Mathematisch Instituut
Roetersstraat 15
Amsterdam-C. The Netherlands

EUCLIDEAN NUMBER FIELDS OF LARGE DEGREE

by H.W. Lenstra, Jr.

Report 76-09

May 1976
Second edition: March 1977

Euclidean number fields of large degree.

H.W. Lenstra, Jr.

Abstract.- It is shown that a number field is Euclidean if it contains many elements all of whose differences are units. Numerous examples of degrees four , five, six, seven and eight are given.

Key words: Euclid's algorithm, algebraic number fields, packing theory.

AMS-MOS subject classification scheme (1970): 12A45, 13F10, 52A45.

Euclidean number fields of large degree.

H.W. Lenstra, Jr.

Introduction.

Let K be a number field, and let R be the ring of algebraic integers in K. We say that K is Euclidean, or that R is Euclidean with respect to the norm, if for every $a, b \in R$, $b \neq 0$, there exist $c, d \in R$ such that $a = cb + d$ and $N(d) < N(b)$. Here N denotes the absolute value of the field norm $K \to \mathbf{Q}$.

This paper deals with a new technique of proving fields to be Euclidean. The method, which is related to an old idea of Hurwitz [14], is based on the observation that for K to be Euclidean it suffices that R contains many elements all of whose differences are units; see section 1 for details. Some remarks about the existence of such elements are made in section 2. In section 3 we illustrate the method by giving 132 new examples of Euclidean fields of degrees four, five, six, seven and eight. A survey of the known Euclidean fields is given in section 4.

Acknowledgements are due to B. Matzat for making available [1] and [23]; to E.M. Taylor for communicating to me the results of [35]; and to P. van Emde Boas, A.K. Lenstra and R.H. Mak for their help in computing discriminants.

§1. A sufficient condition for Euclid's algorithm.

In this section K denotes an algebraic number field of finite degree n and discriminant Δ over the field of rational numbers $\mathbb{Q}$. By r and s we mean the number of real and complex archimedean primes of K, respectively. The ring of algebraic integers in K is denoted by R. We regard K as being embedded in the $\mathbb{R}$-algebra $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$, which, as an $\mathbb{R}$-algebra, is isomorphic to $\mathbb{R}^r \times \mathbb{C}^s$. As an $\mathbb{R}$-vector space we identify $\mathbb{C}$ with $\mathbb{R}^2$ by sending $a + bi$ to $(a + b, a - b)$, for $a, b \in \mathbb{R}$. This leads to an identification of $K_{\mathbb{R}} = \mathbb{R}^r \times \mathbb{C}^s$ with the n-dimensional Euclidean space $\mathbb{R}^n$. It is well known that this identification makes R into a lattice of determinant $|\Delta|^{\frac{1}{2}}$ in $\mathbb{R}^n$.

The function $N: \mathbb{R}^r \times \mathbb{C}^s \to \mathbb{R}$ is defined by

$$(1.1) \qquad N(x) = \prod_{j=1}^{r} |x_j| \cdot \prod_{j=r+1}^{r+s} |x_j|^2, \qquad \text{for } x = (x_j)_{j=1}^{r+s} \in \mathbb{R}^r \times \mathbb{C}^s.$$

The restriction of N to K is just the absolute value of the field norm $K \to \mathbb{Q}$.

Writing R^* for the group of units of R, we define

$$(1.2) \qquad M = \sup\{m \mid \text{there exist } \omega_1, \omega_2, \ldots, \omega_m \in R \text{ such that } \omega_i - \omega_j \in R^* \text{ for all } i, j,\ 1 \le i < j \le m\}.$$

In section 2 we shall see that M is finite.

We recall some notions from packing theory, referring to Rogers's book [32] for precise definitions. Let $U \subset \mathbb{R}^n$ be a bounded Lebesgue measurable set with positive Lebesgue measure $\mu(U)$. If $(a_i)_{i=1}^{\infty}$ is a sequence of points in $\mathbb{R}^n$ which is sufficiently regularly distributed throughout the space, then with the system $\mathcal{U} = (U + a_i)_{i=1}^{\infty}$ of translates of U we can associate a <u>density</u>, denoted by $\rho(U)$. It may be described as the limiting ratio of the sum of the measures of those sets of the system $\mathcal{U}$, which intersect a large cube, to the measure of the cube, as it becomes infinitely large. The system $\mathcal{U} = (U + a_i)_{i=1}^{\infty}$ is called

a packing of U if $(U + a_i) \cap (U + a_j) = \emptyset$ for all $i, j, i \neq j$. The packing constant $\delta(U)$ of U is defined by

$$\delta(U) = \sup_{\mathcal{U}} \rho(\mathcal{U}),$$

the supremum being over all the packings $\mathcal{U}$ of U for which $\rho(\mathcal{U})$ is defined. The centre packing constant $\delta^*(U)$ of U is defined by

(1.3) $\quad \delta^*(U) = \delta(U)/\mu(U),$

cf. [17, sec. 3.1].

(1.4) Theorem. Let K be an algebraic number field of degree n and discriminant Δ over $\mathbb{Q}$, and let N and M be defined by (1.1) and (1.2). Further, let $U \subset \mathbb{R}^n$ be a bounded Lebesgue measurable set with positive Lebesgue measure, having the property

(1.5) $\quad N(u - v) < 1 \quad$ for all $u, v \in U,$

and let $\delta^*(U)$ denote its centre packing constant, defined by (1.3). With these notations, K is Euclidean if the inequality

(1.6) $\quad M > \delta^*(U) \cdot |\Delta|^{\frac{1}{2}}$

is satisfied.

Proof. For any $a, b \in R$, $b \neq 0$, we must find $c, d \in R$ such that $a = cb + d$ and $N(d) < N(b)$. Writing $x = a/b$ we see that it suffices to find an element $c \in R$ with $N(x - c) < 1$.

By (1.6) and (1.2) there exists a sequence $\omega_1, \omega_2, \ldots, \omega_m$ of elements of R such that

$$\omega_i - \omega_j \in R^*, \quad \text{for all } i, j, 1 \leq i < j \leq m,$$
$$m > \delta^*(U) \cdot |\Delta|^{\frac{1}{2}}.$$

The latter inequality is, by (1.3), equivalent to

(1.7) $\quad m \cdot \mu(U)/|\Delta|^{\frac{1}{2}} > \delta(U).$

Consider the system

$$\mathcal{U} = (U + \omega_i x + \alpha)_{1 \le i \le m,\ \alpha \in R}$$

of translates of U. Using [32, theorem 1.5] we find that its density is given by

$$\rho(\mathcal{U}) = m \cdot \mu(U) / |\Delta|^{\frac{1}{2}}$$

so (1.7) tells us that

$$\rho(\mathcal{U}) > \delta(U).$$

By the definition of $\delta(U)$, this implies that the system $\mathcal{U}$ is not a packing of U, so there are different pairs (i, α) and (j, β), with $1 \le i, j \le m$ and $\alpha, \beta \in R$, such that $(U + \omega_i x + \alpha) \cap (U + \omega_j x + \beta) \neq \emptyset$, say

$$u + \omega_i x + \alpha = v + \omega_j x + \beta \qquad (u, v \in U).$$

If $i = j$, then $\beta - \alpha = u - v$, and (1.5) gives $N(\beta - \alpha) < 1$. Since $\beta - \alpha$ is an algebraic integer, this is only possible if $\beta - \alpha = 0$, contradicting that the pairs (i, α) and (j, β) are different. Therefore $i \neq j$, so $\omega_i - \omega_j$ is a unit and $N(\omega_i - \omega_j) = 1$. Put $c = (\beta - \alpha)/(\omega_i - \omega_j)$. Then c belongs to R, and

$$N(x - c) = N((u - v)/(\omega_j - \omega_i)) = N(u - v) < 1,$$

as required. This concludes the proof of theorem (1.4).

A slight modification of the argument shows that, under the condition (1.6), the inhomogeneous minimum of N with respect to R (cf. [19, sec. 46]) does not exceed $\delta^*(U) \cdot |\Delta|^{\frac{1}{2}}/M$.

