Следовательно система сравнений

$$\sum_{\nu=0}^{n} x_i^{\nu} u_i \equiv 0 \pmod{q}, \quad i = 1, \ldots, n+1,$$

имеет решение с условием $(u_0, u_1, \ldots, u_n, q) = 1$. Отсюда вытекает, что ее определитель Δ делится на q. Учитывая, что

$$0 < \Delta \leqslant \prod_{1 \leqslant i < j \leqslant n+1} (x_j - x_i) \leqslant T^{n(n+1)/2} < q,$$

получаем противоречие. Тем самым оценка (7), а вместе с ней и теорема, доказаны.

В заключение заметим, что для $\Omega(q)$ – количества простых делителей q с учетом кратности, для почти всех в смысле асимптотической плотности натуральных q справедлива оценка

$$\Omega(q) \leqslant 10 \ln\ln q$$

(см. [3]). Отсюда вытекает, что для почти всех натуральных q выполнена оценка (6).

Литература

[1] С. В. Конягин, *О числе решений сравнения n-й степени с одним неизвестным*, Мат. сб. 102 (2) (1979), 171–187.

[2] Н. М. Коробов, *Двойные тригонометрические суммы и их приложения к оценке рациональных сумм*, Мат. заметки 6 (1) (1969), 25–34.

[3] Ю. В. Линник, *Дисперсионный метод в бинарных аддитивных задачах*, Изд. Ленинградского гос. ун.-та, 1961.

[4] Д. А. Митькин, *Об оценках и асимптотических формулах для рациональных тригонометрических сумм, близких к полным*, Мат. сб. 122 (4) (1983), 527–545.

[5] С. Б. Стечкин, *Оценка полной рациональной тригонометрической суммы*, Труды Мат. ин-та АН СССР 143 (1977), 188–207.

СССР 119 285
Москва
Мосфильмовская ул., д2, корп. В, кв. 41

Поступило 28.9.1989
и в исправленной форме 29.3.1990 (1970)

ACTA ARITHMETICA
LVIII.2 (1991)

An improvement of Lenstra's criterion for euclidean number fields: The totally real case

by

GERHARD NIKLASCH (München) and ROLAND QUÊME (Breuillet)

1. Introduction. By a theorem of H. W. Lenstra jr. [Le 77], an algebraic number field is euclidean for the norm provided that it contains a sufficiently long "exceptional sequence" of elements whose pairwise differences are units. More precisely, the length must exceed the square root of the discriminant times a (number-geometric) coefficient depending on the signature of the field. We show that a modification of Lenstra's argument leads, for totally real fields, to significantly smaller coefficients, and present seven new euclidean number fields thus obtained. (The totally real case is the hardest to handle because the field discriminants are comparatively large.)

More than 600 euclidean number fields are known; see [Le 80], [LM 82], [LN 87] and the references there. The majority of these was found with the help of Lenstra's criterion, originally formulated in [Le 74, Section 14], and published in its final form in the celebrated *Inventiones* article [Le 77]. [Le 80] provides a very readable survey of the topic.

In order to state the criterion, we need to fix a few notions and notations. Let K be an algebraic number field and R its ring of (algebraic) integers. Let N denote the absolute norm, defined on R by $N(0) = 0$, $N(\alpha) = \#(R/\alpha R)$ for $\alpha \in R \setminus \{0\}$, and extended to K by multiplicativity. R (or K, by a traditional abuse of language) is called *euclidean* (*for the norm*) if for any $\alpha, \beta \in R$ with $\beta \neq 0$ we can find $\kappa, \varrho \in R$ such that $\alpha = \kappa\beta + \varrho$ and $N(\varrho) < N(\beta)$. Equivalently, for each $\xi \in K$ we need to find $\kappa \in R$ such that $N(\xi - \kappa) < 1$.

DEFINITION. An *exceptional sequence of length* m in K is a subset

$$\{\omega_1, \ldots, \omega_m\} \subset K$$

such that each difference $\omega_i - \omega_j$ $(1 \leqslant i < j \leqslant m)$ is an invertible element of R (i.e., a Dirichlet unit in K).

THEOREM 1 [Le 77]. *There are positive constants $\alpha = \alpha(r, s)$, such that every number field K with discriminant D, with r real and s complex places, and containing an exceptional sequence of length $m > \alpha(r, s) \cdot \sqrt{|D|}$ is euclidean for the norm.*

The theorem is designed to be applied to several number fields at once. First one needs good upper bounds $\tilde{\alpha}$ for the coefficients $\alpha(r, s)$. Lenstra computed two series of values, derived from the packing constants of "Minkowski sets" and spheres in the real vector space $K \otimes_{\boldsymbol{Q}} \boldsymbol{R}$. Then one writes down a sequence $\{\omega_1, \ldots, \omega_m\}$ in terms of a field generator x of K over $\boldsymbol{Q}$, and translates the condition that the sequence be exceptional into diophantine relations for the coefficients of the minimal polynomial of x. (This is discussed in detail in [Le 77], [LM 82] and [LN 87].) Finally, one generates irreducible polynomials of the appropriate degree and number of real roots, satisfying these relations, and computes the corresponding field discriminants along with any other properties of interest of the generated fields (e.g., splitting behaviour of small primes). If the discriminant turns out to be too large to apply Theorem 1, one can sometimes extend the prescribed exceptional sequence by direct calculation in K. However, m can never exceed the norm of any nontrivial ideal of R (the ω_i must belong to distinct cosets). When ideals of norm > 1 and $\leqslant \tilde{\alpha}\sqrt{|D|}$ are present, the only way to make Theorem 1 applicable will be to reduce $\tilde{\alpha}$.

