Prime-Producing Polynomials and Principal Ideal Domains

Author(s): Daniel Fendel
Source: *Mathematics Magazine*, Vol. 58, No. 4 (Sep., 1985), pp. 204-210
Published by: Taylor & Francis, Ltd. on behalf of the Mathematical Association of America
Stable URL: https://www.jstor.org/stable/2689515
Accessed: 09-03-2020 15:25 UTC

Prime-producing Polynomials and Principal Ideal Domains

If a certain polynomial yields "enough" prime values, then a corresponding number ring will be a principal ideal domain, and conversely.

DANIEL FENDEL
San Francisco State University
San Francisco, CA 94132

Consider the well-known polynomial

$$x^2+x+41,$$

which produces prime values for every integer x with $0 \leq x \leq 39$. A classic problem is to find the constants C which could replace 41. That is, we ask:

For what integers $C \geq 1$ does the polynomial

$$x^2+x+C$$

produce prime values for all integers x with $0 \leq x \leq C-2$?

(Of course, $C-2$ is the largest upper limit on x for which such an assertion could be true; for if $x=C-1$, then $x^2+x+C=C^2$, which is not prime.)

Interestingly, all such values C are known, and 41 is the largest of them. The values of C which answer the above question are:

$$C=1,2,3,5,11,17, \text{ and } 41.$$

There is a natural connection between the polynomials x^2+x+C and imaginary quadratic fields. We can see this by factoring the polynomial over the complex numbers:

$$x^2+x+C=(x+\alpha)(x+\bar{\alpha}),$$

where

$$\alpha=\frac{1+\sqrt{1-4C}}{2}, \qquad \bar{\alpha}=\frac{1-\sqrt{1-4C}}{2};$$

$\bar{\alpha}$ is the complex conjugate of α. For convenience, we set

$$n=4C-1.$$

It is reasonable to look for a relationship between the "prime-producing" character of the polynomial x^2+x+C and factorization in the field $Q(\sqrt{-n})$. In fact, a strong relationship of this type does exist. Specifically, let D_n be the ring of "algebraic integers" in $Q(\sqrt{-n})$. (This will be defined and described in the next section.) We will prove the following (given as Theorem 4 below):

(I) *If D_n is a unique factorization domain (UFD), with $n=4C-1$, then the polynomial x^2+x+C produces prime values for all integers x with $0 \leq x \leq C-2$.*

Perhaps more surprising is that there is also a connection between these polynomials and the question of whether D_n is a principal ideal domain. We will prove a result of the following type:

(II) *If the polynomial x^2+x+C produces prime values for "enough" integers x, then D_n is a principal ideal domain (PID).*

The "enough" here turns out to be an interval $0 \le x \le C^*$, where C^* depends on n, but is always less than or equal to $C-2$. The details are spelled out in Theorem 3. Because of the elementary fact that every PID is a UFD (see [**2**]), statement (II) is thus a kind of "strong converse" to (I).

Together with a simple discussion of the cases $n \equiv 1$ or 2 mod 4, (I) and (II) constitute an elementary proof of the following well-known result:

COROLLARY. *If D_n is a unique factorization domain, then it is also a principal ideal domain.*

(There is actually a much broader result known for general algebraic number rings, but the proof requires considerable background in ideal theory (see [**4**]). However, it is *not* true for arbitrary rings that a UFD must be a PID.)

Our results (I) and (II) also allow us to deduce the complete list of values for C given earlier, based on the following very deep theorem of Stark (see [**3**]):

THEOREM (Stark). *D_n is a principal ideal domain (for positive n) if and only if n is one of the following values*:

$$n = 1, 2, 3, 7, 11, 19, 43, 67, 163.$$

Since we are using $n = 4C-1$, we can ignore the values $n = 1, 2$. The remaining seven values of n give precisely the values of C listed earlier.

