



universität
wien

DIPLOMARBEIT

Quadratic Number Fields that are Euclidean but not Norm-Euclidean

angestrebter akademischer Grad

Magister der Naturwissenschaften (Mag. rer. nat.)

Verfasser:	Bernhard Lutzmann
Matrikel-Nummer:	0201575
Studienrichtung:	Mathematik
Betreuer:	Ao. Univ.-Prof. Dr. Christoph Baxa

Feldkirch, am 7. Jänner 2009

Contents

1	Introduction	4
2	Prerequisites	6
2.1	Binary quadratic forms	6
2.2	Algebraic number theory	7
2.2.1	Quadratic number fields	10
2.3	Euclidean domains	21
2.3.1	Basic properties of Euclidean domains	21
2.3.2	The smallest Euclidean algorithm	23
2.3.3	Euclidean number fields	27
2.4	Inhomogeneous minima of binary quadratic forms	28
2.4.1	Application to the norm in $\mathbb{Q}(\sqrt{69})$	34
3	$\mathbb{Q}(\sqrt{69})$ is Euclidean	38
4	$\mathbb{Q}(\sqrt{14})$ is Euclidean	43
4.1	Characterization of Euclidean domains	43
4.2	Numerical criterion for Euclidean rings	49
4.3	Admissible set of primes in $\mathbb{Z}[\sqrt{14}]$	54
4.4	The Lower Bound Sieve	60
4.5	Proof that $\mathbb{Q}(\sqrt{14})$ is Euclidean	61
A	Computer proof	65
A.1	Analysis	65
A.2	Implementation	67

A.3 Example session	69
A.4 Source code	71
Bibliography	78
Curriculum Vitæ	80
Zusammenfassung	81

*“Ob es ein d gibt, sodaß O_d euklidisch, aber nicht
normeuklidisch ist, ist unbekannt.”*

E. Hlawka & J. Schoißengeier, 1990 (in [11], p. 155)

Chapter 1

Introduction

This diploma thesis deals with quadratic number fields that are Euclidean but not Norm-Euclidean. All Norm-Euclidean quadratic number fields $\mathbb{Q}(\sqrt{d})$ for squarefree $d \neq 0, 1$ are known since 1950: Chatland & Davenport [3] and independently Inkeri [12] have shown that $\mathbb{Q}(\sqrt{d})$ is Norm-Euclidean exactly for integers d in the set

$$\{-1, -2, -3, -7, -11, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

Additionally, for squarefree $d < 0$ the number field $\mathbb{Q}(\sqrt{d})$ is Euclidean if and only if d is in

$$\{-1, -2, -3, -7, -11\}.$$

This shows that all imaginary quadratic number fields are Euclidean if and only if they are Norm-Euclidean. However, in the real quadratic case it has been unknown for several decades if Euclidean implies Norm-Euclidean or not.

In Chapter 3 we present the proof of D. A. Clark that $\mathbb{Q}(\sqrt{69})$ is Euclidean but not Norm-Euclidean in full detail (see [4]). This was the first example of a quadratic number field with this property. We are able to explicitly specify an Euclidean algorithm for which $\mathbb{Q}(\sqrt{69})$ becomes an Euclidean domain. Parts of the proof rely on a computer program for which the source code is included in Appendix A.

In Chapter 4 we investigate another quadratic number field: $\mathbb{Q}(\sqrt{14})$. It has been conjectured for a long time that $\mathbb{Q}(\sqrt{14})$ is Euclidean because it possesses all the properties an Euclidean domain has, e.g., its ring of integers is a principal ideal domain. But it took until 2004 when M. Harper was able to prove that $\mathbb{Q}(\sqrt{14})$ is Euclidean (see [8]). In fact, Harper proved that all real quadratic number fields with class number 1 and discriminant ≤ 500 are Euclidean without publishing the details. This time we are not able to specify an Euclidean algorithm. Instead we deduce this property from a characterization of Euclidean domains and with the help of sieving methods in number fields.

Recently, W. Narkiewicz (in [16]) was able to prove that all real quadratic number fields with class number one are Euclidean, except for at most two fields. There are no exceptions known yet. If one is found, then this would immediately contradict the *Generalized Riemann hypothesis*. This follows from a result of P. J. Weinberger, who showed in [21] that the *Generalized Riemann hypothesis* implies that every real quadratic number field with class number one is Euclidean.

Acknowledgment

First of all I would like to thank my advisor Prof. Dr. Christoph Baxa for his help and guidance.

Furthermore, I express my gratitude to my family for all their support.

Chapter 2

Prerequisites

2.1 Binary quadratic forms

The theory of binary quadratic forms is a well-studied branch in elementary number theory. The reason why we need it here is the strong connection to quadratic number fields via the norm function and hence to Norm-Euclidean quadratic number fields.

Definition 2.1. A *binary quadratic form* is a function $f : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ with $f(x, y) = ax^2 + bxy + cy^2$ for integers a, b, c . The value $d = b^2 - 4ac$ is called its *discriminant*.

As $b^2 \equiv 0, 1 \pmod{4}$ for integral b , we conclude that $d \equiv 0, 1 \pmod{4}$.

Definition 2.2. Two forms f and f' are called *equivalent*, if there exists a transformation $T \in GL(2, \mathbb{Z})$ with $|\det(T)| = 1$ such that $f' \circ T = f$.

Equivalent forms share some important properties: for example they take the same values. That is, if $f(x_0, y_0) = m$ for real x_0, y_0 and f' is equivalent to f , then there exist real x_1, y_1 such that $f'(x_1, y_1) = m$.

There are several types of binary quadratic forms:

Definition 2.3. A binary quadratic form f is called *positive* (respectively *negative*) *definite* if for all real x, y with $(x, y) \neq (0, 0)$ $f(x, y) > 0$ (respectively $f(x, y) < 0$).

f is called **indefinite** if there exist $(x_0, y_0), (x_1, y_1) \in \mathbb{R}^2$ such that $f(x_0, y_0) < 0 < f(x_1, y_1)$.

f is called **positive** (respectively **negative**) **semidefinite**, if $f(x, y) \geq 0$ (respectively $f(x, y) \leq 0$) for all real x, y and for some real x_0, y_0 with $(x_0, y_0) \neq (0, 0)$ we have that $f(x_0, y_0) = 0$.

It is the discriminant of a binary quadratic form which tells us of what type it is:

Proposition 2.1. Let $f(x, y) = ax^2 + bxy + cy^2$ be a binary quadratic form with discriminant $d = b^2 - 4ac$. Then

1. f is semidefinite if and only if $d = 0$.
2. f is positive definite if and only if $d < 0$ and $a > 0$.
3. f is indefinite if and only if $d > 0$.

Proof. See for example [11], page 82.

□

Proposition 2.2. For every indefinite binary quadratic form there exists an equivalent form $f(x, y) = ax^2 + bxy + cy^2$ such that $0 < |a| < \sqrt{b^2 - 4ac}$.

Proof. A proof can be found in [6], page 97.

□

2.2 Algebraic number theory

In this section we review some definitions and results of basic algebraic number theory. We mainly focus on quadratic number fields. Most of the proofs are omitted, as they can be found in (almost) any book on algebraic number theory, for example [1].

Definition 2.4. An **algebraic number field** $K \subseteq \mathbb{C}$ is a finite field extension of \mathbb{Q} . Its elements are called **algebraic numbers**. An algebraic number is called **algebraic integer** if it is a root of a monic polynomial with integer coefficients.

Every algebraic number field contains a ring of special interest:

Definition 2.5. *Let K be an algebraic number field. The set of algebraic integers in K is called **ring of integers of K** and is denoted by O_K .*

In general, the ring of integers of an algebraic number field is not a unique factorization domain. But there exists an analog of the *Fundamental Theorem of Arithmetic* for ideals:

Theorem 2.1 (Fundamental Theorem of Arithmetic in Number Fields). *Let K be an algebraic number field and O_K its ring of integers. Then every non-zero ideal I in O_K can be written as a product*

$$I = \prod_{i=1}^r P_i^{e_i}$$

where the P_i are distinct non-zero prime ideals in O_K and e_i positive integers. This representation is unique up to rearrangement of the factors.

We now consider the splitting and ramification of primes in algebraic number fields. For this let p be a prime in \mathbb{Z} . Then $p \cdot O_K$ is a (principal) ideal in O_K and by the Theorem above, it can be written as a product

$$p \cdot O_K = \prod_{i=1}^r P_i^{e_i}$$

for distinct non-zero prime ideals P_i and positive integers e_i . The exponent e_i of a prime ideal P_i which divides $p \cdot O_K$ is called **ramification index** of P_i over p and denoted by $e(P_i|p)$. Furthermore, O_K/P_i is a finite field extension of the finite field $\mathbb{Z}/p\mathbb{Z}$ for each prime ideal P_i . The degree of this extension is called **inertial degree** of P_i over p and denoted by $f(P_i|p)$. The formula

$$\sum_{i=1}^r e(P_i|p)f(P_i|p) = [K : \mathbb{Q}]$$

shows the connection between the ramification indices, the inertial degrees and the degree of the field extension K over \mathbb{Q} .

There is a famous theorem on the structure of the group of units in a ring of integers:

Theorem 2.2 (Dirichlet Unit Theorem). *Let K be an algebraic number field and O_K its ring of integers. Then*

$$O_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1}$$

where $\mu(K)$ is the finite cyclic group of roots of unity of O_K^\times , r the number of real embeddings $K \rightarrow \mathbb{R}$ and $2s$ the number of non-real complex embeddings $K \rightarrow \mathbb{C}$.

Next we introduce the *ideal class group* and the *class number* of an algebraic number field. The class number is a measure of how far the ring of integers in the number field is away from being a principal ideal domain (and hence from possessing unique factorization).

First we need a generalization of ideals, called *fractional ideals*:

Definition 2.6. *Let K be an algebraic number field and O_K its ring of integers. A **fractional ideal** is a subset J of K such that there exists a non-zero element b in O_K with the property that $b \cdot J$ is an ideal in O_K .*

The product of two fractional ideals is a fractional ideal. Furthermore, every non-zero fractional ideal is invertible: that is, for any non-zero fractional ideal J_1 there exists a fractional ideal J_2 such that $J_1 \cdot J_2 = O_K$. Therefore, the set of all non-zero fractional ideals in O_K form an abelian group J_K . The principal fractional ideals $a \cdot O_K$ for $a \in K^\times$ form a subgroup of J_K denoted by P_K .

Definition 2.7. *The factor group J_K/P_K is called **(ideal) class group** of K .*

It is an important result in algebraic number theory that the class group is always finite:

Theorem 2.3 (Finiteness of the class group). *Let K be an algebraic number field. Then the class group of K is finite.*

Thus we are able make the following definition:

Definition 2.8. Let K be an algebraic number field. The order of the class group of K is called **class number** of K .

Computing the class number in general is not that easy. For small discriminants, there exists a method based on a theorem by *Minkowski* that enables one to calculate the class number by hand. For other number fields, one can use a computer algebra system such as *Pari/GP*¹ to calculate the class number.

The following proposition can be used to show that a ring of integers is a principal ideal domain:

Proposition 2.3. Let K be an algebraic number field and O_K its ring of integers. Then O_K has class number one if and only if it is a principal ideal domain.

There is a version of the *Chinese Remainder Theorem* for the ring of integers in an algebraic number field that we use:

Proposition 2.4 (Generalized Chinese Remainder Theorem). Let K be an algebraic number field, O_K its ring of integers and I_1, \dots, I_n pairwise coprime ideals in O_K , that is $I_j + I_k = O_K$ for $j \neq k$. Then the product $I := I_1 \dots I_n$ is equal to the intersection $I_1 \cap \dots \cap I_n$ and the quotient ring O_K/I is isomorphic to $O_K/I_1 \times \dots \times O_K/I_n$.

2.2.1 Quadratic number fields

We now consider field extensions K of \mathbb{Q} of degree 2, that is $[K : \mathbb{Q}] = 2$. These fields are called **quadratic number fields**. It is well known how these look:

Proposition 2.5. If K is a quadratic number field, then there exists a unique squarefree integer $d \neq 0, 1$ such that $K = \mathbb{Q}(\sqrt{d})$. On the other side, every squarefree integer $d \neq 0, 1$ defines a quadratic number field $\mathbb{Q}(\sqrt{d})$.

¹Pari/GP can be downloaded for free from <http://pari.math.u-bordeaux.fr/>

Here $\mathbb{Q}(\sqrt{d})$ is the smallest field that contains \mathbb{Q} and \sqrt{d} . It is the intersection of all fields that contain \mathbb{Q} and \sqrt{d} .

If $K = \mathbb{Q}(\sqrt{d})$ is a quadratic number field for some squarefree integer d , there are two possible cases:

1. $d > 0$: then $K \subseteq \mathbb{R}$ and K is called a **real quadratic number field**.
2. $d < 0$: then $K \not\subseteq \mathbb{R}$ and K is called an **imaginary quadratic number field**.

Definition 2.9. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field, $d \neq 0, 1$ a squarefree integer. The **discriminant of K** is d if $d \equiv 1 \pmod{4}$ and $4d$ if $d \equiv 2, 3 \pmod{4}$.

Note that the case $d \equiv 0 \pmod{4}$ is not possible, as this would imply that d is not squarefree. We also see that the discriminant is always congruent to 0 or 1 modulo 4.

For quadratic number fields, we also know exactly how the rings of integers look like:

Proposition 2.6. Let $K = \mathbb{Q}(\sqrt{d})$ for a squarefree integer $d \neq 0, 1$. Then

$$O_K = \begin{cases} \mathbb{Z} + \mathbb{Z} \cdot \sqrt{d} & \text{if } d \equiv 2, 3 \pmod{4} \\ \mathbb{Z} + \mathbb{Z} \cdot \left(\frac{1+\sqrt{d}}{2}\right) & \text{if } d \equiv 1 \pmod{4} \end{cases}$$

The *Dirichlet Unit Theorem* tells us more about the structure of O_K^\times in the quadratic case:

If $K = \mathbb{Q}(\sqrt{d})$ for some squarefree $d > 1$ we have that $r = 2$ and $s = 0$. As -1 is the only real primitive root of unity, we obtain that every unit $u \in O_K^\times$ is of the form $u = \pm \varepsilon_0^n$ for a unique element ε_0 (called the **fundamental unit** of $\mathbb{Q}(\sqrt{d})$) and an integer n . This also shows that there are infinitely many roots of unity in a real quadratic number field.

Definition 2.10. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field and $x + y\sqrt{d} \in K$. The **norm of $x + y\sqrt{d}$** is defined as $N(x + y\sqrt{d}) := x^2 - d \cdot y^2$.

In the case $d \equiv 1 \pmod{4}$, we will use the canonical form $x + y \cdot \left(\frac{1+\sqrt{d}}{2}\right)$ for elements in $\mathbb{Q}(\sqrt{d})$ (x and y rational). This corresponds to the structure of $O_K = \mathbb{Z} + \mathbb{Z} \cdot \left(\frac{1+\sqrt{d}}{2}\right)$. The norm of an element can then be expressed as

$$\begin{aligned} N\left(x + y \cdot \left(\frac{1+\sqrt{d}}{2}\right)\right) &= N\left(\left(x + \frac{y}{2}\right) + \frac{y}{2} \cdot \sqrt{d}\right) \\ &= \left(x + \frac{y}{2}\right)^2 - d \cdot \left(\frac{y}{2}\right)^2 \\ &= x^2 + xy + \frac{y^2}{4} - d \cdot \frac{y^2}{4} \\ &= x^2 + xy + \left(\frac{1-d}{4}\right) \cdot y^2. \end{aligned}$$

As $d \equiv 1 \pmod{4}$, the fraction $\frac{1-d}{4}$ is always an integer.

The norm function is completely multiplicative, that is

$$N(z_1 \cdot z_2) = N(z_1) \cdot N(z_2)$$

for all $z_1, z_2 \in \mathbb{Q}(\sqrt{d})$. An element $u \in O_K$ is a unit if and only if $N(u) = \pm 1$.

Now we also see the connection between the norm function and binary quadratic forms. Every norm in a quadratic number field actually corresponds to a binary quadratic form $f(x, y)$ (the domain is not the same, but can easily be extended to $\mathbb{R} \times \mathbb{R}$). Note that in the case that $K = \mathbb{Q}(\sqrt{d})$ with $d \equiv 1 \pmod{4}$, we consider the binary quadratic form deduced above, that is $f(x, y) = x^2 + xy + \left(\frac{1-d}{4}\right) \cdot y^2$.

Definition 2.11. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field and I a non-zero ideal in O_K . The **norm of I** is defined to be $\mathcal{N}(I) := |O_K/I|$.

Here $|O_K/I|$ is the order of the factor group O_K/I . The norm of ideals is also completely multiplicative, that is

$$\mathcal{N}(I \cdot J) = \mathcal{N}(I) \cdot \mathcal{N}(J)$$

for non-zero ideals I, J .

The ideal-norm corresponds to the norm of an element: if I is a principal ideal $a \cdot O_K$ for a non-zero element $a \in O_K$, then $\mathcal{N}(I) = |N(a)|$.

Now let us have a closer look on the splitting and ramification of primes in the quadratic case. As $[K : \mathbb{Q}] = 2$ for a quadratic number field $K = \mathbb{Q}(\sqrt{d})$, we have the formula

$$\sum_{i=1}^r e(P_i|p) f(P_i|p) = 2.$$

From this equation we deduce that $r \leq 2$, as $e(P_i|p)$ and $f(P_i|p)$ are positive integers. When we write e_i for $e(P_i|p)$ and f_i for $f(P_i|p)$, we see that

$$e_1 f_1 = 2$$

if $r = 1$, or

$$e_1 f_1 + e_2 f_2 = 2$$

if $r = 2$. Thus there are the following possibilities:

1. $e_1 = 1, f_1 = 2$:

That is $p \cdot O_K$ itself is a prime ideal, p is called **inert** in this case.

2. $e_1 = 2, f_1 = 1$:

Then $p \cdot O_K = P^2$ for a prime ideal P and p is called **(totally) ramified**.

3. $e_1 = 1, f_1 = 1, e_2 = 1, f_2 = 1$:

In this case, $p \cdot O_K = P_1 \cdot P_2$ for distinct prime ideals P_1, P_2 , p is called **(totally) split**.

If we consider a prime ideal P in O_K , then O_K/P is a finite field because P is maximal. Therefore, the order of O_K/P equals p^f for a prime p in \mathbb{Z} and a positive integer f . We say that P is **inert**, **(totally) ramified** or **(totally) split**, if p is. If P is a principal prime ideal $P = \pi \cdot O_K$ for an element π in O_K , then π is said to be **inert**, **(totally) ramified** or **(totally) split** if P is.

With the Jacobi symbol we can decide if a rational prime p is inert, split or ramified:

Proposition 2.7. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field and p a rational prime.*

1. If $p > 2$, $\left(\frac{d}{p}\right) = 1$ or $p = 2$, $d \equiv 1 \pmod{8}$, then p is split.
2. If $p > 2$, $p|d$ or $p = 2$, $d \equiv 2, 3 \pmod{4}$, then p is ramified.
3. If $p > 2$, $\left(\frac{d}{p}\right) = -1$ or $p = 2$, $d \equiv 5 \pmod{8}$, then p is inert.

Now we prove some results to be able to show that the group $(O_K/(\pi^s))^\times$ is cyclic for unramified prime elements $\pi \in O_K$ with odd prime norm (when O_K is a unique factorization domain).

Lemma 2.1. *Let R be a finite commutative ring with identity and $x \in R$. Then $x \in R^\times$ if and only if x is not a zero divisor.*

Proof. “ \Rightarrow ”: If $x \in R^\times$, then there exists $y \in R$ with $xy = 1$. Suppose there exists $z \in R \setminus \{0\}$ such that $xz = 0$. Then

$$z = 1 \cdot z = (xy) \cdot z = (xz) \cdot y = 0 \cdot y = 0,$$

a contradiction to $z \neq 0$.

“ \Leftarrow ”: If $x = 1$, then $x \in R^\times$ because $1 \cdot 1 = 1$. Now let $x \neq 1$ be no zero divisor. Then x^n is no zero divisor for $n \geq 1$: Suppose the claim has been proved for $n \geq 1$. If $x^{n+1} \cdot y = 0$ for $y \in R \setminus \{0\}$, then $x \cdot (x^n \cdot y) = 0$. Because x is no zero divisor, $x^n \cdot y = 0$ which is a contradiction to the assumption that x^n is no zero divisor.

Because R is finite, also the set $\{x^n \mid n \geq 1\}$ is finite. Therefore we can find positive integers $m < n$ such that $x^m = x^n$. Then

$$0 = x^n - x^m = x^m \cdot (x^{n-m} - 1).$$

Because x^m is no zero divisor, we have that $x^{n-m} - 1 = 0$. Therefore $x^{n-m} = 1$ which implies that $x \cdot x^{n-m-1} = 1$. This shows that $x \in R^\times$.

□

The following proof has been adopted from [19], page 127f:

Lemma 2.2. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field and P a non-zero prime ideal in O_K . Then $(P^n/P^{n+1}, +) \cong (O_K/P, +)$ for $n \geq 1$.*

Proof. First note that $P^{n+1} \subsetneq P^n$. Furthermore, there exists no ideal I with $P^{n+1} \subsetneq I \subsetneq P^n$: because if $P^{n+1} \subseteq I \subseteq P^n$, then

$$P = P^{n+1}P^{-n} \subseteq IP^{-n} \subseteq P^nP^{-n} = O_K$$

and therefore $IP^{-n} = P$ or $IP^{-n} = O_K$ (in O_K every prime ideal is maximal). It follows that $I = P^{n+1}$ or $I = P^n$.

Now choose $\alpha \in P^n \setminus P^{n+1}$. Then $P^{n+1} \subsetneq P^{n+1} + (\alpha) \subseteq P^n$ which implies that $P^{n+1} + (\alpha) = P^n$.