To our knowledge, Lenstra's $\tilde{\alpha}$ bounds from [Le 77] have never been improved yet. Our aim in this paper is to derive significantly sharper bounds for the case $s = 0$ of totally real number fields. The key to this improvement is a modification of Lenstra's proof of Theorem 1, valid for number fields of all signatures, which we discuss in Section 2. Our bounds will be established in Section 3. Section 4 is devoted to examples. We present seven new euclidean fields, including two quintic and three sextic fields. One quintic and three sextic real fields were known to be euclidean before. In both degrees these represented the smallest possible values of the discriminant, while our new examples belong to some of the next larger discriminants.

It is not difficult to modify the arguments of Section 3 to handle fields of mixed signatures with $2s < r$. The bounds $\tilde{\alpha}$ thus obtained so far are only slightly better than the previously known ones and have not yet led to any new euclidean fields. Present research is aimed at improving them further and extending our method to all signatures.

R may be replaced throughout with a ring of the form R_S, consisting of those elements of K which are integral at all places of K outside the finite set S (containing all infinite and some finite places). The norm N_S and the euclidean property are defined as for R. A theorem of O'Meara [OM 65] implies that, given K, one can always choose S so that R_S will be euclidean. Lenstra's criterion is easily adapted to this situation (D and $\alpha(r, s)$ remain unchanged), and one sees at once that m can be made as large as we please by choosing an arbitrary sequence of ω's and collecting all prime divisors of their pairwise differences into S. This yields a quantitative version of O'Meara's theorem, which also profits from our sharper bounds. We leave the details to the reader, cf. [Le 80], [LM 82] and [Q 82].

2. Lenstra's criterion. For ease of reference and to fix ideas, let us sketch Lenstra's proof of Theorem 1. Using the r real embeddings

$$\iota_1, \ldots, \iota_r\colon K \to \boldsymbol{R}$$

and representatives

$$\iota_{r+1}, \ldots, \iota_{r+s}\colon K \to \boldsymbol{C}$$

of the s pairs of complex conjugate embeddings, we may identify $K_{\boldsymbol{R}} = K \otimes_{\boldsymbol{Q}} \boldsymbol{R}$ with the $\boldsymbol{R}$-algebra $\boldsymbol{R}^r \times \boldsymbol{C}^s$ by sending $\xi \otimes 1$ ($\xi \in K$) to

$$(\iota_1(\xi), \ldots, \iota_{r+s}(\xi)),$$

at the same time identifying K and R with their images. The norm function extends to $K_{\boldsymbol{R}}$ as

$$N(x_1, \ldots, x_r, z_{r+1}, \ldots, z_{r+s}) = \prod_{i=1}^{r} |x_i| \cdot \prod_{i=r+1}^{r+s} |z_i|^2.$$

If we write $\mathscr{V} = \{x \in K_{\boldsymbol{R}} \mid N(x) < 1\}$, K will be euclidean for the norm if and only if the translates of $\mathscr{V}$ by the integral lattice vectors R cover K. As a real vector space, $K_{\boldsymbol{R}}$ has dimension $n = r + 2s = [K : \boldsymbol{Q}]$. We define the Haar measure λ on $\boldsymbol{R}^r \times \boldsymbol{C}^s$ to be the product of the ordinary Lebesgue measure dx on each factor $\boldsymbol{R}$, and twice the Lebesgue measure (i.e., $dz \wedge d\bar{z}$) on each factor $\boldsymbol{C}$. Then the lattice R will have determinant $\sqrt{|D|}$.

Let $U \subset K_{\boldsymbol{R}}$ be a bounded Lebesgue measurable set with positive measure $\lambda(U)$, and $(x^{(i)})_{i=1}^{\infty}$ a sufficiently regularly distributed sequence of points in $K_{\boldsymbol{R}}$. To the family $\mathscr{U}$ of translates $U + x^{(i)}$ we can associate a density

$$\varrho(\mathscr{U}) = \lim\Big(\sum_i \lambda\big((U + x^{(i)}) \cap C\big)\Big)/\lambda(C),$$

C being a cube centred at the origin and becoming infinitely large. $\mathscr{U}$ is a *packing* if translates $U + x^{(i)}$ for distinct i are pairwise disjoint, which obviously implies $\varrho(\mathscr{U}) \leqslant 1$. The *packing constant* of U is $\delta(U) = \sup \varrho(\mathscr{U})$, taken over all packings of U for which the density exists, and the *centre packing constant* of U is defined as $\delta^*(U) = \delta(U)/\lambda(U)$. (See [R 64] and [GL 87] for precise definitions.)

