# Elliptic Curves and Lower Bounds for Class Numbers of Global Fields

Corijn Rudrum

July 14, 2022

Master's thesis

Supervisor: prof. dr. Gunther Cornelissen
Second reader: dr. Valentijn Karemaker

Utrecht University

Utrecht University
Faculty of Science
Department of Mathematics

Corijn Rudrum, BSc: Elliptic Curves and Lower Bounds for Class Numbers of Global Fields
Master's thesis, Mathematical Sciences

Supervisor: prof. dr. Gunther Cornelissen
Second reader: dr. Valentijn Karemaker

Time frame: September 2021 - July 2022

# Abstract

This thesis is concerned with effective lower bounds for class numbers of imaginary quadratic global fields. Finding such bounds is a classical problem in number theory with applications in e.g. cryptography and the theory of error correcting codes. Recently, Griffin and Ono [GO20] have derived such bounds for number fields using elliptic curve ideal class pairings which improved on existing effective bounds for many quadratic fields. Here we generalise their construction to global function fields, yielding similar bounds for the class number of imaginary quadratic function fields. Over function fields, multiple constructions of elliptic curves with arbitrarily large rank are known. We examine in particular the class number bounds we obtain using such a family of elliptic curves constructed by Ulmer [Ulm14]. Our results do not improve on those in the literature. Finally, as an auxiliary result, we bound the difference between the canonical height and the Weil height on an elliptic curve over a global field. All our results are for characteristic unequal to 2 or 3.

# Acknowledgements

First and foremost, I would like to thank Gunther Cornelissen for being my supervisor, for suggesting the topic of this thesis, and for providing valuable comments and suggestions throughout the process. I was always welcome for advice on matters both related and unrelated to this thesis, for which I am very grateful. Thanks also to Valentijn Karemaker for taking the time to be the second reader for this thesis.

Thanks is also due to my housemates, for providing plenty of both support and distraction while I worked on this thesis. Further, I would like to thank my parents and Janna, without whom this thesis (and many other things) would never have been possible. Lastly, thank you Wendy, for your endless encouragement and support, and for everything else.

# Contents

# Introduction

The asymptotic behaviour of class numbers $h_K(-D)$ of imaginary quadratic number fields $K = \mathbb{Q}(\sqrt{-D})$ is an old and extensively studied topic in number theory. In his *Disquisitiones*, Gauss conjectured that $h_K(-D) \to \infty$ as $D \to \infty$, and over a century later this was indeed confirmed by Heilbronn [Hei34]. In recent work [GO20], Griffin and Ono derive effective lower bounds for $h_K(-D)$ that improve on previously known effective lower bounds for certain families of discriminants $-D$. Their method revolves around elliptic curve ideal class pairings, which are maps of the form

$$E(\mathbb{Q}) \times E_{-D}(\mathbb{Q}) \to \mathrm{CL}(-D)$$

where $E/\mathbb{Q}$ is an elliptic curve, $E_{-D}/\mathbb{Q}$ is a quadratic twist of $E$, and $\mathrm{CL}(-D)$ denotes the ideal class group of $\mathbb{Q}(\sqrt{-D})$. For $\varepsilon > 0$, they obtain for sufficiently large discriminants $-D$ in these families a bound of the form

$$h_K(-D) \geq \frac{1}{2}(c(E) - \varepsilon)(\log D)^{\frac{r}{2}}, \tag{1}$$

where $c(E)$ is a constant depending on $E$ and $r$ is the rank of $E$. Asymptotically, this bound becomes stronger if the rank $r$ is large. It is still an open problem whether there exist elliptic curves over $\mathbb{Q}$ of arbitrarily large rank. The current record set by Elkies is an elliptic curve of rank at least 28 [Elk06]. In the paper [PPVW19] heuristics for the rank of elliptic curves over $\mathbb{Q}$ are given, which suggest that in fact there is an absolute bound for the rank of elliptic curves over $\mathbb{Q}$.

Instead of number fields, we will primarily be concerned with global function fields, which are finite field extensions of $\mathbb{F}_q(T)$ where $q$ is a prime power and $T$ is transcendental over the finite field $\mathbb{F}_q$. Global function fields behave much like number fields, and many objects and results from number theory have a function-field analogue. The main result of this thesis is the translation of the strategy of Griffin and Ono to global function fields, yielding lower bounds for the class numbers of imaginary quadratic global function fields. In particular, we derive bounds similar to (1) using elliptic curves $E/\mathbb{F}_q(T)$ for which the rank $r$ becomes arbitrarily large. Although using these large-rank elliptic curves yields asymptotically stronger bounds than Griffin and Ono obtained for number fields, they do not improve on the best known bounds for function fields, see Section 4.5 for details.

One motivation for studying the asymptotic behaviour of class numbers of global function fields is that it might lead to new insights that can be used in the number-field analogue of the problem. Further, effective lower bounds for class numbers of global function fields serve applications in for example cryptography (see e.g. [ST02] and [Kob89]) and the theory of error-correcting codes (see e.g. [TVN07, Prop. 3.2.14] and its applications in Chapter 4 there).

## Outline of the Text

We start by giving an introduction to global function fields in Chapter 1. In Chapter 2 we generalise the development of the theory of height functions on elliptic curves as presented in [Sil09, Chapter VIII] to elliptic curves over global function fields. Further, in Section 2.4 of Chapter 2 we introduce local height functions on elliptic curves over global fields, and we use them to bound the difference between the canonical height and the Weil height on such curves. In Chapter 3 we derive lower bounds for the class numbers of imaginary quadratic number fields, closely following [GO20]. The last section of this chapter gives a brief overview of the literature on lower bounds for class numbers of imaginary quadratic number fields, which we also compare to our results. In the fourth chapter we derive lower bounds for the class number of imaginary quadratic function fields. The structure and material of the first two sections of

Chapter 4 closely resembles that of Sections 3.1 and 3.3. Subsequently, in Sections 4.3 and 4.4 we give a construction of elliptic curves over $\mathbb{F}_q(T)$ with arbitrarily large rank, and we use these curves to give bounds similar to (1) where $r$ can be arbitrarily large. Lastly, in Section 4.5 we give a brief overview of the literature on lower bounds for class numbers of global function fields, and we compare this to our results.

The main original contributions in this thesis are the following.

- In Theorem 2.4.16 we give a bound on the difference between the canonical height and the Weil height on an elliptic curve over a global function field.
- Theorem 4.2.6 gives an explicit bound of the form (1) for class numbers of certain imaginary quadratic global function fields.
- In Theorem 4.4.4 we give an explicit version of the above result for a specific family of elliptic curves whose ranks tend to infinity.

This first result is especially interesting since two separate sources state similar but incorrect bounds, see Remark 2.4.18. We also correct various minor errors in [GO20] in Chapter 3. The class number bounds from Theorems 4.2.6 and 4.4.4 do not improve on the literature.

## Assumptions and Notation

In the List of Symbols at the end of this document we define the notation used in this thesis. Here we highlight some specific notation that may otherwise lead to confusion, and we make clear which assumptions are used throughout this thesis.

First of all, throughout this thesis we let $p \notin \{2, 3\}$ be a prime number, and we let $q$ be a power of $p$. We denote the finite field of $q$ elements by $\mathbb{F}_q$. Our reason for assuming that $p \neq 2$ is that this ensures that quadratic extensions of fields of characteristic $p$ are always separable. Further, the theory of binary quadratic forms is much more complicated in characteristic 2. See for example the preface of [Kne10], which suitably begins with the following limerick.

*A mathematician said who*
*Can quote me a theorem that's true?*
*For the ones that I know*
*Are simply not so,*
*When the characteristic is two!*

The reason that we further assume $p \neq 3$ is because this ensures that all elliptic curves we consider can be given by a short Weierstrass equation, cf. [Sil09, §III.1]. This is important since we only prove Theorem 2.4.16 on the difference between the canonical height and the Weil height for elliptic curves in short form.

Without further specification, the letter $K$ will denote a general field. We write $\overline{K}$ for an algebraic closure of $K$ and $K^{\mathrm{sep}}$ for the separable closure of $K$ in $\overline{K}$. Further, $K_v$ denotes the completion of $K$ at the prime $v$. For a ring $R$ we denote its unit group by $R^*$.

For a global function field $K/\mathbb{F}_q$, we always assume that $\mathbb{F}_q$ is the full constant field of $K$, i.e. if we fix an algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$ then $\overline{\mathbb{F}_q} \cap K = \mathbb{F}_q$. Further, we will assume that we have fixed an element $T \in K$ transcendental over $\mathbb{F}_q$. See also Remark 1.2.2 for some advantages and disadvantages of this assumption. For a global field $K$, this assumption allows us to define the rational subfield $\mathfrak{R}$ of $K$ in Definition 1.2.3 and the ring of integers $\mathcal{O}_K$ of $K$ in Definition 1.2.4. The notation $\mathcal{O}_K$ for the ring of integers should not be confused with our notations $\mathcal{O}_P$ and $\mathcal{O}_v$ for valuation rings corresponding to a place $P$ or prime $v$ of $K$, or with our notation $\mathcal{O}$ for the point at infinity on an elliptic curve in Weierstrass normal form.

We denote by $h$, $h_x$ and $\hat{h}$ the absolute logarithmic height function, the height on an elliptic curve $E$ with respect to the morphism $x : E \to \mathbb{P}^1$, and the canonical height function, respectively. These functions are defined in Chapter 2. This notation should not be confused with our notation $h_K$ for the class number of a global field $K$, or our notation $h_K^I$ for the ideal class number of a global function field (see page 7).

# Prerequisites

Throughout this thesis we assume that the reader is familiar with the basic theory of algebraic number theory, valuations, and elliptic curves. For algebraic number theory we refer to the notes [Ste17] and [Ste02] that are both freely available online. The first gives an introduction to number fields, and the second continues with an introduction to valuations and local fields. For elliptic curves we point to [Sil09].

# Chapter 1

# Global Function Fields

One of the main themes of this thesis is the analogy between number fields and global function fields. In this chapter we will give a brief introduction to the theory of global function fields while emphasizing their similarities with number fields.

## 1.1 Algebraic Function Fields

Before stating the definition of a global function field in the next section, we give a brief introduction to the general theory of algebraic function fields. We assume that the reader is familiar with (discrete) valuation rings. For a more detailed and very clear introduction to algebraic function fields, assuming only some basic knowledge of algebraic field extensions, we refer to [Sti09, Chapter 1].

**Definition 1.1.1** ([Sti09, Def. 1.1.1])**.** Let $k$ be a field. An *algebraic function field $K/k$ of one variable over $k$* is a field extension $K/k$ such that $K$ is a finite extension of $k(T)$ for some element $T \in K$ which is transcendental over $k$.

The simplest example of an algebraic function field over a field $k$ is the *rational function field $k(T)$* of rational functions in the indeterminate $T$ over $k$. In general, a function field $K/k$ is called *rational* if there exists an element $T \in K$ such that $K = k(T)$.

For an algebraic function field $K/k$, the algebraic closure of $k$ in $K$ is a subfield $\widetilde{k} \subset K$ called the *field of constants* or *constant field* of $K/k$. It is always a finite extension of $k$ ([Sti09, Cor. 1.1.16]). The terminology stems from an interpretation of the elements of $K$ as functions. Namely, let $T \in K$ be transcendental over $k$, and for every element $a \in K$ let

$$f_a(X) = X^n + a_1(T)X^{n-1} + \cdots + a_n(T)$$

be the minimal polynomial of $a$ over $k(T)$ (which exists as $a$ is algebraic over $k(T)$), so the coefficients $a_i(T)$ are rational functions of $T$ over $k$. Now, instead of viewing the element $T$ as an indeterminate, we consider $T$ as a variable ranging over $\overline{k}$. There are at most finitely many values for $T$ such that the denominator of one of the coefficients $a_i(T)$ vanishes. For all other values of $T$ in $\overline{k}$ we consider the polynomial $f_{a,T}(X)$ obtained from $f_a(X)$ by evaluating the coefficients at $T$. This polynomial has $n$ (not necessarily distinct) roots in $\overline{k}$. As these roots are determined by $a$ and the value of $T$, we can view $a$ as an $n$-valued function sending elements in $\overline{k}$ to the roots of $f_{a,T}(X)$ in $\overline{k}$. Now suppose that $a \in \widetilde{k}$. It turns out that in that case the coefficients $a_i(T)$ are elements of $k$, see the integrality theorem in [Has80, p. 316]. Hence they are constant functions of $T$, and therefore $a$ is a constant function. Conversely, if $a$ is a constant function, then the coefficients $a_i(T)$ are also constant functions of $T$ as they are the elementary symmetric functions of the $n$ values of $a$. Hence the $a_i(T)$ are elements of $k$, which by the same integrality theorem implies that $a \in \widetilde{k}$. So the elements of the constant field are exactly the constant functions.

Let $K/k$ be an algebraic function field. As explained by Stichtenoth in [Sti09, Chapter 1], there is a one-to-one correspondence between valuation rings of $K/k$ and discrete valuations[1] on $K/k$. Further, each valuation ring has a unique maximal ideal, and given such a maximal ideal we can uniquely recover the corresponding valuation ring.

[1] Note that Stichtenoth includes a normalization in the definition of a discrete valuation, see [Sti09, Def. 1.1.9(4)].

**Definition 1.1.2.** A *place* of the function field $K/k$ is the unique maximal ideal of some valuation ring of $K/k$. We denote the set of all places of $K/k$ by $\mathbb{P}_K$.

For a place $P$ of $K/k$ we denote the corresponding valuation ring and discrete valuation by $\mathcal{O}_P$ and $v_P$, respectively. We have (cf. [Sti09, Theorem 1.1.13])

$$\begin{aligned} \mathcal{O}_P &= \{a \in K : v_P(a) \geq 0\}, \\ P &= \{a \in K : v_P(a) > 0\}. \end{aligned}$$

All places of $K/k$ are principal ideals, and an element $\pi \in P$ such that $P = \pi\mathcal{O}_P$ is called a *uniformizer* for $P$. For $P \in \mathbb{P}_K$, the field $\mathcal{O}_P/P$ is called the *residue class field* of $P$. Since $k \subset \mathcal{O}_P$ and $k \cap P = \{0\}$, the residue class map $\mathcal{O}_P \to \mathcal{O}_P/P$ induces a canonical embedding of $k$ into $\mathcal{O}/P$. We define the *degree* of a place $P$ as

$$\deg(P) = [\mathcal{O}_P/P : k].$$

For the rest of this section we will assume that $k = \widetilde{k}$, the full constant field of $K/k$.

**Definition 1.1.3.** A *divisor* of $K/k$ is a formal sum

$$D = \sum_{P \in \mathbb{P}_K} n_P P \qquad \text{with } n_P \in \mathbb{Z}, \text{ and almost all } n_P = 0.$$

Given two divisors $D = \sum n_P P$ and $D' = \sum n'_P P$ we define their sum as

$$D + D' = \sum_{P \in \mathbb{P}_K} (n_P + n'_P)P.$$

The set $\operatorname{Div}(K)$ of divisors of $K/k$ forms a group under addition of divisors. It is the free abelian group generated by the places of $K/k$. For a divisor $D = \sum n_P P$ of $K/k$ we define $v_P(D) = n_P$. We define a partial ordering on $\operatorname{Div}(K)$ by saying

$$D_1 \leq D_2 \qquad \Longleftrightarrow \qquad v_P(D_1) \leq v_P(D_2) \quad \text{for all } P \in \mathbb{P}_K.$$

The *degree* of a divisor is defined as

$$\deg(D) = \sum_{P \in \mathbb{P}_K} v_P(D) \deg(P).$$

The divisors of degree 0 form a subgroup of $\operatorname{Div}(K)$, denoted by $\operatorname{Div}^0(K)$. For a non-zero element $0 \neq x \in K$ we define the corresponding *principal divisor*

$$(x) = \sum_{P \in \mathbb{P}_K} v_P(x)P.$$

All principal divisors have degree 0, and the set

$$\operatorname{Princ}(K) = \{(x) : x \in K^*\}$$

of principal divisors of $K/k$ forms a subgroup of $\operatorname{Div}^0(K)$.

**Definition 1.1.4.** The quotient group

$$\mathrm{CL}_{\mathrm{div}}(K) = \operatorname{Div}(K)/\operatorname{Princ}(K)$$

is called the *divisor class group of $K/k$*. We denote the class of a divisor $D$ by $[D]$. We say that two divisors are *equivalent* if they share the same class.

Since equivalent divisors have the same degree, we can define the degree of a divisor class $[D]$ as

$$\deg([D]) = \deg(D).$$

**Definition 1.1.5.** The subgroup

$$\mathrm{CL}^0_{\mathrm{div}}(K) = \{[D] \in \mathrm{CL}_{\mathrm{div}}(K) : \deg([D]) = 0\}$$

of $\mathrm{CL}_{\mathrm{div}}(K)$ is called the *group of divisor classes of degree* 0 of $K/k$.

In the next section we will give the definition of a global function field. These fields have much in common with number fields, and the group of divisor classes of degree 0 will serve as the analog of the ideal class group of a number field.

**Definition 1.1.6.** For a divisor $D \in \mathrm{Div}(K)$, the *Riemann-Roch space associated to* $D$ is defined as

$$\mathscr{L}(D) = \{x \in K : (x) \geq -D\} \cup \{0\}.$$

The space $\mathscr{L}(D)$ is a finite dimensional vector space over $k$ ([Sti09, Prop. 1.4.9]), and we denote its dimension by

$$\ell(D) = \dim \mathscr{L}(D).$$

**Definition 1.1.7.** The *genus* of the function field $K/k$ is defined as

$$g = \max\{\deg(D) - \ell(D) + 1 : D \in \mathrm{Div}(K)\}.$$

Note that the maximum in the above definition exists by [Sti09, Prop. 1.4.14]. The genus $g$ of a function field is a non-negative integer (cf. [Sti09, Cor. 1.4.16]), and it is an important invariant of the function field. For example, it shows up in the Riemann-Roch theorem (see e.g. [Sti09, Theorem 1.5.15]), and we will encounter it again in Section 1.3 when discussing the Hasse-Weil theorem (Theorem 1.3.5).

We finish this section with a discussion on the relation between function fields $K/k$ in one variable over $k$ and curves over $k$. We have the following general theorem.

**Theorem 1.1.8** ([Liu02, Chapter 7 Prop. 3.13(a)])**.** *Let $k$ be a field. Then for any function field $K/k$ in one variable over $k$ there exists, up to isomorphism, a unique normal projective curve $C$ such that for the function field $K(C)$ of $C$ we have $K(C) = K$.*

For function fields over a perfect base field we can actually replace the word 'normal' by the stronger 'smooth and irreducible'.

**Theorem 1.1.9.** *Let $k$ be a perfect field. Then for any function field $K/k$ in one variable over $k$ there exists, up to isomorphism, a unique smooth and irreducible curve $C$ such that $K(C) = K$.*

*Proof.* We briefly sketch the proof. By [Liu02, Chapter 4 Cor. 3.33] any algebraic variety over $k$ is smooth if and only if it is regular. Further, from [AM69, Prop. 9.2] it follows that a curve is normal if and only if it is irreducible and regular. The desired statement then follows from Theorem 1.1.8. □

## 1.2 Global Fields

In this thesis, we will primarily consider function fields over finite fields. These will turn out to behave much like number fields.

**Definition 1.2.1.** A function field $K/\mathbb{F}_q$ of one variable over a finite field $\mathbb{F}_q$ is called a *global function field*. In other words, a global function field $K/\mathbb{F}_q$ is of the form $\mathbb{F}_q(T, \alpha)$, where

- $T$ is transcendental over $\mathbb{F}_q$,
- $\alpha$ is algebraic over $\mathbb{F}_q(T)$.

In general, a field $K$ is called a *global field* if it is either a number field or a global function field.

In this thesis, when we let $K/\mathbb{F}_q$ be a global function field we will always mean that $\mathbb{F}_q$ is the full constant field of $K$. Often we will let $K$ be a general global field. In that case we implicitly mean that if $K$ is a function field, then we denote its full constant field by $\mathbb{F}_q$.

Note that the finite field $\mathbb{F}_q$ is perfect, so by Theorem 1.1.9 every global function field corresponds, up to isomorphism, to a unique smooth and irreducible curve $C$ over $\mathbb{F}_q$.

The analogies between global function fields and number fields stem in no small part from the similarities between $\mathbb{Q}$ and the rational function field $\mathbb{F}_q(T)$ in an indeterminate $T$. Note that these fields are the fraction fields of $\mathbb{Z}$ and $\mathbb{F}_q[T]$, respectively, which share many properties. For instance, both $\mathbb{Z}$ and $\mathbb{F}_q[T]$ are Euclidean domains, allowing us to talk about the gcd of two elements. Further, both $\mathbb{F}_q[T]$ and $\mathbb{Z}$ have finite unit groups. Therefore, many number-theoretic questions over $\mathbb{Q}$ have their analog in $\mathbb{F}_q(T)$.

However, these resemblances between $\mathbb{Q}$ and $\mathbb{F}_q(T)$ also bring us to an important difference between number fields and global function fields.

*Remark* 1.2.2. Recall that a number field is by definition a finite extension of $\mathbb{Q}$. From the above discussion it may seem natural to define a global function field as a finite extension of $\mathbb{F}_q(T)$. However, we have to be a bit more careful with function fields. Whereas a given number field contains one canonical copy of $\mathbb{Q}$, namely its prime field, this is not at all the case with $\mathbb{F}_q(T)$ for function fields. Let $K/\mathbb{F}_q$ be a global function field and let $T \in K$ be transcendental over $\mathbb{F}_q$, such that $K$ is a finite extension of $\mathbb{F}_q(T)$. Then many properties of the extension $K/\mathbb{F}_q(T)$ depend on our choice of $T$. For example, suppose that $K/\mathbb{F}_q(T)$ is separable. If we let $T' = T^p \in K$ then clearly $K/\mathbb{F}_q(T')$ is not separable. Moreover, not even the degree $[K : \mathbb{F}_q(T)]$ is invariant under the choice of $T$, as the same example shows.

Despite the fact that there is no canonical choice for $T$, in the rest of this thesis we will assume that for a global function field $K$ with full constant field $\mathbb{F}_q$ we have fixed an element $T \in K$ such that $K$ is a finite extension of $\mathbb{F}_q(T)$. An extension $K'/K$ inherits this choice from $K$. Our main reason for fixing $T$ is that it makes the analogy with number fields particularly clear. The polynomial ring $\mathbb{F}_q[T]$ then takes the role of the integers $\mathbb{Z}$ in the number field case. ♢

**Definition 1.2.3.** Let $K$ be a global field, where in the case that $K$ is a function field we have fixed a transcendental element $T \in K$, cf. Remark 1.2.2. We define the *rational subfield* $\mathfrak{R}$ of $K$ as

$$\mathfrak{R} = \begin{cases} \mathbb{Q} & \text{if } K \text{ is a number field,} \\ \mathbb{F}_q(T) & \text{if } K \text{ is a function field.} \end{cases}$$

Recall that the ring of integers $\mathcal{O}_K$ of a number field $K$ is defined as the integral closure of $\mathbb{Z}$ in $K$. For function fields we take essentially the same definition.

**Definition 1.2.4.** Let $K$ be a global function field. We define the *ring of integers* $\mathcal{O}_K$ of $K$ as the integral closure of $\mathbb{F}_q[T]$ in $K$.

Just as for number fields, the ring of integers of a global function field is a Dedekind domain. The group of invertible ideals of $\mathcal{O}_K$ modulo the principal ideals is called the *ideal class group* of $K$, which for function fields $K$ we denote by $\mathcal{I}_K$. We write $h_K^I$ for the order of $\mathcal{I}_K$, also called the *ideal class number* of $K$. Despite the fact that the ideal class groups in number fields and global function fields have very similar definitions, the term *class group* of a global function field $K$ is reserved for $\mathrm{CL}^0_{\mathrm{div}}(K)$, the group of divisor classes of degree 0. For a global function field $K/\mathbb{F}_q$, the group $\mathrm{CL}_{\mathrm{div}}(K)$ can be infinite but its subgroup $\mathrm{CL}^0_{\mathrm{div}}(K)$ is always finite, see [Sti09, Prop. 5.1.3].

**Definition 1.2.5.** Let $K$ be a global function field. We define the *class group* $\mathrm{CL}(K)$ of $K$ as the finite abelian group

$$\mathrm{CL}(K) = \mathrm{CL}^0_{\mathrm{div}}(K).$$

The order of $\mathrm{CL}(K)$ is called the *class number* of $K$, denoted $h_K$.

The main reason that $\mathrm{CL}(K)$, instead of $\mathcal{I}_K$, is the function field analog for the ideal class group of a number field, is because $\mathcal{I}_K$ is not an invariant of the global function field $K$. Namely, it depends on our choice of the transcendental element $T \in K$. The group $\mathrm{CL}(K)$, on the other hand, is invariant under this choice. Further, the group of non-zero fractional ideals of the ring of integers of a number field is actually very similar to the group of divisors in a global function field. To see this, let $F$ be a number field. Since its ring of integers $\mathcal{O}_F$ is a Dedekind domain, the group of non-zero fractional ideals of $\mathcal{O}_F$ is equal to the free abelian group generated by the non-zero prime ideals of $\mathcal{O}_F$. Now recall that the non-zero prime ideals of $F$ correspond bijectively to the non-archimedean places of $F$. This implies that we can view the group of non-zero fractional ideals of $\mathcal{O}_F$ as the free abelian group generated by the non-archimedean places of $F$. For a global function field $K$, the free abelian group generated by the non-archimedean places of $K$ is exactly $\mathrm{Div}(K)$. The class group of $F$ is defined as the quotient of the group of non-zero fractional ideals of $\mathcal{O}_F$ with the subgroup of principal ideals. Similarly, the group $\mathrm{CL}_{\mathrm{div}}(K)$ is defined as the quotient of $\mathrm{Div}(K)$ with the subgroup $\mathrm{Princ}(K)$ of principal divisors. Since $\mathrm{CL}^0_{\mathrm{div}}(K)$, like the class group of a number field, is finite, whereas $\mathrm{CL}_{\mathrm{div}}(K)$ can be infinite, we think of $\mathrm{CL}(K) = \mathrm{CL}^0_{\mathrm{div}}(K)$ as the function field analog of the ideal class group of a number field.

If we let $C$ be the smooth irreducible curve corresponding to a global function field $K$, then $\mathrm{CL}(K)$ is isomorphic (as groups) to the jacobian $J(C)$ of the curve $C$ (see e.g. [Sti09, Appendix B.10], where this is actually the definition of $J(C)$).

An important difference between the two kinds of global fields is that number fields have characteristic 0, whereas global function fields have positive characteristic. In particular this implies that $\mathbb{Q}$ is a perfect field, but it just so happens that $\mathbb{F}_q(T)$ is not perfect. To see this, let $p$ be the characteristic of $\mathbb{F}_q(T)$ and consider the irreducible polynomial $P = X^p - T$. Let $\alpha$ be a root of $P$ in some extension of $\mathbb{F}_q(T)$. Then $P = X^p - \alpha^p = (X-\alpha)^p$ since we work in characteristic $p$, implying that $\mathbb{F}_q(T)(\alpha)$ is a purely inseparable extension of $\mathbb{F}_q(T)$. For this thesis the non-perfectness of $\mathbb{F}_q(T)$ will not be a problem, since we are mainly interested in quadratic extensions of $\mathbb{F}_q(T)$ and we assume that $q$ is the power of an odd prime. Hence the characteristic will never divide 2, so all quadratic extensions we consider will be separable.

Let $K$ be a global function field with $K/\mathfrak{R}$ separable. Then $\mathcal{O}_K$ is an *order* in $K$, and we can define the *norm* and *trace* maps from $\mathcal{O}_K$ to $\mathbb{F}_q[T]$ as described in [Ste17, §4]. Then, we can define the *discriminant* $D$ of $\mathcal{O}_K$ using the trace map in exactly the same way as for number fields, see e.g. [Rei03, §10] or [Ste17, Def. 4.4]. Since our choice of $K$ determines $\mathcal{O}_K$, we also call $D$ the discriminant of $K$.

## 1.3 The Hasse-Weil Theorem

The best known bounds for the class number of a global function field come from the Hasse-Weil theorem, also called the Riemann hypothesis for function fields. In this section, $K/\mathbb{F}_q$ will denote a global function field with genus $g$.

We define the numbers

$$A_n = \#\{A \in \mathrm{Div}(K) : A \geq 0 \text{ and } \deg A = n\}.$$

**Definition 1.3.1.** The *Zeta function of $K/\mathbb{F}_q$* is defined as the power series

$$Z(t) = \sum_{n=0}^{\infty} A_n t^n.$$

**Proposition 1.3.2** ([Sti09, Prop. 5.1.6 & Cor. 5.1.7])**.** *If we view $Z(t)$ as a power series over the complex number and $t$ as a complex variable, then $Z(t)$ is convergent for $|t| < q^{-1}$. Further, $Z(t)$ can be extended to a rational function on $\mathbb{C}$ with a simple pole at $t = 1$.*

**Definition 1.3.3.** The *L-polynomial of $K/\mathbb{F}_q$* is defined as

$$L(t) = (1-t)(1-qt)Z(t).$$

The fact that $L(t)$ is indeed a polynomial is ensured by the following theorem.

**Theorem 1.3.4** ([Sti09, Theorem 5.1.15])**.** (a) *$L(t) \in \mathbb{Z}[t]$ and $\deg(L) = 2g$.*

(b) *We write $L(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g}$. Then $a_0 = 1$.*

(c) *Let $L^{\perp}(t) = t^{2g} L(t^{-1})$ be the reciprocal polynomial of $L(t)$, and write $\alpha_1, \ldots, \alpha_{2g}$ for the complex roots of $L^{\perp}(t)$. Then $L(t)$ factors over $\mathbb{C}$ as*

$$L(t) = \prod_{i=1}^{2g} (1 - \alpha_i t).$$

(d) *$L(1) = h_K$, the class number of $K$.*

Note in the above theorem that the numbers $\alpha_i$ are the reciprocals of the roots of $L(t)$. The Hasse-Weil theorem is the following statement.

**Theorem 1.3.5** (Hasse-Weil)**.** *Assuming the notation from Theorem 1.3.4, the numbers $\alpha_i$ satisfy*

$$|\alpha_i| = \sqrt{q} \qquad \text{for } i = 1, \ldots, 2g.$$

*Proof.* See e.g. [Sti09, §5.2] for a proof of this theorem. □

As we mentioned before, the Hasse-Weil theorem is sometimes referred to as the *Riemann Hypothesis for function fields*. We will briefly explain this terminology, see also [Sti09, Rem. 5.2.2]. Let $\zeta_R$ denote the classical Riemann zeta function. Then the Riemann hypothesis states that every non-trivial zero $s \in \mathbb{C}$ of $\zeta_R$ satisfies $\mathrm{Re}(s) = \frac{1}{2}$. For a global function field $K/\mathbb{F}_q$ with Zeta function $Z(t)$ we define its *zeta function* as

$$\zeta_K(s) = Z(q^{-s}) \qquad s \in \mathbb{C}.$$

Suppose that $\zeta_K(s) = 0$ for some $s \in \mathbb{C}$. Then $Z(q^{-s}) = 0$, which implies $L(q^{-s}) = 0$. Then the Hasse-Weil theorem states that $|q^{-s}| = q^{-\frac{1}{2}}$. Note that we have $|q^{-s}| = q^{-\mathrm{Re}(s)}$, so this implies $\mathrm{Re}(s) = \frac{1}{2}$. Therefore we can view the Hasse-Weil theorem as the function-field analogue of the Riemann hypothesis. We emphasize that, in contrast to the Riemann hypothesis, the Hasse-Weil theorem has been proven.

The Hasse-Weil theorem can be used to bound the number of places of $K$ of degree one.

**Theorem 1.3.6** (Hasse-Weil Bound). *Write $N$ for the number of places of $K/\mathbb{F}_q$ degree one. Then we have*

$$|N - (q+1)| \leq 2g\sqrt{q}. \tag{1.3.1}$$

*Proof.* See e.g. [Sti09, Theorem 5.2.3]. □

In what follows, we will fix an algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$. Then for every $r \geq 1$ there is a unique extension $\mathbb{F}_{q^r}/\mathbb{F}_q$ of degree $r$ with $\mathbb{F}_{q^r} \subset \overline{\mathbb{F}_q}$. We define the fields

$$K_r = K\mathbb{F}_{q^r} \qquad r \geq 1,$$

where $K\mathbb{F}_{q^r}$ denotes the compositum of $K$ and $\mathbb{F}_{q^r}$. Then for every $r \geq 1$ the field $K_r$ is a constant field extension of $K$ of degree $r$ with $\mathbb{F}_{q^r}$ as its full constant field. Further, the genus of $K_r/\mathbb{F}_{q^r}$ is the same as the genus of $K/\mathbb{F}_q$ (see [Sti09, Lem. 5.1.9]). If we write $L_r$ for the $L$-polynomial of $K_r/\mathbb{F}_{q^r}$, then we have

$$L_r(t) = \prod_{i=1}^{2g}(1 - \alpha_i^r t).$$

The Hasse-Weil bound is a consequence of the Hasse-Weil theorem. However, one might argue that as a statement it is not much weaker, in the following sense. Suppose that we do not know a proof of the Hasse-Weil Theorem, and further suppose that we do have a proof that Theorem 1.3.6 holds for all fields $K_r/\mathbb{F}_{q^r}$ for $r \geq 1$. Then it is relatively easy to derive from this that the Hasse-Weil theorem holds for all fields $K_r/\mathbb{F}_{q^r}$ as well, see [Sti09, §5.2] for details[2]. The actual hard part in the proof of the Hasse-Weil theorem consists of showing that we have a bound similar to (1.3.1) for all fields $K_r/\mathbb{F}_{q^r}$.

