

CYCLOTOMIC RINGS WITH SIMPLE EUCLIDEAN ALGORITHM

NORBERT KAIBLINGER

ABSTRACT. The usual Euclidean algorithms for the rational integers and for the Gaussian integers are especially simple. We investigate the validity of similar Euclidean algorithms for general cyclotomic rings.

1. INTRODUCTION

Let $n \geq 1$ and denote by $m = \phi(n)$ the Euler totient of n . The cyclotomic ring $\mathbb{Z}[\zeta_n]$ is the ring of algebraic integers in the cyclotomic field $\mathbb{Q}(\zeta_n)$ of the n^{th} root of unity $\zeta_n := \exp(2\pi i/n)$. As usual we assume that $n \neq 2 \cdot \text{odd}$ (if n is odd, then $\mathbb{Z}[\zeta_{2n}] = \mathbb{Z}[\zeta_n]$), so that $\mathbb{Q}(\zeta_n)$ is uniquely identified by the number n . The elements of $\mathbb{Z}[\zeta_n]$ have a unique integral power basis representation $\xi = \xi_v$ of the form

$$(1) \quad \xi_v = F(\zeta_n), \quad F(z) = \sum_{k=0}^{m-1} a_k z^k, \quad v = (a_0, \dots, a_{m-1}) \in \mathbb{Z}^m.$$

By $N_{\mathbb{Q}(\zeta_n)} = N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}$ we denote the absolute valued cyclotomic norm, for $n \neq 1$,

$$(2) \quad N_{\mathbb{Q}(\zeta_n)}(\xi_v) = \prod_{z \in C_n^*} F(z), \quad C_n^* = \{\exp(2\pi i k/n) : \gcd(k, n) = 1\},$$

and for $n = 1$ the absolute value function $N_{\mathbb{Q}}(\xi_v) = |\xi_v|$. Notice that $N_{\mathbb{Q}(\zeta_n)}$ is always non-negative valued, since for $n \neq 1$ the factors in (2) come in conjugate pairs. It is known [11, 20], that $\mathbb{Z}[\zeta_n]$ is a euclidean ring if and only if n belongs to the following set of 30 numbers,

$$(3) \quad \mathcal{E} = \{1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, \\ 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84\}.$$

For a euclidean ring, various euclidean algorithms may exist, for example the general construction by Motzkin [18] is always available, see also [19].

We are interested in a simple and direct construction, based on an explicit assignment of the form $\mathbb{Z}[\zeta_n]^2 \rightarrow \mathbb{Z}[\zeta_n]$,

$$(4) \quad (\xi_{v_1}, \xi_{v_2}) \mapsto \xi_{v'},$$

2010 *Mathematics Subject Classification.* 11R18, 11A05, 13F07; 15B36, 11T22, 11R04, 11Y40.

Key words and phrases. Euclidean algorithm, cyclotomic field, euclidean ring, algebraic integer.

Supported by the Austrian Science Fund FWF grant P 21339.

such that the mapping

$$(5) \quad D(\xi_{v_1}, \xi_{v_2}) = (\xi_{v_2}, \xi_{v_1} - \xi_{v'}\xi_{v_2})$$

satisfies

$$(6) \quad \exists k \geq 0: \quad D^k(\xi_{v_1}, \xi_{v_2}) = (\xi_{v_0}, 0), \quad \xi_{v_0} \in \gcd(\xi_{v_1}, \xi_{v_2}).$$

In the most elementary cases the algebraic integer $\xi_{v'} \in \mathbb{Z}[\zeta_n]$ is constructed in terms of the quotient $\xi_v = \xi_{v_1}/\xi_{v_2} \in \mathbb{Q}(\zeta_n)$. For example, the usual Euclidean algorithm for the rational integers \mathbb{Z} defines v' by “flooring” $v = a_0 \in \mathbb{Q}$ to $\lfloor a_0 \rfloor \in \mathbb{Z}$, the greatest integer less than or equal to a_0 ; we can assume $a_0 \geq 0$ here. The usual Euclidean algorithm for the Gaussian integers $\mathbb{Z}[i]$ defines v' by “rounding” the entries of $v = (a_0, a_1) \in \mathbb{Q}^2$ to nearest integers, $v' = (\lfloor a_0 + 1/2 \rfloor, \lfloor a_1 + 1/2 \rfloor) \in \mathbb{Z}^2$. We also notice that in both of these cases the algorithm is 1-step norm-euclidean, that is, we have, for $\xi_{v_1}, \xi_{v_2} \in \mathbb{Z}[\zeta_n]$ ($\xi_{v_2} \neq 0$),

$$(7) \quad N_{\mathbb{Q}(\zeta_n)}(\xi_{v_1} - \xi_{v'}\xi_{v_2}) < N(\xi_{v_2}),$$

or equivalently by writing $\xi_v = \xi_{v_1}/\xi_{v_2}$, for all $\xi_v \in \mathbb{Q}(\zeta_n)$,

$$(8) \quad N_{\mathbb{Q}(\zeta_n)}(\xi_v - \xi_{v'}) < 1.$$

Also the 1-step norm-euclidean algorithm for $\mathbb{Z}[\zeta_8]$ by Eisenstein [6] is implicitly defined by “rounding”; Elia and Monico [8, Sec. 4.1] include an explicit proof. The 1-step norm-euclidean algorithm for $\mathbb{Z}[\zeta_{12}]$ by Masley [15], being more concrete than [9], includes a version of “rounding”/“flooring”, similar to but not exactly in the sense discussed here.