The proofs of (I) and (II) are based on the complex norm ϕ, defined as follows:

$$\phi(\gamma) = \gamma\bar{\gamma} = |\gamma|^2, \quad \text{for } \gamma \in \mathbb{C}.$$

There is a simple condition using ϕ (given as Theorem 1 below) for determining which D_n's are euclidean domains "with respect to ϕ." (The precise meaning of this phrase is given later.) If we visualize D_n and the field $K = Q(\sqrt{-n})$ in the complex plane, then Theorem 1 can be expressed in geometric terms as follows:

(III) *D_n is a euclidean domain (ED) with respect to ϕ if and only if it satisfies*:
(*) *if γ is in K, then it is within one unit of some element of D_n.*

Using the elementary fact that every ED is a PID (see [**2**]), (III) yields *some* of the values of n in Stark's list. But not all: in particular, the last four values ($n = 19, 43, 67, 163$) give rings D_n which are principal ideal domains but not euclidean domains with respect to ϕ. (An elementary proof that D_{19} is not euclidean under any norm is given by Wilson [**5**].) Therefore something more subtle than (III) is needed to handle PID's.

The key idea in the proof of (II) is the existence of an analogue to Theorem 1 for identifying PID's. This analogue (given as Theorem 2 below) can also be expressed geometrically, as follows:

(IV) *D_n is a principal ideal domain if and only if it satisfies*:
(**) *if γ is in K but not in D_n, then some multiple $\chi\gamma$ of γ (with χ in D_n) is within one unit of, <u>but not equal to</u>, some element of D_n.*

(Note: (IV) extends naturally to arbitrary algebraic number fields. In the extended version, K is any algebraic number field, D is its ring of integers, and "distance" is measured by the field norm.)

The bulk of the proof of (II) consists of an analysis of condition (**) above. This analysis is eventually tied in with our polynomials by the fact that $\phi(x+\alpha) = x^2 + x + C$, for integers x (with α as defined earlier).

Preliminaries

We consider the field $K = Q(\sqrt{-n})$, where Q is the field of rational numbers, and n is a positive, square-free integer. Thus, modulo 4, n is congruent to 1, 2, or 3. The case $n \equiv 3$ mod 4 is of primary importance for this paper, since it corresponds to the situation of the polynomial $x^2 + x + C$, where $n = 4C-1$, in our opening question.

Recall that an element of K is an **algebraic integer** if it is the root of some monic polynomial with integral coefficients. The algebraic integers within K form a ring, which will be denoted by D_n. All congruences considered here will be modulo 4 unless otherwise indicated, so we will write $n \equiv a$ to mean $n \equiv a \bmod 4$. We will also use the following standard notation:

Z: *the ring of integers*

(γ): *the ideal generated by an element γ in D_n*

$[a]$: *the largest integer m such that $m \le a$*

$a|b$: *a is a divisor of b (where a and b are in Z).*

The following lemma gives a concrete description of the ring D_n:

LEMMA 1. *D_n is the set of elements of the form $a + b\alpha$, with a and b in Z, where*

$$\alpha = \begin{cases} \sqrt{-n} & \text{if } n \equiv 1 \text{ or } 2 \\ \dfrac{1+\sqrt{-n}}{2} & \text{if } n \equiv 3. \end{cases}$$

(For a proof, see [**1**].) In terms of the complex plane, Lemma 1 says that the elements of D_n form a lattice, which will look like FIGURE 1 or FIGURE 2, depending on whether $n \equiv 1, 2$ or $n \equiv 3$.