(1.8) Corollary. Let K be an algebraic number field of degree n and discriminant Δ over $\mathbb{Q}$, having precisely s complex archimedean primes. Suppose that the number M defined by (1.2) satisfies the inequality

$$(1.9) \qquad M > \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot |\Delta|^{\frac{1}{2}}.$$

Then K is Euclidean.

Proof. We apply (1.4) with

$$U = \{(x_j)_{j=1}^{r+s} \in \mathbb{R}^r \times \mathbb{C}^s \mid \sum_{j=1}^{r} |x_j| + 2 \sum_{j=r+1}^{r+s} |x_j| < \tfrac{1}{2}n\}.$$

The verification of condition (1.5) consists of a direct application of the arithmetic-geometric mean inequality, which we leave to the reader. A classical computation shows that

$$\mu(U) = \frac{n^n}{n!} \cdot \left(\frac{\pi}{4}\right)^s,$$

cf. [16, Ch. V, lemma 3] (the discrepancy by a factor of 2^s is caused by the difference in identifying $\mathbb{C}$ with $\mathbb{R}^2$). Thus, (1.8) is an immediate consequence of (1.4) and the inequality

$$\delta(U) \leq 1$$

which is generally valid [32, theorem 1.3]. This proves (1.8).

Let S be a regular n-simplex in $\mathbb{R}^n$, with edge length 2. Denoting by T the subset consisting of all points in S with distance ≤ 1 from some vertex of S, we define

$$\sigma_n = \mu(T)/\mu(S). \tag{1.10}$$

(1.11) Corollary. Let K be an algebraic number field of degree n and discriminant Δ over $\mathbb{Q}$, and suppose that

$$M > \sigma_n \cdot \frac{\Gamma(1 + \frac{1}{2}n)}{\pi^{n/2}} \cdot \left(\frac{4}{n}\right)^{n/2} \cdot |\Delta|^{\frac{1}{2}}. \tag{1.12}$$

Here M and σ_n are defined by (1.2) and (1.10), respectively. Then K is Euclidean.

Proof. We apply (1.4) with

$$U = \{(x_j)_{j=1}^{r+s} \in \mathbb{R}^r \times \mathbb{C}^s \mid \sum_{j=1}^{r} x_j^2 + 2 \sum_{j=r+1}^{r+s} |x_j|^2 < \tfrac{1}{4}n\}.$$

Our identification of $\mathbb{R}^r \times \mathbb{C}^s$ with $\mathbb{R}^n$ makes U into an n-dimensional sphere of radius $\frac{1}{2}\sqrt{n}$:

$$U = \{(y_j)_{j=1}^{n} \in \mathbb{R}^n \mid \sum_{j=1}^{n} y_j^2 < \tfrac{1}{4}n\}.$$

Property (1.5) is again a simple consequence of the arithmetic-geometric mean inequality. The measure of U is given by

$$\mu(U) = \left(\frac{n}{4}\right)^{n/2} \cdot \frac{\pi^{n/2}}{\Gamma(1 + \frac{1}{2}n)}$$

and a theorem of Rogers [32, theorem 7.1] asserts that

$$\delta(U) \leq \sigma_n .$$

Corollary (1.11) is now immediate from (1.4).

Table 1 gives approximate values of $\sigma_n \cdot \Gamma(1 + \frac{1}{2}n)/\pi^{n/2}$ for $1 \leq n \leq 12$. For $n \leq 2$ the tabulated value is exact; for $n > 2$ the table gives an upper bound exceeding the exact value by at most 10^{-5}. The table is derived from a similar table of lower bounds computed by J. Leech [18].

n		n	
1	0.5	7	0.06982
2	$\sqrt{3}/6$	8	0.06327
3	0.18613	9	0.06008
4	0.13128	10	0.05954
5	0.09988	11	0.06137
6	0.08113	12	0.06560

Table 1. Upper bounds for $\sigma_n \cdot \Gamma(1 + \frac{1}{2}n)/\pi^{n/2}$.

Straightforward computations show that (1.11) is to be preferred to (1.8) if

(1.13) $n = 2, \quad s = 1 \quad$ or $\quad 4 \leq n \leq 7, \quad s \geq 2 \quad$ or $\quad 8 \leq n \leq 12, \quad s \geq 3$

and that (1.8) is sharper in all other cases with $2 \leq n \leq 12$. Applying Stirling's formula and Daniels's asymptotic formula:

(1.14) $$\sigma_n \sim \frac{n}{e} \cdot 2^{-n/2} \qquad (n \to \infty)$$

(cf. [32, Ch. 7, sec. 5]) one finds that (1.11) is superior to (1.8) for all

sufficiently large n, regardless of the value of s; probably $n \geq 30$ suffices. But the significance of this statement is doubtful, since in the next section we shall see that on the assumption of the generalized Riemann hypothesis the inequality (1.12) is satisfied for only finitely many number fields K, up to isomorphism.

We generalize theorem (1.4) by considering multiple packings. We fix an integer $k \geq 1$.

As before, let $U \subset \mathbf{R}^n$ be a bounded Lebesgue measurable set with positive Lebesgue measure $\mu(U)$. A system $\mathcal{U} = (U + a_i)_{i=1}^{\infty}$, with $a_i \in \mathbf{R}^n$, is called a k-fold packing of U if for every system of $k+1$ different positive integers $(h(0), h(1), \ldots, h(k))$ the intersection

$$(U + a_{h(0)}) \cap (U + a_{h(1)}) \cap \ldots \cap (U + a_{h(k)})$$

is empty. The k-fold packing constant $\delta_k(U)$ of U is defined by

$$\delta_k(U) = \sup_{\mathcal{U}} \rho(\mathcal{U}),$$

the supremum being over all the k-fold packings $\mathcal{U}$ of U for which $\rho(\mathcal{U})$ is defined. Further let

$$\delta_k^*(U) = \delta_k(U)/\mu(U). \tag{1.15}$$

Clearly, $\delta_1(U) = \delta(U)$ and $\delta_1^*(U) = \delta^*(U)$.

Returning to the algebraic number field K we define

$$M_k = \sup\{m \mid \text{there exist } \omega_1, \omega_2, \ldots, \omega_m \in R \text{ such that among any } k+1 \text{ distinct indices } h(0), h(1), \ldots, h(k) \in \{1, 2, \ldots, m\} \text{ there are two, } h(i) \text{ and } h(j) \text{ (say), such that } \omega_{h(i)} - \omega_{h(j)} \in R^*\}. \tag{1.16}$$

Notice that it is not required that the ω_i are different. In (2.7) we shall see that M_k is finite. Clearly, $M_1 = M$.

(1.17) Theorem. Let K be an algebraic number field of degree n and discriminant Δ over $\mathbb{Q}$, and let $U \subset \mathbf{R}^n$ be a bounded Lebesgue measurable set with positive Lebesgue measure satisfying (1.5). Further, let $\delta_k^*(U)$ and M_k, for $k \in \mathbb{Z}$, $k \geq 1$, be defined by (1.15) and (1.16). With these notations, K is Euclidean if the inequality

$$M_k > \delta_k^*(U) \cdot |\Delta|^{\frac{1}{2}}$$

is satisfied for some integer $k \geq 1$.

Proof. The proof of (1.17) is completely similar to the proof of (1.4) and is left to the reader.

(1.18) Corollary. Let K be an algebraic number field of degree n and discriminant Δ over $\mathbb{Q}$, having precisely s complex archimedean primes. Suppose that for some integer $k \geq 1$ the number M_k defined by (1.16) satisfies the inequality

$$M_k > k \cdot \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot |\Delta|^{\frac{1}{2}}.$$

Then K is Euclidean.

Proof. Choose U as in the proof of (1.8) and use the trivial upper bound $\delta_k(U) \leq k$. This proves (1.18).

The methods of this section apply to a wider class of rings. For example, they can be used to prove a quantitative version of O'Meara's theorem, stating that for any algebraic number field K there exists $a \in R$, $a \neq 0$, such that $R[a^{-1}]$ is Euclidean with respect to a natural generalization of the norm map, cf. [28, 31, 22]. Replacing packing theory by Riemann-Roch's theorem one obtains similar results on rings of affine curves over arbitrary fields of constants, cf. [22].

§2. Estimates for M.

The notations of section 1 are preserved. We define L to be the smallest norm of a proper ideal of R:

(2.1) $\quad L = \min\{\#(R/I) \mid I \subset R \text{ is an ideal, } I \neq R\}.$

Clearly, L is a prime power.