Now, we will show how we can use the Hasse-Weil theorem to bound the class number $h_K$ of $K$. By Theorem 1.3.4 we have

$$h_K = L(1) = \prod_{i=1}^{2g}(1 - \alpha_i).$$

The Hasse-Weil theorem implies that $\sqrt{q} - 1 \leq |1 - \alpha_i| \leq \sqrt{q} + 1$, giving the following result.

**Corollary 1.3.7.** *The class number $h_K$ of $K/\mathbb{F}_q$ satisfies*

$$(\sqrt{q} - 1)^{2g} \leq h_K \leq (\sqrt{q} + 1)^{2g}.$$

*Remark* 1.3.8. Suppose that we do not know a proof of the Hasse-Weil theorem, but we do know the above corollary. As we did with the Hasse-Weil bound, one might ask if we can (partially) derive the Hasse-Weil theorem from this. To the author's knowledge, there is no relatively easy way to derive the full Hasse-Weil theorem from Corollary 1.3.7, even if we assume that we have Corollary 1.3.7 over the fields $K_r$ for all $r \geq 1$. However, we can derive a quick upper bound for $|\alpha_i|$. Indeed, suppose that we have Corollary 1.3.7 for all fields $K_r$ with $r \geq 1$. If $|\alpha_i| < 1$ for some $1 \leq i \leq 2g$, then $\lim_{r\to\infty} |1 - \alpha_i^r| = 1$.

[2] You might say something like "the Hasse-Weil bound being true for all fields $K_r/\mathbb{F}_{q^r}$ is equivalent to the Hasse-Weil theorem being true over these fields". However, this does not really make sense, since both theorems are proven to be true for all global function fields $K/\mathbb{F}_q$ and therefore they are logically equivalent to any other true statement.

Now suppose for contradiction that for some $1 \leq j \leq 2g$ we have $|\alpha_j| > (\sqrt{q}+1)^{2g}$. Then there exists a constant $c$, effectively computable in terms of the $\alpha_i$, such that if $r \geq c$ then

$$h_{K_r} = \prod_{i=1}^{2g} |1-\alpha_i^r| > (\sqrt{q^r}+1)^{2g}.$$

This contradicts Corollary 1.3.7 for the field $K_r$. Hence, we conclude that we must have

$$|\alpha_i| \leq (\sqrt{q}+1)^{2g}.$$

$\diamondsuit$

*Remark* 1.3.9. In the later chapters of this thesis we will derive a lower bound for the class number $h_K$. Similar to Remark 1.3.8, the author has attempted to use this to bound the modulus of the $\alpha_i$, the reciprocals of the roots of the $L$-polynomial of $K$. However, these attempts were unsuccessful. To see why only a lower bound for the class number does not give much information about the $\alpha_i$, suppose that we have a lower bound

$$B < h_K = \prod_{i=1}^{2g}(1-\alpha_i). \tag{1.3.2}$$

Since that $\alpha_i$ are the complex roots of the polynomial $L^{\perp}(t) \in \mathbb{Z}[t]$, they come in complex conjugate pairs. We assume that we ordered the $\alpha_i$ such that $\alpha_{2g-1}$ is the complex conjugate of $\alpha_{2g}$. Now, if we just want numbers $\alpha_i$ satisfying the bound (1.3.2), then we could choose $\alpha_1, \ldots, \alpha_{2g-2}$ as any set of $g-1$ pairs of complex conjugate numbers, and then we can choose $\alpha_{2g-1}$ and $\alpha_{2g}$ large enough such that the bound is satisfied. The same is true if for finitely many $r \geq 1$ we want to satisfy bounds of the form $B_r < h_{K_r}$. Further, if for every $r \geq 1$ we have a bound $B_r < h_{K_r}$, then if there exist numbers $\alpha_i$ that satisfy these bounds for all $r \geq 1$, then for every choice of the values of $\alpha_1, \ldots, \alpha_{2g-2}$ we can choose $\alpha_{2g-1}$ and $\alpha_{2g}$ large enough such that all the bounds are satisfied. Therefore we cannot bound the modulus of the $\alpha_i$ from just a lower bound for the class number. $\diamondsuit$

## 1.4 Quadratic Fields

Let us briefly restrict our attention to quadratic global function fields, by which we mean global function fields $K$ satisfying $[K : \mathfrak{R}] = 2$. These fields, in particular the imaginary quadratic fields defined in Definition 1.4.2 below, will be the kind of fields for which we derive a lower bound for the class number in the later chapters of this thesis. Recall our assumption that $p \neq 2$.

Recall from Remark 1.2.2 that the degree $[K : \mathbb{F}_q(T)]$ depends on the choice of $T$, so our notion of a quadratic global function field relies on the fact that we fixed a transcendental element $T \in K$.

**Definition 1.4.1.** Let $K/\mathbb{F}_q$ be an algebraic function field such that $\mathbb{F}_q$ is the full constant field of $K$. Then we say that $K$ is a *hyperelliptic function field* if there exists a $T \in K$ such that $T$ is transcendental over $\mathbb{F}_q(T)$ and $[K : \mathbb{F}_q(T)] = 2$. A hyperelliptic function field is called *elliptic* if has genus 1.

Whether a global function field $K$ is hyperelliptic or not is invariant of our choice of $T \in K$ in Remark 1.2.2. Clearly, a quadratic global function field is hyperelliptic.

If $K/\mathbb{F}_q$ is a quadratic global function field, then there exists a square-free polynomial $D \in \mathbb{F}_q[T]$ such that $K = \mathbb{F}_q(T)(\sqrt{D})$. Since $q$ is odd, $K/\mathbb{F}_q(T)$ is separable. The discriminant of $K$ is given by $4D$, see [Ros02, Chapter 17 page 316]. Note that the factor 4 does not really matter here, because $\mathbb{F}_q(T)(\sqrt{D}) \cong \mathbb{F}_q(T)(\sqrt{D/4})$ as $q$ is odd. The genus of $K$ is given by the simple formula

$$g = \frac{\deg(D) - \upsilon}{2} \qquad \text{where } \upsilon = \begin{cases} 1 & \text{if } \deg(D) \text{ is odd,} \\ 2 & \text{if } \deg(D) \text{ is even.} \end{cases}$$

Similar to the number field case, we distinguish between real and imaginary quadratic fields. The following terminology is due to Artin ([Art24]).

**Definition 1.4.2.** Take a quadratic global function field $K = \mathbb{F}_q(T)(\sqrt{D})$ with $D \in \mathbb{F}_q[T]$ square-free. We call $K$ *imaginary quadratic* if either of the following conditions is satisfied:

(i) $\deg(D)$ is odd,

(ii) $\deg(D)$ is even and the leading coefficient of $D$ is not a square in $\mathbb{F}_q^*$.

Otherwise, $K$ is called *real quadratic*.

Equivalent to the above definition, using terminology we will define in then next section we may also call $K$ imaginary quadratic if there is only one prime in $M_K$ at infinity, or real quadratic if $K$ has two primes at infinity, see e.g. [HR92, §0 Part B].

*Remark* 1.4.3. Note in Definition 1.4.2 that when we say "Take a quadratic global function field $K = \mathbb{F}_q(T)(\sqrt{D})$", then we mean that $\mathbb{F}_q(T) = \mathfrak{R}$ is the rational subfield of $K$. In particular, this means that $\mathbb{F}_q$ is the full constant field of $K$. The example below shows that this specification is necessary. If we start with a function field $\mathbb{F}_q(T)$ with full constant field $\mathbb{F}_q$, then the field $\mathbb{F}_q(T)(\sqrt{D})$ for some square-free $D \in \mathbb{F}_q[T]$ may not always be quadratic. ♢

**Example 1.4.4.** Consider the field $\mathbb{F}_5(T)$ with full constant field $\mathbb{F}_5$. We take the polynomial

$$D = 3T^4 + 2T^2 + 2 \quad \in \mathbb{F}_5[T],$$

which is irreducible (and hence square-free) in $\mathbb{F}_5[T]$. We consider the field $K = \mathbb{F}_5(T)(\sqrt{D})$. Note that we have

$$\left(\frac{\sqrt{D}}{T^2+2}\right)^2 = \frac{3T^4 + 2T^2 + 2}{T^4 + 4T^2 + 4} = 3,$$

and over $k' = \mathbb{F}_q(\sqrt{3})$ we can factor $D$ as

$$D = \left(\sqrt{3}T^2 + 2\sqrt{3}\right)^2.$$

Hence $K = k'(T)$. Therefore the full constant field of $K$ is $k'$, and $\mathfrak{R} = k'(T) = K$. We conclude that $K$ is not a quadratic global function field. ♢

Let $K/\mathbb{F}_q$ be a global function field. Then a finite field extension $L/K$ is said to be *geometric* if $\mathbb{F}_q$ is the full constant field of the global function field $L$. The quadratic global function fields with rational subfield $\mathfrak{R} = \mathbb{F}_q(T)$ are exactly the geometric extensions of $\mathfrak{R}$ of degree 2. The example above shows an extension $K/\mathbb{F}_5(T)$ that is not geometric. If $D \in \mathbb{F}_q[T]$ is a polynomial, then by [Has80, p. 362-366] the extension $\mathbb{F}_q(T)(\sqrt{D})$ over $\mathbb{F}_q(T)$ is geometric if and only if the polynomial $D$ is square-free in $k'(T)$ for every algebraic extension $k'/\mathbb{F}_q$. In particular, this implies for any polynomial $D \in \mathbb{F}_q[T]$ of odd degree that the extension $\mathbb{F}_q(T)(\sqrt{D})/\mathbb{F}_q(T)$ is geometric.

We conclude this section by noting that for an imaginary quadratic global function field $K$, which is the type of field of interest for the later chapters of this thesis, the class numbers $h_K$ and $h_K^I$ defined on page 7 differ at most by a factor 2.

**Proposition 1.4.5.** *Let $K = \mathbb{F}_q(T)(\sqrt{D})$ be an imaginary quadratic global function field. Then*

$$h_K = \begin{cases} h_K^I & \textit{if } \deg(D) \textit{ is odd,} \\ \frac{1}{2}h_K^I & \textit{else.} \end{cases}$$

*Proof.* This immediately follows from [Ros02, Prop. 14.7] and [HR92, Prop. 0.3]. □

## 1.5 Absolute Values and the Product Formula

In this section we will concern ourselves with the absolute values on a global function field $K$. Our main result will be that they satisfy the product formula, as stated in Theorem 1.5.5 below. Further, recall that the places of a number field $K$ are defined as the equivalence classes of absolute values on $K$. As we will see, equivalence classes of absolute values on a global function field essentially amount to the same thing as the places we defined in Definition 1.1.2.

Let us start by considering the absolute values on a rational function field $\mathbb{F}_q(T)$. We take an element $f/g \in \mathbb{F}_q(T)$, where $f$ and $g$ are coprime polynomials in $\mathbb{F}_q[T]$ with $g \neq 0$. Let $\mathfrak{p} \in \mathbb{F}_q[T]$ be an irreducible monic polynomial. Then there is a unique integer $n$ such that we can write

$$\frac{f}{g} = \mathfrak{p}^n \cdot \frac{f'}{g'},$$

for some $f', g' \in \mathbb{F}_q[T]$ that are coprime and not divisible by $\mathfrak{p}$. We define the $\mathfrak{p}$-*valuation* $v_\mathfrak{p} : \mathbb{F}_q(T) \to \mathbb{Z}$ as

$$v_\mathfrak{p}(f/g) = n.$$

We also define the *degree valuation* $v_\infty : \mathbb{F}_q(T) \to \mathbb{Z}$ as

$$v_\infty(f/g) = \deg(g) - \deg(f).$$

You may view the degree valuation as taking a rational function $f/g$ in $T$ to its order of vanishing at $\infty$, explaining our choice of notation.

For every irreducible monic polynomial $\mathfrak{p} \in \mathbb{F}_q[T]$, the $\mathfrak{p}$-valuation leads to an absolute value $|\cdot|_\mathfrak{p} : \mathbb{F}_q(T) \to \mathbb{R}_{\geq 0}$ defined as follows: $|0|_\mathfrak{p} = 0$ and for $f/g \in \mathbb{F}_q(T)^*$ we have

$$|f/g|_\mathfrak{p} = q^{-v_\mathfrak{p}(f/g) \cdot \deg p}. \tag{1.5.1}$$

Similarly, the degree valuation induces an absolute value $|\cdot|_\infty : \mathbb{F}_q(T) \to \mathbb{R}_{\geq 0}$ with $|0|_\infty = 0$ and for $f/g \in \mathbb{F}_q(T)^*$ we have

$$|f/g|_\infty = q^{\deg f - \deg g}. \tag{1.5.2}$$

Note that these absolute values are all non-archimedean, and the corresponding valuations are normalised discrete valuations. We define the set

$$M'_{\mathbb{F}_q(T)} = \{|\cdot|_\mathfrak{p} : \mathfrak{p} \in \mathbb{F}_q[T] \text{ irreducible and monic}\} \cup \{|\cdot|_\infty\} \tag{1.5.3}$$

of absolute values on $\mathbb{F}_q(T)$. Then all absolute values in $M'_{\mathbb{F}_q(T)}$ are inequivalent as absolute values, and up to equivalence they are in fact all the non-trivial absolute values on $\mathbb{F}_q(T)$ ([Sti09, Theorem 1.2.2]). From (1.5.1) and (1.5.2) it is easy to see that for $f/g \in \mathbb{F}_q(T)^*$ we have the so-called *product formula*:

$$\prod_{|\cdot|_v \in M'_{\mathbb{F}_q(T)}} |f/g|_v = 1. \tag{1.5.4}$$

*Remark* 1.5.1. Note that the above definitions of the absolute values $|\cdot|_\mathfrak{p}$ and $|\cdot|_\infty$ involve a choice. Namely we could take $|\cdot|_\mathfrak{p} = c^{-v_\mathfrak{p}(\cdot)}$ for any constant $c > 1$ and it would still be an absolute value; similarly for $|\cdot|_\infty$. We choose $c$ as the number of elements of the residue class field of the corresponding valuation, analogous to the definition of the $p$-adic absolute value on $\mathbb{Q}$ for a prime number $p$. The residue field for the absolute value $v_\mathfrak{p}$ on $\mathbb{F}_q(T)$ has $q^{\deg(\mathfrak{p})}$ elements, and the residue field corresponding to $v_\infty$ has $q$ elements ([Sti09, Prop. 1.2.1(a),(c)]). These choices also ensure that the product formula (1.5.4) holds. ♢

It turns out that a similar product formula holds for global fields in general. In fact, one could even define a global field as a field whose completion at each of its absolute values is a local field, and is such that it admits a product formula similar to (1.5.4) ([Sut19]). We will now make more explicit what we mean by 'similar to (1.5.4)'.

For a rational subfield $\mathfrak{R} \in \{\mathbb{F}_q(T), \mathbb{Q}\}$, we define the set $M_\mathfrak{R}$ as the set of all equivalence classes of non-trivial absolute values on $\mathfrak{R}$. For every $v \in M_\mathfrak{R}$ we usually choose a representative absolute value $|\cdot|_v$. The set $M'_{\mathbb{F}_q(T)}$ of representatives for $M_{\mathbb{F}_q(T)}$ from (1.5.3) is called the *standard set of absolute values on* $\mathbb{F}_q(T)$. The set of standard absolute values on $\mathbb{Q}$, i.e. the standard representatives for $M_\mathbb{Q}$, consists of the 'usual' absolute value and the $p$-adic absolute values for primes $p$. If $w$ is an equivalence class of absolute values on $K$, then the restrictions to $\mathfrak{R}$ of the absolute values in $w$ form an equivalence class $v$ of absolute values on $\mathfrak{R}$. Then we say that $w$ restricts[3] to $v$ and we denote this by $w \mid v$. For our purposes, we only consider classes of absolute values on global fields that do not restrict to the trivial absolute value on $\mathfrak{R}$.

[3] One might also say that $w$ extends $v$, $w$ lies above $v$, or $w$ divides $v$.

**Definition 1.5.2.** Let $K$ be a global field with rational subfield $\mathfrak{R}$. Then we define $M_K$ as the set of all equivalence classes of absolute values on $K$ that restrict to elements of $M_{\mathfrak{R}}$. An equivalence class of absolute values on $K$ is also called a *prime* of $K$. For every prime $v \in M_K$ we choose a representative absolute value $|\cdot|_v$, such that on $\mathfrak{R}$ this representative absolute value coincides with one of the standard absolute values on $\mathfrak{R}$.

Note that if $\mathfrak{R} = \mathbb{F}_q(T)$, then all primes in $M_{\mathfrak{R}}$ are non-archimedean, as we showed at the beginning of this section. Therefore the primes of a global function field all restrict to non-archimedean primes, which implies that they themselves are non-archimedean. For a global function field $K$, every non-archimedean prime corresponds uniquely to a normalised discrete valuation, and vice versa. Hence the set $M_K$ of primes of $K$ is in one-to-one correspondence with the set $\mathbb{P}_K$ of places on $K$. Therefore a prime of $K$ is sometimes also called a *place*, analogous to the places of a number field. We write $\mathcal{O}_v$ for the valuation ring corresponding to a prime $v \in M_K$.

Slightly abusing our notation, we write $v_\infty$ for the prime in $M_{\mathbb{F}_q(T)}$ corresponding to the degree valuation on $\mathbb{F}_q(T)$. For a global function field $K$, it will sometimes be useful to distinguish between the primes restricting to $v_\infty$ on $\mathbb{F}_q(T)$ and the other primes in $M_K$.

**Definition 1.5.3.** Let $K$ be a global function field. We define the subset $S \subset M_K$ as the the set of primes on $K$ that restrict to $v_\infty$ on $\mathbb{F}_q(T)$. An element of $S$ is called a *prime at infinity*.

Using the representative absolute values we fixed in Definition 1.5.2, we are almost ready to state the product formula for general global fields. In the product formula we will need to include a normalizing exponent with the absolute values, using the following definition.

**Definition 1.5.4.** For a global field $K$ with rational subfield $\mathfrak{R}$ and for a prime $v \in M_K$, we define the *local degree of $K$ at $v$*, denoted $n_v$, as

$$n_v = [K_v : \mathfrak{R}_v],$$

where $K_v$ and $\mathfrak{R}_v$ denote the completions of $K$ and $\mathfrak{R}$ at (the restriction of) the prime $v$.

**Theorem 1.5.5** (Product Formula). *Let $K$ be a global field. Then it holds for all $x \in K^*$ that*

$$\prod_{v \in M_K} |x|_v^{n_v} = 1. \tag{1.5.5}$$

*Proof.* For the proof of this Theorem we refer to [Art67, Theorem XII.4]. □

*Remark* 1.5.6. Note that in the above discussion we really used the fact that for a global function field $K$ we fixed an element $T \in K$ (and hence its rational subfield), cf. Remark 1.2.2. Let us briefly consider the situation of a global function field $K$ where no rational subfield $\mathfrak{R} \subset K$ is fixed. Then it is not immediately clear how we should choose the representative absolute values for the primes in $M_K$. Also the notion of a local degree does not make sense in this situation. It turns out that this is not really a problem, as there exist representatives $|\cdot|_v$ such that for all $x \in K^*$

$$\prod_{v \in M_K} |x|_v = 1.$$

Then for a field extension $K'/K$ with a corresponding extension of primes $v' \mid v$ we have

$$|\cdot|_{v'} = |\cdot|_v^{[K'_{v'}:K_v]},$$

see e.g. [Has80, p. 333] ♢

The following result on local degrees will also be useful when we consider height functions over global fields. Please note the similarity with [Sil09, VIII.5.2].

**Theorem 1.5.7** (Extension Formula). *Let $L/K$ be an extension of global fields, and let $v \in M_K$. Then*

$$\sum_{\substack{w \in M_L \\ w \mid v}} n_w = [L : K] n_v.$$

*Proof.* For the case that $K$ is the rational subfield $\mathfrak{R}$ of $L$, we again refer to [Art67, Theorem XII.4]. Further, in general it holds that if $F$ is any field with a non-trivial absolute value $v$ and $E/F$ is a finite extension, then

$$\sum_{w|v}[E_w : F_u] \leq [E : F],$$

see [Lan83, §1.4]. Using these two facts, the rest of the proof is easy. We take an arbitrary prime $u \in M_{\mathfrak{R}}$. Then we have

$$\begin{aligned}
[L : \mathfrak{R}] &= \sum_{\substack{w \in M_L \\ w|u}} n_w \\
&= \sum_{\substack{v \in M_K \\ v|u}} \sum_{\substack{w \in M_L \\ w|v}} n_w \\
&= \sum_{\substack{v \in M_K \\ v|u}} \sum_{\substack{w \in M_L \\ w|v}} [L_w : K_v] n_v \\
&= \sum_{\substack{v \in M_K \\ v|u}} n_v \sum_{\substack{w \in M_L \\ w|v}} [L_w : K_v] \\
&\leq \sum_{\substack{v \in M_K \\ v|u}} n_v [L : K] \\
&= [K : \mathfrak{R}][L : K].
\end{aligned}$$

But we know that $[L : \mathfrak{R}] = [K : \mathfrak{R}][L : K]$, so the above inequality must be an equality. Therefore we find that for every $v \in M_K$ it holds that

$$\sum_{\substack{w \in M_L \\ w|v}} [L_w : K_v] = [L : K].$$

Finally multiplying both sides with $n_v$ gives the desired result. □

## 1.6 Quadratic Forms and Ideals

In Chapters 3 and 4 we will consider so-called elliptic curve ideal class pairings. In the construction of ideal class pairings in [GO20], the authors use the a correspondence between ideal classes in the ring of integers of a quadratic number field and classes of binary quadratic forms. In this section we will see that this correspondence can be extended to quadratic global fields. For quadratic extensions of $\mathbb{F}_p(T)$ with $p$ an odd prime this correspondence was first given by Artin in his thesis [Art24, §I.9-10]. In fact, the correspondence extends far more generally in the sense that classes of binary quadratic forms over any commutative ring $R$ are in correspondence with certain modules over quadratic extensions of $R$. For more information we refer to [Est65, Kap68, Kne82, Woo11], more or less in ascending order of generality.

### 1.6.1 Forms and Number Fields

We start by investigating the form-ideal correspondence in the number field case.

**Definition 1.6.1.** Let $R$ be a commutative ring with identity with characteristic $\text{char}(R) \neq 2$. A *binary quadratic form over* $R$ is a homogeneous polynomial of the form

$$F(X, Y) = aX^2 + bXY + cY^2 \qquad a, b, c \in R,$$

also denoted as $F(X, Y) = (a, b, c)$. The *discriminant* of $F$ is given by $D = b^2 - 4ac$.

This definition of a quadratic form is general enough such that we can use it again when considering the function field case, but in the rest of this subsection we will always work with quadratic forms over $\mathbb{Z}$. Let $F(X, Y) = (a, b, c)$ be such a quadratic form satisfying $D < 0$. Then we know that $4ac > b^2 \geq 0$, so

$a$ and $c$ are both non-zero and have equal signs. Suppose first that $a$ is positive. Then if $F(x,y) \leq 0$ for some pair $(x,y) \in \mathbb{Z}^2 \setminus \{0,0\}$ it holds that

$$|bxy| \geq ax^2 + cy^2 > 0$$

Squaring this equation and using that $4ac > b^2$ yields

$$4acx^2y^2 > a^2x^4 + c^2y^4 + 2acx^2y^2,$$

which rewrites to

$$0 > (ax^2 - cy^2)^2.$$

The last equation obviously has no integer solutions, showing that if $D < 0$ and $a > 0$ we have $F(x,y) \geq 0$ for all pairs $(x,y) \in \mathbb{Z}^2$, with equality if and only if $(x,y) = (0,0)$. Similarly, if $D < 0$ and $a < 0$ we have $F(x,y) \leq 0$ for all $(x,y) \in \mathbb{Z}^2$, with equality only when $(x,y) = (0,0)$. For this reason quadratic forms $(a,b,c)$ with negative discriminant are called *positive definite* if $a > 0$ or *negative definite* if $a < 0$. A quadratic form with positive discriminant is called *indefinite*.

**Definition 1.6.2.** An integer $D \in \mathbb{Z}$ is a *fundamental discriminant* if it is the discriminant of a quadratic number field. Equivalently, $D \neq 1$ and either $D \equiv 1 \pmod 4$ and $D$ is square-free, or $D \equiv 0 \pmod 4$, $D/4$ is square-free and $D/4 \equiv 2$ or $3 \pmod 4$.

There is an action of $\mathrm{SL}_2(\mathbb{Z})$ on the set of quadratic forms over $\mathbb{Z}$ where $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ acts as

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} F(X,Y) = F(\alpha X + \beta Y, \gamma X + \delta Y).$$

We say that two forms $F(X,Y)$ and $G(X,Y)$ are $\mathrm{SL}_2(\mathbb{Z})$*-equivalent* if they lie in the same orbit under this group action. The discriminant of a form and it being positive definite, negative definite or indefinite are both invariant under the the action of $\mathrm{SL}_2(\mathbb{Z})$.

For a negative fundamental discriminant $D \in \mathbb{Z}_{<0}$ we denote the set of equivalence classes of positive definite quadratic forms with fundamental discriminant $D$ by $\mathcal{Q}_D$. We do not include the details here, but we can obtain a group structure on $\mathcal{Q}_D$ using composition of forms, see for example [Cox13, §3.A]. The group $\mathcal{Q}_D$ is also called the *form class group*. The next theorem gives the correspondence between $\mathcal{Q}_D$ and the ideal class group of the number field with discriminant $D$.

**Theorem 1.6.3** ([Cox13, Theorem 7.7(ii)])**.** *Let $D$ be a negative fundamental discriminant, i.e. the discriminant of an imaginary quadratic number field $K$. Then the form class group $\mathcal{Q}_D$ is isomorphic (as groups) to the ideal class group* $\mathrm{CL}(K)$. *In particular, the order of $\mathcal{Q}_D$ equals the class number $h_K$ of $K$.*

*Remark* 1.6.4. The above theorem only tells us something about negative discriminants. For real quadratic fields $K$ the correspondence between the two class groups is a bit more subtle, and involves the *narrow class group* of $K$: the group $\mathrm{CL}^+(K)$ of equivalence classes of ideals of $\mathcal{O}_K$ modulo the group of principal ideals generated by an element of positive norm. In this case we take $\mathcal{Q}_D$ as the group of equivalence classes of forms with discriminant $D$ (all indefinite). The next theorem explains the correspondence for positive discriminants. ♢

**Theorem 1.6.5** ([Bue89, Theorems 6.19 & 6.20])**.** *Let $D$ be the discriminant of a real quadratic number field $K$. Then $\mathrm{CL}^+(K) \cong \mathcal{Q}_D$, and further*

(a) *if there exists a solution $(x,y) \in \mathbb{Z}^2$ to*

$$x^2 - Dy^2 = -4, \tag{1.6.1}$$

*then* $\mathrm{CL}^+(D) \cong \mathrm{CL}(K)$.

(b) *if there exists no solution $(x,y) \in \mathbb{Z}^2$ to* (1.6.1), *then* $\mathrm{CL}(K)$ *consists of the subgroup of squares of* $\mathrm{CL}^+(K)$.

### 1.6.2 Forms and Function Fields

In this subsection $k$ will denote a rational function field $\mathbb{F}_q(T)$ where $q$ is a power of an odd prime. As we noted before, the function-field equivalent of $\mathbb{Z}$ is the polynomial ring $\mathbb{F}_q[T]$. Therefore in this subsection we will exclusively work with quadratic forms over $\mathbb{F}_q[T]$. Our main sources for the material in this subsection are [Est65, Kap68].

Analogous to the number field case, we say that two quadratic forms are $\mathrm{SL}_2(\mathbb{F}_q[T])$-*equivalent* if they share the same orbit under the action of $\mathrm{SL}_2(\mathbb{F}_q[T])$. The discriminant of a form is still invariant under equivalence. Note that in this case there are no such things as positive or negative definite forms, since $\mathbb{F}_q[T]$ is not an ordered ring.

**Definition 1.6.6.** A polynomial $D \in \mathbb{F}_q[T]$ is called a *fundamental discriminant* if it is the discriminant of a quadratic global function field. Equivalently (cf. §1.4), $D \in \mathbb{F}_q[T]$ is a fundamental discriminant if and only if for every algebraic extension $k'/\mathbb{F}_q$ the polynomial $D$ is square-free in $k'(T)$.

Let $D \in \mathbb{F}_q[T]$ a fundamental discriminant. We denote by $\mathcal{Q}_D$ the set of equivalence classes of quadratic forms with discriminant $D$. Again, we can obtain a group structure on $\mathcal{Q}_D$ using composition of forms, see [Est65, Chapter I]. Consider the quadratic extension $K = k(\sqrt{D})$. As we saw in Section 1.4, the ring of integers of $K$ is $\mathcal{O}_K = \mathbb{F}_q[T] \oplus \mathbb{F}_q[T]\sqrt{D}$ and has discriminant $D$ (actually $4D$, but the factor 4 is really not important). Recall that we denote the ideal class group of $\mathcal{O}_K$ by $\mathcal{I}_K$.

**Theorem 1.6.7** ([Kap68, §6])**.** *There exists a homomorphism from $\mathcal{Q}_D$ onto $\mathcal{I}_K$ with kernel isomorphic to the units of $\mathbb{F}_q[T]$ modulo the norms of the units of $\mathcal{O}_K$.*

The unit group $\mathbb{F}_q[T]^*$ consists of the constant polynomials in $\mathbb{F}_q[T]$. An element $u = f + g\sqrt{D} \in \mathcal{O}_K$ has norm $N(u) = f^2 - Dg^2$, and $u \in \mathcal{O}_K^*$ if and only if $N(u) \in \mathbb{F}_q[T]^*$. Now we restrict our attention to imaginary quadratic function fields. So we suppose that $D$ either has odd degree or it has even degree and its leading coefficient is not a square. Let $u = f + g\sqrt{D} \in \mathcal{O}_K^*$. This implies in particular that $\deg(f^2 - Dg^2) = 0$, so $f^2$ and $Dg^2$ must have the same degree. If $\deg(D)$ is odd, then $\deg(Dg^2)$ is also odd unless $g = 0$. This implies $g = 0$ and therefore $u = f$ must be a non-zero constant polynomial. If $\deg(D)$ is even and the leading coefficient of $D$ is not a square, then the leading coefficient of $Dg^2$ is not a square. Since $f^2 - Dg^2$ is a constant this implies that $f, g$ and $D$ must all be constants, and therefore $u$ is a non-zero constant as well. This shows that for imaginary quadratic fields $K$ the units of $\mathcal{O}_K$ consist of just the constant polynomials, meaning that

$$\mathcal{O}_K^* = \mathbb{F}_q[T]^* \cong \mathbb{F}_q^*.$$

The norm of a constant polynomial is just its square. Since $\mathbb{F}_q^*$ is a cyclic group of even order $q-1$, we know that $\mathbb{F}_q^*/(\mathbb{F}_q^*)^2 \cong \mathbb{Z}/2\mathbb{Z}$. Hence we obtain the following corollary of Theorem 1.6.7.

**Corollary 1.6.8.** *Let $K$ be an imaginary quadratic global function field with discriminant $D$. Then*

$$\mathcal{Q}_D/(\mathbb{Z}/2\mathbb{Z}) \cong \mathcal{I}_K.$$

*Remark* 1.6.9. Note that Corollary 1.6.8 implies that the order of $\mathcal{Q}_D$ is twice the ideal class number of $K$, whereas for number fields these were equal. It is also possible to use another definition of the equivalence of forms by using the group $\mathrm{GL}_2(\mathbb{F}_q[T])$ instead of $\mathrm{SL}_2(\mathbb{F}_q[T])$. Then, at least in the case that $q$ is prime, we can obtain a form class group that is in bijection with the ideal class group $\mathcal{I}_K$, see [Art24, §I.10]. ♢

## 1.7 Elliptic Curves over Global Fields

In the next chapters we will consider elliptic curves over global function fields. Many classic textbooks covering the basic theory of elliptic curves, e.g. [Sil09] or [Mil06], only consider elliptic curves defined over a perfect base field. As we noted before, global function fields are not perfect. Hence it is not immediately clear which basic facts about elliptic curves also hold over global function fields. It turns out that many results carry over without too many complications. In this section we will state a few basic properties of elliptic curves over global function fields that we will need in subsequent chapters. For a (much) more detailed introduction to elliptic curves over function fields, we refer to [Ulm11].

In this section $K$ denotes a general global field.

We start by showing that every elliptic curve over a global field can be given by a Weierstrass equation.

