Research Article

On the Irreducibility of Polynomials Associated with the Complete Residue Systems in any Imaginary Quadratic Fields

Phitthayathon Phetnun, Narakorn Rompurk Kanasri, and Patiwat Singthongla

Department of Mathematics, Khon Kaen University, Khon Kaen 40002, Thailand

Correspondence should be addressed to Narakorn Rompurk Kanasri; naraka@kku.ac.th

Received 18 February 2021; Accepted 25 March 2021; Published 14 April 2021

Academic Editor: Sergejs Solovjovs

Copyright © 2021 Phitthayathon Phetnun et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

For a Gaussian prime $\pi$ and a nonzero Gaussian integer $\beta = a + bi \in \mathbb{Z}[i]$ with $a \geq 1$ and $|\beta| \geq 2 + \sqrt{2}$, it was proved that if $\pi = \alpha, \beta^n + \alpha\beta + \alpha = f(\beta)$ where $\pi \geq 1, \alpha, \beta \in \mathbb{Z}[i]\{0\}$, and $\alpha_0, \ldots, \alpha_n$ belong to a complete residue system modulo $\beta$, and the digits $\alpha_{n-1}$ and $\alpha_n$ satisfy certain restrictions, then the polynomial $f(x)$ is irreducible in $\mathbb{Z}[i][x]$. For any quadratic field $K = \mathbb{Q}(\sqrt[4]{m})$, it is well known that there are explicit representations for a complete residue system in $K$, but those of the case $m \equiv 1 \pmod{4}$ are inapplicable to this work. In this article, we establish a new complete residue system for such a case and then generalize the result mentioned above for the ring of integers of any imaginary quadratic field.

1. Introduction

According to Pólya and Szegö [1], the classical result of A. Cohn states that if a prime $p$ is expressed in the decimal representation as

$$p = a_n10^n + a_{n-1}10^{n-1} + \cdots + a_110 + a_0,$$  

(1)

then the polynomial $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ is irreducible in $\mathbb{Z}[x]$. For example, since 4831 is prime and 4831 = $4 \cdot 10^3 + 8 \cdot 10^2 + 3 \cdot 10 + 1$, it follows that $f(x) = 4x^3 + 8x^2 + 3x + 1$ is irreducible in $\mathbb{Z}[x]$. This result was subsequently generalized to any base $b$ by Brillhart et al. [2]. In 2002, Murty gave a proof of this fact [3] that was conceptually simpler than the one in [2]. Moreover, Brillhart et al. [2] generalized Cohn’s result in another direction as follows: if

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x],$$  

(2)

where $0 \leq a_i \leq 167$ for all $i$, and $f(10)$ is prime, then $f(x)$ is irreducible. In 1988, Filaseta improved this fact, that is, if coefficients of the polynomial $f(x)$ in (2) satisfy $0 \leq a_i \leq 10^6$ for $0 \leq i \leq n - 1$ and $f(10)$ is prime, then $f(x)$ is irreducible [4].

In another direction, let $K = \mathbb{Q}(\sqrt{m})$, with a unique squarefree integer $m$ unequal to 1, be a quadratic field and $O_K$ be its ring of integers. We have seen in [5] that $O_K$ is an integral domain. The quadratic field $K$ is said to be real if $K \subseteq \mathbb{R}$ and imaginary if $K \not\subseteq \mathbb{R}$. Clearly, $K$ is real if $m > 0$ and imaginary if $m < 0$. It is well known that

$$O_K = \{a + bs_m | a, b \in \mathbb{Z}\},$$  

(3)

where

$$s_m := \begin{cases} \sqrt{m} & \text{if } m \equiv 1 \pmod{4}, \\ 1 + \sqrt{m} & \text{if } m \equiv 1 \pmod{4}. \end{cases}$$  

(4)

We note that the ring of Gaussian integers $\mathbb{Z}[i]$ and the Eisenstein domain $\mathbb{Z}[(1 + \sqrt{-3})/2]$ are rings of integers of $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$, respectively.

We emphasize that a prime element in $O_K$ is an irreducible element, and the converse holds if $O_K$ is a unique factorization domain. Moreover, $K$ is the quotient field of $O_K$ [5], and the units in $O_K[x]$ are the units in $O_K$ [6]. We say that a nonzero polynomial $p(x) \in O_K[x]$ is irreducible in $O_K[x]$ if $p(x)$ is not a unit, and if $p(x) = f(x)g(x)$ with
Polynomials that are not irreducible are called reducible. Furthermore, if \( f(x) \) is a unique factorization domain and \( f(x) \) is irreducible in \( O_K(x) \), then \( f(x) \) is irreducible over \( K \) by using Gauss’s lemma.

In 2017, Singthongla et al. established the result of A. Cohn in \( O_K[x] \) [7], where \( K \) is an imaginary quadratic field such that \( O_K \) is a Euclidean domain, namely, \( m = -1, -2, -3, -7, \) and \( -11 \) [5]. The results are as follows:

(i) For \( \beta \in O_K \setminus \{0\} \), each element in \( O_K \) has a base \( \beta \)-expansion whose digits are bounded by certain constants.

(ii) For a prime element \( \pi \in O_K \), if
\[
\pi = \alpha_n \beta^{n} + \alpha_{n-1} \beta^{n-1} + \cdots + \alpha_1 \beta + \alpha_0 = f(\beta),
\]
(5)
is its base \( \beta \)-expansion in \( O_K \) and the digits \( \alpha_n \) and \( \alpha_{n-1} \) satisfy some natural restrictions, then the polynomial \( f(x) \) is irreducible in \( O_K[x] \).

(iii) For Gaussian integers, a similar base \( \beta \)-expansion but with digits belonging to a complete residue system modulo \( \beta \) is also valid.

(iv) The irreducibility result similar to that in (ii) continues to hold for Gaussian integers with base expansion as described in (iii).

At first thought, we are interested in establishing a generalization of the result in (iv) for the ring of integers \( O_K \) of any imaginary quadratic field. However, to prove this, we must use the property that \( |\beta| \geq 1 \) for all \( \beta \in O_K \setminus \{0\} \) which is valid only in the imaginary quadratic field [8] but not in the real quadratic field. Thus, the goal of this work is to establish a generalization of the result in (iv) for the ring of integers \( O_K \) of any imaginary quadratic field.

Let \( K = \mathbb{Q}(\sqrt{m}) \) be any general quadratic field. For \( \alpha, \beta \in O_K \) with \( \alpha \neq 0 \), we say that \( \alpha \) divides \( \beta \), denoted by \( \alpha | \beta \), if and only if there exists \( \delta \in O_K \) such that \( \beta = a \delta \). For \( \alpha, \beta, \gamma \in O_K \) with \( \gamma \neq \pm 1 \), we say that \( \alpha \) is congruent to \( \beta \) modulo \( \gamma \), and we write \( \alpha \equiv \beta \pmod{\gamma} \) if \( \alpha - \beta \in (\gamma) \), a principal ideal generated by \( \gamma \) or, equivalently, if \( \gamma | (\alpha - \beta) \) [9].

For \( \beta = a + b\sigma_m \in O_K \), we denote the norm of \( \beta \) by
\[
N(\beta) = \begin{cases} 
  a^2 - mb^2 & \text{if } m \not\equiv 1 \pmod{4}, \\
  a^2 + ab + b^2 \left(1 - \frac{m}{4}\right) & \text{if } m \equiv 1 \pmod{4}.
\end{cases}
\]
(6)

We note from [5] that if \( \alpha \in O_K \) is such that \( N(\alpha) = \pm p \), where \( p \) is a rational prime, then \( \alpha \) is an irreducible element. By a complete residue system modulo \( \beta \) in \( O_K \), abbreviated by CRS(\( \beta \)) [9, 10], we mean a set of \( [N(\beta)] \) elements \( \mathcal{C} = \{a_1, a_2, \ldots, a_{[N(\beta)]}\} \) in \( O_K \) such that

(i) for each \( \alpha \in O_K \), there is \( \alpha_i \in \mathcal{C} \) such that \( \alpha \equiv \alpha_i \pmod{\beta} \) and

(ii) \( \alpha_i \neq \alpha_j \pmod{\beta} \) for all \( i, j \in \{1, 2, \ldots, [N(\beta)]\} \) with \( i \neq j \).

In [10], Tadee et al. derived three explicit representations for a complete residue system in any general quadratic field. We are interested in the first one which is as follows: for \( \beta = a + b\sigma_m \in O_K \setminus \{0\} \) and \( d = \gcd(a, b) \), we have the following:

(i) Case \( m \not\equiv 1 \pmod{4} \): the set
\[
\mathcal{C}_1 = \left\{ x + y\sqrt{m} \mid x = 0, 1, \ldots, \left\lfloor \frac{N(\beta)}{d}\right\rfloor - 1 \text{ and } y = 0, 1, \ldots, \frac{d-2}{2} \right\},
\]
(1)

(8)
Then, $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$ is a CRS($\beta$).

