EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
2025, Vol. 18, Issue 1, Article Number 5709
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

Base-$\beta(\mathcal{C})$ Representations and Generalizations of Irreducibility Criteria for Polynomials over Any Imaginary Quadratic Fields

Phitthayathon Phetnun[1], Narakorn Rompurk Kanasri[1,*]

[1] *Department of Mathematics, Faculty of Science, Khon Kaen University, Khon Kaen, 40002, Thailand*

Abstract. Let K be an imaginary quadratic field with the ring of integers O_K. In the authors' earlier work, the so-called base-$\beta(\mathcal{C})$ representation for nonzero elements of O_K was determined, where $\mathcal{C}$ is a complete residue system modulo β. Using such a representation, irreducibility criteria for polynomials in $O_K[x]$ were established. In this paper, we provide the explicit shapes of all base-$\beta(\mathcal{C})$ representations for nonzero elements of O_K. Generalizations of such irreducibility criteria for polynomials in $O_K[x]$ under a certain condition are also established.

2020 Mathematics Subject Classifications: 11R04, 11R09, 11R11

Key Words and Phrases: Imaginary quadratic field, Ring of integers, Complete residue system, Prime element, Irreducible polynomial

1. Introduction

An old and interesting problem in mathematics is determining irreducible polynomials over a field. A polynomial with integer coefficients is said to be *irreducible* in $\mathbb{Z}[x]$ if it is an irreducible element of the polynomial ring $\mathbb{Z}[x]$. A polynomial $f(x)$ of positive degree in $\mathbb{Z}[x]$ is *primitive* if the greatest common divisor of its coefficients is 1. It is well known that a nonconstant polynomial in $\mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ if and only if it is both irreducible over $\mathbb{Q}$ and primitive in $\mathbb{Z}[x]$. Among many irreducibility criteria for polynomials in $\mathbb{Z}[x]$, we are interested in a classical result of A. Cohn, given by Pólya and Szegö [10]: if a prime p is expressed in the decimal representation as

$$p = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0,$$

then the polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is irreducible in $\mathbb{Z}[x]$. This result was subsequently generalized to any base b by Brillhart et al. [2] and Murty [5]. In

[*] Corresponding author.

DOI: https://doi.org/10.29020/nybg.ejpam.v18i1.5709

Email addresses: phitthayathon@kkumail.com (P. Phetnun), naraka@kku.ac.th (N.R. Kanasri)

1982, Filaseta [3] generalized this result in another way by considering wp instead of p: if w and b are positive integers with $w < b$ and

$$wp = b_m b^m + b_{m-1}b^{m-1} + \cdots + b_1 b + b_0$$

is the base-b representation of wp, where p is a prime, then the polynomial $f(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ is irreducible over $\mathbb{Q}$.

In another direction, let $K = \mathbb{Q}(\sqrt{m})$ with a unique squarefree integer $m \neq 1$, be a quadratic field and O_K denotes the set of algebraic integers that lie in K, called the *ring of integers* of K. We note that O_K is an integral domain and K is its quotient field. Moreover, the set of units in the polynomial ring $O_K[x]$ is $U(O_K)$, the group of units in O_K. The quadratic field K is said to be *real* if $m > 0$ and *imaginary* if $m < 0$. By letting the following notation

$$\sigma_m = \begin{cases} \sqrt{m} & \text{if } m \not\equiv 1 \pmod 4, \\ \dfrac{1+\sqrt{m}}{2} & \text{if } m \equiv 1 \pmod 4, \end{cases}$$

we have $O_K = \{a + b\sigma_m \mid a, b \in \mathbb{Z}\}$. More specifically, we see that the ring of *Gaussian integers* $\mathbb{Z}[i]$ is the ring of integers of $\mathbb{Q}(i)$ [1].

It is important to note that every prime element of O_K is irreducible; the converse is not generally true but holds if O_K is a unique factorization domain. We say that a nonzero polynomial $p(x) \in O_K[x]$ is *irreducible* in $O_K[x]$ if it is an irreducible element of $O_K[x]$, in other words, $p(x)$ is not a unit and $p(x) = f(x)g(x)$ in $O_K[x]$ implies $f(x)$ or $g(x)$ is a unit in O_K. Polynomials that are not irreducible are said to be *reducible*. For $\beta = a + b\sigma_m \in O_K$, we denote the *norm* of β by

$$N(\beta) = \begin{cases} a^2 - mb^2 & \text{if } m \not\equiv 1 \pmod 4, \\ a^2 + ab + b^2\left(\dfrac{1-m}{4}\right) & \text{if } m \equiv 1 \pmod 4. \end{cases}$$

We have seen from [1] that if $N(\beta) = \pm p$, where p is a rational prime, then β is an irreducible element. In addition, if K is an imaginary quadratic field, then $|\beta|^2 = N(\beta) \in \mathbb{N}$ for all $\beta \in O_K \backslash \{0\}$ and $|\beta| = 1$ for all $\beta \in U(O_K)$.

Let us recall the divisibility and congruence for elements of O_K as follows: for $\alpha, \beta \in O_K$ with $\alpha \neq 0$, we say that α *divides* β, denoted by $\alpha \mid \beta$, if there exists $\delta \in O_K$ such that $\beta = \alpha\delta$. For $\alpha, \beta, \gamma \in O_K$ with $\gamma \neq 0$, we say that α is *congruent* to β modulo γ, denoted by $\alpha \equiv \beta \pmod{\gamma}$, if $\gamma \mid (\alpha - \beta)$. A *complete residue system* modulo β in O_K is defined as in the following definition [9].

Definition A. *A* complete residue system *modulo β in O_K, abbreviated by $CRS(\beta)$, means a set of $|N(\beta)|$ elements $\mathcal{C} = \{\alpha_1, \alpha_2, \ldots, \alpha_{|N(\beta)|}\}$ in O_K which satisfies the following:*

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

(ii) $\alpha_i \not\equiv \alpha_j \pmod{\beta}$ *for all* $i, j \in \{1, 2, \ldots, |N(\beta)|\}$ *with* $i \neq j$.

For example, the set

$$\mathcal{C} = \left\{ x + yi \mid x = 0, 1, \ldots, \frac{a^2 + b^2}{d} - 1 \text{ and } y = 0, 1, \ldots, d - 1 \right\} \tag{1}$$

is a $CRS(\beta)$, where $\beta = a + bi \in \mathbb{Z}[i]$ with $d = \gcd(a, b)$ [11]. It is clear that the set

$$\mathcal{C}' := \{x + yi \mid x = 0, 1, \ldots, \max\{|a|, |b|\} - 1 \text{ and } y = 0, 1, \ldots, d - 1\} \subseteq \mathcal{C}.$$

In 2017, Singthongla et al. [12] established the irreducibility criterion for polynomials in $\mathbb{Z}[i][x]$ using the $CRS(\beta)$ in (1). The result is as follows.

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

$$\pi = \alpha_n \beta^n + \alpha_{n-1} \beta^{n-1} + \cdots + \alpha_1 \beta + \alpha_0 =: f(\beta),$$

where $n \geq 1$, $\mathrm{Re}(\alpha_n) \geq 1$, *and* $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathcal{C}'$ *satisfying* $\mathrm{Re}(\alpha_{n-1}) \mathrm{Im}(\alpha_n) \geq \mathrm{Re}(\alpha_n) \mathrm{Im}(\alpha_{n-1})$, *then* $f(x)$ *is irreducible in* $\mathbb{Z}[i][x]$.

Afterward, Kanasri et al. [4] generalized Theorem A by considering $\omega\pi$ ($\omega \in \mathbb{Z}[i] \backslash \{0\}$) instead of π as the following theorem.

