set $\overline{\mathcal{P}}$ (the closure of $\mathcal{P}$) and therefore on all of $\mathbb{C}$. Thus by Liouville's theorem [Con78, theorem IV.3.4] applied to f resp. $1/f$ we get:

Theorem 3.2. *An elliptic function with no poles or no zeros is constant.*

Note that this result is not very surprising. It is just the analytic analogue to the already known fact that a rational function without zeros or poles is constant. The next theorem again has an algebraic analogue, compare theorems 1.41 and 2.16.

Theorem 3.3. *Let $f \in \mathbb{C}(\Lambda)$. Then*

1. $\displaystyle\sum_{w \in \mathcal{P}} \operatorname{res}_w(f) = 0$
2. $\displaystyle\sum_{w \in \mathcal{P}} \operatorname{ord}_w(f) = 0$
3. $\displaystyle\sum_{w \in \mathcal{P}} \operatorname{ord}_w(f)w \in \Lambda$

Proof. The statements are all simple consequences from integrating around $\partial \mathcal{P}$ and using the residue theorem [Con78, theorem V.2.2]. A complete proof can for example be found in [Sil92, theorem VI.2.2]. $\square$

Corollary 3.4. *The number of poles of an elliptic function is equal to the number of zeros (counted with multiplicity). Any non-constant elliptic function has at least two poles (again counted with multiplicity).*

Proof. The first statement is just a reformulation of the second point in the last theorem. If f had just a single simple pole, the residue at that pole had to be 0 and f therefore holomorphic. $\square$

For $w \in \mathbb{C}/\Lambda$ and $f \in \mathbb{C}(\Lambda)$ define the *order* $\operatorname{ord}_w(f)$ of f at w by $\operatorname{ord}_z(f)$ for any $z \in \mathbb{C}$ that maps to w under the canonical projection. Like in the algebraic case the following definitions will prove to be useful:

Definition 3.5. The *divisor group* $\operatorname{Div}(\mathbb{C}/\Lambda)$ is the free Abelian group over $\mathbb{C}/\Lambda$. Its elements are written as formal linear combinations $D = \sum_{w \in \mathbb{C}/\Lambda} n_w(w)$ with $n_w \in \mathbb{Z}$ and almost all n_w vanish. Define the *degree* of a divisor D by $\deg D = \sum n_w$ and let

$$\operatorname{Div}^0(\mathbb{C}/\Lambda) = \{ D \in \operatorname{Div}(\mathbb{C}/\Lambda) : \deg D = 0 \}.$$

From any function $f \in \mathbb{C}(\Lambda)^*$ we get a *principal divisor* $\operatorname{div}(f) \in \operatorname{Div}^0(\mathbb{C}/\Lambda)$ by

$$\operatorname{div}(f) = \sum_{w \in \mathbb{C}/\Lambda} \operatorname{ord}_w(f)w.$$

Further we define a *summation map*

$$\operatorname{sum}\colon \begin{cases} \operatorname{Div}^0(\mathbb{C}/\Lambda) \to \mathbb{C}/\Lambda \\ \sum n_w(w) \mapsto \sum n_w w \end{cases}.$$

We will later show that the sequence

$$1 \to \mathbb{C}^* \to \mathbb{C}(\Lambda)^* \overset{\operatorname{div}}{\to} \operatorname{Div}^0(\mathbb{C}/\Lambda) \overset{\operatorname{sum}}{\to} \mathbb{C}/\Lambda \to 0$$

is exact. (The interesting part is the exactness at $\operatorname{Div}^0(\mathbb{C}/\Lambda)$.)

It would be convenient to have a good characterization of the field of elliptic functions and indeed we will prove that $\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp')$ where $\wp$ is the Weierstraß $\wp$-function that we will shortly define.

Notation. We will use the notation

$$\sideset{}{'}\sum_{\omega \in \Lambda} f(\omega) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} f(\omega).$$

Lemma 3.6. *The series*

$$G_{2k} = G_{2k}(\Lambda) = \sideset{}{'}\sum_{\omega \in \Lambda} \frac{1}{\omega^{2k}}$$

converges absolutely for all $k > 1$.

The G_{2k} are called *Eisenstein series of weight* $2k$. For odd numbers the Eisenstein series G_{2k+1} are 0.

Proof. See for example [Sil92, theorem VI.3.1a] or [Hus04, lemma 9.3.1]. $\square$

Now we would like to construct an elliptic function $\wp$ that has only the single pole 0 $(\mathrm{mod}\ \Lambda)$. Of course, by corollary 3.4 this pole must be of order 2 and have residue 0. We could try to set $\wp(z) = \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^2}$ but unfortunately this does not converge. Therefore we have to make it convergent.

Definition 3.7. Let $\Lambda \subset \mathbb{C}$ be a lattice. The *Weierstraß $\wp$-function* for Λ is defined by the series

$$\wp(z) = \wp(z; \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda}' \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Theorem 3.8. *The series in the last definition converges absolutely and uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$. Thus it defines a meromorphic function $\wp$ on $\mathbb{C}$. This function has a double pole with residue 0 at each lattice point an no other poles. It is an even elliptic function.*

Proof. Let C be a compact subset of $\mathbb{C} \setminus \Lambda$ and r such that $\forall z \in C : |z| \leq r$. For $|\omega| \geq 2r$ and $z \in C$ we have

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{z(z-2\omega)}{\omega^2(z-\omega)^2} \right| \leq \frac{r(r+2|\omega|)}{|\omega|^2 \frac{|\omega|^2}{4}} \leq 4\frac{r(\frac{|\omega|}{2}+2|\omega|)}{|\omega|^4} = \frac{10r}{|\omega|^3}.$$

Thus for $z \in C$ there exists a constant $c \in \mathbb{R}$ such that:

$$\left| \frac{1}{z^2} + \sum_{\omega \in \Lambda}' \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) \right| \leq c + \sum_{\substack{\omega \in \Lambda \\ |\omega| > 2r}} \left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| \leq c + \sum_{\substack{\omega \in \Lambda \\ |\omega| > 2r}} \frac{10r}{|\omega|^3} \leq c + 10r \sum_{\omega \in \Lambda}' \frac{1}{|\omega|^3} < \infty.$$

Therefore $\wp$ is holomorphic in $\mathbb{C} \setminus \Lambda$ and from the series it is evident that it has a double pole at every lattice point and that $\wp(z) = \wp(-z)$. Because of the uniform convergence we can compute

$$\wp'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}.$$

Clearly $\wp'$ is an elliptic function, so integrating yields

$$\wp(z+\omega) = \wp(z) + c(\omega)$$

where $c(\omega) \in \mathbb{C}$ is independent of z. Now setting $z = -\frac{\omega}{2}$ and the evenness of $\wp$ implies $c(\omega) = 0$. $\qquad\square$

We can now prove what we had set out to do, namely the following theorem:

Theorem 3.9. *Every elliptic function can be written as a rational function in $\wp$ and $\wp'$:*

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp(\,\cdot\,; \Lambda), \wp'(\,\cdot\,; \Lambda)).$$

Proof. Let $f \in \mathbb{C}(\Lambda)$. Then by

$$f(z) = \frac{f(z) + f(-z)}{2} + \frac{f(z) - f(-z)}{2}$$

it can be decomposed into the sum of an even and an odd elliptic function. Since $\wp'$ times an odd function is even, it suffices to show that every even elliptic function is in $\mathbb{C}(\wp)$. So assume that f is even.

For $w \in \mathbb{C}$ the evenness of f implies $\mathrm{ord}_w(f) = \mathrm{ord}_{-w}(f)$. Differentiate $f(z) = f(-z)$ to get $f^{(i)}(z) = (-1)^i f^{(i)}(-z)$. If $w = -w \mod \Lambda$ (i.e. $2w \in \Lambda$) then $f^{(i)}(w) = -f^{(i)}(w)$ and thus $f^{(i)}(w) = 0$ for all odd i and so $\mathrm{ord}_w(f)$ must be even (if f has a pole at w then the argument has to be applied to $1/f$).

In particular $\mathrm{ord}_0(f) = 2m$ for some integer m. Let $f(z) = \wp(z)^{-m} g(z)$ where $g(z)$ is an even elliptic function with $\mathrm{ord}_0(g) = 0$, i.e. g has no zeros or poles on Λ. By the last paragraph there exist $n \in \mathbb{N}$ and $a_i, b_i \in \mathcal{P}$ such that $a_1, \ldots, a_n, -a_1, \ldots, -a_n$ are exactly the zeros and $b_1, \ldots, b_n, -b_1, \ldots, -b_n$ are exactly the poles of $g \mod \Lambda$ (listed with multiplicities). Thus

$$h(z) = g(z) \frac{\prod_{i=1}^{n}(\wp(z) - \wp(b_i))}{\prod_{i=1}^{n}(\wp(z) - \wp(a_i))}$$

is an elliptic function without zeros or poles (the divisor of $\wp(z) - \wp(w)$ is $(w) + (-w) - 2(0)$). By theorem 3.2, h is constant. $\qquad\square$

Since $\mathbb{C}/\Lambda$ is a complex manifold of dimension 1, its function field $\mathbb{C}(\Lambda)$ should – analogous to the algebraic case – have transcendence degree 1 over $\mathbb{C}$. It can be proven without using the theorem above that any two elliptic functions are algebraically dependent [Cha85, theorem III.9]. We will however just prove that there exists a relation between $\wp$ and $\wp'$.

Theorem 3.10 (Differential equation for $\wp$)**.** *There exist complex numbers g_2 and g_3 (depending on Λ) such that*

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3.$$

Proof. Since $\wp$ is an even function, its Laurent expansion is of the form

$$\wp(z) = \frac{1}{z^2} + c_0 + c_2 z^2 + c_4 z^4 + O(z^6)$$

with $c_0 = 0$ because $(\wp(z) - \frac{1}{z^2})(0) = 0$. This yields

$$\wp'(z) = \frac{-2}{z^3} + 2c_2 + 4c_4 z^3 + O(z^5)$$

$$\wp(z)^3 = \frac{1}{z^6} + \frac{3c_2}{z^2} + 3c_4 + O(z)$$

$$\wp'(z)^2 = \frac{4}{z^6} - \frac{8c_2}{z^2} - 16c_4 + O(z)$$

Therefore (using the again that an elliptic and holomorphic function is constant):

$$\wp'(z)^2 - 4\wp(z)^3 + 20c_2\wp(z) = -28c_4 + O(z) = -28c_4.$$

Set $g_2 = 20c_2$ and $g_3 = 28c_4$. $\square$

It is not difficult to explicitly calculate the Laurent series of $\wp$ in terms of Eisenstein series (see [Sil92, theorem VI.3.5]):

$$\wp(z) = z^{-2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}z^{2k}.$$

This implies $g_2(\Lambda) = 60G_2(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$.

To proceed we need some way of constructing elliptic functions with given zeros and poles. For this it would be convenient to have an elliptic function with just single zeros at the lattice points and no zeros or poles elsewhere. Of course by corollary 3.4 this is impossible. We can however construct a "pseudo-periodic" function with this property. To see the connections between the various functions we also need to introduce a function with single poles at the lattice points.

Definition 3.11. The Weierstraß ζ-function for a lattice Λ is defined by the following infinite product:

$$\zeta(z) = \frac{1}{z} - \sum_{\omega\in\Lambda}{}' \left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right).$$

The Weierstrass σ-function is defined by

$$\sigma(z) = z\prod_{\omega\in\Lambda}{}' \left(1 - \frac{z}{\omega}\right)\exp\left(\frac{z}{\omega} + \frac{1}{2}\left(\frac{z}{\omega}\right)^2\right).$$

Theorem 3.12.

1. *The ζ-function is a well-defined meromorphic function with single poles at the lattice points and no poles elsewhere.*
2. *The σ-function is a well-defined odd entire function with single zeros at the lattice points an no zeros elsewhere.*
3. *$\zeta'(z) = -\wp(z)$ and $\frac{\mathrm{d}}{\mathrm{d}z}\log\sigma(z) = \frac{\sigma'(z)}{\sigma(z)} = \zeta(z)$.*
4. *There exists a group homomorphism $\eta\colon \Lambda \to \mathbb{C}$ such that $\zeta(z+\omega) = \zeta(z) + \eta(\omega)$ for all $z \in \mathbb{C}$ and $\omega \in \Lambda$.*
5. *(Legendre relation) If (ω_1, ω_2) is a basis of Λ with $\mathfrak{Im}\frac{\omega_2}{\omega_1} > 0$ then $\eta(\omega_1)\omega_2 - \eta(\omega_2)\omega_1 = 2\pi i$.*

6. *For all $\omega \in \Lambda$ and $z \in \mathbb{C}$*

$$\sigma(z + \omega) = \lambda(\omega)e^{\eta(\omega)(z+\frac{\omega}{2})}\sigma(z) \tag{3.1}$$

where

$$\lambda(\omega) = \begin{cases} 1 & \text{if } \omega \in 2\Lambda \\ -1 & \text{if } \omega \notin 2\Lambda \end{cases}.$$

Proof.

1. The (absolute!) convergence can be proven just like for the $\wp$-function [Sil94, proposition I.5.1].
2. The product converges by the Weierstraß factorization theorem [Con78, theorem VII.5.12].
3. These are simple calculations (because of the derivation, the branch of log is irrelevant).
4. Since $\frac{\mathrm{d}}{\mathrm{d}z}(\zeta(z+\omega) - \zeta(z)) = -\wp(z+\omega) + \wp(z) = 0$ we can define $\eta(\omega) = \zeta(z+\omega) - \zeta(z)$ independent of z. Now for all $z \in \mathbb{C}$:

$$\eta(\omega_1 + \omega_2) + \zeta(z) = \zeta(z + \omega_1 + \omega_2) = \zeta(z + \omega_1) + \eta(\omega_2) = \zeta(z) + \eta(\omega_1) + \eta(\omega_2).$$

5. Integrate ζ around a fundamental parallelogram of Λ with 0 in its interior and use Cauchy's residue theorem. ([Cha85, theorem IV.2] with $\eta_i = \frac{\eta(\omega_i)}{2}$.)
6. Let $F(z)$ be an antiderivative of $\zeta(z)$. Then

$$\frac{\mathrm{d}}{\mathrm{d}z}(F(z+\omega) - F(z)) = \zeta(z+\omega) - \zeta(z) = \eta(\omega).$$

Hence there exists $h\colon \Lambda \to \mathbb{C}$ such that

$$F(z + \omega) - F(z) = \eta(\omega)z + h(\omega).$$

By (3) this gives

$$\frac{\sigma(z+\omega)}{\sigma(z)} = e^{\eta(\omega)z + h(\omega)}.$$

Define $\lambda(\omega) = \exp(h(\omega) - \eta(\omega)\frac{\omega}{2})$ to get the desired relation. Now we need to show that λ is the function given in the theorem. Let $\omega \notin 2\Lambda$ and $z = -\frac{\omega}{2} \notin \Lambda$.

$$0 \neq \sigma(\frac{\omega}{2}) = \sigma(z+\omega) = \sigma(-\frac{\omega}{2}) \cdot 1 \cdot \lambda(\omega) = -\sigma(\frac{\omega}{2})\lambda(\omega)$$

and thus $\lambda(\omega) = -1$. Let $\omega = 2\omega'$ and z arbitrary:

$$\frac{\sigma(z + 2\omega')}{\sigma(z)} = \frac{\sigma(z + 2\omega')}{\sigma(z + \omega')} \cdot \frac{\sigma(z + \omega')}{\sigma(z)},$$

$$e^{2\eta(\omega')(z+\omega')}\lambda(2\omega') = e^{\eta(\omega')(z+\omega'+\frac{\omega'}{2})}\lambda(\omega') \cdot e^{\eta(\omega')(z+\frac{\omega'}{2})}\lambda(\omega').$$

Therefore $\lambda(\omega) = \lambda(2\omega') = \lambda(\omega')^2$ and induction yields the statement. $\qquad\square$

Theorem 3.13. *Let $f \in \mathbb{C}(\Lambda)$ with divisor*

$$\mathrm{div}(f) = \sum n_i(z_i)$$

Replace z_1 by $z_1 - \omega$ where $\omega = \sum n_i z_i \in \Lambda$. Then there exists a constant $c \in \mathbb{C}$ such that

$$f(z) = c \prod \sigma(z - z_i)^{n_i}.$$

Proof. Let $h(z) = \prod \sigma(z - z_i)^{n_i}$. Using the last theorem one shows that $h(z + \omega) = h(z)$ for all $\omega \in \Lambda$, i.e. $h \in \mathbb{C}(\Lambda)$. Then $\mathrm{div}(\frac{f}{h}) = 0$ and therefore $c = \frac{f}{h}$ is constant. $\qquad\square$

We can now prove the converse of theorem 3.3, i.e. the analytic analogue of theorem 2.16.

Theorem 3.14. *Let $n_1, \ldots, n_r \in \mathbb{Z}$ and $z_1, \ldots, z_n \in \Lambda$ with*

$$\sum n_i = 0 \qquad \text{and} \qquad \sum n_i z_i \in \Lambda.$$

Then there exists $f \in \mathbb{C}(\Lambda)$ satisfying

$$\text{div}(f) = \sum n_i(z_i).$$

Proof. Use the representation in theorem 3.13 to construct f. $\qquad\qquad\qquad\qquad\qquad\qquad\square$

Corollary 3.15. *The sequence*

$$1 \to \mathbb{C}^* \to \mathbb{C}(\Lambda)^* \overset{\text{div}}{\to} \text{Div}^0(\mathbb{C}/\Lambda) \overset{\text{sum}}{\to} \mathbb{C}/\Lambda \to 0$$

is exact.

Proof. Exactness at $\mathbb{C}^*$ is trivial. Exactness at $\mathbb{C}(\Lambda)^*$ is theorem 3.2. Exactness at $\text{Div}^0(\mathbb{C}/\Lambda)$ is theorem 3.14 and exactness as $\mathbb{C}/\Lambda$ is again trivial. $\qquad\qquad\qquad\qquad\qquad\qquad\square$

The differential equation 3.10 looks remarkably like a Weierstraß equation. In fact the following important connection between elliptic functions and elliptic curves over $\mathbb{C}$ holds:

Theorem 3.16. *Let Λ be a lattice in $\mathbb{C}$ and $\wp(z) = \wp(z; \Lambda)$, $g_2 = g_2(\Lambda)$, $g_3 = g_3(\Lambda)$.*

1. *The plane complex curve $E/\mathbb{C}$ defined by*

$$y^2 = 4x^3 - g_2 x - g_3$$

   is an elliptic curve (i.e. it is non-singular).

2. *The function*

$$\phi \colon \mathbb{C}/\Lambda \to E \subseteq \mathbb{P}^2(\mathbb{C})$$

$$z \bmod \Lambda \mapsto \begin{cases} [0 : 1 : 0] & z = 0 \bmod \Lambda \\ [\wp(z) : \wp'(z) : 1] & z \neq 0 \bmod \Lambda \end{cases}$$

   is an analytic isomorphism of complex Lie groups (i.e. an isomorphism of Riemann surfaces that is also a group homomorphism).

3. *Let $E'/\mathbb{C}$ be an elliptic curve defined by a Weierstraß equation*

$$E' \colon y^2 = 4x^3 - ax - b.$$

   (By some change of coordinates every complex elliptic curve can be brought into this form.) Then there exists a lattice Λ' such that $g_2(\Lambda') = a$ and $g_3(\Lambda') = b$, i.e. such that the map ϕ is an isomorphism of $\mathbb{C}/\Lambda'$ to $E'(\mathbb{C})$.

4. *Two elliptic curves are isomorphic over $\mathbb{C}$ if and only if their associated lattices are homothetic (i.e. $\exists \alpha \colon \alpha\Lambda = \Lambda'$).*

Proof.

1. This equivalent to $f(x) = 4x^3 - g_2 x - g_3$ having no double roots. See [Sil92, proposition VI.3.6a] for a proof of this.
2. See [Sil92, proposition VI.3.6b] or [Hus04, theorem 9.4.4].
3. See [Hus04, section 9.6] and [Sil92, section VI.5].
4. See [Sil94, corollary I.4.3]. $\qquad\qquad\qquad\qquad\qquad\qquad\square$

Now we can transfer the addition formulas of 2.15 to the $\wp$-function.

Theorem 3.17 (Analytic Addition Theorem)**.** *Let $z \neq u \bmod \Lambda$. Then*

$$\wp(z + u) = -\wp(z) - \wp(u) + \frac{1}{4}\left(\frac{\wp'(z) - \wp'(u)}{\wp(z) - \wp(u)}\right)^2$$

$$\wp'(z + u) = -\wp'(z) + \left(\frac{\wp'(z) - \wp'(u)}{\wp(z) - \wp(u)}\right)(\wp(z) - \wp(z + u))$$

$$\wp(2z) = -2\wp(z) + \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2 = -2\wp(z) + \frac{1}{4}\left(\frac{6\wp(z)^2 - \frac{g_2}{2}}{\wp'(z)}\right)^2$$

$$\wp'(2z) = -\wp'(z) + \left(\frac{\wp''(z)}{\wp'(z)}\right)(\wp(z) - \wp(2z)) = -\wp'(z) + \left(\frac{6\wp(z)^2 - \frac{g_2}{2}}{\wp'(z)}\right)(\wp(z) - \wp(2z)).$$

Proof. The addition formulas can be obtained like the group law formulas for plane cubics using the slightly different equation $y^2 = 4x^3 - g_2 x - g_3$. The duplication formulas are the result of taking the limit $u \to z$ and using the differential equation for $\wp$ to obtain $\wp''(z) = 6\wp(z)^2 - \frac{g_2}{2}$. $\qquad\square$

There is of course a lot more to say about elliptic functions, but we have to stop here and will finish with a small proposition that we will need later on.

Proposition 3.18.

$$\wp(z) - \wp(u) = -\frac{\sigma(z+u)\sigma(z-u)}{\sigma(z)^2\sigma(u)^2}$$

Proof. By theorem 3.13 (considering $\wp(z) - \wp(u)$ as a function in z and u respectively) there exist $c_1(u)$ and $c_2(z)$ such that

$$\wp(z) - \wp(u) = c_1(u)\frac{\sigma(z+u)\sigma(z-u)}{\sigma(z)^2} = c_2(z)\frac{\sigma(u+z)\sigma(u-z)}{\sigma(u)^2}.$$

Since $\sigma(z-u) = -\sigma(u-z)$ this gives $c_1(u) = \frac{-c_2(z)\sigma(z)^2}{\sigma(u)^2}$ independent of z and hence there exists a constant c such that

$$\wp(z) - \wp(u) = -c\frac{\sigma(z+u)\sigma(z-u)}{\sigma(z)^2\sigma(u)^2}.$$

Multiplying with z^2 and letting $z \to 0$ we deduce that $c = 1$ $\qquad\square$

This formula can be used to deduce the addition theorem for $\wp$ without using elliptic curves at all [Wei93, Art. 12].

For more information about the theory of elliptic functions see for example [Lan87]. Of historical interest is Schwarz's transcription of Weierstraß' lectures [Wei93]. See also [Cha85] which contains many references.

3.2   Two Families of Polynomials

3.2.1   Elliptic Divisibility Sequences and the Division Polynomials

Elliptic divisibility sequences (EDS) were first introduced and studied by Morgan Ward in [War48]. Recently the study of these sequences resurfaced because of their connection to elliptic division polynomials and therefore to the group structure of elliptic curves. Shipsey [Shi00] was the first to realize the possibility to transform the discrete logarithm problem to a problem on elliptic divisibility sequences (more on that in section 7.6).

Definition 3.19. A sequence $u\colon \mathbb{Z} \to R$ where R is an integral domain is called a *divisibility sequence* if $u_n \mid u_m$ for all $n \mid m$. If $R = \mathbb{Z}$ the sequence is called *integral*.

Some trivial examples of divisibility sequences are $u_n = n^k$ and $u_n = a_1^n - a_2^n$.

Definition 3.20. A sequence u_n is *elliptic* if it satisfies

$$u_{m+n}u_{m-n} = u_{m+1}u_{m-1}u_n^2 - u_{n+1}u_{n-1}u_m^2. \tag{3.2}$$

for all $m, n \in \mathbb{Z}$. If it is also a divisibility sequence, it is called *elliptic divisibility sequence*, often shortened to *EDS*.

A simple calculation shows that all sequences of the form $\frac{a^n - b^n}{a - b}$ with $ab = 1$ and $a + b \in \mathbb{Z}$ are integral EDS. For example let a be a primitive complex third root of unity and $b = \bar{a}$ to obtain the sequence $0, 1, -1, 0, 1, -1, \dots$. Note that for $a = b = 1$ this includes the sequence $u_n = n$.

Following Ward, we will call a solution of (3.2) *proper* if $u_0 = 0$, $u_1 = 1$ and not both u_2 and u_3 are zero.

We collect some elementary properties of elliptic sequences in the following lemma:

Lemma 3.21. *Let u_n be a proper elliptic sequence. Then $u_k = -u_{-k}$ for a all $k \in \mathbb{Z}$. The set $\{n : u_n = 0\}$ is a subgroup of $\mathbb{Z}$.*

Proof. Setting $n = 0$, $m = 1$ yields $u_{-1} = -1$. If $u_k = u_{-k} = 0$ then the first claim is trivial. Assume $u_k \neq 0$ and let $m = 0$, $n = -k$ to get $u_k u_{-k} = -u_k^2$ and thus $u_{-k} = -u_k$. If $u_{-k} \neq 0$ replace k by $-k$.

By lemma 4.1 in [War48], if any two consecutive terms of the sequence vanish, then $u_n = 0$ for $n \geq 4$. In this case let $m = 3$, $n = 2$: $0 = 0 - u_1 u_3^3$ and thus $u_3 = 0$. Then let $m = 2$, $n = 0$ to get $u_2^2 = 0$ and so the sequence cannot be proper.

Assume that $u_k = 0$ and $u_l = 0$. Then by the last paragraph $u_{k-1} u_{k+1} \neq 0$. Let $m = k + l$, $n = k$:

$$u_{2k+l} u_l = u_{k+l+1} u_{k+l-1} u_l^2 - u_{k+1} u_{l+1} u_{k+l}^2$$

and hence $u_{k+l} = 0$. $\square$

Definition 3.22. *Let u_n be a proper elliptic sequence. Then the smallest positive integer k such that $u_k = 0$ is called the* rank of zero-apparition *of the sequence.*

For proper sequences the following theorem gives a base set:

Theorem 3.23. *Let u_n be a proper solution of (3.2) with values in the quotient field of R. Then u_n is completely determined by u_2, u_3 and u_4. Further if these values are in R and $u_2 | u_4$, then the sequence is an EDS in R.*

Proof. This is a slight generalization of [War48, theorem 4.1]. $\square$

Theorem 3.24. *Let $\Lambda \subseteq \mathbb{C}$ be a lattice. Define functions $\psi_n(\,\cdot\,; \Lambda)$ on $\mathbb{C}$ by*

$$\psi_n(z; \Lambda) = \frac{\sigma(nz; \Lambda)}{\sigma(z; \Lambda)^{n^2}}.$$

Then for every $z \in \mathbb{C}$ the sequence $n \mapsto \psi_n(z; \Lambda)$ is an elliptic divisibility sequence.

Proof. Because $\mathbb{C}$ is a field and by lemma 3.21 we only need to prove that the sequence is elliptic.

For easier notation we will only write ψ_n for $\psi_n(z; \Lambda)$. By proposition 3.18,

$$\begin{aligned}
\wp(mz) - \wp(nz) &= -\frac{\sigma((m+n)z)\sigma((m-n)z)}{\sigma(nz)^2 \sigma(mz)^2} \\
&= -\frac{\psi_{m+n} \sigma(z)^{(m+n)^2} \psi_{m-n} \sigma(z)^{(m-n)^2}}{\psi_n^2 \sigma(z)^{2n^2} \psi_m^2 \sigma(z)^{2m^2}} \\
&= -\frac{\psi_{m+n} \psi_{m-n}}{\psi_m^2 \psi_n^2}.
\end{aligned} \tag{3.3}$$

Also $\psi_1 = 1$. Dividing (3.2) by $u_m^2 u_n^2$ and using the above formula yields the statement. $\square$

From (3.3) we get a nice multiplication-by-n formula:

$$\wp(nz) = \wp(z) - \frac{\psi_{n-1}(z)\psi_{n+1}(z)}{\psi(z)^2}. \tag{3.4}$$

This is the first hint that elliptic divisibility sequences are connected to the discrete logarithm on elliptic curves. We also see that in order to calculate $\wp(nz)$ we need the *three* values $\psi_{n-1}(z)$, $\psi_n(z)$ and $\psi_{n-1}(z)$. Basically this is already the width 3 EDS discrete logarithm problem considered in section 7.6.1.

The functions ψ_n have many interesting properties. First of all, using the transformation formula (3.1),

$$\psi_n(z + \omega) = \frac{\sigma(nz + n\omega)}{\sigma(z + \omega)^{n^2}} = \frac{\sigma(nz)\lambda(n\omega)e^{n\eta(\omega)n(z + \frac{\omega}{2})}}{\left(\sigma(z)\lambda(\omega)e^{\eta(\omega)(z + \frac{\omega}{2})}\right)^{n^2}} = \frac{\sigma(nz)\lambda(\omega)^n e^{n^2 \eta(\omega)(z + \frac{\omega}{2})}}{\sigma(z)^{n^2} \lambda(\omega)^{n^2} e^{n^2 \eta(\omega)(z + \frac{\omega}{2})}} = \frac{\sigma(nz)}{\sigma(z)^{n^2}} = \psi_n(z)$$

for all ω in Λ. Hence ψ_n is an elliptic function. Now by theorem 3.9 we know that ψ_n is a rational function in $\wp$ and $\wp'$. Actually it is possible to explicitly compute the representation [Kie73, Wei93]:

$$\psi_n(z) = \frac{(-1)^{n-1}}{(1!\,2!\,3!\cdots(n-1)!)^2} \det\left(\wp^{(i+j-1)}(z)\right)_{i,j=1}^{n-1}. \tag{3.5}$$

Using the differential equation 3.10 to get $\wp''(z) = 6\wp(z)^2 - \frac{g_2}{2}$ we see that the functions ψ_n are actually polynomials in $\wp$ and $\wp'$. For the first few n expression (3.5) yields:

$$\psi_1(z) = 1, \qquad \psi_2(z) = -\wp'(z),$$

$$\psi_3(z) = 3\wp^4(z) - \frac{3}{2}g_2\wp^2(z) - 3g_3\wp(z) - \frac{g_2^2}{16}.$$

Similarly one can expand ψ_4 as a polynomial of degree 7 in $\wp(z)$ and degree 1 in $\wp'(z)$. If one chooses g_2, g_3 and z such that these values are integral one obtains an integral EDS. Ward proved that every integral EDS arises in this way [War48, theorem 12.1].

Of course we want to work over finite fields. Here we have to modify the approach to the definition of the ψ_n. We have to work the other way round and define the ψ_n as polynomials in x, y just so that we get an EDS and an analogous relation to (3.4). However, before we define these polynomials we need to show that what we want to do actually makes any sense.

