Mathematisch Instituut
Roetersstraat 15
Amsterdam-C. The Netherlands

EUCLID'S ALGORITHM IN CYCLOTOMIC FIELDS

by H.W. Lenstra Jr.

Report 74-01

Received January 17, 1974

February 1974

EUCLID'S ALGORITHM IN CYCLOTOMIC FIELDS

H.W. Lenstra, Jr.

Abstract.
Eleven full cyclotomic rings are proved to be euclidean for the norm map.

AMS(MOS) subject classification scheme (1970):
12A35, 13F10, 10E20.

Keywords: Euclid's algorithm, cyclotomic field, Gauss measure.

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 note 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 [3, pp. 117-118 and pp. 391-393; 10; 7, pp. 228-231; 5, chapters 12, 14 and 15; 6; 9]. 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 [8]. So there are exactly thirty non-isomorphic rings $\mathbb{Z}[\zeta_m]$ which admit unique factorization. If some generalized Riemann hypotheses would hold, then all these thirty rings would be euclidean for some function, possibly different from the norm map [11].

Our notations are mostly standard. For μ_m, t_m, F_m and c_m see section 1. By an overhead bar we denote the automorphism of $\mathbb{Q}(\zeta_m)$ which sends ζ_m to ζ_m^{-1}. Since the Galois group of $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}$ is abelian, barring commutes with all automorphisms, traces and norms which we shall consider. This trivial remark will be constantly used without further mention. If we view $\mathbb{Q}(\zeta_m)$ as a subfield of $\mathbb{C}$, then barring is just complex conjugation. The end (or absence) of a proof is marked by $\square$.

§1. The Gauss measure.

Let $m \geq 1$ be an integer, and let $t_m:\mathbb{Q}(\zeta_m) \to \mathbb{Q}$ denote the trace function $t_m(x) = \Sigma_\sigma \sigma(x)$, the sum ranging over all automorphisms σ of $\mathbb{Q}(\zeta_m)$. The Gauss measure $\mu_m:\mathbb{Q}(\zeta_m) \to \mathbb{Q}$ is defined by $\mu_m(x) = t_m(x\bar{x})$, cf. [3, p. 395; 1].

(1.1).(a) The function μ_m is a positive definite quadratic form on the $\mathbb{Q}$-vectorspace $\mathbb{Q}(\zeta_m)$.

(b) For every real number r there are only finitely many elements $y \in \mathbb{Z}[\zeta_m]$ for which $\mu_m(y) \leq r$.

(c) For every $x \in \mathbb{Q}(\zeta_m)$ there is a $y \in \mathbb{Z}[\zeta_m]$ such that $\mu_m(x+y) \leq \mu_m(x+z)$ for all $z \in \mathbb{Z}[\zeta_m]$.

Proof. (a) is evident from $\mu_m(x) = \Sigma_\sigma \sigma(x)\overline{\sigma(x)}$, and (b) follows from (a) since $\mathbb{Z}[\zeta_m]$ is a lattice in $\mathbb{Q}(\zeta_m)$.
Finally, (c) follows from (b) since $\sqrt{\mu_m}$ satisfies the triangle inequality. □

Let the fundamental domain F_m be defined by

$$F_m = \{x \in \mathbb{Q}(\zeta_m) \mid \mu_m(x+y) \geq \mu_m(x) \text{ for all } y \in \mathbb{Z}[\zeta_m]\}.$$

Then (1.1)(c) can be restated as: $F_m + \mathbb{Z}[\zeta_m] = \mathbb{Q}(\zeta_m)$.
A real number c is called a bound for F_m if $\mu_m(x) \leq c$ for all $x \in F_m$. It is easily seen that such c do exist. Clearly, there is a smallest bound for F_m, which is denoted by c_m. It is not hard to prove that $\mu_m(x) = c_m$ for some $x \in F_m$, so that c_m is rational, but we shall not need this. A bound c for F_m is called usable if for every $x \in F_m$ satisfying $\mu_m(x) = c$ there is a root of unity $u \in \mathbb{Z}[\zeta_m]$ such that $\mu_m(x+u) = c$. The use of usable bounds will become clear in the next section. Note that every $c > c_m$ is a usable bound, since no $x \in F_m$ satisfies $\mu_m(x) = c > c_m$.

§2. The euclidean algorithm.