**Theorem 1.7.1.** *Let $E/K$ be an elliptic curve. Then $E$ is isomorphic to a projective curve given by an equation of the form*

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

*with coefficients $a_i \in K$, also called a* Weierstrass equation*.*

*Proof.* For perfect fields $K$, this well-known theorem can be found in for example [Sil09, Prop. III.3.1]. However, many authors do not treat the case when $K$ is an algebraic function field. Fortunately, the proof relies mainly on the Riemann-Roch Theorem for curves which also holds over general algebraic function fields, see Remark 1.7.2 below. With the knowledge that we can use the Riemann-Roch Theorem, we refer to [Mil06, pages 47–48] for a proof of the theorem which works in general for elliptic curves over any global field. □

*Remark* 1.7.2. In the proof of the above theorem we need a version of the Riemann-Roch Theorem for smooth projective curves defined over a perfect field $K$ as stated in for example [Sil09, Theorem II.5.4] that allows for curves over an algebraic function field $K$. A second version of the Riemann-Roch Theorem for general algebraic function fields $F/K$ in one variable where the ground field $K$ can be any field can be found in [Sti09, Theorem 1.5.15]. In fact, the Riemann-Roch Theorem for smooth projective curves is a special case of the theorem for algebraic function fields, where we take as function field the function field of the curve. Given a smooth projective curve over any field $K$, its function field will be an algebraic function field in one variable over $K$. Hence the second version of the Riemann-Roch Theorem for general algebraic function fields implies a generalisation of the first version to smooth projective curves over any field $K$. ♢

**Corollary 1.7.3.** *Let $K$ be a global field such that* $\operatorname{char}(K) \notin \{2, 3\}$*. Then any elliptic curve $E/K$ is isomorphic to a curve given by an equation of the form (in affine coordinates)*

$$E' : y^2 = x^3 + a_4x + a_6, \qquad a_4, a_6 \in K,$$

*called a* short Weierstrass equation*.*

*Proof.* This is shown for number fields in [Sil09, §III.1], but using Theorem 1.7.1 the same proof works for general global fields. □

We will mostly be interested in elliptic curves over $\mathbb{Q}$ or $\mathbb{F}_q(T)$. The rational points on these curves can be written in a convenient form.

**Proposition 1.7.4.** *Let $\mathfrak{R} \in \{\mathbb{Q}, \mathbb{F}_q(T)\}$ be a rational global field, and let $E/\mathfrak{R}$ be an elliptic curve given by*

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

*such that the coefficients $a_i$ all lie in the ring of integers $\mathcal{O}_{\mathfrak{R}}$ of $\mathfrak{R}$. Then for every affine point $P \in E(\mathfrak{R}) \setminus \{\mathcal{O}\}$ there exist elements $A, B, C \in \mathcal{O}_{\mathfrak{R}}$ with* $\gcd(A, C) = \gcd(B, C) = 1$*, unique up to multiplication with a unit, such that*

$$P = \left( \frac{A}{C^2}, \frac{B}{C^3} \right).$$

*Proof.* Note that $\mathcal{O}_{\mathfrak{R}}$ is equal to either $\mathbb{Z}$ or $\mathbb{F}_q[T]$, and recall that both of these rings allow unique factorization of non-zero elements as a product of prime elements, up to multiplication with a unit. As we saw in Section 1.5, each prime element $\mathfrak{p} \in \mathcal{O}_{\mathfrak{R}}$ corresponds to a discrete valuation $v_{\mathfrak{p}}$ on $\mathfrak{R}$. Take a point $P = (x, y) \in E(\mathfrak{R})$. For any prime element $\mathfrak{p} \in \mathcal{O}_{\mathfrak{R}}$, we see from the Weierstrass equation for $E$ that $v_{\mathfrak{p}}(x) < 0$ if and only if $v_{\mathfrak{p}}(y) < 0$. Further, since the coefficients of $E$ are all $v_{\mathfrak{p}}$-integral, if $v_{\mathfrak{p}}(x) < 0$ then $3v_{\mathfrak{p}}(x) = 2v_{\mathfrak{p}}(y)$. Therefore, if we write $x = a/b$ and $y = c/d$ as fractions in lowest terms with numerator and denominator in $\mathcal{O}_{\mathfrak{R}}$, we must have $b^3 = d^2$, up to multiplication with a unit. In particular, this implies that $b$ can be written as $b = u \cdot C^2$ with $u \in \mathcal{O}_{\mathfrak{R}}^*$ and $C \in \mathcal{O}_{\mathfrak{R}}$. Then $d = v \cdot C^3$ with $v \in \mathcal{O}_{\mathfrak{R}}^*$. Now, we put $A = a/u$ and $B = c/v$, such that $x = A/C^2$ and $y = B/C^3$. Then $\gcd(A, C) = \gcd(B, C) = 1$, and uniqueness follows from unique factorization in $\mathcal{O}_{\mathfrak{R}}$. □

*Remark* 1.7.5. In the above proposition, the elements $A, B$ and $C$ are unique up to multiplication with a unit. We can ensure that $A$, $B$ and $C$ are truly unique by assuming for example that $C$ is positive if $\mathfrak{R} = \mathbb{Q}$, or that $C$ is monic if $\mathfrak{R} = \mathbb{F}_q[T]$. ♢

Lastly, we will also need a generalisation of the Mordell-Weil theorem to elliptic curves over global function fields. In fact, there exists a much vaster generalisation to abelian varieties over finitely generated regular field extensions, called the Lang-Néron Theorem, but we will only state the specific case that we need.

**Theorem 1.7.6.** *Let $E/K$ be an elliptic curve. Then*

$$E(K) \cong E(K)_{\mathrm{tors}} \times \mathbb{Z}^r,$$

*where $r$ is called the* rank *of $E$.*

*Proof.* This is a special case of [Con06, Cor. 7.2]. □

# Chapter 2

# Heights on Elliptic Curves over Global Fields

In later chapters of this thesis it will be convenient to use the theory of height functions on an elliptic curve over a global field. In the first chapter, we saw that a global field is either a number field or a global function field. Parts of [Sil09, Chapter VIII] are concerned with heights on projective space and on elliptic curves over number fields. In this chapter we will show that most of these results can be generalised to the case of global fields. Our main goal is to prove Theorem 2.3.6 saying that the canonical height on an elliptic curve $E$ over a global field $K$ extends to a positive quadratic form on $E(K) \otimes_{\mathbb{Z}} \mathbb{R}$. In the last section we will use local height functions to bound the difference between the canonical height and the height on an elliptic curve over a global field, similar to how this is done in [Sil90] for number fields. Although heavily inspired by the material in [Lan78, §III.4-5], the proofs and results without reference in the last section are original work by the author.

## 2.1 Heights on Projective Space

Since elliptic curves live in projective space, we will first consider the height of a point in projective space before looking at the height of a point on an elliptic curve. In this section we closely follow [Sil09, §VIII.5].

**Definition 2.1.1.** Let $K$ be a global field. Let $P \in \mathbb{P}^N(K)$ be a point with homogeneous coordinates $P = [x_0, \dots, x_N]$. Then we define the *height of $P$ relative to $K$* as

$$H_K(P) = \prod_{v \in M_K} \max\{|x_0|_v, \dots, |x_N|_v\}^{n_v}.$$

The following proposition gives a few basic properties of the height function defined above.

**Proposition 2.1.2.** *Let $P \in \mathbb{P}^N(K)$.*

(a) *The height $H_K(P)$ is independent of the choice of homogeneous coordinates for $P$.*

(b) *The height satisfies*

$$H_K(P) \geq 1.$$

(c) *For an extension $L/K$ of global fields we have*

$$H_L(P) = H_K(P)^{1/[L:K]}.$$

*Proof.* The proof is easy and follows from Theorems 1.5.5 and 1.5.7, completely analogous to how the proof in [Sil09] follows from [Sil09, VIII.5.2 and VIII.5.3]. □

In what follows it will be convenient to have a height function that is not relative to a particular global field. From Proposition 2.1.2 we see how to construct such a function.

**Definition 2.1.3.** Let $\mathfrak{R} \in \{\mathbb{F}_q(T), \mathbb{Q}\}$, and let $P \in \mathbb{P}^N(\overline{\mathfrak{R}})$. Now let $K$ be any global field such that $P \in \mathbb{P}^N(K)$. We define the *absolute height of* $P$ as

$$H(P) = H_K(P)^{1/[K:\mathfrak{R}]}.$$

Note that it is clear from Proposition 2.1.2 that $H(P)$ is independent of our choice for $K$ and that $H(P) \geq 1$.

We recall the definition of a morphism between projective spaces.

**Definition 2.1.4.** A *morphism of degree* $d$ between projective spaces is a map

$$F : \mathbb{P}^N \to \mathbb{P}^M, \qquad F(P) = [f_0(P), \dots, f_M(P)],$$

where $f_0, \dots, f_M \in \overline{\mathfrak{R}}[X_0, \dots, X_N]$ are homogeneous polynomials of degree $d$, such that their only common zero in $\overline{\mathfrak{R}}^{N+1}$ is $X_0 = \cdots = X_N = 0$. If $F$ can be written such that the $f_i$ have coefficients in a global field $K$, then $F$ is said to be *defined over* $K$.

The next theorem shows how the height changes under morphisms between projective spaces.

**Theorem 2.1.5.** *Let $F : \mathbb{P}^N \to \mathbb{P}^M$ be a morphism of degree $d$. Then there exist positive constants $C_1$ and $C_2$, depending only on $F$, such that*

$$C_1 H(P)^d \leq H(F(P)) \leq C_2 H(P)^d \qquad \text{for all } P \in \mathbb{P}^N(\overline{\mathfrak{R}}).$$

*Proof.* For the case $\mathfrak{R} = \mathbb{Q}$ we refer to [Sil09, VIII.5.6]. For the case $\mathfrak{R} = \mathbb{F}_q(T)$ we note that the same proof works, but we make a few remarks. Since all absolute values on a global function field are non-archimedean, the proof for the upper bound actually simplifies and we can take $C_2 = \prod_{v \in M_K} |F|_v^{n_v/[K:\mathfrak{R}]}$. Here $K$ is a global field such that it contains the homogeneous coordinates for $P$ and the coefficients of the $f_i$ (the coordinate functions of $F$), and we write

$$|F|_v = \max\{|a|_v : a \text{ is a coefficient of some } f_i\}.$$

For the lower bound, a similar thing happens. First of all, we note that the application of the Nullstellensatz ([Har77, I.1.3A]) in the proof works exactly the same for function fields. The rest of the proof also works for function fields, and just like before the bounds even slightly simplify because all absolute values are non-archimedean. □

Recall that for a global field $K$ we can view $\mathbb{P}^1(K)$ as a copy of $K$ with an extra point at infinity. This motivates the following notation: for an element $x \in K$ we write $H_K(x) = H_K([x, 1])$, and similarly for any element $x \in \overline{\mathfrak{R}}$ we write $H(x) = H([x, 1])$. The next theorem gives a relation between the coefficients of a polynomial and the height of its roots.

**Theorem 2.1.6.** *Let*

$$f(T) = a_0 T^d + a_1 T^{d-1} + \cdots + a_d = a_0(T - \alpha_1) \cdots (T - \alpha_d) \in \overline{\mathfrak{R}}[T]$$

*be a polynomial of degree $d$. If $\mathfrak{R} = \mathbb{Q}$ then*

$$2^{-d} \prod_{j=1}^{d} H(\alpha_j) \leq H([a_0, \dots, a_d]) \leq 2^{d-1} \prod_{j=1}^{d} H(\alpha_j),$$

*and if $\mathfrak{R} = \mathbb{F}_q(T)$ we can drop the powers of 2 to obtain*

$$H([a_0, \dots, a_d]) = \prod_{j=1}^{d} H(\alpha_j).$$

*Proof.* We refer to the proof of [Sil09, Theorem VIII.5.9], which works in both the number and the function field case. The fact that the powers of two are not necessary in the function field case follows from the fact that then all absolute values are non-archimedean. □

In order to show that there exist only finitely many points of bounded height in projective space, we will need that the height of a point is not affected by the action of the Galois group. For a field extension $E/F$, we will denote the group of automorphisms of $E$ that leave $F$ fixed by $G_{E/F}$. Note that if $E$ is Galois over $F$, then $G_{E/F} = \mathrm{Gal}(E/F)$. Further, if $\overline{F}$ is an algebraic closure of $F$, and $F^{\mathrm{sep}}$ is the separable closure of $F$ (in $\overline{F}$), then we have $G_{\overline{F}/F} = G_{F^{\mathrm{sep}}/F} = \mathrm{Gal}(F^{\mathrm{sep}}/F)$. Note that for $\mathbb{Q}$ we have $\overline{\mathbb{Q}} = \mathbb{Q}^{\mathrm{sep}}$, but for $\mathbb{F}_q(T)$ this is not the case.

**Theorem 2.1.7.** *Let $P \in \mathbb{P}^N(\overline{\mathfrak{R}})$, and let $\sigma \in G_{\overline{\mathfrak{R}}/\mathfrak{R}}$. Then*

$$H(P^\sigma) = H(P).$$

*Proof.* For $\mathfrak{R} = \mathbb{Q}$ this is proved in [Sil09, Theorem VIII.5.10]. For $\mathfrak{R} = \mathbb{F}_q(T)$, the same proof works. Note that in the latter case $\overline{\mathfrak{R}}/\mathfrak{R}$ is not Galois, but this is not a problem. We only need that $G_{\overline{\mathfrak{R}}/\mathfrak{R}}$ is the group of automorphisms of $\overline{\mathfrak{R}}$ that leave $\mathfrak{R}$ fixed. □

For a point $P = [x_0, \dots, x_N] \in \mathbb{P}^N(\overline{\mathfrak{R}})$ we define its *minimal field of definition*, denoted by $\mathfrak{R}(P)$, as

$$\mathfrak{R}(P) = \mathfrak{R}(x_0/x_i, \dots, x_N/x_i) \qquad \text{for any } i \text{ with } x_i \neq 0.$$

Note that for any point $P \in \mathbb{P}^N(\overline{\mathfrak{R}})$ the field $\mathfrak{R}(P)$ is a global field.

**Theorem 2.1.8.** *Let $C$ and $d$ be two constants. Then the set*

$$\{P \in \mathbb{P}^N(\overline{\mathfrak{R}}) : H(P) < C \text{ and } [\mathfrak{R}(P) : \mathfrak{R}] < d\}$$

*is finite. In particular, for any global field $K$,*

$$\{P \in \mathbb{P}^N(K) : H_K(P) \leq C\}$$

*is a finite set.*

*Proof.* For the proof we refer to [Sil09, Theorem VIII.5.11], which works for number fields and also for function fields by Theorem 2.1.6 and Theorem 2.1.7. However, we note that this proof relies on the easy-to-prove case of this theorem with $K = \mathfrak{R}$. We will show that it is indeed true when $\mathfrak{R} = \mathbb{F}_q(T)$, the other case $\mathfrak{R} = \mathbb{Q}$ can be found in [Sil09, VIII.5.1].

We show that the set $\{P \in \mathbb{P}^N(\mathbb{F}_q(T)) : H_{\mathbb{F}_q(T)}(P) \leq C\}$ is finite. Note from Definition 2.1.3 that for $P \in \mathbb{P}^N(\mathbb{F}_q(T))$ we have $H_{\mathbb{F}_q(T)}(P) = H(P)$. Let $P \in \mathbb{P}^N(\mathbb{F}_q(T))$ be a point, then we can find homogeneous coordinates $P = [x_0, \dots, x_N]$ for $P$ such that

$$x_0, \dots, x_N \in \mathbb{F}_q[T] \qquad \text{and} \qquad \gcd(x_0, \dots, x_N) = 1.$$

From Definition 2.1.1 we see that

$$H(P) = \prod_{v \in M_{\mathbb{F}_q(T)}} \max\{|x_0|_v, \dots, |x_N|_v\}.$$

Recall that the standard set of representative absolute values for $M_{\mathbb{F}_q(T)}$ is given by (1.5.3). Let $p \in \mathbb{F}_q[T]$ be a monic irreducible polynomial. Note that since the coordinates $x_0, \dots, x_N$ of $P$ are all in $\mathbb{F}_q[T]$ it holds that $|x_i|_p \leq 1$ for all $i = 1, \dots, N$. Since $\gcd(x_0, \dots, x_N) = 1$, there must be a coordinate $x_i$ of $P$ such that $\gcd(x_i, p) = 1$, which implies that $|x_i|_p = 1$. Hence we find that for every monic irreducible $p \in \mathbb{F}_q[T]$ it holds that

$$\max\{|x_0|_p, \dots, |x_N|_p\} = 1.$$

Therefore we obtain

$$H(P) = \max\{|x_0|_\infty, \dots, |x_N|_\infty\} = \max_{1 \leq i \leq N} q^{\deg x_i}. \tag{2.1.1}$$

Now, from the fact that there are only finitely many polynomials in $\mathbb{F}_q[T]$ of a given degree, it follows that there are only finitely many points $P \in \mathbb{P}^N(\mathbb{F}_q(T))$ with $H(P) \leq C$. □

## 2.2 Heights on Elliptic Curves

In this section we define a height function on elliptic curves, following [Sil09, §VIII.6]. Throughout this section, $K$ will denote a global field with rational subfield $\mathfrak{R}$ such that $\operatorname{char}(K) \notin \{2,3\}$, unless stated otherwise. We make this assumption on the characteristic of $K$ for simplicity, as it ensures that every elliptic curve over $K$ is given by a short Weierstrass equation, cf. Corollary 1.7.3. By "Let $E/K$ be an elliptic curve" we will mean that we take an elliptic curve $E/K$ given by a short Weierstrass equation of the form

$$E : y^2 = x^3 + a_4 x + a_6, \qquad a_4, a_6 \in K.$$

We start by introducing some notation.

**Definition 2.2.1.** Let $S$ be a set and let $f, g : S \to \mathbb{R}$ be two functions. Then by the formula

$$f = g + O(1)$$

we mean that there exist constants $C_1, C_2 \in \mathbb{R}$ such that

$$C_1 \leq f(P) - g(P) \leq C_2 \quad \text{for all } P \in S. \tag{2.2.1}$$

We may also write

$$f(P) = g(P) + O(1) \quad \text{for all } P \in S$$

to mean the same thing. If only the lower inequality in (2.2.1) holds, then we write $f \geq g + O(1)$. Similarly, if only the upper inequality holds we write $f \leq g + O(1)$.

It will also be convenient to use the logarithmic height.

**Definition 2.2.2.** The *(absolute) logarithmic height* on projective space is the map

$$h : \mathbb{P}^N(\overline{\mathfrak{R}}) \to \mathbb{R}, \qquad h(P) = \log(H(P))$$

Note that Proposition 2.1.2b implies that $h(P) \geq 0$ for all $P$.

Our goal is to define a height function on $E(\overline{K})$. For this purpose we consider the following map:

$$x : E \to \mathbb{P}^1, \qquad P \mapsto \begin{cases} [x,1] & \text{if } P = (x,y) \text{ is an affine point} \\ [1,0] & \text{if } P \text{ is a point at infinity} \end{cases} \tag{2.2.2}$$

Note that this map is in fact a morphism of projective varieties ([Sil09, Example II.2.2]).

**Definition 2.2.3.** Let $E/K$ be an elliptic curve. Then we define the *height on $E$* as the function

$$h_x : E(\overline{K}) \to \mathbb{R}_{\geq 0}, \qquad h_x(P) = h(x(P)).$$

*Remark* 2.2.4. We use the notation $h_x$ to stress the fact that our height function comes from the morphism $x : E \to \mathbb{P}^1$. In general, at least in the case of number fields, for every morphism $f : E \to \mathbb{P}^N$ we can define a *height on $E$ relative to $f$* as

$$h_f : E \to \mathbb{R}_{\geq 0}, \qquad h_f(P) = h(f(P))),$$

see [BG06, §2.4]. A height function on an elliptic curve $E$ relative to a morphism $f$ is also called the *Weil height on $E$ relative to $f$*. In this document we will only consider the height function relative to $x$. In [Sil09, §VIII.6], Silverman treats heights on elliptic curves in slightly more generality, by considering height functions $h_f$ relative to even functions $f \in K(E)$ in the function field of $E$. We chose to just consider the height relative to the even function $x \in K(E)$, because our construction of the canonical height function in Section 2.3 is independent of this choice. ♢

Our first result for the height on an elliptic curve is that there are only finitely many rational points on an elliptic curve with bounded height.

**Theorem 2.2.5.** *Let $E/K$ be an elliptic curve, and let $C \in \mathbb{R}$ be any constant. Then the set*

$$\{P \in E(K) : h_x(P) \leq C\}$$

*is finite.*

*Proof.* Note that if we fix $x$, then the equation $y^2 = x^3 + a_4x + a_6$ has at most two solutions for $y$. Therefore the map $x : E(K) \to \mathbb{P}^1(K)$ as defined above is finite-to-one. Hence $x$ gives a finite-to-one map

$$\{P \in E(K) : h_x(P) \leq C\} \longrightarrow \{Q \in \mathbb{P}^1(K) : H(P) \leq e^C\}.$$

We know from Theorem 2.1.8 that the codomain of this map is finite, which implies that the domain is also finite. □

Next, we look at the relation between the group law on an elliptic curve and the height function.

**Theorem 2.2.6.** *Let $E/K$ be an elliptic curve, and let $P, Q \in E(\overline{K})$ be two points. Then we have*

$$h_x(P+Q) + h_x(P-Q) = 2h_x(P) + 2h_x(Q) + O(1),$$

*where the constants coming from the $O(1)$ term (as in Definition 2.2.1) depend on the elliptic curve $E$, but not on the points $P$ and $Q$.*

*Proof.* For the proof we refer to the proof of [Sil09, Theorem VIII.6.2], which works for number fields as well as for function fields using Theorem 2.1.5 and Theorem 2.1.6. Note that the proof uses the fact that the elliptic curve $E$ is given by a short Weierstrass equation. □

**Corollary 2.2.7.** *Let $E/K$ be an elliptic curve.*

(a) *Fix a point $Q \in E(\overline{K})$. Then*

$$h_x(P+Q) \leq 2h_x(P) + O(1) \qquad \text{for all } P \in E(\overline{K}),$$

*where the $O(1)$-constant depends on $E$ and $Q$, but not on $P$.*

(b) *Let $m \in \mathbb{Z}$. Then*

$$h_x([m]P) = m^2 h_x(P) + O(1) \qquad \text{for all } P \in E(\overline{K}),$$

*where the $O(1)$-constants depend on $E$ and $m$, but not on $P$.*

*Proof.* (a) This follows immediately from Theorem 2.2.6, since $h_x(P-Q) \geq 0$, and $h_x(Q)$ is constant so we can take it inside the $O(1)$ term.

(b) Note that since $x(-P) = x(P)$, we only have to consider non-negative $m$. For $m \in \{0,1\}$ the result is trivial. We complete the proof using induction on $m$. Suppose the result is true for some $m \geq 1$ and also for $m-1$. Now we use Theorem 2.2.6 taking $P = [m]P$ and $Q = P$. Applying our induction hypothesis yields

$$h_x([m+1]P) + (m-1)^2 h_x(P) = 2m^2 h_x(P) + 2h_x(P) + O(1).$$

This rewrites to

$$h_x([m+1]P) = (m+1)^2 h_x(P) + O(1),$$

which finishes the proof by induction. □

## 2.3 The Canonical Height Function

We can interpret the result of Theorem 2.2.6 as saying that the height function $h_x : E(\overline{K}) \to \mathbb{R}_{\geq 0}$ on an elliptic curve $E$ is almost a quadratic form, up to $O(1)$. See Theorem 2.3.3(c) below for what we precisely mean by a function being a quadratic form. It turns out that there exists a quadratic form that only differs from $h_x$ up to $O(1)$, which is called the canonical height function. In this section we will first construct this canonical height function and then we will use it to make $E(\overline{K}) \otimes_{\mathbb{Z}} \mathbb{R}$ into a real inner product space, largely following [Sil09, §VIII.9]. As before, in this section $K$ will denote a global field with rational subfield $\mathfrak{R}$ satisfying $\mathrm{char}(K) \notin \{2,3\}$.

**Proposition 2.3.1.** *Let $E/K$ be an elliptic curve, and let $P \in E(\overline{K})$ be a point. Then the limit*

$$\frac{1}{2} \lim_{N\to\infty} 4^{-N} h_x([2^N]P)$$

*exists.*

*Proof.* The idea of the proof is to use Corollary 2.2.7(b) to show that the sequence is Cauchy, which by the completeness of $\mathbb{R}$ implies that the limit exists. For details, see the proof of [Sil09, Proposition VIII.9.1]. □

The above proposition allows us to make the following definition.

**Definition 2.3.2.** Let $E/K$ be an elliptic curve. The *canonical height on $E$* is the map $\hat{h} : E(\overline{K}) \to \mathbb{R}$ defined by

$$\hat{h}(P) = \frac{1}{2} \lim_{N\to\infty} 4^{-N} h_x([2^N]P).$$

**Theorem 2.3.3.** *Let $E/K$ be an elliptic curve. The canonical height $\hat{h}$ on $E$ has the following properties:*

*(a) Let $P, Q \in E(\overline{K})$ be two points. Then*

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q) \qquad \textit{(parallelogram law).}$$

*(b) For all $P \in E(\overline{K})$ and $m \in \mathbb{Z}$,*

$$\hat{h}([m]P) = m^2\hat{h}(P).$$

*(c) The canonical height $\hat{h}$ on $E$ is a quadratic form, i.e. $\hat{h}$ is an even function and the pairing $\langle\cdot,\cdot\rangle : E(\overline{K}) \times E(\overline{K}) \to \mathbb{R}$ defined as*

$$\langle P, Q\rangle = \tfrac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)), \tag{2.3.1}$$

*is bilinear.*

*(d) For all $P \in E(\overline{K})$ we have $\hat{h}(P) \geq 0$, with equality if and only if $P$ is a torsion point.*

*(e) We have*

$$\hat{h} = h_x + O(1),$$

*where the $O(1)$-constants depend on $E$.*

*Proof.* See [Sil09, Theorem VIII.9.3] for the case that $K$ is a number field. The proof is exactly the same if $K$ is a function field, using Theorem 2.2.5, Theorem 2.2.6 and Corollary 2.2.7(b). □

*Remark* 2.3.4. Note that the pairing in (2.3.1) differs from the one in Silverman's book by a factor $\frac{1}{2}$. This change of definition does not affect the validity of the result or the proof, but adding the factor $\frac{1}{2}$ ensures that $\langle P, P\rangle = \hat{h}(P)$. ♢

Recall from Theorem 1.7.6 that for an elliptic curve $E/K$ we have

$$E(K) \cong E(K)_{\text{tors}} \times \mathbb{Z}^r,$$

where $r$ is called the rank of $E$. Now let $E/K$ be an elliptic curve of rank $r$. We consider the quotient

$$\Lambda = E(K)/E(K)_{\text{tors}} \cong \mathbb{Z}^r.$$

Then the tensor product $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ is a real vector space of dimension $r$, and the lattice $\Lambda$ of rank $r$ embeds injectively into $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$. Note that $E(K) \otimes_{\mathbb{Z}} \mathbb{R} \cong \Lambda \otimes_{\mathbb{Z}} \mathbb{R}$, since the torsion part vanishes in the tensor product. Inspired by Theorem 2.3.3(c,d), which says that the canonical height $\hat{h}$ on $E$ gives a positive definite quadratic form on $\Lambda$, we want to show that the extension of $\hat{h}$ to $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ is also a positive definite quadratic form. The fact that $\hat{h}$ extends uniquely to a quadratic form on $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ follows from the fact that the pairing from (2.3.1) extends uniquely to a bilinear pairing $\langle\cdot,\cdot\rangle : \Lambda \otimes_{\mathbb{Z}} \mathbb{R} \times \Lambda \otimes_{\mathbb{Z}} \mathbb{R} \to \mathbb{R}$, see [Mil06, §IV.6]. Proving that this extension of $\hat{h}$ is also positive definite is less obvious than one might think, but it follows immediately from the next lemma.

**Lemma 2.3.5** ([Sil09, Lemma 9.5])**.** *Let $V$ be a finite dimensional real vector space and let $L \subset V$ be a lattice of full rank in $V$, i.e. $L$ has rank $\dim(V)$. Let $q : V \to \mathbb{R}$ be a quadratic form satisfying the following properties:*

(i) *For $P \in L$, we have $q(P) = 0$ if and only if $P = 0$.*

(ii) *For every constant $C$, the set*

$$\{P \in L : q(P) \leq C\}$$

*is finite.*

*Then $q$ is positive definite on $V$.*

**Theorem 2.3.6.** *Let $E/K$ be an elliptic curve. Then the canonical height on $E$ extends to a positive definite quadratic form on the real vector space $E(K) \otimes_{\mathbb{Z}} \mathbb{R}$.*

*Proof.* This follows immediately from Lemma 2.3.5. We know that $\hat{h}$ satisfies condition (i) from Theorem 2.3.3(d), and condition (ii) follows from Theorem 2.3.3(e) and Theorem 2.2.5. □

The pairing in (2.3.1) is called the *Néron-Tate pairing* or *height pairing* on the elliptic curve. Since the pairing is obviously symmetric, Theorem 2.3.6 implies that the Néron-Tate pairing defines an inner product on $E(K) \otimes_{\mathbb{Z}} \mathbb{R}$. Therefore $E(K) \otimes_{\mathbb{Z}} \mathbb{R}$ becomes a real inner product space of dimension $r$, so there exists an isomorphism $\varphi : E(K) \otimes_{\mathbb{Z}} \mathbb{R} \to \mathbb{R}^r$ where $\mathbb{R}^r$ is equipped with the standard inner product. Hence we can think of $\Lambda$ as a lattice in $\mathbb{R}^r$, where the length of a vector in $\mathbb{R}^r$ corresponding to $P \in \Lambda$ is $\langle P, P\rangle^{\frac{1}{2}} = \hat{h}(P)^{\frac{1}{2}}$. This will be useful later in Section 3.2 when we want to count points in $E(K)$ of bounded canonical height.

## 2.4 Local Heights

We have seen in the previous sections that the logarithmic height of an affine point $P = (x, y)$ on an elliptic curve is given by a sum of local terms, one for each prime $v \in M_K$:

$$h_x(P) = \frac{1}{[K : \mathfrak{R}]} \sum_{v \in M_K} n_v \log \max\{1, |x|_v\}.$$

In this section we will decompose the canonical height function in a similar way as a sum of local height functions, and afterwards we use these local height functions to bound the difference between the canonical height and the height on an elliptic curve over a global field. In the previous sections our references mainly worked over number fields and we had to check for each result whether it holds for global function fields. Here our main references will be [Sil94, Chapter VI] and [Lan78, §III.4-5], and we only have to be careful with Theorem 2.4.6 in this respect.

Recall that we denoted by $M_K$ the set of equivalence classes of absolute values on $K$ that restrict to elements of $M_{\mathfrak{R}}$, and for each prime $v \in M_K$ we chose a representative absolute value $|\cdot|_v$. In what follows we will abuse this notation by also writing $v(\cdot) = -\log|\cdot|_v$ for the additive valuation corresponding to an absolute value $|\cdot|_v$. It should be clear from the context whether $v$ denotes an equivalence class of absolute values or whether it is the additive valuation corresponding to such a class. We call an element $a \in K$ *$v$-integral* if $v(a) \geq 0$.

**Definition 2.4.1.** Let $K$ be a field with an absolute value $|\cdot|_v$, and let $E/K$ be an elliptic curve. We define the *$v$-adic topology on $E(K)$* as follows. For an affine point $P_0 = (x_0, y_0) \in E(K)$, a basis of open neighborhoods of $P_0$ is given by the sets

$$U_\varepsilon = \{(x, y) \in E(K) : |x - x_0|_v < \varepsilon \text{ and } |y - y_0|_v < \varepsilon\}, \qquad \text{all } \varepsilon > 0.$$

For the point $\mathcal{O} \in E(K)$ at infinity a basis of open neighborhoods consists of the sets

$$U_\varepsilon - \{(x, y) \in E(K) : |x|_v > \varepsilon^{-1}\} \cup \{\mathcal{O}\}, \qquad \text{all } \varepsilon > 0.$$

The following theorem describes the local height function corresponding to an absolute value $|\cdot|_v$ and ensures its existence and uniqueness.

**Theorem 2.4.2** ([Sil94, Chapter VI Theorem 1.1])**.** *Let $K$ be a field which is complete with respect to an absolute value $|\cdot|_v$, and let $v(\cdot) = -\log|\cdot|_v$ be the corresponding additive valuation. Let $E/K$ be an elliptic curve given by a Weierstrass equation*

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

*and write $\Delta$ for its discriminant.*

(a) *There exists a unique function* $\lambda_v : E(K) \setminus \{\mathcal{O}\} \to \mathbb{R}$ *with the following properties:*

(i) $\lambda_v$ *is continuous on* $E(K) \setminus \{\mathcal{O}\}$ *and is bounded on the complement of any* $v$*-adic neighborhood of* $\mathcal{O}$.

