International Mathematical Forum, Vol. 9, 2014, no. 31, 1521 - 1537
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/imf.2014.111121

Finding Factors of Factor Rings over Eisenstein Integers

Valmir Buçaj

Department of Mathematics, Texas Lutheran University
1000 West Court Street, Seguin, TX 78155

Dedicated to my parents, Afrim and Drita Buçaj.

Abstract

In this paper we prove a few results related to the factor rings over the Eisenstein integers. In particular we show that the ring $\mathbb{Z}[\omega]$ factored by an ideal generated by any element $m + n\omega$ of this ring, where $g.c.d(m, n) = 1$ is isomorphic to the ring $\mathbb{Z}_{m^2+n^2-mn}$. Next, we find the representatives for the equivalence classes of the ring $\mathbb{Z}[\omega]$ when factoring out by a power of a prime ideal, and also identify all the units of these quotient rings respectively. Then, we give a representation for the factor ring $\mathbb{Z}[\omega]/\langle m + n\omega \rangle$ in terms of the product of other rings. Finally, we end this paper with a few applications to elementary number theory.

Mathematics Subject Classification: Primary 13F15, 13F07, 13B02; Secondary 11D09, 11A51

Keywords: Eisenstein Integers; Eisenstein Primes; Factor Rings; Prime Ideals; Norm; Equivalence Classes; Units

1 Introduction

Eisenstein integers are defined to be the set $Z[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ where $\omega = (-1 + i\sqrt{3})/2$. This set lies inside the set of complex numbers $\mathbb{C}$ and they form a commutative ring in the algebraic number field $\mathbb{Q}(\omega)$. We can define a *ring norm* $N : \mathbb{Z}[\omega] \to \mathbb{Z}^+ \cup \{0\}$ by $N(m + n\omega) = (m + n\omega)(m + n\bar{\omega}) = m^2 + n^2 - mn$, and it is easy to check that N is *multiplicative*; that is, $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$, for all $\alpha, \beta \in \mathbb{Z}[\omega]$.

Proposition 1.1. For $\omega = (-1+i\sqrt{3})/2$, the ring $Z[\omega]$ is a Euclidean Domain.

Proof. Let $\alpha = a+b\omega, \beta = c+d\omega$ be two elements of the ring $\mathbb{Z}[\omega]$ with $\beta \neq 0$. Then in the algebraic number field $\mathbb{Q}(\omega)$ we have

$$\frac{\alpha}{\beta} = t + s\omega, \text{ where } t = \frac{ab + cd - ad}{c^2 + d^2 - cd}, \text{ and } s = \frac{bc - ad}{c^2 + d^2 - cd}.$$

Let p, q be two integers such that $|t - p| \leq \frac{1}{2}$ and $|s - q| \leq \frac{1}{2}$.
Let $\phi = (t - p) + (s - q)\omega$, and let $r = \beta\phi$. Then we get

$$\begin{aligned} r =& \beta\phi \\ =& \beta[(t - p) + (s - q)\omega] \\ =& \beta\left[(t + s\omega) - (p + q\omega)\right] \\ =& \beta\left(\frac{\alpha}{\beta} - (p + q\omega)\right) \\ =& \alpha - \beta(p + q\omega). \end{aligned}$$

We notice that $r \in \mathbb{Z}[\omega]$.

Finally, we have

$$\alpha = \beta(p + q\omega) + r. \tag{1}$$

To conclude the proof, we need to show that $N(r) < N(\beta)$.
So,

$$\begin{aligned} N(r) &= N(\beta\phi) \\ &= N(\beta)N(\phi) \\ &= N(\beta)\left((t - p)^2 + (s - q)^2 - (t - p)(s - q)\right) \\ &\leq N(\beta)\left(\frac{1}{4} + \frac{1}{4} + \frac{1}{4}\right) \\ &= \frac{3}{4}N(\beta), \end{aligned}$$

which is even stronger than necessary. □

Since $\mathbb{Z}[\omega]$ is a Euclidean Domain, it follows that it is also a Principal Ideal Domain and a Unique Factorization Domain.

Fact 1.2. If $\omega = (-1 + i\sqrt{3})/2$ then

$$\mathbb{Z}[\omega] = \{\sum_{i=0}^{n} a_i\omega^i : a_i \in \mathbb{Z}\} = \{a + b\omega : \ a, b \in \mathbb{Z}\}.$$

Proof. We start by observing that ω is a root of the second degree polynomial $x^2 + x + 1$. So,

$$\omega^2 = -\omega - 1. \tag{2}$$

Therefore, from (2) it is easily seen that $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$. □

We know that (See [5]) an element $\alpha = a + b\omega$ is a unit in $\mathbb{Z}[\omega]$ if and only if $N(\alpha) = \pm 1$, where in our case $N(a + b\omega) = (a + b\omega)(a + b\bar{\omega}) = a^2 - ab + b^2$.

Using this fact it readily follows that the only units in $\mathbb{Z}[\omega]$ are $\{\pm 1, \pm\omega, \pm\bar{\omega}\}$.

Fact 1.3. Let $\alpha = m + n\omega \in \mathbb{Z}[\omega]$. If $N(\alpha) = p$, where p is a prime in $\mathbb{Z}$, then α is irreducible in $\mathbb{Z}[\omega]$.

Proof. Let $\alpha = \gamma \cdot \beta$ where $\gamma, \beta \in \mathbb{Z}[\omega]$. Then $N(\alpha) = m^2 + n^2 - mn = N(\beta) \cdot N(\gamma) = p$. Since $N(\beta), N(\gamma) \in \mathbb{Z}$, it follows that $N(\beta) = \pm 1$ and $N(\gamma) = p$, or vice-versa. Thus, β is a unit in $\mathbb{Z}[\omega]$, which concludes the proof. □

Fact 1.4. Up to associates and an integer multiple, $\alpha = 1 - \omega$ is the only element of $\mathbb{Z}[\omega]$ that is associate with its conjugate.