(2.2) Proposition. We have $2 \leq M \leq L \leq 2^n$.

Proof. The sequence 0, 1 shows $M \geq 2$, and consideration of the ideal $I = 2R$ leads to $L \leq 2^n$. To prove $M \leq L$, let $\omega_1, \omega_2, \ldots, \omega_m$ be any sequence of elements of R as in (1.2), and let $I \subset R$ be any ideal different from R. Then I does not contain any of the units $\omega_i - \omega_j$, $1 \leq i < j \leq m$, so the elements $\omega_1, \ldots, \omega_m$ are pairwise incongruent modulo I. Therefore $m \leq \#(R/I)$, which implies that $M \leq L$. This proves (2.2).

We use (2.2) to show that no infinite sequence of Euclidean fields can be expected to result from (1.8) or (1.11). For bounded n this is a consequence of Hermite's theorem [16, Ch. V, theorem 5], so by the remark following (1.14) we need only consider fields satisfying (1.12). For these fields, (1.12) and (2.2) imply

$$|\Delta| < \frac{\pi^n \cdot n^n}{\Gamma(1 + \frac{1}{2}n)^2 \cdot \sigma_n^{\,2}}.$$

Using Stirling's formula and Daniels's formula (1.14) we obtain

$$|\Delta|^{1/n} < 4\pi e + o(1) \qquad (n \to \infty),$$

where $4\pi e = 34.1589..$. On the other hand, Serre [30] has shown on the assumption of the generalized Riemann hypothesis (GRH), that

$$|\Delta|^{1/n} > 8\pi e^{\gamma} + o(1) \qquad (n \to \infty)$$

with $8\pi e^{\gamma} = 44.7632..$ (γ is Euler's constant). Thus, assuming GRH, we conclude that n is bounded and that (1.12) holds for only finitely many number fields K, up to isomorphism. Without any unproven hypothesis,

Odlyzko [30] has shown that

$$|\Delta|^{1/n} > e^{r/n} \cdot 4\pi e^{\gamma} + o(1) \qquad (n \to \infty).$$

While this result does not allow us to draw the same conclusion unconditionally, it does handle the totally real case ($r = n$, $s = 0$). More precisely, it follows that for every $\varepsilon > 0$ we have $r/n < 1 - \gamma + \varepsilon$ for almost all K satisfying (1.12); here $1 - \gamma = 0.42278\ldots$.

It remains undecided whether there exists a better upper bound for M, in terms of n alone, than the bound 2^n implied by (2.2). In (3.1) and (3.3) we shall encounter fields K of arbitrarily large degree for which $M > n$.

From (2.2) it follows that (1.6) can only be satisfied if

$$L > \delta^*(U) \cdot |\Delta|^{\frac{1}{2}} \tag{2.3}$$

(with U as in (1.4)). It is curious to notice that (2.3) already implies that K has class number one, since by a classical argument every ideal class contains an integral ideal of norm at most $\delta^*(U) \cdot |\Delta|^{\frac{1}{2}}$.

Using a multiple packing argument one can establish the following lower bound for M:

$$M \geq L \Big/ \left(\frac{n!}{n^n} \cdot \left(\frac{4}{\pi} \right)^s \cdot |\Delta|^{\frac{1}{2}} \right).$$

Its practical value is limited.

We show that for a given number field the constant M can be effectively determined. Replacing a sequence $(\omega_i)_{i=1}^m$ as in (1.2) by $((\omega_i - \omega_1)/(\omega_2 - \omega_1))_{i=1}^m$, we see that it suffices to consider only sequences for which $\omega_1 = 0$ and $\omega_2 = 1$. Then for $3 \leq j \leq m$ both ω_j and $1 - \omega_j$ are units. In the terminology of Nagell [26] this means that $\omega_3, \ldots, \omega_m$ are <u>exceptional</u> units. Let E be the set of exceptional units:

$$E = \{\varepsilon \in R^* \mid 1 - \varepsilon \in R^*\}.$$

Both Chowla [4] and Nagell [24] proved that E is finite. In fact, the set E can be effectively determined by Baker's methods [12, lemme 4], and it is

clear that a search among the subsets of E suffices to determine M.

The hard step in this procedure is the determination of E by Baker's methods. It has not yet been carried out for a single algebraic number field. For a few fields classical diophantine techniques have been applied to determine E, cf. [25, 26, 36], (3.3), (3.9-11). A substantial portion of E can often be detected by starting from a few exceptional units and applying the following rules:

$$\varepsilon \in E \Rightarrow 1 - \varepsilon \in E, \quad \varepsilon^{-1} \in E;$$

$$\varepsilon, \eta, \varepsilon\eta^{-1} \in E \Rightarrow (1 - \varepsilon)/(1 - \eta) \in E;$$

$$\varepsilon \in E \Rightarrow \sigma\varepsilon \in E \text{ for every automorphism } \sigma \text{ of } K.$$

Most of the examples given in section 3 rely on the following proposition.

(2.4) Proposition. Let x be an element of R, and denote by f its irreducible polynomial over $\mathbb{Q}$. Further, let ζ_m denote a primitive m-th root of unity and let θ be a zero of $X^2 - X - 1$. We then have:

(a) $M \geq 3$ if $f(0)$ and $f(1)$ are both ± 1;

(b) $M \geq 4$ if each one of $f(0)$, $f(1)$ and $f(-1)$ equals ± 1;

(c) $M \geq 5$ if each one of the algebraic integers $f(0)$, $f(1)$, $f(\zeta_6)$ is a unit;

(d) $M \geq 5$ if each one of the algebraic integers $f(0)$, $f(1)$, $f(-1)$, $f(\theta)$ is a unit;

(e) $M \geq 6$ if each one of the algebraic integers $f(0)$, $f(1)$, $f(-1)$, $f(\zeta_3)$, $f(\zeta_4)$ is a unit;

(f) $M \geq 6$ if each one of the algebraic integers $f(0)$, $f(1)$, $f(-1)$, $f(\theta)$, $f(-\theta)$ is a unit.

Proof. In the cases (a), (b), (c), (d), (e), (f) consider the sequences

$$0, 1, x,$$

$$0, 1, x, x + 1,$$

$0, 1, x, 1/(1-x), (x-1)/x,$

$0, 1, x, x+1, x^2,$

$0, 1, x, x^2, x^3, x^4,$

$0, 1, x, x+1, x^2, x^2+x,$

respectively. That, in each case, the sequence satisfies the requirement in the definition of M is a consequence of lemma (2.5), applied to $g = X$, $X - 1$, $X + 1$, $X^2 - X + 1$, $X^2 - X - 1$, $X^2 + X + 1$, $X^2 + 1$ and $X^2 + X - 1$.

(2.5) Lemma. Let $f, g \in \mathbb{Z}[X]$ be irreducible polynomials with leading coefficient 1, and let x and y be zeros of f and g, respectively. Then $f(y)$ is a unit if and only if $g(x)$ is a unit.

Proof. Suppose that $g(x)$ is a unit. Then $g(x)^{-1}$ is integral over $\mathbb{Z}$, which easily implies

$$g(x)^{-1} \in \mathbb{Z}[g(x)] \subset \mathbb{Z}[x].$$

Thus, there exists a polynomial $h_1 \in \mathbb{Z}[X]$ such that $h_1(x) \cdot g(x) = 1$, i.e.

$$h_1 \cdot g + h_2 \cdot f = 1$$

for some $h_2 \in \mathbb{Z}[X]$. Substituting y for X we find $h_2(y) \cdot f(y) = 1$, so $f(y)$ is a unit. This proves the if-part, and the converse follows by symmetry. This finishes the proof of (2.4) and (2.5).

A second fruitful method to estimate M is given by the following trivial result.

(2.6) Proposition. Writing $M(K)$ for M, we have $M(K) \geq M(K_0)$ for every subfield K_0 of K.

Some of the above results can be extended to the numbers M_k. For example, (2.2) generalizes to

(2.7) $\quad 2k \leq k \cdot M_1 \leq M_k \leq k \cdot L \qquad (k \geq 1).$

As before, it follows that (1.18) cannot be expected to yield infinitely many Euclidean fields.