Choose now U such that

$$\Delta U = \{u - v \mid u, v \in U\} \subseteq \mathscr{V}. \tag{1}$$

Lenstra shows that if, in the situation of Theorem 1, $m > \delta^*(U)\sqrt{|D|}$, then indeed all of $K_{\boldsymbol{R}}$ is covered by the integral translates of $\mathscr{V}$. As pointed out above, the strength of this approach stems from the fact that U depends on K only via $K_{\boldsymbol{R}}$, which is determined by the signature (r, s) alone.

The argument runs as follows: Given $x \in K_{\boldsymbol{R}}$, we need to find $\kappa \in R$ such that $N(x - \kappa) < 1$. Consider the family of translates of U by $\omega_i x + \alpha$, $1 \leqslant i \leqslant m$,

$\alpha \in R$. As this has density $m\lambda(U)/\sqrt{|D|}$, which exceeds $\delta(U)$ by assumption, we can find $u, v \in U$, $1 \leqslant i, j \leqslant m$ and $\alpha, \beta \in R$ with $(i, \alpha) \neq (j, \beta)$, such that

$$\omega_i x + \alpha + u = \omega_j x + \beta + v.$$

Since an algebraic integer of norm less than 1 must be zero, (1) implies $\Delta U \cap R = \{0\}$. Therefore we cannot have $i = j$, for otherwise $\beta - \alpha = u - v = 0$. Again because of (1),

$$(\omega_i - \omega_j)x - (\beta - \alpha) \in \mathscr{V}. \tag{2}$$

Since $N(\omega_i - \omega_j) = 1$, we may now take $\kappa = (\beta - \alpha)/(\omega_i - \omega_j) \in R$. ∎

Our point of departure is the observation that condition (1) may be weakened. Indeed, if we knew only that ΔU could be covered by integral translates of $\mathscr{V}$, the last steps of the above argument would still work (possibly with a different κ). However, something else is now required to prevent translates of U belonging to the same ω_i from overlapping.

THEOREM 2. *Let T be any subset of R, containing 0. If $U \subset K_R$ is a bounded Lebesgue measurable set with measure $\lambda(U) > 0$ and centre packing constant $\delta^*(U)$, such that*

(i) *ΔU is covered by the translates of $\mathscr{V}$ by T,*
(ii) *$\Delta U \cap T = \{0\}$,*

and if K contains an exceptional sequence of length $m > \delta^*(U)\sqrt{|D|}$, then K_R is covered by the translates of $\mathscr{V}$ by R, and K is euclidean.

Proof. In view of what was said above, we only need to fill in one step: Condition (i) obviously implies that $\Delta U \cap R$ is contained in T, and (ii) shows that it is in fact $\{0\}$. We may then continue as above, replacing $\beta - \alpha$ in (2) with a suitable element of $\beta - \alpha + T$. (Lenstra's original proof of course corresponds to $T = \{0\}$.) ∎

Let us consider what we have gained. By a careful choice of T, we may now hope to find a set U with larger volume and smaller centre packing constant, and thus to satisfy the criterion with a shorter exceptional sequence. The price we have to pay, in general, is that T (and therefore $\delta^*(U)$) will depend on K. In order to obtain general results we will have to restrict T to contain only rational integers, which are available in every number field; e.g., $T = \{0, \pm 1\}$ or $\{0, \pm 1, \pm 2\}$.

In a sense, Theorem 2 is best possible. Recall that the "first inhomogeneous minimum of the norm-form for K", or *inhomogeneous minimum* for short, is the infimum $\mu(K)$ of all positive numbers μ such that the integral translates of the scaled set $\mu\mathscr{V}$ cover all of K_R [GL 87]. K is euclidean precisely if $\mu(K) < 1$ or if $\mu(K) \geqslant 1$ and the points of K_R which are left uncovered at $\mu = 1$ do not belong to K; conjecturally the latter case never occurs [Le 80]. Now if $\mu(K) < 1$, we can always satisfy the criterion in Theorem 2 by putting $T = R$, $\omega_1 = 0$, $\omega_2 = 1$, and taking for U the interior of a (convex, bounded)

fundamental cell for the lattice R: By assumption, the sets $\mathscr{V} + \alpha$ ($\alpha \in R$) cover K_R, hence ΔU, and ΔU contains no nonzero lattice points. We have $\delta(U) = 1$, $\lambda(U) = \sqrt{|D|}$, and $m = 2 > \delta^*(U)\sqrt{|D|}$. (If larger values of m are known to be possible, one can get by with a smaller U. Maybe some stubborn candidates for euclidean fields would yield to such an attack.)

However, here too something has been lost. As Lenstra himself observed [Le 77, remark preceding Corollary 1.8], whenever his original criterion yields $\mu(K) < 1$, it also provides a sharper estimate $\mu(K) \leqslant \delta^*(U)\sqrt{|D|}/m$ by scaling down $\mathscr{V}$ and U. This fails when $T \neq \{0\}$ because our condition (i) is no longer scale invariant (T cannot be scaled).