Theorem B. *Let* $\beta = a + bi \in \mathbb{Z}[i]$ *be such that* $|\beta| \geq 2|\omega| + \sqrt{2}$ *and* $a \geq |\omega|$. *For a Gaussian prime* π, *if*

$$\omega\pi = \alpha_n \beta^n + \alpha_{n-1} \beta^{n-1} + \cdots + \alpha_1 \beta + \alpha_0 =: f(\beta),$$

where $n \geq 1$, $\mathrm{Re}(\alpha_n) \geq 1$, *and* $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathcal{C}'$ *satisfying* $\mathrm{Re}(\alpha_{n-1}) \mathrm{Im}(\alpha_n) \geq \mathrm{Re}(\alpha_n) \mathrm{Im}(\alpha_{n-1})$, *then* $f(x)$ *is irreducible over* $\mathbb{Q}(i)$.

For any quadratic field $K = \mathbb{Q}(\sqrt{m})$, Tadee et al. [13] proved for the case $m \not\equiv 1 \pmod{4}$ that the set

$$\mathcal{C} = \left\{ x + y\sigma_m \mid x = 0, 1, \ldots, \frac{|N(\beta)|}{d} - 1 \text{ and } y = 0, 1, \ldots, d - 1 \right\} \tag{2}$$

is a $CRS(\beta)$, where $\beta = a + b\sigma_m \in O_K$ with $d = \gcd(a, b)$. Recently, Phetnun et al. [8] verified that (2) is also a $CRS(\beta)$ in any quadratic field $K = \mathbb{Q}(\sqrt{m})$ with $m \equiv 1 \pmod{4}$. These results extend the $CRS(\beta)$ for Gaussian integers in (1) to any quadratic field. Moreover, they determined the so-called *base-*$\beta(\mathcal{C})$ *representation* for nonzero elements of O_K and extended Theorem A to any imaginary quadratic field using such a representation. It was shown for any $m < 0$ in [8] that the set

$$\mathcal{C}' := \{x + y\sigma_m \mid x = 0, 1, \ldots, \max\{|a|, |b|\} - 1 \text{ and } y = 0, 1, \ldots, d - 1\} \subseteq \mathcal{C}.$$

Some results in [8] described above are as follows.

Definition B. *Let $K = \mathbb{Q}(\sqrt{m})$ be an imaginary quadratic field. Let $\beta \in O_K \backslash \{0\}$ and $\mathcal{C}$ be the $CRS(\beta)$ as in* (2)*. We say that $\eta \in O_K \backslash \{0\}$ has a* base-$\beta(\mathcal{C})$ representation *if*

$$\eta = \alpha_n \beta^n + \alpha_{n-1} \beta^{n-1} + \cdots + \alpha_1 \beta + \alpha_0, \tag{3}$$

where $n \geq 1$, $\alpha_n \in O_K \backslash \{0\}$, and $\alpha_i \in \mathcal{C}$ $(i = 0, 1, \ldots, n-1)$. If $\alpha_i \in \mathcal{C}'$ $(i = 0, 1, \ldots, n-1)$, then (3) *is called a* base-$\beta(\mathcal{C}')$ representation *of η.*

Theorem C. *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 $|\beta| \geq 2 + \sqrt{1-m}$ and $a \geq 1 + \sqrt{1-m}$. For an irreducible element π of O_K with $|\pi| \geq |\beta|$, if*

$$\pi = \alpha_n \beta^n + \alpha_{n-1} \beta^{n-1} + \cdots + \alpha_1 \beta + \alpha_0 =: f(\beta)$$

is a base-$\beta(\mathcal{C}')$ representation with $\operatorname{Re}(\alpha_n) \geq 1$ satisfying $\operatorname{Re}(\alpha_{n-1}) \operatorname{Im}(\alpha_n) \geq \operatorname{Re}(\alpha_n) \operatorname{Im}(\alpha_{n-1})$, then $f(x)$ is irreducible in $O_K[x]$.

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

$$\pi = \alpha_n \beta^n + \alpha_{n-1} \beta^{n-1} + \cdots + \alpha_1 \beta + \alpha_0 =: f(\beta)$$

is a base-$\beta(\mathcal{C}')$ representation with $\operatorname{Re}(\alpha_n) \geq 1$ satisfying $\operatorname{Re}(\alpha_{n-1}) \operatorname{Im}(\alpha_n) \geq \operatorname{Re}(\alpha_n) \operatorname{Im}(\alpha_{n-1})$, then $f(x)$ is irreducible in $O_K[x]$.

Recently, Phetnun and Kanasri [7] established further irreducibility criteria for polynomials in $O_K[x]$, which extended Theorem 3.22 in [12] to any imaginary quadratic field. They also provided elements of β that can be applied to these criteria but not to Theorem C and Theorem D.

In the present work, we provide the explicit shapes of all base-$\beta(\mathcal{C})$ representations for nonzero elements of O_K, where K is an imaginary quadratic field. In addition, we generalize Theorem C and Theorem D by considering $\omega\pi$ instead of π, where $\omega \in O_K \backslash \{0\}$ and π is a prime element, which in turn extend Theorem B to any imaginary quadratic field.

2. Explicit Shapes of Base-$\beta(\mathcal{C})$ Representations

Let K be an imaginary quadratic field and $\eta, \beta = a + b\sigma_m$ be nonzero elements of O_K. Let $\mathcal{C}$ be the base-$\beta(\mathcal{C})$ representations as in (2). If $\eta \in \mathcal{C}$, it is clear from Definition B that η cannot be written as a base-$\beta(\mathcal{C})$ representation. Assume henceforth that $\eta \notin \mathcal{C}$. By Definition A, there exists a unique $\alpha_0 \in \mathcal{C}$ such that $\eta \equiv \alpha_0 \pmod{\beta}$, so $\eta = \gamma_0 \beta + \alpha_0$ for some $\gamma_0 \in O_K \backslash \{0\}$. If $\gamma_0 \in \mathcal{C}$, then the process stops, otherwise, there exists a unique $\alpha_1 \in \mathcal{C}$ such that $\gamma_0 \equiv \alpha_1 \pmod{\beta}$, yielding $\gamma_0 = \gamma_1 \beta + \alpha_1$ for some $\gamma_1 \in O_K \backslash \{0\}$. It follows that $\eta = \gamma_1\beta^2 + \alpha_1\beta + \alpha_0$. Continuing the process, we obtain the sequence $(\gamma_i)_{i\geq 0}$ of elements of O_K such that

$$\gamma_{i-1} = \gamma_i\beta + \alpha_i \quad (i \geq 0) \tag{4}$$

with $\gamma_{-1} = \eta$. If there exists $n \in \mathbb{N} \cup \{0\}$ such that $\gamma_n \in \mathcal{C}$, then

$$\begin{aligned} \eta &= \gamma_0\beta + \alpha_0, \\ \eta &= \gamma_1\beta^2 + \alpha_1\beta + \alpha_0, \\ &\vdots \\ \eta &= \gamma_n\beta^{n+1} + \alpha_n\beta^n + \cdots + \alpha_1\beta + \alpha_0 \end{aligned} \tag{5}$$

are $n + 1$ base-$\beta(\mathcal{C})$ representations of η.

The following theorem shows that the equations in (5) are all base-$\beta(\mathcal{C})$ representations of η for the case $\gamma_n \in \mathcal{C}$ for some $n \in \mathbb{N} \cup \{0\}$.

