EUCLID’S ALGORITHM IN CYCLOTOMIC FIELDS

H. W. LENSTRA, JR.

Introduction

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

Theorem. Let $\phi(m) \leq 10$, $m \neq 16$, $m \neq 24$. Then $\mathbb{Z}[\zeta_m]$ is Euclidean for the usual norm map.

Since $\mathbb{Z}[\zeta_m] = \mathbb{Z}[\zeta_{2m}]$ 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 $\mathbb{Z}[\zeta_m]$ has class number one if and only if $\phi(m) \leq 20$ or $m = 70, 84$ or 90, see [6]. So there are exactly thirty non-isomorphic rings $\mathbb{Z}[\zeta_m]$ 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 $\mathbb{Q}$, and $K_\mathbb{R}$ is the $\mathbb{R}$-algebra $K \otimes_\mathbb{Q} \mathbb{R}$. Following Gauss [2; p. 395] we define the general measure $\mu : K_\mathbb{R} \to \mathbb{R}$ by

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

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

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

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

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

$$(1.1) \quad F + R = K_\mathbb{R}.$$

Let

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

A real number $c'$ is called a bound for $F$ if $c' \geq c$. 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 \( N : K_{\mathbb{R}} \to \mathbb{R} \) is defined by
\[
N(x) = \prod_{\sigma} |\sigma(x)|, \quad \text{for } x \in K_{\mathbb{R}},
\]
the product ranging over the \( \mathbb{R} \)-algebra homomorphisms \( \sigma : K_{\mathbb{R}} \to \mathbb{C} \). The arithmetic-geometric mean inequality implies
\[
N(x)^2 \leq (\mu(x)/d)^d, \quad \text{for } x \in K_{\mathbb{R}}.
\]
the equality sign holding if and only if \(|\sigma(x)|^2 = |\tau(x)|^2\) for all \( \mathbb{R} \)-algebra homomorphisms \( \sigma, \tau : K_{\mathbb{R}} \to \mathbb{C} \).

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 \( K = \mathbb{Q}(\zeta_m) \) and \( R = \mathbb{Z}[\zeta_m] \) for some integer \( m > 1 \).

(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 \( \sigma : K \to \mathbb{C} \). Then \( x \in R \).

**Proof.** Let \( y = \sigma(-xu^{-1}) \in \mathbb{C} \); then \( y \bar{y} = 1 \) and \( y + \bar{y} = -1 \), so \( y \) is a cube root of unity. Since \( \sigma : K \to \mathbb{C} \) 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
\[
x = (-xu)^{-1} \cdot (-u) \in R.
\]

(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 \( \mu(x) \leq d \), 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
\[
N(x)^2 \leq (\mu(x)/d)^d = 1,
\]
\[
N(x-u)^2 \leq (\mu(x-u)/d)^d = 1.
\]
If at least one strict inequality holds, then we can take \( y = 0 \) or \( y = u \). If both equality signs hold, then
\[
|\sigma(x)|^2 = |\tau(x)|^2, \quad |\sigma(x-u)|^2 = |\tau(x-u)|^2
\]
for all \( \sigma, \tau : K \to \mathbb{C} \), 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 \( \sigma \). But then (1.3) asserts \( x \in R \), contradicting \( x \in F \) since \( x \neq 0 \).
2. Cyclotomic fields

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

$$\mu_m(x) = \text{Tr}_m(x\bar{x}).$$

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

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

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

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

$$\text{Tr}(x) = \sum_{\sigma \in G} \sigma(x), \quad \text{for} \quad x \in \mathbb{Q}(\zeta_m)_R,$$

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

(2.3) Lemma. Let $x \in \mathbb{Q}(\zeta_m)_R$ and $y \in \mathbb{Q}(\zeta_n)_R$. Then