Proof. Let $\alpha = a+b\omega$ and $u \in \{\pm 1, \pm\omega, \pm\bar{\omega}\}$. We want to know when $\alpha = u\cdot\bar{\alpha}$, where $\bar{\alpha} = a + b\bar{\omega}$. The proof is straightforward, one merely needs to check the truth of the equation for all such u. □

2 Preleminary Results

Theorem 2.1. *If q is a positive integer larger than* 1*, then*

$$\mathbb{Z}[\omega]/\langle q\rangle \cong \mathbb{Z}_q[\omega].$$

Proof. Define $\phi : \mathbb{Z}[\omega] \to \mathbb{Z}_q[\omega]$, by $\phi(m + n\omega) = [m]_q + [n]_q\omega$. First we show that ϕ is a surjective ring homomorphism. The mapping is clearly surjective, so we need to show only that it is a homomorphism. Let $\alpha = a + b\omega$, and $\beta = c + d\omega$. Then

$$\begin{aligned}\phi(\alpha + \beta) =& [a + c]_q + [b + d]_q\omega \\ =& ([a]_q + [b]_q\omega) + ([c]_q + [d]_q\omega) \\ =& \phi(\alpha) + \phi(\beta).\end{aligned}$$

Next, after a few calculations and using tha fact that $\omega^2 = -1 - \omega$, we find that

$$\alpha \cdot \beta = (ac - bd) + (ad + bc - bd)\omega. \tag{3}$$

So,

$$\phi(\alpha \cdot \beta) = [ac - bd]_q + [ad + bc - bd]_q\omega.$$

In a simmilar fashion we find that

$$\phi(\alpha) \cdot \phi(\beta) = [ac - bd]_q + [ad + bc - bd]_q\omega,$$

concluding that ϕ is a ring homomorphism.

Now we show that $ker(\phi) = \langle q \rangle$. Since $\phi(q) = [q]_q = [0]_q = 0$, it follows that $q \in ker(\phi)$. Since $ker(\phi)$ is an ideal we have $\langle q \rangle \subset ker(\phi)$.

To show the reverse inclusion let $\alpha = m + n\omega \in ker(\phi)$. Then, $\phi(\alpha) = \phi(m + n\omega) = [m]_q + [n]_q\omega = 0$, so both $m \equiv 0 \pmod q$ and $n \equiv 0 \pmod q$. So, there are integers m', n' such that $m = m'q$ and $n = n'q$. Then, $m + n\omega = q(m' + n'\omega)$ which shows that $m + nw \in \langle q \rangle$, and thus $\ker(\phi) \subset \langle q \rangle$. Finally, since $\ker(\phi) = \langle q \rangle$, by the First Isomorphism Theorem, we have

$$\mathbb{Z}[\omega]/\langle q \rangle \cong \mathbb{Z}_q[\omega],$$

which is what we wanted to show. □

Lemma 2.2. *Let $\omega = (-1 + i\sqrt{3})/2$. The following conditions are equivalent for a prime p of $\mathbb{Z}$:*
(1) *p is an irreducible element in $\mathbb{Z}[\omega]$;*
(2) *$x^2 + x + 1$ is an irreducible polynomial in $\mathbb{Z}_p[\omega]$;*
(3) $p \equiv 2 \pmod 3$.

For a proof see [1], page 426.

Proposition 2.3. If p is a positive integer larger than 1, then $\mathbb{Z}_p[\omega]$ is a field if and only if p is a prime such that $p \equiv 2 \pmod 3$.

Proof. One can show that the following ring isomorphism holds (See [1]):

$$\mathbb{Z}[\omega]/\langle p\rangle \cong \mathbb{Z}_p[\omega]/\left\langle x^2+x+1\right\rangle. \tag{4}$$

Suppose that $\mathbb{Z}_p[\omega]$ is a field. Then by Theorem 2.1, $\mathbb{Z}_p[\omega]$ is isomorphic to $\mathbb{Z}[\omega]/\langle p\rangle$, thus $\mathbb{Z}[\omega]/\langle p\rangle$ is a field as well. Then, by (4) $\mathbb{Z}_p[\omega]/\langle x^2+x+1\rangle$ is a field, and we know that this happens if and onl if x^2+x+1 is an irreducible polynomial in $\mathbb{Z}_p[x]$. Then the result follows by Lemma 2.2. □

Lemma 2.4. *Let m and n be two relatively prime integers. Then m and m^2+n^2-mn are relatively prime as well.*

Proof. First we show that m and m^2+n^2 are relatively prime. Let $(m, m^2+n^2) = d$, so $m = kd$ and $m^2+n^2 = hd$, for some integers h and k, also since $(m,n) = 1$ there are some integers x, y such that $mx+ny = 1$. Then

$$\begin{aligned} n &= n(mx+ny)\\ &= mnx+n^2y\\ &= mnx+(hd-m^2)y\\ &= mnx+hdy-m^2y\\ &= m(nx-my)+d(hy)\\ &= d(knx-mky)+d(hy)\\ &= d[knx-mky+hy]. \end{aligned}$$

So, d divides n. Thus, since $d|m$ and $d|n$ it follows that $d|1$, thus $d = 1$.

Now let $(m, m^2+n^2-mn) = r$, so there are some integers h, k such that $m = kr$ and $m^2+n^2-mn = hr$. Then

$$\begin{aligned} m^2+n^2 &= (m^2+n^2)(mx+(m^2+n^2)y)\\ &= (m^2+n^2)mx+(m^2+n^2)^2y\\ &= r[kx(m^2+n^2)]+(hr+mn)^2y\\ &= r[kx(m^2+n^2)]+(hr+krn)^2y\\ &= r[kx(m^2+n^2)+r(h+kn)^2y]. \end{aligned}$$

So, since $r|(m^2+n^2)$, $r|m$ and the fact that $mx+(m^2+n^2)y = 1$, for some integers x, y, it follows that $r|1$, which is possible only if $r = 1$. □

Theorem 2.5. *Let m and n be two integers that are relatively prime, then*

$$\mathbb{Z}[\omega]/\langle m+n\omega\rangle \cong \mathbb{Z}_{m^2+n^2-mn}.$$

Proof. First, we wish to note that it suffices to prove the theorem for the case where both m and n are positive integers. From Lemma 2.4 we know that m and m^2+n^2-mn are relatively prime, so the equivalence class of m has an inverse in $\mathbb{Z}_{m^2+n^2-mn}$, that is $([m]_{m^2+n^2-mn})^{-1}$ exists. Using this fact and the fact that $m^2+n^2-mn \equiv 0 \pmod{m^2+n^2-mn}$, we find that $(mn^{-1})^2 \equiv mn^{-1}-1 \pmod{m^2+n^2-mn}$.

