Bayerische
Julius-Maximilians-Universität
Würzburg

Distribution of Squares in Arithmetic Progressions over Number Fields

Diplomarbeit
von
Matthias Waldherr

Betreuer: Prof. Dr. Jörn Steuding

November 2008

Contents

Introduction

"Distribution of Squares in Arithmetic Progressions over Number Fields" – two objects appear in the title of this thesis that are fundamentally different in their number theoretical nature. On the one hand, we have arithmetic progressions – a sequence of numbers obtained by repeatedly adding the same number to its predecessor. Therefore, arithmetic progressions are objects carrying an additive structure. On the other hand, squares are purely multiplicative objects.

In general, whenever one considers the interplay of addition and multiplication many questions arise that turn out to be very hard. This is illustrated by the fact that various conjectures in number theory that have resisted proof for a very long time do combine additive and multiplicative structures. Goldbach's problem or the twin prime conjecture are prominent examples.

If we stick to arithmetic progressions as the additive object and combine it with some multiplicative object or set $\mathcal{S}$, it becomes natural to ask the following questions:

Question 1: What is the maximal length of an arithmetic progression in $\mathcal{S}$?
In more mathematical terms this amounts to the following task: Determine the largest n such that there exist q and d with the property that $d, q+d, 2q+d, 3q+d, \ldots, nq+d$ are elements of $\mathcal{S}$.

Question 2: How are the elements of $\mathcal{S}$ distributed among or in arithmetic progressions?
For instance, this includes questions on how often elements of $\mathcal{S}$ occur in an arithmetic progression $(qn+d)_{n\in\mathbb{N}}$. If they occur finitely many often, one can pose the question for an explicit bound on the number of elements of $\mathcal{S}$ lying in the arithmetic progression. If they occur infinitely many often, one may wish to determine the density or the relative number of occurrences of elements from $\mathcal{S}$ in a specific arithmetic progression $(qn+d)_{n\in\mathbb{N}}$.
Furthermore, one can ask whether the distribution of elements of $\mathcal{S}$ in an arithmetic progression $(qn+d)_{n\in\mathbb{N}}$ is independent of the choice of q and d. If this is not the case, the questions arises how we can classify the distribution by properties of q and d.

These questions were probably asked for the first time in history in the context where $\mathcal{S}$ is the set of prime numbers, and their answers are now famous theorems. For example, the answer to the first question is given by the following theorem.

Theorem. *There are arbitrarily long progressions of primes.*

This is a result due to Ben Green and Terence Tao that has only been proved in 2004. In order to measure the significance of this work it suffices to mention that Terence Tao received the Fields Medal in 2006 partly also for his contribution to this theorem.

The second question on the distribution of primes in arithmetic progression has already been studied in the 19th century. The first progress in this direction was made by Dirichlet.

Theorem. *Let q and d be coprime natural numbers. Then there are infinitely many primes contained in the arithmetic progression $(qn+d)_{n\in\mathbb{N}}$.*

When Dirichlet proved this result in 1837, he revolutionized number theory by the introduction of analytical methods – such as L-functions and characters. The importance of this result can be described by noting that Dirichlet's theorem marked the birth of analytical number theory.

Further research finally culminated in the complete resolution of the distribution of primes in arithmetic progressions.

Theorem (Prime number theorem for arithmetic progressions)**.** *Let q and d be in natural numbers.*

1. *If q and d are not coprime, then there is at most one prime in $(qn+d)_{n\in\mathbb{N}}$.*
2. *If q and d are coprime, then the distribution of primes in $(qn+d)_{n\in\mathbb{N}}$ is given by the following formula*

$$|\{p \leq x | p \text{ prime and } p = qn+d \text{ for some } n \in \mathbb{N}\}| \sim \frac{1}{\varphi(q)}\pi(x),$$

where π is the prime counting function.

These advances in number theory that have been stimulated by the study of primes in arithmetic progressions may serve as a motivation to consider as well other multiplicative sets $\mathcal{S}$ and their interaction with arithmetic progressions. In fact, in this thesis we will be concerned with the case where $\mathcal{S}$ is the set of squares in a number field K. Before getting down to the topic of this thesis, we give an overview over the yet existing results.

It has long been known that three-term arithmetic progressions of rational squares indeed do exist, for example $1, 25, 49$ or $49, 169, 289$. Then, the first question is answered satisfactorily by the following theorem of Fermat:

Theorem (Fermat)**.** *There are no four rational squares in arithmetic progression.*

The second question about the distribution of squares in arithmetic progressions is much more involved. It can be proved that for any $q, d \in \mathbb{Z}$

$$|\{n \leq N | qn + d = x^2 \text{ for some } x \in \mathbb{Q}\}| = O(\sqrt{N}).$$

The implicit constant in this result, however, does depend on q and d. A far-reaching generalization was then proposed by Rudin in [Rud60], who conjectured a uniform version of this result.

Conjecture (Rudin's conjecture)**.** *For $q, d \in \mathbb{Z}$*

$$|\{n \leq N | qn + d = x^2 \textit{ for some } x \in \mathbb{Q}\}| = O(\sqrt{N}),$$

where the implicit constant does not depend on q and d.

This conjecture is still unproven but some partial answers have been found. Each of them depends on a deep result in some other area of mathematics. The first progress in this direction was achieved by Szemeredi in his 1974 paper [Sze74]. Using his celebrated theorem on arithmetic progressions he was able to show that

$$|\{n \leq N | qn + d = x^2 \text{ for some } x \in \mathbb{Q}\}| = o(N)$$

holds uniformly in q and d. In 1992 a significant improvement was obtained by Bombieri, Granville and Pintz in [BGP92]. They showed

$$|\{n \leq N | qn + d = x^2 \text{ for some } x \in \mathbb{Q}\}| = O(N^{\frac{2}{3}} \log^c N)$$

uniformly in q and d. The core of their argument is the application of a variant of the theorem of Faltings on rational points on algebraic curves. Finally, the latest improvement from 2002 is due to Bombieri and Zannier [ZB02]:

Theorem. *For $q, d \in \mathbb{Z}$,*

$$|\{n \leq N | qn + d = x^2 \textit{ for some } x \in \mathbb{Q}\}| = O(N^{\frac{3}{5}} \log^c N),$$

where c is some explicit constant, and the implicit constant does not depend on q and d.

This diploma thesis ties up to these results. We do not attempt to further improve the bounds given in the above theorem. We rather analyze the methods employed in the proofs of the results above in order to figure out whether these methods are applicable in more general situations.

Our aim is to generalize these results to the case of number fields. More precisely, given a number field K and $q, d \in \mathbb{Z}$ we look for a bound for the size of the set

$$\{n \leq N | qn + d = x^2 \text{ for some } x \in K\},$$

which does not depend on q and d.

Unfortunately, we were not able to adapt the method used by Bombieri and Zannier to the number field case. So we cannot hope that the theorem of Bombieri and Zannier is a direct consequence of our results. However, the methods applied by Bombieri, Granville and Pintz do admit a partial generalization to the case of number fields, and we succeeded in proving bounds similar to those in their theorem for a certain family of number fields.

We now briefly describe the organization of this thesis: In chapter 1 we present technical preliminaries from different branches of mathematics that are needed for the later chapters. In chapter 2 we state our two main theorems and explain the strategy of proof in detail. The proof of the first theorem is divided into two cases. The first case is treated in chapter 3, while the second one occupies chapter 4, 5 and 6. In chapter 7 we prove our second main result. We conclude with chapter 8, where we discuss open problems and further generalizations.

Notations

We try to use only standard notation. However, in order to explain what ”standard” means for us and in order to introduce some naming conventions, which we use throughout this thesis, we include this brief summary of symbols and conventions.

We use the symbols $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ to denote the natural numbers, the integers, the rational, the real and the complex numbers respectively.

Number fields are denoted by K. By $K^\times$ we mean the non-zero elements of K, and we write $K^{\times 2}$ for the set of non-zero squares in K. The ring of integers of a number field K is denoted by $\mathcal{O}_K$.

For a ring R the symbol $R^\times$ stands for the set of invertible elements of R. By $R[X_0, \dots, X_n]$ we mean the ring of polynomials in the variables $X_0, \dots, X_n$ over some ring(field) R. In general, the capital letters $X_0, \dots, X_n$ will represent variables, whereas the lower case letters $x_0, \dots, x_n$ refer to concrete elements of the ring(field), which are substituted into the corresponding upper case letters.

The letters i, j, k, m, n, l and M, N are reserved for natural numbers. We use the letter p to indicate a prime number or a prime element of some ring. Prime ideals will be denoted by $\mathfrak{p}$.

By q and d we usually refer to rational numbers or integers which specify an arithmetic progression. When referring to q and d, we have in mind the arithmetic progression $(qn+d)_{n\in\mathbb{N}}$. In this case we implicitly assume that q and d are non-zero.

The letters λ, κ, μ stand for real positive constants. We also use c, c', c_1, c_2 to denote positive constants. Note that in this case these symbols might appear in many results of this thesis, where they, however, need not represent the same value.

By ν, ω we usually refer to places of some number field.

The n-dimensional projective space over some field is denoted by $\mathbb{P}^n$. It will always be clear from the context what the underlying field is. When talking about elements of $\mathbb{P}^n$ in terms of homogenous coordinates we write them as $(x_0 : \ldots : x_n)$. For $(x_0 : \ldots : x_n)$ we write $\mathbf{x}$ for short. If we consider points in the projective space but do not explicitly use homogenous coordinates, we use the letters P or Q.

Varieties are usually denoted by V, curves by the letter C and elliptic curves by the letter E. In order to distinguish the points on two varieties in the case when we are dealing with a map between two varieties $\phi : V_1 \to V_2$, we denote the points on V_1 by P and those on V_2 by Q.

Theorems, propositions and lemmas are numbered by section and then in progressive order. The numbering restarts in every chapter. When referencing to a result inside of the same chapter we only use two numbers indicating the section and the running number inside of the section. If we refer to a statement outside of the current chapter we use three numbers. The first one indicates the chapter and the second and third one refer to the section and the running number inside of the section.

Chapter 1

Preliminaries

In this chapter we introduce definitions and results we need for the main part of this thesis. Since we use results from several different areas of mathematics, a thorough exposition of every single area would make this preliminary chapter very lengthy. Therefore, we drop the wish to make this thesis self-contained. Instead, we treat the particular fields rather informally and concentrate only on those aspects which are essential for the later chapters. To compensate this lack of formality, we give references for the in-depth treatment of the particular theory.

Furthermore, we skip those proofs that are also available in the literature. In those cases, however, where we were not able to find a suitable reference we do provide the proofs, but we do not claim originality for any result stated in this chapter.

1 Classical number theory

Two prominent number theoretical functions are of some importance in this thesis: The ω-function and the π-function. We briefly review their definition and study their asymptotic behavior.

Let R be a unique factorization domain. We define the function $\omega_R : R \to \mathbb{N}$ by

$$\omega_R(r) = |\{ \text{ distinct prime factors of } r \text{ up to units}\}|.$$

For $\omega_{\mathbb{Z}}$ we simply write ω.

The asymptotic behavior of the ω-function is well known (See [HW79], 22.10). However, we later encounter the problem to determine the average size of an expression where the ω-function occurs in the exponent. The statement of the following lemma already appears in [BGP92] but the authors neither prove this result nor refer to the literature. We present a proof of this particular result since we were not able to find a reference for it either.

Lemma 1.1. *Let $u \geq 1$. Then, for $x \to \infty$,*

$$\sum_{n \leq x} u^{\omega(n)} = O(x \log^u x).$$

Proof:
For any $n_1, n_2 \in \mathbb{N}$ the ω-function satisfies the following relation

$$\omega(n_1 n_2) \leq \omega(n_1) + \omega(n_2).$$

Using this property, we now manipulate $\sum_{n \leq x} u^{\omega(n)}$ in the following way:

$$\sum_{n \leq x} u^{\omega(n)} \leq x \sum_{n \leq x} \frac{u^{\omega(n)}}{n} \leq x \prod_{p \leq x} \sum_{k=0}^{\lfloor \log x \rfloor} \frac{u^{\omega(p^k)}}{p^k} \leq x e^{\sum_{p \leq x} \log\left(\sum_{k=0}^{\lfloor \log x \rfloor} \frac{u^{\omega(p^k)}}{p^k}\right)}$$

The exponent can be examined more closely. At first, we split up the interior sum and use that $\omega(p^k) = 1$ for any prime p and any $k \geq 1$. Then, by using Taylor expansion, we obtain

$$\sum_{p \leq x} \log\left(\sum_{k=0}^{\lfloor \log x \rfloor} \frac{u^{\omega(p^k)}}{p^k}\right) = \sum_{p \leq x} \log\left(1 + \sum_{k=1}^{\lfloor \log x \rfloor} \frac{u}{p^k}\right) \leq \sum_{p \leq x} \sum_{k=1}^{\lfloor \log x \rfloor} \frac{u}{p^k}.$$

We write

$$\sum_{p \leq x} \sum_{k=1}^{\lfloor \log x \rfloor} \frac{u}{p^k} = u \sum_{p \leq x} \frac{1}{p} + u \sum_{p \leq x} \sum_{k=2}^{\lfloor \log x \rfloor} \frac{1}{p^k}$$

and investigate both summands separately.

For the first summand we get

$$\sum_{p \leq x} \frac{1}{p} \leq \log\log x + c$$

with a suitable constant c from [HW79], 22.7, theorem 427. For the second one we extend both summations to infinity and obtain

$$\sum_{p \leq x} \sum_{k=2}^{\lfloor \log x \rfloor} \frac{1}{p^k} < \sum_{n=2}^{\infty} \sum_{k=2}^{\infty} \frac{1}{n^k} = \sum_{n=2}^{\infty} \left(\frac{1}{1 - \frac{1}{n}} - \frac{1}{n} - 1\right) = \sum_{n=2}^{\infty} \left(\frac{1}{n-1} - \frac{1}{n}\right) = 1.$$

Recombining the summands again, we conclude

$$\sum_{n \leq x} u^{\omega(n)} \leq x e^{u(1 + c + \log\log x)} \leq x e^{u + uc} e^{u \log\log x} = c' x e^{\log\log^u x} = c' x \log^u x$$

if we choose $c' = e^{u+uc}$. □

We now come to the prime counting function $\pi : \mathbb{R} \to \mathbb{N}$, which is defined by

$$\pi(x) = |\{p \leq x | p \text{ is prime}\}|$$

The asymptotic behavior of π is described in the following well-known theorem.

Theorem 1.2 (Prime number theorem)**.**

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1.$$

Proof:
See [HW79], chapter 1, theorem 6. The proof is given in chapter 22. □

2 The large sieve

In this thesis need some results from sieve theory, however, we do not require significant knowledge of this subject. The main theorem of the large sieve can be stated without having to go deeper into the theory, and so we use this theorem as a black-box result. For a full account of sieve theory see for example the textbook [CM06]. The following variant of the main theorem of the large sieve appears in [Dav00].

Theorem 2.1 (Main theorem of the large sieve)**.** *Let $\mathcal{S}$ be a set of integers with $\mathcal{S} \subseteq [1, N]$ for some $N \in \mathbb{N}$. Let further $\mathcal{P}$ be a set of primes and let M be a natural number.*
Suppose that all primes in $\mathcal{P}$ are less than or equal to M and that there exists some $0 < \tau < 1$ such that for any $p \in \mathcal{P}$ at least τp of the residue classes $n + p\mathbb{Z}$ have empty intersection with $\mathcal{S}$. Then

$$|\mathcal{S}| \leq \frac{N + 3M^2}{\tau|\mathcal{P}|}.$$

Proof:
See [Dav00], chapter 27, theorem 3. □

3 Number fields

We assume familiarity with the standard results from algebraic number theory and refer to [Neu07] for a comprehensive account of this topic. We, however, do recall some definitions and results of this theory in the first subsection but only to fix definitions and notations.

In the second subsection we present a not widely known construction in algebraic number theory due to [Kna92] which establishes the existence of a unique factorization domain R in every number field K with certain properties similar to those of the ring $\mathbb{Z}$. In a later part of this thesis it turns out to more convenient to work with this ring inside of a number field instead of using the ring of algebraic integers.

Finally, we introduce valuations on number fields and heights of points in projective space.

3.1 Algebraic integers, decomposition into prime ideals and the Chebotarev density theorem

A number field K is a finite field extension of $\mathbb{Q}$. An analogue to the rational integers $\mathbb{Z}$ in a number field K is the ring of **algebraic integers**:

$$\mathcal{O}_K = \{x \in K | f(x) = 0 \text{ for a monic polynomial } f(X) \in \mathbb{Z}[X]\}.$$

Some fundamental properties of $\mathcal{O}_K$ are summarized in the next proposition.

Proposition 3.1. *Let K be a number field. Then the following statements about $\mathcal{O}_K$ hold.*

i) $\mathcal{O}_K$ is a subring of K.

ii) K is the quotient field of $\mathcal{O}_K$.

iii) The following diagram of embeddings is commutative.

$$\begin{tikzcd}
\mathbb{Q} \arrow[r] & K \\
\mathbb{Z} \arrow[r] \arrow[u] & \mathcal{O}_K \arrow[u]
\end{tikzcd}$$

iv) The group of units of $\mathcal{O}_K$ is finitely generated.

Proof:
See [Neu07], chapter I, proposition 2.2 for the first statement. The second and third statement are easy consequences of the definition. The fourth assertion is proved in [Neu07], chapter I, theorem 7.4. □

Although $\mathcal{O}_K$ shares many properties with $\mathbb{Z}$, there are also significant differences to the ring of rational integers. The most striking one is maybe the fact that $\mathcal{O}_K$ may fail to be a unique factorization domain.

While elements of $\mathcal{O}_K$ may not have unique factorization into prime elements, ideals do uniquely decompose into prime ideals. That means, given some ideal $\mathfrak{i}$ of $\mathcal{O}_K$, there is a decomposition of $\mathfrak{i}$ into prime ideals $\mathfrak{p}_i$ of the following type

$$\mathfrak{i} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n},$$

where $e_i \in \mathbb{N}_0$. This decomposition is uniquely determined up to the order of the factors.

The case, when $\mathfrak{i}$ is the ideal generated by some rational prime, is of special interest. Note that the ideal generated by a rational prime is a prime ideal in $\mathbb{Z}$ but not necessarily in $\mathcal{O}_K$. Consider a prime $p \in \mathbb{Z}$ and its decomposition into prime ideals

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$$

in $\mathcal{O}_K$. A prime ideal $\mathfrak{p}$ that occurs in this decomposition of $p\mathcal{O}_K$ is said to **lie above** p. In this case it holds $p\mathbb{Z} = \mathbb{Z} \cap \mathfrak{p}$, and we have the following commuting diagram

$$\begin{tikzcd}
\mathbb{Z} \arrow[r] \arrow[d] & \mathcal{O}_K \arrow[d] \\
\mathbb{Z}/p\mathbb{Z} \arrow[r] & \mathcal{O}_K/\mathfrak{p}
\end{tikzcd}$$

where the vertical maps are projections and the horizontal maps are embeddings. Furthermore, $\mathbb{Z}/p\mathbb{Z}$ and $\mathcal{O}_K/\mathfrak{p}$ are both fields, and the field extension induced by the embedding $\mathbb{Z}/p\mathbb{Z} \to \mathcal{O}_K/\mathfrak{p}$ is finite. This allows the following definitions:

Let $p \in \mathbb{Z}$ be a prime having the following decomposition

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$$

into prime ideals over $\mathcal{O}_K$. Then the exponents e_i are called **ramification indices** and the degree of the extension $\mathcal{O}_K/\mathfrak{p}_i|\mathbb{Z}/p\mathbb{Z}$ is called **inertia degree** and is denoted by f_i. These quantities are connected as follows.

Proposition 3.2 (The fundamental equality)**.** *Let K be a number field. Let p be a prime in $\mathbb{Z}$ and let*

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$$

be its decomposition in $\mathcal{O}_K$. Then

$$\sum_{i=1}^{n} e_i f_i = [K : \mathbb{Q}].$$

Proof:
See [Neu07], chapter I, proposition 8.2. □

The next question that can be asked about the decomposition of primes is the following: For "how many" primes occurs a certain "type of decomposition"? In the case when K is Galois over $\mathbb{Q}$, this question is answered by the Chebotarav density theorem. However, the statement of this theorem is quite complicated because it involves some technical notions. Since we do not need the general framework of Chebotarav's density theorem in the course of this thesis, we settle for the answer only in a very special case, which, however, suffices for our purposes.

Definition. Let K be a number field. A rational prime p is called **completely split over** K if it holds

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$$

with $n = [K : \mathbb{Q}]$ and (therefore) $e_i = f_i = 1$.

In this case the Chebotarev density theorem implies the following theorem.

Theorem 3.3. *Let K be a number field which is Galois over $\mathbb{Q}$. Then*

$$\frac{|\{p \leq N | p \text{ is prime and splits completely over } K\}|}{|\{p \leq N | p \text{ is prime}\}|} \overset{N\to\infty}{\longrightarrow} \frac{1}{[K : \mathbb{Q}]}.$$

Proof:
This is corollary 13.6 in chapter VII of [Neu07]. □

3.2 Unique factorization in number fields

We already noted that we cannot expect to have unique factorization in the ring of integers $\mathcal{O}_K$ for every number field K. In fact, it is even possible to measure to what extent $\mathcal{O}_K$ fails to be a unique factorization domain. We briefly explain how this can be done.

Let K be a number field. A subset of $\mathcal{O}_K$ is called a **fractional (principal) ideal** if is of the form xI for some $x \in K^\times$ and some (principal) ideal I of $\mathcal{O}_K$. It can be shown that the set of all fractional ideals carries the structure of a commutative group with the group law given by the multiplication of ideals. Furthermore, the set of fractional principal ideals forms a normal subgroup. The resulting quotient group is called the **ideal class group** Cl_K, and its elements are called **ideal classes**. Now we have the following result.

$$\mathrm{Cl}_K \text{ is trivial} \iff \mathcal{O}_K \text{ is a unique factorization domain}$$

This shows that the size of Cl_K can be seen as an indicator of how far $\mathcal{O}_K$ is away from being a unique factorization domain. Hence, the order of Cl_K is an important parameter associated to a number field. It is called the **class number** and is denoted by h_K. One can show that h_K is finite for any number field K.

Since $\mathcal{O}_K$, in general, does not have unique factorization, the question comes up, whether there are other rings inside of K, which in contrast to $\mathcal{O}_K$ are unique factorization domains. Of course, this approach can only be useful if these rings reflect in some sense arithmetical properties of K in a way like $\mathcal{O}_K$ does.

It is indeed possible to construct such rings and we show how this construction can be carried out. The main role is played by the technique of localizing rings at multiplicative sets. This is a method similar to the construction of the quotient field with the single exception that only the elements of a certain set are made invertible, and not all non-zero elements of the ring. The formal definition is as follows:

Let S be a multiplicative set of a ring R, i.e. $1 \in S$, $0 \notin S$ and S is multiplicatively closed. We define an addition and a multiplication on the (formal) fractions $\frac{r}{s}$ with $r \in R$ and $s \in S$ by

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}, \qquad \frac{r_1}{s_1}\frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}.$$

Additionally, we define an equivalence relation on these formal fractions by

$$\frac{r_1}{s_1} \sim \frac{r_2}{s_2} \text{ if and only if } r_1 s_2 - r_2 s_1 = 0.$$

It is possible to demonstrate that addition and multiplication are compatible with this equivalence relation. Moreover, the set of equivalence classes of these formal fractions forms a ring R_S. The ring R_S is called the **localization** of R at S. The ring R itself can be seen as a subring of R_S by identifying $r \in R$ with $\frac{r}{1}$.

The next proposition shows that localizing $\mathcal{O}_K$ by a suitable multiplicative set yields a unique factorization domain which shares important properties with $\mathcal{O}_K$.

Proposition 3.4. *Let K be a number field and let $\mathcal{O}_K$ be its ring of integers. Let h_K be the class number of K and let $s_1, \dots, s_{h_K}$ be nonzero elements each representing an ideal class in Cl_K. Set $s = s_1 \dots s_h$ and define*

$$S = \{1, s, s^2, \dots\}.$$

We write R for the localization of $\mathcal{O}_K$ by S. Then the following statements hold.

1. *K is the quotient field of R.*
2. *R is a principal ideal domain.*
3. *$R^\times$ is finitely generated.*

Proof:
This is theorem 4.10 in [Kna92] on page 94. The proof is given on page 127. □

As in the case of algebraic integers we are interested in the behavior of primes $p \in \mathbb{Z}$ in the larger ring R. Our goal is to determine how ω_R behaves on $\mathbb{Z}$. We first recall a lemma form commutative algebra.