(ii) *The limit*

$$\lim_{P \xrightarrow{v\text{-adic}} \mathcal{O}} \left\{\lambda_v(P) + \tfrac{1}{2}v(x(P))\right\}$$

*exists.*

(iii) *For all* $P \in E(K)$ *with* $[2]P \neq \mathcal{O}$,

$$\lambda_v([2]P) = 4\lambda_v(P) + v((2y + a_1x + a_3)(P)) - \tfrac{1}{4}v(\Delta).$$

(b) $\lambda_v$ *is independent of the choice of Weierstrass equation for* $E/K$.

(c) *Let* $L/K$ *be a finite extension and* $w$ *the extension of* $v$ *to* $L$. *Then*

$$\lambda_w(P) = \lambda_v(P) \qquad \text{for all } P \in E(K) \setminus \{\mathcal{O}\}.$$

**Definition 2.4.3.** We call the function $\lambda_v$ from Theorem 2.4.2 the *local height function on* $E$ *associated to* $v$.

*Remark* 2.4.4. It is not immediately clear that in Theorem 2.4.2(a)(ii) there exists a sequence of points $\{P_i\}_{i\in\mathbb{N}}$ in $E(K)$ such that the $v$-adic limit of $P_i$ when $i \to \infty$ is equal to $\mathcal{O}$. The result would still hold if such a sequence does not exist, but then the statement would be empty. It turns out that, at least when $K$ is the completion of a global field, such a sequence does exist. The completion of a global field is either a local field or isomorphic to $\mathbb{R}$ or $\mathbb{C}$. For $\mathbb{R}$ and $\mathbb{C}$ the existence of such a sequence is clear. For local fields, one could for example use the canonical $p$-adic filtration on an elliptic curve over a local field to construct such a sequence, see e.g. [Hus04, §14.1]. ♢

*Remark* 2.4.5. Theorem 2.4.2 only gives the defining properties of the local height function and its existence and uniqueness. In many cases it is in fact possible to give explicit formulas for $\lambda_v$, see for example [Sil94, §VI.3-4]. Further, it is important to note that sometimes the local height function is normalized slightly differently. In particular, the term $-\frac{1}{4}v(\Delta)$ in the duplication formula is sometimes left out. The definitions of the local height function in our main sources for this section, see [Sil90, §3], [Sil94, §VI.1] and [Lan78, §III.4], all use the same normalisation as in Definition 2.4.3, cf. [Sil09, Appendix C.18 Prop. 18.1]. Note that what we call the local height function is called the *Néron function* in [Lan78]. ♢

**Theorem 2.4.6.** *Let* $K$ *be a global field with rational subfield* $\mathfrak{R}$, *and let* $E/K$ *be an elliptic curve. Then*

$$\hat{h}(P) = \frac{1}{[K : \mathfrak{R}]} \sum_{v \in M_K} n_v \lambda_v(P) \qquad \text{for all } P \in E(K) \setminus \mathcal{O}.$$

*Proof.* The case that $K$ is a number field is given in [Sil94, Theorem VI.2.1]. We note that the same proof works for global fields using our previous results on the canonical height function for elliptic curves over global function fields and the product formula (1.5.5). □

The main reason why we are interested in local height functions is because they will help us to bound the difference between the canonical height $\hat{h}$ and the 'usual' height $h_x$ on an elliptic curve. When giving these bounds, we will treat the number field case and the function field case separately, starting with number fields.

**Theorem 2.4.7.** *Let* $K$ *be a number field and let* $E/K$ *be an elliptic curve given by a short Weierstrass equation*

$$E : y^2 = x^3 + a_4x + a_6,$$

*such that* $a_4$ *and* $a_6$ *are contained in the ring of integers of* $K$. *We write* $\Delta$ *and* $j$ *for the discriminant and the* $j$*-invariant of* $E$, *respectively. Then for all* $P \in E(\overline{K})$

$$-\tfrac{1}{8}h(j) - \tfrac{1}{12}h(\Delta) - 0.973 \leq \hat{h}(P) - \tfrac{1}{2}h_x(P) \leq \tfrac{1}{12}h(j) + \tfrac{1}{12}h(\Delta) + 1.07.$$

*Proof.* This is a direct consequence of [Sil90, Theorem 1.1]. □

The idea of the proof of Theorem 2.4.7 is to derive similar bounds for the difference between the local height $\lambda_v$ and the local component of $h_x$ for all $v \in M_K$, treating the archimedean and non-archimedean absolute values separately. Then we add the resulting inequalities and use Theorem 2.4.6 to go from local to global. For function fields the idea is the same, except that we only have non-archimedean absolute values. The following theorem will be our starting point. In fact, it is exactly the result we used for non-archimedean absolute values in the number field case.

**Theorem 2.4.8.** *Let $K$ be a field that is complete with respect to a non-archimedean absolute value $|\cdot|_v$, and let $E/K$ be an elliptic curve given by a short Weierstrass equation*

$$E : y^2 = x^3 + a_4x + a_6$$

*such that the coefficients $a_4$ and $a_6$ are both $v$-integral. We write $\Delta$ and $j$ for the discriminant and $j$-invariant of $E$, respectively. Then for all $P \in E(K)$*

$$-\tfrac{1}{24}\log\max\{1, |j|_v\} \le \lambda_v(P) - \tfrac{1}{2}\log\max\{1, |\widetilde{x}(P)|_v\} \le \tfrac{1}{12}\log\max\{1, |\Delta|_v^{-1}\}.$$

*Here the map $\widetilde{x}(P)$ is defined as*

$$\widetilde{x}(P) = \begin{cases} x & \text{if } P = (x, y) \text{ is an affine point} \\ 0 & \text{if } P = \mathcal{O}, \end{cases}$$

*which is different from the morphism $x(P)$ defined in* (2.2.2).

*Proof.* This is proven in [Lan78, Theorem III.4.5]. Note that $v(\Delta) = \log\max\{1, |\Delta|_v^{-1}\}$ because $v(\Delta) = \log|\Delta|_v^{-1}$ and, since the coefficients of $E$ are all $v$-integral, $|\Delta|_v \le 1$. □

Note that Theorem 2.4.8 assumes that the coefficients $a_4$ and $a_6$ of the elliptic curve are both $v$-integral. Compare this to Theorem 2.4.7, where the coefficients of the elliptic curve are assumed to lie in the ring of integers of the number field $K$. In fact, the reason why Theorem 2.4.7 makes this assumption, is because it uses Theorem 2.4.8 for every non-archimedean prime of $K$. We simply use that the ring of integers is the intersection of all the valuation rings corresponding to non-archimedean primes of $K$. For a global function field $K$, the elements of the ring of integers are integral with respect to every prime except those primes extending the prime at infinity. More precisely, we have the following result.

**Proposition 2.4.9.** *Let $K$ be a global function field with ring of integers $\mathcal{O}_K$. We write $S \subset M_K$ for the set of primes lying above the prime at infinity of $\mathbb{F}_q(T)$. Then*

$$\mathcal{O}_K = \bigcap_{v \in M_K \setminus S} \mathcal{O}_v.$$

*Proof.* A proof of this result can be found in [Ros02, §14]. □

The only elements of a global function field $K$ that are integral with respect to every prime, are the constants of $K$ (see [Sti09, Cor. 1.1.20]). Proposition 2.4.9 tells us that elements of the ring of integers $\mathcal{O}_K$ only have poles in the set $S \subset M_K$ of primes at infinity. However, if there are multiple primes above infinity, elements of $\mathcal{O}_K$ can be strictly integral with respect to some of these primes, as demonstrated in the following example.

**Example 2.4.10.** Let $K$ be a global field such that the set $S$ of primes at infinity contains at least two elements. Let $v_1, v_2 \in S$ be distinct primes at infinity. Then the divisor $v_1 - v_2 \in \mathrm{Div}(K)$ has degree 0. Writing $n$ for the class number of $K$, we find that $nv_1 - nv_2$ is a principal divisor of $K$. Hence there exists an element $x \in K$ with $(x) = nv_1 - nv_2$. This means that $v_1(x) = n$ and $v_2(x) = -n$, and for every prime $w \in M_K \setminus S$ we have $w(x) = 0$, showing that $x \in \mathcal{O}_K$. ♢

We want a result similar to Theorem 2.4.7 for a global function field $K$, such that the coefficients of the elliptic curve can be elements from $\mathcal{O}_K$. Proposition 2.4.9 tells us that we can use Theorem 2.4.8 for all primes of $K$, except maybe those at infinity. We will now derive a similar result to Theorem 2.4.8 for elliptic curves with at least one coefficient that, instead of being integral, has non-positive valuation with respect to an non-archimedean absolute value $|\cdot|_v$. Writing $j$ for the $j$-invariant of the elliptic curve, we will treat the cases $v(j) \ge 0$ and $v(j) \le 0$ separately.

**Theorem 2.4.11.** *Let $K$ be a field that is complete with respect to a non-archimedean absolute value $|\cdot|_v$. We assume that the characteristic of the residue class field is not 2 or 3. Let $E/K$ be an elliptic curve given by a short Weierstrass equation*

$$E : y^2 = x^3 + a_4x + a_6,$$

*such that at least one of $v(a_4)$ and $v(a_6)$ is negative. We write $\Delta$ and $j$ for the discriminant and $j$-invariant of $E$, respectively, and we assume $v(j) \geq 0$. Then for all $P \in E(K)$*

$$-\tfrac{1}{12}\log|\Delta|_v \leq \lambda_v(P) - \tfrac{1}{2}\log\max\{1, |\widetilde{x}(P)|_v\} \leq 0,$$

*where $\widetilde{x}$ is defined as in Theorem 2.4.8.*

*Proof.* Our strategy is very similar to that in the proof of [Lan78, Theorem III.4.4]. We take an element $c \in \overline{K}$ such that $c^{12} = 1/\Delta$. From now on we will work over the field $K(c)$. Note that $v$ extends uniquely to a valuation on $K(c)$ (see e.g. [Lan83, Chapter 1 Prop. 2.2]), which we will therefore also denote by $v$. We let

$$a_4' = c^4a_4, \qquad a_6' = c^6a_6, \qquad \Delta' = c^{12}\Delta = 1.$$

Then the elliptic curve

$$E' : y'^2 = x'^3 + a_4'x' + a_6'$$

has discriminant $\Delta'$, and the change of coordinates

$$x' = c^2x, \qquad y' = c^3y$$

gives an isomorphism between $E$ and $E'$. We write $\lambda_v'$ for the local height function corresponding to the elliptic curve $E'$. From Theorem 2.4.2(b) we know that the local height function is independent of the choice of Weierstrass equation for $E/K$. Hence, if $P = (x, y)$ corresponds to $P' = (x', y')$ under the isomorphism, we have

$$\lambda_v(P) = \lambda_v'(P').$$

We denote the $j$-invariant of $E'$ by $j'$. Then $j' = -(48a_4')^3/\Delta'$, which implies $v(j) = v(j') = 3v(a_4')$. Therefore, our assumption that $v(j) \geq 0$ gives $v(a_4') \geq 0$. We have

$$\Delta' = -16(4a_4'^3 + 27a_6'^2).$$

Since $v(\Delta') = 0$ we see that $v(a_6') \geq 0$. Therefore, also using the fact that the reduction of $\Delta'$ in the residue class field is non-zero, by [Lan78, Theorem III.4.3] it holds for any affine point $P' = (x', y')$ corresponding to $P = (x, y)$ that

$$\lambda_v'(P') = \tfrac{1}{2}\log\max\{1, |x'|_v\} = \tfrac{1}{2}\log\max\{1, |c^2x|_v\}.$$

Now let $P = (x, y) \in E(K)$ be an affine point (for $P = \mathcal{O}$ the desired result is trivial). Then

$$\lambda_v(P) - \tfrac{1}{2}\log\max\{1, |\widetilde{x}(P)|_v\} = \tfrac{1}{2}\log\max\{1, |c^2x|_v\} - \tfrac{1}{2}\log\max\{1, |x|_v\}.$$

Note that since at least one of $v(a_4)$ and $v(a_6)$ is negative, and $v(a_4') = v(c^4a_4) \geq 0$ and $v(a_6') = v(c^6a_6) \geq 0$, we must have $v(c) \geq 0$. So in terms of the absolute value we have $|c|_v \leq 1$. Suppose first that $|c^2x|_v \geq 1$. Then it follows that $|x|_v \geq 1$. We obtain

$$\begin{aligned}\lambda_v(P) - \tfrac{1}{2}\log\max\{1, |x|_v\} &= \tfrac{1}{2}\log|c^2x|_v - \tfrac{1}{2}\log|x|_v \\ &= \log|c|_v \\ &= -\tfrac{1}{12}\log|\Delta|_v.\end{aligned}$$

Now suppose that $|c^2x|_v \leq 1$ and $|x|_v \leq 1$. Then clearly

$$\lambda_v(P) - \tfrac{1}{2}\log\max\{1, |x|_v\} = 0 - 0 = 0.$$

Finally, suppose that $|c^2x|_v \leq 1$ and $|x|_v \geq 1$. Then

$$\lambda_v(P) - \tfrac{1}{2}\log\max\{1, |x|_v\} = -\tfrac{1}{2}\log|x|_v.$$

We have $2v(c) + v(x) \geq 0$ and $v(x) \leq 0$, which gives

$$-v(c) \leq \tfrac{1}{2}v(x) \leq 0.$$

Now, using $-v(c) = -\frac{1}{12}\log|\Delta|_v$ and $\frac{1}{2}v(x) = -\frac{1}{2}\log|x|_v$, we find

$$-\tfrac{1}{12}\log|\Delta|_v \leq \lambda_v(P) - \tfrac{1}{2}\log\max\{1, |x|_v\} \leq 0.$$

We have now proved the above inequality for all affine points $P = (x, y) \in E(K)$. □

Next, we consider the case that $v(j) < 0$, so $j$ is not $v$-integral. In that case the elliptic curve is isomorphic to the *Tate curve*. In this thesis we will not give the definition and basic theory of the Tate curve. For more information the reader could look at for example [Lan87, §15.1]. We quickly repeat some material from the second half of [Lan78, §III.5].

Let $E : y^2 = x^3 + a_4x + a_6$ be an arbitrary elliptic curve over a field $K$ that is complete with respect to a non-archimedean absolute value $|\cdot|_v$, and assume that $v(j) < 0$. Then $E$ is isomorphic to the Tate curve, which we denote by $\mathcal{T}$, over at most a quadratic extension $L/K$. With the Tate curve there is a corresponding element $q \in K$ with $|q|_v < 1$. We write $\Delta$ and $\Delta'$ for the discriminants of $E$ and $\mathcal{T}$, respectively. Then there exists a $c \in L$ such that

$$c^{12}\Delta' = \Delta.$$

We write $X$ for the coordinate on the Tate curve corresponding to $x$, given by

$$X = \tfrac{1}{c^2}x - \tfrac{1}{12}$$

Further, we define

$$x' = X + \tfrac{1}{12}.$$

Then

$$v(\Delta') = v(q) = -v(j).$$

We write $\lambda'_v$ for the local height function on $\mathcal{T}$, which is equal to the local height function $\lambda_v$ on $E$ composed with the isomorphism between $\mathcal{T}$ and $E$.

**Theorem 2.4.12** ([Lan78, Cor. of Thm. III.5.2])**.** *On the Tate curve, we have the estimate*

$$\tfrac{1}{24}\log|q|_v \leq \lambda'_v(P') - \tfrac{1}{2}\log\max\{1, |X(P')|_v\} \leq -\tfrac{1}{12}\log|q|_v.$$

Now we are ready to state the equivalent of Theorem 2.4.11 for the case $v(j) < 0$.

**Theorem 2.4.13.** *Let $K$ be a field, complete with respect to a non-archimedean absolute value $|\cdot|_v$. We assume that the characteristic of the residue class field is not 2 or 3. Let $E/K$ be an elliptic curve given by*

$$E : y^2 = x^3 + a_4x + a_6$$

*such that at least one of $v(a_4)$ and $v(a_6)$ is negative. We write $\Delta$ and $j$ for the discriminant and $j$-invariant of $E$, respectively, and we assume $v(j) < 0$. Then for all $P \in E(K)$*

$$-\tfrac{1}{8}\log|j|_v - \tfrac{1}{12}\log|\Delta|_v \leq \lambda_v(P) - \tfrac{1}{2}\log\max\{1, |\widetilde{x}(P)|_v\} \leq \tfrac{1}{12}\log|j|_v,$$

*with $\widetilde{x}$ as defined in Theorem 2.4.8.*

*Proof.* For $P = \mathcal{O}$, the assertion is trivial. For the rest of the proof we let $P = (x, y) \in E(K)$ be an affine point. We will use the isomorphism between $E$ and the Tate curve, using the same notation as in our discussion above Theorem 2.4.12. From $v(\Delta') = -v(j)$ and $v(\Delta) = 12v(c) + v(\Delta')$ we obtain $v(j\Delta) = 12v(c)$. Since $j = -(48a_4)^3/\Delta$, this implies that

$$12v(c) = 3v(a_4). \tag{2.4.1}$$

Suppose for contradiction that $v(a_4) > 0$. Then, by assumption, $v(a_6) < 0$, and therefore $v(\Delta) = 2v(a_6) < 0$. But this implies $v(j) > 0$, contradicting our assumption that $v(j) < 0$. Hence $v(a_4) \leq 0$. Therefore, from (2.4.1) we obtain $v(c) \leq 0$. Writing $P'$ for the point on $\mathcal{T}$ corresponding to $P$, we have

$$\lambda_v(P) - \tfrac{1}{2}\log\max\{1, |x|_v\} = \lambda'_v(P') - \tfrac{1}{2}\log\max\{1, |X|_v\} + \tfrac{1}{2}\log\max\{1, |X|_v\} - \tfrac{1}{2}\log\max\{1, |x|_v\}, \tag{2.4.2}$$

which implies

$$\lambda_v(P) - \tfrac{1}{2}\log\max\{1,|x|_v\} \leq -\tfrac{1}{12}\log|q|_v + \tfrac{1}{2}\log\max\{1,|X|_v\} - \tfrac{1}{2}\log\max\{1,|x|_v\}. \qquad (2.4.3)$$

We will now prove that

$$-\tfrac{1}{12}\log|\Delta|_v - \tfrac{1}{12}\log|j|_v \leq \tfrac{1}{2}\log\max\{1,|X|_v\} - \tfrac{1}{2}\log\max\{1,|x|_v\} \leq 0. \qquad (2.4.4)$$

Indeed, we note first that from $v(j\Delta) = 12v(c)$ it follows that

$$-\log|c|_v = -\tfrac{1}{12}\log|\Delta|_v - \tfrac{1}{12}\log|j|_v.$$

Now, suppose that $X$ is $v$-integral, i.e. $v(X) \geq 0$. Then $\log\max\{1,|X|_v\} = 0$. If also $x$ is $v$-integral, the middle part of (2.4.4) is equal to 0, so the inequality holds. So suppose that $v(x) < 0$. We have $x = c^2(X + \frac{1}{12})$, and from $v(X) \geq 0$ and $v(\frac{1}{12}) = 0$ we obtain $v(X + \frac{1}{12}) \geq 0$. Therefore $|x|_v \leq |c^2|_v$. Then the middle part of (2.4.4) is equal to $-\frac{1}{2}\log|x|_v$ and we have

$$-\log|c|_v \leq -\tfrac{1}{2}\log|x|_v \leq 0,$$

showing that (2.4.4) holds in this case. Now we suppose that $v(X) < 0$. Then $v(X + \frac{1}{12}) = v(X) < 0$, and since $v(c) \leq 0$ this implies $v(x) < 0$. Thus

$$\begin{aligned}\tfrac{1}{2}\log\max\{1,|X|_v\} - \tfrac{1}{2}\log\max\{1,|x|_v\} &= \tfrac{1}{2}\log|X|_v - \tfrac{1}{2}\log|x|_v\\ &= \tfrac{1}{2}\log|X|_v - \log|c|_v - \tfrac{1}{2}\log|X + \tfrac{1}{12}|_v\\ &= -\log|c|_v,\end{aligned}$$

completing our proof of (2.4.4). Using (2.4.2), Theorem 2.4.12 and (2.4.4), we find

$$\begin{aligned}\lambda_v(P) - \tfrac{1}{2}\log\max\{1,|x|_v\} &\geq \tfrac{1}{24}\log|q|_v - \tfrac{1}{12}\log|\Delta|_v - \tfrac{1}{12}\log|j|_v\\ &= -\tfrac{1}{8}\log|j|_v - \tfrac{1}{12}\log|\Delta|_v,\end{aligned}$$

proving the lower bound in the desired result. For the upper bound, we use (2.4.3) and (2.4.4) to obtain

$$\lambda_v(P) - \tfrac{1}{2}\log\max\{1,|x|_v\} \leq -\tfrac{1}{12}\log|q|_v = \tfrac{1}{12}\log|j|_v.$$

□

We can combine Theorem 2.4.11 and Theorem 2.4.13 into one bound without any restrictions on the $j$-invariant.

**Corollary 2.4.14.** *Let $K$ be a field that is complete with respect to a non-archimedean absolute value $|\cdot|_v$, and assume that the characteristic of the residue class field is not* 2 *or* 3*. Let $E/K$ be an elliptic curve given by a short Weierstrass equation*

$$E : y^2 = x^3 + a_4x + a_6,$$

*such that at least one of $v(a_4)$ and $v(a_6)$ is negative. We write $\Delta$ and $j$ for the discriminant and $j$-invariant of $E$, respectively. Then for all $P \in E(K)$*

$$-\tfrac{1}{8}\log\max\{1,|j|_v\} - \tfrac{1}{12}\log\max\{1,|\Delta|_v\} \leq \lambda_v(P) - \tfrac{1}{2}\log\max\{1,|\widetilde{x}(P)|_v\} \leq \tfrac{1}{12}\log\max\{1,|j|_v\},$$

*with $\widetilde{x}$ as in Theorem 2.4.8.*

*Remark* 2.4.15. Note that in Corollary 2.4.14 we could replace the term $\log\max\{1,|\Delta|_v\}$ by $\log|\Delta|_v$ to obtain a better lower bound. When $v(j) \geq 0$ this does not make a difference because from our proof of Theorem 2.4.11 it follows that then $|\Delta|_v \geq 1$. We choose this weaker inequality because it allows us to combine Corollary 2.4.14 and Theorem 2.4.8 to obtain a global bound in terms of height functions, see Theorem 2.4.16 below. ◇

We have now at last come to the point were we can give a bound on the difference between the canonical height $\hat{h}$ and the height $h_x$ on an elliptic curve over a global function field $K$ with coefficients in $\mathcal{O}_K$. In fact, Theorem 2.4.16 below does not even need the assumption that the coefficients lie in $\mathcal{O}_K$, and works for general elliptic curves defined over $K$ (in short Weierstrass form).

**Theorem 2.4.16.** *Let $K$ be a global function field, and let $E/K$ be an elliptic curve given by a short Weierstrass equation*

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

*We write $\Delta$ and $j$ for the discriminant and $j$-invariant of $E$, respectively. Then for all $P \in E(\overline{K})$*

$$-\tfrac{1}{8}h(j) - \tfrac{1}{12}h(\Delta) \leq \hat{h}(P) - \tfrac{1}{2}h_x(P) \leq \tfrac{1}{12}h(\Delta) + \tfrac{1}{12}h(j).$$

*Proof.* Our strategy will be to consider for each prime $v \in M_K$ a local bound given by either Theorem 2.4.8 or Corollary 2.4.14, and then add these local components to obtain the desired global bound. We define the subset $U_E \subset M_K$ as the set of all primes $v \in M_K$ such that at least one of $v(a_4)$ and $v(a_6)$ is negative, and we write $V_E$ for the complement of $U_E$ in $M_K$. We include the subscript $E$ to stress that these sets depend on the specific elliptic curve in consideration. Note that $U_E$ is a subset of the set $S$ of primes at infinity. The primes in $U_E$ are exactly the primes for which we can use Corollary 2.4.14, and the primes in $V_E$ are exactly those for which we can use Theorem 2.4.8. Recall that for an element $a \in K$ we have

$$h(a) = \frac{1}{[K : \mathfrak{R}]} \sum_{v \in M_K} n_v \log \max\{1, |a|_v\}.$$

Clearly, if we only take the sum over a subset of $M_K$, the result will be less than or equal to the entire sum. We put

$$h_{U_E}(a) = \frac{1}{[K : \mathfrak{R}]} \sum_{v \in U_E} n_v \log \max\{1, |a|_v\},$$

and similarly we define $h_{V_E}(a)$. Then $h_{U_E}(a)$ and $h_{V_E}(a)$ are both non-negative, and

$$h_{U_E}(a) + h_{V_E}(a) = h(a).$$

Now, if multiply the local bounds obtained from Theorem 2.4.8 and Corollary 2.4.14 by $n_v/[K : R]$ and add them all up, by Theorem 2.4.6 we obtain for every $P \in E(\overline{K})$

$$-\tfrac{1}{24}h(j) - \tfrac{1}{12}h_{U_E}(j) - \tfrac{1}{12}h_{U_E}(\Delta) \leq \hat{h}(P) - \tfrac{1}{2}h_x(P) \leq \tfrac{1}{12}h_{U_E}(j) + \tfrac{1}{12}h_{V_E}(\Delta^{-1}).$$

Recall that for a prime $v \in V_E$ the coefficients $a_4$ and $a_6$ are $v$-integral. This implies that also $v(\Delta) \geq 0$, giving $|\Delta|_v \leq 1$. Therefore $h_{V_E}(\Delta) = 0$, meaning that $h_{U_E}(\Delta) = h(\Delta)$. The desired result now follows by observing that $h_{U_E}(j) \leq h(j)$ and $h_{V_E}(\Delta^{-1}) \leq h(\Delta^{-1}) = h(\Delta)$. □

*Remark* 2.4.17. Note that for Theorem 2.4.16 we do not need the assumption we made in Remark 1.2.2 that we fix an element $T \in K$ such that $K/\mathbb{F}_q(T)$ is a finite extension. It is invariant under the choice of $T$.

Further, note that in the proof of Theorem 2.4.16 we actually prove the more precise result

$$-\tfrac{1}{24}h(j) - \tfrac{1}{12}h_{U_E}(j) - \tfrac{1}{12}h(\Delta) \leq \hat{h}(P) - \tfrac{1}{2}h_x(P) \leq \tfrac{1}{12}h_{U_E}(j) + \tfrac{1}{12}h_{V_E}(\Delta^{-1}).$$

The downside of these bounds is that the sets $U_E, V_E \in M_K$ depend on the coefficients of the elliptic curve $E$. We could consider a version of Theorem 2.4.16 where we assume that the coefficients of $E$ lie in the ring of integers $\mathcal{O}_K$. Then by Proposition 2.4.9 the set $U_E$ is a subset of the set $S$ of primes at infinity. In that case we can replace $h_{U_E}$ by the larger $h_S$, which is independent of the coefficients of $E$ and gives a more precise bound than using the full height function $h$. Replacing $h_{V_E}$ by $h$ then yields a better bound than the one given in the theorem that is also independent of the coefficients of $E$. Note, however, that this version of Theorem 2.4.16 would no longer be invariant under our choice of the transcendental element $T \in K$. ♢

*Remark* 2.4.18. We remark that [CR16, Example/Proof 5.2] and [Zim01, Theorem 4] both state bounds similar to Theorem 2.4.16 where the upper bound is equal to 0. In [CR16, Example/Proof 5.2] the coefficients of $E$ are assumed to lie in $\mathbb{F}_q[T]$, and [Zim01, Theorem 4] assumes that they are integers of $K$, but without giving a definition of the (ring of) integers of a global field. However, as shown in the example below, if the coefficients of $E$ lie in $\mathbb{F}_q[T]$, the difference $\hat{h} - \frac{1}{2}h_x$ can in fact be strictly positive. In case the coefficients are integral with respect to every prime of the function field $K$, then Theorem 2.4.16 yields an upper bound of 0. But, as we mentioned before, then the coefficients must be constants of $K$. Other bounds for the difference between $\hat{h}$ and $h_x$ can be found in [Zim76, §2]. ♢

**Example 2.4.19.** The calculations in this example were verified using MAGMA [BCP97] (version V2.26-12). Note that the definition of the canonical height used by MAGMA is twice our canonical height.

Let $K = \mathbb{F}_5(T)$ and consider the elliptic curve $E/K$ given by

$$E : y^2 = x^3 + 2Tx + T^2,$$

which contains the affine point $P = (1, T+1)$. Then $h_x(P) = 0$ and $\hat{h}(P) = 1/3$, so we obtain

$$\hat{h}(P) - \tfrac{1}{2} h_x(P) = \frac{1}{3} > 0.$$

◇

# Chapter 3

# Lower Bounds for Class Numbers of Number Fields

In this chapter we will derive lower bounds for class numbers of imaginary quadratic number fields, by making use of elliptic curve ideal class pairings. This method of deriving lower bounds for class numbers is due to Griffin and Ono, see [GO20]. In this chapter we mostly repeat the material from their paper. In the next chapter, we will show that we can extend this way of bounding class numbers to imaginary quadratic global function fields as well. This chapter will only be concerned with number fields, except for Section 3.2. The material in that section is given for general global fields such that we can reuse it in the next chapter.

## 3.1 Elliptic Curve Ideal Class Pairings

One of the major ingredients in the construction of Griffin and Ono are elliptic curve ideal class pairings, which essentially are maps sending pairs of points on elliptic curves to elements of the class group of an imaginary quadratic field. Such maps were first considered by Buell [Bue77], and later also by Bölling, Soleng, and Buell and Call [Bö80, Sol94, BC16]. In this section we will construct such pairings, using the connection between classes of quadratic forms and elements of the ideal class group of imaginary quadratic number fields as explained in Section 1.6. We mostly follow [GO20, §2].

We start by fixing some notation that we will use throughout this chapter. Let $-D \in \mathbb{Z}_{<0}$ be a negative fundamental discriminant. Then $-D$ is the discriminant of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$. We let $E/\mathbb{Q}$ be an elliptic curve given by a short Weierstrass equation

$$E : y^2 = x^3 + a_4x + a_6,$$

whith $a_4, a_6 \in \mathbb{Z}$. We write $\Delta$ and $j$ for the discriminant and $j$-invariant of $E$, respectively. When we consider a family of elliptic curves, we may also write $\Delta(E)$ and $j(E)$ to stress that they depend on $E$. We denote the rank of $E$ by $r$, and for the rest of this section we assume that $r \geq 1$. We write $E_{-D}$ for the quadratic twist[1]

$$E_{-D} : -D \cdot \left(\frac{y}{2}\right)^2 = x^3 + a_4x + a_6. \tag{3.1.1}$$

Now suppose that we have two affine points $P \in E(\mathbb{Q})$ and $Q \in E_{-D}(\mathbb{Q})$. Writing $y(Q)$ for the $y$-coordinate of $Q$, we assume that $y(Q) \neq 0$ and if $-D$ is odd then $v_2(y(Q)) > 0$, where $v_2$ denotes the 2-adic valuation on $\mathbb{Q}$. By Proposition 1.7.4 there exist integers $A, B, C \in \mathbb{Z}$ with $\gcd(A, C) = \gcd(B, C) = 1$ such that

$$P = \left(\frac{A}{C^2}, \frac{B}{C^3}\right).$$

For $Q$ we have the following lemma.

[1] Note that this definition is slightly different from the usual quadratic twist of $E$ by $-D$.

**Lemma 3.1.1.** *There exist unique integers $u, v, w \in \mathbb{Z}$ such that*

$$Q = \left(\frac{u}{w^2}, \frac{v}{w^3}\right),$$

*and* $\gcd(u, w^2)$ *and* $\gcd(v, w^3)$ *are both divisors of $D$.*

*Remark* 3.1.2. Note that in the above lemma, and also in the rest of this section, $v$ denotes an integer. For a prime $p$, we write $v_p$ with a subscript to denote the $p$-adic valuation on $\mathbb{Q}$. ♢

*Proof.* The proof is very similar to that of Proposition 1.7.4. We write $Q = (x, y)$, where $x = a/b$ and $y = c/d$ with $a, b, c, d \in \mathbb{Z}$ are written in lowest terms.

Suppose first that $D$ is even, such that $D/4 \in \mathbb{Z}$. Let $p$ be a prime number not dividing $D/4$. Then from (3.1.1) we see that $v_p(x) < 0$ if and only if $v_p(y) < 0$, and if this is the case then $3v_p(x) = 2v_p(y)$. Hence for such $p$ we have $3v_p(b) = 2v_p(d)$. Now let $p$ be a prime number dividing $D/4$. Note that, since $D$ is a fundamental discriminant, $v_p(D/4) = 1$. Equation (3.1.1) shows that $v_p(x) < 0$ if and only if $v_p(y) < 0$, and if this is the case then $3v_p(x) = 2v_p(y) + 1$. This implies that $3v_p(b) = 2v_p(d) - 1$, and therefore $3v_p(pb) = 2v_p(pd)$. Let $p_1, \dots, p_l$ be the primes dividing $D/4$ such that $v_{p_i}(x) < 0$, and write $s = p_1 \cdots p_l$. Then we find that $s$ is the unique integer dividing $D$ such that $sb$ is a square, say $sb = w^2$ with $w \in \mathbb{Z}$, and $sd = w^3$. Taking $u = sa$ and $v = sc$ yields the desired form for $Q$.