I do not know whether the numbers M_k, for $k \geq 2$, can be effectively determined for a given algebraic number field.

§3. Examples.

This section contains 132 new examples of Euclidean fields; 128 of these are given in tabular form, and the other four can be found in (3.3), (3.5), (3.11) and (3.17).

Cyclotomic fields. We denote by ζ_m a primitive m-th root of unity.

(3.1) Let p be a prime number, and let $q > 1$ be a power of p. Then the field $K = \mathbb{Q}(\zeta_q)$ has $L = p$, and consideration of the sequence $(\omega_i)_{i=1}^{p}$, $\omega_i = (\zeta_p{}^i - 1)/(\zeta_p - 1)$, shows $M \geq p$, so (2.2) implies $M = p$. For $q = p = 2, 3, 5, 7, 11$ the right hand side of (1.12) is approximately equal to 1, 1, 1.47, 3.12, 29.61, respectively. This gives new proofs that $\mathbb{Q}(\zeta_5)$ and $\mathbb{Q}(\zeta_7)$ are Euclidean. The method does not handle $\mathbb{Q}(\zeta_{11})$, which is known to be Euclidean [20].

(3.2) Let $K = \mathbb{Q}(\zeta_m)$, where m is any integer ≥ 1. Then $M \geq p$ for any prime p dividing m, by (2.6) and (3.1). Further, $M \geq 1 + \frac{m}{q}$, where q is the largest prime power dividing m; this follows by considering the sequence $0, 1, \zeta_m, \zeta_m{}^2, \ldots, \zeta_m{}^{(m/q)-1}$. Applying (1.11) we find the known Euclidean fields $\mathbb{Q}(\zeta_{12})$ (for which in fact $M \geq 2$ suffices) and $\mathbb{Q}(\zeta_{15})$, cf. [20].

(3.3) Let p be an odd prime number and $K = \mathbb{Q}(\zeta_p) \cap \mathbf{R} = \mathbb{Q}(\zeta_p + \zeta_p{}^{-1})$. Then $L = p$, except if p is a Fermat prime, in which case $L = p - 1$. The sequence $(\omega_i)_{i=1}^{(p+1)/2}$ defined by

$$\omega_i = \sum_{-i<j<i} \zeta_p{}^j$$

shows that $M \geq (p + 1)/2$. The right hand side of (1.9) is for $p = 3, 5, 7, 11, 13, 17$ approximately equal to 1, 1.12, 1.56, 4.65, 9.40, 48.68, respectively. This yields a new proof that for $p \leq 11$ the field $\mathbb{Q}(\zeta_p + \zeta_p{}^{-1})$ is Euclidean, cf. [10] for $p = 11$. For $p = 13$ we can sharpen $M \geq 7$ to $M \geq 11$ by considering the sequence

$$0, 1, \rho_2{}^{-1}, -\rho_4, -\rho_5{}^{-1}, -\rho_1\rho_4, -\rho_2{}^{-1}\rho_4, (\rho_1\rho_2)^{-1}, -(\rho_2\rho_5)^{-1}, \rho_2\rho_4{}^2, -\rho_1\rho_2\rho_4$$

where $\rho_i = \zeta_{13}^{\,i} + \zeta_{13}^{\,-i}$. Thus we obtain the new Euclidean field $\mathbb{Q}(\zeta_{13} + \zeta_{13}^{\,-1})$. It has $n = 6$, $r = 6$, $s = 0$ and $\Delta = 13^5 = 371293$.

The precise value of M remains open. Clearly $M = L$ for $p = 3$, and in (3.9) we shall see that the same holds for $p = 5$. In the case $p = 7$ all exceptional units have been determined by Nagell [26], and his results imply that $M = L = 7$; in fact, writing $\eta_i = \zeta_7^{\,i} + \zeta_7^{\,-i}$ we have $M \geq 7$ because of the sequence

(3.4) $\quad 0, \quad 1, \quad \eta_1, \quad 1 + \eta_1, \quad 1 + \eta_1 + \eta_2, \quad 2 + \eta_2, \quad 2 + \eta_1 + \eta_2.$

In the same way one proves that also for $p = 11$ one has $M \geq 7$.

(3.5) The field $K = \mathbb{Q}(\zeta_7 + \zeta_7^{\,-1}, \zeta_5 + \zeta_5^{\,-1})$ has $n = r = 6$, $s = 0$, $\Delta = 5^3 \cdot 7^4 = 300125$ and $L = 29$. It is known to be the totally real sextic field with the smallest discriminant [29]. The right hand side of (1.9) is about 8.454, so by (1.8) and (1.18) the field K is Euclidean if $M_1 \geq 9$ or $M_2 \geq 17$. Writing $\eta_i = \zeta_7^{\,i} + \zeta_7^{\,-i}$ and $\theta = -\zeta_5 - \zeta_5^{\,-1}$ we see, by adjoining θ as an eighth member to the sequence (3.4), that $M_1 \geq 8$:

(3.6) $\quad 0, \quad 1, \quad \eta_1, \quad 1 + \eta_1, \quad 1 + \eta_1 + \eta_2, \quad 2 + \eta_2, \quad 2 + \eta_1 + \eta_2, \quad \theta.$

I do not know whether $M_1 \geq 9$; a near miss is provided by

(3.7) $\quad 1 + \theta$

which differs from each of the numbers (3.6) except η_1 by a unit. Replace the non-zero elements in (3.6), (3.7) by their inverses, and apply the field automorphism sending η_1 to itself and θ to $-\theta^{-1}$. Then we obtain another sequence showing $M_1 \geq 8$:

(3.8) $\quad 0, \quad 1, \quad \eta_1^{-1}, \quad (1 + \eta_1)^{-1}, \quad (1 + \eta_1 + \eta_2)^{-1}, \quad (2 + \eta_2)^{-1}, \quad (2 + \eta_1 + \eta_2)^{-1}, \quad -\theta$

and since $1 + \theta$ is replaced by itself we conclude that it differs by a unit from each of (3.8) except η_1^{-1}. We claim that the sequence $(\omega_i)_{i=1}^{17}$ obtained by juxtaposition of (3.6), (3.7) and (3.8) shows $M_2 \geq 17$. To prove this, let ω_h, ω_i, ω_j be three members from this sequence; we must show that at least one of $\omega_h - \omega_i$, $\omega_h - \omega_j$, $\omega_i - \omega_j$ is a unit. If two

of ω_h, ω_i, ω_j both belong to (3.6) or both belong to (3.8) this is clear. So we may assume that ω_h is among (3.6), that $\omega_i = 1 + \theta$, and that ω_j is among (3.8). Then $\omega_h - \omega_i$ is a unit except if $\omega_h = \eta_1$, and similarly $\omega_i - \omega_j$ is a unit except if $\omega_j = \eta_1^{-1}$. Finally, if $\omega_h = \eta_1$ and $\omega_j = \eta_1^{-1}$ then $\omega_h - \omega_j$ is a unit. We conclude that $M_2 \geq 17$ and that K is Euclidean.

Fields of small unit rank. All exceptional units in the fields with $r + s \leq 2$ have been determined by Nagell, see [25] for references. The resulting information about M is collected in (3.9), (3.10) and (3.11).

(3.9) For quadratic K, we have $M = 3$ if $K = \mathbb{Q}(\zeta_3)$ (cf. (3.1)), $M = 4$ if $K = \mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$ (apply (2.4)(b) with $f = X^2 - X - 1$), and $M = 2$ in all other cases.

(3.10) If K is complex cubic, i.e., $n = 3$, $r = s = 1$, then $M = 5$ if $K = \mathbb{Q}(\alpha)$, $\alpha^3 - \alpha - 1 = 0$, $\Delta = -23$ (apply (2.4)(c) to $x = \alpha$), $M = 3$ if $K = \mathbb{Q}(\gamma)$, $\gamma^3 + \gamma - 1 = 0$, $\Delta = -31$ (apply (2.4)(a) to $x = \gamma$), and $M = 2$ in all other cases.