Lemma 3.5. *Let R be a ring, S a multiplicative set and R_S the localization of R at S. Then the maps*

$$\begin{aligned} R_S \to R: &\qquad I \mapsto I \cap R \\ R \to R_S: &\qquad I \mapsto IR \end{aligned}$$

give a one-to-one correspondence between the prime ideals of R_S and the prime ideals of R not intersecting S.

Proof:
See [Eis95], chapter 2, proposition 2.2. □

The next proposition shows that any prime $p \in \mathbb{Z}$ decomposes into at most $[K : \mathbb{Q}]$ different primes in R, where R is the unique factorization domain from proposition 3.4.

Proposition 3.6. *Let K be a number field and let R be constructed like in the proposition above. Then for any prime $p \in \mathbb{Z}$,*

$$\omega_R(p) \le [K : \mathbb{Q}].$$

Proof:
The statement is obvious if p is a unit in R. So, suppose that p is not invertible in R. Consider the decomposition of p into prime ideals $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ over $\mathcal{O}_K$. Then it holds $pR = \mathfrak{p}_1 \cdots \mathfrak{p}_n R$.

Since p is not invertible, we have $pR \neq R$ and therefore $\mathfrak{p}_i R \neq R$ for at least one index i. We drop those indices with $\mathfrak{p}_i R = R$ and write

$$pR = \mathfrak{p}_{i_1} \cdots \mathfrak{p}_{i_k} R = \mathfrak{p}_{i_1} R \cdots \mathfrak{p}_{i_k} R.$$

This product of ideals is in fact a product of prime ideals by lemma 3.5. Since R is a principal ideal domain, all ideals $\mathfrak{p}_{i_1} R, \ldots, \mathfrak{p}_{i_k} R$ are generated by some primes $p_{i_1}, \ldots, p_{i_k} \in R$. We obtain

$$pR = p_{i_1} \cdots p_{i_k} R$$

and this in turn implies $p = up_{i_1} \cdots p_{i_k}$ with some unit $u \in R^\times$. Thus, we have found a decomposition of p into at most n different primes in R. The proposition is proved because $n \leq [K : \mathbb{Q}]$ by proposition 3.2. □

Assembling all these results together, we obtain the following theorem.

Theorem 3.7. *Let K be a number field. Then there exists a unique factorization domain R with the following properties.*

1. *K is the quotient field of R.*
2. *$R^\times$ is finitely generated.*
3. *$\omega_R(n) \leq [K : \mathbb{Q}]\omega(n)$ for all $n \in \mathbb{N}$.*

□

4 Valuations and heights

We review the basic properties of valuations on fields. Furthermore, we introduce the notion of the height of a point in projective space. This short exposition is extracted from the first chapter in [BG06].

4.1 Valuations

A **valuation** $|\ |$ on a field K is a function $|\ | : K \to \mathbb{R}$ that satisfies the following three properties.

1. $|x| \geq 0$ and $|x| = 0$ if and only if $x = 0$.
2. $|xy| = |x||y|$ for all $x, y \in K$.
3. $|x + y| \leq |x| + |y|$ for all $x, y \in K$.

A valuation is called **non-archimedean** if the following strengthening of the triangle inequality is satisfied.

3'. $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in K$

In this case we even have $|x+y| = \max\{|x|, |y|\}$ if $|x| \neq |y|$. Valuations that do not satisfy the strong triangle inequality are called **archimedean**.

Every valuation of a field K defines a metric on K by setting $d(x, y) = |x - y|$, and this metric induces a topology. Two valuations on K are called **equivalent** if they induce the same topology on K. The equivalence classes corresponding to this relation are called **places**.

The following theorem classifies all possible places on $\mathbb{Q}$.

Theorem 4.1. *Let $|\ |$ be a valuation on $\mathbb{Q}$ and suppose that it is not trivial (i.e $|x| = 1$ for all $x \in \mathbb{Q}^\times$ and $|x| = 0$).*

1. *If $|\ |$ is archimedean, then $|\ |$ is equivalent to the ordinary absolute value.*
2. *If $|\ |$ is non-archimedean, then there exists a prime p, such that $|\ |$ is equivalent to the p-adic valuation.*

Proof:
See [Neu07], chapter 2, proposition 3.9. □

The topologies induced by two valuations belonging to the same place do coincide by definition. For many applications, however, it is reasonable to choose distinguished representatives. For the places on $\mathbb{Q}$ we do this as follows.

For the representative $|\ |_\infty$ for the archimedean place we choose the ordinary absolute value. The representative $|\ |_p$ for the p-adic place is defined by

$$|x|_p = p^{-r}$$

for any non-zero $x \in \mathbb{Q}$ written as $x = \frac{a}{b}p^r$ with $p \nmid a, b$.

This choice of representatives for the places of $\mathbb{Q}$ has the property that all places of $\mathbb{Q}$ are connected by the **product formula**: For for any non-zero $x \in \mathbb{Q}$

$$\prod_{\nu} |x|_{\nu} = 1,$$

where the product ranges over all places of $\mathbb{Q}$ and $|\ |_{\nu}$ is the distinguished representative for the place ν defined above. Note that in this product only finitely many factors attain a value different from 1.

We now turn to number fields. It is clear that any valuation on a number field K induces a valuation on $\mathbb{Q}$ by restriction. Let ω be a place on K and ν the place on $\mathbb{Q}$ such that the valuations of ω induce the same topology on $\mathbb{Q}$ as ν. Then we say that ω **lies above** ν and we write $\omega|\nu$.

Let K be a number field and ν a place of $\mathbb{Q}$. It can be proved that there exist $|K : \mathbb{Q}|$ different places of K lying above ν. Furthermore, it is possible to choose representatives $|\ |_{\omega}$ for every place ω of K in such a way that the following relations are satisfied.

i) The product formula holds in K: For any non-zero $x \in K$ we have

$$\prod_{\nu} |x|_{\nu} = 1,$$

where the product ranges over all places of K.

ii) Let ν be a place of $\mathbb{Q}$ and consider all valuations ω of a number field K lying above ν. Then for any $x \in \mathbb{Q}$ it holds

$$\prod_{\omega|\nu} |x|_{\omega} = |x|_{\nu}.$$

If not stated otherwise, we always assume that the valuations $|\ |_{\nu}$ corresponding to the places ν of a number field are chosen in such a way that these formulas hold.

4.2 Heights

Let K be a number field and let $\mathbf{x}$ be a point in the projective space $\mathbb{P}^n$ over K. The **height** of $\mathbf{x} = (x_1 : \ldots : x_n)$ is defined by

$$h(\mathbf{x}) = \sum_{\nu} \max_{i} \log |x_i|_{\nu},$$

where the sum ranges over all valuations of K.

Using the product formula, it can be proved that $h(\mathbf{x})$ is well defined, i.e. that it does not depend on the actual choice of the representative $(x_1 : \ldots : x_n)$ for $\mathbf{x}$.

If $\mathbf{x}$ has a representative whose coordinates are in $\mathbb{Q}$, it also has a representative with all coordinates being integers without common divisor. If $\mathbf{x} = (x_1 : \ldots : x_n)$ is such a representative, then

$$h(\mathbf{x}) = \max_i \log |x_i|_\infty .$$

We define the height of an element x of a number field K by identifying x with the point $(x : 1)$ in projective space $\mathbb{P}^2$. Then we obtain

$$h(x) = \sum_\nu \log^+ |x|_\nu ,$$

where the sum ranges over all valuations of K and $\log^+ = \max\{0, \log\}$. In the case where $x \in \mathbb{Q}$, we simply have $h(x) = \max\{\log |a|, |b|\}$ if $x = \frac{a}{b}$ and $\gcd(a, b) = 1$.

Let $f(X_0, \ldots, X_n) \in K[X_0, \ldots, X_n]$ be a polynomial. If

$$f(X_0, \ldots, X_n) = \sum_{i_0, \ldots, i_n} a_{i_0, \ldots, i_n} X_0^{i_0} \cdots X_n^{i_n},$$

then height of f is defined as

$$h(f) = \sum_\nu \max_{i_0, \ldots, i_n} \log |a_{i_0, \ldots, i_n}|_\nu ,$$

where the sum ranges over all valuations of K.

5 Algebraic varieties

We now introduce some basic concepts from algebraic geometry that are associated to algebraic varieties: the tangent space, the dimension of a variety, smoothness, the degree of a variety and maps on varieties. In later stages, however, we will not be concerned with the actual nature of these notions but only have to be able to calculate them. Therefore, we treat this topic very informally and restrict to what is necessary for the applications later in this thesis. In particular, we only consider projective varieties and we only work over the algebraic closures of number fields instead of algebraically closed fields in general.

The material for this section is adopted from the textbooks [Har92], [Per08] and [Sil86].

In this section K always denotes a number field and $\overline{K}$ a fixed algebraic closure of K. $\mathbb{P}^n$ denotes the n-dimensional projective space over $\overline{K}$.

The fundamental objects in algebraic geometry are algebraic sets. Loosely speaking, these are sets that occur as a zero locus of some family of polynomials. More formally, a **projective algebraic set** is a subset of $\mathbb{P}^n$ that can be written as

$$\{\mathbf{x} \in \mathbb{P}^n | f(\mathbf{x}) = 0 \text{ for all homogenous } f \in I\},$$

where I is some family of polynomials from $\overline{K}[X_0, \dots, X_n]$.

For a projective algebraic set V we define the **vanishing ideal** $I(V)$ to be the ideal of $\overline{K}[X_0, \dots, X_n]$ generated by the set

$$\{f \in \overline{K}[X_0, \dots, X_n] | f \text{ homogenous}, f(\mathbf{x}) = 0 \text{ for all } \mathbf{x} \in V\}.$$

A projective algebraic set is called a **projective variety** if its vanishing ideal is a prime ideal.

5.1 Tangent space, dimension and smoothness

Instead of using the algebraic closure $\overline{K}$, we could work over the field of complex numbers $\mathbb{C}$, which also contains K and is algebraically closed. From the geometrical point of view, algebraic varieties over $\mathbb{C}$ are just objects like curves, surfaces or hypersurfaces in projective space. The definition of the tangent space, the notion of smoothness or dimension then arise quite naturally.

For $\overline{K}$ or other algebraically closed fields it does also make sense to define these notions. However, then their formal definition is of algebraic rather than of geometric nature. Unfortunately, the exact definitions are rather complicated. Since it is more important for us to have a way to calculate the tangent space or check smoothness than to know the precise algebraic definitions, we omit the formal introduction of these notions.

However, it may be a bit unpleasant to work with undefined objects. In order to overcome this inconvenience we decided to turn things around and to use the subsequent propositions as the definitions for the respective objects. I.e. the tangent space is defined by the way how it can be calculated. The dimension is defined by a formula by which it can be computed. Finally, for the definition of smooth points we employ Jacobi's criterion.

At first, we describe the tangent space of a variety in one of its points.

Proposition 5.1. *Let V be a variety in $\mathbb{P}^n$ and $f_1(X_0, \ldots, X_n), \ldots, f_k(X_0, \ldots, X_n)$ be homogenous polynomials that generate the vanishing ideal of V. The* ***tangent space*** *in a point $\mathbf{x} = (x_0 : \ldots : x_n)$ is the zero locus of the polynomials*

$$\sum_{j=0}^{n} \frac{\partial f_i(X_0, \ldots, X_n)}{\partial X_j}(\mathbf{x}) X_j$$

for $i = 1, \ldots, k$.

Proof:
See [Har92], page 181 and 182. □

We observe that the tangent space is exactly the set of points $(x_0 : \ldots : x_n) \in \mathbb{P}^n$, such that $(x_0, \ldots, x_n)^T$ is an element of the kernel of following matrix.

$$\begin{pmatrix} \frac{f_1(X_0,\ldots,X_n)}{\partial X_0}(\mathbf{x}) & \cdots & \frac{f_1(X_0,\ldots,X_n)}{\partial X_n}(\mathbf{x}) \\ \vdots & & \vdots \\ \frac{f_k(X_0,\ldots,X_n)}{\partial X_0}(\mathbf{x}) & \cdots & \frac{f_k(X_0,\ldots,X_n)}{\partial X_n}(\mathbf{x}) \end{pmatrix}$$

There is a relation between the rank of this matrix $M_{\mathbf{x}}(V)$ and the (yet not defined) dimension of the variety V. One shows that $n - \text{rank} M_{\mathbf{x}}(V) \geq \dim V$ and that equality always occurs for some point $\mathbf{x}$ on V. This statement is expressed in the next proposition, which serves as the definition of the dimension of a variety as well.

Proposition 5.2. *Let V be a variety in $\mathbb{P}^n$. Then the* ***dimension*** *of V is given by the following formula.*

$$\dim V = \min_{\mathbf{x} \in V} \dim \ker M_{\mathbf{x}}(V) = n - \max_{\mathbf{x} \in V} \text{rank} M_{\mathbf{x}}(V)$$

Any point, for which equality occurs, is of particular interest and is called **smooth**. If every point of a variety is smooth, the variety itself is called **smooth**. The next proposition shows how we can determine whether this is the case.

Proposition 5.3 (Jacobi's Criterion)**.** *Let V be a variety in $\mathbb{P}^n$ and suppose that its vanishing ideal is generated by homogenous polynomials $f_1(X_0, \ldots, X_n), \ldots, f_k(X_0, \ldots, X_n)$. Then V is smooth a point $\mathbf{x} = (x_0 : \ldots : x_n)$ if the Jacobi matrix*

$$\begin{pmatrix} \frac{f_1(X_0,\ldots,X_n)}{\partial X_0}(\mathbf{x}) & \cdots & \frac{f_1(X_0,\ldots,X_n)}{\partial X_n}(\mathbf{x}) \\ \vdots & & \vdots \\ \frac{f_k(X_0,\ldots,X_n)}{\partial X_0}(\mathbf{x}) & \cdots & \frac{f_k(X_0,\ldots,X_n)}{\partial X_n}(\mathbf{x}) \end{pmatrix}$$

has rank (at least) $n - \dim V$.

Proof:
See [Per08], chapter V, proposition 2.6. □

5.2 The degree of a variety

Another important property of a variety V is its degree, which we denote by $\deg V$. Again, we omit the formal definition and refer to [Har92], chapter 18, as the source for a proper definition. We settle for calculating the degree in some special cases.

Proposition 5.4. *Let V be a variety in $\mathbb{P}^n$.*

1. *If V is a finite set, then $\deg V = |V|$.*
2. *If V is a hyperplane, i.e. V is the zero locus of a single homogenous linear polynomial, then $\deg V = 1$.*

Proof:
See [Har92], page 224 and 225. □

The following theorem turns out to be particularly useful for calculating the degree of certain varieties.

Theorem 5.5 (Bezout's Theorem)**.** *Let V_1 and V_2 be varieties in $\mathbb{P}^n$ and suppose that $\dim V_1 + \dim V_2 \geq n$. Furthermore, assume that the tangent spaces of V_1 and V_2 in every point of the intersection $V_1 \cap V_2$ span $\mathbb{P}^n$. Then*

$$\deg(V_1 \cap V_2) = \deg V_1 \deg V_2.$$

If $\dim V_1 + \dim V_2 = n$, then $V_1 \cap V_2$ is finite.

Proof:
See [Har92], page 227. □

5.3 Functions on varieties and the local ring

After having defined fundamental properties of varieties we turn to functions defined on varieties. Of course, we do not consider arbitrary functions on varieties but only those which are in some sense "natural functions". The definitions are taken from [Sil86] chapter I section 2.

Definition. Let V be a variety in $\mathbb{P}^n$. A **rational function** f on a variety is a equivalence class of the set

$$\left\{ \frac{p_1}{p_2} \middle| p_1, p_2 \in \overline{K}[X_0, \ldots, X_n] \text{ homogenous of the same degree and } p_2 \notin I(V) \right\}$$

with respect to the equivalence relation given by

$$\frac{p_1}{p_2} \sim \frac{p_1'}{p_2'} \text{ if and only if } p_1 p_2' - p_1' p_2 = 0.$$

The set of all rational functions on V is called the **rational function field** of V. We denote it by $\overline{K}(V)$. In fact, rational functions on V are not functions in the classical sense. This is due to the fact that it may not be possible to evaluate a rational function f at certain points of V, so that f does not represent a function $f : V \to \overline{K}$ defined at all points of V.

Definition. Let V be a variety and let $\mathbf{x} = (x_0 : \ldots : x_n)$ be a point lying on V. A rational function f on V is called **regular** at $\mathbf{x}$ if there exists a representative of f of the form $\frac{p_1}{p_2}$ such that $p_2(x_0, \ldots, x_n) \neq 0$.

The set of all functions regular at a point $\mathbf{x}$ is called the **local ring** of V at $\mathbf{x}$ and denoted by $\mathcal{O}_{V,\mathbf{x}}$. If a rational function is regular at a point $\mathbf{x}$, it does make sense to evaluate f at $\mathbf{x} = (x_0 : \ldots : x_n)$ in the following way

$$f(\mathbf{x}) = \frac{p_1(x_0, \ldots, x_n)}{p_2(x_0, \ldots, x_n)}.$$

Note that $f(\mathbf{x})$ is defined and independent of the choice of the representative for $\mathbf{x}$.

5.4 Maps between varieties

It is natural to consider maps between two varieties as well. Our presentation follows [Sil86], chapter I, section 2.

Definition. A **rational map** from a variety $V_1 \subseteq \mathbb{P}^m$ to a variety $V_2 \subseteq \mathbb{P}^n$ is a map of the form

$$\phi = (f_0 : \ldots : f_n)$$

where $f_0, \ldots, f_n \in \overline{K}(V_1)$.

Again, it is not in general possible to evaluate ϕ at every point $\mathbf{x} \in V_1$ but only in the case when certain regularity conditions are satisfied.

Definition. Let $\phi = (f_0 : \ldots : f_n)$ be a rational map from a variety $V_1 \subseteq \mathbb{P}^m$ to a variety $V_2 \subseteq \mathbb{P}^n$. Then ϕ is said to be **regular** at a point $\mathbf{x} \in V_1$, if there exists a rational function $g \in \overline{K}(V_1)$ such that

1. each gf_i is regular at $\mathbf{x}$;
2. for some gf_i it holds $gf_i(\mathbf{x}) \neq 0$.

If a rational map $\phi : V_1 \to V_2$ is regular at every point of V_1, then it is said to be a **morphism**.

6 Algebraic curves

In this section we study fundamental properties of algebraic curves. Thereby, an **algebraic curve** or **projective curve** is a projective variety of dimension 1.

The theory of algebraic curves is rich of new notions that only exist in this context and cannot be generalized to varieties of greater dimension. The most prominent example is maybe the genus of a curve. One of our primary goals in this section is to develop methods to compute this arithmetical quantity. Furthermore, we introduce the notions of the degree of a map and of ramification points. Finally, we study divisors on curves. Our main reference for this section is [Sil86], chapter II.

Throughout this section we assume K to be a number field, $\overline{K}$ a fixed algebraic closure of K and $\mathbb{P}^n$ the n-dimensional projective space over $\overline{K}$.

6.1 Maps on and between curves

We gather some results about functions on projective curves and maps between projective curves.

Proposition 6.1. *Let $\phi : C_1 \to C_2$ be a rational map between projective curves. If C_1 is a smooth curve, then ϕ is a morphism.*

Proof:
See [Sil86], chapter II, proposition 2.1. □

Proposition 6.2. *Let $\phi : C_1 \to C_2$ be a morphism between projective curves. Then ϕ is either constant or surjective.*

Proof:
See [Sil86], chapter II, theorem 2.3. □

The next proposition describes the local ring of a projective curve.

Proposition 6.3. *Let C be a smooth projective curve and P a point on C. Then the local ring $\mathcal{O}_{C,P}$ is a discrete valuation ring.*

Proof:
See [Sil86], chapter II, proposition 1.1. □

This implies that there exists a surjective function

$$\mathrm{ord}_P : \mathcal{O}_{C,P} \to \{0, 1, \ldots, \} \cup \{\infty\},$$

which counts the multiplicity of the zero of f at the point P. Note that $\mathrm{ord}_P(f) = 0$ means that f does not have a zero at P, while $\mathrm{ord}_P(f) = \infty$ means that $f \equiv 0$. The function ord_P extends naturally to a function on the rational function field

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

In this case ord_P describes the multiplicity of zeros or poles of a rational function in $\overline{K}(C)$ at P. A **uniformizer** t_P at P is a rational function with $\mathrm{ord}_P(t_P) = 1$.

6.2 Degree of a rational map

For a rational map $\phi : C_1 \to C_2$ between two projective curves C_1 and C_2 we find an associated homomorphism between their function fields $\phi^* : \overline{K}(C_2) \to \overline{K}(C_1)$ by defining $\phi^*(f) = f \circ \phi$ for any $f \in \overline{K}(C_2)$.

Proposition 6.4. *Let $\phi : C_1 \to C_2$ be a non-constant rational map between projective curves. Then $\phi^* : \overline{K}(C_2) \to \overline{K}(C_1)$ is an injection and the field extension $\overline{K}(C_1)|\phi^*(\overline{K}(C_2))$ is finite.*

Proof:
See [Sil86], chapter II, theorem 2.4. □

This result allows the following definition.

Definition. Let $\phi : C_1 \to C_2$ be a non-constant rational map between projective curves. The **degree** of ϕ is defined by

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

For maps between smooth curves the degree counts the number of preimages of a point in C_2 under ϕ. For certain points this is only true when the preimages are counted with "multiplicities". In a precise manner this is expressed in the next proposition.

Proposition 6.5. *Let $\phi : C_1 \to C_2$ be a non-constant rational map of smooth projective curves. Then*

1. *For any $Q \in C_2$*
$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi,$$
where $e_\phi(P) = \mathrm{ord}_P(\phi^*(t_Q))$ and t_Q is a uniformizer at the point Q.
2. *For a generic point (i.e. for all but finitely many points) $Q \in C_2$ we have*
$$|\phi^{-1}(Q)| = \deg \phi.$$

Proof:
See [Sil86], chapter II, proposition 2.6. □

For any $Q \in C_2$ we have $e_\phi(P) \geq 1$ for all $P \in \phi^{-1}(Q)$. The proposition then implies that only for finitely many points $Q \in C_2$ it may happen that $e_\phi(P) > 1$ for some $P \in \phi^{-1}(Q)$. This occurs if and only if Q has less than $\deg \phi$ different preimages. In this case Q is called a **ramification point** of ϕ.

6.3 Genus and the Hurwitz genus formula

To every smooth projective curve C we can attribute a natural number called the **genus** of C. Many properties of a curve are reflected in its genus. Furthermore, it plays an important role in the classification of curves – for example, conics are exactly those projective curves which have genus 0. Unfortunately, the technical definition of the genus is rather involved (See [Sil86], chapter II, section 5), and for our purposes it suffices to know how to calculate it in certain cases. This is achieved by the Hurwitz genus formula.

Theorem 6.6 (Hurwitz Genus Formula)**.** *Let C_1 and C_2 be smooth projective curves and $\phi : C_1 \to C_2$ be a non-constant rational map. Let g_1 and g_2 denote the genera of C_1 and C_2 respectively. Then*

$$2g_1 - 2 = (2g_2 - 2)\deg\phi + \sum_{P\in C_1}(e_\phi(P) - 1).$$

Proof:
See [Sil86], chapter II, theorem 5.9. □

6.4 Divisors

A divisor D on a projective curve C is finite formal sum of points on C weighted by integers. It can be written as $D = \sum n_P P$, where the sum ranges over all $P \in C$, $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in C$. The formal definition is as follows and indicates that the set of all divisors carries the structure of an abelian group.

Definition. Let C be a projective curve.

1. The **group of divisors** Div$C$ is the free abelian group generated by the points of C.
2. The **degree** of a divisor $D = \sum n_P P$ is defined as
$$\deg D = \sum n_P.$$

Let C be a smooth projective curve and let f be a rational function on C. It can be proved that f has only finitely many zeros and poles (See [Sil86], chapter II, proposition 1.2). Therefore the formal sum

$$\sum \mathrm{ord}_P(f)P$$

is finite and hence a divisor on C. This divisor is denoted by div$f$. Any divisor D that can be written as $D = \mathrm{div}f$ for some rational function f on C is called **principal divisor**. For any principal divisor div$f$ it holds $\deg\mathrm{div}f = 0$ (See [Sil86], chapter II, proposition 3.1).

A non-constant rational map $\phi : C_1 \to C_2$ between smooth projective curves induces a homomorphism between the divisors of C_2 and those of C_1. This homomorphism is called **pullback** and is defined by

$$\sum n_Q Q \mapsto \sum n_Q \sum_{P\in\phi^{-1}(Q)} e_\phi(P)P.$$

By abuse of notation we write $\phi^* : \mathrm{Div}C_2 \to \mathrm{Div}C_1$ for the pullback. This will not lead to any confusion with $\phi^* : \overline{K}(C_2) \to \overline{K}(C_1)$. In contrast, the second statement of the next proposition shows that this notation is quite natural.

