International Mathematical Forum, 4, 2009, no. 42, 2075 - 2086

Factor Rings and their Decompositions of an Imaginary Extension of the Ring of Integers

Manouchehr Misaghian

Mathematics Department
Prairie View A&M University
P.O. Box 519, Mail stop 2225
Prairie View, Texas 77446-0519, USA
mamisaghian@pvamu.edu

Abstract. In this paper we will characterize the structure of factor rings for $\mathbf{Z}[\xi]$ when $\xi = i\sqrt{2}$. Consequently, we can recognize prime numbers (elements) and their ramifications in $\mathbf{Z}\left[i\sqrt{2}\right]$.

Mathematics Subject Classification. 13F15, 13F07 Secondary 13F10.

Keywords: Euclidean Domain, Unique factorization Domain, Factor ring

1. Introduction.

The set of integers, $\mathbf{Z} = \{..., -n, ..., -1, 0, 1, ..., n, ...\}$, 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:
$\langle m \rangle = \{km \,|\, k \in \mathbf{Z}\}$, for all $m \in \mathbf{Z}$.

So the factor rings of $\mathbf{Z}$, are given by $\mathbf{Z}/m\mathbf{Z} = \mathbf{Z}_m$.

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*" [3]. These numbers are now known as Gaussian integers. The Gaussian

integers are sitting in the field of complex numbers, $\square$ and by inherited addition and multiplication operations from $\square$ they constitute an integral domain which is a UFD [1],[7]. In general we can consider some imaginary extensions of the ring of integers as follows.

Let $p \in \mathbf{Z}, p > 1$ 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 $\mathbf{Z}[\xi] = \left\{ a_0 + a_1\xi + \cdots + a_{p-1}\xi^{p-1} \middle| a_i \in \mathbf{Z}, 0 \leq i \leq p-1 \right\}$ with appropriate operations is an extension of $\mathbf{Z}$.

In 1847 Gabriel Lame announced that he had a complete proof of the Last Fermat's Theorem. In his proof, he used the identity $x^p + y^p = (x+y)(x+y\xi)\cdots(x+y\xi^{p-1})$ where p and ξ are as above, with the assumption that all extensions of $\mathbf{Z}$ are UFD. Before the Lame's work, Ernst Kummer had already proven that some of these extensions are not UFD. For example in $\mathbf{Z}[\sqrt{-5}]$ we have:

$$6 = 2.3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

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 R be an integral domain for which there exists a subset P such that every non zero element x of R can be written, in a unique way as

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

Where ε is a unit element in R and $v_p(x)$ are non-negative integers, all but a finitely many are zero. In the other words the set $(Rp)_{p \in \mathsf{P}}$ of principal ideals that coincide with the set of maximal principal ideals distinct from R, 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 U.F.D means that every subvariety W of dimension $n-1$ can be defined by a single equation.

One of the fundamental differences between $\mathbf{Z}$ and its extensions is the structure of their *Factor Rings*. As we know the factor rings of $\mathbf{Z}$, are $\mathbf{Z}/m\mathbf{Z} = \mathbf{Z}_m$ 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 Chinese reminder theorem to factor $\mathbf{Z}_m$ as $\mathbf{Z}_m = \mathbf{Z}_{p_1^{\alpha_1}} \oplus \mathbf{Z}_{p_2^{\alpha_2}} \oplus \cdots \oplus \mathbf{Z}_{p_r^{\alpha_r}}$.

The structure of factor rings for $\mathbf{Z}[\xi]$ is much more complicated. This structure has been studied for Gaussian integers [2]. In this paper we will characterize the structure of factor

rings for $\mathbf{Z}[\xi]$ when $\xi = i\sqrt{2}$. Consequently, we can recognize prime numbers (elements) and their ramifications in $\mathbf{Z}\left[i\sqrt{2}\right]$.

2. The ring $\mathbf{Z}\left[\sqrt{-2}\right]$ and its factor rings.

Let $\mathbf{Z}$ be the ring of integers and set

$$\mathbf{Z}\left[\sqrt{-2}\right] = \left\{a + b\sqrt{-2} \,|\, a, b \in \mathbf{Z}\right\}.$$

Lemma 2.1. $\mathbf{Z}\left[\sqrt{-2}\right]$ With the following operations is an integral Domain.

