EUCLID'S ALGORITHM IN CYCLOTOMIC FIELDS

H. W. LENSTRA, JR.

Introduction

For a positive integer m, let ζ_m denote a primitive m-th root of unity. By ϕ we mean the Euler ϕ-function. In this paper we prove the following theorem.

THEOREM. *Let* $\phi(m) \leqslant 10$, $m \neq 16$, $m \neq 24$. *Then* $\mathbf{Z}[\zeta_m]$ *is Euclidean for the usual norm map.*

Since $\mathbf{Z}[\zeta_m] = \mathbf{Z}[\zeta_{2m}]$ for m odd, this gives eleven non-isomorphic Euclidean rings, corresponding to $m = 1, 3, 4, 5, 7, 8, 9, 11, 12, 15, 20$. The cases $m = 1, 3, 4, 5, 8, 12$ are more or less classical [**2** (pp. 117–118 and pp. 391–393); **8**; **5** (pp. 228–231); **3** (chapters 12, 14 and 15); **4**; **7**]. The other five cases are apparently new.

For m even, the ring $\mathbf{Z}[\zeta_m]$ has class number one if and only if $\phi(m) \leqslant 20$ or $m = 70$, 84 or 90, see [**6**]. So there are exactly thirty non-isomorphic rings $\mathbf{Z}[\zeta_m]$ which admit unique factorization. If certain generalized Riemann hypotheses would hold, then all these thirty rings would be Euclidean for some function different from the norm map [**9**].

1. *The general measure and Euclid's algorithm*

In this section K denotes an algebraic number field of finite degree d over $\mathbf{Q}$, and $K_{\mathbf{R}}$ is the $\mathbf{R}$-algebra $K \otimes_{\mathbf{Q}} \mathbf{R}$. Following Gauss [**2**; p. 395] we define the *general measure* $\mu : K_{\mathbf{R}} \to \mathbf{R}$ by

$$\mu(x) = \sum_{\sigma} |\sigma(x)|^2, \quad \text{for} \quad x \in K_{\mathbf{R}},$$

the sum ranging over the d different $\mathbf{R}$-algebra homomorphisms $\sigma \colon K_{\mathbf{R}} \to \mathbf{C}$, (*cf.* [**1**]). It is easily seen that μ is a positive definite quadratic form on the $\mathbf{R}$-vector space $K_{\mathbf{R}}$.

Let R be a subring of K which is integral over $\mathbf{Z}$ and has K as its field of fractions. Then R is a lattice of maximal rank d in $K_{\mathbf{R}}$. The *fundamental domain* F with respect to R is defined by

$$F = \{x \in K_{\mathbf{R}} \mid \mu(x) \leqslant \mu(x-y) \quad \text{for all} \quad y \in R\}.$$

This is a compact subset of $K_{\mathbf{R}}$ which satisfies

$$F + R = K_{\mathbf{R}}. \tag{1.1}$$

Let

$$c = \max\{\mu(x) \mid x \in F\}.$$

A real number c' is called a *bound* for F if $c' \geqslant c$. A bound c' for F is *usable* if for every $x \in F \cap K$ satisfying $\mu(x) = c'$ there is a root of unity $u \in R$ such that $\mu(x-u) = c'$. Note that every real number $c' > c$ is a usable bound, since no $x \in F$ satisfies $\mu(x) = c' > c$.

Received 14 May, 1974.

[J. LONDON MATH. SOC. (2), 10 (1975), 457–465]

The *norm* $N : K_{\mathbf{R}} \to \mathbf{R}$ is defined by

$$N(x) = \prod_{\sigma} |\sigma(x)|, \quad \text{for} \quad x \in K_{\mathbf{R}},$$

the product ranging over the $\mathbf{R}$-algebra homomorphisms $\sigma : K_{\mathbf{R}} \to \mathbf{C}$. The arithmetic-geometric mean inequality implies

$$(1.2) \qquad N(x)^2 \leqslant (\mu(x)/d)^d, \quad \text{for} \quad x \in K_{\mathbf{R}},$$

the equality sign holding if and only if $|\sigma(x)|^2 = |\tau(x)|^2$ for all $\mathbf{R}$-algebra homomorphisms $\sigma, \tau : K_{\mathbf{R}} \to \mathbf{C}$.

