Armenian Journal of Mathematics
Volume 5, Number 1, 2013, 58–68

Factor Rings and their decompositions in the Eisenstein integers Ring $\mathbb{Z}[\omega]$

Manouchehr Misaghian

Department of Mathematics,
Prairie View A&M University
Prairie View, TX 77446-USA
mamisaghian@pvamu.edu

Abstract

In this paper we will characterize the structure of factor rings for $\mathbb{Z}[\omega]$ where $\omega = \frac{-1+\sqrt{-3}}{2}$,is a 3rd primitive root of unity. Consequently, we can recognize prime numbers (elements) and their ramifications in $\mathbb{Z}[\omega]$.

Key Words: Euclidean Domain, Unique Factorization Domain, Factor ring, Eisenstein integers
Mathematics Subject Classification 2000: Primary 13F15, 13F07; Secondary 13F10

Introduction

The set of integers, $\mathbb{Z} = \{..., -n, ..., -1, 0, 1, ..., n, ...\}$, is the most important and simplest Integral Domain. This ring is Euclidean and thus a Unique Factorization Domain (UFD). It is also a Principal Ideal Domain (PID), thus all ideals of this ring are principal and are given by:

$$\langle m \rangle = \{km \mid k \in \mathbb{Z}\}, \text{for all } m \in \mathbb{Z}$$

So the factor rings of $\mathbb{Z}$, are given by $\mathbb{Z} \diagup m\mathbb{Z} = \mathbb{Z}_m$, the ring of integers $\{0, 1, 2, \cdots, m-1\}$ modulo m.

In an attempt to formulate and prove the Reciprocity Theorem, one of the most important and beautiful Theorems in Number theory arose, Carl Friedrich Gauss realized that he needed to look beyond the set of integers. For this reason Gauss introduced "Complex Integer Numbers" [4]. These numbers are now known as Gaussian integers. The Gaussian integers are sitting in the field of complex numbers, and by inherited addition and multiplication operations from the field of complex numbers constitute an integral domain which is a UFD [2], [6]. In general we can consider some imaginary extensions of the ring of integers as follows.

Let $p \in \mathbb{Z}, p > 1$ be a prime number, and let ξ be a primitive root of the equation $x^p + a = 0$, where a is an integer; i.e. a number for which $\xi^p = -a$ but $\xi^q \neq -a$ for all $q, 0 < q < p$. Then

$$\mathbb{Z}[\xi] = \left\{ a_0 + a_1\xi + \cdots + a_{p-1}\xi^{p-1} \mid a_i \in \mathbb{Z}, 0 \leq i \leq p-1 \right\}$$

with appropriate operations is an extension of $\mathbb{Z}$.

In 1847 Gabriel Lame announced that he had a complete proof of the Last Fermat's Theorem. In his proof, he used the identity

$$x^p + y^p = (x+y)(x+\xi y)\cdots\left(x+\xi^{p-1}y\right)$$

where p and ξ are as above, with the assumption that all extensions of $\mathbb{Z}$ are UFD. Before the Lame's work, Ernst Kummer had already proven that some of these extensions are not UFD. For example in $\mathbb{Z}\left[\sqrt{-5}\right]$ we have:

$$6 = 2 \cdot 3 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$$

In connection with this observation, Kummer defined his Ideal Numbers. This led directly to Richard Dedekind's development of Algebraic Number Theory in 1870s. Dedekind introduced a form of unique factorization using ideals instead of numbers. Let $\Re$ be an integral domain for which there exists a subset $\mathfrak{P}$ such that every non zero element x of $\Re$ can be written, in a unique way as

$$x = \varepsilon \prod_{p \in \mathfrak{P}} p^{v_p(x)}$$

Where ε is a unit element in $\Re$ and $v_p(x)$ are non-negative integers, all but a finitely many are zero. In the other words the set $(\Re_p)_{p\in\mathfrak{P}}$of principal ideals that coincide with the set of maximal principal ideals distinct from $\Re$, is uniquely determined.

A unique factorization domain has also a very simple geometric interpretation. In geometry a ring R occurs as a ring of functions defined on some variety V. If n denotes the dimension of V, then R is a UFD means that every subvariety of dimension $n-1$ can be defined by a single equation.

One of the fundamental differences between $\mathbb{Z}$ and its extensions is the structure of their *Factor Rings*. As we know the factor rings of $\mathbb{Z}$, are $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$, which are isomorphic to the ring $\{0, 1, 2, \cdots, m-1\}$ modulo m. Even when m is a composite number like

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

we can use The Chinese reminder theorem to factor $\mathbb{Z}_m$ as

$$\mathbb{Z}_m = \mathbb{Z}_{p_1^{\alpha_1}} \bigoplus \mathbb{Z}_{p_2^{\alpha_2}} \bigoplus \cdots \bigoplus \mathbb{Z}_{p_r^{\alpha_r}}.$$

The structure of factor rings for $\mathbb{Z}[\xi]$ is much more complicated. This structure has been studied for Gaussian integers [3]. In this paper we will characterize the structure of factor rings for $\mathbb{Z}[\omega]$ where $\omega = \frac{-1+\sqrt{-3}}{2}$ is a primitive 3rd root of unity. Consequently, we can recognize prime numbers (elements) and their ramifications in $\mathbb{Z}[\omega]$.