Let $N = N_m : \mathbb{Q}(\zeta_m) \to \mathbb{Q}$ be the norm function $N_m(x) = \Pi_\sigma \sigma(x)$, the product ranging over the $\phi(m)$ automorphisms σ of $\mathbb{Q}(\zeta_m)$. For $x \in \mathbb{Z}[\zeta_m]\backslash\{0\}$ we have $|N(x)| = |\mathbb{Z}[\zeta_m]/\mathbb{Z}[\zeta_m]x|$. We call $\mathbb{Z}[\zeta_m]$ euclidean for the norm if for every $a, b \in \mathbb{Z}[\zeta_m]$, $b \neq 0$, there are $q, r \in \mathbb{Z}[\zeta_m]$ such that $a = qb+r$ and $|N(r)| < |N(b)|$.
Writing $x = ab^{-1}$ and $y = -q$, we find, using the multiplicativity of the norm:

(2.1). The ring $\mathbb{Z}[\zeta_m]$ is euclidean for the norm if and only if for every $x \in \mathbb{Q}(\zeta_m)$ there is an element $y \in \mathbb{Z}[\zeta_m]$ such that $|N(x+y)| < 1$. □

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

$$|N(x)|^2 \leq \left(\frac{1}{\phi(m)} \mu_m(x)\right)^{\phi(m)}.$$

The equality sign holds if and only if $x\bar{x} \in \mathbb{Q}$.

Proof. $|N(x)|^2 = N(x)^2 = N(x)N(\bar{x}) = N(x\bar{x}) = \Pi_\sigma \sigma(x)\overline{\sigma(x)}$.
If we view $\mathbb{Q}(\zeta_m)$ as a subfield of $\mathbb{C}$, then $\sigma(x)\overline{\sigma(x)}$ is a nonnegative real number for all σ. Using the arithmetic-geometric mean inequality we find

$$\Pi_\sigma \sigma(x)\overline{\sigma(x)} \leq \left(\frac{1}{\phi(m)} \Sigma_\sigma \sigma(x)\overline{\sigma(x)}\right)^{\phi(m)} = \left(\frac{1}{\phi(m)} \mu_m(x)\right)^{\phi(m)}.$$

The equality sign holds if and only if all the $\sigma(x\bar{x})$ are equal, which is the case if and only if $x\bar{x} \in \mathbb{Q}$. □

Remark. From (2.2) one easily deduces: for $x \in \mathbb{Z}[\zeta_m]$, $x \neq 0$, one has $\mu_m(x) \geq \phi(m)$, the equality sign holding if and only if x is a root of unity.

(2.3). Lemma. Let $x \in \mathbb{Q}(\zeta_m)$ be such that $x\bar{x} = (x+u)(\overline{x+u}) = 1$ for some root of unity $u \in \mathbb{Z}[\zeta_m]$. Then $x \in \mathbb{Z}[\zeta_m]$.

Proof. Put $y = x\bar{u}$, then $y\bar{y} = 1$ and $y + \bar{y} = -1$, so y is a primitive third root of unity. Then $y \in \mathbb{Q}(\zeta_m)$ implies that m is divisible by 3, so $y \in \mathbb{Z}[\zeta_m]$ and $x = yu \in \mathbb{Z}[\zeta_m]$. □

(2.4). If $\phi(m)$ is a usable bound for F_m, then $\mathbb{Z}[\zeta_m]$ is euclidean for the norm.

Proof. Let $x \in \mathbb{Q}(\zeta_m)$ be arbitrary. We have to find an element $y \in \mathbb{Z}[\zeta_m]$ such that $|N(x+y)| < 1$. By (1.1)(c) we may assume $x \in F_m$. Then $\mu_m(x) \leq \phi(m)$, since $\phi(m)$ is a bound for F_m.
If the inequality is strict, then $|N(x)| < 1$ by (2.2), and we can take $y = 0$.
If the equality sign holds, then $\mu_m(x) = \mu_m(x+u) = \phi(m)$ for some root of unity $u \in \mathbb{Z}[\zeta_m]$, since $\phi(m)$ is usable.
Then

$$|N(x)|^2 \leq \left(\frac{1}{\phi(m)}\,\mu_m(x)\right)^{\phi(m)} = 1$$

$$|N(x+u)|^2 \leq \left(\frac{1}{\phi(m)}\,\mu_m(x+u)\right)^{\phi(m)} = 1.$$

If at least one inequality holds strictly, then we can take $y = 0$ or $y = u$.
If both equality signs hold, then $x\bar{x}$ and $(x+u)(\overline{x+u})$ are rational, by (2.2).
Moreover, $N(x\bar{x}) = 1$, so we have $x\bar{x} = 1$, and similarly $(x+u)(\overline{x+u}) = 1$.
Using (2.3) we find $x \in \mathbb{Z}[\zeta_m]$, which contradicts $x \in F_m$ since $x \neq 0$. □

§3. Estimating the fundamental domain.

(3.1). Let n be a positive divisor of m. Then

$$\frac{c_m}{\phi(m)^2} \leq \frac{c_n}{\phi(n)^2}.$$

Moreover, if c is a usable bound for F_n, then $\frac{\phi(m)^2}{\phi(n)^2}c$ is a usable bound for F_m.

