EUCLID'S ALGORITHM IN QUARTIC CM-FIELDS

FRANZ LEMMERMEYER

Abstract. In this note we present techniques to compute inhomogeneous minima of norm forms; as an application, we determine all norm-Euclidean complex bicyclic quartic number fields.

1. Introduction

A number field K is said to be Euclidean (with respect to the norm), if for all $\xi \in K$ we can find $\eta \in \mathcal{O}_K$ such that $|N_{K/\mathbb{Q}}(\xi - \eta)| < 1$. Although it is known since the work of Davenport that there are only a finite number of Euclidean fields with unit rank 1, only the quadratic Euclidean fields have been determined so far. In this paper, we will determine the Euclidean normal quartic CM-fields (these are totally complex quartic fields which contain a real quadratic subfield). According to a well known theorem due to Cassels [3], such fields have discriminants $< 230\,202\,117$. In fact, the bound given by Cassels was somewhat smaller, but his computations were shown to contain an error by van der Linden [9]. Using Setzer's solution of the class number 1 problem for complex cyclic quartic number fields, van der Linden was able to prove

Theorem 1. *There are exactly two complex cyclic quartic fields that are norm-Euclidean:* $\mathbb{Q}(\zeta_5)$ *and the quartic subfield of* $\mathbb{Q}(\zeta_{13})$.

He also gave bounds for disc K in case K is a complex bicyclic quartic field, but did not attempt to determine them all. Making use of ideas of Sauvageot [10], we will prove

Theorem 2. *The Euclidean fields* $\mathbb{Q}(\sqrt{-m}, \sqrt{n}\,)$, $m \in \mathbb{N}, n \in \mathbb{Z}$, *are given by*

$$\begin{array}{llll} m = & 1, & n = & 2, 3, 5, 7; \\ m = & 2, & n = & -3, 5; \\ m = & 3, & n = & 2, 5, -7, -11, 17, -19; \\ m = & 7, & n = & 5. \end{array}$$

2. Lower bounds for Euclidean minima

We begin by fixing the notation. For an algebraic number field K, $\mathcal{O}_K$ denotes its ring of integers, and E_K its unit group. For an ideal $\mathfrak{a}$ in $\mathcal{O}_K$, $N\mathfrak{a}$ will always denote the absolute norm of $\mathfrak{a}$, i.e. the index $(\mathcal{O}_K : \mathfrak{a})$. For $\xi \in K$, put

$$M(\xi, K) = \inf \{|N_{K/\mathbb{Q}}(\xi - \alpha)| : \alpha \in \mathcal{O}_K\};$$

$M(\xi, K)$ is called the Euclidean minimum of K at ξ (it can be proved that $M(\xi, K)$ is in fact a minimum; cf. [1], [2] or [8]); obviously, K is Euclidean if and only if $M(\xi, K) < 1$ for all $\xi \in K$. Moreover,

$$M(K) = \sup \{M(\xi, K) : \xi \in K\}$$

is called the Euclidean minimum of K; we know that this supremum is a maximum if K has unit rank ≤ 1, and we conjecture that this holds for all number fields.

There are three simple methods that allow us to prove that a given field is not Euclidean: the use of ramified primes, the residue classes modulo ideals of small norm, and the use of absolute values. These techniques have been used to determine all quadratic Euclidean fields, and their usefulness has been stressed again by Cioffari [5] in his determination of all pure cubic Euclidean fields.

Proposition 1. *Let K/k be a finite extension of number fields of relative degree n, and suppose that the prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ is completely ramified in K/k, i.e. that $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}^n$. If $\beta \equiv \alpha^n \bmod \mathfrak{p}$ for some $\alpha, \beta \in \mathcal{O}_K \setminus \mathfrak{p}$, and if there do not exist $b \in \mathcal{O}_K$ such that*

(1) *$b \equiv \beta \bmod \mathfrak{p}$;*
(2) *$b = N_{K/k}\delta$ for some $\delta \in \mathcal{O}_K$;*
(3) *$|N_{k/\mathbb{Q}}\, b| < N\mathfrak{p}$;*

then K is not Euclidean.