Consider the map $\varphi : (O_K, +) \rightarrow (P^n/P^{n+1}, +)$, $\varphi(x) := \alpha x + P^{n+1}$:

- φ is well defined. If $\alpha \in P^n$, then $\alpha x \in P^n$ for all $x \in O_K$ and therefore $\alpha x + P^{n+1} \in P^n/P^{n+1}$ for all $x \in O_K$.
- φ is a group homomorphism. It is the composition of the two homomorphisms $(O_K, +) \rightarrow (P^n, +)$, $x \mapsto \alpha x$ and $(P^n, +) \rightarrow (P^n/P^{n+1}, +)$, $y \mapsto y + P^{n+1}$.
- φ is surjective. Because $(\alpha) + P^{n+1} = P^n$.
- $\ker(\varphi) = P$. Note that $P \subseteq \ker(\varphi)$, because if $x \in P$ then $\alpha x \in P^n \cdot P = P^{n+1}$ and therefore $\varphi(x) = P^{n+1}$.

Furthermore, $\ker(\varphi)$ is an O_K -module (if $x \in \ker(\varphi)$, that is $\varphi(x) = P^{n+1}$, then $\alpha x + P^{n+1} = P^{n+1}$, so $\alpha x \in P^{n+1}$; therefore $\alpha xy \in P^{n+1}$ for all $y \in O_K$ which implies that $xy \in \ker(\varphi)$ for all $y \in O_K$). As an O_K -submodule of O_K , $\ker(\varphi)$ is an integral ideal. As P is a maximal ideal in O_K , either $\ker(\varphi) = P$ or $\ker(\varphi) = O_K$. Suppose $\ker(\varphi) = O_K$, then from the *First Isomorphism Theorem* for groups we deduce that

$$P^n/P^{n+1} = \text{Im}(\varphi) \cong O_K/\ker(\varphi) = \{0\},$$

which contradicts the fact that $P^{n+1} \subsetneq P^n$. Therefore $\ker(\varphi) = P$, and the claim follows from the *First Isomorphism Theorem*.

□

Proposition 2.8. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field such that O_K is a unique factorization domain. If π is a prime element in O_K , then*

$$|(O_K/(\pi^n))^\times| = |N(\pi)|^{n-1} \cdot (|N(\pi)| - 1)$$

for $n \geq 1$.

Proof. By the properties of the norm it follows that

$$|O_K/(\pi^n)| = |N(\pi^n)| = |N(\pi)|^n.$$

If $\alpha + (\pi^n)$ is a zero divisor in $O_K/(\pi^n)$, then there exists $\beta + (\pi^n)$ with $\pi^n \nmid \beta$ such that $(\alpha + (\pi^n))(\beta + (\pi^n)) = (\pi^n)$. This means that $\pi^n | \alpha\beta$. Because $\pi^n \nmid \beta$, it follows that $\alpha \in (\pi)$.

On the other side, if $\alpha \in (\pi)$, then $\pi | \alpha$ and therefore $\alpha + (\pi^n)$ is a zero divisor in $O_K/(\pi^n)$ because

$$(\alpha + (\pi^n))(\pi^{n-1} + (\pi^n)) = \alpha\pi^{n-1} + (\pi^n) = \pi^n \cdot \frac{\alpha}{\pi} + (\pi^n) = (\pi^n).$$

Therefore the set of zero divisors in $O_K/(\pi^n)$ is $(\pi)/(\pi^n)$.

Next we show by induction on n that $|(\pi)/(\pi^n)| = |N(\pi)|^{n-1}$: The case $n = 1$ is trivial. Let $n \geq 2$, and note that

$$((\pi)/(\pi^n))/((\pi^{n-1})/(\pi^n)) \cong (\pi)/(\pi^{n-1}).$$

Then

$$\begin{aligned} |(\pi)/(\pi^n)| &= |(\pi)/(\pi^{n-1})| \cdot |(\pi^{n-1})/(\pi^n)| \\ &= |N(\pi)|^{n-2} \cdot |O_K/(\pi)| \\ &= |N(\pi)|^{n-2} \cdot |N(\pi)| = |N(\pi)|^{n-1} \end{aligned}$$

where we used the induction hypotheses and Lemma 2.2. The proposition now follows from Lemma 2.1:

$$|(O_K/(\pi^n))^\times| = |N(\pi)|^n - |N(\pi)|^{n-1} = |N(\pi)|^{n-1} \cdot (|N(\pi)| - 1).$$

□

Let O_K be a unique factorization domain and π a prime element in O_K . Then $(O_K/(\pi))^\times$ is cyclic as a finite subgroup of $(O_K/(\pi))^\times$ (because every finite subgroup of the multiplicative group of a field is cyclic). The order of $(O_K/(\pi))^\times$ is $|N(\pi)| - 1$.

Lemma 2.3. *If $\gamma \in O_K$ is a generator of $(O_K/(\pi))^\times$, then also $\gamma + \pi$.*

Proof. We calculate that

$$\begin{aligned} (\gamma + \pi)^n &= \sum_{i=0}^n \binom{n}{i} \gamma^i \pi^{n-i} \\ &= \sum_{i=0}^{n-1} \binom{n}{i} \gamma^i \pi^{n-i} + \gamma^n \\ &\equiv \gamma^n (\pi) \end{aligned}$$

for $0 \leq n < |N(\pi)|$.

□

Lemma 2.4. *Let $\gamma \in O_K$ be a generator of $(O_K/(\pi))^\times$. Then*

$$\gamma^{|N(\pi)|-1} \not\equiv 1 \pmod{\pi^2} \text{ or } (\gamma + \pi)^{|N(\pi)|-1} \not\equiv 1 \pmod{\pi^2}.$$

Proof. Suppose that $\gamma^{|N(\pi)|-1} \equiv (\gamma + \pi)^{|N(\pi)|-1} \equiv 1 \pmod{\pi^2}$. Then

$$\begin{aligned} 1 &\equiv (\gamma + \pi)^{|N(\pi)|-1} = \sum_{i=0}^{|N(\pi)|-1} \binom{|N(\pi)|-1}{i} \gamma^i \pi^{|N(\pi)|-1-i} \\ &= \sum_{i=0}^{|N(\pi)|-3} \binom{|N(\pi)|-1}{i} \gamma^i \pi^{|N(\pi)|-1-i} + (|N(\pi)|-1) \gamma^{|N(\pi)|-2} \pi + \gamma^{|N(\pi)|-1} \\ &\equiv 1 + (|N(\pi)|-1) \gamma^{|N(\pi)|-2} \pi \pmod{\pi^2} \end{aligned}$$

where we used that

$$\pi^{|N(\pi)|-1-i} \equiv 0 \pmod{\pi^2}$$

for $0 \leq i \leq |N(\pi)| - 3$ and

$$\gamma^{|N(\pi)|-1} \equiv 1 \pmod{\pi^2}.$$

Therefore

$$(|N(\pi)| - 1)\gamma^{|N(\pi)|-2}\pi \equiv 0 \pmod{\pi^2}$$

which implies that

$$\pi^2 \mid (|N(\pi)| - 1)\gamma^{|N(\pi)|-2}\pi$$

and so

$$\pi \mid (|N(\pi)| - 1)\gamma^{|N(\pi)|-2}.$$

Because $\pi \mid N(\pi)$ we have that $\pi \mid |N(\pi)|$. But this means that $\pi \nmid (|N(\pi)| - 1)$. Therefore $\pi \mid \gamma^{|N(\pi)|-2}$ and so $\pi \mid 1$ or $\pi \mid \gamma$, which is not possible. \square

Lemma 2.5. *Suppose that π is unramified and of odd prime norm. Let $\gamma \in O_K$ be a generator of $(O_K/(\pi))^\times$ such that $\gamma^{|N(\pi)|-1} \not\equiv 1 \pmod{\pi^2}$. Then γ is a generator of $(O_K/(\pi^s))^\times$ for all $s \geq 1$.*

Proof. We first show inductively that

$$\gamma^{(|N(\pi)|-1)|N(\pi)|^{s-2}} \not\equiv 1 \pmod{\pi^s} \quad (2.1)$$

for all $s \geq 2$. The case $s = 2$ is assumed. By Proposition 2.8, we know that

$$|(O_K/(\pi^{s-1}))^\times| = |N(\pi)|^{s-2} \cdot (|N(\pi)| - 1).$$

Therefore

$$\gamma^{|N(\pi)|^{s-2} \cdot (|N(\pi)|-1)} = \gamma^{|(O_K/(\pi^{s-1}))^\times|} \equiv 1 \pmod{\pi^{s-1}}$$

and so there exists $\alpha \in O_K$, $\pi \nmid \alpha$ such that

$$\gamma^{|N(\pi)|^{s-2} \cdot (|N(\pi)|-1)} = 1 + \alpha\pi^{s-1}.$$

It follows that

$$\begin{aligned} \gamma^{|N(\pi)|^{s-1} \cdot (|N(\pi)|-1)} &= (1 + \alpha\pi^{s-1})^{|N(\pi)|} = \sum_{i=0}^{|N(\pi)|} \binom{|N(\pi)|}{i} \alpha^i \pi^{i(s-1)} \\ &= 1 + |N(\pi)|\alpha\pi^{s-1} + \binom{|N(\pi)|}{2} \alpha^2 \pi^{2s-2} \\ &\quad + \sum_{i=3}^{|N(\pi)|} \binom{|N(\pi)|}{i} \alpha^i \pi^{i(s-1)}. \end{aligned} \quad (2.2)$$

As π has odd prime norm, the fraction $\frac{|N(\pi)|-1}{2}$ is an integer. Furthermore $|N(\pi)| \equiv 0 \pmod{\pi}$. Therefore

$$\binom{|N(\pi)|}{2} \alpha^2 \pi^{2s-2} = \frac{|N(\pi)|-1}{2} |N(\pi)| \alpha^2 \pi^{2s-2} \equiv 0 \pmod{\pi^{2s-1}}.$$

Note that

$$3(s-1) \geq 2s-1 \iff 3s-3 \geq 2s-1 \iff s \geq 2$$

implies that

$$i(s-1) \geq 3(s-1) \geq 2s-1$$

for all $i \geq 3$, $s \geq 2$. Therefore

$$\sum_{i=3}^{|N(\pi)|} \binom{|N(\pi)|}{i} \alpha^i \pi^{i(s-1)} \equiv 0 \pmod{\pi^{2s-1}}$$

and from equation (2.2) it follows that

$$\gamma^{|N(\pi)|^{s-1} \cdot (|N(\pi)|-1)} \equiv 1 + |N(\pi)| \alpha \pi^{s-1} \pmod{\pi^{2s-1}}.$$

As $2s-1 \geq s+1$ for all $s \geq 2$, we deduce that

$$\gamma^{|N(\pi)|^{s-1} \cdot (|N(\pi)|-1)} \equiv 1 + |N(\pi)| \alpha \pi^{s-1} \pmod{\pi^{s+1}}.$$

Now suppose that

$$\gamma^{|N(\pi)|^{s-1} \cdot (|N(\pi)|-1)} \equiv 1 \pmod{\pi^{s+1}}.$$

Then

$$1 + |N(\pi)| \alpha \pi^{s-1} \equiv 1 \pmod{\pi^{s+1}}$$

and therefore

$$\pi^{s+1} \mid |N(\pi)| \alpha \pi^{s-1}.$$

This implies that

$$\pi^2 \mid |N(\pi)| \alpha.$$

As $\pi \nmid \alpha$, it follows that $\pi^2 \mid |N(\pi)|$. But this contradicts the assumption that π is unramified and we have shown that

$$\gamma^{|N(\pi)|^{s-1} \cdot (|N(\pi)|-1)} \not\equiv 1 \pmod{\pi^{s+1}}$$

for all $s \geq 2$.

Let e be the order of γ in $(O_K/(\pi^s))^\times$. By Proposition 2.8 we have that

$$|(O_K/(\pi^s))^\times| = |N(\pi)|^{s-1}(|N(\pi)| - 1)$$

and therefore $e \mid |N(\pi)|^{s-1}(|N(\pi)| - 1)$. Furthermore, $\gamma^e \equiv 1 \pmod{\pi^s}$ which implies that $\gamma^e \equiv 1 \pmod{\pi}$. As $|(O_K/(\pi))^\times| \mid e$ we deduce that $(|N(\pi)| - 1) \mid e$. Because $|N(\pi)| = p$ for some rational prime p , we have that $e \mid p^{s-1}(p - 1)$ and $(p - 1) \mid e$. Therefore $e = p^k(p - 1)$ for an element $k \in \{0, 1, \dots, s - 1\}$. If $k < s - 1$, then

$$1 \equiv \gamma^e = \gamma^{p^k(p-1)} \pmod{\pi^s}$$

from which it follows that

$$\gamma^{p^{s-2}(p-1)} = (\gamma^{p^k(p-1)})^{p^{s-2-k}} \equiv 1^{p^{s-2-k}} = 1 \pmod{\pi^s}.$$

But this contradicts equation (2.1). Therefore $k = s - 1$ and so we have

$$e = p^{s-1}(p - 1) = |N(\pi)|^{s-1}(|N(\pi)| - 1) = |(O_K/(\pi^s))^\times|.$$

It follows that γ is a generator of $(O_K/(\pi^s))^\times$.

□

Now we are able to combine these results to prove that $(O_K/(\pi^s))^\times$ is cyclic:

Proposition 2.9. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field such that O_K is a unique factorization domain. If π is an unramified prime element in O_K with odd prime norm, then $(O_K/(\pi^s))^\times$ is cyclic for all $s \geq 1$.*

Proof. For $s = 1$, the group $(O_K/(\pi))^\times$ is cyclic as a finite subgroup of the multiplicative group $(O_K/(\pi))^\times$ of the field $O_K/(\pi)$.

For $s \geq 2$, let γ be a generator of $(O_K/(\pi))^\times$. By Lemma 2.3, the element $\gamma + \pi$ also generates $(O_K/(\pi))^\times$. Now by Lemma 2.4 it follows that

$$\gamma^{|N(\pi)|-1} \not\equiv 1 \pmod{\pi^2} \text{ or } (\gamma + \pi)^{|N(\pi)|-1} \not\equiv 1 \pmod{\pi^2}.$$

We then apply Lemma 2.5 to show that γ or $\gamma + \pi$ generates $(O_K/(\pi^s))^\times$.

□

2.3 Euclidean domains

Definition 2.12. Let R be an integral domain. An **Euclidean algorithm** on R is a function $\phi : R \rightarrow \mathbb{N}_0$ with the property that for all $a, b \in R, b \neq 0$ there exist $q, r \in R$ such that $a = qb + r$ and $\phi(r) < \phi(b)$.

Definition 2.13. An integral domain R is called **Euclidean** with respect to ϕ , if $\phi : R \rightarrow \mathbb{N}_0$ is an Euclidean algorithm.

For example, \mathbb{Z} is Euclidean with the absolute value as Euclidean algorithm.

2.3.1 Basic properties of Euclidean domains

What makes Euclidean domains interesting is the fact that they are principal ideal domains:

Proposition 2.10. Every integral domain that possesses an Euclidean algorithm is a principal ideal domain.

Proof. Let R be an integral domain and $\phi : R \rightarrow \mathbb{N}_0$ an Euclidean algorithm. We have to show that every ideal I in R is a principal ideal, that is $I = a \cdot R$ for some element $a \in R$. Let $I \neq (0)$ be an ideal in R . Choose $a \in I, a \neq 0$ such that $\phi(a) \leq \phi(b)$ for all $b \in I, b \neq 0$. This is possible, because $\phi(I \setminus \{0\})$ is a subset of \mathbb{N}_0 , and \mathbb{N}_0 is well-ordered.

We show that $I \subseteq a \cdot R$: For this choose an arbitrary $b \in I$. As R is Euclidean and $a, b \in R, a \neq 0$ there exist $q, r \in R$ such that $b = aq + r$ with $\phi(r) < \phi(a)$. But $r = b - aq \in I$ because $a, b \in I$ and I is an ideal. By the minimality of $\phi(a)$ it follows that $r = 0$. So $b = aq$ for some $q \in R$.

We also have $I \supseteq a \cdot R$: this is true because $a \in I$ and I is an ideal in R . □

Proposition 2.11. Let ϕ be an Euclidean algorithm on a domain R . Then $\phi(0)$ is the smallest element of $\phi(R)$, that is $\phi(b) > \phi(0)$ for all $b \in R \setminus 0$.

Proof. Choose $b \in R, b \neq 0$. Then there exist $q_1, b_1 \in R$ such that $0 = q_1b + b_1$ and $\phi(b_1) < \phi(b)$. We define a sequence b, b_1, \dots, b_n inductively: if $b_n = 0$,

stop. If $b_n \neq 0$, there exist $q_{n+1}, b_{n+1} \in R$ such that $0 = q_{n+1}b_n + b_{n+1}$ with $\phi(b_{n+1}) < \phi(b_n)$. As the sequence $\phi(b_1) > \phi(b_2) > \phi(b_3) > \dots$ is strictly decreasing in a well-ordered set, it has to be finite. Therefore $b_n = 0$ for some positive integer n . This shows that $\phi(0) = \phi(b_n) < \phi(b)$ for all non-zero b . Therefore $\phi(0)$ is the smallest element in $\phi(R)$. □

Proposition 2.12. *Let ϕ be an Euclidean algorithm on a domain R . Every element $b \in R$ such that $\phi(b)$ is the smallest element of $\phi(R \setminus \{0\})$ is a unit in R .*

Proof. Let b be an element such that $\phi(b)$ is the smallest element of $\phi(R \setminus \{0\})$. Then $b \neq 0$ by the last proposition. There exist $q, r \in R$ such that $1 = qb + r$ with $\phi(r) < \phi(b)$. By the choice of b , we have that $r = 0$. Therefore $1 = qb$, which shows that b is a unit. □

In every Euclidean domain there exists an Euclidean algorithm with some special properties:

Proposition 2.13. *If $\phi : R \rightarrow \mathbb{N}_0$ is an Euclidean algorithm on an Euclidean domain R , then ϕ_1 , defined by*

$$\begin{aligned}\phi_1(0) &:= \phi(0) \\ \phi_1(a) &:= \min \{ \phi(b) \mid b \in Ra \setminus \{0\} \}, a \neq 0\end{aligned}$$

is an Euclidean algorithm such that

1. $\phi_1(ac) \geq \phi_1(a)$ for $ac \neq 0$,
2. $\phi_1(ac) = \phi_1(a)$ if and only if $Rac = Ra$,
3. $\phi_1(a) \leq \phi(a)$ for all $a \in R$.

Proof. First note that ϕ_1 is well defined, since \mathbb{N}_0 is well ordered.

3. Let $a \in R$. If $a = 0$, then $\phi_1(0) \leq \phi(0)$ by definition. If $a \neq 0$, then $a \in Ra \setminus \{0\}$ and therefore $\phi_1(a) \leq \phi(a)$.

Let $a, b \in R, b \neq 0$. By definition, $\phi_1(b) = \phi(bc)$ for some non-zero $c \in R$. As

ϕ is an Euclidean algorithm on R , there exist $q, r \in R$ such that $a = qbc + r$ and $\phi(r) < \phi(bc)$. Now $\phi_1(r) \leq \phi(r)$ by point 3 above. Therefore $\phi_1(r) \leq \phi(r) < \phi(bc) = \phi_1(b)$. This shows that ϕ_1 is Euclidean.

1. Let $ac \neq 0$. Then $Rac \subseteq Ra$. Therefore by definition $\phi_1(ac) \geq \phi_1(a)$.
2. If $Rac = Ra$, then $\phi_1(ac) = \phi_1(a)$ by definition. On the other side, let $\phi_1(ac) = \phi_1(a)$. Without restriction we can assume that $\phi_1(ac) = \phi_1(a) \neq 0$. Therefore $ac, a \neq 0$. As ϕ_1 is an Euclidean algorithm, there exist $q, r \in R$ such that $a = qac + r$ and $\phi_1(r) < \phi_1(ac) = \phi_1(a)$. As $r = a(1 - cq)$, by 1. it follows that $r = 0$. So we see that $Rac = Ra$.

□

For this kind of Euclidean algorithm the converse of Proposition 2.12 is also true:

Corollary 2.1. *If ϕ_1 is an Euclidean algorithm as in Proposition 2.13 and u a unit in R , then $\phi_1(u)$ is the smallest element of $\phi_1(R \setminus \{0\})$.*

Proof. Let β be the smallest element of $\phi_1(R \setminus \{0\})$ and u' an element with $\phi_1(u') = \beta$. Then by Proposition 2.12 the element u' is a unit in R . As u and u' are associates, by point 2 of Proposition 2.13, we have that $\phi_1(u') = \phi_1(u) = \beta$.

□

2.3.2 The smallest Euclidean algorithm

This section is devoted to the *smallest Euclidean algorithm*. A very readable treatment is P. Samuel's paper [18]. We give a proof of *Motzkin's Lemma*, which will play an important role in showing that $\mathbb{Q}(\sqrt{14})$ is Euclidean (see Chapter 4).

Proposition 2.14. *If $\phi_\alpha : R \rightarrow \mathbb{N}_0$ is any nonempty family of Euclidean algorithms on an Euclidean domain R , then $\phi := \inf_\alpha \phi_\alpha$ is also an Euclidean algorithm.*

Proof. Let $a, b \in R$, $b \neq 0$. Then there exists an index α such that $\phi(b) = \phi_\alpha(b)$. As ϕ_α is an Euclidean algorithm on R , there exist $q, r \in R$ with

$a = qb + r$ and $\phi_\alpha(r) < \phi_\alpha(b)$. Then $\phi(r) \leq \phi_\alpha(r) < \phi_\alpha(b) = \phi(b)$. Therefore ϕ is an Euclidean algorithm on R .