Addition: $\left(a + b\sqrt{-2}\right) + \left(c + d\sqrt{-2}\right) = (a + c) + (b + d)\sqrt{-2}$

Multiplication: $\left(a + b\sqrt{-2}\right)\left(c + d\sqrt{-2}\right) = \left(ac - 2bd\right) + \left(ad + bc\right)\sqrt{-2}$

Definition 2.1. The function $\nu : \mathbf{Z}\left[\sqrt{-2}\right] \to \{0,1,2,\cdots,n,\cdots\}$ defined by

$$\nu\left(a + b\sqrt{-2}\right) = a^2 + 2b^2$$

Is called a norm function and has the following properties:

(i)- $\nu(x) \geq 0$, foe all $x \in \mathbf{Z}\left[\sqrt{-2}\right]$. Further $\nu(x) = 0$ if and only if $x = 0$.

(ii)- $\nu\left(xy\right) = \nu\left(x\right)\nu\left(y\right)$, for all $x, y \in \mathbf{Z}\left[\sqrt{-2}\right]$.

Lemma 2.2. Above norm turns $\mathbf{Z}\left[\sqrt{-2}\right]$ into a Euclidean and hence a Principal Ideal Domain (PID), and a Unique Factorization Domain (U.F.D).

Definition 2.2. (Legendre's Symbols). Let $p \in \mathbf{Z}$ be a prime number. Then the Legendre's symbol, denoted by $\left(\frac{\cdot}{p}\right)$, for each integer, $a \in \mathbf{Z}$ is defined by

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

Theorem 2.1. The Legendre's symbol has the following property:

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

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

Proof. See any standard number theory book e.g. [5], or [7].

Theorem 2.2. (Quadratic Reciprocity Theorem). Let $p \in \mathbf{Z}$ be an odd prime number. Then:

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

(ii)-$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \text{ or } 7 \pmod 8, \\ -1, & \text{if } p \equiv 3 \text{ or } 5 \pmod 8 \end{cases}$

Proof. See [5] or [7].

Corollary 2.1. $\left(\frac{-2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \text{ or } 3 \pmod 8, \\ -1, & \text{if } p \equiv 5 \text{ or } 7 \pmod 8 \end{cases}$.

Proof. By Theorem 2.1, part (i) we have $\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right)$.

Since $p \equiv 1 \pmod 8$ and $p \equiv 5 \pmod 8$ imply $p \equiv 1 \pmod 4$,

and $p \equiv 3 \pmod 8$ and $p \equiv 7 \pmod 8$ imply $p \equiv 3 \pmod 4$ we get the result from Theorem 2.2.

Lemma 2.3. The only units (invertible) elements in $\mathbf{Z}\left[\sqrt{-2}\right]$ are ± 1.

Theorem 2.3. Let $m \in \mathbf{Z}, m > 1$ be an integer. Then

$$\mathbf{Z}\left[\sqrt{-2}\right] \Big/ \langle m \rangle \cong \mathbf{Z}_m\left[\sqrt{-2}\right]$$

Proof. Define $f : \mathbf{Z}\left[\sqrt{-2}\right] \to \mathbf{Z}_m\left[\sqrt{-2}\right]$ by:

$$f\left(a + b\sqrt{-2}\right) = [a]_m + [b]_m \sqrt{-2}$$

Where $[.]_m$ represents the equivalence class modulo *m*. Then f is an onto ring homomorphism with $\ker(f) = \langle m \rangle$. Now the result by the first homomorphism Theorem.

Proposition 2.1. A positive prime number $p \in \mathbf{Z}$, can be written as $p = a^2 + 2b^2$ for some integers $a, b \in \mathbf{Z}$, if and only if either $p = 2, p \equiv 1 (\text{mod } 8)$ or $p \equiv 3 (\text{mod } 8)$.

Proof. If $p = 2$, then $2 = 0^2 + 2(1)^2$. If $p = a^2 + 2b^2$ and $a = 0$, then b must be ± 1. Thus $p = 2$.