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

Proof. Using (2.1), we find:

$$e \left( \frac{1}{e} \text{Tr}(x) - \mu_n \left( \frac{1}{e} \text{Tr}(x-y) \right) \right)$$

$$= e \cdot \text{Tr}_n \left( \frac{1}{e} \text{Tr}(x) \bar{y} + \frac{1}{e} \text{Tr}(\bar{x}y - y\bar{y}) \right)$$

$$= \text{Tr}_n(\text{Tr}(x) \bar{y} + \text{Tr}(\bar{x})y - e \cdot y\bar{y})$$

$$= \text{Tr}_n(\text{Tr}(x\bar{y}) + \text{Tr}(\bar{x}y) - \text{Tr}(y\bar{y}))$$

$$= \text{Tr}_n(x\bar{y} + \bar{x}y - y\bar{y})$$

$$= \mu_n(x) - \mu_n(x-y).$$

(2.4) Lemma. For $x \in \mathbb{Q}(\zeta_m)_R$, we have

$$\mu_m(x) = \frac{1}{m} \sum_{j=1}^{m} \mu_n(\text{Tr}(x\zeta_m^j)).$$
Proof. In the computation below \( \sum_\sigma \) and \( \sum_\tau \) refer to summations over \( G. \)

\[
\sum_{j=1}^m \mu_n(\text{Tr}(x_{m}^{j})) = \sum_{j=1}^m \mu_n \left( \sum_\sigma \sigma(x_{m}^{j}) \right)
\]

\[
= \text{Tr}_n \left( \sum_{j=1}^m \sum_\sigma \sigma(x) \sigma(\zeta_m^j) \tau(\bar{\bar{x}}) \tau(\zeta_m^{-j}) \right)
\]

\[
= \text{Tr}_n \left( \sum_\sigma \sum_\tau \sigma(x) \tau(\bar{\bar{x}}) \left( \sum_{j=1}^m \left( \sigma(\zeta_m^j) \tau(\zeta_m^{-j}) \right) \right) \right).
\]

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

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

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

Hence the above expression becomes

\[
\text{Tr}_n \left( \sum_\sigma \sigma(x) \sigma(\bar{\bar{x}}) \right) m = m \cdot \text{Tr}_n(\text{Tr}(x \bar{x})) = m \cdot \text{Tr}_n(x \bar{x}) = m \cdot \mu_n(x).
\]

This proves (2.4).

Proof of (2.2). Let \( x \in F_n \); we have to prove \( \mu_n(x) \leq e^2 \cdot c_n \). Applying (2.3) with \( y \in \mathbb{Z}[\zeta_m] \) we find that \( x \in F_n \) implies \( (1/e) \text{Tr}(x) \in F_n \). Since also \( x_{m}^{j} \) belongs to \( F_n \), for \( j \in \mathbb{Z} \) we have in the same way \( (1/e) \text{Tr}(x_{m}^{j}) \in F_n \). Therefore

\[
\mu_n(\text{Tr}(x_{m}^{j})) = e^2 \cdot \mu_n \left( \frac{1}{e} \text{Tr}(x_{m}^{j}) \right) \leq e^2 \cdot c_n
\]

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

\[
\mu_n \left( \frac{1}{e} \text{Tr}(x_{m}^{j}) \right) = c_n = c' \quad \text{for all} \quad j \in \mathbb{Z}.
\]

Taking \( j = 0 \) we find that \( (1/e) \text{Tr}(x) \) is an element of \( F_n \cap \mathbb{Q}(\zeta_m) \) for which

\[
\mu_n \left( \frac{1}{e} \text{Tr}(x) \right) = c'.
\]

Since \( c' \) is a usable bound for \( F_n \), there is a root of unity \( u \in \mathbb{Z}[\zeta_m] \) such that

\[
\mu_n \left( \frac{1}{e} \text{Tr}(x - u) \right) = c'.
\]

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

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 \( \phi(m) \leq 4 \), then it follows that \( \phi(m) \) is a usable
bound for \( F_m \) and that \( \mathbb{Z}[[x]] \) 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 \( n \geq 2 \) be an integer, and let \( V \) be an \((n-1)\)-dimensional \( \mathbb{R} \)-vector space with generators \( e_i, 1 \leq i \leq n \), subject only to the relation \( \sum_{i=1}^{n} e_i = 0 \). The positive definite quadratic form \( q \) on \( V \) is defined by