Proof. Suppose that K is Euclidean; then there is a $\pi \in \mathcal{O}_K$ such that $\mathfrak{P} = \pi\mathcal{O}_K$, and for $\xi = \alpha/\pi$ we can find $\eta \in \mathcal{O}_K$ such that $|N_{K/\mathbb{Q}}(\xi - \eta)| < 1$. This implies $|N_{K/\mathbb{Q}}(\alpha - \eta\pi)| < N\mathfrak{P}$; put $b = N_{K/k}(\alpha - \eta\pi)$. Then we find

(1) $b \equiv \beta \bmod \mathfrak{p}$, because $\alpha - \eta\pi \equiv \alpha \bmod \mathfrak{P}$ and the fact that $\mathfrak{p}$ is completely ramified in K/k imply that $N_{K/k}(\alpha - \eta\pi) \equiv N_{K/k}\alpha \bmod \mathfrak{P}$ as a congruence in the normal closure of K/k. Since both sides are $\in \mathcal{O}_K$, the congruence holds $\bmod \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$.
(2) $b = N_{K/k}\delta$ for $\delta = \alpha - \eta\pi$ is clear;
(3) $|N_{k/\mathbb{Q}}b| = |N_{k/\mathbb{Q}}N_{K/k}(\alpha - \eta\pi)| = |N_{K/\mathbb{Q}}(\alpha - \eta\pi)| < N_{K/\mathbb{Q}}\mathfrak{P} = N_{k/\mathbb{Q}}\,\mathfrak{p}$.

□

In the special case $k = \mathbb{Q}$ and $\mathfrak{p} = p\mathbb{Z}$, there are only two $b \in \mathbb{Z}$ satisfying (1) and (3), because $|N_{k/\mathbb{Q}}\, b| = |b|$ and $|N\mathfrak{p}| = p$. Moreover, if K is totally complex, only positive $b \in \mathbb{Z}$ can be norms from K.

We note that we can use a modification of Proposition 1 to determine lower bounds for $M(\xi, K)$; but this will not be needed in the sequel. Moreover, there is an immediate generalization to products of pairwise different completely ramified prime ideals.

The idea behind our next result is due to Barnes and Swinnerton-Dyer (BSD). Let $\xi = \xi_1 \in K$ and $\varepsilon \in E_K$ be given; it is easy to see that there is an $m \in \mathbb{N}$ such that $\varepsilon^m\xi - \xi \in \mathcal{O}_K$ (we will often write $\xi \equiv \eta \bmod \mathcal{O}_K$ for $\xi - \eta \in \mathcal{O}_K$). The set $\mathrm{Orb}_{\,\varepsilon}(\xi) = \{\xi = \xi_0, \xi_1, \ldots, \xi_{\ell-1} : \xi_j \equiv \varepsilon^j\xi \bmod \mathcal{O}_K, 1 \le j \le \ell\}$ of representatives mod $\mathcal{O}_K$ of the $\varepsilon^j\xi$ is called the *orbit* of ξ. It is clear from the definition of the Euclidean minimum that $M(\xi_0, K) = \ldots = M(\xi_{\ell-1}, K)$ for all $\xi_i \in \mathrm{Orb}_{\,\varepsilon}(\xi)$.

Proposition 2. *Let $K = \mathbb{Q}(\sqrt{m}, \sqrt{n}\,)$ be an imaginary bicyclic number field, $\xi \in K$, and suppose that $\{\xi = \xi_0, \ldots, \xi_{\ell-1}\} = \mathrm{Orb}_{\,\varepsilon}(\xi)$ for a unit $\varepsilon \in \mathcal{O}_K^\times$, where $|\varepsilon| > 1$ for some fixed embedding $|\cdot|$ of K into $\mathbb{C}$. If $M(\xi, K) < \kappa$ for some $\kappa \in \mathbb{R}$, then there is an element $\alpha = r_1 + r_2\sqrt{m} + r_3\sqrt{n} + r_4\sqrt{mn} \in K$ with the following properties:*

(1) *$\alpha \equiv \xi_j \bmod \mathcal{O}_K$ for some $0 \le j \le \ell - 1$;*
(2) *$|N_{K/\mathbb{Q}}\,\alpha| < \kappa$;*