Theorem 3.25. *Let E/K be an elliptic curve given by*

$$f(x,y) = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6.$$

Then there exist rational functions $g_n, h_n \in \operatorname{Quot}\left(\mathbb{Z}[a_1, a_2, a_3, a_4, a_6][x,y]/\langle f(x,y)\rangle\right) \subseteq K(E)$ with poles exactly at the points in $E[n]$ and such that for all $n \in \mathbb{Z}$ and every point $P \in E(\bar{K}) \setminus E[n]$:

$$[n]P = (g_n(P),\, h_n(P)).$$

Proof. This follows by induction from the formulas in theorem 2.15. $\qquad\square$

Definition 3.26. Let $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6)$ be a field extension of $\mathbb{Q}$ with transcendence degree 5 and let

$$f(x,y) = y^2 + \alpha_1 xy + \alpha_3 y - x^3 - \alpha_2 x^2 - \alpha_4 x - \alpha_6.$$

Further let

$$\begin{aligned}
\beta_2 &= \alpha_1^2 + 4\alpha_2, \\
\beta_4 &= 2\alpha_4 + \alpha_1\alpha_3, \\
\beta_6 &= \alpha_3^2 + 4\alpha_6, \\
\beta_8 &= \alpha_1^2\alpha_6 + 4\alpha_2\alpha_6 - \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3^2 - \alpha_4^2.
\end{aligned}$$

Define the *abstract division polynomials* $\Psi_n \in \mathbb{Z}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6][x,y]/\langle f(x,y)\rangle$ by

$$\Psi_1 = 1, \qquad \Psi_2 = 2y + \alpha_1 x + \alpha_3,$$

$$\Psi_3 = 3x^4 + \beta_2 x^3 + 3\beta_4 x^2 + 3\beta_6 x + \beta_8,$$

$$\Psi_4 = \Psi_2(x,y) \cdot (2x^6 + \beta_2 x^5 + 5\beta_4 x^4 + 10\beta_6 x^3 + 10\beta_8 x^3 + (\beta_2\beta_8 - \beta_4\beta_6)x + \beta_4\beta_8 - \beta_6^2)$$

and such that for all $m, n \in \mathbb{Z}$:

$$\Psi_{m+n}\Psi_{m-n} = \Psi_{m+1}\Psi_{m-1}\Psi_n^2 - \Psi_{n+1}\Psi_{n-1}\Psi_m^2.$$

(This is well defined by theorem 3.23.)

Let $\mathcal{R} = \mathbb{Z}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6][x,y]/\langle f(x,y)\rangle$. Further let E/K be an elliptic curve defined by

$$f_E(x,y) = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6$$

and define a homomorphism $\phi_E \colon \mathcal{R} \to K(E)$ by $\alpha_i \mapsto a_i$.

Theorem 3.27. *The functions $\psi_n = \phi_E(\Psi_n) \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][x, y]/\langle f_E(x, y)\rangle \subseteq K(E)$ have the following properties:*

1. *They form an EDS with $\psi_1 = 1$.*

2. *For $P \in E(K)$ and $n \in \mathbb{Z}$ with $[n]P \neq \mathcal{O}$:*

$$[n]P = \left(\frac{x\psi_n^2 - \psi_{n+1}\psi_{n-1}}{\psi_n^2}, \frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{4y\psi_n^3} \right)(P).$$

3. *For $P \in E(K)$ and $n \in \mathbb{Z}$: $[n]P = \mathcal{O}$ if and only if $\psi_n(P) = 0$.*

The functions ψ_n are called division polynomials *of E.*

The following proof is inspired by the one in [CR88]. For the sake of better readability we will split it into three parts.

Proof of theorem 3.27, part 1. The first statement is of trivial since homomorphisms transfer algebraic relations. $\qquad\square$

Proof of theorem 3.27, part 2. First we will show that the statement is true for the elliptic curve C/L defined by $f(x, y)$. There exists an isomorphism of L to as subfield L' of $\mathbb{C}$. Therefore we can view C as an elliptic curve defined over $\mathbb{C}$. (This is an application of the Lefschetz principle [Sil92, section VI.6].) Now one can check that the division polynomials defined here evaluated at $(\wp(z), \wp'(z))$ are just the elliptic functions $\frac{\sigma(nz)}{\sigma(z)^{n^2}}$ studied earlier. Thus this case of the theorem follows from classical results about elliptic functions; see [Lan78] for details. (It is actually possible to prove it in a purely algebraic way. See [CR88].)

For an arbitrary elliptic curve E/K we will prove the theorem by induction on n. More precisely, we will use induction on the following statement:

(i) ψ_{n+1} is not identically zero,
(ii) $x([n](x, y)) = g_n = x - \frac{\psi_{n+1}\psi_{n-1}}{\psi_n^2}$ and
(iii) $y([n](x, y)) = h_n = \frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{4y\psi_n^3}$.

The statements can easily be checked for $n \leq 4$. Assume they hold for all $n < m$. From the addition formulas 2.15 we know that

$$g_m = \left(\frac{h_{m-1} - y}{g_{m-1} - x} \right)^2 + \alpha_1 \frac{h_{m-1} - y}{g_{m-1} - x} - \alpha_2 - g_{m-1} - x$$

holds on the curve C of the first paragraph. Here we already know that we can replace g_m, g_{m-1} and h_{m-1} with the rational functions in the Ψs as given in (ii) and (iii). Multiplying this resulting relation by $(\Psi_{m-2}\Psi_{m-1}\Psi_m)^2$ we get a polynomial relation in $\mathcal{R}$ which we can transfer by ϕ_E to a relation of the ψs. By induction we know that $(\psi_{m-2}\psi_{m-1}\psi_m)^2 \neq 0$, so we can divide by that term and again using the induction hypothesis we can resubstitute g_{m-1} and h_{m-1} to get

$$x - \frac{\psi_{m+1}\psi_{m-1}}{\psi_m^2} = \left(\frac{h_{m-1} - y}{g_{m-1} - x} \right)^2 + a_1 \frac{h_{m-1} - y}{g_{m-1} - x} - a_2 - g_{m-1} - x.$$

The right hand side is equal to g_m and thus we have proved (ii) for $n = m$. Similarly we can prove (iii).

If $\psi_{n+1} = 0$, then $g_n - x = 0$. But then $[n]P = \pm P$ or equivalently $[n \mp 1]P = \mathcal{O}$ for all $P \in E(\bar{K})$ and thus either $E[n-1]$ or $E[n+1]$ must be infinite, which is not possible (theorem 2.38). Therefore $\psi_{n+1} \neq 0$, finishing the induction step. $\qquad\square$

Before we continue with the proof we note that it is possible to state a more symmetric version of (ii) in analogy to (3.3).

Corollary 3.28.

$$g_m - g_n = -\frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2}$$

Proof. Using (ii) from the last proof and the recurrence relation for EDS:

$$g_m - g_n = x - \frac{\psi_{m+1}\psi_{m-1}}{\psi_m^2} - \left(x - \frac{\psi_{n+1}\psi_{n-1}}{\psi_n^2}\right) = -\frac{\psi_{m+1}\psi_{m-1}\psi_n^2 - \psi_{n+1}\psi_{n-1}\psi_m^2}{\psi_m^2\psi_n^2} = -\frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2}$$

$\square$

Proof of theorem 3.27, part 3. Again using the Lefschetz principle, we see that $\mathrm{div}(\Psi_n) = E[n] - n^2(\mathcal{O})$. We also know that $-\frac{\psi_{n+1}\psi_{n-1}}{\psi_n^2} = g_n - x$ has poles on $E[n]$ and thus ψ_n must have zeros on $E[n]$. We have to show that it has no other zeros. Let $p = \mathrm{char}(K)$.

First assume that $p = 0$ or n is prime to p. Induction shows that the pole order of Ψ_n at $\mathcal{O}$ is $n^2 - 1$ and if $\pi = \frac{x}{y}$ is a uniformizer at $\mathcal{O}$, then $(\pi^{n^2-1}\Psi)(\mathcal{O}) = n$. By the assumption, $\phi_E(n) \neq 0$ and thus ψ_n also has pole order $n^2 - 1$ at $\mathcal{O}$. There are no other poles and, since $\#E[n] = n^2$, there cannot be any additional zeros. Also from (ii) of the last part we see that the zeros must be simple ($g_n - x$ has poles of order two at the points in $E[n]$). Hence $\mathrm{div}(\psi_n) = E[n] - n^2(\mathcal{O})$.

Now assume that n is not prime to p. From the EDS recurrence relation we get

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n+1}^3\psi_{n-1}.$$

If ψ_n was not prime to ψ_{n+1}, then ψ_{2n+1} would have a triple zero which is not possible since $2n + 1$ is prime to p. Similarly ψ_n must be prime to ψ_{n-1}. Thus again from (ii) we see that ψ_n cannot have any zeros outside of $E[n]$. Of course they need not be simple as we do not know the pole order. $\square$

In light of the last theorem it is natural to define:

Definition 3.29. Let E/K be an elliptic curve defined by

$$f_E(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

and $P \in E(K)$. Then define the *elliptic divisibility sequence associated to E and P* by

$$W_{E,P} \colon \begin{cases} \mathbb{Z} \to K \\ n \mapsto \phi_E(\Psi_n)(P) \end{cases}.$$

From theorem 3.27 we immediately get the following corollary:

Corollary 3.30. *For an elliptic divisibility sequence $W \colon \mathbb{Z} \to K$ associated to an elliptic curve E and a point P on E we have $W(n) = 0$ if and only if $[n]P = \mathcal{O}$ on E.*

3.2.2 The Modular Polynomials

Let $\mathfrak{L}$ be the set of lattices in $\mathbb{C}$. In theorem 3.16 we saw that to two complex elliptic curves are isomorphic if and only if their associated lattices are homothetic. In other words there is a canonical bijection

$$\mathfrak{L}/\mathbb{C}^* \longleftrightarrow \{\text{isomorphism classes of complex elliptic curves}\}.$$

We can describe a lattice completely by its basis $(\omega_1, \omega_2) \in \mathbb{C}^2$ but this description is only unique up to a change of basis. Such a change can of course be described by an invertible 2×2 matrix with integer coefficients, i.e. by an element of $\mathrm{GL}_2(\mathbb{Z})$. On the other hand we can describe a lattice up to homothety by $\tau = \frac{\omega_2}{\omega_1}$. Since reordering a basis does not change the lattice, it is enough to consider $\tau \in \mathbf{H} = \{z \in \mathbb{C} : \mathfrak{Im}\, z > 0\}$ and $\mathrm{SL}_2(\mathbb{Z})$. This gives a surjection

$$\mathbf{H} \to \mathfrak{L}/\mathbb{C}^*,$$
$$\tau \mapsto \Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}.$$

The action of $\mathrm{SL}_2(\mathbb{Z})$ on the basis induces an action on $\mathbf{H}$ which is given by

$$\sigma\tau = \frac{a\tau + b}{c\tau + d}, \qquad \text{for } \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Thus Λ_{τ_1} is homothetic to Λ_{τ_2} if and only if there exists $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\sigma\tau_1 = \tau_2$. Hence there are natural bijections

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathbf{H} \longleftrightarrow \mathfrak{L}/\mathbb{C}^* \longleftrightarrow \{\text{isomorphism classes of complex elliptic curves}\}.$$

This is the fundamental incentive for the study of elliptic curves over $\mathbb{C}$ through the use of modular functions (see [Sil94] or [Kob93]). Note that since $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$ acts trivially on $\mathbf{H}$, one can use $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ instead of $\mathrm{SL}_2(\mathbb{Z})$. Both groups are often called the *modular group*.

All invariants of elliptic curves under isomorphism can now be lifted to functions on $\mathbf{H}$ that are invariant under the action of the modular group. For the *j-invariant* this gives

$$j(\tau) = j(\mathbb{C}/\Lambda_\tau) = 12^3 \frac{g_2(\tau)^3}{\Delta(\tau)},$$

where $g_i(\tau) = g_i(\Lambda_\tau)$ and $\Delta(\tau) = g_2(\tau)^3 - 27 g_3(\tau)^2$ is the *(modular) discriminant*. Obviously $j \circ \sigma = j$ for all $\sigma \in \mathrm{SL}_2(\mathbb{Z})$.

We want to construct monic polynomials $F_n(X, Y)$ such that $F_n(j(E), j(E')) = 0$ if an only if there exists an isogeny $E \to E'$ of degree n. In order to do this we extend the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbf{H}$ to an action of all matrices $\alpha \in M_2(\mathbb{R})$ with $\det \alpha > 0$. Further we define

$$\mathcal{S}_n = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\mathbb{Z}) : ad = n,\, 0 \le b < d \right\},$$

$$\mathcal{S}_n^* = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathcal{S}_n : \gcd(a, b, d) = 1 \right\}.$$

By [Sil94, lemma I.9.3], there exists an isogeny of degree n between $\mathbb{C}/\Lambda_\tau$ and $\mathbb{C}/\Lambda_{\tau'}$ if and only if there exists $\alpha \in \mathcal{S}_n$ with $\tau' = \alpha\tau$. Therefore it is not surprising that we define F_n in the following way:

Definition 3.31. For positive integers n let

$$F_n(j, X) = \prod_{\alpha \in \mathcal{S}_n} (X - j \circ \alpha)$$

and

$$\Phi_n(j, X) = \prod_{\alpha \in \mathcal{S}_n^*} (X - j \circ \alpha).$$

Both are called the nth *modular polynomial*.

Theorem 3.32. *The modular polynomials are symmetric monic polynomials in $\mathbb{Z}[X, Y]$. Let E, E' be two elliptic curves defined over $\mathbb{C}$. Then there exists an isogeny $E \to E'$ of degree n if and only if $F_n(j(E), j(E')) = 0$. The kernel of this isogeny is cyclic if and only if $\Phi_n(j(E), j(E')) = 0$.*

Proof. While the proof is not very difficult it would require an introduction to modular and automorphic forms. Therefore we have to skip it here. For the first family of modular polynomials refer to to [Sil94, theorem II.6.3a and lemma I.9.3]. For the second family refer to [Lan87, theorems 5.3 and 5.5]. $\square$

Note that for prime numbers n, $F_n(x, y) = \Phi_n(x, y)$. The curve in $\mathbb{P}^2(\mathbb{C})$ described by (the homogenization of) $\Phi_n(x, y) = 0$ is a singular model of the *(classical) modular curve* $X_0(n)$ (see [Sil92, section C.13] for the definition and an overview of modular curves, and [Shi71] for details).

Since the modular polynomials are in $\mathbb{Z}[X, Y]$ they make sense in every field. Thus we can ask if it is possible to generalize theorem 3.32 to arbitrary fields:

Theorem 3.33. *Let E and E' be elliptic curves defined over a field K. Let ℓ be a prime different from $\mathrm{char}\, K$. Then there exists a separable isogeny $E \to E'$ with degree ℓ if and only if $\Phi_\ell(j(E), j(E')) = 0$.*

Proof. Fix an elliptic curve E. By theorem 2.39 there are exactly $\ell + 1$ isomorphism classes of elliptic curves isogenous to E. This is equal to the degree of $\Phi_\ell(j(E), T)$. Thus we only have to show that if there exists an isogeny, then $\Phi_\ell(j(E), j(E')) = 0$.

Let E be given by a Weierstraß equation

$$f_E(x, y) = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6 = 0.$$

If P is a nontrivial point in $E[\ell]$ then there exists exactly one subgroup $C_P \subseteq E(\bar{K})$ with order ℓ and $P \in C_P$. It is given by $C_P = \{[i]P : i = 0, \cdots, \ell-1\}$. Using theorem 3.27 we can calculate the coordinates of all points of C_P by rational functions in P (over $\mathbb{Z}(a_1, a_2, a_3, a_4, a_6)$). Then with Vélu's formulas 2.33 we get rational functions over the same ring for the Weierstraß coefficients of an elliptic curve E_P such that there exists an isogeny $\alpha_P \colon E \to E_P$ with $C_P = \ker \alpha_P$. Of course the j-invariant $j(E_P)$ is a rational function of the coefficients. Hence we get a rational function $J_E \in \mathbb{Z}(a_1, a_2, a_3, a_4, a_6)(x, y)$ such that $J_E(P) = j(E_P)$ for all $P \in E[\ell]$. Therefore we have to check that $\Phi_\ell(j(a_1, \cdots, a_6), J_E(P)) = 0$ for all $P \in E[\ell]$.

Like in the proof of theorem 3.27, we first look at the field $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6)$ (of transcendence degree 5 over $\mathbb{Q}$) and an elliptic curve C given by

$$f_C(x, y) = y^2 + \alpha_1 xy + \alpha_3 y - x^3 - \alpha_2 x^2 - \alpha_4 x - \alpha_6 = 0.$$

Using the Lefschetz principle (i.e. embedding L in $\mathbb{C}$) and theorem 3.32 we see that

$$\Phi_\ell(j(\alpha_1, \cdots, \alpha_6), J_C(P)) = 0 \in L \text{ for all } C \in E[\ell].$$

Also as elements of $\mathbb{Z}(a_1, a_2, a_3, a_4, a_6)(x, y)$ we have

$$\phi_E\left(\Phi_\ell(j(\alpha_1, \cdots, \alpha), J_C(x, y))\right) = \Phi_\ell(j(a_1, \cdots, a_6), J_E(x, y)),$$

where ϕ_E is the homomorphism defined by $\alpha_i \to a_i$.

Let $H(x, y) \in \mathbb{Z}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6)[x, y]$ be the polynomial obtained from $\Phi_\ell(j(\alpha_1, \cdots, \alpha_6), J_C(x, y))$ be clearing denominators. Then H as the same roots as $\Phi_\ell(j(\alpha_1, \cdots, \alpha_6), J_C(x, y))$, which includes all points of $C[\ell]$. Hence Ψ_ℓ divides H (over $\mathbb{Q}$), so there exists a polynomial $G(x, y)$ with

$$G(x, y)\Psi_\ell(x, y) = H(x, y). \tag{3.6}$$

Since H is monic and the leading coefficient of Ψ_ℓ is ℓ, we actually have $G(x, y) \in \mathbb{Z}[\frac{1}{\ell}](\alpha_1, \ldots, \alpha_6)[x, y]$.

Since $\ell \neq \operatorname{char} K$ the element $\phi_E(\frac{1}{\ell}) \in K$ is well defined and we can apply ϕ_E to (3.6). Therefore $\psi_\ell(x, y)$ is a divisor of $\phi_E(H)(x, y)$ which has the same roots as $\Phi_\ell(j(a_1, \cdots, a_6), J_E(x, y))$. Thus $\Phi_\ell(j(a_1, \cdots, a_6), J_E(P)) = 0$ for all $P \in E[\ell]$. $\square$

Theorem 3.34 (Kronecker Congruence Relation)**.** *Let p be a prime.*

$$\Phi_p(X, Y) \equiv (X^p - Y)(X - Y^p) \pmod{p}.$$

Proof. [Lan87, section 5.3] $\square$

3.3 Elliptic Curves over Finite Fields

3.3.1 The Weil Conjectures

We will introduce the zeta function of a variety over a finite field. It essentially encodes the size of the variety over all finite extensions of the ground field. It turns out that this function is simpler than one might assume: The Weil conjectures give a very close description. As such they are an essential tool in the study of projective varieties over finite fields.

Definition 3.35. Let V be a projective variety over the finite field $\mathbb{F}_q$. Then the *zeta function* of V/K is the formal power series

$$Z(V/K; T) = \exp\left(\sum_{n=1}^{\infty} \#V(K_n)\frac{T^n}{n}\right).$$

Theorem 3.36 (Weil Conjectures). *Let V/K be a smooth projective variety of dimension n over a finite field with q elements. Then the following properties hold for the zeta function of V:*

1. *Rationality: $Z(V/K; T) \in \mathbb{Q}(T)$.*
2. *Functional Equation: There exists an integer ε (the Euler characteristic of V) so that*

$$Z\left(V/K; \frac{1}{q^n T}\right) = \pm q^{\frac{n\varepsilon}{2}} T^\varepsilon Z(V/K; T).$$

3. *Riemann Hypothesis: The zeta function factorizes as*

$$Z(V/K; T) = \frac{P_1(T) P_3(T) \cdots P_{2n-1}(T)}{P_0(T) P_2(T) \cdots P_{2n}(T)},$$

where each $P_i(T) \in \mathbb{Z}[T]$. Further $P_0(T) = 1 - T$, $P_{2n}(T) = 1 - q^n T$ and for $1 \leq i \leq 2n - 1$ there exist numbers $\alpha_{ij} \in \mathbb{C}$ with $|\alpha_{ij}| = q^{i/2}$ such that

$$P_i(T) = \prod_j (1 - \alpha_{ij} T).$$

Although these statements are still called Weil *conjectures* they, have been full proven since 1973 by the work of Dwork [Dwo60] (rationality), Grothendieck [Gro64] and others (functional equation) and finally Deligne [Del74]. In fact Weil himself proved the conjectures for curves in 1948 [Wei48] even before he published the conjectures themselves in 1949 [Wei49]. An overview of the history of the Weil Conjectures and the techniques used to prove them is given in [Har77, appendix C].

The practical significance of the Weil conjectures is that they say that it is possible to calculate the whole zeta function of a variety if we know the value of $\#V(\mathbb{F}_{q^n})$ for some small values of n. In particular for curves we only need to know the single value $\#V(\mathbb{F}_q)$. Then we can compute the size of the variety over bigger fields by

$$\#V(\mathbb{F}_{q^n}) = \frac{1}{(n-1)!} \frac{\mathrm{d}^n}{\mathrm{d}T^n} \log Z(V/K; T).$$

The following theorem is the key point for proving the Weil conjectures for elliptic curves.

Theorem 3.37. *Let E be an elliptic curve over $K = \mathbb{F}_q$ and ϕ_q the qth-power Frobenius morphism. Then*

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

Proof. Since ϕ_q (topologically) generates the Galois group $\operatorname{Gal}(\bar{K}/K)$ we know that for a point $P \in E(\bar{K})$,

$$P \in E(K) \quad \Leftrightarrow \quad \phi_q(P) = P.$$

In other words $E(K) = \ker(1 - \phi_q)$. Hence by 2.32, 2.28 and 2.52,

$$\#E(K) = \#\ker(1 - \phi_q) = \deg(1 - \phi_q) = \det(1 - \phi_q) = 1 - \operatorname{tr} \phi_q + q,$$

where the last equality is obtained by substituting 1 into the characteristic polynomial of ϕ_q. □

Corollary 3.38. *Let E, E' be two elliptic curves defined over $\mathbb{F}_q$ and $\psi \colon E \to E'$ an isogeny. Then $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$.*

Outline of proof. Let ℓ be a prime such that $\ell \nmid q \deg \psi$. Then ψ gives isomorphisms $E[\ell^i] \to E'[\ell^i]$. Hence the traces of the Frobenius morphisms on E and E' are equal and so the two elliptic curves must have the same number of points. □

Tate proved that the converse also true [Tat66]: Two elliptic curves defined over $\mathbb{F}_q$ are isogenous if and only if $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$. Therefore the zeta function of an elliptic curve completely determines its isogeny class.

Theorem 3.39 (Weil Conjectures for Elliptic Curves). *Let $E/\mathbb{F}_q$ be an elliptic curve. Then there exists an integer a such that*

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

The numerator $1 - aT + qT^2$ factors as $(1 - \alpha T)(1 - \beta T)$ with $|\alpha| = |\beta| = \sqrt{q}$. Further the following functional equation holds:

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

Proof. Let ϕ_q be the qth-power Frobenius morphism on E. The characteristic polynomial of ϕ_q factors over $\mathbb{C}$, say

$$\det(T - \phi_q) = T^2 - \operatorname{tr}(\phi_q)T + q = (T - \alpha)(T - \beta).$$

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

$$\left(\frac{m}{n}\right)^2 - \operatorname{tr}(\phi_q)\frac{m}{n} + q = \frac{m^2 - \operatorname{tr}(n\phi_q)m + n^2 q}{n^2} = \frac{\det(m - n\phi_q)}{n^2} = \frac{\deg(m - n\phi_q)}{n^2} \geq 0.$$

Thus the polynomial $\det(T - \phi_q) \in \mathbb{R}[T]$ cannot have two distinct real roots. Hence $|\alpha| = |\beta|$. Further because of

$$\alpha\beta = \det\phi_q = \deg\phi_q = q,$$

we conclude that $|\alpha| = |\beta| = \sqrt{q}$. Set $a = \alpha + \beta = \operatorname{tr}\phi_q \in \mathbb{Z}$. The $(q^n)^{\text{th}}$-power Frobenius morphism is given by ϕ_q^n and by putting $(\phi_q)_\ell$ into Jordan normal form we see that $(\phi_q)_\ell^n$ has trace $\alpha^n + \beta^n$. In particular

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

Now we can assemble the zeta function:

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

$$- \log(1 - T) + \log(1 - \alpha T) + \log(1 - \beta T) - \log(1 - qT).$$

Therefore

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

Corollary 3.40 (Hasse's Theorem). *Let E be an elliptic curve defined over $\mathbb{F}_q$. Then*

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

Proof. Let ϕ_q be the qth-power Frobenius morphism on E. Then

$$|\#E(\mathbb{F}_q) - q - 1| = |\operatorname{tr}\phi_q| = |\alpha + \beta| \leq 2\sqrt{q}.$$

$$\square$$

Using suitable generalizations of the ideas we have used in this section one can show the Weil conjectures for arbitrary curves. See [Mum74, pp. 203–207] and [Har77, exercise C.5.7].

Theorem 3.41 ([Wei48]). *Let C be an irreducible non-singular curve of genus g defined over $\mathbb{F}_q$. Then*

$$Z(C/\mathbb{F}_q;\, T) = \frac{P_1(T)}{(1 - T)(1 - qT)},$$

where

$$P_1(T) = \prod_{j=1}^{2g}(1 - \alpha_j T) \in \mathbb{Z}[T]$$

with $|\alpha_j| = \sqrt{q}$. Hence Hasse's theorem generalizes to

$$|\#C(\mathbb{F}_{q^r}) - q^r - 1| \leq 2g\sqrt{q^r}.$$

Further,

$$\left|\# \operatorname{Pic}^0_{\mathbb{F}_{q^r}}(C) - q^g\right| = O\left(q^{g - \frac{1}{2}}\right).$$

3.3.2   Torsion Subgroups

A finite field $\mathbb{F}_{q^k}$ contains the nth roots of unity if and only if $x^n - 1 \mid x(x^{q^k-1} - 1)$ and this holds if and only if $n \mid q^k - 1$. Note that this is only possible if n and q are coprime

Definition 3.42. Let $\mathbb{F}_q$ be a finite field and n a positive integer coprime to q. Then the *embedding degree* corresponding to q and n is the smallest positive integer $k = k(q, n)$ such that $n \mid q^k - 1$. In other words it is the smallest k such that $\boldsymbol{\mu}_n(\mathbb{F}_q) \subseteq \mathbb{F}_{q^k}$.

Theorem 3.43. *Let E be an elliptic curve over $\mathbb{F}_q$ and n and k positive integers such that $E[n] \subseteq E(\mathbb{F}_{q^k})$. Then $n \mid q^k - 1$.*

Proof. This follows immediately from theorem 2.46.   □

Theorem 3.44 ([BK98]). *Let E be an elliptic curve over $\mathbb{F}_q$ and ℓ a prime dividing $\#E(\mathbb{F}_q)$. Suppose that ℓ is coprime to q and does not divide $q - 1$. Then $E[\ell] \subseteq E(\mathbb{F}_{q^k})$ if and only if $\ell \mid (q^k - 1)$.*

Proof. Necessity is the preceding theorem. Suppose $\ell \equiv 1 \pmod{q^k}$. Since ℓ is prime to q, $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$. By assumption there exists a point $P \in E(\mathbb{F}_q)$ of order ℓ. Let $Q \in E(\bar{\mathbb{F}}_q)$ be any point such P, Q is a basis of $E[\ell]$. Further let ϕ_q be the qth-power Frobenius morphism on E. Since ϕ_q^k generates $\text{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_{q^k})$, the point Q is defined over $\mathbb{F}_{q^k}$ if and only if $\phi_q^k(Q) = Q$.

The action of ϕ_q on $E[\ell]$ with respect to the basis P, Q is given by the matrix

$$\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}$$

for some integers b and d. From theorem 3.37 we know that

$$q + 1 - \#E(\mathbb{F}_q) = \text{tr}(\phi_q) \equiv 1 + d \pmod{\ell}.$$

Further $\#E(\mathbb{F}_q) \equiv 0 \pmod{\ell}$, so $q \equiv d \pmod{\ell}$. Thus the action of ϕ_q^k on $E[\ell]$ is given by

$$\begin{pmatrix} 1 & b \\ 0 & q \end{pmatrix}^k = \begin{pmatrix} 1 & b\frac{q^k-1}{q-1} \\ 0 & q^k \end{pmatrix}.$$

So $\phi_q^k(Q) = Q$ if and only if this matrix is the identity matrix modulo ℓ, i.e. $q^k \equiv 1 \pmod{\ell}$.   □

Corollary 3.45. *Let E be an elliptic curve over $\mathbb{F}_q$ and ℓ be a prime dividing $\#E(\mathbb{F}_q)$. Suppose that ℓ is coprime to q and does not divide $q - 1$. Then the Weil pairing is defined on $E(\mathbb{F}_{q^k})$ if and only if $\boldsymbol{\mu}_\ell(\mathbb{F}_q) \subseteq \mathbb{F}_{q^k}$.*

The Tate pairing maps into $K^*/(K^*)^n$. For a finite field $K = \mathbb{F}_q$ which contains the nth roots of unity this group is canonically isomorphic to $\boldsymbol{\mu}_n(K)$ under the map

$$\alpha \bmod (\mathbb{F}_q^*)^n \mapsto \alpha^{\frac{q-1}{n}}.$$

Therefore we get the *modified Tate(-Lichtenbaum) pairing*

$$\tilde{\tau}_n \colon E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \to \boldsymbol{\mu}_n$$

$$\tilde{\tau}_n(P, \bar{Q}) = \tau_n(P, \bar{Q})^{\frac{q-1}{n}} = f_P(D_Q)^{\frac{q-1}{n}}. \tag{3.7}$$

We conclude this section with a partial description of the group structure of elliptic curves over finite fields.

Theorem 3.46. *Let E be an elliptic curve over $\mathbb{F}_q$. Then there exist non-negative integers n_1, n_2 with $n_1 \mid \gcd(n_2, q - 1)$ such that*

$$E(\mathbb{F}_q) \cong (\mathbb{Z}/n_1\mathbb{Z}) \oplus (\mathbb{Z}/n_2\mathbb{Z}).$$

(Possibly $n_1 = 1$.)

Proof. $E(\mathbb{F}_q)$ is a finite Abelian group, so, by the fundamental theorem on finitely generated Abelian groups, there exist integers $n_1, n_2, \ldots, n_r$ with $n_i | n_{i+1}$ $(i = 1, \ldots, r-1)$ and $E \cong (\mathbb{Z}/n_1\mathbb{Z}) \oplus (\mathbb{Z}/n_2\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/n_r\mathbb{Z})$. Without loss of generality we can assume that $n_1 > 1$. Then $E(\mathbb{F}_q)$ has at least n_1^r points of order n_1, but by theorem 2.38, $\#E(\mathbb{F}_q)[n_1] \leq n_1^2$. Hence $r \leq 2$. By adding $\mathbb{Z}/1\mathbb{Z}$ summands we can assume that $r = 2$.