Now, let us define a mapping $\phi : \mathbb{Z}[\omega] \to \mathbb{Z}_{m^2+n^2-mn}$, by $\phi(x+yw) = x-(mn^{-1})y$ modulo m^2+n^2-mn. It is not difficult to see that ϕ is surjective and preserves addition. Next we show that it preserves multiplication as well.

Let $\alpha = a+bw$, and $\beta = c+dw$ be two elements from $\mathbb{Z}[\omega]$. Then

$$\begin{aligned}
\phi(\alpha)\cdot\phi(\beta) &= (a-(mn^{-1})b)(c-(mn^{-1})d)\\
&= ac-(mn^{-1})ad-bc(mn^{-1})+(mn^{-1})^2bd\\
&= ac-(mn^{-1})(ad+bc)+(mn^{-1}-1)bd\\
&= (ac-bd)-(mn^{-1})(ad+bc-bd)\\
&= \phi\left((ac-bd)+(ad+bc-bd)w\right)\\
&= \phi\left(a+bw)(c+dw)\right)\\
&= \phi(\alpha\cdot\beta).
\end{aligned}$$

So, ϕ is a surjective ring homomorphism.

Our next task is to show that $\ker(\phi) = \langle m+n\omega\rangle$. Since $\phi(m+n\omega) = m-(mn^{-1})n = m-m = 0$, it follows that $m+nw \in \ker(\phi)$, and thus $\langle m+nw\rangle \subset \ker(\phi)$.

To show the reverse inclustion, let $c+dw \in \ker(\phi)$, then

$$\frac{c+dw}{m+n\omega} = \frac{cm+dn-cn}{m^2+n^2-mn} + \frac{dm-cn}{m^2+n^2-mn}w = x+yw. \tag{5}$$

Then, since $\phi(c+d\omega) = c-(mn^{-1})d \equiv 0$, multiplying both sides by n we get $cn-md \equiv 0$, which shows that y is an integer. Now, multiplying the last expression first by n and then by $(m^{-1})^2$ and using the fact that $(nm^{-1})^2 \equiv nm^{-1}-1$ we get $cm+dn-cn \equiv 0$, which shows that x is an integer as well. Thus, from the relation in (5) follows that $c+dw$ is a multiple of $m+nw$, so $c+dw \in \langle m+nw\rangle$, which shows that $\ker(\phi) \subset \langle m+n\omega\rangle$. Finally, since $\ker(\phi) = \langle m+n\omega\rangle$, the result follows from the Frist Isomorphism Theorem. □

Next we state an important corollary to the above theorem which caracterizes primes in $\mathbb{Z}[\omega]$.

Corollary 2.6. If m and n are relatively prime integers, then $\alpha = m + n\omega$ is a prime in $\mathbb{Z}[\omega]$ if and only if $N(\alpha) = m^2 + n^2 - mn$ is a prime in $\mathbb{Z}$.

Proof. The proof follows immediately from the above theorem. □

Remark 2.7. We wish to note that $N(\alpha) \equiv 0, 1 \pmod 3$.

Theorem 2.8. *Up to associates, the primes in* $\mathbb{Z}[\omega]$ *are:*

(1) $\sigma = m + n\omega$ *and* $\sigma' = n + m\omega$, *where* $N(\sigma) = m^2 + n^2 - mn$ *is a prime in* $\mathbb{Z}$ *and* $N(\sigma)$ *is congruent to* 1 *modulo* 3;

(2) $\sigma = p$, *where* p *is a prime in* $\mathbb{Z}$ *and* $p \equiv 2 \pmod 3$.

(3) $\sigma = 1 - \omega$.

Proof. The proof follows readily from Lemma 2.2 and Corollary 2.6 above. □

Remark: We will refer to the primes in $(1), (2)$ and (3) as Eisenstein primes of the first, second, and third kind, respectively.

Given a nonzero Eisenstein integer $\alpha = m + n\omega \in \mathbb{Z}[\omega]$, we can factor it into primes as follows:

$$m + n\omega = \omega^r \cdot \prod \sigma_k^{u_k} \cdot \prod {\sigma'_k}^{v_k} \cdot \prod p_k^{e_k} \cdot (1 - \omega)^t, \tag{6}$$

where r, t, u_k, v_k, e_k are nonnegative integers with $u_k \leq v_k$, $N(\sigma_k), N(\sigma'_k)$ are integers congruent to either 0 or 1 modulo 3, and p_k are integers congruent to 2 modulo 3.

3 Main Results

Before we state our main results, we prove the following proposition.

Proposition 3.1. Let p be a prime in $\mathbb{Z}^+$. The following conditions are equivalent:

(1) $p \equiv 0 \pmod 3$ or $p \equiv 1 \pmod 3$,

(2) the congruence $x^2 + x \equiv -1 \pmod p$ has a solution in $\mathbb{Z}$,

(3) $p = m^2 + n^2 - mn$.

Let us first prove the following two lemmas.

Lemma 3.2. *Let* p *be a prime in* $\mathbb{Z}^+$. *If* p *is composite in* $\mathbb{Z}[\omega]$, *then* p *must be of the form* $m^2 + n^2 - mn$, *for some* $m, n \in \mathbb{Z}$.

