MATHEMATICS OF COMPUTATION, VOLUME 31, NUMBER 137
JANUARY 1977, PAGES 268–273

Euclid's Algorithm in the Cyclotomic Field $\mathbf{Q}(\zeta_{16})$

By T. Ojala

Abstract. Let ζ_{16} denote a primitive 16th root of unity. It is proved that $\mathbf{Z}[\zeta_{16}]$ is Euclidean for the norm map.

1. **Introduction.** Let K be an algebraic number field of degree n over $\mathbf{Q}$ and R_K the ring of integers of K. Let N: $K \longrightarrow \mathbf{Q}$ be the norm function $N(x) = \Pi_\sigma \sigma(x)$, the product ranging over all n embeddings of K into the complex field. We call R_K *Euclidean for the norm* if for every $a, b \in R_K$, $b \neq 0$, there are $q, r \in R_K$ such that $a = qb + r$ and $|N(r)| < |N(b)|$. In view of the multiplicativity of the norm we may write this as

$$(\forall x \in K)(\exists y \in R_K)(|N(x - y)| < 1). \tag{1}$$

For a positive integer m, let ζ_m denote a primitive mth root of unity. By ϕ we mean the Euler ϕ-function. It is known that if $\phi(m) \leqslant 10$, $m \neq 16$, then $\mathbf{Z}[\zeta_m]$ is Euclidean for the norm map. For more details see, e.g. Lenstra [1] and Masley [2]. The case $m = 24$ has recently been proved by H. W. Lenstra, Jr. (written communication).

We shall now prove that $\mathbf{Z}[\zeta_{16}]$ is Euclidean, too.

2. **Preliminaries.** Let x_1 and x_2 be elements in an algebraic number field K. We shall say that x_1 and x_2 are *equivalent* if there is a unit $\eta \in K$, an integer $z \in K$ and an automorphism σ of K such that

$$x_1 = \eta\sigma(x_2) + z.$$

This definition really gives rise to an equivalence relation.

In order to verify condition (1), it is enough to consider one representative of every equivalence class, because $|N(\eta)| = 1$ for any unit $\eta \in K$. Such a representative will be chosen in the way suggested by the following lemma.

LEMMA 1. *Let $\omega_1, \ldots, \omega_n$ be an integral basis for K. In every equivalence class D there is at least one element $x_D = a_1\omega_1 + \cdots + a_n\omega_n$ ($a_i \in \mathbf{Q}$) such that the sum $S(x_D)$ of the absolute values of the coefficients a_i is as small as possible. Thus*

$$S(x_D) = \sum |a_i| \leqslant \sum |b_i| = S(x)$$

for every $x = b_1\omega_1 + \cdots + b_n\omega_n \in D$.

Proof. Let $x \in D$. Then there is an integer $y \in R_K$ and a rational integer m such that $x = y/m$. All the elements equivalent to x are of the form y'/m with $y' \in R_K$. This proves the assertion.

Received April 6, 1976; revised June 7, 1976.
AMS (MOS) subject classifications (1970). Primary 13F10, 12A35, 12–04.

Copyright © 1977, American Mathematical Society

The elements x_D satisfying the condition of Lemma 1 are called *minimal*.

Let $\zeta = \zeta_{16}$ be a primitive 16th root of unity. In order to evaluate the trace $\mathrm{Tr} = \mathrm{Tr}_{\mathbf{Q}(\zeta)/\mathbf{Q}}$ and the norm $N = N_{\mathbf{Q}(\zeta)/\mathbf{Q}}$ we need the following lemmas.

LEMMA 2. *Let* $x = a_0 + a_1\zeta + \cdots + a_7\zeta^7 \in \mathbf{Q}(\zeta)$. *Then*

$$\mathrm{Tr}(x\bar{x}) = 8(a_0^2 + \cdots + a_7^2) \quad \textit{and} \quad N(x) \leqslant (a_0^2 + \cdots + a_7^2)^4.$$

Proof. Let σ denote any automorphism of $\mathbf{Q}(\zeta)/\mathbf{Q}$. Then we have

$$\mathrm{Tr}(x\bar{x}) = \sum_\sigma \sigma(x\bar{x}) = 8(a_0^2 + \cdots + a_7^2).$$

Hence

$$(N(x))^2 = \prod_\sigma \sigma(x\bar{x}) \leqslant \left(\frac{1}{8}\sum_\sigma \sigma(x\bar{x})\right)^8 = (a_0^2 + \cdots + a_7^2)^8.$$