There are n_1^2 elements of order n_1 contained in $(\mathbb{Z}/n_1\mathbb{Z}) \oplus (\mathbb{Z}/n_2\mathbb{Z})$, so again by theorem 2.38 $E[n_1] \subseteq E(\mathbb{F}_q)$. With a look a theorem 3.43 we conclude that $n_1 \mid q-1$. □

It is possible to give additional conditions that n_1 and n_2 have to satisfy, see [Vol88].

3.3.3 Supersingular Curves

Theorem 3.47. *Let $K = \mathbb{F}_q$, $q = p^n$, and E/K be an elliptic curve. For $r \geq 1$ let ϕ_r be the $(p^r)^{th}$-power Frobenius morphism on E. Then the following statements are equivalent:*

(i) $E[p^r] = 0$ for one (all) $r \geq 1$.
(ii) $\widehat{\phi}_r$ is (purely) inseparable for one (all) $r \geq 1$.
(iii) The map $[p]\colon E \to E$ is purely inseparable for all E.
(iv) $\operatorname{tr}\phi_n \equiv 0 \pmod{p}$.

Proof. For the equivalence of the first three statements see [Sil92, theorem V.3.1]. We will only show (ii) ⇔ (iv). Let $\phi = \phi_n$ be the qth-power Frobenius. By theorem 2.55 we know that $\widehat{\phi} = [\operatorname{tr}\phi] - \phi$ and thus by theorem 2.32 $\widehat{\phi}$ is inseparable if and only if $p \mid \operatorname{tr}\phi$. □

Definition 3.48. An elliptic curve which satisfies the equivalent properties given in the last theorem is called *supersingular*. Otherwise it is *ordinary*. A supersingular curve is said to have *Hasse invariant* 0, an ordinary curve has Hasse invariant 1.

Remark 3.49. There are several other equivalent characterizations for supersingularity. Some of them and further references are given in [Sil92, sections V.3 and V.4] and [Hus04, chapter 13]. We should also note that a supersingular curve is in particular an elliptic curve and hence non-singular (i.e. smooth) and that one should not confuse these two notions.

Using [Wat69, theorem (4.1)] and [Sch87, lemma (4.8)] one can give the following classification of supersingular elliptic curves:

Theorem 3.50. *Let $E/\mathbb{F}_q$, $q = p^e$ be a supersingular elliptic curve with $\#E(\mathbb{F}_q) = q + 1 - t$. Then one of the following holds:*

(I) $t = 0$ and $E(\mathbb{F}_q)$ is cyclic.
(II) $t = 0$, $E(\mathbb{F}_q) = \mathbb{Z}_{\frac{q+1}{2}} \oplus \mathbb{Z}_2$.
(III) $t^2 = q$ and $E(\mathbb{F}_q)$ is cyclic.
(IV) $t^2 = 2q$ and $E(\mathbb{F}_q)$ is cyclic.
(V) $t^2 = 3q$ and $E(\mathbb{F}_q)$ is cyclic.
(VI) $t^2 = 4q$ and $E(\mathbb{F}_q) = \mathbb{Z}_{\sqrt{q}\pm1} \oplus \mathbb{Z}_{\sqrt{q}\pm1}$.

Corollary 3.51 ([MOV93]). *Let $E/\mathbb{F}_q$ be a supersingular elliptic curve and n the order of a subgroup of $E(\mathbb{F}_q)$. Then there exists $k \leq 6$ such that $E[n] \subseteq E(\mathbb{F}_{q^k})$, i.e. the maximal embedding degree is 6.*

Proof. Since $n \mid q + 1 - t$ and $p \mid t$ we know that $\gcd(n, q) = 1$. Now one only has to check the six cases above with theorem 3.44. □

Two elliptic curves E, E' are isogenous if and only $\operatorname{Hom}(E, E') \neq 0$. From [Sil92, corollary III.7.5] we know that $\operatorname{Hom}(E, E')$ is a free $\mathbb{Z}$ module of rank less or equal 4. Using the supersingularity property, one can completely determine the rank.

Theorem 3.52. *Let E, E' be two isogenous elliptic curves. Then the rank of $\operatorname{Hom}(E, E')$ is 2 if E is ordinary and 4 if E is supersingular.*

Proof. [Hus04, proposition 13.8.2] □

3.3.4 The Modular Polynomials

In section 6.2.1 we will need some theorems about the modular polynomials over finite fields which we are going to collect in this section.

Theorem 3.53. *Let E be a ordinary elliptic curve defined over $K = \mathbb{F}_q$ with j-invariant $j \neq 0$, 1728 and let $\ell \neq \operatorname{char} K$ be a prime. Let ϕ_q be the qth-power Frobenius endomorphism on E.*

1. *Let $j' \in \bar{\mathbb{F}}_q$ be a root of $\Phi_\ell(j, T) \in \mathbb{F}_q[T]$. Let C be the kernel of the corresponding isogeny $E \to E/C$ of degree ℓ. Then $j' \in \mathbb{F}_{q^r}$ if and only if C is a one dimensional eigenspace of ϕ_q^r, i.e. if there exists $\nu \in \mathbb{Z}$ such that $\phi_q^r P = \nu P$ for all $P \in C$.*

2. *The polynomial $\Phi_\ell(j, T)$ splits completely in $\mathbb{F}_{q^r}$ if and only if ϕ_q^r acts as a scalar matrix on $E[\ell]$, i.e. if there exists $\nu \in \mathbb{Z}$ such that $\phi_q^r P = \nu P$ for all $P \in E[\ell]$.*

Proof. [Sch95, proposition 6.1] □

Theorem 3.54 (Atkin)**.** *Let E be a ordinary elliptic curve defined over $\mathbb{F}_q$, $q = p^e$ with j-invariant $j \neq 0$, 1728 and let $\ell \neq p$ be a prime. Further let $t = \operatorname{tr} \phi_q$ be the trace of the Frobenius morphism of E over $\mathbb{F}_q$. Write*

$$\Phi_\ell(j, T) = f_1(T) \cdots f_s(T)$$

for the factorization of $\Phi_\ell(j, T)$ in irreducible polynomials in $\mathbb{F}_q[T]$. Then there exists r such that the degrees of the factors are one of the following:

(1) 1 and ℓ (in this case set $r = \ell$);
(2) 1, 1, r, r ..., r;
(3) r, r, r ..., r;

In the first case $t^2 - 4q \equiv 0 \pmod{\ell}$, in the second case $t^2 - 4q$ is a square mod ℓ and in the last one $t^2 - 4q$ is not a square mod ℓ. Further in the last two cases

$$t^2 \equiv \left(\zeta + 2 + \zeta^{-1}\right) q \pmod{\ell},$$

where ζ is a primitive r^{th} root of unity in $\bar{\mathbb{F}}_\ell$.

Proof. Let $(\phi_q)_\ell$ be the action of ϕ_q on $E[\ell]$. Let $F(T) = T^2 - tT + q$ be the characteristic polynomial of ϕ_q. First suppose that it factors as $F(T) = (T - \lambda)(T - \mu) \pmod{\ell}$ with two distinct roots $\lambda, \mu \in \mathbb{F}_\ell$. Then it is possible to find a basis of $E[\ell]$ that diagonalizes $(\phi_q)_\ell$. Hence there exists a subgroup C_λ such that $\phi_q(P) = [\lambda]P$ for all $P \in C_\lambda$ and an analogous subgroup C_μ. These are the only possible eigenspaces of ϕ_q. By the last theorem there are exactly two corresponding j-invariants $j_\lambda, j_\mu \in \mathbb{F}_q$ that are roots of $\Phi_\ell(j, T)$. Let $j' \in \mathbb{F}_q$ be another root of $\Phi_\ell(j, T)$ and let r be the smallest integer such that $j' \in \mathbb{F}_{q^r}$. Choose j' such that r is minimal. Again by the last theorem there exists a subgroup C' of $E[\ell]$ and an integer ν such ϕ_q^r acts on C' as multiplication by ν. Since $j' \neq j_\lambda, j_\mu$ we have $C' \neq C_\lambda, C_\mu$. Thus we have three distinct eigenspaces of $(\phi_q)_\ell^r$ which is only possible if $(\phi_q)_\ell^r$ is scalar. Therefore by part (2) of the preceding theorem, $\Phi_\ell(j, T)$ splits completely in $\mathbb{F}_{q^r}$. By the minimality of r no roots (except j_λ and j_μ) can lie in a smaller field. So we have case (2). Further $F(T)$ factors mod ℓ if and only if the discriminant $t^2 - 4q$ is a square in $\mathbb{F}_\ell$.

If $F(T) = (T - \lambda)^2 \pmod{\ell}$ (i.e. $t^2 - 4q \equiv 0 \pmod{\ell}$) then either $(\phi_q)_\ell = \lambda I$ or there exists some basis of $E[\ell]$ such that $(\phi_q)_\ell = \left(\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix}\right)$. In the first case, theorem 3.53 (2) immediately implies that $\Phi_\ell(j, T)$ splits in linear factors over $\mathbb{F}_q$. This is case $r = 1$ in (2). For the non-diagonal Jordan form case we have

$$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}^k = \begin{pmatrix} \lambda^k & k\lambda^{k-1} \\ 0 & \lambda^k \end{pmatrix}^k,$$

which is non-diagonal for $k < \ell$ and diagonal for $k = \ell$. Therefore the smallest r such that $(\phi_q)_\ell^r$ has two independent eigenvectors is $r = \ell$. The reasoning of the first part can again be applied and we see that $\Phi_\ell(j, T)$ has an irreducible factor of degree ℓ. This yields case (1).

Finally suppose that $F(T)$ is irreducible (i.e. $t^2 - 4q$ is not a square mod ℓ). Then the two roots λ, μ of $F(T)$ lie in $\mathbb{F}_{q^2}$ and are quadratic conjugates. The eigenvalues of $(\phi_q)_\ell^k$ are λ^k and μ^k. Let k be the smallest integer such that $\lambda^k \in \mathbb{F}_\ell$ (or equivalently $\mu^k \in \mathbb{F}_\ell$). This is also the smallest k such that $(\phi_q)_\ell^k$ has an eigenvalue. Hence $\mathbb{F}_{p^k}$ is the smallest field containing a root of $\Phi_\ell(j, T)$. Since λ^k and μ^k are

quadratic conjugates and lie in $\mathbb{F}_\ell$ they are equal and $(\phi_q)_\ell^k$ is scalar. Therefore all irreducible factors of $\Phi_\ell(j, T)$ have degree $r = k$.

In all cases, since $(\phi_q)_\ell^r$ is scalar, $\lambda^r = \mu^r = \frac{q^r}{\lambda^r}$. Hence $\lambda^{2r} = q^r$ or $\lambda^2 = \zeta q$ for some r^{th} root of unity $\zeta \in \bar{\mathbb{F}}_\ell$. From $t = \lambda + \mu \pmod{\ell}$ we get

$$t^2 = (\lambda + \frac{q}{\lambda})^2 = \lambda^2 + 2q + \frac{q^2}{\lambda^2} = q(\zeta + 2 + \zeta^{-1}) \pmod{\ell}.$$

If $\zeta^k = 1$ for some $k < r$ then $\lambda^k = \mu^k$ and $(\phi_q)_\ell^k$ is scalar. This contradicts the minimality of r. $\qquad\square$

Definition 3.55. Let E and ℓ be defined as in the last theorem. If one of the first two cases of the theorem holds, then ℓ is called *Elkies prime*. In case (3), ℓ is called *Atkin prime*

3.4 Elliptic Curves over Local fields

3.4.1 A Short Review of the Theory of Local Fields

For reference briefly state the parts of the theory of local fields that we are going to use. Details and proofs can, for example, be found in [Neu07] or [Ser79].

Definition 3.56. Let R be an integral domain. An *absolute value* on R is a function $|\cdot| \colon R \to \mathbb{R}$ such that for all $x, y \in R$:

1. $|x| \geq 0$,
2. $|x| = 0$ if and only if $x = 0$,
3. $|xy| = |x||y|$ and
4. $|x + y| \leq |x| + |y|$ (triangle inequality).

If instead of the triangle inequality the stronger condition $|x + y| \leq \max\{|x|, |y|\}$ holds, then the absolute value is called *non-Archimedean*. Otherwise it is called *Archimedean*. An absolute value is non-Archimedean if and only if $|n|$ is bounded for $n \in \mathbb{Z}$. Every absolute value induces a topology on R and two absolute values $|\cdot|_1$ and $|\cdot|_2$ are called *equivalent* if they induce the same topology. This is the case if and only if there exists a constant $s > 0$ such that $|x|_1 = |x|_2^s$ for all $x \in R$.

Definition 3.57. Let R be an integral domain. A *valuation* on R is a map $v \colon R \to \mathbb{R} \cup \{\infty\}$ such that for all $x, y \in R$:

1. $v(x) = \infty$ if and only if $x = 0$,
2. $v(xy) = v(x) + v(y)$ and
3. $v(x + y) \geq \min\{v(x) + v(y)\}$.

It is called *discrete* if its image is a discrete subgroup of $\mathbb{R}$ together with ∞. A discrete valuation is *normalized* if $v(R) = \mathbb{Z} \cup \{\infty\}$.

Some authors use the term valuation instead of absolute value and then call a valuation an *exponential valuation*. For any non-Archimedean absolute value $|\cdot|$ one can define valuations by $v(x) = -\log_b |x|$ for any base b (and $v(0) = \infty$).

For $\mathbb{Q}$ (and subrings) and a prime number p define the *p-adic absolute value* by $|x|_p = p^{-m}$ where m is chosen such that $x = p^m \frac{a}{b}$ with $p \nmid ab$. The corresponding *p-adic valuation* v_p is defined by $v_p(x) = m$. The usual absolute value on $\mathbb{Q}$ is denoted by $|\cdot|_\infty$.

Theorem 3.58 (Ostrowski). *Any non-trivial absolute value on $\mathbb{Q}$ is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$ for some prime number p.*

Definition 3.59. A *valuation ring* is an integral domain R such that for every element $x \in \text{Quot}(R)$ at least one of x and x^{-1} belongs to R. A *discrete valuation ring* (DVR) is a local principal ideal domain which is not a field.

Proposition 3.60. *Every valuation ring is a local ring and is integrally closed in its field of fractions. If it is a principal ideal domain, then it is either a field or a DVR.*

Proposition 3.61. *Let R be an integral domain. Then the following conditions are equivalent:*

1. *R is a discrete valuation ring.*
2. *R is a local Dedekind domain but not a field.*
3. *R is a Noetherian local ring with Krull dimension one and a principal maximal ideal.*
4. *R is an integrally closed Noetherian local ring with Krull dimension one.*
5. *R is a unique factorization domain with a unique irreducible element (up to multiplication by units).*
6. *There exists a discrete valuation v on $\mathrm{Quot}(R)$ such that $R = \{x \in \mathrm{Quot}(R) : v(x) \geq 0\}$.*

Let $\mathfrak{m}$ be the maximal ideal of R and π a generator of $\mathfrak{m}$. Then every non-zero element $x \in \mathrm{Quot}(R)$ can be uniquely written as $x = \varepsilon \pi^{v(x)}$ where $\varepsilon \in R^*$ and $v(x) \in \mathbb{Z}$. Further $v(x)$ defines a discrete valuation on $\mathrm{Quot}(R)$. The element π is called a uniformizing parameter *of R.*

Definition and Proposition 3.62. *Let K be any field with a valuation $v : K \to \mathbb{R}$ and corresponding absolute value $|\cdot|$. Then*

$$\mathcal{O}_v = \{x \in K : v(x) \geq 0\} = \{x \in K : |x| \leq 1\}$$

is the ring of integers *or* valuation ring *of K. It is a valuation ring with units*

$$\mathcal{O}_v^* = \{x \in K : v(x) = 0\} = \{x \in K : |x| = 1\}$$

and maximal ideal

$$\mathfrak{m} = \{x \in K : v(x) > 0\} = \{x \in K : |x| < 1\}.$$

The field $k = \mathcal{O}_v/\mathfrak{m}$ is called the residue field *of $\mathcal{O}_v$ (or K). If v is discrete, then $\mathcal{O}_v$ is a DVR.*

When the valuation is implicitly clear we will sometimes write $\mathcal{O}_K$ for the valuation ring of K.

Proposition 3.63. *Let K be a field with discrete valuation v. All non-trivial ideals of $\mathcal{O}_v$ are given by*

$$\mathfrak{m}^n = \pi^n \mathcal{O}_v = \{x \in K : v(x) \geq n\},$$

where π is a fixed uniformizing parameter of $\mathcal{O}_v$ and n runs through the positive integers. Further for every $n \in \mathbb{N}$,

$$\mathfrak{m}^n/\mathfrak{m}^{n+1} \cong \mathcal{O}_v/\mathfrak{m} = k.$$

A discrete valuation v defines a metric on K by $d_v(x, y) = d^{v(x-y)}$ for a fixed $d \in (0, 1)$. For every $x \in K$ a basis of open neighborhoods of x is given by $x + \pi^n \mathcal{O}_v$, $n \in \mathbb{N}$. With this topology K is a topological field which is called a *discrete valuation field*.

Definition 3.64. A *Cauchy sequence* in a discrete valuation field K is a Cauchy sequence with respect to the metric defined above. K is *complete* when every Cauchy sequence is convergent. A complete discrete valuation field with perfect residue field is called a *local field*.

Theorem 3.65. *Local fields are locally compact. The ring of integers of a local field is compact.*

Theorem 3.66. *Local fields are exactly the finite extensions of $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$.*

In a complete discrete valuation field the power series $\sum_{n \geq 0} a_n x^n$ is convergent whenever all $a_n \in \mathcal{O}_v$ and $x \in \mathfrak{m}$.

Theorem 3.67 (Hensel's Lemma). *Let K be a complete discrete valuation field and $f(X)$ a polynomial in $\mathcal{O}_v[X]$. Let $\widetilde{f}(X) \in k[x]$ be the polynomial that arises from $f(X)$ by reducing every coefficient modulo $\mathfrak{m}$. Further let $\widetilde{f}(X)$ have a simple root $\alpha \in k$. Then there exists a unique $a \in \mathcal{O}_v$ such that $f(a) = 0$ and $a \equiv \alpha \bmod \mathfrak{m}$. Further, a is the limit of the sequence*

$$w_0 = \alpha \qquad w_{n+1} = w_n - \frac{f(w_n)}{f'(w_n)}, \tag{3.8}$$

where f' is the formal derivative of f. This sequence has quadratic convergence.

This version of Hensel's lemma can be heavily generalized, see [Eis95, section 7, especially the exercises] and [Bou89, theorem IV.5.2 and corollaries]. We will give a short proof of the version presented here because of its computational importance later on. Like its counterpart in real analysis the approximation of the root using (3.8) is often called *Newton's iteration*.

Proof. We will show by induction on n that w_n is well-defined and $w_n \equiv \alpha \pmod{\mathfrak{m}}$. That α is a simple root of $\widetilde{f}(x)$ is equivalent to $f'(\alpha) \not\equiv 0 \pmod{\mathfrak{m}}$. Assume that $w_n \equiv \alpha \pmod{\mathfrak{m}}$. Then $f(w_n) \equiv f(\alpha) \equiv 0 \pmod{\mathfrak{m}}$ and $f'(w_n) \equiv f'(\alpha) \not\equiv 0 \pmod{\mathfrak{m}}$. Thus w_{n+1} is well-defined and $w_{n+1} \equiv w_n \equiv \alpha \pmod{\mathfrak{m}}$.

Now we will show that $f(w_n) \in \mathfrak{m}^{2^n}$. For $n = 0$ this is the hypothesis of the theorem. Assume that the statement holds for some n. By Taylor expansion we have

$$f(w_{n+1}) = f(w_n) + f'(w_n)(w_{n+1} - w_n) + \beta(w_{n+1} - w_n)^2$$

for some $\beta \in \mathcal{O}_v$. Using (3.8) and the induction hypothesis we obtain

$$f(w_{n+1}) = \beta \left(\frac{f(w_n)}{f'(w_n)} \right)^2 \in \left(\mathfrak{m}^{2^n} \right)^2 = \mathfrak{m}^{2^{n+1}}.$$

In particular we see that $w_{n+1} - w_n \in \mathfrak{m}^{2^n}$. Since $\mathcal{O}_v$ is complete this implies that the limit $a = \lim w_n \in \mathcal{O}_v$ exists and $F(a) = 0$.

All that is left to show is uniqueness. Suppose $b \in O_v$ is another root of $f(x)$ with $b \equiv \alpha \bmod \mathfrak{m}$. Taylor expansion shows that there is an element $\gamma \in \mathcal{O}_v$ such that

$$f(x) = f(a) + f'(a)(x - a) + \gamma(x - a)^2.$$

Evaluating this at $x = b$ yields

$$0 = f(b) = (b - a)(f'(a) + \gamma(b - a)).$$

By assumption, $a - b \neq 0$. Hence,

$$f'(a) = -\gamma(b - a) \equiv -\gamma(\alpha - \alpha) = 0 \pmod{\mathfrak{m}}$$

which is a contradiction to the assumption that $f'(a) \not\equiv 0 \pmod{\mathfrak{m}}$. $\square$

Theorem 3.68. *Let K be complete with respect to a discrete valuation v and let $L|K$ be an algebraic extension. Then there exists a unique discrete valuation w on L such that $w_{|_K} = v$. Further $\mathcal{O}_w$ is the integral closure of $\mathcal{O}_v$ in L. If $[L : K] = n < \infty$, then*

$$w(\alpha) = \frac{1}{n} v(N_{L|K}(\alpha))$$

and L is again complete.

Definition 3.69. Let $L|K$ be a finite extension of complete discrete valuation fields with respective valuations w and v and residue fields l and k. Then

$$e = e(w|v) = [w(L^*) : v(K^*)]$$

is their *ramification index* and

$$f = f(w|v) = [l : k]$$

their *inertia* or *residue degree*.

Theorem 3.70. *With the notation of the definition, $[L : K] \geq ef$. If $L|K$ is separable, then $[L : K] = ef$.*

Definition 3.71. Again with the same notation, if $l|k$ is separable and $e = 1$, then the extension is called *unramified*. The *maximal unramified extension of K*, denoted K^{ur}, is the union of all unramified extensions of K in $\bar{K}$.

Theorem 3.72. *Let K be a complete discrete valuation field with residue field $k = \mathbb{F}_q$, $q = p^r$, and ζ a primitive n^{th} root of unity in $\bar{K}$ with $\gcd(n, p) = 1$. Let $L = K(\zeta)$ and let l be the residue field of L. Then:*

1. *The extension $L|K$ is unramified and of degree f, where f is the smallest positive integer such that $q^f \equiv 1 \pmod{n}$.*
2. *The Galois group $\mathrm{Gal}(L|K)$ is canonically isomorphic to $\mathrm{Gal}(l|k)$ which is generated by $\phi_q \colon x \mapsto x^q$.*
3. *$\mathcal{O}_L = \mathcal{O}_K[\zeta]$.*

Definition 3.73. Using the notation of the last theorem, if $K = \mathbb{Q}_p$ and $n = p^f - 1$ then $[L : K] = f$ and we write $L = \mathbb{Q}_q$ with $q = p^f$. The residue field l is $\mathbb{F}_q$ and $\phi_p \in \mathrm{Gal}(\mathbb{F}_q|\mathbb{F}_p)$ is called *Frobenius automorphism* (it is often denoted by $\bar{\sigma}$). The unique automorphism $\Sigma \in \mathrm{Gal}(\mathbb{Q}_q|\mathbb{Q}_p)$ with $\phi_p \equiv \Sigma \pmod{p}$ is called *Frobenius substitution*. The ring of integers of $\mathbb{Q}_q$ is denoted $\mathbb{Z}_q$.

Note the Σ is not simply p^{th} powering. For more info on p-adic numbers and extension fields, see [Kob84].

3.4.2 Formal Groups

In mathematics there are some objects which proved to be useful in a wide variety of areas. One of them are (formal) power series. So it is not surprising they can be used to describe groups. More precisely the idea is to abstract group laws from the underlying group to get a "group law without any group elements" which is then described by a power series.

In this section let $(R, \mathfrak{m})$ be a local ring that is complete with respect to the topology induced by the powers of the maximal ideal $\mathfrak{m}$. (Some of the following definitions and theorems make sense in a more general setting. However we will only apply them to local fields.)

Definition 3.74. A *(one-parameter, commutative) formal group* $\mathcal{F}$ *defined over* R is a power series $F(X, Y) \in R[\![X, Y]\!]$ satisfying:

1. $F(X, Y) = X + Y + (\text{terms of higher degree})$,
2. $F(X, F(Y, Z)) = F(F(X, Y), Z)$ (associativity),
3. $F(X, Y) = F(Y, X)$ (commutativity),
4. there exists a unique power series $i(T) \in R[\![T]\!]$ such that $F(T, i(T)) = 0$ (existence of inverse),
5. $F(X, 0) = X$ and $F(0, Y) = Y$.

The series $F(X, Y)$ is called the *formal group law of* $\mathcal{F}$.

Let $(\mathcal{G}, G)$ be another formal group defined over R. A *homomorphism from* $\mathcal{F}$ *to* $\mathcal{G}$ *defined over* R is a power series $f(T) \in R[\![T]\!]$ that has no constant term and satisfies

$$f(F(X, Y)) = G(f(X), f(Y)).$$

By abuse of notation we write $f \colon \mathcal{F} \to \mathcal{G}$.

The formal groups $\mathcal{F}$ and $\mathcal{G}$ are *isomorphic over* R if there are homomorphisms $f \colon \mathcal{F} \to \mathcal{G}$ and $g \colon \mathcal{G} \to \mathcal{F}$ (both defined over R) such that

$$f(g(T)) = g(f(T)) = T.$$

Definition 3.75. The *formal additive group* $\widehat{\mathbb{G}}_a$ is given by

$$F(X, Y) = X + Y.$$

The *formal multiplicative group* $\widehat{\mathbb{G}}_m$ is given by

$$F(X, Y) = X + Y + XY = (1 + X)(1 + Y) - 1.$$

Definition 3.76. Let $(\mathcal{F}, F)$ be a formal group. The *multiplication-by-m map* on $\mathcal{F}$ is the homomorphism

$$[m] \colon \mathcal{F} \to \mathcal{F}$$

defined inductively for $m \in \mathbb{Z}$ by $[0](T) = 0$ and

$$[m + 1](T) = F([m](T), T),$$

$$[m - 1](T) = F([m](T), i(T)).$$

The following lemma about formal power series is well-know and easy to prove by induction (see [Sil92, lemma IV.2.4]). So we will skip the proof and only state the result for reference.

Lemma 3.77. *Let* $f \in R[\![T]\!]$ *be a power series starting with* $f(T) = aT + \cdots$, *where* $a \in R^*$. *Then there exists a unique power series* $g(T) \in R[\![T]\!]$ *such that* $f(g(T)) = T$. *Further, it satisfies* $g(f(T)) = T$.

Proposition 3.78. *Let* $\mathcal{F}$ *be a formal group over* R *and* $m \in \mathbb{Z}$. *Then*

$$[m](T) = mT + (\text{higher order terms}).$$

Further if $m \in R^*$, *then* $[m] \colon \mathcal{F} \to \mathcal{F}$ *is an isomorphism.*

Proof. The first statement can be shown by a simple induction. (Note that because of $0 = F(T, i(T)) = T + i(T) + \cdots$, we have $i(T) = -T + \cdots$.) Then the second statement follows from the lemma above. $\square$

Definition 3.79. Let $(\mathcal{F}, F)$ be a formal group over R. Then the *group associated to $\mathcal{F}$*, denoted $\mathcal{F}(\mathfrak{m})$ is the set $\mathfrak{m}$ with the group operations

$$x \oplus_{\mathcal{F}} y = F(x, y),$$
$$\ominus_{\mathcal{F}} x = i(x).$$

Similarly we can define $\mathcal{F}(\mathfrak{m}^n)$. (Since R is complete, $F(x, y)$ and $i(x)$ converge to an element of $\mathfrak{m}$).

The definition of a formal group implies that $\mathcal{F}(\mathfrak{m}^n)$ is indeed a group. Notice that $\widehat{\mathbb{G}}_a(\mathfrak{m})$ is just $\mathfrak{m}$ with the usual addition and $\widehat{\mathbb{G}}_m(\mathfrak{m})$ is isomorphic to the group of 1-units $1 + \mathfrak{m}$.

Theorem 3.80. *For $n \geq 1$ the identity map on sets induces an isomorphism*

$$\mathcal{F}(\mathfrak{m}^n)/\mathcal{F}(\mathfrak{m}^{n+1}) \to \mathfrak{m}^n/\mathfrak{m}^{n+1}.$$

Proof. Bijectivity is obvious since the sets are the same. Thus it is enough to show that the map is a homomorphism. For $x, y \in \mathfrak{m}^n$:

$$x \oplus_{\mathcal{F}} y = F(x, y) = x + y + \cdots \equiv x + y \pmod{\mathfrak{m}^{n+1}}. \qquad \square$$

We would like to have something like a formal logarithm which linearizes the formal group. It turns out that there exists such an object, though we have to introduce another object first.

A *differential form* on a formal group $\mathcal{F}/R$ is just an expression $P(T)\,\mathrm{d}T$ where $P(T) \in R[\![T]\!]$. We are interested in differential forms that respect the group law:

Definition 3.81. An *invariant differential* on $\mathcal{F}/R$ is a differential form $\omega(T) = P(T)\,\mathrm{d}T$ such that

$$w \circ F(T, S) = \omega(T),$$

i.e. $P(F(T,S))F_X(T,S) = P(T)$, where $F_X(X,Y)$ is the formal partial derivate of F with respect to the first variable. It is called *normalized* if $P(0) = 1$.

Theorem 3.82. *Let $\mathcal{F}/R$ be a formal group. Then there exists a unique normalized invariant differential ω on $\mathcal{F}/R$. It is given by*

$$\omega = F_X(0, T)^{-1}\,\mathrm{d}T.$$

Further every invariant differential on $\mathcal{F}/R$ is of the form $a\omega$ for some $a \in R$.

Proof. If $P(T)\,\mathrm{d}T$ is an invariant differential, then by definition

$$P(F(T, S))F_X(T, S) = P(T).$$

Putting $T = 0$ gives (using $F(0, S) = S$)

$$P(S)F_X(0, S) = P(0).$$

Since $F_X(0, S) = 1 + \cdots$, it is invertible in $R[\![S]\!]$. Thus $P(T)$ is fully determined by $P(0)$ and every possible invariant differential has to be of the form $a\omega$ with $a \in R$ and ω as in the statement of the theorem. Since ω is already normalized, we only have to show that it is invariant, i.e.

$$F_X(0, F(T, S))^{-1}F_X(T, S) = F_X(0, T)^{-1}.$$

By differentiating the associative law $F(U, F(T, S)) = F(F(U, T), S)$ with respect to U we obtain

$$F_X(U, F(T, S)) = F_X(F(U, T), S)F_X(U, T).$$

Setting $U = 0$ yields the desired result. $\qquad \square$

The unique normalized invariant differential on $\widehat{\mathbb{G}}_a$ is $\omega = \mathrm{d}T$. On $\widehat{\mathbb{G}}_m$ it is $\omega = (1 + T)^{-1}\,\mathrm{d}T = (1 - T + T^2 - \cdots)\,\mathrm{d}T$.