(3.11) For totally complex quartic K, i.e., $n = 4$, $r = 0$, $s = 2$, we have:

$M = 6$ if $K = \mathbb{Q}(\zeta_3, \beta)$, $\beta^2 + \zeta_3\beta - 1 = 0$, $\Delta = 117 = 3^2 \cdot 13$ (see below),

$M = 5$ if $K = \mathbb{Q}(\zeta_5)$, $\Delta = 125 = 5^3$ (see (3.1)),

$M = 4$ if $K = \mathbb{Q}(\zeta_{12})$, $\Delta = 144 = 2^4 \cdot 3^2$ (cf. (3.2)),

$M = 3$ if $K = \mathbb{Q}(\nu)$, $\nu^4 - \nu + 1 = 0$, $\Delta = 229$ (prime) (see below),

$M = 3$ if $K = \mathbb{Q}(\zeta_4, \xi)$, $\xi^2 - \xi - \zeta_4 = 0$, $\Delta = 272 = 2^4 \cdot 17$ (cf. (2.4)(a)),

and in all other cases

$M = 4$ if $\sqrt{5} \in K$,

$M = 3$ if $\sqrt{5} \notin K$, $\zeta_3 \in K$,

$M = 2$ if $\sqrt{5} \notin K$, $\zeta_3 \notin K$.

For the field $\mathbb{Q}(\zeta_3, \beta)$, $\beta^2 + \zeta_3\beta - 1 = 0$, a sequence showing $M \geq 6$ is given by 0, 1, β, β^2, $-\zeta_3$, $-\zeta_3\beta^{-1}$. The field with $\Delta = 229$ is a new

Euclidean field: by (2.2) and (2.4)(a) it has $M = 3$, while (1.11) only requires $M \geq 2$.

Explanation of the tables. In tables 2 to 9 one finds 128 new Euclidean fields obtained by means of (1.8) and (1.11). In the head of each table one finds n, r and s, and which one of (1.8), (1.11) is applied. Every row corresponds to a field K, represented as $K = K_0(x)$, where K_0 is a subfield of K. If n is composite, then a generator for K_0 is given in the second column; the symbols used are explained in table 10. If this subfield generator is 0, then K has only trivial subfields and $K_0 = \mathbb{Q}$. We also take $K_0 = \mathbb{Q}$ if n is a prime number. In the first column one finds the absolute value of the discriminant of K and its prime factorization. Further the table contains the coefficients $a_0, a_1, \ldots, a_m$ of the irreducible polynomial $a_0 + a_1X + \ldots + a_mX^m$ of x over K_0; here m is the degree of K over K_0. In the column headed "$M \geq$" one finds the lower bound for M required by (1.8) or (1.11) to prove that K is Euclidean. The final column mentions which of our results apply to prove this lower bound.

The fields in the tables have been found in three ways. First, the methods of section 2 were applied to the quartic fields listed by Godwin [6-8], the quintic fields given by Cohn [5, cf. 2] and Matzat [23], and the totally real and totally complex sextic fields listed by Biedermann and Richter [1]. Not all fields could be decided; for example, the field $K = \mathbb{Q}(x)$, $x^5 + x^3 - x^2 - x + 1 = 0$, with $n = 5$, $r = 1$, $s = 2$, $\Delta = 4897 = 59 \cdot 83$, has $M \geq 4$ by (2.4)(b), but the right hand side of (1.12) is about 4.001. The field has $L = 5$, and it remains undecided whether $M = 4$ or $M = 5$.

Secondly, many examples were found by considering extension fields of a given field K_0, and applying (2.6).

Our third approach consisted in constructing polynomials f satisfying

one of the conditions (a)-(f) of (2.4), and computing their discriminants on an electronic computer. Two programs were used, one written by P. van Emde Boas and one by A.K. Lenstra and R.H. Mak. Every irreducible f whose discriminant was found to be sufficiently small gave rise to a Euclidean field, by (2.4) and (1.8), (1.11). All fields in table 8 (degree 7) were discovered in this way. It occurred often that two polynomials had the same discriminant. These discriminants are listed only once. We did not test the corresponding fields for isomorphism.

Special fields. A few fields deserve special mention or require special treatment.

(3.12) The fields $\mathbb{Q}(\delta)$ and $\mathbb{Q}(\varepsilon)$, defined by table 10 and also occurring in table 2, have

$$\Delta = -283, \quad M \geq 6 \quad \text{(by (2.4)(e))}$$

and

$$\Delta = -331, \quad M = L = 5 \quad \text{(by (2.4)(c))},$$

respectively.

(3.13) The totally complex sextic fields with $\Delta = -12167$ and $\Delta = -29791$ occurring in table 5 are the Hilbert class fields of $\mathbb{Q}(\sqrt{-23})$ and $\mathbb{Q}(\sqrt{-31})$, respectively. There are two other fields in table 5 which are normal over $\mathbb{Q}$: the abelian field $\mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \zeta_3)$ with $\Delta = -64827$ and the class field over $\mathbb{Q}(\sqrt{-11})$ with conductor (2), having $\Delta = -21296$. It has $M \geq 4$ because of the sequence $0, 1, x, -\kappa x^2$, where $x^2 + \kappa x + 1 = 0$, $\kappa^3 + \kappa^2 - \kappa + 1 = 0$. The subfield $\mathbb{Q}(\kappa)$ has $n = 3$, $r = s = 1$ and $\Delta = -44$.

(3.14) The only other normal field in our tables is the Hilbert class field of $\mathbb{Q}(\sqrt{-39})$, with $\Delta = 2313441$, occurring in table 9. It can be written as $\mathbb{Q}(\zeta_3, \beta, x)$, with $\beta^2 + \zeta_3\beta - 1 = 0$, $x^2 + \zeta_3^2 x - 1 = 0$ (notice that β and x are conjugate over $\mathbb{Q}$), and it contains the field with $\Delta = -507$ occurring in table 2. The field has $M \geq 7$ because of the

sequence $0,\ 1,\ \beta,\ \beta^2,\ -\zeta_3,\ -\zeta_3\beta^{-1},\ -\zeta_3 x.$

(3.15) The field with $\Delta = 1890625$ occurring in table 9 is normal over $\mathbb{Q}(\zeta_5 + \zeta_5^{-1})$. It has $M \geq 6$ because of the sequence $0,\ 1,\ -\zeta_5 - \zeta_5^{-1},\ 1 - \zeta_5 - \zeta_5^{-1},\ 1 + \zeta_5^2,\ x,$ where $x^2 - x + (\zeta_5 + \zeta_5^{-1}) = 0.$

(3.16) The field with $\Delta = -21168$ occurring in table 5 has $M \geq 4$ because of $0,\ 1,\ 1 + \zeta_3,\ x,$ where $x^3 - \zeta_3 x^2 + (\zeta_3 - 1)x + 1 = 0.$

(3.17) Let $K = \mathbb{Q}(x)$, with $x^5 + 2x^4 + x^3 - x^2 - 3x - 1 = 0$. The field has $n = 5$, $r = 3$, $s = 1$, $-\Delta = 11119$ (prime), $L = 7$ and the right hand side of (1.9) is about 5.156. Thus, K is Euclidean if $M_1 \geq 6$ or $M_2 \geq 11$, by (1.18). I do not know whether $M_1 \geq 6$; but a sequence showing $M_2 \geq 12$ is given by

$$0,\ 1,\ x + 1,\ (x + 1)^2/x,\ x/(x + 1),$$
$$0,\ 1,\ (x + 1)^{-1},\ x/(x + 1)^2,\ (x + 1)/x,$$
$$x,\ x^{-1},$$

as can be verified by the method of (3.5). It follows that K is Euclidean.

Table 2.

$n = 4$, $r = 2$, $s = 1$; (1.8) is applied.

$-\Delta$	K_0	$a_0, a_1, \ldots, a_m$	$M \geq$	method
$275 = 5^2 \cdot 11$	θ	$-\theta, 1, 1$	2	(2.2)
283 (prime)	0	$-1, -1, 0, 0, 1$	3	(2.4)(a)
331 (prime)	0	$-1, 3, -2, 0, 1$	3	(2.4)(a)
$400 = 2^4 \cdot 5^2$	θ	$-\theta, 0, 1$	3	(2.6),(3.9)
$448 = 2^6 \cdot 7$	λ	$1, -\lambda, 1$	3	(2.4)(a)
$475 = 5^2 \cdot 19$	θ	$\theta, 1, 1$	3	(2.6),(3.9)
491 (prime)	0	$-1, 3, -1, -1, 1$	3	(2.4)(a)
$507 = 3 \cdot 13^2$	μ	$1, -\mu, 1$	3	(2.4)(a)
563 (prime)	0	$-1, -1, 1, -1, 1$	3	(2.4)(a)
643 (prime)	0	$-1, -3, 0, 2, 1$	4	(2.4)(b)
$775 = 5^2 \cdot 31$	θ	$1 - \theta, \theta, 1$	4	(2.6),(3.9)

Table 3.