(2) If $d$ is odd, let

\[
\mathcal{C}_1 = \left\{ x + y\sqrt{m} \mid x, y \in \mathbb{Z}, \frac{|N(\beta)|}{d} - 1 \text{ and } y = 0, 1, \ldots, \frac{d-1}{2} \right\}.
\]

\[
\mathcal{C}_2 = \left\{ x + y \left( \frac{1}{2} \right) \sqrt{m} \mid x = 0, 1, \ldots, \frac{|N(\beta)|}{d} - 1 \text{ and } y = 0, 1, \ldots, \frac{d-3}{2} \right\}.
\]

It follows from (11) and (12) that

\[
\alpha - v' \left[ (s - r) + r_m \beta \right] = u - v' \left[ a (s - r) + rb \left( \frac{m-1}{4} \right) \right] + v'' \sigma_m.
\]  
(13)

Again, by the division algorithm, there exist $t', t'' \in \mathbb{Z}$ such that

\[
u - v' \left[ a (s - r) + rb \left( \frac{m-1}{4} \right) \right] = \left( \frac{N(\beta)}{d} \right) t' + t''.
\]  
(14)

where $0 \leq t'' \leq \frac{|N(\beta)|}{d} - 1$. It follows from (13) and (14) that

\[
\alpha = v' \left[ (s - r) + r_m \beta \right] + \left( \frac{N(\beta)}{d} \right) t' + t'' + v'' \sigma_m,
\]

\[
= v' \left[ (s - r) + r_m \beta \right] + \left( \frac{\overline{\beta} \overline{t}'}{d} \right) t' + t'' + v'' \sigma_m,
\]

\[
= \beta v' \left[ (s - r) + r_m \beta \right] + \left( \frac{\overline{\overline{\beta}} t'}{d} \right) t' + t'' + v'' \sigma_m,
\]

where $\overline{\overline{\beta}} = a + b(1 - \sqrt{m})/2 = a + b - b_m \in \mathcal{O}_K$. We consequently get $v' ((s - r) + r_m \beta) + (\overline{\beta}/d) t' \in \mathcal{O}_K$, and so, $\alpha \equiv t'' + v'' \sigma_m (\text{mod} \beta)$, where $t'' + v'' \sigma_m \in \mathcal{C}$.

Next, we show that $\alpha_1 \neq \alpha_2 (\text{mod} \beta)$ for all $\alpha_1, \alpha_2 \in \mathcal{C}$, with $\alpha_1 \neq \alpha_2$. To see this, let $\alpha_1 = s_1 + s_2 \sigma_m, \alpha_2 = t_1 + t_2 \sigma_m \in \mathcal{C}$ be such that $\alpha_1 \equiv \alpha_2 (\text{mod} \beta).$ We now show that $\alpha_1 = \alpha_2$. Since $d \beta$ and $\beta (\alpha_1 - \alpha_2)$ is $\mathcal{O}_K$, we have $d (\alpha_1 - \alpha_2)$, and so, $d (s_2 - t_2)$. It follows that $s_2 = t_2$ because $0 \leq t_2 \leq d - 1$. Consequently, $\alpha_1 - \alpha_2 = s_1 - t_1$, and so, $\beta (s_1 - t_1)$.

If $a = 0$ and $b \neq 0$, we obtain that $\beta = b \sigma_m, d = |b|$, and $|N(\beta)/d| = |b| (1 - m)/4$. Thus, there exist $k, l \in \mathbb{Z}$ such that

\[
s_1 - t_1 = b \sigma_m (k + l \sigma_m)
\]

\[
= bk \sigma_m + bl \overline{\sigma}_m.
\]

\[
= bk \sigma_m + bl ( \sigma_m + \frac{m-1}{4} )
\]

\[
= bl ( \frac{m-1}{4} ) + (bk + bl) \sigma_m.
\]

Hence, $s_1 - t_1 = bl (m-1)/4$, and so, $b (m-1)/4 |(s_1 - t_1)$. It follows that $s_1 = t_1$ because
From all cases, we deduce that $s_1 = t_1$, because $0 \leq s_1, t_1 \leq |a| - 1$.

For the case $a \neq 0$ and $b \neq 0$, since $d = \gcd(a, b)$, there exist $a_0, b_0 \in \mathbb{Z}$ such that $a = da_0$, $b = db_0$, and $\gcd(a_0, b_0) = 1$. From $\beta(s_1 - t_1)$ in $O_K$, there exist $c_0, d_0 \in \mathbb{Z}$ such that

$$s_1 - t_1 = (a + b\sigma_m)(c_0 + d_0\sigma_m)$$

$$= d(a_0 + b_0\sigma_m)(c_0 + d_0\sigma_m)$$

$$= d\left[ a_0c_0 + b_0\frac{m-1}{4} + (a_0d_0 + b_0c_0 + d_0b_0)\sigma_m \right].$$

(17)

It follows that $d(a_0c_0 + b_0\sigma_m) c_0 + d_0\sigma_m)$ is, that is,

$$a_0d_0 = -b_0(c_0 + d_0).$$

(18)

Since $\gcd(a_0, b_0) = 1$, we have $a_0|c_0 + d_0$ and $b_0|d_0$. Thus, there exist $d_0, b'_0 \in \mathbb{Z}$ such that

$$c_0 + d_0 = a_0d_0'$$

and $b_0 = b_0d_0'$. Now, we have that

$$s_1 - t_1 = (a + b\sigma_m)(c_0 + d_0\sigma_m)$$

$$= (a + b\sigma_m)\left[ c_0 + d_0 - \frac{\sqrt{m}}{2}\right]$$

$$= (a + b\sigma_m)\left[ a_0d_0' - (b_0\sigma_m)\left( \frac{1 - \sqrt{m}}{2} \right) \right]$$

$$= (a + b\sigma_m)\left[ a_0d_0' - (b_0\sigma_m)\left( \frac{1 - \sqrt{m}}{2} \right) \right]$$

$$= (a + b\sigma_m)\left[ \frac{d_0b_0'}{4} \right]$$

$$= (a + b\sigma_m)\left[ \frac{a_0'}{d_0} \right]$$

$$= (\beta\overline{\beta})\frac{a_0'}{d_0}$$

$$= \frac{N(\beta)}{d} \cdot a_0'$$

(20)

so $|N(\beta)/d|(s_1 - t_1)$. Since $0 \leq s_1, t_1 \leq |N(\beta)/d| - 1$, it follows that $s_1 = t_1$.

From all cases, we deduce that $s_1 = t_1$, and so, $\alpha_1 = \alpha_2$, as desired.

Remark 1. Keeping the notation of Theorem 1 with $m < 0$, we have that

$$s_1 - t_1 \leq |N(\beta)/d| - 1.$$

(21)

Proof. To show that $\mathcal{C}' \subseteq \mathcal{C}$, we must show that

$$\max(|a|, |b|) \leq \frac{a^2 + ab + b^2 (1 - m)/4}{d} = \frac{N(\beta)}{d}.$$

(22)

It is easy to see that inequality (22) holds if $a = 0$ or $b = 0$. We now assume that $a \neq 0$ and $b \neq 0$. Note that $d \leq |a|, d \leq |b|$, and $a^2 - |a|b + b^2 \leq a^2 + ab + b^2$. Since $d$ (max $|a|, |b|$) $\leq |a|b$ and $(|a| - |b|)^2 \geq 0$, we have

$$d(\max(|a|, |b|)) \leq |a|b + (|a| - |b|)^2$$

$$= a^2 - |a|b + b^2$$

$$\leq a^2 + ab + b^2$$

(23)

$$\leq a^2 + ab + b^2 \left( \frac{1 - m}{4} \right),$$

and (22) is proved.

For a quadratic field $K = \mathbb{Q}(\sqrt{m})$, with $m \not\equiv 1 (\mod 4)$ and $\beta = a + b\sigma_m \in O_K\{0\}$, we recall that

$$\mathcal{C} = \left\{ x + y\sigma_m \mid x = 0, 1, \ldots, \frac{|N(\beta)|}{d} - 1, y = 0, 1, \ldots, d - 1 \right\}.$$

(24)

is a CRS($\beta$), where $d = \gcd(a, b)$. It is clear that

$$\max(|a|, |b|) \leq \frac{(\sqrt{a^2 + \sqrt{m}})^2}{d}$$

whenever $m < 0$. It follows that

$$\mathcal{C}' = \left\{ x + y\sigma_m \mid x = 0, 1, \ldots, \max(|a|, |b|) - 1 \right\}$$

$$- 1, y = 0, 1, \ldots, d - 1 \right\}.$$

(25)

From both cases, we observe that if $d = 1$, then $\mathcal{C}' = \{0, 1, \ldots, \max(|a|, |b|) - 1\}$, while if $b = 0$, then $\mathcal{C}' = \{x + y\sigma_m \mid x = 0, 1, \ldots, |a| - 1\}$.

We end this section by determining the so-called base $\beta(\mathcal{C}')$-representation.