Below we include more details for $\mathbb{Z}[\zeta_8]$ that allow us to confirm a suggestion in [8] improving the bound in (8), for $\mathbb{Z}[\zeta_8]$. In addition we prove that also the “rounding” algorithm for $\mathbb{Z}[\zeta_{12}]$ is 1-step norm-euclidean. In fact, we completely characterize those cyclotomic rings such that the “flooring” or “rounding” algorithm for $\mathbb{Q}(\zeta_n)$ is 1-step norm-euclidean, and our results include optimal bounds.

2. MAIN RESULT

For $v = (a_0, \dots, a_{m-1}) \in \mathbb{Q}^m$, define $\lfloor v \rfloor, \lfloor v + 1/2 \rfloor \in \mathbb{Z}^m$ by

$$(9) \quad \lfloor v \rfloor = (\lfloor a_0 \rfloor, \dots, \lfloor a_{m-1} \rfloor), \quad \lfloor v + 1/2 \rfloor = (\lfloor a_0 + 1/2 \rfloor, \dots, \lfloor a_{m-1} + 1/2 \rfloor).$$

For $n \geq 1$ ($n \neq 2 \cdot \text{odd}$), we say the “flooring” algorithm for $\mathbb{Z}[\zeta_n]$ is 1-step norm-euclidean, if

$$(10) \quad \forall \xi_v \in \mathbb{Q}(\zeta_n): \quad N_{\mathbb{Q}(\zeta_n)}(\xi_v - \xi_{\lfloor v \rfloor}) < 1,$$

and we say the “rounding” algorithm for $\mathbb{Z}[\zeta_n]$ is 1-step norm-euclidean, if

$$(11) \quad \forall \xi_v \in \mathbb{Q}(\zeta_n): \quad N_{\mathbb{Q}(\zeta_n)}(\xi_v - \xi_{\lfloor v + 1/2 \rfloor}) < 1.$$

By the next theorem, our main result, we determine all cyclotomic rings $\mathbb{Z}[\zeta_n]$ such that the “flooring” algorithm or the “rounding” algorithm for $\mathbb{Z}[\zeta_n]$ are 1-step norm-euclidean.

Theorem 1. *Let $n \geq 1$ ($n \neq 2 \cdot \text{odd}$).*

(i) *The “flooring” algorithm for $\mathbb{Z}[\zeta_n]$ is 1-step norm-euclidean if and only if $n = 1, 3$. We have*

$$\forall \xi_v \in \mathbb{Q}(\zeta_n): \quad N_{\mathbb{Q}(\zeta_n)}(\xi_v - \xi_{[v]}) < 1, \quad n = 1, 3,$$

and in both cases the upper bound is best possible.

(ii) *The “rounding” algorithm for $\mathbb{Z}[\zeta_n]$ is 1-step norm-euclidean if and only if $n = 1, 3, 4, 8, 12$. We have*

$$\forall \xi_v \in \mathbb{Q}(\zeta_n): \quad N_{\mathbb{Q}(\zeta_n)}(\xi_v - \xi_{[v+1/2]}) \leq \begin{cases} 1/2, & n = 1, \\ 3/8, & n = 3, \\ 1/2, & n = 4, \\ 9/16, & n = 8, \\ 225/256, & n = 12. \end{cases}$$

and the upper bounds are best possible.

Remark 2. (i) In Theorem 1(ii), the relation “ \leq ” can be replaced by “ $<$ ”, for $n = 3$, but not for $n = 1, 4, 8, 12$.

(ii) Compare the constants in Theorem 1(i) and (ii) with the known norm-euclidean minima [11], cf. [1, 7],

$$\max_{v \in \mathbb{Q}(\zeta_n)} \min_{v' \in \mathbb{Z}[\zeta_n]} N_{\mathbb{Q}(\zeta_n)}(\xi_v - \xi_{v'}) = \begin{cases} 1/2, & n = 1, \\ 1/3, & n = 3, \\ 1/2, & n = 4, \\ 1/2, & n = 8, \\ 1/4, & n = 12. \end{cases}$$

For example, we obtain that for the Eisenstein integers $\mathbb{Z}[\zeta_3]$ the “rounding” algorithm is better than the “flooring” algorithm; to achieve the norm-euclidean minimum in this case requires more delicate constructions [17], see also [5]. We also observe that the “rounding” algorithm is optimal exactly for the rational integers, see [10], and for the Gaussian integers.

(iii) Theorem 1(ii) shows that the “flooring” and “rounding” algorithms are 1-step norm-euclidean in only a few cases. We do not know if in some of the excluded cases they are 2-step (or k -step, $k = 1, 2, \dots$) norm-euclidean in the sense of Cooke [3, 4], where (6) still holds but (7) is replaced by a weaker condition.

(iv) Inspired by Nagata’s pairwise algorithm [14], one may consider a refined but still simple variant of the algorithms above, obtained by applying (5) only if $N(\xi_{v_1}) \leq N(\xi_{v_2})$, exchanging ξ_{v_1} and ξ_{v_2} beforehand if necessary. Numerical experiments suggest that it is interesting to analyze this variant of the “rounding” algorithm for $\mathbb{Z}[\zeta_5]$.