□

If we now consider the family $\phi_\alpha : R \rightarrow \mathbb{N}_0$ of **all** Euclidean algorithms on R and define $\theta := \inf_\alpha \phi_\alpha$ as above, then θ is an Euclidean algorithm with the property that $\theta(x) \leq \phi(x)$ for all $x \in R$ and every Euclidean algorithm ϕ on R .

Definition 2.14. *The infimum of all Euclidean algorithms on R is called the **smallest Euclidean algorithm** on R .*

Proposition 2.15. *Let R be an Euclidean domain and ϕ an Euclidean algorithm on R . The smallest Euclidean algorithm $\theta : R \rightarrow \mathbb{N}_0$ has the following properties:*

1. $\theta(ac) \geq \theta(a)$ for $ac \neq 0$
2. $\theta(ac) = \theta(a)$ if and only if $Rac = Ra$
3. $\theta(a) \leq \phi(a)$ for all $a \in R$
4. $\theta(x) = 0 \Leftrightarrow x = 0$
5. $\theta(x) = 1 \Leftrightarrow x$ is a unit

Proof. 3. follows from the definition of the smallest Euclidean algorithm.

1. and 2. follow from Proposition 2.13: because if θ_1 is constructed out of θ , then $\theta_1(x) \leq \theta(x)$ for all $x \in R$ (this is 3. in Proposition 2.13). But on the other hand, $\theta(x) \leq \theta_1(x)$ for all $x \in R$, as θ is the smallest Euclidean algorithm. Therefore θ equals θ_1 and they have the same properties.

4. is a consequence of Proposition 2.11. Note that two Euclidean algorithms ϕ, ϕ' for which there exists an order-isomorphism $h : \phi(R) \rightarrow \phi'(R)$ with $\phi' = h \circ \phi$, have the same properties. In this case they are called *isomorphic*. Therefore $\theta(0) = 0$.

5. follows from Proposition 2.12, Corollary 2.1 and the last note on isomorphic Euclidean algorithms.

□

The next result gives a hint on how to construct the smallest Euclidean algorithm:

Proposition 2.16. *Let R be an Euclidean domain and $\theta : R \rightarrow \mathbb{N}_0$ the smallest Euclidean algorithm on R . For $n \in \mathbb{N}_0$ define*

$$A_n := \{x \in R \setminus \{0\} \mid \theta(x) \leq n + 1\}.$$

Then A_n is the set of all non-zero $b \in R$ such that the canonical map

$$A_{n-1} \cup \{0\} \rightarrow R/Rb$$

is surjective.

Proof. “ \subseteq ”: Let $b \in A_n$ be a non-zero element. Consider any class $a + Rb$ with $a \in R$. As R is Euclidean, we find $q, r \in R$ such that $a = qb + r$ with $\theta(r) < \theta(b) \leq n + 1$. From the equation we see that r is a representative of $a + Rb$ with the property $\theta(r) \leq n$. Therefore r is in $A_{n-1} \cup \{0\}$ and the canonical map $A_{n-1} \cup \{0\} \rightarrow R/Rb$ is surjective.

“ \supseteq ”: Let $b \neq 0$ and $A_{n-1} \cup \{0\} \rightarrow R/Rb$ surjective. Indirectly suppose that $\theta(b) > n + 1$. We define $\theta_1(b) := n + 1$ and $\theta_1(x) := \theta(x)$ for $x \neq b$. Then $\theta_1(x) \leq \theta(x)$ for all x in R . We claim that θ_1 is an Euclidean algorithm on R : for $a, b_1 \in R, b_1 \neq 0$, there exist $q, r \in R$ such that $a = qb_1 + r$ and $\theta(r) < \theta(b_1)$. If $b_1 \neq b$, then $\theta_1(r) \leq \theta(r) < \theta(b_1) = \theta_1(b_1)$. In the case that $b_1 = b$, there exists a representative r in $A_{n-1} \cup \{0\}$ of $a + Rb$. That is $a = qb_1 + r$ for some $q \in R$ with $\theta_1(r) \leq \theta(r) \leq n < n + 1 = \theta_1(b_1)$. Therefore θ_1 is an Euclidean algorithm on R .

But in an equation $a = cq + b$ for $c \neq 0$, where b is the remainder, we have that $\theta_1(b) = n + 1 < \theta(b) < \theta(c)$. But this contradicts the fact that θ is the smallest Euclidean algorithm on R . Therefore $\theta(b) \leq n + 1$ which implies that $b \in A_n$.

□

But what is A_0 ? From Proposition 2.15 it follows that

$$A_0 = \{x \in R \setminus \{0\} \mid \theta(x) \leq 1\} = \{x \in R \mid \theta(x) = 1\} = R^\times.$$

This motivates the following definition:

Definition 2.15. *Let R be an integral domain. Then we define*

$$\begin{aligned} A_0 &:= R^\times \\ A_n &:= \{b \in R \setminus \{0\} \mid A_{n-1} \cup \{0\} \rightarrow R/Rb \text{ is surjective}\}, n \geq 1 \\ A &:= \bigcup_{n \geq 0} A_n, \end{aligned}$$

where the map in the definition of the A_n 's ($n \geq 1$) is the canonical map. We refer to this sets as **Motzkin's construction**.

Note that A_n (for $n \geq 1$) is the set of all non-zero elements $b \in R$ such that every non-zero residue class $(\text{mod } Rb)$ has a representative in A_{n-1} .

Additionally, $(A_n)_{n \geq 0}$ is an increasing sequence of sets. We show this by induction on n :

For $n = 0$, A_0 consists of units of R . And every unit u is in A_1 , because the canonical map $A_0 \cup \{0\} \rightarrow R/Ru = R/R = \{0\}$ is surjective.

If $n > 0$ and $b \in A_n$, then the canonical map $A_{n-1} \cup \{0\} \rightarrow R/Rb$ is surjective. As $A_{n-1} \subseteq A_n$ by induction hypothesis, we have that the canonical map $A_n \cup \{0\} \rightarrow R/Rb$ is also surjective and therefore $b \in A_{n+1}$.

Now we are able to prove the following characterization of Euclidean domains:

Proposition 2.17 (Motzkin's Lemma). *Let R be an integral domain. Then R is Euclidean if and only if every non-zero element of R is in A .*

Proof. " \Rightarrow ": Let R be Euclidean and $\theta : R \rightarrow \mathbb{N}_0$ the smallest Euclidean algorithm on R . For a non-zero $b \in R$ we have that $\theta(b) = n + 1$ for some non-negative integer n . Then $b \in A_n \subseteq A$ by Proposition 2.16.

" \Leftarrow ": Suppose that every non-zero $b \in R$ is in A and therefore in one A_n for $n \geq 0$. We define an Euclidean algorithm on R as follows: define $\theta(0) := 0$. For $b \in R \setminus \{0\}$, define $\theta(b) := n + 1$ where n is the unique non-negative

integer with $b \in A_n \setminus A_{n-1}$. Please note that n is unique as $(A_n)_{n \in \mathbb{N}}$ is an increasing sequence of sets. Now let $a, b \in R$, $b \neq 0$. Then $\theta(b) = n + 1$ for some non-negative integer n . As $A_{n-1} \cup \{0\} \rightarrow R/Rb$ is surjective, the class $a + Rb$ has a representative $r \in A_{n-1}$. That is, $a = qb + r$ for some $q \in R$ and $\theta(r) \leq n < \theta(b) = n + 1$. This shows that θ is an Euclidean algorithm. \square

2.3.3 Euclidean number fields

In this section we extend the property “Euclidean” to quadratic number fields. Of special interest will be number fields for which the absolute value of the norm defines an Euclidean algorithm on the ring of integers.

Definition 2.16. *Let K be a quadratic number field and O_K its ring of integers. K is called **Euclidean** if O_K is. K and O_K are called **Norm-Euclidean** if O_K is Euclidean with respect to the absolute value of the norm.*

Note that if O_K is Euclidean with respect to the absolute value of the norm, then it is also Euclidean. The converse is not true as we will see in Chapter 3.

Let K be a quadratic number field and O_K its ring of integers. If O_K is Euclidean with respect to a function ϕ and ϕ is completely multiplicative, that is $\phi(ab) = \phi(a)\phi(b)$, then ϕ can be extended to a completely multiplicative function $\bar{\phi} : K \rightarrow \mathbb{Q}$. As O_K is Euclidean with respect to ϕ , for any $a, b \in O_K, b \neq 0$ there exist $q, r \in O_K$ such that $a = qb + r$ and $\phi(r) < \phi(b)$. This can be rewritten to the following property: for any $a, b \in O_K, b \neq 0$ there exist $q, r \in O_K$ such that $\frac{a}{b} - q = \frac{r}{b}$ with $\phi(r) < \phi(b)$ where $\frac{a}{b} \in K, q \in O_K$. If we apply the extended $\bar{\phi} : K \rightarrow \mathbb{Q}$ to the last equation we get:

Proposition 2.18. *Let K be a quadratic number field and O_K its ring of integers. Let $\phi : O_K \rightarrow \mathbb{N}_0$ be completely multiplicative and $\bar{\phi} : K \rightarrow \mathbb{Q}$ its extension to K . Then O_K is Euclidean with respect to ϕ if and only if for all $x \in K$ there exists $\gamma \in O_K$ such that $\bar{\phi}(x - \gamma) < 1$.*

As the absolute value of the norm is completely multiplicative, we have the following result:

Corollary 2.2. *The quadratic number field K is Norm-Euclidean if and only if for all $x \in K$ there exists $\gamma \in O_K$ such that $|N(x - \gamma)| < 1$.*

2.4 Inhomogeneous minima of binary quadratic forms

In this chapter we develop some of the theory of inhomogeneous minima for binary quadratic forms. We are specially interested in the minimum of the norm form in $\mathbb{Q}(\sqrt{69})$. We will follow the papers [2] and [13]. In [13], the first explicit calculation of this minimum is given.

Let $f(x, y) = ax^2 + bxy + cy^2$ be an indefinite binary quadratic form with integral a, b, c and discriminant $d = b^2 - 4ac$.

Definition 2.17. *Let x_0, y_0 be real numbers. We define*

$$M(f; x_0, y_0) := \inf |f(x + x_0, y + y_0)|,$$

where the infimum is taken over all integer values x, y .

It is clear from this definition, that if $x_0 \equiv x_1, y_0 \equiv y_1 \pmod{1}$ then $M(f; x_0, y_0) = M(f; x_1, y_1)$. If we identify tuples (x_0, y_0) with points $P \in \mathbb{R}^2$, we can write $M(f; P)$ instead of $M(f; x_0, y_0)$.

Definition 2.18. *For an indefinite binary quadratic form f we define*

$$M(f) := \sup M(f; P),$$

where the supremum is taken over all points P in the plane. $M(f)$ is called the **inhomogeneous minimum of $f(x, y)$** .

Proposition 2.19. *Equivalent forms have the same inhomogeneous minimum.*

Proof. Let f and f' be equivalent forms and $T \in GL(2, \mathbb{Z})$ with $|\det(T)| = 1$ such that $f' \circ T = f$. For any point P_0 in the plane we have $M(f', T(P_0)) =$

$M(f, P_0)$, because

$$\begin{aligned} \inf |f(P + P_0)| &= \inf |(f' \circ T)(P + P_0)| \\ &= \inf |f'(T(P) + T(P_0))| \\ &= \inf |f'(P + T(P_0))|, \end{aligned}$$

where the last equality is valid because the infimum is taken over all $P \in \mathbb{Z}^2$ and T is a bijection of \mathbb{Z}^2 . Now $M(f) = M(f')$ follows again, because we take the supremum over all $P_0 \in \mathbb{R}^2$ and T is a bijection of \mathbb{Z}^2 . □

We are now able to develop the (minimal) theory needed to calculate the inhomogeneous minimum of the norm form in $\mathbb{Q}(\sqrt{69})$. We follow Inkeris paper [13] closely. The interested reader may consult this paper also for a much more general theory applicable to other forms.

We restrict ourselves to indefinite binary quadratic forms $f(x, y) = ax^2 + bxy + cy^2$ with discriminant $d = b^2 - 4ac$ such that $0 < |a| < \sqrt{|d|}$. We can assume this last condition, as every binary quadratic form is equivalent to a form with this property (see Proposition 2.2).

If we define $D := \frac{d}{4a^2}$, then $D > \frac{1}{4}$.

We will use the following definitions in this section (X, Y and r will be specified later):

$$\begin{aligned} G(X, Y) &:= G(x, y; X, Y; r) = (x - X + rY)^2 - D(y - Y)^2 \\ C_1 &:= \frac{1}{4} \left(1 - \frac{(D - r^2 - r)^2}{D} \right) \\ C_2 &:= \frac{1}{4} ((r + 1)^2 - D) \\ C_4 &:= \frac{1}{4} (\sqrt{2D - r^2} - r)^2 \end{aligned}$$

Please note that we use C_4 instead of C_3 here to go with Inkeri's definitions.

Lemma 2.6. *Let C be a positive constant and $D = \frac{d}{4a^2}$. If for any real x_1, y_1 with*

$$-(C + Dy_1^2)^{\frac{1}{2}} \leq x_1 < 1 - (C + Dy_1^2)^{\frac{1}{2}}, \quad 0 \leq y_1 \leq \frac{1}{2}$$

there exist integral X, Y such that

$$|(x_1 - X - \frac{b}{2a}Y)^2 - D(y_1 - Y)^2| \leq C,$$

then $M(f) \leq C|a|$.

Proof. Let x_0, y_0 be real. We show that there exist real x, y with $x \equiv x_0, y \equiv y_0 \pmod{1}$ such that $|f(x, y)| \leq C|a|$. That $M(f) \leq C|a|$ then follows from the definition of $M(f; x_0, y_0)$ and $M(f)$.

If $x \equiv x_0, y \equiv y_0 \pmod{1}$ and $|f(x, y)| \leq C|a|$, then $-x \equiv -x_0, -y \equiv -y_0 \pmod{1}$ and $|f(-x, -y)| = |f(x, y)| \leq C|a|$. Therefore it suffices to consider x_0, y_0 for which there exists $y_1 \in [0, \frac{1}{2}]$ such that $y_0 \equiv y_1 \pmod{1}$.

Now choose x_1 such that $-(C + Dy_1^2)^{\frac{1}{2}} \leq x_1 < 1 - (C + Dy_1^2)^{\frac{1}{2}}$ with $x_1 \equiv \frac{b}{2a}y_1 + x_0 \pmod{1}$. By assumption, there exist integers X, Y such that

$$|(x_1 - X - \frac{b}{2a}Y)^2 - D(y_1 - Y)^2| \leq C.$$

Now define $x := x_1 - \frac{b}{2a}y_1 - X$ and $y := y_1 - Y$. Then $x \equiv x_0, y \equiv y_0 \pmod{1}$ and

$$\begin{aligned} |f(x, y)| &= |a((x + \frac{b}{2a}y)^2 - Dy^2)| \\ &= |a|(x_1 - X - \frac{b}{2a}(y_1 - (y_1 - Y)))^2 - D(y_1 - Y)^2| \leq C|a|. \end{aligned}$$

□

Lemma 2.7. Let C be a positive constant, $D = \frac{d}{4a^2}$ and r a constant satisfying $r \equiv -\frac{b}{2a} \pmod{1}$. If for any real x, y with

$$-(C + Dy^2)^{\frac{1}{2}} \leq x < 1 - (C + Dy^2)^{\frac{1}{2}}, 0 \leq y \leq \frac{1}{2} \quad (2.3)$$

there exist integral X, Y such that

$$|G(X, Y)| = |(x - X + rY)^2 - D(y - Y)^2| \leq C,$$

then $M(f) \leq C|a|$.

Proof. As $r \equiv -\frac{b}{2a} \pmod{1}$, $r = n - \frac{b}{2a}$ for an integral n . The assumption of the lemma tells us that for any x, y satisfying (2.3) there exist integral X, Y such that $|(x - X + rY)^2 - D(y - Y)^2| = |(x - (X - nY) - \frac{b}{2a}Y)^2 - D(y - Y)^2| \leq C$. As $X - nY$ is integral, we can apply Lemma 2.6.

□

Lemma 2.8. *If x, y are numbers for which (2.3) is valid and $|G(0, 0)| > C \geq \frac{1}{4}D$, then*

$$(C + Dy^2)^{\frac{1}{2}} < x < 1 - (C + Dy^2)^{\frac{1}{2}}, 0 \leq y \leq \frac{1}{2}. \quad (2.4)$$

Proof. We calculate that $G(0, 0) = x^2 - Dy^2 \geq -Dy^2 \geq -\frac{1}{4}D \geq -C$. Because $|G(0, 0)| > C$ by assumption, we get that $G(0, 0) = x^2 - Dy^2 > C$. From that we deduce that $x^2 > C + Dy^2$ and therefore $|x| > (C + Dy^2)^{\frac{1}{2}}$. Now (2.4) follows from (2.3). □

Lemma 2.9. *If $r \geq 0, r^2 + r \leq D < (r + 1)^2$ and x, y satisfy (2.4) and the relations*

$$|G(0, 1)| > C \geq C_1, \quad (2.5)$$

then

$$G(0, 1) < -C. \quad (2.6)$$

Proof. First we show that $C_1 > 0$: because $D < (r + 1)^2$ and $D > r^2$, it follows that

$$(D - r^2 - r)^2 - D = (D - (r + 1)^2) (D - r^2) < 0.$$

Therefore, $0 \leq \frac{(D - r^2 - r)^2}{D} < 1$ and so $C_1 > 0$.

Now we show that $G(0, 1) \leq C$: for that, suppose indirectly that $G(0, 1) > C$. From (2.4) we deduce that

$$0 < x + r < r + 1 - (C + Dy^2)^{\frac{1}{2}}.$$

Combination of these two gives us

$$G(0, 1) = (x + r)^2 - D(y - 1)^2 = (x + r)^2 - Dy^2 + 2Dy - D > C$$

and therefore

$$\begin{aligned} & \left(r + 1 - (C + Dy^2)^{\frac{1}{2}} \right)^2 - Dy^2 + 2Dy - D \\ &= (r + 1)^2 - 2(r + 1)(C + Dy^2)^{\frac{1}{2}} + (C + Dy^2) - Dy^2 + 2Dy - D \\ &= (r + 1)^2 - 2(r + 1)(C + Dy^2)^{\frac{1}{2}} + C + 2Dy - D > C. \end{aligned}$$

This implies that

$$(r+1)^2 - D > 2(r+1)(C + Dy^2)^{\frac{1}{2}} - 2Dy$$

and from that we have

$$(r+1)(C + Dy^2)^{\frac{1}{2}} - Dy < \frac{1}{2}((r+1)^2 - D) = 2C_2.$$

Now let us define

$$F(u, y) := (r+1)(u + Dy^2)^{\frac{1}{2}} - Dy.$$

Because $C \geq C_1 \geq 0$, we also have that

$$F(C_1, y) < 2C_2. \tag{2.7}$$

If we calculate the partial derivate of $F(u, y)$ to the variable y , we get

$$F_y(u, y) = \frac{D}{(u + Dy^2)^{\frac{1}{2}}} \left((r+1)y - (u + Dy^2)^{\frac{1}{2}} \right) = K(u, y)(4C_2y^2 - u)$$

where

$$K(u, y) = \frac{D}{(u + Dy^2)^{\frac{1}{2}} \left((r+1)y + (u + Dy^2)^{\frac{1}{2}} \right)}.$$

Note that $K(u, y) > 0$ for $u > 0, y \geq 0$.

Now consider the function $F(C_1, y)$. Let y_1 be the non-negative root of the equation

$$(C_1 + Dy^2)^{\frac{1}{2}} = \frac{1}{2},$$

that is

$$y_1 = \frac{D - r^2 - r}{2D}$$

because $D \geq r^2 + r$. As $C \geq C_1 \geq 0$, we have

$$(C_1 + Dy^2)^{\frac{1}{2}} \leq (C + Dy^2)^{\frac{1}{2}} < \frac{1}{2}$$

which implies $0 \leq y < y_1$. The last inequality follows from (2.4).

Since $C_2 > 0$, the expression $4C_2y^2 - C_1$ increases for increasing $y \in [0, \frac{1}{2}]$. Therefore, if $F_y(C_1, y) > 0$ for a y with $0 \leq y \leq y_1$, then also $F_y(C_1, y_1) > 0$. But

$$\begin{aligned} (r+1)y_1 - (C_1 + Dy_1^2)^{\frac{1}{2}} &= (r+1)\frac{D - r^2 - r}{2D} - \frac{1}{2} \\ &= -\frac{r}{2D}((r+1)^2 - D) \leq 0. \end{aligned}$$

Therefore $F_y(C_1, y) \leq 0$ for all y with $0 \leq y \leq y_1$. This means that $F(C_1, y)$ is monotonically decreasing in the interval $0 \leq y \leq y_1$. This implies that $F(C_1, y) \geq F(C_1, y_1)$ for $0 \leq y \leq y_1$. But

$$F(C_1, y_1) = \frac{1}{2}(r+1) - D \cdot \frac{D - r^2 - r}{2D} = 2C_2,$$

and therefore $F(C_1, y) \geq 2C_2$ which is a contradiction to (2.7). Thus $G(0, 1) \leq C$.

Now $G(0, 1) < -C$ because $|G(0, 1)| > C$ by assumption. □

Theorem 2.4 (K. Inkeri). *Suppose $D < 1$ and set*

$$C = \max(\frac{1}{4}D, C_1, C_4). \tag{2.8}$$

If $r \equiv -\frac{b}{2a} \pmod{1}$, $r \in [0, \frac{1}{2}]$ with $D \geq r^2 + r$, then $M(f) \leq C|a|$.

Proof. The constant C_4 is real, because $D > r^2$. This follows for $r > 0$ from the assumption $D \geq r^2 + r$ and for $r = 0$ from $D > \frac{1}{4}$.