The proof of (3.1) makes use of two formulas. Let $t: \mathbb{Q}(\zeta_m) \to \mathbb{Q}(\zeta_n)$ denote the trace function of the field extension $\mathbb{Q}(\zeta_n) \subset \mathbb{Q}(\zeta_m)$, and let $d = [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_n)] = \frac{\phi(m)}{\phi(n)}$.

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

$$\mu_m(x+y) - \mu_m(x) = d(\mu_n(\tfrac{1}{d}t(x)+y) - \mu_n(\tfrac{1}{d}t(x))).$$

(3.3). For $x \in \mathbb{Q}(\zeta_m)$ we have

$$\mu_m(x) = \frac{1}{m} \Sigma_{j=1}^{m} \mu_n(t(x\zeta_m{}^j)).$$

Proof of (3.1), assuming (3.2) and (3.3).

Let $x \in F_m$ be arbitrary. We have to prove $\mu_m(x) \le d^2.c_n$. Applying (3.2) to $y \in \mathbb{Z}[\zeta_n]$ and looking at the definition of F_n we find $\frac{1}{d}t(x) \in F_n$. Since also $x.\,\zeta_m^j \in F_m$ for all $j \in \mathbb{Z}$, we have in the same way $\frac{1}{d}\,t(x.\,\zeta_m^j) \in F_n$. Therefore

$$\mu_n(t(x.\,\zeta_m^j)) = d^2.\mu_n(\tfrac{1}{d}\,t(x.\,\zeta_m^j)) \le d^2.c_n$$

for all $j \in \mathbb{Z}$, and using (3.3) it follows that $\mu_m(x) \le d^2.c_n$. This proves the first part of (3.1).

Next assume c is a usable bound for F_n, and let $x \in F_m$ satisfy $\mu_m(x) = d^2.c$. Then from the above reasoning we see $c = c_n$ and $\mu_n(\frac{1}{d}\,t(x.\zeta_m^j)) = c_n = c$ for all $j \in \mathbb{Z}$. Take $j = 0$.
Since c is a usable bound for F_n, there is a root of unity $u \in \mathbb{Z}[\zeta_n]$ such that $\mu_n(\frac{1}{d}\,t(x) + u) = c$. Applying (3.2) with $y = u$ we get $\mu_m(x+u) = \mu_m(x) = d^2.c$, which proves that $d^2.c$ is a usable bound for F_m. □

Proof of (3.2).

$$\begin{aligned} d.(\mu_n(\tfrac{1}{d}\,t(x) + y) - \mu_n(\tfrac{1}{d}\,t(x))) &= \\ &= d.t_n(\tfrac{1}{d}\,t(x)\overline{y} + \tfrac{1}{d}\,t(\overline{x})y + y\overline{y}) \\ &= t_n(t(x)\overline{y}) + t_n(t(\overline{x})y) + d.t_n(y\overline{y}) \\ &= t_n(t(x\overline{y})) + t_n(t(\overline{x}y)) + t_n(t(y\overline{y})) \\ &= t_m(x\overline{y} + \overline{x}y + y\overline{y}) \\ &= \mu_m(x+y) - \mu_m(x). \end{aligned}$$

□

Proof of (3.3). Let G be the Galoisgroup of $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}(\zeta_n)$. In the computation below Σ_σ and Σ_τ refer to summations over G. We have

$$\Sigma_{j=1}^m \ \mu_n(t(x\zeta_m^j)) = \Sigma_{j=1}^m \ \mu_n(\Sigma_\sigma \ \sigma(x\zeta_m^j))$$

$$= t_n(\Sigma_{j=1}^m \ \Sigma_\sigma \ \Sigma_\tau \ \sigma(x)\sigma(\zeta_m^j)\tau(\bar{x})\tau(\zeta_m^{-j}))$$

$$= t_n(\Sigma_\sigma \ \Sigma_\tau \ \sigma(x)\tau(\bar{x})(\Sigma_{j=1}^m(\sigma(\zeta_m)\tau(\zeta_m)^{-1})^j)).$$

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

$$\Sigma_{j=1}^m \ \zeta_{\sigma,\tau}^j \begin{cases} = 0 & \text{if} \quad \zeta_{\sigma,\tau} \neq 1 \\ = m & \text{if} \quad \zeta_{\sigma,\tau} = 1. \end{cases}$$

Hence the above expression becomes

$$t_n(\Sigma_\sigma \ \sigma(x)\sigma(\bar{x}) \ m) = m.t_n(t(x\bar{x})) = m.t_m(x\bar{x}) = m.\mu_m(x)$$

which proves (3.3). □

§4. Proof of the theorem.