1 Notation and Prerequisites

Let $\mathbb{Z}$ be the ring of integers and let $\omega = \frac{-1+\sqrt{-3}}{2}$ be a primitive 3rd root of unity; i.e. $\omega^3 = 1$, and $\omega^2 + \omega + 1 = 0$. Set

$$\mathbb{Z}[\omega] = \{a + b\omega \,| a, b \in \mathbb{Z}\}$$

Then $\mathbb{Z}[\omega]$ with the following operations is an integral domain

$$(a + b\omega) + (c + d\omega) = (a + c) + (b + d)\,\omega$$
$$(a + b\omega)(c + d\omega) = (ac - bd) + (ad + bc - bd)\,\omega$$

for $(a + b\omega), (c + d\omega) \in \mathbb{Z}[\omega]$. For each $z = a + b\omega \in \mathbb{Z}[\omega]$, its norm is defined by

$$\begin{aligned} \nu(z) &= (a + b\omega)\left(a + b\omega^2\right) \\ &= a^2 + b^2 - ab \end{aligned}$$

Then by basic ring theory we have:

Theorem 1 *$\mathbb{Z}[\omega]$ with above norm is an Euclidean Domain and so a Unique Factorization Domain(UFD).*

Definition 1 *An element $z \in \mathbb{Z}[\omega]$ is called a unit if it has a multiplicative inverse in $\mathbb{Z}[\omega]$.*

Lemma 1 *The only unit elements in $\mathbb{Z}[\omega]$ are $\{\pm 1, \pm\omega, \pm\omega^2\}$.*

Proof. A non zero element $z = a + b\omega \in \mathbb{Z}[\omega]$ is unit if and only if $\nu(z) = a^2 + b^2 - ab = 1$. If $ab = 0$, then $z = \pm 1$ or $z = \pm\omega$. If $ab \neq 0$ then $a^2 + b^2 \geqslant 2$ and this with $a^2 + b^2 - ab = 1$ gives $ab \geqslant 1$. on the other hand from $a^2 + b^2 - ab = 1$ we have $a^2 + b^2 - 2ab = 1 - ab$ so $ab \leq 1$, hence we must have $ab = 1$ that gives us $a = b = \pm 1$, i.e. $z = \pm(1 + \omega) = \mp\omega^2$. □

Definition 2 ***(Legendre's Symbols)***. *Let $p \in \mathbb{Z}$ be a prime number. Then the Legendre's symbol, denoted by $\left(\frac{\cdot}{p}\right)$, for each integer $a \in \mathbb{Z}$, is defined by*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \textit{if there is an integer } x \in \mathbb{Z} \textit{ such that } x^2 \equiv a \,(\operatorname{mod} p), \\ -1 & \textit{if there is no integer } x \in \mathbb{Z} \textit{ such that } x^2 \equiv a \,(\operatorname{mod} p), \\ 0 & \textit{if } p \textit{ divides } a \end{cases}$$

The following two theorems can be found in any standard Number Theory book, for example [2], [6] and [5].

Theorem 2 *Let $p \in \mathbb{Z}$ be a prime number. The Legendre's symbol has the following property:*

(i). $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$*, for all integers $a, b \in \mathbb{Z}$.*

(ii). $a \equiv b \,(\mathrm{mod}\, p) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Theorem 3 *(**Quadratic Reciprocity Theorem**). Let $p \in \mathbb{Z}$ be a prime number. Then:*

(i). $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1(\mathrm{mod}\, 4), \\ -1 & \text{if } p \equiv 3(\mathrm{mod}\, 4) \end{cases}$

(ii). $\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 11(\mathrm{mod}\, 12), \\ -1 & \text{if } p \equiv 5 \text{ or } 7(\mathrm{mod}\, 12) \end{cases}$

The following lemmas can be proved in a strait manner.

