KYUNGPOOK Math. J. 57(2017), 581-600
https://doi.org/10.5666/KMJ.2017.57.4.581
pISSN 1225-6951 eISSN 0454-8124

Prime Elements and Irreducible Polynomials over Some Imaginary Quadratic Fields

Patiwat Singthongla and Narakorn Rompurk Kanasri*
Department of Mathematics, Khon Kaen University, Khon Kaen 40002, Thailand
e-mail : thepativat@gmail.com *and* naraka@kku.ac.th

Vichian Laohakosol
Department of Mathematics, Kasetsart University, Bangkok 10900, Thailand
e-mail : fscivil@ku.ac.th

Abstract. A classical result of A. Cohn states that, if we express a prime p in base 10 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 problem was subsequently generalized to any base b by Brillhart, Filaseta, and Odlyzko. We establish this result of A. Cohn in $O_K[x]$, K an imaginary quadratic field such that its ring of integers, O_K, is a Euclidean domain. For a Gaussian integer β with $|\beta| > 1 + \sqrt{2}/2$, we give another representation for any Gaussian integer using a complete residue system modulo β, and then establish an irreducibility criterion in $\mathbb{Z}[i][x]$ by applying this result.

1. Introduction

A classical result of A. Cohn [7] states that, if we express a prime p in base 10 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 problem was subsequently generalized to any base b by Brillhart, Filaseta, and Odlyzko [2]. In 2002, Murty gave a proof of this fact [5] that was conceptually simpler than the one in [2]. Later, Girstmair obtained an easy but useful generalization

* Corresponding Author.
Received March 8, 2017; revised August 1, 2017; accepted November 17, 2017.
2010 Mathematics Subject Classification: 11R04, 11R09.
Key words and phrases: imaginary quadratic field, ring of integers, Gaussian integer, complete residue system, irreducible polynomial.
The corresponding author is supported by the Research and Academic Affairs Promotion Fund, Faculty of Science, Khon Kaen University, Fiscal year 2017 (RAAPF) and the third author is supported by the Center for Advanced Studies in Industrial Technology and the Faculty of Science, Kasetsart University, Thailand.

of Murty's result [4]. In addition, Brillhart, Filaseta, and Odlyzko [2] generalized Cohn's result in another direction by proving that, if $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$, where $0 \le a_i \le 167$ for all i, and if $f(10)$ is prime, then $f(x)$ is irreducible. In 1988, Filaseta improved this fact by proving that, if $f(x) = \sum_{i=0}^{n} a_i x^i$ is a polynomial in $\mathbb{Z}[x]$ such that $0 \le a_i \le a_n 10^{30}$ for $0 \le i \le n-1$, and if $f(10)$ is prime, then $f(x)$ is irreducible [3].

In another direction, let K be an imaginary quadratic field and O_K the ring of integers of K. We are interested in constructing a base β representation in O_K. We prove that for fixed $\beta \in O_K \backslash \{0\}$, any algebraic integer η has a base β representation by using the division algorithm in O_K. Henceforth, the ring of integers O_K in this paper must be a Euclidean domain. Thus, O_K is a unique factorization domain and so is $O_K[x]$. We know that K is the quotient field of O_K [1] and the units in $O_K[x]$ are the units in O_K [6]. We say that a non-zero polynomial $p(x) \in O_K[x]$ is *irreducible* if $p(x)$ is not a unit and if $p(x) = f(x)g(x)$ with $f(x), g(x)$ in $O_K[x]$, then $f(x)$ or $g(x)$ is a unit in O_K. For a unique factorization domain (UFD) R, a polynomial $f(x) \in R[x]$ is *primitive* if its coefficients are relatively prime, equivalently, no irreducible element of R divides every coefficient of $f(x)$. Gauss's lemma for unique factorization domain states that if R is a unique factorization domain, then the product of primitive polynomials in $R[x]$ is primitive. If F is the quotient field of R and $p(x) \in R[x] \backslash R$, then $p(x)$ is irreducible in $R[x]$ if and only if $p(x)$ is primitive and irreducible over F [8]. From this fact, we get that a non-constant polynomial in $O_K[x]$ is irreducible in $O_K[x]$ if and only if it is both irreducible over K and primitive in $O_K[x]$. Consequently, to prove that a polynomial f in $O_K[x]$ is irreducible over K, it suffices to prove that f is irreducible in $O_K[x]$.

In the present work, we establish the result of A. Cohn in $O_K[x]$ by using base β representation in O_K. In addition, another base β representation in the ring of Gaussian integers, $\mathbb{Z}[i]$, is also constructed using a complete residue system modulo $\beta \in \mathbb{Z}[i]$. Applying this result, we establish an irreducibility criterion in $\mathbb{Z}[i][x]$ and then show that the generalized result of A. Cohn in [2], for prime numbers in $\mathbb{Z}$ that remain prime in $\mathbb{Z}[i]$, can be deduced from our results.

2. Basic Results

In this section, we give some definition, notation and results to be used throughout.

Let $m \in \mathbb{Z}$ be square-free. The function $\phi_m : \mathbb{Q}(\sqrt{m}) \to \mathbb{Q}$ ([1]) defined by

$$\phi_m(r + s\sqrt{m}) = |r^2 - ms^2| \qquad (r, s \in \mathbb{Q})$$

possesses the following properties.

(O1) $\phi_m(\alpha) \in \mathbb{N} \cup \{0\}$ for all $\alpha \in O_{\mathbb{Q}(\sqrt{m})}$.

(O2) For $\alpha \in \mathbb{Q}(\sqrt{m}), \phi_m(\alpha) = 0 \Leftrightarrow \alpha = 0$.

(O3) $\phi_m(\alpha\beta) = \phi_m(\alpha)\phi_m(\beta)$ for all $\alpha, \beta \in \mathbb{Q}(\sqrt{m})$.

(O4) If $m < 0$, then $|\alpha|^2 = \phi_m(\alpha)$ for all $\alpha \in \mathbb{Q}(\sqrt{m})$.

Theorem 2.1.([1]) *Let $m < 0$ be square-free. Then $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ is a Euclidean domain with respect to ϕ_m if and only if $m = -1, -2$.*

Theorem 2.2.([1]) *Let $m < 0$ be square-free with $m \equiv 1 \pmod 4$. Then $\mathbb{Z} + \mathbb{Z}\left((1+\sqrt{m})/2\right)$ is a Euclidean domain with respect to ϕ_m if and only if $m = -3, -7, -11$.*

Proposition 2.3. *Let $K = \mathbb{Q}(\sqrt{m})$ be an imaginary quadratic field such that O_K is a Euclidean domain. For $\alpha \in O_K$, we have*

(1) *$\alpha \in U\left(O_K\right)$ if and only if $\phi_m(\alpha) = 1$.*

(2) *If $\phi_m(\alpha) = p$, a rational prime, then α is a prime element in O_K.*

Proof. (1) If $\alpha \in U\left(O_K\right)$, we clearly have $\phi_m(\alpha) = 1$. Conversely, assume that $\phi_m(\alpha) = 1$. Since O_K is a Euclidean domain, there exist $\lambda, \rho \in O_K$ such that $1 = \alpha\lambda + \rho$, where $0 \le \phi_m(\rho) < \phi_m(\alpha) = 1$. It follows from (O2) that $\rho = 0$ and so $\alpha \in U\left(O_K\right)$.

(2) Assume that $\phi_m(\alpha) = p$, a rational prime. If $\alpha = \beta\gamma$ for some $\beta, \gamma \in O_K$, then $p = \phi_m(\alpha) = \phi_m(\beta)\phi_m(\gamma)$, which implies by (O1) that either $\phi_m(\beta) = 1$ or $\phi_m(\gamma) = 1$. Using (1), $\beta \in U\left(O_K\right)$ or $\gamma \in U\left(O_K\right)$. This shows that α is an irreducible element and so α is prime element in O_K, because O_K is a unique factorization domain. $\square$

3. Main Results

Let $K = \mathbb{Q}(\sqrt{m})$ be an imaginary quadratic field such that its ring of integers O_K is a Euclidean domain. By Theorems 2.1 and 2.2, we know that $m = -1, -2, -3, -7$, or -11. Our first objective is to establish the result of A. Cohn to $O_K[x]$. Let us first prove that for fixed $\beta \in O_K \backslash \{0\}$, any algebraic integer η has a base β representation.