Let $p > 2$. If $p = a^2 + 2b^2$, then it is obvious that a must be odd, so let $a = 2k + 1$, for some $k \in \mathbf{Z}$. If $b = 2l$, for some $l \in \mathbf{Z}$, then we have

$$\begin{aligned} p &= (2k+1)^2 + 2(2l)^2 \\ &= 4k^2 + 4k + 1 + 8l^2 \\ &= 8\left(\frac{k(k+1)}{2} + l\right) + 1 \end{aligned}$$

Thus $p \equiv 1 \pmod 8$. (Note that $k(k+1)$ is divisible by 2 for all integers k.) If $b = 2l+1$ for some $l \in \mathbf{Z}$, then we have

$$\begin{aligned} p &= (2k+1)^2 + 2(2l+1)^2 \\ &= 4k^2 + 4k + 1 + 8l^2 + 8l + 2 \\ &= 8\left(\frac{k(k+1)}{2} + l(l+1) \right) + 3 \end{aligned}$$

Thus $p \equiv 3 \pmod 8$.

Now let $p > 2$ and $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$. Then from Corollary 2.1 we have $\left(\frac{-2}{p} \right) = 1$, thus there is an integer $x \in \mathbf{Z}$ such that $x^2 = -2 \pmod p$ i.e. $x^2 = -2 + pt$, for some $t \in \mathbf{Z}$ and $0 < t < p$. This is the same as $x^2 + 2(1)^2 = pt$, for some $t \in \mathbf{Z}$ and $0 < t < p$. If $t = 1$, we are done. If $t \geq 2$, then we can choose integer $y \in \mathbf{Z}$ such that

$$y \equiv x \pmod t, \text{and} -\frac{t}{2} < y < \frac{t}{2}$$

From here and reflexive property of congruence relation we get:

$$y^2 \equiv x^2 \pmod t,$$

$$2 \equiv 2 \pmod t$$

Thus $(y^2 + 2) \equiv (x^2 + 2) \equiv 0 \pmod t$. Thus for some $r \in \mathbf{Z}, 1 \leq r < t$, we have $y^2 + 2 = rt$. Since we also have $x^2 + 2 = pt$, by multiplying these two equalities side by side we will get

$$(y^2 + 2)(x^2 + 2) = prt^2 \qquad (1)$$

The product on the left hand side of this equality can be written as:

$$(y^2 + 2)(x^2 + 2) = (xy + 2)^2 + 2(x - y)^2 \qquad (2)$$

Thus by combining equations (1) and (2) we get:

$$(xy + 2)^2 + 2(x - y)^2 = prt^2$$

The relationship between x and y show that $(xy + 2)^2$ and $(x - y)^2$ are both divisible by t^2. So by dividing both sides of above equation we obtain

$$\left(\frac{xy + 2}{t} \right)^2 + 2\left(\frac{x - y}{t} \right)^2 = pr .$$

This equation shows that a smaller multiple of p can be written as $a^2 + 2b^2$. If $r = 1$, we are done, if not, we can repeat the above procedure. After a finite number of steps of repetition we get the result.

Definition 2.3. A polynomial $q(x) \in \mathbf{Z}_p[x]$ is said to be irreducible in $\mathbf{Z}_p[x]$ whenever $q(x) = a(x)b(x)$ with $a(x), b(x) \in \mathbf{Z}_p[x]$, then one of $a(x)$ or $b(x)$ has degree 0 (i.e., is a constant).

Remark 2.1. $\mathbf{Z}_p$ is the factor ring $\mathbf{Z}/p\mathbf{Z}$ which is isomorphic to the ring $\{0,1,2\cdots, p-1\}$ modulo p.

Proposition 2.2. Let $p \in \mathbf{Z}$ be an odd prime number. Then x^2+2 in $\mathbf{Z}_p[x]$ is irreducible if and only if $p \equiv 5$ or $7 \pmod 8$.

Proof. Let $p \equiv 5$ or $7 \pmod 8$. Then x^2+2 is reducible if and only if $x^2+2 \equiv 0 \pmod p$ has a solution , i.e., $\left(\frac{-2}{p}\right) = 1$. Thus by Corollary 2.1 we must have $p \equiv 1$ or $3 \pmod 8$ which is contrary to our assumption, thus x^2+2 is irreducible. Conversely let x^2+2 is irreducible in $\mathbf{Z}_p[x]$. If $p \not\equiv 5$ or $7 \pmod 8$ then $p \equiv 1$ or $3 \pmod 8$. So $\left(\frac{-2}{p}\right) = 1$ i.e., there is some $a \in \mathbf{Z}$ such that $a^2 \equiv -2 \pmod p$; from here we get $x^2+2 = (x+a)(x-a)$ which is contrary to our assumption.