Elements of K can be written as $a + b\alpha$, with a and b in Q. We can express the norm $\phi(\gamma) = |\gamma|^2$ on K in terms of this description, as follows:

$$\phi(a + b\alpha) = \begin{cases} a^2 + nb^2 & \text{if } n \equiv 1 \text{ or } 2 \\ \left(a + \dfrac{b}{2}\right)^2 + \dfrac{nb^2}{4} = a^2 + ab + \dfrac{n+1}{4}b^2 & \text{if } n \equiv 3. \end{cases}$$

Note that, in the $n \equiv 3$ case, if we set $a = x$ and $b = 1$, we obtain

$$\phi(x + \alpha) = x^2 + x + C, \qquad \text{where } C = \frac{n+1}{4}. \tag{1}$$

The following is a summary of some elementary facts we will need about ϕ:

LEMMA 2. (i) $\phi(\gamma_1\gamma_2) = \phi(\gamma_1)\phi(\gamma_2)$.
(ii) *if $\gamma \ne 0$, then $\phi(\gamma) > 0$.*
(iii) *if $\gamma \in D_n$, then $\phi(\gamma) \in Z$.*
(iv) *if $\gamma \in D_n$, and $\phi(\gamma) = 1$, then γ is a unit.*
(v) *if γ_1 and γ_2 are in D_n, with $(\gamma_1) \subsetneq (\gamma_2)$, then $\phi(\gamma_2) < \phi(\gamma_1)$.*
(vi) *if a, b, c, d, and t are integers, with $a \equiv c \bmod t$ and $b \equiv d \bmod t$, then $\phi(a + b\alpha) \equiv \phi(c + d\alpha) \bmod t$.*
(vii) *if $n \equiv 3 \bmod 4$ and $x \in Z$, then $\phi(x + \alpha) = \phi(-1 - x + \alpha)$.*

(Verification of these properties of ϕ is left to the reader.) We also need the following result, which says, in effect, that elements of $D_n \setminus Z$ cannot be "small":

LEMMA 3. *Suppose $\gamma \in D_n \setminus Z$.*
(i) *If $n \equiv 1$ or 2, then $\phi(\gamma) \ge n$.*
(ii) *If $n \equiv 3$, then $\phi(\gamma) \ge (n+1)/4$.*

Proof. Write γ as $a + b\alpha$, so $b \ne 0$. Thus (i) is obvious. If $|b| = 1$, then $(a + b/2)^2 \ge 1/4$, so (ii) follows. But if $|b| > 1$, then $\phi(\gamma) \ge nb^2/4 \ge n$, and (ii) follows as well.

Finally, we have the following simple consequence.

LEMMA 4. *If $n > 3$ with $n \equiv 3$ and $0 \le t \le \sqrt{n/3}$, then the equation $t = \phi(x + \alpha)$ has no integral solution for x.*

This follows from Lemma 3, (ii), since $\sqrt{n/3} < (n+1)/4$ for $n > 3$, and $x + \alpha$ is in $D_n \setminus Z$.

Conditions for euclidean and principal ideal domains

We say that a ring D of complex numbers is a euclidean domain (ED) (with respect to the norm ϕ) if

(i) $\phi(\gamma)$ is an integer for all γ in D,

and

(ii) (division algorithm) if γ_1 and γ_2 are in D, with $\gamma_2 \neq 0$, then there are elements in δ and η in D satisfying $\gamma_1 = \gamma_2\delta + \eta$, and such that $\phi(\eta) < \phi(\gamma_2)$.

The following theorem is a formal statement of result (III) from the introduction.

THEOREM 1. *The following are equivalent*:
(i) D_n *is a euclidean domain.*
(ii) *For each* $\gamma \in K$, *there exists a* $\delta \in D_n$ *such that* $\phi(\gamma - \delta) < 1$.

Proof. (i) $\to$ (ii): Suppose $\gamma \in K$, and let t be an integer such that $t\gamma \in D_n$, and divide $t\gamma$ by t using the division algorithm. This gives $t\gamma = t\delta + \eta$, with δ and η in D_n and $\phi(\eta) < \phi(t)$. Then $\phi(\gamma - \delta) = \phi(\eta/t) < 1$.

(ii) $\to$ (i): First note that $\phi(\gamma) \in Z$ for all γ in D_n, by Lemma 2, (iii). Next, suppose that γ_1 and γ_2 are in D_n, with $\gamma_2 \neq 0$. Set $\gamma = \gamma_1/\gamma_2$, and choose $\delta \in D_n$ as provided so that $\phi(\gamma - \delta) < 1$, and set $\eta = \gamma_1 - \gamma_2\delta$. Then $\gamma_1 = \gamma_2\delta + \eta$, and $\phi(\eta) = \phi(\gamma_2)\phi(\gamma - \delta) < \phi(\gamma_2)$, as desired.