Recall the following result [9], which is the division algorithm for Gaussian integers. Its proof is also valid for the case $m = -2$.

Proposition 3.1. *Let $K = \mathbb{Q}(\sqrt{m})$, where $m = -1, -2$ and let $\beta \in O_K \backslash \{0\}$ be fixed. For $\alpha \in O_K$, there exist $\lambda, \rho \in O_K$ such that $\alpha = \lambda\beta + \rho$, with $0 \le |\rho| \le (\sqrt{1-m}/2)|\beta|$.*

Proof. Suppose that $\alpha/\beta = r + s\sqrt{m}$, where $r, s \in \mathbb{Q}$. It is clear that $r, s \in \mathbb{Z}$ if and only if β divides α. Let

$$a = \left\lfloor r + \frac{1}{2} \right\rfloor \quad \text{and} \quad b = \left\lfloor s + \frac{1}{2} \right\rfloor . \tag{3.1}$$

Then $|r - a| \le 1/2$ and $|s - b| \le 1/2$. Now, let $\lambda = a + b\sqrt{m}$ and $\rho = \alpha - \lambda\beta$. Then

$\lambda, \rho \in O_K$, $\alpha = \lambda\beta + \rho$, and so

$$\begin{aligned} 0 \le |\rho| &= |\beta| \left| \frac{\alpha}{\beta} - \lambda \right| \\ &= |\beta| \left| (r-a) + (s-b)\sqrt{m} \right| \\ &= |\beta| \sqrt{(r-a)^2 - m(s-b)^2} \\ &\le \frac{\sqrt{1-m}}{2} |\beta| . \end{aligned}$$ □

The division algorithm for the cases $m = -3, -7, -11$ is as follows:

Proposition 3.2. *Let $K = \mathbb{Q}(\sqrt{m})$, where $m = -3, -7$ or -11 and let $\beta \in O_K\backslash\{0\}$ be fixed. For $\alpha \in O_K$, there exist $\lambda, \rho \in O_K$ such that $\alpha = \lambda\beta + \rho$, with $0 \le |\rho| \le (\sqrt{4-m}/4)|\beta|$.*

Proof. Suppose that $\alpha/\beta = r + s\sqrt{m}$, where $r, s \in \mathbb{Q}$. Let

$$a = \left\lfloor 2s + \frac{1}{2} \right\rfloor \quad \text{and} \quad b = \left\lfloor r - \frac{a}{2} + \frac{1}{2} \right\rfloor . \tag{3.2}$$

It follows that $|2s - a| \le 1/2$ and $|r - a/2 - b| \le 1/2$. Now, let $\lambda = b + a(1+\sqrt{m})/2$ and $\rho = \alpha - \lambda\beta$. Then $\lambda, \rho \in O_K$, $\alpha = \lambda\beta + \rho$, and so

$$\begin{aligned} 0 \le |\rho| &= |\beta| \left| \frac{\alpha}{\beta} - \lambda \right| \\ &= |\beta| \left| \left(r - \frac{a}{2} - b\right) + \left(s - \frac{a}{2}\right)\sqrt{m} \right| \\ &= |\beta| \sqrt{\left(r - \frac{a}{2} - b\right)^2 - m\left(s - \frac{a}{2}\right)^2} \\ &\le \frac{\sqrt{4-m}}{4} |\beta| . \end{aligned}$$ □

The following two theorems show that for fixed $\beta \in O_K$, any $\eta \in O_K\backslash\{0\}$ has a *base β representation*.

Theorem 3.3. *Let $K = \mathbb{Q}(\sqrt{m})$, where $m = -1, -2$. Let $\beta \in O_K$ be such that $|\beta| > 1 + \sqrt{1-m}/2$. Then any $\eta \in O_K\backslash\{0\}$ can be written as*

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

where $n \ge 0$, $\alpha_i \in O_K$ $(0 \le i \le n)$, $\alpha_n \ne 0, |\alpha_n| < |\beta|$, and $0 \le |\alpha_i| \le (\sqrt{1-m}/2)|\beta| \quad (0 \le i \le n-1)$.

Proof. If $|\eta| < |\beta|$, then $\eta = 0 \cdot \beta + \eta$ and we are done. Now we assume that $|\eta| \ge |\beta|$. By Proposition 3.1, we obtain

$$\eta = \delta_0\beta + \alpha_0,\ 0 \le |\alpha_0| \le \frac{\sqrt{1-m}}{2}|\beta|. \tag{3.3}$$

We claim that $|\eta| > |\delta_0|$. For if $|\delta_0| \geq |\eta|$, then $|\delta_0| \geq |\delta_0\beta + \alpha_0| \geq |\delta_0||\beta| - |\alpha_0|$ and so

$$|\alpha_0| \geq |\delta_0|\,(|\beta| - 1)\,. \tag{3.4}$$

Using (3.3), (3.4) and $|\beta| > 1 + \sqrt{1-m}/2$, we obtain

$$|\delta_0| \geq |\eta| \geq |\beta| \geq \frac{2}{\sqrt{1-m}}|\alpha_0| \geq \frac{2}{\sqrt{1-m}}|\delta_0|\,(|\beta| - 1) > |\delta_0|,$$

which is a contradiction.

Returning to (3.3), if $|\delta_0| < |\beta|$, then we are done, while, if $|\delta_0| \geq |\beta|$, then we continue by dividing δ_0 by β and using the last claim to get

$$\delta_0 = \delta_1\beta + \alpha_1,\ 0 \leq |\alpha_1| \leq \frac{\sqrt{1-m}}{2}|\beta| \text{ and } |\delta_0| > |\delta_1|.$$

Continue this process to obtain

$$\begin{aligned}
&\delta_1 = \delta_2\beta + \alpha_2,\ 0 \leq |\alpha_2| \leq \frac{\sqrt{1-m}}{2}|\beta| \ \text{ and } \ |\delta_1| > |\delta_2|,\\
&\quad\vdots\\
&\delta_{n-2} = \delta_{n-1}\beta + \alpha_{n-1},\ 0 \leq |\alpha_{n-1}| \leq \frac{\sqrt{1-m}}{2}|\beta| \ \text{ and } \ |\delta_{n-2}| > |\delta_{n-1}|,\\
&\delta_{n-1} = 0\cdot\beta + \alpha_n,\ |\alpha_n| = |\delta_{n-1}| < |\beta| \ \text{ and } \ |\delta_{n-1}| > |\delta_n| = 0.
\end{aligned}$$

The last step occurs when a quotient, 0 is obtained because

$$|\eta|^2 > |\delta_0|^2 > |\delta_1|^2 > |\delta_2|^2 > \cdots \geq 0,$$

i.e. $(|\delta_k|^2)_{k\geq 0}$ is a decreasing sequence of non-negative integers.

Replacing δ_0 in (3.3), we get

$$\eta = (\delta_1\beta + \alpha_1)\beta + \alpha_0 = \delta_1\beta^2 + \alpha_1\beta + \alpha_0.$$

Successively substituting for $\delta_1, \delta_2, \ldots, \delta_{n-1}$, we obtain

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

where $\alpha_n = \delta_{n-1} \neq 0, |\alpha_n| < |\beta|$, and $0 \leq |\alpha_i| \leq (\sqrt{1-m}/2)|\beta|$ for all $i \in \{0, 1, \ldots, n-1\}$. $\square$

Similar to the cases $m = -1, -2$, we have:

Theorem 3.4. *Let $K = \mathbb{Q}(\sqrt{m})$, where $m = -3, -7$ or -11 and let $\beta \in O_K$ be fixed with $|\beta| > 1 + \sqrt{4-m}/4$. Then any $\eta \in O_K\backslash\{0\}$ has a base β representation in the form*

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

where $n \geq 0$, $\alpha_i \in O_K$ $(0 \leq i \leq n)$, $\alpha_n \neq 0$, $|\alpha_n| < |\beta|$ *and* $0 \leq |\alpha_i| \leq (\sqrt{4-m}/4)|\beta| \quad (0 \leq i \leq n-1)$.

