

Euclidean Windows

Stefania Cavallar
CWI, Kruislaan 413
P.O. Box 94079
1090 GB Amsterdam
The Netherlands
Stefania.Cavallar@cwi.nl

Franz Lemmermeyer
Bilkent University, Department of Mathematics
06800 Bilkent, Ankara, Turkey
franz@fen.bilkent.edu.tr

September 11, 2003

Abstract

In this paper we study number fields which are Euclidean with respect to a function different from the absolute value of the norm. We also show that the Euclidean minimum with respect to weighted norms may be irrational and not isolated.

Introduction

Let R be an integral domain. A function $f : R \rightarrow \mathbb{R}_{\geq 0}$ is called a Euclidean function on R if it satisfies the following conditions with $\kappa = 1$:

- i) $f(R) \cap [0, c]$ is finite for every $c \geq 0$;
- ii) $f(r) = 0$ if and only if $r = 0$;
- iii) for all $a, b \in R$ with $b \neq 0$ there exists a $q \in R$ such that $f(a - bq) < \kappa \cdot f(b)$.

If $f : R \rightarrow \mathbb{R}_{\geq 0}$ is a function satisfying i) and ii), then the infimum of all $\kappa \in \mathbb{R}$ such that iii) holds is called the Euclidean minimum of R with respect to f and will be denoted by $M(R, f)$; thus for all $a, b \in R \setminus \{0\}$ and every $\varepsilon > 0$ there is a $q \in R$ such that $f(a - bq) < M(R, f) \cdot f(b) + \varepsilon$.

If f is a multiplicative function, then we can replace iii) by the equivalent condition that for all $\xi \in K$ (K being the quotient field of R) there is a $q \in R$ such that $f(\xi - q) < \kappa$. The infimum of all $\kappa \in \mathbb{R}$ such that this condition holds for a fixed ξ is denoted by $M(\xi, f)$; clearly $M(R, f)$ is the supremum of the $M(\xi, f)$.

If $R = \mathcal{O}_K$ is the ring of integers in a number field K , then the absolute value of the norm satisfies i) and ii), and $M(K) := M(R, |N|)$ coincides conjecturally with the inhomogeneous minimum of the norm form of \mathcal{O}_K (this conjecture is known to hold for number fields with unit rank at most 1). Let C_1 be the set of representatives modulo \mathcal{O}_K of all $\xi = \frac{a}{b} \in K$ with $M(\xi) = M(K)$ (here $M(\xi) := M(\xi, |N|)$); then we say that $M(K)$ is isolated if there is a $\kappa_2 < \kappa$ such that $M(\xi) \leq \kappa_2$ for all $\xi \in K$ that are not represented by some point in C_1 .

Replacing K in these definitions by $\overline{K} = \mathbb{R}^n$ (this is the topological closure of the image of K under the standard embedding $K \rightarrow \mathbb{R}^n$; for totally real fields we have $\overline{K} = K \otimes_{\mathbb{Q}} \mathbb{R}$), the Euclidean minimum becomes the inhomogeneous minimum of the norm form of K ; we clearly have $M_j(\overline{K}) \geq M_j(K)$ whenever these minima are defined, and it is conjectured that $M_1(\overline{K}) = M_1(K)$ is rational.

The aim of this paper is to explain how the Euclidean minimum of \mathcal{O}_K with respect to “weighted norms” can be computed in some cases; we will show that the Euclidean minimum for certain weighted norms in $\mathbb{Q}(\sqrt{69})$ is irrational and not isolated, thereby showing that these conjectured properties for minima with respect to the usual norm do not carry over to weighted norms.

1 Weighted norms

Let K be a number field, \mathcal{O}_K its ring of integers, and \mathfrak{p} a prime ideal in \mathcal{O}_K . Then, for any real number $c > 0$,

$$\phi : \mathfrak{q} \mapsto \begin{cases} N\mathfrak{q}, & \text{if } \mathfrak{q} \neq \mathfrak{p} \\ c, & \text{if } \mathfrak{q} = \mathfrak{p} \end{cases}$$

defines a map from the set of prime ideals \mathfrak{q} of \mathcal{O}_K into the positive real numbers, which can be uniquely extended to a multiplicative map $\phi : I_K \rightarrow \mathbb{R}_{>0}$ on the group I_K of fractional ideals. Putting $f(\alpha) = \phi(\alpha\mathcal{O}_K)$ for any $\alpha \in K^\times$ and $f(0) = 0$, we get a function $f = f_{\mathfrak{p},c} : K \rightarrow \mathbb{R}_{\geq 0}$ which H. W. Lenstra [12] called a *weighted norm*.

Our aim is to study examples of number fields which are Euclidean with respect to some weighted norm. Lenstra [12] showed that $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_4)$ are such fields, but the first examples that are not norm-Euclidean were given by D. Clark [7, 8].

A formal condition for $f_{\mathfrak{p},c}$ to be a Euclidean function is the finiteness of the sets $\{f_{\mathfrak{p},c}(\alpha) < \lambda : \alpha \in \mathcal{O}_K\}$ for all $\lambda \in \mathbb{R}$. This property is easily seen to be equivalent to $c > 1$.

For weighted norms $f = f_{\mathfrak{p},c}$ on K , we define the *Euclidean window* of \mathfrak{p} by

$$w(\mathfrak{p}) = \{c \in \mathbb{R} : f_{\mathfrak{p},c} \text{ is a Euclidean function on } \mathcal{O}_K\}.$$

Proposition 1.1. *The Euclidean window is a (possibly empty) interval contained in $(1, \infty)$.*

Proof. Assume that $w(\mathfrak{p})$ is not empty, and let $r, t \in w(\mathfrak{p})$ with $r < t$. Then it is sufficient to show that $f_{\mathfrak{p},s}$ is a Euclidean function on \mathcal{O}_K for every $r \leq s \leq t$. Now \mathcal{O}_K is Euclidean with respect to e.g. $f_{\mathfrak{p},r}$, so \mathcal{O}_K is a principal ideal domain, hence every $\xi \in K$ has the form $\xi = \alpha/\beta$ with $(\alpha, \beta) = 1$. Moreover, there exist $\gamma_r, \gamma_t \in \mathcal{O}_K$ such that

$$f_{\mathfrak{p},r}(\alpha - \beta\gamma_r) < f_{\mathfrak{p},r}(\beta), \quad f_{\mathfrak{p},t}(\alpha - \beta\gamma_t) < f_{\mathfrak{p},t}(\beta).$$

If $\mathfrak{p} \nmid \beta$, then $f_{\mathfrak{p},s}(\alpha - \beta\gamma_t) \leq f_{\mathfrak{p},t}(\alpha - \beta\gamma_t) < f_{\mathfrak{p},t}(\beta) = f_{\mathfrak{p},s}(\beta)$; if $\mathfrak{p} \mid \beta$, on the other hand, then $\mathfrak{p} \nmid \alpha$, hence $\mathfrak{p} \nmid (\alpha - \beta\gamma_r)$, and $f_{\mathfrak{p},s}(\alpha - \beta\gamma_r) = f_{\mathfrak{p},r}(\alpha - \beta\gamma_r) < f_{\mathfrak{p},r}(\beta) \leq f_{\mathfrak{p},s}(\beta)$. Thus $f_{\mathfrak{p},s}$ is indeed a Euclidean function on \mathcal{O}_K . \square

In this paper, we investigate Euclidean windows for various algorithms in some quadratic and cubic number fields; we will give examples of empty, finite and infinite Euclidean windows, and we show that the first minima with respect to weighted norms need not be rational.

2 Weighted norms in \mathbb{Z}

The Euclidean window for primes in \mathbb{Z} can easily be determined:

Proposition 2.1. *The Euclidean minimum $M(f_{p,c})$ of a weighted norm in \mathbb{Z} is given by*

$$M(f_{p,c}) = \begin{cases} \infty & \text{if } c < p \\ \frac{1}{2} & \text{if } c = p \\ 1 & \text{if } c > p \end{cases}.$$

Moreover, $w(p) = [p, \infty)$.

Proof. We first show that $M(f_{p,c}) = \infty$ if $c < p$ (this implies that $w(\mathfrak{p}) \subseteq [p, \infty)$). To this end, put $b = p^n$ and

$$a = \begin{cases} \frac{1}{2}(p^n - 1) & \text{if } p \neq 2, \\ 2^{n-1} - 1 & \text{if } p = 2. \end{cases}$$

Then $p \nmid (a - bq)$, hence $f_{p,c}(a - bq) = |a - bq|$ for all $q \in \mathbb{Z}$. If the minimum $\kappa = M(f_{p,c})$ were finite, there would exist a $q \in \mathbb{Z}$ such that $f_{p,c}(a - bq) < \kappa f_{p,c}(b) = \kappa c^n$. But clearly $|a| \leq |a - bq| = f_{p,c}(a - bq)$, hence we get $|a|c^{-n} < \kappa$ for all $n \in \mathbb{N}$: but since $c < p$, the expression on the left hand side tends to ∞ with n .