For $x \in R$, $x \neq 0$, we have $N(x) = |R/Rx|$. The ring R is called *Euclidean for the norm* if for every $a, b \in R$, $b \neq 0$, there are $q, r \in R$ such that $a = qb + r$ and $N(r) < N(b)$. Using the multiplicativity of the norm one easily proves that R is Euclidean for the norm if and only if for each $x \in K$ there exists $y \in R$ such that $N(x-y) < 1$.

In the rest of this section we assume that every cube root of unity contained in K is actually contained in R. This condition is necessary for R to be Euclidean, since any unique factorization domain is integrally closed inside its field of fractions. Notice that the condition is satisfied if $K = \mathbf{Q}(\zeta_m)$ and $R = \mathbf{Z}[\zeta_m]$ for some integer $m \geqslant 1$.

(1.3) LEMMA. *Let $x \in K$ be such that $|\sigma(x)|^2 = 1$ and $|\sigma(x-u)|^2 = 1$ for some root of unity $u \in R$ and some field homomorphism $\sigma : K \to \mathbf{C}$. Then $x \in R$.*

Proof. Let $y = \sigma(-xu^{-1}) \in \mathbf{C}$; then $y\bar{y} = 1$ and $y + \bar{y} = -1$, so y is a cube root of unity. Since $\sigma : K \to \mathbf{C}$ is injective, it follows that $-xu^{-1}$ is a cube root of unity in K. Therefore our assumption on R implies that $-xu^{-1} \in R$; hence

$$x = (-xu)^{-1}.(-u) \in R.$$

(1.4) PROPOSITION. *If d is a usable bound for F, then R is Euclidean for the norm.*

Proof. Let $x \in K$ be arbitrary; we have to exhibit an element $y \in R$ for which $N(x-y) < 1$. Using (1.1) we reduce to the case $x \in F$. Then $\mu(x) \leqslant d$, since d is a bound for F. If the inequality is strict, then $N(x) < 1$ by (1.2), and we can take $y = 0$. If the equality sign holds, then $\mu(x) = \mu(x-u) = d$ for some root of unity $u \in R$, since d is usable. We get

$$N(x)^2 \leqslant (\mu(x)/d)^d = 1,$$
$$N(x-u)^2 \leqslant (\mu(x-u)/d)^d = 1.$$

If at least one strict inequality holds, then we can take $y = 0$ or $y = u$. If both equality signs hold, then

$$|\sigma(x)|^2 = |\tau(x)|^2, \qquad |\sigma(x-u)|^2 = |\tau(x-u)|^2$$

for all $\sigma, \tau : K \to \mathbf{C}$, and since

$$\prod_{\sigma} |\sigma(x)|^2 = N(x)^2 = 1,$$
$$\prod_{\sigma} |\sigma(x-u)|^2 = N(x-u)^2 = 1$$

it follows that $|\sigma(x)|^2 = |\sigma(x-u)|^2 = 1$ for all σ. But then (1.3) asserts $x \in R$, contradicting $x \in F$ since $x \neq 0$.

2. *Cyclotomic fields*

In the case when $K = \mathbf{Q}(\zeta_m)$ and $R = \mathbf{Z}[\zeta_m]$ for some integer $m \geqslant 1$, we write μ_m, F_m and c_m instead of μ, F and c, respectively. The function $\mathrm{Tr}_m : \mathbf{Q}(\zeta_m)_{\mathbf{R}} \to \mathbf{R}$ denotes the natural extension of the trace $\mathbf{Q}(\zeta_m) \to \mathbf{Q}$. The field automorphism of $\mathbf{Q}(\zeta_m)$ which sends ζ_m to ζ_m^{-1} extends naturally to an $\mathbf{R}$-algebra automorphism of $\mathbf{Q}(\zeta_m)_{\mathbf{R}}$, which is called *complex conjugation* and denoted by an overhead bar. For $x \in \mathbf{Q}(\zeta_m)_{\mathbf{R}}$, we have

$$\mu_m(x) = \mathrm{Tr}_m(x\bar{x}). \tag{2.1}$$

Note that a similar formula holds for arbitrary K, if complex conjugation is suitably defined.

(2.2) PROPOSITION. *Let n be a positive divisor of m, and*

$$e = [\mathbf{Q}(\zeta_m) : \mathbf{Q}(\zeta_n)] = \phi(m)/\phi(n).$$

Then $c_m \leqslant e^2 . c_n$. Moreover, if c' is a usable bound for F_n, then $e^2 . c'$ is a usable bound for F_m.