Explicit consideration of the case $n = 1$ shows that $c_1 = \frac{1}{4}$ is a usable bound for F_1. Then $\frac{1}{4} \ \phi(m)^2$ is a usable bound for F_m, by (3.1). If

(4.1) $\qquad \phi(m) \leq 4$

then $\frac{1}{4}\phi(m)^2 \leq \phi(m)$, and $\phi(m)$ is a usable bound for F_m. By (2.4) it follows that the ring $\mathbb{Z}[\zeta_m]$ is euclidean for the norm if (4.1) holds. This gives us exactly the cases $m = 1, 3, 4, 5, 8, 12$ which were already known. To get new cases we use the following result, which will be proved in the next section.

(4.2). Let n be a prime number. Then $c_n = \dfrac{n^2-1}{12}$ and this is a usable bound for F_n.

Now suppose that m has a prime divisor n such that

(4.3) $\qquad \phi(m) \leq \dfrac{12.(n-1)}{(n+1)}$.

Then a usable bound for F_m is given by

$$\frac{\phi(m)^2}{\phi(n)^2} \ c_n = \frac{\phi(m)^2}{(n-1)^2} \cdot \frac{n^2-1}{12} = \frac{\phi(m)^2(n+1)}{12(n-1)} \leq \phi(m)$$

so $\mathbb{Z}[\zeta_m]$ is euclidean for the norm, by (2.4).
For which m, n does (4.3) hold? In any case $n|m$ implies $\phi(m) \geq \phi(n) = n-1$ so $n+1 \leq 12$ is necessary. For $n = 2$ we get $\phi(m) \leq 4$, which is (4.1). For $n = 3$ we have $\phi(m) \leq 6$ which gives us the new case $m = 9$. For $n = 5$ we find $\phi(m) \leq 8$ which is satisfied by $m = 15$ and $m = 20$. For $n = 7$ and $n = 11$, finally, $m = n$ satisfies (4.3). This proves the theorem, up to (4.2).

§5. Determination of the bound in a special case.

Let n be an integer ≥ 2, and let V be an $(n-1)$-dimensional $\mathbb{R}$-vectorspace with generators e_i, $1 \leq i \leq n$, subject only to the relation $\Sigma_{i=1}^n e_i = 0$. So for $x_i, y_i \in \mathbb{R}$ $(1 \leq i \leq n)$ we have $\Sigma_{i=1}^n x_i e_i = \Sigma_{i=1}^n y_i e_i$ if and only if $x_i - y_i = x_j - y_j$ for all i, j.
We define a positive definite quadratic form Q on V by

$$Q(x) = \Sigma_{1\leq i<j\leq n} (x_i - x_j)^2, \qquad x = \Sigma_{i=1}^n x_i e_i \in V.$$

Let $(\ , \ ): V \times V \to \mathbb{R}$ denote the symmetric bilinear form induced by Q:

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

We have

$$\begin{aligned} (x,x) &= Q(x) && \text{for } x \in V, \\ (e_i, e_i) &= n-1 && \text{for } 1 \leq i \leq n, \\ (e_i, e_j) &= -1 && \text{for } 1 \leq i < j \leq n. \end{aligned}$$

Let $L \subset V$ be the subgroup generated by $\{e_i \mid 1 \leq i \leq n\}$. Clearly, L is a lattice in V. We put

$$\begin{aligned} F &= \{x \in V \mid Q(x) \leq Q(x-y) \text{ for all } y \in L\} \\ &= \{x \in V \mid (x,y) \leq \tfrac{1}{2}Q(y) \text{ for all } y \in L\}. \end{aligned}$$

Since F is compact, Q assumes a maximum c on V. We are going to prove:

<u>(5.1)</u>. The set of points $x \in F$ for which $Q(x) = c$ is given by

(5.2) $$\{\tfrac{1}{n} \Sigma_{i=1}^n i e_{\sigma(i)} \mid \sigma \text{ is a permutation of } \{1, 2, \ldots, n\}\} .$$

Moreover,

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

We prove (5.1) after a series of lemmas. At the end of this section we show how (5.1) implies (4.2).

If A is a subset of $\{1, 2, \ldots, n\}$, then we put $\Sigma_{i\in A} e_i = e_A \in L$.

We call A <u>proper</u> if $\emptyset \neq A \neq \{1, 2, \ldots, n\}$.

<u>(5.3). Lemma</u>. Let $y \in L$ be such that there is no $A \subset \{1, 2, \ldots, n\}$ with $y = e_A$. Then there is an element $z = \pm e_j \in L$ such that $Q(z) + Q(y-z) < Q(y)$.