Theorem 1. *Let $K = \mathbb{Q}(\sqrt{m})$ be an imaginary quadratic field and let β, $\eta \in O_K\backslash\{0\}$ with $\eta \notin \mathcal{C}$. Let $(\gamma_i)_{i\geq 0}$ be the sequence described in (4). If $\gamma_n \in \mathcal{C}$ for some $n \in \mathbb{N} \cup \{0\}$, then all equations in (5) are the base-$\beta(\mathcal{C})$ representations of η.*

Proof. By the description mentioned above, all $n + 1$ equations in (5) are base-$\beta(\mathcal{C})$ representations of η. Next, let

$$\eta = \delta_k\beta^k + \delta_{k-1}\beta^{k-1} + \cdots + \delta_1\beta + \delta_0 \tag{6}$$

be any base-$\beta(\mathcal{C})$ representation of η. Then $k \in \mathbb{N}$, $\delta_i \in \mathcal{C}$ $(0 \leq i \leq k-1)$, and $\delta_k \in O_K\backslash\{0\}$. Suppose that $k \geq n + 2$. By the last equation in (5) together with (6), we obtain that $\eta \equiv \alpha_0 \pmod{\beta}$ and $\eta \equiv \delta_0 \pmod{\beta}$. It follows from Definition A(ii) that $\alpha_0 = \delta_0$. Then

$$\eta_1 := \gamma_n\beta^n + \alpha_n\beta^{n-1} + \cdots + \alpha_2\beta + \alpha_1 = \delta_k\beta^{k-1} + \delta_{k-1}\beta^{k-2} + \cdots + \delta_2\beta + \delta_1,$$

so $\alpha_1 \equiv \delta_1 \pmod{\beta}$. Again, by Definition A(ii), we obtain $\alpha_1 = \delta_1$ and so

$$\eta_2 := \gamma_n\beta^{n-1} + \alpha_n\beta^{n-2} + \cdots + \alpha_2 = \delta_k\beta^{k-2} + \delta_{k-1}\beta^{k-3} + \cdots + \delta_2.$$

Proceeding in the same manner, we deduce that $\alpha_i = \delta_i$ $(0 \leq i \leq n)$ and $\gamma_n = \delta_k\beta^{k-n-1} + \cdots + \delta_{n+2}\beta + \delta_{n+1}$, implying $\gamma_n \equiv \delta_{n+1} \pmod{\beta}$. Since $\gamma_n, \delta_{n+1} \in \mathcal{C}$, it follows that $\gamma_n = \delta_{n+1}$. Thus we have

$$\delta_k\beta^{k-n-2} + \cdots + \delta_{n+3}\beta + \delta_{n+2} = 0, \tag{7}$$

so $\delta_{n+2} \equiv 0 \pmod{\beta}$. If $k = n + 2$, then (7) implies $\delta_k = 0$, a contradiction. If $k > n + 2$, then $\delta_{n+2} \in \mathcal{C}$ and thus $\delta_{n+2} = 0$ by Definition A(ii). Continuing similarly, we finally obtain $\delta_k = 0$, which is a contradiction. Hence $k \leq n + 1$, implying the base-$\beta(\mathcal{C})$ representation of η in (6) is one of that in (5) as desired.

The base-$\beta(\mathcal{C})$ representations for the case $\gamma_n \in \mathcal{C}$ for some $n \in \mathbb{N} \cup \{0\}$ are shown in the following example.

Example 1. *Let $K = \mathbb{Q}(\sqrt{-1})$, $\beta = -3 + 2i$, and $\eta = -439 - 258i$. Then $d = 1$, $N(\beta) = 13$, and thus $\mathcal{C} = \{0, 1, \ldots, 12\}$ is a $CRS(\beta)$. One can compute that*

$$\begin{aligned} \eta &= (63 + 128i)\beta + 6, \\ 63 + 128i &= (7 - 38i)\beta + 8, \\ 7 - 38i &= (-7 + 8i)\beta + 2, \\ -7 + 8i &= 4\beta + 5. \end{aligned}$$

Thus, $\gamma_0 = 63 + 128i$, $\gamma_1 = 7 - 38i$, $\gamma_2 = -7 + 8i$, $\gamma_3 = 4 \in \mathcal{C}$ and $\alpha_0 = 6$, $\alpha_1 = 8$, $\alpha_2 = 2$, $\alpha_3 = 5$. By Theorem 1, we conclude that

$$\eta = \gamma_k \beta^{k+1} + \alpha_k \beta^k + \cdots + \alpha_1 \beta + \alpha_0 \quad (0 \le k \le 3)$$

are the base-$\beta(\mathcal{C})$ representations of η.

To provide the explicit shapes of the base-$\beta(\mathcal{C})$ representations of η for the case $\gamma_i \notin \mathcal{C}$ for all $i \in \mathbb{N} \cup \{0\}$, we require the following lemma.

Lemma 1. *Let $K = \mathbb{Q}(\sqrt{m})$ be an imaginary quadratic field and let $\beta = a + b\sigma_m \in O_K$ such that $|\beta| \ge 2$ and $d = \gcd(a, b)$. Let*

$$S = \begin{cases} \sqrt{\left(\frac{|N(\beta)|}{d} - 1\right)^2 - m(d-1)^2} & \text{if } m \not\equiv 1 \pmod 4, \\ \sqrt{\left(\frac{|N(\beta)|}{d} - 1\right)^2 + \left(\frac{|N(\beta)|}{d} - 1\right)(d-1) + (d-1)^2\left(\frac{1-m}{4}\right)} & \text{if } m \equiv 1 \pmod 4. \end{cases} \tag{8}$$

For $\eta \in O_K$ with $|\eta| \ge S$, if $\eta = \gamma_0\beta + \alpha_0$, where $\gamma_0 \in O_K \backslash \{0\}$ and $\alpha_0 \in \mathcal{C}$, then $|\eta| \ge |\gamma_0|$.

Proof. Suppose to the contrary that $|\gamma_0| > |\eta|$. Then $|\gamma_0| > |\gamma_0\beta + \alpha_0| \ge |\gamma_0||\beta| - |\alpha_0|$ and thus $|\alpha_0| > |\gamma_0|(|\beta| - 1)$. Since $\alpha_0 \in \mathcal{C}$, we have $|\alpha_0| \le S$ and hence $|\gamma_0| > |\eta| \ge S \ge |\alpha_0| > |\gamma_0|(|\beta| - 1) \ge |\gamma_0|$, which is a contradiction.

Theorem 2. *Let $K = \mathbb{Q}(\sqrt{m})$ be an imaginary quadratic field and let $\beta = a + b\sigma_m, \eta \in O_K$ be such that $|\beta| \ge 2$, $\eta \notin \mathcal{C}$, and $|\eta| \ge S$, where S is defined as in (8). Let $(\gamma_i)_{i \ge 0}$ be the sequence described in (4). If $\gamma_i \notin \mathcal{C}$ for all $i \in \mathbb{N} \cup \{0\}$, then there exist nonnegative integers u and v with $u < v$ such that $\gamma_u = \gamma_v$ and the base-$\beta(\mathcal{C})$ representations of η are of the form*

$$\eta = \gamma_k \beta^{k+1} + \sum_{0 \le i \le k} \alpha_i \beta^i \quad (0 \le k \le u), \tag{9}$$

$$\eta = \gamma_k \beta^{k+1} + \sum_{u < j \le k} \alpha_j \beta^j + \sum_{0 \le i \le u} \alpha_i \beta^i \quad (u < k < v), \tag{10}$$

$$\begin{aligned} \eta = {} & \gamma_u \beta^{(v-u)n+u+1} + \alpha_v \beta^{(v-u)n+u} + \alpha_{v-1} \beta^{(v-u)n+u-1} \\ & + \cdots + \alpha_{u+1} \beta^{(v-u)n+2u-v+1} + \cdots + \sum_{u < j \le v} \alpha_j \beta^j + \sum_{0 \le i \le u} \alpha_i \beta^i \quad (n \in \mathbb{N}), \end{aligned} \tag{11}$$