Note that a base β representation in O_K is not unique. For example,

$$33 + 100i = (-3 - i)\beta^2 + (-2 - 2i)\beta + (-1 - 2i),$$

$$33 + 100i = -3\beta^2 + (3 + 2i)\beta + (4 + i)$$

are two base β representations of $33 + 100i$ in $\mathbb{Z}[i]$ when $\beta = -3 + 5i$.

To establish the result of A. Cohn in $O_K[x]$, we prove the following lemma.

Lemma 3.5. *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) $\mathrm{Re}(\alpha_n) \geq 1, \mathrm{Re}(\alpha_{n-1}) \geq 0, \mathrm{Im}(\alpha_{n-1}) \geq 0$ *and*

(ii) $\mathrm{Re}(\alpha_{n-1})\,\mathrm{Im}(\alpha_n) \geq \mathrm{Re}(\alpha_n)\,\mathrm{Im}(\alpha_{n-1})$,

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

Proof. Let $\alpha = a + bi$ be any complex zero of $f(x)$. If $|\alpha| \leq 1$, then $|\alpha| < (1 + \sqrt{1+4M})/2$. Now we assume that $|\alpha| > 1$ and $a = \mathrm{Re}(\alpha) \geq 0$. Then

$$\left|\frac{f(\alpha)}{\alpha^n}\right| + \left|\frac{\alpha_{n-2}}{\alpha^2}\right| + \cdots + \left|\frac{\alpha_0}{\alpha^n}\right| \geq \left|\frac{f(\alpha)}{\alpha^n} - \Big(\frac{\alpha_{n-2}}{\alpha^2} + \cdots + \frac{\alpha_0}{\alpha^n}\Big)\right|.$$

Since $|\alpha_i| \leq M$ $(0 \leq i \leq n-2)$, we have

$$\left|\frac{f(\alpha)}{\alpha^n}\right| + \frac{M}{|\alpha|^2 - |\alpha|} > \left|\frac{f(\alpha)}{\alpha^n} - \Big(\frac{\alpha_{n-2}}{\alpha^2} + \cdots + \frac{\alpha_0}{\alpha^n}\Big)\right|$$

so that

$$\left|\frac{f(\alpha)}{\alpha^n}\right| > \left|\alpha_n + \frac{\alpha_{n-1}}{\alpha}\right| - \frac{M}{|\alpha|^2 - |\alpha|}. \tag{3.5}$$

Next, we will show that

$$\left|\alpha_n + \frac{\alpha_{n-1}}{\alpha}\right| \geq 1. \tag{3.6}$$

For convenience, we set

$$\alpha_n = a_n + b_n i \ \text{ and } \ \alpha_{n-1} = a_{n-1} + b_{n-1}i, \ i = \sqrt{-1}.$$

If $b = \mathrm{Im}(\alpha) \geq 0$, then by condition (i) and $a \geq 0$, we obtain

$$\begin{aligned}\left|\alpha_n + \frac{\alpha_{n-1}}{\alpha}\right| &\geq \mathrm{Re}\left(\alpha_n + \frac{\alpha_{n-1}}{\alpha}\right), \\ &= a_n + \frac{1}{|\alpha|^2}\left(a_{n-1}a + b_{n-1}b\right), \\ &\geq a_n \geq 1.\end{aligned}$$

Now, assume that $b < 0$. Then

$$\begin{aligned}\left|\alpha_n + \frac{\alpha_{n-1}}{\alpha}\right|^2 &= \left(\mathrm{Re}(\alpha_n) + \mathrm{Re}\left(\frac{\alpha_{n-1}}{\alpha}\right)\right)^2 + \left(\mathrm{Im}(\alpha_n) + \mathrm{Im}\left(\frac{\alpha_{n-1}}{\alpha}\right)\right)^2, \\ &\geq 1 + 2a_n \,\mathrm{Re}\left(\frac{\alpha_{n-1}}{\alpha}\right) + 2b_n \,\mathrm{Im}\left(\frac{\alpha_{n-1}}{\alpha}\right), \\ &= 1 + \frac{2a_n}{|\alpha|^2}\left(a_{n-1}a + b_{n-1}b\right) + \frac{2b_n}{|\alpha|^2}\left(b_{n-1}a - a_{n-1}b\right).\end{aligned}$$

If $b_n < 0$, then condition (ii) implies $a_{n-1} = b_{n-1} = 0$ so that $|\alpha_n + \alpha_{n-1}/\alpha|^2 \geq 1$. If $b_n \geq 0$, then using conditions (i), (ii) and $a \geq 0$, we get

$$\begin{aligned}\left|\alpha_n + \frac{\alpha_{n-1}}{\alpha}\right|^2 &\geq 1 + \frac{2a_n}{|\alpha|^2} b_{n-1}b - \frac{2b_n}{|\alpha|^2} a_{n-1}b, \\ &= 1 + \frac{2(-b)}{|\alpha|^2}\left(a_{n-1}b_n - a_n b_{n-1}\right) \geq 1\end{aligned}$$

so that $|\alpha_n + \alpha_{n-1}/\alpha| \geq 1$. Thus, by (3.5) and (3.6), we deduce that

$$\left|\frac{f(\alpha)}{\alpha^n}\right| > 1 - \frac{M}{|\alpha|^2 - |\alpha|} = \frac{|\alpha|^2 - |\alpha| - M}{|\alpha|^2 - |\alpha|}.$$

Since $f(\alpha) = 0$ and $|\alpha| > 1$, we obtain

$$|\alpha| < \frac{1 + \sqrt{1 + 4M}}{2},$$

as desired. □

The following five theorems are our first main results.

Theorem 3.6. *Let $\beta \in \mathbb{Z}[i]$ be such that $|\beta| \geq (6 + \sqrt{2} + \sqrt{6 + 12\sqrt{2}})/4 \approx 3.05$ and $\mathrm{Re}(\beta) \geq 1$. For a Gaussian prime π, if*

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

is its base β representation with $n \geq 1$, satisfying the conditions (i) and (ii) of Lemma 3.5, then $f(x) = \alpha_n x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0$ is irreducible in $\mathbb{Z}[i][x]$.

Proof. Clearly, $f(x)$ is irreducible if $\deg f(x) = 1$. Now we suppose that $\deg f(x) \geq 2$ and $f(x)$ is reducible in $\mathbb{Z}[i][x]$. Then we have $f(x) = g(x)h(x)$ for some non-constant polynomials $g(x)$ and $h(x)$ in $\mathbb{Z}[i][x]$ and so $\pi = g(\beta)h(\beta)$. Since π is a Gaussian prime, 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 suppose that $|g(\beta)| = 1$.

Since $|\beta| \geq (6 + \sqrt{2} + \sqrt{6 + 12\sqrt{2}})/4$, we have

$$|\beta|^2 - 2\left(\frac{6+\sqrt{2}}{4}\right)|\beta| + \left(\frac{6+\sqrt{2}}{4}\right)^2 - \left(\frac{6+\sqrt{2}}{4}\right)^2 + 2 \geq 0$$

and so $4|\beta|^2 - 2\left(6 + \sqrt{2}\right)|\beta| + 8 \geq 0$. Thus $(2|\beta| - 3)^2 = 4|\beta|^2 - 12|\beta| + 9 \geq 1 + 2\sqrt{2}|\beta|$. It follows that

$$|\beta| - \frac{1 + \sqrt{1 + 2\sqrt{2}|\beta|}}{2} \geq 1. \tag{3.7}$$

Since $\deg g(x) \geq 1$, we can express $g(x)$ in the form

$$g(x) = \epsilon \prod_i (x - \gamma_i),$$

where ϵ is the leading coefficient of $g(x)$ and the product is over the set of complex zeros of $g(x)$. By Theorem 3.3, we have $|\alpha_i| \leq (\sqrt{2}/2)|\beta|$ for all $i \in \{0, 1, \ldots, n-1\}$. It follows by Lemma 3.5 that any zero γ of $g(x)$ satisfies either $\mathrm{Re}(\gamma) < 0$ or