Now suppose that $D$ is odd. Recall that in that case we assumed that $v_2(y) > 0$, which by (3.1.1) also implies $v_2(x) \geq 0$. Let $p_1, \dots, p_l$ be the primes dividing $D$ such that $v_{p_i}(x) < 0$, and write $s = p_1 \cdots p_l$. Then, completely analogous to the case when $D$ is even but replacing $D/4$ with $D$, we find that $sb = w^2$ is a square and $sd = w^3$. Taking $u = sa$ and $v = sc$ yields the desired form for $Q$. □

*Remark* 3.1.3. In [GO20], the result of Lemma 3.1.1 is stated before the assumption that if $-D$ is odd then $v_2(y(Q)) > 0$, but this assumption is a necessary condition for the lemma. Indeed, consider the following example. We take the fundamental discriminant $-D = -167$, and the elliptic curve

$$E : y^2 = x^3 - x + 1$$

of rank $r = 1$. Then $E_{-D}(\mathbb{Q})$ contains the point

$$Q = \left(-\frac{7}{4}, \frac{1}{4}\right).$$

Now, if we find integers $v, w \in \mathbb{Z}$ such that $v/w^3 = 1/4$, we must have that $v$ and $w$ are both even, and therefore $\gcd(v, w^3)$ is even. Hence there exist no such integers $v, w$ satisfying $\gcd(v, w^3) \mid D$. ♢

Further, we define

$$\alpha := |Aw^2 - uC^2| \qquad \text{and} \qquad G := \gcd(\alpha, C^6v^2).$$

The next theorem gives an explicit description (up to the correspondence between quadratic forms and ideals) of the elliptic curve ideal class pairings that we will use in this thesis. It is exactly the same result as [GO20, Theorem 2.1], but with a minor correction to the proof, see Remark 3.1.6.

**Theorem 3.1.4** ([GO20, Theorem 2.1])**.** *Assuming the foregoing notation and hypotheses, there exist infinitely many integers $\ell$ such that*

$$F_{P,Q}(X, Y) := \frac{\alpha}{G} \cdot X^2 + \frac{2w^3B + \ell \cdot \frac{\alpha}{G}}{C^3v} \cdot XY + \frac{(2w^3B + \ell \cdot \frac{\alpha}{G})^2 + C^6v^2D}{4C^6v^2 \cdot \frac{\alpha}{G}} \cdot Y^2$$

*is a discriminant $-D$ positive definite integral binary quadratic form. Moreover, the choice of $\ell$ does not affect the* $\mathrm{SL}_2(\mathbb{Z})$*-equivalence class of $F_{P,Q}$, and if we have two pairs of points $(P_1, Q_1)$ and $(P_2, Q_2)$ for which $F_{P_1,Q_1}$ and $F_{P_2,Q_2}$ are* $\mathrm{SL}_2(\mathbb{Z})$*-equivalent, then $\frac{\alpha_1}{G_1} = \frac{\alpha_2}{G_2}$ or $\frac{\alpha_1\alpha_2}{G_1G_2} \geq D/4$.*

*Proof.* A simple calculation shows that $F_{P,Q}(X, Y)$ has discriminant $-D$. It is also positive definite since $-D < 0$ and $\frac{\alpha}{G} > 0$. Now we will show that there exist integers $\ell$ such that $F_{P,Q}(X, Y)$ is integral. We are looking for integers $\ell$ such that $2w^3B + \ell \cdot \frac{\alpha}{G}$ is divisible by $C^3v$ and $(2w^3B + \ell \cdot \frac{\alpha}{G})^2 + C^6v^2D$ is divisible by $4C^6v^2 \cdot \frac{\alpha}{G}$. Clearly, if some integer $\ell$ satisfies the latter condition it also satisfies the first.

We start by defining $f(x) := x^3 + a_4 x + a_6$. Then $f(\frac{A}{C^2}) = \frac{B^2}{C^6}$ and $f(\frac{u}{w^2}) = -D \cdot \frac{v^2}{4w^6}$. Note that

$$f\left(\frac{A}{C^2}\right) - f\left(\frac{u}{w^2}\right) = \left(\frac{A}{C^2} - \frac{u}{w^2}\right)\left(\frac{A^2}{C^4} + \frac{Au}{C^2w^2} + \frac{u^2}{w^4} + a_4\right),$$

and that $\alpha = \left|w^2C^2(\frac{A}{C^2} - \frac{u}{w^2})\right|$. Therefore $\alpha$ is a divisor of

$$w^6C^6\left(f\left(\frac{A}{C^2}\right) - f\left(\frac{u}{w^2}\right)\right) = w^6B^2 + C^6 \cdot \frac{Dv^2}{4}, \tag{3.1.2}$$

which in turn implies that $G$ divides $4w^6B^2$. We define $H := \gcd(2w^3B, C^3v)$. Then $H^2 = \gcd(4w^6B^2, C^6v^2)$, so $G \mid H^2$. Now $C^3v/H$ is an integer that divides $C^6v^2/H^2$. Since $G \mid H^2$ we find that $C^3v/H$ divides $C^6v^2/G$. Suppose that $p$ is a prime divisor of $C^3v/H$. Then $p \mid C^6v^2/G$, which implies that $p \not| \alpha/G$. Hence $\gcd(C^3v/H, \alpha/G) = 1$. We will now choose integers $k$ such that

$$\frac{\alpha}{G} \cdot k \equiv -\frac{2w^3B}{H} - \frac{C^3vD}{H} \pmod{\tfrac{2C^3v}{H}}. \tag{3.1.3}$$

To see that such integers $k$ exist, we distinguish two cases. In the case that $\frac{\alpha}{G}$ is odd it is coprime to $2C^3v/H$, so we can invert it modulo $2C^3v/H$ to find $k$. In the case that $\frac{\alpha}{G}$ is even we consider $\frac{\alpha}{2G}$, which is coprime with $C^3v/H$. Therefore, if $-w^3B/H - C^3vD/2H$ is an integer, there exist integers $k'$ such that

$$\frac{\alpha}{2G} \cdot k' \equiv -\frac{w^3B}{H} - \frac{C^3vD}{2H} \pmod{\tfrac{C^3v}{H}}. \tag{3.1.4}$$

Note that if $-w^3B/H - C^3vD/2H \notin \mathbb{Z}$, then we can still find integers $k'$ satisfying (3.1.4) since 2 is coprime to (and hence invertible modulo) $C^3v/H$. However, in that case such integers $k'$ do not necessarily satisfy (3.1.3) (see also Remark 3.1.5). On the other hand, if $-w^3B/H - C^3vD/2H \in \mathbb{Z}$, we note that for $k'$ satisfying (3.1.4) we have

$$\frac{\alpha}{2G} \cdot k' = -\frac{w^3B}{H} - \frac{C^3vD}{2H} + N \cdot \frac{C^3v}{H}$$

for some $N \in \mathbb{Z}$. Therefore we find that

$$\begin{aligned}\frac{\alpha}{G} \cdot k' &= -\frac{2w^3B}{H} - \frac{C^3vD}{H} + 2N \cdot \frac{C^3v}{H}\\ &\equiv -\frac{2w^3B}{H} - \frac{C^3vD}{H} \pmod{\tfrac{2C^3v}{H}}.\end{aligned}$$

So these integers $k'$ are the integers $k$ we were looking for. What is left to show, is that $-w^3B/H - C^3vD/2H \in \mathbb{Z}$ (in the case that $\frac{\alpha}{G}$ is even). First, suppose that $D$ is odd. Then, by assumption, $v$ is even. The fact that $\frac{\alpha}{G}$ is even implies that $v_2(\alpha) > v_2(C^6v^2)$, where $v_2(n)$ denotes the 2-adic valuation of an integer $n$. Since $\alpha$ divides (3.1.2) and $D$ is odd, this implies that $v_2(w^6B^2) = v_2(C^6v^2/4)$. Recall that $2w^3B/H$ and $C^3v/H$ are coprime. Suppose that $2w^3B/H$ is even. Then $v_2(2w^3B) > v_2(C^3v)$, which implies that $v_2(w^6B^2) > v_2(C^6v^2/4)$. This gives a contradiction, so we conclude that $2w^3B/H$ must be odd. Now suppose that $C^3v/H$ is even. Then $v_2(C^3v) > v_2(2w^3B)$, which implies that $v_2(C^6v^2/4) > v_2(w^6B^2)$. Again we obtain a contradiction, so we conclude that $2w^3B/H$ and $C^3v/H$ are both odd. Since $D$ is also odd, this implies that the expression $2w^3B/H + C^3vD/H$ is even. Hence $-w^3B/H - C^3vD/2H$ is indeed an integer in the case that $D$ is odd. Now, in the case that $D$ is even we have $C^3vD/2H \in \mathbb{Z}$. Therefore we have to show that in this case $w^3B/H \in \mathbb{Z}$. It is sufficient to show that $v_2(2w^3B) > v_2(C^3v)$. Since $\frac{\alpha}{G}$ is even, we know that $v_2(\alpha) > v_2(C^6v^2)$. Since $\alpha$ divides (3.1.2) we know that $v_2(w^6B^2 + C^6v^2D/4) \geq v_2(\alpha)$. Therefore we know that either $v_2(w^6B^2) = v_2(C^6v^2D/4)$, or both $v_2(w^6B^2) \geq v_2(\alpha)$ and $v_2(C^6v^2D/4) \geq v_2(\alpha)$. Hence, since $D \equiv 0 \pmod 4$ and $v_2(\alpha) > v_2(C^6v^2)$, we obtain $v_2(w^6B^2) \geq v_2(C^6v^2)$. This shows that indeed $v_2(2w^3B) > v_2(C^3v)$. This completes the proof that $-w^3B/H - C^3vD/2H$ is always an integer.

We now define $\ell' := Hk$ for each such integer $k$. Then we have

$$\frac{\alpha}{G} \cdot \ell' \equiv -2w^3B - C^3vD \pmod{2C^3v}. \tag{3.1.5}$$

Recall that we want to show that there exist integers $\ell$ such that $(2w^3B + \ell \cdot \frac{\alpha}{G})^2 + C^6v^2D$ is divisible by $4C^6v^2 \cdot \frac{\alpha}{G}$. From (3.1.5) it follows that

$$\left(2w^3B + \ell' \cdot \frac{\alpha}{G}\right)^2 + C^6v^2D \equiv C^6v^2(D^2 + D) \pmod{4C^6v^2}.$$

Since $-D$ is a fundamental discriminant, we know that $D$ is equivalent to 0 or 3 modulo 4. Therefore $D^2 + D \equiv 0 \pmod 4$, which shows that $(2w^3B + \ell' \cdot \frac{\alpha}{G})^2 + C^6v^2D$ is divisible by $4C^6v^2$. We will now show that we can choose $\ell'$ such that it is also divisible by $4\alpha$, because then it is divisible by $16C^6v^2\alpha/\gcd(4\alpha, 4C^6v^2) = 4C^6v^2 \cdot \frac{\alpha}{G}$. Using that $\alpha$ divides (3.1.2), we find that

$$\left(2w^3B + \ell' \cdot \frac{\alpha}{G}\right)^2 + C^6v^2D \equiv \ell'^2 \cdot \frac{\alpha^2}{G^2} + 4w^3B\ell' \cdot \frac{\alpha}{G} \pmod{4\alpha}.$$

Since $(2w^3B + \ell' \cdot \frac{\alpha}{G})^2 + C^6v^2D$ is divisible by $4C^6v^2$, it is also divisible by $4G$. We also know that $4G \mid 4\alpha$, hence we obtain that $4G$ divides $\ell'^2 \cdot \frac{\alpha^2}{G^2} + 4w^3B\ell' \cdot \frac{\alpha}{G}$. We define the integer

$$I := \frac{\ell'^2 \cdot \frac{\alpha^2}{G^2} + 4w^3B\ell' \cdot \frac{\alpha}{G}}{4G}.$$

Now we want to choose $\ell'$ such that $\frac{\alpha}{G} \mid I$. To see that this is possible, note that we can choose $\ell'$ such that it is divisible by $\frac{\alpha}{G}$ as many times as we like. Indeed, recall that $\ell' = Hk$. If $\frac{\alpha}{G}$ is odd, it is coprime with $2C^3v/H$. Then by the Chinese remainder theorem, for any $n \geq 0$ there are integers $k$ that satisfy (3.1.3) and further satisfy $k \equiv 0 \pmod{\frac{\alpha^n}{G^n}}$. Similarly, if $\frac{\alpha}{G}$ is even, then $\frac{\alpha}{G}$ is coprime to $C^3v/H$. Then, again by the Chinese remainder theorem, for any $n \geq 0$ there are integers $k'$ that satisfy (3.1.4) and further satisfy $k' \equiv 0 \pmod{\frac{\alpha^n}{G^n}}$. We conclude that in both cases, for every $n \geq 0$ there exist integers $k$ satisfying (3.1.3) and $k \equiv 0 \pmod{\frac{\alpha^n}{G^n}}$. Since we defined $\ell' = Hk$, for every $n \geq 0$ there exist such integers $\ell'$ that satisfy $\ell' \equiv 0 \pmod{\frac{\alpha^n}{G^n}}$. If we take $n$ large enough, we obtain such integers $\ell'$ such that $\frac{\alpha}{G} \mid I$. We will denote such integers by $\ell$. Then, taking $\ell' = \ell$, it follows that $4GI$ is divisible by $4\alpha$, and therefore $(2w^3B + \ell \cdot \frac{\alpha}{G})^2 + C^6v^2D$ is divisible by $4\alpha$. We conclude that for these $\ell$ the expression $(2w^3B + \ell \cdot \frac{\alpha}{G})^2 + C^6v^2D$ is divisible by $4C^6v^2 \cdot \frac{\alpha}{G}$, so $F_{P,Q}(X,Y)$ is integral.

We will now show that the choice of $\ell$ does not affect the $\mathrm{SL}_2(\mathbb{Z})$-equivalence class of $F_{P,Q}$. Note that we have

$$F_{P,Q}(X,Y) = \frac{G}{\alpha}\left[\left(\frac{\alpha}{G}X + \frac{2w^3B + \ell \cdot \frac{\alpha}{G}}{2C^3v}Y\right)^2 + \frac{D}{4}Y^2\right]. \tag{3.1.6}$$

Suppose that $\ell_1 = Hk_1$ and $\ell_2 = Hk_2$ are two possible choices for $\ell$ such that $F_{P,Q}$ is integral. To distinguish between the two quadratic forms for $\ell_1$ and $\ell_2$ we write $F_{P,Q,\ell_i}$ for $i \in \{1,2\}$. From (3.1.3) we know that there is an $n \in \mathbb{Z}$ such that

$$\frac{\alpha}{G} \cdot k_2 = \frac{\alpha}{G} \cdot k_1 + n \cdot \frac{2C^3v}{H},$$

which implies

$$\frac{\alpha}{G} \cdot \ell_2 = \frac{\alpha}{G} \cdot \ell_1 + n \cdot 2C^3v.$$

Then by (3.1.6) we find that $F_{P,Q,\ell_2}(X,Y) = F_{P,Q,\ell_1}(X + nY, Y)$. This shows that the two quadratic forms are $\mathrm{SL}_2(\mathbb{Z})$-equivalent, with $F_{P,Q,\ell_2} = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) F_{P,Q,\ell_1}$.

Finally, suppose that $(P_1, Q_1)$ and $(P_2, Q_2)$ are two pairs of points for which $F_{P_1,Q_1}$ and $F_{P_2,Q_2}$ are $\mathrm{SL}_2(\mathbb{Z})$-equivalent. For $i \in \{1,2\}$ we write $A_i, B_i, C_i, u_i, v_i, w_i, \alpha_i, G_i$ and $\ell_i$ for the quantities corresponding to these two pairs of points. Then there is an element $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that $F_{P_2,Q_2}(X,Y) = F_{P_1,Q_1}(aX + bY, cX + dY)$. By (3.1.6), the coefficient of $X^2$ in $\mathbb{F}_{P_2,Q_2}$ satisfies

$$\frac{\alpha_2}{G_2} = \frac{G_1}{\alpha_1}\left[\left(\frac{\alpha_1}{G_1}a + \frac{2w_1^3B_1 + \ell_1 \cdot \frac{\alpha_1}{G_1}}{2C_1^3v_1}c\right)^2 + \frac{D}{4}c^2\right].$$

Now, if $c = 0$, then $\frac{\alpha_2}{G_2} = \frac{\alpha_1}{G_1}a^2$. Since $ad - bc = 1$, the fact that $c = 0$ implies that $a = \pm 1$, so $a^2 = 1$ and $\frac{\alpha_1}{G_1} = \frac{\alpha_2}{G_2}$. If $c \neq 0$, then both terms inside the square brackets are non-negative and their sum is at least $D/4$, whence $\frac{\alpha_1\alpha_2}{G_1G_2} \geq D/4$.

□

*Remark* 3.1.5. In the proof above where we show that there exist integers $k$ satisfying (3.1.3) in the case that $\frac{\alpha}{G}$ is even, it is not enough to just find integers $k'$ satisfying (3.1.4). Namely, if $k'$ satisfies (3.1.4) but $-w^3B/H - C^3vD/2H$ is not an integer, then it does not necessarily satisfy (3.1.3). Consider the following simple example: If $a$ and $b$ are integers and $a \equiv b \pmod 5$, then $2a \equiv 2b \pmod{10}$. However, if $b$ is a half-integer this does not work, even though 2 is invertible modulo 5. For example:

$$4 \equiv \frac{3}{2} \pmod 5 \quad \text{but} \quad 8 \not\equiv 3 \pmod{10}.$$

Therefore it is indeed necessary to show that $-w^3B/H - C^3vD/2H \in \mathbb{Z}$. ♢

*Remark* 3.1.6. In the proof of [GO20, Theorem 2.1], the authors choose integers $k$ satisfying (3.1.3), just as we did. Next, for such integers $k$ they take $\ell$ as any integer satisfying $\ell \equiv Hk \pmod{2C^3v}$ (or even $(\bmod\ C^3v)$, depending on $k$), and claim that these integers $\ell$ satisfy the desired result. However, this is not necessarily true, which is why in our proof we distinguish between $\ell'$ and $\ell$. To see that this is necessary, consider the following example. Note that the condition $\ell \equiv Hk \pmod{2C^3v}$ automatically implies that $\ell \equiv Hk \pmod{C^3v}$. The calculations in this example were verified using SageMath [The22].

We take the fundamental discriminant $-D = -119$, and the elliptic curve

$$E : y^2 = x^3 - x + 1$$

of rank $r = 1$. Let $P' = (1, 1) \in E(\mathbb{Q})$, and let $P = 16P'$. Further, we take $Q = (-5, 2) \in E_{-D}(\mathbb{Q})$, such that $u = -5$, $v = 2$ and $w = 1$. These choices also fix the values of $A, B, C, \alpha, G$ and $H$. Now, we let

$$k = 45161597 \qquad \text{and} \qquad \ell = 90323194.$$

Then, one can check that $k$ satisfies (3.1.3) and $\ell \equiv Hk \pmod{2C^3v}$. However, we obtain

$$\frac{(2w^3B + \ell \cdot \frac{\alpha}{G})^2 + C^6v^2D}{4C^6v^2 \cdot \frac{\alpha}{G}} = \frac{13329}{2} \notin \mathbb{Z}.$$

♢

From Section 1.6 we know that the (equivalence class of the) quadratic form $F_{P,Q}$ described in Theorem 3.1.4 corresponds to a class of ideals in the ideal class group of the field $K = \mathbb{Q}(\sqrt{-D})$. Let us denote this element in the class group by $\xi_{P,Q}$.

**Definition 3.1.7.** Assume the same notation and hypotheses as in Theorem 3.1.4. Then we define the *elliptic curve ideal class pairing* corresponding to the elliptic curve $E$ and the discriminant $-D$ as

$$\Psi_{-D} : E(\mathbb{Q}) \times E_{-D}(\mathbb{Q}) \to \mathrm{CL}(K), \qquad (P, Q) \mapsto \xi_{P,Q}.$$

## 3.2 Counting Points on Elliptic Curves

In this section we will give a lower bound for the number of rational points on an elliptic curve with bounded canonical height. We will use this result in the next section to construct pairs of points that map to inequivalent quadratic forms via the pairing $\Psi_{-D}$ described in Theorem 3.1.4 and Definition 3.1.7. This will give us a lower bound on the class number of $K = \mathbb{Q}(\sqrt{-D})$. We will need the results in this section also for the next chapter, so we will prove them at once for number fields as well as function fields. Specifically, we let $\mathfrak{R} \in \{\mathbb{Q}, \mathbb{F}_q(T)\}$ denote a rational global field. For $\mathfrak{R} = \mathbb{Q}$, the material in this section is roughly the same as in [GO20, §3].

Recall from Definition 2.2.3 that we defined the logarithmic height $h_x(P)$ of a point $P \in E(\mathfrak{R})$ as $h_x(P) = h(x(P))$. Further, recall from Section 2.3 that

$$E(\mathfrak{R})/E(\mathfrak{R})_{\text{tors}} \cong \mathbb{Z}^r,$$

and that the Néron-Tate pairing $\langle \cdot, \cdot \rangle : E(\overline{\mathfrak{R}}) \times E(\overline{\mathfrak{R}}) \to \mathbb{R}$ defined by

$$\langle P, Q \rangle = \tfrac{1}{2}(\hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q))$$

defines an inner product on $E(\mathfrak{R})/E(\mathfrak{R})_{\text{tors}} \otimes_{\mathbb{Z}} \mathbb{R}$. This then becomes a real inner product space of dimension $r$, and therefore isomorphic to $\mathbb{R}^r$ equipped with the standard inner product. This isomorphism is easy to construct. Indeed, using the Gram-Schmidt procedure we can construct an orthonormal basis $\{\beta_1, \dots, \beta_r\}$ of $E(\mathfrak{R})/E(\mathfrak{R})_{\text{tors}} \otimes_{\mathbb{Z}} \mathbb{R}$. We write $\{e_1, \dots, e_r\}$ for the canonical basis of $\mathbb{R}^r$. Then the map $\varphi : E(\mathfrak{R})/E(\mathfrak{R})_{\text{tors}} \otimes_{\mathbb{Z}} \mathbb{R} \to \mathbb{R}^r$ sending $\beta_i$ to $e_i$ is an isomorphism of inner product spaces.

Let $\mathcal{B} = \{P_1, \dots, P_r\}$ be a set of linearly independent points in the lattice

$$\Lambda = E(\mathfrak{R})/E(\mathfrak{R})_{\text{tors}}$$

contained in $E(\mathfrak{R})/E(\mathfrak{R})_{\text{tors}} \otimes_{\mathbb{Z}} \mathbb{R}$. Then the points in $\mathcal{B}$ generate a sublattice $\Lambda_{\mathcal{B}} \subset \Lambda$. In this chapter we will mostly be interested in the case that $\mathcal{B}$ is a basis of $E(\mathfrak{R})/E(\mathfrak{R})_{\text{tors}}$, in which case $\Lambda_{\mathcal{B}} = \Lambda$. We put $v_i = \varphi(P_i) \in \mathbb{R}^r$. Note that for $1 \leq i, j \leq r$ we have $v_i \cdot v_j = \langle P_i, P_j \rangle$. Then the lattice $\Lambda_{\mathcal{B}}$ is isomorphic to the lattice $\varphi(\Lambda_{\mathcal{B}}) \subset \mathbb{R}^r$ spanned by the vectors $v_i$, and the canonical height of a point $P \in \Lambda_{\mathcal{B}}$ corresponding to a vector $v \in \varphi(\Lambda_{\mathcal{B}})$ is equal to $|v|^2$. Therefore, the points in $\Lambda_{\mathcal{B}}$ with canonical height at most $\tau$ correspond to points in $\varphi(\Lambda_{\mathcal{B}}) \cap B(\tau^{\frac{1}{2}})$, where $B(R)$ is the closed ball in $\mathbb{R}^r$ of radius $R$ centered at the origin.

**Definition 3.2.1.** Let $\mathcal{B} = \{P_1, \dots, P_r\} \subset \Lambda$ be a set of linearly independent points. The *diameter of* $\mathcal{B}$ is defined as

$$d(\mathcal{B}) = \max_{\delta_i \in \{\pm 1, 0\}} \hat{h}\left(\sum_{i=1}^{r} \delta_i P_i\right).$$

Writing $\mathscr{B}$ for the set of all bases for $\Lambda$, we further define the *diameter of the elliptic curve* $E$ as

$$d(E) = \min_{\mathcal{B} \in \mathscr{B}} d(\mathcal{B}).$$

For a set $\mathcal{B} = \{P_1, \dots, P_r\}$ of linearly independent points in $\Lambda$ corresponding to vecors $v_1, \dots, v_r \in \mathbb{R}^r$, the diameter $d(\mathcal{B})$ is equal to the squared length of the longest diagonal of the parallelepiped spanned by the vectors $v_i$.

*Remark* 3.2.2. Note that in the definition of $d(E)$ the minimum $\min_{\mathcal{B} \in \mathscr{B}} d(\mathcal{B})$ does indeed exist. Namely, if $\mathcal{B} \in \mathscr{B}$ is a basis for $\Lambda$, then the parallelepiped spanned by the corresponding vectors $v_i$ is contained in the ball $B(d(\mathcal{B})) \subset \mathbb{R}$. Any parallelepiped corresponding to another basis $\mathcal{B}'$ such that $d(\mathcal{B}') < d(\mathcal{B})$ must be contained in $B(d(\mathcal{B}))$. This ball contains only finitely many lattice points in $\varphi(\Lambda)$, implying that there are only finitely many parallelepipeds with vertices in $\varphi(\Lambda)$ contained in $B(d(\mathcal{B}))$. Hence the minimum diameter for bases of $\Lambda$ exists. ♢

*Remark* 3.2.3. In [GO20, Eq. (3.3)] and [GOT21, Eq. (2.3)] the authors add another factor 2 in the definition of the diameter, and (wrongly) state that $d(\mathcal{B})$ is equal to the squared length of the longest diagonal of the parallelepiped spanned by the vectors $v_i$. ♢

Note that the diameter of a basis $\mathcal{B}$ for a sublattice $\Lambda_{\mathcal{B}} \subset \Lambda$ does depend on the choice of the basis. For example, if $\mathcal{B}_0 = \{P_1, P_2\}$ is a basis for $\Lambda_{\mathcal{B}}$ corresponding to vectors $\{v_1, v_2\}$, then $\mathcal{B}_n = \{P_1, nP_1 + P_2\}$ is also a basis for $\Lambda_{\mathcal{B}}$ for all $n > 0$. If we let $n$ tend to infinity, the length of the longest diagonal of the parallelogram spanned by $v_1$ and $nv_1 + v_2$ will also approach infinity, and therefore $d(\mathcal{B}_n)$ does so too.

On the other hand, the volume of the parallelepiped spanned by the vectors $v_i$ is invariant under the choice of $\mathcal{B}$, since a basis transformation on $\Lambda_{\mathcal{B}}$ has determinant $\pm 1$. In fact, when $\Lambda_{\mathcal{B}} = \Lambda$ it is closely related to an important invariant of $E/\mathfrak{R}$, called the *regulator of* $E/\mathfrak{R}$. Indeed, for a basis $\mathcal{B} = \{P_1, \dots, P_r\}$ of $\Lambda$ the regulator is defined as

$$R_{\mathfrak{R}}(E) = |\det(\langle P_i, P_j \rangle)_{1 \leq i,j \leq r}|.$$

If we write $V$ for the $r \times r$ matrix whose columns are the vectors $v_i$, then

$$\det(V) = \sqrt{\det(VV^t)} = \sqrt{\det(v_i \cdot v_j)_{1 \leq i,j \leq r}} = \sqrt{R_{\mathfrak{R}}(E)}. \tag{3.2.1}$$

For a general set $\mathcal{B} = \{P_1, \dots, P_r\} \subset \Lambda$ of linearly independent points, we define the $\mathcal{B}$*-regulator of* $E/\mathfrak{R}$ as

$$R_{\mathfrak{R}}(E, \mathcal{B}) = |\det(\langle P_i, P_j \rangle)_{1 \leq i,j \leq r}|.$$

In this case (3.2.1) still holds true if we replace $R_{\mathfrak{R}}(E)$ by $R_{\mathfrak{R}}(E, \mathcal{B})$. In particular, this implies that if $\mathcal{B}_1$ and $\mathcal{B}_2$ generate the same sublattice $\Lambda_{\mathcal{B}} \subset \Lambda$, then $R_{\mathfrak{R}}(E, \mathcal{B}_1) = R_{\mathfrak{R}}(E, \mathcal{B}_2)$. Please note that the above definition of the $\mathcal{B}$-regulator of $E/\mathfrak{R}$ is non-standard and invented by the author.

Writing $\Omega_r$ for the volume of the unit ball in $\mathbb{R}^r$, we define the constant

$$c(E, \mathcal{B}) = \frac{|E(\mathfrak{R})_{\text{tors}}| \cdot \Omega_r}{\sqrt{R_{\mathfrak{R}}(E, \mathcal{B})}}.$$

If we know that $\mathcal{B}$ forms a basis for $\Lambda$, then $R_{\mathfrak{R}}(E, \mathcal{B}) = R_{\mathfrak{R}}(E)$ is independent of the specific basis $\mathcal{B}$, and we may simply write $c(E)$ for the constant defined above.

**Definition 3.2.4.** For two functions $f, g : \mathbb{R} \to \mathbb{R}$, we say that $f$ and $g$ are *asymptotic* to each other, denoted $f \sim g$, if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

Asymptotically, as a function of $\tau \in \mathbb{R}_{\geq 0}$, the number of $\mathfrak{R}$-rational points on an elliptic curve over $\mathfrak{R}$ with canonical height at most $\tau$ is well known. We have

$$\#\{P \in E(\mathfrak{R}) : \hat{h}(P) \leq \tau\} \sim c(E)\tau^{\frac{r}{2}}.$$

See for example [Kna92, Prop. 4.18] for the case $\mathfrak{R} = \mathbb{Q}$, where using our results from Section 2.3 the proof also works if $\mathfrak{R} = \mathbb{F}_q(T)$. The next proposition gives an explicit lower bound in terms of $\tau$.

**Proposition 3.2.5.** *Let $\mathcal{B}$ be a set of $r$ linearly independent points in $\Lambda = E(\mathfrak{R})/E(\mathfrak{R})_{\text{tors}}$ with diameter $d = d(\mathcal{B})$. Then for $\tau \geq d$ we have*

$$\#\{P \in E(\mathfrak{R}) : \hat{h}(P) \leq \tau\} \geq c(E, \mathcal{B}) \left(\tau^{\frac{r}{2}} - r\sqrt{d}\tau^{\frac{r-1}{2}}\right).$$

*We may replace $d$ by $d(E)$ to obtain a statement independent of the set $\mathcal{B}$.*

*Proof.* As we noted before, the points in $\Lambda$ with canonical height at most $\tau$ correspond to points in $\varphi(\Lambda) \cap B(\tau^{\frac{1}{2}})$, where $B(R)$ is the closed ball in $\mathbb{R}^r$ of radius $R$ centered at the origin. Therefore, the points in $\Lambda_{\mathcal{B}} \subset \Lambda$ with canonical height at most $\tau$ correspond to points in $\varphi(\Lambda_{\mathcal{B}}) \cap B(\tau^{\frac{1}{2}})$. For every point $\lambda \in \varphi(\Lambda_{\mathcal{B}})$, we write $\mathcal{P}_\lambda$ for the half-open parallelepiped

$$\mathcal{P}_\lambda = \left\{ \lambda + \sum_{i=1}^{r} x_i v_i : x_i \in [0, 1) \right\},$$

where the vectors $v_i$ correspond to the points in $\mathcal{B}$ as described above. Note that the set $\{\mathcal{P}_\lambda : \lambda \in \varphi(\Lambda_{\mathcal{B}})\}$ forms a partition of $\mathbb{R}^r$. Further, note that the length of the longest diagonal of $\mathcal{P}_\lambda$ is $\sqrt{d}$, and by (3.2.1) its volume is equal to $\sqrt{R_{\mathfrak{R}}(E, \mathcal{B})}$. Therefore, if $\mathcal{P}_\lambda$ intersects with $B(\tau^{\frac{1}{2}} - d^{\frac{1}{2}})$ then $\lambda \in B(\tau^{\frac{1}{2}})$. The ball $B(\tau^{\frac{1}{2}} - d^{\frac{1}{2}})$ intersects with at least $\operatorname{Vol}(B(\tau^{\frac{1}{2}} - d^{\frac{1}{2}}))/\sqrt{R_{\mathfrak{R}}(E)}$ parallelepipeds $\mathcal{P}_\lambda$ for different $\lambda$. Using that $\operatorname{Vol}(B(\tau^{\frac{1}{2}} - d^{\frac{1}{2}})) = \Omega_r \cdot (\tau^{\frac{1}{2}} - d^{\frac{1}{2}})^r$, we obtain

$$\#\left(\varphi(\Lambda_{\mathcal{B}}) \cap B(\tau^{\frac{1}{2}})\right) \geq \frac{\Omega_r}{\sqrt{R_{\mathfrak{R}}(E, \mathcal{B})}} \cdot \left(\tau^{\frac{1}{2}} - d^{\frac{1}{2}}\right)^r. \tag{3.2.2}$$

Now, using induction on $r$, we will show that for all $r \geq 1$ we have

$$\left(\tau^{\frac{1}{2}} - d^{\frac{1}{2}}\right)^r \geq \left(\tau^{\frac{r}{2}} - r\sqrt{d}\tau^{\frac{r-1}{2}}\right). \tag{3.2.3}$$

For $r = 1$, the statement is obvious. Now, let (IH) be the induction hypothesis that (3.2.3) holds for some $r \geq 1$. Then

$$\begin{aligned} \left(\tau^{\frac{1}{2}} - d^{\frac{1}{2}}\right)^{r+1} &\geq \left(\tau^{\frac{1}{2}} - d^{\frac{1}{2}}\right)\left(\tau^{\frac{r}{2}} - r\sqrt{d}\tau^{\frac{r-1}{2}}\right) && \text{by (IH)} \\ &= \tau^{\frac{r+1}{2}} - (r+1)\sqrt{d}\tau^{\frac{r}{2}} + rd\tau^{\frac{r-1}{2}} \\ &\geq \tau^{\frac{r+1}{2}} - (r+1)\sqrt{d}\tau^{\frac{r}{2}}, \end{aligned}$$

which completes our proof by induction. The desired result now follows by plugging (3.2.3) into (3.2.2), and by noting that torsion points have canonical height 0, so

$$\#\{P \in E(\mathfrak{R}) : \hat{h}(P) \leq \tau\} = \#\left(\varphi(\Lambda) \cap B(\tau^{\frac{1}{2}})\right) \cdot |E(\mathfrak{R})_{\text{tors}}| \geq \#\left(\varphi(\Lambda_{\mathcal{B}}) \cap B(\tau^{\frac{1}{2}})\right) \cdot |E(\mathfrak{R})_{\text{tors}}|.$$

□

*Remark* 3.2.6. We can optimise the bound in Proposition 3.2.5 by replacing $d$ with $d(E)$ and $c(E, \mathcal{B})$ with $c(E)$, which also makes the statement independent of the set $\mathcal{B}$. However, for computational purposes the version stated is often easier to work with. ♢

*Remark* 3.2.7. Proposition 3.2.5 is almost identical to [GO20, Prop. 3.2], except that there the authors assume that $\tau > d/4$. We chose to assume $\tau \geq d$ instead, since the obtained lower bound becomes negative when $\tau < d$. ♢

## 3.3 Lower Bounds for Class Numbers

Recall that in this chapter we let $-D \in \mathbb{Z}_{<0}$ be te discriminant of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$. We will denote the class number of $K$ by $h_K$. Please note that in this thesis $h_K$ will always denote the class number of the field $K$, and not the logarithmic height relative to $K$. We will denote by $h, h_x$ and $\hat{h}$ the height functions defined in the previous chapter. Since the field $K$ is determined by the discriminant $-D$, we will write the class number $h_K(-D)$ as a function of the discriminant. In this section we will derive a lower bound for $h_K(-D)$ in terms of the discriminant $-D$, and we will compare the bound we obtain to the literature in the next section. We follow [GO20, §4].