$$\begin{aligned}
\eta &= \gamma_{u+1}\beta^{(v-u)n+u+2} + \alpha_{u+1}\beta^{(v-u)n+u+1} + \alpha_v\beta^{(v-u)n+u} \\
&\quad + \alpha_{v-1}\beta^{(v-u)n+u-1} + \cdots + \alpha_{u+1}\beta^{(v-u)n+2u-v+1} + \cdots + \sum_{u<j\le v}\alpha_j\beta^j + \sum_{0\le i\le u}\alpha_i\beta^i \quad (n\in\mathbb{N}), \\
\eta &= \gamma_{u+2}\beta^{(v-u)n+u+3} + \alpha_{u+2}\beta^{(v-u)n+u+2} + \alpha_{u+1}\beta^{(v-u)n+u+1} + \alpha_v\beta^{(v-u)n+u} \\
&\quad + \alpha_{v-1}\beta^{(v-u)n+u-1} + \cdots + \alpha_{u+1}\beta^{(v-u)n+2u-v+1} + \cdots + \sum_{u<j\le v}\alpha_j\beta^j + \sum_{0\le i\le u}\alpha_i\beta^i \quad (n\in\mathbb{N}), \\
&\vdots \\
\eta &= \gamma_{v-1}\beta^{(v-u)n+v} + \alpha_{v-1}\beta^{(v-u)n+v-1} + \alpha_{v-2}\beta^{(v-u)n+v-2} \\
&\quad + \cdots + \alpha_{u+1}\beta^{(v-u)n+u+1} + \alpha_v\beta^{(v-u)n+u} + \alpha_{v-1}\beta^{(v-u)n+u-1} \\
&\quad + \cdots + \alpha_{u+1}\beta^{(v-u)n+2u-v+1} + \cdots + \sum_{u<j\le v}\alpha_j\beta^j + \sum_{0\le i\le u}\alpha_i\beta^i \quad (n\in\mathbb{N}).
\end{aligned} \tag{12}$$

Proof. We first verify two important claims:

Claim 1. $|\gamma_i| \le \max\{2S, |\eta|\} =: N$ for all $i \in \mathbb{N}\cup\{0\}$.

Proof of Claim 1. For $i = 0$, we have $\eta = \gamma_0\beta + \alpha_0$. Since $|\eta| \ge S$, it follows from Lemma 1 that $|\gamma_0| \le |\eta| \le N$. For $i = 1$, we have $\gamma_0 = \gamma_1\beta + \alpha_1$, where $\gamma_1 \in O_K\backslash\{0\}$ and $\alpha_1 \in \mathcal{C}$, so $|\alpha_1| \le S$. If $|\gamma_0| \ge S$, then it follows from Lemma 1 again that $|\gamma_1| \le |\gamma_0| \le N$. If $|\gamma_0| < S$, then $S > |\gamma_1\beta + \alpha_1| \ge |\gamma_1||\beta| - |\alpha_1|$ and thus

$$|\gamma_1| < 2|\gamma_1| \le |\gamma_1||\beta| < S + |\alpha_1| \le S + S = 2S \le N.$$

Proceeding in the same manner, we obtain $|\gamma_i| \le N$ for all $i \in \mathbb{N}\cup\{0\}$.

Claim 2. There exist nonnegative integers u and v with $u < v$ such that $\gamma_u = \gamma_v$.

Proof of Claim 2. By Claim 1, we have $|\gamma_i| \le N$ for all $i \in \mathbb{N}\cup\{0\}$. For each $i \in \mathbb{N}\cup\{0\}$, we denote $\gamma_i := a_i + b_i\sigma_m$ and $A := \{(a_0, b_0), (a_1, b_1), (a_2, b_2), \ldots\}$, where $a_i, b_i \in \mathbb{Z}$ for all $i \in \mathbb{N}\cup\{0\}$. We first show that A is a finite set by considering the following two cases:

Case 1. $m \not\equiv 1 \pmod 4$. Then $a_i^2 - mb_i^2 = N(\gamma_i) = |\gamma_i|^2 \le N^2$ for all $i \in \mathbb{N}\cup\{0\}$. Thus $a_i^2 \le N^2$ and $b_i^2 \le N^2$ and so $|a_i| \le N$ and $|b_i| \le N$. It follows that the set A is finite.

Case 2. $m \equiv 1 \pmod 4$. Then $a_i^2 + a_ib_i + b_i^2(1-m)/4 = N(\gamma_i) = |\gamma_i|^2 \le N^2$ for all $i \in \mathbb{N}\cup\{0\}$, so $(2a_i + b_i)^2 - mb_i^2 = 4a_i^2 + 4a_ib_i + b_i^2 - mb_i^2 \le 4N^2$. It follows that $|b_i| \le 2N$ and $|2a_i + b_i| \le 2N$ and thus $|a_i| \le |2a_i| \le |2a_i + b_i| + |b_i| \le 2N + 2N = 4N$, implying the set A is finite. Consequently, $(a_u, b_u) = (a_v, b_v)$ for some nonnegative integers u and v with $u < v$. This implies that $\gamma_u = a_u + b_u\sigma_m = a_v + b_v\sigma_m = \gamma_v$.

Next, we show that the base-$\beta(\mathcal{C})$ representations of η are the equations in (9), (10), (11), and (12). Recall that $\eta = \gamma_0\beta + \alpha_0$ and

$$\gamma_{i-1} = \gamma_i\beta + \alpha_i \quad (i \ge 1), \tag{13}$$

where $\gamma_i \in O_K\backslash\{0\}$ and $\alpha_i \in \mathcal{C}$ for all $i \ge 0$. Then we obtain

$$\eta = \gamma_k\beta^{k+1} + \alpha_k\beta^k + \alpha_{k-1}\beta^{k-1} + \cdots + \alpha_1\beta + \alpha_0 \ \ (0 \le k \le u), \tag{14}$$

which are base-$\beta(\mathcal{C})$ representations in (9). Again, using (13) repeatedly, we get

$$\eta = \gamma_k\beta^{k+1} + \alpha_k\beta^k + \cdots + \alpha_{u+1}\beta^{u+1} + \alpha_u\beta^u + \cdots + \alpha_1\beta + \alpha_0 \quad (u < k < v),$$

which are base-$\beta(\mathcal{C})$ representations in (10). Since $\gamma_u = \gamma_v$, we obtain from (13) that

$$\begin{aligned}\gamma_u &= \gamma_{u+1}\beta + \alpha_{u+1}\\ &= \gamma_{u+2}\beta^2 + \alpha_{u+2}\beta + \alpha_{u+1}\\ &\ \vdots\\ &= \gamma_u\beta^{v-u} + \alpha_v\beta^{v-u-1} + \alpha_{v-1}\beta^{v-u-2} + \cdots + \alpha_{u+2}\beta + \alpha_{u+1}.\end{aligned} \tag{15}$$

Substituting (15) into (14) with $k = u$ leads to

$$\eta = \gamma_u\beta^{v+1} + \alpha_v\beta^v + \alpha_{v-1}\beta^{v-1} + \cdots + \alpha_{u+1}\beta^{u+1} + \alpha_u\beta^u + \alpha_{u-1}\beta^{u-1} + \cdots + \alpha_1\beta + \alpha_0. \tag{16}$$

Again, substituting (15) into (16) yields

$$\begin{aligned}\eta = \gamma_u\beta^{2v-u+1} &+ \alpha_v\beta^{2v-u} + \alpha_{v-1}\beta^{2v-u-1} + \cdots + \alpha_{u+1}\beta^{v+1} + \alpha_v\beta^v\\ &+ \alpha_{v-1}\beta^{v-1} + \cdots + \alpha_{u+1}\beta^{u+1} + \alpha_u\beta^u + \alpha_{u-1}\beta^{u-1} + \cdots + \alpha_1\beta + \alpha_0.\end{aligned} \tag{17}$$

Continuing this process, in general, we have

$$\begin{aligned}\eta = \gamma_u\beta^{(v-u)n+u+1} &+ \alpha_v\beta^{(v-u)n+u} + \alpha_{v-1}\beta^{(v-u)n+u-1}\\ &+ \cdots + \alpha_{u+1}\beta^{(v-u)n+2u-v+1} + \cdots + \sum_{u<j\le v}\alpha_j\beta^j + \sum_{0\le i\le u}\alpha_i\beta^i \qquad (n \in \mathbb{N}),\end{aligned} \tag{18}$$

yielding base-$\beta(\mathcal{C})$ representations in (11). Using (13) successively and (18), we obtain the base-$\beta(\mathcal{C})$ representations in (12).