$n = 5$, $r = 1$, $s = 2$; (1.11) is applied.

Δ	$a_0, a_1, a_2, a_3, a_4, a_5$	$M \geq$	method
1609 (prime)	-1, 1, 1, -1, 0, 1	3	(2.4)(a)
1649 = 17·97	-1, 1, 0, -1, 1, 1	3	(2.4)(a)
1777 (prime)	-1, 2, 1, -2, 0, 1	3	(2.4)(a)
$2209 = 47^2$	1, -2, 2, -1, 0, 1	3	(2.4)(a)
2297 (prime)	-1, 1, -1, 1, 0, 1	3	(2.4)(a)
2617 (prime)	-1, 0, -2, 1, 0, 1	3	(2.4)(a)
2665 = 5·13·41	-1, -2, 0, 1, 0, 1	3	(2.4)(a)
2869 = 19·151	-1, -1, 0, 0, 0, 1	4	(2.4)(b)
3017 = 7·431	1, 0, -1, 0, 0, 1	4	(2.4)(b)
3889 (prime)	-1, 1, -1, 0, -1, 1	4	(2.4)(c)
4417 = 7·631	-1, 2, -2, 1, 0, 1	4	(2.4)(c)
4549 (prime)	1, 1, -2, -2, 2, 1	4	(2.4)(b)

Table 4.

$n = 5$, $r = 3$, $s = 1$; (1.8) is applied.

$-\Delta$	$a_0, a_1, a_2, a_3, a_4, a_5$	$M \geq$	method
4511 = 13·347	-1, 0, 1, -2, 0, 1	4	(2.4)(b)
4903 (prime)	-1, 1, 1, -2, 1, 1	4	(2.4)(b)
5519 (prime)	-1, 1, 1, -3, 0, 1	4	(2.4)(b)
5783 (prime)	-1, 2, 1, -3, 1, 1	4	(2.4)(b)
7031 = 79·89	-1, -1, 1, -1, 0, 1	5	(2.4)(c)
7367 = 53·139	1, 2, 0, -3, -2, 1	5	(2.4)(d)
7463 = 17·439	1, -2, 1, 0, -2, 1	5	(2.4)(c)
8519 = 7·1217	1, -1, -1, 0, -1, 1	5	(2.4)(d)
8647 (prime)	1, 2, -2, -3, 0, 1	5	(2.4)(d)

Table 5.

$n = 6$, $r = 0$, $s = 3$; (1.11) is applied.

$-\Delta$	K_0	$a_0, a_1, \ldots, a_m$	$M \geq$	method
$9747 = 3^3 \cdot 19^2$	ζ_3	$\zeta_3, 1 - \zeta_3, -1, 1$	3	(2.6),(3.9)
$10051 = 19 \cdot 23^2$	α	$\alpha - 1, 1, 1$	3	(2.6),(3.10)
$10571 = 11 \cdot 31^2$	γ	$-\gamma + 1, 1, 1$	3	(2.6),(3.10)
$10816 = 2^6 \cdot 13^2$	ζ_4	$-1, 1, \zeta_4 - 1, 1$	3	(2.4)(a)
$11691 = 3^3 \cdot 433$	ζ_3	$\zeta_3, 1, -1, 1$	3	(2.6),(3.9)
$12167 = 23^3$	α	$1, \alpha - 1, 1$	3	(2.6),(3.10)
$14283 = 3^3 \cdot 23^2$	α	$1, 1, 1$	3	(2.6),(3.10)
14731 (prime)	0	$1, 0, -1, -1, 0, 1, 1$	3	(2.4)(a)
$16551 = 3^3 \cdot 613$	ζ_3	$-\zeta_3, -2, \zeta_3, 1$	4	(2.4)(b)
$18515 = 5 \cdot 7 \cdot 23^2$	α	$1, \alpha, 1$	4	(2.6),(3.10)
$21168 = 2^4 \cdot 3^3 \cdot 7^2$	ζ_3	$1, \zeta_3 - 1, -\zeta_3, 1$	4	(3.16)
$21296 = 2^4 \cdot 11^3$	κ	$1, \kappa, 1$	4	(3.13)
22291 (prime)	0	$1, -3, 6, -6, 4, -2, 1$	4	(2.4)(c)
$22592 = 2^6 \cdot 353$	ζ_4	$1, -\zeta_4, \zeta_4 - 1, 1$	4	(2.4)(c)
$22747 = 23^2 \cdot 43$	α	$\alpha + 1, 1, 1$	4	(2.6),(3.10)
$23031 = 3^3 \cdot 853$	ζ_3	$\zeta_3, -1, 0, 1$	4	(2.4)(b)
$24003 = 3^3 \cdot 7 \cdot 127$	ζ_3	$\zeta_3, -1, 1, 1$	4	(2.4)(b)
$27971 = 83 \cdot 337$	0	$1, -1, 1, -2, 3, -2, 1$	5	(2.4)(c)
$29095 = 5 \cdot 11 \cdot 23^2$	α	$\alpha^2, 1, 1$	5	(2.6),(3.10)
$29791 = 31^3$	γ	$1, -\gamma - 1, 1$	5	(2.4)(c)
$31211 = 23^2 \cdot 59$	α	$\alpha, \alpha, 1$	5	(2.6),(3.10)
$33856 = 2^6 \cdot 23^2$	α	$1, 0, 1$	5	(2.6),(3.10)
$33856 = 2^6 \cdot 23^2$	α	$\alpha, 0, 1$	5	(2.6),(3.10)
$36235 = 5 \cdot 7247$	0	$1, -1, 1, 0, 0, -1, 1$	5	(2.4)(c)
$41791 = 23^2 \cdot 79$	α	$\alpha, 1, 1$	5	(2.6),(3.10)
$64827 = 3^3 \cdot 7^4$	η	$1, 1, 1$	7	(2.6),(3.3)

Table 6.

$n = 6$, $r = 2$, $s = 2$; (1.11) is applied.

Δ	K_0	$a_0, a_1, \ldots, a_m$	$M \geq$	method
$28037 = 23^2 \cdot 53$	α	$-1, \alpha^2 - \alpha, 1$	5	(2.6),(3.10)
29077 (prime)	0	$-1, 2, -1, 0, 1, -1, 1$	5	(2.4)(c)
$29189 = 17^2 \cdot 101$	0	$1, 1, 1, 0, -3, 0, 1$	5	(2.4)(d)
$30125 = 5^3 \cdot 241$	θ	$1 - \theta, 1, -\theta, 1$	5	(2.4)(c)
$31133 = 163 \cdot 191$	0	$1, 2, 0, -1, -2, 0, 1$	5	(2.4)(d)
$31213 = 7^4 \cdot 13$	η	$\eta^2, 1, 1$	5	(2.6),(3.3)
$31709 = 37 \cdot 857$	0	$-1, 1, 3, -2, -3, 0, 1$	5	(2.4)(d)
$32269 = 23^2 \cdot 61$	α	$-\alpha, \alpha, 1$	5	(2.6),(3.10)
$33856 = 2^6 \cdot 23^2$	α	$-\alpha, 0, 1$	5	(2.6),(3.10)
$35125 = 5^3 \cdot 281$	θ	$1, -\theta, 0, 1$	5	(2.4)(c)
$35557 = 31^2 \cdot 37$	γ	$-1, -\gamma, 1$	5	(2.4)(d)
37253 (prime)	0	$-1, 0, 1, 0, -1, -1, 1$	5	(2.4)(d)
$37568 = 2^6 \cdot 587$	0	$-1, 2, -1, 0, 2, -2, 1$	5	(2.4)(c)
$39269 = 107 \cdot 367$	0	$1, -1, -2, 2, 0, -2, 1$	5	(2.4)(d)
40277 (prime)	0	$-1, 2, -3, 0, 3, -3, 1$	5	(2.4)(c)
$40733 = 7 \cdot 11 \cdot 23^2$	α	$\alpha - 1, \alpha^2, 1$	5	(2.6),(3.10)
$41069 = 7 \cdot 5867$	0	$-1, 0, 2, 0, -2, -1, 1$	5	(2.4)(d)
$45301 = 89 \cdot 509$	0	$-1, -1, 0, 0, 1, 1, 1$	6	(2.4)(e)
$47081 = 23^2 \cdot 89$	α	$-1, \alpha^{-1}, 1$	6	(2.4)(f)
$47669 = 73 \cdot 653$	0	$-1, 0, -1, 0, 1, 1, 1$	6	(2.4)(e)
$49664 = 2^9 \cdot 97$	λ	$\lambda, -1, 0, 1$	6	(2.4)(f)
$53429 = 23^2 \cdot 101$	α	$-1, \alpha, 1$	6	(2.4)(f)
$61193 = 11 \cdot 5563$	0	$-1, -1, -1, 1, 1, 1, 1$	6	(2.4)(e)
$61504 = 2^6 \cdot 31^2$	γ	$\gamma - 1, 0, 1$	6	(2.4)(f)
$69629 = 7^4 \cdot 29$	η	$-\eta, 1, 1$	7	(2.6),(3.3)