Lemma 2 *Let $p \in \mathbb{Z}$ be a prime integer. Then $p \equiv 1 \,(\mathrm{mod}\, 3)$ if and only if $p \equiv 1 \,(\mathrm{mod}\, 6)$.*

Lemma 3 *Let $p \in \mathbb{Z}$ be a prime integer. If $p \equiv 1 or\ 7 \,(\mathrm{mod}\, 12)$ then $p \equiv 1 \,(\mathrm{mod}\, 6)$.*

Theorem 4 *Let $p \in \mathbb{Z}$ be a prime integer. Then $\left(\frac{-3}{p}\right) = 1$ if and only if $p \equiv 1 \,(\mathrm{mod}\, 6)$.*

Proof. By part (i) of the Theorem 2 we have $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$.If $\left(\frac{-3}{p}\right) = 1$ then we must have $\left(\frac{-1}{p}\right) = \left(\frac{3}{p}\right) = 1$or $\left(\frac{-1}{p}\right) = \left(\frac{3}{p}\right) = -1$. In the first case we have $p \equiv 1(\mathrm{mod}\, 4)$ and $p \equiv 1$ or $11(\mathrm{mod}\, 12)$. These conditions lead to $p \equiv 1(\mathrm{mod}\, 12)$, so by the Lemma 3 we get $p \equiv 1 \,(\mathrm{mod}\, 6)$. In the second case we have $p \equiv 3(\mathrm{mod}\, 4)$ and $p \equiv 5$ or $7(\mathrm{mod}\, 12)$. These conditions lead to $p \equiv 7(\mathrm{mod}\, 12)$, so by the Lemma 3 we get $p \equiv 1 \,(\mathrm{mod}\, 6)$. Now suppose we have $p \equiv 1 \,(\mathrm{mod}\, 6)$. So $p = 1 + 6k$ for some integer $k \in \mathbb{Z}$. If k is even then $p \equiv 1(\mathrm{mod}\, 12)$, so by the Theorem 3 we have$\left(\frac{-1}{p}\right) = \left(\frac{3}{p}\right) = 1$. If k is odd then $p \equiv 7(\mathrm{mod}\, 12)$, so by the Theorem 3 we have$\left(\frac{-1}{p}\right) = \left(\frac{3}{p}\right) = -1$. □

Lemma 4 *Let $p \in \mathbb{Z}$ be a prime integer. Then $p = \alpha^2 + 3\beta^2$ for some integers $\alpha, \beta \in \mathbb{Z}$ if and only if $p = 3$ or $p \equiv 1 \,(\mathrm{mod}\, 6)$.*

Proof. Suppose $p = \alpha^2 + 3\beta^2$ for some integer $\alpha, \beta \in \mathbb{Z}$. If $\alpha = 0$, then we must have $p = 3$, because p is a prime. If $\alpha \neq 0$, then $\alpha \equiv 1 \,(\mathrm{mod}\, 3)$ or $\alpha \equiv 2 \,(\mathrm{mod}\, 3)$. In either case from $p = \alpha^2 + 3\beta^2$ we get $p \equiv 1 \,(\mathrm{mod}\, 3)$ so by the Lemma 2 we have $p \equiv 1 \,(\mathrm{mod}\, 6)$. Conversely if $p = 3$ or $p \equiv 1 \,(\mathrm{mod}\, 6)$, then for $p = 3$ we have $3 = 0^2 + 3\,(1)^2$. For $p \equiv 1 \,(\mathrm{mod}\, 6)$ by the

Theorem 4 there is an integer α such that $\alpha^2 + 3 = pt$ for some integer $t \in \mathbb{Z}$, $0 < t < p$. If $t = 1$ then $p = \alpha^2 + 3(1)^2$. If $t \neq 1$, then we can choose an integer $\beta \in \mathbb{Z}$ such that, $\beta \equiv \alpha \pmod{t}$, and -$\frac{t}{2} < \beta < \frac{t}{2}$. From here and reflexive property of congruence relation we get $\alpha^2 \equiv \beta^2 \pmod{t}$ and $3 \equiv 3 \pmod{t}$, thus $(\alpha^2 + 3) \equiv (\beta^2 + 3) \equiv 0 \pmod{t}$. So for some integer $\lambda \in \mathbb{Z}$, $1 \leq \lambda < t$, we have $\beta^2 + 3 = \lambda t$. Since we also have $\alpha^2 + 3 = pt$, by multiplying these equalities side by side we get $(\alpha^2 + 3)(\beta^2 + 3) = \lambda p t^2$. On the other hand we have $(\alpha^2 + 3)(\beta^2 + 3) = (\alpha\beta + 3)^2 + 3(\alpha - \beta)^2$. Thus we have $(\alpha\beta + 3)^2 + 3(\alpha - \beta)^2 = \lambda p t^2$. One can easily show that both $(\alpha\beta + 3)^2$ and $(\alpha - \beta)^2$ are divisible by t^2 so we have $\left(\frac{\alpha\beta+3}{t}\right)^2 + 3\left(\frac{\alpha-\beta}{t}\right)^2 = \lambda p$. This equation shows that a smaller multiple of p can be written as $\alpha^2 + 3\beta^2$. If $\lambda = 1$, we are done, if not, we can repeat the above procedure. After a finite number of steps of repetition we get the result. □

Theorem 5 *Let $p \in \mathbb{Z}$ be a prime integer. Then $p = a^2 + b^2 - ab$ for some integers $a, b \in \mathbb{Z}$ if and only if $p = 3$ or $p \equiv 1 \pmod{6}$.*