3. PROOF OF THEOREM 1

Let $n \geq 1$ ($n \neq 2 \cdot \text{odd}$), as above. Recall that $\mathbb{Z}[\zeta_n]$ is euclidean (for some euclidean function that may or may not be the absolute valued norm function) if and only if $n \in \mathcal{E}$. It is known that $\mathbb{Z}[\zeta_n]$ is norm-euclidean (that is, euclidean for the absolute valued norm function as euclidean function) for n in a nonempty, proper subset $\mathcal{E}_0 \subset \mathcal{E}$; for details on \mathcal{E}_0 we refer the most recent update of [11], see also [2, 12, 13, 16]. While we need the following two lemmas only for $n \in \mathcal{E}_0$, it imposes no additional difficulty to formulate them more generally for $n \in \mathcal{E}$.

Lemma 3. *Let $n \in \mathcal{E}$, that is, $\mathbb{Q}(\zeta_n)$ is a euclidean cyclotomic field. Then we have*

$$\begin{cases} \forall v \in [0, 1]^{\phi(n)}: N_{\mathbb{Q}(\zeta_n)}(\xi_v) < 1, & n = 1, 3, \\ \exists v \in [0, 1]^{\phi(n)}: N_{\mathbb{Q}(\zeta_n)}(\xi_v) > 1, & \text{otherwise.} \end{cases}$$

Proof. (i) For $n = 1, 3$, we have

$$(12) \quad \begin{aligned} \{N_{\mathbb{Q}}(\xi_v): v \in [0, 1]\} &= \{|a|: a \in [0, 1]\} = [0, 1], \\ \{N_{\mathbb{Q}(\zeta_3)}(\xi_v): v \in [0, 1]^2\} &= \{a^2 - ab + b^2: (a, b) \in [0, 1]^2\} = [0, 1]. \end{aligned}$$

(ii) Let $n = 5$. For $v_0 = (1, 1, 0, 1/2)$, we compute $N_{\mathbb{Q}(\zeta_5)}(\xi_{v_0}) = 25/16$. Let $v = 9/10 \cdot v_0$. Then $v \in [0, 1]^4$ and

$$(13) \quad N_{\mathbb{Q}(\zeta_5)}(\xi_v) = (9/10)^4 \cdot N_{\mathbb{Q}(\zeta_5)}(\xi_{v_0}) = (9/10)^4 \cdot 25/16 = 1.02 > 1.$$

(iii) Let $n \in \mathcal{E} \setminus \{1, 3, 5\}$. Then there exists $v_0 \in [0, 1]^{\phi(n)}$ such that $N_{\mathbb{Q}(\zeta_n)}(\xi_{v_0}) \geq 2$; for example, the vector in the third column of Table 1. Let $k \geq 2$ such that

$$(14) \quad (1 - 1/k)^{\phi(n)} > 1/2,$$

and let $v = (1 - 1/k) \cdot v_0$. Then $v \in [0, 1]^{\phi(n)}$ and

$$(15) \quad \begin{aligned} N_{\mathbb{Q}(\zeta_n)}(\xi_v) &= N_{\mathbb{Q}(\zeta_n)}(\xi_{(1-1/k) \cdot v_0}) = (1 - 1/k)^{\phi(n)} N_{\mathbb{Q}(\zeta_n)}(\xi_{v_0}) \\ &= (1 - 1/k)^{\phi(n)} \cdot 2 > 1. \end{aligned} \quad \square$$

Lemma 4. *Let $n \in \mathcal{E}$, that is, $\mathbb{Q}(\zeta_n)$ is a euclidean cyclotomic field. Then we have*

$$\max\{N_{\mathbb{Q}(\zeta_n)}(\xi_v): v \in [-1, 1]^{\phi(n)}\} = \begin{cases} 1, & n = 1, \\ 3, & n = 3, \\ 2, & n = 4, \\ 9, & n = 8, \\ 225/16, & n = 12, \\ > 2^{\phi(n)}, & \text{otherwise.} \end{cases}$$

Proof. (i) For $n = 1, 3, 4$, we have

$$(16) \quad \begin{aligned} \{N_{\mathbb{Q}}(\xi_v): v \in [-1, 1]\} &= \{|a|: a \in [-1, 1]\} = [0, 1], \\ \{N_{\mathbb{Q}(\zeta_3)}(\xi_v): v \in [-1, 1]^2\} &= \{a^2 - ab + b^2: a, b \in [-1, 1]\} = [0, 3], \\ \{N_{\mathbb{Q}(i)}(\xi_v): v \in [-1, 1]^2\} &= \{a^2 + b^2: a, b \in [-1, 1]\} = [0, 2]. \end{aligned}$$

(ii) Let $n = 8$. Then $\zeta_8 = \exp(2\pi i/8) = (1 + i)/2$ and $m = \phi(8) = 4$. We have

$$(17) \quad \xi_v = a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3, \quad v = (a, b, c, d) \in \mathbb{Z}^4,$$

and the norm of ξ_v is

$$(18) \quad \begin{aligned} N_8(a, b, c, d) &= (a^2 - c^2 + 2bd)^2 + (b^2 - d^2 - 2ac)^2 \\ &= a^4 + b^4 + c^4 + d^4 + 2a^2c^2 + 2b^2d^2 + 4a^2bd - 4ab^2c - 4bc^2d + 4acd^2. \end{aligned}$$