Finally, we let $\eta = \delta_l\beta^l + \cdots + \delta_1\beta + \delta_0$ be any base-$\beta(\mathcal{C})$ representation of η, where $l \in \mathbb{N}$, $\delta_l \in O_K\backslash\{0\}$, and $\delta_i \in \mathcal{C}$ for all $i \in \{0, 1, \ldots, l-1\}$. Then

$$\eta = \gamma_{l-1}\beta^l + \alpha_{l-1}\beta^{l-1} + \cdots + \alpha_1\beta + \alpha_0$$

is one of the equations in (9), (10), (11), or (12). By the same proof as in Theorem 1, we can conclude that $\alpha_i = \delta_i$ $(0 \le i \le l-1)$ and $\gamma_{l-1} = \delta_l$. This completes the proof.

Note that the base-$\beta(\mathcal{C})$ representations of η in (11) and (12) are periodic with period $v - u$.

The following examples show the explicit shapes of the base-$\beta(\mathcal{C})$ representations of η for the case $\gamma_i \notin \mathcal{C}$ for all $i \in \mathbb{N} \cup \{0\}$.

Example 2. *Let $K = \mathbb{Q}(\sqrt{-5})$, $\beta = 4 + 2\sqrt{-5}$, and $\eta = -5 + 10\sqrt{-5}$. Then $d = 2$, $N(\beta) = 36$, and thus $\mathcal{C} = \left\{x + y\sqrt{-5} \mid x = 0, 1, \ldots, 17 \text{ and } y = 0, 1\right\}$ is a $CRS(\beta)$. We have $|\beta| = \sqrt{36} > 2$ and $|\eta| = \sqrt{525} > \sqrt{294} = S$. One can compute that*

$$\eta = (1 + 2\sqrt{-5})\beta + 11,$$

$$\begin{aligned}
1+2\sqrt{-5} &= (-1+\sqrt{-5})\beta+15,\\
-1+\sqrt{-5} &= (-2+\sqrt{-5})\beta+(17+\sqrt{-5}),\\
-2+\sqrt{-5} &= (-2+\sqrt{-5})\beta+(16+\sqrt{-5}).
\end{aligned}$$

Thus $\gamma_0 = 1+2\sqrt{-5}$, $\gamma_1 = -1+\sqrt{-5}$, $\gamma_2 = -2+\sqrt{-5} = \gamma_3$, *and so* $\gamma_i = \gamma_2$ *for all* $i \geq 2$. *One can see that* $\gamma_i \notin \mathcal{C}$ *for all* $i \in \mathbb{N}\cup\{0\}$. *Note that* $\alpha_0 = 11$, $\alpha_1 = 15$, $\alpha_2 = 17+\sqrt{-5}$, *and* $\alpha_3 = 16+\sqrt{-5} = \alpha_i$ *for all* $i \geq 3$. *Using Theorem 2 with* $u = 2$ *and* $v = 3$, *we conclude that the base-*$\beta(\mathcal{C})$ *representations of* η *are*

$$\eta = \gamma_k\beta^{k+1}+\alpha_k\beta^k+\cdots+\alpha_1\beta+\alpha_0 \quad (0\leq k\leq 2)$$

and $\eta = \gamma_2\beta^{n+3}+\alpha_3\beta^{n+2}+\cdots+\alpha_3\beta^3+\alpha_2\beta^2+\alpha_1\beta+\alpha_0$ *for all* $n \in \mathbb{N}$.

Example 3. *Let* $K = \mathbb{Q}(\sqrt{-7})$, $\beta = 2+3\sigma_{-7}$, *and* $\eta = 3112-13810\sigma_{-7}$. *Then* $d = 1$, $N(\beta) = 28$, *and thus* $\mathcal{C} = \{0,1,\ldots,27\}$ *is a CRS*(β). *We have* $|\beta| = \sqrt{28} > 2$ *and* $|\eta| = \sqrt{348140024} > 27 = S$. *One can compute that*

$$\begin{aligned}
\eta &= (-2405-1319\sigma_{-7})\,\beta+8,\\
-2405-1319\sigma_{-7} &= (-713+164\sigma_{-7})\,\beta+5,\\
-713+164\sigma_{-7} &= (-97+91\sigma_{-7})\,\beta+27,\\
-97+91\sigma_{-7} &= (2+17\sigma_{-7})\,\beta+1,\\
2+17\sigma_{-7} &= (4+\sigma_{-7})\,\beta,\\
4+\sigma_{-7} &= (-3+2\sigma_{-7})\,\beta+22,\\
-3+2\sigma_{-7} &= (-1+\sigma_{-7})\,\beta+5,\\
-1+\sigma_{-7} &= (-3+2\sigma_{-7})\,\beta+17,\\
-3+2\sigma_{-7} &= (-1+\sigma_{-7})\,\beta+5.
\end{aligned}$$

Thus $\gamma_0 = -2405-1319\sigma_{-7}$, $\gamma_1 = -713+164\sigma_{-7}$, $\gamma_2 = -97+91\sigma_{-7}$, $\gamma_3 = 2+17\sigma_{-7}$, $\gamma_4 = 4+\sigma_{-7}$, $\gamma_5 = -3+2\sigma_{-7} = \gamma_7 = \gamma_9 = \cdots$, *and* $\gamma_6 = -1+\sigma_{-7} = \gamma_8 = \gamma_{10} = \cdots$. *One can see that* $\gamma_i \notin \mathcal{C}$ *for all* $i \in \mathbb{N}\cup\{0\}$. *We also have* $\alpha_0 = 8$, $\alpha_1 = 5$, $\alpha_2 = 27$, $\alpha_3 = 1$, $\alpha_4 = 0$, $\alpha_5 = 22$, $\alpha_6 = 5 = \alpha_8 = \alpha_{10} = \cdots$, *and* $\alpha_7 = 17 = \alpha_9 = \alpha_{11} = \cdots$. *Using Theorem 2 with* $u = 5$ *and* $v = 7$, *we conclude that the base-*$\beta(\mathcal{C})$ *representations of* η *are*

$$\begin{aligned}
\eta &= \gamma_k\beta^{k+1}+\alpha_k\beta^k+\cdots+\alpha_1\beta+\alpha_0 \quad (0\leq k\leq 5),\\
\eta &= \gamma_6\beta^7+\alpha_6\beta^6+\alpha_5\beta^5+\alpha_4\beta^4+\alpha_3\beta^3+\alpha_2\beta^2+\alpha_1\beta+\alpha_0,\\
\eta &= \gamma_5\beta^{2n+6}+\alpha_7\beta^{2n+5}+\alpha_6\beta^{2n+4}+\cdots+\alpha_7\beta^7+\alpha_6\beta^6\\
&\quad +\alpha_5\beta^5+\alpha_4\beta^4+\alpha_3\beta^3+\alpha_2\beta^2+\alpha_1\beta+\alpha_0 \quad (n\in\mathbb{N}),\\
\eta &= \gamma_6\beta^{2n+7}+\alpha_6\beta^{2n+6}+\alpha_7\beta^{2n+5}+\alpha_6\beta^{2n+4}+\cdots+\alpha_7\beta^7+\alpha_6\beta^6\\
&\quad +\alpha_5\beta^5+\alpha_4\beta^4+\alpha_3\beta^3+\alpha_2\beta^2+\alpha_1\beta+\alpha_0 \quad (n\in\mathbb{N}).
\end{aligned}$$

3. Generalizations of Irreducibility Criteria for Polynomials in $O_K[x]$

Let $K = \mathbb{Q}(\sqrt{m})$ be an imaginary quadratic field. In this section, we extend Theorem B to any imaginary quadratic field, which in turn generalize Theorem C and Theorem D by considering $\omega\pi$ instead of π, where $\omega \in O_K\backslash\{0\}$ and π is a prime element. To prove these, we first recall the essential three lemmas.