The proof of (2.2) relies on the relative trace function $\mathbf{Q}(\zeta_m) \to \mathbf{Q}(\zeta_n)$ and its natural extension $\mathbf{Q}(\zeta_m)_{\mathbf{R}} \to \mathbf{Q}(\zeta_n)_{\mathbf{R}}$, notation: Tr. This is a $\mathbf{Q}(\zeta_n)_{\mathbf{R}}$-linear map, given by

$$\mathrm{Tr}\,(x) = \sum_{\sigma \in G} \sigma(x), \quad \text{for} \quad x \in \mathbf{Q}(\zeta_m)_{\mathbf{R}},$$

where G denotes the Galois group of $\mathbf{Q}(\zeta_m)$ over $\mathbf{Q}(\zeta_n)$, acting naturally on $\mathbf{Q}(\zeta_m)_{\mathbf{R}}$. We have $\mathrm{Tr}_m = \mathrm{Tr}_n \circ \mathrm{Tr}$, and one easily proves that Tr commutes with complex conjugation.

(2.3) LEMMA. *Let $x \in \mathbf{Q}(\zeta_m)_{\mathbf{R}}$ and $y \in \mathbf{Q}(\zeta_n)_{\mathbf{R}}$. Then*

$$\mu_m(x) - \mu_m(x-y) = e\left(\mu_n\left(\frac{1}{e}\,\mathrm{Tr}\,(x)\right) - \mu_n\left(\frac{1}{e}\,\mathrm{Tr}\,(x) - y\right)\right).$$

Proof. Using (2.1), we find:

$$\begin{aligned} & e\left(\mu_n\left(\frac{1}{e}\,\mathrm{Tr}\,(x)\right) - \mu_n\left(\frac{1}{e}\,\mathrm{Tr}\,(x) - y\right)\right) \\ &= e . \mathrm{Tr}_n\left(\frac{1}{e}\,\mathrm{Tr}\,(x)\,\bar{y} + \frac{1}{e}\,\mathrm{Tr}\,(\bar{x})\,y - y\bar{y}\right) \\ &= \mathrm{Tr}_n(\mathrm{Tr}\,(x)\,\bar{y} + \mathrm{Tr}\,(\bar{x})\,y - e . y\bar{y}) \\ &= \mathrm{Tr}_n\,(\mathrm{Tr}\,(x\bar{y}) + \mathrm{Tr}\,(\bar{x}y) - \mathrm{Tr}\,(y\bar{y})) \\ &= \mathrm{Tr}_m(x\bar{y} + \bar{x}y - y\bar{y}) \\ &= \mu_m(x) - \mu_m(x-y). \end{aligned}$$

(2.4) LEMMA. *For $x \in \mathbf{Q}(\zeta_m)_{\mathbf{R}}$, we have*

$$\mu_m(x) = \frac{1}{m} \sum_{j=1}^{m} \mu_n(\mathrm{Tr}\,(x\zeta_m^{\,j})).$$

Proof. In the computation below $\sum_\sigma$ and $\sum_\tau$ refer to summations over G.

$$\sum_{j=1}^{m} \mu_n(\mathrm{Tr}\,(x\zeta_m{}^j)) = \sum_{j=1}^{m} \mu_n\left(\sum_\sigma \sigma(x\zeta_m{}^j)\right)$$

$$= \mathrm{Tr}_n\left(\sum_{j=1}^{m} \sum_\sigma \sum_\tau \sigma(x)\,\sigma(\zeta_m{}^j)\,\tau(\bar{x})\,\tau(\zeta_m{}^{-j})\right)$$

$$= \mathrm{Tr}_n\left(\sum_\sigma \sum_\tau \sigma(x)\,\tau(\bar{x})\left(\sum_{j=1}^{m} (\sigma(\zeta_m)\,\tau(\zeta_m)^{-1})^j\right)\right).$$

For $\sigma,\ \tau \in G$, let $\zeta_{\sigma,\tau}$ denote the m-th root of unity $\sigma(\zeta_m)\,\tau(\zeta_m)^{-1}$. Then $\zeta_{\sigma,\tau} = 1$ if and only if $\sigma = \tau$, and

$$\sum_{j=1}^{m} \zeta_{\sigma,\tau}^j = 0 \quad \text{if} \quad \zeta_{\sigma,\tau} \neq 1,$$

$$= m \quad \text{if} \quad \zeta_{\sigma,\tau} = 1.$$

Hence the above expression becomes

$$\mathrm{Tr}_n\left(\sum_\sigma \sigma(x)\,\sigma(\bar{x})\,m\right) = m.\mathrm{Tr}_n(\mathrm{Tr}\,(x\bar{x})) = m.\mathrm{Tr}_m(x\bar{x}) = m.\mu_m(x).$$

This proves (2.4).