We define a linear change of variables, $N_8(a, b, c, d) = M_8(e, f, g, h)$,

$$(19) \quad \begin{aligned} e &= a + (b - d)/\sqrt{2}, & f &= a - (b - d)/\sqrt{2}, \\ g &= c + (b + d)/\sqrt{2}, & h &= c - (b + d)/\sqrt{2}. \end{aligned}$$

Then

$$(20) \quad M_8(e, f, g, h) = (e^2 + g^2)(f^2 + h^2).$$

Hence M_8 , and thus N_8 , have no local maximum in \mathbb{R}^4 . Consequently, the maximum of N_8 over the tesseract $T = [-1, 1]^4$ is on the boundary of T . The boundary of T consists of eight cubes, the intersections of T with each of the eight 3-spaces

$$(21) \quad \begin{aligned} \{a = 1\}, & \quad \{b = 1\}, & \quad \{c = 1\}, & \quad \{d = 1\}, \\ \{a = -1\}, & \quad \{b = -1\}, & \quad \{c = -1\}, & \quad \{d = -1\}. \end{aligned}$$

By making use of the equivalences

$$(22) \quad N_8(a, b, c, d) = \begin{cases} N_8(-a, -b, -c, -d), \\ N_8(-d, a, b, c) = N_8(-c, -d, a, b) = N_8(-b, -c, -d, a), \\ N_8(-a, b, -c, d) = N_8(a, -b, c, -d), \\ N_8(c, -b, a, d), \\ N_8(-a, d, c, b), \end{cases}$$

we only need to analyze one of these cubes, say $\{a = 1\}$. For

$$(23) \quad F(e, f, g, h) = a = (e + f)/2,$$

solve the Lagrange multiplier condition $\nabla N_8(v) = \lambda \nabla F(v)$ with constraint $F(v) = 1$. The computation in the (e, f, g, h) coordinates is simple, pointing out the significance of the change of variables (19), a key step of our approach. The calculation yields exactly one critical point

$$(24) \quad (e, f, g, h) = (1, 1, 0, 0),$$

expressed in the (a, b, c, d) coordinates by

$$(25) \quad (a, b, c, d) = (1, 0, 0, 0),$$

it lies in the center of the cube. Its norm is

$$(26) \quad N_8(1, 0, 0, 0) = 1.$$

Since we will obtain bigger norms than that, we conclude that the maximum is on the boundary of the cube, that is, on one of the six squares

$$(27) \quad (1, \pm 1, r, s), \quad (1, r, \pm 1, s), \quad (1, r, s, \pm 1), \quad r, s \in [-1, 1].$$

By making use of the equivalences above we are left with two cases, say, the squares

$$(28) \quad (1, 1, r, s), \quad (1, r, 1, s), \quad r, s \in [-1, 1].$$

We show that there is no maximum of N_{12} on the inner of these squares. Indeed, since the polynomial

$$(29) \quad \begin{aligned} N_8(1, 1, r, s) & \\ &= N_8(1, 1, t+u, t-u) & r = t+u, \\ &= 2(t^4 + 2t^2(2u^2 + (u-1)^2) + (u^2 + 2u - 1)^2), & s = t-u, \end{aligned}$$

increases, if $|t|$ increases, there will be no maximum on the inner of the first square in (28). Secondly, since the polynomial

$$(30) \quad N_8(1, r, 1, s) = (r^2 + s^2)^2 + 4s^2 - 4r^2 + 4$$

increases, if $|s|$ increases, there also will be no maximum on the inner of the second square in (28).

Hence, the maximum is to be found on the line segments that form the boundary of the squares in (28). By making use of the equivalences above, we only have to consider two cases, that is, the overall maximum is the maximal of the following two numbers,

$$(31) \quad \begin{aligned} \max_{r \in [-1, 1]} N_8(1, 1, 1, r) &= \max_{r \in [-1, 1]} r^4 + 6r^2 + 1 = 8, & (r = \pm 1), \\ \max_{r \in [-1, 1]} N_8(1, 1, r, 1) &= \max_{r \in [-1, 1]} r^4 - 2r^2 + 9 = 9, & (r = 0), \end{aligned}$$

and we obtain $\max\{N_{\mathbb{Q}(\zeta_8)}(\xi_v) : v \in [-1, 1]^4\} = 9$.