Let x, y be arbitrary fixed values satisfying (2.3). Indirectly suppose that

$$|G(x, y; X, Y; r)| > C \tag{2.9}$$

for all integral X, Y . By Lemma 2.8 and the definition of C we have that

$$(C + Dy^2)^{\frac{1}{2}} < x < 1 - (C + Dy^2)^{\frac{1}{2}}, 0 \leq y \leq \frac{1}{2}.$$

From Lemma 2.9 we deduce that

$$G(0, 1) < -C$$

because $D < (r + 1)^2$ which follows from $D < 1$. Since

$$\sqrt{C} \geq \sqrt{C_4} = \frac{\sqrt{2D - r^2} - r}{2} \quad (2.10)$$

we have that

$$x + r > (C + Dy^2)^{\frac{1}{2}} + r \geq \sqrt{C_4} + r \geq \frac{1}{2}(\sqrt{2D - r^2} + r) \geq 0.$$

Now

$$G(0, 1) > \left((C + Dy^2)^{\frac{1}{2}} + r \right)^2 - D(1 - y)^2 = C + r^2 - D + 2f_1(y), \quad (2.11)$$

where $f_1(y) = Dy + r(C + Dy^2)^{\frac{1}{2}}$. Since $y, r \geq 0$ we have that $f_1(y) \geq f_1(0) = r\sqrt{C}$. From $G(0, 1) < -C$ and (2.11) we deduce that

$$D > 2C + 2r\sqrt{C} + r^2.$$

On the other side, we know from (2.10) that $2\sqrt{C} + r \geq 2\sqrt{C_4} + r = \sqrt{2D - r^2}$. If we square this result, we get

$$2C + 2r\sqrt{C} + r^2 \geq D$$

which is a contradiction to the inequality above.

Therefore equation (2.9) cannot be true for all integral X, Y . That is, there exist integral X, Y such that

$$|G(x, y; X, Y; r)| \leq C.$$

By Lemma 2.7 it follows that $M(f) \leq C|a|$.

□

2.4.1 Application to the norm in $\mathbb{Q}(\sqrt{69})$

We are now able to calculate the minimum of the form $f_{69}(x, y) = x^2 + xy - 17y^2$. We first apply the transformation $T = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}$ to f_{69} and get the equivalent form $-5x^2 + 7xy + y^2$. We now apply the transformation

$U = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ and obtain the form $f(x, y) = -5x^2 - 7xy + y^2$. Note that f_{69} and f are equivalent and therefore have the same inhomogeneous minimum according to Proposition 2.19.

Now let us use Theorem 2.4 to calculate an upper bound for $M(f)$:

As $a = -5, b = -7, c = 1$ we get that $r \equiv -\frac{b}{2a} \equiv -\frac{7}{10} \equiv \frac{3}{10} \pmod{1}$, so $r = \frac{3}{10} \in [0, \frac{1}{2}]$. Also $D = \frac{d}{4a^2} = \frac{69}{100}$ and therefore $\frac{1}{4} < D < 1$.

What is the constant C : $C = \max(\frac{1}{4}D, C_1, C_4)$

- $\frac{1}{4}D = \frac{69}{400} = 0.1725$
- $C_1 = \frac{1}{4} \left(1 - \frac{(D-r^2-r)^2}{D} \right) = \frac{1}{4} \left(1 - \frac{(\frac{69}{100} - \frac{9}{100} - \frac{30}{100})^2}{\frac{69}{100}} \right) = \frac{1}{4} \left(1 - \frac{(\frac{30}{100})^2}{\frac{69}{100}} \right) = \frac{1}{4} \left(1 - \frac{3}{23} \right) = \frac{1}{4} \left(\frac{20}{23} \right) = \frac{5}{23} = 0.217\dots$
- $C_4 = \frac{1}{4} (\sqrt{2D - r^2} - r)^2 = \frac{1}{4} \left(\sqrt{\frac{138}{100} - \frac{9}{100} - \frac{3}{10}} \right)^2 = \frac{1}{4} \left(\frac{\sqrt{129-3}}{10} \right)^2 = \frac{(\sqrt{129-3})^2}{400} = 0.174\dots$

Therefore we have $C = \frac{5}{23}$.

What about the condition $D \geq r^2 + r$? We calculate that $D = \frac{69}{100} > \frac{1}{2}$ and $r^2 + r = \frac{9}{100} + \frac{3}{10} = \frac{39}{100} < \frac{1}{2}$, so the condition is satisfied.

If we apply the theorem, we get that $C|a| = \frac{25}{23}$ is an upper bound for the form $f(x, y)$ and therefore $M(f) \leq \frac{25}{23}$.

We will prove now that $M(f) = \frac{25}{23}$: If there exist real x_0, y_0 such that $M(f; x_0, y_0) \geq \frac{25}{23}$, that is

$$|f(x_0 + x, y_0 + y)| \geq \frac{25}{23}$$

for all integral x, y , then $M(f) \geq \frac{25}{23}$.

Now note that $f_{69}(x, y) = N \left(x + y \left(\frac{1+\sqrt{69}}{2} \right) \right)$ for rational x, y where $N : \mathbb{Q}(\sqrt{69}) \rightarrow \mathbb{R}$ is the norm in $\mathbb{Q}(\sqrt{69})$. So we have to show that there exists $z \in \mathbb{Q}(\sqrt{69})$ such that

$$|N(\gamma + z)| \geq \frac{25}{23}$$

for all $\gamma \in O_{\mathbb{Q}(\sqrt{69})}$. Now set $z = -\frac{4}{23}\sqrt{69} \in \mathbb{Q}(\sqrt{69})$. An algebraic integer in $\mathbb{Q}(\sqrt{69})$ has the form $\gamma = \frac{1}{2}(u + v\sqrt{69})$ with integral u, v and $u \equiv v \pmod{2}$. We calculate that

$$\begin{aligned}
|N(\gamma - \frac{4}{23}\sqrt{69})| &= |N(\frac{1}{2}(u + v\sqrt{69}) - \frac{4}{23}\sqrt{69})| \\
&= |N(\frac{u}{2} + (\frac{v}{2} - \frac{4}{23})\sqrt{69})| \\
&= |(\frac{u}{2} + (\frac{v}{2} - \frac{4}{23})\sqrt{69}) \cdot (\frac{u}{2} - (\frac{v}{2} - \frac{4}{23})\sqrt{69})| \\
&= |\frac{u^2}{4} - 69(\frac{v}{2} - \frac{4}{23})^2| \\
&= |\frac{u^2}{4} - 69\frac{(23v-8)^2}{(2 \cdot 23)^2}| \\
&= |\frac{u^2}{4} - \frac{3}{4 \cdot 23}(23v - 8)^2| \\
&= \frac{1}{4 \cdot 23} \cdot |23u^2 - 3(23v - 8)^2|
\end{aligned}$$

and therefore

$$4 \cdot 23 \cdot |N(\gamma - \frac{4}{23}\sqrt{69})| = |U|, \quad (2.12)$$

where $U = 23u^2 - 3(23v - 8)^2$. Now note that $U \equiv -8 \pmod{23}$ and $U \equiv 23u^2 - 3 \cdot 23^2v^2 \equiv -u^2 + v^2 \equiv 0 \pmod{4}$. This implies that $U \equiv -8 \pmod{4 \cdot 23}$.

If we assume $U = -8$, then $-8 \equiv 23u^2 \equiv -u^2 \pmod{3}$ and therefore $u^2 \equiv 2 \pmod{3}$. But this is not possible as 2 is not a quadratic residue modulo 3. So we have $U \neq -8$.

In the case $U = 4 \cdot 23 - 8 = 84$ we get $3 \equiv 5u^2 + 6v^2 + 6v + 6 \pmod{9}$ and this is equivalent to $0 \equiv 5u^2 + 6(v^2 + v - 1) \pmod{9}$. For integral v we calculate that $v^2 + v - 1 \equiv 1, 2, 5$ or $8 \pmod{9}$. This implies that $6(v^2 + v - 1) \equiv 3$ or $6 \pmod{9}$. For integral u we get $u^2 \equiv 0, 1, 4$ or $7 \pmod{9}$ and therefore $5u^2 \equiv 0, 2, 5$ or $8 \pmod{9}$. From that we deduce that $5u^2 + 6(v^2 + v - 1) \equiv 2, 3, 5, 6$ or $8 \pmod{9}$ but not $\equiv 0 \pmod{9}$. So $U \neq 84$.

Therefore $|U| \geq 100$ and from (2.12) we deduce that

$$|N(\gamma - \frac{4}{23}\sqrt{69})| \geq \frac{25}{23}.$$

This implies that $M(f) \geq \frac{25}{23}$.

Noting the results above, we proved the following:

Proposition 2.20. *The inhomogeneous minimum of $f_{69}(x, y) = x^2 + xy - 17y^2$ is $M(f_{69}) = \frac{25}{23}$. It is attained (at least) in the points $z_1 = (\frac{19}{23}, \frac{8}{23})$, $z_2 = (\frac{4}{23}, \frac{15}{23})$.*

Chapter 3

$\mathbb{Q}(\sqrt{69})$ is Euclidean

In this chapter we will give a detailed outline of the proof of D. A. Clark that the ring of integers of $\mathbb{Q}(\sqrt{69})$ is Euclidean. This is the first example of a quadratic number field which is Euclidean but not Norm-Euclidean. For the original proof see [4]. For this we will explicitly define a completely multiplicative Euclidean algorithm on the prime elements which can then be extended to the ring of integers.

If we set $\alpha = \frac{1+\sqrt{69}}{2}$, then $\mathbb{Z}[\alpha]$ is the ring of integers of $\mathbb{Q}(\sqrt{69})$. Note that $\{1, \alpha\}$ is a \mathbb{Z} -basis for $\mathbb{Z}[\alpha]$. So every element $\gamma \in \mathbb{Z}[\alpha]$ can be uniquely written as $\gamma = a + b \cdot \alpha$ where a and b are integers.

Let $N : \mathbb{Q}(\sqrt{69}) \rightarrow \mathbb{Q}$ denote the norm in the number field $\mathbb{Q}(\sqrt{69})$. That is $N(x + y \cdot \alpha) = x^2 + x \cdot y - 17 \cdot y^2$ for rational x, y .

Please note that in this section we use the following notion of divisibility: if $z \in \mathbb{Q}(\sqrt{69})$, $z \neq 0$ and $\gamma \in \mathbb{Z}[\alpha]$, then “ z is divisible by γ ” (in symbols $\gamma|z$) means that if $z = \frac{z_1}{z_2}$ with $z_1, z_2 \in \mathbb{Z}[\alpha]$ and $\gcd(z_1, z_2) = 1$, then z_1 does not contain the factor γ when written as a product of elements of $\mathbb{Z}[\alpha]$. The element 0 is not divisible by any other element.

The following lemma tells us how to define an Euclidean algorithm:

Lemma 3.1 (Clark, [4]). *Let $z \in \mathbb{Q}(\sqrt{69})$. If z is not congruent to $\pm \frac{26+7\alpha}{10+3\alpha}$ modulo $\mathbb{Z}[\alpha]$, then there exists a translate $\gamma \in \mathbb{Z}[\alpha]$ such that $|N(z + \gamma)| < 1$*

and $z + \gamma$ is not divisible by $10 + 3\alpha$.

Proof. Without loss of generality we can assume that $z = x + y \cdot \alpha$ where x, y are rational numbers and $0 \leq x, y < 1$. So we can identify z with an element of the 2-torus $X = \mathbb{R}^2/\mathbb{Z}^2$, where the second component is the α -coordinate.

We then use a computer program that splits $X \cong [0, 1) \times [0, 1)$ into small rectangles. For every rectangle it searches for two translates $\gamma_1, \gamma_2 \in \mathbb{Z}[\alpha]$ such that for every point z in the rectangle we have $|N(z + \gamma_1)| < 1$ and $|N(z + \gamma_2)| < 1$ and $\gamma_1 - \gamma_2$ is not divisible by $10 + 3\alpha$. The last condition ensures that $z + \gamma_1$ or $z + \gamma_2$ is not divisible by $10 + 3\alpha$. If both would be divisible by $10 + 3\alpha$, then also the difference $(z + \gamma_1) - (z + \gamma_2) = \gamma_1 - \gamma_2$ would be - a contradiction. The program shows that this works for almost all parts of X except for three small areas (Proposition A.3). If we define a norm on $X = \mathbb{R}^2/\mathbb{Z}^2$ via $|z| = \min\{\|r\| : r \in \mathbb{R}^2, r + \mathbb{Z}^2 = z\}$ (where $\|\cdot\|$ is the Euclidean norm on \mathbb{R}^2), then these areas are all contained in balls with radius $\delta = \frac{6}{1000}$ and center points $(0, 0)$, $(\frac{19}{23}, \frac{8}{23})$ and $(\frac{4}{23}, \frac{15}{23})$. Please note that the last two points are congruent to $\pm \frac{26+7\alpha}{10+3\alpha}$ modulo $\mathbb{Z}[\alpha]$. So every point that does not lie in one of these balls fulfills the lemma. Have a look at Appendix A for an example implementation of such a computer program.

Now we want to show the following: let z be an element for which there exists a unit u in $\mathbb{Z}[\alpha]$ such that $u \cdot z$ modulo $\mathbb{Z}[\alpha]$ lies outside of all three balls, then z fulfills the lemma.

Let $u \cdot z = y$ be an element outside of the three balls. Then there exists $\gamma \in \mathbb{Z}[\alpha]$ such that $|N(y + \gamma)| < 1$ and $y + \gamma$ is not divisible by $10 + 3\alpha$. This implies that $|N(z + u^{-1} \cdot \gamma)| = |N(u \cdot z + \gamma)| < 1$ where $u^{-1} \cdot \gamma$ is an element of $\mathbb{Z}[\alpha]$. We also have $10 + 3\alpha \nmid z + u^{-1} \cdot \gamma$, because $10 + 3\alpha \nmid u \cdot z + \gamma$ and the right parts only differ by a product of a unit in $\mathbb{Z}[\alpha]$. Therefore z fulfills the lemma with $u^{-1} \cdot \gamma$ as an appropriate translate.

Now we show that for every point $z \in X$ not congruent to $(0, 0)$, $(\frac{19}{23}, \frac{8}{23})$ and $(\frac{4}{23}, \frac{15}{23})$ there exists a unit u in $\mathbb{Z}[\alpha]$ such that $u \cdot z$ modulo $\mathbb{Z}[\alpha]$ lies outside of the three balls. This can be shown with the principle of *expan-*

siveness from the theory of dynamical systems. We especially used ideas of M. Einsiedler from his notes [7].

If z is an element that lies outside of the three balls there is nothing to show (choose $u = 1$). So first take $z \neq (0, 0)$ to be an element with $|z| < \delta$, that is z lies in the δ -ball around $(0, 0)$. By *Dirichlet's Unit Theorem* (see Theorem 2.2) there exists a unit ε_0 (the *fundamental unit*), such that every unit is of the form $\pm \varepsilon_0^n$ for integral n . If we consider $\mathbb{Q}(\sqrt{69})$, then $\varepsilon_0 = 11 + 3\alpha$ (see for example [11] on how to calculate the fundamental unit). In matrix notation ε_0 corresponds to the fundamental automorph $T = \begin{pmatrix} 11 & 51 \\ 3 & 14 \end{pmatrix}$.

Let us interpret T as a toral automorphism, that is an automorphism on $\mathbb{R}^2/\mathbb{Z}^2$. The eigenvalues of T are $\lambda = \frac{25+3\sqrt{69}}{2}$ and $\mu = \frac{1}{\lambda}$. The corresponding eigenvectors v_λ and v_μ form a basis of \mathbb{R}^2 . There exists an element $v \in \mathbb{R}^2$ with $\|v\| < \delta$ and $\pi(v) = z$, where $\pi : \mathbb{R}^2 \rightarrow \mathbb{R}^2/\mathbb{Z}^2$ is defined as $\pi(x) = x + \mathbb{Z}^2$. There exist real a_1, a_2 such that $v = a_1 v_\lambda + a_2 v_\mu$. If we apply powers of T to v we deduce that

$$T^n v = \lambda^n a_1 v_\lambda + \mu^n a_2 v_\mu$$

because λ and μ are eigenvalues of the eigenvectors v_λ and v_μ . Note that n is an integer, so also negative values for n are allowed. The matrix T^{-1} also has integer entries because T has determinant 1.

First let $a_1 \neq 0$. The equation above tells us that for increasing n the point $T^n v$ expands to the direction v_λ by a factor $\lambda < 25$ (note that $\lambda > 1$). At the same time, $T^n v$ contracts to the direction v_μ because $\mu = \frac{1}{\lambda} < 1$. Therefore we can find an integer $n \geq 0$ such that $\delta < |T^n v| < 25 \cdot \delta$. But this means we have found a unit $u = \varepsilon_0^n$ such that $u \cdot z$ modulo $\mathbb{Z}[\alpha]$ lies outside of the three balls.

If $a_1 = 0$, then $T^n v$ converges to $(0, 0)$ for increasing n . Therefore we have to consider negative values of n . As $v \neq 0$ we know that $a_2 \neq 0$. Because $T^n v = \mu^n a_2 v_\mu$, there exists an integer $n \leq 0$ such that $\delta < |T^n v| < 25 \cdot \delta$. Again we have found a unit $u = \varepsilon_0^n$ for which $u \cdot z$ modulo $\mathbb{Z}[\alpha]$ is an element outside of the three balls.

Note that for the point $(0, 0)$ this cannot work, because it is a fixed point of the toral automorphism T . This is also true for the two other center points $z_0 = (\frac{19}{23}, \frac{8}{23})$ and $z_1 = (\frac{4}{23}, \frac{15}{23})$.

What remains to show is that for every point in the δ -balls around z_0 and z_1 (and not equal to the center points) there again exists a unit such that multiplication with it brings us out of the tree balls. To show this, let z be an element with $0 < |z - z_i| < \delta$ where $i \in \{0, 1\}$. As the element $z - z_i \neq (0, 0)$ lies in the δ -ball around $(0, 0)$ there exists an integer n such that $\delta < |T^n(z - z_i)| < 25 \cdot \delta$. But this implies that $\delta < |T^n z - T^n z_i| = |T^n z - z_i| < 25 \cdot \delta$, where we used that z_0, z_1 are fixed points of T . So we again found a unit $u = \varepsilon_0^n$ such that $u \cdot z$ modulo $\mathbb{Z}[\alpha]$ is not contained in any of the three δ -balls.

So for every point not congruent to $(0, 0)$, $(\frac{19}{23}, \frac{8}{23})$ and $(\frac{4}{23}, \frac{15}{23})$ there exists a unit u in $\mathbb{Z}[\alpha]$ such that $u \cdot z$ modulo $\mathbb{Z}[\alpha]$ lies outside of the balls. From what we have shown above, it follows that all these points fulfill the lemma.

The point $(0, 0)$ satisfies the conditions of the lemma, because $|N(0)| = 0 < 1$.

□

We are now able to show that $\mathbb{Z}[\alpha]$ is Euclidean. For every prime element π in $\mathbb{Z}[\alpha]$ define

$$\phi(\pi) = \begin{cases} |N(\pi)|, & \text{if } \pi \neq 10 + 3\alpha \\ 26, & \text{if } \pi = 10 + 3\alpha \end{cases}$$

Then ϕ extends to a completely multiplicative function $\phi : \mathbb{Z}[\alpha] \rightarrow \mathbb{N}$. We write $\bar{\phi} : \mathbb{Q}(\sqrt{69}) \rightarrow \mathbb{Q}$ for the extension to the number field.

Now let z be an element of $\mathbb{Q}(\sqrt{69})$. If z is congruent to $\pm \frac{26+7\alpha}{10+3\alpha}$ modulo $\mathbb{Z}[\alpha]$ there exists $\gamma \in \mathbb{Z}[\alpha]$ such that $z + \gamma = \pm \frac{26+7\alpha}{10+3\alpha}$. We calculate that $\bar{\phi}(z + \gamma) = \bar{\phi}(\pm \frac{26+7\alpha}{10+3\alpha}) = \frac{\bar{\phi}(\pm(26+7\alpha))}{\bar{\phi}(10+3\alpha)} = \frac{|N(\pm(26+7\alpha))|}{26} = \frac{25}{26} < 1$. If z is not congruent to $\pm \frac{26+7\alpha}{10+3\alpha}$, then by Lemma 3.1 there exists a translate $\gamma \in \mathbb{Z}[\alpha]$ such that $|N(z + \gamma)| < 1$ and $z + \gamma$ is not divisible by $10 + 3\alpha$. The last condition ensures that $\bar{\phi}(z + \gamma) \leq |N(z + \gamma)| < 1$.

So for every $z \in \mathbb{Q}(\sqrt{69})$ we have found an element $\gamma \in \mathbb{Z}[\alpha]$ such that

$\bar{\phi}(z + \gamma) < 1$. Now by Proposition 2.18 it follows that $\mathbb{Q}(\sqrt{69})$ is Euclidean with respect to ϕ .

It remains to show that $\mathbb{Q}(\sqrt{69})$ is not Norm-Euclidean. From section 2.4.1 we know that there exists an element $z \in \mathbb{Q}(\sqrt{69})$ such that for all $\gamma \in \mathbb{Z}[\alpha]$ we have $|N(\gamma - z)| \geq \frac{25}{23} > 1$. Corollary 2.2 implies that $\mathbb{Q}(\sqrt{69})$ cannot be Norm-Euclidean.

Chapter 4

$\mathbb{Q}(\sqrt{14})$ is Euclidean

In this chapter we prove that another quadratic number field, namely $\mathbb{Q}(\sqrt{14})$, is Euclidean. This has first been proven by M. Harper in his paper [8]. This time we are not able to explicitly write down an Euclidean algorithm as in the previous chapter.

Let K denote a real quadratic number field and O_K its ring of integers. We only consider O_K that are principal ideal domains, as this is a necessary condition for O_K to be Euclidean (see Proposition 2.10). That $\mathbb{Z}[\sqrt{14}]$ is a principal ideal domain follows from Proposition 2.3 because it has class number one. This can be verified by a computer algebra system, for example *Pari/GP*¹.