<u>Proof</u>. Let $y = \Sigma_{i=1}^{n} m_i e_i$ with $m_i \in \mathbb{Z}$. Using $\Sigma_{i=1}^{n} e_i = 0$ we may assume $0 \leq \Sigma_{i=1}^{n} m_i \leq n-1$. For $z = \pm e_j$ we have

$$\tfrac{1}{2}(Q(y) - Q(z) - Q(y-z)) = (y,z) - (z,z)$$

$$= \pm (nm_j - \Sigma_{i=1}^{n} m_i) - (n-1).$$

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

$$nm_j \leq \Sigma_{i=1}^{n} m_i + (n-1) \leq 2n-2 < 2n$$

$$nm_j \geq \Sigma_{i=1}^{n} m_i - (n-1) \geq -n+1 > -n$$

so m_j is 0 or 1 for all j, contradicting that y has not the form e_A.□

<u>(5.4)</u>. Let $x \in V$. Then $x \in F \iff (x,e_A) \leq \tfrac{1}{2}Q(e_A)$ for all $A \subset \{1, 2, \ldots, n\}$.

<u>Proof</u>. $\Rightarrow$ is clear. $\Leftarrow$: we know

$$(x, e_A) \leq \tfrac{1}{2}Q(e_A) \qquad \text{for all } A \subset \{1, 2, \ldots, n\}$$

and we have to prove

$$(x,y) \leq \tfrac{1}{2}Q(y) \qquad \text{for all } y \in L.$$

This is done by an obvious induction on $Q(y)$, using (5.3). □

<u>(5.5)</u>. Let $x_o \in F$ be such that $Q(x_o) = c$. Then there are $n-1$ different proper subsets $A(i) \subset \{1, 2, \ldots, n\}$, $1 \leq i \leq n-1$, such that x_o is the unique solution of the system of linear equalities

(5.6) $$(x, e_{A(i)}) = \tfrac{1}{2}Q(e_{A(i)}), \qquad 1 \leq i \leq n-1.$$

<u>Proof</u>. Let

$$S = \{A \subset \{1, 2, \ldots, n\} \mid (x_o, e_A) = \tfrac{1}{2}Q(e_A)\} ,$$

then we have $(x_o, e_A) < \tfrac{1}{2}Q(e_A)$ for all $A \subset \{1, 2, \ldots, n\}$, $A \notin S$.

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_o is the unique solution of (5.6), and each

$A(i)$ is proper since $e_{A(i)} \neq 0$.

Therefore assume that the linear span of $\{e_A \mid A \in S\}$ has codimension ≥ 1 in V. We derive a contradiction. The subspace

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

has dimension at least 1, so for some $z \in V$, $z \neq 0$ we have

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

Replacing z by $-z$, if necessary, we may assume

(5.7) $\quad (x_o, z) \geq 0.$

Finally, multiplying z by a sufficiently small positive real number we may assume

$$(z, e_A) \leq \tfrac{1}{2}Q(e_A) - (x_o, e_A) \quad \text{for all} \quad A \subset \{1, 2, \ldots, n\}, \ A \notin S.$$

Then for all $A \subset \{1, 2, \ldots, n\}$ we have

$$(x_o + z, e_A) \leq \tfrac{1}{2}Q(e_A)$$

so $x_o + z \in F$ by (5.4). But using (5.7) we find

$$Q(x_o + z) \geq Q(x_o) + Q(z) > Q(x_o)$$

which contradicts our assumption $Q(x_o) = c = \max \{Q(x) \mid x \in F\}$. □

<u>(5.8)</u>. Let x_o, $A(1), \ldots, A(n-1)$ be as in (5.5). Then $A(i) \subset A(j)$ or $A(j) \subset A(i)$, for all i, j, $1 \leq i \leq j \leq n-1$.

<u>Proof</u>. Fix i and j, and put $A = A(i)$ and $B = A(j)$. Let $C = A \backslash B$ and $D = B \backslash A$. If $C = \emptyset$ or $D = \emptyset$ we are done. So suppose $C \neq \emptyset \neq D$. Then $C \cap D = \emptyset$ implies

$$(e_C, e_D) = -|C| \cdot |D| < 0.$$

This is equivalent to

$$(e_{A \cap B}, e_{A \cup B}) > (e_A, e_B).$$

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

$$(x_o, e_{A \cap B}) + (x_o, e_{A \cup B}) = (x_o, e_A) + (x_o, e_B) = \tfrac{1}{2}(Q(e_A) + Q(e_B))$$

$$= \tfrac{1}{2}Q(e_A + e_B) - (e_A, e_B) > \tfrac{1}{2}Q(e_{A \cap B} + e_{A \cup B}) - (e_{A \cap B}, e_{A \cup B})$$

$$= \tfrac{1}{2}Q(e_{A \cap B}) + \tfrac{1}{2}Q(e_{A \cup B}).$$

So for $X = A \cap B$ or for $X = A \cup B$ we have $(x_o, e_X) > \tfrac{1}{2}Q(e_X)$, contradicting $x_o \in F$. □