Definition 1. Let $K = \mathbb{Q}(\sqrt{m})$ be an imaginary quadratic field. Let $\beta \in O_K\{0\}$ and $\mathcal{C}'$ be a CRS($\beta$). We say that $\eta \in O_K\{0\}$ has a base $\beta(\mathcal{C}')$-representation if

$$\eta = a_0\beta^0 + a_{n-1}\beta^{-1} + \cdots + a_1\beta + a_0,$$

(26)

for some $n \geq 1$, $a_i \in O_K\{0\}$, and $\eta \in \mathcal{C}' (i = 0, 1, \ldots, n - 1)$. If $a_i \in \mathcal{C}' (i = 0, 1, \ldots, n - 1)$, then (26) is called a base $\beta(\mathcal{C}')$-representation of $\eta$.

Example 1. Let $K = \mathbb{Q}(\sqrt{-2})$, $\beta = 3 + 2\sqrt{-2}$, and $\eta = -12 + 15\sqrt{-2}$. Then, $d = 1$ and $N(\beta) = 17$, and so,

$$\mathcal{C} = \{0, 1, \ldots, 16\}$$

(27)

is a CRS($\beta$). Since $\eta \in O_K$, there exists a unique $a_0 \in \mathcal{C}$ such that $\eta \equiv a_0 \pmod{\beta}$. We see that $a_0 = 1$ and
\[ \eta = 5\sqrt{-2}\beta + 1. \]  
(28)

Since \( 5\sqrt{-2} \in \mathbb{O}_K \), there exists a unique \( \alpha_1 \in \mathbb{O} \) such that \( 5\sqrt{-2} \equiv \alpha_1 (\text{mod}\beta) \). We see that \( \alpha_1 = 1 \) and

\[ 5\sqrt{-2} = (1 + \sqrt{-2})\beta + 1. \]  
(29)

It follows from (28) and (29) that

\[ \eta = (1 + \sqrt{-2})\beta^2 + \beta + 1. \]  
(30)

Since \( 1 + \sqrt{-2} \in \mathbb{O}_K \), there exists a unique \( \alpha_2 \in \mathbb{O} \) such that \( 1 + \sqrt{-2} \equiv \alpha_2 (\text{mod}\beta) \). We see that \( \alpha_2 = 8 \) and

\[ 1 + \sqrt{-2} = (-1 + \sqrt{-2})\beta + 8. \]  
(31)

It follows from (30) and (31) that

\[ \eta = (-1 + \sqrt{-2})\beta^3 + 8\beta^2 + \beta + 1. \]  
(32)

Since \( -1 + \sqrt{-2} \in \mathbb{O}_K \), there exists a unique \( \alpha_3 \in \mathbb{O} \) such that \( -1 + \sqrt{-2} \equiv \alpha_3 (\text{mod}\beta) \). We see that \( \alpha_3 = 6 \) and

\[ -1 + \sqrt{-2} = (-1 + \sqrt{-2})\beta + 6. \]  
(33)

It follows from (32) and (33) that

\[ \eta = (-1 + \sqrt{-2})\beta^4 + 6\beta^3 + 8\beta^2 + \beta + 1. \]  
(34)

Continuing the process, we conclude that \( \eta \) can be written as a base \( \beta(\mathbb{O}') \)-representation in infinite ways as (28), (30), and (32), and

\[ \eta = (-1 + \sqrt{-2})\beta^n + 6\beta^{n-1} + \cdots + 6\beta^3 + 8\beta^2 + \beta + 1, \]  
(35)

for all \( n \geq 4 \).

Since \( \mathbb{O}' = \{0, 1, 2\} \), we note that (28) and (30) are two base \( \beta(\mathbb{O}') \)-representations of \( \eta \).

Example 2. Let \( K = \mathbb{Q}(\sqrt{-3}), \) \( \beta = 7, \) and \( \eta = 4427 + 12504\sqrt{-3}. \) Then, \( d = 7 \) and \( N(\beta) = 49, \) and so,

\[ \mathbb{O}' = \{x + y\sqrt{-3} | x, y = 0, 1, 2, 3, 4, 5, 6\} = \mathbb{O}'. \]  
(36)

is a CRS (\( \beta \)). By using the process as in the previous example, we obtain that

\[ \eta = (632 + 1786\sqrt{-3})\beta + (3 + 2\sqrt{-3}), \]  
(37)

\[ \eta = (90 + 255\sqrt{-3})\beta^2 + (2 + \sqrt{-3})\beta + (3 + 2\sqrt{-3}), \]  
(38)

\[ \eta = (12 + 36\sqrt{-3})\beta^3 + (6 + 3\sqrt{-3})\beta^2 + (2 + \sqrt{-3})\beta + (3 + 2\sqrt{-3}), \]  
(39)

\[ \eta = (1 + 5\sqrt{-3})\beta^4 + (5 + \sqrt{-3})\beta^3 + (6 + 3\sqrt{-3})\beta^2 + (2 + \sqrt{-3})\beta + (3 + 2\sqrt{-3}). \]  
(40)

Since \( 1 + 5\sqrt{-3} \in \mathbb{O}', \) we get that the process stops, and

(37)-(40) are four base \( \beta(\mathbb{O}') \)-representations (base \( \beta(\mathbb{O}') \)-representations) of \( \eta \).

Example 3. Let \( K = \mathbb{Q}(\sqrt{-3}), \) \( \beta = 10 - 5\sigma_3, \) and \( \eta = 7184 - 4667\sigma_3. \) Then, \( d = 5 \) and \( N(\beta) = 75, \) and so,

\[ \mathbb{O}' = \{x + y\sigma_3 | x = 0, 1, \ldots, 14 \text{ and } y = 0, 1, 2, 3, 4\} \]  
(41)

is a CRS (\( \beta \)). By using the process as in the previous examples, we conclude that \( \eta \) can be written as a base \( \beta(\mathbb{O}') \)-representation in infinite ways as

\[ \eta = (790 - 144\sigma_3)\beta + (4 + 3\sigma_3), \]  
(42)

\[ \eta = (62 + 33\sigma_3)\beta^2 + (5 + \sigma_3)\beta + (4 + 3\sigma_3), \]  
(43)

\[ \eta = (2 + 8\sigma_3)\beta^3 + (2 + 3\sigma_3)\beta^2 + (5 + \sigma_3)\beta + (4 + 3\sigma_3), \]  
(44)

\[ \eta = -\beta^4 + (12 + 3\sigma_3)\beta^3 + (2 + 3\sigma_3)\beta^2 + (5 + \sigma_3)\beta + (4 + 3\sigma_3), \]  
(45)

\[ \eta = (-\sigma_3)\beta^5 + (4 + 5\sigma_3)\beta^4 + (12 + 3\sigma_3)\beta^3 + (2 + 3\sigma_3)\beta^2 + (5 + \sigma_3)\beta + (4 + 3\sigma_3), \]  
(46)

\[ \eta = (-\sigma_3)\beta^6 + (5 + 4\sigma_3)\beta^5 + \cdots + (5 + 4\sigma_3)\beta^2 + (5 + \sigma_3)\beta + (4 + 3\sigma_3), \]  
(47)

\[ (n \geq 6). \]

Since \( \mathbb{O}' = \{x + y\sigma_3 | x = 0, 1, \ldots, 9 \text{ and } y = 0, 1, 2, 3, 4\}, \) we note that (42)-(44) are three base \( \beta(\mathbb{O}') \)-representations of \( \eta \).

3. Irreducibility Criteria for Polynomials over Imaginary Quadratic Fields

We first recall the result in (iv) as in the following theorem [7].

Theorem 2. Let \( \beta \in \{2 \pm 2i, 1 \pm 3i, 3 \pm 3i \} \) or \( \beta = a + bi \in \mathbb{Z}[i] \) be such that \( |\beta| \geq 2 + \sqrt{2} \) and \( a \geq 1 \). For a Gaussian prime \( \pi, \)

\[ \pi = a_{\pi}\beta^0 + a_{\pi-1}\beta^{n-1} + \cdots + a_{i}\beta + a_0 = f(\beta) \]  
(46)

is its base \( \beta(\mathbb{O}') \)-representation with \( n \geq 1 \) and \( \text{Re}(a_{\pi}) \geq 1 \) satisfying the condition \( \text{Re}(a_{\pi}) \text{Im}(a_{\pi}) \geq \text{Re}(a_{\pi-1}) \text{Im}(a_{\pi-1}) \). then \( f(x) \) is irreducible in \( \mathbb{Z}[i][x]. \)

In this section, we establish a generalization of Theorem 2 for the ring of integers \( \mathbb{O}_K \) of any imaginary quadratic field. To prove this, we next recall the two essential lemmas from [7, 8] as follows.