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

In the former case, since $\mathrm{Re}(\beta) \geq 1$, we have $|\beta - \gamma| \geq \mathrm{Re}(\beta - \gamma) = \mathrm{Re}(\beta) - \mathrm{Re}(\gamma) > 1$. In the latter case, we have

$$|\beta - \gamma| \geq |\beta| - |\gamma| > |\beta| - \frac{1 + \sqrt{1 + 2\sqrt{2}|\beta|}}{2} \geq 1,$$

by (3.7). It follows that

$$1 = |g(\beta)| = |\epsilon| \prod_i |\beta - \gamma_i| \geq \prod_i |\beta - \gamma_i| > 1,$$

which is a contradiction. □

Example 3.7. Let $\beta = 4 - i$ and $\pi = 230 + i$. Since $\phi_{-1}(230 + i) = 52901$ is a rational prime, $230 + i$ is a Gaussian prime by Proposition 2.3 (2). Since

$$230 + i = (2 + 2i)(4 - i)^3 + 2(4 - i)^2 + 2i(4 - i) - i,$$

the polynomial $f(x) = (2+2i)x^3 + 2x^2 + 2ix - i$ is irreducible in $\mathbb{Z}[i][x]$, by Theorem 3.6.

Theorem 3.8. *Let $\beta \in \mathbb{Z} + \mathbb{Z}\sqrt{-2}$ be such that $\mathrm{Re}(\beta) \geq 1$ and $|\beta| \geq (6 + \sqrt{3} + \sqrt{7 + 12\sqrt{3}})/4 \approx 3.2508$. For a prime element π in $\mathbb{Z} + \mathbb{Z}\sqrt{-2}$, if*

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

is its base β representation with $n \geq 1$, satisfying the conditions (i) and (ii) of Lemma 3.5, then $f(x) = \alpha_n x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0$ is irreducible in $\left(\mathbb{Z} + \mathbb{Z}\sqrt{-2}\right)[x]$.

Proof. The proof is similar to that of Theorem 3.6, and so we merely mention the crucial step. Since $|\beta| \geq (6 + \sqrt{3} + \sqrt{7 + 12\sqrt{3}})/4$, we have

$$|\beta|^2 - 2\left(\frac{6+\sqrt{3}}{4}\right)|\beta| + \left(\frac{6+\sqrt{3}}{4}\right)^2 - \left(\frac{6+\sqrt{3}}{4}\right)^2 + 2 \geq 0,$$

and so $4|\beta|^2 - 2\left(6 + \sqrt{3}\right)|\beta| + 8 \geq 0$. Thus, $(2|\beta| - 3)^2 = 4|\beta|^2 - 12|\beta| + 9 \geq 1 + 2\sqrt{3}|\beta|$. It follows that

$$|\beta| - \frac{1 + \sqrt{1 + 2\sqrt{3}|\beta|}}{2} \geq 1. \qquad \square$$

Theorem 3.9. *Let $\beta \in \mathbb{Z} + \mathbb{Z}\left(\left(1 + \sqrt{-3}\right)/2\right)$ be such that $\mathrm{Re}(\beta) \geq 1$ and $|\beta| \geq (12 + \sqrt{7} + \sqrt{23 + 24\sqrt{7}})/8 \approx 2.99327$. For a prime element π in $\beta \in \mathbb{Z} + \mathbb{Z}\left(\left(1 + \sqrt{-3}\right)/2\right)$, if*

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

is its base β representation with $n \geq 1$, satisfying the conditions (i) and (ii) of Lemma 3.5, then $f(x) = \alpha_n x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0$ is irreducible in $\left(\mathbb{Z} + \mathbb{Z}\left(\left(1 + \sqrt{-3}\right)/2\right)\right)[x]$.

Proof. Since $|\beta| \geq (12 + \sqrt{7} + \sqrt{23 + 24\sqrt{7}})/8$, we have

$$|\beta|^2 - 2\left(\frac{12+\sqrt{7}}{8}\right)|\beta| + \left(\frac{12+\sqrt{7}}{8}\right)^2 - \left(\frac{12+\sqrt{7}}{8}\right)^2 + 2 \geq 0$$

and so $4|\beta|^2 - \left(12 + \sqrt{7}\right)|\beta| + 8 \geq 0$. Thus $(2|\beta| - 3)^2 = 4|\beta|^2 - 12|\beta| + 9 \geq 1 + \sqrt{7}|\beta|$. It follows that

$$|\beta| - \frac{1 + \sqrt{1 + \sqrt{7}|\beta|}}{2} \geq 1. \qquad \square$$

Example 3.10. Let $\beta = 4$ and $\pi = 69 + \left(1+\sqrt{-3}\right)/2$. Since $\phi_{-3}\left(69+(1+\sqrt{-3})/2\right) = 4831$ is a rational prime, by Proposition 2.3 (2), π is a prime element in $\mathbb{Z}+\mathbb{Z}\left(\left(1+\sqrt{-3}\right)/2\right)$. Since

$$69 + \frac{1+\sqrt{-3}}{2} = 4^3 + 4 + \frac{3+\sqrt{-3}}{2},$$

the polynomial $f(x) = x^3 + x + \left(3+\sqrt{-3}\right)/2$ is irreducible in $\left(\mathbb{Z}+\mathbb{Z}((1+\sqrt{-3})/2)\right)[x]$, by Theorem 3.9.

Theorem 3.11. *Let $\beta \in \mathbb{Z}+\mathbb{Z}\left(\left(1+\sqrt{-7}\right)/2\right)$ be such that $\mathrm{Re}(\beta) \geq 1$ and $|\beta| \geq (12+\sqrt{11}+\sqrt{27+24\sqrt{11}})/8 \approx 3.20516$. For a prime element π in $\mathbb{Z}+\mathbb{Z}\left(\left(1+\sqrt{-7}\right)/2\right)$, if*

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

is its base β representation with $n \geq 1$ satisfying the conditions (i) and (ii) of Lemma 3.5, then $f(x) = \alpha_n x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0$ is irreducible in $\left(\mathbb{Z}+\mathbb{Z}\left(\left(1+\sqrt{-7}\right)/2\right)\right)[x]$.

Proof. Since $|\beta| \geq (12+\sqrt{11}+\sqrt{27+24\sqrt{11}})/8$, we have

$$|\beta|^2 - 2\left(\frac{12+\sqrt{11}}{8}\right)|\beta| + \left(\frac{12+\sqrt{11}}{8}\right)^2 - \left(\frac{12+\sqrt{11}}{8}\right)^2 + 2 \geq 0$$

and so $4|\beta|^2 - \left(12+\sqrt{11}\right)|\beta| + 8 \geq 0$. Thus $(2|\beta|-3)^2 = 4|\beta|^2 - 12|\beta| + 9 \geq 1 + \sqrt{11}|\beta|$. It follows that

$$|\beta| - \frac{1+\sqrt{1+\sqrt{11}|\beta|}}{2} \geq 1. \qquad \square$$

Theorem 3.12. *Let $\beta \in \mathbb{Z}+\mathbb{Z}\left(\left(1+\sqrt{-11}\right)/2\right)$ be such that $\mathrm{Re}(\beta) \geq 1$ and $|\beta| \geq (12+\sqrt{15}+\sqrt{31+24\sqrt{15}})/8 \approx 3.37579$. For a prime element π in $\mathbb{Z}+\mathbb{Z}\left(\left(1+\sqrt{-11}\right)/2\right)$, if*

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

is its base β representation with $n \geq 1$ satisfying the conditions (i) and (ii) of Lemma 3.5, then $f(x) = \alpha_n x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0$ is irreducible in $\left(\mathbb{Z}+\mathbb{Z}\left(\left(1+\sqrt{-11}\right)/2\right)\right)[x]$.