Recall that we consider an elliptic curve $E/\mathbb{Q}$ given by a short Weierstrass equation

$$E : y^2 = x^3 + a_4x + a_6, \qquad a_4, a_6 \in \mathbb{Z}.$$

The elliptic curve ideal class pairing $\Psi_{-D}$ from Section 3.1 allows us to construct elements of the ideal class group of $K$ from pairs of points on $E$ and $E_{-D}$. We will now restrict our attention to a specific family of fundamental discriminants, depending on the elliptic curve $E$ we are considering. Namely, we consider the discriminants of the form

$$-D_E(t) = -4(t^3 + a_4t - a_6) \qquad \text{with } t \in \mathbb{Z}_{>0}. \tag{3.3.1}$$

*Remark* 3.3.1. Note that $-D_E(t)$ is not a fundamental discriminant for all $t \in \mathbb{Z}_{>0}$. We just consider discriminants that happen to be of this form for some positive integer $t$. Note that $-D_E(t)$ is a fundamental discriminant if and only if $t^3 + a_4t - a_6$ is square-free and not equivalent to 3 (mod 4). Erdös proved in [Erd53, Theorem 1.1] that $t^3 + a_4t - a_6$ is square-free for infinitely many $t \in \mathbb{Z}_{>0}$. If we want to be absolutely sure that there exist fundamental discriminants of the form (3.3.1), we could further assume that if $a_4$ is odd then $a_6$ is even and if $a_4$ is even then $a_6 \equiv 3 \pmod 4$, such that $t^3 + a_4t - a_6 \not\equiv 1 \pmod 4$ for all $t \in \mathbb{Z}_{>0}$. ♢

For these discriminants $-D_E(t)$, the curve $E_{-D_E(t)}$ always contains the rational point $Q_t = (-t, 1)$. Writing $j$ and $\Delta$ for the $j$-invariant and discriminant of $E$, respectively, we define

$$\delta(E) = \tfrac{1}{8}h(j) + \tfrac{1}{12}h(\Delta) + \tfrac{5}{3}, \tag{3.3.2}$$

and we put

$$\tau_E(t) = \tfrac{1}{4}\log\left(\frac{D_E(t)}{(t+1)^2}\right) - \delta(E). \tag{3.3.3}$$

Now, we will show that for different points $P_1, P_2 \in E(\mathbb{Q})$ with $P_1 \neq -P_2$ and satisfying $\hat{h}(P_i) \leq \tau_E(t)$ for $i \in \{1, 2\}$, the quadratic forms $F_{P_i,Q_t}$ obtained from Theorem 3.1.4 are inequivalent. Since, by Theorem 1.6.3, inequivalent forms correspond to distinct elements of the class group $\mathrm{CL}(-D)$, this yields a lower bound for the class number $h_K(-D)$. We obtain the following result.

**Theorem 3.3.2.** *Let $\mathcal{B}$ be a set of $r$ linearly independent points in $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$ with diameter $d = d(\mathcal{B})$. Suppose that we have a positive integer $t \in \mathbb{Z}_{>0}$ such that $\tau_E(t) \geq d$ and $-D_E(t)$ is a negative fundamental discriminant satisfying $D_E(t) \leq t^2(t+1)^2$. Then*

$$h_K(-D_E(t)) \geq \frac{c(E,\mathcal{B})}{2}\left(\tau_E(t)^{\frac{r}{2}} - r\sqrt{d}\tau_E(t)^{\frac{r-1}{2}}\right).$$

*Proof.* By Proposition 3.2.5 we have

$$\#\{P \in E(\mathbb{Q}) : \hat{h}(P) \leq \tau_E(t)\} \geq c(E,\mathcal{B})\left(\tau_E(t)^{\frac{r}{2}} - r\sqrt{d}\tau_E(t)^{\frac{r-1}{2}}\right). \tag{3.3.4}$$

We will now examine the inequivalence of the forms we obtain when pairing the rational points on $E$ with canonical height at most $\tau_E(t)$ with the point $Q_t$. Suppose we have two points $P_i = (A_i/C_i^2, B_i/C_i^3)$ for $i \in \{1, 2\}$ such that $\hat{h}(P_i) \leq \tau_E(t)$. We let $F_1 = F_{P_1,Q_t}$ and $F_2 = F_{P_2,Q_t}$. Since $Q_t = (-t, 1)$, we have $\alpha_i = |A_i + tC_i^2|$ and $G_i = \gcd(\alpha_i, C_i^6)$. Therefore the fact that $\gcd(A_i, C_i) = 1$ implies that $G_i = 1$, so

$\frac{\alpha_i}{G_i} = \alpha_i$. Using Theorem 2.4.7, which bounds the difference between $\hat{h}$ and $h_x$ on $E$, we find

$$\begin{aligned} h_x(P_i) &\leq 2\left(\hat{h}(P_i) + \tfrac{1}{8}h(j) + \tfrac{1}{12}h(\Delta) + 0.973\right) && \text{by Theorem 2.4.7} \\ &\leq 2\tau_E(t) + \tfrac{1}{4}h(j) + \tfrac{1}{6}h(\Delta) + 1.946 \\ &= \tfrac{1}{2}\log\left(\frac{D_E(t)}{(t+1)^2}\right) + 1.946 - \tfrac{10}{3} && \text{by (3.3.3) and (3.3.2)} \\ &\leq \tfrac{1}{2}\log\left(\frac{D_E(t)}{(t+1)^2}\right) - 2\log(2) \\ &= \tfrac{1}{2}\log\left(\frac{D_E(t)}{16(t+1)^2}\right). && (3.3.5) \end{aligned}$$

We now consider the height function $H(P) := \exp(h_x(P))$. This gives us the convenient notation $H(P_i) = \max\{|A_i|, |C_i^2|\}$. We have

$$\alpha_i = |A_i + tC_i^2| \leq (1+t)H(P_i).$$

Further, $H(P_i) = \exp(h_x(P_i))$ implies by (3.3.5) that

$$H(P_i) \leq \sqrt{D_E(t)}/(4(t+1)). \tag{3.3.6}$$

This shows that

$$\alpha_i \leq \frac{\sqrt{D_E(t)}}{4}.$$

Hence $\alpha_1\alpha_2 < D_E(t)/4$. If $\alpha_1 \neq \alpha_2$, then Theorem 3.1.4 implies that $F_1$ and $F_2$ are inequivalent. Now suppose $\alpha_1 = \alpha_2$. Our assumption that $D_E(t) \leq t^2(t+1)^2$ implies by (3.3.6) that $H(P_i) \leq t/4$. Therefore also $|A_i| \leq t/4$. Note that $C \neq 0$, so $C^2 \geq 1$. Therefore $tC_i^2 \geq t > 0$. This implies that $|A_i + tC_i^2| = A_i + tC_i^2$. From $\alpha_1 = \alpha_2$ we obtain

$$A_1 + tC_1^2 = A_2 + tC_2^2, \tag{3.3.7}$$

showing that $A_1 \equiv A_2 \pmod{t}$. Since $|A_i| \leq t/4$, this implies that $A_1 = A_2$. Then by (3.3.7) we get $C_1^2 = C_2^2$. Hence $P_1$ and $P_2$ have the same $x$-coordinate, which by the Weierstrass equation shows that $P_1 = \pm P_2$. Note that for any point $P \in E(\mathbb{Q})$ we have $\hat{h}(P) = \hat{h}(-P)$. So we have now shown that for two points $P_1$ and $P_2$ in the set $\{P \in E(\mathbb{Q}) : \hat{h}(P) \leq \tau_E(t)\}$, either $P_1 = \pm P_2$ or the quadratic forms $F_1$ and $F_2$ are inequivalent. We obtain

$$\begin{aligned} h_K(-D_E(t)) &\geq \frac{\#\{P \in E(\mathbb{Q}) : \hat{h}(P) \leq \tau_E(t)\}}{2} && \text{by Theorem 1.6.3} \\ &\geq \frac{c(E,\mathcal{B})}{2}\left(\tau_E(t)^{\frac{r}{2}} - r\sqrt{d}\tau_E(t)^{\frac{r-1}{2}}\right) && \text{by (3.3.4).} \end{aligned}$$

□

*Remark* 3.3.3. Note that since $D_E(t)$ is a cubic function of $t$, the condition $D_E(t) \leq t^2(t+1)^2$ is satisfied for all $t \geq t_1$, where $t_1 \in \mathbb{Z}_{>0}$ is effectively computable in terms of $a_4$ and $a_6$. Further, there exists an integer $t_2 \in \mathbb{Z}_{\geq 0}$, effectively computable in terms of $a_4, a_6, \delta(E)$ and $d$, such that the condition $\tau_E(t) \geq d$ is satisfied for all $t \geq t_2$. ♢

**Lemma 3.3.4.** *Let $-D_E(t)$ and $\tau_E(t)$ be the functions of $t \in \mathbb{Z}_{>0}$ defined in* (3.3.1) *and* (3.3.3), *respectively. Then we have*

$$\tau_E(t) \sim \frac{\log(D_E(t))}{12}.$$

*Proof.* We have $\tau_E(t) = \frac{1}{4}\log(D_E(t)) - \frac{1}{2}\log(t+1) - \delta(E)$. Now we put

$$\rho(t) = \frac{\tau_E(t)}{\frac{1}{12}\log(D_E(t))} = 3 - 6\cdot\frac{\log(t+1)}{\log(D_E(t))} - 12\delta(E)\cdot\frac{1}{\log(D_E(t))}.$$

Our goal is to show $\lim_{t\to\infty}\rho(t) = 1$. We have $\log(D_E(t)) = \log(4) + 3\log(\sqrt[3]{t^3 + a_4t - a_6})$, so

$$\lim_{t\to\infty} 3\cdot\frac{\log(t+1)}{\log(D_E(t))} = \lim_{t\to\infty}\frac{\log(t+1)}{\frac{1}{3}\log(4) + \log(\sqrt[3]{t^3 + a_4t - a_6})} = 1.$$

Hence

$$\lim_{t\to\infty} \rho(t) = 3 - 2 - 0 = 1.$$

□

For a given elliptic curve $E$, the next Theorem uses Theorem 3.3.2 to give a lower bound on the class number $h_K(-D_E(t))$ as a function of $-D_E(t)$. It is the main result in the paper [GO20] by Griffin and Ono. Such bounds have been extensively studied for over 200 years. In the next section we will compare our obtained result to the literature.

**Theorem 3.3.5** ([GO20, Theorem 1.2])**.** *Let $E/\mathbb{Q}$ be an elliptic curve of rank $r \geq 1$ given by*

$$E : y^2 = x^3 + a_4x + a_6, \qquad a_4, a_6 \in \mathbb{Z},$$

*and let $\mathcal{B}$ be a basis for $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$. Let $\varepsilon > 0$. Then there exists an effectively computable constant $N(E, \mathcal{B}, \varepsilon)$ such that, if $t \in \mathbb{Z}_{>0}$ is an integer such that $-D_E(t)$ is a negative fundamental discriminant and $t \geq N(E, \mathcal{B}, \varepsilon)$, then*

$$h_K(-D_E(t)) \geq \frac{c(E,\mathcal{B})}{2\sqrt{12^r}} (1-\varepsilon) \left(\log\left(D_E(t)\right)\right)^{\frac{r}{2}}.$$

*Proof.* We let $d = d(\mathcal{B})$. By Remark 3.3.3, Theorem 3.3.2 says that there is an effectively computable constant $t_0(E, \mathcal{B})$ such that, if $-D_E(t)$ is a negative fundamental discriminant and $t \geq t_0(E, \mathcal{B})$, then

$$h_K(-D_E(t)) \geq \frac{c(E,\mathcal{B})}{2} \left(\tau_E(t)^{\frac{r}{2}} - r\sqrt{d}\tau_E(t)^{\frac{r-1}{2}}\right). \tag{3.3.8}$$

From Lemma 3.3.4 we see that for any $\varepsilon' > 0$ there exists an effectively computable constant $n'(E, \varepsilon')$ such that for all $t \geq n'(E, \varepsilon')$ we have

$$\tau_E(t)(1-\varepsilon') \leq \frac{\log(D_E(t))}{12} \leq \tau_E(t)(1+\varepsilon'). \tag{3.3.9}$$

Now, we let $\varepsilon > 0$ as in the statement of the Theorem, and we take $\varepsilon' > 0$ such that $(1+\varepsilon')^{\frac{r}{2}} < (1-\varepsilon)^{-1}$. Then there exists an effectively computable constant $n(E, \varepsilon, \varepsilon')$ such that for all $t \geq n(E, \varepsilon, \varepsilon')$ we have

$$\frac{1 - r\sqrt{d}\tau_E(t)^{-\frac{1}{2}}}{1-\varepsilon} \geq (1+\varepsilon')^{\frac{r}{2}}.$$

Multiplying the numerator and denominator on the left-hand side by $\tau_E(t)^{\frac{r}{2}}$ and taking the resulting denominator to the right-hand side, we obtain

$$\tau_E(t)^{\frac{r}{2}} - r\sqrt{d}\tau_E(t)^{\frac{r-1}{2}} \geq (1-\varepsilon)\left((1+\varepsilon')\tau_E(t)\right)^{\frac{r}{2}}. \tag{3.3.10}$$

Now, we let $N(E, \mathcal{B}, \varepsilon) = \max\{t_0(E, \mathcal{B}), n'(E, \varepsilon), n(E, \varepsilon, \varepsilon')\}$, noting that an appropriate $\varepsilon'$ can be effectively computed from $\varepsilon$. Then, for $t \in \mathbb{Z}_{>0}$ such that $-D_E(t)$ is a negative fundamental discriminant and $t \geq N(E, \mathcal{B}, \varepsilon)$, we obtain

$$\begin{aligned} h_K(-D_E(t)) &\geq \frac{c(E,\mathcal{B})}{2} \left(\tau_E(t)^{\frac{r}{2}} - r\sqrt{d}\tau_E(t)^{\frac{r-1}{2}}\right) && \text{by (3.3.8),} \\ &\geq \frac{c(E,\mathcal{B})}{2} \left((1-\varepsilon)\left((1+\varepsilon')\tau_E(t)\right)^{\frac{r}{2}}\right) && \text{by (3.3.10),} \\ &\geq \frac{c(E,\mathcal{B})}{2\sqrt{12^r}} (1-\varepsilon) \log\left(D_E(t)\right)^{\frac{r}{2}} && \text{by (3.3.9).} \end{aligned}$$

□

## 3.4 Comparison with the Literature

In this section we compare the bound we obtained in Theorem 3.3.5 to the literature.

One year after Heilbronn proved Gauss's conjecture that $h_K(-D) \to \infty$ as $D \to \infty$, Siegel [Sie35] proved the following theorem.

**Theorem 3.4.1** (Siegel)**.** *For every $\varepsilon > 0$, there exist constants $c_1(\varepsilon), c_2(\varepsilon) > 0$ such that*

$$c_1(\varepsilon)D^{\frac{1}{2}-\varepsilon} \leq h_K(-D) \leq c_2(\varepsilon)D^{\frac{1}{2}+\varepsilon}.$$

The bound in Siegel's theorem is much stronger than the original conjecture by Gauss, but unfortunately the constants $c_1(\varepsilon)$ and $c_2(\varepsilon)$ are not effectively computable, which makes the bound impractical for computational purposes. Tatuzawa [Tat51] has shown that Siegel's theorem holds with effectively computable constants for all fundamental discriminants $-D < 0$, except for at most one exceptional discriminant $-D$. The state-of-the-art effective lower bound for $h(-D)$ in general is the following bound given by Oesterlé [Oes85]:

$$h_K(-D) > \frac{1}{7000}(\log D) \prod_{\substack{p \mid D \text{ prime} \\ p \neq D}} \left(1 - \frac{\lfloor 2\sqrt{p} \rfloor}{p+1}\right). \tag{3.4.1}$$

Note that the product on the right-hand side of (3.4.1) is smaller than 1 for all fundamental discriminants $-D$. Therefore, asymptotically, Oesterlé's bound grows at most as fast as $c \log D$ for some constant $c$. Hence we see that our bound from Theorem 3.3.5 gives a $(\log D)$-power improvement on (3.4.1) as soon as $r \geq 3$.

**Example 3.4.2.** Consider the curve

$$E : y^2 = x^3 - 52x + 100.$$

Then $|E(\mathbb{Q})_{\text{tors}}| = 1$, $r = 3$ and $R_{\mathbb{Q}}(E) \approx 0.2737$ (see [LMF22]). Using that $\Omega_3 = 4\pi/3$, we compute

$$\frac{c(E)}{2\sqrt{12^r}} \geq \frac{1}{11}.$$

Therefore, for sufficiently large discriminants of the form $-D_E(t) = -4(t^3 - 52t - 100)$ with $t \in \mathbb{Z}_{>0}$ we obtain

$$h_K(-D_E(t)) \geq \frac{1}{11} \left(\log\left(D_E(t)\right)\right)^{\frac{3}{2}},$$

which asymptotically improves on (3.4.1) by a factor $(\log(D_E(t)))^{\frac{1}{2}}$. ♢

However, note that any positive power of $D$ eventually grows faster than any power of $\log D$. Therefore, asymptotically our bounds are weaker than Siegel's ineffective bound.

*Remark* 3.4.3. For elliptic curves over $\mathbb{Q}$ it is an open problem whether the rank of an elliptic curve can be arbitrarily large. The largest example known to date is an elliptic curve constructed by Elkies with rank at least 28. So if we would have used that curve in the above example[2], we would obtain a class number bound that asymptotically improves on (3.4.1) by a factor $(\log(D_E(t)))^{13}$. In the paper [PPVW19], the authors present a probabilistic model providing heuristics for the rank of elliptic curves over $\mathbb{Q}$. These heuristics suggest that there are only finitely many elliptic curves over $\mathbb{Q}$ with rank larger than 21. In particular, this would imply that there is an absolute bound for the rank of elliptic curves over $\mathbb{Q}$. This would give a remarkable dissimilarity between number fields and global function fields, since for elliptic curves over $\mathbb{F}_q(T)$ it is in fact proven that there are curves of arbitrarily large rank. In Section 4.3 we will look at a construction by Ulmer [Ulm14] of curves over $\mathbb{F}_q(T)$ for which the rank becomes arbitrarily large. ♢

In Section 4.5 in the next chapter, we do the same as in this section but for global function fields instead of number fields. As we will see, the Hasse-Weil theorem (Theorem 1.3.5) plays an important role in bounding the class number of global function fields. Since the Hasse-Weil theorem is the function-field analogue of the Riemann hypothesis, it is interesting to examine what bounds for class numbers of number fields we can obtain assuming the generalised Riemann hypothesis. We have the following theorem.

**Theorem 3.4.4.** *Assuming the generalised Riemann hypothesis, there exists an effectively computable constant $c_0$ such that if $-D$ is a fundamental discriminant and $D > c_0$ then*

$$h_K(-D) > c_1 \frac{\sqrt{D}}{\log D},$$

*where $c_1 > 0$ is a fixed absolute constant.*

[2] We didn't, because the coefficients of this curve are very big.

*Proof.* See [Gol85, §3] and the references there for a proof of this theorem. □

Note that Theorem 3.4.4 gives a bound that is both effective and, for any given $\varepsilon > 0$, asymptotically stronger than the one given by Siegel.

# Chapter 4

# Lower Bounds for Class Numbers of Function Fields

In this chapter we derive a lower bound for the class number of certain families of imaginary quadratic function fields, using the same strategy as in the previous chapter. In the first two sections, we give the function-field analogue of Sections 3.1 and 3.3 of the previous chapter. Our proofs and results will be very similar to those in [GO20], but apart from that are original work by the author. As in the number field case, the bound we obtain depends on the rank of the elliptic curve we use. In Section 4.3 we give a construction due to Ulmer [Ulm14] of elliptic curves over constant extensions of $\mathbb{F}_q(T)$ for which the rank becomes arbitrarily large. In section 4.4 we take a closer look at the bound from Section 4.2 using this specific family of elliptic curves. Lastly, Section 4.5 gives an overview of the literature on lower bounds for class numbers of global function fields, which we also compare to our results from the previous sections. All fields considered in this chapter will be global function fields.

## 4.1 Class Pairings for Function Fields

In this section we generalise the results from Section 3.1 to function fields. As shown below in Theorem 4.1.3, we can generalize Theorem 3.1.4 to function fields, yielding what we will call form class pairings. However, since for function fields we found in Section 1.6 that inequivalent quadratic forms with fundamental discriminant $D \in \mathbb{F}_q[T]$ do not correspond one-to-one with elements of the ideal class group $\mathcal{I}_K$ of $K = \mathbb{F}_q(T)(\sqrt{D})$, we cannot define an ideal class pairing $\Psi_D$ as in Definition 3.1.7. Instead, in Definition 4.1.5 we will define form class pairings as maps of the form

$$\Phi_D : E(\mathbb{F}_q(T)) \times E_D(\mathbb{F}_q(T)) \to \mathcal{Q}_D.$$

From Section 1.6 we know that

$$\mathcal{Q}_D/(\mathbb{Z}/2\mathbb{Z}) \cong \mathcal{I}_K,$$

so we see that if we can construct $n$ inequivalent quadratic forms using $\Phi_D$, then $h_K^I = |\mathcal{I}_K| \geq n/2$.

Let us start by fixing some notation for the rest of this chapter.

We let $D \in \mathbb{F}_q[T]$ be a fundamental discriminant such that $D$ is the discriminant of an imaginary quadratic field $K = \mathbb{F}_q(T)(\sqrt{D})$. We call such a fundamental discriminant *imaginary*. Recall from Section 1.4 that this is equivalent to taking $D \in \mathbb{F}_q[T]$ square-free such that either $\deg(D)$ is odd, or $\deg(D)$ is even and the leading coefficient of $D$ is not a square in $\mathbb{F}_q^*$. Further, we let $E/\mathbb{F}_q(T)$ be an elliptic curve given by

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6, \qquad a_2, a_4, a_6 \in \mathbb{F}_q[T]$$

with rank $r \geq 1$, discriminant $\Delta$, and $j$-invariant $j$. Note that we take a slightly more general Weierstrass form for $E$ then the usual short Weierstrass form. We do this because in the Section 4.4 we want to use explicit curves that are of this form. Note that since we are working in characteristic unequal to 2 or 3, the curve $E$ is isomorphic to a curve given by a short Weierstrass equation. We let $E_D$ be the quadratic twist of $E$ by $D$:

$$E_D : Dy^2 = x^3 + a_2x^2 + a_4x + a_6. \tag{4.1.1}$$

Note that this definition of $E_D$ does not contain a factor $\frac{1}{4}$ on the left-hand side like in the previous chapter. This is because 2 is a unit in $\mathbb{F}_q[T]$, so we do not have to be as careful with factors 2 or $\frac{1}{2}$ as in the number field case. As we will see, this will actually make our lives easier when proving the function-field equivalent of Theorem 3.1.4, which will be Theorem 4.1.3 below.

We take two affine points $P \in E(\mathbb{F}_q(T))$ and $Q \in E_D(\mathbb{F}_q(T))$, such that $y(Q) \neq 0$. By Proposition 1.7.4 there exist polynomials $A, B, C \in \mathbb{F}_q[T]$ with $\gcd(A, C) = \gcd(B, C) = 1$ such that

$$P = \left(\frac{A}{C^2}, \frac{B}{C^3}\right).$$

**Lemma 4.1.1.** *There exist unique polynomials $u, v, w \in \mathbb{F}_q[T]$ such that*

$$Q = \left(\frac{u}{w^2}, \frac{v}{w^3}\right),$$

*and $\gcd(u, w^2)$ and $\gcd(v, w^3)$ both divide $D$.*

*Remark* 4.1.2. In this chapter, $v$ will always denote a polynomial. We write $v_{\mathfrak{p}}$ for the valuation on $\mathbb{F}_q(T)$ corresponding to a monic irreducible polynomial $\mathfrak{p} \in \mathbb{F}_q[T]$, cf. Section 1.5. ♢

*Proof.* The proof is (almost) the same as that of Lemma 3.1.1 in the case that $D$ is even, where we replace $D/4 \in \mathbb{Z}$ by $D \in \mathbb{F}_q[T]$ and instead of prime numbers $p$ we consider monic irreducible polynomials $\mathfrak{p} \in \mathbb{F}_q[T]$. □

Lastly, we put

$$\alpha = Aw^2 - uC^2 \qquad \text{and} \qquad G = \gcd(\alpha, C^6v^2).$$

The next theorem gives the function-field analogue of Theorem 3.1.4.

**Theorem 4.1.3.** *Assuming the foregoing notation and hypotheses, there exist infinitely many polynomials $\ell \in \mathbb{F}_q[T]$ such that*

$$F_{P,Q}(X,Y) := \frac{\alpha}{G} \cdot X^2 + \frac{w^3B + \ell \cdot \frac{\alpha}{G}}{C^3v} \cdot XY + \frac{(w^3B + \ell \cdot \frac{\alpha}{G})^2 - C^6v^2D}{4C^6v^2 \cdot \frac{\alpha}{G}} \cdot Y^2$$

*is a discriminant $D$ binary quadratic form with coefficients in $\mathbb{F}_q[T]$. Further, the choice of $\ell$ does not affect the $\mathrm{SL}_2(\mathbb{F}_q[T])$-equivalence of $F_{P,Q}$, and if we have two pairs of points $(P_1, Q_1)$ and $(P_2, Q_2)$ such that $F_{P_1,Q_1}$ and $F_{P_2,Q_2}$ are $\mathrm{SL}_2(\mathbb{F}_q[T])$-equivalent, then there exists a unit $a \in \mathbb{F}_q^*$ such that*

$$\frac{\alpha_1}{G_1} = a \cdot \frac{\alpha_2}{G_2} \qquad \textit{or} \qquad \left|\frac{\alpha_1\alpha_2}{G_1G_2}\right|_\infty \geq |D|_\infty.$$

*Remark* 4.1.4. Note that the factor 4 in the denominator of the $Y^2$-coefficient is necessary such that $F_{P,Q}$ has discriminant $D$. ♢

*Proof.* A straightforward calculation shows that $F_{P,Q}$ has discriminant $D$. We will now show that $F_{P,Q}$ is integral, i.e. its coefficients lie in $\mathbb{F}_q[T]$. We have $\frac{\alpha}{G} \in \mathbb{F}_q[T]$, so we want to prove the existence of polynomials $\ell \in \mathbb{F}_q[T]$ such that $w^3B + \ell \cdot \frac{\alpha}{G}$ is divisible by $C^3v$ and $(w^3B + \ell \cdot \frac{\alpha}{G})^2 - C^6v^2D$ is divisible by $4C^6v^2 \cdot \frac{\alpha}{G}$. Clearly, if some polynomial $\ell$ satisfies the second condition then it also satisfies the first.

We define $f(x) := x^3 + a_2x^2 + a_4x + a_6$. Then $f(\frac{A}{C^2}) = \frac{B^2}{C^6}$ and $f(\frac{u}{w^2}) = D \cdot \frac{v^2}{w^6}$. We have

$$f\left(\frac{A}{C^2}\right) - f\left(\frac{u}{w^2}\right) = \left(\frac{A}{C^2} - \frac{u}{w^2}\right)\left(\frac{A^2}{C^4} + \frac{Au}{C^2w^2} + \frac{u^2}{w^4} + a_2\frac{A}{C^2} + a_2\frac{u}{w^2} + a_4\right),$$

and $\alpha = w^2C^2\left(\frac{A}{C^2} - \frac{u}{w^2}\right)$. Hence $\alpha$ divides

$$w^6C^6\left(f\left(\frac{A}{C^2}\right) - f\left(\frac{u}{w^2}\right)\right) = w^6B^2 - C^6v^2D, \tag{4.1.2}$$

implying that $G$ divides $w^6B^2$. If we let $H = \gcd(w^3B, C^3v)$, then $G$ divides $H^2 = \gcd(w^6B^2, C^6v^2)$. Hence $C^3v/H$ divides $C^6v^2/G$, showing that $\gcd(C^3v/H, \frac{\alpha}{G}) = 1$. We let $k$ be any polynomial satisfying

$$\frac{\alpha}{G} \cdot k \equiv -\frac{w^3B}{H} \pmod{\frac{C^3v}{H}}. \tag{4.1.3}$$

Note that since $\frac{\alpha}{G}$ is coprime to $C^3v/H$, such polynomials can easily be found by inverting $\frac{\alpha}{G}$ modulo $\frac{C^3v}{H}$. We define $\ell' = Hk$, such that

$$\frac{\alpha}{G} \cdot \ell' \equiv -w^3B \pmod{C^3v}.$$

Then $(w^3B + \ell' \cdot \frac{\alpha}{G})^2 - C^6v^2D$ is divisible by $C^6v^2$. We want that it is also divisible by $\alpha$, since in that case it is divisible by $4C^6v^2 \cdot \frac{\alpha}{G}$ (recall that $4 \in \mathbb{F}_q[T]^*$). By (4.1.2) we have

$$\left(w^3B + \ell' \cdot \frac{\alpha}{G}\right)^2 - C^6v^2D \equiv \ell'^2 \cdot \frac{\alpha^2}{G^2} + 2w^3B\ell' \cdot \frac{\alpha}{G} \pmod{\alpha}.$$

Since the expression on the left-hand side of the above equation is divisible by $C^6v^2$, it is divisible by $G$. As $\alpha$ is also divisible by $G$, the expression on the right-hand side must also be divisible by $G$. We define the polynomial

$$I = \frac{\ell'^2 \cdot \frac{\alpha^2}{G^2} + 2w^3B\ell' \cdot \frac{\alpha}{G}}{G}.$$

What is left to show, is that we can choose $\ell'$ such that $I$ is divisible by $\frac{\alpha}{G}$. Exactly like in the proof of Theorem 3.1.4, this follows from the fact that by the Chinese remainder theorem we can choose $k$ such that it is divisible sufficiently many times by $\frac{\alpha}{G}$. Taking $\ell = \ell'$ for such $k$, we conclude that for these polynomials $\ell$ the quadratic form $F_{P,Q}$ is integral.