(iii) Let $n = 12$. Then $\zeta_{12} = \exp(\pi i/6) = (\sqrt{3} + i)/2$ and $m = \phi(12) = 4$. The elements of $\mathbb{Z}[\zeta_{12}]$ are of the form

$$(32) \quad \xi_v = a + b\zeta_{12} + c\zeta_{12}^2 + d\zeta_{12}^3, \quad v = (a, b, c, d) \in \mathbb{Z}^4,$$

and the norm of ξ_v is

$$(33) \quad \begin{aligned} N_{12}(a, b, c, d) &= a^4 + b^4 + c^4 + d^4 + 2a^3c + 2ac^3 + 2b^3d + 2bd^3 + 3a^2c^2 + 3b^2d^2 + 2a^2d^2 \\ &\quad - a^2b^2 - b^2c^2 - c^2d^2 + 2a^2bd + 2acd^2 - 4ab^2c - 4bc^2d - 4abcd. \end{aligned}$$

We define a linear change of variables, $N_{12}(a, b, c, d) = M_{12}(e, f, g, h)$,

$$(34) \quad \begin{aligned} e &= (a + \sqrt{3}b + 2c + \sqrt{3}d)/2, & f &= (a - \sqrt{3}b + 2c - \sqrt{3}d)/2, \\ g &= (\sqrt{3}a + b - d)/2, & h &= (\sqrt{3}a - b + d)/2. \end{aligned}$$

Then

$$(35) \quad M_{12}(e, f, g, h) = (e^2 + g^2)(f^2 + h^2).$$

Hence M_{12} , and thus N_{12} , have no local maximum in \mathbb{R}^4 . Consequently, the maximum of N_{12} over the tesseract $T = [-1, 1]^4$ is on the boundary of T . The boundary of T consists of eight cubes, the intersections of T with each of the eight 3-spaces listed in (21) above. By making use of the equivalences

$$(36) \quad N_{12}(a, b, c, d) = \begin{cases} N_{12}(-a, -b, -c, -d), \\ N_{12}(d, c, b, a) \end{cases}$$

we only need to analyze two cubes, say, $\{a = 1\}$ and $\{c = 1\}$. Let

$$(37) \quad F_a(e, f, g, h) = a = \frac{g+h}{\sqrt{3}}, \quad \text{and} \quad F_c(e, f, g, h) = c = \frac{e+f}{2} - \frac{g+h}{2\sqrt{3}}.$$

For $F = F_a, F_c$, solving the Lagrange multiplier condition $\nabla N_{12}(v) = \lambda \nabla F(v)$ with constraint $F(v) = 1$, yields exactly two critical points,

$$(38) \quad (e, f, g, h) = (0, 0, \sqrt{3}/2, \sqrt{3}/2), \quad (3/4, 3/4, -\sqrt{3}/4, -\sqrt{3}/4),$$

or expressed in the (a, b, c, d) coordinates,

$$(39) \quad (a, b, c, d) = (1, 0, -1/2, 0), \quad (-1/2, 0, 1, 0).$$

Their norm is

$$(40) \quad N_{12}(1, 0, -1/2, 0) = N_{12}(-1/2, 0, 1, 0) = 9/16.$$

Since we will obtain bigger norms than that, we conclude that the maximum is on the boundary of one of the two cubes, that is, one of the 12 squares

$$(41) \quad \begin{aligned} &(1, \pm 1, r, s), \quad (1, r, \pm 1, s), \quad (1, r, s, \pm 1), \\ &(\pm 1, r, 1, s), \quad (r, \pm 1, 1, s), \quad (r, s, 1, \pm 1), \end{aligned} \quad r, s \in [-1, 1].$$

By making use of the equivalences above we are left with four cases, say, the squares

$$(42) \quad (1, 1, r, s), \quad (1, r, 1, s), \quad (1, r, -1, s), \quad (r, 1, 1, s), \quad r, s \in [-1, 1].$$

We show that there is no maximum of N_{12} on the inner of these squares. Indeed, since the polynomial

$$(43) \quad \begin{aligned} &N_{12}(1, 1, r, s) \\ &= N_{12}(1, 1, t+u, t-u-1) && r = t+u, \\ &= t^4 + 2t^2(3u^2 + (2u+1)^2) + (u^2 + 4u+1)^2 && s = t-u-1, \end{aligned}$$

increases, if $|t|$ increases, there is no maximum on the inner of the first square of (42). Next, since we have the equivalence

$$(44) \quad \begin{aligned} N_{12}(1, r, 1, s) &= N_{12}(1, s' - r', 1, 2r' + s') & r = -r' + s' \\ &= 9N_{12}(1, r', -1, s') & s = 2r' + s', \end{aligned}$$

and since the polynomial

$$(45) \quad \begin{aligned} N_{12}(1, r, -1, s) &= N_{12}(1, t - u/\sqrt{3}, -1, 2u/\sqrt{3}) & r = t - u/\sqrt{3}, \\ &= 1 - 2u^2 + u^4 + 2t^2 + 2u^2t^2 + t^4 & s = 2u/\sqrt{3}, \\ &= (t^2 + u^2)^2 + 2t^2 - 2u^2 + 1 \end{aligned}$$

increases, if $|t|$ increases, there is also no maximum on the inner of the second and third squares of (42). Finally, since the polynomial

$$(46) \quad \begin{aligned} N_{12}(r, 1, 1, s) &= N_{12}(u + t, 1, 1, u - t) & r = u + t, \\ &= t^4 + ((u + 1)^2 + u^2 + 1)t^2 + u^4 + 2u^3 - u & s = u - t, \end{aligned}$$

increases, if $|t|$ increases, there is also no maximum on the inner of the fourth square of (42).