Since it is well known that $M(f_{p,p}) = \frac{1}{2}$, we next show that $M(f_{p,c}) = 1$ if $c > p$. To this end, choose $\alpha, \beta \in \mathbb{N}$ not divisible by p such that $p < \frac{\alpha}{\beta} < c$. If we put $a = p^n \beta^n$ and $b = \alpha^n + p^n \beta^n$, then we get

$$\begin{aligned} f_{p,c}\left(\frac{a}{b}\right) &= \frac{c^n \beta^n}{\alpha^n + p^n \beta^n} = \frac{c^n}{(\alpha/\beta)^n + p^n} > \frac{c^n}{c^n + p^n}, \\ f_{p,c}\left(\frac{a}{b} - 1\right) &= \frac{\alpha^n}{\alpha^n + p^n \beta^n}, \end{aligned}$$

and both expressions tend to 1 as n goes to ∞ . Note also that $f_{p,c}(\frac{a}{b} - q) \geq |\frac{a}{b} - q| > 1$ for all $q \in \mathbb{N} \setminus \{0, 1\}$, since the denominator of $\frac{a}{b} - q$ is prime to p and since $c > p$.

Thus $M(f_{p,c}) \geq 1$ if $c > p$; but we can easily show that $M(f_{p,c}) \leq 1$ by proving that $f_{p,c}$ is a Euclidean function for all $p \geq c$. In fact, suppose that $a, b \in \mathbb{Z} \setminus \{0\}$ are given, and that they are relatively prime. If $p \mid b$, then $p \nmid (a - bq)$ for all $q \in \mathbb{Z}$, hence $f_{p,c}(a - bq) = |a - bq|$, and we can certainly find $q \in \mathbb{Z}$ such that $|a - bq| < |b|$. But $|b| \leq f_{p,c}(b)$ since $c \geq p$.

Now consider the case $p \nmid b$; then we choose $q \in \mathbb{Z}$ such that $|a - bq|, |a - b(q+1)| \leq b$. But $r = a - bq$ and $r' = a - b(q+1)$ cannot both be divisible by p ; if $p \nmid r$, then $f_{p,c}(r) = |r| < |b| = f_{p,c}(b)$, and if $p \nmid r'$, then $f_{p,c}(r') < f_{p,c}(b)$. \square

3 Weighted norms in $\mathbb{Q}(\sqrt{14})$

Since it is well known that an imaginary quadratic number field is Euclidean if and only if it is norm-Euclidean, only the case of real quadratic fields is interesting. We will deal with only two examples here: one is $\mathbb{Q}(\sqrt{14})$, which has been studied often in this respect (cf. Bedocchi [2], Nagata [13, 14] and Cardon [3]), and the other is $\mathbb{Q}(\sqrt{69})$, which was shown to be Euclidean with respect to a weighted norm by Clark [7] (see also Niklasch [15] and Hainke [10]).

Consider the quadratic number field $K = \mathbb{Q}(\sqrt{14})$. It is well known that $M_1(K) = \frac{5}{4}$ and $M_2(K) = \frac{31}{32}$ (cf. [11]); moreover M_1 is attained exactly at the points $\xi \equiv \frac{1}{2}(1 + \sqrt{14}) \pmod{\mathcal{O}_K}$. Now we claim

Proposition 3.1. *For $K = \mathbb{Q}(\sqrt{14})$ and $\mathfrak{p} = (2, \sqrt{14})$ we have $w(\mathfrak{p}) \subseteq (\sqrt{5}, \sqrt{7})$.*

Proof. Put $\alpha = 1 + \sqrt{14}$, $\beta = 2$. Then $|N(\alpha - \beta\gamma)|$ is an odd integer ≥ 5 for all $\gamma \in \mathcal{O}_K$. Thus $f_{\mathfrak{p},c}(\alpha - \beta\gamma) = |N(\alpha - \beta\gamma)| \geq 5$, and if $f_{\mathfrak{p},c}$ is a Euclidean function, we must have $5 < f_{\mathfrak{p},c}(\beta) = c^2$. This shows that $c > \sqrt{5}$.

In order to show that $c < \sqrt{7}$ we look at the ideal $\mathfrak{q} = (7, \sqrt{14}) = (7 + 2\sqrt{14})$ of norm 7. If $f_{\mathfrak{p},c}$ is Euclidean, then every residue class modulo \mathfrak{q} must contain an element α such that $f_{\mathfrak{p},c}(\alpha) < f_{\mathfrak{p},c}(\mathfrak{q}) = 7$. Since the unit group generates the subgroup $\{-1, +1\}$ of $(\mathcal{O}_K/\mathfrak{q})^\times$ (and $f_{\mathfrak{p},c}(\pm 1) = 1$), and since $\pm 3 + \sqrt{14} \equiv \pm 3 \pmod{\mathfrak{q}}$ (where $f_{\mathfrak{p},c}(\pm 3 + \sqrt{14}) = |N(\pm 3 + \sqrt{14})| = 5$), we must find elements in the residue classes $\pm 2 \pmod{\mathfrak{q}}$. The only possible candidates are powers of $4 + \sqrt{14}$, because the only ideals of odd norm < 7 are (0) ,

(1), and $(3 \pm \sqrt{14})$, none of which yields elements $\equiv \pm 2 \pmod{\mathfrak{q}}$. Moreover, $\pm 4 + \sqrt{14} \equiv \pm 3 \pmod{\mathfrak{q}}$, and we see that if there exist elements $\alpha \equiv 2 \pmod{\mathfrak{q}}$ with $f_{\mathfrak{p},c}(\alpha) < 7$, then $\alpha = 2$ is one of them. But $f_{\mathfrak{p},c}(2) = c^2$, and we find $c < \sqrt{7}$. \square

We remark that it is not known whether $w(\mathfrak{p})$ is empty or not.

If we look at prime ideals other than $(2, \sqrt{14})$, the situation is quite different:

Proposition 3.2. *Let $K = \mathbb{Q}(\sqrt{14})$, and let \mathfrak{p} be a prime ideal in \mathcal{O}_K of norm $N\mathfrak{p} \equiv \pm 1 \pmod{8}$. Then $w(\mathfrak{p}) = \emptyset$.*

Proof. Assume that $f_{\mathfrak{p},c}$ is a Euclidean function. Then there exists an $\alpha = x + y\sqrt{14} \equiv 1 + \sqrt{14} \pmod{2}$ such that $f_{\mathfrak{p},c}(\alpha) < f_{\mathfrak{p},c}(2) = 4$. Since α cannot be a unit, this is only possible if α is divisible by \mathfrak{p} . If α is divisible by some other prime ideal \mathfrak{q} , then $f_{\mathfrak{p},c}(\mathfrak{q}) = N\mathfrak{q} \geq 5$, and we conclude $f_{\mathfrak{p},c}(\mathfrak{p}) < 1$: contradiction. Thus $(\alpha) = \mathfrak{p}^m$ for some $m \geq 1$. But $\mathfrak{p} = (a + b\sqrt{14})$ since K has class number 1, and b must be even since $\pm p = a^2 - 14b^2 \equiv \pm 1 \pmod{8}$: thus $a + b\sqrt{14} \not\equiv 1 + \sqrt{14} \pmod{2}$, and again we have a contradiction. \square

4 The Euclidean Algorithm in $\mathbb{Q}(\sqrt{69})$

Next we study the field $\mathbb{Q}(\sqrt{69})$; we will prove the following result that corrects a claim¹ announced without proof in [11]:

Theorem 4.1. *In $K = \mathbb{Q}(\sqrt{69})$, we have*

$$\begin{aligned} M_1 &= \frac{25}{23}, & C_1 &= \{ \pm \frac{4}{23}\sqrt{69} \}, \\ M_2 &= \frac{1}{46} (165 - 15\sqrt{69}), & C_2 &= \{ (\pm P_r, \pm P'_r) \}, r \geq 0 \end{aligned}$$

where

$$P_r = \frac{1}{2}\varepsilon^{-r} + \left(\frac{4}{23} + \frac{1}{2\sqrt{69}}\varepsilon^{-r} \right) \sqrt{69}, \quad P'_r = \frac{1}{2}\varepsilon^{-r} - \left(\frac{4}{23} + \frac{1}{2\sqrt{69}}\varepsilon^{-r} \right) \sqrt{69}.$$

Here M_j denotes the j -th inhomogeneous minimum of the norm form of \mathcal{O}_K , C_j is a set of representatives modulo \mathcal{O}_K of the points where M_j is attained, and $\varepsilon = \frac{1}{2}(25 + 3\sqrt{69})$ is the fundamental unit of K . The second minimum $M_2(K) = M_2(\overline{K})$ is not isolated.

The proof of Theorem 4.1 is based on methods developed by Barnes and Swinnerton-Dyer [1]. In the following, we will regard K as a subset of \mathbb{R}^2 via the embedding $x + y\sqrt{69} \rightarrow (x, y)$. Conversely, any point $P = (x, y) \in \mathbb{R}^2 = \overline{K}$ corresponds to a pair $\xi_P = x + y\sqrt{69}$, $\xi'_P = x - y\sqrt{69}$. These elements are not necessarily in K ; nevertheless we call $\xi'_P = x - y\sqrt{69}$ the conjugate of ξ_P . Note that e.g. $\xi_P = \sqrt{69}$ alone does not determine P , since both $P = (0, 1)$

¹namely that $M_2(K) < M_2(\overline{K})$, and that $M_2(\overline{K})$ is isolated.

and $P = (\sqrt{69}, 0)$ correspond to such a ξ_P . The “ \overline{K} -valuations” $|\cdot|_1$ and $|\cdot|_2$ are defined by $|(x, y)|_1 = |x + y\sqrt{69}|$ and $|(x, y)|_2 = |x - y\sqrt{69}|$, with a positive square root of 69.