Lemma 2. *[12] Let $f(x) = \alpha_n x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0 \in \mathbb{C}[x]$ be such that $n \geq 2$ and $|\alpha_i| \leq M$ $(0 \leq i \leq n-2)$ for some positive real number M. If $f(x)$ satisfies*

- *(i)* $\operatorname{Re}(\alpha_n) \geq 1$, $\operatorname{Re}(\alpha_{n-1}) \geq 0$, *and* $\operatorname{Im}(\alpha_{n-1}) \geq 0$*; and*
- *(ii)* $\operatorname{Re}(\alpha_{n-1})\operatorname{Im}(\alpha_n) \geq \operatorname{Re}(\alpha_n)\operatorname{Im}(\alpha_{n-1})$,

then any complex zero α of $f(x)$ satisfies either $\operatorname{Re}(\alpha) < 0$ *or* $|\alpha| < \big(1 + \sqrt{1+4M}\big)/2$.

Lemma 3. *[8] 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*

$$M = \sqrt{(\max\{a, |b|\} - 1)^2 - m(d-1)^2}, \tag{19}$$

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

Lemma 4. *[8] Let $K = \mathbb{Q}(\sqrt{m})$ be an imaginary quadratic field with $m \equiv 1 \pmod 4$. Let $\beta = a + b\sigma_m \in O_K$ be such that $a \geq 1$ and*

$$M = \sqrt{(\max\{a, |b|\} - 1)^2 + (\max\{a, |b|\} - 1)(d-1) + (d-1)^2\left(\frac{1-m}{4}\right)}, \tag{20}$$

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

If $f(x)$ is a nonconstant polynomial in $O_K[x]$, we say that $f(x) = g(x)h(x)$ in $O_K[x]$ is a *proper factorization* if both $g(x)$ and $h(x)$ have a smaller degree than $f(x)$. We now proceed to our second main result and start with the case $m \not\equiv 1 \pmod 4$.

Theorem 3. *Let $K = \mathbb{Q}(\sqrt{m})$ be an imaginary quadratic field with $m \not\equiv 1 \pmod 4$. Let $\beta = a + b\sqrt{m} \in O_K$ and $\omega \in O_K\backslash\{0\}$ be such that $|\beta| \geq 2|\omega| + \sqrt{1-m}$ and $a \geq |\omega| + \sqrt{1-m}$. For a prime element π of O_K with $|\pi| \geq |\beta|$, if*

$$\omega\pi = \alpha_n\beta^n + \alpha_{n-1}\beta^{n-1} + \cdots + \alpha_1\beta + \alpha_0 =: f(\beta)$$

is a base-$\beta(\mathcal{C}')$ representation with $n \geq 2$ and $\operatorname{Re}(\alpha_n) \geq 1$ *satisfying the condition (ii) of Lemma 2, then $f(x)$ has no proper factorization in $O_K[x]$. Moreover,*

- *(i) if $\delta \nmid f(x)$ for all $\delta \in O_K\backslash U(O_K)$, then $f(x)$ is irreducible in $O_K[x]$;*
- *(ii) if O_K is a unique factorization domain, then $f(x)$ is irreducible over K.*

Proof. Suppose to the contrary that $f(x)$ has proper factorization in $O_K[x]$. Then $f(x) = g(x)h(x)$ for some nonconstant polynomials $g(x)$ and $h(x)$ in $O_K[x]$, so $\omega\pi = g(\beta)h(\beta)$. Since π is a prime element, either $\pi \mid g(\beta)$ and $h(\beta) \mid \omega$ or $\pi \mid h(\beta)$ and $g(\beta) \mid \omega$. This implies that either $|\omega| \geq |h(\beta)|$ or $|\omega| \geq |g(\beta)|$. Without loss of generality, we may assume that $|\omega| \geq |g(\beta)|$.

Since $\alpha_i \in \mathcal{C}'$ for all $i \in \{0, 1, \ldots, n-1\}$, we have $|\alpha_i| \leq M$ for all $i \in \{0, 1, \ldots, n-1\}$, where M is defined as in (19). We now show that

$$|\beta| - \frac{1 + \sqrt{1 + 4M}}{2} \geq |\omega|. \tag{21}$$

Since $|\beta| \geq 2|\omega| + \sqrt{1-m}$, we have $|\beta|^2 - \left(2|\omega| + 1 + \sqrt{1-m}\right)|\beta| + 2|\omega| + \sqrt{1-m} = (|\beta| - 1)\left[|\beta| - \left(2|\omega| + \sqrt{1-m}\right)\right] \geq 0$. As $|\omega|^2 + |\omega| \geq 2|\omega|$, we obtain $4\left[|\beta|^2 - \left(2|\omega| + 1 + \sqrt{1-m}\right)|\beta| + |\omega|^2 + |\omega| + \sqrt{1-m}\right] \geq 0$ and so $[2|\beta| - (2|\omega| + 1)]^2 = 4|\beta|^2 - 4(2|\omega| + 1)|\beta| + 4|\omega|^2 + 4|\omega| + 1 \geq 1 + 4\sqrt{1-m}\,(|\beta| - 1)$. Again, $|\beta| \geq 2|\omega| + \sqrt{1-m}$ implies $2|\beta| - (2|\omega| + 1) > 0$ and thus, $2|\beta| - (2|\omega| + 1) \geq \sqrt{1 + 4\sqrt{1-m}\,(|\beta| - 1)}$. Hence

$$|\beta| \geq \frac{2|\omega| + 1 + \sqrt{1 + 4\sqrt{1-m}\,(|\beta| - 1)}}{2}.$$

As $a \geq |\omega| + \sqrt{1-m}$, it follows from Lemma 3 that $\sqrt{1-m}\,(|\beta| - 1) \geq M$. Therefore,

$$|\beta| \geq \frac{2|\omega| + 1 + \sqrt{1 + 4M}}{2} = |\omega| + \frac{1 + \sqrt{1 + 4M}}{2},$$

which proves (21).

Now, we have that $\deg g(x) \geq 1$, so $g(x)$ can be expressed in the form $g(x) = \varepsilon \prod_i (x - \gamma_i)$, where $\varepsilon \in O_K$ 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 γ of $g(x)$ satisfies either $\mathrm{Re}(\gamma) < 0$ or

$$|\gamma| < \frac{1 + \sqrt{1 + 4M}}{2}. \tag{22}$$

In the former case, we have $|\beta - \gamma| \geq \mathrm{Re}(\beta - \gamma) = \mathrm{Re}(\beta) - \mathrm{Re}(\gamma) > \mathrm{Re}(\beta) = a \geq |\omega| + \sqrt{1-m} > |\omega|$. In the latter case, we obtain by using (21) and (22) that

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

From both cases and $|\varepsilon| \geq 1$, we deduce that

$$|\omega| \geq |g(\beta)| = |\varepsilon| \prod_i |\beta - \gamma_i| \geq \prod_i |\beta - \gamma_i| > |\omega|,$$

which is a contradiction.

We have that $f(x)$ has no proper factorization in $O_K[x]$. Then, (i) is true. If O_K is a unique factorization domain, $f(x)$ is irreducible over K. To see this, suppose to the contrary that $f(x) = g_1(x)h_1(x)$ for some nonconstant polynomials $g_1(x)$ and $h_1(x)$ in $K[x]$. Since every element of K is of the form α/r, where $\alpha \in O_K$ and $r \in \mathbb{Z}\backslash\{0\}$, we may take $g_2(x) = rg_1(x)$ and $h_2(x) = sh_1(x)$, where $g_2(x), h_2(x) \in O_K[x]$ with $\deg g_2(x) \geq 1, \deg h_2(x) \geq 1$ and $r, s \in \mathbb{Z}\backslash\{0\}$ so that $rsf(x) = g_2(x)h_2(x)$. Let π be a prime divisor of rs in O_K. Considering the contents of the above polynomials and using Gauss's lemma for O_K, we get that π divides $g_2(x)$ or $h_2(x)$, yielding

$$\frac{rs}{\pi}f(x) = g_3(x)h_3(x)$$

for some nonconstant polynomials $g_3(x), h_3(x) \in O_K[x]$. Continuing in the same manner, we finally get $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are positive degree polynomials in $O_K[x]$, which is a contradiction. This proves (ii) and we complete the proof.