Hence, the maximum is to be found on the lines that form the boundary of the squares. By making use of the equivalences above, indeed all 32 lines that form the edges of the tesseract T are equivalent to the following four cases. That is, the overall maximum is the maximal of the following four numbers,

$$(47) \quad \begin{aligned} \max_{r \in [-1, 1]} N_{12}(r, 1, 1, 1) &= \max_{r \in [-1, 1]} r^4 + 2r^3 + 6r^2 - 4r + 4 = 13, & (r = -1), \\ \max_{r \in [-1, 1]} N_{12}(r, -1, 1, 1) &= \max_{r \in [-1, 1]} r^4 + 2r^3 + 2r^2 + 4r + 4 = 13, & (r = 1), \\ \max_{r \in [-1, 1]} N_{12}(1, r, 1, 1) &= \max_{r \in [-1, 1]} r^4 + 2r^3 - 3r^2 - 4r + 13 = 225/16, & (r = -1/2). \\ \max_{r \in [-1, 1]} N_{12}(-1, r, 1, 1) &= \max_{r \in [-1, 1]} r^4 + 2r^3 + 5r^2 + 4r + 1 = 13, & (r = 1). \end{aligned}$$

and we obtain $\max\{N_{12}(\xi_v) : v \in [-1, 1]^4\} = 225/16 = 14.0625$.

(iv) Suppose that $n \in \mathcal{E} \setminus \{1, 3, 4, 8, 12\}$. By explicit computations, displayed in Table 2, we observe that

$$(48) \quad \max\{N_{\mathbb{Q}(\zeta_n)}(\xi_v) : v \in \{-1, 1\}^{\phi(n)}\} > 2^{\phi(n)},$$

whence $\max\{N_{\mathbb{Q}(\zeta_n)}(\xi_v) : v \in [-1, 1]^{\phi(n)}\} \geq \max\{N_{\mathbb{Q}(\zeta_n)}(\xi_v) : v \in \{-1, 1\}^{\phi(n)}\} > 2^{\phi(n)}$. \square

Proof of Theorem 1. (i) CASE I. Let $n = 1, 3$. Since $v - \lfloor v \rfloor \in [0, 1)^{\phi(n)}$, we have by Lemma 3,

$$(49) \quad N_{\mathbb{Q}(\zeta_n)}(\xi_v - \xi_{\lfloor v \rfloor}) = N_{\mathbb{Q}(\zeta_n)}(\xi_{v - \lfloor v \rfloor}) < 1.$$

n	$\phi(n)$	$v \in \arg \min\{N_{\mathbb{Q}(\zeta_n)}(\xi_v) \geq 2: v \in \{0, 1\}^{\phi(n)}\}$	$N_{\mathbb{Q}(\zeta_n)}(\xi_v)$
1	1	—	-
3	2	—	-
4	2	(1, 1)	2
5	4	—	-
8	4	(1, 1, 0, 0)	2
12	4	(1, 1, 1, 0)	4
7	6	(1, 1, 0, 1, 0, 0)	8
9	6	(1, 1, 0, 1, 0, 0)	3
15	8	(1, 1, 0, 0, 1, 0, 0, 0)	16
16	8	(1, 1, 0, 0, 0, 0, 0, 0)	2
20	8	(1, 1, 0, 0, 1, 0, 0, 0)	5
24	8	(1, 1, 1, 0, 0, 0, 0, 0)	4
11	10	(1, 1, 0, 1, 0, 0, 0, 0, 0, 0)	23
13	12	(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)	27
21	12	(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)	7
28	12	(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)	8
36	12	(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)	9
17	16	(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)	103
32	16	(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)	2
40	16	(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)	16
48	16	(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)	4
60	16	(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)	16
19	18	(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)	191
27	18	(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)	3
25	20	(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)	5
33	20	(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)	67
44	20	(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)	89
35	24	(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)	71
45	24	(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)	81
84	24	(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)	49

TABLE 1. For all cyclotomic fields $\mathbb{Q}(\zeta_n)$ that are euclidean, the table shows the value $\min\{N_{\mathbb{Q}(\zeta_n)}(\xi_v) \geq 2: v \in \{0, 1\}^{\phi(n)}\}$ (in the last column), and a vector v that produces this minimum. (For $n = 1, 3, 5$, the set is empty.) If $n = 2^k$ ($k \geq 2$), then $v = (1, 1, 0, \dots, 0) \in \mathbb{Z}^{2^{k-1}}$ and $N_{\mathbb{Q}(\zeta_n)}(\xi_v) = 2$.