Using the technique described in [6], it is easy to cover the whole fundamental domain of the lattice \mathcal{O}_K with a bound of $k = 0.875$ except for $\pm S_0 \cup \pm S_1 \cup \pm S_2 \cup \pm T$, where

$$\begin{aligned} S_0 &= [-0.00085, 0.00085] \times [0.1739, 0.1742] \\ S_1 &= [0.01917, 0.02005] \times [0.1763, 0.1765] \\ S_2 &= [-0.02005, -0.01917] \times [0.1763, 0.1765] \\ T &= [0.4999, 0.5001] \times [0.2341, 0.2342]. \end{aligned}$$

Transforming these exceptional sets by multiplication with the units ε and $\bar{\varepsilon} = \frac{1}{2}(25 - 3\sqrt{69})$ we find e.g.

$$\varepsilon S_0 \subset 18 + 2\sqrt{69} + [-0.012, 0.041] \times [0.172, 0.179],$$

that is, $\varepsilon S_0 - (18 + 2\sqrt{69})$ is contained in covered regions or $S_0 \cup S_1$, which we will denote by $\varepsilon S_0 - (18 + 2\sqrt{69}) \tilde{\subset} S_0 \cup S_1$. Similar calculations show that

$$\begin{aligned} \varepsilon S_0 - (18 + 2\sqrt{69}) &\tilde{\subset} S_0 \cup S_1, & \bar{\varepsilon} S_0 + (18 - 2\sqrt{69}) &\tilde{\subset} S_0 \cup S_2, \\ \varepsilon S_1 - (18 + 2\sqrt{69}) &\tilde{\subset} T, & \bar{\varepsilon} S_1 + (18 - 2\sqrt{69}) &\tilde{\subset} S_0 \cup S_2, \\ \varepsilon S_2 - (18 + 2\sqrt{69}) &\tilde{\subset} S_0 \cup S_1, & \bar{\varepsilon} S_2 + (19 - 2\sqrt{69}) &\tilde{\subset} T, \\ \varepsilon T - \frac{1}{2}(61 + 7\sqrt{69}) &\tilde{\subset} S_2, & \bar{\varepsilon} T + (18 - 2\sqrt{69}) &\tilde{\subset} S_1. \end{aligned}$$

Remark. The inclusions on the right hand side can be computed from those on the left: for example, all exceptional points in S_2 must come from T , so the exceptional points in $\varepsilon^{-1}S_2$ must be congruent modulo \mathcal{O}_K to points in T , and since $\frac{1}{2}(61 + 7\sqrt{69})\varepsilon^{-1} = 19 - 2\sqrt{69}$, we conclude that $\bar{\varepsilon}S_2 + (19 - 2\sqrt{69}) \tilde{\subset} T$.

We will need the following result (this is Prop. 2 of [6]):

Proposition 4.2. *Let K be a number field and ε a non-torsion unit of E_K . Suppose that $S \subset \tilde{F}$ has the following property:*

There exists a unique $\theta \in \mathcal{O}_K$ such that, for all $\xi \in S$, the element $\varepsilon\xi - \theta$ lies in a k -covered region of \tilde{F} or again in S .

Then every k -exceptional point $\xi_0 \in S$ satisfies $|\xi_0 - \frac{\theta}{\varepsilon-1}|_j = 0$ for every \overline{K} -valuation $|\cdot|_j$ such that $|\varepsilon|_j > 1$.

We also need a method to compute Euclidean minima of given points. Recall that the orbit of $\xi \in \overline{K}$ is the set $\text{Orb}(\xi) = \{\varepsilon\xi : \varepsilon \in E_K\}$, where E_K is the unit group of \mathcal{O}_K . Note that all the elements in an orbit have the same minimum.

Proposition 4.3. *Let $m \in \mathbb{N}$ be squarefree, $K = \mathbb{Q}(\sqrt{m})$ a real quadratic number field, $\varepsilon > 1$ a unit in \mathcal{O}_K , and $\xi \in \overline{K}$. If $M(K, \xi) < k$ for some real k , then there exists an element $\eta = r + s\sqrt{m} \in K$ with the following properties:*

- i) $\eta \equiv \xi_j \pmod{\mathcal{O}_K}$ for some $\xi_j \in \text{Orb}(\xi)$;
- ii) $|N\eta| < k$;
- iii) $|r| < \mu$, $|s| < \frac{\mu}{\sqrt{m}}$, where $\mu = \frac{\sqrt{k}}{2} \left(\sqrt{\varepsilon} + \frac{1}{\sqrt{\varepsilon}} \right)$.

Proof. Assume that $M(K, \xi) < k$; then there is an $\alpha \in \mathcal{O}_K$ such that $|N(\xi - \alpha)| < k$. Choose $m \in \mathbb{Z}$ such that $\sqrt{k/\varepsilon} \leq |(\xi - \alpha)\varepsilon^m| < \sqrt{k\varepsilon}$ and put $\eta = (\xi - \alpha)\varepsilon^m$. Then

- i) $\eta = (\xi - \alpha)\varepsilon^m \equiv \xi\varepsilon^m \pmod{\mathcal{O}_K}$, and clearly $\xi\varepsilon^m \in \text{Orb}(\xi)$;
- ii) $|N\eta| = |N(\xi - \alpha)| < k$;
- iii) Write $\eta = r + s\sqrt{m}$ and $\eta' = r - s\sqrt{m}$. Then $|\eta| < \sqrt{k\varepsilon}$ and $|\eta'| = |\eta\eta'|/|\eta| < k/|\eta| \leq \sqrt{k\varepsilon}$. Thus $2|r| = |\eta + \eta'| \leq |\eta| + |\eta'|$ and $2|s|\sqrt{m} = |\eta - \eta'| \leq |\eta| + |\eta'|$. Using the lemma below, this yields the desired bounds.

This concludes the proof. \square

Lemma 4.4. *If x, y are positive real numbers such that $x < a$, $y < a$ and $xy < b$, then $x + y < a + \frac{b}{a}$.*

Proof. $0 < (a - x)(a - y) = a^2 - a(x + y) + xy < a^2 - a(x + y) + b$. \square

Now we are ready to determine a certain class of exceptional points inside S_0 :

Claim 4.1. *If P is an exceptional point in S_0 that stays inside S_0 under repeated applications of the maps*

$$\alpha : \xi \longmapsto \varepsilon^{-1}\xi + 18 - 2\sqrt{69} \quad (1)$$

$$\beta : \xi \longmapsto \varepsilon\xi - (18 + 2\sqrt{69}) \quad (2)$$

then $P = \frac{18+2\sqrt{69}}{\varepsilon-1} = (0, \frac{4}{23})$. Moreover, $M(P) = \frac{25}{23}$.

This follows directly from Proposition 4.2; the Euclidean minimum $M(P) = \frac{25}{23}$ is easily computed using Proposition 4.3. Any exceptional point that does not stay inside S_0 must eventually come through T ; it is therefore sufficient to consider exceptional points in T from now on.

Let $P_0 \in T$ be such an exceptional point and define the series of points P_0, P_1, P_2, \dots recursively by $P_{j+1} = \alpha(P_j)$. Then $P_1 \in S_1$, and now there are two possibilities:

- (A) $P_j \in S_0$ for all $j \geq 2$;
- (B) there is an $n \geq 2$ such that $P_n \in S_1$.

Before we can go in the other direction we have to adjust P_0 somewhat. In fact, $\beta(P_0) \in T$ implies that $\beta(P_0) - \varepsilon \tilde{c} S_2$; thus we can define a sequence of points $P_0 - 1, P_{-1}, P_{-2}, \dots$ by $P_{-1} = \beta(P_0 - 1)$ and $P_{-j-1} = \beta(P_{-j})$ for $j \geq 1$. Again, there are two possibilities:

(C) $P_{-j} \in S_0$ for all $j \geq 2$;

(D) there is an $n \geq 2$ such that $P_{-n} \in S_1$.

Claim 4.2. If $P_0 \in T$ is an exceptional point satisfying conditions (A) and (C), then $P_0 = (\frac{1}{2}, \frac{4}{23} + \frac{1}{2\sqrt{69}}) \approx (0.5, 0.234105)$.

Note that this point is not contained in K . Of course we knew this before: every point in K has a finite orbit, whereas P_0 does not.

For a proof, we apply Proposition 4.2 to the set $S = \{P_0, P_1, P_2, \dots\}$; this shows that any $\xi = P_j$ lies on the line $|\xi + \frac{18-2\sqrt{69}}{\varepsilon-1}|_2 = 0$ (the \overline{K} -valuation $|\cdot|_2$ chosen so that $|\varepsilon|_2 > 1$), that is, $\xi' = -\frac{4}{23}\sqrt{69}$. Applying the same proposition to $S = \{P_0 - 1, P_{-1}, P_{-2}, \dots\}$ gives $|\xi - \frac{18+2\sqrt{69}}{\varepsilon-1}|_1 = 0$, with $\frac{18+2\sqrt{69}}{\varepsilon-1} = \frac{4}{23}\sqrt{69}$, hence such $P_0 = (x, y)$ satisfy $x + y\sqrt{69} = 1 + \frac{4}{23}\sqrt{69}$.