We note that the condition $a \geq |\omega| + \sqrt{1-m}$ in Theorem 3 can be reduced to $a \geq |\omega|$ for the case of Gaussian integers and one can see that $\mathbb{Z}[i]$ is a unique factorization domain. This implies that Theorem 3 extends Theorem B to any imaginary quadratic field with $m \not\equiv 1 \pmod 4$.

Applying Theorem 3, we can find irreducible polynomials as the following examples.

Example 4. *Let $K = \mathbb{Q}(\sqrt{-2})$, $\beta = 9-3\sqrt{-2}$, $\omega = 2+\sqrt{-2}$, and $\pi = -8177-28932\sqrt{-2}$. Then $d = 3$ and thus $\mathcal{C}' = \left\{x + y\sqrt{-2} \mid x = 0, 1, \ldots, 8 \text{ and } y = 0, 1, 2\right\}$. One can see that $|\beta| = \sqrt{99} > 2\sqrt{6} + \sqrt{3} = 2|\omega| + \sqrt{1-m}$ and $a = 9 > \sqrt{6} + \sqrt{3} = |\omega| + \sqrt{1-m}$. Since $N(\pi) = 1740984577$ is a rational prime, we have that π is an irreducible element and so is a prime element because O_K is a unique factorization domain. Now, we have $|\pi| > |\beta|$ and*

$$\omega\pi = 41510 - 66041\sqrt{-2} = (8+4\sqrt{-2})\beta^4 + 6\beta^3 + (4+2\sqrt{-2})\beta^2 + 6\beta + (2+\sqrt{-2}),$$

which is a base-$\beta(\mathcal{C}')$ representation of $\omega\pi$. Moreover, $\mathrm{Re}(\alpha_4) = 8 > 1$ and $\mathrm{Re}(\alpha_3)\,\mathrm{Im}(\alpha_4) = (6)(4\sqrt{2}) > (8)(0) = \mathrm{Re}(\alpha_4)\,\mathrm{Im}(\alpha_3)$. By Theorem 3, we obtain that $f(x) = (8+4\sqrt{-2})x^4 + 6x^3 + (4+2\sqrt{-2})x^2 + 6x + (2+\sqrt{-2})$ has no proper factorization in $O_K[x]$ and so is irreducible over K. Observe that $f(x)$ is reducible in $O_K[x]$ because $f(x) = (2+\sqrt{-2})\left[4x^4 + (2-\sqrt{-2})x^3 + 2x^2 + (2-\sqrt{-2})x + 1\right]$.

Example 5. *Let $K = \mathbb{Q}(\sqrt{-1})$, $\beta = 15-16i$, $\omega = 3+2i$, and $\pi = -831565 + 715166i$. Then $d = 1$ and thus $\mathcal{C}' = \{0, 1, \ldots, 15\}$. Note that $|\beta| = \sqrt{481} > 2\sqrt{13} + \sqrt{2} = 2|\omega| + \sqrt{1-m}$ and $a = 15 > \sqrt{13} + \sqrt{2} = |\omega| + \sqrt{1-m}$. Since $N(\pi) = 1202962756781$ is a rational prime, we get that π is a Gaussian prime. Now, we have $|\pi| > |\beta|$ and*

$$\omega\pi = -3925027 + 482368i = 17\beta^4 + 3\beta^3 + 7\beta^2 + 5\beta + 13,$$

which is a base-$\beta(\mathcal{C}')$ representation of $\omega\pi$. Moreover, $\mathrm{Re}(\alpha_4) = 17 > 1$ and $\mathrm{Re}(\alpha_3)\,\mathrm{Im}(\alpha_4) = (3)(0) \geq (17)(0) = \mathrm{Re}(\alpha_4)\,\mathrm{Im}(\alpha_3)$. By Theorem 3, we obtain that $f(x) = 17x^4 + 3x^3 + 7x^2 + 5x + 13$ has no proper factorization in $\mathbb{Z}[i][x]$ and so is irreducible over K. Since 3 and 7 are Gaussian primes, it follows that $f(x)$ is irreducible in $\mathbb{Z}[i][x]$.

By taking $\omega \in U(O_K)$ in Theorem 3, we obtain that the polynomial $f(x)$ has no proper factorization in $O_K[x]$. Since π is also an irreducible element, then $\delta \nmid f(x)$ for all $\delta \in O_K \backslash U(O_K)$, by Lemma 4 in [8]. This shows that $f(x)$ is irreducible in $O_K[x]$. Therefore, Theorem 3 is a generalization of Theorem C by considering $\omega\pi$ instead of π, where $\omega \in O_K \backslash \{0\}$ and π is a prime element.

For the case $m \equiv 1 \pmod 4$, we now prove the following.

Theorem 4. *Let $K = \mathbb{Q}(\sqrt{m})$ be an imaginary quadratic field with $m \equiv 1 \pmod 4$. Let $\beta = a + b\sigma_m \in O_K$ and $\omega \in O_K \backslash \{0\}$ be such that $|\beta| \geq 2|\omega| + \sqrt{(9-m)/4}$, $a \geq 1$, and $a + (b/2) \geq |\omega|$. For a prime element π of O_K with $|\pi| > \sqrt{(9-m)/4}\,(|\beta| - 1)$, if*

$$\omega\pi = \alpha_n\beta^n + \alpha_{n-1}\beta^{n-1} + \cdots + \alpha_1\beta + \alpha_0 =: f(\beta)$$

is a base-$\beta(\mathcal{C}')$ representation with $n \geq 2$ and $\mathrm{Re}(\alpha_n) \geq 1$ satisfying the condition (ii) of Lemma 2, then $f(x)$ has no proper factorization in $O_K[x]$. Moreover,

(i) if $\delta \nmid f(x)$ for all $\delta \in O_K \backslash U(O_K)$, then $f(x)$ is irreducible in $O_K[x]$;

(ii) if O_K is a unique factorization domain, then $f(x)$ is irreducible over K.

Proof. Suppose to the contrary that $f(x)$ has proper factorization in $O_K[x]$, namely $f(x) = g(x)h(x)$ for some nonconstant polynomials $g(x)$ and $h(x)$ in $O_K[x]$. By the same proof as in Theorem 3, we have that either $|\omega| \geq |h(\beta)|$ or $|\omega| \geq |g(\beta)|$. Without loss of generality, we may assume that $|\omega| \geq |g(\beta)|$.