LEMMA 3. *Let* $c_1, \ldots, c_n$ *be positive constants of which* c_1 *is the least one. Let* $u_1, \ldots, u_n$ *be real numbers such that*

$$\sum_i u_i^2 \leqslant A^2, \tag{2}$$

where $A \geqslant 0$ *is fixed. Then*

$$\prod_i (c_i + u_i) \leqslant 2^{-n} \prod_i (c_i + (c_i^2 + 4(c_1 + C)C)^{1/2}),$$

where

$$C = A\left(\sum_i (c_1/c_i)^2\right)^{-1/2}.$$

Proof. The set T of points $(u_1, \ldots, u_n) \in \mathbf{R}^n$ satisfying (2) is compact. Furthermore the function $f\colon T \longrightarrow \mathbf{R}$, $f(u_1, \ldots, u_n) = \Pi(c_i + u_i)$, is continuous so that there is a point $(v_1, \ldots, v_n) \in T$ such that $f(u_1, \ldots, u_n) \leqslant f(v_1, \ldots, v_n)$ for every $(u_1, \ldots, u_n) \in T$. Clearly, the v_i are nonnegative and

$$\sum_i v_i^2 = A^2. \tag{3}$$

First, we shall prove that all of the quantities $(c_i + v_i)v_i$ are equal. Suppose, on the contrary, $(c_i + v_i)v_i > (c_j + v_j)v_j$ for some i and j. Hence $v_i > 0$. Let $\delta > 0$ be an arbitrary small real number. We can define

$$\delta' = \delta'(\delta) = v_i - (v_i^2 - 2\delta v_j - \delta^2)^{1/2} = \delta v_i^{-1} v_j + O(\delta^2)$$

if δ is small enough. Then δ and δ' satisfy

$$(v_i - \delta')^2 + (v_j + \delta)^2 = v_i^2 + v_j^2.$$

On the other hand,

$$\begin{aligned}
&(c_i + v_i - \delta')(c_j + v_j + \delta) \\
&\qquad = (c_i + v_i)(c_j + v_j) + \delta v_i^{-1}[(c_i + v_i)v_i - (c_j + v_j)v_j] + O(\delta^2) \\
&\qquad > (c_i + v_i)(c_j + v_j)
\end{aligned}$$

if $\delta > 0$ is small enough. Hence we have a contradiction.

On account of the equalities

$$(c_i + v_i)v_i = (c_1 + v_1)v_1 \qquad (i = 1, \ldots, n) \tag{4}$$

we have

$$v_i = \frac{c_1 v_1 + v_1^2 - v_i^2}{c_i} \geqslant \frac{c_1}{c_i} \cdot v_1 \qquad (i = 1, \ldots, n) \tag{5}$$

since $c_1 \leqslant c_i$ implies $v_1 \geqslant v_i$. Finally, in view of (3), (5) and (4) we have

$$v_1 \leqslant A\left(\sum (c_1/c_i)^2\right)^{-1/2} = C$$

and

$$v_i \leqslant \tfrac{1}{2}(-c_i + (c_i^2 + 4(c_1 + C)C)^{1/2}).$$

This proves the lemma.

3. The Outline of the Computations. Let $\zeta = \zeta_{16}$ denote a primitive 16th root of unity. We consider the integral basis $1, \zeta, \ldots, \zeta^7$ for the field $\mathbf{Q}(\zeta)$. According to Section 2, we have to verify (1) for one minimal element in every equivalence class.

Let $x_D = a_0 + a_1\zeta + \cdots + a_7\zeta^7$ be a minimal element. We clearly have

$$-\tfrac{1}{2} \leqslant a_i \leqslant \tfrac{1}{2} \qquad (i = 0, \ldots, 7).$$

On multiplying x_D by an appropriate power of ζ we can suppose that

$$a_0 = \max |a_i|. \tag{6}$$

According to Lemma 2, we have without restrictions $a_0 \geqslant \sqrt{2}/4$, since otherwise $N(x_D) < 1$.

Consider all the conjugates of x_D and the coefficients of ζ, ζ^2 and ζ^4 in the conjugates with respect to the basis $1, \zeta, \ldots, \zeta^7$. These coefficients can be given in eight triplets

$$(a_1, a_2, a_4), (-a_5, -a_2, a_4), (-a_1, a_2, a_4), (a_5, -a_2, a_4) \tag{7}$$

and

$$(-a_3, a_6, -a_4), (a_7, -a_6, -a_4), (a_3, a_6, -a_4), (-a_7, -a_6, -a_4) \tag{8}$$

which are classified according to the coefficient of ζ^4. Consider those of the triplets (7) and (8) with nonnegative coefficients of ζ^4. Among these there is at least one with nonnegative coefficients of ζ and ζ^2. Hence on applying a suitable automorphism of $\mathbf{Q}(\zeta)/\mathbf{Q}$ we may assume that $a_1, a_2, a_4 \geqslant 0$.