The following result implies that the pullback respects principal divisors and maps divisors of degree 0 to divisors of degree 0.

Proposition 6.7. *Let $\phi : C_1 \to C_2$ be a non-constant rational map between smooth projective curves. Then*

1. $\deg(\phi^* D) = \deg \phi \cdot \deg D$ *for all* $D \in \mathrm{Div}C_2$.

2. $\phi^*(\mathrm{div}f) = \mathrm{div}\phi^*(f)$ *for all rational functions* f *on* C_2.

Proof:
See [Sil86], chapter II, proposition 3.6. □

7 Algebraic geometry over number fields

Thus far we developed algebraic geometry only over the algebraic closure $\overline{K}$ of a number field K. We did this because most theorems do in fact only hold if the base field is algebraically closed. Actually, we are interested in varieties over number fields, i.e. zero loci of polynomials in the projective space over a number field.

Suppose I is a family of polynomials from $K[X_1, \ldots, X_n]$. Then the zero locus of I in the projective space over K can be described as the intersection of the variety

$$V = \{\mathbf{x} \in \mathbb{P}^n | f(\mathbf{x}) = 0 \text{ for all } f \in I\}$$

in the projective space $\mathbb{P}^n$ over $\overline{K}$ and the projective space over K. We write

$$V(K) = \{\mathbf{x} \in \mathbb{P}^n(K) | f(\mathbf{x}) = 0 \text{ for all } f \in I\}$$

and call $V(K)$ a **variety over** K. With regard to this fact we consider a variety over a number field as the subset of a "variety in the usual sense" whose coordinates lie in the projective space over K. However, we note that it is essential that the polynomials defining V are elements of $K[X_1, \ldots, X_n]$, so that $V(K)$ is defined. In this case we say that V is **defined over** K.

If we refer to the dimension of a variety or the genus of a curve over a number field, we always mean the dimension or the genus of the underlying variety over $\overline{K}$.

Let V_1 and V_2 be varieties over $\overline{K}$ and let $\phi : V_1 \to V_2$ be a rational map between them. Then ϕ is a map that is given through polynomials. We say that ϕ is **defined over** K if we can choose representatives for the polynomials defining ϕ to be elements of $K[X_1, \ldots, X_n]$.

Let $\phi : V_1 \to V_2$ be a rational map between two varieties V_1 and V_2 defined over some number field K, and suppose that ϕ is defined over K as well. Then the image of the restricted map $\phi : V_1(K) \to V_2$ lies in $V_2(K)$, hence, we have a map $\phi : V_1(K) \to V_2(K)$.

We note that all maps appearing in this thesis are always defined over the underlying number field.

8 Abelian varieties and Jacobians

Later in this thesis we work with varieties that carry an algebraic structure additionally to their geometric structure. We only outline the basic properties of these varieties. A thorough treatment of this topic can be found in [Gri89] or [BL04].

8.1 Abelian varieties

An **abelian variety** V is a projective variety together with a group structure on V such that the group law can be expressed by regular functions. The name abelian is justified by the fact that the group law of an abelian variety is always commutative.

In the case of abelian varieties over number fields it is possible to describe the group structure.

Theorem 8.1 (Mordell-Weil Theorem)**.** *Let V be a abelian variety defined over a number field K. Then $V(K)$ is a finitely generated abelian group.*

Proof:
See [Ser97], page 52. □

8.2 Jacobians

For every curve C of genus g it is possible to construct an abelian variety $J(C)$ – the so called **Jacobian** of C – having the following properties.

- $J(C)$ has dimension g.

- The curve C is contained in $J(C)$ as a subvariety.

- For every point C there is an embedding morphism $\alpha : C \to J(C)$.

- In the sense of groups, $J(C)$ is generated by C.

We do not carry out an explicit construction of the Jacobian. Instead we refer to [Gri89], chapter 5, or [BL04], chapter 11, where Jacobians are introduced formally.

Theorem 8.2 (Abel-Jacobi Theorem). *Let C be a smooth projective curve. Then there is a canonical (group) isomorphism*

$$\mathrm{Pic}^0 C \to J(C),$$

where $\mathrm{Pic}^0 C$ denotes the quotient group of $\mathrm{Div}^0 C$ (the divisors of degree zero on C) by the normal subgroup of principal divisors of $\mathrm{Div}^0 C$.

Proof:
See [Gri89], page 156 or [BL04], chapter 11, theorem 11.13. □

This means that one can identify $\mathrm{Pic}^0 C$ and $J(C)$ in the sense of groups. Although we did not define $J(C)$ formally, we could interpret $J(C)$ as $\mathrm{Pic}^0 C$. This approach has the disadvantage that there is no natural geometric structure on $\mathrm{Pic}^0 C$, while it is of course possible to endow $\mathrm{Pic}^0 C$ with a geometric structure due to the isomorphism $\mathrm{Pic}^0 C \cong J(C)$. However, there is also the advantage that the group structure of $\mathrm{Pic}^0 C$ is immediately visible. This is especially useful for the next proposition. Here and in the sequel of this thesis we denote the elements of Pic^0 as $\mathrm{cl}(\sum n_P P)$, i.e. as the equivalence class of the divisor $\sum n_P P$ with respect to the equivalence relation induced by the principal divisors.

Proposition 8.3. *Let C_1 and C_2 be smooth projective curves and let $\phi : C_1 \to C_2$ be a morphism. Then ϕ induces a map $\phi_* : J(C_1) \to J(C_2)$ being a morphism and a group homomorphism. If the Jacobians are interpreted as $\mathrm{Pic}^0 C_1$ and $\mathrm{Pic}^0 C_2$, then the map ϕ_* is given by*

$$\mathrm{cl}(\sum n_P P) \mapsto \mathrm{cl}(\sum n_P \phi(P)).$$

Proof:
See [BL04], page 331. □

9 Elliptic curves

A smooth projective curve is called **elliptic curve** if it has genus 1. It is a remarkable fact that elliptic curves admit a group structure thus making it an abelian variety. This can be explained as follows.

The Jacobian of an elliptic curve E is an abelian variety of dimension 1, thus a curve. Every embedding $\alpha : E \to J(E)$ relative to some base points has to be an isomorphism by proposition 6.2. Note that this means that one can identify E with its Jacobian. Furthermore, in the sense of groups $J(E)$ is canonically isomorphic to $\text{Pic}^0 E$. This means that there is a bijection $E \cong \text{Pic}^0 E$, and, therefore, E can be equipped with the group structure induced by $\text{Pic}^0 E$.

However, this bijection is not canonical, but depends on the base point chosen for the embedding $\alpha : E \to J(E)$. So, if we want to talk about elliptic curves not only as geometric objects but also algebraic objects, we have to specify the isomorphism $E \to J(E)$. This is done by distinguishing a point of E, which we call the **base point** and denote by $\mathcal{O}$. With this choice $E \overset{\alpha_{\mathcal{O}}}{\to} J(E) \overset{\sim}{\to} \text{Pic}^0 E$ induces a group structure on E with the property that $\mathcal{O}$ is the neutral element.

The natural notion of a mapping that preserves the structure of elliptic curves is that of an isogeny:

Definition. A morphism $\phi : E_1 \to E_2$ between two elliptic curves E_1 and E_2 is called **isogeny** if ϕ fixes the neutral elements.

In fact, then one can prove that isogenies do not only preserve the neutral elements but the entire group structure.

Proposition 9.1. *Let E_1 and E_2 be elliptic curves and let $\phi : E_1 \to E_2$ be an isogeny. Then*

1. *ϕ is a group homomorphism.*
2. *If ϕ is non-constant, then $\ker \phi$ is a finite subgroup of E_1.*

Proof:

1. See [Sil86], chapter III, theorem 4.8.
2. See [Sil86], chapter III, corollary 4.9.

□

For computational purposes it is often convenient or even inevitable to have the elliptic curve in a more manageable form – i.e. as zero set of some polynomial and not as abstract variety. The following proposition shows that every elliptic curve is isomorphic to the zero locus of a single polynomial in $\mathbb{P}^2$.

Proposition 9.2. *Let E be an elliptic curve. Then E is isomorphic over $\overline{K}$ to a curve in $\mathbb{P}^2$ given by an equation of the form*

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

where $a_j \in \overline{K}$ and the base point is $[0:1:0]$.

Proof:
See [Sil86], chapter III, proposition 3.1. □

The proof of this proposition does not give an explicit method for constructing an isomorphic elliptic curve of this form. Moreover, the isomorphism may only be defined over $\overline{K}$ and not over K. However, since we know that such a isomorphism exists, we are encouraged to search for one by hand. Indeed, it is often possible to exhibit an isomorphism explicitly, which additionally is defined over K.

Note that we can consider the elliptic curve as the zero locus of

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

in the affine space over $\overline{K}$ and the additional point $[0:1:0]$, which we call the **point at infinity**. In this case we say that the elliptic curve is given in **Weierstrass form**.

Suppose an elliptic curve E is given in the form

$$Y^2 = (X-\gamma_1)(X-\gamma_2)(X-\gamma_3) = X + a_2X^2 + a_4X + a_6.$$

Then the **discriminant** of E is defined as

$$\Delta = -16(4a_2^3a_6 - a_2^2a_4 + 4a_4^3 + 27a_6^2 - 18a_2a_4a_6) = -16(\gamma_1-\gamma_2)^2(\gamma_2-\gamma_3)^2(\gamma_1-\gamma_3)^2.$$

(In [Sil86] chapter III the discriminant is defined for any curve in Weierstrass form, but we do not need this generality here.)

Proposition 9.3. *Let C be a curve that is given in Weierstrass form. Then C is an elliptic curve if and only if $\Delta \neq 0$.*

Proof:
See [Sil86], chapter III, proposition 3.1 and proposition 1.4. □

The addition on an elliptic curve in Weierstrass form can be described geometrically. In the affine part this roughly works as follows:

Let P_1 and P_2 be two points of affine parte of the elliptic curve and consider the line through these two points. This line intersects with the elliptic curve in a third point P_3. For these points it holds $P_1 + P_2 + P_3 = \mathcal{O}$, hence $P_1 + P_2 = -P_3$. It can be shown that P_3 and $-P_3$ only differ by the sign in the y-coordinate. Therefore, the point $P_1 + P_2$ has coordinates (x, y), if $P_3 = (x, -y)$.

For a precise description of the addition including the point at infinity and special cases such as $P_1 = P_2$ we refer to [Sil86], chapter III, section 2. In [Sil86], chapter III, proposition 3.4 (e) it is proved that this geometric construction gives the same group law as defined on the elliptic curve by $E \cong \mathrm{Pic}^0 E$.

Chapter 2

Distribution of squares in arithmetic progressions

In this chapter we give an overview of the topic of this diploma thesis.

At first, we illustrate the distribution of squares in arithmetic progressions over number fields by considering a concrete example. We will discover that the distribution of squares in a fixed arithmetic progression may vary as we vary the underlying number field.

Then, we discuss reasonable possibilities how the results of Bombieri, Granville and Pintz might be generalized to number fields. This leads us directly to the statement of the main theorems of this diploma thesis.

In the remaining sections of this chapter we outline the proofs of the main theorems.

1 Introduction and statement of our results

We start off with an example of an arithmetic progression $(qn + d)_{n\in\mathbb{N}}$ with $q = 2$ and $d = 2$. At first, we consider this sequence over the rationals. Those numbers which are squares in $\mathbb{Q}$ are put in bold:

$$\mathbf{4}, \quad 6, \quad 8, \quad 10, \quad 12, \quad 14, \quad \mathbf{16}, \quad 18, \quad 20, \quad 22, \ldots$$

We now examine the same arithmetic progression as above for different number fields. For example, over $\mathbb{Q}(\sqrt[3]{2})$ we obtain:

$$\mathbf{4}, \quad 6, \quad 8, \quad 10, \quad 12, \quad 14, \quad \mathbf{16}, \quad 18, \quad 20, \quad 22, \ldots$$

In this case no ”new” squares appear. We get a quite different behavior for the number field $\mathbb{Q}(\sqrt{2})$, where the same arithmetic progression now has many more squares:

$$\mathbf{4}, \quad 6, \quad \mathbf{8}, \quad 10, \quad 12, \quad 14, \quad \mathbf{16}, \quad \mathbf{18}, \quad 20, \quad 22, \ldots$$

Over $\mathbb{Q}(\sqrt{3}+\sqrt{5})$ ”new” squares turn up as well, but in other positions as in the case of $\mathbb{Q}(\sqrt{2})$:

$$\mathbf{4}, \quad 6, \quad 8, \quad 10, \quad \mathbf{12}, \quad 14, \quad \mathbf{16}, \quad 18, \quad \mathbf{20}, \quad 22, \ldots$$

This shows that the distribution of squares might differ significantly between different number fields. Hence, we come to the conclusion that we should work with a fixed number field if we seek to understand the behavior of squares in arithmetic progressions. We might still expect that for any number field the qualitative behavior of the distribution of squares in arithmetic progressions remains the same. However, we cannot expect to obtain results that hold uniformly for all number fields, i.e. the implicit constants in our theorems will depend on the underlying number field.

A prototype for a theorem that describes the distribution of squares in arithmetic progressions is the theorem of Bombieri, Granville and Pintz in [BGP92], which we have already mentioned in the introduction.

Theorem. *For $q, d \in \mathbb{Z}$,*

$$|\{n \leq N | qn + d = x^2 \textit{ for some } x \in \mathbb{Q}\}| = O(N^{\frac{2}{3}} \log^c N),$$

where c is some explicit constant, and the implicit constant does not depend on q and d.

Our aim is to find a suitable generalization of this statement over a number field K. The most natural approach may be to study

$$\max_{q,d \in K} |\{n \leq N | qn + d = x^2 \text{ for some } x \in K\}|$$

for some number field K and try to describe its behavior as a function of N. However, several problems arise, when q and d are allowed to be elements of the number field itself. Unfortunately, we were not able to solve these problems. Hence, we decided to study a weaker statement, where q and d are restricted to the rational numbers. We wish to determine the order of magnitude of

$$\max_{q,d \in \mathbb{Q}} |\{n \leq N | qn + d = x^2 \text{ for some } x \in K\}|$$

for number fields K.

To shorten our notation, we use the following abbreviations. For $q, d \in \mathbb{Q}$ and $N \in \mathbb{N}$ we set

$$\mathcal{S}_{q,d,N} = \{n \leq N | qn + d = x^2 \text{ for some } x \in K\}$$

and

$$S_{q,d,N} = |\{n \leq N | qn + d = x^2 \text{ for some } x \in K\}|.$$

In order to comprise also the dependence of these quantities on K we should write $\mathcal{S}_{q,d,N}(K)$ or $S_{q,d,N}(K)$. However, it is more convenient to simplify the notation by not expressing the dependence on K explicitly. This will cause no confusion because at any time it will be clear which number field K we are working over.

Even in this restricted case, where q and d are only allowed to be elements of $\mathbb{Q}$, we were not able to find a bound for $S_{q,d,N}$ for an arbitrary number field K. However, we achieved this goal for number fields satisfying a certain technical condition, which we call MHU condition. Assuming the MHU condition for a number field K, we can show that squares over K are distributed in arithmetic progressions in the same manner as in the theorem of Bombieri, Granville and Pintz. This is our main result.

Theorem I. *Let K be a number field that is Galois over $\mathbb{Q}$ and that satisfies the MHU condition. Then*

$$\max_{q,d \in \mathbb{Q}} S_{q,d,N} = O(N^{\frac{2}{3}} \log^c N),$$

where c is some positive constant.

In chapter 7 we investigate more closely the MHU condition and we exhibit a class of number fields which fulfill this condition. We prove that number fields of the form $\mathbb{Q}(\sqrt{p})$, where p is a prime number, do in fact meet this condition. Together with the theorem just stated this yields the following generalization of the theorem of Bombieri, Granville and Pintz.

Theorem II. *Let p be a prime. Then over $\mathbb{Q}(\sqrt{p})$ we have*

$$\max_{q,d \in \mathbb{Q}} S_{q,d,N} = O(N^{\frac{2}{3}} \log^c N),$$

where c is some positive constant.

Before we proceed, we should mention two important remarks.

Let q, d be rational numbers and write them as fractions $q = \frac{q_1}{q_2}$ and $d = \frac{d_1}{d_2}$ with $q_1, d_1 \in \mathbb{Z}$ and $q_2, d_2 \in \mathbb{N}$. Then $n \in \mathcal{S}_{q,d,N}$ if and only if $qn + d = x^2$ for some $x \in K$.

This can be rewritten as $q_1 q_2 d_2^2 n + d_1 d_2 q_2^2 = d_2^2 q_2^2 x^2$ for the same $x \in K$. This is clearly equivalent to $q_1 d_2^2 n + d_1 q_2^2 = x'^2$ for some $x' \in K$. Hence, we have

$$\mathcal{S}_{q,d,N} = \mathcal{S}_{q_1 q_2 d_2^2, d_1 d_2 q_2^2, N}.$$

This shows

$$\max_{q,d \in \mathbb{Q}} S_{q,d,N} = \max_{q,d \in \mathbb{Z}} S_{q,d,N}.$$

Therefore, in our investigations we can restrict ourselves to q and d being integers.

The second remark concerns a convention that we already have mentioned in the chapter on notations. However, we want to stress it one more time since it is very important: Everywhere in this thesis the parameters q and d associated to an arithmetic progression $(qn + d)_{n \in \mathbb{N}}$ are used with the tacit understanding that q and d are non-zero.

Note that without this assumption the above stated theorems cannot hold. To see this, consider $q = 0$ and d being a square.

2 Strategy of proof

The rest of this diploma thesis is devoted to the proofs of Theorem I and II. The final results emerge from the interplay of some numerous intermediate steps that may not seem to be interconnected at first sight. Furthermore, each of these steps is carried out in a different area of mathematics requiring its own techniques and methods. Therefore, it might be difficult to see the general idea connecting all the different results appearing in the course of this thesis.

In this section we seize the chance to look at the entire proof from a higher point of view. We try to highlight the main ideas, thus giving a consistent general frame for the whole proof. On the other hand, we try to keep quite many details in this short exposition. We present it in such a way that every chapter or section in the following can be found to form an intermediate step in achieving the final goal.

As this work is mainly based on the article [BGP92] of Bombieri, Granville and Pintz, both the organization of the proof and the principal ideas used in this thesis are very similar to those appearing in the original paper. In view of this, we also use this section to describe the original approach in the case of rational numbers and contrast it to our contribution in the case of number fields.

We hope that this overview helps to facilitate the understanding of this thesis and to make it more readable.

2.1 Theorem I: First case

In the first case we wish to find a bound for $S_{q,d,N}$ over a number field K assuming that q has small height relative to N. From this assumption it follows that q is divided by only "few" primes that are less than or equal to N. By an elementary argument Bombieri, Granville and Pintz showed that for all the other primes p, which do not divide q, at least half of the residue classes mod p cannot contain elements of $\mathcal{S}_{q,d,N}$. Then, an application of the large sieve gives a bound $S_{q,d,N} = O(\sqrt{N} \log N)$ uniformly in q and d.

In the case of number fields this approach is obstructed by the fact that it is no longer valid that for all primes $p \nmid q$ at least half of the residue classes mod p do not contain elements of $\mathcal{S}_{q,d,N}$.

However, it is not hopeless to try to adapt their method to the case of number fields. The following idea may be used to resolve the above stated problem:
If we cannot prove that for all primes $p \nmid q$ at least half of the residue classes mod p cannot contain elements of $\mathcal{S}_{q,d,N}$, maybe we can find a certain subset $\mathcal{P}$ of primes not dividing q for which this conclusion remains true. However, we have to take care that $\mathcal{P}$ is not too small since the application of the large sieve only yields good bounds for $\mathcal{S}_{q,d,N}$ if $\mathcal{P}$ is large enough.

Indeed, we were able to put this idea into practice. In chapter 2 we define $\mathcal{P}$ to be the set of primes which do not divide q and are completely split over K. Then, we prove that in fact half of the residue classes mod p cannot contain elements of $\mathcal{S}_{q,d,N}$ and we use the Chebotarev density theorem to determine the size of $\mathcal{P}$. This allows us to apply the large sieve in order to obtain a bound of the form $S_{q,d,N} = O(\sqrt{N} \log N)$ uniformly in q and d.

2.2 Theorem I: Second case

The second case covers all q that do not have a small height relative to N. The idea to obtain a bound for $S_{q,d,N}$ over a number field K is to make a detour via algebraic curves in three steps. At first, we associate algebraic curves $C_l(\mathbf{g})$ to squares in arithmetic progression. Then, we prove a bound for the number of K-rational points on the curves $C_3(\mathbf{g})$. In the last step we bound the size of $\mathcal{S}_{q,d,N}$ uniformly in q and d under the assumption of the MHU condition.

Again, this idea goes back to the work of Bombieri, Granville and Pintz. In chapter 5 we follow their approach and introduce a certain family of algebraic curves $C_l(\mathbf{g})$. The algebro-geometric properties of these curves are already given in [BGP92] but mainly without proofs. For the sake of completeness we include detailed proofs for all the relevant assertions about the curves $C_l(\mathbf{g})$.

In the next step we are concerned with bounding the number of K-rational points on the curves $C_3(\mathbf{g})$. The most important ingredient is a deep theorem by Bombieri that gives us the possibility of determining the number of points on $C_3(\mathbf{g})$ over K if we have sufficient knowledge about the rank of the Jacobian of $C_3(\mathbf{g})$. Using the same idea as in [BGP92], we obtain information about the rank of the Jacobian of $C_3(\mathbf{g})$ by relating it to the ranks of some associated elliptic curves. Up to this point there is only little to be altered in the proofs of [BGP92] in order to make them work over number fields. However, we are faced now with the problem of finding the rank of an elliptic curve over a number field, which requires considerably more effort than in the rational case. We devote chapter 4 to the solution of this problem. Essentially, this is achieved by combining the method from [BGP92] for obtaining bounds for the rank of elliptic curves over $\mathbb{Q}$ with a result from [Kna92] about unique factorization domains in number fields.

Finally, we have to take the step back from the algebraic curves and return to squares in arithmetic progression. However, we were not able to prove that it is possible to perform this transition over all number fields.

This led us to the introduction of the MHU condition. In this condition we comprise the technical requirements which are needed for taking the step back from algebraic curves to squares in arithmetic progressions. The abbreviation MHU stands for majorizing, height and uniqueness. The reason for choosing this name is as follows.

If $q, d \in \mathbb{Z}$ satisfy a certain height condition and uniqueness condition, we can derive a bound for the number of squares in K lying in the progression $(qn + d)_{n\in\mathbb{N}}$ from the bounds obtained for the number of K-rational points on the curves $C_3(\mathbf{g})$. Although these conditions are not satisfied for every $q, d \in \mathbb{Z}$, we can obtain a bound for the number of squares in $(qn + d)_{n\in\mathbb{N}}$ over K involving all $q, d \in \mathbb{Z}$ under the following hypothesis:

> For any $q, d \in \mathbb{Z}$ there exist $q', d' \in \mathbb{Z}$ such that q', d' satisfy the height and the uniqueness condition, and we have
>
> $$S_{q,d,N} \leq S_{q',d',N}$$
>
> for all $N \in \mathbb{N}$.

In other words, all pairs $q, d \in \mathbb{Z}$ are **m**ajorized by some $q', d' \in \mathbb{Z}$ satisfying a **h**eight and a **u**niqueness condition. This explains the term MHU condition.

Assuming the MHU condition for a number field K, we proceed analogously to [BGP92] and prove a bound of the form

$$S_{q,d,N} = O(N^{\frac{2}{3}} \log^c N)$$

uniformly in q and d, thus establishing Theorem I.

2.3 Theorem II: The MHU condition

Although the term MHU condition does not appear in [BGP92], this condition is used implicitly. Using our terminology, we can say that Bombieri, Granville and Pintz in fact prove that the field $\mathbb{Q}$ fulfills the MHU condition.

More precisely, they prove that $q, d \in \mathbb{Z}$ satisfy the height and the uniqueness condition if q and d are coprime. Furthermore, they show that for any $q, d \in \mathbb{Z}$ there exist $q', d' \in \mathbb{Z}$ coprime such that

$$S_{q,d,N} \leq S_{q',d',N}$$

for all $N \in \mathbb{N}$, hence, establishing the MHU condition for the field $\mathbb{Q}$.

In chapter 7 we extend these results to number fields showing that coprime integers q and d also satisfy the height and the uniqueness condition over any number field K. Secondly, we use an explicit description of the squares in $\mathbb{Q}(\sqrt{p})$ to show that for any $q, d \in \mathbb{Z}$ there exist $q', d' \in \mathbb{Z}$ coprime such that over K we have

$$S_{q,d,N} \leq S_{q',d',N}$$

for all $N \in \mathbb{N}$. This leads to a proof of Theorem II.