Proof of (5.1). Let $x_o \in F$ satisfy $Q(x_o) = c$, and let $A(1), \ldots, A(n-1)$ be as above. From (5.5) and (5.8) we conclude that $\{A(i) \mid 1 \le i \le n-1\}$ is a system of $n-1$ proper subsets of $\{1, 2, \ldots, n\}$ which 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

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

By (5.5), we have

$$\Sigma_{j=1}^{i} (x_o, e_j) = \tfrac{1}{2}Q(e_{A(i)}), \qquad \text{for} \quad 1 \le i \le n-1.$$

Writing $x_o = \Sigma_{j=1}^{n} x_j e_j$ in such a manner that $\Sigma_{j=1}^{n} x_j = 0$, we find $(x_o, e_j) = nx_j$. Also $Q(e_A) = |A| \,.\, (n- |A|)$ so our system becomes

$$\Sigma_{j=1}^{i} x_j = \frac{1}{2n} i\,(n-i), \quad 1 \le i \le n-1,$$

$$\Sigma_{j=1}^{n} x_j = 0.$$

Clearly, this implies

$$nx_i = \tfrac{1}{2}(n+1) - i, \qquad 1 \le i \le n,$$

$$x_o = \frac{1}{n} \Sigma_{i=1}^{n} i e_{n+1-i} .$$

We renumbered the e_i at one point in the argument, so it follows that x_o is in the set (5.2). Since there is at least one $x_o \in F$ for which $Q(x_o) = c$, it follows by reasons of symmetry that conversely every element x of (5.2) satisfies $x \in F$ and $Q(x) = c$. Finally, we have

$$c = \frac{1}{n^2} \Sigma_{1 \le i<j \le n} (i-j)^2 = \frac{n^2-1}{12}$$

This proves (5.1). □

Proof of (4.2). Let n be a prime number. The $\mathbb{Q}$-vectorspace $\mathbb{Q}(\zeta_n)$ is generated by the n elements ζ_n^i, $1 \le i \le n$, subject only to the relation $\Sigma_{i=1}^{n} \zeta_n^i = 0$. For rational numbers x_i, $1 \le i \le n$, we have

$$\mu_n(\Sigma_{i=1}^{n} x_i \zeta_n^i) = t_n(\Sigma_{i=1}^{n}\Sigma_{j=1}^{n} x_i x_j \zeta_n^{i-j}) =$$

$$= (n-1) \Sigma_{i=1}^{n} x_i^2 - \Sigma_{i=1}^{n} \Sigma_{j=1}^{n} x_i x_j =$$

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

All this implies that V can be considered as $\mathbb{R} \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_n)$, by $e_i = 1 \otimes \zeta_n^i$, and that Q is the natural extension of μ_n to V.
We have $L = \mathbb{Z}[\zeta_n]$, so $F_n = F \cap \mathbb{Q}(\zeta_n)$. Applying (5.1) yields:

(5.9). Let n be prime. Then $c_n = \frac{n^2-1}{12}$, and the set of elements $x \in F_n$ for which $\mu_n(x) = c_n$ is given by

$$\{\frac{1}{n} \Sigma_{i=1}^n i \zeta_n^{\sigma(i)} \mid \sigma \text{ is a permutation of } \{1, 2, \ldots, n\}\}. \square$$

To prove (4.2), we need only check usability of c_n. So let $x \in F_n$ satisfy $\mu_n(x) = c_n$. Then $x = \frac{1}{n} \Sigma_{i=1}^n i \zeta_n^{\sigma(i)}$ for some permutation σ of $\{1, 2, \ldots, n\}$. Hence

$$x - \zeta_n^{\sigma(n)} = \frac{1}{n} \Sigma_{i=o}^{n-1} i\zeta_n^{\sigma(i)} = \frac{1}{n} \Sigma_{i=1}^n i \zeta_n^{\sigma(i-1)}$$

where $\sigma(o) = \sigma(n)$. By (5.9) it follows that $\mu_n(x - \zeta_n^{\sigma(n)}) = c_n$. This proves that c_n is usable. $\square$

This completes the proof of the theorem.

Remark. The result (5.1) can also be described as follows. Let $T = \mathbb{R}/\mathbb{Z}$ be a circle with circumference 1, and for $t_1, t_2 \in T$ let $d(t_1, t_2)$ be the length of the shortest arc between t_1 and t_2. For $x = (x_i)_{i=1}^n \in T^n$ let

$$q(x) = \min \{\Sigma_{i=1}^n d(x_i, t)^2 \mid t \in T\}.$$

Then

$$\max \{q(x) \mid x \in T^n\} = \frac{n^2-1}{12n},$$

the maximum being attained at those n-tuples of points $x_i \in T$ which divide T into n equal parts.