By integrating ω we would like to get a homomorphism from $\mathcal{F}$ to $\widehat{\mathbb{G}}_a$. Unfortunately, integrating T^n gives $\frac{T^{n+1}}{n+1}$ which might not be well defined in R. So first of all we will have to restrict to $\mathrm{char}(R) = 0$, so that $n + 1 \neq 0$ for all n. However $n + 1$ could still fail to be invertible in R. One possibility to proceed is to go from R to $R \otimes \mathbb{Q}$. However we will restrict ourselves even further: For the rest of this section let K be a local field of characteristic zero complete with respect to the normalized discrete valuation v and $R = \mathcal{O}_v$ its ring of integers.

Definition 3.83. Let $\omega = (1 + \sum_{n \geq 1} c_n T^n)\, dT$ be the normalized invariant differential of $\mathcal{F}/R$ (where R is the ring of integers of a local field K). Then the *formal logarithm* of $\mathcal{F}/R$ is the power series

$$\log_{\mathcal{F}}(T) = \int \omega = T + \sum_{n \geq 1} \frac{c_n}{n+1} T^{n+1} \in K[\![T]\!].$$

The unique power series $\exp_{\mathcal{F}}(T) \in K[\![T]\!]$ with

$$\log_{\mathcal{F}} \circ \exp_{\mathcal{F}}(T) = \exp_{\mathcal{F}} \circ \log_{\mathcal{F}}(T) = T$$

is called the *formal exponential* of $\mathcal{F}/R$. (It exists by lemma 3.77.)

The formal logarithm of $\widehat{\mathbb{G}}_m$ is given by

$$\log_{\widehat{\mathbb{G}}_m}(T) = \int \frac{dT}{1+T} = \sum_{n \geq 1} \frac{(-1)^{n+1}}{n} T^n.$$

and the formal exponential by

$$\exp_{\widehat{\mathbb{G}}_m}(T) = \sum_{n \geq 1} \frac{1}{n!} T^n.$$

So the names "logarithm" and "exponential" are indeed justified. (The "identity" is at $T = 0$, so in terms of the usual series these series are $\log(1+T)$ and $\exp(T) - 1$.)

Proposition 3.84. *The formal exponential is given by a power series of the form*

$$\exp_{\mathcal{F}}(T) = \sum_{n \geq 1} \frac{a_n}{n!} T^n,$$

where $a_n \in R$ and $a_1 = 1$.

Proof. This is a direct consequence of [Sil92, lemma IV.5.4]. $\qquad\square$

Theorem 3.85. *The map $\log_{\mathcal{F}} \colon \mathcal{F} \to \widehat{\mathbb{G}}_a$ is an isomorphism of formal groups over K.*

Proof. The normalized invariant differential ω satisfies

$$\omega(F(T,S)) = \omega(T).$$

Integrating with respect to T gives

$$\log_{\mathcal{F}} F(T,S) = \log_{\mathcal{F}}(T) + f(S)$$

for some "constant of of integration" $f(S) \in K[\![S]\!]$. Putting $T = 0$, we see that $f(S) = \log_{\mathcal{F}}(S)$, and hence that $\log_{\mathcal{F}}$ is a homomorphism. Its inverse is $\exp_{\mathcal{F}}$, so it is an isomorphism. $\qquad\square$

Theorem 3.86. *Let $\mathcal{F}/R$ be a formal group.*

1. *The formal logarithm of $\mathcal{F}$ induces a homomorphism*

$$\log_{\mathcal{F}} \colon \mathcal{F}(\mathfrak{m}) \to K^+.$$

2. *Let $p \in \mathbb{Z}$ be a prime with $v(p) > 0$ and let $r > \frac{v(p)}{p-1}$ be an integer. Then the formal logarithm induces an isomorphism*

$$\log_{\mathcal{F}} \colon \mathcal{F}(\mathfrak{m}^r) \to \widehat{\mathbb{G}}_a(\mathfrak{m}^r) = \mathfrak{m}^r.$$

Proof.

1. We only have to show that the function is well defined, i.e. that the power series defining $\log_{\mathcal{F}}(x)$ converges for every $x \in \mathfrak{m}$. By definition we have

$$\log_{\mathcal{F}}(T) = \sum_{n \geq 1} \frac{a_n}{n} T^n \quad \text{with } a_n \in R.$$

Let $p \in \mathbb{Z}$ be a prime with $v(p) > 0$. Since $a_n \in R$, we have for $x \in \mathfrak{m}$:

$$v(\frac{a_n}{n} x^n) \geq nv(x) - v(n) \geq n - (\log_p n)v(p).$$

For $n \to \infty$ this tends to ∞ and therefore the power series converges.

2. It suffices to show that for $x \in \mathfrak{m}^r$ both $\log_{\mathcal{F}}$ and $\exp_{\mathcal{F}}$ converge and lie in $\mathfrak{m}^r$. In order to do this let

$$g(T) = \sum_{n \geq 1} \frac{b_n}{n!} T^n$$

be any power series with $b_n \in R$ and $b_1 \in R^*$. We will show that if $v(x) > \frac{v(p)}{p-1}$ then the series converges and $v(g(x)) = v(x)$. Like above and using [Sil92, lemma IV.6.2] for the second estimation

$$v\left(\frac{b_n}{n!} x^n\right) \geq nv(x) - v(n!) \geq nv(x) - (n-1)\frac{v(p)}{p-1} \geq v(x) + (n-1)\left(v(x) - \frac{v(p)}{p-1}\right).$$

For $n \to \infty$ this tends to infinity, so the series converges. Further for $n \geq 2$ the estimate gives

$$v\left(\frac{b_n}{n!} x^n\right) > v(x).$$

Hence the leading term determines $v(g(x))$. $\qquad\square$

Having worked through the general theory we can start to apply it to elliptic curves. We will try to capture the elliptic curve E and its group law "close to $\mathcal{O}$" in a power series. Since $\mathcal{O}$ is outside our usual affine subset of the curve, we need to choose another affine piece. Since $\mathcal{O} = [0 : 1 : 0]$ it is natural to make the following change of coordinates:

$$z = -\frac{x}{y} \qquad w = -\frac{1}{y}.$$

This takes $\mathcal{O}$ to $(z, w) = (0, 0)$. Now z has a zero of order 1 at $\mathcal{O}$ and hence is a local uniformizer. The usual Weierstraß equation 2.3 of E is transformed to

$$w = z^3 + a_1 zw + a_2 z^2 w + a_3 w^2 + a_4 zw^2 + a_6 w^3 = f(z, w).$$

We want to expand w as a power series in z, so we resubstitute $f(z, w)$ for w in the equation to get $w = f(z, f(z, w))$ and iterate the process. More formally we define recursively

$$f_1(z, w) = f(z, w) \quad \text{and} \quad f_{n+1}(z, w) = f(z, f_n(z, w))$$

and look at the limit

$$w(z) = \lim_{n \to \infty} f_n(z, 0)$$

in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6][\![z]\!]$, provided it makes sense. (This idea is not unique to elliptic curves, see [Sha94a, section II.2.2] for the theoretical background.)

Theorem 3.87. *The procedure just described gives a power series*

$$w(z) = z^3(1 + A_1 z + A_2 z^2 + \cdots) \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][\![z]\!].$$

Further $w(z)$ is the unique power series satisfying $w(z) = f(z, w(z))$.

Proof. See [Sil92, proposition IV.1.1]. $\qquad\square$

We can use this to get Laurent series for x, y and the invariant differential ω with coefficients in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$:

$$x(z) = \frac{z}{w(z)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z - (a_4 + a_1 a_3)z^2 + \cdots$$

$$y(z) = \frac{-1}{w(z)} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + (a_4 + a_1 a_3)z + \cdots$$

$$\omega(z) = \left(1 + a_1 z + (a_1^2 + a_2)z^2 + (a_1^3 + 2a_1 a_2 + 2a_3)z^3 + \cdots\right)\,\mathrm{d}z$$

By construction, $(x(z), y(z))$ is still a solution to the Weierstraß equation

$$E\colon y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

If K is a local field and all a_i are in $R = \mathcal{O}_v$, then these Laurent series converge for every $z \in \mathfrak{m}$. Hence we get a map

$$\mathfrak{m} \to E(K)$$
$$z \mapsto (x(y),\, y(z))$$

(3.9)

which is injective (its inverse is $z = -\frac{x}{y}$).

Now that we obtained an expansion of the curve around $\mathcal{O}$ we take a closer look at the group law. We will emulate the calculations done in section 2.1 and apply the group law in the (z, w)-plane. Let $w_i = w(z_i)$. Then the slope of the line connecting (z_1, w_1) and (z_2, w_2) is

$$\lambda = \lambda(z_1, z_2) = \frac{w_2 - w_1}{z_2 - z_1} = \sum_{n=3}^{\infty} A_{n-3} \frac{z_2^n - z_1^n}{z_2 - z_1} \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][\![z_1, z_2]\!].$$

Set $\nu = \nu(z_1, z_2) = w_1 - \lambda z_1 \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][\![z_1, z_2]\!]$, so that the line connecting the two points is given by $w = \lambda z + \nu$. Substituting this into the Weierstrass equation yields a cubic in z of which we know the two roots z_1 and z_2. Using Viète's formulas we see that the third root z_3 can be expressed as

$$z_3 = z_3(z_1, z_2) = -z_1 - z_2 + \frac{a_1 \lambda + a_3 \lambda^2 - a_2 \nu - 2a_4 \lambda \nu - 3a_6 \lambda^2 \nu}{1 + a_2 \lambda + a_4 \lambda^2 + a_6 \lambda^3} \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][\![z_1, z_2]\!].$$

For the group law on E we must have $(z_1, w_1) \oplus (z_2, w_2) \oplus (z_3, w_3) = \mathcal{O}$, so in order to add the first two we must take the inverse of (z_3, w_3). In the (x, y)-plane inverses are given by $(x, -y - a_1 x - a_3)$, so the inverse of (z, w) has z-coordinate

$$i(z) = -\frac{x(z)}{-y(z) - a_1 x(z) - a_3} \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][\![z]\!].$$

Finally we can write the formal group law

$$F(z_1, z_2) = i(z_3(z_1, z_2)) = z_1 + z_2 + a_1 z_1 z_2 + \cdots \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][\![z_1, z_2]\!].$$

From the corresponding properties of the elliptic curve group law we see that $F(z_1, z_2)$ is indeed a formal group law:

Definition 3.88. Let E be an elliptic curve given by a Weierstraß equation with coefficients in R. The power series we have just described gives the *formal group associated to E* over R. It is denoted by $\widehat{E}$.

The above expansion of the invariant differential of E gives the unique normalized invariant differential of $\widehat{E}$. As we have already seen (3.9), we have an injective homomorphism $\widehat{E}(\mathfrak{m}) \to E(K)$ given by $z \mapsto (x(z), y(z))$. This map will play an important role in the next section.

3.4.3 Reduction mod π

We can now finally study elliptic curves over a local field K. In the general theory one breaks up the "big" elliptic curve $E(K)$ into "smaller" parts, one of them being an elliptic curve over the residue field. Then one studies the individual parts and hopes to learn something about the whole curve. We will however use the theory in the opposite way: Starting from an elliptic curve $\widetilde{E}$ over the (finite) residue field k of K

we will go up to an elliptic curve E over K and use this new curve to derive information about $\widetilde{E}$. The advantage of working over K is that it will have characteristic 0 and that we can attach the formal group $\widehat{E}$ where we can do calculations. Therefore this chapter contains only parts of the theory of elliptic curves over local fields. The remaining pieces can be found in any standard reference about elliptic curves like [Sil92] or [Hus04].

Again let K be a local field that is complete with respect to a valuation v with ring of integers $R = \mathcal{O}_v$. Further let $\mathfrak{m} = \pi R$ be the maximal ideal of R with uniformizing parameter π and $k = R/\mathfrak{m}$ the residue field of K. As usual, E denotes an elliptic curve over K.

Let $P = [x_0 : x_1 : \cdots : x_n] \in \mathbb{P}^n(K)$. When we multiply every coordinate with the common denominator, we get a representation of P where all coordinates are in R. We can assume that at least one of the coordinates is in R^*. Then we can reduce every coordinate separately modulo $\mathfrak{m}$ to get a well-defined point $\widetilde{P} = [\widetilde{x}_0 : \widetilde{x}_1 : \cdots : \widetilde{x}_n] \in \mathbb{P}^n(k)$. Hence we have a *reduction map*

$$\widetilde{\cdot}\colon \mathbb{P}^n(K) \to \mathbb{P}^n(k).$$

This map is also called *reduction modulo π* and we will sometimes also denote it by π. We could try to apply this to the points of E. However the result depends on the particular embedding of E in $\mathbb{P}^3(K)$, i.e. its Weierstrass equation.

If $a_1, \cdots, a_6$ are the coefficients of a Weierstraß equation of E and u their common denominator, the change of coordinates $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ will result in a Weierstraß equation where all coefficients are in R. Hence the transformed discriminant Δ satisfies $v(\Delta) \geq 0$. Since v is discrete we can look for an equation of E defined over R where $v(\Delta)$ is as small as possible.

Definition 3.89. A Weierstraß equation of E/K is called a *minimal Weierstraß equation for E* if $v(\Delta)$ is minimal under the condition $a_1, a_2, a_3, a_4, a_6 \in R$. In this case Δ is the *minimal discriminant of E*.

Theorem 3.90.

1. *Every elliptic curve E/K has a minimal Weierstraß equation. It is unique up to a change of coordinates*
$$x = u^2 x' + r \qquad y = u^3 y' + u^2 s x' + t$$
with $u \in R^*$ and $r, s, t \in R$.

2. *The invariant differential*
$$\omega = \frac{\mathrm{d}x}{2y + a_1 x + a_3}$$
associated to a minimal Weierstraß equation is unique up to multiplication with an element of R^*.

Proof. The existence has already been discussed. The uniqueness properties can be deduced by explicitly calculating how the Weierstraß coefficients change under a change of coordinates, see [Sil92, proposition VI.1.3b]. □

Proposition 3.91. *If $\operatorname{char} K \neq 2, 3$ then a Weierstraß equation of E is minimal if and only if all $a_i \in R$ and $v(c_4) < 4$ or $v(c_6) < 6$.*

Definition 3.92. Let E/K have minimal Weierstraß equation
$$E\colon y^3 + a_1 yx + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$
Then the (possibly singular) curve $\widetilde{E}/k$ given by
$$\widetilde{E}\colon y^3 + \widetilde{a}_1 yx + \widetilde{a}_3 y = x^3 + \widetilde{a}_2 x^2 + \widetilde{a}_4 x + \widetilde{a}_6$$
is called the *reduction of E modulo π* and E is called a *lift of $\widetilde{E}$ to K*.

By theorem 3.90 the reduced equation is unique up to a standard change of coordinates for Weierstraß equations over k and hence the curve $\widetilde{E}$ is well defined as an abstract curve. Further from the reduction map on $\mathbb{P}^2(K)$ we get a *reduction map* $E(K) \to \widetilde{E}(k)$. The curve $\widetilde{E}$ might be non-singular or not, but in any case the set $\widetilde{E}_{ns}(k)$ of nonsingular points forms a group.

Definition 3.93.

1. If $\widetilde{E}$ is non-singular, then E has *good* (or *stable*) *reduction*.
2. If $\widetilde{E}$ has a node, then E has *multiplicative* (or *semi-stable*) *reduction*.
3. If $\widetilde{E}$ has a cusp, then E has *additive* (or *unstable*) *reduction*.

Theorem 3.94. *Let E/K be an elliptic curve, Δ its minimal discriminant and c_4 the usual combination of the $a_i s$ (2.4) of a minimal Weierstraß equation of E.*

1. *E has good reduction if and only if $v(\Delta) = 0$ (i.e. $\widetilde{\Delta} \neq 0$). In this case $\widetilde{E}/k$ is an elliptic curve.*
2. *E has multiplicative reduction if and only if $v(\Delta) > 0$ and $v(c_4) = 0$. In this case $\widetilde{E}_{ns}(\bar{k}) \cong \bar{k}^*$.*
3. *E has additive reduction if and only if $v(\Delta) > 0$ and $v(c_4) > 0$. In this case $\widetilde{E}_{ns}(\bar{k}) \cong \bar{k}^+$.*

Proof. This follows directly from the general theorems and conditions in section 2.1. □

Definition 3.95. The *filtration of $E(K)$ with respect to v* is given by the sets

$$E_n(K) = \{P \in E(K) : v(x(P)) \leq -2n\}$$

for $n \geq 1$ and

$$E_0(K) = \{P \in E(K) : \widetilde{P} \in \widetilde{E}_{ns}(k)\}.$$

Lemma 3.96. *The set $E_0(K)$ is a subgroup of $E(K)$ and the reduction map $\pi_{|_{E_0(K)}} : E_0(K) \to \widetilde{E}_{ns}(k)$ is a homomorphism.*

Proof. The reduction map takes lines into lines and maps $[0 : 1 : 0] \in \mathbb{P}^2(K)$ to $[0 : 1 : 0] \in \mathbb{P}^2(k)$. Hence it is compatible with the elliptic curve group law. □

Lemma 3.97. *$E_1(K) = \{P \in E(K) : \widetilde{P} = \widetilde{\mathcal{O}}\} = \ker \pi_{|_{E_0(K)}}$. In particular $E_1(K)$ is a subgroup of $E_0(K)$.*

Proof. If $(x, y) \in \{P \in E(K) : \widetilde{P} = \widetilde{\mathcal{O}}\}$, then (x, y) reduces modulo π to the point at infinity on $\widetilde{E}(k)$. Hence $v(x) < 0$ or $v(y) < 0$. But from the Weierstraß equation $y^2 + \cdots = x^3 + \cdots$ we have

$$2v(y) = 3v(x).$$

Thus they must both be negative and $v(y) = \frac{3}{2}v(x)$ a whole number, i.e. $v(x) \leq -2$.

The other inclusion follows by the same argument. □

Theorem 3.98. *The reduction map induces an exact sequence*

$$0 \to E_1(K) \to E_0(K) \to \widetilde{E}_{ns}(k) \to 0.$$

Proof. By the lemmata we only have to show that the reduction map is surjective. Let $f(x, y) = 0$ be a minimal Weierstraß equation of E, $\widetilde{f}(x, y) = 0$ the corresponding reduced equation and choose any point $\widetilde{P} = (\alpha, \beta) \in \widetilde{E}_{ns}(k)$. Assume that $\frac{\partial \widetilde{f}}{\partial x}(\widetilde{P}) \neq 0$ (the case $\frac{\partial \widetilde{f}}{\partial y}(\widetilde{P}) \neq 0$ is analogous). Let $y_0 \in R$ be any lift of β, i.e. $\widetilde{y}_0 = \beta$. When reduced modulo π the equation $\widetilde{f}(x, y_0) = 0$ has the simple root α since $\frac{\partial \widetilde{f}}{\partial x}(\alpha, \widetilde{y}_0) \neq 0$. Thus by Hensel's lemma 3.67 α can be lifted to $x_0 \in R$ such that $f(x_0, y_0) = 0$. Hence the point $P = (x_0, y_0) \in E_0(K)$ reduces to $\widetilde{P}$. □

Theorem 3.99. *Let E/K be given by a minimal Weierstraß equation. Then the sets $E_n(K)$ ($n \geq 1$) are groups and the maps*

$$\vartheta_n \colon \widehat{E}(\mathfrak{m}^n) \to E_n(K)$$

$$z \mapsto \left(\frac{z}{w(z)}, -\frac{1}{w(z)} \right)$$

(and $z = 0 \mapsto \mathcal{O}$) are isomorphisms.

Proof. First we will show that the maps are well-defined and bijective. We already know that ϑ_n is well-defined and injective as a map to $E(K)$ and has inverse $(x,y) \mapsto -\frac{x}{y}$ on the image. Since $w(z) = z^3(1 + \cdots) \in R[\![z]\!]$ we have $v(x(\vartheta_n(z))) = -2v(z) \leq -2n$ and hence $\vartheta_n(\widehat{E}(\mathfrak{m}^n)) \subseteq E_n(K)$. Further for $(x,y) \in E_n(K)$ we know from the proof of lemma 3.97 that $3v(x) = 2v(y) = -6r$ with $r \geq n$. Thus $v(-\frac{x}{y}) = -2r + 3r \geq n$ and $-\frac{x}{y} \in \mathfrak{m}^n$. Therefore the map is surjective.

The set $E_1(K)$ is a group and ϑ_1 is a homomorphism. For all $n > 1$ the sets $\widehat{E}(\mathfrak{m}^n)$ are subgroups of $\widehat{E}(\mathfrak{m})$ and the maps ϑ_n are just the restrictions of ϑ_1. Because they are homomorphisms as maps to $E_1(K)$ the sets $E_n(K)$ must be closed under the group operations. $\qquad\square$

Corollary 3.100. *For $n \geq 1$ there is an exact sequence*

$$0 \to E_{n+1}(K) \to E_n(K) \to k^+ \to 0.$$

Proof. By the last theorem and 3.80 there are isomorphisms

$$E_n(K)/E_{n+1}(K) \cong \widehat{E}(\mathfrak{m}^n)/\widehat{E}(\mathfrak{m}^{n+1}) \cong \mathfrak{m}^n/\mathfrak{m}^{n+1} \cong R/\mathfrak{m} = k^+. \qquad\square$$

The whole situation is summarized in the following commutative diagram (note that the maps marked id are not homomorphisms, only the factor groups are homomorphic).

$$
\begin{array}{ccccccccc}
\cdots & \longrightarrow & E_3(K) & \longrightarrow & E_2(K) & \longrightarrow & E_1(K) & \longrightarrow & E_0(K) \xrightarrow{\ \mathrm{mod}\ \pi\ } \widetilde{E}_{ns}(k) \\
 & & \cong \big\uparrow & & \cong \big\uparrow & & \cong \big\uparrow & & \\
\cdots & \longrightarrow & \widehat{E}(\mathfrak{m}^3) & \longrightarrow & \widehat{E}(\mathfrak{m}^2) & \longrightarrow & \widehat{E}(\mathfrak{m}) & & \\
 & & \mathrm{id} \big\uparrow & & \mathrm{id} \big\uparrow & & \mathrm{id} \big\uparrow & & \\
\cdots & \longrightarrow & \mathfrak{m}^3 & \longrightarrow & \mathfrak{m}^2 & \longrightarrow & \mathfrak{m} & \longrightarrow & k^+
\end{array}
$$

3.4.4   The Canonical Lift

Assume that we are given an elliptic curve $E/\mathbb{F}_q$. Then we can easily lift it to a curve $\mathcal{E}$ over $\mathbb{Q}_q$. However, there are many possible lifts of E and in the last section we have only seen how one can canonically reduce a curve. First we state what we would expect from a canonical lift:

Definition 3.101. The *canonical lift* of an elliptic curve $E/\mathbb{F}_q$ is an elliptic curve $\mathcal{E}/\mathbb{Q}_q$ that satisfies:

1. $\mathcal{E}$ is a lift of E;
2. $\mathrm{End}(E) \cong \mathrm{End}(\mathcal{E})$ as a ring.

Theorem 3.102 ([Deu41])**.** *The canonical lift of an ordinary elliptic curve always exists and is unique up to isomorphism.*

Theorem 3.103 ([Mes72])**.** *Let E_1, E_2 be ordinary elliptic curves over $\mathbb{F}_q$ and $\mathcal{E}_1$, $\mathcal{E}_2$ their respective canonical lifts. Then*

$$\mathrm{Hom}(E_1, E_2) \cong \mathrm{Hom}(\mathcal{E}_1, \mathcal{E}_2).$$

A consequence of this is that the Frobenius lifts:

Corollary 3.104. *Let $E/\mathbb{F}_q$ be an elliptic curve and $\phi_p \colon E \to E^{(p)}$ the pth-power Frobenius morphism. Then the Frobenius substitution Σ of $\mathbb{Q}_q$ induces an isogeny $\Sigma \colon \mathcal{E} \to \mathcal{E}^{(p)}$ of the corresponding canonical lifts.*

Lubin, Serre and Tate showed how one can explicitly compute the canonical lift by solving a system of equations (e.g. with Newton iteration). Note that from the knowledge of $J = j(\mathcal{E})$ it is easy to get a Weierstraß equation: Set $A = \frac{3J}{1728-J}$ and $B = \frac{2J}{1728-J}$, then an equation for $\mathcal{E}$ is $y^2 = x^3 + Ax + B$.

Theorem 3.105 ([LST64]). *Let $E/\mathbb{F}_q$, $q = p^e$, have j-invariant $j(E) \notin \mathbb{F}_{p^2}$ (in particular E is ordinary). Let Σ be the Frobenius substitution of $\mathbb{Q}_q$ and $\Phi_p(x, y)$ the pth modular polynomial. Then the system of equations*

$$\Phi_p(x, \Sigma(x)) = 0$$
$$x \equiv j(E) \pmod{p} \tag{3.10}$$

has a unique solution $J \in \mathbb{Z}_q$, which is the j-invariant of the canonical lift $\mathcal{E}$ of E.

Proof. Let $\phi_p \colon E \to E^{(p)}$ be the pth-power Frobenius morphism and let $\Sigma \colon \mathcal{E} \to \mathcal{E}^{(p)}$ be its canonical lift. Then $\Sigma(j(\mathcal{E}))$ is the j-invariant of $\mathcal{E}^{(p)}$ and thus by theorem 3.33, $\Phi_p(J, \Sigma(J)) = 0$. By the definition of a lift, $J \in \mathbb{Z}_q$.

We will now show uniqueness of the solution. Using the Kronecker relation 3.34 we see that for any solution J of (3.10),

$$\frac{\partial}{\partial X}\Phi(J, \Sigma(J)) \equiv j(E)^p - j(E)^p = 0 \pmod{p}, \tag{3.11}$$

$$\frac{\partial}{\partial Y}\Phi(J, \Sigma(J)) \equiv j(E) - j(E)^{p^2} \neq 0 \pmod{p} \tag{3.12}$$

Here we use that $j(E) \notin \mathbb{F}_{p^2}$. Let J_1, J_2 be two different solutions. By Taylor expansion at $(J_1, \Sigma(J_1))$ there exist $\alpha, \beta \in \mathbb{Z}_q$ such that

$$0 = \Phi(J_2, \Sigma(J_2)) = (J_2 - J_1)\left(\frac{\partial}{\partial X}\Phi\left(J_1, \Sigma\left(J_1\right)\right) + \alpha\left(J_2 - J_1\right)\right) + $$
$$\left(\Sigma\left(J_2\right) - \Sigma\left(J_1\right)\right)\left(\frac{\partial}{\partial Y}\Phi\left(J_1, \Sigma\left(J_1\right)\right) + \beta\left(\Sigma\left(J_2\right) - \Sigma\left(J_1\right)\right)\right) \tag{3.13}$$

We have $J_2 - J_1 \in p\mathbb{Z}_q$. Write $J_2 - J_1 = \gamma p^n$ such that $\gamma \in \mathbb{Z}_q^*$. Then $\Sigma(J_2 - J_1) = \Sigma(\gamma p^n) = \gamma' p^n$ for some $\gamma' \in \mathbb{Z}_q^*$. Therefore from (3.13),

$$0 = p^n\left(\gamma\frac{\partial}{\partial X}\Phi(J_1, \Sigma(J_1)) + \gamma'\frac{\partial}{\partial Y}\Phi(J_1, \Sigma(J_1)) + \delta p^n\right)$$

for some $\delta \in \mathbb{Z}_q$. Now $p^n \neq 0$, so the expression in the parenthesis has to vanish. Using (3.11) we deduce

$$0 = \gamma\frac{\partial}{\partial X}\Phi(J_1, \Sigma(J_1)) + \gamma'\frac{\partial}{\partial Y}\Phi(J_1, \Sigma(J_1)) + \delta p^n \equiv \gamma'\frac{\partial}{\partial Y}\Phi(J_1, \Sigma(J_1)) \pmod{p}$$

which is a contradiction to (3.12). $\qquad\qquad\square$

Chapter 4

More on Elliptic Divisibility Sequences and Elliptic Nets

In section 3.2.1 we already introduced elliptic divisibility sequence on our way to the definition of the division polynomials for elliptic curves. Besides being interesting on their own (see for example [EvSW03]) they will turn out to have several connections with the elliptic curve discrete logarithm problem. In the present chapter we will study them more closely by first generalizing them to elliptic nets and then specializing to a certain class of sequences and nets.

4.1 Elliptic Nets

Following Stange [Sta07a] we will now generalize elliptic divisibility sequences to higher dimensions.

Definition 4.1. Let A be a finitely generated free Abelian group, R an integral domain and n an integer. An *elliptic net* is any map $W \colon A \to R$ that satisfies the following recurrence for all p, q, r, $s \in A$:

$$W(p+q+s)W(p-q)W(r+s)W(r)$$
$$+ W(q+r+s)W(q-r)W(p+s)W(p)$$
$$+ W(r+p+s)W(r-p)W(q+s)W(q) = 0 \quad (4.1)$$

and such that $W(0) = 0$[1]. The rank of A is also called the *rank* of the elliptic net W. An elliptic net of rank one is called a *generalized elliptic sequence*.

We begin our study of elliptic nets with some simple properties.

Lemma 4.2. *Let $W \colon A \to R$ be an elliptic net. Then $W(-z) = -W(z)$ for all $z \in A$.*

Proof. If $W(z) = W(-z) = 0$ then we are already done. If $W(z) \neq 0$, set $p = q = z$, $r = s = 0$ so that (4.1) reduces to $0 + W(z)^4 + W(z)^3 W(-z) = 0$, i.e. $W(z) = -W(-z)$. If $W(-z) \neq 0$, set $p = q = -z$, $r = s = 0$ to get the same result. $\square$

Lemma 4.3. *A generalized elliptic sequence $W \colon \mathbb{Z} \to R$ with $W(1) = \pm 1$ is an elliptic sequence.*

Proof. Let $s = 0$, $r = 1$, $p = m$ and $q = n$ to get the EDS recurrence relation. $\square$

Lemma 4.4. *Let $W \colon A \to R$ be an elliptic net and $B \leq A$ a subgroup. Then the restriction $W|_B$ of W to B is also an elliptic net. It is called a* subnet *of W.*

Like in the case of EDS we can get elliptic nets from elliptic curves. First we take a look at the complex case:

---

[1]Stange does not demand that $W(0) = 0$. Instead she proves that this is always the case. Unfortunately her proof does not work for $\operatorname{char}(R) = 3$.

Definition 4.5. Let $\Lambda \subseteq \mathbb{C}$ be a lattice. For $\mathsf{v} = (v_1, \ldots, v_n) \in \mathbb{Z}^n$ define a function Ω_{v} on $\mathbb{C}^n$ in variables $\mathsf{z} = (z_1, \ldots, z_n)$ by

$$\Omega_{\mathsf{v}}(\mathsf{z}; \Lambda) = \frac{\sigma(v_1 z_1 + \cdots + v_n z_n; \Lambda)}{\displaystyle\prod_{i=1}^{n} \sigma(z_i; \Lambda)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j} \prod_{1 \le i < j \le n} \sigma(z_i + z_j; \Lambda)^{v_i v_j}}$$

(and $\Omega_0 \equiv 0$).