Lemma 1. Let \( K = \mathbb{Q}(\sqrt{m}) \) be an imaginary quadratic field. If \( \beta \in \mathbb{O}_K \setminus \{0\}, \) then \( |\beta| \geq 1. \) We note for an imaginary quadratic field \( K \) that \( |a| = 1 \) for all \( a \in U(\mathbb{O}_K), \) the group of units in \( \mathbb{O}_K. \)

Lemma 2. Let \( f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{C}[x] \) be such that \( n \geq 2 \) and \( |a_1| \leq M(0 \leq i \leq n - 2) \) for some positive real number \( M. \) If \( f(x) \) satisfies
Lemma 3. Let $K = \mathbb{Q}(\sqrt{m})$ be an imaginary quadratic field, with $m \not\equiv 1 \pmod{4}$. Let $\beta = a + b\sqrt{m} \in O_K$ be such that $a \geq 1 + \sqrt{1-m}$, and let

$$M = \sqrt{\max\{|a|, |b|\} - 1}^2 - m(d-1)^2,$$

(47)

where $d = \gcd(a, b)$. Then, $\sqrt{1-m}(|\beta| - 1) \geq M$.

Proof. If $b = 0$, then $\beta = a$ and $d = a$. It follows that

$$\sqrt{1-m}(|\beta| - 1) = \sqrt{1-m}(|a| - 1) = \sqrt{(a-1)^2 - m(a-1)^2} = M.$$

(48)

Now, we assume that $b \neq 0$, so there are two possible cases.

Case 1. $a \geq |b|$. We have $a \geq 1 + \sqrt{1-m} > 2$ and $|b| \geq 1$. Since $d = \gcd(a, b)$, we obtain (1 - $m$)$(a-1)^2 - (1 - m)(m)(d-1)^2 + 2(1 - m)^2(-m) = [1 - m]$ $(a-1)|b| + [(1 - m)$ $(a-1)^2] |b|^2 > 0$, and so,

$$(1 - m)^2(a-1)^2 + 2(1 - m)^2(-m) = (a-1)|b| + [(1 - m)(a-1)^2] |b|^2$$

(49)

$$(1 - m)(a-1)^2 + (1 - m)(m)(d-1)^2 > 0.$$ 

It follows from (49) that

$$\sqrt{1-m}(|\beta| - 1) = \sqrt{1-m}(\sqrt{a^2 - mb^2} - 1)$$

(53)

$$> \sqrt{(a-1)^2 - m(d-1)^2} = M.$$ 

Case 2. $a < |b|$. Since $d = \gcd(a, b)$ and $a \geq 1 + \sqrt{1-m}$, we obtain that $|b| > 3$ and $(1 - m)(a-1)^2 - (1 - m)(m)(d-1)^2 + 2(1 - m)^2(-m) = [1 - m]$ $(d^2) > 0$. Hence,

$$(1 - m)^2(|b| - 1)^2 + 2(1 - m)^2(-m)a(|b| - 1)$$

(54)

$$+ [(1 - m)(a-1)^2] a^2 > (1 - m)(|b| - 1)^2 + (1 - m)(m)(d-1)^2.$$ 

It follows from (54) that

$$[(1 - m)(a-1)^2 + (1 - m)(|b| - 1) + (1 - m)(m)(a-1)^2]$$

$$= [(1 - m)(|b| - 1) + (1 - m)(m)a]$$

$$= (1 - m)^2(|b| - 1)^2 + 2(1 - m)^2(-m)a(|b| - 1)$$

$$+ [(1 - m(a-1)^2] a^2$$

(55)

$$> (1 - m)(|b| - 1)^2 + (1 - m)(m)(d-1)^2.$$ 

Hence,

$$
\begin{align*}
\text{(i) } & Re(a_n) \geq 1, \ Re(a_{n-1}) \geq 0, \text{ and } Im(a_{n-1}) \geq 0 \text{ and } \\
\text{(ii) } & Re(a_n)Im(a_n) \geq Re(a_{n-1})Im(a_{n-1}), \\
& \text{then any complex zero } \alpha \text{ of } f(x) \text{ satisfies either } \text{Re}(a) < 0 \text{ or } |a| < (1 + \sqrt{1 + 4M})/2.
\end{align*}
\]
Thus,
\[
(1 - m)(-m) + (1 - m)(|b| - 1) + (1 - m)(-m)(a - 1) > \sqrt{(1 - m)[(|b| - 1)^2 - m(d - 1)^2]},
\]
which implies that
\[
\Delta' = 2(1 - m)(-m) + 2(1 - m)(|b| - 1) + 2(1 - m)(-m)(a - 1) > 0.
\]
Let \(\delta' = (1 - m)(-m)(a - 1)^2 - (1 - m)(-m) - m(|b| - 1)^2 + m(d - 1)^2\).
We will show that \(\delta' > 0\), since \(d = \gcd(a, b)\), it follows that \((1 - m)(-m)(a - 1)^2 + m(d - 1)^2 = -m[(1 - m)(a - 1)^2 - (d - 1)^2] \geq 0\), since \(|b| > a \geq 1 + \sqrt{1 - m}\), we obtain that \(|(b - 1)^2 - 1 > m\), and so, \((-1 - m)(a - 1)^2 - (d - 1)^2 > 0\). Thus, \(\delta' > 0\), and so, \(\Delta' + \delta' > 0\), which implies that
\[
(1 - m)(a^2 - mb^2) = (1 - m)(|b|^2 + (-1 - m)|b|^2 + a^2) \geq (1 - m)(|b|^2 + (-1 - m)a^2 + a^2) = (1 - m)(|b|^2 - ma^2) \geq (|b| - 1)^2 - m(d - 1)^2 + 2(1 - m)[(|b| - 1)^2 - m(d - 1)^2] + (1 - m) = \left(\sqrt{|b| - 1)^2 - m(d - 1)^2 + \sqrt{1 - m}}\right)^2.
\]
Hence,
\[
\sqrt{1 - m}(|b| - 1) = \sqrt{1 - m}\left(\sqrt{a^2 - mb^2 - 1} \right) > \sqrt{|b - 1|^2 - m(d - 1)^2} = M,
\]
as desired.

**Lemma 4.** Let \(K = \mathbb{Q}(\sqrt{m})\) be an imaginary quadratic field, with \(m \neq 1 \pmod{4}\), and let \(\pi\) be an irreducible element in \(O_K\). Let \(\beta = a + b \sqrt{m} \in O_K\langle 0 \rangle\) be such that \(a \geq 1\), \(|\beta| \geq 1 + \sqrt{1 - m}\), \(|\pi| \geq |\beta|\), and
\[
\pi = \alpha_0 \beta^n + \alpha_{n-1} \beta^{n-1} + \ldots + \alpha_1 \beta + \alpha_0
\]
is a base \(\beta\)-representation, with \(\Re(\alpha_i) \geq 1\) satisfying condition (ii) of Lemma 2. If there exists \(\delta \in O_K\) such that \(\delta |\alpha_i|\) for all \(i = 0, 1, \ldots, n\), then \(\delta \in U(O_K)\).

**Proof.** If \(\alpha_0 = 0\), then \(\pi = \beta(\alpha_0 \beta^{n-1} + \ldots + \alpha_1)\). Hence, \(\alpha_0 \beta^{n-1} + \ldots + \alpha_1 \in U(O_K)\) because \(\beta \notin U(O_K)\langle |\beta| \neq 1\rangle\). Since \(\delta |\alpha_i|\) for all \(i = 0, 1, \ldots, n\), we have \(\delta(\alpha_0 \beta^{n-1} + \ldots + \alpha_1)\), and so, \(\delta \in U(O_K)\). Now, assume that \(\alpha_0 \neq 0\). We first show that \(|\delta| < |\pi|\). We treat two separate cases:

(i) Case 1: \(b \neq 0\). Since \(\delta |\alpha_0\), \(\alpha_0 \neq 0\), it follows from Lemma 1 that \(|\delta| < |\alpha_1|\). Note that \(d = \gcd(a, b)\) and \(a \geq 1\). Since \(a_0 \in \mathbb{C}^\prime\), we have that \(a_0 = x + y \sqrt{m}\), where \(0 \leq x \leq \max[|a|, |b|] - 1\) and \(0 \leq y \leq d - 1\). There are two further subcases:

1. Subcase 1: \(a > |b|\). Then, \(0 \leq x \leq a - 1\), and
\[
|\delta| \leq |\alpha_0| = \sqrt{x^2 - my^2} \leq \sqrt{(a - 1)^2 - m(d - 1)^2} \leq \sqrt{(a - 1)^2 - m(|b| - 1)^2} = \sqrt{a^2 - mb^2} - (2a - 1) + m(2b - 1) < \sqrt{a^2 - mb^2} = |\beta| < |\pi|.
\]

2. Subcase 2: \(a < |b|\). Then, \(0 \leq x \leq |b| - 1\), and
\[
|\delta| \leq |\alpha_0| = \sqrt{x^2 - my^2} \leq \sqrt{(|b| - 1)^2 - m(d - 1)^2} \leq \sqrt{(|b| - 1)^2 - m(a - 1)^2} = \sqrt{b^2 - ma^2} - (2b - 1) + m(2a - 1) < \sqrt{b^2 - ma^2} \leq \sqrt{a^2 - mb^2} = |\beta| < |\pi|.
\]