Chapter 3

First case: The case of q having small height

In this chapter our purpose is to show that the size of $\mathcal{S}_{q,d,N}$ can be bounded uniformly in q and d for all q that have a small height relative to N (more precisely, if $h(q) \leq \lambda \log N$ for some fixed constant $\lambda > 0$).

The principal idea is adopted from [BGP92]. We intend to prove that for "many" primes p and for "many" residue classes mod p no element n of these residue classes can give rise to a square of the form $qn + d = x^2$ with $x \in K$. Then, applying the large sieve gives the desired bound uniformly in q and d.

In the brief outline of the entire proof we have already mentioned the problems arising when working over number fields instead of over $\mathbb{Q}$. We overcome these obstructions only by employing rather deep theorems. For example, we could not avoid using the prime number theorem and the Chebotarev density theorem. However, these are not too deep if compared with Faltings' theorem, which will be used in the proof of the second case.

1 Residue classes that do not give rise to squares

Lemma 1.1. *Let K be a number field an let p be a prime. Suppose that p is completely split in K and let $\mathfrak{p}$ be a prime ideal lying above p. Then a full system of residues of $\mathcal{O}_K/\mathfrak{p}$ is given by $n + \mathfrak{p}$, where $n = 0, \ldots, p-1$.*

Proof:
By definition, the inertia degree of $\mathfrak{p}$ is 1 since p is completely split. This is equivalent

to the statement that the field extension $\mathcal{O}_K/\mathfrak{p}|\mathbb{Z}/p\mathbb{Z}$ has degree 1. We have the following commutative diagram

$$\begin{tikzcd}
\mathbb{Z} \arrow[r] \arrow[d] & \mathcal{O}_K \arrow[d] \\
\mathbb{Z}/p\mathbb{Z} \arrow[r] & \mathcal{O}_K/\mathfrak{p}
\end{tikzcd}$$

where the vertical maps are projections and the horizontal maps are embeddings. The map $\mathbb{Z}/p\mathbb{Z} \to \mathcal{O}_K/\mathfrak{p}$ is given by $n + p\mathbb{Z} \mapsto n + \mathfrak{p}$. Now the assertion follows because this map is an isomorphism. □

This lemma enables us to show that in certain residue classes mod p there cannot exist natural numbers n that satisfy $qn + d = x^2$ for some $x \in K$.

Proposition 1.2. *Let q and d be integers and let $p \nmid q$ be a prime that splits completely over K. Then there are $\frac{p-1}{2}$ residue classes mod p such that $qn+d$ is not a square in K for any element n from these classes.*

Proof:
Let $\mathfrak{p}$ be a prime ideal lying above p. Suppose that $r + \mathfrak{p}$ is a quadratic non-residue mod $\mathfrak{p}$. Then no natural number n contained in $(d-r)q^{-1} + \mathfrak{p}$ can satisfy a relation $qn + d = x^2$ for some $x \in K$ since this would imply

$$r = qn + d = x^2 \mod \mathfrak{p},$$

contradicting the fact that $r + \mathfrak{p}$ is a quadratic non-residue.

As p is completely split, we have $|\mathcal{O}_K/\mathfrak{p}| = p$, and this implies that there are $\frac{p-1}{2}$ quadratic non-residues mod $\mathfrak{p}$. By lemma 1.1 these classes can be written as $n_1 + \mathfrak{p}, \ldots, n_{\frac{p-1}{2}} + \mathfrak{p}$, where $n_1, \ldots, n_{\frac{p-1}{2}} \in \mathbb{N}$. Using $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, it now follows immediately that no natural number n which is an element of one of the residue classes $n_1 + p\mathbb{Z}, \ldots, n_{\frac{p-1}{2}} + p\mathbb{Z}$ can satisfy a relation $qn + d = x^2$ with $x \in K$. This proves the proposition. □

2 An application of the large sieve

Lemma 2.1. *Let $\lambda > 0$ and let $\epsilon > 0$. For all sufficiently large N and for all q satisfying $h(q) \leq \lambda \log N$ we have*

$$|\{p \leq \sqrt{N} | p \text{ is prime and } p \text{ does not divide } q\}| \geq (1-\epsilon)\pi(\sqrt{N}).$$

Proof:
Since q has height bounded by $\lambda \log N$, the number of prime factors of q is $O(\log N)$ uniformly in q. On the other hand, the prime number theorem states that there are asymptotically $\frac{2\sqrt{N}}{\log N}$ prime numbers below $\sqrt{N}$. This means that the ratio

$$\frac{|\{p \leq \sqrt{N} | p \text{ is prime and } p \text{ divides } q\}|}{|\{p \leq \sqrt{N} | p \text{ is prime}\}|}$$

becomes arbitrarily small for sufficiently large N. □

Now we are in the position to prove an estimate for $S_{q,d,N}$ using sieve theory.

Theorem 2.2. *Let K be a number field which is Galois over $\mathbb{Q}$ and let $\lambda > 0$. There exists a constant c, such that for all N, for all q satisfying $h(q) \leq \lambda \log N$ and for all d, we have the following estimate*

$$S_{q,d,N} \leq c\sqrt{N} \log N.$$

Proof:
We define $\mathcal{P} = \{p \leq \sqrt{N} | p \nmid q, p \text{ prime and splits completely over } K\}$. This can be rewritten as

$$\mathcal{P} = \{p \leq \sqrt{N} | p \text{ prime and } p \nmid q\} \cap \{p \leq \sqrt{N} | p \text{ prime and splits completely over } K\}.$$

Now we choose N such that

$$\{p \leq \sqrt{N} | p \text{ prime and splits completely over } K\} \geq \frac{1}{2[K:\mathbb{Q}]} \pi(\sqrt{N}).$$

Note that this is possible by the Cheboratev density theorem 1.3.3. By lemma 2.1 we can assume

$$|\{p \leq \sqrt{N} | p \text{ is prime and } p \nmid q\}| \geq \frac{4[K:\mathbb{Q}] - 1}{4[K:\mathbb{Q}]} \pi(\sqrt{N}).$$

for sufficiently large N. Thus, if we choose N large enough, we can write $\mathcal{P}$ as intersection of two subsets of $\{p \leq \sqrt{N} | p \text{ prime}\}$, which have relative density $\frac{1}{2[K:\mathbb{Q}]}$ and $\frac{4[K:\mathbb{Q}]-1}{4[K:\mathbb{Q}]}$. This implies that $\mathcal{P}$ has density at least $\frac{1}{4[K:\mathbb{Q}]}$ and so $|\mathcal{P}| \geq \frac{1}{4[K:\mathbb{Q}]} \pi(\sqrt{N})$.

According to lemma 1.2, the intersection of $\mathcal{S}_{q,d,N}$ with at least half of the residue classes mod p is empty for all $p \in \mathcal{P}$. In terms of the main theorem of the large sieve this means that we can set $\tau = \frac{1}{2}$ and $M = \sqrt{N}$. Then we obtain

$$|\mathcal{S}_{q,d,N}| \leq \frac{N + 3N}{\frac{1}{8[K:\mathbb{Q}]} \pi(\sqrt{N})} \leq c\sqrt{N} \log N,$$

where the last inequality results from the prime number theorem for large N and and appropriate constant c. By enlarging c sufficiently, the theorem follows. □

Chapter 4

Second case: Estimating the rank of elliptic curves

At a later stage of this diploma thesis we are concerned with the problem of finding good bounds for the rank of elliptic curves $E(K)$ over a number field K in terms of the coefficients of a defining equation (e.g. Weierstrass form). This chapter is devoted to the study of this problem.

At first, we see how the problem of computing the rank can be reduced to a question on the order of the group $E(K)/mE(K)$. Subsequently, we seek to find adequate bounds for the size of $E(K)/mE(K)$. Basically, this means proving the weak Mordell-Weil theorem in an effective way, i.e. bounding $E(K)/mE(K)$ explicitly in the terms of the coefficients of a defining equation.

Classical proofs of the weak Mordell-Weil theorem over $\mathbb{Q}$ are indeed effective. In their paper [BGP92] Bombieri, Granville and Pintz use this fact to obtain explicit bounds for the rank of elliptic curves over $\mathbb{Q}$. The authors mention that they adopted their proof from [Lan78]. Actually, in [Lan78] it is shown that the proof for elliptic curves in the rational case can be extended to the case of number fields as well, however, only at the cost of no longer obtaining explicit bounds.

Modern proofs of the weak Mordell-Weil theorem work over arbitrary number fields, but have the same disadvantage of not giving explicit bounds.

We pursue another approach which is inspired by [Kna92]. The idea is similar to the approach in [Lan78], but this time it can be modified to yield explicit bounds for $E(K)/mE(K)$ even in the case of number fields.

1 Estimating the rank of finitely generated groups

First of all, we relate $E(K)/mE(K)$ to the rank of the elliptic curve $E(K)$. In fact, this argument applies to all finitely generated abelian groups.

Proposition 1.1. *Let A be a finitely generated abelian group. Suppose we have an estimate for $|A : mA|$ of the form*

$$|A : mA| \leq m^k.$$

Then k is an upper bound for the rank of A.

Proof:
By the structure theorem of finitely generated abelian groups there is an isomorphism $A \cong \mathbb{Z}^r \times G$, where r is the rank of A and G some finite abelian group. Then we have

$$|A : mA| = \underbrace{|\mathbb{Z}^r : m\mathbb{Z}^r|}_{=m^r} \cdot |G : mG| \geq m^r.$$

If there is a k such that $|A : mA| \leq m^k$, we obtain $k \geq r$ by taking logarithms, and the assertion follows. □

In the following, we describe how to find inequalities of the form

$$|E(K) : 2E(K)| \leq 2^k.$$

This is achieved by introducing a homomorphism α from $E(K)$ to the group of squares in a number field. We investigate the kernel and the image of this homomorphism and derive the desired estimates from that.

2 Homomorphisms from $E(K)$ to the group of squares in a number field

Let K be a number field and let $E(K)$ be an elliptic curve given by a Weierstrass equation of the form

$$Y^2 = (X - \gamma_1)(X - \gamma_2)(X - \gamma_3).$$

For $i = 1, 2, 3$, we define the map $\alpha_i : E(K) \to K^\times / K^{\times 2}$ by

$$\alpha_i(P) = \begin{cases} 1, & \text{if } P \text{ is the point at infinity} \\ x - \gamma_i, & \text{if } P = (x, y) \text{ and } x \neq \gamma_i \\ (\gamma_i - \gamma_j)(\gamma_i - \gamma_k), & \text{if } P = (\gamma_i, 0) \end{cases}$$

In the next proposition we prove that these maps are actually homomorphisms. Our argument is a modification of the proof of proposition 4.6 in chapter 4 of [Kna92].

Proposition 2.1. *Let K be a number field and let $E(K)$ be an elliptic curve given by a Weierstrass equation of the form*

$$Y^2 = (X - \gamma_1)(X - \gamma_2)(X - \gamma_3)$$

Then the map α_i defined above is a homomorphism for every $i = 1, 2, 3$.

Proof:
Let P_1, P_2, P_3 be points on the curve such that $P_1 + P_2 = P_3$.

We have to show that $\alpha_i(P_1)\alpha_i(P_2) = \alpha_i(P_3)$ in $K^\times/K^{\times 2}$. This is equivalent to proving that $\alpha_i(P_1)\alpha_i(P_2)\alpha_i(P_3)$ is a square in $K^\times$.

At first, we treat the case that one of the points is the point at infinity. Then, either the other two points are the point at infinity as well (because it is the neutral element of the group) or the two other points are elements of the affine part of the elliptic curve. In the first case the assertion is obvious. In the latter case the addition law on $E(K)$ implies that the line through the two affine points is a vertical line forcing the x-coordinates of these two points to be equal. Looking at the definition of α_i we immediately conclude that $\alpha_i(P_1)\alpha_i(P_2)\alpha_i(P_3)$ is a square.

Suppose now that none of the points is the point at infinity. Then all points are affine and have coordinates $P_k = (x_k, y_k)$. Recall that addition on an elliptic curve $P_1 + P_2 = P_3$ implies that $P_1, P_2, -P_3$ are points lying on one line.

Let $Y = mX + t$ be the line connecting the three points P_1, P_2 and $-P_3$. Then we have

$$(x_k - \gamma_1)(x_k - \gamma_2)(x_k - \gamma_3) = y_k^2 = (mx_k + t)^2$$

for $k = 1, 2, 3$. This means that x_1, x_2 and x_3 are the roots of the polynomial

$$(X - \gamma_1)(X - \gamma_2)(X - \gamma_3) - (mX + t)^2.$$

Since this polynomial has degree 3, we conclude

$$(X - \gamma_1)(X - \gamma_2)(X - \gamma_3) - (mX + t)^2 = (X - x_1)(X - x_2)(X - x_3).$$

Now we distinguish two cases:

1. None of the points P_k is equal to $(\gamma_i, 0)$.
   Setting $X = \gamma_i$ in the above equation yields
   $$(m\gamma_i + t)^2 = (x_1 - \gamma_i)(x_2 - \gamma_i)(x_3 - \gamma_i).$$
   Looking at the definition of α_i we conclude that the right hand side of the equation is simply $\alpha_i(P_1)\alpha_i(P_2)\alpha_i(P_3)$ and the assertion is proved in this case.

2. One of the points P_k is equal to $(\gamma_i, 0)$.
   Without loss of generality we can assume P_1 to be that point. The y-coordinate is non-zero for both the other points since otherwise the third point had to be the point at infinity.

   Looking at the equation
   $$(X - \gamma_1)(X - \gamma_2)(X - \gamma_3) - (mX + t)^2 = (X - \gamma_i)(X - x_2)(X - x_3)$$
   we see that $(X - \gamma_i)$ divides the right hand side and the first term on the left hand side. Therefore $(X - \gamma_i)$ also divides $(mX + t)^2$ and we can conclude $mX + t = m(X - \gamma_i)$. Substituting $mX + t$ by $m(X - \gamma_i)$ in the equation above yields
   $$(X - \gamma_1)(X - \gamma_2)(X - \gamma_3) - (m(X - \gamma_i))^2 = (X - \gamma_i)(X - x_2)(X - x_3).$$
   We divide by $(X - \gamma_i)$ and obtain
   $$(X - \gamma_j)(X - \gamma_k) - m^2(X - \gamma_i) = (X - x_2)(X - x_3).$$
   Finally, we replace X by γ_i and obtain
   $$(\gamma_i - \gamma_j)(\gamma_i - \gamma_k) = (\gamma_i - x_2)(\gamma_i - x_3).$$
   A look at the definition of α_i now shows
   $$\alpha_i(P_1) = \alpha_i(P_2)\alpha_i(P_3).$$
   This immediately implies the assertion in this case.

□

The three homomorphisms α_i can be put together in a way such that they form a homomorphism to a larger set. This simple observation is recorded in the next proposition.

Proposition 2.2. *Let $\alpha_i : E(K) \to K^\times/K^{\times 2}$ be the homomorphism defined above. Then the map*
$$\alpha : E(K) \to K^\times/K^{\times 2} \times K^\times/K^{\times 2} \times K^\times/K^{\times 2}$$
defined by
$$\alpha = \alpha_1 \times \alpha_2 \times \alpha_3$$
is also a homomorphism. □

3 Investigation of the kernel

Our next objective is to determine the kernel of α. Here, the multiplication-by-two lemma plays a crucial role. This lemma characterizes the elements of an elliptic curve $E(K)$ which lie in the image of the map $[2] : E(K) \rightarrow E(K)$ defined by $P \mapsto 2P$.

Lemma 3.1 (Multiplication-by-two lemma)**.** *Let K be a number field and let $E(K)$ be an elliptic curve given by a Weierstrass equation of the form*

$$Y^2 = (X - \gamma_1)(X - \gamma_2)(X - \gamma_3).$$

A point (x, y) lying on $E(K)$ is contained in the image of the multiplication-by-two map $[2] : E(K) \rightarrow E(K)$ if and only if $x - \gamma_i$ are squares in K for $i = 1, 2, 3$.

Proof:
See [Kna92], chapter IV, theorem 4.2 or [Lan78], pages 104,105. □

The following proposition describes the kernel of α. See [Kna92], corollary 4.7 in chapter 4 or [Lan78], page 104ff for similar results and proofs.

Proposition 3.2. *The homomorphism*

$$\alpha : E(K) \rightarrow K^\times/K^{\times 2} \times K^\times/K^{\times 2} \times K^\times/K^{\times 2}$$

has kernel $2E(K)$.

Proof:
We first note that

$$\ker \alpha = \bigcap_i \ker \alpha_i.$$

Obviously, the point at infinity is contained in both $\ker \alpha$ and $2E(K)$.

A point $(\gamma_i, 0)$ is in the kernel of α if and only if $\alpha_1(\gamma_i, 0)$, $\alpha_2(\gamma_i, 0)$ and $\alpha_3(\gamma_i, 0)$ are squares in $K^\times$. From the definition of the homomorphisms this is easily seen to be equivalent to $(\gamma_i - \gamma_j)$ and $(\gamma_i - \gamma_k)$ being squares in K for $j, k \neq i$. Furthermore, $\gamma_i - \gamma_i$ trivially is a square in K. Hence, $(\gamma_i, 0) \in \ker \alpha$ is equivalent to $(\gamma_i, 0) \in 2E(K)$ by lemma 3.1.

Similarly, let (x, y) be a point different from the ones above. Then (x, y) is an element of the kernel if and only if $\alpha_i(x, y)$ is a square in $K^\times$ for $i = 1, 2, 3$. Since $\alpha_i(x, y) = x - \gamma_i$ for $i = 1, 2, 3$, we see that this is equivalent to $(x, y) \in 2E(K)$ by lemma 3.1. □

4 Investigation of the image

While the results of the last section can be proved also over arbitrary fields of characteristic zero, the description of the image of α is much more involved.

It is also this part where passing from $\mathbb{Q}$ to number fields causes additional obstructions. The description of the image in the case of elliptic curves over $\mathbb{Q}$ relies heavily on unique factorization of the integers. In order to transfer the proof of the rational case over to number fields, it would be desirable to have unique factorization also in number fields. However, as we mentioned before, the ring of integers $\mathcal{O}_K$ in a number field K need not be a unique factorization domain. At this point it seems to be more promising to use the construction of a unique factorization domain given in proposition 1.3.4, rather than to work with algebraic integers.

The ideas for the proofs of the following results have its source in the proofs of similar statements in the rational case. See for example [Kna92], chapter 4, proposition 4.8. The general strategy of proof remains the same in the case of number fields. However, quite some work has to be done in order to transfer the proof in rational case into the context of number fields. First of all, the rational integers have to be replaced by an appropriate ring inside of K. This role is played by the unique factorization domain constructed in 1.3.4. Furthermore, we use valuations on the number field K to replace divisibility arguments which are employed in the rational case.

Before we proceed like indicated, we observe that for any prime p of a unique factorization domain R we can construct a non-archimedean valuation $|\ |_p$ on its quotient field K analogously to the construction of non-archimedean valuations on $\mathbb{Q}$:
Let $x \in K$ and write x as a fraction $x = \frac{a}{b}p^r$, with $a, b \in R$, $p \nmid a, b$ and $r \in \mathbb{Z}$. Then define

$$|x|_p = 2^{-r}.$$

The values attained by this valuation are exactly the elements of the following set

$$\mathfrak{B} = \{\ldots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \ldots\} \cup \{0\}.$$

Obviously, $\mathfrak{B}$ is multiplicatively closed. An element of $\mathfrak{B}$ is called a square in $\mathfrak{B}$ if it is the square of some element of $\mathfrak{B}$. It is easy to see that $|x|_p$ is a square in $\mathfrak{B}$ if and only if $x = 0$ or $x = \frac{a}{b}p^r$ with $a, b \in R$, $p \nmid a, b$ and r is even.

If the quotient field of R is a number field, $|\ |_p$ is also a valuation on K. Of course, $|\ |_p$ belongs to some place of K. However, in general, $|\ |_p$ does not coincide with the normalized valuations on K discussed in the first chapter.

Proposition 4.1. *Let K be a number field and let R be a unique factorization domain that has K as its quotient field. Let $E(K)$ be an elliptic curve given by a Weierstrass equation of the form*

$$Y^2 = (X - \gamma_1)(X - \gamma_2)(X - \gamma_3)$$

with $\gamma_i \in R$.

The image of the homomorphism $\alpha : E(K) \to K^\times/K^{\times 2} \times K^\times/K^{\times 2} \times K^\times/K^{\times 2}$ is contained in

$$\{(r_1K^{\times 2}, r_2K^{\times 2}, r_3K^{\times 2}) | r_i \in R \textit{ only contains prime factors of } \Delta\},$$

where $\Delta = -16(\gamma_1 - \gamma_2)^2(\gamma_2 - \gamma_3)^2(\gamma_1 - \gamma_3)^2$ is the discriminant of the elliptic curve.

Proof:
Obviously, the image of the point at infinity is $(1, 1, 1)$. Looking at the definition of α, we also see that $(\gamma_i, 0)$ is mapped to an element of the proposed set for all $i = 1, 2, 3$.

Let p be a prime in R that does not divide $\gamma_i - \gamma_j$. This means $|\gamma_i - \gamma_j|_p = 1$.

Let us now consider some other point (x, y) different from those above. Then the image of (x, y) under α is $(x - \gamma_1, x - \gamma_2, x - \gamma_3)$. To prove the proposition it suffices to show that for all i the prime p occurs as a factor in $x - \gamma_i$ only in squared form. Obviously, this is equivalent to proving that $|x - \gamma_i|_p$ is a square in $\mathfrak{B}$ for all i.

At first, we observe that $(x - \gamma_1)(x - \gamma_2)(x - \gamma_3)$ is a square in K because (x, y) lies on the curve $E(K)$. This implies that the following product

$$\prod_{i=1}^{3} |x - \gamma_i|_p$$

is also a square in $\mathfrak{B}$ because of the multiplicativity of $| \ |_p$. Now we distinguish two cases

1. There is some k such that $|x - \gamma_k|_p > 1$:
   Then we have

   $$|x|_p = |x - \gamma_i + \gamma_k|_p = \max\{|x - \gamma_k|_p, \underbrace{|\gamma_k|_p}_{\leq 1}\} = |x - \gamma_k|_p.$$

   For $i \neq k$ we get

   $$|x - \gamma_i|_p = \max\{|x|_p, \underbrace{|\gamma_i|_p}_{\leq 1}\} = |x - \gamma_k|_p.$$

This shows

$$\prod_{i=1}^{3} |x-\gamma_i|_p = |x-\gamma_k|_p^3.$$

Since $\prod_{i=1}^{3} |x-\gamma_k|_p$ is a square in $\mathfrak{B}$, $|x-\gamma_k|_p^3$ and then $|x-\gamma_k|_p$ are squares in $\mathfrak{B}$ as well. Therefore, $|x-\gamma_i|_p$ is a square in $\mathfrak{B}$ for any i.

2. For all k it holds $|x-\gamma_k|_p \leq 1$:
   If all valuations are 1, there is nothing to prove. Suppose that $|x-\gamma_k|_p < 1$ for some k. Since p does not divide $\gamma_k - \gamma_i$, we obtain for $k \neq i$:

   $$1 = |\gamma_k - \gamma_i|_p \leq \max\{\underbrace{|x-\gamma_k|_p}_{<1}, |x-\gamma_i|_p\} = |x-\gamma_i|_p \leq 1$$

   We conclude that $|x-\gamma_i|_p = 1$ and, therefore, $|x-\gamma_i|_p$ is a square in $\mathfrak{B}$ for $k \neq i$. Finally, the product relation above implies that $|x-\gamma_k|_p$ is also a square in $\mathfrak{B}$.

□

Now we have a quite explicit way to describe the image of α. We use this to give a bound for $|E(K) : 2E(K)|$ solely in terms of the coefficients of the defining equation.

Proposition 4.2. *Let K be a number field and let R be a unique factorization domain that has K as its quotient field. Additionally, suppose that $R^\times$ is finitely generated. Let $E(K)$ be an elliptic curve given by a Weierstrass equation of the form*

$$Y^2 = (X-\gamma_1)(X-\gamma_2)(X-\gamma_3)$$

with $\gamma_i \in R$. Then we have

$$|E(K) : 2E(K)| \leq 2^{c(1+\omega_R(\Delta))},$$

where Δ is the discriminant of E, and c is a positive constant depending only on R.