This follows from (5.1) and the identity

$$n \Sigma_{i=1}^n r_i^2 = \Sigma_{1\le i<j\le n} (r_i - r_j)^2 + (\Sigma_{i=1}^n r_i)^2,$$

for real numbers $r_1, \ldots, r_n$.

§6. Remarks.

(6.1). Let n be a positive divisor of m such that every prime which divides m also divides n. Put $d = \frac{m}{n} = \frac{\phi(m)}{\phi(n)}$. Then $\{1, \zeta_m, \ldots, \zeta_m^{d-1}\}$ is a $\mathbb{Z}[\zeta_n]$-basis for $\mathbb{Z}[\zeta_m]$ and a straightforward computation (e.g. using (3.3)) shows

$$\mu_m(\Sigma_{i=o}^{d-1} x_i \zeta_m^i) = d. \Sigma_{i=o}^{d-1} \mu_n(x_i), \quad \text{for } x_i \in \mathbb{Q}(\zeta_n),$$

cf. [1, (3.16)]. All this implies $c_m = d^2 c_n$, i.e.:

(6.2). If n and m have the same prime divisors, then the equality sign holds in (3.1). $\square$

Since we know $c_2 = \frac{1}{4}$ and $c_{2p} = \frac{p^2-1}{12}$ for $p \geq 3$ prime, it follows that

$$c_{2^t} = 2^{2t-4}, \quad \text{for } t \in \mathbb{Z},\ t \geq 1,$$

$$c_{2^t p^u} = \frac{1}{3}.2^{2t-4}.\ p^{2u-2}.(p^2-1), \text{ for } t,\ u \in \mathbb{Z}, \geq 1,\ p \geq 3 \text{ prime.}$$

In particular $c_{16} = 16 > \phi(16) = 8$ and $c_{24} = 10\frac{2}{3} > \phi(24) = 8$, so our method does not apply to the cases 16 and 24.

I do not know the exact value of c_m if m has more than one odd prime divisor. But using different methods I can prove the following partial converse to our theorem:

<u>(6.3)</u>. Suppose $\phi(m) > 10$ or $m \in \{16,24\}$. Then $c_m > \phi(m)$. □

Of course, (6.3) does not imply that the only values of m for which $\mathbb{Z}[\zeta_m]$ is euclidean for the norm are given by the theorem. In fact, I know of no principal ideal domain $\mathbb{Z}[\zeta_m]$ which is proved to be not euclidean for the norm.

(6.4). The ring $\mathbb{Z}[\zeta_{11} + \zeta_{11}^{-1}]$ is euclidean for the norm [4] . We show how this can be proved by our methods. Note that an element $x = \Sigma_{i=1}^{11} x_i \zeta_{11}^i \in \mathbb{Q}(\zeta_{11})$, with $x_i \in \mathbb{Q}$ for $1 \leq i \leq 11$, belongs to $\mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$ if and only if $x_i = x_{11-i}$ for $1 \leq i \leq 10$.

Let $x \in \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$ be arbitrary. We have to exhibit an element $y \in x + \mathbb{Z}[\zeta_{11} + \zeta_{11}^{-1}]$ for which $|N'(y)| < 1$, where $N' : \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1}) \to \mathbb{Q}$ is the norm.

From our proof that $\mathbb{Z}[\zeta_{11}]$ is euclidean it follows that there is an element $y \in F_{11}$, $y \in x + \mathbb{Z}[\zeta_{11}]$, such that $|N(y)| < 1$; here $N = N_{11} : \mathbb{Q}(\zeta_{11}) \to \mathbb{Q}$ is the norm. Write $y = \Sigma_{i=1}^{11} y_i \zeta_{11}^i$ with $y_i \in \mathbb{Q}$ for $1 \leq i \leq 11$. From $y \in x + \mathbb{Z}[\zeta_{11}]$ we deduce $y_i - y_{11-i} \in \mathbb{Z}$, for $1 \leq i \leq 10$. Also $y \in F_{11}$, so $|y_i - y_{11-i}| = \frac{1}{11}|t_{11}(y(\zeta_{11}^{-i} - \zeta_{11}^{i}))| \leq \frac{10}{11}$ by § 3. Hence $y_i = y_{11-i}$ for $1 \leq i \leq 10$, so $y \in \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$. This implies $y - x \in \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1}) \cap \mathbb{Z}[\zeta_{11}] = \mathbb{Z}[\zeta_{11} + \zeta_{11}^{-1}]$, and since $|N'(y)| = |N(y)|^{\frac{1}{2}} < 1$, we find that y satisfies our requirements.

An immediate generalization of this argument yields: if $n \leq 11$ is prime, then any integrally closed subring of $\mathbb{Z}[\zeta_n]$ is euclidean for the norm. The ring $\mathbb{Z}[\zeta_9 + \zeta_9^{-1}]$ can be treated analogously.