Using Theorem 1 and FIGURES 1 and 2, it is fairly routine to show the following:

COROLLARY 1. D_n *is a euclidean domain* (*with respect to* ϕ) *if and only if n is one of the following values*:

$$n = 1, 2, 3, 7, 11.$$

We will need the cases $n = 1$ and $n = 2$ to complete the discussion of the situation where $n \equiv 1$ or 2. The cases $n = 3$ and 7 will allow us to avoid problems with later inequalities.

We now give the analogue of Theorem 1 for principal ideal domains. (The following is (IV) from the introduction.)

THEOREM 2. *The following are equivalent*:
(i) D_n *is a principal ideal domain.*
(ii) *For each* $\gamma \in K \setminus D_n$, *there exist* χ *and* δ *in* D_n *such that* $0 < \phi(\chi\gamma - \delta) < 1$.

Proof. (i) $\to$ (ii): Suppose $\gamma \in K \setminus D_n$, and let t be an integer such that $t\gamma \in D_n$. Let I be the ideal of D_n generated by $t\gamma$ and t. By assumption, there exists $\beta \in I$ with $I = (\beta)$. Choose χ and δ in D_n with $\beta = \chi(t\gamma) - \delta t$. Since $\gamma \notin D_n$, we have $t\gamma \notin (t)$, so $(t) \subsetneq (\beta)$. By Lemma 2, (v), we have $\phi(\beta) < \phi(t)$. Since $\beta \neq 0$, we have $0 < \phi(\beta/t) = \phi(\chi\gamma - \delta) < 1$, as desired.

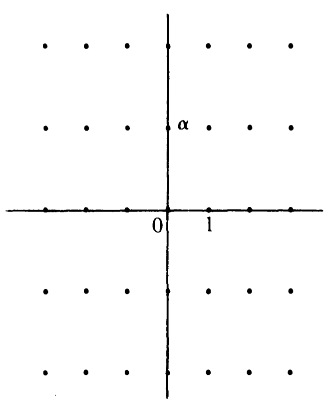

FIGURE 1. $n \equiv 1$ **or 2 mod 4.**

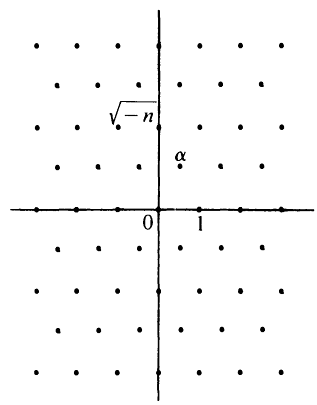

FIGURE 2. $n \equiv 3$ **mod 4.**

(ii) → (i): Let I be a nonzero ideal of D_n, and choose $\beta \in I$, $\beta \neq 0$, with $\phi(\beta)$ minimal. Thus $(\beta) \subseteq I$. Suppose $I \neq (\beta)$, so there exists $\theta \in I \setminus (\beta)$. Let $\gamma = \theta/\beta \in K \setminus D_n$, and choose χ and δ in D_n as described in (ii), so $0 < \phi(\chi\gamma - \delta) < 1$. Then $\chi\theta - \delta\beta = (\chi\gamma - \delta)\beta \in I \setminus \{0\}$, and so $0 < \phi(\chi\theta - \delta\beta) = \phi(\chi\gamma - \delta)\phi(\beta) < \phi(\beta)$, contradicting the choice of β. Thus, $I = (\beta)$, so D_n is a principal ideal domain.

The polynomial $x^2 + x + C$ and principal ideal domains

Our goal in this section is to prove the following more precise version of (II) from the introduction (recall $n = 4C - 1$).