(3) $|r_i| \le \mu_i$ *for* $1 \le i \le 4$, *where the bounds* μ_i *are defined by*

$$\mu_1 = \tfrac{1}{2}\sqrt[4]{\kappa}\Big(\sqrt{|\varepsilon|} + 1/\sqrt{|\varepsilon|}\Big), \quad \mu_2 = \mu_1/\sqrt{|m|},$$
$$\mu_3 = \mu_1/\sqrt{|n|}, \qquad\qquad \mu_4 = \mu_1/\sqrt{|mn|}.$$

Proof. Assume that $M(\xi, K) < \kappa$; then $|N_{K/\mathbb{Q}}(\xi - \eta)| < \kappa$ for some $\eta \in \mathcal{O}_K$. Since $|\varepsilon| > 1$, we can find $n \in \mathbb{N}$ such that

$$\sqrt[4]{k} \cdot \sqrt{|\varepsilon|}^{\,-1} \le |(\xi - \eta)\varepsilon^n| < \sqrt[4]{\kappa} \cdot \sqrt{|\varepsilon|}.$$

If we let $\alpha = (\xi - \eta)\varepsilon^n$, α will satisfy conditions 1. (with $j \equiv n \bmod \ell$) and 2. Now

$$4|r_1| = |\alpha + \alpha' + \alpha'' + \alpha'''| \le 2|\alpha| + 2|\alpha'|,$$

where α, α', α'', α''', are the conjugates of α, and where α'' denotes the complex conjugate of α (this implies $|\alpha''| = |\alpha|$). The inequality

$$\begin{aligned} 0 &< (\sqrt[4]{\kappa} \cdot \sqrt{|\varepsilon|} - |\alpha|)(\sqrt[4]{\kappa} \cdot \sqrt{|\varepsilon|} - |\alpha'|) \\ &= \sqrt{\kappa} \cdot |\varepsilon| - \sqrt[4]{\kappa} \cdot \sqrt{|\varepsilon|}\,(|\alpha| + |\alpha'|) + |\alpha\alpha'|, \end{aligned}$$

together with $|\alpha\alpha'|^2 = N_{k/\mathbb{Q}}\alpha < \kappa$ yields $4|r_1| < 4\mu_1$. Similarly, we get

$$4|r_2\sqrt{m}| = |\alpha - \alpha' + \alpha'' - \alpha'''| \le 2|\alpha| + 2|\alpha'| < 4\mu_1 \text{ etc.},$$

if we assume that $\sqrt{m}$ is fixed by complex conjugation, i.e. that $m > 0$. In case $m < 0$, we have to switch some signs in $|\alpha - \alpha' + \alpha'' - \alpha'''|$, but this does not change the resulting bound. □

Propositions 3 and 4 below will not be needed for the proofs of Theorems 1 and 2; they are included because they might turn out to be useful in the determination of Euclidean CM-fields of higher degree.

Proposition 3. *Let* L *be a CM-field with maximal real subfield* K*; if* L *is norm-Euclidean, but* K *is not, then* $N_{K/\mathbb{Q}}\,\mathrm{disc}(L/K) < 4^{(K:\mathbb{Q})}$.

Proof. Suppose that L is Euclidean; for every $\xi \in K$ we can find $\eta \in \mathcal{O}_L$ such that $N_{L/\mathbb{Q}}(\xi - \eta) < 1$. Let σ denote complex conjugation; then

$$\begin{aligned} N_{L/K}(\xi - \eta) &= (\xi - \eta)(\xi - \eta^\sigma) = \xi^2 - \xi(\eta + \eta^\sigma) + \eta\eta^\sigma \\ &= \tfrac{1}{4}\left((2\xi - T_{L/K}\eta)^2 - (\eta - \eta^\sigma)^2\right). \\ &= \tfrac{1}{4}\left(\left(2\xi - T_{L/K}\eta\right)^2 + N_{L/K}(\eta - \eta^\sigma)\right). \end{aligned}$$

Choose $\xi \in K$ with $M(\xi, K) \ge 1$; this implies $\eta \ne \eta^\sigma$, because otherwise

$$N_{L/\mathbb{Q}}(\xi - \eta) = N_{K/\mathbb{Q}}(\xi - \eta)^2 \ge M(\xi, K) \ge 1.$$