Thus any point $\xi = P_0$ giving rise to a doubly infinite sequence $(P_j)_{j \in \mathbb{Z}}$ that stays inside S_0 modulo \mathcal{O}_K for all $j \neq 0, \pm 1$ satisfies $\xi = 1 + \frac{4}{23}\sqrt{69}$ and $\xi' = -\frac{4}{23}\sqrt{69}$. If we write $P_0 = (x, y)$, then this gives $x = \frac{1}{2}(\xi + \xi') = \frac{1}{2}$ and $y = \frac{1}{2\sqrt{69}}(\xi - \xi') = \frac{4}{23} + \frac{1}{2\sqrt{69}} \approx 0.2341059$ as claimed.

Before we go on exploring the other possibilities, we study the orbit of P_0 and compute its Euclidean minimum.

Claim 4.3. The points $P_r \equiv \varepsilon^{-r}P_0 \pmod{\mathcal{O}_K}$ in the orbit of P_0 coincide with the P_r given in Theorem 4.1.

This is done by induction: the case $r = 0$ is clear. For the induction step, notice that $\varepsilon^{-1}(x, y) = (\frac{25}{2}x - \frac{207}{4}y, \frac{25}{2}y - \frac{3}{2}x)$; now

$$\begin{aligned} \varepsilon^{-1}P_r &= \left(\frac{25}{4}\varepsilon^{-r} - 18 - \frac{207}{2\sqrt{69}}\varepsilon^{-r}, \frac{50}{23} + \frac{25}{4\sqrt{69}}\varepsilon^{-r} - \frac{3}{4}\varepsilon^{-r} \right) \\ &= (-18, 2) + \left(\left(\frac{25}{4} - \frac{3}{4}\sqrt{69} \right)\varepsilon^{-r}, \frac{4}{23} + \left(-\frac{3}{4} + \frac{25}{4\sqrt{69}} \right)\varepsilon^{-r} \right) \\ &= (-18, 2) + \left(\frac{1}{2}\varepsilon^{-r-1}, \frac{4}{23} + \frac{1}{2\sqrt{69}}\varepsilon^{-r-1} \right) \equiv P_{r+1} \pmod{\mathcal{O}_K} \end{aligned}$$

Next one computes that $\varepsilon P_0 = (\frac{61}{2}, \frac{7}{2}) - P'_1$ and shows, again by induction, that $\varepsilon^r P_0 \equiv -P'_r \pmod{\mathcal{O}_K}$ for all $r \geq 0$. Thus the orbit of P_0 under the action of the unit group E_K of \mathcal{O}_K is represented modulo \mathcal{O}_K by the points $\{\pm P_r, \pm P'_r : r \geq 0\}$.

Claim 4.4. The points P_r have Euclidean minimum

$$M(K, P_r) = M(K, P_0) = \frac{1}{46}(165 - 15\sqrt{69}).$$

First we observe that the points P_r have the same Euclidean minimum since they all belong to the same orbit. Now assume that $\varepsilon = t + u\sqrt{m}$ has positive norm. We want to apply Proposition 4.3 and find $\varepsilon^{-1} = t - u\sqrt{m}$, hence $(\sqrt{\varepsilon} + \frac{1}{\sqrt{\varepsilon}})^2 = 2t + 2$ and $\mu = \sqrt{k(t+1)/2}$. In the case $m = 69$, we have $t = \frac{25}{2}$, hence $\mu/\sqrt{m} = \sqrt{k}\sqrt{27/276} < \frac{1}{3}\sqrt{k}$.

The orbit of $P_0 = \frac{1}{2} + (\frac{4}{23} + \frac{1}{2\sqrt{69}})\sqrt{69}$ is $\{\pm P_r, \pm P'_r : r \in \mathbb{N}_0\}$, so it is clearly sufficient to compute $M(K, P_r)$ for $r \geq 0$. We start with P_0 itself. The only $\eta \equiv P_0 \pmod{\mathcal{O}_K}$ satisfying the bounds of Proposition 4.3 have the form $P_0 + a$ for some $a \in \mathbb{Z}$ or $P_0 - \frac{b+\sqrt{69}}{2}$ for some odd $b \in \mathbb{Z}$. The minimal absolute value of the norm of these elements is $|N(\eta - \frac{5+\sqrt{69}}{2})| = \frac{1}{46}(165 - 15\sqrt{69})$.

Similarly, the minimal norm for the $\eta \equiv P_1 \pmod{\mathcal{O}_K}$ is attained at $P_1 + \frac{5-\sqrt{69}}{2}$ and again equals $\frac{1}{46}(165 - 15\sqrt{69})$.

Finally, consider the $\eta \equiv P_r \pmod{\mathcal{O}_K}$ for some $r \geq 2$. Then $P_r = x_r + y_r\sqrt{69}$ with $|x_r| \leq 0.00081 =: \delta_0$ and $|y_r - \frac{4}{23}| < 0.0001 =: \delta_1$. The minimal absolute value of the norm of $P_r + a$ for some $a \in \mathbb{Z}$ is attained for $a = 1$, and equals $|(1+\delta_0)^2 - 69(\frac{4}{23} - \delta_1)^2| \geq 1.07$; similarly, we find that $|N(P_r - \frac{b+\sqrt{69}}{2})| \geq 1.07$.

Thus we have seen that $\inf \{|N(P_r - \alpha)| : \alpha \in \mathcal{O}_K, r \in \mathbb{Z}\}$ is attained for $r = 0$ and $\alpha = \frac{5+\sqrt{69}}{2}$, giving $M(K, P_0) = \frac{1}{46}(165 - 15\sqrt{69})$ as claimed.

Before we go on, let us recall what we know by now: $K = \mathbb{Q}(\sqrt{69})$ has first minimum $M_1(K) = \frac{25}{23}$, and M_1 is isolated. Moreover, the orbit of every k -exceptional point for $k = 0.875$ not congruent to $\pm \frac{4}{23}\sqrt{69} \pmod{\mathcal{O}_K}$ has a representative in the exceptional set T . Finally, if the orbit of such a point visits T exactly once, then the point is $P_0 = \frac{1}{2} + (\frac{4}{23} + \frac{1}{2\sqrt{69}})\sqrt{69}$, and its minimum is $M(K, P_0) = \frac{1}{46}(165 - 15\sqrt{69})$.

Claim 4.5. Any exceptional point $Q \neq P_0$ in T has Euclidean minimum $M(K, Q) < M(K, P_0) = \frac{1}{46}(165 - 15\sqrt{69})$, and $M_2(K) = M(P_0)$ is attained only at points in the orbit of P_0 .

In fact, let $Q_0 \neq P_0$ be an exceptional point in T and consider the orbit $\{Q_r : r \in \mathbb{Z}\}$ of Q_0 , where the Q_j are defined by $Q_j \equiv \varepsilon^{-j}Q_0 \pmod{\mathcal{O}_K}$. Since $Q_0 \neq P_0$, we know that we are in one of the following situations:

1. (A) and (D) hold;
2. (B) and (C) hold;
3. (B) and (D) hold.

In each case, there exists a point $Q \neq P_0$ in T whose orbit moves into T both to the right and to the left:

$$\dots T \longrightarrow S_2 \longrightarrow S_0 \cdots S_0 \longrightarrow S_1 \longrightarrow Q \longrightarrow S_2 \longrightarrow S_0 \cdots S_0 \longrightarrow S_1 \longrightarrow T \dots \quad (3)$$

Now we prove the following lemma:

Lemma 4.5. *Suppose there is a $Q_0 \in T$ such that $Q_1 = \beta(Q_0 - 1) \in S_2$ and $Q_{m+1} = (x, y) = \beta^m(Q_1) \in S_1$ with β as in (2). Then $x - y\sqrt{69} < -\frac{4}{23}\sqrt{69}$.*

Proof. Write $Q_n = (x_n, y_n)$ and put $\xi'_n = x_n - y_n\sqrt{69}$. Then $\xi'_1 \approx -1.48 < -\frac{4}{23}\sqrt{69}$; now we use induction to show that $\xi'_n < -\frac{4}{23}\sqrt{69}$ for $1 \leq n \leq m$. In fact, if $Q_{n+1} = \beta(x_n, y_n)$, then $\xi'_{n+1} = (\varepsilon\xi_n - (18 + 2\sqrt{69}))' = \varepsilon'\xi'_n - 18 + 2\sqrt{69} < -\varepsilon'\frac{4}{23}\sqrt{69} - 18 + 2\sqrt{69} = -\frac{4}{23}\sqrt{69}$. \square

A similar result holds for the other direction:

Lemma 4.6. *Suppose there is a $Q_0 \in T$ such that $Q_{-1} = \alpha(Q_0) \in S_1$ and $Q_{-m-1} = (x, y) = \alpha^m(Q_{-1}) \in S_2$. Then $x + y\sqrt{69} > 1 + \frac{4}{23}\sqrt{69}$.*

Proof. Similar. □

This shows that, in (3), we have $\xi > \xi_0 = 1 + \frac{4}{23}\sqrt{69}$ and $\xi' < \xi'_0 = -\frac{4}{23}\sqrt{69}$ for the point $Q = (x, y)$ and $\xi = x + y\sqrt{69}$, $\xi' = x - y\sqrt{69}$.

Put $\alpha = \xi_0 - \frac{5+\sqrt{69}}{2}$ and $\alpha' = \xi'_0 - \frac{5-\sqrt{69}}{2}$. Then $-\alpha\alpha' = \frac{1}{46}(165 - 15\sqrt{69})$, and, since $\alpha < 0$ and $\alpha' > 0$, $0 < (\xi - \frac{5+\sqrt{69}}{2})(\xi' - \frac{5-\sqrt{69}}{2}) < -\alpha\alpha'$. Thus any such point has Euclidean minimum strictly smaller than $\frac{1}{46}(165 - 15\sqrt{69})$.