However, no new results are obtained in this way: the case of quadratic rings is classical [5, ch. 14], and more precise information on the cubic rings $\mathbb{Z}[\zeta_7 + \zeta_7^{-1}]$ and $\mathbb{Z}[\zeta_9 + \zeta_9^{-1}]$ can be found in [2]. I don't know whether my method applies to the ring $\mathbb{Z}[\zeta_{15} + \zeta_{15}^{-1}]$, which was proved to be euclidean for the norm in [4]. Note that the integrally closed subrings $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{-15}] \subset \mathbb{Z}[\zeta_{15}]$ and $\mathbb{Z}[\sqrt{-5}] \subset \mathbb{Z}[\zeta_{20}]$ are not euclidean, since they are not even principal ideal domains.

(6.5). Throughout this note we have used that complex conjugation commutes with the other automorphisms of $\mathbb{Q}(\zeta_m)$. This is not essential for our method. If K is any finite field extension of $\mathbb{Q}$, then the Gauss measure $\mu_K : K \to \mathbb{R}_{\geq 0}$ may be defined by $\mu_K(x) = \Sigma_\sigma |\sigma(x)|^2$, the sum ranging over the $[K:\mathbb{Q}]$ field homomorphisms $\sigma: K \to \mathbb{C}$. Then the main results of §§ 1-3 carry over to the general case.
Some care is required in stating (1.1)(a), since μ_K may assume non-rational values. The fundamental domain F_K and the smallest bound c_K for F_K are defined in the obvious way, so that $F_{\mathbb{Q}(\zeta_m)} = F_m$ and $c_{\mathbb{Q}(\zeta_m)} = c_m$. But c_K need not be rational, and there is not necessarily an element $x \in F_K$ for which $\mu_K(x) = c_K$. Writing R_K for the ring of algebraic integers in K, we can generalize (2.4) as follows.

<u>(6.6)</u> If $[K:\mathbb{Q}]$ is a usable bound for F_K, then R_K is euclidean for the norm. □

The generalization of (3.1) reads:

<u>(6.7)</u> Let K be a finite field extension of $\mathbb{Q}$, and let $m \in \mathbb{Z}$, $m \geq 1$. Let L be a field extension of the form $L = K(\alpha)$, where $\alpha^m = a \in R_K$. Suppose there is a real number $r > 0$ such that $|\sigma(a)|^2 = r$ for all field homomorphisms $\sigma : K \to \mathbb{C}$. Then

(6.8) $$c_L \leq \frac{d^2}{m} c_K \Sigma_{i=0}^{m-1} r^{i/m},$$

where $d = [L:K]$. Moreover, if c_K is a usable bound for F_K, then the right hand side of (6.8) is a usable bound for F_L. Finally, if $\{\alpha^i \mid 0 \leq i \leq m-1\}$ is an R_K-basis for R_L (so that in particular $d = m$), then the equality sign holds in (6.8).

The <u>proof</u> of (6.7) is analogous to the proof of (3.1).□

The validity of (6.6) and (6.7) is not affected if the concept of a "usable bound" (end § 1) is weakened as follows:
a bound c for F_K is usable if for every $x \in F_K$ for which $\mu_K(x) = c$ there exists a unit $u \in R_K$ such that $\mu_K(x+u) = c$.
Only the proof of (2.3) needs a small modification.

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. H. Davenport, On the product of three non-homogeneous linear forms, Proc. Cambridge Philos.Soc. 43 (1947)137-152.
3. C.F. Gauss, Werke, Zweiter Band, Göttingen 1876.
4. H.J. Godwin, On Euclid's algorithm in some quartic and quintic fields, J. London Math.Soc. 40(1965)699-704.
5. G.H. Hardy and E.M. Wright, An introduction to the theory of numbers, Oxford 1938[1], 1945[2], 1954[3], 1960[4].
6. R.B. Lakein, Euclid's algorithm in complex quartic fields, Acta Arith. 20 (1972) 393-400.
7. E. Landau, Vorlesungen über Zahlentheorie, Band 3, Leipzig 1927.
8. J.M. Masley, On the class number of cyclotomic fields, thesis, Princeton University 1972.
9. J.M. Masley, On cyclotomic fields Euclidean for the norm map, Notices Amer.Math.Soc. 19 (1972) p.A-813 (abstract 700-A3).
10. J. Ouspensky, Note sur les nombres entiers dépendant d'une racine cinquième de l'unité, Math.Ann.66(1909)109-112.
11. P.J. Weinberger, On Euclidean rings of algebraic integers, Proc.Symp. Pure Math. 24, Analytic Number Theory, Amer. Math.Soc. 1973, 321-332.