Proof. Since p is composite in $\mathbb{Z}[\omega]$, there exist non-units $\alpha, \beta \in \mathbb{Z}[\omega]$, such that $p = \alpha \cdot \beta$. Then, $N(p) = p^2 = N(\alpha)N(\beta)$. Since $N(\alpha) \neq 1$ and $N(\beta) \neq 1$, it follows that $N(\alpha) = N(\beta) = p$. So, if $\alpha = m+n\omega$, then $N(\alpha) = m^2+n^2-mn = p$, which is what we wanted to show. □

Lemma 3.3. *Let p be a prime in $\mathbb{Z}^+$. If p divides $(1-\omega x)(1-\bar{\omega}x)$ then p is not a prime in $\mathbb{Z}[\omega]$.*

Proof. To contradiction, suppose that p is a prime in $\mathbb{Z}[\omega]$. Then, since $p|(1-\omega x)(1-\bar{\omega}x)$, it follows that $p|(1-\omega x)$ or $p|(1-\bar{\omega}x)$. If $p|(1-\omega x)$, then $(1-\omega x) = p(m+n\omega)$, for some $m+n\omega \in \mathbb{Z}[\omega]$. But then $pm = 1$, which is not possible sine $p, m \in \mathbb{Z}$. On the other hand, if $p|(1-\bar{\omega}x)$, then $(1-\bar{\omega}x) = p(m+n\omega)$. Using the fact that $\bar{\omega} = -\omega - 1$, it follows that $p(m-n) = 1$, which is again impossible since $p, m, n \in \mathbb{Z}$. This concludes the proof. □

Now we return to the main proof.

Proof. First we show that (1) implies (2). When $p = 3$ the proof is trivial. So, let $p = 3k+1$, for some $k \in \mathbb{Z}$, and consider the following polynomial factorization:

$$X^{p-1} - 1 = \left(X^{(p-1)/3}\right)^3 - 1 \tag{7}$$

$$= \left(X^{(p-1)/3} - 1\right)\left(X^{(2p-2)/3} + X^{(p-1)/3} + 1\right). \tag{8}$$

Next we will count the roots of these polynomials modulo p. By Fermat's little theorem, the left polynomial in (7) has $p-1$ roots modulo p. On the other hand, the first polynomial in (8) has degree $(p-1)/3$, so it can have at most $(p-1)/3$ roots modulo p. Therefore, the second polynomial in (8) must have some root r modulo p, as well. That is r satisfies

$$r^{(2p-2)/3} + r^{(p-1)/3} \equiv -1 \pmod{p}.$$

Therefore, since $p = 3k+1$ we have

$$\left(r^k\right)^2 + r^k \equiv -1 \pmod{p},$$

which proves the first part.

Now we show that (2) implies (3) by showing that (2) implies that p is composite in $\mathbb{Z}[\omega]$. Since $x^2+x \equiv -1 \pmod{p}$, it means that $p|(x^2+x+1)$, in $\mathbb{Z}$. Since $x^2+x+1 = (1-\omega x)(1-\bar{\omega}x)$, in $\mathbb{Z}[\omega]$ this relation can be interpreted as

$$p|(1-\omega x)(1-\bar{\omega}x).$$

Then, by Lemma 3.3, p is composite in $\mathbb{Z}[\omega]$ and therefore, by Lemma 3.2, it must be of the form m^2+n^2-mn. This proves (3).

That (3) implies (1) follows readily by Remark 2.7. This concludes the proof! □

Now, we are ready to state and prove the main results of this paper. In the first theorem we find representatives for the equivalence classes for the ring $\mathbb{Z}[\omega]$ when factored out by some power of a prime ideal, then we identify the units in these quotient rings respectively, and finally in the last theorem we give a decomposition of the ring $\mathbb{Z}[\omega]$ when factored out by some ideal.

Theorem 3.4. *The equivalence classes of* $\mathbb{Z}[\omega]$ *modulo a power of a prime are as follows:*

(1) $\mathbb{Z}[\omega]/\langle p^n\rangle = \{[a+b\omega]_{p^n} : 0 \le a \le p^n-1$ *and* $0 \le b \le p^n-1\}$, *where* p *is a prime in* $\mathbb{Z}$ *such that* $p \equiv 2 \pmod 3$*;*

(2) $\mathbb{Z}[\omega]/\langle \pi^n\rangle = \{[a]_{\pi^n} : 0 \le a \le q^n-1\}$, *where* q *is a prime in* $\mathbb{Z}$ *such that* $q \equiv 1 \pmod 3$, *and* π *is a prime factor of* q *in* $\mathbb{Z}[\omega]$ (*i.e.* $q = \pi\bar{\pi}$);

(3) $\mathbb{Z}[\omega]/\langle \alpha^{2m}\rangle = \{[a+b\omega]_{\alpha^{2m}} : 0 \le a \le 3^m-1,$ *and* $0 \le b \le 3^m-1\}$, *where* $\alpha = 1-\omega$;

(4) $\mathbb{Z}[\omega]/\langle \alpha^{2m+1}\rangle = \{[a+b\omega]_{\alpha^{2m+1}} : 0 \le a \le 3^{m+1}-1,$ *and* $0 \le b \le 3^m-1\}$, *where* $\alpha = 1-\omega$.

Proof. First let us show that the equivalence classes in (1) are distinct. Suppose that $[a+b\omega]_{p^n} = [c+d\omega]_{p^n}$. Then p^n must divide both $a-c$ and $b-d$. But since $0 \le a-c, b-d \le p^n-1$, it follows that $a=c$ and $b=d$. Thus, the classes in (1) are distinct.

Now, let $\alpha = a+b\omega$ be some element of $\mathbb{Z}[\omega]$. We will show that it belongs to one of the equivalence classes in (1). Reducing both a and b modulo p^n, that is $a \equiv x \pmod{p^n}$ and $b \equiv y \pmod{p^n}$ we get

$$a+b\omega = x+t_1p^n+(y+t_2p^n)\omega = (x+y\omega)+(t_1+t_2\omega)p^n \in \mathbb{Z}[\omega]/\langle p^n\rangle,$$

which is what we needed to show.

Now, as before, we first show that the equivalence classes in (2) are distinct. If $[x]_{\pi^n} = [y]_{\pi^n}$, then π^n divides $x-y$. Then, there exists some $\alpha \in \mathbb{Z}[\omega]$ such that $\pi^n \cdot \alpha = x-y$. Taking the conjugates we get $\bar{\pi}^n\bar{\alpha} = \overline{x-y} = x-y$ (since, x and y are integers), so $\bar{\pi}^n$ also divides $x-y$. But, since $q^n = \pi^n\bar{\pi}^n$, and π and $\bar{\pi}$ are not associates, then q^n must divide $x-y$ as well. Since, $0 \le x-y \le q^n-1$, this is possible only when $x=y$, proving that the equivalence classes of $\mathbb{Z}[\omega]/\langle \pi^n\rangle$ are distinct.