Claim 4.6. The second minimum $M_2(K)$ is not isolated.

This is accomplished by constructing a series of rational points $Q_r \in K \setminus C_2$ such that $\lim_{r \rightarrow \infty} M(Q_r) = M_2(K)$. To this end, we look for a point $Q_r \in T - 1$ that gets mapped (multiplication by ε plus reduction modulo \mathcal{O}_K) to S_2 , stays in S_0 exactly r times, and then goes to S_1 and back to the point in T congruent to $Q_r \pmod{\mathcal{O}_K}$, then Q_r will satisfy the following equation:²

$$\varepsilon^{r+4}Q_r = \varepsilon^{r+4} + (\varepsilon^{r+3} + \dots + \varepsilon + 1)(18 + 2\sqrt{69}) + Q_r.$$

This gives

$$Q_r = 1 + \frac{4}{23}\sqrt{69} + \frac{1}{\varepsilon^{r+4} - 1}.$$

Here's a short table with explicit coordinates for small values of r :

r	Q_r	$M(Q_r)$
-1	$\frac{1}{2} + \frac{97}{414}\sqrt{69}$	$\frac{541}{621} \approx 0.871175523$
0	$\frac{1}{2} + \frac{70}{299}\sqrt{69}$	$\frac{13651}{15548} \approx 0.877990738$
1	$\frac{1}{2} + \frac{2423}{10350}\sqrt{69}$	$\frac{340876}{388125} \approx 0.878263446$
2	$\frac{1}{2} + \frac{6989}{29854}\sqrt{69}$	$\frac{8508391}{9687623} \approx 0.878274371$
3	$\frac{1}{2} + \frac{30239}{129168}\sqrt{69}$	$\frac{212369041}{241802496} \approx 0.878274809$
4	$\frac{1}{2} + \frac{174445}{745154}\sqrt{69}$	$\frac{5300717776}{6035374823} \approx 0.878274826$

We claim that $M(Q_r)$ tends to $M_2(K) = \frac{1}{46}(165 - 15\sqrt{69}) \approx 0.87827$ as $r \rightarrow \infty$. Applying Proposition 4.3 shows that, for given $r \geq 0$, the Euclidean minimum of Q_r is attained at $Q_r - \frac{5+\sqrt{69}}{2}$. Writing $n = r+4$ and $Q_r - \frac{5+\sqrt{69}}{2} = (\xi, \xi')$ we have

$$\begin{aligned} \xi &= -\frac{3}{2} - \frac{15}{46}\sqrt{69} + \frac{1}{\varepsilon^n - 1}, \\ \xi' &= -\frac{3}{2} + \frac{15}{46}\sqrt{69} + \frac{1}{\varepsilon^{-n} - 1} = -\frac{5}{2} + \frac{15}{46}\sqrt{69} - \frac{1}{\varepsilon^n - 1}, \end{aligned}$$

²For more details, see the analogous construction of the points R_r in Section 5.

and now we find

$$\left| N\left(Q_r - \frac{5 + \sqrt{69}}{2}\right) \right| = -\xi\xi' = \frac{165 - 15\sqrt{69}}{46} - \frac{1}{\varepsilon^n - 1} \left(-1 + \frac{15}{23}\sqrt{69}\right).$$

Since the “error term” $\frac{1}{\varepsilon^n - 1}(-1 + \frac{15}{23}\sqrt{69})$ is positive and tends to 0 as $n \rightarrow \infty$, Claim 4.6 follows, and Theorem 4.1 is proved.

5 Weighted norms in $\mathbb{Q}(\sqrt{69})$

Now we study the weighted norm $f_{\mathfrak{p},c}$ defined by $\mathfrak{p} = (23, \sqrt{69})$. We claim

Theorem 5.1. *Let $R = \mathcal{O}_K$ be the ring of integers in $K = \mathbb{Q}(\sqrt{69})$, and let $\mathfrak{p} = (23, \sqrt{69})$ be the prime ideal above 23. Then the Euclidean window of $f = f_{\mathfrak{p},c}$ is $w(\mathfrak{p}) = (25, \infty)$; the Euclidean minimum is*

$$M_1(\mathcal{O}_K, f_{\mathfrak{p},c}) = \max \left\{ \frac{25}{c}, \frac{1}{23}(-600 + 75\sqrt{69}) \right\}$$

for all $c \in w(\mathfrak{p})$, and M_1 is isolated exactly when $c \in [23, \frac{23}{15}(8 + \sqrt{69})]$.

Using the method described in [7], with some modifications described in the next section, we can cover the fundamental domain of \mathcal{O}_K with a bound of $k = 0.99$ except for a set surrounding $(0, 0)$ that contains no exceptional point, and $\pm S_1 \cup \pm S_2 \cup \pm S'_2$, where

$$\begin{aligned} S_1 &= [-0.0084, 0.0084] \times [0.1739, 0.175] \\ S_2 &= [0.2086, 0.2087] \times [0.19903, 0.19904] \\ S'_2 &= [0.2086, 0.2087] \times [-0.19904, -0.19903] \end{aligned}$$

Transforming by units, we find

$$\begin{aligned} \varepsilon S_1 - (18 + 2\sqrt{69}) &\tilde{\subset} S_1 \cup S_2, & \bar{\varepsilon} S_1 + (18 - 2\sqrt{69}) &\tilde{\subset} S_1 \cup (-S'_2), \\ \varepsilon S_2 - (23 + 3\sqrt{69}) &\tilde{\subset} S'_2, & \bar{\varepsilon} S_2 + (18 - 2\sqrt{69}) &\tilde{\subset} S_1, \\ \varepsilon S'_2 + (18 + 2\sqrt{69}) &\tilde{\subset} -S_1, & \bar{\varepsilon} S'_2 - (23 - 3\sqrt{69}) &\tilde{\subset} S_2. \end{aligned}$$

Claim 5.1. If P is an exceptional point that stays inside S_1 under repeated transformations by ε and ε^{-1} , then $P = (0, \frac{4}{23})$ has Euclidean minimum $M(P, f_{\mathfrak{p},c}) = \frac{25}{23c}$.

This is easy to see. Again, this enables us to reduce everything to exceptional points $P \in S_2$, and for the orbit (P_j) of such P (here P_{j+1} is the image of P_j under multiplication by ε plus reduction modulo \mathcal{O}_K) there are the following possibilities:

- (a) $P_j \in -S_1$ and $P_{-j} \in S_1$ for all $j \geq 2$;
- (b) there exist $m \neq n$ such that $P_m, P_n \in S_2$.

Claim 5.2. If $P_0 \in S_2$ is an exceptional point with property (a), then

$$P_0 = \left(\frac{-115+15\sqrt{69}}{46}, \frac{-5+\sqrt{69}}{2\sqrt{69}} \right) \approx (0.20868169, 0.19903536).$$

For a proof, suppose that P_0 is a point in S_2 with property (a). Then $P_1 = -\varepsilon P_0 + (23+3\sqrt{69}) \in -S'_2$, and $P_2 = \varepsilon P_1 - (18+2\sqrt{69})$ is a point whose transforms by powers of ε stay inside S_1 . By Proposition 4.2, this implies that $|P_2 - \frac{4}{23}\sqrt{69}|_1 = 0$, and going back to P_0 we find that $|P_0 - (-5 + \frac{19}{23}\sqrt{69})|_1 = 0$.

Similarly, any exceptional point $\xi \in S_2$ whose transforms by powers of $\bar{\varepsilon}$ stay inside S_1 satisfies $|\xi + \frac{4}{23}\sqrt{69}|_2 = 0$. Thus any point satisfying (a) has x -coordinate $(\xi + \xi')/2 = \frac{-115+15\sqrt{69}}{46}$ and y -coordinate $(\xi - \xi')/2\sqrt{69} = \frac{-5+\sqrt{69}}{2\sqrt{69}}$ as claimed.

Note that there is no obvious definition of a ‘‘Euclidean minimum’’ of P_0 with respect to weighted norms $f_{\mathfrak{p},c}$, since $f_{\mathfrak{p},c}$ is a continuous function on K (with respect to the topology inherited from the embedding $K \rightarrow \mathbb{R}^2$) if and only if $c = \mathfrak{p}$, that is, if and only if $f_{\mathfrak{p},c}$ is the absolute value of the usual norm. Thus we cannot extend $f_{\mathfrak{p},c}$ by continuity to \mathbb{R}^2 . On the other hand, we can put

$$\overline{M}(P, f_{\mathfrak{p},c}) = \sup \{M(P_r, f_{\mathfrak{p},c}) : P_r \in K, \lim P_r = P\},$$

that is, define the minimum at a point $P \in K$ as the supremum of the minima at $P_r \in K$ over all sequences (P_r) converging to P in the topology mentioned above. If $P \in K$, then clearly $\overline{M}(P, f_{\mathfrak{p},c}) \geq M(P, f_{\mathfrak{p},c})$, as the constant series $P_r = P$ shows. We don’t know an example where this last inequality is strict.

Claim 5.3. We have $\overline{M}(P_0) \leq \kappa_0 = \frac{1}{23}(-600 + 75\sqrt{69})$ for all $c \geq 23$. Moreover, any K -rational exceptional point with property (b) has minimum strictly smaller than κ_0 . In particular, we have $M_1(K) = \frac{25}{23c}$ for all $c \in [23, \frac{25}{23}(24 + 3\sqrt{69})]$, and M_1 is isolated for these values of c unless possibly when $c = \frac{25}{23}(24 + 3\sqrt{69})$.