THEOREM 3. *If $x^2 + x + C$ produces prime values for all integers x with $0 \leq x \leq \left[\frac{1}{2}\sqrt{n/3}\right]$, then D_n is a principal ideal domain.*

Thus, the C^* of (II) is actually $[(1/2)\sqrt{n/3}]$. Clearly $C^* < (n-7)/4$ $(= C - 2)$ for large n; in fact, this holds for $n \geq 11$. Corollary 1 already tells us that D_3 and D_7 are PID's, and we shall assume $n \geq 11$.

Our results will therefore give us the following curious situation. The primality of $x^2 + x + C$ over the short interval $0 \leq x \leq [(1/2)\sqrt{n/3}]$ will guarantee that D_n is a PID, and hence also a UFD. We will see (Theorem 4) that this in turn guarantees the primality of the polynomial over the generally longer interval $0 \leq x \leq (n-7)/4$!

In the proof of Theorem 3, we will use the identity (1),

$$\phi(x + \alpha) = x^2 + x + C$$

together with the criterion for PID's given by Theorem 2. Thus, following Theorem 2, we consider an arbitrary $\gamma \in K \setminus D_n$. We must find elements χ, $\delta \in D_n$ such that $0 < \phi(\chi\gamma - \delta) < 1$.

The following technical lemma is based on a famous approximation theorem of Dirichlet. It holds for any field $K = Q(\sqrt{-n})$, $n \equiv 3 \bmod 4$, and any $\gamma \in K$, whether or not the ring D_n is a PID. We defer the proof to the end of our article.

LEMMA 5. *There is a positive integer t, with $t \leq \sqrt{n/3}$, and an element δ in D_n, such that $\phi(t\gamma - \delta) < 1$.*

We shall now make two attempts to satisfy condition (ii) of Theorem 2, first with $\chi = t$ (as in Lemma 5), and if that fails, with $\chi = t\bar{\gamma}$. If both of these fail, we shall show that the polynomial $x^2 + x + C$ takes a composite value somewhere in the interval $0 \leq x \leq C^*$, contradicting the assumption of Theorem 3. Here are the details:

Let t be the smallest integer satisfying Lemma 5, and δ as provided there. If $t\gamma$ is not in D_n, then we also have $0 < \phi(t\gamma - \delta)$, and so we have fulfilled condition (ii) of Theorem 2, using $\chi = t$. So we now assume $t\gamma \in D_n$. This implies that $t\bar{\gamma}$ is also in D_n, and so we can use it as a new candidate for χ. Thus let $\chi = t\bar{\gamma}$. Then $\chi\gamma = (1/t)\phi(t\gamma)$, which is a rational number, and so $\chi\gamma$ must in fact be less than one unit from some ordinary integer δ in D_n. Thus once again we will have satisfied (ii) of Theorem 2, unless $\chi\gamma = \delta$, i.e., $\chi\gamma \in Z$. This can only happen if $t | \phi(t\gamma)$.

The following lemma tells us what we need in order to prevent that:

LEMMA 6. *If $t | \phi(t\gamma)$, then $\phi(x + \alpha)$ is composite for some integer x with $0 \leq x < t/2$.*

Proof. Since $t\gamma \in D_n$, we can write $t\gamma = a + b\alpha$, with a, $b \in Z$. We first show that b and t are relatively prime, as follows: any prime dividing t must also divide $\phi(t\gamma)$ by hypothesis, but $\phi(t\gamma) = a^2 + ab + ((n+1)/4)b^2$. Thus any prime which divides both b and t must also divide a^2, and hence a. This would mean that a, b, and t would have a common factor, contradicting the minimality of t.