Next, we want to show that any element $\alpha = x + y\omega$ belongs to one of the equivalence classes in (2). Observe, that since x and y belong to one of the classes in (2), it suffices to show that ω belongs to one of the equivalence classes of $\mathbb{Z}[\omega]/\langle\pi^n\rangle$.

Let $\pi^n = c + d\omega$ (we wish to note that π is an Eisenstein prime of the first kind). First, we show that c and d are relatively prime. Let p be a prime in $\mathbb{Z}$ such that $p \equiv 2 \pmod 3$, then by Theorem 2.8, p is also a prime in $\mathbb{Z}[\omega]$. To contradiction, suppose that p divides $c + d\omega$. Then, p would have to be an associate to π, that is, $\pi = u \cdot p$, for some $u \in \{\pm 1, \pm\omega, \pm\bar{\omega}\}$. But, then we would get for the norm of π, $N(\pi) = p^2$, which by Corollary 2.6 would contradict the fact that π is a prime in $\mathbb{Z}[\omega]$. If $p = 3$, then since $3 = (1-\omega)\cdot(1-\bar{\omega})$, and $\pi \neq (1-\omega)$, it is clear that 3 cannot divide $c + d\omega$. Next, if p is a prime in $\mathbb{Z}$ such that $p \equiv 1 \pmod 3$, then by Proposition 3.1, $p = \sigma \cdot \bar{\sigma}$, for some Eisenstein prime, σ, of the first kind. If p divides $c + d\omega$, then this would imply that both σ and $\bar{\sigma}$ divide π. So, then for some $u_1, u_2 \in \{\pm 1, \pm\omega, \pm\bar{\omega}\}$ we would have $\pi = u_1\sigma = u_2\bar{\sigma}$. This in turn would imply that $\sigma = u\bar{\sigma}$ for some unit u, which by Fact 1.4 is not possible. The contradiction we arrived at demonstrates that $g.c.d(c, d) = 1$. So, there are some integers s, t such that $cs + td = 1$. After a few calculations one finds $\omega - s(c + d\omega)(\omega + 1) - (c + d\omega)t$ to be a real number. From this, it follows that ω is congruent modulo $c + d\omega = \pi^n$ to a real number, say r, in $\mathbb{Z}[\omega]$; that is, $\omega \equiv r \pmod{\pi^n}$. Then, if we reduce r by multiples of q^n, we find that ω belongs to one of the equivalence classes of $\mathbb{Z}[\omega]/\langle\pi^n\rangle$, which is what we wanted to show.

Again, let us first show that the equivalence classes in (3) are distinct. First, observe that because $(1-\omega)^2 = -3\omega$, we have $\langle(1-\omega)^{2m}\rangle = \langle 3^m\rangle$, and thus $\mathbb{Z}[\omega]/\langle\alpha^{2m}\rangle = \mathbb{Z}[\omega]/\langle 3^m\rangle$. Now, if $[a + b\omega]_{3^m} = [c + d\omega]_{3^m}$, then 3^m must divide both $a-c$ and $b-d$. But, since $0 \leq a-b,\ c-d < 3^m$, then it follows that $a = b$ and $c = d$. Thus, the equivalence classes in (3) are distinct. Now, let $\alpha = x + y\omega$ be any element in $\mathbb{Z}[\omega]$. Then, as we did in (1) above, by reducing each x and y modulo 3^m we get α to be in one of the equivalence classes in (3).

Lastly,, as before, we will first show that the equivalence classes in (4) are distinct. First, we notice that $\langle\alpha^{2m+1}\rangle = \langle(1-\omega)^{2m}(1-\omega)\rangle = \langle 3^m\alpha\rangle$. Now, if $[a + b\omega]_{\alpha^{2m+1}} = [c + d\omega]_{\alpha^{2m+1}}$, where $0 \leq a, c \leq 3^{m+1} - 1$ and $0 \leq b, d \leq 3^m - 1$, then $(a - c) + (b - d)\omega \equiv 0 \pmod{3^m\alpha}$, in $\mathbb{Z}[\omega]$. So,

$$(a - c) + (b - d)\omega = \gamma\ 3^m\alpha, \text{ for some } \gamma \in \mathbb{Z}[\omega].$$

Then,

$$[2(a-c)-(b-d)]+[(a-c)+(b-d)]\omega = 3^{m+1}\gamma.$$

Thus,

$$3^{m+1}|[2(a-c)-(b-d)] \text{ and } 3^{m+1}|[(a-c)+(b-d)], \tag{9}$$

so it must divide also $2[(a-c)+(b-d)]-[2(a-c)-(b-d)] = 3(b-d)$. Then, 3^m divides $(b-d)$, which implies that $b=d$. Now, from the second expression in (9), it follows that 3^{m+1} divides $(a-c)$, which in turn implies that $a=c$.

Next, let $\gamma = x+y\omega$. If we reduce x and y by multiples of 3^{m+1} we get $\gamma \equiv c+d\omega \pmod{3^{m+1}}$, where $c,d<3^{m+1}$. Now, if $d<3^m$, then γ belongs to one of the classes in (4). Otherwise, suppose $d=3^m+k$, where $k<3^m$. Then,

$$c+d\omega = (c+3^m)+k\omega-3^m\alpha.$$

Then

$$\gamma \equiv (c+3^m)+k\omega \pmod{3^m\alpha},$$

and by reducing $c+3^m$ by powers of 3^{m+1} we get γ to be in one of the classes in (4). This concludes the proof! □

Notice that the above theorem implies that $\mathbb{Z}[\omega]/\langle p^n\rangle$ has p^{2n} elements, $\mathbb{Z}[\omega]/\langle \pi^n\rangle$ has q^n, elements and $\mathbb{Z}[\omega]/\langle \alpha^n\rangle$ has 3^n elements. This is a special case of Theorem 2.5 which we have proved in the previous section.