Proof:
Suppose $\omega_R(\Delta) = n$ and let $p_1, \dots, p_n$ be the primes in R dividing Δ. Then, any element from

$$\{rK^{\times 2} | r \in R \text{ only contains prime factors of } \Delta\}$$

can be written uniquely as $up_1^{e_1} \dots p_n^{e_n} K^{\times 2}$, where $u \in R^\times / R^{\times 2}$, and the exponents e_i attain the values 0 or 1. Since $R^\times$ is finitely generated, the group $R^\times/R^{\times 2}$ is finite of some order c. Hence,

$$|\{rK^{\times 2} | r \in R \text{ only contains prime factors of } \Delta\}| \leq c2^{\omega_R(\Delta)}.$$

By proposition 4.1 the image of the homomorphism α is contained in

$$\{(r_1 K^{\times 2}, r_2 K^{\times 2}, r_3 K^{\times 2}) | r_i \in R \text{ only contains prime factors of } \Delta\}$$

Therefore, the image of α has cardinality at most $c^3 2^{3\omega_R(\Delta)}$. This can be seen to be less than or equal to $2^{c(1+\omega_R(\Delta))}$ provided that $c \geq 10$. If $c < 10$, we redefine c to be equal to 10. □

Combining all the results in this section with theorem 1.3.7, we obtain our final result:

Theorem 4.3. *Let K be a number field and let $E(K)$ be an elliptic curve given by a Weierstrass equation of the form*

$$Y^2 = (X - \gamma_1)(X - \gamma_2)(X - \gamma_3)$$

and $\gamma_i \in \mathbb{Z}$. Then there exists a constant c depending only on K such that

$$|E(K) : 2E(K)| \leq 2^{c\omega(\Delta)},$$

where Δ denotes the discriminant of E. In particular, the rank of $E(K)$ is bounded by $c\omega(\Delta)$.

Proof:
By theorem 1.3.4 we can find a unique factorization domain R such that K is the quotient field of R, $R^\times$ is finitely generated and $\omega_R(z) \leq c_1 \omega(z)$ for some constant $c_1 > 0$. With this choice of R proposition 4.2 can be applied, and we conclude

$$|E(K) : 2E(K)| \leq 2^{c_2(1+\omega_R(\Delta))} \leq 2^{c_2(1+c_1\omega(\Delta))}$$

for some constant $c_2 > 0$. Since Δ is an integer and $\Delta \neq \pm 1$, we have $\omega(\Delta) \geq 1$. Hence, we can find a constant c depending on c_1 and c_2 such that

$$|E(K) : 2E(K)| \leq 2^{c\omega(\Delta)}.$$

The assertion for the rank follows from proposition 1.1. □

Chapter 5

Second case: Curves associated to squares in arithmetic progressions

This chapter deals with the core part of the second case. The principal idea is to introduce a certain type of curves $C_l(\mathbf{g})$ which represent squares in an arithmetic progression.

We shall investigate these curves using methods from arithmetic geometry. Our focus lies on the curves $C_3(\mathbf{g})$ and their relation to elliptic curves of similar type. This enables us to gather information about $C_3(\mathbf{g})$ and allows us to employ a deep theorem by Bombieri ([Bom90], explicit version in [BGP92]) to estimate the number of K-rational points on these curves for a number field K. This will be used in the next chapter to bound the number of squares in K lying in an arithmetic progression.

The ideas and the proofs originate from the article by Bombieri, Granville and Pintz, and there is only little to be altered to make the proofs work when switching from $\mathbb{Q}$ to an arbitrary number field. The organization is also similar to [BGP92]. For the sake of completeness we additionally fill in some details that had been left out in the original article.

In this chapter K denotes a number field and $\overline{K}$ an algebraic closure of K. All varieties that appear are assumed to be varieties over $\overline{K}$ if not indicated otherwise.

1 Definition of $C_l(\mathbf{g})$

Let q and d be integers and consider a 3-tuple (n_0, n_1, n_2) such that $qn_i + d = x_i^2$ for some $x_i \in K$. Simply by multiplying out, we get the following equation.

$$(x_1^2 - x_2^2)x_0^2 + (x_2^2 - x_0^2)x_1^2 + (x_0^2 - x_1^2)x_2^2 = 0.$$

Using the relation $qn_i + d = x_i^2$ and dividing by q, we obtain

$$(n_1 - n_2)x_0^2 + (n_2 - n_0)x_1^2 + (n_0 - n_1)x_2^2 = 0.$$

This means that $(x_0 : x_1 : x_2)$ is a point on the projective curve given by

$$(n_1 - n_2)X_0^2 + (n_2 - n_0)X_1^2 + (n_0 - n_1)X_2^2 = 0.$$

We observe that the parameters q and d do not appear in the defining equation of this curve. This is crucial since it means that we can prove statements about squares in arithmetic progressions $(qn+d)_{n \in N}$ uniformly in q and d by studying such curves.

However, this type of curves will not suffice for our purposes. Rather, we have to consider a generalized class of curves which arises from considering not only three squares in an arithmetic progression. It will turn out to be more convenient to define these curves a bit more abstractly. In order to do this we have to introduce the following notation.

Definition. A tuple $\mathbf{g}$ consisting of non-zero integers g_{ij} for every $i \neq j$ with $0 \leq i, j \leq l+1$ satisfying the relations

$$g_{ij} + g_{ji} = 0$$

$$g_{ij} + g_{jk} = g_{ik}$$

is called an l-**gap tuple**.

The gap tuples provide the coefficients for certain projective curves, which we now define.

Definition. Let $\mathbf{g}$ be an l-gap tuple. The curve $C_l(\mathbf{g})$ associated to $\mathbf{g}$ is the curve that is described by the l equations

$$g_{i+1,i+2}X_i^2 + g_{i+2,i}X_{i+1}^2 + g_{i,i+1}X_{i+2}^2 = 0$$

for $i = 0, \ldots, l-1$ in $\mathbb{P}^{l+1}$ over $\overline{K}$.

Note that these curves are defined over K since the defining polynomials having integer coefficients.

We chose the name gap tuple because gap tuples represent the gaps i.e. differences between the elements of a set containing $(l+2)$ natural numbers. Most gap tuples in this thesis will arise from the following situation:

Let $\mathbf{n} = (n_0, \ldots, n_{l+1})$ be an $(l+2)$-tuple of natural numbers and let $\mathbf{x} = (x_0, \ldots, x_{l+1})$ be an $(l+2)$-tuple of elements of K having the property $qn_i + d = x_i^2$ for $i = 0, \ldots, l+1$. By doing the same computations as at the beginning of this chapter, it is easy to see that the projective point $(x_0 : \ldots : x_{l+1})$ is a point on the projective curve described by the equations

$$(n_{i+1} - n_{i+2})X_i^2 + (n_{i+2} - n_i)X_{i+1}^2 + (n_i - n_{i+1})X_{i+2}^2 = 0$$

for $i = 0, \ldots, l-1$. Note, that this is exactly the curve $C_l(\mathbf{g})$ if we define an l-gap tuple by $g_{ij} = n_i - n_j$.

At a later stage we will need the following definition.

Definition. Let $\mathbf{g}$ be an l-gap tuple $\mathbf{g}$ and let $0 \leq k \leq l+1$. For $0 \leq i, j \leq l$ define

$$g'_{i,j} = \begin{cases} g_{i,j}, & \text{if } i < k, j < k; \\ g_{i+1,j}, & \text{if } i \geq k, j < k; \\ g_{i,j+1}, & \text{if } i < k, j \geq k; \\ g_{i+1,j+1}, & \text{if } i \geq k, j \geq k. \end{cases}$$

Then, these numbers form an $(l-1)$-gap tuple, which we denote by $\mathbf{g}^{(k)}$.

Roughly speaking, $\mathbf{g}^{(k)}$ arises from $\mathbf{g}$ by omitting all entries with index k and "shrinking" it, so that it fits into the definition of gap tuples.

2 Properties of the curves $C_l(\mathbf{g})$

In this section we study geometric properties of the curves $C_l(\mathbf{g})$. Actually, up to this point we have not verified that $C_l(\mathbf{g})$ are in fact curves. This will be our first task. Then, we calculate the genus of $C_l(\mathbf{g})$ and determine the degree of $C_l(\mathbf{g})$. These parameters of the curves $C_l(\mathbf{g})$ are needed later when we want to apply the theorem of Bombieri.

To carry out this program we will later need the following two lemmas.

Lemma 2.1. *Let $\mathbf{g}$ be an l-gap tuple and let $\mathbf{x} = (x_0 : \ldots : x_{l+1})$ be a point on $C_l(\mathbf{g})$. Then at most one coordinate of $\mathbf{x}$ is zero.*

Proof:
If all coordinates are non-zero, there is nothing to prove. If this is not the case, let k be the index of the first entry of $(x_0 : \ldots : x_{l+1})$ such that $x_k = 0$. If $k = l+1$,

there is nothing to prove either. So we can assume $k \leq l$. Then, x_{k+1} cannot be zero because $x_k = x_{k+1} = 0$ would imply $x_i = 0$ for all $0 \leq i \leq l+1$, which is a contradiction. Since we work in projective space, we may suppose that $x_{k+1} = 1$.

We now show by induction that for any $k+1 \leq i \leq l+1$ the value of x_i is determined via $x_i^2 = \frac{g_{k,i}}{g_{k,k+1}}$. Then, the definition of gap tuples yields that $\frac{g_{k,i}}{g_{k,k+1}}$ is non-zero and this proves the lemma.

For $i = k+1$ the assertion is certainly true. For $i = k+2$ we look at the equation

$$g_{k+1,k+2}X_k^2 + g_{k+2,k}X_{k+1}^2 + g_{k,k+1}X_{k+2}^2 = 0.$$

Using that the coordinates of $\mathbf{x}$ satisfy this equation, we immediately conclude from $x_k = 0$ and $x_{k+1} = 1$ that we have

$$x_{k+2}^2 = -\frac{g_{k+2,k}}{g_{k,k+1}} = \frac{g_{k,k+2}}{g_{k,k+1}}.$$

This shows the truth of our assertion in the case $i = k+2$.

Now suppose that this assertion is true for some $i-1$ and i and consider the equation

$$g_{i,i+1}X_{i-1}^2 + g_{i+1,i-1}X_i^2 + g_{i-1,i}X_{i+1}^2 = 0.$$

Since $\mathbf{x}$ is a point on $C_l(\mathbf{g})$, this equation is satisfied by the coordinates of $\mathbf{x}$. Using the induction hypothesis, we get

$$g_{i,i+1}\frac{g_{k,i-1}}{g_{k,k+1}} + g_{i+1,i-1}\frac{g_{k,i}}{g_{k,k+1}} = -g_{i-1,i}x_{i+1}^2.$$

This yields

$$x_{i+1}^2 = -\frac{g_{i,i+1}g_{k,i-1} + g_{i+1,i-1}g_{k,i}}{g_{i-1,i}g_{k,k+1}}.$$

Since $\mathbf{g}$ is a gap tuple, we conclude $g_{i,i+1} = g_{i,k} + g_{k,i+1}$ and $g_{i+1,i-1} = g_{i+1,k} + g_{k,i-1}$. Replacing these terms in the above equations and using the properties of gap tuples, we obtain

$$\begin{aligned} x_{i+1}^2 &= -\frac{(g_{i,k} + g_{k,i+1})g_{k,i-1} + (g_{i+1,k} + g_{k,i-1})g_{k,i}}{g_{i-1,i}g_{k,k+1}} \\ &= -\frac{g_{k,i+1}g_{k,i-1} + g_{i+1,k}g_{k,i}}{g_{i-1,i}g_{k,k+1}} = \frac{g_{k,i+1}(-g_{k,i-1} + g_{k,i})}{g_{i-1,i}g_{k,k+1}} = \frac{g_{k,i+1}}{g_{k,k+1}}. \end{aligned}$$

This shows the truth of the assertion for $i+1$ and concludes the proof. □

This lemma can be used to count the number of points in the intersection of $C_l(\mathbf{g})$ with the hyperplane $X_{l+1} = 0$.

Lemma 2.2. *Let* $\mathbf{g}$ *be an* l*-gap tuple. Then the intersection of* $C_l(\mathbf{g})$ *with the hyperplane defined by* $X_{l+1} = 0$ *consists of exactly* 2^l *points.*

Proof:
We describe how these 2^l points can be obtained. To that end let $\mathbf{x} = (x_0 : \ldots : x_{l+1})$ be a point lying in this intersection. Then it is obvious that $x_{l+1} = 0$. This implies that x_l has to be non-zero. If it were zero, we would get $x_i = 0$ inductively for all i by looking at the defining equations – a contradiction. Working projectively, we may additionally assume that $x_l = 1$.

Therefore, for any point in the intersection we have $x_{l+1} = 0$ and $x_l = 1$. Suppose we have already found the coordinates $x_k, \ldots, x_{l+1}$, then the coordinate x_{k-1} is determined by the quadratic equation

$$g_{i+1,i+2}X_i^2 + g_{i+2,i}x_{i+1}^2 + g_{i,i+1}x_{i+2}^2 = 0$$

for $i = k-1$ up to the sign. This means that once chosen $x_k, \ldots, x_{l+1}$ the coordinate x_{k-1} attains exactly two values, at least, under the hypothesis that $x_{k-1} \neq 0$. But this is assured by the preceding lemma which implies that none of the coordinates $x_0, \ldots, x_l$ can be zero because we already have $x_{l+1} = 0$. □

2.1 $C_l(\mathrm{g})$ is a smooth curve

We now describe the tangent space of $C_l(\mathbf{g})$. Subsequently, this allows us to prove that $C_l(\mathbf{g})$ is a smooth curve.

Proposition 2.3. *Let* $\mathbf{g}$ *be an* l*-gap tuple and let* $\mathbf{x} = (x_0, \ldots, x_{l+1})$ *be a point on* $C_l(\mathbf{g})$*.*

1. *The tangent space of* $C_l(\mathbf{g})$ *in* $\mathbf{x}$ *is given by the equations*

$$g_{i+1,i+2}x_iX_i + g_{i+2,i}x_{i+1}X_{i+1} + g_{i,i+1}x_{i+2}X_{i+2} = 0$$

   for $i = 0, \ldots, l-1$*.*

2. *For any point* $\mathbf{x}$ *on* $C_l(\mathbf{g})$ *the Jacobi matrix has rank* l*.*

3. $C_l(\mathbf{g})$ *is a smooth curve.*

Proof:

1. The defining equations for $C_l(\mathbf{g})$ are
$$g_{i+1,i+2}X_i^2 + g_{i+2,i}X_{i+1}^2 + g_{i,i+1}X_{i+2}^2 = 0$$
for $i = 0, \dots, l-1$. Differentiating the i-th equation with respect to the variable X_j we obtain $2g_{i+1,i+2}X_i$ if $j = i$, $2g_{i+2,i}X_{i+1}$ if $j = i+1$, $g_{i,i+1}X_{i+2}$ if $j = i+2$ and 0 in all other cases. Now the assertion follows directly from the characterization of the tangent space in proposition 1.5.1.

2. Using the calculations in 1., we conclude that the Jacobi matrix (defined in proposition 1.5.3) in the point $\mathbf{x}$ is given by
$$\begin{pmatrix}
2g_{1,2}x_0 & 2g_{2,1}x_1 & 2g_{0,1}x_2 & 0 & \cdots & \cdots & 0 \\
0 & 2g_{2,3}x_1 & 2g_{3,1}x_2 & 2g_{1,2}x_3 & & & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & & \vdots \\
\vdots & & \ddots & 2g_{l-1,l}x_{l-2} & 2g_{l,l-2}x_{l-1} & 2g_{l-2,l-1}x_l & 0 \\
0 & \cdots & \cdots & 0 & 2g_{l,l+1}x_{l-1} & 2g_{l+1,l-1}x_l & 2g_{l-1,l}x_{l+1}
\end{pmatrix}$$
This is a diagonal matrix of dimension $l \times (l+2)$. We obtain from lemma 2.1 that at most one coordinate of $\mathbf{x}$ is zero. From this fact we can easily conclude that the Jacobi matrix has full rank l.

3. We apply 2. to the situation of proposition 1.5.2 and proposition 1.5.3. This shows that any point of $C_l(\mathbf{g})$ is smooth and that $C_l(\mathbf{g})$ is a curve.

□

2.2 A projection morphism

Our next goal is to determine the genus of the curves $C_l(\mathbf{g})$. In the preliminary chapter we only mentioned one tool for computing the genus of a curve: Hurwitz genus formula. However, using this formula one cannot expect to compute the genus of a curve directly but only relate it to the genus of another curve by a map between the two curves. In our case we will relate the genera of the curves $C_{l+1}(\mathbf{g})$ and $C_l(\mathbf{g}^{(l+2)})$. In order to do that we first have to study a suitable morphism between

these two curves:
Let $\mathbf{g}$ be an $(l+1)$-gap tuple and consider a point $\mathbf{x} = (x_0 : \ldots : x_{l+2})$ lying on $C_{l+1}(\mathbf{g})$. Then, the coordinates of $\mathbf{x}$ satisfy the equations

$$g_{i+1,i+2}X_i^2 + g_{i+2,i}X_{i+1}^2 + g_{i,i+1}X_{i+2}^2 = 0$$

for $i = 0, 1, \ldots, l$. If we simply omit the last equation, it is clear that $(x_0 : \ldots : x_{l+1})$ satisfies the equations

$$g_{i+1,i+2}X_i^2 + g_{i+2,i}X_{i+1}^2 + g_{i,i+1}X_{i+2}^2 = 0$$

for $i = 0, \ldots, l-1$. It is easy to check, that then $(x_0 : \ldots : x_{l+1})$ is a point on $C_l(\mathbf{g}^{(l+2)})$.

This implies that the projection $(x_0 : \ldots : x_{l+2}) \mapsto (x_0 : \ldots : x_{l+1})$ induces a map $\pi : C_{l+1}(\mathbf{g}) \to C_l(\mathbf{g}^{(l+2)})$. Obviously, this is a rational map, and since $C_{l+1}(\mathbf{g})$ and $C_l(\mathbf{g}^{(l+2)})$ are smooth curves, it follows from proposition 1.6.1 that π is even a morphism.

The next lemma gives a description of the ramification points of the projection morphism $\pi : C_{l+1}(\mathbf{g}) \to C_l(\mathbf{g}^{(l+2)})$.

Lemma 2.4. *Let $\mathbf{g}$ be an $(l+1)$-gap tuple. Let $\pi : C_{l+1}(\mathbf{g}) \to C_l(\mathbf{g}^{(l+2)})$ be the map which is induced by the projection $(x_0 : \ldots : x_{l+2}) \mapsto (x_0 : \ldots : x_{l+1})$.*

1. *The morphism π is of degree 2 and if $(x_0 : \ldots : x_{l+2}) \in \pi^{-1}(x_0 : \ldots : x_{l+1})$, then $(x_0 : \ldots : -x_{l+2}) \in \pi^{-1}(x_0 : \ldots : x_{l+1})$.*
2. *A point $(x_0 : \ldots : x_{l+1})$ is a ramification point if and only if we have $x_{l+2} = 0$ for any $(x_0 : \ldots : x_{l+2}) \in \pi^{-1}(x_0 : \ldots : x_{l+1})$.*
3. *There are 2^{l+1} ramification points all having ramification index 2.*

Proof:
At first, we show that a generic point on $C_l(\mathbf{g}^{(l+2)})$ has two preimages under π.

Fix a point $(x_0 : \ldots : x_{l+1})$ on $C_l(\mathbf{g}^{(l+2)})$. Then the preimages under the projection are of the form $(x_0 : \ldots : x_{l+1} : x_{l+2})$. A point of this form lies on the curve $C_{l+1}(\mathbf{g})$ if and only if the coordinates additionally satisfy the equation

$$g_{l+1,l+2}X_l^2 + g_{l+2,l}X_{l+1}^2 + g_{l,l+1}X_{l+2}^2 = 0.$$

Since $(x_0 : \ldots : x_{l+1})$ is fixed, we conclude that this is the case when x_{l+2} is a solution of the equation

$$g_{l+1,l+2}x_l^2 + g_{l+2,l}x_{l+1}^2 + g_{l,l+1}X_{l+2}^2 = 0.$$

In the generic case this quadratic equation in X_{l+2} has exactly two solutions which only differ by the sign. Therefore, the degree of π is 2 by proposition 1.6.5.

We also observe that π is ramified at a point $(x_0 : \ldots : x_{l+1})$ if and only if

$$g_{l+1,l+2}x_l^2 + g_{l+2,l}x_{l+1}^2 + g_{l,l+1}X_{l+2}^2 = 0$$

has the only solution $x_{l+2} = 0$. This happens if and only if $(x_0 : \ldots : x_{l+1} : 0)$ lies on $C_{l+1}(\mathbf{g})$. So, every ramification point arises in a unique way from a point in the intersection of $C_{l+1}(\mathbf{g})$ with the hyperplane defined by $X_{l+2} = 0$. By lemma 2.2 their number is 2^{l+1}.

Since π is a map of degree 2, ramification indices can only attain the values 1 and 2. This means that the ramification points must have the ramification index 2 and all statements of the lemma are proved. □

This lemma is sufficient for calculating the genus of the curves $C_l(\mathbf{g})$. However, for later applications we need a more general version of this result. Namely, we intend to show that the projection deleting the k-th coordinate

$$(x_0 : \ldots : x_{l+2}) \mapsto (x_0 : \ldots : x_{k-1} : x_{k+1} : \ldots : x_{l+2})$$

induces a morphism

$$\pi_k : C_{l+1}(\mathbf{g}) \to C_l(\mathbf{g}^{(k)}).$$

In this case we need considerably more computational effort than before in order to establish the assertion:
Let $(x_0 : \ldots : x_{l+2})$ be a point on $C_{l+1}(\mathbf{g})$. In order to avoid confusion we write $(x_0 : \ldots : x_{k-1} : x_{k+1} : \ldots : x_{l+2}) = (y_0, \ldots, y_{l+1})$, i.e. $x_i = y_i$ if $i < k$ and $y_i = x_{i+1}$ if $i \geq k$. Then, the point $(y_0 : \ldots : y_{l+1})$ lies on $C_l(\mathbf{g}^{(k)})$ if an only if the coordinates satisfy

$$g'_{i+1,i+2}Y_i^2 + g'_{i+2,i}Y_{i+1}^2 + g'_{i,i+1}Y_{i+2}^2 = 0$$

for $i = 0, \ldots, l-1$, where the coefficients are those of $\mathbf{g}^{(k)}$. Using the definition of the gap tuple $\mathbf{g}^{(k)}$ we now retranslate these equations into the original variables. We obtain that $(x_0 : \ldots : x_{k-1} : x_{k+1} : \ldots : x_{l+2})$ is a point on $C_l(\mathbf{g}^{(k)})$ if an only if $(x_0 : \ldots : x_{k-1} : x_{k+1} : \ldots : x_{l+2})$ satisfies the following l equations.

I. $g_{i+1,i+2}X_i^2 + g_{i+2,i}X_{i+1}^2 + g_{i,i+1}X_{i+2}^2 = 0$ for $i = 0, \ldots, k-3$

II. $g_{k-1,k+1}X_{k-2}^2 + g_{k+1,k-2}X_{k-1}^2 + g_{k-2,k-1}X_{k+1}^2 = 0$

III. $g_{k+1,k+2}X_{k-1}^2 + g_{k+2,k-1}X_{k+1}^2 + g_{k-1,k+1}X_{k+2}^2 = 0$

IV. $g_{i+1,i+2}X_i^2 + g_{i+2,i}X_{i+1}^2 + g_{i,i+1}X_{i+2}^2 = 0$ for $i = k+1, \ldots, l$

Now, our aim is to show that for any point $(x_0 : \ldots : x_{l+2}) \in C_{l+1}(\mathbf{g})$ these equations are in fact satisfied. First of all, we see that the equations in I. and IV. are trivially satisfied since they are part of the defining equations of $C_{l+1}(\mathbf{g})$. Therefore, we only have to check that any point on $C_{l+1}(\mathbf{g})$ additionally satisfies the equations II. and III.

We present the proof of this fact exemplarily for equation II. The other case one can be handled analogously:
Let $(x_0 : \ldots : x_{l+2}) \in C_{l+1}(\mathbf{g})$. From the defining equations of $C_{l+1}(\mathbf{g})$ we obtain

$$g_{k-1,k}x_{k-2}^2 + g_{k,k-2}x_{k-1}^2 + g_{k-2,k-1}x_k^2 = 0 \text{ and } g_{k,k+1}x_{k-1}^2 + g_{k+1,k-1}x_k^2 + g_{k-1,k}x_{k+1}^2 = 0.$$

We multiply the first equation by $g_{k+1,k-1}$ and the second one by $-g_{k-2,k-1}$. Summing up yields

$$g_{k+1,k-1}g_{k-1,k}x_{k-2}^2 + (g_{k+1,k-1}g_{k,k-2} - g_{k-2,k-1}g_{k,k+1})x_{k-1}^2 - g_{k-2,k-1}g_{k-1,k}x_{k+1}^2 = 0.$$

By using the properties of gap tuples, we know that $g_{k+1,k-1} = g_{k+1,k-2} + g_{k-2,k-1}$ and $g_{k,k+1} = g_{k,k-2} + g_{k-2,k+1}$. Hence,

$$g_{k+1,k-1}g_{k,k-2} - g_{k-2,k-1}g_{k,k+1} = (g_{k+1,k-2} + g_{k-2,k-1})g_{k,k-2} - g_{k-2,k-1}(g_{k,k-2} + g_{k-2,k+1})$$

$$= g_{k+1,k-2}g_{k,k-2} - g_{k-2,k-1}g_{k-2,k+1} = g_{k+1,k-2}(g_{k,k-2} + g_{k-2,k-1}) = g_{k+1,k-2}g_{k,k-1}.$$

This yields

$$g_{k+1,k-1}g_{k-1,k}x_{k-2}^2 + g_{k+1,k-2}g_{k,k-1}x_{k-1}^2 - g_{k-2,k-1}g_{k-1,k}x_{k+1}^2 = 0.$$

Dividing by $-g_{k-1,k}$ and using $g_{k-1,k+1} = -g_{k+1,k-1}$, we obtain

$$g_{k-1,k+1}x_{k-2}^2 + g_{k+1,k-2}x_{k-1}^2 + g_{k-2,k-1}x_{k+1}^2 = 0.$$

This shows that the equation II. is satisfied.