In particular for $n = 1$ this definition agrees with the $\psi_n(z; \Lambda)$ of 3.24. In rank 2 these functions are of the following form:

$$\Omega_{m,n}(z, w; \Lambda) = \frac{\sigma(mz + nw; \Lambda)}{\sigma(z; \Lambda)^{m^2 - mn} \sigma(z + w; \Lambda)^{mn} \sigma(w; \Lambda)^{n^2 - mn}}$$

Like in the rank one case one shows

Theorem 4.6. *The functions Ω_{v} are elliptic functions with respect to Λ in each variable.*

The following two useful statements can be checked by direct calculations using the theory of elliptic functions we developed in section 3.1.

Theorem 4.7. *The divisor of Ψ_{v} as a function of z_1 is*

$$\left(\sum_{j=2}^{n} \left[-\frac{v_j}{v_1} \right] z_j \right) - \sum_{j=2}^{n} v_1 v_j (-z_j) - \left(v_1^2 - \sum_{j=2}^{n} v_1 v_j \right) (0).$$

Theorem 4.8. *Let $\mathsf{v} \in \mathbb{Z}^m$ and $\mathsf{z} \in \mathbb{C}^n$. Further let $T \in \mathbb{Z}^{n \times n}$ with transpose T^T. Then*

$$\Omega_{\mathsf{v}}(T^T(\mathsf{z}); \Lambda) = \frac{\Omega_{T(\mathsf{v})}(\mathsf{z}; \Lambda)}{\displaystyle\prod_{i=1}^{n} \Omega_{T(\mathsf{e}_i)}(\mathsf{z}; \Lambda)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j} \prod_{1 \le i < j \le n} \Omega_{T(\mathsf{e}_i + \mathsf{e}_j)}(\mathsf{z}; \Lambda)^{v_i v_j}},$$

where the e_i are the standard basis of $\mathbb{Z}^m$.

Theorem 4.9 ([Sta07a, theorem 4.5])**.** *Let $E/\mathbb{C}$ be an elliptic curve with associated lattice $\Lambda \subseteq \mathbb{C}$. Further choose points $P_1, \ldots, P_n$ on E and let $z_1, \ldots, z_n$ be the associated points in $\mathbb{C}$. Define a function $W : \mathbb{Z}^n \to \mathbb{C}$ by*

$$W(\mathsf{v}) = \Omega_{\mathsf{v}}(z_1, \ldots, z_n; \Lambda).$$

Then W is an elliptic net.

We would like to get something equivalent to the division polynomials ψ_n and indeed it is possible to define *net polynomials*. Unfortunately, the proof uses some more advanced parts of algebraic geometry than we introduced in chapter 1. It also relies on some complicated nested inductions for a recursive definition of the polynomials. Therefore we have to skip the proof and can only state the resulting theorem.

Theorem 4.10 ([Sta07a, theorem 6.1])**.** *Let E be an elliptic curve defined over K by*

$$f(x, y) = y^2 + \alpha_1 xy + \alpha_3 y - x^3 - \alpha_2 x^2 - \alpha_4 x - \alpha_6.$$

Let $n > 0$ be an integer. For all $\mathsf{v} \in \mathbb{Z}^n$ there are functions $\Psi_{\mathsf{v}} : E^n \to K$ in the ring

$$\mathbb{Z}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6][x_i, y_i]_{i=1}^{n}[(x_i - x_j)^{-1}]_{1 \le i < j \le n} / \langle f(x_i, y_i) \rangle_{i=1}^{n} \subseteq K(E^n)$$

such that

1. *$W(\mathsf{v}) = \Psi_{\mathsf{v}}$ is an elliptic net.*
2. *$\Psi_{\mathsf{v}} = 1$ whenever $\mathsf{v} = \mathsf{e}_i$ for some $1 \le i \le n$ or $\mathsf{v} = \mathsf{e}_i - \mathsf{e}_j$ for some $1 \le i < j \le n$.*
3. *Ψ_{v} vanishes at $\mathsf{P} = (P_1, \ldots, P_n) \in E^n$ if and only if $\mathsf{v} \cdot \mathsf{P} = \mathcal{O}$ on E (and v is not one of the vectors specified in 2).*

In the case of rank one, the Ψ_{v} agree with the division polynomials. Like there the following definition is natural:

Definition 4.11. Let E be an elliptic curve over K and choose non-zero points $P_1, \ldots, P_n \in E$ such that no two are equal or inverses. Then the map

$$W_{E,P_1,\ldots,P_n} \colon \begin{cases} \mathbb{Z}^n \to K \\ \mathsf{v} \mapsto \Psi_{\mathsf{v}}(P_1, \ldots, P_n) \end{cases}$$

is the *elliptic net associated to E and $P_1, \ldots, P_n$.*

Definition 4.12. Let $W \colon \mathbb{Z}^n \to K$ be an elliptic net associated to a curve. Then by theorem 4.10 (3) the zeros of W form a sublattice of $\mathbb{Z}^n$. It is called the *lattice of zero-apparition.*

Finally we can translate theorem 4.8 to elliptic nets.

Theorem 4.13. *Let $\mathsf{v} \in \mathbb{Z}^m$ and $\mathsf{P} \in E^n$. Further let $T \in \mathbb{Z}^{n \times n}$. Then*

$$W_{E,T^T(\mathsf{P})}(\mathsf{v}) = \frac{W_{E,\mathsf{P}}(T(\mathsf{v}))}{\displaystyle\prod_{i=1}^{n} W_{E,\mathsf{P}}(T(\mathsf{e}_i))^{2v_i^2 - \sum_{j=1}^{n} v_i v_j} \prod_{1 \leq i < j \leq n} W_{E,\mathsf{P}}(T(\mathsf{e}_i + \mathsf{e}_j))^{v_i v_j}},$$

4.2 Perfectly Periodic Sequences and Nets

Definition 4.14. An EDS is called *perfectly periodic* if it is periodic with respect to its rank of zero-apparition. Similarly, an elliptic net is *perfectly periodic* if it is periodic with respect to its lattice of zero-apparition.

Definition 4.15. A function $f \colon A \to B$ between two Abelian groups A and B is a *quadratic function* if the function $b \colon A \times A \to B$ defined by $b(x,y) = f(x+y) - f(x) - f(y)$ is bilinear. If f is also homogeneous of degree two with respect to multiplication by integers, it is called a *quadratic form.*

By symmetry, b is bilinear in the first coordinate if and only if it is bilinear in the second one. So the condition above is equivalent to $b(x, y + z) = b(x, y) + b(x, z)$ for all $x, y, z \in A$. Applying the definition of b to this equation we immediately get the following alternative definition of quadratic functions:

Lemma 4.16. *A function $f \colon A \to B$ is quadratic if and only if for all $x, y, z \in A$,*

$$f(x + y + z) - f(x + y) - f(y + z) - f(z + x) + f(x) + f(y) + f(z) = 0. \tag{4.2}$$

Lemma 4.17. *If $f \colon A \to B$ is a quadratic form, then*

1. *$f(0) = 0$;*
2. *$f(x) = f(-x)$ for all $x \in A$ and*
3. *$f(x + y) + f(x - y) = 2f(x) + 2f(y)$ for all $x, y \in A$ (*parallelogram law*).*

Proof. Let $x = y = z = 0$ in equation (4.2) to obtain $f(0) = 0$. Since f is homogeneous of degree 2, $f(-x) = (-1)^2 f(x) = f(x)$. Now use the original definition of quadratic functions to get

$$f(x + y) + f(x - y) = b(x, y) + f(x) + f(y) + b(x, -y) + f(x) + f(-y) = 2f(x) + 2f(y).$$

$\square$

Theorem 4.18. *Let $W \colon A \to K$ be an elliptic net and $f \colon A \to K^*$ a quadratic form. Then $W' \colon A \to K$ with $W'(\mathsf{v}) = f(\mathsf{v})W(\mathsf{v})$ is also an elliptic net.*

Proof. We use the parallelogram law and equation (4.2) to get (written multiplicatively in K^*)

$$f(p + q + s)f(p - q)f(r + s)f(r) = f(q + s)f(p + s)f(r + s)f(p)f(q)f(q)f(s)^{-1},$$

where the right hand side is symmetric in p, q, r. Hence

$$f(p + q + s)f(p - q)f(r + s)f(r) = f(q + r + s)f(q - r)f(p + s)f(p) = f(r + p + s)f(r - p)f(q + s)f(q).$$

Therefore multiplication with f does not change the validity of the elliptic net recurrence. $\square$

Definition 4.19. Two elliptic nets W and W' of rank n defined over K are called *equivalent* if there exists $k \in K^*$ and a quadratic form $f\colon A \to K^*$ with $W'(\mathsf{v}) = kf(\mathsf{v})W(\mathsf{v})$ for all $\mathsf{v} \in A$.

Surprisingly many elliptic nets in a finite field have an equivalent elliptic net that is perfectly periodic.

Theorem 4.20 ([LS08]). *Let $K = \mathbb{F}_q$ and E an elliptic curve defined over K. For all points $P \in E(K)$ of order relatively prime to $q-1$ and greater than 3 define*

$$\Phi(P) = \left(\frac{W_{E,P}(q-1)}{W_{E,P}(q-1+\mathrm{ord}(P))} \right)^{\frac{1}{\mathrm{ord}(P)^2}}. \tag{4.3}$$

Let $\mathsf{P} \in E(K)^n$ be a collection of non-zero points of a single subgroup of $E(K)$ having prime order greater than 3 and relatively prime to $q-1$ such that no two points are equal or inverses. Then $\Phi(\mathsf{v} \cdot \mathsf{P})$ forms a perfectly periodic elliptic net equivalent to $W_{E,\mathsf{P}}(\mathsf{v})$. Specifically,

$$\Phi(\mathsf{v} \cdot \mathsf{P}) = W_{E,\mathsf{P}}(\mathsf{v}) \prod_{i=1}^{n} \Phi(P_i)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j} \prod_{1 \le i < j \le n} \Phi(P_i + P_j)^{v_i v_j}.$$

In particular, if P is a point of prime order greater than 3 and relatively prime to $q-1$ then $\Phi([n]P)$ is a perfectly periodic EDS equivalent to $W_{E,P}(n)$ with

$$\Phi([n]P) = \Phi(P)^{n^2} W_{E,P}(n).$$

Proof. We will first prove the EDS case and then indicate how to proceed in the general case without explicitly calculating every single step.

In theorem 4.13 take $T = (l)$:

$$W_{E,[l]P}(n)W_{E,P}(l)^{n^2} = W_{E,P}(nl).$$

By symmetry,

$$W_{E,[n]P}(l)W_{E,P}(n)^{l^2} = W_{E,P}(nl).$$

Let $m = \mathrm{ord}(P)$. We combine the two formulas, isolate $W_{E,[l]P}(n)$ and use this with $l = q-1$ and $l = q-1+m$:

$$\frac{W_{E,[n]P}(q-1)W_{E,P}(n)^{(q-1)^2}}{W_{E,P}(q-1)^{n^2}} = W_{E,[q-1]P}(n) =$$

$$= W_{E,[q-1+m]P}(n) = \frac{W_{E,[n]P}(q-1+m)W_{E,P}(n)^{(q-1+m)^2}}{W_{E,P}(q-1+m)^{n^2}}$$

We are working in $\mathbb{F}_q^*$, so $W_{E,P}(n)^{q-1} = 1$. Thus rearranging yields

$$\Phi([n]P) = \Phi(P)^{n^2} W_{E,P}(n).$$

Hence by theorem 4.18, $\Phi([n]P)$ is an EDS. By definition, $\Phi([n]P)$ has period $\mathrm{ord}(P)$ witch is equal to the rank of zero-apparition of $W_{E,P}$ and $\Phi([n]P)$.

In the case of elliptic nets of rank n let m be the order of the subgroup containing all points of P. We will again use theorem 4.13: first with $T = \begin{pmatrix} v_1 & v_2 & \cdots & v_n \end{pmatrix}^T$ for

$$W_{E,\mathsf{P}}(l\mathsf{v}) = W_{E,\mathsf{v}\cdot\mathsf{P}}(l)W_{E,\mathsf{P}}(\mathsf{v})^{l^2},$$

and then with $T = l\,\mathrm{Id}_n$ for

$$W_{E,\mathsf{P}}(l\mathsf{v}) = W_{E,l\mathsf{P}}(\mathsf{v}) \prod_{i=1}^{n} W_{E,\mathsf{P}}(l\mathsf{e}_i)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j} \prod_{1 \le i < j \le n} W_{E,\mathsf{P}}(l\mathsf{e}_i + l\mathsf{e}_j)^{v_i v_j}.$$

Using $W_{E,\mathsf{P}}(l\mathsf{e}_i) = W_{E,P_i}(l)$ and $W_{E,\mathsf{P}}(l\mathsf{e}_i + l\mathsf{e}_j) = W_{E,P_i+P_j}(l)$ and combining the two equations above, we have

$$W_{E,l\mathsf{P}}(\mathsf{v}) = \frac{W_{E,\mathsf{v}\cdot\mathsf{P}}(l)W_{E,\mathsf{P}}(\mathsf{v})^{l^2}}{\displaystyle\prod_{i=1}^{n} W_{E,P_i}(l)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j} \prod_{1 \le i < j \le n} W_{E,P_i+P_j}(l)^{v_i v_j}}.$$

Like in the rank one case we set $l = q-1$ and $l = q-1+m$ and compare the two resulting equations to get the required result. We can easily check that the multiplicative factor is indeed a quadratic form. $\qquad\square$

In light of the preceding theorem we define

Definition 4.21. Let E be an elliptic curve defined over $K = \mathbb{F}_q$ and $P \in E(K)$ of prime order $m \geq 3$ with $\gcd(m, q - 1) = 1$. Then

$$\widetilde{W}_{E,P}(n) = \Phi([n]P)$$

is the *perfectly periodic elliptic divisibility sequence associated to E and P*.

The most important property of $\widetilde{W}_{E,P}$ is that by formula (4.3) we can calculate $\widetilde{W}_{E,P}(n)$ as a function of the point $[n]P$ without knowledge of n. We will exploit this property in section 7.6.

Chapter 5

Elliptic Curve Cryptography

So far we only considered the abstract theory of elliptic curves. Although we discussed some topics that do not normally appear in an introduction to elliptic curves, nothing directly related to cryptography. Yet the title of this thesis is "Mathematical Foundations of Elliptic Curve Cryptography". The previous chapters covered the mathematical foundations, so we will now have a look at the "cryptography" part.

Elliptic curve cryptography (ECC) was invented independently by Koblitz [Kob87] and Miller [Mil86b] in 1985. The groundwork for this simultaneous invention was laid by Schoof in the same year when he first described an efficient algorithm for counting the number of rational points on an elliptic curve defined over a finite field (see section 6.2.1). Another inspiration was the recent use of elliptic curves in Lenstra's Elliptic Curve Method (ECM) integer factorization algorithm [Len87].

The basic idea of ECC is simple: take any cryptographic algorithm that is defined over an arbitrary (cyclic) group and use it on the group of rational points of an elliptic curve over a finite field (or a cyclic subgroup of these points). Before 1985 these algorithms had only been applied on the multiplication groups of finite fields. However, advances in solving the discrete logarithm problem in finite fields (especially index calculus methods, see section 7.2.1) drastically reduced the security of these cryptography schemes. At the same time the security of the RSA method was gradually reduced, for example by Lenstra's ECM or a bit later by index calculus methods (algorithms for finite field discrete logarithm and integer factorization are often closely related). To provide high security the size of the underlying field had to be increased. The caused problem when computational resources were restricted, for example in smart cards. ECC promised to require lower field sizes for the same strength of encryption. Nevertheless there was severe opposition to the use of ECC. Many cryptographers thought that the elliptic curve discrete logarithm problem, on which ECC relies, had not been adequately examined to be used in for security. Also RSA had a very strong market position and for many people was synonymous with public key cryptography. Therefore it took several years before ECC was widely accepted. A detailed account of the history of ECC is given by Koblitz et al. in [KKM08].

For RSA it is currently recommended to use a key length of at least 2048 bits. This corresponds to an effective security of about 175 bits, i.e. using the best known method (the general number field sieve) it will take about 2^{175} operations to break the cipher. Using ECC on a suitably chosen curve one only needs a 350-bit ground field to obtain comparable security. The suite B published by NSA in 2005 recommends a 384-bit elliptic curve for the protection of top secret information [NSA].

5.1   Basic Principles

The elliptic curve discrete logarithm problem (ECDLP) is the following problem: given two $\mathbb{F}_q$-rational points P and Q on an elliptic curve over $\mathbb{F}_q$ with $Q \in \langle P \rangle$, find an integer h such that $Q = [h]P$. For general elliptic curves there are no known algorithms that are able to solve this problem in less than $O(\sqrt{q})$ steps. Note that this is exponential in $\log_2 q$, i.e., in the number of bits needed for representing a point of E. We will analyze the ECDLP in more depth in chapter 7. Most ECC schemes are based on the following problem:

Definition 5.1 (Elliptic Curve Diffie-Hellman Problem (EC-DHP))**.** Given the points P, $[n]P$ and $[m]P$ of an elliptic curve, determine $[nm]P$.

Obviously, if one can efficiently solve the ECDLP, then the EC-DHP is easy. The other direction is less obvious and in fact has not been proven in general. However, for some groups orders it can be shown that the DLP can be solved with a polynomial amount of calls to a DHP solving algorithm so that in these cases the two problems are computationally equivalent [MW96]. It is interesting that elliptic curves play a crucial part of the proof even for general abstract cyclic groups. For the EC-DHP the situation has been analyzed in depth in [MSV04].

Before one can apply any ECC scheme, the participants have to agree upon a some common values, called *domain parameters*. In principle it would be possible that everybody separately chooses domain parameters and makes them available as part of their public key. However it is more practical to agree on common parameters. The parameters necessary for almost all ECC schemes are the following:

1. The size q of a finite field $\mathbb{F}_q$ and a representation of that field.
2. An elliptic curve $E/\mathbb{F}_q$.
3. A base point $P \in E(\mathbb{F}_q)$ such that the index of $\langle P \rangle$ in $E(\mathbb{F}_q)$ is small (preferably 1).

Typically one chooses $q = 2^e$ or q prime. There are several constraints on the elliptic curve E and the order n of the subgroup generated by P. Let n be the order of P.

1. The order n should be prime or at least divisible by a large prime (to avoid Pohlig-Hellman reduction 7.1.1).
2. The embedding degree $k(q, n)$ (see 3.42) should not be too small (to avoid pairing based attacks 7.3). In particular E should not be supersingular.
3. If $q = p^e$, then n should not be divisible by p (to avoid anomalous curve attacks 7.4).
4. If $q = p^e$ with $e \neq 1$, then e should be prime (to avoid Weil decent attacks 7.5).

There are two approaches to choosing domain parameters: Either one tries to construct a curve that satisfies the above constraints and has as few additional properties that might be used for future attacks as possible; or one generates random curves until the constraints are met and hopes that the randomness thwarts any attacks in the future. Both approaches have advantages ans disadvantages. See [KKM08, section 11] for some discussion of the approaches. The books [HMV04] and [CF06] include further discussion relating to the generation of domain parameters.

Typically ECC schemes transmit points of the elliptic curve. To keep bandwidth usage low one should consider to use *point compression*. Since there are at most two points with any given x-coordinate, it is sufficient to transmit the x-coordinates of points together with a bit that indicates which y-coordinate to choose. Note that calculating square roots in finite fields can be done reasonably fast (see [CF06, chapter 11]).

All forms of elliptic curve cryptography are based around the principle of *asymmetric encryption*; different keys are used for en- and decryption.

Definition 5.2 (ECC key pair). The private key for ECC schemes is a randomly chosen integer $d \in [1, n{-}1]$ and the public key is $Q = [n]P$.

While users typically publish their public key on a publicly accessible place (like a key server) they must under all circumstances keep their private key secret. All asymmetric schemes are based on the fact that only the user who generated the key knows the private key. It is important to note that in most cryptographic schemes when the private key is compromised all past messages can easily be decrypted by a third party. Protocols where this is impossible are said to provide *forward secrecy*.

Another problem is to verify that a public key does indeed belong to the correct person. Otherwise a man-in-the-middle attack is trivial. The usual way to verify this is via a trusted third party known as certificate authority (CA) [MvV97, chapter 13] or key exchange in person.

We will use the archetypal *Alice* and *Bob* for the two communicating parties and *Mallory* for the attacker.

5.2   Key Exchange

The aim of *key exchange protocols* is to establish a shared key for subsequent communication using a symmetric key cipher. The first key exchange protocol was the Diffie-Hellman key exchange over prime fields. Since it can be formulated for any cyclic group, it can also be used on cyclic subgroups of elliptic curves and gives the *Elliptic Curve Diffie-Hellman* (ECDH) key exchange protocol we will now describe.

First the two communicating create key pairs (Q_A, d_A) and (Q_B, d_B). Alice computes $K_A = [d_A]Q_B$ and Bob computes $K_B = [d_B]Q_A$. Then

$$K_A = [d_A][d_B]P = [d_B][d_A]P = K_B$$

and the common key is the image of K_A under a predefined map $\langle P \rangle \rightarrow \mathbb{Z}$. For example if the curve is defined over $\mathbb{F}_p$, one can just take the x-coordinate of K_A.

Diffie-Hellman protocols should never be used on their own, because they are susceptible to man-in-the-middle attacks. Key exchange protocols are typically used on a per-session basis, hence the authenticity of the keys has not been previously established. Mallory could trick Alice into thinking that she is Bob and Bob into believing that she is Alice (for example by intercepting the traffic between them). She could then individually create shared keys with both Alice and Bob. Any message sent between Alice an Bob can be intercepted by Mallory, decrypted and then encrypted with the other shared key. Thus Mallory has access to the full communication while being completely transparent to the senders.

One way to remove the possibility of a man-in-the-middle attack on DH is to use preauthenticated key pairs. However, this would result in the same symmetric key for every communication session and it is a bad cryptographic practice to reuse the same key multiple times. However, there are several ways to use preauthenticated key pairs together with a new random number on every key exchange. One possible way is to use standard ECDH (with new keys for every key exchange) and sign the transmitted keys using the already known authentic keys. We will discuss signature schemes later on. One variant of this approach is the Station-To-Station (STS) protocol [HMV04, section 4.6.1]. However the one most widely used key exchange protocol is ECMQV (Elliptic Curve Menezes-Qu-Vanstone) which we will describe next.

Suppose that the authenticity of the key pairs (Q_A, d_A) and (Q_B, d_B) is already known to the communicating parties. For key exchange both parties create a new key (Q'_A, d'_A) and (Q'_B, d'_B) respectively and exchange Q'_A and Q'_B. In order to provide forward security it is important that d'_A and d'_B are new random numbers for every key exchange. The shared key is then derived by the following algorithm:

Algorithm 5.3 (MQV key generation)**.** *Suppose we are Alice. Then Q_A, Q'_A, Q_B, Q'_B, d_A and d'_A are known. Further let $n = \operatorname{ord} P$ be the group size and let $l = \lceil (\lfloor \log_2 n \rfloor + 1)/2 \rceil$.*

  1. Convert Q'_A to an integer i.
  2. Put $s_A = (i \bmod 2^l) + 2^l$.
  3. Convert Q'_B to an integer j.
  4. Put $t_A = (j \bmod 2^l) + 2^l$.
  5. Put $h_A = d'_A + s_A d_A$.
  6. Return $K = [h_A](Q'_B + [t_A]Q_B)$.

Bob's algorithm works by interchanging A and B in the subscripts.

Note that Bob has $s_B = t_A$ and $s_A = t_B$. Therefore

$$K = [h_A](Q'_B + [s_B]Q_B) = [d'_A + s_A d_A]([d'_B]P + [s_B][d_B]P) = [d'_A d'_B + s_A d_A d'_B + s_B d_B d'_A + s_A s_B d_A d_B]P,$$

which is symmetric in A and B. Thus Alice and Bob arrive at the same key. Also the key can only be calculated correctly when the respective private keys are known. Therefore the knowledge of the correct key serves as implicit authentication. A complete description of the full procedure including all necessary communication is given in [HMV04, section 4.6.2]. Recently a possible weakness of the MQV protocol has been found and fixed in [Kra05]. However, the validity of the arguments in this paper and of the underlying security model has been challenged [Men07].

5.3 Message Encryption

While we have just seen that the Diffie-Hellman and MQV protocols can easily be applied on elliptic curves, ElGamal cannot. The main problem is that there exists no canonical map $\mathbb{Z} \rightarrow \langle P \rangle$ with computable inverse. Therefore a variant called ECIES (*Elliptic Curve Integrated Encryption Scheme*) is often used for message encryption. With ECIES a form of Diffie-Hellman is used to create a key which is then used to encrypt the message using a symmetric cipher (e.g. AES). Additionally a second key is derived and used for message authentication. This guards against chosen-ciphertext attacks.

ECIES needs three "subschemes", called cryptographic primitives:

- A *key derivation function* (KDF) with accepts points of the underlying curve as input and returns a pair of keys used for the symmetric encryption and message authentication. KDFs are usually constructed using a hash function.

- A symmetric cipher. We write ENC_k and DEC_k for encryption and decryption using the key k.

- A *message authentication code* (MAC) algorithm such as HMAC. It accepts a key and a message as input and returns a hash code depending on both the key and the message.

We can now describe the ECIES procedure:

Algorithm 5.4 (ECIES encryption). *Let m be the message and Q be the public key of the receiver. The following algorithm is used to generate the ciphertext for ECIES.*

1. *Choose a random integer $r \in [1, n-1]$ (where n is the group size).*
2. *Put $R = [r]P$ and $Z = [r]Q$. If $Z = \mathcal{O}$ then return to step 1.*
3. *Compute $(k_1, k_2) = KDF(Z)$.*
4. *Compute $c = ENC_{k_1}(m)$ and $t = MAC_{k_2}(c)$.*
5. *Return (R, c, t).*

Algorithm 5.5 (ECIES decryption). *Let (R, c, t) be an encrypted message and let d be the private key of the receiver. The following algorithm returns the plain text m or rejects the message if it cannot be authenticated.*

1. *If R is no valid element of $\langle P \rangle$, reject the message.*
2. *Compute $Z = [d]R$. If $Z = \mathcal{O}$, reject the message.*
3. *Put $(k_1, k_2) = KDF(Z)$.*
4. *If $t \neq MAC_{k_2}(c)$, reject the message.*
5. *Return $DEC_{k_1}(c)$.*

Because of $Z = [r]Q = [r][d]P = [d][r]P = [d]R$, both parties generate the same key, so ECIES does indeed work.

5.4 Signatures

A signature scheme is used to verify that a message does indeed originate from the specified sender and that is was not altered during transmission. We will describe the *Elliptic Curve Digital Signature Algorithm* (ECDSA). Like every signature scheme, ECDSA consists of two algorithms: one for signature generation and one for signature verification. Let H be a cryptographic hash function (that is collision and preimage resistant). Further the base point P must have prime order n.

Algorithm 5.6 (ECDSA signature generation). *Let m be the message to sign and let d be the private key of the sender.*

1. *Choose a random $k \in [1, n-1]$.*
2. *Convert $[k]P$ into an integer x.*
3. *Compute $r = x \bmod n$. If $r = 0$, return to 1.*
4. *Compute $e = H(m)$.*
5. *Compute $s = k^{-1}(e + dr) \bmod n$. If $s = 0$, return to 1.*
6. *Return (r, s).*

Algorithm 5.7 (ECDSA signature verfication). *Let m be a message with signature (r, s) and let Q be the public key of the sender.*

1. *If r or s is not in $[1, n-1]$, reject the signature.*
2. *Compute $e = H(m)$.*
3. *Compute $u_1 = es^{-1} \bmod n$ and $u_2 = rs^{-1} \bmod n$.*
4. *Compute $X = [u_1]P + [u_2]Q$.*
5. *If $X = \mathcal{O}$, reject the signature.*

6. *Convert X to an integer x (in the same way as in the signature generation algorithm) and compute*
   $v = x \bmod n$.
7. *If $v = r$, accept the signature, otherwise reject it.*

The algorithm works because

$$k \equiv s^{-1}(e + dr) \equiv s^{-1}e + s^{-1}dr \equiv u_1 + u_2 d \pmod{n}$$

and thus

$$X = [u_1]P + [u_2]Q = [u_1 + u_2 d]P = [k]P.$$

5.5   Related Cryptography Schemes

Looking for groups which might provide even better security Koblitz suggested to apply cryptographic algorithms in the Jacobian of a hyperelliptic curve [Kob89]. As we have seen in section 2.6, it is possible to efficiently do computations in this group. Since the genus of a curve can be interpreted as a measure for its "complexity", he reasoned that hyperelliptic curve cryptosystems might provide even better security than ECC. Unfortunately it turned out that the opposite is true. The discrete logarithm problem for hyperelliptic curves can be solved faster with growing genus (cf. section 7.2.2). As he writes in in [KKM08, p. 9]:

> Isn't it reasonable to assume that a problem would be at least as hard to solve on a more complicated object (a g-dimensional Jacobian) as on a relatively simple object?
>
> That way of thinking was a "rookie mistake" for a cryptographer to make, because [Koblitz] was confusing two meanings of "complexity": conceptual complexity and computational complexity.

The only case where hyperelliptic curves might provide better security than elliptic curves is the case of genus 2.

Slightly related to ECC is *pairing-based cryptography*. Here the Weil and Tate pairings are used for cryptographic applications (note that we will also use them, but in a less constructive way by showing that certain instances of the ECDLP are not secure). One problem that can be solved by pairing-based techniques is identity-based cryptography, where the public key of a user is just a unique piece information about that user (e.g. the email address). A discussion of pairing-bases cryptography schemes is beyond the scope of this document. For details see [BSS05, chapter X].

Chapter 6

Computational Aspects

Elliptic curve cryptography depends on the fact that one can efficiently calculate in the group of points of an elliptic curve. It also depends on the existence of fast algorithms to count the number of $\mathbb{F}_q$-rational points of a given curve. In the present chapter we take a look at the computational problems that arise in connection with ECC and present algorithms to solve them. We will also study some algorithms which will used in the various attacks on ECC in the next chapter.

6.1 Elliptic Curve Arithmetic

The basic operation on elliptic curves is of course *point addition*. Using the formulas of section 2.1 we see that adding two points takes a fixed amount of multiplications, inversions and additions in the ground field. How many operations are exactly necessary depends on the equation of the curve. Usually field inversions are much slower than multiplications while additions are so fast that they can be ignored in time estimates. Also multiplication with a (small) integer can normally be done fast. Therefore one would like to do point addition with as few inversions as possible.

In the addition formulas there are only two places where an inversion in necessary: when calculating the slope λ and the y-intercept ν of the line through the points. The denominators of both are the same, so we need to do only one inversion. However there is a trick to save even this one inversion at the cost of a few multiplications and additional storage requirements. Instead of using the standard affine coordinates to specify a point we use *weighted projective* or *Jacobian coordinates*: a triplet $[X : Y : Z]$ corresponds to the affine point $(\frac{X}{Z^2}, \frac{Y}{Z^3})$. The motivation for this are of course the multiplication formulas of theorem 3.27. For point addition in characteristic $p \geq 3$ we take $Z_3 = Z_1 Z_2 (X_2 Z_1^2 - X_1 Z_2^2)$. Multiplying the addition formulas for x and y by Z_3^2 resp. Z_3^3 we see that all denominators vanish. Similarly one can find good choices for Z_3 for point doubling and characteristic 2, see [BSS99] for details.