The next result helps us identify the units of the quotient rings mentioned in Theorem 3.4. Below we let q, π, p, and α be as in Theorem 3.4.

Theorem 3.5. *Let $[a]_{\pi^n}$ be in $\mathbb{Z}[\omega]/\langle \pi^n\rangle$. Then $[a]_{\pi^n}$ is a unit if and only if a and q are relatively prime. Let $[a+b\omega]_{p^n}$ be in $\mathbb{Z}[\omega]/\langle p^n\rangle$. Then $[a+b\omega]_{p^n}$ is a unit if and only if a or b is relatively prime with p. Let $[a+b\omega]_{\alpha^n}$ be in $\mathbb{Z}[\omega]/\langle \alpha^n\rangle$. Then $[a+b\omega]_{\alpha^n}$ is a unit if and only if $2a \not\equiv b \pmod 3$.*

Proof. Let $[a]_{\pi^n}$ be in $\mathbb{Z}[\omega]/\langle \pi^n\rangle$. Then $[a]_{\pi^n}$ is a unit if and only if there is some $\gamma \in \mathbb{Z}[\omega]$ such that $[a]_{\pi^n}\cdot[\gamma]_{\pi^n} = [1]$ in $\mathbb{Z}[\omega]/\langle \pi^n\rangle$, or equivalently $a\cdot\gamma \equiv 1 \pmod{\pi^n}$ in $\mathbb{Z}[\omega]$. Then $a\cdot\gamma+\beta\cdot\pi^n = 1$, for some $\beta \in \mathbb{Z}[\omega]$. But this means that a and π are relatively prime, and since $q=\pi\cdot\bar{\pi}$, then a and q must be relatively prime as well. Next, let $[a+b\omega]_{p^n}$ be a unit in $\mathbb{Z}[\omega]/\langle p^n\rangle$. This is possible if and only if there is some $\gamma \in \mathbb{Z}[\omega]/\langle p^n\rangle$ such that $(a+b\omega)\cdot\gamma+(\beta p^{n-1})\cdot p = 1$, which is true if and only if p and $a+b\omega$ are relatively prime. But, since p is a prime in $\mathbb{Z}$ such that $p \equiv 2 \pmod 3$ and thus is a prime in $\mathbb{Z}[\omega]$ as well, then p is relatively prime to $a+b\omega$ if and only if p is relatively prime to a or b. Next, following the same logic as before,

$[a+b\omega]_{\alpha^n}$ is a unit in $\mathbb{Z}[\omega]/\langle\alpha^n\rangle$ if and only if $(a+b\omega)$ and $\alpha = 1-\omega$ are relatively prime; that is if and only if $1-\omega$ does not divide $a+b\omega$. But since

$$\frac{a+b\omega}{1-\omega} = \frac{2a-b}{3} + \frac{a+b}{3}\omega, \tag{10}$$

then (10) is an Eisenstein integer if and only if $2a \equiv b \pmod 3$. Therefore, $\alpha = 1-\omega$, does not divide $a+b\omega$ if and only if $2a \not\equiv b \pmod 3$. This concludes the proof! □

Example 3.6. Let $\pi = 3+\omega$. Observe that π is a prime and $\pi\cdot\bar{\pi} = 7$. Then by Theorem 3.4 and 3.5 we know that:

$$\mathbb{Z}[\omega]/\left\langle\pi^2\right\rangle = \{[0],[1],[2],...,[48]\}.$$

Moreover, an element $[a]$ of this ring is a unit if and only if 7 does not divide a. Next we find the equivalence class to which ω belongs. Since $\pi^2 = 8+5\omega$, we have $5\omega \equiv -8 \pmod{\pi^2}$. Multiplying both sides by 10 we get $50\omega \equiv -80 \pmod{\pi^2}$, and since π^2 divides 49 we have $\omega \equiv 18 \pmod{\pi^2}$. So, $\omega \in [18]_{\pi^2}$. We can check this result directly as well; that is since

$$\frac{\omega-18}{8+5\omega} = -1+2\omega,$$

then $\pi^2 = 8+5\omega$ divides $\omega-18$ in $\mathbb{Z}[\omega]$, but this in turn means that $\omega \equiv 18 \pmod{\pi^2}$, so ω belongs to $[18]_{\pi^2}$.

In what follows, let us adopt the foollowing notation $\alpha = \prod N(\sigma_k)^{u_k}, \beta = \prod N(\sigma_k')^{\,v_k}, \gamma = \prod p_k^{e_k}$. Observe that $N(m+n\omega) = \alpha\cdot\beta\cdot\gamma^2$, and that α divides β.

Theorem 3.7. *If m and n are integers not both zero, and $R_t = \mathbb{Z}[\omega]/\langle(1-\omega)^t\rangle$, then the following hold:*

$$\mathbb{Z}[\omega]/\langle m+n\omega\rangle \cong \mathbb{Z}_\alpha \oplus \mathbb{Z}_\beta \oplus \mathbb{Z}_\gamma[\omega] \oplus \mathbb{Z}_{3^{t/2}}[\omega] \qquad \textit{for } t \textit{ even},$$

and

$$\mathbb{Z}[\omega]/\langle m+n\omega\rangle \cong \mathbb{Z}_\alpha \oplus \mathbb{Z}_\beta \oplus \mathbb{Z}_\gamma[\omega] \oplus R_t \qquad \textit{for } t \textit{ odd}.$$

Proof. By the factorization in (6) we can write

$$\langle m+n\omega\rangle = \left\langle \prod \sigma_k^{u_k}\cdot\prod \sigma_k'^{\,v_k}\cdot\prod p_k^{e_k}\cdot(1-\omega)^t \right\rangle. \tag{11}$$

