

2015

Application of the Euler Phi Function in the Set of Gaussian Integers

Catrina A. May

University of North Georgia, camay1224@uga.edu

Follow this and additional works at: http://digitalcommons.northgeorgia.edu/honors_theses



Part of the [Physical Sciences and Mathematics Commons](#)

Recommended Citation

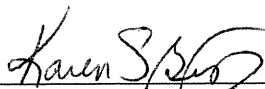
May, Catrina A., "Application of the Euler Phi Function in the Set of Gaussian Integers" (2015). *Honors Theses*. 11.
http://digitalcommons.northgeorgia.edu/honors_theses/11

This Honors Thesis is brought to you for free and open access by the Honors Program at Nighthawks Open Institutional Repository. It has been accepted for inclusion in Honors Theses by an authorized administrator of Nighthawks Open Institutional Repository.


Accepted by the Honors Faculty
of the University of North Georgia

In partial fulfillment of the requirements for the Degree of Bachelor of Science


Thesis Committee:




Thesis Chair



Committee Member



Committee Member



Director, Honors Program

Application of the Euler- ϕ Function in $\mathbb{Z}[i]$

Catrina May
University of North Georgia
Advisor: Dr. Karen Briggs

Introduction

Integral domains behave mathematically like the set of integers, and as a result, mathematicians are often interested in applying properties and functions of \mathbb{Z} to other integral domains in order more thoroughly analyze these sets. One such integral domain is the set of Gaussian Integers, denoted $\mathbb{Z}[i]$. The set of Gaussian Integers shares many characteristics with the set of integers, and it has multiple algebraic and number theoretic applications, including identification of pythagorean triples. In addition to being an integral domain, $\mathbb{Z}[i]$, like \mathbb{Z} , is further classified as both a unique factorization domain and a euclidean domain. Along with the Gaussian Norm Function, these classifications allow us to analyze relative primality within the set. Because of this, the the Euler- ϕ function, which has historically been applied to \mathbb{Z} , can also be analyzed within the set of Gaussian Integers.

Background

The Euler- ϕ Function

The Euler- ϕ function, denoted $\phi(n)$ is a multiplicative function defined by:

$$\phi(n) = |\{x \in \mathbb{Z} : 1 \leq x < n : (x, n) = 1\}| \text{ where } (x, n) = \gcd(x, n)$$

More simply, $\phi(n)$ represents the number of integers less than n that are relatively prime to n . It is important to note that if p is a prime integer, $\phi(p) = p - 1$.

Example 1.1: $\phi(15) = 8$ since there are 8 positive integers less than 15, namely, 1, 2, 4, 7, 8, 11, 13, 14.

Example 1.2: $\phi(23) = 22$ since 23 is a prime integer.

Since \mathbb{C} and its subsets do not have the same ype of ordering as \mathbb{Z} , the previous definition of the function may be difficult to apply in the set of Gaussian Integers. Therefore, we need to look at an alternate definition in order to look at the functions evaluation within $\mathbb{Z}[i]$. To do so, we will first need to look at the multiplicative property of the function. The multiplicative nature of the ϕ function is helpful in the functions evaluation. The following theorems will be used to prove the multiplicativity of ϕ .

Theorem 1.3: Let $a, n \in \mathbb{Z}$ such that $a < n$. Then a and n are relatively prime if and only if a is invertible modulo n .

Proof: Let $a, n \in \mathbb{Z}$ such that $a < n$, and assume that a and n are relatively prime. Then we know $ax + ny = 1$ for some $x, y \in \mathbb{Z}$. This implies that $ny = 1 - ax$. Rewriting, we see that $n(-y) = ax - 1$, implying that $n|(ax - 1)$. By definition of modular congruence, we know that $ax \equiv 1 \pmod{n}$. So a is invertible modulo n .

Next, assume that $a, n \in \mathbb{Z}$ such that $a < n$ and a is invertible modulo n . Then $aj \equiv 1 \pmod{n}$ for some $j \in \mathbb{Z}$. This implies that $n|aj - 1$, meaning that $nk = aj - 1$ for some $k \in \mathbb{Z}$. Therefore, $nk - aj = -1$. Rewriting, we see that $n(-k) + a(j) = 1$. So we know that $(a, n) = 1$. Thus, a and n are relatively prime. ■

By Theorem 1.3, we can see that

$$\phi(n) = |\{x \in \mathbb{Z} : 1 \leq x < n | (x, n) = 1\}| = |U(\mathbb{Z}_n)|$$

Theorem 1.4: Let $m, n, x \in \mathbb{Z}$ with $\gcd(m, n) = 1$ and $mn = x$. For all $y \in \mathbb{Z}$, $\gcd(y, x) = 1$ if and only if $\gcd(y, m) = 1$ and $\gcd(y, n) = 1$.

Proof: Let $m, n, x \in \mathbb{Z}$ with $\gcd(m, n) = 1$ and $mn = x$.

First, assume that y and m are not relatively prime or y and n are not relatively prime. Without loss of generality, assume that $\gcd(m, y) = d$ for some $d \in \mathbb{Z}$ where $d > 1$. Then $d|y$ and $d|m$. Furthermore, since $d|m$ and $m|x$, we know that $d|x$. So we have $d|x$ and $d|y$ for $d \in \mathbb{Z}$ with $d > 1$. Thus, $\gcd(x, y) > 1$ implying that x and y are not relatively prime.