Hence, the projection $(x_0 : \ldots : x_{l+2}) \mapsto (x_0 : \ldots : x_{k-1} : x_{k+1} : \ldots : x_{l+2})$, which deletes the k-th coordinate, induces a map $\pi_k : C_{l+1}(\mathbf{g}) \to C_l(\mathbf{g}^{(k)})$. This map is a rational map and by proposition 1.6.1 it is even a morphism. Now we can state the analogue of lemma 2.4 for the maps π_i. For the proof of this proposition we can argue along the lines of the proof of lemma 2.4 as well.

Proposition 2.5. *Let $\mathbf{g}$ be an $(l+1)$-gap tuple and let $\pi_k : C_{l+1}(\mathbf{g}) \to C_l(\mathbf{g}^{(k)})$ be the map induced by the projection $(x_0 : \ldots : x_{l+2}) \mapsto (x_0 : \ldots : x_{k-1} : x_{k+1} : \ldots : x_{l+2})$.*

1. *The morphism π_k is of degree 2 and if $(x_0 : \ldots : x_{k-1} : x_k : x_{i+1} : \ldots : x_{l+2})$ is a point in the preimage of $(x_0 : \ldots : x_{k-1} : x_{k+1} : \ldots : x_{l+2})$, then so is $(x_0 : \ldots : x_{k-1} : -x_i : x_{k+1} : \ldots : x_{l+2})$.*
2. *A point $(x_0 : \ldots : x_{k-1} : x_{k+1} : \ldots : x_{l+2})$ is a ramification point if and only if we have $x_k = 0$ for any $(x_0 : \ldots : x_{l+2}) \in \pi_i^{-1}(x_0 : \ldots : x_{k-1} : x_{k+1} : \ldots : x_{l+2})$.*

□

2.3 Calculation of the genus

The knowledge about the morphism $\pi : C_{l+1}(\mathbf{g}) \to C_l(\mathbf{g}^{(l+2)})$ provided in the previous subsection now allows us to determine the genus of the curves $C_l(\mathbf{g})$.

Proposition 2.6. *The curve $C_l(\mathbf{g})$ has genus $(l-2)2^{l-1}+1$ for any l-gap tuple $\mathbf{g}$.*

Proof:
We prove the proposition by induction. For $l = 1$ the curve $C_l(\mathbf{g})$ is given by the zero set of

$$g_{1,2}X_0^2 + g_{2,0}X_1^2 + g_{0,1}X_2^2 = 0$$

in $\mathbb{P}^2$. In this case the curve describes a conic and, hence, has genus 0 in accordance with the proposed formula.

Now let $\pi : C_{l+1}(\mathbf{g}) \to C_l(\mathbf{g}^{(l+2)})$ be the morphism which is induced by the projection $(x_0 : \ldots : x_{l+2}) \mapsto (x_0 : \ldots : x_{l+1})$. By lemma 2.4 this map has degree 2 and exactly 2^{l+1} ramification points with ramification index 2. The Hurwitz genus formula 1.6.6 now gives

$$2g_{l+1} - 2 = 2(2g_l - 2) + \sum_{P \in C_{l+1}} (e_\pi(P) - 1),$$

where g_l is genus of $C_l(\mathbf{g}^{(l+2)})$ and g_{l+1} that of the $C_{l+1}(\mathbf{g})$. Using the induction hypothesis for $C_l(\mathbf{g}^{(l+2)})$, we get

$$2g_{l+1} - 2 = (l-2)2^{l+1} + \sum_{P \in C_{l+1}} (e_\pi(P) - 1) = (l-2)2^{l+1} + 2^{l+1}.$$

Solving for g_{l+1} proves the proposition. □

It is important to remark that for $l = 2$ the above formula yields genus 1 and this means that $C_2(\mathbf{g})$ are elliptic curves. This observation is used later in this thesis.

2.4 Calculation of the degree

The degree is the last arithmetical quantity of the curves $C_l(\mathbf{g})$ we are interested in. We calculate it by using Bezout's theorem.

Proposition 2.7. *Let $\mathbf{g}$ be an l-gap tuple. Then $C_l(\mathbf{g})$ has degree 2^l.*

Proof:
We choose the hyperplane H given by $X_{l+1} = 0$. By the description of the tangent space of $C_l(\mathbf{g})$ in proposition 2.3 and since H is its own tangent space, we see that the tangent spaces of every point in the intersection $C_l(\mathbf{g}) \cap H$ span $\mathbb{P}^{l+1}$. This allows us to apply Bezout's theorem 1.5.5, and we conclude

$$\deg H \deg C_l(\mathbf{g}) = \deg(C_l(\mathbf{g}) \cap H).$$

Now by lemma 2.2 the intersection $C_l(\mathbf{g}) \cap H$ consists of 2^l points. Then, proposition 1.5.4 yields

$$\deg C_l(\mathbf{g}) = 2^l.$$

□

3 The Jacobian of $C_3(\mathbf{g})$ and elliptic curves

The main objective of this chapter is to derive bounds for the number of rational points on the curves $C_3(\mathbf{g})$ over a number field K using Bombieri's theorem. We have already computed the genus and the degree of the curves $C_3(\mathbf{g})$. However, in order to apply Bombieri's theorem a last important ingredient is still lacking.

In this section we are devoted to providing this ingredient: We obtain good bounds for the rank of the Jacobian of the curves $C_3(\mathbf{g})$ over the number field K.

To this end we first study the Jacobian of $C_3(\mathbf{g})$ over $\overline{K}$. We prove that the curves $C_3(\mathbf{g})$ are in some sense covered by elliptic curves of the form $C_2(\mathbf{g}')$ and we use this fact to relate the rank of the Jacobian $J(C_3(\mathbf{g}))(K)$ to the ranks of the elliptic curves $C_2(\mathbf{g}')(K)$.

Finally, we employ the results of chapter 4 and obtain explicit bounds for the rank of $J(C_3(\mathbf{g}))(K)$ in terms of $\mathbf{g}$.

3.1 A reduction to elliptic curves

In the following certain automorphisms of $C_3(\mathbf{g})$ play a crucial role. We observe that $C_3(\mathbf{g})$ admits automorphisms of the form

$$(x_0 : x_1 : x_2 : x_3 : x_4) \mapsto (\epsilon_0 x_0 : \epsilon_1 x_1 : \epsilon_2 x_2 : \epsilon_3 x_3 : \epsilon_4 x_4)$$

with $\epsilon_k = \pm 1$. We write t_k for the automorphism which only switches the sign of the k-th coordinate.

Automorphisms on $C_3(\mathbf{g})$ extend to automorphisms of $J(C_3(\mathbf{g}))$. This is a direct consequence of proposition 1.8.3 and we record this fact in the next lemma.

Lemma 3.1. *Let $t : C_3(\mathbf{g}) \to C_3(\mathbf{g})$ be an automorphism. Then t extends to an automorphism $t : J(C_3(\mathbf{g})) \to J(C_3(\mathbf{g}))$, which is given by*

$$\mathrm{cl}(\sum n_P P) \mapsto \mathrm{cl}(\sum n_P t(P)).$$

□

The next proposition relates the Jacobians of $C_3(\mathbf{g})$ and $C_2(\mathbf{g}^{(k)})$. Recall that $\mathbf{g}^{(k)}$ is the gap tuple arising from $\mathbf{g}$ by removing all entries with index containing k.

Proposition 3.2. *Let*

$$\pi_k : C_3(\mathbf{g}) \to C_2(\mathbf{g}^{(k)})$$

be the projection morphism that deletes the k-th coordinate.

1. *Then π_k induces a map*

   $$\pi_{k*} : J(C_3(\mathbf{g})) \to J(C_2(\mathbf{g}^{(k)})),$$

   which is a morphism and a group homomorphism. It is explicitly given by $\mathrm{cl}(\sum n_P P) \mapsto \mathrm{cl}(\sum n_P \pi_k(P))$.

2. *For any element $\mathrm{cl}(\sum n_P P)$ of the kernel of π_{k*} we have*

   $$\mathrm{cl}(\sum n_P P) = -\mathrm{cl}(\sum n_P t_k(P)).$$

Proof:

1. This follows from proposition 1.8.3.

2. Consider the pullback of divisors $\pi_k^* : \mathrm{Div}C_2(\mathbf{g}^{(k)}) \to \mathrm{Div}C_3(\mathbf{g})$ associated to the morphism $\pi_k : C_3(\mathbf{g}) \to C_2(\mathbf{g}^{(k)})$. For a divisor consisting of a single point Q the pullback is given by

   $$Q \mapsto \sum_{P \in \pi_k^{-1}(Q)} e_{\pi_k}(P)P.$$

   From proposition 2.5 we know that π_k is a morphism of degree 2. Additionally, proposition 2.5 implies that in the generic case the two points in $\pi_k^{-1}(Q)$ only differ by the sign in the k-th coordinate. Furthermore, proposition 2.5 shows that the k-th coordinate of $P \in \pi_k^{-1}(Q)$ is zero for any ramification point Q, and that the ramification index is equal to 2. This implies

   $$\pi_k^*(Q) = \sum_{P \in \pi_k^{-1}(Q)} e_{\pi_k}(P)P = P + t_k(P)$$

for some $P \in \pi_k^{-1}(Q)$ irrespective of whether Q is a ramification point or not.

Now let D be a divisor of degree 0 on $C_3(\mathbf{g})$ and $\mathrm{cl}(D)$ its class in $J(C_3(\mathbf{g})) = \mathrm{Pic}^0 C_3(\mathbf{g})$ and suppose that $\mathrm{cl}(D)$ is in the kernel of π_{k*}. If we set $D = \sum n_P P$, then we get $\mathrm{cl}(\sum n_P \pi_k(P)) = 0$ by the explicit description of π_{k*} in 1.

The pullback $\pi_k^* : \mathrm{Div} C_2(\mathbf{g}^{(k)}) \to \mathrm{Div} C_3(\mathbf{g})$ respects principal divisors and divisors of degree 0 by proposition 1.6.7. Therefore, we may apply it to elements of $J(C_2(\mathbf{g}^{(k)}))$ as follows

$$0 = \pi_k^*(\mathrm{cl}(\sum n_P \pi_k(P))) = \mathrm{cl}(\pi_k^*(\sum n_P \pi_k(P))) = \mathrm{cl}(\sum n_P \pi_k^*(\pi_k(P))).$$

From the description of the pullback given above, we now obtain

$$0 = \pi_k^*(\mathrm{cl}(\sum n_P \pi_k(P))) = \mathrm{cl}(\sum n_P (P + t_k(P)))$$

and therefore,

$$\mathrm{cl}(\sum n_P t_k(P)) = -\mathrm{cl}(\sum n_P P).$$

□

We combine the projections $\pi_0, \ldots, \pi_4$ to a single morphism and investigate its kernel.

Proposition 3.3. *Let*

$$p : C_3(\mathbf{g}) \to \prod_{k=0}^{4} C_2(\mathbf{g}^{(k)})$$

be the morphism $p = \pi_0 \times \ldots \times \pi_4$ that is induced by the projection morphisms $\pi_0, \ldots, \pi_4$.

1. *Then p induces a map $p_* : J(C_3(\mathbf{g})) \to \prod_{k=0}^{4} J(C_2(\mathbf{g}^{(k)}))$, which is a morphism and a group homomorphism.*
2. *All elements of the kernel of p_* have order 2.*

Proof:

1. This follows directly by combining the maps π_{k*} for $k = 0, \ldots, 4$ from the above proposition 3.2.

2. Consider the extension of the automorphism $t_k : C_3(\mathbf{g}) \to C_3(\mathbf{g})$ to the Jacobian $t_k : J(C_3(\mathbf{g})) \to J(C_3(\mathbf{g}))$. By lemma 3.1 this extension is given by

$$\mathrm{cl}(\sum n_P P) \mapsto \mathrm{cl}(\sum n_P t_k(P)).$$

Now, if $\mathrm{cl}(\sum n_P P)$ is in the kernel of p_*, it is also in the kernel of π_{k*} for any $i = 0, \dots, 4$. Then, from proposition 3.2 we obtain

$$\mathrm{cl}(\sum n_P P) = -\mathrm{cl}(\sum n_P t_k(P))$$

for $k = 0, \dots, 4$. This equivalent to

$$t_k(\mathrm{cl}(\sum n_P P)) = -\mathrm{cl}(\sum n_P P).$$

We concatenate the maps $t_0, \dots, t_4$ and conclude

$$(t_0 \circ \dots \circ t_4)(\mathrm{cl}(\sum n_P P)) = -\mathrm{cl}(\sum n_P P).$$

On the other hand, $t_0 \circ \dots \circ t_4$ is the identity on $C_3(\mathbf{g})$ because of

$$\begin{aligned}(t_0 \circ \dots \circ t_4)(x_0 : x_1 : x_2 : x_3 : x_4) &= (-x_0 : -x_1 : -x_2 : -x_3 : -x_4) \\ &= (x_0 : x_1 : x_2 : x_3 : x_4).\end{aligned}$$

Then, also the extension of $t_0 \circ \dots \circ t_4$ to $J(C_3(\mathbf{g}))$ given by lemma 3.1 is the identity map. This means $-\mathrm{cl}(\sum n_P P) = \mathrm{cl}(\sum n_P P)$ and the proposition is proved.

□

We now pass to number fields and investigate the points of the Jacobian $J(C_3(\mathbf{g}))$ of $C_3(\mathbf{g})$ over the number field K and no longer over its algebraic closure. Using the results from above, we obtain the next proposition relating the rank of $J(C_3(\mathbf{g}))(K)$ and the ranks of the elliptic curves $C_2(\mathbf{g}^{(k)})(K)$.

Proposition 3.4. *The rank of $J(C_3(\mathbf{g}))(K)$ is less than or equal to the sum of the ranks of the elliptic curves $C_2(\mathbf{g}^{(k)})(K)$ for $k = 0, \dots, 4$.*

Proof:
By the last proposition we obtain that the map $p_* : J(C_3(\mathbf{g})) \to \prod_{k=0}^{4} J(C_2(\mathbf{g}^{(k)}))$ results from combining the morphisms $\pi_{k*} : J(C_3(\mathbf{g})) \to J(C_2(\mathbf{g}^{(k)}))$ for $k = 0, \dots, 4$. These maps are explicitly given by

$$\mathrm{cl}(\sum n_P P) \mapsto \mathrm{cl}(\sum n_P \pi_k(P)).$$

Since the projection morphisms π_k are defined over K, it follows that also p_* is defined over K.

Hence, restricting the map p_* to the rational points over K yields a group homomorphism

$$p_* : J(C_3(\mathbf{g}))(K) \to \prod_{k=0}^{4} J(C_2(\mathbf{g}^{(k)}))(K).$$

The Mordell-Weil Theorem 1.8.1 states that $J(C_3(\mathbf{g}))(K)$ and $J(C_2(\mathbf{g}^{(k)}))(K)$ are finitely generated groups. Then, from the first isomorphism theorem we conclude that the image of $J(C_3(\mathbf{g}))(K)$ is a subgroup of $\prod_{k=0}^{4} J(C_2(\mathbf{g}^{(k)}))(K)$ having the same rank as $J(C_3(\mathbf{g}))(K)$ because the kernel of p_* only consists of elements of finite order according to proposition 3.3. Therefore, the rank of $J(C_3(\mathbf{g}))(K)$ is less than or equal to the rank of $\prod_{k=0}^{4} J(C_2(\mathbf{g}^{(k)}))(K)$.

The rank of $\prod_{k=0}^{4} J(C_2(\mathbf{g}^{(k)}))(K)$ can be computed as the sum of the ranks of $J(C_2(\mathbf{g}^{(k)})(K)$. Now the proposition follows because elliptic curves can be identified with its Jacobians. □

3.2 Explicit bounds for the rank of the Jacobian of $C_3(\mathbf{g})$

We now want to derive bounds for the rank of the Jacobian $C_3(\mathbf{g})$ over K only in terms of $\mathbf{g}$. Thus far we have reduced this question to the question of determining the ranks of the elliptic curves $C_2(\mathbf{g})$ over K. This is exactly the problem we have discussed in chapter 4. However, the results from chapter 4 are not directly applicable to the curves $C_2(\mathbf{g})$ since they are not given in Weierstrass form.

The goal in this section is to associate to every elliptic curve $C_2(\mathbf{g})$ another elliptic curve in Weierstrass form in order to derive explicit bounds for $C_2(\mathbf{g})$ in terms of $\mathbf{g}$. The construction of the associated elliptic curve originates from [ZB02].

A curve $C_2(\mathbf{g})$ is given by the equations

$$g_{1,2}X_0^2 + g_{2,0}X_1^2 + g_{0,1}X_2^2 = 0$$

$$g_{2,3}X_1^2 + g_{3,1}X_2^2 + g_{1,2}X_3^2 = 0$$

Now any point (x_0, x_1, x_2, x_3) on this curve satisfies the following relation.

$$(g_{1,2}x_0x_3)^2 = (g_{2,0}x_1^2 + g_{0,1}x_2^2)(g_{2,3}x_1^2 + g_{3,1}x_2^2)$$

This can be seen directly by looking at the defining equations, moving the term with the coefficient $g_{1,2}$ to the right hand side and then multiplying both equations.

Multiplying both sides by $g_{2,0}^2 g_{2,3}^2 \frac{x_1^2}{x_2^6}$ yields

$$y^2 = x(x + g_{0,1}g_{2,3})(x + g_{3,1}g_{2,0}),$$

where $y = g_{1,2}g_{2,0}g_{2,3}\frac{x_0x_1x_3}{x_2^3}$ and $x = g_{2,0}g_{2,3}\frac{x_1^2}{x_2^2}$.

This motivates the following definition.

Definition. Let $\mathbf{g}$ be a 2-gap tuple. Then the curve in $\mathbb{P}^2$ given by the Weierstrass equation

$$Y^2 = X(X + g_{0,1}g_{2,3}Z)(X + g_{3,1}g_{2,0}Z)$$

is called the elliptic curve associated to $\mathbf{g}$ and will be denoted by $E(\mathbf{g})$.

This definition is justified by the following proposition which shows that $E(\mathbf{g})$ is in fact an elliptic curve.

Proposition 3.5. *Let* $\mathbf{g}$ *be a* 2*-gap tuple. Then* $E(\mathbf{g})$ *is an elliptic curve and has discriminant*

$$-16 \prod_{i<j} g_{i,j}^2.$$

Proof:
The curve $E(\mathbf{g})$ is given in Weierstrass form. Hence, by proposition 1.9.3 it is an elliptic curve if and only if $\Delta \neq 0$. Therefore, we have to calculate the discriminant.

Since $\mathbf{g}$ is a gap tuple, we have

$$g_{2,3} = g_{2,0} + g_{0,3} \qquad \text{and} \qquad g_{3,1} = g_{0,1} - g_{0,3}.$$

This yields,

$$g_{3,1}g_{2,0} - g_{0,1}g_{2,3} = (g_{0,1} - g_{0,3})g_{2,0} - g_{0,1}(g_{2,0} + g_{0,3}) = -g_{2,0}g_{0,3} - g_{0,1}g_{0,3} = -g_{0,3}g_{2,1}.$$

By definition, the discriminant of an elliptic curve is -16 times the squared differences of the roots. So we have

$$\begin{aligned}\Delta(E(\mathbf{g})) &= -16(g_{0,1}g_{2,3})^2(g_{1,3}g_{0,2})^2(g_{1,3}g_{0,2} - g_{0,1}g_{2,3})^2 \\ &= -16(g_{0,1}g_{2,3})^2(g_{1,3}g_{0,2})^2(-g_{0,3}g_{2,1})^2.\end{aligned}$$

This is non-zero because the entries of a gap tuple are non-zero integers.

By using $g_{i,j} = -g_{j,i}$ from the properties of gap tuples we can write the discriminant as follows which can be written as $16 \prod_{i<j} g_{i,j}^2$. □

Now we see how $E(\mathbf{g})$ and $C_2(\mathbf{g})$ are related.

Proposition 3.6. *Let* $\mathbf{g}$ *be a 2-gap tuple.*

1. *The map* $\phi : C_2(\mathbf{g}) \to E(\mathbf{g})$*, given by*

$$(x_0 : x_1 : x_2 : x_3) \mapsto (g_{2,0}g_{2,3}x_1^2x_2 : g_{1,2}g_{2,0}g_{2,3}x_0x_1x_3 : x_2^3),$$

   is an non-constant isogeny and is defined over K*.*

2. *The rank of* $C_2(\mathbf{g})(K)$ *is less than or equal to the rank of* $E(\mathbf{g})(K)$*.*

3. *There exists a constant* c *only depending on* K *such that the rank of* $C_2(\mathbf{g})(K)$ *is bounded by* $c\sum_{i<j}\omega(g_{ij})$*.*

Proof:

1. If $x_2 \neq 0$, then $(x_0 : x_1 : x_2 : x_3) \mapsto (g_{2,0}g_{2,3}x_1^2\frac{x_1^2}{x_2^2} : g_{1,2}g_{2,0}g_{2,3}\frac{x_0x_1x_3}{x_2^3} : 1)$. The calculation at the beginning of this subsection shows that the image lies in the affine part of $E(\mathbf{g})$. If $x_2 = 0$, then $(x_0 : x_1 : x_2 : x_3) \mapsto (0 : 1 : 0)$ being the point at infinity of $E(\mathbf{g})$. Hence, ϕ is a map from $C_2(\mathbf{g})$ to $E(\mathbf{g})$. Additionally, ϕ is a rational map. Proposition 1.6.1 implies that ϕ even is a morphism. Since $C_2(\mathbf{g})$ is an elliptic curve but has no distinguished group law, we can define the group law in a way that turns ϕ into an isogeny.

2. From proposition 1.9.1 we conclude that ϕ is group homomorphism and $\ker\phi$ is a finite group. This is not changed when we restrict ϕ to the K-rational points of $C_2(\mathbf{g})$ because ϕ is defined over K. Now, the assertion on the ranks follows because the image of $C_2(\mathbf{g})(K)$ is a subgroup of $E(\mathbf{g})(K)$ having the same rank as $C_2(\mathbf{g})(K)$ by the first isomorphism theorem.

3. By proposition 4.4.3 we find a constant c depending only on K such that the rank of $E(\mathbf{g})(K)$ is bounded by

$$c\omega(-16\prod_{i<j} g_{i,j}^2) \leq c(1 + \sum_{i<j}\omega(g_{ij})).$$

   Since $\mathbf{g}$ contains entries different from ±1, we can redefine c in such a way that the rank of $E(\mathbf{g})(K)$ is bounded by

$$c\sum_{i<j}\omega(g_{ij}).$$

□

Now we have gathered all the information which is necessary to obtain a bound for the rank of the Jacobian of the curves $C_3(\mathbf{g})$ only in terms of $\mathbf{g}$.

Proposition 3.7. *Let* $\mathbf{g}$ *be a* 3*-gap tuple. Then there exists a constant* c *only depending on* K *such that the rank of the Jacobian of* $J(C_3(\mathbf{g}))(K)$ *is bounded by*

$$c \sum_{i<j} \omega(g_{ij}).$$

Proof:
By proposition 3.4 the rank of $J(C_3(\mathbf{g}))(K)$ is less than or equal to the sum of the ranks of the elliptic curves $C_2(\mathbf{g}^{(k)})(K)$ for $k = 0, \dots, 4$. Their ranks can be bounded using proposition 3.6 above. So, we obtain that the rank of $J(C_3(\mathbf{g}))(K)$ is less than or equal to

$$\sum_{k=0}^{4} c \sum_{i<j} \omega(g_{ij}^{(k)}).$$

By close inspection we see that this is just

$$c \sum_{i<j} \omega(g_{ij}).$$

□

4 An effective version of Faltings' theorem by Bombieri

In his 1983 paper [Fal83] Faltings proved Mordell's conjecture claiming that every curve of genus greater than 1 defined over a number field has only finitely many rational points. However, his proof does not provide explicit bounds for the number of rational points.