(ii) Case 2: \(b = 0\). Then, \(\beta = a\) and \(d = a\). Since \(a = \sqrt{a} \geq 1 + \sqrt{1 - m}\), we have \(a \geq 3\). We consider two further subcases:

1. Subcase 1: \(n = 1\). Then, \(\pi = \alpha_1 a + \alpha_0\). Let \(\alpha_1 = x_1 + y_1 \sqrt{m} \in O_K\langle 0 \rangle\) and \(\alpha_0 = x_0 + y_0 \sqrt{m} \in \mathbb{C}^\prime\), that is, \(0 \leq x_0, y_1 \leq a - 1\). Now, we obtain that
\[
\pi = (x_1 + y_1 \sqrt{m})a + (x_0 + y_0 \sqrt{m}) = (ax_1 + x_0) + (ay_1 + y_0) \sqrt{m}.
\]
By the assumption, we have that \(x_1 \geq 1\) and \(x_0, y_1 \geq x_1, y_1\). If \(x_0 = 0\), then \(y_0 = 0\), which is impossible because \(\alpha_0 \neq 0\). Thus, \(x_0 > 0\), and so, \(y_1 \geq 1\). Hence,
\[
|\pi| = \sqrt{(ax_1 + x_0)^2 - m(ay_1 + y_0)^2} > \sqrt{(ax_1)^2 - m(ay_1)^2} = |\alpha_1| > |\alpha_1| < |\beta|.
\]

2. Subcase 2: \(n \geq 2\). Then, \(\pi = \alpha_0 \alpha_n + \ldots + \alpha_1 + \alpha_0\), where \(\alpha_i \in O_K\langle 0 \rangle\) and \(\alpha_i \in \mathbb{C}^\prime\) for all \(i = 0, 1, \ldots, n - 1\). Let \(\alpha_i = x_i + y_i \sqrt{m}\) for all \(i = 0, 1, \ldots, n\). Thus,
\[ \pi = (x_n a^n + \cdots + x_1 a + x_0) + (y_n a^n + \cdots + y_1 a + y_0) \sqrt{m}. \]  

(65)

Note that \( x_n \geq 1 \) and \( 0 \leq x_i, y_i \leq a - 1 \) for all \( i = 0, 1, \ldots, n - 1 \).

If \( y_n \geq 0 \), then
\[ |\pi| = \sqrt{(x_n a^n + \cdots + x_1 a + x_0)^2 - m(y_n a^n + \cdots + y_1 a + y_0)^2} \]
\[ \geq \sqrt{x_n^2 - my_n^2} \geq |\alpha| \geq \delta. \]  

(66)

If \( y_n < 0 \), then by the property of a base \( a \)-representation of any positive integer, we must have
\[ 0 \leq y_0 + y_1 a + \cdots + y_{n-1} a^{n-1} < a^n \leq -y_n a^n. \]

Hence, \( y_0 + y_1 a + \cdots + y_{n-1} a^{n-1} < 0 \) so that
\[ (y_n a^n + \cdots + y_1 a + y_0)^2 \geq 1. \]  

(67)

Since \( a = |\beta| \geq 1 + \sqrt{1 - m} \), we have \( (a - 1)^2 \geq 1 - m \), and so,
\[ a^4 - m > a^4 > (a - 1)^4 \geq (1 - m)(a - 1)^2. \]  

(68)

It follows from (67) and (68), \( x_n \geq 1 \), and \( n \geq 2 \) that
\[ |\pi| = \sqrt{(x_n a^n + \cdots + x_1 a + x_0)^2 - m(y_n a^n + \cdots + y_1 a + y_0)^2} \]
\[ \geq \sqrt{a^4 - m} \]
\[ \geq \sqrt{(1 - m)(a - 1)^2} \]
\[ = \sqrt{(a - 1)^2 - m(a - 1)^2} \]
\[ \geq \sqrt{x_n^2 - my_n^2} = |\alpha| \geq \delta. \]  

(69)

From all cases, we now have that \( |\delta| < |\pi| \), as required.

As \( \delta \sigma_i \), for all \( i = 0, 1, \ldots, n \), we have \( |\delta| \pi \), and so, \( \pi = \delta \gamma \) for some \( \gamma \in \mathbb{Q} \).

Since \( \pi \) is an irreducible element in \( \mathbb{Q} \), either \( \delta \) or \( \gamma \) is a unit. If \( \delta \) is not a unit, then \( |\gamma| = 1 \), and hence, \( |\pi| = |\delta| \gamma = |\delta| < |\pi| \), which is a contradiction. This proves the lemma.

By applying Lemmas 2–4, we obtain an irreducibility criterion for the case \( m \neq 1 \) (mod 4) as in the following theorem.

**Theorem 3.** Let \( K = \mathbb{Q}(\sqrt{m}) \) be an imaginary quadratic field, with \( m \neq 1 \) (mod 4). Let \( \beta = a + b \sqrt{m} \in \mathbb{Q} \) be such that \( |\beta| \geq 2 + \sqrt{1 - m} \) and \( a \geq 1 + \sqrt{1 - m} \). For an irreducible element \( \pi \) in \( \mathbb{O}_K \), with \( |\pi| \geq |\beta| \), if
\[ \pi = a_0 \beta^n + a_{n-1} \beta^{n-1} + \cdots + a_1 \beta + a_0 = f(\beta) \]  

(70)

is a base \( \beta \)-representation with \( \text{Re}(a_n) \geq 1 \) satisfying condition (ii) of Lemma 2, then \( f(\beta) \) is irreducible in \( \mathbb{O}_K \).

**Proof.** If \( f(x) = 1 \), then \( f(x) = a_1 x + a_0 \) is irreducible in \( \mathbb{O}_K[x] \) by using Lemma 4. We now suppose that \( \text{deg} f(x) = 2 \) and \( f(x) \) is reducible in \( \mathbb{O}_K[x] \).

4 implies that \( f(x) = g(x) h(x) \) for some positive-degree polynomials \( g(x) \) and \( h(x) \) in \( \mathbb{O}_K[x] \) so that \( \pi = f(\beta) = g(\beta) h(\beta) \).

Since \( \pi \) is an irreducible element, either \( g(\beta) \) or \( h(\beta) \) is a unit, and so, either \( |g(\beta)| = 1 \) or \( |h(\beta)| = 1 \). Without loss of generality, we may assume that \( |g(\beta)| = 1 \). Since \( a_i \in \mathbb{O} \) for all \( i \in \{0, 1, \ldots, n-1\} \), we have that \( |a_i| \leq M \) for all \( i \in \{0, 1, \ldots, n-1\} \), where \( M \) is defined as in Lemma 3. Since \( |\beta| \geq 2 + \sqrt{1 - m} \), we have that \( 4(|\beta| - 1) \geq 0 \), and so, \( (2|\beta| - 3)^2 \geq 4 \sqrt{1 - m} |\beta| - 1 \). It follows from Lemma 3 that
\[ |\beta| \geq \frac{3 + \sqrt{1 + 4 \sqrt{1 - m}(|\beta| - 1)}}{2} \geq 1 + \sqrt{1 + 4 \sqrt{1 - m}(|\beta| - 1)} \]  

(71)

so
\[ |\beta| - \frac{1 + \sqrt{1 + 4 \sqrt{1 - m}(|\beta| - 1)}}{2} \geq 1. \]  

(72)

Since \( \text{deg} g(\beta) \geq 1 \), \( g(x) \) can be expressed in the form
\[ g(x) = \varepsilon \prod_i (x - \gamma_i), \]  

(73)

where \( \varepsilon \in \mathbb{O}_K \) is the leading coefficient of \( g(x) \) and the product is over the set of complex zeros of \( g(x) \). It follows from Lemma 2 that any zero \( \gamma \) of \( g(x) \) satisfies either \( \text{Re}(\gamma) < 0 \) or
\[ |\gamma| < \frac{1 + \sqrt{1 + 4 \sqrt{1 - m}(|\beta| - 1)}}{2}. \]  

(74)

If \( \text{Re}(\gamma) < 0 \), then \( |\beta - \gamma| \geq \text{Re}(\beta - \gamma) = \text{Re}(\beta) - \text{Re}(\gamma) = a - \text{Re}(\gamma) > 1 \). In the latter case, we obtain by (72) and (74) that
\[ |\beta - \gamma| > |\beta| - |\gamma| \geq |\beta| - \frac{1 + \sqrt{1 + 4 \sqrt{1 - m}(|\beta| - 1)}}{2} \geq 1. \]  

(75)

From both cases, we deduce by Lemma 1 that
\[ 1 = |g(\beta)| = |\varepsilon| \prod_i |\beta - \gamma_i| \geq \prod_i |\beta - \gamma_i| > 1, \]  

(76)

which is a contradiction. This completes the proof.