We start by observing that

$$\begin{aligned} |N(P_0 - 2)| &= \frac{94-10\sqrt{69}}{23} \approx 0.47538092916, \quad \text{and} \\ |N(P_0 - \frac{1}{2}(5 + \sqrt{69}))| &= \frac{-600+75\sqrt{69}}{23} \approx 0.99986042255. \end{aligned}$$

Using the same technique as in Lemma 4.5 and 4.6 we can show that the K -rational points in S_2 that satisfy condition (b) have minimum strictly smaller than κ_0 ; observe that the difference $\eta_1 - \eta_2$ for $\eta_1 = \frac{1}{2}(5 + \sqrt{69})$ and $\eta_2 = 2$ is not divisible by \mathfrak{p} , hence we have $f_{\mathfrak{p},c}(P_0 - \eta_j) \leq |N(P_0 - \eta_j)|$ for $j = 1$ or $j = 2$. Since any sequence of K -rational points P_r converging to P_0 eventually stays inside S_2 this also proves that $M_1(\mathcal{O}_K, f_{\mathfrak{p},c}) = \frac{25}{23c}$ as long as $\frac{25}{23c} \geq \kappa_0$; but the last inequality holds for all $c \leq \frac{23}{15}(8 + \sqrt{69}) \approx 25.0034899$. It also shows that the minimum is isolated for these values unless possibly when $c = \frac{23}{15}(8 + \sqrt{69})$.

Claim 5.4. We have $\overline{M}(P_0, f_{\mathfrak{p},c}) = \kappa_0 = \frac{1}{23}(-600 + 75\sqrt{69})$ for all $c > 23$, and $\overline{M}(P_0, f_{\mathfrak{p},c}) = M(P) = \frac{94-10\sqrt{69}}{23}$ for $c = 23$.

In order to show that κ_0 is a lower bound for $M(P_0)$ for $c > 23$, we construct a series of K -rational points converging to P_0 whose minima converge to κ_0 . We do this in the following way: assume that $R_r \in S_2$ gets mapped to S'_2 , stays in $-S_1$ exactly $r-2$ times and then gets mapped to the point $-R_r \in -S_2$. Then $\varepsilon R_r - (23 + 3\sqrt{69}) \in S'_2$, $\varepsilon^2 R_r - \varepsilon(23 + 3\sqrt{69}) + (18 + 2\sqrt{69}) \in -S_1$, \dots , $\varepsilon^r R_r - \varepsilon^{r-1}(23 + 3\sqrt{69}) + (18 + 2\sqrt{69})(1 + \varepsilon + \dots + \varepsilon^{r-2}) \in -S_1$ and finally

$$(\varepsilon^{r+1} + 1)R_r = \varepsilon^r(23 + 3\sqrt{69}) - (18 + 2\sqrt{69})\frac{\varepsilon^r - 1}{\varepsilon - 1}$$

Now we use $\frac{\varepsilon^r - 1}{\varepsilon - 1} = \frac{\varepsilon^{r+1} - 1}{\varepsilon - 1} - \varepsilon^r$ to find

$$\begin{aligned} (\varepsilon^{r+1} + 1)R_r &= \varepsilon^r(41 + 5\sqrt{69}) - (18 + 2\sqrt{69})\frac{\varepsilon^{r+1} - 1}{\varepsilon - 1} \\ &= \varepsilon^{r+1}(-5 + \sqrt{69}) - (18 + 2\sqrt{69})\frac{\varepsilon^{r+1} - 1}{\varepsilon - 1}. \end{aligned}$$

Dividing through by $\varepsilon^{r+1} + 1$ and simplifying we get

$$R_r = -5 + \frac{19}{23}\sqrt{69} + \frac{1}{\varepsilon^{r+1} + 1}\left(5 - \frac{15}{23}\sqrt{69}\right).$$

The explicit coordinates for the first few points are given in the following table:

r	R_r	$ N(R_r - \frac{1}{2}(5 + \sqrt{69})) $	$ N(R_r - 2) $
1	$\frac{1}{5} + \frac{1}{5}\sqrt{69}$	$\frac{23}{25} = 0.92$	$\frac{12}{25} = 0.48$
2	$\frac{5}{24} + \frac{43}{216}\sqrt{69}$	$\frac{3875}{3888} \approx 0.996656378$	$\frac{1849}{3888} \approx 0.475565843$
3	$\frac{130}{623} + \frac{124}{623}\sqrt{69}$	$\frac{388025}{388129} \approx 0.999732047$	$\frac{184512}{388129} \approx 0.475388337$
4	$\frac{125}{599} + \frac{1073}{5391}\sqrt{69}$	$\frac{9686225}{9687627} \approx 0.999855279$	$\frac{4605316}{9687627} \approx 0.475381225$
5	$\frac{649}{3110} + \frac{619}{3110}\sqrt{69}$	$\frac{2417687}{2418025} \approx 0.999860216$	$\frac{1149483}{2418025} \approx 0.475380941$
6	$\frac{3120}{14951} + \frac{26782}{134559}\sqrt{69}$	$\frac{6034532375}{6035374827} \approx 0.999860414$	$\frac{2935561516}{6035374827} \approx 0.475380929$

Claim 5.5. The Euclidean minimum of R_r ($r \geq 2$) with respect to $f_{\mathfrak{p},c}$ is attained at $R_r - 2$ or $R_r - \frac{1}{2}(5 + \sqrt{69})$.

In fact, applying Proposition 4.3 to R_r one checks that the two smallest values of $|N(R_r - \eta)|$ occur for $\eta_1 = 2$ or $\eta_2 = \frac{1}{2}(5 + \sqrt{69})$; one also verifies that $|N(R_r - 2)| \approx 0.47$ and $|N(R_r - \frac{1}{2}(5 + \sqrt{69}))| \approx 0.99$. Since the denominator of $R_r - \eta$ is not divisible by \mathfrak{p} for any $\eta \in \mathcal{O}_K$ (it divides $\varepsilon^{r+1} + 1 \equiv 2 \pmod{\mathfrak{p}}$), and since $\eta_1 - \eta_2$ is an integer not divisible by \mathfrak{p} , our claim follows.

Where the minimum with respect to $f_{\mathfrak{p},c}$ is attained depends on whether the numerator of $R_r - 2$ is divisible by \mathfrak{p} or not: if it isn't, then the Euclidean minimum is attained there, and we have $M(P, f_{\mathfrak{p},c}) = |N(R_r - 2)| < \frac{1}{2}$. If this numerator, however, is divisible by \mathfrak{p} , then $f_{\mathfrak{p},c}(R_r - 2)$ can be made as large as we please by adding weight to \mathfrak{p} , and in this case the minimum is attained at $R_r - \frac{1}{2}(5 + \sqrt{69})$ for large values of c .

Claim 5.6. The numerator of $R_r - 2$ is divisible by \mathfrak{p} if and only if $r \equiv 10 \pmod{23}$. In this case, it is even divisible by $(23) = \mathfrak{p}^2$.

Let us compute $R_r \pmod{\mathfrak{p}}$. Since $\varepsilon \equiv 1 \pmod{\mathfrak{p}}$, we find $\frac{\varepsilon^{r+1}-1}{\varepsilon-1} = 1 + \varepsilon + \dots + \varepsilon^r \equiv r + 1 \pmod{\mathfrak{p}}$, hence $2R_r = \varepsilon^r(23 + 3\sqrt{69}) - (18 + 2\sqrt{69})\frac{\varepsilon^r-1}{\varepsilon-1} \equiv 5r \pmod{\mathfrak{p}}$, and therefore $R_r - 2 \equiv 0 \pmod{\mathfrak{p}}$ if and only if $5r \equiv 4 \pmod{23}$, which in turn is equivalent to $r \equiv 10 \pmod{23}$.

The second part of the claim follows by observing $\varepsilon^s \equiv (1 + 13\sqrt{69}) \equiv 1 + 13s\sqrt{69} \pmod{23}$, in particular $\varepsilon^{23m+10} \equiv 1 + 13\sqrt{69} \pmod{23}$ and $\frac{\varepsilon^r-1}{\varepsilon-1} = \varepsilon^{r-1} + \dots + \varepsilon + 1 \equiv r + 1 + 13\frac{r(r+1)}{2}\sqrt{69} \pmod{23}$.