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

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

\[
(x, y) = \frac{1}{2}(q(x+y) - q(x) - q(y)).
\]

Then

\[
(x, x) = q(x), \quad \text{for} \quad x \in V,
\]

\[
(e_i, e_i) = n-1, \quad \text{for} \quad 1 \leq i \leq n,
\]

\[
(e_i, e_j) = -1, \quad \text{for} \quad 1 \leq i < j \leq n.
\]

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

\[
E = \{ x \in V \mid q(x) \leq q(x-y) \quad \text{for all} \quad y \in L \}
\]

\[
= \{ x \in V \mid (x, y) \leq \frac{1}{2}q(y) \quad \text{for all} \quad y \in L \}
\]

is a compact subset of \( V \), and we put

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

(3.1) \textbf{Proposition.} \emph{The set of points \( x \in E \) for which \( q(x) = b \) is given by}

\[
\left\{ \frac{1}{n} \sum_{i=1}^{n} \sigma_{a(i)} \mid \sigma \text{ is a permutation of } \{1, 2, \ldots, n\} \right\}.
\]

Moreover,

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

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

(3.3) \textbf{Lemma.} \emph{Let } \( y \in L \text{ be such that } y \neq e_A \text{ for all } A \subseteq N \text{. Then there is an element } z = \pm e_j \in L \text{ such that }}

\[
q(z) + q(y-z) < q(y).
\]

\textbf{Proof.} Let \( y = \sum_{i=1}^{n} m_i e_i \) with \( m_i \in \mathbb{Z} \). Using \( \sum_{i=1}^{n} e_i = 0 \) we may assume that \( 0 \leq \sum_{i=1}^{n} m_i \leq n-1 \). For \( z = \pm e_j \) we have

\[
\frac{1}{2}(q(y) - q(z) - q(y-z)) = (y, z) - (z, z)
\]

\[
= \pm \left( nm_j - \sum_{i=1}^{n} m_i \right) - (n-1).
\]
If this is $>0$ for some $j$ and some choice of the sign we are done. Therefore suppose it is $\leq 0$ for all $j$ and for both signs. Then for $1 \leq j \leq n$ we have

$$\begin{align*}
nm_j &\leq \left( \sum_{i=1}^{n} m_i \right) + (n-1) \leq 2n-2 < 2n, \\
nm_j &\geq \left( \sum_{i=1}^{n} m_i \right) - (n-1) \geq -n+1 > -n,
\end{align*}$$

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 $(x, e_A) \leq \frac{1}{2}q(e_A)$ for all $A \subset N$.

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

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

and we have to prove that

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

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 $1 \leq i \leq n-1$, such that $x_0$ is the unique solution of the system of linear equations

$$
(x, e_{A(i)}) = \frac{1}{2}q(e_{A(i)}), \quad 1 \leq i \leq n-1.
$$

**Proof.** Put

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

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 $\{e_{A(i)} \mid 1 \leq i \leq n-1\}$ 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 $\geq 1$ in $V$. Then for some $z \in V, z \neq 0$, we have

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

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

$$
(x_0, z) \geq 0 \\
(z, e_A) \leq \frac{1}{2}q(e_A) - (x_0, e_A) \quad \text{for all } A \subset N, \quad A \notin S.
$$