Proof. Let $p = a^2 + b^2 - ab$ for some integer $a, b \in \mathbb{Z}$, then a and b are relatively prime. so they are not both even. Suppose one of them, say a is even, then we have

$$\begin{aligned} p &= a^2 + b^2 - ab \\ &= \left(\frac{a}{2} - b\right)^2 + 3\left(\frac{a}{2}\right)^2 \end{aligned}$$

and by the Lemma 4, $p = 3$ or $p \equiv 1 \pmod{6}$. If both a and b are odd then $b - a = 2t$ for some $t \in \mathbb{Z}$. From here we have $b = a + 2t$ and

$$\begin{aligned} p &= a^2 + b^2 - ab \\ &= a^2 + b(b - a) \\ &= a^2 + 2t(a + 2t) \\ &= (a + t)^2 + 3t^2 \end{aligned}$$

and again by the Lemma 4 we have $p = 3$ or $p \equiv 1 \pmod{6}$. Conversely, if $p = 3$ or $p \equiv 1 \pmod{6}$, then for $p = 3$ we have $3 = 2^2 + 1^2 - 2$. If $p \equiv 1 \pmod{6}$, then by the Lemma 4 There are integers $\alpha, \beta \in \mathbb{Z}$ such that $p = \alpha^2 + 3\beta^2$. Now set $a = \alpha + \beta$ and $b = 2\beta$. Then we have

$$\begin{aligned} p &= \alpha^2 + 3\beta^2 \\ &= \left(a - \frac{b}{2}\right)^2 + 3\left(\frac{b}{2}\right)^2 \\ &= a^2 + b^2 - ab \end{aligned}$$

□

Lemma 5 *Let $m \in \mathbb{Z}$ be an integer. Then*

$$\mathbb{Z}[\omega] / \langle m \rangle \simeq \mathbb{Z}_m[\omega]$$

Proof. For $a \in \mathbb{Z}$, let $[a]_m$ denotes the equivalence class modulo m in $\mathbb{Z}$. Now define $f : \mathbb{Z}[\omega] \to \mathbb{Z}_m[\omega]$, by $f(a + b\omega) = [a]_m + [b]_m \omega$. One can show that this is a surjective ring homomorphism with the Kernel equal $\langle m \rangle$. □

Lemma 6 *The polynomial $q(x) = x^2 + x + 1$ is irreducible in $\mathbb{Z}_p$ iff and only if $p = 2$ or $p \equiv 5 \,(\mathrm{mod}\, 6)$.*

Proof. Let $q(x) = x^2 + x + 1$ be irreducible in $\mathbb{Z}_p$. If $p \neq 2$ and $p \neq 5 \,(\mathrm{mod}\, 6)$, then $p = 3$ or $p \equiv 1 \,(\mathrm{mod}\, 6)$. If $p = 3$ then we have $q(x) = x^2 + x + 1 = (x + 2)^2$ in $\mathbb{Z}_3$, this is contrary to our assumption. If $p \equiv 1 \,(\mathrm{mod}\, 6)$, then by the Theorem 5, $p = a^2 + b^2 - ab$ for some relatively prime integers $a, b \in \mathbb{Z}$. Since a^{-1} and b^{-1} exist in $\mathbb{Z}_p$ and we have $a^2 + b^2 \equiv ab \,(\mathrm{mod}\, p)$, so we have $ab^{-1} + ba^{-1} \equiv 1 \,(\mathrm{mod}\, p)$, Now we have $q(x) = x^2 + x + 1 = (x + ab^{-1})(x + ba^{-1})$ in $\mathbb{Z}_p$ and again this is contrary to our assumption. Conversely, if $p = 2$, then $q(x) = x^2 + x + 1$ doesn't have any root in $\mathbb{Z}_2$ so it is irreducible. Suppose $p \equiv 5 \,(\mathrm{mod}\, 6)$ and $q(x) = x^2 + x + 1$ is not irreducible in $\mathbb{Z}_p$, then there is $a \in \mathbb{Z}_p$ such that $q(a) = a^2 + a + 1 = 0$ in $\mathbb{Z}_p$, so by the Theorem 5 we must have $p = 3$ or $p \equiv 1 \,(\mathrm{mod}\, 6)$ which is contrary to our assumption. □

Theorem 6 *Let p be a prime integer. Then $\mathbb{Z}_p[\omega]$ is a field if and only if $p = 2$ or $p \equiv 5 \,(\mathrm{mod}\, 6)$.*