Theorem 2.4. Let $p \in \mathbf{Z}$ be an odd prime number such that $p \equiv 5$ or $7 \pmod 8$. Then $\mathbf{Z}_p[\sqrt{-2}]$ is a field.

Proof. Define $f : \mathbf{Z}_p[x] \to \mathbf{Z}_p[\sqrt{-2}]$ by:

$$f(a) = a, \qquad a \in \mathbf{Z}_p$$
$$f(x) = \sqrt{-2}$$

And extend it to $\mathbf{Z}_p[x]$ as a ring homomorphism. Now note that f is onto with $\ker(f) = \langle x^2+2 \rangle$. Since $p \equiv 5$ or $7 \pmod 8$ by proposition 2.2, x^2+2 is irreducible in $\mathbf{Z}_p[x]$, thus $\mathbf{Z}_p[x]/\langle x^2+2 \rangle$ is a field. Now apply the first Isomorphism Theorem.

Theorem 2.5. Let a and b be two integers that are relatively prime. Then

$$\mathbf{Z}[\sqrt{-2}] \Big/ \langle a + b\sqrt{-2} \rangle \cong \mathbf{Z}_{a^2+2b^2}$$

Proof. Since $a,$ and b are relatively prim so a and a^2+2b^2, and b and a^2+2b^2 are relatively prime as well. So $a^{-1},$ and b^{-1} exist and $a^{-1}, b^{-1} \in \mathbf{Z}_{a^2+2b^2}$. Now define $f : \mathbf{Z}\left[\sqrt{-2}\right] \to \mathbf{Z}_{a^2+2b^2}$ by

$$f\left(x+y\sqrt{-2}\right) = x - ab^{-1}y \left(\operatorname{mod} a^2+2b^2\right)$$

Then f is an onto ring homomorphism:

$$\begin{aligned} f\left(x+y\sqrt{-2}+x'+y'\sqrt{-2}\right) &= f\left(\left(x+x'\right)+\left(y+y'\right)\sqrt{-2}\right) \\ &= \left(x+x'\right) - ab^{-1}\left(y+y'\right)\left(\operatorname{mod} a^2+2b^2\right) \\ &= \left(x-ab^{-1}y\right)+\left(x'-ab^{-1}y'\right)\left(\operatorname{mod} a^2+2b^2\right) \\ &= f\left(x+y\sqrt{-2}\right)+f\left(x'+y'\sqrt{-2}\right) \end{aligned}$$

Before we show that f preserves rings multiplicative structures note that:

$$a^2+2b^2 \equiv 0\left(\operatorname{mod} a^2+2b^2\right) \Rightarrow a^2b^{-2}+2 \equiv 0\left(\operatorname{mod} a^2+2b^2\right)$$

Thus $\left(ab^{-1}\right)^2 \equiv -2\left(\operatorname{mod} a^2+2b^2\right)$. Now from here we get:

$$\begin{aligned} f\left(\left(x+y\sqrt{-2}\right)\left(x'+y'\sqrt{-2}\right)\right) &= f\left(\left(xx'-2yy'\right)+\left(xy'+x'y\right)\sqrt{-2}\right) \\ &= \left(xx'-2yy'\right) - ab^{-1}\left(xy'+x'y\right)\left(\operatorname{mod} a^2+2b^2\right) \\ &= \left(x-ab^{-1}y\right)\left(x'-ab^{-1}y'\right)\left(\operatorname{mod} a^2+2b^2\right) \\ &= f\left(x+y\sqrt{-2}\right) f\left(x'+y'\sqrt{-2}\right) \end{aligned}$$

Since $f\left(a+b\sqrt{-2}\right) = a-ab^{-1}b = 0,$ so $\left\langle a+b\sqrt{-2}\right\rangle \subset \ker\left(f\right).$ Now let $x+y\sqrt{-2} \in \ker\left(f\right)$. Then we have

$$x-ab^{-1}y \equiv 0\left(\operatorname{mod} a^2+2b^2\right)$$

i.e.

$$x-ab^{-1}y = k\left(a^2+2b^2\right) \Leftrightarrow bx-ay = kb\left(a^2+2b^2\right), \text{ for some } k \in \mathbf{Z} \qquad (3)$$