We will refer to one point addition on an elliptic curve as one *group operation*. For most algorithms which we will discuss in this and the next section we will give the running time in the number of group operations. We have just seen that group operations need a fixed amount (actually less than 16) ground field multiplications. With a naive implementation of the ground field multiplication this means $O((\log q)^2)$ basic operations (where q is the size of the ground field). With fast multiplication we can reduce this to $O((\log q)^{1+\varepsilon})$ for any $\varepsilon > 0$, but the constant in the O-notation will grow quite fast ([Knu97, section 4.3.3]). Which implementation is the fastest depends on the characteristic and size of the ground field. For a detailed discussion see [CF06]. When not mentioned otherwise we will assume naive, i.e. $O((\log q)^2)$, implementation of ground field multiplication.

We should also note that for calculating $[k]P$ one needs at most $2 \log_2(k)$ group operations using a standard double-and-add algorithm ([Knu97, section 4.6.3]). Since inversion of points on elliptic curve (i.e. computing $-P$) is very easy one can improve on the standard algorithm by using an "addition-and-subtraction"-chain ([BSS99, section 4.2.4]). Of course one can often exploit any additional structure of the elliptic curve, for example when it is defined over a subfield.

Similar considerations also hold true for group operations in the Picard group of a hyperelliptic curve, see [BSS05, chapter VII].

6.2 Determining the Group Order

One of the domain parameters in elliptic curve cryptography is the size of the group $E(\mathbb{F}_q)$. ECC is only practical if one is able to compute it fairly quickly for large q. There is of course a naive way to point counting: Run through all possible $x \in \mathbb{F}_q$ and count how many ys there are that fulfill the curve equation (the only possibilities are 0, 1 ore 2). For a Weierstrass equation $y^2 = x^3 + Ax + B$ this amounts to checking the quadratic residuosity of $x^3 + Ax + B$. Even if we have access to a precomputed lookup table for determining residuosity, this approach needs $O(q)$ time. Hence it is not practical.

If for a point P there is exactly one number $m \in [q + 1 - 2\sqrt{q},\, q + 1 - 2\sqrt{q}]$ such that $[m]P = \mathcal{O}$, then by Hasse's theorem (3.40) m is the group order. J. F. Mestre has shown how one can always find a point with this property. Then, in order to find m, one can apply any (general purpose) discrete logarithm algorithm. Historically it was first suggested to use the baby-step-giant-step algorithm. Therefore the resulting point counting algorithm is often called *Shanks-Mestre algorithm*. A complete description can be found in [Sch95]. Though this approach is much faster than the naive one, it still has exponential running time.

The breakthrough in point counting came in 1985, when Schoof published an algorithm with polynomial running time [Sch85]. He uses an ℓ-adic approach by determining the group order modulo several (small) primes ℓ and then combining this knowledge with the Chinese remainder theorem. In 2000, Satoh [Sat00] suggested a p-adic algorithm which lifts the curve to the local field $\mathbb{Q}_q$ and uses the lift to determine the trace of the Frobenius (and thus the group order).

Before describing the approaches in more detail, it should be noted that in the case of *subfield curves*, i.e. curves over $\mathbb{F}_{p^m}$ with coefficients in a subfield $\mathbb{F}_{p^n}$, one only needs to determine $\#E(\mathbb{F}_{p^n})$ and apply the Weil conjectures 3.39.

6.2.1 Schoof's Algorithm and Improvements

We will begin by giving a short description of Schoof's original algorithm. Afterwards we will discuss how ideas of Elkies and Atkin can be used to speed it up. Let $E/\mathbb{F}_q$ be defined by the Weierstrass equation $f(x, y) = 0$.

In order to determine the group order of $E(\mathbb{F}_q)$, it is sufficient to know the trace of the qth-power Frobenius ϕ_q. Let S be a set of primes not equal to $p = \operatorname{char} \mathbb{F}_q$ with $\prod_{\ell \in S} \ell > 4\sqrt{q}$. We will compute $t_\ell = \operatorname{tr} \phi_q \pmod{\ell}$ for all $\ell \in S$. By the Chinese remainder theorem and Hasse's theorem this is enough to fully determine $t = \operatorname{tr} \phi_q$. For a positive integer x, the product of all primes smaller than $\log x$ is of order x [HW60, theorems 420 and 6]. Therefore by the prime number theorem [HW60, theorem 6], we know that we can take $|S| = O(\log q / \log \log q)$ primes of size at most $O(\log q)$.

The case $\ell = 2$ is trivial, since $\#E(\mathbb{F}_q)$ is even if and only if it contains a point of order two. Assume $f(x, y) = y^2 - x^3 - Ax - B$. Then points of order two can only have the form $(e, 0)$ for some root e of $x^3 + Ax + B$ and such a root exists if and only if $\gcd(x^3 + Ax + B, x^q - x) \neq 1$.

From now on assume that $\ell > 2$. Let $P \in E[\ell]$ and $q_\ell \equiv q \pmod{\ell}$, where the representative with least absolute value is taken. Then the characteristic polynomial 2.54 of ϕ_q gives

$$\phi_q^2(P) + [q_\ell]P = [t_\ell]\phi_q(P). \tag{6.1}$$

If $P \neq \mathcal{O}$, there is exactly one $t_\ell \pmod{\ell}$ for which this equation holds. The idea is to calculate the left hand side of the equation and then find a value τ such that $[\tau]\phi_q(P)$ is equal to it. The only problem is that we do not know how to find a point $P \in E[\ell] \cap E(\mathbb{F}_q)$. Thus we have to modify this approach a bit.

Let ψ_ℓ be the ℓth division polynomial of E as defined in 3.27. Then $P \in E[\ell]$ if and only if $\psi_\ell(P) = 0$. When we set $P = (x, y)$ in (6.1), the relation becomes

$$(x^{q^2},\, y^{q^2}) + [q_\ell](x,\, y) \equiv [t_\ell](x^q,\, y^q) \mod \langle f(x, y),\, \psi_\ell(x, y) \rangle.$$

All we have to do is check for which t_ℓ the above equality of polynomials is true modulo f and ψ_ℓ (note that the addition above is addition on the elliptic curve). The modulus ψ_ℓ is of degree $O(\ell^2)$, so every operation in the ring $\mathbb{F}_q[x, y]/\langle f(x, y),\, \psi_\ell(x, y) \rangle$ takes $O((\ell^2)^2) = O(\log^4 q)$ operations in $\mathbb{F}_q$. Thus we need $O\left(\log^4 q \cdot \log^2 q\right)$ bit operations for every curve addition. Further, calculating the left side takes $O(\log q)$

curve operations while the right side take $O(\log t_\ell) = O(\log \log q)$ curve operations, but $O(\ell) = O(\log q)$ times. Since $|S| = O(\log q / \log \log q)$ this gives an overall complexity of $O(\log^8 q)$.

The procedure just described is not exactly how one would implement Schoof's algorithm. At the cost of some additional considerations and special cases one only needs to check half the possible t_ℓ but this does not change the asymptotic behavior. For details see [Was08, section 4.5] and [BSS99, section VII.1].

The most time consuming part of Schoof's algorithm is the computations modulo ψ_ℓ which is a polynomial of degree $\frac{\ell^2 - 1}{2}$. It would be nice to be able to do calculations modulo a polynomial of smaller degree and indeed with ideas of Elkies and Atkin this is possible. The resulting algorithm is often called *SEA algorithm* after the names of its inventors. Since the exact calculations and formulas are rather tedious we will only give a short overview of the ideas. A full discussion is given in [BSS99]. The algorithm does not work for supersingular curves (but in this case point counting is trivial) or if the j-invariant of E is 0 or 1728 (in this case see [Sch95] for alternatives). So we will assume that E is ordinary and $j(E) \neq 0, 1728$.

The first part is to decide whether ℓ is an Elkies or an Atkin prime (see definition 3.55). This is possible by using 3.54 and simply checking how many zeros $\Phi_\ell(j, T)$ has in $\mathbb{F}_q$. The number of zeros is equal to the degree of

$$\gcd(T^q - T, \Phi_\ell(j, T)).$$

Suppose first that ℓ is an Atkin prime. We compute

$$\gcd(T^{q^i} - T, \Phi_\ell(j, T)).$$

for $i = 1, 2, \ldots$ until it is equal to $\Phi_\ell(j, T)$. This number i must be equal to r of theorem 3.54. Of course it is not necessary to compute the gcd for all i since the theorem states that r divides $\ell + 1$. Further, if $q = p$ is an odd prime then Schoof proved that

$$(-1)^{\frac{\ell+1}{r}} = \left(\frac{p}{\ell}\right),$$

where $\left(\frac{p}{\ell}\right)$ is the Legendre symbol [Sch95, proposition 6.3]. Having determined r, the last statement of theorem 3.54 at least halves the possible $t \pmod{\ell}$: Since r divides $\ell + 1$, there are $\varphi(r) \leq \frac{\ell+1}{2}$ primitive r^{th} roots of unity in $\bar{\mathbb{F}}_\ell$. So there are at most $\frac{\ell+1}{4}$ values for $t^2 \pmod{\ell}$ (here φ is the Euler function). Atkin then combines this with the information gained from Elkies primes (see below) and uses a baby-step-giant-step algorithm to obtain the exact value of the trace.

Now let ℓ be an Elkies prime. By theorem 3.53, ϕ_q has at least one eigenspace $C \subseteq E[\ell]$ with eigenvalue $\lambda \in \mathbb{F}_\ell$. Let F_ℓ be a polynomial that vanishes exactly at the points in C. Then F_ℓ is a divisor of ψ_ℓ of degree $\frac{\ell-1}{2}$. It is obtained by clever use of the modular polynomial and isogenies, see the discussion in [BSS99] or [Sch95]. Since $t \equiv \lambda + \frac{q}{\lambda} \pmod{\ell}$ we only have to find λ. Hence we simply check for which $\lambda' = 1, \ldots, \ell - 1$ we have

$$\phi_q(x, y) = (x^q, y^q) \equiv [\lambda'](x, y) \mod \langle f(x, y), F_\ell(x, y) \rangle.$$

The degree of F_ℓ is $O(\ell)$ compared with $O(\ell^2)$ for ψ_ℓ. Hence the running time of this step is $O(\log^5 q)$ instead of $O(\log^7 q)$ in the original algorithm.

The biggest problem in the SEA algorithm is that the coefficients of the modular polynomials grow quite fast. In practice one tries to replace them with polynomials with similar splitting properties but smaller coefficients. The basic idea is to find different models for the modular curve $X_0(\ell)$. One such family of polynomials is given in [Mül95].

6.2.2 p-adic Algorithms

We will give a short overview of Satoh's p-adic algorithm for point counting. This algorithm is fast for elliptic curves over $\mathbb{F}_{p^n}$ where p is a small prime. Let μ be a constant such that the multiplication of two m-bit integers can be computed in $O(m^\mu)$ time (i.e. 2 for naive multiplication and $1 + \varepsilon$ for fast multiplication). For fixed p, the algorithm has time complexity $O(n^{2\mu+1})$, instead of $O(n^{2\mu+2})$ of the SEA-algorithm. However with growing p the O-constant grows a lot faster for Satoh's algorithm.

First a bit of notation. Let E_1, E_2 be elliptic curves defined over the same field and $\phi\colon E_1 \to E_2$ an isogeny. Further let τ_1 and τ_2 be the uniformizing element $-\frac{x}{y}$ of E_1 resp. E_2 at $\mathcal{O}$. Then there is an expansion

$$\phi^*(\tau_2) = c_1\tau_1 + c_2\tau_1^2 + \cdots.$$

We call c_1 the *leading coefficient of* ϕ and denote it by $\mathrm{lc}(\phi)$. If ϕ is separable, then by 2.28 and the definition of the ramification index (1.33), $c_1 \neq 0$.

Let E be an elliptic curve over $\mathbb{F}_q$, $q = p^n$. We will assume that $j(E) \notin \mathbb{F}_{p^2}$ (in particular E is not supersingular). If $j(E) \in \mathbb{F}_{p^2}$, then E is isomorphic to a curve E' defined over $\mathbb{F}_{p^2}$. Hence we just count $\#E'(\mathbb{F}_{p^2})$ and apply the Weil conjectures. Let ϕ_q be the qth-power Frobenius endomorphism of E and ϕ_p the pth-power Frobenius automorphism of $\mathbb{F}_q$ and by abuse of notation also every isogeny it induces. Further let $\mathcal{E}$ be the canonical lift of E to $\mathbb{Q}_q$ and $\mathcal{F}$ be the lift of ϕ_q. We want to compute $\mathrm{tr}\,\phi_q = \mathrm{tr}\,\mathcal{F}$. Since $\mathbb{Q}_q$ has characteristic 0 it would be possible to directly compute $\mathrm{tr}\,\mathcal{F}$, but computationally this approach is too expensive because $\deg\mathcal{F}$ is q. On the other hand $\deg\phi_p = p$ which is assumed to be small and ϕ_q is equal to the n-fold iteration of ϕ_p. Let Σ be the Frobenius substitution of $\mathbb{Q}_q$. Put $E_0 = E$ and $E_{i+1} = \phi_p(E_i)$. Then ϕ_q and its lift $\mathcal{F}$ can be decomposed in the following way:

$$\begin{array}{ccccccccc}
\mathcal{E}_0 & \xrightarrow{\Sigma_0} & \mathcal{E}_1 & \xrightarrow{\Sigma_1} & \cdots & \xrightarrow{\Sigma_{n-2}} & \mathcal{E}_{n-1} & \xrightarrow{\Sigma_{n-1}} & \mathcal{E}_0 \\
\pi\downarrow & & \pi\downarrow & & & & \pi\downarrow & & \pi\downarrow \\
E_0 & \xrightarrow{\phi_p} & E_1 & \xrightarrow{\phi_p} & \cdots & \xrightarrow{\phi_p} & E_{n-1} & \xrightarrow{\phi_p} & E_0
\end{array} \qquad (6.2)$$

So instead of lifting E, we will lift the cycle $(E_0, E_1, \ldots, E_{n-1})$. There is one additional problem: ϕ_q is inseparable. However this can be easily circumvented by using its dual isogeny $\widehat{\phi}_q$ which has the same trace and determinant as ϕ_q and is separable since E is ordinary. We can use the same decomposition (with the arrows pointing the other way) and the dual isogenies $\widehat{\phi}_p$ and $\widehat{\Sigma}_i$ which are often called *Verschiebung*. The characteristic equation

$$\widehat{\mathcal{F}}^2 - \mathrm{tr}(\widehat{\mathcal{F}})\widehat{\mathcal{F}} + q = 0$$

implies

$$\mathrm{lc}(\widehat{\mathcal{F}})^2 - \mathrm{tr}(\widehat{\mathcal{F}})\,\mathrm{lc}(\widehat{\mathcal{F}}) + q = 0.$$

From the observation above we know that $\pi(\mathrm{lc}(\widehat{\mathcal{F}})) = \mathrm{lc}(\widehat{\phi}_q) \neq 0$ and hence $\mathrm{lc}(\widehat{\mathcal{F}}) \in \mathbb{Z}_p^*$. Therefore,

$$\mathrm{tr}(\phi_q) = \mathrm{tr}(\mathcal{F}) = \mathrm{tr}(\widehat{\mathcal{F}}) = \mathrm{lc}(\widehat{\mathcal{F}}) + \frac{q}{\mathrm{lc}(\widehat{\mathcal{F}})} \equiv \mathrm{lc}(\widehat{\mathcal{F}}) \pmod{p\mathbb{Z}_q}.$$

Thus it is sufficient to know $\mathrm{lc}(\widehat{\mathcal{F}})$ with sufficiently high precision. From the diagram (6.2) we see that

$$\mathrm{lc}(\widehat{\mathcal{F}}) = \prod_{i=0}^{n-1} \mathrm{lc}(\widehat{\Sigma}_i). \qquad (6.3)$$

The Frobenius substitution Σ generates $\mathrm{Gal}(\mathbb{Q}_q|\mathbb{Q}_p)$, so the squares are all conjugates and we get for all $i \in \{0, \ldots, n-1\}$,

$$\mathrm{lc}(\widehat{\mathcal{F}}) = N_{\mathbb{Q}_q|\mathbb{Q}_p}(\mathrm{lc}(\widehat{\Sigma}_i)). \qquad (6.4)$$

We can use (6.3) or (6.4) to calculate the group order. Note that though with (6.4) we only need to lift one of the squares of (6.2), norm computation is also not easy.

Now we are in a good position to give an outline of Satoh's algorithm:

(1) Compute the j-invariants of $\mathcal{E}_0$ and $\mathcal{E}_1$ (and from this equations for the curves, according to 2.8).
(2) Compute $c = \mathrm{lc}(\widehat{\Sigma}_0)$.
(3) Compute $N_{\mathbb{Q}_q|\mathbb{Q}_p}(c)$

All computation have to be done with sufficiently high precision so that we can deduce the trace t of which we know that $|t| < 2\sqrt{q}$.

Step (1) can be done with theorem 3.105 and Newton iteration. Norm computation is nothing special to elliptic curves so we will not discuss it here (see for example [BSS05, section VI.5]). Of course one can also completely ignore it and use (6.3) instead. See also Vercauteren's improvement of Satoh's algorithm [VPV01]. There are several improvements of these parts of Satoh's algorithm, see [BSS05, section VI.4].

We will now give a short overview of step (2). Assume that we know $\ker \widehat{\Sigma}_0$. Using Vélu's formulas we can explicitly calculate a Weierstraß equation of $\mathcal{E}' = \mathcal{E}_1 / \ker \widehat{\Sigma}_0$ and the isogeny $u \colon \mathcal{E}_1 \to \mathcal{E}'$. We see that $\mathrm{lc}(u) = 1$. Further by theorem 2.30 and comparison of degrees there exists an isomorphism λ making the following diagram commutative:

$$
\begin{array}{ccc}
\mathcal{E}_1 & \xrightarrow{\ \widehat{\Sigma}_0\ } & \mathcal{E} \\
& {\scriptstyle u} \searrow \quad \nearrow {\scriptstyle \lambda} & \\
& \mathcal{E}' &
\end{array}
$$

Using that isomorphisms for Weierstraß forms have very specific forms one can easily calculate $\mathrm{lc}(\lambda) = \mathrm{lc}(\widehat{\Sigma}_0)$. Therefore the only problem is to calculate $\ker \widehat{\Sigma}_0$. This is done using a modified version of Hensel's lemma to compute the polynomial[1]

$$
H(x) = \sum_{P \in \left(\ker \widehat{\Sigma}_0 \setminus \{\mathcal{O}\}\right)/\pm} (X - x(P)).
$$

See [BSS05, section VI.2.5] for details.

The AGM Algorithm

We will discuss a different p-adic algorithm by Harley and Mestre for the case $p = 2$. Again we will only give a high level overview and refer to [BSS05, section VI.3] and [Sat02] for details. We should note that the algorithm is covered by a US patent.

Let $a_0 \geq b_0 > 0$ be two real numbers and define two sequences a_i, b_i by

$$
(a_{i+1},\, b_{i+1}) = \mathcal{M}(a_i,\, b_i) = \left(\frac{a_i + b_i}{2},\ \sqrt{a_i b_i} \right).
$$

One can easily show that both sequences converge to the same number called the *arithmetic-geometric mean* (AGM) of a_0, b_0. The AGM is closely related to elliptic curves, see for example [Sil92, exercise 6.14] and [BB87]. Let $q = 2^n$ and $a, b \in 1 + 4\mathbb{Z}_q \subseteq \mathbb{Q}_q$ with $\frac{a}{b} \in 1 + 8\mathbb{Z}_q$. Then

$$
(a',\, b') = \mathcal{M}(a, b) = \left(\frac{a + b}{2},\ b\sqrt{\frac{a}{b}} \right)
$$

is well defined and $a', b' \in 1 + 4\mathbb{Z}_q$ with $\frac{a'}{b'} \in 1 + 8\mathbb{Z}_q$. For a, b with these properties define

$$
E_{a,b} \colon y^2 = x(x - a)(x - b).
$$

Then $E_{a,b}$ and $E_{\mathcal{M}(a,b)}$ are 2-isogenous. There exists a lift of $E/\mathbb{F}_q$ of the form $E_{a,b}$. Define two sequences a_i, b_i by $(a_0, b_0) = (a, b)$ and $(a_{i+1}, b_{i+1}) = \mathcal{M}(a_i, b_i)$. In general these sequences do not converge. However if $\mathcal{E}$ is the canonical lift of E, then $j(E_{a_{ni}, b_{ni}})$ converges to $j(\mathcal{E})$:

$$
j(E_{a_i, b_i}) \equiv \Sigma^i(j(\mathcal{E})) \pmod{2^{i+1}}.
$$

Hence this gives an alternative method for step (1) of Satoh's algorithm. Also the AGM provides a very efficient way for computing the trace of the Frobenius. See the references given above for explicit formulas.

6.3 Calculating Values of EDS and Elliptic Nets

Before we can apply elliptic divisibility sequences and nets to solving the elliptic curve discrete logarithm problem we need to figure out how to calculate their values. Let W be an EDS and assume $W(1) = 1$. In (4.1) we let $p = i - 1$, $q = i$, $r = 1$ and $s = 0$ to obtain

$$
W(2i - 1) = W(i + 1)W(i - 1)^3 - W(i - 2)W(i)^3. \tag{6.5}
$$

---

[1]Actually, this approach only works for $p \geq 3$. For $p = 2$ one has to use a different method to obtain $\ker \widehat{\Sigma}_0$. Also note that $\left| \ker \widehat{\Sigma}_0 \right| = p$ is very small.

Further, with $p = i + 1$, $q = i - 1$, $r = 1$ and $s = 0$,

$$W(2i) = \frac{W(i)W(i+2)W(i-1)^2 - W(i)W(i-2)W(i+1)^2}{W(2)}. \tag{6.6}$$

Actually these two formulas are used to prove theorem 3.23.

Theorem 6.1. *Let $W = W_{E,P}$ be the EDS associated to an elliptic curve E over $\mathbb{F}_q$ and point $P \in E(\mathbb{F}_q)$ of order at least 4. Then it is possible to calculate $W(k)$ in $O((\log k)(\log q)^2)$ time.*

Proof. Let $\langle W(i) \rangle$ be the *block centered at i* consisting of the 8 values $W(i-3), \ldots, W(i+4)$. Using formulas (6.5) and (6.6) it is possible to calculate the blocks centered at $2i$ and $2i+1$ using only the values of the block centered at i. The amount of $\mathbb{F}_q$ multiplications and divisions needed for this is independent of i. The block centered on 0 can be calculated as in definition 3.26. Therefore we can use a double-and-add algorithm to calculate the block centered at k and hence the value of $W(k)$. $\square$

Additional discussion and refinements can be found in [Shi00].

Calculating the values of an elliptic net is by far more difficult because the recurrence relations one needs quickly become complicated. However, the only computational application of elliptic nets will be in corollary 6.6 and there we will only need $W(k, 0)$ and $W(k, 1)$. For a general discussion about calculating terms of elliptic nets see [Sta07a].

Theorem 6.2. *Let $W = W_{E,P,Q}$ be the elliptic net associated to an elliptic curve E over $\mathbb{F}_q$ and points $P, Q \in E(\mathbb{F}_q)$. Then it is possible to calculate $W(k, 0)$ and $W(k, 1)$ in $O((\log k)(\log q)^2)$ time.*

Proof. The algorithm we will use is very similar to the one of the last theorem. Now a block centered at k consists of the values $W(k-3, 0), \ldots, W(k+4, 0)$ together with $W(k-1, 1)$, $W(k, 1)$ and $W(k+1, 1)$. Calculating the $W(\cdot, 0)$-values of the block centered at $2k$ or $2k+1$ can again be done using equations (6.5) and (6.6). For the other three values we need the following formulas obtained form (4.1) using $(p, q, r, s) = ((k, 0), (k-1, 0), (1, 0), (0, 1))$, $((k+1, 0), (k, 0), (1, 0), (-1, 1))$, $((k+1, 0), (k, 0), (-1, 0), (0, 1))$ and $((k+2, 0), (k, 1), (1, 0), (0, 0))$ respectively.

$$W(2k-1, 1) = \frac{W(k+1, 1)W(k-1, 1)W(k-1, 0)^2 - W(k, 0)W(k-2, 0)W(k, 1)^2}{W(1, 1)},$$

$$W(2k, 1) = W(k-1, 1)W(k+1, 1)W(k, 0)^2 - W(k-1, 0)W(k+1, 0)W(k, 1)^2,$$

$$W(2k+1, 1) = \frac{W(k-1, 1)W(k+1, 1)W(k+1, 0)^2 - W(k, 0)W(k+2, 0)W(k, 1)^2}{W(-1, 1)},$$

$$W(2k+2, 1) = \frac{W(k+1, 0)W(k+3, 0)W(k, 1)^2 - W(k-1, 1)W(k+1, 1)W(k+2, 0)^2}{W(2, -1)}.$$

$\square$

6.4   Evaluating Pairings

We will present two polynomial time algorithms for evaluating the pairings of section 2.4. The first one is the classical algorithm by Miller [Mil86a]. The second one is a relatively new algorithm for the Tate pairing based on elliptic nets.

6.4.1   Miller's algorithm

Let E be an elliptic curve defined over a finite field and let P and Q be rational points on E. Let n denote the order of P. In order to calculate the pairings we need to calculate $f(D_Q)$ for a function f with $\text{div}(f) = n(P) - n(\mathcal{O})$ and a divisor $D_Q \sim (Q) - (\mathcal{O})$ with support disjoint from $\text{div}(f)$. Note that this is sufficient for both the Tate and the Weil pairing because the latter is essentially just a quotient of two such functions (compare [Mil04]).

Lemma 6.3. *Recursively define a sequence of functions on E by $f_1 = 1$ and*

$$f_{i+j} = f_i f_j \frac{l_{i,j}}{l_{i+j,0}}$$

where $l_{i,j} = 0$ and $l_{i+j,0} = 0$ are the equations of the lines used in the calculation of $[i]P + [j]P = [i+j]P$. Then

$$\mathrm{div}(f_i) = i(P) - ([i]P) - (i-1)(\mathcal{O}).$$

Proof. Like in the proof of theorem 2.13,

$$\mathrm{div}\left(\frac{l_{i,j}}{l_{i+j,0}}\right) = ([i]P) + ([j]P) - ([i+j]P) - (\mathcal{O}).$$

Therefore by induction,

$$\mathrm{div}(f_{i+j}) = \mathrm{div}\left(f_i f_j \frac{l_{i,j}}{l_{i+j,0}}\right) =$$
$$i(P) - ([i]P) - (i-1)(\mathcal{O}) + j(P) - ([j]P) - (j-1)(\mathcal{O}) + ([i]P) + ([j]P) - ([i+j]P) - (\mathcal{O}) =$$
$$(i+j)(P) - ([i+j]P) - (i+j-1)(\mathcal{O}). \quad \square$$

We are of course interested in f_n. Miller's algorithm uses an addition chain to calculate $f_n(D_Q) = \tau_n(P, Q)$. It will use $D_Q = (Q + S) - (S)$ for a point $S \neq P, \mathcal{O}$.

Algorithm 6.4 (Miller's Algorithm). *Let $P, Q \in E(K)$ where P has order n. The following algorithm computes $\tau_n(P, Q)$.*

1. *Choose a suitable point $S \in E(K)$ and set $Q' \leftarrow Q + S$.*
2. *Set $T \leftarrow P$, $m \leftarrow \lfloor \log_2(n) \rfloor - 1$, $f \leftarrow 1$.*
3. *If $m < 0$, return f.*
4. *Calculate the lines $l_{T,T}$ and $l_{[2]T,\mathcal{O}}$ for doubling T.*
5. *Set $T \leftarrow [2]T$.*
6. *Set $f \leftarrow f^2 \dfrac{l_{T,T}(Q')l_{[2]T,\mathcal{O}}(S)}{l_{[2]T,\mathcal{O}}(Q')l_{T,T}(S)}$.*
7. *If the mth bit of n is zero, go to 11.*
8. *Compute lines $l_{T,P}$ and $l_{T+P,\mathcal{O}}$ for the addition of T and P.*
9. *Set $T \leftarrow T + P$.*
10. *Set $f \leftarrow f \dfrac{l_{T,P}(Q')l_{T+P,\mathcal{O}}(S)}{l_{T+P,\mathcal{O}}(Q')l_{T,P}(S)}$.*
11. *Set $m \leftarrow m - 1$ and go to 3.*

Clearly the algorithms has $\log_2(n)$ iterations of the main loop. There are several ways to improve the efficiency of the algorithm (without reducing its overall complexity), see [BSS05, section IX.14].

6.4.2 Using Elliptic Nets to Calculate the Tate Pairing

Theorem 6.5 ([Sta07b]). *Let $n \geq 4$ and let E be an elliptic curve defined over a finite field K containing the nth roots of unity. Let $P \in E[n]$ and $Q, S \in E$ with $S \notin \{\mathcal{O}, P\}$. Further let W be the elliptic net of rank m associated to E and points $\mathsf{T} \in E(K)^m$. Choose $\mathsf{s}, \mathsf{p}, \mathsf{q} \in \mathbb{Z}^m$ such that*

$$P = \mathsf{p} \cdot \mathsf{T}, \qquad Q = \mathsf{q} \cdot \mathsf{T}, \qquad S = \mathsf{s} \cdot \mathsf{T}.$$

Then the Tate pairing τ_n satisfies

$$\tau_n(P, Q) = \frac{W(n\mathsf{p} + \mathsf{q} + \mathsf{s})W(\mathsf{s})}{W(n\mathsf{p} + \mathsf{s})W(\mathsf{q} + \mathsf{s})}.$$

We will only give a sketch of the proof. For details see [Sta07b].