3. The totally real case. We will now apply Theorem 2 to totally real fields ($r = n$, $s = 0$), using $T = \{-1, 0, +1\}$ and a set U of the following shape. In $K_R \cong \boldsymbol{R}^n$, let A be the endomorphism which has $1 \in R$ as eigenvector for the simple eigenvalue 1, and the hyperplane orthogonal to it as eigenspace for an eigenvalue $\tau_n > 1$ which we shall prescribe later. Then we take U to be the image under A of the open ball of radius $\sqrt{n}/2$ about 0. U is convex and symmetric about the origin, so ΔU is just $2U$, and this does not contain ± 1 (condition (ii)). Below we shall choose τ_n such that

(3) the open ball of radius $\tau_n\sqrt{n}$ about the origin is covered by $\mathscr{V} + T$

so as to ensure condition (i) (this ball contains ΔU). The packing constant is an affine invariant; therefore Rogers' upper bound σ_n for the packing density of an n-dimensional ball [R 64, Theorem 7.1] applies to U. Finally,

$$\lambda(U) = \tau_n^{n-1}\left(\frac{\pi n}{4}\right)^{n/2} \Big/ \Gamma\left(1 + \frac{n}{2}\right).$$

Theorem 2 now gives

THEOREM 3. *Assume τ_n chosen as in (3). Then any totally real number field of degree n, containing an exceptional sequence of length*

$$m > \tau_n^{1-n}\left(\frac{4}{\pi n}\right)^{n/2} \Gamma\left(1 + \frac{n}{2}\right)\sigma_n\sqrt{|D|}$$

has inhomogeneous minimum $\mu(K) < 1$ and is euclidean for the norm. ∎

We turn now to determining suitable values for the τ_n. Recall that the norm of $x = (x_1, \ldots, x_n) \in K_R$ is just $\prod_1^n |x_i|$ in the totally real case. Elements of the algebra K_R are multiplied coordinatewise. The euclidean length of x will be denoted $d(x) = \left(\sum_1^n x_i^2\right)^{1/2}$.

LEMMA. *There are constants $\tau_n \geqslant \tau > 1$ such that for all $x \in K_R$ satisfying $N(x) \geqslant 1$ and $N(x^2 - 1) \geqslant 1$, we have $d(x) \geqslant \tau_n\sqrt{n}$. ($\tau$ does not depend on n.)*

(Thus conversely $d(x) < \tau_n\sqrt{n}$ implies $x \in \mathscr{V} \cup (\mathscr{V} + 1) \cup (\mathscr{V} - 1)$.)

Proof. If $n = 1$, we may take $\tau_1 = \sqrt{2}$, so let $n > 1$. No coordinate x_i of x can be 0 or ± 1 if x is to satisfy the two norm inequalities. Applying the inequality of arithmetic and geometric means to the left-hand side of $N(x^2-1)^{1/n} \geqslant 1$, we find

$$\sum_{i=1}^{n} |x_i^2 - 1| \geqslant n. \tag{4}$$

Therefore at least one x_i satisfies $|x_i^2-1| \geqslant 1$, and in fact $x_i^2 > 1$. Assume without loss of generality $x_i^2 > 1$ for $1 \leqslant i \leqslant k$ and $x_i^2 < 1$ for $k < i \leqslant n$, where $1 \leqslant k \leqslant n$. If $k = n$, we can drop the absolute value signs in (4), obtaining $d^2(x) - n \geqslant n$, or $d(x) \geqslant \sqrt{2n}$. We shall have to take $\tau_n \leqslant \sqrt{2}$. If $k < n$, (4) reads

$$\sum_{i=1}^{k} x_i^2 \geqslant 2k + \sum_{i=k+1}^{n} x_i^2$$

or, adding the left-hand side to both sides and halving,

$$\sum_{i=1}^{k} x_i^2 \geqslant k + \tfrac{1}{2} d^2(x). \tag{5}$$

From the means inequality (twice) and $N(x^2) \geqslant 1$ we get

$$\begin{aligned} \sum_{i=k+1}^{n} x_i^2 &\geqslant (n-k)\Big(\prod_{i=k+1}^{n} x_i^2\Big)^{1/(n-k)} \\ &\geqslant (n-k)\Big(\prod_{i=1}^{k} x_i^2\Big)^{1/(k-n)} \\ &\geqslant (n-k)\left(\frac{1}{k}\sum_{i=1}^{k} x_i^2\right)^{k/(k-n)} \end{aligned}$$

and

$$d^2(x) \geqslant \sum_{i=1}^{k} x_i^2 + (n-k)\left(\frac{1}{k}\sum_{i=1}^{k} x_i^2\right)^{k/(k-n)} \tag{6}$$

The real function $y \mapsto y + (n-k)(y/k)^{k/(k-n)}$ grows monotonically for $y > k$. Therefore we may substitute (5) into (6) to obtain

$$d^2(x) \geqslant k + \frac{1}{2} d^2(x) + (n-k)\left(1 + \frac{d^2(x)}{2k}\right)^{k/(k-n)} \tag{7}$$