Proof of (2.2). Let $x \in F_m$; we have to prove $\mu_m(x) \leqslant e^2.c_n$. Applying (2.3) with $y \in \mathbf{Z}[\zeta_n]$ we find that $x \in F_m$ implies $(1/e)\,\mathrm{Tr}\,(x) \in F_n$. Since also $x\zeta_m{}^j$ belongs to F_m, for $j \in \mathbf{Z}$, we have in the same way $(1/e)\,\mathrm{Tr}\,(x\zeta_m{}^j) \in F_n$. Therefore

$$\mu_n(\mathrm{Tr}\,(x\zeta_m{}^j)) = e^2.\mu_n\left(\frac{1}{e}\,\mathrm{Tr}\,(x\zeta_m{}^j)\right) \leqslant e^2.c_n$$

for all $j \in \mathbf{Z}$, and (2.4) implies that $\mu_m(x) \leqslant e^2.c_n$. This proves that $c_m \leqslant e^2.c_n$. Next assume that c' is a usable bound for F_n, and let $x \in F_m \cap \mathbf{Q}(\zeta_m)$ satisfy $\mu_m(x) = e^2.c'$. Then the above reasoning implies that $c' = c_n$ and

$$\mu_n\left(\frac{1}{e}\,\mathrm{Tr}\,(x\zeta_m{}^j)\right) = c_n = c' \quad \text{for all } j \in \mathbf{Z}.$$

Taking $j = 0$ we find that $(1/e)\,\mathrm{Tr}\,(x)$ is an element of $F_n \cap \mathbf{Q}(\zeta_n)$ for which

$$\mu_n\left(\frac{1}{e}\,\mathrm{Tr}\,(x)\right) = c'.$$

Since c' is a usable bound for F_n, there is a root of unity $u \in \mathbf{Z}[\zeta_n]$ such that

$$\mu_n\left(\frac{1}{e}\,\mathrm{Tr}\,(x) - u\right) = c'.$$

Applying (2.3) with $y = u$ we get $\mu_m(x-u) = \mu_m(x) = e^2.c'$, which proves that $e^2.c'$ is a usable bound for F_m.

Without proof we remark that the equality sign holds in (2.2) if m and n are divisible by the same primes.

Since $c_1 = \frac{1}{4}$ is a usable bound for F_1, we conclude from (2.2) that $\frac{1}{4}\phi(m)^2$ is a usable bound for F_m, for any m. If $\phi(m) \leqslant 4$, then it follows that $\phi(m)$ is a usable bound for F_m, and that $\mathbf{Z}[\zeta_m]$ is Euclidean for the norm, by (1.4). This gives us exactly the cases $m = 1, 3, 4, 5, 8, 12$ which were already known. In §4 we will obtain better results by applying (2.2) to a prime divisor n of m.

3. *A computation in linear algebra*

Let $n \geqslant 2$ be an integer, and let V be an $(n-1)$-dimensional $\mathbf{R}$-vector space with generators e_i, $1 \leqslant i \leqslant n$, subject only to the relation $\sum_{i=1}^{n} e_i = 0$. The positive definite quadratic form q on V is defined by

$$q(x) = \sum_{1 \leqslant i < j \leqslant n} (x_i - x_j)^2, \quad \text{for} \quad x = \sum_{i=1}^{n} x_i e_i \in V.$$

Denote by $(\ ,\ ) : V \times V \to \mathbf{R}$ the symmetric bilinear form induced by q:

$$(x, y) = \tfrac{1}{2}(q(x+y) - q(x) - q(y)).$$

Then

$$(x, x) = q(x), \quad \text{for} \quad x \in V,$$
$$(e_i, e_i) = n-1, \quad \text{for} \quad 1 \leqslant i \leqslant n,$$
$$(e_i, e_j) = -1, \quad \text{for} \quad 1 \leqslant i < j \leqslant n.$$