n	$\phi(n)$	$v \in \arg \max\{N_{\mathbb{Q}(\zeta_n)}(\xi_v) : v \in \{-1, 1\}^{\phi(n)}\}$	$N_{\mathbb{Q}(\zeta_n)}(\xi_v)$
1	1	(1)	1
3	2	(1, -1)	3
4	2	(1, 1)	2
5	4	(1, -1, -1, 1)	25
8	4	(1, 1, 1, 1)	8
12	4	(1, 1, 1, -1)	13
7	6	(1, 1, -1, 1, -1, -1)	343
9	6	(1, 1, -1, -1, -1, 1)	513
15	8	(1, 1, 1, -1, 1, -1, -1, -1)	22 801
16	8	(1, 1, 1, 1, 1, -1, 1, 1)	2 176
20	8	(1, 1, 1, -1, 1, -1, 1, 1)	7 625
24	8	(1, 1, 1, -1, 1, 1, 1, -1)	15 633
11	10	(1, -1, 1, 1, 1, -1, -1, -1, 1, -1)	161 051
13	12	(1, -1, 1, 1, -1, -1, -1, -1, 1, 1, -1, 1)	4 826 809
21	12	(1, 1, 1, -1, 1, 1, -1, -1, -1, -1, 1, -1)	24 397 297
28	12	(1, 1, 1, -1, 1, 1, -1, 1, -1, 1, 1, 1)	4 863 181
36	12	(1, 1, 1, 1, -1, 1, 1, 1, 1, 1, -1, 1)	10 708 281
17	16	(1, 1, -1, 1, -1, -1, -1, 1, 1, -1, -1, -1, 1, -1, 1, 1)	6.98×10^9
32	16	(1, 1, 1, 1, 1, 1, -1, 1, -1, 1, 1, -1, -1, 1, 1, 1)	2.31×10^9
40	16	(1, 1, 1, 1, 1, 1, -1, 1, 1, -1, -1, -1, 1, -1, 1, -1)	1.22×10^{10}
48	16	(1, 1, 1, 1, -1, -1, 1, -1, 1, 1, 1, 1, -1, -1, 1, -1)	4.04×10^{10}
60	16	(1, 1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, -1, -1, 1)	3.84×10^{10}
19	18	(1, -1, -1, 1, 1, 1, 1, -1, 1, -1, 1, -1, -1, -1, -1, 1, 1, -1)	3.23×10^{11}
27	18	(1, -1, 1, 1, -1, 1, 1, 1, -1, -1, -1, -1, -1, 1, -1, -1, -1, 1)	2.65×10^{12}
25	20	(1, 1, 1, -1, 1, -1, -1, -1, 1, -1, -1, -1, -1, 1, -1, 1, 1, 1, -1, 1)	4.35×10^{13}
33	20	(1, -1, 1, 1, 1, 1, -1, 1, -1, -1, -1, -1, 1, 1, -1, -1, -1, 1, -1, 1)	2.83×10^{14}
44	20	(1, 1, 1, 1, 1, -1, 1, -1, 1, 1, 1, -1, -1, 1, -1, 1, 1, -1, 1, 1)	1.88×10^{13}
35	24	(1, 1, -1, 1, 1, 1, -1, -1, -1, -1, -1, -1, 1, -1, 1, -1, 1, 1, -1, -1, 1, -1, 1, 1)	9.77×10^{17}
45	24	(1, 1, 1, 1, 1, -1, -1, 1, -1, 1, -1, -1, -1, 1, -1, -1, -1, -1, -1, -1, 1, 1, -1, 1)	2.20×10^{18}
84	24	(1, 1, 1, 1, -1, -1, 1, 1, -1, 1, -1, 1, -1, -1, 1, 1, 1, 1, -1, -1, 1, 1, -1, 1)	2.42×10^{18}

TABLE 2. For all cyclotomic fields $\mathbb{Q}(\zeta_n)$ that are euclidean, the table shows the value $\max\{N_{\mathbb{Q}(\zeta_n)}(\xi_v) : v \in \{-1, 1\}^{\phi(n)}\}$ (in the last column), and a vector v that produces this maximum. For $n = p$ prime, v is the Dirichlet character $\chi = \left(\left(\frac{1}{p}\right), \dots, \left(\frac{p-1}{p}\right)\right)$, so $|\xi_\chi| = \sqrt{p}$ and $N_{\mathbb{Q}(\zeta_n)}(\xi_\chi) = p^{(p-1)/2}$.

CASE II. Let $n \in \mathcal{E} \setminus \{1, 3\}$. Then by Lemma 3 there exists $v \in [0, 1]^{\phi(n)}$ such that $N_{\mathbb{Q}(\zeta_n)}(\xi_v) > 1$. Then $\lfloor v \rfloor = (0, \dots, 0) \in \mathbb{Z}^{\phi(n)}$ and

$$(50) \quad N_{\mathbb{Q}(\zeta_n)}(\xi_v - \xi_{\lfloor v \rfloor}) = N_{\mathbb{Q}(\zeta_n)}(\xi_v) > 1.$$

CASE III. Let $n \notin \mathcal{E}$. Then $\mathbb{Q}(\zeta_n)$ is not euclidean, hence in particular there does not exist any 1-step norm-euclidean algorithm.

(ii) CASE I. Let $n = 1, 3, 4, 8, 12$. Since $v - \lfloor v + 1/2 \rfloor \in [-1/2, 1/2]^{\phi(n)}$ we obtain by Lemma 4,

$$(51) \quad \begin{aligned} & N_{\mathbb{Q}(\zeta_n)}(\xi_v - \xi_{\lfloor v+1/2 \rfloor}) \\ &= N_{\mathbb{Q}(\zeta_n)}(\xi_{v-\lfloor v+1/2 \rfloor}) \\ &\leq \max\{N_{\mathbb{Q}(\zeta_n)}(\xi_v) : v \in [-1/2, 1/2]^{\phi(n)}\} \\ &= \frac{1}{2^{\phi(n)}} \max\{N_{\mathbb{Q}(\zeta_n)}(\xi_v) : v \in [-1, 1]^{\phi(n)}\} = \begin{cases} 1/2, & n = 1, \\ 3/8, & n = 3, \\ 1/2, & n = 4, \\ 9/16, & n = 8, \\ 225/256, & n = 12. \end{cases} \end{aligned}$$