Since $\prod \sigma_k^{u_k}$, $\prod {\sigma'_k}^{v_k}$, $(1-\omega)^t$, and $\prod p_k^{e_k}$ are pairwise relatively prime and $\mathbb{Z}[\omega]$ is a Euclidean domain we can appeal to the Chinese Remainder Theorem for rings and use (11) to get

$$\begin{aligned}\mathbb{Z}[\omega]/\langle m+n\omega\rangle \cong \mathbb{Z}[\omega]/\left\langle \prod \sigma_k^{u_k}\right\rangle \oplus \mathbb{Z}[\omega]/\left\langle \prod {\sigma'_k}^{v_k}\right\rangle \\ \oplus \mathbb{Z}[\omega]/\left\langle \prod p_k^{e_k}\right\rangle \oplus \mathbb{Z}[\omega]/\left\langle (1-\omega)^t\right\rangle. \end{aligned} \tag{12}$$

Our next task is to demonstrate that (12) implies our claimed result. Let $\prod \sigma_k^{u_k} = c + d\omega$. We want to show that c and d are relatively prime so that we can appeal to Theorem 2.5 to obtain our desired result. Let p be a prime in $\mathbb{Z}$ such that $p \equiv 2 \pmod 3$. Then since all such p are also prime in $\mathbb{Z}[\omega]$, it follows that p cannot divide $c + d\omega$. For if p were to divide $c + d\omega$, then there would exist some k such that p would divide σ_k, as well. Then $\sigma_k = s \cdot p$, for some $s \in \{\pm 1, \pm\omega, \pm\bar{\omega}\}$. But then, $N(\sigma_k) = p^2$, contradicting the fact that σ_k is a prime in $\mathbb{Z}[\omega]$. If $p = 3$, then p clearly cannot divide $c + d\omega$. Next, if $p \equiv 1 \pmod 3$, then by Proposition 3.1, up to a unit we have $p = \sigma_k \cdot \sigma'_k$, for some k(since $\bar{\sigma}_k = \bar{\omega}\sigma'_k$), therefore it cannot divide $c + d\omega$. So, since c and d are relatively prime integers, by Theorem 2.5, we conclude that

$$\mathbb{Z}[\omega]/\left\langle \prod \sigma_k^{u_k}\right\rangle \cong \mathbb{Z}[\omega]/\langle c+d\omega\rangle \cong \mathbb{Z}_{N(c+d\omega)} \cong \mathbb{Z}_\alpha. \tag{13}$$

The last isomorphism in (13) follows from the fact that the norm function N is multiplicative. Similarly we have

$$\mathbb{Z}[\omega]/\left\langle \prod {\sigma'_k}^{v_k}\right\rangle \cong \mathbb{Z}_\beta. \tag{14}$$

Also, by Theorem 2.1 we have

$$\mathbb{Z}[\omega]/\langle\gamma\rangle \cong \mathbb{Z}_\gamma[\omega]. \tag{15}$$

The last term by definition is R_t. However, for t even R_t simplifies. That is, since $(1-\omega)^2 = -3\omega$, then we have $\langle (1-\omega)^t\rangle = \left\langle (-\omega\cdot 3)^{t/2}\right\rangle = \left\langle 3^{t/2}\right\rangle$. Thus, for t even we have

$$\mathbb{Z}[\omega]/\left\langle (1-\omega)^t\right\rangle \cong \mathbb{Z}_{3^{t/2}}[\omega]. \tag{16}$$

Finally, the result follows by (12), (13), (14), (15), and (16). □

3.1 Applications

Below we present a few applications to elementary number theory.

Proposition 3.8. Let p be a prime that is not congruent to 2 (mod 3). Then, the equation $p = m^2 + n^2 - mn$ has at most four solutions(not necessarily distinct) for $m, n \in \mathbb{Z}^+$, and $m \geq n$.

Proof. By Proposition 3.1, we know there is a solution to $p = m^2 + n^2 - mn$. Suppose that there is another solution to this equation, namely there are $m_1, n_1 \in \mathbb{Z}^+$ such that $p = m_1^2 + n_1^2 - m_1 n_1$. Then, making use of the prime factorization of p in $\mathbb{Z}[\omega]$ and setting these expressions for p equal to one another we get $(m + n\omega)(m + n\bar{\omega}) = (m_1 + n_1\omega)(m_1 + n_1\bar{\omega})$. Since prime factorization in $\mathbb{Z}[\omega]$ is unique (remember $\mathbb{Z}[\omega]$ is a U.F.D) we have one of the following two possibilities: $m + n\omega = u(m_1 + n_1\omega)$ or $m + n\omega = u(m_1 + n_1\bar{\omega})$, where $u \in \{\pm 1, \pm\omega, \pm\bar{\omega}\}$.

Case 1. Suppose $m + n\omega = u(m_1 + n_1\omega)$.

(i) If $u = \pm 1$, then $m_1 = \pm m$ and $n_1 = \pm n$;

(ii) If $u = \pm\omega$, then $n_1 = \mp m$ and $m_1 = \pm n \mp m$;

(iii) If $u = \pm\bar{\omega}$, then $m_1 = \mp n$ and $n_1 = \pm m \mp n$.

Case 2. Suppose $m + n\omega = u(m_1 + n_1\bar{\omega})$.

(i) If $u = \pm 1$, then $n_1 = \mp n$ and $m_1 = \pm m \mp n$;

(ii) If $u = \pm\omega$, then $n_1 = \pm n$ and $m_1 = \pm m$;

(iii) If $u = \pm\bar{\omega}$, then $m_1 = \mp m$ and $n_1 = \pm n \mp m$.

So, the only other two solutions of the equation $p = m^2 + n^2 - mn$ are $(m, m - n)$ and $(m - n, m)$. Notice, that if $m = 2n$ then we get only two distinct solutions, namely (m, n) and (n, m). □

Proposition 3.9. A positive integer M is of the form $M = m^2 + n^2 - mn$, where $m, n \in \mathbb{Z}$ if and only if any prime $p|M$ such that $p \equiv 2 \pmod 3$ occurs to an even power in the prime factorization of M.

Proof. Observe that $M = m^2 + n^2 - mn$ if and only if $N(\alpha) = M$ for some $\alpha \in \mathbb{Z}[\omega]$; that is if and only if M is the norm of some element in $\mathbb{Z}[\omega]$.