Putting for $0 < t < 1$, $0 < u$,

$$F(t, u) = u - 2t - 2(1-t)\left(1 + \frac{u}{2t}\right)^{t/(t-1)}$$

(7) may be written as

$$F\left(\frac{k}{n}, \frac{d^2(x)}{n}\right) \geqslant 0. \tag{8}$$

F is monotonic in u for each t, in fact $\partial/\partial u(F(t, u)) > 0$. One immediately sees $F(t, 2t) < 0$ and $F(t, 2) > 0$, so that there is a unique $\varphi(t)$ between $2t$ and 2 such that $F(t, \varphi(t)) = 0$, and (8) is equivalent to

$$d(x) \geqslant \sqrt{\varphi(k/n)} \cdot \sqrt{n}.$$

Furthermore, $\varphi(t) > 1$, since, for $t < 1/2$, $F(t, 1) < 0$ is equivalent to

$$\left(1 + \frac{1}{2t}\right)^{t} < \left(1 + \frac{1}{2(t-1)}\right)^{t-1},$$

which is true (the left-hand side takes values between 1 and $\sqrt{2}$, while the right-hand side is always larger than 2). Obviously $\lim_{t\to 1} \varphi(t) = 2$, and as, for fixed u, $\lim_{t\to 0} F(t, u) = u - 2$, we must also have $\lim_{t\to 0} \varphi(t) = 2$. By the implicit function theorem, φ is continuous (and has continuous first and second derivatives) on $0 < t < 1$. We conclude that it attains a global minimum $\varphi_0 = \varphi(t_0) > 1$ for some t_0. Hence we may take $\tau = \sqrt{\varphi_0}$ and

$$\tau_n = \min_{1 \leqslant k < n} \{\sqrt{\varphi(k/n)}\},$$

which ensures $\sqrt{2} > \tau_n \geqslant \tau > 1$, and the Lemma is proved.

But we can get still more information about φ. Restrict u to $2t < u < 2$ and write $F(t, u) = 0$ as

$$t \ln\left(1 + \frac{u}{2t}\right) = (t-1)\ln\left(1 + \frac{2-u}{2(t-1)}\right). \tag{9}$$

Substitute $u = \varphi(t)$, take derivatives, use (9) to get rid of the logarithm on the right-hand side, differentiate again and put $\varphi'(t) = 0$. The resulting expression for $\varphi''(t)$ in terms of t and $u = \varphi(t)$ is positive for all permitted values of t and u; in other words, every local extremum of φ must be a minimum. Therefore there is precisely one global and local minimum. Incidentally, $\varphi(t)$ is algebraic for rational values of t (e.g., $\varphi(1/2) = \sqrt{2}$), but $\varphi'(t) = 0$ is impossible for rational t and algebraic $\varphi(t)$, so that t_0 must be irrational. ∎

It is easy to evaluate φ numerically by Newton's method, and a second-order iteration produces the approximate values

$$\begin{aligned} t_0 &\approx 0.43072292, \\ \varphi_0 &\gtrsim 1.40844642, \\ \tau &\gtrsim 1.18677985. \end{aligned}$$

In order to compute τ_n, it suffices to check only the k/n adjacent to t_0, i.e., $k = \lfloor nt_0 \rfloor$ and $\lceil nt_0 \rceil$.

In Table 1 we have collected, for $2 \leqslant n \leqslant 20$, the values τ_n (rounded towards zero), preceded by the corresponding k which minimize $\varphi(k/n)$, the coefficients $\alpha_n^{(Q)} = \tau_n^{1-n}(4/(\pi n))^{n/2}\Gamma(1+n/2)\sigma_n$ needed in Theorem 3 (rounded

away from zero), and (for comparison) the Minkowski coefficients $\tilde{\alpha}_n^{(M)} = n!/n^n$, which were the lowest ones known before in this range. Exact values have been marked as such.

Asymptotically, the Minkowski coefficients grow like $\sqrt{2\pi n}e^{-n}$. For sufficiently large n, Lenstra's sphere packing coefficients [Le 77, (1.12)]

$$\left(\frac{4}{\pi n}\right)^{n/2}\Gamma\left(1+\frac{n}{2}\right)\sigma_n \sim 0.652n^{3/2}e^{-1.0724n}$$

become smaller than the former. Our coefficients are less than either, with asymptotic behaviour

$$0.774n^{3/2}e^{-1.2436n}.$$

Table 1. Coefficients for the Lemma and for Theorem 3

n	k	τ_n	$\tilde{\alpha}_n^{(Q)}$	$\tilde{\alpha}_n^{(M)}$
2	1	$\sqrt[4]{2} \gtrsim 1.1892071$	0.48549178	$1/2 = 0.5$
3	1	1.1917481	0.20176332	$1/9 \lesssim 0.222222223$
4	2	$\sqrt[4]{2}$	0.07805681	$= 0.09375$
5	2	1.1872593	0.02877318	$= 0.0384$
6	3	$\sqrt[4]{2}$	0.01010640	0.0154320988
7	3	1.1867821	0.00352448	0.00611989903
8	3	1.1883710	0.0011815	0.00240325928
9	4	1.1868747	0.0003970	0.000936656709
10	4	1.1872593	0.00013008	$= 0.00036288$
11	5	1.1870657	0.00004238	0.000139905949
12	5	1.1868798	0.000013669	0.000053723218
13	6	1.1872582	0.000004354	0.00002055970
14	6	1.1867821	0.000001390	0.00000784542
15	6	1.1872593	0.0000004362	0.00000298629
16	7	1.1868030	0.00000013767	0.00000113423
17	7	1.1869618	0.000000042935	0.00000042997
18	8	1.1868747	0.000000013379	0.00000016272
19	8	1.1868271	0.0000000041516	0.00000006149
20	9	1.1869670	0.0000000012802	0.00000002321