Therefore, $0 \ne \eta - \eta^\sigma \in \mathrm{diff}(L/K)$, i.e. $\mathrm{diff}(L/K) | (\eta - \eta^\sigma)$. Hence

$$N_{L/K}(\xi - \eta) \ge \frac{1}{4}\left(N_{L/K}(\eta - \eta^\sigma)\right),$$

$$1 > N_{L/\mathbb{Q}}(\xi - \eta) \ge 4^{-(K:\mathbb{Q})} N_{K/\mathbb{Q}}\left(N_{L/K}(\eta - \eta^\sigma)\right) \ge 4^{-(K:\mathbb{Q})} N_{L/\mathbb{Q}}\,\mathrm{diff}\,(L/K),$$

and the asserted inequality follows from $\mathrm{disc}\,(L/K) = N_{L/K}\,\mathrm{diff}\,(L/K)$. □

Proposition 4. *Let* L *be a CM-field with maximal real subfield* K*; if* $\mathrm{diff}(L/K) \equiv 0 \bmod 2$*, then* $M(L) \ge M(K)^2$.

This result is best possible: for $L = \mathbb{Q}(\zeta_{12})$ and $K = \mathbb{Q}(\sqrt{3}\,)$ we actually have equality since $M(K) = \frac{1}{2}$ and $M(L) = \frac{1}{4}$.

Proof. If $\operatorname{diff}(L/K) \equiv 0 \bmod 2$, then $2 \mid T_{L/K}\eta$. Moreover, $T_{L/K}\eta = \eta + \eta^\sigma \equiv \eta - \eta^\sigma \bmod 2$ for every $\eta \in \mathcal{O}_L$. Therefore, $N_{L/K}(\xi-\eta) = \big(\xi - \frac12 T_{L/K}\eta\big)^2 - (\eta-\eta^\sigma)^2$ for every $\xi \in K$, and so $N_{L/\mathbb{Q}}(\xi-\eta) \ge N_{K/\mathbb{Q}}(\xi - \frac12 T_{L/K}\eta)^2 \ge M(\xi,K)^2$. This proves the claim. □

3. Normal quartic CM-fields

In this section we will prove that if K is a normal quartic Euclidean CM-field, then K is one of the fields listed in Theorem 1 or 2.

3.1. **Cyclic Fields.** Suppose first that K is a cyclic complex quartic number field; if K is Euclidean, its class number is 1 and according to Setzer, its conductor belongs to the set $\{5, 13, 16, 29, 37, 53, 61\}$.

The field with conductor $\mathfrak{f} = 16$ is $K = \mathbb{Q}\big(\sqrt{-2+\sqrt{2}}\big)$; it has fundamental unit $\varepsilon = 1+\sqrt{2}$. Therefore, the residue class $1 + \sqrt{-2+\sqrt{2}} \bmod 2$ does not contain units; since (3) is inert in $K/\mathbb{Q}$, it does not contain an element of norm 3. The primes $5, 7, 11, 13$ do not split completely in $K/\mathbb{Q}$, so there are no elements in $\mathcal{O}_K \setminus E_K$ with odd norms $< 2^4$: this shows that K is not Euclidean.

Next we apply Proposition 1 to $K/\mathbb{Q}$ with $\mathfrak{p} = p\mathbb{Z}$ and with the values of α, β given in the following table:

p	29	37	53	61
α	6	14	15	4
β	20	10	10	12

In order to show that β is not a norm in $K/\mathbb{Q}$ ($\beta - p$ is never norm because norms from K are always positive), just notice that $(2/p) = -1$.

We remark that it is easy to prove Thm. 1 without making use of Setzer's results: if a cyclic quartic complex field L has odd class number, then its conductor must be a prime power. Since the quadratic fields with prime power discriminant > 73 are not norm Euclidean, Prop. 3 shows that any norm Euclidean L with conductor $p > 73$ must satisfy $p = N_{K/\mathbb{Q}} \operatorname{disc}(L/K) < 4^2 = 16$. This contradiction shows that $f \le 73$. Now we compute the class numbers for the fields in this finite list and continue as above.