Hence in every equivalence class D there is at least one minimal element $x_D = a_0 + a_1\zeta + \cdots + a_7\zeta^7$ such that

$$\tfrac{1}{2} \geqslant a_0 = \max |a_i| \geqslant \sqrt{2}/4, \tag{9}$$

$$a_1, a_2, a_4 \geqslant 0. \tag{10}$$

It can be proved that for such a minimal element x_D one of the numbers

$$(11) \qquad y = 0, 1, i, 1 + i$$

satisfies $N(x_D - y) < 1$.

We have good reason to restrict our attention to only these four numbers y, if we consider the location of the conjugates of x_D in the complex plane. Let, namely, $x_D^* = a_0 + a_4\zeta^4$ with $\sqrt{2}/4 \leqslant a_0 \leqslant ½$, $0 \leqslant a_4 \leqslant a_0$. Then any conjugate $\sigma(x_D^*)$ of x_D^* lies in the square bounded by the corresponding conjugates $\sigma(y)$ of the numbers (11). Thus, we can suppose that x_D is partly eliminated by one of the numbers y so that $N(x_D - y) < 1$.

We have verified this assertion by a computer. The idea of the process is as follows.

We divide the proof into cases according to which of the intervals

$$[-0.5, -0.4], [-0.4, -0.3], \ldots, [0.4, 0.5]$$

the coefficients a_i belong. On taking into account the restrictions (9) and (10), there are 1512144 cases to be considered. Every case corresponds with a cube I in $\mathbf{R}^8$ with edge 0.1. Such a cube will be divided into 2^8 smaller ones by bisecting all the edges if needed. The procedure of bisection will be repeated sufficiently many times.

In the following we say that x is in I if $(a_0, \ldots, a_7) \in I$.

Every cube will be considered by three steps in the following way.

Step A. We estimate the norm function by means of Lemma 2. If $N(x) < 1$ for every x in I, then this case is finished. Otherwise we must proceed to

Step B. We shall estimate $N(x - y)$ for x in I and for $y = 0, 1, i, 1 + i$ in the following way.

Let x_0 be the center of I. If σ denotes any automorphism of $\mathbf{Q}(\zeta)/\mathbf{Q}$, then

$$N(x - y) = \prod_\sigma |\sigma(x - y)| \leqslant \prod_\sigma (|\sigma(x_0 - y)| + |\sigma(x - x_0)|),$$

where

$$\sum_\sigma |\sigma(x - x_0)|^2 = \mathrm{Tr}((x - x_0)\overline{(x - x_0)}) \leqslant 8 \cdot 8 \cdot 0.05^2 = 0.16$$

according to Lemma 2. The numbers $|\sigma(x_0 - y)|$ are positive constants so that we can apply Lemma 3. Hence we have an upper bound for $N(x - y)$. If for any one of the numbers $y = 0, 1, i, 1 + i$ we have $N(x - y) < 1$ for every x in I, then the case is finished. Otherwise we must proceed to

Step C. It may be so that in the cube I there does not exist any minimal element. The existence of such an element is tested as follows.

Suppose there is a minimal element $x_D = a_0 + a_1\zeta + \cdots + a_7\zeta^7$ in I, i.e. $(a_0, \ldots, a_7) \in I$. Hence the inequality

$$(12) \qquad S(x_D) \leqslant S(\eta x_D + z)$$

is satisfied for any $z \in \mathbf{Z}[\zeta]$ and for any one of the following four units

$$\eta = 1 + \zeta + \zeta^2, \quad 1 + \zeta^3 + \zeta^6, \quad 1 - \zeta^2 + \zeta^5, \quad 1 - \zeta^6 + \zeta^7. \tag{13}$$

If in I there is no point $(a_0, \ldots, a_7)$ satisfying the inequalities (12) we have a contradiction.

For instance, consider the case

$$(a_0, \ldots, a_7) \in [0.4, 0.5] \times [0.4, 0.5] \times [0.3, 0.4] \times [0.2, 0.3] \times [0.4, 0.5] \times [-0.4, -0.3] \times [0.3, 0.4] \times [0, 0.1].$$

Hence

$$\begin{aligned}
&S((1 + \zeta + \zeta^2)(a_0 + a_1\zeta + \cdots + a_7\zeta^7) + z) - S(a_0 + a_1\zeta + \cdots + a_7\zeta^7) \\
&\quad = S((a_0 - a_7 - a_6) + (a_1 + a_0 - a_7)\zeta + (a_2 + a_1 + a_0)\zeta^2 + \cdots + (a_7 + a_6 + a_5)\zeta^7 + z) \\
&\qquad - S(a_0 + a_1\zeta + \cdots + a_7\zeta^7) \\
&\quad \leqslant 0.2 + (1 - a_1 - a_0 + a_7) + (-1 + a_2 + a_1 + a_0) + 0.2 + 0.2 + (a_5 + a_4 + a_3) \\
&\qquad + (a_6 + a_5 + a_4) + 0.2 - (a_0 + a_1 + a_2 + a_3 + a_4 - a_5 + a_6 + a_7) \\
&\quad = -a_0 - a_1 + a_4 + 3a_5 + 0.8 \leqslant -0.4 - 0.4 + 0.5 - 0.9 + 0.8 < 0
\end{aligned}$$

for $z = -\zeta - \zeta^2$. Thus the cube in question cannot contain any minimal element.