Nevertheless, this should not be taken to suggest that our Theorem 3 were best possible. The reader should draw a picture to convince herself or himself that for $n = 2$ the "true" coefficient $\delta^*(U)$ should be $1/\sqrt{5} \approx 0.4472136$ (U is a rectangle, and $T = \{0, \pm 1\}$). In fact, if condition (i) in Theorem 2 is satisfied only for $\Delta U \cap K$, one may still conclude that K is euclidean (start the proof with an $x \in K$ and observe that this implies $u - v \in K$); thus for real quadratic fields *except* $\boldsymbol{Q}(\sqrt{5})$ one may use an even larger rectangle with

$\delta^*(U) = 1/\sqrt{8} \approx 0.3535534$ and $T = \{0, \pm 1, \pm 2\}$. This handles the eight fields with discriminants $5 < D < 32$ ($m = 2$ throughout; compare this to [HW 79, Theorem 248]). The seven euclidean real quadratic fields with larger discriminants would need a $T \not\subseteq \boldsymbol{Z}$. — In the real cubic case, one can have $\delta^*(U)$ as small as 0.14343246 (with $T = \{0, \pm 1, \pm 2\}$ and unrestricted condition (i)). This works for the fields of discriminants 49, 81, 148, 169, 257, 361, all known to be euclidean already, and probably no others. Higher degrees are being investigated; the results will appear elsewhere.

As mentioned in the introduction, the arguments leading to our lemma may be modified to handle non-totally real fields, at least as long as $2s < r$, and yield values $\tau_{r,s}$ for Theorem 3 which are unfortunately not large enough to detect any new euclidean fields. Here, too, we expect that other choices of U and/or refined calculations will lead to further improvements.

4. Examples. In this section we present nine totally real number fields in degrees 4, 5 and 6 which are proved euclidean by Theorem 3. Two of the quartic fields have before been shown to be euclidean by different methods [G 65], the other seven are new. The results are summarized in Table 2.

Table 2. Euclidean number fields from Theorem 3

n	D	m	$\tilde{\alpha}_n^{(Q)}\sqrt{\lvert D\rvert}$	Earlier reference
4	2000	4	3.491	
4	2225	4	3.682	[G 65]
4	2525	$\geqslant 4$	3.923	
4	2624	4	3.999	[G 65]
5	24217	5	4.478	
5	38569	7	5.651	
6	453789	7	6.809	
6	485125	9	7.040	
6	703493	$\geqslant 9$	8.477	

We let ζ_n denote a primitive nth root of unity, $\theta = -\zeta_5 - \bar{\zeta}_5$ a generator of $\boldsymbol{Q}(\sqrt{5})$ satisfying $\theta^2 - \theta - 1 = 0$, and $\eta = \zeta_7 + \bar{\zeta}_7$ a generator of the cyclic cubic field of discriminant 49, satisfying $\eta^3 + \eta^2 - 2\eta - 1 = 0$. In any field containing $\boldsymbol{Q}(\sqrt{5})$, $\{0, 1, \theta, \theta^2\}$ is an exceptional sequence of length 4; similarly, any field containing $\boldsymbol{Q}(\eta)$ has the exceptional sequence $\{0, 1, \eta, \eta^{-1}, 3-\eta^2, \eta+1, \eta^2+\eta-1\}$ of length 7 (cf. [Le 77, (2.4b), (3.4)] and [LN 87, 3.1]). All fields in our list are characterized by their signatures and discriminants, and may be found in the tables of [PWZ 82] or [PZ 89].

4.1. $n = 4$, $D = 2000 = 2^4 5^3$ (fifth smallest discriminant). Abelian field generated by $\zeta_{20} + \bar{\zeta}_{20} = \sqrt{2+\theta}$. The subfield $\boldsymbol{Q}(\sqrt{5})$ gives $m = 4$, which is best possible since 2 is the square of an ideal of norm 4. This is a new euclidean field.

4.2. $n = 4$, $D = 2225 = 5^2 89$ (seventh discriminant). Ray class field over $Q(\sqrt{5})$ with conductor the prime ideal $(9+\theta)$ of norm 89 (or its conjugate), generated by a root of $X^2+\theta X-2$. We have $m = 4$ from the subfield. See [G 65].