We note that the condition \( a - 1 + \sqrt{1 - m} \) in Theorem 3 can be replaced by \( a \geq 1 \) for the case of Gaussian integers. Moreover, it is known that an irreducible element is a prime element (Gaussian prime) in \( \mathbb{Z}[i] \). Therefore, Theorem 3 is a generalization of Theorem 2.

By applying Theorem 3, we can find an irreducible polynomial in \( \mathbb{O}_K[x] \) as in the following example.

**Example 4.** Let \( K = \mathbb{Q}(\sqrt{-5}) \) and \( \beta = 7 \in \mathbb{O}_K \). Then, \( \mathbb{O} = \{x + y \sqrt{-5} \mid x, y = 0, 1, 2, 3, 4, 5, 6\} \). Note that \( |\beta| = \sqrt{7 + \sqrt{6}} \) and \( a = 7 > 1 + \sqrt{6} \). Let \( \pi = 4427 + 12504 \sqrt{-5} \in \mathbb{O}_K \). Clearly, \( |\pi| \geq |\beta| \). Since \( N(\pi) = 4427^2 + 5(12504) = 801348409 \) which is a rational prime, we deduce that \( \pi \) is an irreducible element. By Example 2, we have that \( |\beta| = 7 \Rightarrow 7 + \sqrt{6} = (1 + 5 \sqrt{7})^2 + (5 + 3 \sqrt{7})^2 + (2 + 3 \sqrt{7})^2 + (3 + 2 \sqrt{7})^2 \) is its base \( \beta \)-representation and \( \text{Re}(a_n) = 1 \geq 1 \) satisfying condition (ii) of Lemma 2, i.e.,
is irreducible in $O_K[x]$.

\[ M = \sqrt{(\max\{a,|b|\} - 1)^2 + (\max\{a,|b|\} - 1)(d - 1) + (d - 1)^2\left(\frac{1 - m}{4}\right)}, \]  

(78)

where $d = \gcd(a,b)$. Then, $\sqrt{(9 - m)/4(\beta - 1)} \geq M$.

**Proof.** We first prove the following:

\[ \left(\frac{9 - m}{4}\right)\left[a^2 - a|b| + b^2\left(\frac{1 - m}{4}\right)\right] \geq \left(\sqrt{(\max\{a,|b|\} - 1)^2 + (\max\{a,|b|\} - 1)(d - 1) + (d - 1)^2\left(\frac{1 - m}{4}\right)}\right)^2 + \frac{9 - m}{4}. \]  

(79)

Proof of the claim: If $b = 0$, then we are done. Now, assume that $|b| \geq 1$, and we treat two separate cases:

(i) **Case 1:** $a \geq |b|$. Since $(m^2 - 6m - 11)(|b| - 1)^2/16 - (1 - m)(d - 1)^2/4 \geq 0$ and

\[ \Delta := \left(\frac{m^2 - 6m - 11}{16}\right)(|b| - 1)^2 - (d - 1)^2\left(\frac{1 - m}{4}\right) \]  

(80)

\[ + \left(\frac{1 - m}{4}\right)(a - 1)(|b| - 1) - (a - 1)(d - 1) + \frac{m^2 - 6m - 27}{16} \geq 0. \]

Now, we let

\[ \delta := \left(\frac{5 - m}{4}\right)(a - |b|)^2 + \left(\frac{9 - m}{4}\right)(a - 1) + \left(\frac{m^2 - 8m - 9}{8}\right)(|b| - 1) \]  

(81)

\[ - 2\left(\frac{9 - m}{4}\right)\left[(a - 1)^2 + (a - 1)(d - 1) + (d - 1)^2\left(\frac{1 - m}{4}\right)\right]. \]
and we show that $\delta \geq 0$. Since $m \equiv 1 \pmod{4}$ and $m < 0$, we consider two separate cases, that is, $m = -3$ and $m \leq -7$.

If $m = -3$, then

$$
\left[ \frac{5 - m}{4} (a - |b|)^2 + \frac{9 - m}{4} (a - 1) + \frac{m^2 - 8m - 9}{8} (|b| - 1) \right]^2
$$

$$
= \left[ 2 (a - |b|)^2 + 3 (a - 1) + 3 (|b| - 1) \right]^2
$$

$$
= 4 (a - |b|)^4 + 9 (a - 1)^2 + 9 (|b| - 1)^2 + 12 (a - |b|)^2 (a - 1)
+ 18 (a - 1) (|b| - 1) + 12 (a - |b|)^2 (|b| - 1)

= 4 (a - |b|)^4 + 3 \left[ (a - 1)^2 - 2 (a - 1) (|b| - 1) + (|b| - 1)^2 \right]
+ 12 (a - 1)^2 + 12 (|b| - 1)^2 + 12 (a - 1) (|b| - 1)
+ 12 (a - |b|)^2 (a - 1) + 12 (a - |b|)^2 (|b| - 1)

= 4 (a - |b|)^4 - 3 (a - |b|)^2
+ 12 (a - 1)^2 + 12 (|b| - 1)^2 + 12 (a - 1) (|b| - 1)
+ 12 (a - |b|)^2 (a - 1) + 12 (a - |b|)^2 (|b| - 1)

\geq 12 (a - 1)^2 + 12 (a - 1) (|b| - 1) + 12 (|b| - 1)^2
\geq 12 (a - 1)^2 + 12 (a - 1) (d - 1) + 12 (d - 1)^2

= (9 - m) (a - 1)^2 + (9 - m) (a - 1) (d - 1) + (9 - m) (d - 1)^2 \left( \frac{1 - m}{4} \right)

= (9 - m) \left[ (a - 1)^2 + (a - 1) (d - 1) + (d - 1)^2 \left( \frac{1 - m}{4} \right) \right].

For \( m \leq -7 \), we see that \( \lfloor (9 - m)/4 \rfloor \geq 9 - m \),
\( 2 \lfloor (9 - m)/4 \rfloor \lfloor m^2 - 8m - 9 \rfloor /8 > 9 - m \),
and \( \lfloor m^2 - 8m - 9 \rfloor /8 > (9 - m)(1 - m)/4 \). Thus,

\[
\left[ \frac{5 - m}{4} \right] (a - |b|)^2 + \left( \frac{9 - m}{4} \right) (a - 1) + \left( \frac{m^2 - 8m - 9}{8} \right) (|b| - 1)^2 \geq (9 - m)(a - 1)^2 + (9 - m)(a - 1)(|b| - 1) + (9 - m)(|b| - 1)^2 \left( \frac{1 - m}{4} \right) \]

It follows from both cases that

\[
\left( \frac{5 - m}{4} \right) (a - |b|)^2 + \left( \frac{9 - m}{4} \right) (a - 1) + \left( \frac{m^2 - 8m - 9}{8} \right) (|b| - 1) \geq 0. \]

which implies that

\[
\delta = \left( \frac{5 - m}{4} \right) (a - |b|)^2 + \left( \frac{9 - m}{4} \right) (a - 1) + \left( \frac{m^2 - 8m - 9}{8} \right) (|b| - 1) - 2 \sqrt{\left( \frac{9 - m}{4} \right) (a - 1)^2 + (a - 1) (d - 1) + (d - 1)^2 \left( \frac{1 - m}{4} \right) } \geq 0. \]
Hence, \(\Delta + \delta \geq 0\), which implies that

\[
\begin{align*}
(a - 1)^2 &+ \left(\frac{m^2 - 6m - 11}{16}\right)(|b| - 1)^2 + \left(\frac{1 - m}{4}\right)(a - 1)(|b| - 1) \\
+ &\left(\frac{5 - m}{4}\right)(a - |b|)^2 + \left(\frac{9 - m}{4}\right)(a - 1) + \left(\frac{m^2 - 8m - 9}{8}\right)(|b| - 1) \\
+ &\left(\frac{m^2 - 6m - 27}{16}\right) + \frac{9 - m}{4} \geq (a - 1)^2 + (a - 1)(d - 1) + (d - 1)^2 \left(\frac{1 - m}{4}\right) \\
+ &2\sqrt{\left(\frac{9 - m}{4}\right)} \left[(a - 1)^2 + (a - 1)(d - 1) + (d - 1)^2 \left(\frac{1 - m}{4}\right) + \frac{9 - m}{4}\right].
\end{align*}
\] (86)

Thus,

\[
\begin{align*}
\left(\frac{9 - m}{4}\right) \left[a^2 - a|b| + b^2 \left(\frac{1 - m}{4}\right)\right] \\
\geq \left(\sqrt{(a - 1)^2 + (a - 1)(d - 1) + (d - 1)^2 \left(\frac{1 - m}{4}\right) + \frac{9 - m}{4}}\right)^2.
\end{align*}
\] (87)