4.1 Characterization of Euclidean domains

We first repeat the main result of section 2.3.2 - *Motzkin's Lemma*. The definitions of A and A_n ($n \geq 0$) are as follows:

¹Pari/GP can be downloaded for free from <http://pari.math.u-bordeaux.fr/>

Definition 4.1. Let R be an integral domain. Then we define

$$\begin{aligned} A_0 &:= R^\times \\ A_n &:= \{b \in R \setminus \{0\} \mid A_{n-1} \cup \{0\} \rightarrow R/Rb \text{ is surjective}\}, n \geq 1 \\ A &:= \bigcup_{n \geq 0} A_n, \end{aligned}$$

where the map in the definition of the A_n ($n \geq 1$) is the canonical map. We refer to this sets as **Motzkin's construction**.

Proposition 4.1 (Motzkin's Lemma). Let R be an integral domain. R is Euclidean if and only if every non-zero element of R is in A .

Proof. See Proposition 2.17 for a proof. □

Harper then used a similar definition of the A_n to show an analog of *Motzkin's Lemma*. For this we need the concept of an *admissible set of primes*:

Definition 4.2. Let $\pi_1, \dots, \pi_s \in O_K$ be distinct non-associate primes. The set $\{\pi_1, \dots, \pi_s\}$ is an **admissible set of primes** if for all $\beta = \pi_1^{a_1} \dots \pi_s^{a_s}$ with $a_i \in \mathbb{N}_0$, every coprime residue class modulo β can be represented by a unit of O_K .

By a proposition of Clark and Murty (see [5], page 160), it suffices to check this condition for all $\beta = \pi_1^2 \dots \pi_s^2$:

Proposition 4.2 (Clark and Murty). Let $\pi_1, \dots, \pi_s \in O_K$ be distinct non-associate primes. Further suppose that each π_i is unramified and of odd prime norm. If every coprime residue class modulo $\pi_1^2 \dots \pi_s^2$ contains a unit, then $\{\pi_1, \dots, \pi_s\}$ is an admissible set of s primes in O_K .

Proof. We show that if O_K^\times maps onto $(O_K/(\pi_1^2 \dots \pi_s^2))^\times$, then O_K^\times maps onto $(O_K/(\pi_1^{a_1} \dots \pi_s^{a_s}))^\times$ for all $a_i \in \mathbb{N}_0$, $i = 1, \dots, s$. Here the map is just the canonical map. The proposition then directly follows from the definition of an admissible set of primes.

Suppose this statement is true for all products $\pi_1^{m_1} \dots \pi_s^{m_s}$, where $m_i \leq n_i$ for $i = 1, \dots, s$ and at least one of the inequalities is strict. By the *Generalized Chinese Remainder Theorem* (Proposition 2.4) and the fact that $(R \times S)^\times \cong R^\times \times S^\times$ for rings R, S , we have that

$$(O_K/(\pi_1^{a_1} \dots \pi_s^{a_s}))^\times \cong (O_K/(\pi_1^{a_1}))^\times \times \dots \times (O_K/(\pi_s^{a_s}))^\times \quad (4.1)$$

for all non-negative integers a_i , $i = 1, \dots, s$. From Proposition 2.9 it follows that $(O_K/(\pi_1^{n_1-1}))^\times$ is cyclic. Let $x + (\pi_1^{n_1-1})$, $x \in O_K$ be a generator of $(O_K/(\pi_1^{n_1-1}))^\times$. As O_K^\times maps onto

$$(O_K/(\pi_1^{n_1-1}))^\times \times (O_K/(\pi_2^{n_2}))^\times \times \dots \times (O_K/(\pi_s^{n_s}))^\times$$

by equation (4.1), there exists an element $\varepsilon_1 \in O_K^\times$ that maps to

$$(x + (\pi_1^{n_1-1}), 1 + (\pi_2^{n_2}), \dots, 1 + (\pi_s^{n_s})).$$

This element satisfies $\varepsilon_1 \equiv 1 \pmod{\pi_i^{n_i}}$ for $i = 2, \dots, s$. Furthermore, by Proposition 2.8, ε_1 has order $p_1^{n_1-2}(p_1-1)$ modulo $\pi_1^{n_1-1}$ and therefore also modulo $\pi_1^{n_1-1}\pi_2^{n_2} \dots \pi_s^{n_s}$, where $p_1 = |N(\pi_1)|$.

Additionally we have that

$$\varepsilon_1^{p_1^{n_1-3}(p_1-1)} \equiv 1 \pmod{\pi_1^{n_1-2}},$$

as $|(O_K/(\pi_1^{n_1-2}))^\times| = p_1^{n_1-3}(p_1-1)$. Because $\varepsilon_1 \equiv 1 \pmod{\pi_i^{n_i}}$, $i = 2, \dots, s$ it follows that

$$\varepsilon_1^{p_1^{n_1-3}(p_1-1)} \equiv 1 \pmod{\pi_1^{n_1-2}\pi_2^{n_2} \dots \pi_s^{n_s}}$$

which means that

$$\varepsilon_1^{p_1^{n_1-3}(p_1-1)} = 1 + k\pi_1^{n_1-2}\pi_2^{n_2} \dots \pi_s^{n_s}, \text{ where } \pi_1 \nmid k. \quad (4.2)$$

Because if $\pi_1 \mid k$, then $k = \pi_1 \cdot l$ for some l , and so

$$\varepsilon_1^{p_1^{n_1-3}(p_1-1)} = 1 + l\pi_1\pi_1^{n_1-2}\pi_2^{n_2} \dots \pi_s^{n_s} = 1 + l\pi_1^{n_1-1}\pi_2^{n_2} \dots \pi_s^{n_s}$$

from which it follows that

$$\varepsilon_1^{p_1^{n_1-3}(p_1-1)} \equiv 1 \pmod{\pi_1^{n_1-1}\pi_2^{n_2} \dots \pi_s^{n_s}},$$

a contradiction to the order of ε_1 modulo $\pi_1^{n_1-1}\pi_2^{n_2}\dots\pi_s^{n_s}$.

Furthermore, we have that $0 \equiv k'\pi_1^{n_1} (\pi_1^{n_1-1}\pi_2^{n_2}\dots\pi_s^{n_s})$ for some k' with $\pi_1 \nmid k'$ (e.g. $k' = \pi_2^{n_2}\dots\pi_s^{n_s}$). This implies the equation

$$\varepsilon_1^{p_1^{n_1-2}(p_1-1)} \equiv 1 + k'\pi_1^{n_1} (\pi_1^{n_1-1}\pi_2^{n_2}\dots\pi_s^{n_s}), \text{ where } \pi_1 \nmid k'. \quad (4.3)$$

From equations (4.2) and (4.3) we deduce that ε_1 has order $p_1^{n_1-1}(p_1-1)$ modulo $\pi_1^{n_1}\pi_2^{n_2}\dots\pi_s^{n_s}$.

In the same way, we can show that there exist elements $\varepsilon_i \in O_K^\times$, $i = 2, \dots, s$ such that $\varepsilon_i \equiv 1 (\pi_j^{n_j})$ for $j \neq i$ and ε_i has order $p_i^{n_i-1}(p_i-1)$ modulo $\pi_1^{n_1}\pi_2^{n_2}\dots\pi_s^{n_s}$, where $p_i = |N(\pi_i)|$.

If we consider the multiplicative group G generated by $\varepsilon_1, \dots, \varepsilon_s$, then G is a subgroup of O_K^\times and maps onto $(O_K/(\pi_1^{n_1}\dots\pi_s^{n_s}))^\times$. Therefore also O_K^\times maps onto $(O_K/(\pi_1^{n_1}\dots\pi_s^{n_s}))^\times$.

□

Definition 4.3. *Let B_0 be the monoid generated by the unit group of O_K and an admissible set of primes. For $n \geq 1$ define*

$$B_n := \{\text{primes } \pi \in O_K \mid B_{n-1} \cup B_0 \rightarrow (O_K/\pi)^\times \text{ is surjective}\}$$

where the map is the canonical map. We define

$$B := \bigcup_{n \geq 0} B_n.$$

Note that for the construction of B_n ($n \geq 1$) only primes of the ring of integers are considered. Then the variant of *Motzkin's Lemma* that Harper proved is as follows:

Lemma 4.1. *Let O_K be a principal ideal domain. If all primes of O_K are in B , then O_K is Euclidean.*

Proof. Let all primes of O_K be in B . By Proposition 4.1, if every non-zero element of O_K is in A , then O_K is Euclidean. That is what we want to use.

To show that a non-zero $\beta \in O_K$ is in A , it suffices to show that every non-zero residue class $(\text{mod } \beta)$ has a representative in A :

Because if $\beta \neq 0$ and every non-zero residue class $(\text{mod } \beta)$ has a representative in A , then each of these representatives lie in one A_n . Now there are only finitely many such representatives (this follows from the fact that $|O_K/(\beta \cdot O_K)| = \mathcal{N}(\beta \cdot O_K) < \infty$) and $A_n \subseteq A_{n+1}$ as we have seen next to the definition of the A_n 's in section 2.3.2. From this we deduce that all these representatives lie in one A_n for n sufficiently large. But this means that $\beta \in A_{n+1}$ which implies that $\beta \in A$.

Now we continue with induction to show that a non-zero β of O_K is in A . For this we need the following definitions: $\Omega_0(\beta)$ counts the prime divisors of β that are in B_0 (according to multiplicity) and $\Omega_1(\beta)$ those prime divisors that are not in B_0 (again according to their multiplicity). For a prime element π of O_K we define

$$\lambda(\pi) = \begin{cases} 0, & \text{if } \pi \in B_0 \\ n, & \text{if } \pi \in B_n \setminus B_{n-1} \end{cases}$$

Then we extend λ to $O_K \setminus \{0\}$ by complete additivity: if $\beta = \pi_1^{a_1} \cdots \pi_s^{a_s}$, then

$$\begin{aligned} \lambda(\beta) &= \sum_i a_i \lambda(\pi_i) \\ \Omega_0(\beta) &= \sum_{\pi_i \in B_0} a_i \\ \Omega_1(\beta) &= \sum_{\pi_i \notin B_0} a_i \end{aligned}$$

Note that λ , Ω_0 and Ω_1 are well defined: O_K is a principal ideal domain and therefore has unique factorization; by assumption, all primes of O_K are in B ; $B_n \subseteq B_{n+1}$ (same proof as for the A_n 's); B_n is closed under taking of associates.

For induction we use the triple $(\Omega_1(\beta), \Omega_0(\beta), \lambda(\beta))$ which we order lexicographically:

If $\beta \in O_K^\times$, then $(\Omega_1(\beta), \Omega_0(\beta), \lambda(\beta)) = (0, 0, 0)$ and $\beta \in A$ by definition of A .

Now take $\beta \neq 0$ to be no unit and consider a non-zero residue class $\alpha \pmod{\beta}$. We will show there exists an $\alpha' \equiv \alpha \pmod{\beta}$ that precedes β in the ordering. By the induction hypothesis, we have that $\alpha' \in A$. Therefore $\alpha \pmod{\beta}$ has a representative in A and by what we have shown at the beginning of this proof, β is in A .

We first consider the case when α and β are coprime. There are several possibilities:

1. $\beta \in B_0$: that is $\Omega_1(\beta) = 0, \Omega_0(\beta) \geq 1$

By the definition of B_0 (admissible primes), we can represent $\alpha \pmod{\beta}$ by a unit α' so that $\Omega_1(\alpha') = 0$ and $\Omega_0(\alpha') = 0 < \Omega_0(\beta)$.

2. β is a prime not in B_0 : $\Omega_1(\beta) = 1, \Omega_0(\beta) = 0$

Then $\beta \in B_n \setminus B_{n-1}$ for some $n \geq 1$ and $\lambda(\beta) = n$. By the definition of B_n , $\alpha \pmod{\beta}$ can be represented by an element α' in $B_{n-1} \cup B_0$: If $\alpha' \in B_0$, then $\Omega_1(\alpha') = 0$.

If $\alpha' \notin B_0$, then $\alpha' \in B_{n-1}$ for some $n > 1$. α' is a prime with $\Omega_1(\alpha') = 1, \Omega_0(\alpha') = 0$ and $\lambda(\alpha') < n = \lambda(\beta)$.

3. Otherwise: $\Omega_1(\beta) = 1$ and $\Omega_0(\beta) \geq 1$ or else $\Omega_1(\beta) \geq 2$

We use an analog of *Dirichlet's theorem on primes in arithmetic progression* (see H. Hasse [9], page 32). From this theorem follows the existence of a prime element α' with $\alpha' \equiv \alpha \pmod{\beta}$. There are two possible cases:

$\alpha' \in B_0$: then $\Omega_1(\alpha') = 0$ and $\Omega_0(\alpha') = 1$.

$\alpha' \notin B_0$: then $\Omega_1(\alpha') = 1$ and $\Omega_0(\alpha') = 0$.

In each case we were able to find an element α' preceding β with $\alpha' \equiv \alpha \pmod{\beta}$.

Now let us assume that α and β are not coprime, that is $\gcd(\alpha, \beta) = \delta \neq 1$. Then $a = \frac{\alpha}{\delta}$ and $b = \frac{\beta}{\delta}$ are coprime. If $\frac{\beta}{\delta}$ is no unit, we can find a' preceding b with $a' \equiv a \pmod{b}$. But then $a' \cdot \delta \equiv \alpha \pmod{\beta}$ and $a' \cdot \delta$ precedes $\beta = b \cdot \delta$

in our ordering (because Ω_0, Ω_1 and λ are completely additive). If $\frac{\beta}{\delta}$ is a unit, then $\frac{\beta}{\delta}$ divides $\frac{\alpha}{\delta}$ and therefore β divides α . But then $\alpha \pmod{\beta}$ is the zero class which we need not consider.

Therefore, every non-zero residue class $\alpha \pmod{\beta}$ (for $\beta \neq 0$) has a representative in A . This implies that every non-zero $\beta \in O_K$ is in A . By Proposition 4.1 (*Motzkin's Lemma*), O_K is Euclidean. □

4.2 Numerical criterion for Euclidean rings

To be able to apply Lemma 4.1 to some ring of integers O_K , one has to verify that all primes of O_K are in B . In this section we prove a numerical estimate that enables us to show that a number field is Euclidean. Remember that we only consider O_K that are principal ideal domains.

Definition 4.4. For $S \subseteq O_K$, we define \mathcal{S} to be the set of ideals generated by elements of S :

$$\mathcal{S} = \{\alpha \cdot O_K \mid \alpha \in S\}.$$

For a set \mathcal{S} of ideals, $\mathcal{S}(x)$ denotes the set of those ideals in \mathcal{S} with norm less than or equal to x :

$$\mathcal{S}(x) = \{\mathfrak{a} \in \mathcal{S} \mid \mathcal{N}(\mathfrak{a}) \leq x\}.$$

Definition 4.5. Let \mathfrak{M} be a monoid in O_K whose elements are coprime to an ideal \mathfrak{a} . Under reduction $\pmod{\mathfrak{a}}$, the image of \mathfrak{M} forms a subgroup of $(O_K/\mathfrak{a})^\times$. The order of this subgroup will be denoted by $f_{\mathfrak{M}}(\mathfrak{a})$. If $\mathfrak{M} = O_K^\times$, we write $f(\mathfrak{a})$.

Definition 4.6. $\alpha_1, \dots, \alpha_t \in K$ are called **multiplicatively independent** if $\alpha_1^{a_1} \cdot \dots \cdot \alpha_t^{a_t} = 1$ with $a_i \in \mathbb{Z}$ implies $a_i = 0$ for all $1 \leq i \leq t$.

Then Gupta and Murty provided the following bound on prime ideals:

Proposition 4.3 (Gupta-Murty). Let \mathfrak{M} be a monoid in O_K . If \mathfrak{M} contains a set of t multiplicatively independent elements, then

$$\#\{\text{prime ideals } \mathfrak{p} \mid f_{\mathfrak{M}}(\mathfrak{p}) \leq Y\} \ll Y^{\frac{t+1}{t}}.$$

The implied constant depends only on K and \mathfrak{M} .

Proof. See [5], Lemma 6. □

To be able to apply the large sieve inequality, we use the following objects and definitions:

- \mathcal{A} ... a finite set of non-associated elements of O_K
- \mathcal{P} ... a finite set of non-ramifying prime ideals of K
- Z ... the cardinality of \mathcal{A}
- $Z(\alpha, \mathfrak{p})$... the cardinality of $\{\beta \in \mathcal{A} \mid \beta \equiv \alpha \pmod{\mathfrak{p}}\}$
- $\mathfrak{w}(\mathfrak{p})$... the number of residue classes $\alpha \pmod{\mathfrak{p}}$ with $Z(\alpha, \mathfrak{p}) = 0$
- X ... a bound such that $X \geq \max_{\beta \in \mathcal{A}} |N(\beta)|$
- Q ... a bound such that $Q \geq \max_{\mathfrak{p} \in \mathcal{P}} \mathcal{N}(\mathfrak{p})$

Then we are able to formulate a Theorem on the large sieve in number fields:

Proposition 4.4 (The Large Sieve in Number Fields).

$$\sum_{\mathfrak{p} \in \mathcal{P}} \left(\mathcal{N}(\mathfrak{p}) \sum_{\alpha \pmod{\mathfrak{p}}} \left(Z(\alpha, \mathfrak{p}) - \frac{Z}{\mathcal{N}(\mathfrak{p})} \right)^2 \right) \ll (Q^2 + X) \cdot Z$$

where the implied constant depends only on K .

Proof. See [22], Theorem 1. □

From the inequality

$$\sum_{\alpha \pmod{\mathfrak{p}}} \left(Z(\alpha, \mathfrak{p}) - \frac{Z}{\mathcal{N}(\mathfrak{p})} \right)^2 \geq \frac{Z^2 \cdot \mathfrak{w}(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})^2}$$

we deduce that

$$\frac{\mathcal{N}(\mathfrak{p})^2}{Z^2} \cdot \sum_{\alpha \pmod{\mathfrak{p}}} \left(Z(\alpha, \mathfrak{p}) - \frac{Z}{\mathcal{N}(\mathfrak{p})} \right)^2 \geq \mathfrak{w}(\mathfrak{p}).$$

With the help of the inequality we can prove the following corollary:

Corollary 4.1.

$$\sum_{\mathfrak{p} \in \mathcal{P}} \frac{\mathfrak{w}(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})} \ll \frac{Q^2 + X}{Z}$$

Proof. By applying the last result and Proposition 4.4 we deduce that:

$$\sum_{\mathfrak{p} \in \mathcal{P}} \frac{\mathfrak{w}(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})} \leq \frac{1}{Z^2} \sum_{\mathfrak{p} \in \mathcal{P}} \mathcal{N}(\mathfrak{p}) \sum_{\alpha \pmod{\mathfrak{p}}} \left(Z(\alpha, \mathfrak{p}) - \frac{Z}{\mathcal{N}(\mathfrak{p})} \right)^2 \ll \frac{Q^2 + X}{Z}.$$

□

The next result is the numerical criterion that helps us to show that some rings of integers are Euclidean:

Lemma 4.2. *If*

$$\#\mathcal{B}_1(x) \gg \frac{x}{\log^2(x)}$$

then O_K is Euclidean.

Proof. We show that $\#\mathcal{B}_2(x) \sim \frac{x}{\log(x)}$. Then all primes must be in B_3 (and therefore in B): indirectly suppose that there is a prime $\pi \notin B_3$. This means there is a residue class $\pmod{\pi}$ which has no representative in B_2 . By the *Dirichlet density theorem* (see [17], page 567f), the density of prime ideals in a class are the same for every class. Therefore, the density of \mathcal{B}_2 is less than 1 (if it exists). On the other side, from $\#\mathcal{B}_2(x) \sim \frac{x}{\log(x)}$ it follows that \mathcal{B}_2 has density 1, a contradiction. A more detailed explanation of this step can be found in [16].

Therefore, if $\#\mathcal{B}_2(x) \sim \frac{x}{\log(x)}$, then by Lemma 4.1 the ring of integers O_K is Euclidean.

Note that $\#\mathcal{B}_2(x) \sim \frac{x}{\log(x)}$ is equivalent to $\#\mathcal{B}_2^c(x) = o\left(\frac{x}{\log(x)}\right)$, where \mathcal{B}_2^c is the complement of \mathcal{B}_2 in the set of prime ideals. By the *Landau prime ideal theorem* (see [14]) we know that $\#\{\text{prime ideals } \mathfrak{p} \mid \mathcal{N}(\mathfrak{p}) \leq x\} \sim \frac{x}{\log(x)}$.

We therefore have $\#\mathcal{B}_2(x) + \#\mathcal{B}_2^c(x) \sim \frac{x}{\log(x)}$. Then

$$\begin{aligned} \lim_{x \rightarrow \infty} \frac{\#\mathcal{B}_2^c(x)}{\frac{x}{\log(x)}} &= \lim_{x \rightarrow \infty} \frac{\#\{\text{prime ideals } \mathfrak{p} \mid \mathcal{N}(\mathfrak{p}) \leq x\} - \#\mathcal{B}_2(x)}{\frac{x}{\log(x)}} \\ &= \lim_{x \rightarrow \infty} \frac{\#\{\text{prime ideals } \mathfrak{p} \mid \mathcal{N}(\mathfrak{p}) \leq x\}}{\frac{x}{\log(x)}} - \lim_{x \rightarrow \infty} \frac{\#\mathcal{B}_2(x)}{\frac{x}{\log(x)}} \\ &= 1 - \lim_{x \rightarrow \infty} \frac{\#\mathcal{B}_2(x)}{\frac{x}{\log(x)}}. \end{aligned}$$

Now if $\#\mathcal{B}_2^c(x) = o\left(\frac{x}{\log(x)}\right)$, then $\lim_{x \rightarrow \infty} \frac{\#\mathcal{B}_2^c(x)}{\frac{x}{\log(x)}} = 0$ and therefore $\lim_{x \rightarrow \infty} \frac{\#\mathcal{B}_2(x)}{\frac{x}{\log(x)}} = 1$, so $\#\mathcal{B}_2(x) \sim \frac{x}{\log(x)}$. The other direction is also true, because we can invert the implications of the last sentence.