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

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

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

$$(x_0, e_A) = \frac{1}{2}q(e_A), \quad (x_0, e_B) = \frac{1}{2}q(e_B).$$

Then $A \subset B$ or $B \subset A$. 
Proof. Put \( C = A - B \) and \( D = B - A \). If \( C = \emptyset \) or \( D = \emptyset \) we are done, so suppose \( C \neq \emptyset \neq D \). Then \( C \cap D = \emptyset \) implies
\[
(e_{A \cap B}, e_{A \cup B}) - (e_A, e_B) = -(e_C, e_D) = |C| \cdot |D| > 0.
\]
Using \( e_{A \cap B} + e_{A \cup B} = e_A + e_B \) we find that
\[
(x_0, e_{A \cap B}) + (x_0, e_{A \cup B}) = (x_0, e_A) + (x_0, e_B)
= \frac{1}{2}q(e_A) + \frac{1}{2}q(e_B)
= \frac{1}{2}q(e_A + e_B) - (e_A, e_B)
> \frac{1}{2}q(e_A + e_B) - (e_{A \cap B}, e_{A \cup B})
= \frac{1}{2}q(e_A + e_B) + \frac{1}{2}q(e_{A \cup B}).
\]
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 \( \{A(i) \mid 1 \leq i \leq n-1\} \) 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
\[
A(i) = \{i+1, i+2, \ldots, n\}, \quad \text{for} \quad 1 \leq i \leq n-1.
\]
By (3.5) we have
\[
\sum_{j=1}^{n} (x_0, e_j) = \frac{1}{2}q(e_{A(i)}) = \frac{1}{2}i(n-i), \quad \text{for} \quad 1 \leq i \leq n-1.
\]
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
\[
\sum_{j=1}^{n} nx_j = \frac{1}{2}i(n-i), \quad \text{for} \quad 0 \leq i \leq n-1.
\]
This implies
\[
x_i = i - \frac{1}{2}(n+1), \quad \text{for} \quad 1 \leq i \leq n,
\]
\[
x_0 = \frac{1}{n} \sum_{i=1}^{n} ie_i.
\]
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,
\[
b = \sum_{1 \leq i < j \leq n} (i-j)^2/n^2 = (n^2-1)/12.
\]
This proves (3.1).

4. Proof of the theorem

(4.1) Proposition. Let \( n \) be a prime number. Then \( e_n = (n^2-1)/12 \), and this is a usable bound for \( F_n \).

Proof. We apply the results of §3. The \( \mathbb{R} \)-vector space \( Q(\zeta_n)_{\mathbb{R}} \) is generated by \( n \) elements \( \zeta_n^i, 1 \leq i \leq n \), subject only to the relation \( \sum_{i=1}^{n} \zeta_n^i = 0 \). For real numbers
\[ x_i, \ 1 \leq i \leq n, \ \text{we have} \]
\[ \mu_n \left( \sum_{i=1}^{n} x_i \zeta_n^i \right) = \text{Tr}_n \left( \sum_{i=1}^{n} \sum_{j=1}^{n} x_i x_j \zeta_n^{i-j} \right) \]
\[ = n \cdot \sum_{i=1}^{n} x_i^2 - \sum_{i=1}^{n} \sum_{j=1}^{n} x_i x_j \]
\[ = \sum_{1 \leq i < j \leq n} (x_i - x_j)^2. \]

Therefore there is an isomorphism of quadratic spaces \((\mathbb{Q}(\zeta_n)/\mathbb{Q}), \mu_n) \cong (V, q)\) which maps \(\zeta_n^i \) to \(e_i\), for \(1 \leq i \leq n\). Clearly, \(\mathbb{Z}[\zeta_n]\) 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

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

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

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

This element belongs to the set (4.2), so \(\mu_n(x - \zeta_n^{\sigma(0)}) = c_n\), 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

\[ c_7 = 4 < 6 = \phi(7), \]
\[ c_9 \leq 3^2 \cdot c_3 = 6 = \phi(9), \]
\[ c_{11} = 10 = \phi(11), \]
\[ c_{15} \leq 2^2 \cdot c_5 = 8 = \phi(15), \]
\[ c_{20} \leq 2^2 \cdot c_5 = 8 = \phi(20), \]

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 \(m \geq 1\) be an integer for which \(c_m \leq \phi(m)\). Then \(\phi(m) \leq 10\) and \(m \neq 16, m \neq 24\).

**References**


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