Sketch of proof. Let

$$f_P = \frac{\Psi_{1,0,0}(-S, P, Q)}{\Psi_{1,n,0}(-S, P, Q)}.$$

Using 4.7 (one has to show that it is still true for the Ψ_v!) we can calculate the divisor of f_P as a function of S,

$$\mathrm{div}(f_P) = -([n]P) + (1-n)(\mathcal{O}) + n(P) = n(P) - n(\mathcal{O})$$

and see that the name for this function is indeed justified. Let $D_Q = (-S) - (-S - Q) \sim (Q) - (O)$. Using theorem 4.8 (again in K) with $T = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{smallmatrix}\right)$ we calculate

$$f_P(D_Q) = \frac{\Psi_{1,0,0}(S, P, Q)\Psi_{1,n,0}(S + Q, P, Q)}{\Psi_{1,n,0}(S, P, Q)\Psi_{1,0,0}(S + Q, P, Q)} = \frac{\Psi_{1,0,0}(S, P, Q)\Psi_{1,n,1}(S, P, Q)}{\Psi_{1,n,0}(S, P, Q)\Psi_{1,0,1}(S, P, Q)} \mod (K^*)^n$$

Transforming again (with $T = (\mathsf{s}, \mathsf{p}, \mathsf{q})^T$) we get in $K^*/(K^*)^n$:

$$\tau_n(P, Q) = f_P(D_Q) = \frac{\Psi_{1,0,0}(S, P, Q)\Psi_{1,n,1}(S, P, Q)}{\Psi_{1,n,0}(S, P, Q)\Psi_{1,0,1}(S, P, Q)} = \frac{W(n\mathsf{p} + \mathsf{q} + \mathsf{s})W(\mathsf{s})}{W(n\mathsf{p} + \mathsf{s})W(\mathsf{q} + \mathsf{s})}.$$

$\square$

Corollary 6.6. *Let n, E, K, P and Q be as above. Then*

$$\tau_n(P, Q) = \frac{W_{E,P,Q}(n+1, 1)W_{E,P,Q}(1, 0)}{W_{E,P,Q}(n+1, 0)W_{E,P,Q}(1, 1)}.$$

Proof. Take $\mathsf{T} = (P, Q)$, $\mathsf{p} = \mathsf{s} = (1, 0)$ and $\mathsf{q} = (0, 1)$. $\square$

As we have already discussed how to calculate values of an elliptic net, the corollary immediately yields a way to calculate the Tate pairing. The basic algorithm should not be much slower than an optimized version of Miller's algorithm. Optimization possibilities as well as an implementation for Sage can be found at `http://maths.straylight.co.uk/archives/110` and `http://maths.straylight.co.uk/archives/111`.

Chapter 7

Elliptic Curve Discrete Logarithm

Definition 7.1. Let G be a cyclic group with generator g. The *minimal multiplier* of an element $h \in G$ (with respect to g) is the smallest non-negative integer m such that $h = g^m$.

The *discrete logarithm problem* (DLP) in a cyclic group G is, given a generator g of G and an element $h \in G$, to find the minimal multiplier of h with respect to g.

The name "logarithm" is justified by the fact that the map

$$\log_g \colon h \mapsto \text{minimal multiplier of } h$$

is a homomorphism of a complicated "multiplicative" group G to the "easy" additive group $\mathbb{Z}/\operatorname{ord}(g)\mathbb{Z}$.

As we have seen in chapter 5, discrete logarithm problems in (finite) cyclic groups are of fundamental importance to cryptography. Of special interest for us is the case where $G = \langle P \rangle$ is a subgroup of an elliptic curve defined over a finite field. This is called the *elliptic curve discrete logarithm problem* (ECDLP). In general the ECDLP is believed to be hard (i.e. it is conjectured that there are no sub-exponential[1] algorithms to solve it for arbitrary elliptic curves). However in special instances of the ECDLP on might have additional useful information about the structure of the underlying elliptic curve. We will study several families of curves where we can exploit this knowledge to obtain sub-exponential (or even polynomial) time algorithms.

Using the Pohlig-Hellman reduction – which we will discuss in a moment – it is always possible to assume that the generator P has prime order. This will greatly simplify things. Then our strategy will be to construct an isomorphism of our given group $\langle P \rangle$ to a group where we already know how to solve the DLP (relatively) quickly. Of course we cannot just take any isomorphism, but one we can compute efficiently.

Before we discuss any specific attacks on th ECDLP we will have a look at generic methods to solve discrete logarithm problems and then study some groups which we will later take as targets for the isomorphisms.

7.1 General Purpose Methods

The following methods will work in every group. We will assume that $G = \langle g \rangle$ is a cyclic group of order n. We want to solve the DLP $h = [m]g$.

7.1.1 Pohlig-Hellman Reduction

Let $n = \prod p_i^{e_i}$ be the prime factor decomposition of n. The reduction of Pohlig and Hellman consists of three steps:

---

[1]An algorithm is said to have *sub-exponential* time, if it runs slower than polynomial, but faster than exponential time. A typical example is $O\left(2^{\sqrt{n}}\right)$.

1. *For each i, obtain $m \bmod p_i$*: Let $n_i = \frac{n}{p_i}$. Multiplication of the DLP by n_i gives the new DLP

$$h' = [n_i]h = [n_i]([m]g) = [m]\left([n_i]g\right) = [m]g'$$

   in the subgroup $\langle g' \rangle$ of order p_i. Solving this DLP yields $m_i^{(0)} = m \bmod p_i$.

2. *For each i, inductively obtain $m \bmod p_i^j$ until $j = e_i$*: Suppose $m_i^{(j)} = m \bmod p_i^j$ is known. Then there exists some (unknown) integer λ such that $m = m_i^{(j)} + \lambda p_i^j$. If we could determine $\lambda \bmod p_i$, then we would know $m_i^{(j+1)}$. Let $s = \frac{n}{p_i^{j-1}}$ and $l = h - [m_i^{(j)}]g = [\lambda]([p_i^j]g)$. We obtain the DLP

$$l' = [s]l = [s]\left([\lambda]([p_i^j]g)\right) = [\lambda]([n_i]g) = [\lambda]g',$$

   which yields $\lambda \bmod p_i$.

3. *Combine this information*: Use the Chinese Remainder Theorem to solve the system

$$m \equiv m_i^{(e_i)} \pmod{p_i^{e_i}}.$$

In conclusion the DLP in a group of order n is not harder than the DLP in a group of order p where p is the largest prime divisor of n. Therefore groups that are used in cryptosystems based on the DLP should have order that is prime or at least divisible by a large prime.

7.1.2 Baby-Step Giant-Step

The baby-step giant-step (BSGS) algorithm was first described by Shanks [Sha71]. It is a more sophisticated version of trail division and a classic example of space-time trade-off: it uses $O(\sqrt{n})$ space and time instead of $O(n)$ time and $O(1)$ space of the naive trail division.

There exist (unknown) integers $0 \leq i, j \leq \lceil \sqrt{n} \rceil$ such that $m = i \lceil \sqrt{n} \rceil + j$. The algorithm finds these integers by first precomputing $[j]g$ for all j and then searching for i.

Algorithm 7.2 (Baby-Step Giant-Step)**.** *Let g be of order n and $h \in \langle g \rangle$. The following algorithm returns* $\log_g h$.

1. Baby steps*: For all $0 \leq j \leq \lceil \sqrt{n} \rceil$, compute $[j]g$ and store the pair $(j, [j]g)$ in a lookup table[2].*

2. *Compute $g' = \left[- \lceil \sqrt{n} \rceil \right] g$ and set $h' \leftarrow h$, $i \leftarrow 0$.*

3. Giant steps*: For $0 \leq j \leq \lceil \sqrt{n} \rceil - 1$, check if h' is equal to the second component of the pair $(j, [j]g)$ stored in the table. If so, return $i \lceil \sqrt{n} \rceil + j$. Otherwise set $h' \leftarrow h' + g'$, $i \leftarrow i + 1$ and repeat step 3.*

7.1.3 Pollard-ρ

We will only describe the most basic version of the rho algorithm. Many improvements as well as Pollard's lambda algorithm (also known as Pollard's kangaroo algorithm) are described in [CF06, chapter 19]. Note that the algorithm can be efficiently parallelized; a description can be found at the same place.

Assume that we know two different pairs of integers (c, d) and (c', d') such that

$$[c]g + [d]h = [c']g + [d']h.$$

Then,

$$[c - c']g = [d - d']h = [d - d'][m]g.$$

Hence $m = (c - c')(d - d')^{-1} \bmod n$ (the existence of the inverse is guaranteed if we assume that n is prime). Therefore an approach to solving the DLP is to randomly choose pairs (c, d) and store $(c, d, [c]g + [d]h)$ into a lookup table until a collision occurs. By the birthday paradox the expected number of pairs needed before a there is a collision is about $\sqrt{\pi n / s} \approx 1.24\sqrt{n}$ [FGKP95]. Using the following idea of Pollard, one can eliminate the huge storage cost of this approach while keeping the expected $O(\sqrt{n})$ time complexity.

---

[2]In practice one would of course inductively compute $[j-1]g + g$. Also since the lookup will be on the second component one should use a hash table where hashing is done on the second component.

Let $f\colon G \to G$ be a function, called *iterating function*, such that given $x = [c]g + [d]h$ one can easily compute $c', d' \in [0, n-1]$ with $f(x) = [c']g + [d']h$. Further f should have the characteristic of a random function. One possibility for f is the following construction: let $G_1, \ldots G_r$ be a partition of G into r "random" subsets and select integers c_i, d_i $(1 \le i \le r)$. If $x \in G_i$, then take $f(x) = x + [c_i]g + [d_i]h$.

Let $x_0 \in G$. Then $x_{i+1} = f(x_i)$ defines a random walk in G. Since G is finite, there exist integers μ, τ such that $x_i = x_{i+\tau}$ for all $i \ge \mu$. The number τ is called *cycle length* and μ is called *tail length*. By the birthday paradox we expect that $\mu + \tau \approx \sqrt{\pi n/2}$. It possible to find a cycle without comparing all x_i using the following algorithm (note that this algorithm is not the fastest possibility, but the simplest one):

Algorithm 7.3 (Floyd's cycle-finding algorithm)**.** *Let $x_{i+1} = f(x_i)$ be a sequence as described above. The algorithm returns an index i such that $x_i = x_{2i}$.*

    1. Set $x \leftarrow f(x_0)$, $y \leftarrow f(x) = f(f(x_0))$, $i \leftarrow 1$.
    2. If $x = y$, return i.
    3. Set $i \leftarrow i + 1$, $x \leftarrow f(x)$, $y \leftarrow f(f(y))$.
    4. Return to 2.

One can show (see [Knu97, exercise 3.1.1]) that the number of iterations needed in this approach lies between μ and $\mu + \tau$. In particular the expected running time is $O(\sqrt{n})$. Once one has obtained a collision one can apply the idea we discussed at the beginning of the section to find m. There is a small chance that $d_i = d_{2i}$. In this case it is necessary to restart with a different x_0.

7.2   Index Calculus

We will now consider a group of algorithms collectively known as *index calculus*. We will first describe the general principle and then how it can be applied to the finite field DLP and the hyperelliptic DLP.

Definition 7.4. Let $\mathcal{P}$ be a countable set, called *primes*, and let $\mathcal{M}$ be the free Abelian monoid with free generators $\mathcal{P}$ such that there exists a congruence relation $\sim$ with $G \cong \mathcal{M}/\!\!\sim$. A *size map* is a map $|\cdot|\colon (\mathcal{M}, \oplus) \to (\mathbb{R}, +)$ such that all primes have positive size. Further let $\iota\colon G \to \mathcal{M}$ be a section, i.e. an injection with $[\iota(g)]_\sim = g$ for all $g \in G$. Then $(G, (\mathcal{M}, \oplus), \sim, \iota, |\cdot|)$ is called an (*arithmetic*) *formation*.

Definition 7.5. Let B be a positive integer, called *smoothness bound*. An element $g \in G$ is called *B-smooth* if the decomposition of $\iota(g) \in \mathcal{M}$ only contains primes of size less than B.

For notational convenience we will identify elements $g \in G$ with their representation $\iota(g) \in \mathcal{M}$.

Algorithm 7.6 (Index Calculus)**.** *Let $G = \langle g \rangle$ be a cyclic group of order n and let $h \in G$. Let $\mathcal{M}$ be a formation for G. The algorithm described below will return $\log_g h$.*

    1. *Construction of a factor base*:
       Define a set $S = \{p_1, \ldots, p_t\}$ of primes of $\mathcal{M}$. Typically one chooses a smoothness bound B and sets S to be the set of all B-smooth primes. The set S is called a *factor base*.

    2. *Gather relations*:
       Choose random numbers (a_i, b_i) and compute $[a_i]g + [b_i]h$. If this element can be decomposed over S, set

$$[a_i]g + [b_i]h = \bigoplus_{j=1}^{t} [e_{i,j}]p_j.$$

       If the element does not factor, choose a different pair (a_i, b_i). Let A be the matrix with rows

$$(e_{i,1}, e_{i,2}, \ldots, e_{i,t}).$$

       Keep adding rows to the matrix until there is linear relation between the rows (i.e. the map defined by A^T has nontrivial kernel). This should be the cases after $t + 1$ rows were added to A.

    3. *Linear algebra*:
       Compute a column vector x in the kernel of A^T, i.e. such that $A^T\mathsf{x} = 0$. This can be done by Gauß elimination or by a more sophisticated method.

4. *Extract the solution*:
   Let $\mathsf{a} = (a_1, \ldots, a_{t+1})$ and $\mathsf{b} = (b_1, \ldots, b_{t+1})$. The relations found in step (2) assert that

$$[\mathsf{ax}]g + [\mathsf{bx}]h = 0.$$

If $\gcd(\mathsf{bx}, n) = 1$, return

$$\log_g h = -\frac{\mathsf{ax}}{\mathsf{bx}} \bmod n.$$

Otherwise add relations to A and choose different vectors in the kernel of A^T until $\gcd(\mathsf{bx}, n) = 1$.

The efficiency of index calculus algorithms depends on the choice of a good factor base. Its size represents a trade-off between the relation gathering step and the linear algebra step. A larger factor base means that it is easer to find elements that are smooth with respect to the base. On the other hand a smaller factor base makes the linear algebra step faster. Further it should be easy to actually factor elements into prime factors of the base. See [CF06, chapter 20] for recommendations for implementations.

The most important point of elliptic curve cryptography is that it is highly unlikely that index calculus methods can be *directly* applied to solve the ECDLP (sometime they can be indirectly applied, see section 7.5). A discussion (with both theoretical and empirical evidence) why this is so is given in [SS98].

7.2.1   Finite Field DLP

Prime fields: The classical and easiest application of index calculus is in the multiplicative groups of prime fields $\mathbb{F}_p$. Here we can take $\mathcal{M} = \mathbb{N}$ which is freely generated (as a multiplicative monoid) by the usual prime numbers. As size of a natural number we take the bit length of its binary representation and ι is the canonical injection $\mathbb{F}_p \to \mathbb{N}$. With a suitable smoothness bound this yields a sub-exponential algorithm for the discrete logarithm problem in $\mathbb{F}_p$.

Non-prime fields: Every non-prime finite field $\mathbb{F}_q$ can be represented in the form $\mathbb{F}_p[X]/\langle f(X) \rangle$ for some polynomial $f(X) \in \mathbb{F}_p[X]$. Hence we can take $\mathcal{M} = \mathbb{F}_p[X]$. A polynomial in $\mathcal{M}$ is prime if it is monic and irreducible. The size of an element can be taken to be its degree.

The fastest known variant of index calculus for the general finite field DLP is a variant of the *number field sieve* as described in [Sch00]. Its running time is about $L_p[\frac{1}{3}, 1.923]$ where

$$L_n[\alpha, c] = O\left(e^{(c+o(1))(\ln n)^\alpha (\ln \ln n)^{1-\alpha}}\right).$$

For binary fields $\mathbb{F}_{2^d}$, the fastest know algorithm is Coppersmith's function field sieve [Cop84], which runs in $L_{2^d}[\frac{1}{3}, 1.588]$ time.

7.2.2   Hyperelliptic Curve DLP

Lemma 7.7. *Let $C/\mathbb{F}_q$ be a hyperelliptic curve and let (U, V) be a pair of polynomials in $\mathbb{F}_q[x]$ representing a semi-reduced divisor $D \in \mathrm{Div}^0_{\mathbb{F}_q}(C)$. Let $U(x) = \prod U_i(x)$ be the factorization of $U(x)$ into irreducible polynomials $U_i(x) \in \mathbb{F}_q[x]$. Further let $V_i = V \bmod U_i$ with $\deg V_i < \deg U_i$. Then each pair (U_i, V_i) represents a semi-reduces divisor D_i and $\sum D_i = D$. If D is reduced, so is each D_i.*

Proof. [Was08, proposition 13.12] $\square$

Definition 7.8. The *size* (in the sense of definition 7.4) of a semi-reduced divisor is the degree of the corresponding polynomial U. A semi-reduced divisor is called *prime*, if it has degree at least 1, is defined over $\mathbb{F}_q$ and cannot be written as a sum of semi-reduced divisors.

This is already enough to apply index calculus in the Jacobian of hyperelliptic curves. The factor base is selected as usual by a smoothness bound B. For small genera one usually takes $B = 1$. To list all elements of the factor base, one can simply look at every irreducible polynomial T in $\mathbb{F}_q[x]$ of degree at most B and then find a suitable $W \in \mathbb{F}_q[x]$ such that (T, W) is the Mumford representation of a divisor class. This is of course rather trivial in the case $B = 1$.

Note that for elliptic curves every semi-reduced divisor has size 1 and is prime. Therefore this definition does not help to apply index calculus methods on elliptic curves.

With some optimizations this approach gives the algorithms behind the following result:

Theorem 7.9 ([Thé03])**.** *Let $C/\mathbb{F}_q$ be an elliptic curve of genus g. Let $\varepsilon > 0$ be arbitrary.*

1. *If $q > (g-1)!$, then there exists an algorithm that solves the DLP in the Jacobian of C in $O\left(g^5 q^{2-\frac{2}{g+1}+\varepsilon}\right)$ time.*

2. *If $q < \frac{(g-1)!}{g}$, then there exists an algorithm that solves the DLP in the Jacobian of C in $O\left(g^5 q^{2-\frac{2}{2g+1}+\varepsilon}\right)$ time.*

In particular for $g \geq 3$ the hyperelliptic DLP can be asymptotically solved faster than with the general purpose algorithms.

More algorithms for the hyperelliptic DLP and possible optimizations are described in [CF06, chapter 21].

7.3   Pairing Based Attacks

We can now return to our goal of providing sub-exponential algorithms for the ECDLP on some special curves. The first such result was published by Menezes, Okamoto and Vanstone in 1993 [MOV93] and became known as the MOV attack. Shortly afterwards it was generalized by Frey and Rück [FR94, FMR99] to the divisor class groups of general curves. The idea of these attacks is to use a pairing on the elliptic curve to reduce the ECDLP to a finite field DLP.

We will again denote the underlying elliptic curve defined over $\mathbb{F}_q$ (with $q = p^r$) by E. Further let $P \in E(\mathbb{F}_q)$ be of prime order n and $Q \in \langle P \rangle$. Our aim is to recover an integer m such that $Q = [m]P$.

Suppose that $\mathbb{F}_q$ contains the nth roots of unity and that we have a bilinear pairing $e\colon G_1 \times G_2 \to \boldsymbol{\mu}_n$ where the G_i are subgroups of $E(\mathbb{F}_q)$ and $P \in G_1$. Suppose further that we have a point S with $e(P,S) \neq 1$. Then, since n is prime, $e(P,S)$ is a primitive n^{th} root. By linearity

$$e(Q,S) = e([m]P,S) = e(P,S)^m$$

gives a DLP-equation in $\mathbb{F}_q$ which can be solved with index calculus methods.

We already studied two pairings on E with values in $\boldsymbol{\mu}_n$: the Weil pairing e_n (2.44) and the modified Tate-Lichtenbaum pairing $\widetilde{\tau}_n$ (3.7). In fact the first one is used in the MOV attack while the second one is used in the Frey-Rück attack. We note that by theorem 3.43 the Tate pairing is defined on $E(\mathbb{F}_q)$ whenever the Weil pairing is defined there. (The converse is not always true. However by theorem 3.45 it is true in most cryptographically interesting situations.) Also in general the Tate pairing can be computed faster then the Weil pairing. Therefore we will only describe the Frey-Rück attack.

Algorithm 7.10 (MOV/Frey-Rück)**.** *Let E be an elliptic curve over $\mathbb{F}_q$ and $P \in E(\mathbb{F}_q)$ of prime order n and coprime to q. Further let $Q \in \langle P \rangle$. The following algorithm returns the minimal multiplier of Q with respect to P.*

1. *Construct a field $\mathbb{F}_{q^k}$ such that $n \mid q^k - 1$.*

2. *Choose a random point $S \in E(\mathbb{F}_{q^k})$.*

3. *Set $A \leftarrow e(P,S)$. If $A = 1$ return to 2 and choose a different point S.*

4. *Set $B \leftarrow e(Q,S)$.*

5. *Find $m \bmod n$ such that $A^m = B$ using index calculus methods in $\mathbb{F}_{q^k}$.*

6. *Return m.*

Since the Tate pairing is non-degenerate and n is prime, its image contains a primitive n^{th} root of unity and hence the map $S \mapsto \tau_n(P, S)$ is surjective. By linearity the size of its kernel is $\frac{|E(K)/nE(K)|}{|\boldsymbol{\mu}_n|}$. So the probability that $\tau_n(P, S) = 1$ is $\frac{1}{|\boldsymbol{\mu}_n|} = \frac{1}{n}$ for a random S. Considering that n is typically quite large, we expect that a suitable point S is picked on the first try virtually every time.

We already know that we can compute the Tate pairing in polynomial time (in $k \log q$), so by far the most computational expensive part is step 5. Thus the whole algorithm runs in sub-exponential time in $k \log q$. For most curves one can expect k to be fairly large and this attack will not reduce the computation time. However, we have seen in corollary 3.51 that supersingular elliptic curves have embedding degree at most 6. Hence we get the following result:

Corollary 7.11. *On supersingular elliptic curves the ECDLP can be solved in sub-exponential running time.*

In practice it is easy to avoid curves with small k as a random curve will have a big embedding degree with high probability [BK98]. Historically however, supersingular curves have been proposed for elliptic curve cryptography schemes. See section V of [MOV93] for further discussion.

7.4   Anomalous Curves

In principle the Frey-Rück attack applies to all elliptic curves $E/\mathbb{F}_{p^l}$ with $\gcd(\#E(\mathbb{F}_q), p) = 1$. Thus an obvious way to create secure elliptic curve cryptosystems would be to take curves with $\#E(\mathbb{F}_q) = q$, i.e. curves where the qth power Frobenius has trace 1. Such curves are called *anomalous*. Unfortunately it turned out that the ECDLP on anomalous curves can be broken in linear time. There are two different approaches to the anomalous curve DLP: one by Smart [Sma99] and Satoh and Araki [SA98] and one by Semaev [Sem98]. The first idea is rather number theoretic and uses properties special to elliptic curves while Semaev's approach comes from algebraic geometry and can be generalized to curves of higher genus [Rüc99]. Even though Semaev's (and Rück's) results are stronger, both approaches are interesting and we will present both.

For Smart's and Satoh-Araki's   technique let $K = \mathbb{F}_p$ and $\#E(\mathbb{F}_p) = p$ where p is a prime number. As usual we have two points $Q = [m]P$ and have to solve for m. Obviously $\operatorname{ord} P = p$. The first step is to compute and arbitrary lift of P and Q to points $\mathcal{P}, \mathcal{Q}$ on an elliptic curve $\mathcal{E}$ over $\mathbb{Q}_p$ that reduces to $E(\mathbb{F}_p)$ modulo $p\mathbb{Z}_p$ (the maximal ideal of the ring of integers $\mathbb{Z}_p$ in the local field $\mathbb{Q}_p$). In order to do this choose any lifts of the x-coordinates of the points and calculate the y-coordinates with Hensel's lemma 3.67.

By the general theory of elliptic curves over local fields we have the exact sequences

$$0 \to \mathcal{E}_1(\mathbb{Q}_p) \to \mathcal{E}_0(\mathbb{Q}_p) \to E(\mathbb{F}_p) \to 0, \tag{7.1}$$

$$0 \to \mathcal{E}_2(\mathbb{Q}_p) \to \mathcal{E}_1(\mathbb{Q}_p) \to \mathbb{F}_p^+ \to 0. \tag{7.2}$$

Define an isomorphism

$$\log_p = \log_{\widehat{\mathcal{E}}} \circ \vartheta_1^{-1} \colon \mathcal{E}_1(\mathbb{Q}_p) \to p\mathbb{Z}_p,$$

where ϑ_1 is the isomorphism defined in theorem 3.99. This is well defined by theorem 3.86. The restriction gives isomorphisms $\mathcal{E}_n(\mathbb{Q}_p) \to p^n\mathbb{Z}_p$ for $n \geq 1$.

Since E is non-singular, $\mathcal{E}_0(\mathbb{Q}_p) = \mathcal{E}(\mathbb{Q}_p)$. In general it is not the case that $[m]\mathcal{P} = \mathcal{Q}$. However,

$$[m]\mathcal{P} = \mathcal{Q} \mod \mathcal{E}_1(\mathbb{Q}_p).$$

Let $\mathcal{R} = \mathcal{Q} - [m]\mathcal{P} \in \mathcal{E}_1(\mathbb{Q}_p)$. By (7.2),

$$[p]\mathcal{Q} - [m]([p]\mathcal{P}) = [p]\mathcal{R} \in \mathcal{E}_2(\mathbb{Q}_p).$$

By (7.1), $[p]\mathcal{P} \in \mathcal{E}_1(\mathbb{Q}_p)$ for every point $\mathcal{P} \in \mathcal{E}(\mathbb{Q}_p)$ (here we use the anomaly of $E/\mathbb{F}_p$). Hence we can take the logarithm of the last equation:

$$\log_p([p]\mathcal{Q}) - m\log_p([p]\mathcal{P}) = \log([p]\mathcal{R}) \equiv 0 \mod p^2\mathbb{Z}_p.$$

Thus all we have to do is to solve a DLP in $\mathbb{Z}_p/p^2\mathbb{Z}_p = \mathbb{Z}/p^2\mathbb{Z}$, i.e. to calculate

$$m \equiv \frac{\log_p([p]\mathcal{Q})}{\log_p([p]\mathcal{P})} \pmod{p^2}.$$

It suffices to do all calculations modulo p^2 so the only nontrivial calculations that have to be done are the $O(\log p)$ group operations on $\mathcal{E}$. With a very small possibility $(1/p)$ the denominator $\log_p([p]\mathcal{P})$ vanishes. In this case one can simply take a different lift $\mathcal{E}$.

The attack of Semaev-Rück uses a different approach to construct a "logarithm". As we have seen in theorem 2.13 there is an isomorphism $\kappa : E \to \mathrm{Pic}^0(E)$ mapping a point P to the class of $D_P = (P) - (\mathcal{O})$. Let $\mathrm{Pic}^0(E)_p = \kappa(E[p])$. To each class $\bar{D} \in \mathrm{Pic}^0(E)_p$ associate a function f with $pD = \mathrm{div}(f)$. While logarithms might not be defined in K we can still look at the logarithmic differential $\frac{df}{f}$. By a result of Serre [Ser58, Proposition 10] this defines an isomorphism of $\mathrm{Pic}^0(E)_p$ into the space of holomorphic differentials of E. Let $t = -\frac{x}{y}$ be a uniformizer at $\mathcal{O}$ and look at the power series expansion

$$\frac{df/dt}{f} = \sum_{i \geq 0} a_i t^i.$$

Remember that $\mathscr{L}(K_E) \cong \{\omega \in \Omega_E : \omega \text{ is holomorphic}\}$ and $\ell(K_E) = g = 1$. Hence $\frac{df/dt}{f}$ is uniquely determined by a_0. So we get an isomorphism $\phi \colon E[p] \to \bar{K}^+$ sending a point P to

$$\phi(P) = \frac{df_P/dt}{f_P}(\mathcal{O}) \in \bar{K},$$

where f_P is a rational function on E with $\mathrm{div}(f_P) = p(P) - p(\mathcal{O})$. Actually, since everything is defined over K, we have $\phi(P) \in K$. Then in order to solve the ECDLP $[m]P = Q$, we only need to solve $m\phi(P) = \phi(Q)$ in K, which is trivial.

The hard part of this procedure is to calculate f_P. However, this is not needed. It is possible to obtain $\phi(P)$ without knowing f_P using the following idea: For arbitrary points $P_1, P_2 \in E(K)$ define a function h_{P_1,P_2} by $\mathrm{div}(h_{P_1,P_2}) = (P_1) + (P_2) - (P_1 + P_2) - (\mathcal{O})$. Then up to multiplication with a constant,

$$h_{P_1,P_2} = \frac{l_{P_1,P_2}}{l_{P_1+P_2,\mathcal{O}}}$$

where $l_{P,Q} = 0$ is the equation of the line through P and Q. Let $\delta(P_1, P_2)$ be the constant term of $\frac{dh_{P_1,P_2}/dt}{h_{P_1,P_2}}$. On the set $E[p] \times K$ define a group law by

$$(P_1, v_1) \odot (P_2, v_2) = (P_1 + P_2, v_1 + v_2 + \delta(P_1, P_2)).$$

Then using induction one can show that

$$\underbrace{(P, 0) \odot \cdots \odot (P, 0)}_{p \text{ times}} = (\mathcal{O}, \phi(P)).$$

Hence using a double-and-add algorithm the ECDLP can be solved in $O(\log p)$ time. Further one can show that $\delta(P_1, P_2)$ is just the slope of the line through P_1 and P_2 (the slope of the tangent if $P_1 = P_2$, and 0 if $P_1 = -P_2$).

A slight reformulation of this algorithm can be applied to p-torsion points in curves of higher genus [Rüc99].

7.5 Weil Descent Attacks

Attacks on the ECDLP using the so-called "Weil descent" method[3] are a relatively new invention. The possibility of these attacks was first recognized by Frey [Fre98]. The first successful application was given

---

[3]The usage of the term "Weil descent" in cryptography is different from its usage in general algebraic geometry were it describes a proof technique similar to Fermat's infinite descent.

by Gaudry, Heß and Smart in 2002 [GHS02]. After the names of the inventors it is called the *GHS attack*. The application of Weil decent to elliptic and hyperelliptic curve DLP is still a subject of ongoing work.

Usually these attacks use more sophisticated parts of algebraic geometry than we have introduced in chapter 1. However, it is relatively simple to describe the basic idea. We will give the following definitions only for projective varieties (in the sense of definition 1.15). The usual definitions are far more general, see for example [BLR90].

Definition 7.12. An *Abelian variety* is a projective variety G with a group structure on G such that the group operations $\cdot\colon G \times G \to G$ and $^{-1}\colon G \to G$ are given by regular maps.

Proposition 7.13. *An Abelian variety is an Abelian group.*

Proof. [Sha94a, theorem III.4.2]   □

Definition 7.14. Let $L|K$ be a field extension of degree s and let $X \subset \mathbb{A}^n$ be an affine variety defined over L. Then the *Weil restriction* or *restriction of scalars* of X with respect to $L|K$, denoted $\mathrm{Res}_{L|K}(X)$, is defined in the following way:

Let $f_1, \ldots, f_m \in L[X_1, \ldots, X_n]$ define X and let $\alpha_1, \ldots, \alpha_s \in L$ be a basis of L over K. Further let $Y_{i,j}$ with $1 \leq i \leq n, 1 \leq j \leq s$ be new variables. Define polynomials $g_{l,r} \in K[Y_{i,j}]$ such that $f_t = g_{t,1}\alpha_1 + \cdots + g_{t,s}\alpha_s$ $(1 \leq t \leq m)$ with $X_i = Y_{i,1}\alpha_1 + \cdots + Y_{i,s}\alpha_s$. Then $\mathrm{Res}_{L|K}(X)$ is the variety in $\mathbb{A}^{ns}$ given by $\langle g_{r,s} \rangle$. Obviously it is defined over K.

For projective varieties the construction can be carried through by passing first to a non-empty affine piece of X, then to its Weil restrictions and finally to the projective closure of the Weil restriction.