Since $\alpha_i \in \mathcal{C}'$ for all $i \in \{0, 1, \ldots, n-1\}$, we have $|\alpha_i| \leq M$ for all $i \in \{0, 1, \ldots, n-1\}$, where M is defined as in (20). We now show that

$$|\beta| - \frac{1 + \sqrt{1 + 4M}}{2} \geq |\omega|. \tag{23}$$

As $|\beta| \geq 2|\omega| + \sqrt{(9-m)/4}$, we have $|\beta|^2 - \left(2|\omega| + 1 + \sqrt{(9-m)/4}\right)|\beta| + 2|\omega| + \sqrt{(9-m)/4} = (|\beta| - 1)\left[|\beta| - \left(2|\omega| + \sqrt{(9-m)/4}\right)\right] \geq 0$. Since $|\omega|^2 + |\omega| \geq 2|\omega|$, it follows that $4\left[|\beta|^2 - \left(2|\omega| + 1 + \sqrt{(9-m)/4}\right)|\beta| + |\omega|^2 + |\omega| + \sqrt{(9-m)/4}\right] \geq 0$ and so $[2|\beta| - (2|\omega| + 1)]^2 = 4|\beta|^2 - 4(2|\omega| + 1)|\beta| + 4|\omega|^2 + 4|\omega| + 1 \geq 1 + 4\sqrt{(9-m)/4}\,(|\beta| - 1)$. Again, $|\beta| \geq 2|\omega| + \sqrt{(9-m)/4}$ shows that $2|\beta| - (2|\omega| + 1) > 0$ and thus, $2|\beta| - (2|\omega| + 1) \geq \sqrt{1 + 4\sqrt{(9-m)/4}\,(|\beta| - 1)}$. Hence,

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

Since $a \geq 1$, it follows from Lemma 4 that $\sqrt{(9-m)/4}\,(|\beta| - 1) \geq M$. Thus,

$$|\beta| \geq \frac{2|\omega| + 1 + \sqrt{1 + 4M}}{2} = |\omega| + \frac{1 + \sqrt{1 + 4M}}{2},$$

which proves (23).

The remaining proof is similar to that of Theorem 3, so we omit it here.

We end this paper with the following examples, illustrating the use of Theorem 4.

Example 6. *Let $K = \mathbb{Q}(\sqrt{-3})$, $\beta = 7 + \sigma_{-3}$, $\omega = 2$, and $\pi = 54343 + 63615\sigma_{-3}$. Then $d = 1$ and thus $\mathcal{C}' = \{0, 1, 2, 3, 4, 5, 6\}$. One can see that $|\beta| = \sqrt{57} > 4 + \sqrt{3} = 2|\omega| + \sqrt{(9 - m)/4}$, $a = 7 > 1$, and $a + (b/2) = 7 + (1/2) > 2 = |\omega|$. Note that O_K is a unique factorization domain and π is a prime element because $N(\pi) = 10457059819$ is a rational prime. Now, we have $|\pi| > \sqrt{(9 - m)/4}\,(|\beta| - 1)$ and*

$$\omega\pi = 108686 + 127230\sigma_{-3} = 8\beta^5 + 2\beta^4 + 4\beta^3 + 2\beta^2 + 6\beta + 2,$$

which is a base-$\beta(\mathcal{C}')$ representation of $\omega\pi$. Moreover, $\mathrm{Re}(\alpha_5) = 8 > 1$ and $\mathrm{Re}(\alpha_4)\,\mathrm{Im}(\alpha_5) = (2)(0) \geq (8)(0) = \mathrm{Re}(\alpha_5)\,\mathrm{Im}(\alpha_4)$. By Theorem 4, we obtain that $f(x) = 8x^5 + 2x^4 + 4x^3 + 2x^2 + 6x + 2$ has no proper factorization in $O_K[x]$ and so is irreducible over K. It is noticed that $f(x)$ is reducible in $O_K[x]$ because $f(x) = 2(4x^5 + x^4 + 2x^3 + x^2 + 3x + 1)$.

Example 7. *Let $K = \mathbb{Q}(\sqrt{-7})$, $\beta = 11 + 3\sigma_{-7}$, $\omega = 2 + \sigma_{-7}$, and $\pi = 158481 + 166844\sigma_{-7}$. Then $d = 1$ and thus $\mathcal{C}' = \{0, 1, \ldots, 10\}$. One can see that $|\beta| = \sqrt{172} > 2\sqrt{8} + 2 = 2|\omega| + \sqrt{(9 - m)/4}$, $a = 11 > 1$, and $a + (b/2) = 11 + (3/2) > \sqrt{8} = |\omega|$. Note that O_K is a unique factorization domain and π is a prime element because $N(\pi) = 107231671997$ is a rational prime. Now, we have $|\pi| > \sqrt{(9 - m)/4}\,(|\beta| - 1)$ and*

$$\omega\pi = -16726 + 659013\sigma_{-7} = 31\beta^4 + 4\beta^3 + 3\beta^2 + 9\beta + 5,$$

which is a base-$\beta(\mathcal{C}')$ representation of $\omega\pi$. Moreover, $\mathrm{Re}(\alpha_4) = 31 > 1$ and $\mathrm{Re}(\alpha_3)\,\mathrm{Im}(\alpha_4) = (4)(0) \geq (31)(0) = \mathrm{Re}(\alpha_4)\,\mathrm{Im}(\alpha_3)$. By Theorem 4, we obtain that $f(x) = 31x^4 + 4x^3 + 3x^2 + 9x + 5$ has no proper factorization in $O_K[x]$ and so is irreducible over K. By Theorem 9.29(3) in [6], one can verify that the rational primes 3, 5, and 31 are prime elements of O_K. This implies that $f(x)$ is irreducible in $O_K[x]$.

By taking $\omega \in U(O_K)$ in Theorem 4, we obtain that the polynomial $f(x)$ has no proper factorization in $O_K[x]$. Since π is also an irreducible element, then $\delta \nmid f(x)$ for all $\delta \in O_K \backslash U(O_K)$, by Lemma 6 in [8]. This shows that $f(x)$ is irreducible in $O_K[x]$. Therefore, Theorem 4 is a generalization of Theorem D by considering $\omega\pi$ instead of π, where $\omega \in O_K \backslash \{0\}$ and π is a prime element.

4. Conclusion

For any imaginary quadratic field K, we provide the explicit shapes of all base-$\beta(\mathcal{C})$ representations for nonzero elements of O_K. Using such a representation, irreducibility criteria for polynomials in $O_K[x]$ are established, which extend and generalize the authors' earlier work.

Acknowledgements

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

References

[1] S Alaca and K S Williams. *Introductory Algebraic Number Theory.* Cambridge University Press, Cambridge, 2004.

[2] J Brillhart, M Filaseta, and A Odlyzko. On an irreducibility theorem of A Cohn. *Canadian Journal of Mathematics*, 33(5):1055–1059, 1981.

[3] M Filaseta. A further generalization of an irreducibility theorem of A Cohn. *Canadian Journal of Mathematics*, 34(6):1390–1395, 1982.

[4] N R Kanasri, P Singthongla, and V Laohakosol. Irreducibility criteria for polynomials over some imaginary quadratic fields. *Southeast Asian Bulletin of Mathematics*, 43(1):367–376, 2019.

[5] M R Murty. Prime numbers and irreducible polynomials. *The American Mathematical Monthly*, 109(5):452–458, 2002.

[6] I Niven, H S Zuckerman, and H L Montgomery. *An Introduction to the Theory of Numbers. 5th ed.* Wiley, New York, 1991.

[7] P Phetnun and N R Kanasri. Further irreducibility criteria for polynomials associated with the complete residue systems in any imaginary quadratic field. *AIMS Mathematics*, 7(10):18925–18947, 2022.

[8] P Phetnun, N R Kanasri, and P Singthongla. On the irreducibility of polynomials associated with the complete residue systems in any imaginary quadratic fields. *International Journal of Mathematics and Mathematical Sciences*, 2021:17 pages, 2021.

[9] H Pollard and H G Diamond. *The Theory of Algebraic Numbers.* Cambridge University Press, Cambridge, 1975.

[10] G Pólya and G Szegö. *Problems and Theorems in Analysis.* Springer-Verlag, New York, 1976.

[11] K H Rosen. *Elementary Number Theory and Its Applications. 5th ed.* Addison-Wesley, New York, 2005.

[12] P Singthongla, N R Kanasri, and V Laohakosol. Prime elements and irreducible polynomials over some imaginary quadratic fields. *Kyungpook Mathematical Journal*, 57(4):581–600, 2017.

[13] S Tadee, V Laohakosol, and S Damkaew. Explicit complete residue systems in a general quadratic field. *Divulgaciones matemáticas*, 18(2):1–17, 2017.