We apply the large sieve as follows:

- $\mathcal{A} \dots$ a set of representatives of $\mathcal{B}_1(x^2)$
- $Z := \#\mathcal{A} = \#\mathcal{B}_1(x^2)$
- $X := x^2$
- $\mathcal{P} := \mathcal{B}_2^c(x)$
- $Q := x$

Then X and Q are upper bounds on the norms of all elements of \mathcal{A} and \mathcal{P} respectively.

By Corollary 4.1 and the assumption that $\#\mathcal{B}_1(x) \gg \frac{x}{\log^2(x)}$, we deduce that

$$\sum_{\mathfrak{p} \in \mathcal{B}_2^c(x)} \frac{\mathfrak{w}(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})} \ll \frac{Q^2 + X}{Z} = \frac{2 \cdot x^2}{\#\mathcal{B}_1(x^2)} \ll \frac{x^2}{\left(\frac{x^2}{\log^2(x^2)}\right)} = \log^2(x^2) = 4 \cdot \log^2(x)$$

and therefore

$$\sum_{\mathfrak{p} \in \mathcal{B}_2^c(x)} \frac{\mathfrak{w}(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})} \ll \log^2(x). \quad (4.4)$$

As we want to measure the number of elements of \mathcal{B}_2^c , we need a lower bound on $\mathfrak{w}(\mathfrak{p})$. We show that for $\mathfrak{p} \in \mathcal{B}_2^c$, $\mathfrak{w}(\mathfrak{p}) \geq f(\mathfrak{p})$:

If $\mathfrak{p} \in \mathcal{B}_2^c$, then $\mathfrak{p} \notin \mathcal{B}_2$. This means that there exists a non-zero residue class $(\text{mod } \mathfrak{p})$ which has no representative in B_1 . Note that $f(\mathfrak{p})$ is the size of the unit group reduced $(\text{mod } \mathfrak{p})$ embedded into $(O_K/\mathfrak{p})^\times$ and that by definition, B_1 is closed under the taking of associates. So if one non-zero residue class $(\text{mod } \mathfrak{p})$ is not represented by an element in B_1 , then at least $f(\mathfrak{p})$ aren't. Therefore $\mathfrak{w}(\mathfrak{p}) \geq f(\mathfrak{p})$.

By the Gupta-Murty bound (Prop. 4.3), if O_K has a unit of infinite order (e.g., the fundamental unit) then

$$\#\{\text{prime ideals } \mathfrak{p} \mid f(\mathfrak{p}) \leq Y\} \ll Y^2.$$

If we set $Y = x^{\frac{1}{2}-\varepsilon}$ (where $0 < \varepsilon < 1/2$), then

$$\#\{\text{prime ideals } \mathfrak{p} \mid \mathcal{N}(\mathfrak{p}) \leq x \text{ and } f(\mathfrak{p}) \leq \mathcal{N}(\mathfrak{p})^{\frac{1}{2}-\varepsilon}\} \ll x^{1-2\varepsilon}.$$

Because

$$\begin{aligned} \lim_{x \rightarrow \infty} \frac{\#\{\text{prime ideals } \mathfrak{p} \mid \mathcal{N}(\mathfrak{p}) \leq x \text{ and } f(\mathfrak{p}) \leq \mathcal{N}(\mathfrak{p})^{\frac{1}{2}-\varepsilon}\}}{\frac{x}{\log(x)}} \\ \leq \lim_{x \rightarrow \infty} \frac{c \cdot \frac{x}{x^{2\varepsilon}}}{\frac{x}{\log(x)}} = \lim_{x \rightarrow \infty} c \cdot \frac{\log(x)}{x^{2\varepsilon}} = 0 \end{aligned}$$

for some $c > 0$, it follows that

$$\#\{\text{prime ideals } \mathfrak{p} \mid \mathcal{N}(\mathfrak{p}) \leq x \text{ and } f(\mathfrak{p}) \leq \mathcal{N}(\mathfrak{p})^{\frac{1}{2}-\varepsilon}\} = o\left(\frac{x}{\log(x)}\right). \quad (4.5)$$

From equation (4.4) above, we deduce that

$$\begin{aligned} \log^2(x) &\gg \sum_{\substack{\mathfrak{p} \in \mathcal{B}_2^c(x) \\ f(\mathfrak{p}) > \mathcal{N}(\mathfrak{p})^{\frac{1}{2}-\varepsilon}}} \frac{\mathfrak{w}(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})} \geq \sum_{\substack{\mathfrak{p} \in \mathcal{B}_2^c(x) \\ f(\mathfrak{p}) > \mathcal{N}(\mathfrak{p})^{\frac{1}{2}-\varepsilon}}} \frac{f(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})} \\ &> \sum_{\substack{\mathfrak{p} \in \mathcal{B}_2^c(x) \\ f(\mathfrak{p}) > \mathcal{N}(\mathfrak{p})^{\frac{1}{2}-\varepsilon}}} \frac{1}{\mathcal{N}(\mathfrak{p})^{\frac{1}{2}+\varepsilon}} > \frac{\#\{\mathfrak{p} \in \mathcal{B}_2^c(x) \mid f(\mathfrak{p}) > \mathcal{N}(\mathfrak{p})^{\frac{1}{2}-\varepsilon}\}}{x^{\frac{1}{2}+\varepsilon}} \end{aligned}$$

where we use that $\mathfrak{w}(\mathfrak{p}) \geq f(\mathfrak{p})$ and $\mathcal{N}(\mathfrak{p}) \leq x$ for $\mathfrak{p} \in \mathcal{B}_2^c(x)$. Then

$$\#\{\mathfrak{p} \in \mathcal{B}_2^c(x) \mid f(\mathfrak{p}) > \mathcal{N}(\mathfrak{p})^{\frac{1}{2}-\varepsilon}\} = o\left(\frac{x}{\log(x)}\right), \quad (4.6)$$

because

$$\begin{aligned} \lim_{x \rightarrow \infty} \frac{\#\{\mathfrak{p} \in \mathcal{B}_2^c(x) \mid f(\mathfrak{p}) > \mathcal{N}(\mathfrak{p})^{\frac{1}{2}-\varepsilon}\}}{\frac{x}{\log(x)}} &\leq \lim_{x \rightarrow \infty} \frac{c \cdot \log^2(x) \cdot x^{\frac{1}{2}+\varepsilon}}{\frac{x}{\log(x)}} \\ &= \lim_{x \rightarrow \infty} c \cdot \frac{\log^3(x)}{x^{\frac{1}{2}-\varepsilon}} = 0. \end{aligned}$$

If we combine equations (4.5) and (4.6), then

$$\#\mathcal{B}_2^c(x) = o\left(\frac{x}{\log(x)}\right),$$

as we see from

$$\begin{aligned} \#\mathcal{B}_2^c(x) &\leq \#\{\mathfrak{p} \in \mathcal{B}_2^c(x) \mid f(\mathfrak{p}) > \mathcal{N}(\mathfrak{p})^{\frac{1}{2}-\varepsilon}\} \\ &\quad + \#\{\text{prime ideals } \mathfrak{p} \mid \mathcal{N}(\mathfrak{p}) \leq x \text{ and } f(\mathfrak{p}) \leq \mathcal{N}(\mathfrak{p})^{\frac{1}{2}-\varepsilon}\} \\ &= o\left(\frac{x}{\log(x)}\right) + o\left(\frac{x}{\log(x)}\right) = o\left(\frac{x}{\log(x)}\right). \end{aligned}$$

At the beginning we have shown that this is equivalent to $\#\mathcal{B}_2(x) \sim \frac{x}{\log(x)}$. This implies that all primes are in B_3 and therefore by Lemma 4.1 that O_K is Euclidean. □

4.3 Admissible set of primes in $\mathbb{Z}[\sqrt{14}]$

We construct an admissible set of two primes here. This will guarantee the existence of three multiplicatively independent elements in the set B_0 . For this let $\varepsilon_0 = 15 + 4\sqrt{14}$ be the fundamental unit of $\mathbb{Z}[\sqrt{14}]$. If we set

- $\pi_1 := 5 - \sqrt{14}$
- $\pi_2 := 3 - 2\sqrt{14}$

then

Proposition 4.5. $\{\pi_1, \pi_2\}$ is an admissible set of primes in $\mathbb{Z}[\sqrt{14}]$.

Proof. We use Proposition 4.2 to show that $\{\pi_1, \pi_2\}$ is an admissible set of primes. The norms of π_1 and π_2 are

$$\begin{aligned} N(\pi_1) &= 5^2 - (-1)^2 \cdot 14 = 25 - 14 = 11 \\ N(\pi_2) &= 3^2 - (-2)^2 \cdot 14 = 9 - 56 = -47 \end{aligned}$$

and therefore π_1, π_2 are distinct non-associate primes with odd prime norm. Furthermore, the Jacobi symbols $\left(\frac{14}{11}\right)$ and $\left(\frac{14}{47}\right)$ both equal 1 and by Proposition 2.7, π_1 and π_2 are split primes and therefore unramified.

Next we show that ε_0 is a generator of $(\mathbb{Z}[\sqrt{14}]/(\pi_1^2))^\times$ and $-\varepsilon_0$ a generator of $(\mathbb{Z}[\sqrt{14}]/(\pi_2^2))^\times$:
By Proposition 2.8, $|(\mathbb{Z}[\sqrt{14}]/(\pi_1))^\times| = |N(\pi_1)| - 1 = 10$. ε_0 is a generator of $(\mathbb{Z}[\sqrt{14}]/(\pi_1))^\times$, if $\varepsilon_0, \varepsilon_0^2$ and $\varepsilon_0^5 \not\equiv 1 \pmod{\pi_1}$ and $\varepsilon_0^{10} \equiv 1 \pmod{\pi_1}$:

- $\varepsilon_0 \not\equiv 1 \pmod{\pi_1}$:

$$\begin{aligned} \frac{\varepsilon_0 - 1}{\pi_1} &= \frac{14 + 4\sqrt{14}}{5 - \sqrt{14}} = \frac{(14 + 4\sqrt{14})(5 + 4\sqrt{14})}{25 - 14} \\ &= \frac{70 + 20\sqrt{14} + 14\sqrt{14} + 56}{11} = \frac{126 + 34\sqrt{14}}{11} \notin \mathbb{Z}[\sqrt{14}] \end{aligned}$$

- $\varepsilon_0^2 \not\equiv 1 \pmod{\pi_1}$:

$$\begin{aligned} \varepsilon_0^2 &= (15 + 4\sqrt{14})^2 = 225 + 120\sqrt{14} + 224 = 449 + 120\sqrt{14} \\ \frac{\varepsilon_0^2 - 1}{\pi_1} &= \frac{448 + 120\sqrt{14}}{5 - \sqrt{14}} = \frac{(448 + 120\sqrt{14})(5 + \sqrt{14})}{11} \\ &= \frac{2240 + 600\sqrt{14} + 448\sqrt{14} + 1680}{11} \\ &= \frac{3920 + 1048\sqrt{14}}{11} \notin \mathbb{Z}[\sqrt{14}] \end{aligned}$$

- $\varepsilon_0^5 \not\equiv 1 \pmod{\pi_1}$:

$$\begin{aligned}
\varepsilon_0^5 &= (449 + 120\sqrt{14})^2(15 + 4\sqrt{14}) \\
&= (201601 + 107760\sqrt{14} + 201600)(15 + 4\sqrt{14}) \\
&= (403201 + 107760\sqrt{14})(15 + 4\sqrt{14}) \\
&= 6048015 + 1616400\sqrt{14} + 1612804\sqrt{14} + 6034560 \\
&= 12082575 + 3229204\sqrt{14} \\
\frac{\varepsilon_0^5 + 1}{\pi_1} &= \frac{12082576 + 3229204\sqrt{14}}{5 - \sqrt{14}} \\
&= \frac{(12082576 + 3229204\sqrt{14})(5 + \sqrt{14})}{11} \\
&= \frac{60412880 + 16146020\sqrt{14} + 12082576\sqrt{14} + 45208856}{11} \\
&= \frac{105621736 + 28228596\sqrt{14}}{11} \\
&= 9601976 + 2566236\sqrt{14} \in \mathbb{Z}[\sqrt{14}]
\end{aligned}$$

Therefore $\varepsilon_0^5 \equiv -1 \pmod{\pi_1}$. Because $-1 \not\equiv 1 \pmod{\pi_1}$, it follows that $\varepsilon_0^5 \not\equiv 1 \pmod{\pi_1}$.

- $\varepsilon_0^{10} \equiv 1 \pmod{\pi_1}$:

From above we know that $\pi_1 | (\varepsilon_0^5 + 1)$. This implies that

$$\pi_1 | (\varepsilon_0^5 + 1)(\varepsilon_0^5 - 1) = (\varepsilon_0^{10} - 1).$$

Therefore ε_0 is a generator of $(\mathbb{Z}[\sqrt{14}]/(\pi_1))^\times$. Additionally, $\varepsilon_0^{10} \equiv 1 \pmod{\pi_1^2}$:
Suppose that $\pi_1^2 | (\varepsilon_0^{10} - 1)$, then $\pi_1^2 | (\varepsilon_0^5 - 1)(\varepsilon_0^5 + 1)$. As $\pi_1 \nmid (\varepsilon_0^5 - 1)$ it follows that $\pi_1^2 | (\varepsilon_0^5 + 1)$. But

$$\begin{aligned}
\frac{\varepsilon_0^5 + 1}{\pi_1^2} &= \frac{9601976 + 2566236\sqrt{14}}{5 - \sqrt{14}} \\
&= \frac{(9601976 + 2566236\sqrt{14})(5 + \sqrt{14})}{11} \\
&= \frac{48009880 + 12831180\sqrt{14} + 9601976\sqrt{14} + 35927304}{11} \\
&= \frac{83937184 + 22433156\sqrt{14}}{11} \notin \mathbb{Z}[\sqrt{14}].
\end{aligned}$$

We get that $\varepsilon_0^{10} \not\equiv 1 \pmod{\pi_1^2}$. The fact that ε_0 is a generator of $(\mathbb{Z}[\sqrt{14}]/(\pi_1^2))^\times$ now follows from Lemma 2.5 (as a principal ideal domain, $\mathbb{Z}[\sqrt{14}]$ is also a unique factorization domain). By Proposition 2.8,

$$|(\mathbb{Z}[\sqrt{14}]/(\pi_1^2))^\times| = |N(\pi_1)| \cdot (|N(\pi_1)| - 1) = 11 \cdot 10 = 110.$$

The order of $(\mathbb{Z}[\sqrt{14}]/(\pi_2))^\times$ is $|N(\pi_2)| - 1 = 46$. Therefore $-\varepsilon_0$ generates $(\mathbb{Z}[\sqrt{14}]/(\pi_2))^\times$, if $-\varepsilon_0, (-\varepsilon_0)^2$ and $(-\varepsilon_0)^{23} \not\equiv 1 \pmod{\pi_2}$ and $(-\varepsilon_0)^{46} \equiv 1 \pmod{\pi_2}$:

- $-\varepsilon_0 \not\equiv 1 \pmod{\pi_2}$:

$$\begin{aligned} \frac{-\varepsilon_0 - 1}{\pi_2} &= \frac{-16 - 4\sqrt{14}}{3 - 2\sqrt{14}} = \frac{(-16 - 4\sqrt{14})(3 + 2\sqrt{14})}{-47} \\ &= \frac{(16 + 4\sqrt{14})(3 + 2\sqrt{14})}{47} = \frac{48 + 12\sqrt{14} + 32\sqrt{14} + 112}{47} \\ &= \frac{160 + 44\sqrt{14}}{47} \notin \mathbb{Z}[\sqrt{14}] \end{aligned}$$

- $(-\varepsilon_0)^2 \not\equiv 1 \pmod{\pi_2}$:

$$\begin{aligned} (-\varepsilon_0)^2 &= \varepsilon_0^2 = 449 + 120\sqrt{14} \\ \frac{(-\varepsilon_0)^2 - 1}{\pi_2} &= \frac{448 + 120\sqrt{14}}{3 - 2\sqrt{14}} = \frac{(448 + 120\sqrt{14})(3 + 2\sqrt{14})}{-47} \\ &= -\frac{1344 + 360\sqrt{14} + 896\sqrt{14} + 3360}{47} \\ &= -\frac{4704 + 1256\sqrt{14}}{47} \notin \mathbb{Z}[\sqrt{14}] \end{aligned}$$

- $(-\varepsilon_0)^{23} \not\equiv 1 \pmod{\pi_2}$:

We used *Mathematica*² for the following calculation:

```
In[1] := Epsilon = 15 + 4*Sqrt[14];
In[2] := ((-Epsilon)^23 + 1)*(3 + 2*Sqrt[14])/-47//Simplify//Expand
Out[2] = 1023393020653197993190258226750950 +
        273513289664281073438698673954768 Sqrt[14]
```

²Mathematica is a product of Wolfram Research, Inc., <http://www.wolfram.com/>

This shows that $(-\varepsilon_0)^{23} \equiv -1 \pmod{\pi_2}$. Therefore $(-\varepsilon)^{23} \not\equiv 1 \pmod{\pi_2}$, as $-1 \not\equiv 1 \pmod{\pi_2}$.

- $(-\varepsilon_0)^{46} \equiv 1 \pmod{\pi_2}$:

We have shown that $\pi_2 \mid ((-\varepsilon_0)^{23} + 1)$ above. It follows that

$$\pi_2 \mid ((-\varepsilon_0)^{23} + 1)((-\varepsilon_0)^{23} - 1) = ((-\varepsilon_0)^{46} - 1)$$

and so $(-\varepsilon_0)^{46} \equiv 1 \pmod{\pi_2}$.

Therefore $-\varepsilon_0$ generates $(\mathbb{Z}[\sqrt{14}]/(\pi_2))^\times$. Furthermore, $(-\varepsilon_0)^{46} \not\equiv 1 \pmod{\pi_2^2}$: Suppose that $\pi_2^2 \mid ((-\varepsilon_0)^{46} - 1)$, then $\pi_2^2 \mid ((-\varepsilon_0)^{23} - 1)((-\varepsilon_0)^{23} + 1)$. As $\pi_2 \nmid ((-\varepsilon_0)^{23} - 1)$, we deduce that $\pi_2^2 \mid ((-\varepsilon_0)^{23} + 1)$. But $\frac{(-\varepsilon_0)^{23} + 1}{\pi_2^2} \notin \mathbb{Z}[\sqrt{14}]$, as the following calculation with *Mathematica* shows:

```
In[1] := Epsilon = 15 + 4*Sqrt[14];
In[2] := ((-Epsilon)^23 + 1)*(3 + 2*Sqrt[14])^2/(-47)^2//Simplify//Expand
Out[2] = -10728551172559464035854337550986354/47 -
(2867325910299239206696612475366204 Sqrt[14])/47
```

Therefore $(-\varepsilon_0)^{46} \not\equiv 1 \pmod{\pi_2^2}$. By Lemma 2.5, the element $-\varepsilon_0$ generates $(\mathbb{Z}[\sqrt{14}]/(\pi_2^2))^\times$. The order of $(\mathbb{Z}[\sqrt{14}]/(\pi_2^2))^\times$ is 2162 (by Proposition 2.8).

Next we calculate the order of ε_0 in $(\mathbb{Z}[\sqrt{14}]/(\pi_2^2))^\times$:

First note that $\varepsilon_0 \not\equiv 1 \pmod{\pi_2}$, as

$$\begin{aligned} \frac{\varepsilon_0 - 1}{\pi_2} &= \frac{14 + 4\sqrt{14}}{3 - 2\sqrt{14}} = \frac{(14 + 4\sqrt{14})(3 + 2\sqrt{14})}{-47} \\ &= \frac{42 + 12\sqrt{14} + 28\sqrt{14} + 112}{-47} = -\frac{154 + 40\sqrt{14}}{47} \notin \mathbb{Z}[\sqrt{14}] \end{aligned}$$

As

$$\varepsilon_0^{23} = -(-\varepsilon_0)^{23} \equiv 1 \pmod{\pi_2},$$

we see that ε_0 has order 23 in $(\mathbb{Z}[\sqrt{14}]/(\pi_2))^\times$. Let n be the order of ε_0 in $(\mathbb{Z}[\sqrt{14}]/(\pi_2^2))^\times$, then $n \mid |(\mathbb{Z}[\sqrt{14}]/(\pi_2^2))^\times| = 47 \cdot 46 = 2162$. As $\varepsilon_0^n \equiv 1 \pmod{\pi_2^2}$ we have that $\varepsilon_0^n \equiv 1 \pmod{\pi_2}$ and therefore $23 \mid n$. We conclude that $n \in \{23, 23 \cdot 2, 23 \cdot 47, 23 \cdot 2 \cdot 47\}$:

- $\varepsilon_0^{23} \not\equiv 1 \pmod{\pi_2^2}$:

With the help of *Mathematica*, we compute that:

```

In[1] := Epsilon = 15 + 4*Sqrt[14];
In[2] := (Epsilon^23 - 1)*(3 + 2*Sqrt[14])^2/(-47)^2//Simplify//Expand
Out[2] = 10728551172559464035854337550986354/47 +
        (2867325910299239206696612475366204 Sqrt[14])/47

```

This shows that $\varepsilon_0^{23} \not\equiv 1 \pmod{\pi_2^2}$.

- $\varepsilon_0^{23 \cdot 2} \not\equiv 1 \pmod{\pi_2^2}$:

We have shown above that $\varepsilon_0^{46} = (-\varepsilon_0)^{46} \not\equiv 1 \pmod{\pi_2^2}$.