Proof. Since $|\beta| \geq (12+\sqrt{15}+\sqrt{31+24\sqrt{15}})/8$, we have

$$|\beta|^2 - 2\left(\frac{12+\sqrt{15}}{8}\right)|\beta| + \left(\frac{12+\sqrt{15}}{8}\right)^2 - \left(\frac{12+\sqrt{15}}{8}\right)^2 + 2 \geq 0$$

and so $4|\beta|^2 - \left(12+\sqrt{15}\right)|\beta| + 8 \geq 0$. Thus $(2|\beta|-3)^2 = 4|\beta|^2 - 12|\beta| + 9 \geq 1 + \sqrt{15}|\beta|$. It follows that

$$|\beta| - \frac{1+\sqrt{1+\sqrt{15}|\beta|}}{2} \geq 1. \qquad \square$$

For the second part of this work, we establish an irreducibility criterion in $\mathbb{Z}[i][x]$ by using a complete residue system for Gaussian integers.We first recall the definition of congruence and a complete residue system for Gaussian integers.

Definition 3.13.([9]) Let α, β and γ be Gaussian integers such that $\gamma \neq 0$. We say that α is *congruent* to β modulo γ and we write $\alpha \equiv \beta \pmod{\gamma}$ if $\gamma \mid (\alpha - \beta)$.

Definition 3.14.([9]) A *complete residue system modulo* γ, where γ is a non-zero Gaussian integer, is a set of Gaussian integers such that every Gaussian integer is congruent modulo γ to exactly one element of this set.

Example 3.15.([9]) For a Gaussian integer $\gamma = a + bi$ with $d = \gcd(a, b)$, the set

$$\mathcal{C} := \left\{ x + yi \mid x = 0, 1, \ldots, \frac{a^2+b^2}{d} - 1 \text{ and } y = 0, 1, \ldots, d-1 \right\} \tag{3.8}$$

is a complete residue system modulo γ.

By using (3.8), we prove in the following proposition that for fixed a Gaussian integer β with $|\beta| > 1 + 1/\sqrt{2}$, any Gaussian integer η can be written under a *base* $\beta(\mathcal{C})$ *representation*.

Proposition 3.16. *Let $\beta = a + bi \in \mathbb{Z}[i]$ be such that $|\beta| > 1 + 1/\sqrt{2}$. Then any $\eta \in \mathbb{Z}[i]\backslash\{0\}$ can be written as a base $\beta(\mathcal{C})$ representation in the form*

$$\eta = \gamma_n \beta^n + \gamma_{n-1}\beta^{n-1} + \cdots + \gamma_1 \beta + \gamma_0,$$

where $n \geq 0, \gamma_n \in \mathbb{Z}[i]\backslash\{0\}$, and $\gamma_i \in \mathcal{C}$ $(0 \leq i \leq n-1)$.

Proof. If $|\eta| < |\beta|$, then $\eta = \eta \cdot \beta^0$ and so we are done. Assume that $|\eta| \geq |\beta|$. By Theorem 3.3, η can be written as base β representation in the form

$$\eta = \alpha_k \beta^k + \alpha_{k-1}\beta^{k-1} + \cdots + \alpha_1 \beta + \alpha_0.$$

By Definition 3.14 and Example 3.15, there exists $\gamma_0 \in \mathcal{C}$ such that $\alpha_0 \equiv \gamma_0 \pmod{\beta}$ and so $\alpha_0 = \gamma_0 + \delta_0 \beta$ for some $\delta_0 \in \mathbb{Z}[i]$. It follows that

$$\eta = \alpha_k \beta^k + \cdots + (\alpha_1 + \delta_0)\beta + \gamma_0.$$

As there exists $\gamma_1 \in \mathcal{C}$ such that $\alpha_1 + \delta_0 \equiv \gamma_1 \pmod{\beta}$, we have $\alpha_1 + \delta_0 = \gamma_1 + \delta_1 \beta$ for some $\delta_1 \in \mathbb{Z}[i]$, and so

$$\eta = \alpha_k \beta^k + \cdots + (\alpha_2 + \delta_1)\beta^2 + \gamma_1 \beta + \gamma_0.$$

Continuing the process, we obtain

$$\eta = (\alpha_k + \delta_{k-1})\beta^k + \gamma_{k-1}\beta^{k-1} + \cdots + \gamma_1\beta + \gamma_0,$$

where $\gamma_0, \gamma_1, \dots, \gamma_{k-1} \in \mathcal{C}$. Since there exists $\gamma_k \in \mathcal{C}$ such that $\alpha_k + \delta_{k-1} \equiv \gamma_k \pmod{\beta}$, then $\alpha_k + \delta_{k-1} = \gamma_k + \delta_k\beta$ for some $\delta_k \in \mathbb{Z}[i]$. It follows that

$$\eta = \delta_k\beta^{k+1} + \gamma_k\beta^k + \cdots + \gamma_1\beta + \gamma_0.$$

If $\delta_k \neq 0$, then we are done. If $\delta_k = 0$, then there exists the largest integer $i \in \{0, 1, \dots, k\}$ such that $\gamma_i \neq 0$ and thus

$$\eta = \gamma_i\beta^i + \gamma_{i-1}\beta^{i-1} + \cdots + \gamma_1\beta + \gamma_0,$$

as desired. □

For a non-zero Gaussian integer $\beta = a + bi$, it is clear that

$$\max\{|a|, |b|\} \leq \frac{a^2 + b^2}{d},$$

where $d = \gcd(a, b)$. It follows that

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

Note that if $d = 1$, then

$$\mathcal{C}' = \{0, 1, \dots, \max\{|a|, |b|\} - 1\},$$

while if $b = 0$, then $d = |a|$ and so

$$\mathcal{C}' = \{x + yi \mid x, y = 0, 1, \dots, |a| - 1\} = \mathcal{C}.$$

By applying Lemma 3.5 and Proposition 3.16, we obtain an irreducibility criterion in $\mathbb{Z}[i][x]$.

Theorem 3.17. *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*

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

is its base $\beta(\mathcal{C}')$ representation with $n \geq 1$ and $\mathrm{Re}(\alpha_n) \geq 1$ satisfying condition (ii) of Lemma 3.5, then $f(x) = \alpha_n x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0$ is irreducible in $\mathbb{Z}[i][x]$.

Proof. Clearly, $f(x)$ is irreducible if $\deg f(x) = 1$. Now we suppose that $\deg f(x) \geq 2$ and $f(x)$ is reducible in $\mathbb{Z}[i][x]$. As $\pi = f(\beta)$ is a Gaussian prime, so $f(x) = g(x)h(x)$ for some positive degree polynomials $g(x)$ and $h(x)$ in $\mathbb{Z}[i][x]$. It follows that $g(\beta)$ or $h(\beta)$ is a unit and so either $|g(\beta)| = 1$ or $|h(\beta)| = 1$. Without loss of generality, we may assume that $|g(\beta)| = 1$.

Let $M = \sqrt{(\max\{a,|b|\}-1)^2+(d-1)^2}$. Since $\alpha_i \in \mathcal{C}'$ for all $i \in \{0,1,\ldots,n-1\}$, we have $|\alpha_i| \leq M$ for all $i \in \{0,1,\ldots,n-1\}$. Now we show that

$$|\beta| \geq \frac{3+\sqrt{1+4M}}{2}. \tag{3.9}$$

Clearly, (3.9) holds if $\beta \in \{2\pm 2i, 1\pm 3i, 3\pm i\}$. For the case $|\beta| \geq 2+\sqrt{2}$ with $a \geq 1$, we prove the following.

Claim. If $|\beta| \geq 2+\sqrt{2}$, $a \geq 1$, then $\sqrt{2}(|\beta|-1) \geq M$.