From equation on the right hand side of (3) we deduce that *b* must divide *y* because *a* and *b* are relatively prime. So $y = \lambda b$, for some $\lambda \in \mathbf{Z}$. From here and (3) we get

$$x = \lambda a + k\left(a^2 + 2b^2\right),$$

$$\begin{aligned} x + y\sqrt{-2} &= \lambda a + k\left(a^2 + 2b^2\right) + \lambda b\sqrt{-2} \\ &= \lambda\left(a + b\sqrt{-2}\right) + k\left(a^2 + 2b^2\right) \\ &= \lambda\left(a + b\sqrt{-2}\right) + k\left(a - b\sqrt{-2}\right)\left(a + b\sqrt{-2}\right) \\ &= \left(\left(\lambda + ka\right) - b\sqrt{-2}\right)\left(a + b\sqrt{-2}\right) \end{aligned}$$

Thus $x + y\sqrt{-2} \in \left\langle a + b\sqrt{-2}\right\rangle$, i.e., $\ker(f) \subset \left\langle a + b\sqrt{-2}\right\rangle$. So $\ker(f) = \left\langle a + b\sqrt{-2}\right\rangle$. It is obvious that *f* is onto, so the result.

Corollary 2.2. Up to a sign, there are three type prime elements in $\mathbf{Z}\left[\sqrt{-2}\right]$ as follows:

(i)- $\varpi = p$, where $p \in \mathbf{Z}$ is a prime such that $p \equiv 5$ or $7 \pmod 8$.

(ii)- $\pi = a + b\sqrt{-2}$ Such that $a^2 + 2b^2$ is a prime in $\mathbf{Z}$.

(iii)- $\tau = \sqrt{-2}$

Proof. This is a consequence of the Theorems 2.4 and 2.5.

Remark 2.2. $\tau = \sqrt{-2}$ is a prime of the type $\pi = a + b\sqrt{-2}$, however, we consider it separately because, this prime is related to the ramified prime.

Corollary 2.3. Every element $\zeta = a + b\sqrt{-2} \in \mathbf{Z}\left[\sqrt{-2}\right]$ can be factored as:

$$\zeta = a + b\sqrt{-2} = \varepsilon\left(\prod_i \varpi^{\alpha_i}{}_i\right)\left(\prod_j \pi^{\beta_j}{}_j\right)\left(\sqrt{-2}\right)^n$$

Where $\varepsilon \in \{-1, 1\}$, α_i, β_j, and n are non-negative integers and $\alpha_i = 0, \beta_j = 0$, for almost all i and j. $\varpi_i \in \mathbf{Z}$ is a prime such that $\varpi_i \equiv 5$ or $7 \pmod 8$, and $\nu\left(\pi_j\right)$ is a prime in $\mathbf{Z}$. Let $u + v\sqrt{-2} = \prod_j \pi^{\beta_j}{}_j$. Then one can easily show that *u* and *v* are relatively prime and $\prod_j \left|\pi^{\beta_j}{}_j\right| = u^2 + 2v^2$. Thus by Theorem 2.5 we have:

$$\mathbf{Z}\left[\sqrt{-2}\right] \Big/ \left\langle \prod_j \pi^{\beta_j}{}_j \right\rangle \cong \mathbf{Z}_{u^2+2v^2}$$

Also by Theorem 2.3 we have $\mathbf{Z}\left[\sqrt{-2}\right] \Big/ \left\langle \prod_i \varpi^{\alpha_i}{}_i \right\rangle \cong \mathbf{Z}_P\left[\sqrt{-2}\right]$, where $P = \prod_i \varpi^{\alpha_i}{}_i$.

Now let $\zeta_n = \left(\sqrt{-2}\right)^n$. Then $\zeta_n = \begin{cases} (-2)^k, & \text{if } n = 2k \\ (-2)^k \sqrt{-2}, & \text{if } n = 2k+1 \end{cases}$. From here and by Theorem 2.3 we get:

$$\mathbf{Z}\left[\sqrt{-2}\right] \Big/ \left\langle \zeta_n \right\rangle \cong \mathbf{Z}_{2^k}\left[\sqrt{-2}\right]$$

Whenever n = 2k. For other cases we have:

Theorem 2.6. For n = 1, we have:

$$\mathbf{Z}\left[\sqrt{-2}\right] \Big/ \left\langle \zeta_1 \right\rangle = \mathbf{Z}\left[\sqrt{-2}\right] \Big/ \left\langle \sqrt{-2} \right\rangle \cong \mathbf{Z}_2$$

Proof. Define $f : \mathbf{Z}\left[\sqrt{-2}\right] \to \mathbf{Z}_2$ by $f\left(x + y\sqrt{-2}\right) = \left[x\right]_2$. Here $\left[x\right]_2$ is the equivalence class modulo 2. f is an onto ring homomorphism:

$$\begin{aligned} f\left(\left(x + y\sqrt{-2}\right) + \left(x' + y'\sqrt{-2}\right)\right) &= f\left(\left(x + x'\right) + \left(y + y'\right)\sqrt{-2}\right) \\ &= \left[x + x'\right]_2 \\ &= \left[x\right]_2 + \left[x'\right]_2 \\ &= f\left(x + y\sqrt{-2}\right) + f\left(x' + y'\sqrt{-2}\right) \end{aligned}$$

and

$$\begin{aligned} f\left(\left(x + y\sqrt{-2}\right)\left(x' + y'\sqrt{-2}\right)\right) &= f\left(\left(xx' - 2yy'\right) + \left(xy' + x'y\right)\sqrt{-2}\right) \\ &= \left[xx' - 2yy'\right]_2 \\ &= \left[x\right]_2\left[x'\right]_2 \\ &= f\left(x + y\sqrt{-2}\right) f\left(x' + y'\sqrt{-2}\right) \end{aligned}$$

Since $f\left(\sqrt{-2}\right) = \left[0\right]_2$, so $\left\langle \sqrt{-2} \right\rangle \subset \ker\left(f\right)$. Now let $x + y\sqrt{-2} \in \ker\left(f\right)$, then $f\left(x + y\sqrt{-2}\right) = \left[x\right]_2 = \left[0\right]_2$ so $x = 2l$, for some $l \in \mathbf{Z}$. From here we get

$$x + y\sqrt{-2} = 2l + y\sqrt{-2} = \left(y - l\sqrt{-2}\right)\sqrt{-2} \in \left\langle \sqrt{-2} \right\rangle$$

Thus $\ker\left(f\right) = \left\langle \sqrt{-2} \right\rangle$. Now the result by the first Isomorphism Theorem.

Theorem 2.7. Let $n = 2k+1$ and $k > 0$. Then $\zeta_n = (-2)^k \sqrt{-2}$ and from here $\langle \zeta_n \rangle = \left\langle (2)^k \sqrt{-2} \right\rangle$. In this case we have:

$$\mathbf{Z}\left[\sqrt{-2}\right] \Big/ \left\langle (2)^k \sqrt{-2} \right\rangle \cong \mathbf{Z}[x] \Big/ \left\langle 2^k x, 2^{k+1}, x^2+2 \right\rangle$$

Proof. Define $f : \mathbf{Z}[x] \to \mathbf{Z}\left[\sqrt{-2}\right] \Big/ \left\langle (2)^k \sqrt{-2} \right\rangle$ by

$$f\left(p(x)\right) = \left[p\left(\sqrt{-2}\right) \right], \text{ for } p(x) \in \mathbf{Z}[x]$$

Here $\left[p\left(\sqrt{-2}\right) \right] = \left[p\left(\sqrt{-2}\right) \right]_{\left\langle 2^k \sqrt{-2} \right\rangle}$ is equivalence class modulo $\left\langle 2^k \sqrt{-2} \right\rangle$. f as evaluation function is a ring homomorphism. It is onto because for every $\left[a + b\sqrt{-2} \right] \in \mathbf{Z}\left[\sqrt{-2}\right] \Big/ \left\langle 2^k \sqrt{-2} \right\rangle$ if we take $p(x) = a + bx$ we have

$$\begin{aligned} f\left(p(x)\right) &= f(a+bx) \\ &= \left[a + b\sqrt{-2} \right] \end{aligned}$$

Obviously we have

$$\begin{aligned} f\left(2^k x\right) &= \left[2^k \sqrt{-2} \right] \\ &= [0] \end{aligned}$$

and

$$\begin{aligned} f\left(2^{k+1}\right) &= \left[2^{k+1} \right] \\ &= \left[-\sqrt{-2}\left(2^k \sqrt{-2}\right) \right] \\ &= [0] \end{aligned}$$

and

$$\begin{aligned} f\left(x^2+2\right) &= \left[\left(\sqrt{-2}\right)^2 + 2 \right] \\ &= [0] \end{aligned}$$