- $\varepsilon_0^{23 \cdot 47} \equiv 1 \pmod{\pi_2^2}$:

We performed the following calculation in *Mathematica*:

```

In[1] := Epsilon = 15 + 4*Sqrt[14];
In[2] := (Epsilon^1081 - 1)*(3 + 2*Sqrt[14])^2/(-47)^2//Simplify//Expand

```

The output is an element in $\mathbb{Z}[\sqrt{14}]$. We omitted it here for lack of space.

This shows that ε_0 has order 1081 in $(\mathbb{Z}[\sqrt{14}]/(\pi_2^2))^\times$.

As 110 and 1081 are coprime, ε_0^{1081} is also a generator of $(\mathbb{Z}[\sqrt{14}]/(\pi_1^2))^\times$ such that $\varepsilon_0^{1081} \equiv 1 \pmod{\pi_2^2}$. There exists a positive integer a such that $\varepsilon_0^{1081a} \equiv (-\varepsilon_0)^{-1} \pmod{\pi_1^2}$. This implies that $-\varepsilon_0^{1081a+1} \equiv 1 \pmod{\pi_1^2}$. The element $-\varepsilon_0^{1081a+1}$ generates $(\mathbb{Z}[\sqrt{14}]/(\pi_1^2))^\times$.

By the *Chinese Remainder Theorem* (see Proposition 2.4), we know that

$$\left(\mathbb{Z}[\sqrt{14}]/(\pi_1^2 \cdot \pi_2^2)\right) \cong \left(\mathbb{Z}[\sqrt{14}]/(\pi_1^2)\right) \times \left(\mathbb{Z}[\sqrt{14}]/(\pi_2^2)\right),$$

because (π_1^2) and (π_2^2) are coprime ideals. The isomorphism is given by

$$z + (\pi_1^2 \cdot \pi_2^2) \xrightarrow{\sigma} (z + (\pi_1^2), z + (\pi_2^2)).$$

For rings R, S we have the relation $(R \times S)^\times \cong R^\times \times S^\times$, so we conclude that

$$\left(\mathbb{Z}[\sqrt{14}]/(\pi_1^2 \cdot \pi_2^2)\right)^\times \cong \left(\mathbb{Z}[\sqrt{14}]/(\pi_1^2)\right)^\times \times \left(\mathbb{Z}[\sqrt{14}]/(\pi_2^2)\right)^\times.$$

Now consider an arbitrary coprime residue class modulo $\pi_1^2 \cdot \pi_2^2$ – that is an element $z + (\pi_1^2 \cdot \pi_2^2)$ in $(\mathbb{Z}[\sqrt{14}]/(\pi_1^2 \cdot \pi_2^2))^\times$. The isomorphism above tells us that we can interpret the residue class as an element in

$$\left(\mathbb{Z}[\sqrt{14}]/(\pi_1^2)\right)^\times \times \left(\mathbb{Z}[\sqrt{14}]/(\pi_2^2)\right)^\times.$$

Because ε_0^{1081} is a generator for $(\mathbb{Z}[\sqrt{14}]/(\pi_1^2))^\times$ and $-\varepsilon_0^{1081a+1}$ is a generator for $(\mathbb{Z}[\sqrt{14}]/(\pi_2^2))^\times$, there exist non-negative integers x, y such that

$$(z + (\pi_1^2), z + (\pi_2^2)) = ((\varepsilon_0^{1081})^x + (\pi_1^2), (-\varepsilon_0^{1081a+1})^y + (\pi_2^2)).$$

Now the unit $u := (\varepsilon_0^{1081})^x \cdot (-\varepsilon_0^{1081a+1})^y$ is a representative of this element: Let $\pi : O_K \rightarrow (O_K/(\pi_1^2 \cdot \pi_2^2))$ be the canonical map. Then

$$\begin{aligned} \sigma(\pi(u)) &= (u + (\pi_1^2), u + (\pi_2^2)) \\ &= ((\varepsilon_0^{1081})^x \cdot (-\varepsilon_0^{1081a+1})^y + (\pi_1^2), (\varepsilon_0^{1081})^x \cdot (-\varepsilon_0^{1081a+1})^y + (\pi_2^2)) \\ &= ((\varepsilon_0^{1081})^x \cdot 1 + (\pi_1^2), 1 \cdot (-\varepsilon_0^{1081a+1})^y + (\pi_2^2)) \\ &= ((\varepsilon_0^{1081})^x + (\pi_1^2), (-\varepsilon_0^{1081a+1})^y + (\pi_2^2)). \end{aligned}$$

Therefore every coprime residue class modulo $\pi_1^2 \cdot \pi_2^2$ can be represented by a unit.

By Proposition 4.2, $\{\pi_1, \pi_2\}$ is an admissible set of primes. □

4.4 The Lower Bound Sieve

In this section we present a result which allows us to estimate the number of certain primes. This will later allow us to show that the ring of integers $\mathbb{Z}[\sqrt{14}]$ fulfills the numerical condition of Lemma 4.2.

Lemma 4.3. *Suppose a and k are coprime integers. Set $d = \gcd(a - 1, k)$ and suppose $\gcd(\frac{a-1}{d}, d) = 1$. The number of primes $p \leq x$ such that*

- $p \equiv a \pmod{k}$ and

- $\frac{p-1}{d}$ is divisible only by primes l exceeding $x^{\frac{2}{7}-\varepsilon}$

is $\gg \frac{x}{\log^2(x)}$.

Proof. For a similar proof see Heath-Brown [10], Lemma 1. □

4.5 Proof that $\mathbb{Q}(\sqrt{14})$ is Euclidean

Now we are able to prove the main result of this chapter:

Theorem 4.1 (M. Harper). $\mathbb{Z}[\sqrt{14}]$ is an Euclidean domain.

Proof. Let B_0 be the monoid generated by the units of $\mathbb{Z}[\sqrt{14}]$ and the two admissible primes π_1, π_2 of section 4.3. With the help of Lemma 4.3 we will show that $\#\mathcal{B}_1(x) \gg \frac{x}{\log^2(x)}$. Then by Lemma 4.2 it follows that $\mathbb{Z}[\sqrt{14}]$ is Euclidean.

To apply Lemma 4.3, we set $a = 11$ and $k = 56$. Then $d = \gcd(a - 1, k) = \gcd(10, 56) = 2$, a and k are coprime and $\gcd(\frac{a-1}{d}, d) = \gcd(5, 2) = 1$. Therefore the set of primes $p \leq x$ with $p \equiv 11 \pmod{56}$ and $\frac{p-1}{2}$ is only divisible by primes l with $l > x^{\frac{2}{7}-\varepsilon}$ has cardinality $\gg \frac{x}{\log^2(x)}$.

Each prime $p \equiv 11 \pmod{56}$ splits in $\mathbb{Z}[\sqrt{14}]$: As $p \neq 2$, if the Jacobi symbol $\left(\frac{14}{p}\right)$ equals 1, then p splits (this follows from Proposition 2.7). By the properties of the Jacobi symbol, it follows that $\left(\frac{14}{p}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{7}{p}\right)$. Because $p \equiv 3 \pmod{8}$, $\left(\frac{2}{p}\right) = -1$ (because of the second supplementary law). By quadratic reciprocity we deduce that $\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right)$, as $p \equiv 7 \equiv 3 \pmod{4}$. Additionally, $\left(\frac{p}{7}\right) = \left(\frac{4}{7}\right)$ because $p \equiv 4 \pmod{7}$. Therefore $\left(\frac{14}{p}\right) = \left(\frac{4}{7}\right) = \left(\frac{2}{7}\right)^2 = 1$.

As every $p \equiv 11 \pmod{56}$ splits in $\mathbb{Z}[\sqrt{14}]$, there exist two different prime ideals $\mathfrak{p}, \mathfrak{p}'$ in $\mathbb{Z}[\sqrt{14}]$ such that $p \cdot \mathcal{O}_K = \mathfrak{p} \cdot \mathfrak{p}'$. From

$$p^2 = \mathcal{N}(p \cdot \mathcal{O}_K) = \mathcal{N}(\mathfrak{p} \cdot \mathfrak{p}') = \mathcal{N}(\mathfrak{p}) \cdot \mathcal{N}(\mathfrak{p}'),$$

we deduce that $p = \mathcal{N}(\mathfrak{p}) = \mathcal{N}(\mathfrak{p}')$. So for two different rational primes $p, \bar{p} \leq x$, the corresponding prime ideals are also different and have norm less or equal to x .

Therefore, we have shown that the set of prime ideals \mathfrak{p} in $\mathbb{Z}[\sqrt{14}]$ such that $\mathcal{N}(\mathfrak{p}) \equiv 11 \pmod{56}$, $\mathcal{N}(\mathfrak{p}) \leq x$ and $\frac{\mathcal{N}(\mathfrak{p})-1}{2}$ is only divisible by primes $l > x^{\frac{2}{7}-\varepsilon}$ has cardinality $\gg \frac{x}{\log^2(x)}$.

Now we show that $\mathfrak{p} \in \mathcal{B}_1$ if and only if $f_{B_0}(\mathfrak{p}) = \mathcal{N}(\mathfrak{p}) - 1$:

$f_{B_0}(\mathfrak{p})$ is defined to be the order of $B_0 \pmod{\mathfrak{p}}$ embedded into $(\mathbb{Z}[\sqrt{14}]/\mathfrak{p})^\times$. Note that $\mathcal{N}(\mathfrak{p}) - 1 = |(\mathbb{Z}[\sqrt{14}]/\mathfrak{p})^\times|$ for prime ideals \mathfrak{p} : as $\mathbb{Z}[\sqrt{14}]$ is a principal ideal domain and \mathfrak{p} a prime ideal, \mathfrak{p} is also a maximal ideal in $\mathbb{Z}[\sqrt{14}]$. Therefore $\mathbb{Z}[\sqrt{14}]/\mathfrak{p}$ is a field which implies that $(\mathbb{Z}[\sqrt{14}]/\mathfrak{p})^\times = (\mathbb{Z}[\sqrt{14}]/\mathfrak{p}) \setminus \{(0)\}$. The equation follows because $\mathcal{N}(\mathfrak{p}) = |\mathbb{Z}[\sqrt{14}]/\mathfrak{p}|$ by definition. Now if $\mathfrak{p} \in \mathcal{B}_1$, then the embedding is surjective. Therefore $f_{B_0}(\mathfrak{p}) = |(\mathbb{Z}[\sqrt{14}]/\mathfrak{p})^\times| = \mathcal{N}(\mathfrak{p}) - 1$. On the other hand, if $f_{B_0}(\mathfrak{p}) = \mathcal{N}(\mathfrak{p}) - 1 = |(\mathbb{Z}[\sqrt{14}]/\mathfrak{p})^\times|$ then the embedding is surjective which implies that $\mathfrak{p} \in \mathcal{B}_1$.

As $\mathcal{N}(\mathfrak{p}) \equiv 11 \pmod{56}$, we deduce that $\mathcal{N}(\mathfrak{p}) \equiv 3 \pmod{4}$. Without loss of generality, we can assume that $2|f_{B_0}(\mathfrak{p})$ (since $-1 \in B_0$). Therefore $2 \nmid \frac{\mathcal{N}(\mathfrak{p})-1}{f_{B_0}(\mathfrak{p})}$, as $\mathcal{N}(\mathfrak{p}) - 1 \equiv 2 \pmod{4}$.

Then $\frac{\mathcal{N}(\mathfrak{p})-1}{f_{B_0}(\mathfrak{p})} = 1$ or $\frac{\mathcal{N}(\mathfrak{p})-1}{f_{B_0}(\mathfrak{p})} > x^{\frac{2}{7}-\varepsilon}$:

Set $l = \frac{\mathcal{N}(\mathfrak{p})-1}{f_{B_0}(\mathfrak{p})}$. Note that $f_{B_0}(\mathfrak{p}) \leq \mathcal{N}(\mathfrak{p}) - 1$. Now there are two possible cases:

1. $f_{B_0}(\mathfrak{p}) = \mathcal{N}(\mathfrak{p}) - 1$, that is $l = 1$.
2. $f_{B_0}(\mathfrak{p}) < \mathcal{N}(\mathfrak{p}) - 1$, then $l > 1$ and l is a natural number (because $f_{B_0}(\mathfrak{p})$ denotes the order of a subgroup of $(\mathbb{Z}[\sqrt{14}]/\mathfrak{p})^\times$). Also $l \mid \frac{\mathcal{N}(\mathfrak{p})-1}{2}$, because $2|f_{B_0}(\mathfrak{p})$ and therefore $l = \frac{\mathcal{N}(\mathfrak{p})-1}{f_{B_0}(\mathfrak{p})} > x^{\frac{2}{7}-\varepsilon}$.

In the second case above, as $\mathcal{N}(\mathfrak{p}) \leq x$, it follows that

$$x^{\frac{2}{7}-\varepsilon} < \frac{\mathcal{N}(\mathfrak{p}) - 1}{f_{B_0}(\mathfrak{p})} \leq \frac{x - 1}{f_{B_0}(\mathfrak{p})} < \frac{x}{f_{B_0}(\mathfrak{p})}.$$

From this inequality, we easily deduce that $f_{B_0}(\mathfrak{p}) \leq x^{\frac{5}{7}+\varepsilon}$. By the Gupta-Murty bound (Prop. 4.3), as B_0 has three multiplicatively independent elements (Prop. 4.5),

$$\#\{\text{prime ideals } \mathfrak{p} \mid f_{B_0}(\mathfrak{p}) \leq x^{\frac{5}{7}+\varepsilon}\} \ll x^{(\frac{5}{7}+\varepsilon)\cdot\frac{4}{3}}.$$

If we choose $\varepsilon < \frac{1}{28}$, then $x^{(\frac{5}{7}+\varepsilon)\cdot\frac{4}{3}} = o\left(\frac{x}{\log^2(x)}\right)$:

Set $\varepsilon = \frac{1}{28} - \delta$ with $0 < \delta < \frac{1}{28}$, then $0 < \varepsilon < \frac{1}{28}$. We deduce that

$$\begin{aligned} \lim_{x \rightarrow \infty} \frac{x^{(\frac{5}{7}+\varepsilon)\cdot\frac{4}{3}}}{\frac{x}{\log^2(x)}} &= \lim_{x \rightarrow \infty} \frac{x^{(\frac{5}{7}+\frac{1}{28}-\delta)\cdot\frac{4}{3}}}{\frac{x}{\log^2(x)}} = \lim_{x \rightarrow \infty} \frac{x^{(\frac{20}{21}+\frac{4}{84}-\frac{4}{3}\cdot\delta)} \cdot \log^2(x)}{x} \\ &= \lim_{x \rightarrow \infty} \frac{x^{(1-\frac{4}{3}\cdot\delta)} \cdot \log^2(x)}{x} = \lim_{x \rightarrow \infty} \frac{\log^2(x)}{x^{\frac{4}{3}\cdot\delta}} = 0. \end{aligned}$$

Therefore

$$\#\{\text{prime ideals } \mathfrak{p} \mid f_{B_0}(\mathfrak{p}) \leq x^{\frac{5}{7}+\varepsilon}\} = o\left(\frac{x}{\log^2(x)}\right).$$

This implies that

$$\begin{aligned} &\#\{\text{prime ideals } \mathfrak{p} \mid \mathcal{N}(\mathfrak{p}) \leq x, \mathcal{N}(\mathfrak{p}) \equiv 11 \pmod{56}, \frac{\mathcal{N}(\mathfrak{p})-1}{f_{B_0}(\mathfrak{p})} > x^{\frac{2}{7}-\varepsilon}\} \\ &= o\left(\frac{x}{\log^2(x)}\right). \end{aligned}$$

Then

$$\#\{\text{prime ideals } \mathfrak{p} \mid \mathcal{N}(\mathfrak{p}) \leq x \text{ and } f_{B_0}(\mathfrak{p}) = \mathcal{N}(\mathfrak{p}) - 1\} \gg \frac{x}{\log^2(x)}.$$

This follows from

$$\begin{aligned} &\# \{ \mathfrak{p} \text{ prime} \mid \mathcal{N}(\mathfrak{p}) \leq x, \mathcal{N}(\mathfrak{p}) \equiv 11 \pmod{56}, f_{B_0}(\mathfrak{p}) = \mathcal{N}(\mathfrak{p}) - 1 \} \\ &\geq \#\{\mathfrak{p} \text{ prime} \mid \mathcal{N}(\mathfrak{p}) \leq x, \mathcal{N}(\mathfrak{p}) \equiv 11 \pmod{56}, l \mid \frac{\mathcal{N}(\mathfrak{p})-1}{2} \Rightarrow l > x^{\frac{2}{7}-\varepsilon}\} \\ &\quad - \#\{\mathfrak{p} \text{ prime} \mid \mathcal{N}(\mathfrak{p}) \leq x, \mathcal{N}(\mathfrak{p}) \equiv 11 \pmod{56}, \frac{\mathcal{N}(\mathfrak{p})-1}{f_{B_0}(\mathfrak{p})} > x^{\frac{2}{7}-\varepsilon}\} \\ &\gg \frac{x}{\log^2(x)}. \end{aligned}$$

Because $f_{B_0}(\mathfrak{p}) = \mathcal{N}(\mathfrak{p}) - 1$ if and only if $\mathfrak{p} \in \mathcal{B}_1$, we have shown that

$$\#\mathcal{B}_1(x) = \{\mathfrak{p} \text{ prime} \mid \mathcal{N}(\mathfrak{p}) \leq x, \mathfrak{p} \in \mathcal{B}_1\} \gg \frac{x}{\log^2(x)}.$$

By Lemma 4.2 it follows that $\mathbb{Z}[\sqrt{14}]$ is Euclidean.

□

Appendix A

Computer proof

For the proof of Lemma 3.1, a computer program is needed. We first analyse the problem that has to be solved and present an example implementation. The used definitions are the same as in Chapter 3.

A.1 Analysis

The program has to split the square $[0, 1] \times [0, 1]$ into small rectangles. For every rectangle it has to search for two translates $\gamma_1, \gamma_2 \in \mathbb{Z}[\alpha]$ such that:

1. $|N(z + \gamma_i)| < 1$ for all points z in the rectangle, $i \in \{1, 2\}$
2. $\gamma_1 - \gamma_2$ is not divisible by $10 + 3\alpha$

Let us analyse the first point from above. What we actually have to do is to calculate global maxima. If, for a given rectangle R and translate γ , the global maximum of the function $|N(z + \gamma)|$ in the area R is less than 1, then the translate γ is good.

As the calculation of global maxima for functions in several variables is in general a little bit tricky, we will make use of the following proposition:

Proposition A.1. *Let R be a rectangle and $\gamma \in \mathbb{Z}[\alpha]$ a translate. Then the global maximum of the function $|N(z + \gamma)|$, where z is a point from the rectangle, is attained at the border.*

Proof. Let $z = x + y \cdot \alpha$ for rational x, y with $0 \leq x, y < 1$. Then $|N(z)| = |f(x, y)|$, where $f(x, y) = x^2 + xy - 17y^2$. Especially, if $\gamma \in \mathbb{Z}[\alpha]$ is a translate with $\gamma = a + b \cdot \alpha$, then $|N(z + \gamma)| = |f(x + a, y + b)|$.

Let $R \subseteq [0, 1] \times [0, 1]$ be a rectangle. Note that $|N((x + y \cdot \alpha) + \gamma)|$ is actually only defined for rational x, y . But it is clear that if the maximum of $|f(x + a, y + b)|$ in R , where x, y could be real, is less than 1 then also the maximum of $|N((x + y \cdot \alpha) + \gamma)|$, where x, y are restricted to be rational, is less than 1.

Now where is $|f(x + a, y + b)|$ maximal for $(x, y) \in R$?

It is necessary for the partial derivatives (if they exist) to equal 0 to be a maximum that lies inside the rectangle (not at the border). When does this happen:

$$\begin{aligned} |f(x + a, y + b)| &= |(x + a)^2 + (x + a)(y + b) - 17(y + b)^2| \\ &= |x^2 + 2xa + a^2 + xy + xb + ya + ab - 17y^2 - 34yb - 17b^2| \\ &= |x^2 + x(2a + b) + xy - 17y^2 + y(a - 34b) + (a^2 + ab - 17b^2)|. \end{aligned}$$

The partial derivatives of the function are:

- $\frac{\partial}{\partial x}|f(x + a, y + b)| = \text{sgn}(f(x + a, y + b)) \cdot (2x + (2a + b) + y)$
- $\frac{\partial}{\partial y}|f(x + a, y + b)| = \text{sgn}(f(x + a, y + b)) \cdot (-34y + (a - 34b) + x)$

If $\text{sgn}(f(x + a, y + b)) = 0$, then both partial derivatives would be 0 and the function is probably not differentiable there. But we can ignore these points as $|f(x + a, y + b)|$ would be zero and therefore cannot be a global maximum for our function. So let us assume that $\text{sgn}(f(x + a, y + b)) \neq 0$. Then both derivatives equal 0 if

1. $2x + (2a + b) + y = 0$
2. $-34y + (a - 34b) + x = 0$

From the second equation we deduce that $x = 34y - a + 34b$. If we insert this value for x in the first equation, we get $68y - 2a + 68b + (2a + b) + y = 69y + 69b = 0$ and therefore $y = -b$. Therefore $34b + (a - 34b) + x = 0$, which

leads to $x = -a$. As a and b are both integers, this is only possible if (x, y) is a corner point of $[0, 1] \times [0, 1]$.

Therefore, the global maximum is not attained inside the rectangle. That the global maximum exists follows from the fact that $|f(x + a, y + b)|$ is a continuous real function defined on a compact set R . So the global maximum has to be attained at the border.

□

We therefore reduced the problem of finding the global maximum of a 2-variable function to finding the maximum at the border of a rectangle, which is of course just a one-dimensional problem.