3.2. **Bicyclic Fields.** Next we will deal with bicyclic fields. Let $D(m,n)$ denote the ring of integers in $\mathbb{Q}(\sqrt{m}, \sqrt{n}\,)$ and suppose that $D(m,n)$ is Euclidean. We will distinguish the following cases:

I. $D(m,n)$ contains an ideal of norm 2. Since $D(m,n)$ has class number 1, this ideal of norm 2 is principal. Taking relative norms shows that each of the two complex quadratic subfields of $\mathbb{Q}(\sqrt{m}, \sqrt{n}\,)$ contains an element of norm 2. The only such fields are $\mathbb{Q}(\sqrt{-1}\,)$, $\mathbb{Q}(\sqrt{-2}\,)$, and $\mathbb{Q}(\sqrt{-7}\,)$, and this leaves us with $D(-1,2)$, $D(-1,7)$ and $D(-2,-7)$.

Let $R = D(-2,-7)$; we know that $2R = (\mathfrak{2}_1\mathfrak{2}_2)^2$ for prime ideals $\mathfrak{2}_1, \mathfrak{2}_2$ of norm 2. If R were Euclidean, the prime residue classes mod $\mathfrak{m} = \mathfrak{2}_1^2\mathfrak{2}_2$ would contain elements of odd norm $< 8 = N\mathfrak{m}$. Since the unit group is generated by -1 and $\varepsilon = 2\sqrt{-2} + \sqrt{-7}$, the congruence $-1 \equiv \varepsilon \equiv 1 \bmod 2$ shows that only the residue class 1 mod $\mathfrak{m}$ contains units. Since there are no elements of norm 3, 5, or 7 in R, this ring is not Euclidean.

II. $D(m,n)$ **does not contain an ideal of norm** 2**.** This implies that 2 is inert in one of the quadratic subfields of K; there are the following possibilities:

(A) 2 is inert in the real subfield and ramified in the complex subfields;
Let $R = D(m,n)$; we may assume that $m \equiv 2,3 \bmod 4, n \equiv 5 \bmod 8$ and $n > 0$. At least one of the complex quadratic subfields contains an element of norm 2: otherwise, both subfields would have class number > 1, and since K is ramified over at most one of them, K would have non-trivial class number. Therefore, K contains $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-2})$: the possibility $\mathbb{Q}(\sqrt{-7})$ is excluded since we assumed that $m \equiv 2,3 \bmod 4$.

(A.1) $R = D(-1,n), n \equiv 5 \bmod 8$
If R is Euclidean, the residue class $\frac{1+\sqrt{-n}}{1+i} \bmod 2$ contains an element $\alpha \in R$ such that $N\alpha < 16$. This implies that $N_{K/\mathbb{Q}(\sqrt{-n})}\alpha \equiv \sqrt{-n} \bmod 2$. Therefore, $\mathbb{Q}(\sqrt{-n})$ contains an element $\beta \equiv \sqrt{-n} \bmod 2$ of norm < 16. This shows $n < 16$, i.e. $n \in \{5, 13\}$.

Let $R = D(-1,13)$; we will apply Proposition 1 with $k = \mathbb{Q}(i), K = \mathbb{Q}(i,\sqrt{13}), \mathfrak{p} = (3+2i), \alpha = 2, \beta = 4$. The only $b \in \mathbb{Z}[i]$ satisfying (1) and (3) are $b = -1+i$ and $b = 1-2i$: since the prime ideals $(1-i)$ and $(1-2i)$ remain inert in K, these b cannot be norms, and we get a contradiction.

(A.2) $R = D(-2,n), n \equiv 5 \bmod 8$
We look at the residue class $\alpha \equiv \sqrt{-2n} + \frac{1}{2}(1+\sqrt{n}) \bmod 2$ instead and find that $\mathbb{Z}[i]$ contains an element $\equiv 1 + \sqrt{-2n} \bmod 2$ of norm < 16. Now $n \equiv 5 \bmod 8$ and $1 + 2n < 16$ imply $n = 5$.