Proof. If $\mathbb{Z}_p[\omega]$ is a field and $p \neq 2$ and $p \neq 5 \,(\mathrm{mod}\, 6)$, then either $p = 3$ or $p \equiv 1 \,(\mathrm{mod}\, 6)$. If $p = 3$, then we have $(2 + \omega)^2 = 0$ in $\mathbb{Z}_3[\omega]$. If $p \equiv 1 \,(\mathrm{mod}\, 6)$, then by the Lemma 6 there is $a \in \mathbb{Z}_p$ such that $a^2 + a + 1 = 0$ in $\mathbb{Z}_p$, so we have $(\omega - a)(\omega^2 - a) = 0$ in $\mathbb{Z}_p[\omega]$. Thus in either case $\mathbb{Z}_p[\omega]$ is not a field that is contrary to our assumption. Now suppose $p = 2$ or $p \equiv 5 \,(\mathrm{mod}\, 6)$. For $p = 2$, we have $\mathbb{Z}_2[\omega] = \{0, 1, \omega, \omega^2\}$ which is a field. For $p \equiv 5 \,(\mathrm{mod}\, 6)$ consider the following ring homomorphism

$$\varphi : \mathbb{Z}_p[x] \to \mathbb{Z}_p[\omega],$$
$$\varphi(x) = \omega, \varphi(m) = m, \text{ for all } m \in \mathbb{Z}_p$$

Obviously it is a surjective homomorphism. Since $\varphi(x^2 + x + 1) = \omega^2 + \omega + 1 = 0$, so $\langle x^2 + x + 1 \rangle \subseteq Ker(\varphi)$. Let a polynomial $h(x) \in Ker(\varphi)$, then since all coefficients of $x^2 + x + 1$ are 1 we have $h(x) = (x^2 + x + 1)g(x) + ax + b$, for some $g(x) \in \mathbb{Z}_p[x]$ and $a, b \in \mathbb{Z}_p$. From here we get $\varphi(h(x)) = 0$, so $a = b = 0$ in $\mathbb{Z}_p$ i.e.$\langle x^2 + x + 1 \rangle = Ker(\varphi)$ and by the canonical ring Isomorphism Theorem we have $\mathbb{Z}_p[x] / \langle x^2 + x + 1 \rangle \simeq \mathbb{Z}_p[\omega]$. Since $p \equiv 5 \,(\mathrm{mod}\, 6)$ so by the Lemma 6, $x^2 + x + 1$ is irreducible and thus $\mathbb{Z}_p[x] / \langle x^2 + x + 1 \rangle$ is a field. □

Definition 3 *An element $\pi \in \mathbb{Z}[\omega]$ is a called a prime element if whenever we have $\pi \mid \alpha\beta$, for $\alpha, \beta \in \mathbb{Z}[\omega]$, then either $\pi \mid \alpha$ or $\pi \mid \beta$.*

Corollary 1 *A prime integer $p \in \mathbb{Z}$, is a prime in $\mathbb{Z}[\omega]$ if and only if $p = 2$ or $p \equiv 5 \pmod 6$.*

Proof. This is a result of the Theorem 6 because $\mathbb{Z}[\omega]$ is an Euclidean Domain. □

Theorem 7 *If a and b are relatively prime integers, then $\mathbb{Z}[\omega] / \langle a + b\omega\rangle \simeq \mathbb{Z}_{a^2+b^2-ab}$.*

Proof. For simplicity, for $x \in \mathbb{Z}$, we will denote by$[x]$, the equivalence class$[x]_{a^2+b^2-ab}$. Since a and b are relatively prime, so $[b]^{-1}$ exists in $\mathbb{Z}_{a^2+b^2-ab}$. Now define the following mapping:

$$f : \mathbb{Z}[\omega] \to \mathbb{Z}_{a^2+b^2-ab}$$
$$f(x + y\omega) = [x] - [a][b]^{-1}[y] .$$

This is a ring homomorphism. To this ends, first note that $a^2+b^2-ab \equiv 0 \,(\mathrm{mod}\,(a^2 + b^2 - ab))$ so from here we get $[a]^2 [b]^{-2} = [a][b]^{-1} - 1$. Now for every $x+y\omega$, and $u+v\omega \in \mathbb{Z}[\omega]$ we have $(x + y\omega)(u + v\omega) = (xu - vy)+(xv + yu - vy)\omega$ and $\left([x] - [a][b]^{-1}[y]\right)\left([u] - [a][b]^{-1}[v]\right) = [xu - vy] - [a][b]^{-1}[xv + yu - vy]$, so from here we have:

$$\begin{aligned} f((x + y\omega)(u + v\omega)) &= f((xu - vy) + (xv + yu - vy)\omega) \\ &= [xu - vy] - [a][b]^{-1}[xv + yu - vy] \\ &= \left([x] - [a][b]^{-1}[y]\right)\left([u] - [a][b]^{-1}[v]\right) \\ &= f((x + y\omega)) f((u + v\omega)) . \end{aligned}$$