(ii) Case 2: \(a < |b|\). Since

\[
(m^2 - 6m - 11)(a - 1)^2/16 - (1 - m)(d - 1)^2/4 \geq 0
\]

and \((1 - m)(a - 1)(|b| - 1)/4 - (|b| - 1)(d - 1)/2 \geq 0\),

it follows that

\[
\Delta' = \left(\frac{m^2 - 6m - 11}{16}\right)(a - 1)^2 - (d - 1)^2 \left(\frac{1 - m}{4}\right) + \left(\frac{1 - m}{4}\right)(a - 1)(|b| - 1)
\] - \((|b| - 1)(d - 1) + \frac{m^2 - 6m - 27}{16} \geq 0.
\] (88)

We now let

\[
\delta' = \left(\frac{5 - m}{4}\right)(|b| - a)^2 + \left(\frac{9 - m}{4}\right)(|b| - 1) + \left(\frac{m^2 - 8m - 9}{8}\right)(a - 1)
\] - 2\sqrt{\left(\frac{9 - m}{4}\right)} \left[(|b| - 1)^2 + (|b| - 1)(d - 1) + (d - 1)^2 \left(\frac{1 - m}{4}\right)\right].
\] (89)
and we show that $\delta' > 0$. If $m = -3$, then

\[
\left[ \frac{5 - m}{4} (|b| - a)^2 + \left( \frac{9 - m}{4} \right) (|b| - 1) + \left( \frac{m^2 - 8m - 9}{8} \right) (a - 1) \right]^2 \\
= \left[ 2 (|b| - a)^2 + 3 (|b| - 1) + 3 (a - 1) \right]^2 \\
= \left[ 2 (|b| - a)^2 + 3 (a - 1) + 3 (|b| - 1) \right]^2 \\
= 4 (|b| - a)^4 + 9 (a - 1)^2 + 9 (|b| - 1)^2 \\
+ 12 (|b| - a)^2 (a - 1) + 18 (a - 1) (|b| - 1) \\
+ 12 (|b| - a)^2 (|b| - 1) \\
= 4 (|b| - a)^4 - 3 \left[ (a - 1)^2 - 2 (a - 1) (|b| - 1) + (|b| - 1)^2 \right] \\
+ 12 (a - 1)^2 + 12 (|b| - 1)^2 + 12 (a - 1) (|b| - 1) \\
+ 12 (|b| - a)^2 (a - 1) + 12 (|b| - a)^2 (|b| - 1) \\
= 4 (|b| - a)^4 - 3 (|b| - a)^2 + 12 (a - 1)^2 + 12 (|b| - 1)^2 \\
+ 12 (a - 1) (|b| - 1) + 12 (|b| - a)^2 (a - 1) + 12 (|b| - a)^2 (|b| - 1) \\
> 12 (|b| - 1)^2 + 12 (|b| - 1) (a - 1) + 12 (a - 1)^2 \geq 12 (|b| - 1)^2 \\
+ 12 (|b| - 1) (d - 1) + 12 (d - 1)^2 = (9 - m) (|b| - 1)^2 \\
+ (9 - m) (|b| - 1) (d - 1) + (9 - m) (d - 1)^2 \left( \frac{1 - m}{4} \right) \\
= (9 - m) \left[ (|b| - 1)^2 + (|b| - 1) (d - 1) + (d - 1)^2 \left( \frac{1 - m}{4} \right) \right].
\]
For $m \leq -7$, we see that $\lfloor (9 - m)/4 \rfloor^2 \geq 9 - m$, $2[(9 - m)/4][(m^2 - 8m - 9)/8] > 9 - m$, and $[(m^2 - 8m - 9)/8]^2 > (9 - m)(1 - m)/4$. Thus,

\[
\left[ \frac{5 - m}{4} (|b| - a)^2 + \frac{9 - m}{4} (|b| - 1) + \frac{m^2 - 8m - 9}{8} (a - 1) \right]^2
\]

\[
= \left( \frac{5 - m}{4} \right)^2 (|b| - a)^4 + \frac{9 - m}{4} \left( |b| - 1 \right)^2 + \frac{m^2 - 8m - 9}{8} (a - 1)^2
\]

\[
+ 2 \left( \frac{5 - m}{4} \right) \left( \frac{9 - m}{4} \right) (|b| - a)^2 (|b| - 1)
\]

\[
+ 2 \left( \frac{9 - m}{4} \right) \left( \frac{m^2 - 8m - 9}{8} \right) (a - 1)(|b| - 1)
\]

\[
+ 2 \left( \frac{5 - m}{4} \right) \left( \frac{m^2 - 8m - 9}{8} \right) (|b| - a)^2 (a - 1)
\]

\[
> (9 - m)(|b| - 1)^2 + (9 - m)(a - 1)(|b| - 1) + (9 - m)(a - 1)^2 \left( \frac{1 - m}{4} \right)
\]

\[
\geq (9 - m)(|b| - 1)^2 + (9 - m)(|b| - 1)(d - 1) + (9 - m)(d - 1)^2 \left( \frac{1 - m}{4} \right)
\]

\[
= (9 - m) \left[ (|b| - 1)^2 + (|b| - 1)(d - 1) + (d - 1)^2 \left( \frac{1 - m}{4} \right) \right].
\]

It follows from both cases that

\[
\left( \frac{5 - m}{4} \right) (|b| - a)^2 + \frac{9 - m}{4} (|b| - 1) + \frac{m^2 - 8m - 9}{8} (a - 1)
\]

\[
> 2 \sqrt{\frac{9 - m}{4}} \left[ (|b| - 1)^2 + (|b| - 1)(d - 1) + (d - 1)^2 \left( \frac{1 - m}{4} \right) \right],
\]

so

\[
\delta = \left( \frac{5 - m}{4} \right) (|b| - a)^2 + \frac{9 - m}{4} (|b| - 1) + \frac{m^2 - 8m - 9}{8} (a - 1)
\]

\[
- 2 \sqrt{\frac{9 - m}{4}} \left[ (|b| - 1)^2 + (|b| - 1)(d - 1) + (d - 1)^2 \left( \frac{1 - m}{4} \right) \right] > 0.
\]

\[
\text{International Journal of Mathematics and Mathematical Sciences}
\]
Hence, $\Delta' + \delta' > 0$, which implies that

\[
(b-1)^2 + \left( \frac{m^2 - 6m - 11}{16} \right) (a-1)^2 + \left( \frac{1-m}{4} \right) (a-1)(b-1) + \left( \frac{5-m}{4} \right) (b-a)^2
\]

\[
+ \left( \frac{9-m}{4} \right) (b-1) + \left( \frac{m^2 - 8m - 9}{8} \right) (a-1) + \frac{m^2 - 6m - 27}{16} + \frac{9-m}{4}
\]

\[
> (b-1)^2 + (b-1)(d-1) + (d-1)^2 \left( \frac{1-m}{4} \right)
\]

\[
+ 2 \sqrt{\left( \frac{9-m}{4} \right) \left[ (b-1)^2 + (b-1)(d-1) + (d-1)^2 \left( \frac{1-m}{4} \right) \right]} + \frac{9-m}{4},
\]

and so,

\[
\left( \frac{9-m}{4} \right) \left[ b^2 - a|b| + a^2 \left( \frac{1-m}{4} \right) \right]
\]

\[
> \left( \sqrt{(b-1)^2 + (b-1)(d-1) + (d-1)^2 \left( \frac{1-m}{4} \right) + \frac{9-m}{4}} \right)^2.
\]

Because of $b^2 - a^2 < ((b^2 - a^2)(1-m)/4)$ and (95), we have

\[
\left( \frac{9-m}{4} \right) \left[ a^2 - a|b| + b^2 \left( \frac{1-m}{4} \right) \right]
\]

\[
> \left( \sqrt{(b-1)^2 + (b-1)(d-1) + (d-1)^2 \left( \frac{1-m}{4} \right) + \frac{9-m}{4}} \right)^2,
\]

which proves the Claim. Since

\[
a^2 + ab + b^2 \left( (1-m)/4 \right) \geq a^2 - a|b| + b^2 \left( (1-m)/4 \right),
\]

it follows from the Claim that

\[
\sqrt{\frac{9-m}{4}} (|b| - 1) \geq \sqrt{\frac{9-m}{4}} \left( \sqrt{a^2 + ab + b^2 \left( \frac{1-m}{4} \right)} - 1 \right)
\]

\[
\geq \sqrt{\frac{9-m}{4}} \left( \sqrt{a^2 - a|b| + b^2 \left( \frac{1-m}{4} \right)} - 1 \right)
\]

\[
\geq \sqrt{\left( \max\{a,|b|\} - 1 \right)^2 + (\max\{a,|b|\} - 1)(d-1) + (d-1)^2 \left( \frac{1-m}{4} \right)} = M,
\]
as desired.