It is worth noticing that the missing four conjugates $1 - \zeta + \zeta^2$, $1 - \zeta^3 + \zeta^6$, $1 - \zeta^2 - \zeta^5$, $1 - \zeta^6 - \zeta^7$ of $1 + \zeta + \zeta^2$ are the units (13) multiplied by suitable roots of unity. Hence in (12) it is of no use to consider all of the conjugates of $1 + \zeta + \zeta^2$. If the unit η is a sum of more than three roots of unity, then the estimation of (12) is not so accurate.

If in I there possibly exists a minimal element, then I is divided into 2^8 cubes as described above. The inequalities (12) may, however, imply some restrictions concerning the coefficients a_i.

For instance, consider the case

$$(a_0, \ldots, a_7) \in [0.3, 0.4] \times [0.3, 0.4] \times [0.3, 0.4] \times [0.1, 0.2] \times [0.2, 0.3] \times [-0.4, -0.3] \times [0.2, 0.3] \times [0.3, 0.4].$$

Then

$$\begin{aligned}
&S((1 + \zeta + \zeta^2)(a_0 + a_1\zeta + \cdots + a_7\zeta^7) + z) - S(a_0 + a_1\zeta + \cdots + a_7\zeta^7) \\
&\quad \leqslant (-a_0 + a_7 + a_6) + (a_1 + a_0 - a_7) + 0.2 + (1 - a_3 - a_2 - a_1) \\
&\qquad + (1 - a_4 - a_3 - a_2) + 0.2 + (a_6 + a_5 + a_4) + (a_7 + a_6 + a_5) \\
&\qquad - (a_0 + a_1 + a_2 + a_3 + a_4 - a_5 + a_6 + a_7) \\
&\quad = -a_0 - a_1 - 3a_2 - 3a_3 - a_4 + 3a_5 + 2a_6 + 2.4 \leqslant 0.1
\end{aligned} \tag{14}$$

if $z = -\zeta^3 - \zeta^4$. Thus there may be a minimal element in the cube. But if $a_2 > 0.35$ or $a_3 > 0.15$ or $a_5 < -0.35$ or $a_6 < 0.25$ then the difference (14) is negative. Hence we may restrict our attention to the subcubes with

$$a_2 \leqslant 0.35, \quad a_3 \leqslant 0.15, \quad a_5 \geqslant -0.35, \quad a_6 \geqslant 0.25.$$

so we have 16 subcubes left. But six of these are impossible because of (6). Hence there are only 10 cases to be considered.

Finally the Steps B and C are applied to the smaller cubes. The process of bisection must be repeated five times in some cases before the assertion is verified.

The numerical calculations were carried out on a UNIVAC 1108 system. The computing time was about an hour.

The following table indicates how many times the Steps A, B and C were applied during the calculations.

Edge of cube	Step A	Step B	Step C
0.1	1512144	671376	55136
$0.1 \cdot 2^{-1}$		882915	8705
$0.1 \cdot 2^{-2}$		114203	2796
$0.1 \cdot 2^{-3}$		54432	1033
$0.1 \cdot 2^{-4}$		15986	244
$0.1 \cdot 2^{-5}$		2322	8

The computations were tested in several cubes I by outputting the upper bounds of $N(x - y)$ and $S(\eta x + z) - S(x)$ for $x \in I$ and for suitable fixed numbers y, η and z. The values were found to be correct. If the cube I had to be divided into subcubes, then we checked that every subcube either was found to be impossible or was considered by Steps B and C, and so on.

Acknowledgment. I would like to express my gratitude to Professor Veikko Ennola for many ideas concerning this problem and for reading the computer program.

Department of Mathematical Sciences
University of Turku
SF-20500 Turku 50, Finland

1. H. W. LENSTRA, JR., "Euclid's algorithm in cyclotomic fields," *J. London Math. Soc.* (2), v. 10, 1975, pp. 457–465.

2. J. M. MASLEY, "On cyclotomic fields Euclidean for the norm map," *Notices Amer. Math. Soc.*, v. 19, 1972, A-813. Abstract # 700-A3.