Also we have

$$\begin{aligned} f((x + y\omega) + (u + v\omega)) &= f((x + u) + (y + v)\omega) \\ &= [x + u] - [a][b]^{-1}[y + v] \\ &= \left([x] - [a][b]^{-1}[y]\right) + \left([u] - [a][b]^{-1}[v]\right) \\ &= f(x + y\omega) + f(u + v\omega) \end{aligned}$$

Since $f(a + b\omega) = [a] - [a][b]^{-1}[b] = [0]$, we have $\langle a + b\omega\rangle \subseteq Ker(f)$. Now let $x + y\omega \in Ker(f)$. In $\mathbb{Q}[\omega]$ we can write

$$x + y\omega = (a + b\omega)\left(\left(\frac{ax + by - bx}{a^2 + b^2 - ab}\right) + \left(\frac{ay - bx}{a^2 + b^2 - ab}\right)\omega\right)$$

Since $f(x + y\omega) = [x] - [a][b]^{-1}[y] = [0]$ we have $bx - ay = \lambda(a^2 + b^2 - ab)$ for some $\lambda \in \mathbb{Z}$. On the other hand from $bx - ay \equiv 0 \,(\mathrm{mod}\,(a^2 + b^2 - ab))$ we get $ab^2x - a^2by \equiv 0 \,(\mathrm{mod}\,(a^2 + b^2 - ab))$ which is equivalent to $ax - (a^2b^{-2})by \equiv 0 \,(\mathrm{mod}\,(a^2 + b^2 - ab))$ Since $a^2b^{-2} = ab^{-1}-1 \,(\mathrm{mod}\,(a^2 + b^2 - ab))$ we obtain $ax-ay+by \equiv ax-bx+by \equiv 0 \,(\mathrm{mod}\,(a^2 + b^2 - ab))$, so we have $ax - bx + by = \mu(a^2 + b^2 - ab)$, for some $\mu \in \mathbb{Z}$. Thus we have $x + y\omega = (a + b\omega)(\mu + \lambda\omega)$. This shows that $Ker(f) \subseteq \langle a + b\omega\rangle$. So $Ker(f) = \langle a + b\omega\rangle$. Since f is surjective by standard ring Isomorphism Theorem we have $\mathbb{Z}[\omega] / \langle a + b\omega\rangle \simeq \mathbb{Z}_{a^2+b^2-ab}$. □

Corollary 2 *If a and b are relatively prime integers, then $z = a + b\omega$ is prime in $\mathbb{Z}[\omega]$ if and only if $a^2 + b^2 - ab$ is prime in $\mathbb{Z}$.*

Theorem 8 *Up to multiplication by a unit, the prime elements in $\mathbb{Z}[\omega]$ are as follows:*

1. Every prime integer p, that is $p = 2$ or $p \equiv 5 \,(\mathrm{mod}\, 6)$.
2. Every element $\varsigma = a + b\omega$ such that $p = a^2 + b^2 - ab$ is an integer prime in $\mathbb{Z}$ such that $p \equiv 1 \,(\mathrm{mod}\, 6)$.
3. Element $z = 1 + 2\omega$.

Proof. This is an immediate consequence of the Theorems 6, 7 and the Corollaries 1 and 2. . □

Remark 1 *The prime, $z = 1 + 2\omega$ has Ramification property; the integer prime $p = 3$ is not a prime in $\mathbb{Z}[\omega]$ and we have $3 = -(1 + 2\omega)^2$. $p = 3$ is called a ramified prime in $\mathbb{Z}[\omega]$.*

Remark 2 *Every element $z = x + y\omega$ in $\mathbb{Z}[\omega]$ can be written uniquely (up to order and multiplication by a unit) as a product of primes as follows:*

$$x + y\omega = \varepsilon 2^{\alpha} \left(\prod_{\varsigma} \varsigma^{\beta_{\varsigma}} \right) \left(\prod_{i=1}^{m} p_i^{\gamma_i} \right) (1 + 2\omega)^n$$

where ε is a unit element in $\mathbb{Z}[\omega]$, $\alpha, \beta_{\varsigma}, \gamma_i$, m and n are non-negative integers, $\varsigma = a+b\omega$ are elements in $\mathbb{Z}[\omega]$ for which $p = a^2+b^2-ab$ is an integer prime in $\mathbb{Z}$ with $p \equiv 1 \,(\mathrm{mod}\, 6)$, and p_i are integer primes bigger than 3. Since for each prime number p such that $p \equiv 1 \,(\mathrm{mod}\, 6)$ there are only two distinct prime elements, $\varsigma_1 = a + b\omega$ and $\varsigma_2 = b + a\omega$ such that $p = a^2 + b^2 - ab$, (a and b are relatively prime integers), so we can rewrite this factorization as

$$x + y\omega = \varepsilon 2^{\alpha} \left(\prod_{\varsigma_1} \varsigma_1^{\beta_{\varsigma_1}} \right) \left(\prod_{\varsigma_2} \varsigma_2^{\beta_{\varsigma_2}} \right) \left(\prod_{i=1}^{m} p_i^{\gamma_i} \right) (1 + 2\omega)^n$$