Now, for the $\mathrm{SL}_2(\mathbb{F}_q[T])$-equivalence of $F_{P,Q}$ for different choices of $\ell$, we note that

$$F_{P,Q}(X,Y) = \frac{G}{\alpha}\left[\left(\frac{\alpha}{G}X + \frac{w^3B + \ell \cdot \frac{\alpha}{G}}{2C^3v}Y\right)^2 + \tfrac{1}{4}DY^2\right]. \tag{4.1.4}$$

Suppose that $\ell_1 = Hk_1$ and $\ell_2 = Hk_2$ are two polynomials such that $F_{P,Q}$ is integral. We write $F_{P,Q,\ell_1}$ and $F_{P,Q,\ell_2}$ to distinguish between the two quadratic forms. By (4.1.3) we have

$$\ell_1 \cdot \frac{\alpha}{G} = \ell_2 \cdot \frac{\alpha}{G} + n \cdot C^3v$$

for some $n \in \mathbb{F}_q[T]$. This shows that $F_{P,Q,\ell_1}(X,Y) = F_{P,Q,\ell_2}(X + \frac{1}{2}nY, Y)$. Since $\frac{1}{2}n \in \mathbb{F}_q[T]$ and $1 \cdot 1 - \frac{1}{2}n \cdot 0 = 1$, we see that $F_{P,Q,\ell_1}$ and $F_{P,Q,\ell_2}$ are $\mathrm{SL}_2(\mathbb{F}_q[T])$-equivalent.

Finally, suppose that $(P_1, Q_1)$ and $(P_2, Q_2)$ are two pairs of points for which $F_{P_1,Q_1}$ and $F_{P_2,Q_2}$ are $\mathrm{SL}_2(\mathbb{F}_q[T])$-equivalent. For $i \in \{1,2\}$ we write $A_i, B_i, C_i, u_i, v_i, w_i, \alpha_i, G_i$ and $\ell_i$ for the quantities corresponding to these two pairs of points. Then there is an element $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{F}_q[T])$ such that $F_{P_2,Q_2}(X,Y) = F_{P_1,Q_1}(aX + bY, cX + dY)$. By (4.1.4), the coefficient of $X^2$ in $\mathbb{F}_{P_2,Q_2}$ satisfies

$$\frac{\alpha_2}{G_2} = \frac{G_1}{\alpha_1}\left[\left(\frac{\alpha_1}{G_1}a + \frac{w_1^3B_1 + \ell_1 \cdot \frac{\alpha_1}{G_1}}{2C_1^3v_1}c\right)^2 + \tfrac{1}{4}Dc^2\right].$$

If $c = 0$, then $ad = 1$. This implies that $a \in \mathbb{F}_q^*$ and therefore $a^2 \in \mathbb{F}_q^*$. We obtain $\frac{\alpha_2}{G_2} = \frac{\alpha_1}{G_1}a^2$. Now suppose that $c \neq 0$. In this case, the fact that $D$ is an *imaginary* fundamental discriminant will play a crucial roll[1]. Namely, this implies that either the degree of $\frac{1}{4}Dc^2$ is odd, or its leading coefficient is not a square in $\mathbb{F}_q^*$. In both cases, we find that

$$\deg\left(\left(\frac{\alpha_1}{G_1}a + \frac{w_1^3B_1 + \ell_1 \cdot \frac{\alpha_1}{G_1}}{2C_1^3v_1}c\right)^2 + \tfrac{1}{4}Dc^2\right) \geq \deg D.$$

Hence, we obtain

$$\left|\frac{\alpha_1\alpha_2}{G_1G_2}\right|_\infty \geq |D|_\infty.$$

□

[1] Note that in the proof of Theorem 3.1.4 this is also the case, as we used there that the discriminant $-D$ was negative.

As explained at the start of this section, we cannot define an elliptic curve ideal class pairing for function fields like $\Psi_{-D}$ from the previous chapter. Instead, we will remove the correspondence between classes of quadratic forms and ideal classes from these pairings, yielding elliptic curve form class pairings.

**Definition 4.1.5.** Assume the same notation and hypotheses as in Theorem 4.1.3. We define the *elliptic curve form class pairing* corresponding to the elliptic curve $E$ and the discriminant $D$ as the map

$$\Phi_D : E(\mathbb{F}_q(T) \times E_D(\mathbb{F}_q(T)) \to \mathcal{Q}_D, \qquad (P, Q) \mapsto [F_{P,Q}],$$

where $[F_{P,Q}]$ denotes the $\mathrm{SL}_2(\mathbb{F}_q[T])$-equivalence class of the quadratic form $F_{P,Q}$ from Theorem 4.1.3.

## 4.2 Lower Bounds for Class Numbers

In this section we will use the elliptic curve form class pairings from Definition 4.1.5 to give a lower bound for the class number $h_K(D)$ of $K = \mathbb{F}_q(T)(\sqrt{D})$ in terms of $D$. Please note that we use the notation $h_K$ and $h_K^I$ for the class number and ideal class number of a global function field, respectively, and we write $h, h_x$ and $\hat{h}$ for the height functions defined in Chapter 2. Our strategy will be very similar to that in Section 3.3.

Recall that we consider an elliptic curve $E/\mathbb{F}_q(T)$ given by

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6, \qquad a_2, a_4, a_6 \in \mathbb{F}_q[T].$$

Using the elliptic curve form class pairing described in Theorem 4.1.3 we can construct discriminant $D$ binary quadratic forms from pairs of points on $E$ and $E_D$. By constructing inequivalent such quadratic forms, we can give a lower bound for the class number $h_K(D)$. However, for function fields this is slightly more complicated than for number fields. In the number field case, $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of quadratic forms obtained from Theorem 3.1.4 corresponded one-to-one with elements in the (ideal) class group. For function fields this is different in two ways. First, by Corollary 1.6.8 there is no one-to-one correspondence between the group $\mathcal{Q}_D$ of $\mathrm{SL}_2(\mathbb{F}_q[T])$-equivalence classes of discriminant $D$ binary quadratic forms and the ideal class group $\mathcal{I}_K$ of $\mathcal{O}_K$. Instead, we have

$$\mathcal{Q}_D/(\mathbb{Z}/2\mathbb{Z}) \cong \mathcal{I}_K.$$

Therefore, if we construct $n$ distinct equivalence classes of binary quadratic forms using Theorem 4.1.3, then we can only say that $h_K^I = |\mathcal{I}_K| \geq \frac{1}{2}n$. Secondly, the number $h_K^I$ is not what we call the class number of $K$, as it is not an invariant of $K$ but rather depends on the choice for $T$ we made in Remark 1.2.2. The class number of $K$ is the number of degree zero equivalence classes of divisors of $K$, and is denoted by $h_K$ or $h_K(D)$ since $D$ determines the field $K$. By Proposition 1.4.5 we have $h_K = h_K^I$ if $\deg(D)$ is odd, and $h_K = \frac{1}{2}h_K^I$ otherwise. So in total, if we obtain $n$ distinct classes of binary quadratic forms from Theorem 4.1.3, we obtain

$$h_K(D) \geq \frac{1}{2\sigma}n \qquad \text{where } \sigma = \begin{cases} 1 & \text{if } \deg(D) \text{ is odd,} \\ 2 & \text{else.} \end{cases} \tag{4.2.1}$$

Just as in the previous chapter, we will only consider a specific family of discriminants. Namely, we consider those of the form

$$D_E(f) = f^3 + a_2f^2 + a_4f + a_6, \qquad \text{with } f \in \mathbb{F}_q[T]. \tag{4.2.2}$$

For fundamental discriminants $D_E(f)$ of this shape, we always have the point $Q_f = (f, 1) \in E_D(\mathbb{F}_q(T))$.

We note that since $E$ is isomorphic to a curve given by a short Weierstrass equation, the results in 3.2 still hold for $E$. However, in order to use our Theorem 2.4.16 which bounds the difference between $\hat{h}$ and $h_x$ on $E$, we will have to adapt the theorem because these bounds depend on the specific Weierstrass model we choose for the elliptic curve. In [Sil09, §III.1] it is shown that via the coordinate transformation

$$x' = \frac{x - 12a_2}{36} \qquad \text{and} \qquad y' = \frac{1}{216}y,$$

the curve $E$ is isomorphic to the curve

$$E' : y'^2 = x'^3 + A'x' + B',$$

where

$$A' = 1296a_4 - 432a_2^2 \qquad \text{and} \qquad B' = 3456a_2^3 - 15552a_2a_4 + 46656a_6$$

We denote the discriminant of $E'$ by $\Delta'$, and we write $j$ for the $j$-invariant of $E$ and $E'$.

**Proposition 4.2.1.** *Let $E/\mathbb{F}_q(T)$ be an elliptic curve given by*

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6, \qquad a_2, a_4, a_6 \in \mathbb{F}_q[T],$$

*and let $E'$, $\Delta'$ and $j$ be as defined above. Then for all $P \in E(\mathbb{F}_q(T))$ we have*

$$-\tfrac{1}{8}h(j) - \tfrac{1}{12}h(\Delta') - \tfrac{1}{2}h(a_2) \leq \hat{h}(P) - \tfrac{1}{2}h_x(P) \leq \tfrac{1}{12}h(\Delta') + \tfrac{1}{12}h(j) + \tfrac{1}{2}h(a_2).$$

*Proof.* For $P = \mathcal{O}$ the result is clear, so let $P = (x, y) \in E(\mathbb{F}_q(T))$ be an affine point, and write $P' = (x', y')$ for the corresponding point on $E'(\mathbb{F}_q(T))$. By Theorem 2.4.16 we have

$$-\tfrac{1}{8}h(j) - \tfrac{1}{12}h(\Delta') \leq \hat{h}(P') - \tfrac{1}{2}h_x(P') \leq \tfrac{1}{12}h(\Delta') + \tfrac{1}{12}h(j). \tag{4.2.3}$$

We note that the canonical height function $\hat{h}$ is independent of the chosen Weierstrass model for $E$, which follows from Theorem 2.4.2(b) and Theorem 2.4.6. Hence, we have $\hat{h}(P) = \hat{h}(P')$. We write $\frac{1}{36}x = f/g$ with coprime polynomials $f, g \in \mathbb{F}_q[T]$, and $h = -\frac{1}{3}a_2 \in \mathbb{F}_q[T]$. Then we have

$$x' = \frac{f}{g} + h = \frac{f + gh}{g}.$$

Since $f$ and $g$ are coprime, we must have that $f + gh$ and $g$ are coprime. Then, by (2.1.1) in the proof of Theorem 2.1.8, and since multiplication by constants does not affect the height, we have

$$\begin{aligned} h(x) &= \log \max\{|f|_\infty, |g|_\infty\}, \\ h(a_2) &= \log |h|_\infty, \\ h(x') &= \log \max\{|f + gh|_\infty, |g|_\infty\}. \end{aligned}$$

This implies that $h(x') \leq h(x) + h(a_2)$. Now suppose that $h(x') < h(x)$. Then we must have $|g|_\infty < |f|_\infty$, and $|f|_\infty = |g|_\infty \cdot |h|_\infty$. Since $h(x') \geq \log |g|_\infty$, this implies that

$$h(x') \geq \log\left(|f|_\infty / |h|_\infty\right) = h(x) - h(a_2).$$

So, using that $h_x(P) = h(x)$ and $h_x(P') = h(x')$, in total we have

$$h_x(P) - h(a_2) \leq h_x(P') \leq h_x(P) + h(a_2). \tag{4.2.4}$$

Then the desired result follows by combining (4.2.4) and (4.2.3), and using that $\hat{h}(P) = \hat{h}(P')$. □

In light of the above proposition, we define

$$\delta(E) = \tfrac{1}{8}h(j) + \tfrac{1}{12}h(\Delta) + \tfrac{1}{2}h(a_2) + \tfrac{1}{4}\log(2). \tag{4.2.5}$$

Further, we define

$$\tau_E(f) = \tfrac{1}{4}\log\left(\left|\frac{D_E(f)}{f^2}\right|_\infty\right) - \delta(E). \tag{4.2.6}$$

The following theorem is our function-field equivalent of Theorem 3.3.2.

**Theorem 4.2.2.** *Let $\mathcal{B}$ be a set of linearly independent points in $E(\mathbb{F}_q(T))/E(\mathbb{F}_q(T)_{\mathrm{tors}})$ with diameter $d = d(\mathcal{B})$. Suppose that $f \in \mathbb{F}_q[T]$ is a polynomial such that $\tau_E(f) \geq d$ and $D_E(f)$ is an imaginary fundamental discriminant satisfying $|D_E(f)|_\infty \leq |f^4|_\infty$. Then*

$$h_K(D_E(f)) \geq \frac{c(E, \mathcal{B})}{4\sigma}\left(\tau_E(f)^{\frac{r}{2}} - r\sqrt{d}\tau_E(f)^{\frac{r-1}{2}}\right).$$

*Proof.* By Proposition 3.2.5 we have

$$\#\{P \in E(\mathbb{F}_q(T)) : \hat{h}(P) \leq \tau_E(f)\} \geq c(E, \mathcal{B}) \left(\tau_E(f)^{\frac{r}{2}} - r\sqrt{d}\tau_E(f)^{\frac{r-1}{2}}\right). \tag{4.2.7}$$

Now, we will examine which points $P \in E(\mathbb{F}_q(T))$ such that $\hat{h}(P) \leq \tau_E(f)$ get mapped to inequivalent quadratic forms when paired with $Q_f$ by the form class pairing $\Phi_D$ from Definition 4.1.5. Suppose that we have two points $P_i = (A_i/C_i^2, B_i/C_i^3)$ for $i \in \{1, 2\}$ such that $\hat{h}(P_i) \leq \tau_E(t)$. We write $F_1 = F_{P_1,Q_f}$ and $F_2 = F_{P_2,Q_f}$. Since $Q_f = (f, 1)$, we have $\alpha_i = A_i - fC_i^2$ and $G_i = \gcd(\alpha_i, C^6)$. Hence by $\gcd(A_i, C_i) = 1$ we obtain $G_i = 1$. Using Proposition 4.2.1 we find

$$\begin{aligned}
h_x(P_i) &\leq 2\left(\hat{h}(P_i) + \tfrac{1}{8}h(j) + \tfrac{1}{12}h(\Delta) + \tfrac{1}{2}h(a_2)\right) && \text{by Theorem 2.4.16}\\
&\leq 2\tau_E(f) + \tfrac{1}{4}h(j) + \tfrac{1}{6}h(\Delta) + h(a_2)\\
&= \tfrac{1}{2}\log\left(\left|\frac{D_E(f)}{f^2}\right|_\infty\right) - \tfrac{1}{2}\log(2) && \text{by (4.2.6) and (4.2.5)}\\
&= \tfrac{1}{2}\log\left(\frac{|D_E(f)|_\infty}{2|f^2|_\infty}\right). && (4.2.8)
\end{aligned}$$

We define the height function $H(P) = \exp(h_x(P))$, such that $H(P_i) = \max\{|A_i|_\infty, |C_i^2|_\infty\}$. Then

$$|\alpha_i|_\infty \leq |f|_\infty H(P_i)$$

Further, by (4.2.8) we have

$$H(P_i) \leq \frac{\sqrt{|D_E(f)|_\infty}}{\sqrt{2} \cdot |f|_\infty}, \tag{4.2.9}$$

implying that $|\alpha_i|_\infty \leq \sqrt{|D_E(f)|_\infty}/\sqrt{2}$. Therefore, we obtain

$$|\alpha_1\alpha_2|_\infty \leq \frac{|D_E(f)|_\infty}{2}.$$

If there does not exist a unit $a \in \mathbb{F}_q^*$ such that $\alpha_1 = a\alpha_2$, then Theorem 4.1.3 tells us that $F_1$ and $F_2$ are inequivalent quadratic forms. Now suppose there does exist such a unit $a$. Then

$$A_1 + fC_1^2 = aA_2 + afC_2^2, \tag{4.2.10}$$

which in particular implies that $A_1 \equiv aA_2 \pmod f$. Our assumption that $|D_E(f)|_\infty \leq |f^4|_\infty$ implies by (4.2.9) that $H(P_i) \leq |f|_\infty/\sqrt{2}$. Hence $|A_i|_\infty \leq |f|_\infty/\sqrt{2}$, showing that $\deg(A_i) < \deg(f)$. Then, since $A_1 \equiv aA_2 \pmod f$, we must have $A_1 = aA_2$. Then by (4.2.10) we also have $C_1^2 = aC_2^2$, so

$$\frac{A_1}{C_1^2} = \frac{aA_2}{aC_2^2} = \frac{A_2}{C_2^2}.$$

This shows that the points $P_1$ and $P_2$ have the same $x$-coordinate, which by the Weierstrass equation implies that $P_1 = \pm P_2$. Note that this also implies that $\hat{h}(P_1) = \hat{h}(P_2)$. So we have shown that for two points $P_1$ and $P_2$ in the set $\{P \in E(\mathbb{F}_q(T)) : \hat{h}(P) \leq \tau_E(f)\}$ we either have $P_1 = \pm P_2$ or their associated quadratic forms $F_1$ and $F_2$ are inequivalent. Hence, from the points in this set we obtain

$$\frac{\#\{P \in E(\mathbb{F}_q(T)) : \hat{h}(P) \leq \tau_E(f)\}}{2}$$

distinct equivalence classes of binary quadratic forms in $\mathcal{Q}_{D_E(f)}$. Then, by (4.2.1) we find that

$$h_K(D_E(f)) \geq \frac{1}{4\sigma} \cdot \#\{P \in E(\mathbb{F}_q(T)) : \hat{h}(P) \leq \tau_E(f)\}.$$

Substituting (4.2.7) in the above inequality yields the desired result. □

*Remark* 4.2.3. From the proof of Theorem 4.2.2, it is obvious that in (4.2.5) we can take any constant $\epsilon > 0$ instead of $\frac{1}{4}\log(2)$ and the proof still works. If we choose a smaller constant there, the number $\tau_E(f)$ becomes larger for a given $f$, which gives a slightly stronger version of Theorem 4.2.2. However, asymptotically the difference is negligible, so we chose the constant $\frac{1}{4}\log(2)$ because it works out nicely in the proof. ♢

*Remark* 4.2.4. We make a few additional short remarks. First, note from (4.2.2) that there is an effectively computable constant $n_0(a_2,a_4,a_6)$ such that if $|f|_\infty \geq n_0$ then $\deg(D_E(f))$ is odd. Second, we remark that since $D_E(f)$ is cubic in $f$, the condition that $|D_E(f)|_\infty \leq |f^4|_\infty$ is satisfied for all $f$ such that $|f|_\infty \geq n_1(a_2,a_4,a_6)$, where $n_1(a_2,a_4,a_6)$ is effectively computable. Lastly, there exists an effectively computable constant $n_2(a_2,a_4,a_6,d)$ such that if $|f|_\infty \geq n_2$ then $\tau_E(f) \geq d$. ♢

If $|f|_\infty$ is large enough, we have $|D_E(f)|_\infty = |f|_\infty^3$. For such polynomials $f$ we have $\tau_E(f) = \frac{1}{4}\log(|f|_\infty) - \delta(E)$. So for polynomials $f$ with $|f|_\infty$ sufficiently large, we can view $|D_E(f)|_\infty$ and $\tau_E(f)$ as functions of $|f|_\infty$.

**Lemma 4.2.5.** *Asymptotically, viewing $|D_E(f)|_\infty$ and $\tau_E(f)$ as functions of $|f|_\infty$, we have*

$$\tau_E(f) \sim \frac{\log(|D_E(f)|_\infty)}{12}.$$

*Proof.* By the above discussion, for polynomials $f$ with $|f|_\infty$ sufficiently large we have

$$\tau_E(f) = \frac{1}{4}\log(|D_E(f)|_\infty^{\frac{1}{3}}) - \delta(E) = \frac{\log(|D_E(f)|_\infty)}{12} - \delta(E),$$

from which the result is obvious. □

The next theorem is the function-field analogue of Theorem 3.3.5. For a given elliptic curve $E$, it gives a lower bound on the class number $h_K(D_E(f))$ in terms of $|D_E(f)|_\infty$.

**Theorem 4.2.6.** *Let $E/\mathbb{F}_q(T)$ be an elliptic curve of rank $r \geq 1$ given by*

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6, \qquad a_2,a_4,a_6 \in \mathbb{F}_q[T],$$

*and let $\mathcal{B}$ be a set of $r$ linearly independent points in $E(\mathbb{F}_q(T))/E(\mathbb{F}_q(T))_{\text{tors}}$. Let $\varepsilon > 0$. Then there exists an effectively computable constant $N(E,\mathcal{B},\varepsilon)$ such that, if $f \in \mathbb{F}_q[T]$ is a polynomial such that $D_E(f)$ is an imaginary fundamental discriminant and $|f|_\infty \geq N(E,\mathcal{B},\varepsilon)$, then*

$$h_K(D_E(f)) \geq \frac{c(E,\mathcal{B})}{4\sqrt{12^r}}(1-\varepsilon)\log\left(|D_E(f)|_\infty\right)^{\frac{r}{2}}.$$

*Proof.* We let $d = d(\mathcal{B})$. By Remark 4.2.4 there exists an effectively computable constant $n(E,d)$ such that if $D_E(f)$ is an imaginary fundamental discriminant and $|f|_\infty \geq n(E,d)$ then

$$h_K(D_E(f)) \geq \frac{c(E)}{4}\left(\tau_E(f)^{\frac{r}{2}} - r\sqrt{d}\tau_E(f)^{\frac{r-1}{2}}\right). \tag{4.2.11}$$

Using Lemma 4.2.5, we can show that there exists an effectively computable constant $N(E,\varepsilon)$ such that, if $f \in \mathbb{F}_q[T]$ is a polynomial such that $D_E(f)$ is an imaginary fundamental discriminant and $|f|_\infty \geq N(E,\varepsilon)$, then

$$\tau_E(f)^{\frac{r}{2}} - r\sqrt{d}\tau_E(f)^{\frac{r-1}{2}} \geq \frac{1}{\sqrt{12^r}}(1-\varepsilon)\log(|D_E(f)|_\infty)^{\frac{r}{2}}. \tag{4.2.12}$$

The proof of the above equation works exactly the same as in the proof of Theorem 3.3.5. We only have to replace $\log(D_E(t))$ by $\log(|D_E(f)|_\infty)$, and use Lemma 4.2.5 instead of Lemma 3.3.4. The desired result follows by plugging (4.2.12) into (4.2.11). □

## 4.3 Elliptic Curves of Large Rank

Note that the bound we obtain in Theorem 4.2.6 depends on the rank $r$ of the elliptic curve $E$. Asymptotically, the larger the rank, the better the bound we obtain, exactly like in the number field case in the previous chapter. For elliptic curves over $\mathbb{Q}$, it is still an open problem whether there are curves of arbitrarily large rank. However, for elliptic curves over $\mathbb{F}_q(T)$ it there exist multiple constructions of families of elliptic curves with arbitrarily large rank. In this section we will give such a construction due to Ulmer [Ulm14], and in the next section we examine the bounds that result from Theorem 4.2.6 using these curves. The elliptic curves we construct will all be defined over a rational function field $\mathbb{F}_q(T)$. However, we emphasize that the number $q$ will vary between different elliptic curves.

Let $\theta \geq 1$ be an integer. We put

$$d = p^\theta + 1.$$

Note that our assumption that $p \neq 2, 3$ implies that $d$ is even. In this chapter, we will study elliptic curves $E^\theta$ of the form

$$E^\theta : y^2 = x(x+1)(x+T^d), \tag{4.3.1}$$

defined over a rational function field $\mathbb{F}_q(T)$ that contains a $d$'th root of unity.

**Lemma 4.3.1.** *The smallest positive integer $n$ such that $\mathbb{F}_{p^n}$ contains a primitive $d$'th root of unity equals $n = 2\theta$.*

*Proof.* Write $q = p^n$. Then the group $\mathbb{F}_q^*$ is cyclic of order $p^n - 1$. Hence, $\mathbb{F}_q^*$ contains a primitive $d$'th root of unity if and only if $d = p^\theta + 1 \mid p^n - 1$. Suppose that $p^\theta + 1 \mid p^n - 1$ for some positive integer $n$. Then we must have $n > \theta$, so there exists a positive integer $\delta$ such that $n = \theta + \delta$. We have

$$p^n - 1 = p^{\theta+\delta} - 1 = p^\delta(p^\theta + 1) - (p^\delta + 1).$$

Therefore the fact that $p^\theta + 1 \mid p^n - 1$ implies that $p^\theta + 1 \mid p^\delta + 1$. This means that $\delta \geq \theta$, and therefore $n \geq 2\theta$. From $(p^{2\theta} - 1) = (p^\theta + 1)(p^\theta - 1)$ we see that $\mathbb{F}_{p^{2\theta}}$ indeed contains a $d$'th root of unity. □

By the above lemma, for the rest of this chapter we will put

$$q = p^{2\theta},$$

such that $\mathbb{F}_q(T)$ contains a primitive $d$'th root of unity. We fix such a root in $\mathbb{F}_q(T)$ and denote it by $\zeta_d$. The elliptic curve $E^\theta$ defined in (4.3.1) is defined over the field $\mathbb{F}_q(T)$, which depends on $\theta$. Since $d - 1 = p^\theta$ and $\mathbb{F}_q(T)$ has characteristic $p$, we have

$$1 + (\zeta_d^i T)^{d-1} = (1 + \zeta_d^i T)^{d-1}, \qquad \text{for all } i = 1, \ldots, d.$$

From this we obtain the identity

$$\zeta_d^i T(\zeta_d^i T + 1)(\zeta_d^i T + (\zeta_d^i T)^d) = \zeta_d^{2i} T^2 (\zeta_d^i T + 1)^d,$$

showing that $E^\theta(\mathbb{F}_q(T))$ contains the rational points

$$P_i = (\zeta_d^i T, \zeta_d^i T(\zeta_d^i T + 1)^{\frac{d}{2}}), \qquad i = 1, \ldots, d.$$

We denote the subgroup of $E^\theta(\mathbb{F}_q(T))$ generated by the points $P_i$ by $V_\theta$, and we write $r(\theta)$ for the rank of $E^\theta(\mathbb{F}_q(T))$. One of the main results in [Ulm14] is the following theorem.

**Theorem 4.3.2** ([Ulm14, Theorem 12.1(4)]). *The group $V_\theta$ has rank $d - 2$, and its index in $E^\theta(\mathbb{F}_q(T))$ is finite. In particular, this means that $r(\theta) = d - 2 = p^\theta - 1$, and therefore $r(\theta)$ tends to $\infty$ if $\theta \to \infty$.*

This implies that among the points $P_i$ there is a subset of $d - 2$ linearly independent points. As Ulmer shows in [Ulm14, Prop. 8.4], the sums

$$\sum_{i=1}^{d/2} P_{2i} \qquad \text{and} \qquad \sum_{i=1}^{d/2} P_{2i-1}$$

are both contained in the torsion group $E^\theta(\mathbb{F}_q(T))_{\text{tors}}$. These are the only relations between the points $P_i$. Therefore, the set

$$\mathcal{B}_\theta = \{P_1, \ldots, P_{d-2}\}$$

consists of linearly independent points in $E^\theta(\mathbb{F}_q(T))$. If we identify the points $P_i$ with their equivalence classes in the lattice $\Lambda = E^\theta(\mathbb{F}_q(T))/E^\theta(\mathbb{F}_q(T))_{\text{tors}}$, then we can also view $\mathcal{B}_\theta$ as a set of linearly independent points in $\Lambda$. In the next section we will use the class number bounds we derived in Section 4.2, where $E^\theta$ will take the role of $E$ and $\mathcal{B}_\theta$ that of $\mathcal{B}$.

## 4.4 Class Number Bounds With Large Ranks

In this section we will use the elliptic curves $E^\theta$ in our construction of lower bounds for class numbers of imaginary quadratic function fields given in Section 4.2. We want to see what happens if we use a family of curves for which the rank becomes infinitely large. Note that if we vary the elliptic curve in this construction, then the quantity $c(E)$ will vary accordingly. Further, recall that the elliptic curves $E^\theta$ are defined over different fields $\mathbb{F}_q(T)$, where $q = p^{2\theta}$.

Let us give a brief overview of the situation. We let $\theta$ be a positive integer, and we let $d$, $E^\theta$, $r(\theta)$, $\mathcal{B}_\theta$ and $q = p^{2\theta}$ as defined in the previous section. For a fundamental discriminant $D \in \mathbb{F}_q[T]$, the quadratic twist $E_D^\theta$ of $E^\theta$ is defined as in (4.1.1). We can write the elliptic curve $E^\theta$ as

$$E^\theta : y^2 = x^3 + (1 + T^d)x^2 + T^d x.$$

Therefore, for each $\theta$ we consider discriminants of the form

$$D_\theta(f) = f^3 + (1 + T^d)f^2 + T^d f, \qquad \text{with } f \in \mathbb{F}_q[T].$$

We define the field

$$K_\theta = \mathbb{F}_q(T)(\sqrt{D_\theta(f)}),$$

and we denote its class number by $h_{K_\theta}(D_\theta(f))$. From Theorem 4.2.6 we obtain the following bound for the class number.

**Corollary 4.4.1.** *Assume the foregoing notation, and let $\varepsilon > 0$. Then there exists an effectively computable constant $N(\theta, \varepsilon)$ such that, if $f \in \mathbb{F}_q[T]$ is a polynomial for which $D_\theta(f)$ is an imaginary fundamental discriminant and $|f|_\infty \geq N(\theta, \varepsilon)$, then*

$$h_{K_\theta}(D_\theta(f)) \geq \frac{c(E^\theta, \mathcal{B}_\theta)}{4\sqrt{12^{r(\theta)}}}(1 - \varepsilon)\log(|D_\theta(f)|_\infty)^{\frac{r(\theta)}{2}}.$$

We want to write the bound in the above corollary as an explicit function of $p, \theta$ and $|D_\theta(f)|_\infty$. For this we have to take a closer look at the function $c(E^\theta, \mathcal{B}_\theta)$.

Recall from the previous chapter that

$$c(E^\theta, \mathcal{B}_\theta) = \frac{|E^\theta(\mathbb{F}_q(T))_{\text{tors}}| \cdot \Omega_{r(\theta)}}{\sqrt{R_{\mathbb{F}_q(T)}(E^\theta, \mathcal{B}_\theta)}}.$$

Writing the number of torsion points on $E^\theta$ as a function of $\theta$ is easy, since by [Ulm14, Prop. 6.1] we have for all $\theta \geq 1$ that

$$|E^\theta(\mathbb{F}_q(T))_{\text{tors}}| = 8.$$

Recall that $\Omega_{r(\theta)}$ is the volume of the unit ball in $\mathbb{R}^r$. We have

$$\Omega_{r(\theta)} = \frac{\pi^{\frac{r(\theta)}{2}}}{(\frac{r(\theta)}{2})!}.$$

Lastly, we consider the $\mathcal{B}_\theta$-regulator $R_{\mathbb{F}_q(T)}(E^\theta, \mathcal{B}_\theta)$. Recall that $\mathcal{B}_\theta = \{P_1, \dots, P_{d-2}\}$, so we have

$$R_{\mathbb{F}_q(T)}(E^\theta, \mathcal{B}_\theta) = |\det(\langle P_i, P_j \rangle)_{1 \leq i,j \leq d-2}|.$$

**Theorem 4.4.2** ([Ulm14, Theorem 8.2])**.** *The height pairing of the points in $\mathcal{B}_\theta$ is given by*

$$\langle P_i, P_j \rangle = \begin{cases} \frac{(d-1)(d-2)}{2d} \cdot \log(q) & \textit{if } i = j, \\ \frac{1-d}{d} \cdot \log(q) & \textit{if } i - j \textit{ is even and} \neq 0, \\ 0 & \textit{if } i - j \textit{ is odd.} \end{cases}$$

We define the matrix $M_\theta = (\langle P_i, P_j\rangle)_{1\le i,j\le d-2}$, such that $R_{\mathbb{F}_q(T)}(E^\theta, \mathcal{B}_\theta) = |\det M_\theta|$ . For example, when $d-2=6$ this matrix is of the form

$$M_\theta = \begin{pmatrix} a & 0 & b & 0 & b & 0 \\ 0 & a & 0 & b & 0 & b \\ b & 0 & a & 0 & b & 0 \\ 0 & b & 0 & a & 0 & b \\ b & 0 & b & 0 & a & 0 \\ 0 & b & 0 & b & 0 & a \end{pmatrix},$$

where the values of $a, b \in \mathbb{R}$ can be found in Theorem 4.4.2. The following lemma gives a nice formula for the determinant of matrices of this form.