So $\left\langle 2^k x, 2^{k+1}, x^2+2 \right\rangle \subset \ker(f)$. Now let $p(x) \in \ker(f)$. Then by division algorithm in $\mathbf{Z}[x]$ we have

$$p(x) = q(x)\left(x^2+2\right) + ax + b, \text{ for some } q(x) \in \mathbf{Z}[x], \text{ and } a, b \in \mathbf{Z}.$$

Then one gets

$$\begin{aligned} f\left(p(x)\right) &= \left[a\sqrt{-2}+b\right] \\ &= [0] \end{aligned}$$

This forces us to have

$$a\sqrt{-2}+b = \lambda 2^k\sqrt{-2}, \text{ for some } \lambda = c+d\sqrt{-2} \in \mathbf{Z}\left[\sqrt{-2}\right]$$

So we have

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

And this gives us $a=-2^{k+1}d,$ and $b=2^k c$. From here we have

$$\begin{aligned} p(x) &= q(x)\left(x^2+2\right)+\left(-2^{k+1}d\right)+2^k cx \\ &= q(x)\left(x^2+2\right)+c\left(2^k x\right)-d\left(2^{k+1}\right) \in \left\langle 2^k x, 2^{k+1}, x^2+2\right\rangle \end{aligned}$$

Thus $\ker(f) \subset \left\langle 2^k x, 2^{k+1}, x^2+2\right\rangle$. This shows that $\ker(f) = \left\langle 2^k x, 2^{k+1}, x^2+2\right\rangle$. Now proof is complete.

Corollary 2.4. Let notation be as in the Corollary 2.3 and onward. Then:

$$\mathbf{Z}\left[\sqrt{-2}\right] \Big/ \left\langle a+b\sqrt{-2}\right\rangle \cong \mathbf{Z}_P\left[\sqrt{-2}\right] \oplus \mathbf{Z}_{u^2+2v^2} \oplus \mathbf{Z}\left[\sqrt{-2}\right] \Big/ \left\langle \zeta_n \right\rangle$$

Where

$$\mathbf{Z}\left[\sqrt{-2}\right] \Big/ \left\langle \zeta_n \right\rangle \cong \begin{cases} \mathbf{Z}_{2^k}\left[\sqrt{-2}\right], \text{if } n=2k, k\in\mathbf{Z}, k>0, \\ \mathbf{Z}_2, \qquad\quad \text{if } n=1, \\ \mathbf{Z}[x] \Big/ \left\langle 2^k x, 2^{k+1}, x^2+2\right\rangle, \text{ if } n=2k+1, k\in\mathbf{Z}, k>0, \end{cases}$$

Proof. This is a consequence of the Chinese Remainder Theorem and Theorems 2.3, 2.5, 2.6, and 2.7 along with the Corollaries.

Remark. 2.3. The prime number $2 \in \mathbf{Z}$ is a ramified prime for $\mathbf{Z}\left[\sqrt{-2}\right]$, because $\langle 2 \rangle = \left\langle \sqrt{-2} \right\rangle^2$. In fact 2 is no longer a prime in $\mathbf{Z}\left[\sqrt{-2}\right]$, it is associate to the square of a prime in $\mathbf{Z}\left[\sqrt{-2}\right]$, i.e. $2 = -\left(\sqrt{-2}\right)^2$.

References

1. John A. Beachy and William D. Blair, "Abstract Algebra", Third edition, Waveland Press, Inc, 2006.

2. 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.

3. C. F. Gauss, "Theoria residuorum biquadraticorum". Reprinted in Werke, George Olms Verlag, Hidelsheim, 1973.

4. Thomas W. Hungerford, "Algebra", Springer-Verlag, New York, 1974.

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

6. Manouchehr Misaghian, "Gaussian Prime Numbers", Journal of Mathematics Culture, and Thought, Iranian Mathematical Society, No. 39, pp 45-54, fall 2007.

7. Silverman, J. H., "A Friendly Introduction to Number Theory", 2nd Edition, Prentice Hall, 2001.

Received: March, 2009