Now, since b and t are relatively prime, there exists $y \in Z$ with $yb \equiv 1 \bmod t$. We then find $x \in Z$, with $ya \equiv x \bmod t$; we can choose x so that $-t/2 \leq x < t/2$. Thus $\phi(yt\gamma) = \phi(ya + yb\alpha) \equiv \phi(x + \alpha) \bmod t$ (see Lemma 2, (vi)). By assumption, $t | \phi(t\gamma)$, and so clearly $t | \phi(yt\gamma)$, and hence $t | \phi(x + \alpha)$. But $t \neq \phi(x + \alpha)$ by Lemma 4 (we have $n > 3$ here). On the other hand, Theorem 2 provides that $\gamma \notin D_n$, but we are assuming $t\gamma \in D_n$, and so $t \neq 1$. Thus $\phi(x+\alpha)$ must be composite.

Finally, we can improve the restriction on x as follows: if $-t/2 \le x < 0$, then we let $x^* = -1 - x$, which satisfies $0 \le x^* < t/2$. Since $\phi(x+\alpha) = \phi(-1-x+\alpha)$ (Lemma 2, (vii)), we have that $\phi(x^*+\alpha)$ is also composite, completing the proof.

Thus, to get D_n to be a PID, we need only assure that the conclusion of Lemma 6 is false. Using $t \le \sqrt{n/3}$, and the identity $\phi(x+\alpha) = x^2 + x + C$, this is precisely the hypothesis of Theorem 3.

The polynomial $x^2 + x + C$ and unique factorization domains

Before looking at our specific situation, we mention an elementary result about UFD's in general. Recall that an element w of a ring is called **irreducible** if a factorization $w = uv$ implies that u or v is a unit. We will need the following well-known result.

LEMMA 7. *If a ring D is a unique factorization domain, and an irreducible element $w \in D$ divides a product of elements in D, then w divides one of the factors.* (For a proof, see [**2**].)

The main result of this section is the following (this is (I) from the introduction):

THEOREM 4. *Suppose that $n \equiv 3$. If D_n is a unique factorization domain, then $x^2 + x + C$ produces prime values for all integers x with $0 \le x \le C - 2$ (where $C = (n+1)/4$).*

It turns out that we can take care of the cases $n \equiv 1, 2$ with the same basic analysis. The result in that case is the following.

THEOREM 5. *Suppose $n \equiv 1$ or 2. If $n > 2$, then D_n is not a unique factorization domain.*

Corollary 1 tells us that D_1 and D_2 are ED's, and hence PID's and UFD's. Using that fact and Theorem 5 if $n \equiv 1$ or 2, and Theorems 3 and 4 if $n \equiv 3$, we get the following consequence, mentioned in the introduction:

COROLLARY 2. *If D_n is a unique factorization domain, then it is also a principal ideal domain.*

We now turn to the proofs of Theorems 4 and 5, initially handling all cases together. We noted in Lemma 3 that there is a lower bound for $\phi(\gamma)$ if γ is in $D_n \setminus Z$. For convenience in handling the different cases, we set

$$L = \begin{cases} n & \text{if } n \equiv 1 \text{ or } 2 \\ \dfrac{n+1}{4} & \text{if } n \equiv 3. \end{cases}$$

Thus, if $\gamma \in D_n \setminus Z$, then $\phi(\gamma) \ge L$. From this we get the following:

LEMMA 8. *If p is a prime in Z, with $p < L$, then p is irreducible in D_n.*

Proof. Suppose $p = \gamma_1\gamma_2$, with $\gamma_1, \gamma_2 \in D_n$, and neither a unit. Then γ_1 and γ_2 are not integers, since p is a prime, so $p^2 = \phi(p) = \phi(\gamma_1)\phi(\gamma_2) \ge L^2$, which is a contradiction.

LEMMA 9. *If D_n is a UFD and $a \in Z$, then $\phi(a+\alpha)$ has no prime factors less than L.*

Proof. Suppose p is such a prime, so it is irreducible by Lemma 8. Then $p \mid (a+\alpha)$ or $p \mid \overline{(a+\alpha)}$ by Lemma 7 since $\phi(a+\alpha) = (a+\alpha)\overline{(a+\alpha)}$. If $n \equiv 1$ or 2 then $\overline{a+\alpha} = a - \alpha$; if $n \equiv 3$ then $\overline{a+\alpha} = a + 1 - \alpha$. In either case, p divides neither $a+\alpha$ nor $\overline{a+\alpha}$, since the coefficient of the basis element α is ± 1.