**Lemma 6.** Let $K = \mathbb{Q}(\sqrt{m})$ be an imaginary quadratic field, with $m \equiv 1 \pmod{4}$, and let $\pi$ be an irreducible element in $\mathcal{O}_K$. Let $\beta = a + b\sigma_m \in \mathcal{O}_K \setminus \{0\}$ be such that $a \geq 1$, $|\beta| \geq 2 + \sqrt{(9 - m)/4}$, $|\pi| > \sqrt{(9 - m)/4}(|\beta| - 1)$, and

$$\pi = a_0\beta^n + a_{n-1}\beta^{n-1} + \cdots + a_1\beta + a_0$$

(98)

is a base $\beta(\mathcal{O}')$-representation, with $\text{Re}(\alpha_i) \geq 1$ satisfying condition (ii) of Lemma 2. If there exists $\delta \in \mathcal{O}_K$ such that $\delta|\alpha_i$ for all $i = 0, 1, \ldots, n$, then $\delta \in \mathcal{O}_K$.

**Proof.** If $\alpha_0 = 0$, then $\pi = \beta(a_0\beta^{n-1} + \cdots + a_1)$. Since $\pi$ is an irreducible element, we have $a_0\beta^{n-1} + \cdots + a_1 \in \mathcal{O}_K$, because $\beta \notin \mathcal{O}_K$. Hence, $\delta|\alpha_i$ for all $i = 0, 1, \ldots, n$, it follows that $\delta|\alpha_i$, and so, $\delta \in \mathcal{O}_K$. Now, assume that $\alpha_0 \neq 0$. Let $M$ be as in Lemma 5. Since $\alpha_i \in \mathcal{O}_K$ for all $i = 0, 1, \ldots, n-1$, we obtain that $|a_i| \leq M$ for all $i = 0, 1, \ldots, n-1$. Since $|\delta| \neq 0$, we get

$$|\delta| \leq |\alpha_0| \leq M \leq \frac{9 - m}{4}(|\beta| - 1)$$

by using Lemmas 1 and 5. Since $|\delta|$, it follows that $\pi = \delta y$ for some $y \in \mathcal{O}_K$. As $\pi = \delta y$ is an irreducible element in $\mathcal{O}_K$, either $\delta \in \mathcal{O}_K$ or $y \in \mathcal{O}_K$. If $\delta \notin \mathcal{O}_K$, then $y \in \mathcal{O}_K$, and so, $|y| = 1$. Hence,

$$|\pi| = |\delta||y| = |\delta| < |\pi|,$$

which is a contradiction. Thus, $\delta \in \mathcal{O}_K$, as desired.

By applying Lemmas 5 and 6, we obtain an irreducibility criterion for the case $m \equiv 1 \pmod{4}$ as in the following theorem.

**Theorem 4.** Let $K = \mathbb{Q}(\sqrt{m})$ be an imaginary quadratic field, with $m \equiv 1 \pmod{4}$. Let $\beta = a + b\sigma_m \in \mathcal{O}_K$ be such that $|\beta| \geq 2 + \sqrt{(9 - m)/4}$, $a \geq 1$, and $a + (b/2) \geq 1$. For an irreducible element $\pi$ in $\mathcal{O}_K$ such that $|\pi| > \sqrt{(9 - m)/4}(|\beta| - 1)$, if

$$\pi = a_0\beta^n + a_{n-1}\beta^{n-1} + \cdots + a_1\beta + a_0 = f(\beta)$$

(101)

is a base $\beta(\mathcal{O}')$-representation with $\text{Re}(\alpha_i) \geq 1$ satisfying condition (ii) of Lemma 2, then $f(x)$ is irreducible in $\mathcal{O}_K[x]$.

**Proof.** If $\deg f(x) = 1$, then $f(x)$ is irreducible in $\mathcal{O}_K[x]$ by using Lemma 6. Now, we suppose that $\deg f(x) \geq 2$ and $f(x)$ is reducible in $\mathcal{O}_K[x]$. Again, Lemma 6 implies that $f(x) = g(x)h(x)$ for some positive-degree polynomials $g(x)$ and $h(x)$ in $\mathcal{O}_K[x]$, and so, $\pi = f(\beta) = g(\beta)h(\beta)$. Since $\pi$ is an irreducible element, either $g(\beta)$ or $h(\beta)$ is a unit so that either $|g(\beta)| = 1$ or $|h(\beta)| = 1$. Without loss of generality, we may assume that $|g(\beta)| = 1$. Since $\alpha_i \in \mathcal{O}_K'$ for all $i = 0, 1, \ldots, n-1$, we have that $|a_i| \leq M$ for all $i = 0, 1, \ldots, n-1$, where $M$ is defined as in Lemma 5. Since $|\beta| > 2 + \sqrt{(9 - m)/4}$, we obtain that $4(|\beta| - 1)|\beta| > 2 + \sqrt{(9 - m)/4}$, so that

$$2|\beta| - 3|\beta| \geq 2 + \sqrt{(9 - m)/4}(|\beta| - 1).$$

It follows from Lemma 5 that

$$|\beta| \geq \frac{3 + \sqrt{1 + 4\sqrt{(9 - m)/4}(|\beta| - 1)}}{2} \geq \frac{3 + \sqrt{1 + 4M}}{2}.$$  

(102)

This shows that

$$|\beta| - \frac{1 + \sqrt{1 + 4M}}{2} \geq 1.$$  

(103)

Since $\deg g(x) \geq 1$, $g(x)$ can be expressed in the form

$$g(x) = \varepsilon \prod_{i=1}^{\ell} (x - y_i),$$

(104)

where $\varepsilon \in \mathcal{O}_K$ is the leading coefficient of $g(x)$ and the product is over the set of complex zeros of $g(x)$. It follows from Lemma 2 that any zero $\gamma$ of $g(x)$ satisfies either $\text{Re}(\gamma) < 0$ or

$$|\gamma| < \frac{1 + \sqrt{1 + 4M}}{2}.$$  

(105)

If $\text{Re}(\gamma) < 0$, then $|\beta - \gamma| \geq \text{Re}(\beta - \gamma) = \text{Re}(\beta) - \text{Re}(\gamma) = (a + (b/2)) - \text{Re}(\gamma) > 1$. In another case, we get by (103) and (105) that

$$|\beta - \gamma| \geq |\beta| - |\gamma| \geq |\beta| - \frac{1 + \sqrt{1 + 4M}}{2} \geq 1.$$  

(106)

From both cases, we deduce by Lemma 1 that

$$1 = |g(\beta)| = |\varepsilon| \prod_{i=1}^{\ell} |\beta - y_i| \geq \prod_{i=1}^{\ell} |\beta - y_i| > 1,$$

(107)

which is a contradiction. This completes the proof.

By applying Theorem 4, we can find an irreducible polynomial in $\mathcal{O}_K[x]$ as in the following example.

**Example 5.** Let $K = \mathbb{Q}(\sqrt{-3})$ and $\beta = 10 - 5\sigma_3 \in \mathcal{O}_K$. Then, $\mathcal{O}' = \{x + y\sigma_3 | x, y \in \mathbb{Z}, 0 \leq y \leq 3\}$. Note that $|\beta| = 5\sqrt{3} \geq 2 + \sqrt{3}$, $a + (b/2) = 10 - (5/2) \geq 1$, and $a = 10 \geq 1$. Let $\pi = 7184 - 4667\sigma_3 \in \mathcal{O}_K$. We see that $|\pi| = \sqrt{39863017} = 6313.72 > \sqrt{3(5\sqrt{3} - 1)} = \sqrt{3(|\beta| - 1)}$. Since $N(\pi) = 7184^2 - 7184 \cdot 4667 + 4667^2 = 39863017$ is a rational prime, we deduce that $\pi$ is an irreducible element. By Example 3, we have that $\pi = (2 + 8\sigma_3)\beta^3 + (2 + 3\sigma_3)\beta^2 + (5 + \sigma_3)\beta + (4 + 3\sigma_3)$ is its base $\beta(\mathcal{O}')$-representation and $\text{Re}(\alpha_i) = 6 \geq 1$ satisfying condition (ii) of Lemma 2, i.e., $\text{Re}(\alpha_i)\text{Im}(\alpha_i) = (3.5)(4\sqrt{3}) \geq (6)(1.5\sqrt{3}) = \text{Re}(\alpha_i)\text{Im}(\alpha_{n-1})$, and it follows from Theorem 4 that

$$f(x) = (2 + 8\sigma_3)x^3 + (2 + 3\sigma_3)x^2 + (5 + \sigma_3)x + (4 + 3\sigma_3)$$

(108)

is irreducible in $\mathcal{O}_K[x]$ and so is irreducible over $K$ because $\mathcal{O}_K$ is a unique factorization domain.

**4. Conclusion.**

For any quadratic field $K = \mathbb{Q}(\sqrt{m})$, we establish a new complete residue system for the case $m \equiv 1 \pmod{4}$. Then, we determine the so-called base $\beta(\mathcal{O}')$-representation and
generalize the result in Theorem 2 for the ring of integers of any imaginary quadratic field.

**Data Availability**

No data were used to support this study.

**Conflicts of Interest**

The authors declare that they have no conflicts of interest.

**Acknowledgments**

This work was supported by the Science Achievement Scholarship of Thailand (SAST).

**References**