Let

$$M = \prod p_i^{e_i} \prod q_j^{f_j}$$

be the prime factorization for M in $\mathbb{Z}^+$, where each $p_i \equiv 2 \pmod 3$ and $q_j \not\equiv 2 \pmod 3$. Then, by Proposition 3.1, each $q_j = \pi_j\bar{\pi}_j$, where π_j is an Eisenstein prime of the first or third kind. So,

$$M = \prod p_i^{e_i} \prod \pi_j^{f_j}\bar{\pi}_j^{f_j}, \tag{17}$$

is the prime factorization of M in $\mathbb{Z}[\omega]$.

Now, suppose that $M = m^2 + n^2 - mn$, for some $m, n \in \mathbb{Z}$; that is, suppose that $N(\alpha) = M$, for some $\alpha \in \mathbb{Z}[\omega]$. Let

$$\alpha = \prod r_i^{u_i} \prod s_j^{v_j}$$

be the prime factorization of α in $\mathbb{Z}[\omega]$ where each of $r_i \equiv 2 \pmod 3$ and each of s_j is an Eisenstein prime of the first or third kind. Then,

$$\bar{\alpha} = \prod r_i^{u_i} \prod \bar{s}_j^{v_j},$$

is the prime factorization of $\bar{\alpha}$. Then, since $N(\alpha) = \alpha\bar{\alpha} = M$, we get

$$\alpha\bar{\alpha} = \prod r_i^{2u_i} \prod s_j^{v_j} \bar{s}_j^{v_j} = M = \prod p_i^{e_i} \prod \pi_j^{f_j} \bar{\pi}_j^{f_j}.$$

Since, $\mathbb{Z}[\omega]$ is a U.F.D we must have $e_i = 2u_i$, which is what we wanted to prove.

On the other hand, suppose that any prime $p|M$ such that $p \equiv 2 \pmod 3$ occurs to an even power in the prime factorization of M. Then, as in (17) let

$$M = \prod p_i^{e_i} \prod \pi_j^{f_j} \bar{\pi}_j^{f_j},$$

be the factorization of M in $\mathbb{Z}[\omega]$, but now, in addition, suppose that $e_i = 2t_i$, for some integer t_i; that is

$$M = \prod p_i^{2t_i} \prod \pi_j^{f_j} \bar{\pi}_j^{f_j}.$$

Now, let

$$\alpha = \prod p_i^{t_i} \prod \pi_j^{f_j}, \text{ then } \bar{\alpha} = \prod p_i^{t_i} \prod \bar{\pi}_j^{f_j}.$$

Then

$$\alpha\bar{\alpha} = \prod p_i^{2t_i} \prod \pi_j^{f_j} \bar{\pi}_j^{f_j} = M.$$

Let $\alpha = m + n\omega$, then since $N(\alpha) = \alpha\bar{\alpha} = m^2 + n^2 - mn$, we conclude that $M = m^2 + n^2 - mn$, for some $m, n \in \mathbb{Z}$, as we wanted to show. □

Below we present a different proof of the infinitude of primes of the form $3k + 1$. This proof relies on one of our previous results in this paper, but its methodology is similar to one of the methods used to prove the infinitude of primes of the form $4k + 1$. To the best of our knowledge, the proof we present here has not appeared in this form elsewhere.

Proposition 3.10. There are infinitely many primes of the form $3k+1$.

Proof. The statement is equivalent to saying that there are infinitely many primes that are congruent to 1 mod 3. Then, by Proposition 3.1 it is sufficient to prove that there are infinitely many primes p that divide the polynomial $f(x) = x^2 + x + 1$, for some value in $\mathbb{Z}$. To contradiction, suppose there are only a finite number of primes $p_1, p_2, ..., p_n$ that divide $f(x)$. Then, consider

$$g(y) = f(p_1 \cdot p_2 \cdot ... \cdot p_n y) = (p_1 \cdot p_2 \cdot ... \cdot p_n)^2 y^2 + (p_1 \cdot p_2 \cdot ... \cdot p_n)y + 1.$$

Clearly since all $g(y)$ are contained in $f(x)$, the only primes that divide $g(y)$ are p_i for $i = 1, 2, .., n$. But since

$$g(y) \equiv 1 \pmod{p_i}, \qquad \text{for } i = 1, 2, ..., n,$$

then $g(1) = (p_1 \cdot p_2 \cdot ... \cdot p_n)^2 + (p_1 \cdot p_2 \cdot ... \cdot p_n) + 1 > 1$ is not divisible by any of the primes p_i, a contradiction, hence the statement of the proposition. □

3.2 Conclusion Remarks

We would like to end this note with a conjecture and some suggestions for further investigation.

Conjecture 3.11. If m, n, and d are positive integers with m and n relatively prime, then the equivalence classes of $\mathbb{Z}[\omega]/\langle dm + dn\omega\rangle$ are $\{[x + y\omega] : 0 \leq x < d(m^2 + n^2 - mn), 0 \leq y < d\}$.

It would also be of interest to have a generalization of Theorem 3.5; that is, a result which would characterize all the units in the quotient ring $\mathbb{Z}[\omega]/\langle dm + dn\omega\rangle$.

Acknowledgment

The author would like to thank Dr. William Hager of Texas Lutheran University for his guidance, invaluable suggestions, and comments which have increased the quality of this paper.

References

[1] John A. Bechy and William D. Blair. *Abstract Algebra*. Waveland Press, INC, third edition, 2006.

[2] Keith Conrad. *The Gaussian Integers*. Pre-Print, paper edition, 2008.

[3] James T. Cross. The euler ϕ function in the gaussian integers. *The American Mathematical Monthly*, 90(8):518–528, 1983.

[4] Al Cuoco. Meta-problems in mathematics. *The College Mathematics Journal*, 31(5):373–378, 2000.

[5] Greg Dersden and Wayne M. Dymacek. Finding factors of factor rings over the gaussian integers. *The American Mathematical Monthly*, 112(7):602–611, 2005.

[6] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Wiley, INC, second edition, 1999.

[7] Judy L. Smith; Joseph A. Gallian. Factoring finite factor rings. *Mathematics Magazine*, 58(2):93–95, 1985.

[8] Richard B. Lakein. Computation of the ideal class group of certain complex quartic fields. ii. *Mathematics of Computation*, 29(129):137–144, 1975.

Received: November 1, 2011