2. Factor rings in $\mathbb{Z}[\omega]$and their Decompositions

Theorem 9 *Let $k \geq 1$ be an integer. Then for $n = 2k + 1$ we have*

$$\mathbb{Z}[\omega] / \langle (1 + 2\omega)^n \rangle \simeq \mathbb{Z}[x] / \left\langle 3^k x, 3^{k+1}, x^2 + x + 1 \right\rangle$$

Proof. First note that

$$\begin{aligned} (1 + 2\omega)^n &= (1 + 2\omega)^{2k+1} \\ &= (1 + 2\omega)^{2k} (1 + 2\omega) \\ &= (-3)^k (1 + 2\omega) \end{aligned}$$

Now define $f : \mathbb{Z}[x] \to \mathbb{Z}[\omega] / \langle (1+2\omega)^n \rangle$ by $f(p(x)) = p(\omega - 1) \pmod{(1+2\omega)^n}$ This is an onto ring homomorphism. Now note that

$$\begin{aligned} f\left(3^k x\right) &= 3^k (\omega - 1) \\ &= (-1)^k (1+\omega)(1+2\omega)^n \in \langle (1+2\omega)^n \rangle \end{aligned}$$

So $3^{k+1} x \in Ker(f)$. Also we have

$$\begin{aligned} f\left(3^{k+1}\right) &= 3^{k+1} \\ &= (-1)^{k+1} (1+2\omega)(1+2\omega)^n \in \langle (1+2\omega)^n \rangle \end{aligned}$$

So $3^{k+1} \in Ker(f)$. Obviously we have $x^2+x+1 \in Ker(f)$ because $\omega^2+\omega+1 = 0$, thus $\left\langle 3^{k+1}x, 3^{k+1}, x^2+x+1 \right\rangle \subseteq Ker(f)$. Conversely, let $q(x) \in Ker(f)$. Then since all coefficients of x^2+x+1 are 1, we have $q(x) = p(x)(x^2+x+1)+ax+b$, for some $p(x) \in \mathbb{Z}[x]$, and $a, b \in \mathbb{Z}$. From here we get $f(q(x)) = a(\omega-1)+b = 0 \pmod{(1+2\omega)^n}$, so we must have $a(\omega-1)+b = (c+d\omega)(1+2\omega)^n = (-3)^k (c+d\omega)(1+2\omega)$, for some $c + d\omega \in \mathbb{Z}[\omega]$. Thus we have

$$a\omega + b - a = (-3)^k (2c-d)\omega + (-3)^k (c-2d)$$

From here we must have

$$\begin{cases} a = (-3)^k (2c-d), \\ b - a = (-3)^k (c-2d) \end{cases}$$

These give us $b = (-3)^k (3c-3d) = (-1)^k (c-d)(3)^{k+1}$ and $a = (-1)^k (2c-d)(3)^k$, so $q(x) = p(x)(x^2+x+1) + \left((-1)^k (2c-d)(3)^k\right) x + \left((-1)^k (c-d)(3)^{k+1}\right) \in \left\langle 3^k x, 3^{k+1}, x^2+x+1 \right\rangle$. Now by Fundamental Isomorphism Theorem we have

$$\mathbb{Z}[\omega] / \langle (1+2\omega)^n \rangle \simeq \mathbb{Z}[x] / \left\langle 3^k x, 3^{k+1}, x^2+x+1 \right\rangle.$$

□

Lemma 7 *Let $k \geq 1$ be an integer. Then for $n = 2k$ we have*

$$\mathbb{Z}[\omega] / \langle (1+2\omega)^n \rangle \simeq \mathbb{Z}_{3^k}[\omega].$$

Proof. We have $(1+2\omega)^n = \left((1+2\omega)^2\right)^k = (-3)^k$. So $\langle (1+2\omega)^n \rangle = \left\langle 3^k \right\rangle$. Now apply the Lemma 5. □

Corollary 3 *Let $\Re_n = \mathbb{Z}[\omega] / \langle (1+2\omega)^n \rangle$. Then we have*

$$\Re_n = \begin{cases} \mathbb{Z}_3, & \text{if } n = 3 \\ \mathbb{Z}_{3^k}[\omega], & \text{if } n = 2k, k \geqslant 1 \\ \mathbb{Z}[x] / \left\langle 3^k x, 3^{k+1}, x^2+x+1 \right\rangle, & \text{if } n = 2k+1, k \geqslant 1 \end{cases}$$