The subgroup L of V generated by $\{e_i \mid 1 \leqslant i \leqslant n\}$ is a lattice of rank $n-1$ in V. The fundamental domain

$$E = \{x \in V \mid q(x) \leqslant q(x-y) \quad \text{for all} \quad y \in L\}$$
$$= \{x \in V \mid (x, y) \leqslant \tfrac{1}{2}q(y) \quad \text{for all} \quad y \in L\}$$

is a compact subset of V, and we put

$$b = \max\{q(x) \mid x \in E\}.$$

(3.1) Proposition. *The set of points $x \in E$ for which $q(x) = b$ is given by*

$$\left\{ \frac{1}{n} \sum_{i=1}^{n} i e_{\sigma(i)} \mid \sigma \text{ is a permutation of } \{1, 2, \ldots, n\} \right\}. \tag{3.2}$$

Moreover,

$$b = \frac{n^2-1}{12}.$$

This proposition is proved after a series of lemmas. We put $N = \{1, 2, \ldots, n\}$. For $A \subset N$, let $e_A = \sum_{i \in A} e_i$. We call A *proper* if $\varnothing \neq A \neq N$.

(3.3) Lemma. *Let $y \in L$ be such that $y \neq e_A$ for all $A \subset N$. Then there is an element $z = \pm e_j \in L$ such that*

$$q(z) + q(y-z) < q(y).$$

Proof. Let $y = \sum_{i=1}^{n} m_i e_i$ with $m_i \in \mathbf{Z}$. Using $\sum_{i=1}^{n} e_i = 0$ we may assume that $0 \leqslant \sum_{i=1}^{n} m_i \leqslant n-1$. For $z = \pm e_j$ we have

$$\tfrac{1}{2}(q(y) - q(z) - q(y-z)) = (y, z) - (z, z)$$
$$= \pm\left(nm_j - \sum_{i=1}^{n} m_i\right) - (n-1).$$

If this is >0 for some j and some choice of the sign we are done. Therefore suppose it is $\leqslant 0$ for all j and for both signs. Then for $1 \leqslant j \leqslant n$ we have

$$nm_j \leqslant \left(\sum_{i=1}^{n} m_i\right) + (n-1) \leqslant 2n-2 < 2n,$$

$$nm_j \geqslant \left(\sum_{i=1}^{n} m_i\right) - (n-1) \geqslant -n+1 > -n,$$

so $m_j \in \{0, 1\}$ for all j. Hence $y = e_A$ for some $A \subset N$, contradicting our assumption.

(3.4) LEMMA. *Let $x \in V$. Then $x \in E$ if and only if $(x, e_A) \leqslant \frac{1}{2}q(e_A)$ for all $A \subset N$.*

Proof. The "only if" part is clear. "If": we know that

$$(x, e_A) \leqslant \tfrac{1}{2}q(e_A) \quad \text{for all} \quad A \subset N$$

and we have to prove that

$$(x, y) \leqslant \tfrac{1}{2}q(y) \quad \text{for all} \quad y \in L.$$

This is done by an obvious induction on $q(y)$, using (3.3).

(3.5) LEMMA. *Let $x_0 \in E$ satisfy $q(x_0) = b$. Then there are $n-1$ different proper subsets $A(i) \subset N$, for $1 \leqslant i \leqslant n-1$, such that x_0 is the unique solution of the system of linear equations*

$$(x, e_{A(i)}) = \tfrac{1}{2}q(e_{A(i)}), \qquad 1 \leqslant i \leqslant n-1. \tag{3.6}$$

Proof. Put

$$S = \{A \subset N \mid (x_0, e_A) = \tfrac{1}{2}q(e_A)\},$$

then $(x_0, e_A) < \frac{1}{2}q(e_A)$ for each $A \subset N$, $A \notin S$. If the linear span of $\{e_A \mid A \in S\}$ has dimension $n-1$, then there are $n-1$ subsets $A(i) \in S$ such that $\{e_{A(i)} \mid 1 \leqslant i \leqslant n-1\}$ is linearly independent over $\mathbb{R}$. Then clearly x_0 is the unique solution of (3.6), and each $A(i)$ is proper since $e_{A(i)} \neq 0$.