4.3. $n = 4$, $D = 2525 = 5^2 101$ (ninth discriminant, [G 56]). Ray class field over $Q(\sqrt{5})$ with conductor the prime ideal $(9+4\theta)$ of norm 101 (or its conjugate), generated by a root of $X^2+X-(2+\theta)$. Again $m \geqslant 4$ is guaranteed by the subfield; the presence of prime ideals of norm 5 implies $m \leqslant 5$. This is a new euclidean field.

4.4. $n = 4$, $D = 2624 = 2^6 41$ (tenth discriminant). Class field of conductor $(7+2\sqrt{2})$ of norm 41 over $Q(\sqrt{2})$, generated by a root x of $X^2+(1+\sqrt{2})X-1$ (the ray class field has degree eight). $\{0, 1, x, x+1\}$ is an exceptional sequence by [Le 77, (2.4b)] applied to the minimal polynomial $X^4+2X^3-3X^2-2X+1$ of x over Q; hence $m = 4$, which is best possible. See [G 65].

4.5. $n = 5$, $D = 24217 = 61 \cdot 397$ (second discriminant [P 75]). The field is generated by a root x of $X^5+2X^4-4X^3-3X^2+2X+1$. [Le 77, (2.4d)] yields the exceptional sequence $\{0, 1, x+1, x^2\}$ and $m = 5$ (best possible). This is a new euclidean field, and so are the remaining four.

4.6. $n = 5$, $D = 38569$ (a prime; fourth discriminant [P 75]). Field generated by a root x of X^5-5X^3+4X+1. From [LM 82, (3.2)A] we have the exceptional sequence $\{0, 1, x, x+1, x^2, x/(x-1), 1/(2-x)\}$ of length 7 (best possible).

4.7. $n = 6$, $D = 453789 = 3^3 7^5$ (fourth discriminant). Ray class field of conductor $(3)\cdot(2-\eta)$ over $Q(\eta)$ (the second factor being the unique prime ideal of norm 7), generated by a root of $X^2+(\eta^2+\eta-1)X+(\eta-1)$. Since $(2-\eta)$ ramifies again in the extension, the value $m = 7$ guaranteed by the subfield is best possible.

4.8. $n = 6$, $D = 485125 = 5^3 3881$ (fifth discriminant [BMO 88]). Non-Galois extension of $Q(\sqrt{5})$, generated by a root of $X^3+X^2+(\theta-3)X+(\theta-2)$, or by a root x of the polynomial $X^3-\theta^{-2}X^2-\theta^2X-\theta^{-1}$ of norm $X^6-3X^5-2X^4+8X^3+2X^2-4X-1$ over Q. The sequence [LM 82, (3.3)A2]

$$\left\{0, 1, x, x+1, x^2, \frac{x}{x-1}, \frac{1}{2-x}, \frac{x^2-1}{x^2-x-1}, \frac{-x^2}{x^3-2x^2-x+1}\right\}$$

shows $m = 9$ (best possible).

4.9. $n = 6$, $D = 703493 = 7^4 293$ (seventh discriminant). Ray class field of conductor $(\eta^2-2\eta+5)$ (or a conjugate), a prime ideal of norm 293, generated by a root x of $X^2+(1-\eta)X-1$. The bound to be met is ≈ 8.477, so the sequence in the subfield $Q(\eta)$ is too short; on the other hand, $m \leqslant 13$ from the splitting behaviour of small primes. A. Leutbecher and the first author found the exceptional sequence

$$\left\{0, 1, x, 1-x, \frac{1}{x+1}, \frac{x}{x+1}, \frac{x+1}{x+2}, (2-\eta^2)x, (1-\eta-\eta^2)x\right\}$$

of length 9 by explicit calculation. ∎

There is little hope of Theorem 3 yielding any euclidean fields in degrees $n \geqslant 7$. For $n = 7$, the minimal discriminant is 20134393 [P 77], leading to a bound of ≈ 15.815, but all fields of reasonably small discriminants known in this signature have ideals of norm 7, 9 or 13. The situation in degrees 8 and 9 is similar, and beyond this not even candidates for the totally real fields of minimal discriminant are known.

Acknowledgements. It is our pleasure to express our gratitude to Professors A. Leutbecher and J. Martinet for many interesting discussions accompanying our work, and to Professor H. W. Lenstra for having provided its *raison d'être* and for valuable suggestions concerning the formulation of our lemma. A careful referee has saved us from a number of errors and omissions; any remaining flaws in our exposition are our own.

Note added in proof (February 1991): As we have discovered only recently, H. Davenport (*The product of n homogeneous linear forms*, Indag. Math. 8 (1946), 525–531) had already obtained slightly better values for τ_n and τ under the same conditions as in our Lemma; indeed his values can be shown to be best possible under those conditions. Using the improved $\tau_6 \gtrsim 1.494$, we can now also prove the sextic field of sixth smallest (prime) discriminant 592661 to be euclidean: One has $\alpha_6^{(D)}\sqrt{|D|} < 6.783$ and $m = 7$ on account of [LM 82, (3.2)A] – the same sequence as in 4.6 above – applied to a root of the polynomial $X^6-5X^5+5X^4+6X^3-8X^2-X+1$.

References

[BMO 88] A.-M. Bergé, J. Martinet and M. Olivier, *The computation of sextic fields with a quadratic subfield*, Preprint, Bordeaux 1988; to appear.