Table 7.

$n = 6$, $r = 4$, $s = 1$; (1.8) is applied.

$-\Delta$	K_0	$a_0, a_1, \ldots, a_m$	$M \geq$	method
92779 (prime)	0	1, 2, -1, -3, -2, 1, 1	6	(2.4)(f)
$103243 = 7^4 \cdot 43$	η	$\eta^2 - 2, \eta, 1$	7	(2.6),(3.3)

Table 8.

$n = 7$, $r = 1$, $s \mp 3$; (1.11) is applied.

$-\Delta$	$a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7$	$M \geq$	method
184607 (prime)	-1, -1, 1, 1, 0, -1, -1, 1	5	(2.4)(d)
193327 (prime)	-1, 2, 0, -2, 2, 0, -1, 1	5	(2.4)(c)
193607 (prime)	-1, 0, -1, -1, 1, 0, 0, 1	5	(2.4)(c)
196127 = 29·6763	1, -2, 2, 0, -1, 2, -2, 1	5	(2.4)(c)
199559 (prime)	1, -1, 0, 1, 0, 0, -1, 1	5	(2.4)(c)
201671 = 17·11863	1, 1, -1, -1, 2, 0, -2, 1	5	(2.4)(d)
202471 (prime)	1, -1, -1, 2, 0, -1, 0, 1	5	(2.4)(c)
207911 = 11·41·461	-1, 0, 1, -1, 1, 1, -1, 1	5	(2.4)(c)
211831 = 19·11149	1, -1, 2, -1, 0, 1, -2, 1	5	(2.4)(c)
214607 (prime)	-1, -1, 2, 3, -2, -3, 0, 1	5	(2.4)(d)
224647 = 277·811	-1, 0, 2, 1, -2, -2, 0, 1	5	(2.4)(d)
227287 = 167·1361	-1, 0, 2, 0, 1, 0, -2, 1	5	(2.4)(d)
237751 = 23·10337	-1, -1, 3, 4, -2, -3, 0, 1	5	(2.4)(d)
242147 (prime)	1, -1, 2, -1, -1, 2, -2, 1	5	(2.4)(c)
242971 (prime)	-1, -1, 1, 2, 0, -2, -1, 1	5	(2.4)(d)
250367 = 13·19259	1, 1, -1, 2, 0, -3, 0, 1	5	(2.4)(d)
252071 = 83·3037	-1, -1, 0, 2, 1, -2, -1, 1	5	(2.4)(d)
267347 = 101·2647	1, -1, -4, 3, 5, -2, -2, 1	6	(2.4)(f)
270607 = 461·587	-1, 0, 2, 2, 0, -2, -1, 1	6	(2.4)(f)
272671 = 7·38953	1, -2, -3, 6, 3, -4, -1, 1	6	(2.4)(f)
319831 (prime)	-1, -3, -3, -1, 1, 3, 2, 1	6	(2.4)(e)
330487 = 23·14369	1, -1, 0, -1, 0, 1, 0, 1	6	(2.4)(e)
349847 = 19·18413	-1, -1, -1, -1, 0, 1, 1, 1	6	(2.4)(e)

Table 9.

$n = 8$, $r = 0$, $s \neq 4$; (1.11) is applied.

Δ	K_0	$a_0, a_1, \ldots, a_m$	$M \geq$	method
$1257728 = 2^8 \cdot 17^3$	ξ	$-1, -\xi, 1$	5	(2.4)(d)
$1282789 = 1103 \cdot 1163$	0	$1, 0, -3, 0, 5, 1, -3, -1, 1$	5	(2.4)(d)
$1327833 = 3^4 \cdot 13^2 \cdot 97$	β	$1, \beta + 1, 1$	5	(2.6),(3.11)
$1342413 = 3^4 \cdot 16573$	ζ_3	$-\zeta_3, \zeta_3, 1 - \zeta_3, \zeta_3 - 1, 1$	5	(2.4)(c)
$1361513 = 17 \cdot 283^2$	δ	$\delta + 1, 1, 1$	5	(2.6),(3.12)
$1385533 = 29 \cdot 47777$	0	$1, 0, 0, 0, 1, -3, 3, -2, 1$	5	(2.4)(c)
$1424293 = 13 \cdot 331^2$	ε	$1, \varepsilon, 1$	5	(2.6),(3.12)
$1474013 = 617 \cdot 2389$	0	$1, -1, 1, 0, -1, 1, -1, 0, 1$	5	(2.4)(c)
$1492101 = 3^4 \cdot 13^2 \cdot 109$	β	$\beta + 1, 1, 1$	5	(2.6),(3.11)
$1513728 = 2^8 \cdot 3^4 \cdot 73$	ζ_{12}	$\zeta_{12} + 1, -\zeta_{12} - 1, 1$	5	(2.4)(c)
$1520789 = 29 \cdot 229^2$	ν	$-1, \nu - 1, 1$	5	(2.4)(d)
$1578125 = 5^6 \cdot 101$	ζ_5	$-1, \zeta_5^2 + \zeta_5, 1$	5	(2.6),(3.11)
$1590773 = 179 \cdot 8887$	0	$1, -2, 1, 1, -2, 2, 0, -1, 1$	5	(2.4)(c)
$1601613 = 3^6 \cdot 13^3$	β	$-\zeta_3^2, \beta - 1, 1$	6	(2.6),(3.11)
$1797309 = 3^4 \cdot 22189$	ζ_3	$-\zeta_3, -\zeta_3 - 1, 2\zeta_3 - 1, \zeta_3 + 1, 1$	6	(2.4)(f)
$1820637 = 3^4 \cdot 7 \cdot 13^2 \cdot 19$	β	$1, \beta, 1$	6	(2.6),(3.11)
1867553 (prime)	0	$1, 1, 1, -1, -2, -1, 0, 1, 1$	6	(2.4)(e)
$1890625 = 5^6 \cdot 11^2$	ζ_5	$\zeta_5 + \zeta_5^{-1}, -1, 1$	6	(3.15)
$2149173 = 3^4 \cdot 13^2 \cdot 157$	β	$\beta, \zeta_3, 1$	6	(2.6),(3.11)
$2313441 = 3^4 \cdot 13^4$	β	$-1, \zeta_3^2, 1$	7	(3.14)

Table 10. Subfield generators.

symbol	defining equation	ref.
α	$\alpha^3 - \alpha - 1 = 0$	(3.10)
β	$\beta^2 + \zeta_3\beta - 1 = 0$	(3.11)
γ	$\gamma^3 + \gamma - 1 = 0$	(3.10)
δ	$\delta^4 - \delta - 1 = 0$	(3.12)
ε	$\varepsilon^4 - 2\varepsilon^2 + 3\varepsilon - 1 = 0$	(3.12)
ζ_m	m-th cyclotomic equation	(3.1),(3.2)
η	$\eta^3 + \eta^2 - 2\eta - 1 = 0 \quad (\eta = \zeta_7 + \zeta_7^{-1})$	(3.3)
θ	$\theta^2 - \theta - 1 = 0 \quad (\theta = -\zeta_5 - \zeta_5^{-1})$	(3.9)
κ	$\kappa^3 + \kappa^2 - \kappa + 1 = 0$	(3.13)
λ	$\lambda^2 - 2\lambda - 1 = 0 \quad (\lambda = 1 + \sqrt{2})$	
μ	$\mu^2 - \mu - 3 = 0 \quad (\mu = \frac{1}{2}(1 + \sqrt{13}))$	
ν	$\nu^4 - \nu + 1 = 0$	(3.11)
ξ	$\xi^2 - \xi - \zeta_4 = 0$	(3.11)

§4. The number of known Euclidean fields.