(B) 2 is inert in a complex subfield and ramified in the real subfield;
Here we may assume that $m \equiv 2,3 \bmod 4, n \equiv 5 \bmod 8$ and $n < 0$. Apply Proposition 1 with $k = \mathbb{Q}(\sqrt{n}), K = \mathbb{Q}(\sqrt{m},\sqrt{n}), \mathfrak{p} = 2\mathcal{O}_K, \beta = \frac{1}{2}(1+\sqrt{n})$; note that β is a square $\bmod 2$ since $\mathcal{O}_K/2\mathcal{O}_K$ has order 3. If $D(m,n)$ is Euclidean, $\mathcal{O}_K$ must contain an element $\equiv \beta \bmod 2$ with norm < 4; obviously, β is no unit if $n < -3$, and this implies that $N_{k/\mathbb{Q}}\beta = 3$. Therefore, $n \in \{-3,-11\}$, and if $n = -11$, β must be norm of an element in $D(m,n)$ with absolute norm 3. Taking the relative norm to $\mathbb{Q}(\sqrt{m})$ of this element shows that $\mathbb{Z}[\sqrt{m}]$ contains an element of norm 3, and this gives $m = -2$. In order to show that $D(-2,-11)$ is not Euclidean, we apply Proposition 2 with $t = 2, \kappa = \frac{6523}{5808}$, and $\xi = \xi_1 = \frac{13}{66}\sqrt{-11}(1-\sqrt{-2}), \varepsilon = 7\sqrt{-2}+3\sqrt{-11}$. This implies $\xi\varepsilon^2 \equiv \xi \bmod R$, and $\mu_1 \approx 2.41, \mu_2 \approx 1.71, \mu_3 \approx 0.73, \mu_4 \approx 0.52$, so only a few values have to be tested.

We are left with $R = D(m,-3)$. Let ρ be a primitive third root of unity, and let N_m denote the relative norm of $K/\mathbb{Q}(\sqrt{m})$. If there is an element $\alpha \equiv \rho + \sqrt{m} \bmod 2$, then $N_m\alpha \equiv m+1+\sqrt{m} \bmod 2$. In case $m \equiv 2 \bmod 4$, this implies the existence of an element $\beta \equiv 3+\sqrt{m} \bmod 2$ with norm < 16 in $\mathbb{Z}[\sqrt{m}]$ and this yields $|m| < 16$. The only domains with class number 1 among these are $D(2,-3)$ and $D(-2,-3)$. Similarly, in case $m \equiv 3 \bmod 4$ we find only $D(-1,-3)$.

(C) 2 is unramified in K.
Write $R = D(m,n)$ and assume that $m, n < 0$. If R is Euclidean, then the residue class $\alpha \equiv \frac{1}{2}(1+\sqrt{m}) \bmod 2$ contains an element of norm < 16; therefore, one of the classes $\frac{1}{2}(1 \pm \sqrt{m})$, $\frac{1}{2}(3 \pm \sqrt{m}) \bmod 2$ contains such

an element, and this implies $|m| < 64$. Similarly, $|n| < 64$, and among the remaining $D(m,n)$, only the following have class number 1:

$$\begin{array}{llll} m = & -3, & n = & -7,-11,-15,-19,-43,-51; \\ m = & -7, & n = & -11,-19,-35,-43; \\ m = & -11, & n = & -19. \end{array}$$

Applying Proposition 1 to $K = \mathbb{Q}(\sqrt{m},\sqrt{n}\,)$ and $k = \mathbb{Q}(\sqrt{n}\,)$, we can exclude the following fields:

m	n	α	$\mathfrak{p}$	$b \bmod \mathfrak{p}$
-3	-43	$\frac{1}{2}(1+\sqrt{-43})$	(3)	$\sqrt{-43}$
-7	-11	$2+\sqrt{-11}$	(7)	$-3\sqrt{-11}$
-7	-19	2	$\frac{1}{2}(3+\sqrt{-19})$	-3
-7	-43	$\frac{1}{2}(3+\sqrt{-43})$	(7)	$\frac{1}{2}(-3+3\sqrt{-43})$
-11	-19	4	$\frac{1}{2}(5+\sqrt{-19})$	5

This takes care of the negative part of Theorem 2. In order to prove that the fields listed there (as well as a few others, cf. [8]) are in fact Euclidean, we used programs written in BASIC (partial results have been obtained by Lakein [6]). The algorithms are described in [4] for the case of cubic fields; we hope to present computational results for the quartic case in the near future. Here is what is known about the Euclidean minima of the fields in Thm. 2:

m	n	$M(K)$
-1	-2	$1/2$
	-3	$1/4$
	5	$5/16$
	-7	$1/2$
-7	5	$9/16$
-2	5	$11/16$

m	n	$M(K)$
-3	2	$\geq 1/4$
	-2	$1/3$
	5	$1/4$
	-7	$4/9$
	-11	< 0.46
	17	$13/16$
	-19	< 0.95