With a little more effort we can show much more, namely that there is a subsequence of $R_r - 2$ with numerators divisible by an arbitrarily large power of \mathfrak{p} . In fact, the numerator of $R_r - 2$ will be divisible by \mathfrak{p}^k if and only if $T_r = 23(\varepsilon^{r+1} + 1)(R_r - 2) \equiv 0 \pmod{\mathfrak{p}^{k+2}}$, and here T_r is an algebraic integer. An elementary calculation shows that the last congruence is equivalent to

$$\varepsilon^{r+1} \equiv -\frac{47 + 5\sqrt{69}}{22} =: \alpha \pmod{\mathfrak{p}^{k+2}}. \quad (4)$$

This will hold for arbitrarily large k if and only if there is a 23-adic integer $s = r + 1$ such that

$$\varepsilon^s = \alpha \quad (5)$$

holds in $K_{\mathfrak{p}} = \mathbb{Q}_{23}(\sqrt{69})$. Since both sides are congruent 1 mod \mathfrak{p} , we can take the π -adic logarithm (with $\pi = \frac{23+3\sqrt{69}}{2}$) and get $s = \frac{\log_{\pi} \alpha}{\log_{\pi} \varepsilon}$ as an equation in $K_{\mathfrak{p}}$, and (5) holds if we can show that s is in \mathbb{Z}_{23} . To this end,³ let σ denote the non-trivial automorphism of $K_{\mathfrak{p}}/\mathbb{Q}_{23}$. Since \log_{π} is Galois-equivariant, and since $\varepsilon^{1+\sigma} = \alpha^{1+\sigma} = 1$, we get

$$s^{\sigma} = \frac{\log_{\pi} \alpha^{\sigma}}{\log_{\pi} \varepsilon^{\sigma}} = \frac{-\log_{\pi} \alpha}{-\log_{\pi} \varepsilon} = s.$$

Thus $s \in \mathbb{Z}_{23}$, and since it is a π -adic unit, $s \in \mathbb{Z}_{23}$ as desired. We remark that $s = 11 + 13 \cdot 23 + 15 \cdot 23^2 + 5 \cdot 23^3 + 3 \cdot 23^4 + \dots$

This proves Claim 5.4 and completes the proof of Theorem 5.1.

6 Weighted norms in cubic number fields

Using the idea of Clark (see [7, 8, 10, 15]; it actually first appears in Lenstra [12, p. 35]), we modified the programs described in [6] slightly in order to examine weighted norms in cubic fields. Many of the results in this section have been obtained by the first author in [5]; see Table 1 for the results obtained so far.

The idea is simple. Assume that K is a number field with class number 1 such that $M = M_1(K) \geq 1$ and $M_2(K) < 1$; assume that $\#C_1(K)$ is finite

³We thank (in chronological order) Hendrik Lenstra, Gerhard Niklasch and David Kohel for this argument.

Table 1:

disc K	$M_1(K)$	$M_2(K)$	$N\mathfrak{p}$	$w(\mathfrak{p})$
-367	1	9/13	13	(13, 279/8)
-351	1	9/11	11	(11, ∞)
-327	101/99	< 0.9	11	(101/9, ∞)
-199	1	< 0.47	7	(7, ∞)
985	1	5/11	5	(5, ∞)
1345	7/5	< 0.4	5	(7, ∞)
1825	7/5	< 0.5	5	(7, ∞)
1929	1	3/7	7	(7, ∞)
1937	1	5/9	3	(3, ∞)
2777	5/3	17/19	3	\emptyset
2836	7/4	7/8	2	($\sqrt{7}$, ∞)
2857	8/5	< 0.5	5	(8, ∞)
3305	13/9	37/45	3	($\sqrt{13}$, 5)
3889	13/7	1	7	(13, ∞)
4193	7/5	< 0.65	5	(7, ∞)
4345	7/5	11/13	5	(7, ∞)
4360	41/35	7/10	7	(41/5, ∞)
5089	17/11	7/11	11	(17, ∞)
5281	1	< 0.6	5	(5, ∞)
5297	21/11	23/33	11	(21, ∞)
5329	9/8	63/73	2^3	(9, 73)
5369	21/19	17/19	19	(21, ∞)
5521	23/7	8/7	7	(23, ∞)
7273	973/601	729/601	601	(973, ∞)
7465	1	< 0.8	5	(5, ∞)
7481	1	< 0.7	5	(5, ∞)

and write the points $\xi \in C_1(K)$ ($1 \leq i \leq t$) in the form $\xi_i = \alpha_i/\beta_i$, where $(\alpha_i, \beta_i) = 1$. Assume moreover that there is a prime ideal \mathfrak{p} such that $\mathfrak{p} \mid \beta_i$ for all i .

Now consider the weighted norm $f_{\mathfrak{p},c}$; by making c big enough we can

certainly arrange that $f_{\mathfrak{p},c}(\xi_i) < 1$ for all $i \leq t$: in fact, if $\mathfrak{p}^m \parallel \gcd(\beta_1, \dots, \beta_t)$, then $f_{\mathfrak{p},c}(\xi_i) \leq M(N\mathfrak{p})^m c^{-m}$; thus we only need to choose $c > N\mathfrak{p} \sqrt[m]{M}$ (actually this shows that $w(\mathfrak{p}) \subseteq (N\mathfrak{p} \sqrt[m]{M}, \infty)$).

In order to guarantee that, for every $\xi \in K$, there exists a $\gamma \in \mathcal{O}_K$ such that $f_{\mathfrak{p},c}(\xi - \gamma) < 1$, we will look for $\gamma_1, \gamma_2 \in \mathcal{O}_K$ such that $|N_{K/\mathbb{Q}}(\xi - \gamma_i)| < 1$ for $i = 1, 2$ and $\mathfrak{p} \nmid (\gamma_1 - \gamma_2)$; then at least one of the $\xi - \gamma_i$, say $\xi - \gamma_1$, has numerator not divisible by \mathfrak{p} , and this implies that $f_{\mathfrak{p},c}(\xi - \gamma_1) \leq |N(\xi - \gamma_1)| < 1$.

By modifying the programs described in [6] slightly we can use them to find new examples of cubic fields that are not norm-Euclidean but Euclidean with respect to some weighted norm. We represented prime ideals of the maximal order $\mathcal{O}_K = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \beta\mathbb{Z}$ in the form $\mathfrak{p} = (p, \alpha + a)$, $(p, \beta + a\alpha + b)$ or (p) according as \mathfrak{p} has degree 1, 2 or 3. Testing the divisibility of an integer of \mathcal{O}_K by \mathfrak{p} then can be done using only rational arithmetic.

Let us call $\xi \in K$ covered if there exist $\gamma_1, \gamma_2 \in \mathcal{O}_K$ such that $|N_{K/\mathbb{Q}}(\xi - \gamma_i)| < 1$ and $\mathfrak{p} \nmid (\gamma_1 - \gamma_2)$; if ξ is covered, then so is $\varepsilon\xi$ for any unit $\varepsilon \in \mathcal{O}_K^\times$ (this allows us to use the program E-3 of [6]).

We first consider the field K generated by a root α of $x^3 + x^2 - 6x - 1$; we have $\text{disc } K = 985$, and the only point with minimum ≥ 1 is $\xi_1 = \frac{3\alpha - \alpha^2}{\alpha - 1} = \frac{2 - \alpha + 2\alpha^2}{5}$. The ideal $\mathfrak{p} = (\alpha - 1)$ occurring in the denominator is a prime ideal of norm 5. Our programs cover a fundamental domain of K except for the possible exceptional points $\xi = 0$ and $\xi = \xi_1$. Thus $f_{\mathfrak{p},c}$ is a Euclidean function for every $c > N\mathfrak{p} = 5$, i.e. $w(\mathfrak{p}) = (5, \infty)$.

Now let K be the field with $\text{disc } K = 1937$ generated by a root α of $x^3 + x^2 - 8x + 1$. It has Euclidean minimum $M(K) = 1$ attained at $\frac{4+4\alpha^2}{9}$; in fact $|N(\xi_1)| = 1$ for $\xi_1 = \frac{1}{9}(-14 + 9\alpha + 4\alpha^2)$, and the prime ideal factorization of ξ_1 is $(\xi_1) = (3, \alpha^2 + 1)(3, \alpha + 1)^{-2}$. Our programs cover a fundamental domain of K except for the possible exceptional points $\xi_0 = 0$, $\xi = \xi_1$ and $\xi = \frac{1}{3}(1 + \alpha^2)$. This last point has Euclidean minimum $\frac{1}{3} = |N(\frac{1}{3}(1 - 3\alpha + \alpha^2))|$ with respect to the usual norm, and since $(1 - 3\alpha + \alpha^2)/3 = \mathfrak{p}^{-1}$, adding weight to \mathfrak{p} does not increase its minimum.

Our third example is the cubic field K with discriminant $\text{disc } K = 3305$, generated by a root α of $x^3 - x^2 - 10x - 3$. It has minimum $M_1 = \frac{13}{9}$ attained at $\frac{1}{9}(1 - 2\alpha - 4\alpha^2)$, with $|N(\xi_1)| = \frac{13}{9}$ for $\xi_1 = \frac{1}{9}(-71 + 52\alpha + 32\alpha^2)$. Its prime ideal factorization is $(\xi_1) = (13, \alpha - 1)(3, \alpha)^{-2}$; we thus add weight $c > \sqrt{13}$ to $\mathfrak{p} = (3, \alpha)$, and we can cover a fundamental domain of K except for the possible exceptional points $\xi_0 = 0$, $\xi = \xi_1$ and $\xi = \frac{1}{5}(2 - \alpha + 2\alpha^2)$. Now $M(\xi) = |N(\xi_2)| = \frac{3}{5}$, where $\xi_2 = \frac{1}{5}(-3 + 4\alpha + 2\alpha^2)$ has the prime ideal factorization $(\xi_2) = \mathfrak{p}(5, \alpha + 2)^{-1}$. Thus the weighted prime ideal occurs in the numerator of ξ_2 , and we have $f_{\mathfrak{p},c}(\xi_2) < 1$ if and only if $c < 5$; since $|N(\xi)| \geq 1$ for all $\xi \equiv \xi_2 \pmod{\mathcal{O}_K}$, this implies that $w(\mathfrak{p}) = (\sqrt{13}, 5)$.