Therefore suppose that the linear span of $\{e_A \mid A \in S\}$ has codimension $\geqslant 1$ in V. Then for some $z \in V$, $z \neq 0$, we have

$$(z, e_A) = 0 \quad \text{for all} \quad A \in S.$$

Multiplying z by a suitably chosen real number we can achieve that

$$\begin{aligned} &(x_0, z) \geqslant 0 \\ &(z, e_A) \leqslant \tfrac{1}{2}q(e_A) - (x_0, e_A) \quad \text{for all} \quad A \subset N, \quad A \notin S. \end{aligned} \tag{3.7}$$

Then for all $A \subset N$ we have $(x_0 + z, e_A) \leqslant \frac{1}{2}q(e_A)$, which implies $x_0 + z \in E$, by (3.4). But using (3.7) we find that

$$q(x_0+z) \geqslant q(x_0) + q(z) > q(x_0),$$

which contradicts our assumption $q(x_0) = b = \max\{q(x) \mid x \in E\}$.

(3.8) LEMMA. *Let $x_0 \in E$, and let $A, B \subset N$ be such that*

$$(x_0, e_A) = \tfrac{1}{2}q(e_A), \qquad (x_0, e_B) = \tfrac{1}{2}q(e_B).$$

Then $A \subset B$ or $B \subset A$.

Proof. Put $C = A-B$ and $D = B-A$. If $C = \varnothing$ or $D = \varnothing$ we are done, so suppose $C \neq \varnothing \neq D$. Then $C \cap D = \varnothing$ implies

$$(e_{A \cap B}, e_{A \cup B})-(e_A, e_B) = -(e_C, e_D) = |C|.|D| > 0.$$

Using $e_{A \cap B}+e_{A \cup B} = e_A+e_B$ we find that

$$\begin{aligned}(x_0, e_{A \cap B})+(x_0, e_{A \cup B}) &= (x_0, e_A)+(x_0, e_B)\\ &= \tfrac{1}{2}q(e_A)+\tfrac{1}{2}q(e_B)\\ &= \tfrac{1}{2}q(e_A+e_B)-(e_A, e_B)\\ &> \tfrac{1}{2}q(e_{A \cap B}+e_{A \cup B})-(e_{A \cap B}, e_{A \cup B})\\ &= \tfrac{1}{2}q(e_{A \cap B})+\tfrac{1}{2}q(e_{A \cup B}).\end{aligned}$$

Hence for $X = A \cap B$ or for $X = A \cup B$ we have $(x_0, e_X) > \frac{1}{2}q(e_X)$, contradicting $x_0 \in E$.

Proof of (3.1). Let $x_0 \in E$ satisfy $q(x_0) = b$, and let $\{A(i) \mid 1 \leqslant i \leqslant n-1\}$ be a system of $n-1$ proper subsets of N as in (3.5). By (3.8), this system is linearly ordered by inclusion. This is only possible if after a suitable renumbering of the vectors e_i and the sets $A(i)$ we have

$$A(i) = \{i+1, i+2, \ldots, n\}, \quad \text{for} \quad 1 \leqslant i \leqslant n-1.$$

By (3.5) we have

$$\sum_{j=i+1}^{n} (x_0, e_j) = \tfrac{1}{2}q(e_{A(i)}) = \tfrac{1}{2}i(n-i), \quad \text{for} \quad 1 \leqslant i \leqslant n-1.$$

Write $x_0 = \sum_{j=1}^{n} x_j e_j$ in such a manner that $\sum_{j=1}^{n} x_j = 0$. Then $(x_0, e_j) = nx_j$; so our system becomes

$$\sum_{j=i+1}^{n} nx_j = \tfrac{1}{2}i(n-i), \quad \text{for} \quad 0 \leqslant i \leqslant n-1.$$

This implies

$$nx_i = i-\tfrac{1}{2}(n+1), \quad \text{for} \quad 1 \leqslant i \leqslant n,$$

$$x_0 = \frac{1}{n} \sum_{i=1}^{n} ie_i.$$

We renumbered the e_i once; so we conclude that x_0 is in the set (3.2). Since at least one $x_0 \in E$ satisfies $q(x_0) = b$, it follows for reasons of symmetry that conversely every element x of (3.2) satisfies $x \in E$ and $q(x) = b$. Finally,

$$b = \sum_{1 \leqslant i < j \leqslant n} (i-j)^2/n^2 = (n^2-1)/12.$$

This proves (3.1).