Now let us consider the second point from above: when is the difference of two translates not divisible by $10 + 3\alpha$. Here calculation takes place in $\mathbb{Z}[\alpha]$, that is $\gamma \in \mathbb{Z}[\alpha]$ is divisible by $\rho \in \mathbb{Z}[\alpha]$ if there exists $\sigma \in \mathbb{Z}[\alpha]$ such that $\rho \cdot \sigma = \gamma$. We use the notation $\rho|\gamma$ if γ is divisible by ρ in $\mathbb{Z}[\alpha]$.

If $10 + 3\alpha|\gamma$, then also $N(10 + 3\alpha)|N(\gamma)$ (now in \mathbb{Z} !). Therefore, if $N(10 + 3\alpha) \nmid N(\gamma)$ then we are sure that γ is not divisible by $10 + 3\alpha$. That will be the sufficient condition we use in our program:

Proposition A.2. *If $N(10 + 3\alpha) \nmid N(\gamma)$, then $10 + 3\alpha \nmid \gamma$.*

A.2 Implementation

The source code for an example implementation can be found in section A.4. Because speed matters, the program has been implemented in “C++”. If you are not familiar with this language, then the standard reference [20] is highly recommended. As “C++” does not support rational arithmetic out of the box, we used the “GNU MP Bignum Library”¹.

The program has been compiled under GNU/Linux with the “GNU Compiler Collection”².

¹The library and documentation can be found at <http://gmplib.org/>

²The “GNU Compiler Collection” website is <http://gcc.gnu.org/>

The program has to be started with six parameters. The first four parameters ($xmin$, $xmax$, $ymin$, $ymax$) define the rectangle R to be checked. The next parameter (n) defines the size of the translates. The last one (md) sets the maximum recursion depth.

The first five parameters and a sixth parameter called *depth* and initially set to 0 are given to the function **checkrect**. This function searches for two translates γ_1, γ_2 such that

1. $|N(z + \gamma_i)| < 1$ for all points z in the rectangle R , $i \in \{0, 1\}$ (implemented in the function **checkmax**, see Proposition A.1)
2. $\gamma_1 - \gamma_2$ is not divisible by $10 + 3\alpha$ (implemented in the function **checkdiv**, see Proposition A.2).

As we are not able to check all possible translates, we only consider translates $\gamma = a + b \cdot \alpha$ with $|a|, |b| \leq n$. If the program fails to find two translates that fulfill the two points from above, then the rectangle is split into four smaller rectangles and the function **checkrect** is applied to this rectangles again (but now with the *depth* parameter increased by one). Therefore it is a recursive algorithm. Now two things could happen:

1. We are able to find two translates for the rectangle that satisfy the points 1 and 2 from above.
2. The value of *depth* equals md (max depth). This happens if we are not able to find translates and go deeper and deeper in the recursion (that is, the rectangles get smaller and smaller). As we don't want to go down to infinity, it is natural to stop at a given maximum recursion depth. In this case the program goes up to the level $\lfloor \frac{md}{2} \rfloor$ in the recursion and prints the coordinates of this rectangle.

For further details on how the program works, have a look at the source code in section A.4.

A.3 Example session

Here is the output of an example session of our program:

```
xmin = 0
xmax = 1
ymin = 0
ymax = 0.5
n     = 50
md    = 10
No translates: 0.00000000, 0.06250000, 0.00000000, 0.03125000
No translates: 0.93750000, 1.00000000, 0.00000000, 0.03125000
No translates: 0.00000000, 0.06250000, 0.37500000, 0.40625000
No translates: 0.75000000, 0.81250000, 0.34375000, 0.37500000
No translates: 0.81250000, 0.87500000, 0.34375000, 0.37500000
No translates: 0.87500000, 0.93750000, 0.34375000, 0.37500000
No translates: 0.56250000, 0.62500000, 0.37500000, 0.40625000
Bounding box:
xmin = 0.00000000, xmax = 1.00000000
ymin = 0.00000000, ymax = 0.40625000
```

This means that the program succeeded in finding translates except for five connected areas (note that the lines 4-6 of “No translates” above define one connected area). We continue with handling each of this five areas separately. Please note that we increased the parameters n and md to get smaller areas where the program fails to find “good” translates:

1.

```
xmin = 0
xmax = 0.0625
ymin = 0
ymax = 0.03125
n     = 100
md    = 20
No translates: 0.00000000, 0.00012207, 0.00000000, 0.00006104
Bounding box:
xmin = 0.00000000, xmax = 0.00012207
ymin = 0.00000000, ymax = 0.00006104
```
2.

```
xmin = 0.9375
xmax = 1
```

```
ymin = 0
ymax = 0.03125
n     = 100
md    = 20
No translates: 0.99987793, 1.00000000, 0.00000000, 0.00006104
Bounding box:
xmin = 0.99987793, xmax = 1.00000000
ymin = 0.00000000, ymax = 0.00006104
```

3. xmin = 0
xmax = 0.0625
ymin = 0.375
ymax = 0.40625
n = 100
md = 50
Success.

4. xmin = 0.75
xmax = 0.9375
ymin = 0.34375
ymax = 0.375
n = 100
md = 20
No translates: 0.82580566, 0.82617188, 0.34777832, 0.34783936
No translates: 0.82543945, 0.82580566, 0.34783936, 0.34790039
No translates: 0.82580566, 0.82617188, 0.34783936, 0.34790039
No translates: 0.82507324, 0.82543945, 0.34796143, 0.34802246
No translates: 0.82543945, 0.82580566, 0.34790039, 0.34796143
No translates: 0.82434082, 0.82470703, 0.34814453, 0.34820557
No translates: 0.82324219, 0.82360840, 0.34832764, 0.34838867
No translates: 0.82360840, 0.82397461, 0.34832764, 0.34838867
No translates: 0.82617188, 0.82653809, 0.34777832, 0.34783936
No translates: 0.82617188, 0.82653809, 0.34783936, 0.34790039
No translates: 0.82617188, 0.82653809, 0.34790039, 0.34796143
No translates: 0.82653809, 0.82690430, 0.34796143, 0.34802246
No translates: 0.82727051, 0.82763672, 0.34814453, 0.34820557
No translates: 0.82800293, 0.82836914, 0.34832764, 0.34838867
Bounding box:
xmin = 0.82324219, xmax = 0.82836914
ymin = 0.34777832, ymax = 0.34838867

```

5. xmin = 0.5625
   xmax = 0.625
   ymin = 0.375
   ymax = 0.40625
   n     = 100
   md    = 50
Success.

```

If we combine the results of points 1 and 2 from above, we see that the area (modulo \mathbb{Z}^2) is contained in a circle with center point $(0, 0)$ and a radius of $\frac{6}{1000}$. For the areas three and five the program succeeded in finding translates. The fourth area is contained in a circle with center point $(\frac{19}{23}, \frac{8}{23})$ and radius $\frac{6}{1000}$.

Please note that up to this point, we have only checked the points (x, y) with $0 \leq y \leq \frac{1}{2}$. If we consider the transformation $z \mapsto -z$ then we get all the remaining points (x, y) with $\frac{1}{2} \leq y \leq 1$ (modulo \mathbb{Z}^2 , but this is enough). If for a point z there exist $\gamma_1, \gamma_2 \in \mathbb{Z}[\alpha]$ such that $|N(z + \gamma_i)| < 1$, $i \in \{0, 1\}$ and $10 + 3\alpha \nmid \gamma_1 - \gamma_2$ then this is also true for $-z$ - just replace γ_1, γ_2 by $-\gamma_1, -\gamma_2$.

Under this transformation, the areas in the corners $(0, 0)$ and $(1, 0)$ are mirrored to the upper corners $(1, 1)$ and $(0, 1)$. Modulo \mathbb{Z}^2 , they still lie in the circle with center $(0, 0)$ and radius $\frac{6}{1000}$. The point $(\frac{19}{23}, \frac{8}{23})$ is transformed to $(-\frac{19}{23}, -\frac{8}{23})$ which is congruent to $(\frac{4}{23}, \frac{15}{23})$ modulo \mathbb{Z}^2 .

With the help of a computer program we therefore proved the following result:

Proposition A.3. *Let $z \in \mathbb{Q}(\sqrt{69})$ and $z_0 = (0, 0)$, $z_1 = (\frac{19}{23}, \frac{8}{23})$, $z_2 = (\frac{4}{23}, \frac{15}{23})$. If $|z - z_i| > \frac{6}{1000}$ for $i = 0, 1, 2$, then there exists $\gamma_1, \gamma_2 \in \mathbb{Z}[\alpha]$ such that $|N(z + \gamma_1)| < 1$, $|N(z + \gamma_2)| < 1$ and $\gamma_1 - \gamma_2$ is not divisible by $10 + 3\alpha$.*

A.4 Source code

```
#include <iostream>
```



```

#include <gmpxx.h>

using namespace std;

#define MAXTRANS 100

int maxdepth;

long lasta1 = 0, lastb1 = 0, lasta2 = 0, lastb2 = 1;

int bound_init = 0;
mpq_class bound_xmin, bound_xmax, bound_ymin, bound_ymax;

// Calculate the absolute value of the norm of the algebraic number of
// the form  $x+y*(1+\sqrt{69})/2$ .
mpq_class
f (const mpq_class x, const mpq_class y)
{
    return abs(x*x + x*y - 17*y*y);
}

// Check if  $10+3\alpha$  does not divide  $a+b\alpha$  in  $\mathbb{Z}[\alpha]$ .
// It is sufficient to check if the norm of  $10+3\alpha$  does not divide
// the norm of  $a+b\alpha$  in  $\mathbb{Z}$ .
// Return 0 if not divisible, 1 otherwise.
int
checkdiv (const long a, const long b)
{
    mpz_class z(a*a + a*b - 17*b*b);

    if (!mpz_divisible_ui_p (z.get_mpz_t(), 23))
        return 0; // not divisible

    return 1; // divisible
}

```

```

// Check if f(x, y) is < 1 in the given square.
// Returns 1 if it is, 0 otherwise.
int
checkmax (const mpq_class x1, const mpq_class x2, const mpq_class y1,
          const mpq_class y2, long a, long b)
{
    // Check corners
    if (f(x1+a, y1+b) >= 1)
        return 0;

    if (f(x2+a, y1+b) >= 1)
        return 0;

    if (f(x1+a, y2+b) >= 1)
        return 0;

    if (f(x2+a, y2+b) >= 1)
        return 0;

    // Check border
    if ((x1 <= (-2*a-b-y1)/2) && ((-2*a-b-y1)/2 <= x2)) {
        if (f((-b-y1)/2, y1+b) >= 1)
            return 0;
    }

    if ((x1 <= (-2*a-b-y2)/2) && ((-2*a-b-y2)/2 <= x2)) {
        if (f((-b-y2)/2, y2+b) >= 1)
            return 0;
    }

    if ((y1 <= (x1+a-34*b)/34) && ((x1+a-34*b)/34 <= y2)) {
        if (f(x1+a, (x1+a)/34) >= 1)
            return 0;
    }

    if ((y1 <= (x2+a-34*b)/34) && ((x2+a-34*b)/34 <= y2)) {
        if (f(x2+a, (x2+a)/34) >= 1)
            return 0;
    }
}

```

```

    }

    return 1;
}

void
update_bounding (const mpq_class xmin, const mpq_class xmax,
                 const mpq_class ymin, const mpq_class ymax)
{
    if (bound_init) {
        if (xmin < bound_xmin)
            bound_xmin = xmin;

        if (bound_xmax < xmax)
            bound_xmax = xmax;

        bound_ymax = ymax;
    } else {
        bound_xmin = xmin;
        bound_xmax = xmax;
        bound_ymin = ymin;
        bound_ymax = ymax;
        bound_init = 1;
    }
}

int
checkrect (const mpq_class xmin, const mpq_class xmax, const mpq_class ymin,
           const mpq_class ymax, long n, const int depth)
{
    mpq_class xhalf(0), yhalf(0);
    long a, b;
    long transa[MAXTRANS + 1], transb[MAXTRANS + 1];
    long pos = 0, i;

    if (checkmax (xmin, xmax, ymin, ymax, lasta1, lastb1) &&
        checkmax (xmin, xmax, ymin, ymax, lasta2, lastb2))

```

```

return 1;

for (a = 0; a <= n; a = -a) {
  for (b = 0; b <= a || b <= -a; b = -b) {
    if (checkmax (xmin, xmax, ymin, ymax, a, b)) {
      for (i = 0; i < pos; i++) {
        if (!checkdiv (a - transa[i], b - transb[i])) {
          lasta1 = a;
          lastb1 = b;
          lasta2 = transa[i];
          lastb2 = transb[i];

          return 1;
        }
      } // for (i=0)

      // Append current translate to list.
      if (pos < MAXTRANS) {
        transa[pos] = a;
        transb[pos] = b;
        pos++;
      } else {
        cerr << "ERROR: MAXTRANS overflow: " << pos << endl;
        exit(1);
      }
    } // if (checkmax)

    if (b >= 0)
      b++;
  } // for (b)

  if (a >= 0)
    a++;
} // for (a)

if (depth >= maxdepth) {
  return 0;
} else {

```

```

    xhalf = (xmin + xmax) / 2;
    yhalf = (ymin + ymax) / 2;

    n = n + 100;

    if (!checkrect (xmin, xhalf, ymin, yhalf, n, depth + 1) ||
        !checkrect (xhalf, xmax, ymin, yhalf, n, depth + 1) ||
        !checkrect (xmin, xhalf, yhalf, ymax, n, depth + 1) ||
        !checkrect (xhalf, xmax, yhalf, ymax, n, depth + 1)) {
        if (depth >= maxdepth / 2) {
            return 0;
        } else {
            update_bounding (xmin, xmax, ymin, ymax);

            printf("No translates: %.8f, %.8f, %.8f, %.8f\n", xmin.get_d(),
                xmax.get_d(), ymin.get_d(), ymax.get_d());
        }
    }
}

return 1;
}

int
main (int argc, char **argv)
{
    if (argc != 7)
    {
        cout << "Usage: " << argv[0] << " xmin xmax ymin ymax n md" << endl;
        exit(1);
    }

    mpq_class xmin(atoi(argv[1]));
    mpq_class xmax(atoi(argv[2]));
    mpq_class ymin(atoi(argv[3]));
    mpq_class ymax(atoi(argv[4]));
    long n = atol(argv[5]);
    maxdepth = atoi(argv[6]);

```

```

xmin.canonicalize();
xmax.canonicalize();
ymin.canonicalize();
ymax.canonicalize();

cout << "xmin = " << xmin.get_d() << endl;
cout << "xmax = " << xmax.get_d() << endl;
cout << "ymin = " << ymin.get_d() << endl;
cout << "ymax = " << ymax.get_d() << endl;
cout << "n    = " << n << endl;
cout << "md   = " << maxdepth << endl;

checkrect (xmin, xmax, ymin, ymax, n, 0);

if (bound_init) {
    cout << "Bounding box:" << endl;
    printf("xmin = %.8f, xmax = %.8f\n", bound_xmin.get_d(),
          bound_xmax.get_d());
    printf("ymin = %.8f, ymax = %.8f\n", bound_ymin.get_d(),
          bound_ymax.get_d());
} else {
    cout << "Success." << endl;
}

return 0;
}

```

Bibliography

- [1] Ş. Alaca and K. S. Williams, *Introductory Algebraic Number Theory*, Cambridge University Press, Cambridge, 2004.
- [2] E. S. Barnes and H. P. F. Swinnerton-Dyer, *The inhomogeneous minima of binary quadratic forms (I)*, Acta Math. **87** (1952), 259–323.
- [3] H. Chatland and H. Davenport, *Euclid's algorithm in real quadratic fields*, Canad. J. Math. Vol. **2** (1950), 289–296.
- [4] D. A. Clark, *A quadratic field which is euclidean but not norm-euclidean*, manuscripta math. **83** (1994), 327–330.
- [5] D. A. Clark and M. R. Murty, *The Euclidean algorithm for Galois extensions of \mathbb{Q}* , J. Reine Angew. Math. **459** (1995), 151–162.
- [6] L. E. Dickson, *Einführung in die Zahlentheorie*, Teubner Verlag, Leipzig, 1931.
- [7] M. Einsiedler, *Introduction to the Habilitationsschrift: Algebraic methods in higher-dimensional dynamics*, <http://www.mat.univie.ac.at/~manfred/habil.pdf>
- [8] M. Harper, *$\mathbb{Z}[\sqrt{14}]$ is Euclidean*, Canad. J. Math. Vol. **56** (2004), 55–70.
- [9] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil I, Zweite Auflage, Physica-Verlag, Würzburg-Vienna, 1965.

- [10] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) **37** (1986), 27–38.
- [11] E. Hlawka and J. Schoißengeier, *Zahlentheorie. Eine Einführung*, Zweite Auflage, Vorlesungen über Mathematik, Manz Verlag, Wien, 1990.
- [12] K. Inkeri, *Über den Euklidischen Algorithmus in quadratischen Zahlkörpern*, Ann. Acad. Sci. Fennicæ Ser. **A41** (1947), 1–35.
- [13] K. Inkeri, *On the Minkowski constant in the theory of binary quadratic forms*, Ann. Acad. Sci. Fennicæ Ser. **A66** (1950), 1–34.
- [14] E. Landau, *Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes*, Math. Annalen **56** (1903), 645–670.
- [15] Th. Motzkin, *The Euclidean Algorithm*, Bull. Amer. Math. Soc. **55** (1949), 1142–1146.
- [16] W. Narkiewicz, *Euclidean algorithm in small Abelian fields*, Funct. Approx. Comment. Math. **37** (2007), 337–340.
- [17] J. Neukirch, *Algebraische Zahlentheorie*, Springer Verlag, Berlin, 1992.
- [18] P. Samuel, *About Euclidean rings*, J. Algebra **19** (1971), 282–301.
- [19] I. Stewart and D. Tall, *Algebraic Number Theory*, 2nd Edition, Chapman & Hall, 1987.
- [20] B. Stroustrup, *The C++ Programming Language*, Addison-Wesley, 1997.
- [21] P. J. Weinberger, *On Euclidean rings of algebraic integers*, Analytic number theory (Proc. Sympos. Pure Math., Vol. **XXIV**, St. Louis Univ., St. Louis, Mo., 1972), Amer. Math. Soc., Providence, R. I., 1973, pp. 321–332.
- [22] R. J. Wilson, *The large sieve in algebraic number fields*, Mathematika **16** (1969), 189–204.

Curriculum Vitæ

Personal data

Name	Bernhard Lutzmann
Address	Hörmannweg 6, 6800 Feldkirch
Date of birth	September 19th, 1981
Place of birth	Feldkirch

Education

since Oct. 2002	Studies of Mathematics at the University of Vienna, Austria
1996 - 2001	Handelsakademie Feldkirch, Austria

Social Service

2001 - 2002	Paramedic at the Red Cross, Feldkirch
-------------	---------------------------------------

Zusammenfassung

Diese Diplomarbeit befasst sich mit quadratischen Zahlkörpern welche euklidisch aber nicht normeuclidisch sind. Alle normeuclidischen quadratischen Zahlkörper $\mathbb{Q}(\sqrt{d})$ für quadratfreies $d \neq 0, 1$ sind seit 1950 bekannt: Chatland & Davenport [3] und davon unabhängig Inkeri [12] haben gezeigt, dass $\mathbb{Q}(\sqrt{d})$ genau dann normeuclidisch ist, wenn d eine ganze Zahl in

$$\{-1, -2, -3, -7, -11, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$$

ist. Zusätzlich gilt, dass für quadratfreies $d < 0$ der Zahlkörper $\mathbb{Q}(\sqrt{d})$ genau dann euklidisch ist, wenn d eine ganze Zahl in

$$\{-1, -2, -3, -7, -11\}$$

ist. Dies zeigt, dass ein imaginärquadratischer Zahlkörper genau dann euklidisch ist, wenn er normeuclidisch ist. Im reellquadratischen Fall war es jedoch jahrzehntelang unbekannt, ob aus euklidisch automatisch normeuclidisch folgt oder nicht.

In Kapitel 3 präsentieren wir den Beweis von D. A. Clark, dass $\mathbb{Q}(\sqrt{69})$ euklidisch aber nicht normeuclidisch ist (siehe [4]). Dies ist das erste Beispiel für einen quadratischen Zahlkörper mit dieser Eigenschaft. Dabei ist es uns möglich, explizit einen euklidischen Algorithmus anzugeben. Teile des Beweises beruhen auf einem Computerprogramm, für welches der Quellcode in Appendix A enthalten ist.

In Kapitel 4 untersuchen wird den quadratischen Zahlkörper $\mathbb{Q}(\sqrt{14})$. Es wurde lange Zeit vermutet, dass $\mathbb{Q}(\sqrt{14})$ euklidisch ist, da er alle Eigenschaften eines euklidischen Bereiches besitzt (zum Beispiel ist dessen Ganzheitsring ein Hauptidealbereich). Erst 2004 gelang es M. Harper zu beweisen, dass $\mathbb{Q}(\sqrt{14})$ tatsächlich euklidisch ist (siehe [8]). Er konnte sogar zeigen, dass alle reellquadratischen Zahlkörper mit Klassenzahl 1 und Diskrimi-

nante ≤ 500 euklidisch sind. Diesmal ist es uns nicht möglich, einen euklidischen Algorithmus anzugeben. Stattdessen verwenden wir eine Charakterisierung von euklidischen Bereichen und die Hilfe von Siebmethoden in Zahlkörpern.

Kürzlich konnte W. Narkiewicz (in [16]) zeigen, dass alle - mit Ausnahme höchstens zweier - reellquadratischen Zahlkörper mit Klassenzahl 1 euklidisch sind. Bisher sind keine solchen Ausnahmen bekannt. Falls jedoch eine gefunden würde, so wäre dies ein Widerspruch zur *Verallgemeinerten Riemannschen Hypothese*. Dies folgt aus einem Resultat von P. J. Weinberger, der in [21] aus der *Verallgemeinerten Riemannschen Hypothese* folgerte, dass alle reellquadratischen Zahlkörper mit Klassenzahl 1 euklidisch sind.