By a completely different approach Vojta in [Voj91] was able to prove Faltings' theorem. Based on this work, Bombieri in [Bom90] found a simplified proof of Faltings' theorem in which he replaced the usage of some deep theorems in the proof of Vojta by more elementary considerations.

Although this proof is much more technical and not as elegant as the previous one by Vojta, it has the undeniable advantage that it provides an explicit bound for the number of rational points on the curve.

In order to apply this theorem in the situation of [BGP92], Bombieri, Granville and Pintz still had to generalize the result of [Bom90] slightly. We now state their theorem (See [BGP92], page 12) in a simplified version that suffices for our purposes.

Theorem 4.1. *Let C be a smooth projective curve of genus at least 2 defined over a number field K and let $h(C)$ be the lowest upper bound for the height of a set of homogenous generators for the vanishing ideal of C relative to the projective embedding.*

Then the number of K-rational points of C with height greater than $\kappa(h(C)+1)$ is at most

$$12((\log(\deg C))+1)7^r,$$

where r is the rank of the Jacobian of C over K. Here, the constant parameter κ only depends on the degree and the embedding dimension of C.

Using this deep theorem and all the results proved in this chapter, we obtain a bound for the number of rational points on the curves $C_3(\mathbf{g})$.

Theorem 4.2. *Let K be a number field. Let $\mathbf{g}$ be a 3-gap tuple and $H \geq 3$ be a number greater than or equal to the absolute value of all entries of $\mathbf{g}$. Then the number of points on $C_3(\mathbf{g})(K)$ with height greater than $\kappa \log H$ is at most*

$$7^{c\sum\limits_{i<j}\omega(g_{ij})}$$

with some constants κ, c not depending on $\mathbf{g}$.

Proof:
The coefficients of the defining equations of the curves $C_3(\mathbf{g})$ are the entries of $\mathbf{g}$. Since these integers have absolute value less than H, we obtain that the defining equations have a height that is bounded by $\log H$. Hence, an upper bound for a set of generators of the homogenous ideal of $C_3(\mathbf{g})$ is given by $\log H$.

The genus of $C_3(\mathbf{g})$ is 5 by proposition 2.6 and the degree is 8 by proposition 2.7. Since the curves $C_3(\mathbf{g})$ have all the same degree and the same imbedding dimension, the above theorem yields the existence of constants c and κ such that the number of points on $C_3(\mathbf{g})(K)$ having height greater than $\kappa(\log H + 1)$ is bounded by

$$12(\log 8 + 1)7^r.$$

Since $H \geq 3$, we can redefine κ such that there are at most $12(\log 8 + 1)7^r$ points on $C_3(\mathbf{g})(K)$ with height greater than or equal to $\kappa \log H$.

From proposition 3.7 we obtain that the rank of the Jacobian of $C_3(\mathbf{g})$ over K is bounded by

$$c\sum_{i<j}\omega(g_{ij}),$$

where c is some constant only depending on K. Now the theorem follows by redefining c appropriately. □

Chapter 6

Second Case: Proving the asymptotics

In the last two chapters, dealing with the second case of the proof of Theorem I, we studied rational points on the algebraic curves $C_3(\mathbf{g})$ rather than squares in arithmetic progressions. This was motivated by the observation that squares in arithmetic progressions are related to points on these curves.

Now we have to take the step back and return to squares in arithmetic progressions. Unfortunately, the results obtained for the rational points on $C_3(\mathbf{g})$ cannot be transferred directly to the situation of squares in arithmetic progressions, since there is, in general, no one-to-one correspondence between the squares in an arithmetic progression and the rational points on the associated curve $C_3(\mathbf{g})$.

However, such a strong statement is not necessary for our purposes either. It suffices to pursue a similar strategy as the one used by Bombieri, Granville and Pintz. They proved that for arithmetic progressions $(qn + d)_{n\in\mathbb{N}}$, where q and d are coprime, there is indeed something like a one-to-one correspondence between squares and the rational points on $C_3(\mathbf{g})$. Furthermore, they showed that this is sufficient to capture the general case.

We follow a similar approach. However, we first extract the precise technical conditions which are necessary to transfer the bounds for the number of K-rational points on the curves $C_3(\mathbf{g})$ to bounds for the number of squares in the arithmetic progression over K. These technical requirements are comprised into the notion of the MHU condition.

Then, assuming the truth of the MHU condition for a number field K, we can proceed analogously to the original paper. We use the same combinatorial argument as in [BGP92] in order to prove Theorem I.

The investigation of the MHU condition will be postponed to the next chapter.

1 The MHU condition

The MHU condition consists of two parts. The first one is modeled to ensure that there is a one-to-one correspondence between the elements in an arithmetic progression $(qn+d)_{n\in\mathbb{N}}$, which are squares over a number field K, and the K-rational points on the associated curve $C_3(\mathbf{g})$ having a big height.

Definition. Let K be a number field and let $\mu_1, \mu_2 > 0$. We call a pair (q, d) of integers a (μ_1, μ_2)-**HU pair** over K if it satisfies the following conditions.

1. Height condition:
   Suppose $x_i \in K$ such that $qn_i + d = x_i^2$ for some $n_i \in \mathbb{N}$ and $i = 0, \dots, l+1$. Let $\mathbf{g}$ be the l-gap tuple associated to $\mathbf{n} = (n_0, \dots, n_{l+1})$. Then the point $\mathbf{x} = (x_0 : \dots : x_{l+1})$ lying on $C_l(\mathbf{g})$ satisfies
   $$h(\mathbf{x}) \geq \mu_1 h(q) - \mu_2.$$

2. Uniqueness condition:
   Let $\mathbf{g}$ be an l-gap tuple with entries that are smaller than some natural number N and suppose that $\mathbf{x}$ is a point on $C_l(\mathbf{g})$ over K.

   If $h(q) \geq 2\log N$, then there is at most one tuple $\mathbf{n} = (n_0, \dots, n_{l+1})$ of natural numbers such that $qn_i + d = x_i^2$, where $1 \leq n_i \leq N$ and $x_i \in K$ satisfying $\mathbf{x} = (x_0 : \dots : x_{l+1})$, and $\mathbf{g}$ is the gap tuple corresponding to $\mathbf{n}$.

It would be desirable that any pair (q, d) were a (μ_1, μ_2)-HU pair. However, this is not true in general. Fortunately, for the purpose of this thesis it suffices to show that there are many HU pairs such that they cover all other pairs in a certain sense. This is the second part of the MHU condition.

Definition. We say that a number field satisfies the **MHU condition** if there exist $\mu_1, \mu_2 > 0$ such that for any $q, d \in \mathbb{Z}$ there exists a (μ_1, μ_2)-HU pair (q', d') such that
$$S_{q,d,N} \leq S_{q',d',N}.$$

If this is the case, we say that the pair (q, d) is **majorized** by the pair (q', d').

2 Relating squares and points

In this section we see how we can count the number of squares in certain arithmetic progressions and relate this number to rational points on curves.

More precisely, we show that 5-tuples of squares in some arithmetic progression $(qn+d)_{n\in\mathbb{N}}$ over a number field K are in a one-to-one correspondence with the K-rational points of large height on the associated curves $C_3(\mathbf{g})$, if q and d form an HU pair.

This could be done in a rather straightforward manner like indicated on page 2 of [BGP92]. However, it has already been shown in [BGP92] that one can even obtain a better bound for the number of squares in arithmetic progressions with only a little more effort. We also pursue this way.

Definition. For $q, d \in \mathbb{Q}$ and $r, m, N \in \mathbb{N}$ we define

$$\mathcal{S}_{q,d,N}(r,m) = \{n \leq N | qn + d = x^2 \text{ for some } x \in K \text{ and } n \equiv r \mod m\}$$

and

$$S_{q,d,N}(r,m) = |\mathcal{S}_{q,d,N}(r,m)|.$$

In order to simplify the notation we introduce the following abbreviation:

Definition. Let $\mathbf{g}$ be a 3-gap tuple. By $\mathrm{N}_h(\mathbf{g})$ we denote the number of K-rational points on $C_3(\mathbf{g})$ that have height greater than or equal to h.

Now we can state and prove the main proposition of this section.

Proposition 2.1. *Let $q, d \in \mathbb{Z}$ form a (μ_1, μ_2)-HU pair for some $\mu_1, \mu_2 > 0$. Then for any $N \in \mathbb{N}$ with $h(q) \geq 2\log N$ and for any $M \in \mathbb{N}$ we have*

$$\sum_{m=M+1}^{\infty} \sum_{r=1}^{m} \binom{S_{q,d,N}(r,m)}{5} \leq \sum_{\mathbf{g}' \leq \frac{N}{M}} \mathrm{N}_{\lambda\mu_1 h(q) - \mu_2}(\mathbf{g}').$$

Here and in the following $\mathbf{g}' \leq \frac{N}{M}$ means that all entries of $\mathbf{g}'$ have absolute value less than or equal to $\frac{N}{M}$.

Proof:
Obviously, the left hand side of this inequality is the cardinality of the set

$$\bigcup_{m=M+1}^{\infty} \bigcup_{r=1}^{m} \{(n_0, n_1, n_2, n_3, n_4, m) | 0 \leq n_0 < n_1 < \ldots < n_4 \leq N, n_i \in \mathcal{S}_{q,d,N}, n_i \equiv r \bmod m\},$$

which can be rewritten as

$$\{(n_0, n_1, n_2, n_3, n_4, m) | m > M, 0 \leq n_0 < n_1 < \ldots < n_4 \leq N, n_i \in \mathcal{S}_{q,d,N}, m | n_i - n_j\}.$$

We show that each tuple of this set corresponds to exactly one point on a curve $C_3(\mathbf{g}')$ with $\mathbf{g}'$ having entries not exceeding $\frac{N}{M}$.

For any tuple $(n_0, n_1, n_2, n_3, n_4, m)$ we have $qn_i + d = x_i^2$ for some $x_i \in K$. Therefore, $\mathbf{x}$ is a point on the curve $C_3(\mathbf{g})$, where $\mathbf{g}$ is the gap tuple associated to $\mathbf{n} = (n_0, \dots, n_4)$. Recall that this curve is given by the equations

$$(n_{i+1} - n_{i+2})X_i^2 + (n_{i+2} - n_i)X_{i+1}^2 + (n_i - n_{i+1})X_{i+2}^2 = 0$$

for $i = 0, \dots, 2$.

Since all n_i have the same residue modulo m, each coefficient is divisible by m. Hence, we do not change the curve if we divide out m in every coefficient of the defining equation. This implies that $\mathbf{x}$ is a point on the curve $C_3(\mathbf{g}')$, where $\mathbf{g}'$ emerges form $\mathbf{g}$ by dividing every entry by m. This implies that all entries of $\mathbf{g}'$ are less than or equal to $\frac{N}{M}$.

As (q, d) is a (μ_1, μ_2)-HU pair, it follows from the height condition that

$$\mathbf{x} \in \mathrm{N}_{\mu_1 h(q) - \mu_2}(\mathbf{g}) = \mathrm{N}_{\mu_1 h(q) - \mu_2}(\mathbf{g}').$$

Finally, the uniqueness condition implies that no other tuple $(n_0, n_1, n_2, n_3, n_4, m)$ can give rise to the same point $\mathbf{x}$. □

We briefly review what we have achieved. From the last proposition it will be possible to obtain bounds for $S_{q,d,N}$. However, the far more important observation is that the right hand side of the inequality in the last proposition does not depend on the actual values of q and d (as long as q has sufficiently large height). Therefore, any bound which we derive will be uniform in q and d.

Now it is rather clear that the next step should be estimating the right hand side of

$$\sum_{m=M+1}^{\infty} \sum_{r=1}^{m} \binom{S_{q,d,N}(r,m)}{5} \leq \sum_{\mathbf{g}' \leq \frac{N}{M}} \mathrm{N}_{\lambda \mu_1 h(q) - \mu_2}(\mathbf{g}'),$$

and then finding a bound for the size of $\mathcal{S}_{q,d,N}$. This is the objective of the next (and last) two sections.

3 Estimation of the number of rational points

Proposition 3.1. *Let* $\mathbf{g}$ *be a* 3*-gap tuple and let* $H \geq 3$ *be a number greater than or equal to the absolute values of the entries of* $\mathbf{g}$*. Let* κ *be the constant appearing in theorem 5.4.2. Then*

$$\mathrm{N}_{\kappa \log H}(\mathbf{g}) \leq \sum_{i<j} 7^{c\omega(g_{ij})},$$

where c *is a constant not depending on* $\mathbf{g}$*.*

Proof:
Theorem 5.4.2 shows

$$\mathrm{N}_{\kappa \log H}(\mathbf{g}) \leq 7^{c \sum\limits_{i<j} \omega(g_{ij})}$$

for some constant c not depending on $\mathbf{g}$. Observe that the sum in the exponent has exactly 10 summands since we are dealing with a 3-gap tuple. We obtain

$$\begin{aligned}\mathrm{N}_{\kappa \log H}(\mathbf{g}) &\leq 7^{\frac{1}{10}\sum_{i<j} 10c\omega(g_{ij})} = \sqrt[10]{7^{\sum_{i<j} 10c\omega(g_{ij})}} \\ &= \sqrt[10]{\prod_{i<j} 7^{10c\omega(g_{ij})}} \leq \frac{1}{10}\sum_{i<j} 7^{10c\omega(g_{ij})},\end{aligned}$$

where the last inequality is the inequality of the arithmetic and geometric mean. Now the assertion follows by redefining c to $10c$. □

The next result gives a bound for the right hand side of the inequality in proposition 3.1. The main ingredient is an estimate for the sum in which the ω-function occurs as the exponent, which we proved in the first chapter.

Proposition 3.2. *There exists a constant* c *such that for any natural number* $N \geq 3$ *and any natural number* M *we have*

$$\sum_{\mathbf{g}' \leq \frac{N}{M}} \mathrm{N}_{\kappa \log N}(\mathbf{g}') \leq \frac{N^4}{M^4} \log^c N,$$

where κ *is the constant appearing in theorem 5.4.2.*

Proof:
Since the absolute values of the entries of the gap tuples that appear in the above sum are bounded by N, proposition 3.1 yields

$$\sum_{\mathbf{g}' \leq \frac{N}{M}} \mathrm{N}_{\kappa \log N}(\mathbf{g}') \leq \sum_{\mathbf{g}' \leq \frac{N}{M}} \sum_{j<k} 7^{c\omega(g'_{jk})}.$$

In the right sum any non-zero integer with absolute value less than or equal to $\frac{N}{M}$ might occur for some g'_{ij}. From the definition of l-gap tuples it follows that for any index pair (i,j) of a gap tuple there are l other index pairs such that the gap tuple is completely determined by specifying the values of the entries at these indices. Since there are $2\frac{N}{M}$ non-zero integers with absolute value less than or equal to $\frac{N}{M}$, and since all these might occur at any of the 10 index pairs of the gap tuple, we conclude that there are at most $10\left(2\frac{N}{M}\right)^3$ gap tuples containing a specific integer value.

Using this fact, we obtain

$$\sum_{\mathbf{g}' \le \frac{N}{M}} \sum_{i<j} 7^{c\omega(g'_{ij})} \le 80 \left(\frac{N}{M}\right)^3 \cdot 2 \sum_{n < \frac{N}{M}} 7^{c\omega(n)}.$$

Now lemma 1.1.1 yields

$$\sum_{n < \frac{N}{M}} 7^{c\omega(n)} \le c' \frac{N}{M} \log^{7^c} \frac{N}{M}$$

for some constant $c' > 0$. This implies

$$\sum_{\mathbf{g}' \le \frac{N}{M}} \sum_{i<j} 7^{c\omega(g'_{ij})} \le 160c' \left(\frac{N}{M}\right)^4 \log^{7^c} N.$$

Now the assertion follows by redefining c appropriately. □

4 Proof of Theorem I

We now combine all results from the last sections in order to find a bound for $S_{q,d,N}$ uniformly in q and d. The details of the proof are rather technical. The main idea of the proof is due to Bombieri, Granville and Pintz (See [BGP92], pages 15 and 16). We have to modify it at some points in order to make it work in the more general situation. However, these changes are only of technical nature.

Subsequently, we finally prove Theorem I.

Theorem 4.1. *Let $\mu_1, \mu_2 > 0$ and let κ be the constant appearing in theorem 5.4.2. Then there exists a constant c such that for all natural numbers $N \ge 3$ and all (μ_1,μ_2)-HU pairs (q,d) with $h(q) \ge \max\{\frac{\kappa \log N + \mu_2}{\mu_1}, 2\log N\}$ it holds*

$$S_{q,d,N} \le N^{\frac{2}{3}} \log^c N.$$

Proof:
For any $M \in \mathbb{N}$,

$$MS_{q,d,N} = \sum_{M<m\leq 2M} S_{q,d,N} = \sum_{M<m\leq 2M} \sum_{r=1}^{m} S_{q,d,N}(r,m).$$

For the inner sum we either have $S_{q,d,N}(r,m) \leq 5$ or $S_{q,d,N}(r,m) \leq \binom{S_{q,d,N}(r,m)}{5}$. This yields

$$MS_{q,d,N} \leq \sum_{M<m\leq 2M} \sum_{r=1}^{m} \left(5 + \binom{S_{q,d,N}(r,m)}{5}\right).$$

The first sum can be estimated in the following way

$$\sum_{M<m\leq 2M} \sum_{r=1}^{m} 5 = \sum_{M<m\leq 2M} 5m \leq 5\frac{M(M+1)}{2},$$

while the second sum is less than or equal to

$$\sum_{m=M+1}^{\infty} \sum_{r=1}^{m} \binom{S_{q,d,N}(r,m)}{5}.$$

All assumptions in proposition 2.1 are satisfied, and, hence, we derive

$$\sum_{m=M+1}^{\infty} \sum_{r=1}^{m} \binom{S_{q,d,N}(r,m)}{5} \leq \sum_{\mathbf{g}'\leq \frac{N}{M}} \mathrm{N}_{\mu_1 h(q)-\mu_2}(\mathbf{g}') \leq \sum_{\mathbf{g}'\leq \frac{N}{M}} \mathrm{N}_{\kappa \log N}(\mathbf{g}').$$

We are now able to apply proposition 3.2 and we get

$$\sum_{m=M+1}^{\infty} \sum_{r=1}^{m} \binom{S_{q,d,N}(r,m)}{5} \leq \frac{N^4}{M^4} \log^c N$$

for some constant c.

Combining the two estimates from above, we obtain

$$S_{q,d,N} \leq 5\frac{M+1}{2} + \frac{N^4}{M^5} \log^c N.$$

Balancing this equation with $M = N^{\frac{2}{3}}$ yields

$$S_{q,d,N} \leq N^{\frac{2}{3}} \log^c N$$

if we redefine c in an appropriate way. □

We have found a uniform bound for $S_{q,d,N}$ when q has big height. This completes the treatment of the second case. Together with the theorem in the case of q having small height we can prove Theorem I.

Theorem I. *Let K be a number field that is Galois over $\mathbb{Q}$ and that satisfies the MHU condition. Then*

$$\max_{q,d\in\mathbb{Q}} S_{q,d,N} = O(N^{\frac{2}{3}} \log^c N),$$

where the implicit constants depend only on K.

Proof:
Since K satisfies the MHU condition, there exist $\mu_1, \mu_2 > 0$ such that all pairs can be majorized by (μ_1, μ_2)-HU pairs. Let κ be the constant appearing in theorem 5.4.2. Choose λ such that $\lambda \log N \geq \max\{\frac{\kappa \log N + \mu_2}{\mu_1}, 2\log N\}$ for all $N \in \mathbb{N}$ with $N \geq 3$.

Let $N \geq 3$ and consider $q, d \in \mathbb{Z}$. Then there exists a (μ_1, μ_2)-HU pair (q', d') which majorizes (q, d). We distinguish two cases

1. $h(q') \leq \lambda \log N$:
   Then by theorem 3.2.2 there exists a constant c_1, which only depends on λ and K, such that
   $$S_{q',d',N} \leq c_1\sqrt{N}\log N.$$

2. $h(q') \geq \lambda \log N$:
   In this case we can apply theorem 4.1 proved just before and we obtain
   $$S_{q',d',N} \leq N^{\frac{2}{3}} \log^{c_2} N$$
   for some constant c_2 only depending on λ and K.

Combining both cases, yields

$$S_{q,d,N} \leq S_{q',d',N} \leq \max\{c_1\sqrt{N}\log N, N^{\frac{2}{3}} \log^{c_2} N\}.$$

By choosing suitable constants, the theorem follows. □

Chapter 7

The MHU condition

This chapter is devoted to the problem of finding concrete examples of number fields which satisfy the MHU condition.

In the first two sections we show that over any number field every pair (q, d) of coprime integers q and d satisfies the height condition and the uniqueness condition in the definition of HU pairs.

In order to establish the MHU condition it remains to show that any pair (q, d) is majorized by a coprime pair (q', d'). However, we were not able to prove this for all number fields.

Though, for a special class of number fields we can indeed prove the MHU condition by generalizing an argument of Bombieri, Granville and Pintz from [BGP92]. This is established in the third section and eventually leads to a proof of Theorem II. Subsequently, we provide a counterexample which shows that this argument cannot be extended further in order to demonstrate the validity of the MHU condition in a more general setting.

1 The height condition

The purpose of this section is to show that over any number field K all the pairs (q, d), where q and d are coprime integers, satisfy the height condition in the definition of a (μ_1, μ_2)-HU pair for some $\mu_1, \mu_2 > 0$. Actually, we even prove that μ_1, μ_2 only depend on the number field K.

The principal idea is to mimic the proof given by Bombieri, Granville and Pintz in the rational case (See lemma 4 in [BGP92]). Due to some additional difficulties, which arise in the case of number fields, the proof is considerably more technical.

Lemma 1.1. *Let K be a number field and let q, d be coprime integers. Suppose $x_i \in K$ such that $qn_i + d = x_i^2$ for some $n_i \in \mathbb{N}$ and $i = 0, \ldots, l+1$. We define $f = \gcd(x_0^2, \ldots, x_{l+1}^2)$. Then*

$$|f| \leq \max_{i \neq j} |n_i - n_j|.$$

Proof:
For any $i \neq j$

$$x_i^2 - x_j^2 = q(n_i - n_j).$$

Here f divides the left hand side of the equation and, hence, also the right hand side. Furthermore, f does not have any factor in common with q, since otherwise it would follow from

$$qn_i + d = x_i^2$$

that q and d had also a factor in common.

This means that f divides $n_i - n_j$ and the lemma is proved. □

We now prove the height condition for pairs (q, d), where q and d are coprime.

Proposition 1.2. *Let K be a number field and let q, d be coprime integers. Suppose $x_i \in K$ such that $qn_i + d = x_i^2$ for some $n_i \in \mathbb{N}$ and $i = 0, \ldots, l+1$. Then $\mathbf{x} = (x_1 : \ldots : x_{l+1})$ is a point on $C_l(\mathbf{g})$, where $\mathbf{g}$ is the gap tuple associated to $\mathbf{n} = (n_0, \ldots, n_{l+1})$. For the height of $\mathbf{x}$ we have the estimate*

$$h(\mathbf{x}) \geq \mu_1 h(q) - \mu_2$$

with $\mu_1 = \frac{1}{2}$ and $\mu_2 = \frac{1}{2}[K : \mathbb{Q}] \log 2$.

Proof:
Let f be the greatest common divisor of $x_0^2, \ldots, x_{l+1}^2$. In order to determine $h(\mathbf{x})$ over K, we can equivalently determine it over $K(\sqrt{f})$. Furthermore, the height of $\mathbf{x}$ is independent of its representative and, hence, we can work with the representative $(\frac{x_0}{\sqrt{f}} : \ldots : \frac{x_{l+1}}{\sqrt{f}})$ instead of $(x_0 : \ldots : x_{l+1})$.

We now calculate

$$h(\mathbf{x}) = \sum_{\nu} \max_i \log \left| \frac{x_i}{\sqrt{f}} \right|_{\nu},$$

where the sum ranges over all valuations of $K(\sqrt{f})$.

We distinguish between the two types of valuations ν on $K(\sqrt{f})$. The non-archimedean valuations, which arise from p-adic valuations on $\mathbb{Q}$, and the archimedean ones arising from the ordinary absolute value.

1. The non-archimedean case:
   Let p be a prime and let i_p the index such that x_i attains the maximum in $\max_i \log \left|\frac{x_i^2}{f}\right|_p$.