4. *Proof of the theorem*

(4.1) PROPOSITION. *Let n be a prime number. Then $c_n = (n^2-1)/12$, and this is a usable bound for F_n.*

Proof. We apply the results of §3. The $\mathbf{R}$-vector space $\mathbf{Q}(\zeta_n)_{\mathbf{R}}$ is generated by n elements $\zeta_n{}^i$, $1 \leqslant i \leqslant n$, subject only to the relation $\sum_{i=1}^{n} \zeta_n{}^i = 0$. For real numbers

x_i, $1 \leqslant i \leqslant n$, we have

$$\mu_n\left(\sum_{i=1}^{n} x_i \zeta_n^{\,i}\right) = \mathrm{Tr}_n\left(\sum_{i=1}^{n}\sum_{j=1}^{n} x_i x_j \zeta_n^{\,i-j}\right)$$

$$= n\,.\sum_{i=1}^{n} x_i^2 - \sum_{i=1}^{n}\sum_{j=1}^{n} x_i x_j$$

$$= \sum_{1 \leqslant i < j \leqslant n} (x_i - x_j)^2.$$

Therefore there is an isomorphism of quadratic spaces $(\mathbf{Q}(\zeta_n)_{\mathbf{R}}, \mu_n) \cong (V, q)$ which maps $\zeta_n^{\,i}$ to e_i, for $1 \leqslant i \leqslant n$. Clearly, $\mathbf{Z}[\zeta_n]$ corresponds to L, so F_n corresponds to E and $c_n = b$. Translating (3.1) we find: $c_n = (n^2-1)/12$, and the set of $x \in F_n$ for which $\mu_n(x) = c_n$ is given by

$$\left\{\frac{1}{n}\sum_{i=1}^{n} i\zeta_n^{\,\sigma(i)} \mid \sigma \text{ is a permutation of } \{1, 2, \ldots, n\}\right\}. \tag{4.2}$$

Let x be in this set. Putting $\sigma(0) = \sigma(n)$ we have

$$x - \zeta_n^{\,\sigma(n)} = \frac{1}{n}\sum_{i=0}^{n-1} i\zeta_n^{\,\sigma(i)} = \frac{1}{n}\sum_{j=1}^{n} j\zeta_n^{\,\sigma(j-1)}.$$

This element belongs to the set (4.2), so $\mu_n(x - \zeta_n^{\,\sigma(n)}) = c_n$, which proves usability of c_n.

We turn to the proof of the theorem. The cases $m = 1, 3, 4, 5, 8, 12$ have been dealt with in §2. Further, (2.2) and (4.1) imply that

$$c_7 = 4 < 6 = \phi(7),$$
$$c_9 \leqslant 3^2 . c_3 = 6 = \phi(9),$$
$$c_{11} = 10 = \phi(11),$$
$$c_{15} \leqslant 2^2 . c_5 = 8 = \phi(15),$$
$$c_{20} \leqslant 2^2 . c_5 = 8 = \phi(20),$$

and in each of these cases $\phi(m)$ is a usable bound for F_m. Application of (1.4) concludes the proof.

Without proof we remark that our method does not apply to other fully cyclotomic fields:

(4.3) PROPOSITION. *Let $m \geqslant 1$ be an integer for which $c_m \leqslant \phi(m)$. Then $\phi(m) \leqslant 10$ and $m \neq 16$, $m \neq 24$.*

References

1. J. W. S. Cassels, " On a conjecture of R. M. Robinson about sums of roots of unity ", *J. Reine Angew. Math.*, 238 (1969), 112–131.
2. C. F. Gauss, *Werke*, Zweiter Band (Göttingen, 1876).
3. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers* (Oxford, 1938).
4. R. B. Lakein, " Euclid's algorithm in complex quartic fields ", *Acta Arith.*, 20 (1972), 393–400.
5. E. Landau, *Vorlesungen über Zahlentheorie*, Band 3 (Leipzig, 1927).
6. J. M. Masley, *On the class number of cyclotomic fields* (thesis, Princeton University, 1972).

7. ———, " On cyclotomic fields Euclidean for the norm map ", *Notices Amer. Math. Soc.*, 19 (1972), A–813 (abstract 700–A3).

8. J. Ouspensky, " Note sur les nombres entiers dépendant d'une racine cinquième de l'unité ", *Math. Ann.*, 66 (1909), 109–112.

9. P. J. Weinberger, " On Euclidean rings of algebraic integers ", *Proc. Symp. Pure Math.*, 24 (Analytic Number Theory), 321–332 (*Amer. Math. Soc.*, 1973).

Mathematisch Instituut,
Universiteit van Amsterdam,
Amsterdam, The Netherlands.