We leave it to the reader to verify the following simple inequality:

LEMMA 10. *If $n \equiv 3$ and $0 \le x \le (n-7)/4$, then $\phi(x+\alpha) < L^2$.*

Our main results are now easy.

Proof of Theorem 4. Suppose $\phi(x+\alpha) = x^2 + x + C$ is not prime, with x in the given range of values. Then $\phi(x+\alpha) < L^2$, by Lemma 10, and so $\phi(x+\alpha)$ has a prime factor less than L, contradicting Lemma 9.

Proof of Theorem 5. We have $\phi(n+\alpha) = n^2 + n$, so $\phi(n+\alpha)$ has the prime factor 2. But $2 < L$ by assumption (here $L = n$). Thus Lemma 9 says D_n cannot be a UFD.

Proof of Lemma 5. The following result concludes the proof of Theorem 3.

LEMMA 5. *Suppose $n \equiv 3$. For any $\gamma \in K$, there is a positive integer t, with $t \le \sqrt{n/3}$, and an element δ in D_n, such that $\phi(t\gamma - \delta) < 1$.*

To prove Lemma 5, we write $\gamma = a + b\alpha$ and set $m = [\sqrt{n/3}\,] + 1$. Our final lemma tells how to choose t:

LEMMA 11. *Let m be an integer ≥ 2, and $b \in Q$. Then there exists $t \in Z$, with $1 \le t \le m-1$, and $m_1 \in Z$, with $|tb - m_1| \le 1/m$.*

Proof. The proof uses the "pigeonhole principle." Let $((x))$ denote the fractional part of x, i.e., $((x)) = x - [x]$. Set $b_j = ((jb))$, $j = 1,\dots,m-1$, and $I_j = [j/m, (j+1)/m]$, $j = 0,\dots,m-1$. If some b_t is in either I_0 or I_{m-1}, then tb is within $1/m$ of an integer, as desired. If not, then we have $m-1$ b_j's and only $m-2$ remaining intervals, so two b_j's must be in the same interval. Thus, some b_r and b_s are in the same interval, with $1 \le r < s \le m-1$. Then $(s-r)b$ is within $1/m$ of some integer, so $t = s - r$ satisfies the stated condition.

We now complete the proof of Lemma 5. Choose t and m_1 as in Lemma 11, and set $c = tb - m_1$. Then choose $m_2 \in Z$ as close as possible to $ta + c/2$, (so that $|ta + c/2 - m_2| \le 1/2$), and set $\delta = m_2 + m_1\alpha$. Then

$$\begin{aligned}\phi(t\gamma - \delta) &= \phi\left[(ta - m_2) + (tb - m_1)\alpha\right]\\ &= \phi\left[(ta - m_2) + c\alpha\right]\\ &= \left(ta - m_2 + \frac{c}{2}\right)^2 + \frac{n}{4}c^2\\ &\le \frac{1}{4} + \frac{n}{4}\cdot\frac{1}{m^2}\\ &< \frac{1}{4} + \frac{n}{4}\cdot\frac{3}{n} = 1,\end{aligned}$$

as desired.

I wish to express my thanks to the referee whose suggestions were very helpful in preparing the final draft of this article.

References

[1] William W. Adams and Larry Joel Goldstein, Introduction to Number Theory, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1976, p. 216.

[2] Thomas Hungerford, Algebra, Springer-Verlag, New York, 1974, Section III.3.

[3] Harold Stark, A complete determination of the complex quadratic fields of class-number one, Michigan Math J., 14 (1967) 1–27.

[4] Edwin Weiss, Algebraic Number Theory, McGraw-Hill, New York, 1963, chapter 4.

[5] J. C. Wilson, A principal ideal ring that is not a euclidean ring, this MAGAZINE, 46 (1973) 34–38.