   Consider all valuations ν that lie above p in $K(\sqrt{f})$. We obtain

$$\sum_{\nu|p} \max_i \log \left|\frac{x_i}{\sqrt{f}}\right|_\nu = \frac{1}{2}\sum_{\nu|p} \max_i \log \left|\frac{x_i^2}{f}\right|_\nu \geq \frac{1}{2}\sum_{\nu|p} \log \left|\frac{x_{i_p}^2}{f}\right|_\nu$$
$$= \frac{1}{2}\log \left|\frac{x_{i_p}^2}{f}\right|_p = \frac{1}{2}\log \max_i \left|\frac{x_i^2}{f}\right|_p \geq 0.$$

   We shall explain the last inequality:
   Since f is the greatest common divisor of $x_0^2, \dots, x_{l+1}^2$, there is some i such that p does not divide $\frac{x_i^2}{f}$. Therefore, the valuation of $\frac{x_i^2}{f}$ is greater than or equal to 1. Taking the logarithm, yields this inequality.

2. The archimedean case:
   First of all, we note that

$$\max_i \left|\frac{x_i^2}{f}\right|_\nu \geq \frac{1}{2}\left|\frac{x_i^2}{f} - \frac{x_j^2}{f}\right|_\nu$$

   by the triangle inequality for all $i \neq j$.

   Similar to the non-archimedean case, we consider all archimedean valuations that lie above the ordinary absolute value. These are all the archimedean valuations on $K(\sqrt{f})$. We obtain

$$\sum_{\nu|\infty} \max_i \log \left|\frac{x_i}{\sqrt{f}}\right|_\nu \geq \frac{1}{2}\sum_{\nu|\infty} \max_i \log \left|\frac{x_i^2}{f}\right|_\nu \geq \frac{1}{2}\sum_{\nu|\infty} \log \frac{1}{2}\left|\frac{x_i^2}{f} - \frac{x_j^2}{f}\right|_\nu$$
$$= \frac{1}{2}\sum_{\nu|\infty} \log \frac{1}{2} + \frac{1}{2}\sum_{\nu|\infty} \log \left|\frac{x_i^2}{f} - \frac{x_j^2}{f}\right|_\nu$$

   for all $i \neq j$. As explained in the first chapter, there are exactly $[K(\sqrt{f}) : \mathbb{Q}]$ valuations lying above ∞. Since $[K(\sqrt{f}) : \mathbb{Q}] \leq 2[K : \mathbb{Q}]$, we find for all $i \neq j$

$$\sum_{\nu|\infty} \max_i \log \left|\frac{x_i}{\sqrt{f}}\right|_\nu \geq \frac{1}{2}\log \left|\frac{x_i^2}{f} - \frac{x_j^2}{f}\right| - [K : \mathbb{Q}]\log 2.$$

   By observing

$$\left|\frac{x_i^2}{f} - \frac{x_j^2}{f}\right| = |q|\frac{|n_i - n_j|}{|f|}$$

for all $i \neq j$ and applying lemma 1.1, we finally obtain

$$\sum_{\nu|\infty} \max_i \log \left| \frac{x_i}{\sqrt{f}} \right|_\nu \geq \frac{1}{2} \log |q| - [K : \mathbb{Q}] \log 2.$$

Combining the archimedean and non-archimedean valuations, we determine the height of $\mathbf{x}$ as follows:

$$h(\mathbf{x}) = \sum_{\nu} \max_i \log \left| \frac{x_i}{\sqrt{f}} \right|_\nu \geq \frac{1}{2} \log |q| - [K : \mathbb{Q}] \log 2 = \frac{1}{2} h(q) - [K : \mathbb{Q}] \log 2.$$

□

2 The uniqueness condition

In this section we prove that a pair (q, d), where q and d are coprime integers, satisfies the uniqueness condition over any number field. The proof is essentially the same as in the rational case given in [BGP92] on page 4.

Proposition 2.1. *Let K be a number field and let q, d be coprime integers. Let $\mathbf{g}$ be an l-gap tuple with entries that are smaller than some natural number N and suppose that $\mathbf{x}$ is a point on $C_l(\mathbf{g})$ over K.*

If $h(q) \geq 2 \log N$, then there exists at most one tuple $\mathbf{n} = (n_0, \ldots, n_{l+1})$ of natural numbers such that $qn_i + d = x_i^2$ for some $1 \leq n_i \leq N$ and $x_i \in K$ satisfying $\mathbf{x} = (x_0 : \ldots : x_{l+1})$, and $\mathbf{g}$ is the gap tuple corresponding to $\mathbf{n}$.

Proof:
Consider two tuples $\mathbf{n} = (n_0, \ldots, n_{l+1})$ and $\mathbf{n}' = (n'_0, \ldots, n'_{l+1})$ such that for all $i = 0, \ldots, l+1$ we have $qn_i + d = x_i^2$ and $qn'_i + d = x_i'^2$, where $x_i, x'_i \in K$ satisfying $\mathbf{x} = (x_0 : \ldots : x_{l+1}) = (x'_0 : \ldots : x'_{l+1})$.

The proposition is proved if we can show that $\mathbf{n} = \mathbf{n}'$.

Since $\mathbf{x} = (x_0 : \ldots : x_{l+1}) = (x'_0 : \ldots : x'_{l+1})$, there is some $\theta \in K$ such that $x'_i = \theta x_i$ for $i = 0, \ldots, l+1$. Hence, for $0 < i \leq l+1$ we obtain

$$\frac{qn_0 + d}{qn_i + d} = \frac{x_0^2}{x_i^2} = \frac{\theta^2 x_0^2}{\theta^2 x_i^2} = \frac{qn'_0 + d}{qn'_i + d},$$

and we deduce

$$q(n_i n'_0 - n'_i n_0) = d(n'_0 + n_i - n_0 - n'_i).$$

Since q and d are coprime, q divides $(n_0'+n_i-n_0-n_i')$. However, $(n_0'+n_i-n_0-n_i')$ has absolute value less than N and since $h(q) \geq 2\log N$, we obtain $n_0'+n_i-n_0-n_i' = 0$. As $d \neq 0$, this also implies $n_i n_0' - n_i' n_0 = 0$, which in turn is equivalent to $\frac{n_0}{n_0'} = \frac{n_i}{n_i'}$.

We rewrite $n_0' + n_i - n_0 - n_i' = 0$ as

$$n_i(1 - \frac{n_i'}{n_i}) - n_0(1 - \frac{n_0'}{n_0}) = 0.$$

From $n_0 \neq n_i$ we now conclude

$$\frac{n_0}{n_0'} = \frac{n_i}{n_i'} = 1.$$

This proves the assertion. □

3 Majorizing by coprime HU pairs

In the previous two sections we have seen that coprime pairs form HU pairs. In order to establish the MHU condition for a concrete number field K we are supposed to prove that all pairs (q, d) are majorized by coprime pairs (q', d') over K.

The proof of this result in the rational case is given in [BGP92]. It is mainly based on the following fact:
If q and d are not coprime, but $\gcd(q, d)$ is squarefree, then the elements of $\mathcal{S}_{q,d,N}$ itself lie in an arithmetic progression mod $\gcd(q, d)$.

In this case it is easy to show that any square in the arithmetic progression $(qn+d)_{n\in\mathbb{N}}$ gives rise to a square in an arithmetic progression $(q'n+d')_{n\in\mathbb{N}}$, where $q' = \gcd(q, d)$. Then it follows $S_{q,d,N} \leq S_{q',d',N}$. Since $q' < q$, the repeated application of this argument has to terminate eventually. In this case q' and d' have to be coprime, and this means that the MHU condition holds.

We now generalize this result of Bombieri, Granville and Pintz to the case where the underlying number field is of the form $\mathbb{Q}(\sqrt{p})$ for some prime p. Subsequently, this will permit us to prove Theorem II.

We finish this chapter with a counterexample. We show that the conclusion above – namely that elements of $\mathcal{S}_{q,d,N}$ itself lie in an arithmetic progression – is in general not valid for all quadratic extensions of $\mathbb{Q}$. Note that this fact is the reason which keeps us from proving an analogue of Theorem II for any number field, although we expect it to be true.

3.1 Proof of Theorem II

We start off with a reduction that lets us assume that q and d have no common square factor.

Lemma 3.1. *Let K be a number field. For any $q, d \in \mathbb{Z}$ there exist q', d' such that*

$$S_{q,d,N} = S_{q',d',N}$$

for all $N \in \mathbb{N}$, and q', d' do not have a common integer factor being a square in K.

Proof:
We write $q = q^*\gcd(q,d)$ and $d = d^*\gcd(q,d)$. Then, we decompose $\gcd(q,d) = rs$ such that $r, s \in \mathbb{Z}$ and r is not divided by an integer which is a square in K while s is a square in K. Then we have

$$\begin{aligned}\mathcal{S}_{q,d,N} &= \{n \leq N | qn + d = x^2 \text{ for some } x \in K\} \\ &= \{n \leq N | q^*rsn + d^*rs = x^2 \text{ for some } x \in K\} \\ &= \{n \leq N | q^*rn + d^*r = x^2 \text{ for some } x \in K\} = \mathcal{S}_{q',d',N}\end{aligned}$$

for all $N \in \mathbb{N}$ by setting $q' = q^*r$ and $d' = d^*r$. □

The next lemma is crucial in order to establish the MHU condition for the fields $\mathbb{Q}(\sqrt{p})$, where p is prime. It shows that if $qn + d = x^2$ for some $\mathbb{Q}(\sqrt{p})$, then x^2, although it may not be the square of an integer, behaves in some way as if x indeed were an integer.

Lemma 3.2. *Let p be a prime. Suppose $q, d \in \mathbb{Z}$ such that* $\gcd(q,d)$ *does not have an integer factor being a square in $\mathbb{Q}(\sqrt{p})$.*

If $qn + d = x^2$ for some $n \in \mathbb{N}$ and some $x \in \mathbb{Q}(\sqrt{p})$, then $\gcd(q,d)^2$ *divides x^2.*

Proof:
By an elementary computation we see that if $x^2 \in \mathbb{Z}$ for some $x \in \mathbb{Q}(\sqrt{p})$, then x is of the form $x = t$ or $x = t\sqrt{p}$ for some $t \in \mathbb{Z}$.

Hence, we have $qn + d = t^2$ or $qn + d = (t\sqrt{p})^2 = t^2p$ for some $t \in \mathbb{Z}$. Let r be some prime dividing $\gcd(q,d)$. Then, by assumption, r is not a square in $\mathbb{Q}(\sqrt{p})$ and so in particular $r \neq p$.

Since r divides $qn + d$, it also divides t^2 or t^2p respectively. As $r \neq p$, it follows $r|t$. Since $\gcd(q,d)$ is squarefree, we obtain that $\gcd(q,d)$ divides t. This in turn implies that $\gcd(q,d)^2$ divides x^2. □

Now we can prove that over the field $\mathbb{Q}(\sqrt{p})$ all pairs (q, d) are majorized by coprime pairs (q', d') in the sense of the MHU condition.

Proposition 3.3. *Let p be a prime. Then for any $q, d \in \mathbb{Z}$ there exist coprime integers q', d' such that over $\mathbb{Q}(\sqrt{p})$ we have*

$$S_{q,d,N} \leq S_{q',d',N}$$

for all $N \in \mathbb{N}$.

Proof:
By lemma 3.1 we can assume that q and d do not have a common factor which is a square in K.

We claim that all n in $\mathcal{S}_{q,d,N}$ lie in an arithmetic progression mod $\gcd(q, d)$:
In order to prove this, let n_1, n_2 be elements of $\mathcal{S}_{q,d,N}$ and let r be a prime dividing $\gcd(q, d)$. Then, lemma 3.2 above yields

$$qn_1 + d = r^2 f_1 \qquad \text{and} \qquad qn_2 + d = r^2 f_2$$

for some $f_1, f_2 \in \mathbb{Z}$. This implies $r^2 \nmid q$ because otherwise we had $r^2 | d$ – a contradiction as $\gcd(q, d)$ is squarefree. Now we obtain

$$q(n_1 - n_2) = r^2(f_1 - f_2),$$

and this implies $r | n_1 - n_2$. Since r is an arbitrary prime dividing $\gcd(q, d)$, it follows that $\gcd(q, d) | n_1 - n_2$.

Hence, all elements of $\mathcal{S}_{q,d,N}$ lie in an arithmetic progression mod $\gcd(q, d)$. Therefore, they can be written as $n = \gcd(q, d)n^* + a$ for some fixed $a \in \mathbb{Z}$ and some $1 \leq n^* \leq N$. We write $q = q^*\gcd(q, d)$ and $d = d^*\gcd(q, d)$.

Consider some element n of $\mathcal{S}_{q,d,N}$. This means that we have $qn + d = x^2$ for some $x \in \mathbb{Q}(\sqrt{p})$. Then, we get

$$x^2 = q^*\gcd(q, d)(a + n^*\gcd(q, d)) + d^*\gcd(q, d) = q^*\gcd(q, d)^2 n^* + \gcd(q, d)(d^* + q^*a).$$

Lemma 3.2 above yields that x^2 is divided by $\gcd(q, d)^2$. Therefore, $\gcd(q, d)(d^* + q^*a)$ is divided by $\gcd(q, d)^2$ as well.

This means that any $n \in \mathcal{S}_{q,d,N}$ gives rise to a square in the arithmetic progression $(q'n^* + d')_{n^* \in \mathbb{N}}$ with $q' = \gcd(q, d)$ and $d' = \frac{d^* + q^*a}{\gcd(q,d)}$ with $n^* \leq N$. This implies $S_{q,d,N} \leq S_{q',d',N}$.

If q' and d' are coprime, the proposition is proved. However, if this is not the case, a iterated application of the reduction in 3.1 and the reduction in this proposition yields the desired result. Note that this process will terminate eventually. □

In fact, Theorem II is now a simple consequence of Theorem I and the results proved above.

Theorem II. *Let p be a prime. Then over $\mathbb{Q}(\sqrt{p})$ we have*

$$\max_{q,d\in\mathbb{Q}} S_{q,d,N} = O(N^{\frac{2}{3}} \log^c N),$$

where c is some positive constant.

Proof:
From the propositions 1.2,2.1 and 3.3 we obtain that $\mathbb{Q}(\sqrt{p})$ satisfies the MHU condition.

Since $\mathbb{Q}(\sqrt{p})$ is an extension of degree 2 of $\mathbb{Q}$, it is a Galois extension. Now the theorem follows from Theorem I. □

3.2 A counterexample

The key ingredient in the proof of Theorem II is lemma 3.2, which leads to the conclusion that if q and d are not coprime, but $\gcd(q, d)$ is squarefree, then all elements of $\mathcal{S}_{q,d,N}$ lie in an arithmetic progression modulo $\gcd(q, d)$.

We now show that this conclusion is false for the quadratic extension $\mathbb{Q}(\sqrt{6})$.

Consider the arithmetic progression $(2n + 4)_{n\in\mathbb{N}}$ over $\mathbb{Q}(\sqrt{6})$. This sequence starts as follows

$$\mathbf{6}, \quad 8, \quad 10, \quad 12, \quad 14, \quad \mathbf{16}, \quad 18, \quad 20, \quad \mathbf{24}, \quad 26, \ldots$$

where the highlighted numbers are those which are squares in $\mathbb{Q}(\sqrt{6})$. The greatest common divisor of q and d is 2, which is not a square in $\mathbb{Q}(\sqrt{6})$. We observe that the first elements of $\mathcal{S}_{q,d,N}$ are $1, 6$ and 10, which obviously do not lie in an arithmetic progression.

Although we have not verified it, it seems very likely that this behavior always occurs over quadratic number fields which result from $\mathbb{Q}$ by adjoining the squareroot of a composite number.

Chapter 8

Open questions and generalizations

At the end of this thesis we want to discuss some problems that remain open. Furthermore, we propose some generalizations of the theorems of this thesis, which let them appear as consequences of some wider conjectural statements.

Our primary objective was to generalize the theorem of Bombieri, Granville and Pintz to the number field case. So far the only number fields for which we proved this are those of the form $\mathbb{Q}(\sqrt{p})$ for a prime p. Besides, it is easy to see that all number fields K which have odd degree over $\mathbb{Q}$ satisfy the same asymptotics for the number of squares in arithmetic progressions simply because there do not appear any new squares. Even though these two examples are very specific, we believe that indeed one should expect that a theorem similar to Theorem II holds in fact for any number field.

It is clear that this would follow if the MHU condition holds for an arbitrary number field. As indicated in the last chapter we might not expect that proving the MHU condition can be achieved by using coprime pairs. However, it is possible that other pairs do, on the one hand, satisfy the height and the uniqueness condition and, on the other hand, majorize all other pairs.

We tried to put this idea into practice by considering pairs which satisfied some conditions involving all valuations of a number field. However, this approach did not turn out to be successful. So we leave as our major open problem to prove the MHU condition for other number fields.

In fact, we believe that an even stronger statement may be true. We think that the order of the asymptotics appearing in Theorem I and II is not the true order. Rather, we expect that the true order is indeed the order suggested by Rudin's conjecture.

Conjecture (Rudin's conjecture)**.** *It holds*

$$\max_{q,d\in\mathbb{Q}} |\{n \leq N | qn + d = x^2 \textit{ for some } x \in K\}| = O(\sqrt{N}).$$

Rudin's Conjecture can be seen as both the most natural and optimistic conjecture on the distribution of squares in arithmetic progressions. On the one hand, it is natural because a similar statement can be proven if we do not require uniformity in q and d. On the other hand, it is the most optimistic formulation of such a conjecture because one can easily prove that it is not possible to replace $O(\sqrt{N})$ by a stronger asymptotics.

Furthermore, Rudin's conjecture reflects the opinion that arithmetic progression and squares are not related and in some sense independent objects such that squares should not occur more often inside of arithmetic progressions than they do inside of the natural numbers.

If we subscribe to this view, we see no compelling reason why the situation should change fundamentally if we consider the same problem over number fields instead of over $\mathbb{Q}$. This leads to the following conjecture.

Conjecture ("Rudin's conjecture" over number fields)**.** *Let K be a number field. Then*

$$\max_{q,d\in\mathbb{Q}} |\{n \leq N | qn + d = x^2 \textit{ for some } x \in K\}| = O(\sqrt{N}).$$

This is not the only possible generalization of Rudin's conjecture to the number field case. The following statement is both more natural and stronger at the same time.

Conjecture (Extended "Rudin's conjecture" over number fields, version 1)**.** *Let K be a number field. Then*

$$\max_{q,d\in K} |\{n \leq N | qn + d = x^2 \textit{ for some } x \in K\}| = O(\sqrt{N}).$$

Interestingly, this conjecture is related to a seemingly stronger statement. Indeed, any asymptotical formula for

$$\max_{q,d\in K} |\{n \leq N | qn + d = x^2 \text{ for some } x \in K\}|$$

would lead to the same asymptotical formula for

$$\max_{q,d\in K} |\{n \leq N | qn + d = f(x) \text{ for some } x \in K\}|,$$

where f is some quadratic polynomial in $K[X]$. Hence, the conjecture above can be restated as follows.

Conjecture (Extended "Rudin's conjecture" over number fields, version 2)**.** *Let K be a number field and let $f(X) \in K[X]$ be a quadratic polynomial. Then*

$$\max_{q,d\in K} |\{n \leq N | qn + d = f(x) \text{ for some } x \in K\}| = O(\sqrt{N}),$$

where the implicit constant does not depend on f.

In view of this statement, it is also natural to ask what happens with polynomials of higher degree. Maybe the most optimistic guess is also the right one in this case.

Conjecture ("Rudin's conjecture" for polynomials)**.** *Let K be a number field and let $f(X) \in K[X]$ be a polynomial of degree* $\deg f \geq 1$*. Then*

$$\max_{q,d\in K} |\{n \leq N | qn + d = f(x) \text{ for some } x \in K\}| = O(N^{\frac{1}{\deg f}}),$$

where the implicit constant does not depend on f.

For $\deg f = 1$ the conjecture is trivially true, while for $\deg f = 2$ this is exactly the extended "Rudin's conjecture" over number fields.

For the case $\deg f \geq 3$ there is even less evidence supporting these conjectures than in the case of quadratic polynomials. Although one can also show that $O(N^{\frac{1}{\deg f}})$ cannot be replaced by a stronger asymptotic, we do not know of corresponding non-uniform results in this case. Hence, we propose the following conjecture, which would follow from "Rudin's conjecture" for polynomials.

Conjecture. *Let K be a number field and let $q, d \in K$. Suppose that $f(X) \in K[X]$ is a polynomial of degree* $\deg f \geq 3$*. Then*

$$|\{n \leq N | qn + d = f(x) \text{ for some } x \in K\}| = O(N^{\frac{1}{\deg f}}).$$

Note that in this non-uniform version the implicit constants might depend on q and d, and on the polynomial f. Even though this conjecture is far more weaker than the uniform version, it seems that there has not been done any research in this direction. We have had a look into the literature but we did not encounter any results related to this question, not even for special cases. Therefore, apart from the general conjectures, it would be interesting to have results in the restricted case. Maybe progress on these questions might also shed some light on the general conjectures.

Bibliography

[BG06] Enrico Bombieri and Walter Gubler. *Heights in Diophantine geometry.* New Mathematical Monographs 4. Cambridge: Cambridge University Press. xvi, 652 p., 2006.

[BGP92] Enrico Bombieri, Andrew Granville, and János Pintz. Squares in arithmetic progressions. *Duke Math. J.*, 66(3):369–385, 1992.

[BL04] Christina Birkenhake and Herbert Lange. *Complex abelian varieties. 2nd augmented ed.* Grundlehren der Mathematischen Wissenschaften 302. Berlin: Springer. xii, 635 p., 2004.

[Bom90] Enrico Bombieri. The Mordell conjecture revisited. *Ann. Sc. Norm. Super. Pisa, Cl. Sci., IV. Ser.*, 17(4):615–640, 1990.

[CM06] Alina Carmen Cojocaru and M. Ram Murty. *An introduction to sieve methods and their applications.* London Mathematical Society Lecture Note Series 66. Cambridge: Cambridge University Press. xii, 224 p., 2006.

[Dav00] Harold Davenport. *Multiplicative number theory. Revised and with a preface by Hugh L. Montgomery. 3rd ed.* Graduate Texts in Mathematics. 74. New York, NY: Springer. x, 177 p., 2000.

[Eis95] David Eisenbud. *Commutative algebra. With a view toward algebraic geometry.* Graduate Texts in Mathematics. 150. Berlin: Springer-Verlag. xvi, 785 p., 1995.

[Fal83] Gerd Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. (Finiteness theorems for abelian varieties over number fields). *Invent. Math.*, 73:349–366, 1983.

[Gri89] Phillip A. Griffiths. *Introduction to algebraic curves. Transl. from the Chinese by Kuniko Weltin.* Translations of Mathematical Monographs, 76. Providence, RI: American Mathematical Society (AMS). x, 221 p., 1989.

[Har92] Joe Harris. *Algebraic geometry. A first course.* Graduate Texts in Mathematics. 133. Berlin etc.: Springer-Verlag. xix, 328 p., 1992.

[HW79] G.H. Hardy and E.M. Wright. *An introduction to the theory of numbers. 5th ed.* Oxford etc.: Oxford at the Clarendon Press. XVI, 426 p., 1979.

[Kna92] Anthony W. Knapp. *Elliptic curves.* Mathematical Notes (Princeton). 40. Princeton, NJ: Princeton University Press. xv, 427 p., 1992.

[Lan78] Serge Lang. *Elliptic curves: Diophantine analysis.* Grundlehren der Mathematischen Wissenschaften. 231. Berlin-Heidelberg-New York: Springer-Verlag. XI, 261 p., 1978.

[Neu07] Jürgen Neukirch. *Algebraic number theory. (Algebraische Zahlentheorie.) Reprint of the 1992 original.* Berlin: Springer. xiv, 595 p., 2007.

[Per08] Daniel Perrin. *Algebraic geometry. An introduction. Transl. from the French by Catriona Maclean.* Universitext. Berlin: Springer; Les Ulis: EDP Sciences. xii, 258 p., 2008.

[Rud60] Walter Rudin. Trigonometric series with gaps. *J. Math. Mech.*, 9:203–227, 1960.

[Ser97] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem. Transl. and ed. by Martin Brown from notes by Michel Waldschmidt. 3rd ed.* Aspects of Mathematics. E 15. Wiesbaden: Vieweg. x, 218 p., 1997.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves.* Graduate Texts in Mathematics, 106. New York etc.: Springer-Verlag. XII, 400 p., 1986.

[Sze74] Endre Szemeredi. The number of squares in an arithmetic progression. *Studia Sci. Math. Hungar.*, 9, 1974.

[Voj91] Paul Vojta. Siegel's theorem in the compact case. *Ann. Math. (2)*, 133(3):509–548, 1991.

[ZB02] Umberto Zannier and Enrico Bombieri. A note on squares in arithmetic progressions. II. *Atti Accad. Naz. Lincei, Cl. Sci. Fis. Mat. Nat., IX. Ser., Rend. Lincei, Mat. Appl.*, 13(2):69–75, 2002.

Erklärung

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

Würzburg, den 4. November 2008

Matthias Waldherr