Proof of the Claim: *Case 1.* $a \geq |b|$: Since $d = \gcd(a,b)$ and $a \geq 1$, we have $2(a-1)^2 - 2(d-1)^2 + 8(a-1)|b| + 4|b|^2 \geq 0$ and so

$$(2(a-1)+2|b|)^2 = 4(a-1)^2 + 8(a-1)|b| + 4|b|^2 \geq 2(a-1)^2 + 2(d-1)^2.$$

It follows that $2+2(a-1)+2(|b|-1) \geq \sqrt{2\,(a-1)^2+2\,(d-1)^2}$, which implies

$$\Delta := 4+4(a-1)+4(|b|-1) - 2\sqrt{2\left((a-1)^2+(d-1)^2\right)} \geq 0.$$

Let

$$\delta := 2\,(|b|-1)^2 - 2 + (a-1)^2 - (d-1)^2\,.$$

We will show that $\delta \geq 0$. If $b=0$, then $d=a$ and so $\delta = 0$. If $|b|=1$, then $d=1$. Since $|\beta| \geq 2+\sqrt{2}$, we get $a \geq 4$ and so $\delta = (a-1)^2 - 2 > 0$. If $|b| > 1$, then $2\,(|b|-1)^2 - 2 \geq 0$ and so $\delta \geq 0$. Thus $\delta + \Delta \geq 0$, which implies that

$$\begin{aligned} 2\left(a^2+b^2\right) &\geq (a-1)^2 + (d-1)^2 + 2\sqrt{2\left((a-1)^2+(d-1)^2\right)} + 2 \\ &= \left(\sqrt{(a-1)^2+(d-1)^2} + \sqrt{2}\right)^2. \end{aligned}$$

Hence

$$\sqrt{2}\left(\sqrt{a^2+b^2}-1\right) \geq \sqrt{(a-1)^2+(d-1)^2} = M.$$

Case 2. $a < |b|$: By the proof similar to Case 1, we get

$$\sqrt{2}\left(\sqrt{a^2+b^2}-1\right) > \sqrt{(|b|-1)^2+(d-1)^2} = M,$$

and so we have the Claim.

Since $|\beta| \geq 2+\sqrt{2}$, we have

$$4|\beta|^2 - (12+4\sqrt{2})|\beta| + 8 + 4\sqrt{2} = 4(|\beta|-1)\left(|\beta|-\sqrt{2}-2\right) \geq 0$$

and so $(2|\beta|-3)^2 \geq 1+4\sqrt{2}(|\beta|-1)$. It follows by the Claim that

$$|\beta| \geq \frac{3+\sqrt{1+4\sqrt{2}\,(|\beta|-1)}}{2} \geq \frac{3+\sqrt{1+4M}}{2},$$

showing that

$$|\beta| - \frac{1+\sqrt{1+4M}}{2} \geq 1. \tag{3.10}$$

Since $\deg g(x) \geq 1$, we can express $g(x)$ in the form

$$g(x) = \epsilon \prod_i (x-\gamma_i),$$

where ϵ is the leading coefficient of $g(x)$ and the product is over the set of complex zeros of $g(x)$. By Lemma 3.5, any zero γ of $g(x)$ satisfies either $\mathrm{Re}(\gamma) < 0$ or

$$|\gamma| < \frac{1+\sqrt{1+4M}}{2}. \tag{3.11}$$

In the former case, since $a \geq 1$, we have $|\beta-\gamma| \geq \mathrm{Re}(\beta-\gamma) = a - \mathrm{Re}(\gamma) > 1$; in the latter case, by (3.10) and (3.11), we obtain

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

Thus, we deduce

$$1 = |g(\beta)| = |\epsilon| \prod_i |\beta-\gamma_i| \geq \prod_i |\beta-\gamma_i| > 1,$$

which is a contradiction. This completes the proof. □

Let $\beta = 1+5i$ and $\pi = 1+10i$, a Gaussian prime. We see that $\pi = \beta^2+25$ and $f(x) = x^2+25 = (x-5i)\,(x+5i)$ so that $f(x)$ is a reducible polynomial in $\mathbb{Z}[i][x]$. Observe that $25 \notin \mathcal{C}' = \{0,1,2,3,4\}$.

The following two corollaries are immediate consequences of Theorem 3.17.

Corollary 3.18. *Let $\beta \in \{1\pm 3i, 3\pm i\}$ or $\beta = a+bi \in \mathbb{Z}[i]$ be such that $\gcd(a,b)=1$, $a \geq 1$, and $|\beta| \geq 2+\sqrt{2}$. For a Gaussian prime π, if*

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

is its base $\beta(\mathcal{C}')$ representation with $n \geq 1$ and $\mathrm{Re}(\alpha_n) \geq 1$ satisfying condition (ii) of Lemma 3.5, then $f(x) = \alpha_n x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0$ is irreducible in $\mathbb{Z}[i][x]$.

Example 3.19. Let $\beta = 4 + i$ and $\pi = 92 + 65i$. Then π is a Gaussian prime because $\phi_{-1}(92 + 65i) = 12689$ is a rational prime. Since

$$92 + 65i = (4 + i)^3 + 2(4 + i)^2 + 2(4 + i) + 2,$$

by Corollary 3.18, $f(x) = x^3 + 2x^2 + 2x + 2$ is irreducible in $\mathbb{Z}[i][x]$.

Corollary 3.20. *Let $\beta = a \in \mathbb{Z}$ be such that $a \geq 4$ and π a Gaussian prime. If*

$$\pi = \alpha_n a^n + \alpha_{n-1} a^{n-1} + \cdots + \alpha_1 a + \alpha_0,$$

is its base $\beta(\mathcal{C})$ representation with $n \geq 1$ and $\mathrm{Re}(\alpha_n) \geq 1$ satisfying condition (ii) of Lemma 3.5, then $f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_1 x + \alpha_0$ is irreducible in $\mathbb{Z}[i][x]$.

If p is a rational prime with $p \equiv 3 (\mathrm{mod}\ 4)$, $b \geq 4$ a positive integer and

$$p = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0, \tag{3.12}$$

where $n \geq 1, a_n \neq 0$ and $a_i \in \{0, 1, 2, \ldots, b-1\}$ for all $0 \leq i \leq n$. Then p is a Gaussian prime and we see that (3.12) is a base $b(\mathcal{C})$ representation. Using Corollary 3.20, the polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ is irreducible in $\mathbb{Z}[i][x]$ and so is irreducible in $\mathbb{Z}[x]$. This is a generalization of A. Cohn in [2] for prime numbers in $\mathbb{Z}$ that remain prime in $\mathbb{Z}[i]$.

Finally for the case $\beta = 3$, we prove:

Lemma 3.21. *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 $n \geq 3$ and $|\alpha_i| \leq M$ $(0 \leq i \leq n-2)$ for some real number $M \geq 1$. If $f(x)$ satisfies

(i) $\mathrm{Re}(\alpha_n) \geq 1, \mathrm{Re}(\alpha_{n-1}) \geq 0, \mathrm{Im}(\alpha_{n-1}) \geq 0, \mathrm{Re}(\alpha_{n-2}) \geq 0, \mathrm{Im}(\alpha_{n-2}) \geq 0,$

(ii) $\mathrm{Re}(\alpha_{n-1}) \mathrm{Im}(\alpha_n) \geq \mathrm{Re}(\alpha_n) \mathrm{Im}(\alpha_{n-1}),$

(iii) $\mathrm{Re}(\alpha_{n-2}) \mathrm{Im}(\alpha_n) \geq \mathrm{Re}(\alpha_n) \mathrm{Im}(\alpha_{n-2})$ *and*

(iv) $\mathrm{Re}(\alpha_{n-2}) \mathrm{Im}(\alpha_{n-1}) \geq \mathrm{Re}(\alpha_{n-1}) \mathrm{Im}(\alpha_{n-2}),$

then for any complex zero α of $f(x)$, if $|\arg \alpha| \leq \pi/6$, then $|\alpha| < M^{1/3} + 0.465572$, otherwise

$$\mathrm{Re}(\alpha) < \frac{\sqrt{3}}{2} \left(\frac{1 + \sqrt{1 + 4M}}{2} \right).$$

Proof. Let $\alpha = a + bi$ be any complex zero of $f(x)$. If $|\alpha| \leq 1$, then $|\alpha| < M^{1/3} + 0.465572$. Now assume that $|\arg \alpha| \leq \pi/6$ and $|\alpha| > 1$. Then

$$\begin{aligned} \left| \frac{f(\alpha)}{\alpha^n} \right| + \left| \frac{\alpha_{n-3}}{\alpha^3} \right| + \cdots + \left| \frac{\alpha_0}{\alpha^n} \right| &\geq \left| \frac{f(\alpha)}{\alpha^n} \right| + \left| \frac{\alpha_{n-3}}{\alpha^3} + \cdots + \frac{\alpha_0}{\alpha^n} \right| \\ &\geq \left| \frac{f(\alpha)}{\alpha^n} - \left(\frac{\alpha_{n-3}}{\alpha^3} + \cdots + \frac{\alpha_0}{\alpha^n} \right) \right|. \end{aligned}$$