There exists a natural bijection between $\mathrm{Res}_{L|K}(X)$ and X given by

$$(y_{i,j})_{i,j} \in \mathbb{A}^{ns} \mapsto (y_{i,1}\alpha_1 + \cdots + y_{i,s}\alpha_s)_i \in \mathbb{A}^n$$

(respectively the homogenization of this map). If X is an Abelian variety, this induces a group structure on $\mathrm{Res}_{L|K}(X)$ which makes $\mathrm{Res}_{L|K}(X)$ into an Abelian variety. If additionally the group operations on X are defined over L, then the group operations on $\mathrm{Res}_{L|K}(X)$ are defined over K and $X(L) \cong \mathrm{Res}_{L|K}(X)(K)$.

We will now describe the idea behind Weil descent attacks as introduced in [GS99]. Let $X = E$ be an elliptic curve defined over a finite field $L = \mathbb{F}_{q^s}$. Using Weil restriction the DLP in $E(\mathbb{F}_q)$ can be transfered to a DLP in $\mathrm{Res}_{\mathbb{F}_{q^s}|\mathbb{F}_q}(E)(\mathbb{F}_q)$. Let $A = \mathrm{Res}_{\mathbb{F}_{q^s}|\mathbb{F}_q}(E)$ and $K = \mathbb{F}_q$. In general the structure of A is quite complicated. However, suppose we can find a curve C^0 defined over K and a map $C^0 \to \mathrm{Res}_{L|K}(E)$. Then by the universal property of the Jacobian [GS99, proposition 1] this map induces a homomorphism $\phi\colon J(C^0) \to A$. If we find a suitable curve such that we can lift the DLP from $A(K)$ to $J(C^0)(K)$ we might be able to efficiently solve it using index calculus methods in $J(C^0)$. In particular, this is the case if C^0 is a hyperelliptic curve.

The GHS attack implements this idea for some curves over binary fields. Details as well as further results are collected in [BSS05, chapter VIII]. The important implication of these attack is that the security of curves over a field $\mathbb{F}_{p^k}$ might suffer if k is composite, especially if it is divisible by a small integer larger than 2 (since [BSS05] was written further improvements have been made, e.g. [Gau08]). The usual recommendation it to use only prime fields or fields of prime extension degree.

7.6   Connection to Elliptic Divisibility Sequences

We will give a short description of the ideas of Lauter and Stange [LS08] which might be used in the future for devising new attacks on the ECDLP – or proving that some families of elliptic curves are secure.

In this section we will always assume that $\mathrm{ord}\, P$ and $q - 1$ are coprime. This is no real restriction because if this was not the case than we could use the Frey-Rück attack.

7.6.1   The EDS Discrete Logarithm Problem

The *width s EDS discrete logarithm problem* (EDSDLP) is to find the integer k given an EDS W in $\mathbb{F}_q$ and terms $W(k), W(k+1), \ldots, W(k+s-1)$.

Theorem 7.15. *If one of the following problems is solvable in sub-exponential time, then both are:*

1. *the elliptic curve discrete logarithm;*
2. *the width 3 EDS discrete logarithm for perfectly periodic sequences associated to a curve (see definition 4.21).*

Proof. First assume that we can solve the ECDLP in sub-exponential time. We are given an elliptic curve E over $\mathbb{F}_q$, a point P of prime order n (with $\gcd(n, q-1) = 1$) and terms $\widetilde{W}_{E,P}(k)$, $\widetilde{W}_{E,P}(k+1)$ and $\widetilde{W}_{E,P}(k+2)$. We will show that the point $Q = [k+1]P$ can be calculated in probabilistic $O((\log q)^4)$ time without knowledge of k. Then we can use the sub-exponential algorithm for the ECDLP to solve for k.

Using theorem 3.27 we have

$$x([m]P) = x(P) - \frac{\widetilde{W}_{E,P}(m)\widetilde{W}_{E,P}(m+1)}{\widetilde{W}_{E,P}(m)^2}, \tag{7.3}$$

where $x(P)$ is the x-coordinate of P. From this we can calculate $x([k+1]P)$ in $O((\log q)^2)$ time. Then we can compute the two possible values for the corresponding y-coordinate in probabilistic $O((\log q)^4)$ time [BS96]. In order to find out which value of y is the correct one we choose one of the values and calculate $x([k+2]P)$ and $x([k+3]P)$ using addition on the elliptic curve. Next we use (7.3) to determine $\widetilde{W}(k+3)$ and $\widetilde{W}(k+4)$ in turn. Since 4 consecutive terms of an EDS determine the entire sequence, we simply have to check whether

$$\widetilde{W}(k+4)\widetilde{W}(k) = \widetilde{W}(k+1)\widetilde{W}(k+3)\widetilde{W}(2)^2 - \widetilde{W}(3)\widetilde{W}(1)\widetilde{W}(k+2)^2.$$

If this holds, then our choice was correct, otherwise we have to take the other possible value for y.

Now assume that we can solve the EDSDLP in sub-exponential time. We are again given an elliptic curve E over $\mathbb{F}_q$, a point P of prime order n with $\gcd(n, q-1) = 1$ and a point $Q = [k]P$. We will show that we can calculate $\widetilde{W}_{E,P}(k)$ in $O((\log q)^3)$ time without knowledge of k. Then we can do the same for $Q + P$ and $Q + P + P$ and we get an instance of the EDSDLP. We will of course use formula (4.3) which states

$$\Phi(P) = \left(\frac{W_{E,P}(q-1)}{W_{E,P}(q-1+n)} \right)^{\frac{1}{n^2}}.$$

By theorem 6.1 we can compute the terms $W_{E,P}(q-1)$ and $W_{E,P}(q-1+n)$ in $O((\log q)^2(\log(q-1) + \log(q-1+n))$ time. By Hasse's theorem, $n = O(q)$, so this is $O((\log q)^3)$. Finding the inverse of n^2 mod $q-1$ and raising to that power are also $O((\log q)^3)$ operations. $\qquad\square$

7.6.2   EDS Association and EDS Quadratic Residuosity

Assume again that we are given an elliptic curve E over $K = \mathbb{F}_q$ and a point $P \in E(K)$ of prime order $n = \operatorname{ord} P$ with $n > 3$ and $\gcd(n, q-1) = 1$.

The *EDS association problem* is, given a point $Q \in \langle P \rangle$, to calculate $W_{E,P}(k)$, where k is the minimal multiplier of Q. The *EDS residue problem* is to determine the quadratic residuosity of $W_{E,P}(k)$ (in K). Note that while it is easy to determine $\widetilde{W}_{E,P}(k)$ without knowledge of k, there are no known fast algorithms for determining $W_{E,P}(k)$.

We will start with an observation that is true for any discrete logarithm problem:

Lemma 7.16. *Let G be a cyclic group of odd order q and let P be a generator of G. Suppose we are given an oracle that, given an element $[k]P \in G$, can determine the parity of k. Then the discrete logarithm problem in G can be solved in $O(\log q)$ steps where each step consists of one call to the oracle and $O(\log q)$ operations in the group.*

Proof. Suppose that we are given $Q = [k]P$. The following algorithm will determine the minimal multiplier k of Q.

1. Set $k = 1$.
2. If $Q = P$, stop with result k.
3. Use the oracle to determine the parity $\lambda \in \{0, 1\}$ of the minimal multiplier of Q. Find Q' such that $[2]Q' = Q - \lambda P$ and set $k = 2k + \lambda$.
4. Set $Q = Q'$ and continue with step 2.

Since the order of the group is odd, there is a unique Q'. It can be calculated by determining $l = 2^{-1}$ (mod $|G|$) (with the Euclidean algorithm) and calculating $Q' = [l](Q - [\lambda]P)$ (with a double-and-add algorithm in $O(\log q)$ operations). The number of steps required is $O(\log_2 k) = O(\log q)$. $\qquad\square$

We return to elliptic curves. Let E, $K = \mathbb{F}_q$, $P \in E(\mathbb{F}_q)$, $n = \operatorname{ord} P$ and $Q = [k]P$ as above.

Theorem 7.17. *If one of the following problems is solvable in sub-exponential time, then both are:*

1. *elliptic curve discrete logarithm;*
2. *EDS association;*

Proof. If we can solve the ECDLP, we can calculate k in sub-exponential time and then use theorem 6.1 to calculate $W_{E,P}(k)$ in polynomial time.

If we can solve the EDS association problem, we know $W_{E,P}(k)$. By theorem 4.20,

$$\frac{\Phi(Q)}{W_{E,P}(k)} = \Phi(P)^{k^2}, \tag{7.4}$$

so we can reduce the ECDLP to a DLP in $\mathbb{F}_q$, which is solvable in sub-exponential time. $\qquad\square$

Theorem 7.18. *Suppose that* $\operatorname{char} K \neq 2$ *and that* $\Phi(P)$ *is a quadratic non-residue of K. If one of the following problems is solvable in sub-exponential time, then both are:*

1. *elliptic curve discrete logarithm;*
2. *EDS quadratic residue.*

Of course the assumption that q is not a power of 2 is necessary since otherwise $x \mapsto x^2$ would be an automorphism and hence every element of K a quadratic residue. If $\Phi(P)$ is a quadratic residue then we can try to find an integer m such that $\Phi([m]P)$ is a quadratic non-residue and consider the equivalent problem $[m]Q = [k]([m]P)$. If -1 is a quadratic non-residue, then we can take $m = n - 1$ because $\Phi([n-1]P) = \Phi(-P) = -\Phi(P)$.

Proof. If we can solve the ECDLP then, by the last theorem, we also know $W_{E,P}(k)$ and can calculate its residuosity in polynomial time [BS96].

Assume that we can solve the EDS quadratic residue problem. Looking at (7.4) we can determine the quadratic residuosity of the left hand side in polynomial time. We know that $\Phi(P)$ is a quadratic non-residue. Thus if the left hand side is a quadratic residue, then k^2 must be even; otherwise it must be odd. Using this we apply lemma 7.16. $\qquad\square$

Lauter and Stange argue in [LS08] that the knowledge of the value or residuosity of any product of the form

$$\prod_{i=1}^{N} W_{E,P}(p_i(k))^{e_i},$$

where $p_i(x) \in \mathbb{Z}[x]$ and $e_i \in \mathbb{Z}$ with some restrictions, is sufficient to solve the ECDLP. For example they deduce the equation

$$\left(\frac{W_{E,P,Q}(n+1,0)W_{E,P,Q}(2,0)}{W_{E,P,Q}(n+2,0)} \right)^k = \left(\frac{W_{E,P}(k-1)}{W_{E,P}(k)} \right)^n \left(-\frac{W_{E,P,Q}(1,n)W_{E,P,Q}(2,0)}{W_{E,P,Q}(2,n)W_{E,P,Q}(1,-1)^n} \right).$$

Here everything except $\frac{W_{E,P}(k-1)}{W_{E,P}(k)}$ can be calculated in polynomial time and when we assume knowledge of that term, the equation yields a $\mathbb{F}_q$ DLP. Note that if $n = q - 1$, then $\left(\frac{W_{E,P}(k-1)}{W_{E,P}(k)} \right)^n = 1$ and we do not need to know anything about the fraction. Also Shipsey [Shi00, eq. (6.3)] deduces an equation of this type:

$$\frac{W_{E,P}((n+1)(k+1))W_{E,P}(k)}{W_{E,P}((n+1)k)W_{E,P}(k+1)} = W_{E,P}(n+1)^{2k+1}.$$

7.7   Quantum Computers

As we have seen in this chapter there are several attacks on the ECDLP that could severely reduce the
security of an ECC scheme. However, they only apply to very special curves. If one avoids all curves
where security has already been reduced or that look like they could be threatened by future attacks
there are still plenty of curves left. Indeed, the general opinion amongst researchers seems to be that
a complete breach of ECC security on *classical* computers will never happen. On the other hand, in
quantum computing the situation is different: there already exists an algorithm that solves the ECDLP in
quantum polynomial time [PZ03, CMMP07]. Therefore whenever quantum computing would move nearer
to existence (currently there are still severe technical problems preventing its realization), it would be
prudent to abandon ECC. Unfortunately this is true for almost all classical encryption schemes, including
symmetric schemes.

Bibliography

[AM69]   Michael F. Atiyah and Ian G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley, Reading, MA, 1969.

[BB87]   Jonathan M. Borwein and Peter B. Borwein. *Pi and the AGM*. Wiley, New York, 1987.

[BK98]   R. Balasubramanian and Neil Koblitz. The Improbability That an Elliptic Curve Has Subexponential Discrete Log Problem under the Menezes-Okamoto-Vanstone Algorithm. *Journal of Cryptology*, 11(2):141–145, 1998.

[BLR90]   S. Bosch, W. Lutkebohmert, and M. Raynaud. *Neron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*. Springer, Berlin, 1990.

[Bou89]   Nicolas Bourbaki. *Commutative Algebra: Chapters 1-7*. Springer, 1989.

[BS96]   Eric Bach and Jeffrey Shallit. *Algorithmic Number Theory, Volume 1: Efficient Algorithms*. MIT Press, Cambridge, MA, 1996.

[BSS99]   Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart, editors. *Elliptic Curves in Cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1999.

[BSS05]   Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart, editors. *Advances in Elliptic Curve Cryptography*, volume 317 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2005.

[Can87]   David G. Cantor. Computing in the Jacobian of a Hyperelliptique Curve. *Mathematics of Computation*, 48:95–101, 1987.

[CF06]   Henri Cohen and Gerhard Frey, editors. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[Cha85]   Komaravolu Chandrasekharan. *Elliptic Functions*, volume 281 of *Grundlehren der Mathematischen Wissenschaften*. Springer, Berlin Heidelberg, 1985.

[CMMP07]   Donny Cheung, Dimitri Maslov, Jimson Mathew, and Dhiraj K. Pradhan. On the Design and Optimization of a Quantum Polynomial-Time Attack on Elliptic Curve Cryptography. October 2007.

[Con78]   John B. Conway. *Functions of One Complex Variable*, volume 11 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 1978.

[Cop84]   Don Coppersmith. Fast Evaluation of Logarithms in Fields of Characteristic Two. *IEEE Transactions on Information Theory*, 30(4):587–594, 1984.

[CR88]   Leonard S. Charlap and David P. Robbins. An elementary introduction to elliptic curves. CRD Expository Report 31. Technical report, Center for Communications Research, Princeton, Dec 1988. Available from: `http://www.idaccr.org/reports/reports.html`.

[Dar99]   Henri Darmon. A Proof of the Full Shimura-Taniyama-Weil Conjecture Is Announced. *Notices of the AMS*, 46(11):1397–1401, Dec 1999.

[Del74]   Pierre Deligne. La conjecture de Weil. I. *Publications Mathématiques de L'IHÉS*, 43(1):273–307, 1974.

[Deu41]   Max Deuring. Die Typen der Multiplicatorenringe elliptischer Funktionenkörper. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 14:197–272, 1941.

[DH76]   Whitfield Diffie and Martin E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[Dwo60]   Bernard Dwork. On the rationality of the zeta function of an algebraic variety. *American Journal of Mathematics*, 82(3):631–648, July 1960.

[Eis95]   David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer, 1995.

[EvSW03]   Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. *Recurrence Sequences*, volume 104 of *Mathematical Surveys and Monographies*, chapter Elliptic Divisibility Sequences. American Mathematical Society, Providence, 2003.

[FGKP95]   Philippe Flajolet, Peter J. Grabner, Peter Kirschenhofer, and Helmut Prodinger. On Ramanujan's Q-function. *Journal of Computational and Applied Mathematics*, 58(1):103–116, 1995.

[FMR99]   Gerhard Frey, Michael Müller, and Hans-Georg Rück. The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems. *IEEE Transactions on Information Theory*, 45(5):1717–1719, July 1999.

[FR94]   Gerhard Frey and Hans-Georg Rück. A Remark Concerning m-Divisibilty and the Discrete Logarithm in the Divisor Class Group of Curves. *Mathematics of Computation*, 62(206):865–874, April 1994.

[Fre98]   Gerhard Frey. How to disguise an elliptic curve (Weil descent), 1998. Talk at ECC '98 (Waterloo). Available from: `http://www.cacr.math.uwaterloo.ca/conferences/1998/ecc98/frey.ps`.

[Ful89]   William Fulton. *Algebraic Curves*. Addison-Wesley, 1989. reissue.

[Gau08]   Pierrick Gaudry. Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem. *Journal of Symbolic Computation*, 2008. to appear in print. `doi:10.1016/j.jsc.2008.08.005`.

[GHS02]   Pierrick Gaudry, Florian Heß, and Nigel P. Smart. Constructive and Destructive Facets of Weil Descent on Elliptic Curves. *Journal of Cryptology*, 15(1):19–46, 2002. `doi:10.1007/s00145-001-0011-x`.

[Gro64]   Alexander Grothendieck. Formule de Lefschetz et rationalité des fonctions L. *Séminaire Bourbaki*, 9(279), 1964.

[GS99]   Steven D. Galbraith and Nigel P. Smart. A Cryptographic Application of Weil Descent. In *Cryptography and Coding*, volume 1746 of *Lecture Notes in Computer Science*, pages 191–200, Berlin Heidelberg, 1999. Springer. `doi:10.1007/3-540-46665-7_23`.

[Har77]   Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer, New York, 1977.

[Heß04]   Florian Heß. A Note on the Tate Pairing of Curves over Finite Fields. *Archiv der Mathematik*, 82:28–32, 2004.

[HMV04]   Darrel Hankerson, Alfred J. Menezes, and Scott Vanstone. *Guide to Elliptic Curve Cryptography*. Springer, New York, 2004.

[Hus04]   Dale Husemöller. *Elliptic Curves*. Springer, New York, second edition, 2004.

[HW60]   G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, Oxford, fourth edition, 1960.

[Kie73]   L. Kiepert. Wirkliche Ausführung der ganzzahligen Multiplication der elliptischen Functionen. *Journal für die reine und angewandte Mathematik*, 76:21–33, 1873.

[KKM08]   Ann Hibner Koblitz, Neil Koblitz, and Alfred J. Menezes. Elliptic Curve Cryptography: The Serpentine Course of a Paradigm Shift. *Preprint*, 2008. Available from: `http://eprint.iacr.org/2008/390`.

[Knu97]   Donald E. Knuth. *The Art of Computer Programming. Volume 2: Seminumerical Algorithms.* Addison-Wesley, Boston, MA, third edition, 1997.

[Kob84]   Neil Koblitz. *p-Adic Numbers, p-Adic Analysis, and Zeta-Functions*, volume 58 of *Graduate Texts in Mathematics.* Springer, New York, second edition, 1984.

[Kob87]   Neil Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48:203–209, 1987.

[Kob89]   Neil Koblitz. Hyperelliptic Cryptosystems. *Journal of Cryptology*, 1(3):139–150, 1989.

[Kob93]   Neil Koblitz. *Introduction to Elliptic Curves and Modular Forms*, volume 97 of *Graduate Texts in Mathematics.* Springer, New York, 1993.

[Kra05]   Hugo Krawczyk. HMQV: A High-Performance Secure Diffie-Hellman Protocol. *Preprint*, 2005. Available from: `http://eprint.iacr.org/2005/176.pdf`.

[Lan78]   Serge Lang. *Elliptic Curves. Diophantine Analysis*, volume 231 of *Grundlehren der Mathematischen Wissenschaften.* Springer, Berlin Heidelberg, 1978.

[Lan82]   Serge Lang. *Introduction to Algebraic and Abelian Functions*, volume 89 of *Graduate Texts in Mathematics.* Springer, New York, second edition, 1982.

[Lan87]   Serge Lang. *Elliptic Functions*, volume 112 of *Graduate Texts in Mathematics.* Springer, New York, second edition, 1987.

[Lan02]   Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics.* Springer, New York, revised third edition, 2002.

[Len87]   Jr H. W. Lenstra. Factoring integers with elliptic curves. *Annals of Mathematics*, 126:649–673, 1987.

[LS08]   Kristin E. Lauter and Katherine E. Stange. The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences. *Preprint*, August 2008. `arXiv:0803.0728`.

[LST64]   Jonathan Lubin, Jean-Pierre Serre, and John Tate. Elliptic Curves and Formal Groups. *Lecture notes prepared in connection with the seminars held at the Summer Institute on Algebraic Geometry, Whitney Estate, Woods Hole, MA*, 1964. Available from: `http://www.ma.utexas.edu/users/voloch/lst.html`.

[Mat80]   Hideyuki Matsumura. *Commutative Algebra.* Benjamin, Reading, MA, second edition, 1980.

[Men07]   Alfred J. Menezes. Another look at HMQV. *Journal of Mathematical Cryptology*, 1(1):47–64, 2007. `doi:10.1515/JMC.2007.004`.

[Mes72]   William Messing. *The Crystals Associated to Barsotti-Tate Groups: with Applications to Abelian Schemes*, volume 264 of *Lecture Notes in Mathematics.* Springer, Berlin Heidelberg, 1972.

[Mil86a] Victor S. Miller. Short Programs for Functions on Curves. *IBM Thomas J. Watson Research Center*, 1986. Available from: `http://crypto.stanford.edu/miller/`.

[Mil86b] Victor S. Miller. Use of Elliptic Curves in Cryptography. In *Advances in Cryptology – CRYPTO '85*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426, Berlin Heidelberg, 1986. Springer.

[Mil04]   Victor S. Miller. The Weil Pairing, and Its Efficient Calculation. *Journal of Cryptology*, 17(4):235–261, September 2004. `doi:10.1007/s00145-004-0315-8`.

[MOV93]   Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. *IEEE Transactions on Information Theory*, 39(5):1639–1646, September 1993.

[MSV04]   A. Muzereau, Nigel P. Smart, and Frederik Vercauteren. The equivalence between the DHP and DLP for elliptic curves used in practical applications. *LMS Journal of Computation and Mathematics*, 7:50–72, 2004.

[Mül95]   Volker Müller. *Ein Algorithmus zur Bestimmung der Punktanzahl elliptischer Kurven über endlichen Körpern der Charakteristik größer drei*. PhD thesis, Universtät des Saarlandes, Saarbrücken, 1995.

[Mum74]   David Mumford. *Abelian Varieties*. Oxford University Press, London, 1974.

[Mum84]   David Mumford. *Tata Lectures on Theta II*. Birkhauser, Boston, 1984.

[MvV97]   Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, FL, 1997.

[MW96]   Ueli M. Maurer and Stefan Wolf. Diffie-Hellman Oracles. In *Advances in Cryptology – CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 268–282, Berlin Heidelberg, 1996. Springer. `doi:10.1007/3-540-68697-5_21`.

[MWZ98]   Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato. An Elementary Introduction to Hyperelliptic Curves. In *Algebraic Aspects of Cryptography*. Springer, Berlin Heidelberg, 1998.

[Neu07]   Jürgen Neukirch. *Algebraic number theory (Algebraische Zahlentheorie). Reprint of the 1992 original*. Springer, Berlin Heidelberg, 2007.

[NSA]   NSA Suite B Cryptography. Available from: `http://www.nsa.gov/ia/programs/suiteb_ cryptography/index.shtml`.

[PZ03]   J. Proos and C. Zalka. Shor's discrete logarithm quantum algorithm for elliptic curves. *Quantum Information and Computation*, 3:317–344, 2003.

[RSA78]   Ron L. Rivest, Adi Shamir, and Leonard Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978. `doi: 10.1145/359340.359342`.

[Rüc99]   Hans-Georg Rück. On the Discrete Logarithm in the Divisor Class Group of Curves. *Mathematics of Computation*, 68(226):805–806, April 1999.

[SA98]   Takakazu Satoh and K. Araki. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. *Commentarii Math. Univ. St. Pauli*, 47:81–92, 1998.

[Sat00]   Takakazu Satoh. The Canonical Lift of an Ordinary Elliptic Curve over a Finite Field and Its Point Counting. *Journal of the Ramanujan Mathematical Society*, 15(4):247–270, 2000.

[Sat02]   Takakazu Satoh. On p-adic Point Counting Algorithms for Elliptic Curves over Finite Fields. In *ANTS 2002*, volume 2369 of *Lecture Notes in Computer Science*, pages 43–66, Berlin Heidelberg, 2002. Springer.

[Sch85]   René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44:483–494, 1985.

[Sch87]   René Schoof. Nonsingular Plane Cubic Curves over Finite Fields. *Journal of Combinatorial Theory, Series A*, 46(2):183–211, November 1987.

[Sch95]   René Schoof. Counting points on elliptic curves over finite fields. *Journale de Théorie des Nombers de Bordaux*, 7:219–254, 1995.

[Sch00]   Oliver Schirokauer. Using number fields to compute logarithms in finite fields. *Mathematics of Computation*, 69(231):1267–1284, 2000.

[Sem98]   Igor A. Semaev. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. *Mathematics of Computation*, 67(221):353–356, 1998.

[Ser58]   Jean-Pierre Serre. Sur la topologie des variétés algébriques en caractéristique p. In *Symposium internacional de topología algebraica*, pages 24–53, Mexico City, 1958.

[Ser79]   Jean-Pierre Serre. *Local Fields*, volume 67 of *Graduate Texts in Mathematics*. Springer, New York, 1979.

[Sha71]   Daniel Shanks. Class number, a theory of factorization, and genera. In *1969 Number Theory Institute*, volume 20 of *Proceedings of Symponsia in Pure Mathematics*, pages 415–446, 1971.

[Sha94a]   Igor R. Shafarevich. *Basic Algebraic Geometry 1. Varieties in Projective Space*. Springer, Berlin Heidelberg, second edition, 1994.

[Sha94b]   Igor R. Shafarevich. *Basic Algebraic Geometry 2. Schemes and Complex Manifolds*. Springer, Berlin Heidelberg, second edition, 1994.

[Shi71]   Goro Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, Princeton, 1971.

[Shi00]   Rachel Shipsey. *Elliptic Divisibility Sequences*. PhD thesis, Goldsmiths College, Univerity of London, 2000. Available from: `http://homepages.gold.ac.uk/rachel/rachthesis.ps.gz`.

[Sil92]   Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 1992.

[Sil94]   Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer, New York, 1994.

[Sma99]   Nigel P. Smart. The Discrete Logarithm Problem on Elliptic Curves of Trace One. *Journal of Cryptology*, 12(3):193–196, 1999.

[SS98]   Joseph H. Silverman and Joe Suzuki. Elliptic Curve Discrete Logarithms and the Index Calculus. In *Advances in Cryptology – ASIACRYPT'98*, volume 1514 of *Lecture Notes in Computer Science*, pages 110–125, Berlin Heidelberg, 1998. Springer. `doi:10.1007/3-540-49649-1_10`.

[ST92]   Joseph H. Silverman and John Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer, New York, 1992.

[Sta07a]   Katherine E. Stange. Elliptic Nets And Elliptic Curves. *Preprint*, 2007. `arXiv:0710.1316v2`.

[Sta07b]   Katherine E. Stange. The Tate Pairing Via Elliptic Nets. In *Pairing Based Cryptography – Pairing 2007*, volume 4575/2007 of *Lecture Notes in Computer Science*, pages 329–348, Berlin Heidelberg, 2007. Springer. `doi:10.1007/978-3-540-73489-5`.

[Tat66]   J. Tate. Endomorphisms of Abelian Varieties over Finite Fields. *Inventiones Mathematicae*, 2(2):134–144, 1966.

[Thé03]   Nicolas Thériault. Index Calculus Attack for Hyperelliptic Curves of Small Genus. In *Advances in Cryptology – ASIACRYPT 2003*, volume 2895 of *Lecture Notes in Computer Science*, pages 75–92, Berlin Heidelberg, 2003. Springer. `doi:10.1007/b94617`.

[Vol88]   José Filipe Voloch. A note on elliptic curves over finite fields. *Bulletin de la Société mathématique de France*, 116(4):455–458, 1988. Available from: `http://www.numdam.org/item?id=BSMF_1988__116_4_455_0`.

[VPV01]   Frederik Vercauteren, Bart Preneel, and Joos Vandewalle. A Memory Efficient Version of Satoh's Algorithm. In *EUROCRYPT 2001*, number 2045 in Lecture Notes in Computer Science, pages 1–13, Berlin Heidelberg, 2001. Springer.

[War48]   Morgan Ward. Memoir on elliptic divisibility sequences. *American Journal of Mathematics*, 70(1):31–74, January 1948.

[Was08]   Lawrence C. Washington. *Elliptic curves. Number theory and cryptography*. Chapman and Hall/CRC, Boca Raton, FL, second edition, 2008.

[Wat69]   William C. Waterhouse. Abelian varieties over finite fields. *Annales scientifiques de l'É.N.S.*, 2(4):521–560, 1969.

[Wei93]   Karl Weierstraß. *Formeln und Lehrsätze zum Gebrauche der elliptischen Functionen.* Springer, Berlin, 1893.

[Wei48]   André Weil. *Sur les courbes algébraiques et les variétés qui s'en déduisent.* Hermann, Paris, 1948.

[Wei49]   André Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc*, 55(5):497–508, 1949.

List of Notation

$\widehat{\mathbb{G}}_m$	formal multiplicative group	50
$\mathbf{H}$	upper half plane $\{\tau \in \mathbb{C} : \mathfrak{Im}\,\tau > 0\}$	39
$\mathrm{Hom}(E_1, E_2)$	{isogenies $E_1 \to E_2$}	18
$I(Y)$	homogeneous ideal associated to $Y \subseteq \mathbb{P}^n$	4
$I(Y)$	ideal associated to $Y \subseteq \mathbb{A}^n$	2
J	Jacobian variety	27
$j(\tau)$	modular j-invariant	40
$j(E)$	j-invariant of an elliptic curve	15
$\bar{K}$	a (fixed) algebraic closure of K	1
K	a perfect field (in some sections K is further restricted)	1
k	residue field of a discrete valuation field K	48
$k(q,n)$	embedding degree corresponding to $\mathbb{F}_q$ and n	44
K^+	additive group of K	18
K^*	multiplicative group of K	3
K_C	a canonical divisor of C	10
K^{ur}	maximal unramified extension of K	49
$K(V)$	function field of V/K	2
$K[V]$	coordinate ring of V/K	2
$\bar{K}[V]_P$	local ring at P	3
$K[X]$	polynomial ring	1
$\mathscr{L}(D)$	Riemann-Roch space of $D \in \mathrm{Div}(C)$	10
$\ell(D)$	$\dim_{\bar{K}} \mathscr{L}(D)$	10
$\lambda(w)$	"parity" of lattice points	33
$\mathfrak{L}$	set of complex lattices	39
Λ	lattice	29
Λ_τ	the lattice $\mathbb{Z}\tau + \mathbb{Z}$	39
$\mathrm{lc}(\phi)$	leading coefficient of the isogeny ϕ	74
$L_n[\alpha, c]$	L-notation, $O\left(e^{(c+o(1))(\ln n)^\alpha (\ln \ln n)^{1-\alpha}}\right)$	82
$\log_{\mathcal{F}}$	formal logarithm	52
$\log_g h$	minimal multiplier of h with respect to g	79
$\log_p$	p-adic formal logarithm	84
$[m]$	multiplication by m	17
$\mathcal{M}(a,b)$	AGM iteration	75
$M_n(R)$	$n \times n$-matrices over R	25
$\mathfrak{m}_P$	maximal ideal at P	3

Index