CASE II. Let $n \in \mathcal{E} \setminus \{1, 3, 4, 8, 12\}$. Then by Lemma 4 there exists $v_0 \in [-1, 1]^{\phi(n)}$ such that $N_{\mathbb{Q}(\zeta_n)}(\xi_{v_0}) > 2^{\phi(n)}$. Hence, there exists $k \geq 1$ such that

$$(52) \quad N_{\mathbb{Q}(\zeta_n)}(\xi_{v_0}) > ((1 + 1/k) \cdot 2)^{\phi(n)}.$$

Let

$$(53) \quad v = k/(2k + 2) \cdot v_0,$$

and observe that $v \in (-1/2, 1/2)^{\phi(n)}$. Thus $\lfloor v + 1/2 \rfloor = (0, \dots, 0) \in \mathbb{Z}^{\phi(n)}$ and

$$(54) \quad \begin{aligned} & N_{\mathbb{Q}(\zeta_n)}(\xi_v - \xi_{\lfloor v+1/2 \rfloor}) = N_{\mathbb{Q}(\zeta_n)}(\xi_v) = N_{\mathbb{Q}(\zeta_n)}(\xi_{k/(2k+2) \cdot v_0}) \\ &= (k/(2k + 2))^{-\phi(n)} N_{\mathbb{Q}(\zeta_n)}(\xi_{v_0}) \\ &> (k/(2k + 2))^{-\phi(n)} (2 + 2/k)^{\phi(n)} = 1. \end{aligned}$$

CASE III. Suppose that $n \notin \mathcal{E}$. Then $\mathbb{Q}(\zeta_n)$ is not euclidean, hence in particular there is no 1-step norm-euclidean algorithm. \square

REFERENCES

- [1] E. Bayer Fluckiger, *Upper bounds for Euclidean minima of algebraic number fields*, J. Number Theory **121** (2006), 305–323.
- [2] T. Chella, *Dimostrazione dell' esistenza di un algoritmo delle divisioni successive per alcuni corpi circolari* (Italian), Annali di Mat. **1** (1924), 199–218.
- [3] G. E. Cooke, *A weakening of the Euclidean property for integral domains and applications to algebraic number theory I*, J. Reine Angew. Math. **282** (1976), 133–156.
- [4] G. E. Cooke, *A weakening of the Euclidean property for integral domains and applications to algebraic number theory II*, J. Reine Angew. Math. **283/284** (1976), 71–85.
- [5] I. B. Damgård, G. S. Frandsen, *Efficient algorithms for the gcd and cubic residuosity in the ring of Eisenstein integers*, J. Symbolic Comput. **39** (2005), 643–652.

- [6] G. Eisenstein, *Über einige allgemeine Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt, nebst Anwendungen derselben auf die Zahlentheorie* (German), J. Reine Angew. Math. **39** (1850), 224–274; 275–287.
- [7] M. Elia, J. C. Interlando, *On the computation of the norm-Euclidean minimum of algebraic number fields*, Int. J. Algebra **3** (2009), 341–354.
- [8] M. Elia, C. Monico, *On the representation of primes in $\mathbb{Q}(\sqrt{2})$ as sums of squares*, JP J. Algebra Number Theory Appl. **8** (2007), 121–133.
- [9] R. B. Lakein, *Euclid's algorithm in complex quartic fields*, Acta Arith. **20** (1972), 393–400.
- [10] D. Lazard, *Le meilleur algorithme d'Euclide pour $K[X]$ et Z* , C. R. Acad. Sci. Paris Sér. A-B **284** (1977), A1–A4.
- [11] F. Lemmermeyer, *The Euclidean algorithm in algebraic number fields*, Exposition. Math. **13** (1995), 385–416, updated version 2004.
- [12] H. W. Lenstra, Jr., *Euclid's algorithm in cyclotomic fields*, J. London Math. Soc. **10** (1975), 457–465.
- [13] H. W. Lenstra, Jr., *Euclidean number fields. I*, Math. Intelligencer **2** (1979/80), 6–15.
- [14] M.-G. Leu, *The restricted Nagata's pairwise algorithm and the Euclidean algorithm* Osaka J. Math. **45** (2008), 807–818.
- [15] J. M. Masley, *On Euclidean rings of integers in cyclotomic fields*, J. Reine Angew. Math. **272** (1975), 45–48.
- [16] J. M. Masley, H. L. Montgomery, *Cyclotomic fields with unique factorization*, J. Reine Angew. Math. **286/287** (1976), 248–256.
- [17] G. Meissner, *Bemerkung zur Bestimmung der nächsten ganzen Zahl im Gebiete der komplexen Zahlen $a + b\varrho$* (German), Hamb. Mitt. **4** (1909), 441–444.
- [18] T. Motzkin, *The Euclidean algorithm* Bull. Amer. Math. Soc. **55** (1949), 1142–1146.
- [19] P. Samuel, *About Euclidean rings*, J. Algebra **19** (1971) 282–301.
- [20] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1997.

FACULTY OF MATHEMATICS, UNIVERSITY OF VIENNA, NORDBERGSTRASSE 15, 1090 VIENNA, AUSTRIA
E-mail address: `norbert.kaiblinger@univie.ac.at`