Since $|\alpha| > 1$ and $|\alpha_i| \le M$ $(0 \le i \le n-2)$, we have

$$\left|\frac{f(\alpha)}{\alpha^n}\right| + \frac{M}{|\alpha|^2(|\alpha|-1)} > \left|\frac{f(\alpha)}{\alpha^n} - \left(\frac{\alpha_{n-3}}{\alpha^3} + \cdots + \frac{\alpha_0}{\alpha^n}\right)\right|$$

and so

$$\left|\frac{f(\alpha)}{\alpha^n}\right| > \left|\alpha_n + \frac{\alpha_{n-1}}{\alpha} + \frac{\alpha_{n-2}}{\alpha^2}\right| - \frac{M}{|\alpha|^2(|\alpha|-1)}. \tag{3.13}$$

Since $|\arg\alpha| \le \pi/6$, we get

$$a = |\alpha| \cos(\arg\alpha) > 0 \tag{3.14}$$

and

$$a^2 - b^2 = |\alpha|^2 \cos(2\arg\alpha) > 0. \tag{3.15}$$

For convenience, we set $\alpha_n = a_n + b_n i, \alpha_{n-1} = a_{n-1} + b_{n-1} i$ and $\alpha_{n-2} = a_{n-2} + b_{n-2} i$. Then

$$\begin{aligned}
\frac{\alpha_{n-1}}{\alpha} &= \frac{(a_{n-1}a + b_{n-1}b) + (ab_{n-1} - a_{n-1}b)\, i}{|\alpha|^2},\\
\frac{\alpha_{n-2}}{\alpha^2} &= \frac{\left(a_{n-2}\left(a^2-b^2\right) + 2abb_{n-2}\right) + \left(b_{n-2}\left(a^2-b^2\right) - 2aba_{n-2}\right) i}{|\alpha|^4}.
\end{aligned}$$

We now prove the following.
Claim. $\left|\alpha_n + \frac{\alpha_{n-1}}{\alpha} + \frac{\alpha_{n-2}}{\alpha^2}\right| \ge 1.$
Proof of the Claim. If $b \ge 0$, then, by (i), (3.14) and (3.15), we have

$$\begin{aligned}
\left|\alpha_n + \frac{\alpha_{n-1}}{\alpha} + \frac{\alpha_{n-2}}{\alpha^2}\right| &\ge \mathrm{Re}\left(\alpha_n + \frac{\alpha_{n-1}}{\alpha} + \frac{\alpha_{n-2}}{\alpha^2}\right)\\
&= a_n + \frac{a_{n-1}a + b_{n-1}b}{|\alpha|^2} + \frac{a_{n-2}\left(a^2-b^2\right) + 2abb_{n-2}}{|\alpha|^4} \ge a_n \ge 1.
\end{aligned}$$

Now, we assume that $b < 0$. Using (i), (ii) and the same proof of Lemma 3.5, we obtain

$$\left|\alpha_n + \frac{\alpha_{n-1}}{\alpha}\right|^2 \ge 1,$$

which implies

(3.16)

$$\begin{aligned}
\left|\alpha_n + \frac{\alpha_{n-1}}{\alpha} + \frac{\alpha_{n-2}}{\alpha^2}\right|^2 &= \left(\operatorname{Re}\left(\alpha_n + \frac{\alpha_{n-1}}{\alpha}\right) + \operatorname{Re}\left(\frac{\alpha_{n-2}}{\alpha^2}\right)\right)^2 \\
&\quad + \left(\operatorname{Im}\left(\alpha_n + \frac{\alpha_{n-1}}{\alpha}\right) + \operatorname{Im}\left(\frac{\alpha_{n-2}}{\alpha^2}\right)\right)^2 \\
&\geq \left[\operatorname{Re}\left(\alpha_n + \frac{\alpha_{n-1}}{\alpha}\right)\right]^2 + \left[\operatorname{Im}\left(\alpha_n + \frac{\alpha_{n-1}}{\alpha}\right)\right]^2 \\
&\quad + 2\operatorname{Re}\left(\alpha_n + \frac{\alpha_{n-1}}{\alpha}\right)\operatorname{Re}\left(\frac{\alpha_{n-2}}{\alpha^2}\right) + 2\operatorname{Im}\left(\alpha_n + \frac{\alpha_{n-1}}{\alpha}\right)\operatorname{Im}\left(\frac{\alpha_{n-2}}{\alpha^2}\right) \\
&= \left|\alpha_n + \frac{\alpha_{n-1}}{\alpha}\right|^2 + 2\operatorname{Re}\left(\alpha_n + \frac{\alpha_{n-1}}{\alpha}\right)\operatorname{Re}\left(\frac{\alpha_{n-2}}{\alpha^2}\right) \\
&\quad + 2\operatorname{Im}\left(\alpha_n + \frac{\alpha_{n-1}}{\alpha}\right)\operatorname{Im}\left(\frac{\alpha_{n-2}}{\alpha^2}\right) \\
&\geq 1 + 2\left[\operatorname{Re}(\alpha_n)\operatorname{Re}\left(\frac{\alpha_{n-2}}{\alpha^2}\right) + \operatorname{Im}(\alpha_n)\operatorname{Im}\left(\frac{\alpha_{n-2}}{\alpha^2}\right)\right] \\
&+ 2\left[\operatorname{Re}\left(\frac{\alpha_{n-1}}{\alpha}\right)\operatorname{Re}\left(\frac{\alpha_{n-2}}{\alpha^2}\right) + \operatorname{Im}\left(\frac{\alpha_{n-1}}{\alpha}\right)\operatorname{Im}\left(\frac{\alpha_{n-2}}{\alpha^2}\right)\right].
\end{aligned}$$

By using (i) and (3.15), we obtain

(3.17)

$$\operatorname{Re}(\alpha_n)\operatorname{Re}\left(\frac{\alpha_{n-2}}{\alpha^2}\right) = \frac{1}{|\alpha|^4}\left(a_n a_{n-2}\left(a^2 - b^2\right) + 2a_n ab b_{n-2}\right) \geq \frac{2}{|\alpha|^4} a_n ab b_{n-2}$$

and

(3.18)

$$\operatorname{Im}(\alpha_n)\operatorname{Im}\left(\frac{\alpha_{n-2}}{\alpha^2}\right) = \frac{1}{|\alpha|^4}\left(b_n b_{n-2}\left(a^2 - b^2\right) - 2b_n ab a_{n-2}\right) \geq \frac{2}{|\alpha|^4} b_n a(-b) a_{n-2},$$

provided $b_n \geq 0$. Note that if $b_n < 0$, then the condition (iii) implies $a_{n-2} = b_{n-2} = 0$ so that (3.18) holds for this case. Combining (3.17), (3.18) and using (iii), we obtain

(3.19)

$$\operatorname{Re}(\alpha_n)\operatorname{Re}\left(\frac{\alpha_{n-2}}{\alpha^2}\right) + \operatorname{Im}(\alpha_n)\operatorname{Im}\left(\frac{\alpha_{n-2}}{\alpha^2}\right) \geq \frac{2a(-b)}{|\alpha|^4}\left(a_{n-2}b_n - a_n b_{n-2}\right) \geq 0.$$