At the time of writing this (September 1976) I know 311 non-isomorphic Euclidean number fields. Table 11 shows how they are distributed with respect to n and $r + s$. We indicate the sources; the references are to the most informative rather than to the original publications.

$n \leq 2$: see [13, Ch. 14].

$n = 3$, $r + s = 2$: see [11, 35].

$n = 3$, $r + s = 3$: see [9, 33, 34].

$n = 4$, $r + s = 2$: thirty fields appear in [15]; for the other two, with $\Delta = 125$ and $\Delta = 229$, see (3.10).

$n = 4$, $r + s = 3$: see sec. 3, table 2.

$n = 4$, $r + s = 4$: see [10].

$n = 5$, $r + s = 3$: see sec. 3, table 3.

$n = 5$, $r + s = 4$: see sec. 3, table 4, and (3.17).

$n = 5$, $r + s = 5$: see [10] or (3.3).

$n = 6$, $r + s = 3$: twenty-six fields appear in sec. 3, table 5; the other two are $\mathbb{Q}(\zeta_7)$ and $\mathbb{Q}(\zeta_9)$, with $\Delta = -16807$ and $\Delta = -19683$, see [20].

$n = 6$, $r + s = 4$: see sec. 3, table 6.

$n = 6$, $r + s = 5$: see sec. 3, table 7.

$n = 6$, $r + s = 6$: see (3.5) and (3.3).

$n = 7$, $r + s = 4$: see sec. 3, table 8.

$n = 8$, $r + s = 4$: twenty fields appear in sec. 3, table 9; the other four are $\mathbb{Q}(\zeta_{15})$, $\mathbb{Q}(\zeta_{20})$, $\mathbb{Q}(\zeta_{24})$ and $\mathbb{Q}(\zeta_{16})$, having $\Delta = 1265625$, $\Delta = 4000000$, $\Delta = 5308416$ and $\Delta = 16777216$, respectively [20, 21, 27].

$n = 10$, $r + s = 5$: this is $\mathbb{Q}(\zeta_{11})$, with $\Delta = -2357947691$, see [20].

It has been proved that the only Euclidean fields with $n \leq 2$ are the known ones [13, Ch. 14], and that there exist only finitely many Euclidean fields with $r + s \leq 2$, up to isomorphism [3].

r + s \ n	1	2	3	4	5	6	7	8	9	10	total
1	1	5									6
2		16	52	32							100
3			57	11	12	28					108
4				9	10	25	23	24			91
5					1	2	0	0	0	1	4
6						2	0	0	0	0	2
total	1	21	109	52	23	57	23	24	0	1	311

Table 11. The number of known Euclidean fields.

References.

1. Biedermann, D. and W. Richter, Minimaldiskriminanten von primitiven Zahlkörpern sechsten Grades im totalreellen und totalkomplexen Fall, Universität Karlsruhe, 1974.

2. Cartier, P. and Y. Roy, On the enumeration of quintic fields with small discriminant, J. Reine Angew. Math. 268/269 (1974), 213-215.

3. Cassels, J.W.S., The inhomogeneous minimum of binary quadratic, ternary cubic and quaternary quartic forms, Proc. Cambridge Philos. Soc. 48 (1952), 72-86,519-520.

4. Chowla, S., Proof of a conjecture of Julia Robinson, Norske Vid. Selsk. Forh. (Trondheim), 34 (1961), 100-101.

5. Cohn, H., A numerical study of quintics of small discriminant, Comm. Pure Appl. Math. 8 (1955), 377-385.

6. Godwin, H.J., Real quartic fields with small discriminant, J. London Math. Soc. 31 (1956), 478-485.

7. Godwin, H.J., On totally complex quartic fields with small discriminants, Proc. Cambridge Philos. Soc. 53 (1957), 1-4.

8. Godwin, H.J., On quartic fields of signature one with small discriminant, Quart. J. Math. Oxford Ser. 8 (1957), 214-222.

9. Godwin, H.J., On the inhomogeneous minima of totally real cubic norm-forms, J. London Math. Soc. 40 (1965), 623-627.

10. Godwin, H.J., On Euclid's algorithm in some quartic and quintic fields, J. London Math. Soc. 40 (1965), 699-704.

11. Godwin, H.J., On Euclid's algorithm in some cubic fields with signature one, Quart. J. Math. Oxford Ser. 18 (1967), 333-338.

12. Györy, K., Sur les polynômes à coefficients entiers et de discriminant donné, II, Publ. Math. Debrecen 21 (1974), 125-144.

13. Hardy, G.H. and E.M. Wright, An introduction to the theory of numbers, 4th ed., Oxford 1960.

14. Hurwitz, A., Der Euklidische Divisionssatz in einem endlichen algebraischen Zahlkörper, Math. Z. 3 (1919), 123-126.

15. Lakein, R.B., Euclid's algorithm in complex quartic fields, Acta Arith. 20 (1972), 393-400.

16. Lang, S., Algebraic number theory, Reading, Mass. 1970.

17. Leech, J., Some sphere packings in higher space, Canad. J. Math. 16 (1964), 657-682.

18. Leech, J., Notes on sphere packings, Canad. J. Math. 19 (1967), 251-267.

19. Lekkerkerker, C.G., Geometry of numbers, Groningen-Amsterdam, 1969.

20. Lenstra, Jr., H.W., Euclid's algorithm in cyclotomic fields, J. London Math. Soc. 10 (1975), 457-465.

21. Lenstra, Jr., H.W., private communication.

22. Markanda, R., Euclidean rings of algebraic numbers and functions, J. Algebra 37 (1975), 425-446.

23. Matzat, B.H., Zahlentheoretische Programme und einige Ergebnisse, Universität Karlsruhe, 1969.

24. Nagell, T., Sur une propriété des unités d'un corps algébrique, Ark. Mat. 5 (1964), 343-356.

25. Nagell, T., Quelques problèmes relatifs aux unités algébriques, Ark. Mat. 8 (1969), 115-127.

26. Nagell, T., Sur un type particulier d'unités algébriques, Ark. Mat. 8 (1969), 163-184.

27. Ojala, T., Euclid's algorithm in the cyclotomic field $\mathbb{Q}(\zeta_{16})$, to appear.

28. O'Meara, O.T., On the finite generation of linear groups over Hasse domains, J. Reine Angew. Math. 217 (1965), 79-108.

29. Pohst, M., Berechnung kleiner Diskriminanten total reeller algebraischer Zahlkörper, J. Reine Angew. Math. 278/279 (1975), 278-300.

30. Poitou, G., Minorations de discriminants (d'après A.M. Odlyzko), Sém. Bourbaki 28 (1975/76), exp. 479.

31. Queen, C.S., Euclidean subrings of global fields, Bull. Amer. Math. Soc. 79 (1973), 437-439.

32. Rogers, C.A., Packing and covering, Cambridge, 1964.

33. Smith, J.R., On Euclid's algorithm in some cyclic cubic fields, J. London Math. Soc. 44 (1969), 577-582.

34. Smith, J.R., The inhomogeneous minima of some totally real cubic fields, pp. 223-224 in: A.O.L. Atkin and B.J. Birch (eds), Computers in number theory, London 1971.

35. Taylor, E.M., Euclid's algorithm in cubic fields with complex conjugates, J. London Math. Soc. 14 (1976), 49-54.

36. Wasén, R., On sequences of algebraic integers in pure extensions of prime degree, Colloq. Math. 30 (1974), 89-104.

H.W. Lenstra, Jr.

Mathematisch Instituut

Universiteit van Amsterdam

Roetersstraat 15

Amsterdam - The Netherlands.