4. A family of bicyclic fields

It is known that there exist constants $c_1, c_2 > 0$ such that, for complex quartic fields K with discriminant $\operatorname{disc} K$, we have $c_1 \operatorname{disc} K \leq M(K) \leq c_2 \operatorname{disc} K$. In this section, we show that $c_1 \leq \frac{1}{32}\operatorname{disc} K \leq c_2$ by computing $M(K)$ for a family of bicyclic quartic fields K:

Theorem 3. *Let n be an odd integer, and put $m = n^2+1$. Put $K = \mathbb{Q}(\sqrt{-1},\sqrt{m}\,)$ and let $\mathcal{O}$ denote the order $\mathbb{Z}[i,\sqrt{m},\frac{1}{2}(\sqrt{m}+\sqrt{-m})\,]$. Then $M(\mathcal{O}) = \frac{m}{4}$, and the minimum is attained at $\xi \equiv \frac{1}{2}(1+i+\sqrt{m}) \bmod \mathcal{O}$. In particular, if m is squarefree, then $M(K) = \frac{m}{4}$.*

Note that $\Delta = \operatorname{disc} K = 4^3m^2$, $\sqrt{\Delta} = 8m$, and $M(K) = \frac{1}{32}\sqrt{\Delta}$.

Proof. Put $m = n^2+1$, $\theta = n+\sqrt{m}$; it is easy to see that $\mathcal{O} = \mathbb{Z}[i,\theta,\gamma]$ with $\gamma = \frac{1}{2}(1+i+\theta+i\theta)$. Consider the set

$$F = \{\xi = x+y\theta \,|\, x = a+bi, y = c+di,\ |a|,\,|b|,\,|c|,\,|d| \leq \tfrac{1}{2}\}.$$

Then F clearly contains a fundamental domain of the lattice $\mathcal{O}$. Thinking of $\mathbb{Z}[i]$ as being contained in $\mathbb{C}$ we see that $N_{K/\mathbb{Q}}(\xi) = |x^2 + 2nxy - y^2|^2$. Therefore ξ is an exceptional point for $k = \frac{1}{4}n^2 = \frac{m-1}{4}$ if and only if $|x^2 + 2nxy - y^2| \geq \frac{n}{2}$.

Lemma 1. *Consider the lattice $\Lambda = (1,0)\mathbb{Z} \oplus (\frac{1}{2}, \frac{1}{2})\mathbb{Z}$ in $\mathbb{R}^2$. Then for every $(r,s) \in \mathbb{R}^2$ there exists a lattice point $(e,f) \in \Lambda$ such that $|r-e| + |s-f| \leq \frac{1}{2}$.*

This lemma is verified by sketching the fundamental domain of Λ.

Applying Lemma 1 to the 'y-coordinate' of our 4-dimensional lattice we see that, by subtracting appropriate multiples of θ and γ we can find a translate of ξ such that $|c| + |d| \leq \frac{1}{2}$; subtracting multiples of 1 and i we can make $|a|, |b| \leq \frac{1}{2}$. This gives at once $|x|^2 = a^2 + b^2 \leq \frac{1}{2}$ and $|y|^2 = c^2 + d^2 \leq (|c| + |d|)^2 \leq \frac{1}{4}$. Thus, if ξ is k-exceptional, we must have

$$\frac{n}{2} \leq |x^2 + 2nxy - y^2| \leq |x|^2 + 2n|xy| + |y|^2 \leq \frac{1}{2} + n|x| + \frac{1}{2} = n|x| + \frac{1}{4}.$$

This implies that $|x| \geq \frac{1}{2} - \frac{3}{4n}$.

Similarly we can obtain $|a| + |b| \leq \frac{1}{2}$ and $|c|, |d| \leq \frac{1}{2}$, and the same computation shows that any exceptional point ξ must satisfy $|y| \geq \frac{1}{2} - \frac{3}{4n}$.