By using (i), (3.14) and (3.15), we get

$$\begin{aligned}
\text{(3.20)}\quad \operatorname{Re}\left(\frac{\alpha_{n-1}}{\alpha}\right)\operatorname{Re}\left(\frac{\alpha_{n-2}}{\alpha^2}\right) &= \frac{1}{|\alpha|^6}\left[\left(a_{n-1}a_{n-2}a\left(a^2 - b^2\right)\right) + \left(2a^2 b a_{n-1} b_{n-2}\right)\right] \\
&\quad + \frac{1}{|\alpha|^6}\left[\left(b_{n-1}a_{n-2}b\left(a^2 - b^2\right)\right) + \left(2b_{n-1}b_{n-2}ab^2\right)\right] \\
&\geq \frac{1}{|\alpha|^6}\left[\left(2a^2 b a_{n-1} b_{n-2}\right) + \left(b_{n-1}a_{n-2}b\left(a^2 - b^2\right)\right)\right]
\end{aligned}$$

and

$$\operatorname{Im}\left(\frac{\alpha_{n-1}}{\alpha}\right)\operatorname{Im}\left(\frac{\alpha_{n-2}}{\alpha^2}\right) = \frac{1}{|\alpha|^6}\left[\left(b_{n-1}b_{n-2}a\left(a^2-b^2\right)\right)-\left(2a^2bb_{n-1}a_{n-2}\right)\right]$$
$$-\frac{1}{|\alpha|^6}\left[\left(a_{n-1}b_{n-2}b\left(a^2-b^2\right)\right)+\left(2a_{n-1}a_{n-2}ab^2\right)\right]$$
$$\geq \frac{1}{|\alpha|^6}\left[\left(2a^2(-b)b_{n-1}a_{n-2}\right)+\left(a_{n-1}b_{n-2}(-b)\left(a^2-b^2\right)\right)\right]. \tag{3.21}$$

Combining (3.20), (3.21) and using (3.15), (iv), we obtain

$$\begin{aligned}
\operatorname{Re}\left(\frac{\alpha_{n-1}}{\alpha}\right)\operatorname{Re}\left(\frac{\alpha_{n-2}}{\alpha^2}\right) &+ \operatorname{Im}\left(\frac{\alpha_{n-1}}{\alpha}\right)\operatorname{Im}\left(\frac{\alpha_{n-2}}{\alpha^2}\right)\\
&\geq \frac{2a^2(-b)}{|\alpha|^6}\left(a_{n-2}b_{n-1}-a_{n-1}b_{n-2}\right)\\
&+\frac{(-b)\left(a^2-b^2\right)}{|\alpha|^6}\left(a_{n-1}b_{n-2}-a_{n-2}b_{n-1}\right)\\
&=\left(a_{n-2}b_{n-1}-a_{n-1}b_{n-2}\right)\frac{(-b)}{|\alpha|^6}\left(2a^2-\left(a^2-b^2\right)\right)\\
&=\left(a_{n-2}b_{n-1}-a_{n-1}b_{n-2}\right)\frac{(-b)}{|\alpha|^6}\left(a^2+b^2\right)\geq 0.
\end{aligned} \tag{3.22}$$

Returning to (3.16) and using (3.19), (3.22), we conclude that

$$\left|\alpha_n+\frac{\alpha_{n-1}}{\alpha}+\frac{\alpha_{n-2}}{\alpha^2}\right|^2 \geq 1$$

and so we have the Claim.

By (3.13) and the Claim, we have

$$\left|\frac{f(\alpha)}{\alpha^n}\right| > 1-\frac{M}{|\alpha|^2(|\alpha|-1)} = \frac{|\alpha|^3-|\alpha|^2-M}{|\alpha|^2(|\alpha|-1)}.$$

Let $h(x) := x^3-x^2-M$. Then $h'(x)>0$ for $x\in(-\infty,0)\cup(2/3,\infty)$. Since $M\geq 1$, we obtain $M^{1/3}+0.465572>2/3$ and

$$\begin{aligned}
h\left(M^{1/3}+0.465572\right) &> 0.396716M^{2/3}-0.280873M^{1/3}-0.115842\\
&=\left(M^{1/3}\left(0.396716M^{1/3}-0.280873\right)-0.115842\right)>0.
\end{aligned}$$

If $|\alpha|\geq M^{1/3}+0.465572$, then $h(|\alpha|)>0$. It follows that

$$0=\left|\frac{f(\alpha)}{\alpha^n}\right| > \frac{|\alpha|^3-|\alpha|^2-M}{|\alpha|^2\left(|\alpha|-1\right)} = \frac{h(|\alpha|)}{|\alpha|^2\left(|\alpha|-1\right)},$$

which is impossible. Thus, $|\alpha| < M^{1/3} + 0.465572$.

For the case $|\arg\alpha| > \pi/6$, by Lemma 3.5, we have either $\mathrm{Re}(\alpha) < 0$ or $|\alpha| < (1+\sqrt{1+4M})/2$. If $\mathrm{Re}(\alpha) < 0$, then it is clear that $\mathrm{Re}(\alpha) < (\sqrt{3}/2)\left((1+\sqrt{1+4M})/2\right)$, while if $|\alpha| < (1+\sqrt{1+4M})/2$, we obtain $\mathrm{Re}(\alpha) = |\alpha|\cos(\arg\alpha) < |\alpha|\cos\pi/6 < (\sqrt{3}/2)\left((1+\sqrt{1+4M})/2\right)$, as desired. □

Theorem 3.22. *If π is a Gaussian prime where base $3(\mathcal{C})$-representation is*

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

with $n \geq 3$, $\mathrm{Re}(\alpha_n) \geq 1$ satisfying the conditions (ii)-(iv) of Lemma 3.21, then $f(x) = \alpha_n x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0$ is irreducible in $\mathbb{Z}[i][x]$.

Proof. Suppose that $f(x)$ is reducible in $\mathbb{Z}[i][x]$. As $\pi = f(3)$ is a Gaussian prime, if $f(x) = g(x)h(x)$ for some positive degree polynomials $g(x)$ and $h(x)$ in $\mathbb{Z}[i][x]$, then either $|g(3)| = 1$ or $|h(3)| = 1$. Without loss of generality, we may assume that $|g(3)| = 1$.

Since $\deg g(x) \geq 1$, we can express $g(x)$ in the form

$$g(x) = \epsilon \prod_i (x - \gamma_i),$$

where ϵ is the leading coefficient of $g(x)$ and the product is over the set of complex zeros of $g(x)$. By Lemma 3.21 with $M = 2\sqrt{2}$, any zero γ of $g(x)$ satisfies either $|\gamma| < (2\sqrt{2})^{1/3} + 0.465572 \approx 1.879572$ or

$$\mathrm{Re}(\gamma) < \frac{\sqrt{3}}{2}\left(\frac{1+\sqrt{1+8\sqrt{2}}}{2}\right) \approx 1.952.$$

In the former case, we get $|3-\gamma| \geq 3 - |\gamma| > 3 - 1.879572 > 1$; in the latter case, we obtain $|3-\gamma| \geq \mathrm{Re}(3-\gamma) = 3 - \mathrm{Re}(\gamma) > 3 - 1.952 > 1$. Thus, we deduce

$$1 = |g(3)| = |\epsilon| \prod_i |3-\gamma_i| \geq \prod_i |3-\gamma_i| > 1,$$

which is a contradiction. □

Example 3.23 Let $\beta = 3$ and $\pi = 36 + i$. Then π is a Gaussian prime because $\phi_{-1}(\pi) = 36^2 + 1^1 = 1297$ is a rational prime. Since

$$36 + i = 3^3 + 3^2 + i,$$

the polynomial $f(x) = x^3 + x^2 + i$ is irreducible in $\mathbb{Z}[i][x]$, by Theorem 3.22.

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*, Canad. J. Math., **33**(1981), 1055–1059.

[3] M. Filaseta, *Irreducibility criteria for polynomials with nonnegative coefficients*, Canad. J. Math., **40**(1988), 339–351.

[4] K. Girstmair, *On an irreducibility criterion of M. Ram Murty*, Amer. Math. Monthly, **112**(2005), 269–270.

[5] M. R. Murty, *Prime numbers and irreducible polynomials*, Amer. Math. Monthly, **109**(2002), 452–458.

[6] W. K. Nicholson, *Introduction to abstract algebra*, John Wiley & Sons, New Jersey, 2007.

[7] G. Pólya and G. Szegö, *Problems and theorems in analysis, Vol. II*, Springer-Verlag, New York, 1976.

[8] S. Roman, *Field theory*, Graduate Texts in Mathematics **158**, springer-verlag, New York, 1995.

[9] K. H. Rosen, *Elementary number theory and its applications*, Addison-Wesley, New York, 2000.