Finally, consider the cubic field K with discriminant $\text{disc } K = 3889$. Its first minimum is attained at $\xi_1 = \frac{1}{7}(3 - \alpha - 3\alpha^2)$, and its denominator is the prime ideal \mathfrak{p} that divides the denominator of $\xi_2 = \frac{1}{7}(2 - 3\alpha - 2\alpha^2)$, where the second minimum $M_2(K) = 1$ is attained (something similar happens for $\text{disc } K = 5521$ and $\text{disc } K = 7273$, where $M_2(K) > 1$; in these cases, we

have to verify that $M_3(K) < 1$). Here we find the possible exceptional points $\xi = 0, \xi_1, \xi_2$, as well as $\eta_1 = \frac{1}{7}(1 - \alpha - 2\alpha^2)$, $\eta_2 = \frac{1}{7}(2 - 2\alpha + 3\alpha^2)$ and $\eta_3 = \frac{1}{7}(3 - 3\alpha + \alpha^2)$. Since their denominator is the prime ideal $(7, 2 + \alpha)$, their Euclidean minimum is $\frac{1}{7}$ both for the usual as well as for the weighted norm.

Some of our examples of cubic fields that are Euclidean with respect to some weighted norm were found independently by Amin Coja-Oghlan; see his forthcoming thesis [9].

7 Norm-Euclidean cubic fields

We take this opportunity to report on recent computations concerning norm-Euclidean cubic fields. Calculations for the totally real cubic fields up to disc $K \leq 13,000$ have produced the following results:

disc K	E	N	Σ
$0 < d \leq 1000$	26	1	27
$1000 < d \leq 2000$	29	5	34
$2000 < d \leq 3000$	31	4	35
$3000 < d \leq 4000$	36	6	42
$4000 < d \leq 5000$	28	7	35
$5000 < d \leq 6000$	35	7	42
$6000 < d \leq 7000$	30	8	38
$7000 < d \leq 8000$	37	10	47
$8000 < d \leq 9000$	30	11	41
$9000 < d \leq 10000$	29	10	39
$10000 < d \leq 11000$	34	9	43
$11000 < d \leq 12000$	37	16	53
$12000 < d \leq 13000$	31	6	37
Σ	413	100	513

The columns E and N display the number of norm-Euclidean and not norm-Euclidean number fields of fields with discriminants in the indicated intervals.

We also have to correct the entries for the fields with discriminant 3969 in our tables in [6]: the field K_1 generated by a root of $x^3 - 21x - 28$ has $M_1(K_1) = 4/3$, $M_2(K_1) = 31/24$ and $M_3(K_1) = 1$, and the field K_2 generated by $x^3 - 21x - 35$ has $M_1(K_2) = 7/3$ and $M_2(K_2) = 125/63$.

For complex cubic fields, calculations by R. Quême indicated that the fields with disc $K = -999$ and disc $K = -1055$ are not norm-Euclidean, and we could meanwhile verify that $M(K) \geq 294557/272112$ for disc $K = -999$ and $M(K) \geq 1483/1370$ for disc $K = -1055$, and that there are no norm-Euclidean number fields with $-876 > \text{disc } K \geq -1600$, suggesting the following

Conjecture. There are exactly 58 norm-Euclidean complex cubic fields, and their discriminants are $-23, -31, -44, -59, -76, -83, -87, -104, -107, -108, -116, -135, -139, -140, -152, -172, -175, -200, -204, -211, -212, -216, -231, -239, -243, -244, -247, -255, -268, -300, -324, -356, -379, -411, -419, -424, -431, -440, -451, -460, -472, -484, -492, -499, -503, -515, -516, -519, -543, -628, -652, -687, -696, -728, -744, -771, -815, -876$.

Note that, by a result of Cassels [4], there are only finitely many norm-Euclidean complex cubic number fields K , and in fact their discriminant is bounded by $|\text{disc } K| < 170\,520$.

$d = \text{disc } K $	E	N	Σ
$0 < d \leq 200$	18	1	19
$200 < d \leq 400$	15	9	24
$400 < d \leq 600$	16	10	26
$600 < d \leq 800$	7	20	27
$800 < d \leq 1000$	2	29	31
$1000 < d \leq 1200$	0	29	29
$1200 < d \leq 1400$	0	35	35
$1400 < d \leq 1600$	0	27	27
Σ	58	160	218

In the real case, the situation is not so clear. The numerical data suggest that the proportion of norm-Euclidean fields is decreasing with $\text{disc } K$, but they do not yet support the conjecture that the norm-Euclidean real cubic number fields have density 0 among the real cubic fields with class number 1.

8 Some Open Problems

In this last section we would like to mention several open problems concerning the Euclidean algorithm with respect to weighted norms. One of the most studied questions is of course whether $\mathbb{Z}[\sqrt{14}]$ is Euclidean with respect to some $f_{\mathfrak{p},c}$, where $\mathfrak{p} = (2, \sqrt{14})$. Is it true, in particular, that $w(\mathfrak{p}) = (\sqrt{5}, \sqrt{7})$ in this case?

More generally: assume that K is a number field with unit rank ≥ 1 . Is $w(\mathfrak{p})$ always an open subset of $(1, \infty) \subset \mathbb{R}$ for every prime ideal \mathfrak{p} in \mathcal{O}_K ? If this were the case, then there would also exist number fields such that $f_{\mathfrak{p},c}$ is a Euclidean function for some $c < N\mathfrak{p}$ since there do exist number fields with $w(\mathfrak{p}) \supseteq [p, \infty)$ for suitable primes (take norm-Euclidean fields, for example).

A related question is whether $M(f_{\mathfrak{p},c})$ is a continuous function of c on $[N\mathfrak{p}, \infty)$ for number fields with unit rank ≥ 1 .

The cubic field with discriminant $\text{disc } K = -335$ has $M_1(K) = 1$; the minimum is attained at points that have different prime ideals above 5 in their denominator. Calculations have not yet confirmed that \mathcal{O}_K is Euclidean with respect to a norm that is weighted at two different prime ideals. Similar

remarks apply to algorithms with respect to functions that are not multiplicative: instead of giving weight c to a prime ideal \mathfrak{p} , one could look at functions with $f(\mathfrak{p}) = N\mathfrak{p}$ and $f(\mathfrak{p}^2) = c$ for some $c \geq N\mathfrak{p}^2$. This idea is applicable whenever the denominators of the exceptional points are divisible by the square of a prime ideal, e.g. for $\mathbb{Z}[\sqrt{14}]$.

References

- [1] E.S. Barnes, H.P.F. Swinnerton-Dyer, *The inhomogeneous minima of binary quadratic forms I*, Acta Math. **87** (1952), 259–323; II, *ibid.* **88** (1952), 279–316 5
- [2] E. Bedocchi, *L’anneau $\mathbb{Z}[\sqrt{14}]$ et l’algorithme Euclidien*, Manuscripta math. **53** (1985), 199–216 4
- [3] D. Cardon, *A Euclidean Ring Containing $\mathbb{Z}[\sqrt{14}]$* , C. R. Math. Acad. Sci., Soc. R. Can. **19** (1997), 28–32 4
- [4] J. W. S. Cassels, *The inhomogeneous minima of binary quadratic, ternary cubic, and quaternary quartic forms*, Proc. Cambridge Phil. Soc. **48** (1952), 72–86; Addendum: *ibid.*, 519–520 18
- [5] S. Cavallar, *Alcuni esempi di campi di numeri cubici non euclidei rispetto alla norma ma euclidei rispetto ad una norma pesata*, Tesi di Laurea, Univ. Trento, 1995 14
- [6] S. Cavallar, F. Lemmermeyer, *The Euclidean Algorithm in Cubic Number Fields*, Proceedings Number Theory Eger 1996, (Györy, Pethö, Sos eds.), Gruyter 1998, 123–146 6, 14, 16, 17
- [7] D. A. Clark, *A quadratic field which is Euclidean but not norm-Euclidean*, Manuscripta math. **83** (1994), 327–330 2, 4, 11, 14
- [8] D. A. Clark, *Non-Galois cubic fields which are Euclidean but not norm-Euclidean*, Math. Comp. **65** (1996), 1675–1679 2, 14
- [9] A. Coja-Oghlan, *Berechnung kubischer euklidischer Zahlkörper*, Diplomarbeit FU Berlin, 1999 17
- [10] B. Hainke, *Euklidische Algorithmen in den Ganzheitsringen von $\mathbb{Q}(\sqrt{14})$ und $\mathbb{Q}(\sqrt{69})$* , Diplomarbeit Univ. Mainz, 1998 4, 14
- [11] F. Lemmermeyer, *The Euclidean Algorithm in Algebraic Number Fields*, Expo. Math. **13** (1995), 385–416 4, 5
- [12] H. W. Lenstra, *Euclidean Rings*, Lecture Notes, Bielefeld 1974 2, 14
- [13] M. Nagata, *A pairwise algorithm and its application to $\mathbb{Z}[\sqrt{14}]$* , Algebraic geometry Seminar, Singapore 1987, 69–74 4

- [14] M. Nagata, *Some questions on $\mathbb{Z}[\sqrt{14}]$* , Algebraic geometry and its applications (Ch. Bajaj, ed.), Conf. Purdue Univ. USA, June 1–4, 1990, Springer Verlag (1994), 327–332 4
- [15] G. Niklasch, *On Clarks example of a Euclidean field which is not norm-euclidean*, Manuscripta math. **83** (1994), 443–446 4, 14