Now the only subsets of F which can possibly contain exceptional points are

$$\begin{array}{rcll} S_1 & = & (0, \frac{1}{2}, \frac{1}{2}, 0) + [-\delta, \delta] \times [-\delta, \delta] \times [-\delta, \delta] \times [-\delta, \delta] & \text{and} \\ S_2 & = & (\frac{1}{2}, 0, \frac{1}{2}, 0) + [-\delta, \delta] \times [-\delta, \delta] \times [-\delta, \delta] \times [-\delta, \delta] & \end{array}$$

(observe that $(0, \frac{1}{2}, \frac{1}{2}, 0) \equiv (\frac{1}{2}, 0, 0, \frac{1}{2}) \bmod \mathcal{O}$).

Next we claim that $(\frac{1}{2}, 0, \frac{1}{2}, 0)$ is the only possible k-exceptional point contained in S_2.

These bounds allow the application of [4, Thm. 3], and we find that $\xi_1 = \frac{1}{2}(i+\theta)$ and $\xi_2 = \frac{1}{2}(1+\theta)$ are the only possible exceptional points of F. Moreover, $N(\xi_1) = \frac{m}{4}$ and $N(\xi_2) = \frac{m-1}{4}$ show that $M(K) \leq M(\xi, K) = \frac{m}{4}$ and $M_2(K) \leq \frac{m-1}{4}$

In order to prove that $M(\xi, K) \geq \frac{m}{4}$ we assume that $a, b, c, d \in \mathbb{Q}$ satisfy the congruences $a \equiv d \equiv 0, b \equiv c \equiv \frac{1}{2} \bmod \mathbb{Z}$. Putting $x = a + bi$ and $y = c + di$ we find the congruences

$$\begin{array}{rcll} 2xy & \equiv & 2(ac - bd) + 2(ad + bc)i & \equiv \frac{i}{2} \bmod \mathbb{Z}[i], \quad \text{and} \\ x^2 - y^2 & \equiv & a^2 - b^2 - c^2 + d^2 + 2(ab - cd)i & \equiv \frac{1}{2} \bmod \mathbb{Z}[i]. \end{array}$$

Thus $|\mathrm{Re}\,(x^2 + 2nxy - y^2)| \geq \frac{1}{2}$ and $|\mathrm{Im}\,(x^2 + 2nxy - y^2)| \geq \frac{n}{2}$, hence $N(\xi - \alpha) \geq \frac{1}{4}(1 + n^2) = \frac{m}{4}$ for all $\alpha \in \mathcal{O}$. This proves our claim for all $n \geq 7$; for $n = 1, 3, 5$ it is verified by computer. $\square$

References

[1] E.S. Barnes, H.P.F. Swinnerton-Dyer, *The inhomogeneous minima of binary quadratic forms I*, Acta Math. **87** (1952), 259–323 1

[2] E.S. Barnes, H.P.F. Swinnerton-Dyer, *The inhomogeneous minima of binary quadratic forms II*, Acta Math. **88** (1952), 279–316 1

[3] J. W. S. Cassels, *The inhomogeneous minima of binary quadratic, ternary cubic, and quaternary quartic forms*, Proc. Cambridge Phil. Soc. **48** (1952), 519–520 1

[4] S. Cavallar, F. Lemmermeyer, *The Euclidean algorithm in cubic number fields*, Proc. Number Theory Eger 1996 (1998), 123–146 6, 7

[5] V. Cioffari, *The Euclidean condition in pure cubic and complex quartic fields*, Math. Comp. **33** (1979), 389–398

[6] R. B. Lakein, *Euclid's algorithm in complex quartic fields*, Acta Arithm. **20** (1972) 393–400 2 6

[7] F. Lemmermeyer, *Euklidische Ringe*, Diplomarbeit Univ. Heidelberg, 1989

[8] F. Lemmermeyer, *The Euclidean Algorithm in Algebraic Number Fields*, Expo. Math. **13** (1995), 385–416 1, 6

[9] F. J. van der Linden, *Euclidean rings of integers of fourth degree fields*, Lecture notes in Math. **1068** (1983), 139–148 1

[10] J. Sauvageot, *Algorithmes d'Euclide dans certains corps biquadratiques*, Sem. Delange-Pisot-Poitou (1972/73) 1

Bilkent University, Department of Mathematics, 06533 Bilkent, Ankara, Turkey
E-mail address: franz@fen.bilkent.edu.tr