**Lemma 4.4.3.** *Let $n \ge 2$, and let $M = (m_{ij})_{1\le i,j\le n} \in M_n(\mathbb{R})$ be an $n\times n$ matrix with real coefficients $m_{ij}$, such that*

$$m_{ij} = \begin{cases} a & \text{if } i = j, \\ b & \text{if } i-j \text{ is even and } \neq 0, \\ 0 & \text{if } i-j \text{ is odd.} \end{cases}$$

*Further, if $n \ge 3$ assume that $a + lb \neq 0$ for all $l = 0, \dots, \lceil \frac{n-4}{2} \rceil$. Then the determinant of $M$ is given by*

$$\det M = (a-b)^{n-2}\left(a + \left\lfloor \frac{n-2}{2} \right\rfloor b\right)\left(a + \left\lceil \frac{n-2}{2} \right\rceil b\right). \tag{4.4.1}$$

*Proof.* We prove this lemma using induction on $n$. For $n=2$, the formula (4.4.1) gives the correct determinant $\det M = a^2$. Now let $n \ge 3$ be a positive integer and suppose that the lemma holds for $n-1$. We write $M'$ for the $(n-1)\times(n-1)$ matrix we obtain by deleting the bottom row and right-most column of $M$. Then $M'$ satisfies the conditions in the lemma, so by our induction hypothesis we have

$$\det M' = (a-b)^{n-3}\left(a + \left\lfloor \frac{n-3}{2} \right\rfloor b\right)\left(a + \left\lceil \frac{n-3}{2} \right\rceil b\right).$$

We distinguish between the cases that $n$ is even or odd. First suppose that $n$ is even. Then by assumption we have $a + \frac{n-4}{2}b \neq 0$. We define

$$c = \frac{b}{a + \frac{n-4}{2}b}.$$

Then $b - ca - \frac{n-4}{2}cb = 0$. Since $n$ is even, the bottom row of $M$ has even index. The $j$'th element in the bottom row is 0 if and only if the same holds for the $j$'th element in all the other even-indexed rows. The number of even-indexed rows that are not the bottom row is $\frac{n-2}{2}$. If the $j$'th element in the bottom row is a $b$, then exactly $\frac{n-4}{2}$ other even-indexed rows have a $b$ as $j$'th element, and exactly one even-indexed row has $a$ as its $j$'th element. Lastly, the $n$'th element of the bottom row is an $a$, and the $n$'th element of all the other even indexed rows is a $b$. We write $S$ for the sum of all even-indexed rows except the bottom row, multiplied by $c$. Then if we subtract $S$ from the bottom row, the bottom row becomes

$$\begin{pmatrix} 0 & \cdots & 0 & a - \frac{n-2}{2}cb \end{pmatrix},$$

which consists of only zeroes except for the $n$'th element. Since subtracting $S$ from the bottom row does not affect the determinant, and using that $\lfloor \frac{n-3}{2} \rfloor = \frac{n-4}{2}$ and $\lceil \frac{n-3}{2} \rceil = \frac{n-2}{2}$, we obtain

$$\begin{aligned} \det M &= \left(a - \frac{n-2}{2}cb\right) \cdot \det M', \\ &= \left(\frac{a^2 + \frac{n-4}{2}ab - \frac{n-2}{2}b^2}{a + \frac{n-4}{2}b}\right) \cdot \det M', \\ &= \left(\frac{(a-b)(a + \frac{n-2}{2}b)}{a + \lfloor \frac{n-3}{2} \rfloor b}\right) \cdot \det M', \\ &= (a-b)^{n-2}\left(a + \frac{n-2}{2}b\right)\left(a + \frac{n-2}{2}b\right). \end{aligned}$$

Now suppose that $n$ is odd. Our strategy will be very similar to the case that $n$ is even. Now, by assumption, we have $a + \frac{n-3}{2}b \neq 0$. We put

$$c = \frac{b}{a + \frac{n-3}{2}b},$$

such that $b - ca - \frac{n-3}{2}cb = 0$. Since $n$ is odd, the bottom row of $M$ has odd index, and there are $\frac{n-1}{2}$ other odd-indexed rows. This time, we let $S$ be the sum of all odd-indexed rows except the bottom row, multiplied by $c$. Subtracting $S$ from the bottom row of $M$ yields

$$\begin{pmatrix} 0 & \cdots & 0 & a - \frac{n-1}{2}cb \end{pmatrix},$$

which consists of only zeroes except for the $n$'th element. Therefore the determinant of $M$ is given by

$$\begin{aligned}
\det M &= \left(a - \frac{n-1}{2}cb\right) \cdot \det M', \\
&= \left(\frac{a^2 + \frac{n-3}{2}ab - \frac{n-1}{2}b^2}{a + \frac{n-3}{2}b}\right) \cdot \det M', \\
&= \left(\frac{(a-b)(a + \frac{n-1}{2}b)}{a + \frac{n-3}{2}b}\right) \cdot \det M', \\
&= (a-b)^{n-2}\left(a + \frac{n-3}{2}b\right)\left(a + \frac{n-1}{2}\right).
\end{aligned}$$

This proves the lemma. □

For the matrix $M_\theta$, we have in the notation of the above lemma

$$a = \frac{(d-1)(d-2)}{2d} \cdot \log(q), \qquad b = \frac{1-d}{d} \cdot \log(q), \qquad n = d-2.$$

Then $b \neq 0$ and $a + \frac{n}{2}b = 0$, implying that $a + kb \neq 0$ for all $l = 0, \ldots, \lceil \frac{n-4}{2} \rceil$. Therefore Lemma 4.4.3 gives

$$\begin{aligned}
R_{\mathbb{F}_q(T)}(E^\theta, \mathcal{B}_\theta) &= \left| \left(\frac{d-1}{2}\log(q)\right)^{d-4} \left(\frac{d-1}{d}\log(q)\right)^2 \right| \\
&= \frac{4}{d^2}\left(\frac{d-1}{2}\log(q)\right)^{d-2}.
\end{aligned}$$

Now we can write $c(E^\theta, \mathcal{B}_\theta)$ completely in terms of $\theta$. We obtain

$$c(E^\theta, \mathcal{B}_\theta) = 8 \cdot \frac{\pi^{\frac{p^\theta-1}{2}}}{(\frac{p^\theta-1}{2})!} \cdot \frac{1}{\frac{2}{p^\theta+1}\left(p^\theta\theta\log(p)\right)^{\frac{p^\theta-1}{2}}} = 4 \cdot \frac{p^\theta+1}{(\frac{p^\theta-1}{2})!}\left(\frac{\pi}{\theta p^\theta \log(p)}\right)^{\frac{p^\theta-1}{2}}.$$

From this we compute

$$\frac{c(E^\theta, \mathcal{B}_\theta)}{4\sqrt{12^{p^\theta-1}}} = \frac{p^\theta+1}{(\frac{p^\theta-1}{2})!}\left(\frac{\pi}{12\theta p^\theta \log(p)}\right)^{\frac{p^\theta-1}{2}}. \tag{4.4.2}$$

We have now proved the following theorem.

**Theorem 4.4.4.** *Assume the foregoing notation, and let $\varepsilon > 0$. Then there exists an effectively computable constant $N(\theta, \varepsilon)$ such that, if $f \in \mathbb{F}_q[T]$ is a polynomial for which $D_\theta(f)$ is an imaginary fundamental discriminant and $|f|_\infty \geq N(\theta, \varepsilon)$, then*

$$h_{K_\theta}(D_\theta(f)) \geq \frac{p^\theta+1}{(\frac{p^\theta-1}{2})!}\left(\frac{\pi}{12\theta p^\theta \log(p)}\right)^{\frac{p^\theta-1}{2}} (1-\varepsilon)\log(|D_\theta(f)|_\infty)^{\frac{p^\theta-1}{2}}. \tag{4.4.3}$$

*Proof.* This follows from Corollary 4.4.1 and (4.4.2). □

The above theorem shows that if $m$ is any integer satisfying $m < \frac{p^{\theta}-1}{2}$, then for large enough discriminants $D_\theta(f)$ (in terms of $|\cdot|_\infty$) we have

$$h_{K_\theta}(D_\theta(f)) > \log(|D_\theta(f)|_\infty])^m. \tag{4.4.4}$$

How large is 'large enough' depends on the constant $N(\theta, \varepsilon)$ and the bound given in the theorem. It turns out that even for relatively small $m$, the discriminant $D_\theta(f)$ has to be huge in order to satisfy (4.4.4), making the bound less suited for computational purposes. This can already be seen from the expression (4.4.2), which obviously tends to 0 very fast if $\theta \to \infty$. In the following example we compute for small values of $p$ and $\theta$ how large the discriminant $D_\theta(f)$ should be such that the bound from Theorem 4.4.4 is non-trivial.

**Example 4.4.5.** In this example we compute for small values of $p$ and $\theta$ how large the degree of the discriminant $D_\theta(f)$ should be such that the bound in (4.4.3) is non-trivial, i.e. its right-hand side is at least 1. Note that we only compute how large $\deg D_\theta(f)$ should be under the assumption that the assumption $|f|_\infty \geq N(\theta, \varepsilon)$ from Theorem 4.4.4 is satisfied. Clearly, if we find a minimal value for $\deg D_\theta(f)$ such that the bound is non-trivial, but it turns out that this condition is not satisfied, then we should take $\deg D_\theta(f)$ even larger to obtain a non-trivial bound from Theorem 4.4.4. The calculations in this example were verified using SageMath [The22].

Optimistically, we will for the moment forget about the factor $(1-\varepsilon)$ in (4.4.3). Note that adding this factor only means that we have to take even larger discriminants for the bounds to be non-trivial, so this gives us a strict lower bound on the degree of the discriminant. Recall that

$$|D_\theta(f)|_\infty = q^{\deg D_\theta(f)} = p^{2\theta \deg D_\theta(f)}.$$

Since we assume that $p \notin \{2, 3\}$, the smallest value we can take for $p$ is $p = 5$. For $p = 5$, the following table lists for small values of $\theta$ the smallest degree $\deg D_\theta(f)$ such that the bound (4.4.3) is non-trivial:

| $\theta$ | 1 | 2 | 3 | 5 |
|---|---|---|---|---|
| $\deg D_\theta(f)$ | 6 | 193 | 5285 | 3421987 |

.

Similarly, if we take $\theta = 2$ and we vary the prime $p$, we obtain

| $p$ | 5 | 7 | 11 | 13 | 17 |
|---|---|---|---|---|---|
| $\deg D_\theta(f)$ | 193 | 780 | 4948 | 9740 | 28783 |

.

◇

For the asymptotic behaviour of the class number of the fields $K_\theta$, we can either study the behaviour when $\theta \to \infty$, or the behaviour when $p \to \infty$. The above example shows that in both situations, if we want to use Theorem 4.4.4 to bound the class number, then we can only say something about fields $K_\theta = \mathbb{F}_q(T)(\sqrt{D_\theta(f)})$ for which the degree of the discriminant quickly becomes extremely large. This is not very practical. In the next section, we will give an overview of the known class number bounds for global function fields, and compare them to Theorem 4.4.4. As we will see, Theorem 4.4.4 is in fact inferior to the best known bounds in all aspects.

## 4.5 Comparison to the Literature

In this section we discuss how our bounds from Theorem 4.4.4 compare to the literature. Note that although we only considered imaginary quadratic fields, most bounds from the literature are for general global function fields. We start by giving an overview of the known bounds for class numbers of global function fields.

Recall from Section 1.4 that the genus of an imaginary quadratic global function field $\mathbb{F}_q(T)(\sqrt{D})$ is given by

$$g = \frac{\deg(D) - \upsilon}{2} \qquad \text{where } \upsilon = \begin{cases} 1 & \text{if } \deg(D) \text{ is odd,} \\ 2 & \text{if } \deg(D) \text{ is even.} \end{cases}$$

So studying the asymptotic behaviour of the class number $h_K(D)$ as a function of $\deg D$ is equivalent to studying it as a function of $g$.

Now, let $K/\mathbb{F}_q$ be a global function field with class number $h_K$ and genus $g$. We are mainly interested in the asymptotic behaviour of $h_K$ when $g \to \infty$. There appears to be rather little literature on this topic for the specific case that $K$ is imaginary quadratic, but for general function fields it is a classical problem just like its number theoretic analogue. Recall from Corollary 1.3.7 that the Hasse-Weil theorem implies

$$(\sqrt{q}-1)^{2g} \leq h_K \leq (\sqrt{q}+1)^{2g}. \tag{4.5.1}$$

If $K$ is imaginary quadratic then $(\sqrt{q})^{2g} = q^{-\upsilon}\sqrt{|D|_\infty}$. Hence we see that asymptotically as function of $g$, Equation (4.5.1) is very similar to Siegel's theorem on page 43 for number fields. Moreover, unlike Siegel's result these bounds are completely explicit and effective. So asymptotically as a function of $|D|_\infty$, the class numbers of imaginary quadratic function fields grow similar to the class numbers of imaginary quadratic number fields as a function of the discriminant $D$. However, from the Hasse-Weil theorem, or the (proven) Riemann hypothesis for function fields, we obtain effective lower bounds for the class number that are much better than we have for number fields. In fact, they are similar to the effective bounds we obtain for number fields assuming the generalised Riemann hypothesis. This is especially clear when we compare Theorem 3.4.4 to the following result by Lachaud and Martin-Deschamps.

**Theorem 4.5.1.** *Assuming that the degree $[K : \mathbb{F}_q(T)]$ remains bounded as we let $g \to \infty$, there exist explicit constants $c_1$ and $c_2$ such that*

$$c_1 \frac{\sqrt{\Theta}}{\log \Theta} \leq h_K \leq c_2 \sqrt{\Theta}(\log \sqrt{\Theta})^{n-1},$$

*where $\Theta = q^{2g-2}$.*

*Proof.* For the proof we refer to [LMD90, §5]. □

Note that the assumption in the above theorem is of course satisfied for imaginary quadratic function fields, and for such fields we have $\Theta = q^{-2-\upsilon}|D|_\infty$. Therefore, if we assume that we leave $q$ fixed, we can actually replace $\Theta$ by $|D|_\infty$ in the above theorem, yielding exactly the same lower bound as in Theorem 3.4.4 with $D$ replaced by $|D|_\infty$.

At the time of writing, the best known lower bound for class numbers of global fields that can be expressed purely in terms of $q$ and $g$, and with no assumptions on the field except that $g \geq 1$, is given by

$$h_K \geq q^{g-1} \frac{(q-1)^2}{(q+1)(g+1)}, \tag{4.5.2}$$

see [LMD90, Theorem 2(1)]. In the same paper, the authors give two improvements on this bound in special cases where for example we know that the smooth irreducible curve $C$ corresponding to $K$ (cf. Theorem 1.1.9) has at least one $\mathbb{F}_q$-rational point. Similarly, relatively recent results by Ballet, Rolland and Tutdere [BRT15] and Aubry, Haloui and Lachaud [AHL13] improve on the bound in (4.5.2) in many cases, assuming that we have some extra information about the function field.

We will now compare the bound in (4.5.2) to our own result from Theorem 4.4.4. So we go back to considering imaginary quadratic global function fields $K = \mathbb{F}_q(T)(\sqrt{D})$. To facilitate the comparison, we write (4.5.2) in terms of $|D|_\infty$ instead of $g$. We have

$$g = \frac{\log(|D|_\infty) - \upsilon \log(q)}{2\log(q)} \qquad \text{and} \qquad q^{g-1} = q^{-\frac{\upsilon}{2}-1}\sqrt{|D|_\infty}.$$

Therefore (4.5.2) becomes

$$h_K(D) \geq \frac{2(q-1)^2 \log(q)}{\sqrt{q^{\upsilon+2}}(q+1)} \cdot \frac{\sqrt{|D|_\infty}}{\log(|D|_\infty) + (2-\upsilon)\log(q)}. \tag{4.5.3}$$

Since any positive power of $|D|_\infty$ eventually grows faster than any power of $\log(|D|_\infty)$, we see that no matter how large we take $\theta$ or $p$ in Theorem 4.4.4, the bound we obtain will asymptotically in terms of $|D|_\infty$ always be inferior to (4.5.3). Therefore, our only hope to improve on (4.5.3) is to do this for small values of $|D|_\infty$. However, we note that the bound in Theorem 4.4.4 only holds for sufficiently large discriminants. Moreover, as we saw in Example 4.4.5, the discriminant $|D|_\infty$ has to become very large very quickly in order for the bounds in Theorem 4.4.4 to be non-trivial. We note that at least for the small values of $p$ and $\theta$ we considered in Example 4.4.5, if $|D_\theta(f)|_\infty$ is large enough that our bound is non-trivial, then the bound is long surpassed by that in (4.5.3).

*Remark* 4.5.2. As a final remark, let us briefly summarise why our strategy for bounding the class number from below using elliptic curve form class pairings yields a bound asymptotic to

$$c(\log(|D|_\infty))^{\frac{r}{2}} \tag{4.5.4}$$

for some constant $c > 0$, instead of a faster growing function of $|D|_\infty$.

In Theorem 4.1.3 we gave a necessary condition for two quadratic forms obtained via the construction in that theorem to be $\mathrm{SL}_2(\mathbb{F}_q[T])$-equivalent. We used this in the proof of Theorem 4.2.2 to show that we can use the elliptic curve form class pairing and rational points on the elliptic curve $E$ with canonical height at most $\tau_E$ to construct inequivalent quadratic forms. Recall that we defined

$$\tau_E(f) = \tfrac{1}{4}\log\left(\left|\frac{D_E(f)}{f^2}\right|_\infty\right) - \delta(E). \tag{4.5.5}$$

If we took another definition of $\tau_E(f)$ that asymptotically grows faster, then the bound we obtain in Theorem 4.2.2 would become stronger. However, we cannot do this because we need (4.2.8) and (4.2.9) to show that the quadratic forms we obtain are inequivalent. The best we can do is change $\tau_E(f)$ such that the factor $\sqrt{2}$ in (4.2.9) gets replaced by any smaller factor $\epsilon' > 1$. We can do this by taking any constant $\epsilon > 0$ instead of $\frac{1}{4}\log(2)$ in the definition of $\delta(E)$. As we noted in Remark 4.2.3, this does not affect the proof of Theorem 4.2.2, but it also does not affect the asymptotic behaviour of $\tau_E(f)$. So, asymptotically, we cannot define $\tau_E(f)$ such that it grows faster than in (4.5.5) and such that the proof of Theorem 4.2.2 still works.

The shape of the bound we obtain in Theorem 4.2.2 in terms of $\tau_E(f)$ comes from Proposition 3.2.5 which gives a lower bound for the number of rational points on $E$ of canonical height at most $\tau_E(f)$. As we noted just before stating Proposition 3.2.5, asymptotically this bound only differs from the actual amount of rational points of bounded canonical height by a constant factor. So also in this Proposition there is, asymptotically speaking, not much room for improvement.

Together, our choice for $\tau_E(f)$ and the bound from Proposition 3.2.5 determine the lower bound we obtain in Theorem 4.2.6. Therefore, by the above discussion, apart from obtaining a larger constant $c$, we cannot derive a lower bound for class numbers of imaginary quadratic global function fields that is asymptotically stronger than (4.5.4), without making significant changes or additions to our strategy using elliptic curve form class pairings. ♢

# Bibliography

[AHL13] Yves Aubry, Safia Haloui, and Gilles Lachaud. On the number of points on abelian and Jacobian varieties over finite fields. *Acta Arith.*, 160(3):201–241, 2013.

[AM69] Michael F. Atiyah and Ian G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[Art24] Emil Artin. Quadratische Körper im Gebiete der höheren Kongruenzen. I. *Math. Z.*, 19(1):153–206, 1924.

[Art67] Emil Artin. *Algebraic numbers and algebraic functions*. Gordon and Breach Science Publishers, New York-London-Paris, 1967.

[BC16] Duncan A. Buell and Gregory S. Call. Class pairings and isogenies on elliptic curves. *J. Number Theory*, 167:31–73, 2016.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BG06] Enrico Bombieri and Walter Gubler. *Heights in Diophantine geometry*, volume 4 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2006.

[BRT15] Stéphane Ballet, Robert Rolland, and Seher Tutdere. Effective bounds on class number and estimation for any step of towers of algebraic function fields over finite fields. *Mosc. Math. J.*, 15(4):653–677, 2015.

[Bue77] Duncan A. Buell. Elliptic curves and class groups of quadratic fields. *J. London Math. Soc. (2)*, 15(1):19–25, 1977.

[Bue89] Duncan A. Buell. *Binary quadratic forms*. Springer-Verlag, New York, 1989. Classical theory and modern computations.

[Bö80] Reinhard Bölling. Über einen Homomorphismus der rationalen Punkte elliptischer Kurven. *Math. Nachr.*, 96:207–244, 1980.

[Con06] Brian Conrad. Chow's $K/k$-image and $K/k$-trace, and the Lang-Néron theorem. *Enseign. Math. (2)*, 52(1-2):37–108, 2006.

[Cox13] David A. Cox. *Primes of the form $x^2 + ny^2$*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[CR16] Gunther Cornelissen and Jonathan Reynolds. The perfect power problem for elliptic curves over function fields. *New York J. Math.*, 22:95–114, 2016.

[Elk06] Noam D. Elkies. $\mathbb{Z}^{28}$ in $E(\mathbb{Q})$, etc., 2006. Listserv. 3 Apr. 2006. NmbrThry.

[Erd53] Paul Erdös. Arithmetical properties of polynomials. *J. London Math. Soc.*, 28:416–425, 1953.

[Est65] Dennis Ray Estes. *Classes of binary quadratic forms over polynomial rings*. ProQuest LLC, Ann Arbor, MI, 1965. Thesis (Ph.D.)–Louisiana State University and Agricultural & Mechanical College.

[GO20] Michael Griffin and Ken Ono. Elliptic curves and lower bounds for class numbers. *J. Number Theory*, 214:1–12, 2020.

[Gol85] Dorian Goldfeld. Gauss's class number problem for imaginary quadratic fields. *Bull. Amer. Math. Soc. (N.S.)*, 13(1):23–37, 1985.

[GOT21] Michael Griffin, Ken Ono, and Wei-Lun Tsai. Quadratic twists of elliptic curves and class numbers. *J. Number Theory*, 227:1–29, 2021.

[Har77] Robin Hartshorne. *Algebraic geometry.* Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[Has80] Helmut Hasse. *Number theory*, volume 229 of *Grundlehren der Mathematischen Wissenschaften.* Springer-Verlag, Berlin-New York, 1980. Translated from the third German edition and with a preface by Horst G. Zimmer.

[Hei34] Hans Heilbronn. On the class-number in imaginary quadratic fields. *Q. J. Math., Oxf. Ser.*, 5:150–160, 1934.

[HR92] Jeffrey Hoffstein and Michael Rosen. Average values of $L$-series in function fields. *J. Reine Angew. Math.*, 426:117–150, 1992.

[Hus04] Dale Husemöller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen.

[Kap68] Irving Kaplansky. Composition of binary quadratic forms. *Studia Math.*, 31:523–530, 1968.

[Kna92] Anthony W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes.* Princeton University Press, Princeton, NJ, 1992.

[Kne82] Martin Kneser. Composition of binary quadratic forms. *J. Number Theory*, 15(3):406–413, 1982.

[Kne10] Manfred Knebusch. *Specialization of quadratic and symmetric bilinear forms*, volume 11 of *Algebra and Applications.* Springer-Verlag London, Ltd., London, 2010. Translated from the German by Thomas Unger. Draft version available at `https://maths.ucd.ie/~tpunger/papers/book.pdf`.

[Kob89] Neal Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1(3):139–150, 1989.

[Lan78] Serge Lang. *Elliptic curves: Diophantine analysis*, volume 231 of *Grundlehren der Mathematischen Wissenschaften.* Springer-Verlag, Berlin-New York, 1978.

[Lan83] Serge Lang. *Fundamentals of Diophantine geometry.* Springer-Verlag, New York, 1983.

[Lan87] Serge Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics.* Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[LMD90] Gilles Lachaud and Mireille Martin-Deschamps. Nombre de points des jacobiennes sur un corps fini. *Acta Arith.*, 56(4):329–340, 1990.

[LMF22] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2022. [Online; accessed 4 July 2022].

[Mil06] James S. Milne. *Elliptic curves.* BookSurge Publishers, Charleston, SC, 2006.

[Oes85] Joseph Oesterlé. Nombres de classes des corps quadratiques imaginaires. Number 121-122, pages 309–323. 1985. Seminar Bourbaki, Vol. 1983/84.

[PPVW19] Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood. A heuristic for boundedness of ranks of elliptic curves. *J. Eur. Math. Soc. (JEMS)*, 21(9):2859–2903, 2019.

[Rei03] Irving Reiner. *Maximal orders*, volume 28 of *London Mathematical Society Monographs. New Series.* The Clarendon Press, Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original, With a foreword by M. J. Taylor.

[Ros02] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[Sie35] Carl L. Siegel. Über die Classenzahl quadratischer Zahlkörper. *Acta Arith.*, 1:83–86, 1935.

[Sil90] Joseph H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.*, 55(192):723–743, 1990.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Sol94] Ragnar Soleng. Homomorphisms from the group of rational points on elliptic curves to class groups of quadratic number fields. *J. Number Theory*, 46(2):214–229, 1994.

[ST02] Andreas Stein and Edlyn Teske. Explicit bounds and heuristics on class numbers in hyperelliptic function fields. *Math. Comp.*, 71(238):837–861, 2002.

[Ste02] Peter Stevenhagen. *Voortgezette Getaltheorie*, 2002. English. `https://websites.math.leidenuniv.nl/algebra/localfields.pdf`, consulted on 04/07/2022.

[Ste17] Peter Stevenhagen. *Number Rings*, 2017. `https://websites.math.leidenuniv.nl/algebra/ant.pdf`, date of online version: 13/08/2017.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[Sut19] Andrew V. Sutherland. Lecture 13: Global fields and the product formula. In *Number Theory I—MIT Course No. 18.785*. MIT OpenCourseWare, 2019. `https://ocw.mit.edu/courses/mathematics/18-785-number-theory-i-fall-2019/lecture-notes/MIT18_785F19_lec13.pdf`, consulted 18/05/2022.

[Tat51] Tikao Tatuzawa. On a theorem of Siegel. *Jpn. J. Math.*, 21:163–178 (1952), 1951.

[The22] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.6)*, 2022. `https://www.sagemath.org`.

[TVN07] Michael Tsfasman, Serge Vlăduţ, and Dmitry Nogin. *Algebraic geometric codes: basic notions*, volume 139 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2007.

[Ulm11] Douglas Ulmer. Elliptic curves over function fields. In *Arithmetic of L-functions*, volume 18 of *IAS/Park City Math. Ser.*, pages 211–280. Amer. Math. Soc., Providence, RI, 2011.

[Ulm14] Douglas Ulmer. Explicit points on the Legendre curve. *J. Number Theory*, 136:165–194, 2014.

[Woo11] Melanie Matchett Wood. Gauss composition over an arbitrary base. *Adv. Math.*, 226(2):1756–1771, 2011.

[Zim76] Horst G. Zimmer. On the difference of the Weil height and the Néron-Tate height. *Math. Z.*, 147(1):35–51, 1976.

[Zim01] Horst G. Zimmer. Height functions on elliptic curves. In *Public-key cryptography and computational number theory (Warsaw, 2000)*, pages 303–322. de Gruyter, Berlin, 2001.

# List of Symbols

| | |
|---|---|
| $\lvert\cdot\rvert_v$ | the absolute value on $K$ corresponding to a prime $v \in M_K$. |
| $\#\{\dots\}$ | the number of elements in the finite set $\{\dots\}$ |
| $\langle\cdot,\cdot\rangle$ | the Néron-Tate pairing |
| $\Delta$ | the discriminant of $E$ |
| $\varepsilon$ | a positive real constant |
| $\zeta_R$ | the Riemann zeta function |
| $\zeta_K$ | the zeta function of a global function field $K$ |
| $\Lambda$ | the lattice $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$ |
| $\Lambda_{\mathcal{B}}$ | the sublattice of $\Lambda$ generated by $\mathcal{B}$ |
| $\lambda_v$ | the local height function associated to a prime $v$ |
| $\Phi_D$ | the elliptic curve form class pairing defined in Definition 4.1.5 |
| $\Psi_{-D}$ | the elliptic curve ideal class pairing defined in Definition 3.1.7 |
| $\Omega_r$ | the volume of the unit ball in $\mathbb{R}^r$ |
| $\mathcal{B}$ | a set of $r$ linearly independent points in $\Lambda$ |
| $B(R)$ | the closed ball in $\mathbb{R}^r$ or radius $R$ centered at the origin |
| $\mathbb{C}$ | the complex numbers |
| $\mathrm{CL}(K)$ | the class group of a global field $K$ |
| $\mathrm{CL}^+(K)$ | the narrow class group of a real quadratic number field $K$ |
| $\mathrm{CL}_{\mathrm{div}}(K)$ | the divisor class group of an algebraic function field $K$ |
| $\mathrm{CL}^0_{\mathrm{div}}(K)$ | the subgroup of divisor classes of degree 0 of $\mathrm{CL}_{\mathrm{div}}(K)$ |
| $c(E,\mathcal{B})$ | the constant defined on page 38 |
| $\mathrm{char}(K)$ | the characteristic of $K$ |
| $\mathrm{Div}(K)$ | the group of divisors of an algebraic function field $K$ |
| $\mathrm{Div}^0(K)$ | the subgroup of divisors of degree 0 of $\mathrm{Div}(K)$ |
| $\deg(\cdot)$ | the degree of a divisor (class) or polynomial |
| $\det(M)$ | the determinant of the matrix $M$ |
| $E$ | an elliptic curve |
| $E(\mathbb{Q})_{\mathrm{tors}}$ | the torsion subgroup of $E(\mathbb{Q})$ |
| $\mathbb{F}_q$ | the finite field with $q$ elements |
| $\mathrm{GL}_2(\mathbb{Z})$ | the general linear group of degree 2 over $\mathbb{Z}$ |
| $g$ | the genus of a function field |
| $h$ | the absolute logarithmic height |
| $\hat{h}$ | the canonical height on $E$ |
| $h_K$ | the class number of a global field $K$ |
| $h^I_K$ | the ideal class number of a global function field |
| $h_x$ | the (Weil) height on $E$ (corresponding to $x : E \to \mathbb{P}^1$) |
| $\mathcal{I}_K$ | for a global function field $K$, the ideal class group of $\mathcal{O}_K$ |
| $J(C)$ | the Jacobian of a curve $C$ |
| $j$ | the $j$-invariant of $E$ |
| $K$ | a field |
| $K^*$ | the unit group of $K$ |
| $\overline{K}$ | an algebraic closure of $K$ |
| $K^{\mathrm{sep}}$ | the separable closure of $K$ in $\overline{K}$ |
| $K_v$ | the completion of $K$ at the prime $v$ |
| $K(C)$ | the function field of an irreducible smooth curve $C$ |
| $K_1K_2$ | the compositum of two fields $K_1$ and $K_2$ |

| | |
|---|---|
| $k$ | a field |
| $\widetilde{k}$ | the constant field of an algebraic function field $K/k$ |
| $\mathscr{L}(D)$ | the Riemann-Roch space associated to a divisor $D \in \mathrm{Div}(K)$ |
| $L(t)$ | the $L$-polynomial of a global function field |
| $M_K$ | the set of primes of a global field $K$ defined in Definition 1.5.2 |
| $n_v$ | the local degree of a global field $K$ at a valuation $v$ |
| $\mathcal{O}$ | the point at infinity on $E$ |
| $\mathcal{O}_K$ | the ring of integers of a global field $K$ |
| $\mathcal{O}_P$ | the valuation ring corresponding to a place $P$ of a field $K$ |
| $\mathcal{O}_v$ | the valuation ring corresponding to a prime $v$ of a field $K$ |
| $\mathbb{P}_K$ | the set of places on a global function field $K$ |
| $\mathbb{P}^n(K)$ | $n$-dimensional projective space over $K$ |
| $\mathrm{Princ}(K)$ | the group of principal divisors of $K$ |
| $p$ | a prime number unequal to 2 or 3 |
| $\mathfrak{p}$ | an irreducible monic polynomial in $\mathbb{F}_q[T]$ |
| $\mathbb{Q}$ | the rational numbers |
| $\mathcal{Q}_D$ | the form class group for forms with discriminant $D$ |
| $q$ | a power of $p$ |
| $\mathbb{R}$ | the real numbers |
| $\mathfrak{R}$ | the rational subfield of a global field |
| $R_{\mathfrak{R}}(E)$ | the regulator of $E/\mathfrak{R}$ |
| $R_{\mathfrak{R}}(E, \mathcal{B})$ | the $\mathcal{B}$-regulator of $E/\mathfrak{R}$ as defined on page 38 |
| $\mathrm{Re}(s)$ | the real part of an element $s \in \mathbb{C}$ |
| $r$ | the rank of $E$ |
| $S$ | for a global function field, the set of primes at infinity |
| $\mathrm{SL}_2(\mathbb{Z})$ | the special linear group of degree 2 over $\mathbb{Z}$ |
| $T$ | a fixed element in a global field $K/\mathbb{F}_q$ transcendental over $\mathbb{F}_q$ |
| $\mathcal{T}$ | the Tate curve |
| $\mathrm{Vol}(U)$ | the volume of a subset $U \subset \mathbb{R}^r$ |
| $v_{\mathfrak{p}}$ | the $\mathfrak{p}$-valuation on $\mathbb{F}_q(T)$ |
| $v_\infty$ | the degree valuation on $\mathbb{F}_q(T)$ or the prime of $\mathbb{F}_q(T)$ corresponding to it |
| $x$ | the morphism $x : E \to \mathbb{P}^1$ defined in (2.2.2) |
| $\widetilde{x}$ | the map $\widetilde{x} : E \to \mathbb{R}$ defined in Theorem 2.4.8 |
| $(x)$ | the principal divisor corresponding to an element $x \in K$ |
| $\mathbb{Z}$ | the integers |
| $Z(t)$ | the Zeta-function of a global function field |

# Index