[G 56] H. J. Godwin, *Real quartic fields with small discriminant*, J. London Math. Soc. 31 (1956), 478–485.

[G 65] – *On Euclid's algorithm in some quartic and quintic fields*, ibid. 40 (1965), 699–704.

[GL 87] P. M. Gruber and C. G. Lekkerkerker, *Geometry of Numbers*, 2nd ed., North-Holland, Amsterdam 1987.

[HW 79] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford University Press, Oxford 1979.

[Le 74] H. W. Lenstra, jr., *Lectures on euclidean rings*, Mimeographed lecture notes, Bielefeld, summer 1974.

[Le 77] – *Euclidean number fields of large degree*, Invent. Math. 38 (1977), 237–254.

[Le 80] – *Euclidean number fields (II)*, Math. Intelligencer 2 # 2 (1980), 73–77.

[LM 82] A. Leutbecher and J. Martinet, *Lenstra's constant and euclidean number fields*, Journées Arithmétiques Metz 1981, Astérisque 94 (1982), 87–131.

[LN 87] A. Leutbecher and G. Niklasch, *On cliques of exceptional units and Lenstra's construction of euclidean fields*, Journées Arithmétiques Ulm 1987 (E. Wirsing, ed.), Lecture Notes in Math. 1380, Springer, Heidelberg *et al.* 1989.

[OM 65] O. T. O'Meara, *On the finite generation of linear groups over Hasse domains*, J. Reine Angew. Math. 217 (1965), 79–108.

[P 75] M. Pohst, *Berechnung kleiner Diskriminanten total reeller algebraischer Zahlkörper*, ibid. 278/279 (1975), 278–300.

[P 77] — *The minimum discriminant of seventh degree totally real number fields*, in: *Number Theory and Algebra*, H. Zassenhaus (ed.), Academic Press, New York *et al.* 1977, 235–240.

[PWZ 82] M. Pohst, P. Weiler and H. Zassenhaus, *On effective computation of fundamental units (II)*, Math. Comp. 38 # 157 (1982), 293–329.

[PZ 89] M. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge University Press, Cambridge 1989.

[Q 82] R. Quême, *Étude des algorithmes de divisibilité et de factorisation des anneaux et monoïdes de fractions*, Thèse de 3ème cycle, Université d'Orsay, 1982.

[R 64] C. A. Rogers, *Packing and Covering*, Cambridge University Press, Cambridge 1964.

MATHEMATISCHES INSTITUT
TECHNISCHE UNIVERSITÄT MÜNCHEN
Postfach 20 24 20, D-W8000 München 2
Germany

32 Hameau de la Caravelle
Port Sud
F-91650 Breuillet
France

Received on 17.11.1989
and in revised form on 12.3.1990 (1990)

ACTA ARITHMETICA
LVIII.2 (1991)

The density of the set of sums

by

IMRE Z. RUZSA* (Budapest)

Let $1 \leqslant a_1 \leqslant a_2 \leqslant \ldots$ be a sequence of integers, and let S be the set of all sums of the form $\sum e_i a_i$, where $e_i = 0$ or 1.

THEOREM. *If*

(1) $$a_{n+1} \leqslant 2a_n$$

for all but at most finitely many values of n, then S has an asymptotic density.

This problem was proposed by U. Zannier at the 1989 September number theory conference in Amalfi. In [1], he proves the same conclusion under the stronger assumption that $a_{n+1} \sim a_n$. I heard it from P. Erdős at the DIMACS conference in October 1989. He also asked how (1) can be weakened, in particular, whether

(2) $$a_n \leqslant a_1 + a_2 + \ldots + a_{n-1} + c$$

is sufficient. My proof makes a heavy use of (1). It is easy to see that if we do not impose any restriction on the sequence (a_i), then S need not have a density. Taking long intervals and large gaps in (a_i) one can easily achieve $\bar{d}(S) = 1$ and $\underline{d}(S) = c$ for an arbitrary prescribed number $0 \leqslant c \leqslant 1$, and I believe even $\underline{d}(S) = c$, $\bar{d}(S) = C$ is possible with an arbitrary pair of numbers $0 \leqslant c \leqslant C \leqslant 1$.

(1) or (2) implies that $\underline{d}(S) > 0$, even that S has bounded gaps.

$S(x)$ will denote the number of integers $s \in S$, $1 \leqslant s \leqslant x$.

LEMMA 1. *If* $x = a_{i_1} + a_{i_2} + \ldots + a_{i_k}$, *where* $i_1 > i_2 > \ldots > i_k$ *and* $y < a_{i_k}$, *then*

(3) $$S(x+y) \geqslant S(x) + S(y).$$

Indeed, all the numbers $x+s$, where $s \in S$, $1 \leqslant s \leqslant y$, are elements of S between x and $x+y$.

Write

$$u = \underline{d}(S), \quad v = \bar{d}(S).$$

* Supported by DIMACS Center for Discrete Mathematics and Theoretical Computer Science, a National Science Foundation Science and Technology Center – NSF-STC88-09648.