Proof. This follows from the Theorems 7 and 9 and the Lemma7. □

Theorem 10 *For each element $z = x + y\omega$ in $\mathbb{Z}[\omega]$ we have*

$$\mathbb{Z}[\omega] / \langle x + y\omega\rangle \simeq \mathbb{Z}_{2^\alpha}[\omega] \oplus \mathbb{Z}_{(c^2+d^2-cd)^{\beta_{\varsigma_1}}} \oplus \mathbb{Z}_{(c^2+d^2-cd)^{\beta_{\varsigma_2}}} \oplus \mathbb{Z}_{p_1^{\gamma_1}}[\omega] \oplus \cdots \oplus \mathbb{Z}_{p_m^{\gamma_m}}[\omega] \oplus \Re_n$$

where $c + d\omega = \prod\limits_{\varsigma_1} \varsigma_1^{\beta_{\varsigma_1}}$, $d + c\omega = \prod\limits_{\varsigma_2} \varsigma_2^{\beta_{\varsigma_2}}$ *and* $\Re_n = \mathbb{Z}[\omega] / \langle (1+2\omega)^n\rangle$.

Proof. First note that, from the Remark 2, for
$x + y\omega = \varepsilon 2^\alpha \left(\prod\limits_{\varsigma_1} \varsigma_1^{\beta_{\varsigma_1}}\right)\left(\prod\limits_{\varsigma_2} \varsigma_2^{\beta_{\varsigma_2}}\right)\left(\prod\limits_{i=1}^{m} p_i^{\gamma_i}\right)(1+2\omega)^n$
we have

$$\langle x + y\omega\rangle = \left\langle 2^\alpha \left(\prod_{\varsigma} \varsigma_1^{\beta_{\varsigma_1}}\right)\left(\prod_{\varsigma} \varsigma_2^{\beta_{\varsigma_2}}\right)\left(\prod_{i=1}^{m} p_i^{\gamma_i}\right)(1+2\omega)^n\right\rangle$$

Now by standard facts in an Euclidean Domain we have
$\mathbb{Z}[\omega] / \langle x + y\omega\rangle \simeq \mathbb{Z}[\omega] / \langle 2^\alpha\rangle \oplus \mathbb{Z}[\omega] / \left\langle \prod\limits_{\varsigma_1} \varsigma_1^{\beta_{\varsigma_1}}\right\rangle \oplus \mathbb{Z}[\omega] / \left\langle \prod\limits_{\varsigma_2} \varsigma_2^{\beta_{\varsigma_2}}\right\rangle \oplus \mathbb{Z}[\omega] / \left\langle \prod\limits_{i=1}^{m} p_i^{\gamma_i}\right\rangle \oplus$
$\mathbb{Z}[\omega] / \langle (1+2\omega)^n\rangle$.
Now apply the Lemma 5 and the Theorem 7 and this fact that

$$\mathbb{Z}[\omega] / \left\langle \prod_{i=1}^{m} p_i^{\gamma_i}\right\rangle = \mathbb{Z}[\omega] / \langle p_1^{\gamma_1}\rangle \oplus \cdots \oplus \mathbb{Z}[\omega] / \langle p_m^{\gamma m}\rangle$$

□

Example 1 *Since* $22 + 26\omega = -2(2+3\omega)^2(1+2\omega)$ *we have*

$$\mathbb{Z}[\omega] / \langle 22 + 26\omega\rangle \simeq \mathbb{Z}_2[\omega] \oplus \mathbb{Z}_{49} \oplus \mathbb{Z}_3$$

Example 2 *For* $z = 49(1+3\omega)$ *we have*

$$\mathbb{Z}[\omega] / \langle 49(1+3\omega)\rangle \simeq \mathbb{Z}_7[\omega] \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_{49}$$

because we can rewrite $z = 49(1+3\omega) = -7(2+3\omega)(1+3\omega)^2$ *which is also isomorphic to* $\mathbb{Z}_{49} \oplus \mathbb{Z}_{343}$ *because* $z = 49(1+3\omega) = -(2+3\omega)^2(3+2\omega)^3$.

Acknowledgements The author would like to thank the anonymous referees for their very careful evaluation of my paper and their meaningful comments.

References

[1] John A. Beachy and William D. Blair, “Abstract Algebra ”, Third edition, Waveland Press, Inc, 2006.

[2] David M. Burton, “Elementary Number Theory”, Revised edition, Allyn and Bacon, 1980.

[3] Greg Dresden, and Wayne M. Dymacek, “Finding Factors of Factor Rings over the Gaussian Integers”, the American Mathematical Monthly, Vol. 112, No. 7, August-September 2005, pp 602-611.

[4] C. F. Gauss, “Theoria residuorum biquadraticorum”. Reprinted in Werke, George Olms Verlag, Hidelsheim, 1973.

[5] Kenneth Ireland and Michael Rosen, “A Classical Introduction to Modern Number Theory”, second edition, Springer-Verlag, 1990.

[6] Silverman, J. H., “A Friendly Introduction to Number Theory”, 3rd, Edition, Prentice Hall, 2006.

[7] E.B. Vinberg, ”A course in Algebra”, American Mathematical Society, 2003.