Next, assume that $\gcd(m, y) = 1$ and $\gcd(n, y) = 1$. Then $ma + yb = 1$ and $nj + yk = 1$ for some $a, b, j, k \in \mathbb{Z}$. Then we can say $(ma + yb)(nj + yk) = (1)(nj + yk)$. Expanding on the right and substituting on the left, we see that $mn(aj) + y(mak) + y(bnj) + y(byk) = (1)(1)$. Thus, $x(aj) + y(mak + bnj + byk) = 1$. Therefore, $\gcd(x, y) = 1$. ■

We can now use this theorem to prove the following:

Theorem 1.5: If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

Proof: Let $m, n \in \mathbb{Z}$ such that $\gcd(m, n) = 1$. By Theorems 1.3 and 1.4, we can say

$$\begin{aligned} \phi(mn) &= |\{x \in U(\mathbb{Z}_{mn})\}| \\ &= |\{(y, z) \in U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)\}| \\ &= |U(\mathbb{Z}_m)||U(\mathbb{Z}_n)| \\ &= \phi(m)\phi(n). \quad \blacksquare \end{aligned}$$

While this function can be evaluated by listing all numbers less than n and analyzing them individually, this method becomes inefficient when n becomes sufficiently large. Luckily, there is a less tedious way to evaluate the function.

Theorem 1.6: If $(p_1^{\alpha_1})(p_2^{\alpha_2})\dots(p_k^{\alpha_k})$ is the unique prime factorization of some $n \in \mathbb{Z}^+$, then $\phi(n) = \prod_{i=1}^k (p_i - 1)(p_i^{\alpha_i - 1})$.

Note: Let $a \in \mathbb{Z}$ such that $(p_1^{\alpha_1})(p_2^{\alpha_2})\dots(p_k^{\alpha_k})$ is the prime factorization of a . By definition of primality, we know that $p_i \neq p_j$ for any $1 \leq i < j \leq k$. Since we know that the ϕ function is multiplicative, we know that

$$\phi(a) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})\dots\phi(p_k^{\alpha_k})$$

So it suffices to show that $\phi(p^\alpha) = (p - 1)(p^{\alpha-1})$

Proof: Let $p, \alpha \in \mathbb{Z}$ such that p is a prime. Let's say that S is the set of all integers less than or equal to p^α and let A_1 be the set of all integers less than or equal to p^α that are relatively prime to p^α . By Definition, we know that

$$\begin{aligned} |A_1| &= \phi(p^\alpha) \\ &= |\{x \in \mathbb{Z} : 1 \leq x \leq p^\alpha \wedge (x, p^\alpha) = 1\}| \\ &= |\{x \in \mathbb{Z} : 1 \leq x < p^\alpha\}| - |\{x \in \mathbb{Z} : 1 \leq x \leq p^\alpha \wedge (x, p^\alpha) > 1\}| \\ &= |S| - |\bar{A}_1|. \end{aligned}$$

We know that there are p^α positive integers less than or equal to p^α , so $|S| = p^\alpha$. To find the cardinality of A_1 , we need to find the number of positive integers less than or equal to p^α that are *not* relatively prime to p^α . Since p is a prime, we know the only integers not coprime to p^α are multiples of p . So the elements of \bar{A}_1 are $p, 2p, 3p, \dots, (p^{\alpha-1})p$. There are $p^{\alpha-1}$ of these multiples, so $|\bar{A}_1| = p^{\alpha-1}$. Finally, we can say

$$\begin{aligned} \phi(p^\alpha) &= |A_1| \\ &= p^\alpha - p^{\alpha-1} \\ &= (p - 1)(p^{\alpha-1}). \blacksquare \end{aligned}$$

Example 1.7: Consider $\phi(24)$. The prime factorization of 24 is $2^3 \cdot 3$. So $\phi(n) = (2 - 1)(2^{2-1})(3 - 1)(3^{1-1}) = 8$.

The Gaussian Integers

The set of Gaussian Integers is a subset of \mathbb{C} , denoted $\mathbb{Z}[i]$, and is an integral domain defined as follows:

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{C} | a, b \in \mathbb{Z}, i^2 = -1\}$$

In \mathbb{Z} , the only units are 1 and -1 . However, in $\mathbb{Z}[i]$, we have the following four units: $(1 + 0i)$, $(-1 + 0i)$, $(0 + i)$, and $(0 - i)$.

The definitions for divisibility and relative primality in $\mathbb{Z}[i]$ are similar to their definitions in \mathbb{Z} .

Definition 2.1: Let $(a + bi), (c + di) \in \mathbb{Z}[i]$. We say $(a + bi)$ divides $(c + di)$, denoted $(a + bi)|(c + di)$, if $(a + bi)(x + yi) = (c + di)$ for some $(x + yi) \in \mathbb{Z}[i]$.

Example: We can say that $(3 + 2i)|(10 + 11i)$ since $(3 + 2i)(4 + i) = (10 + 11i)$

Definition 2.2: Let $(a + bi), (c + di) \in \mathbb{Z}[i]$. We say that $(a + bi)$ and $(c + di)$ are *relatively prime* if $(x + yi)|(a + bi)$ and $(x + yi)|(c + di)$ for $(x + yi) \in \mathbb{Z}[i]$ implies that $(x + yi)$ is a unit in $\mathbb{Z}[i]$.

Similarly to \mathbb{Z} , we can additionally say that two Gaussian Integers $(a + bi)$ and $(c + di)$ are relatively prime if for some Gaussian unit u and some $(j + ki), (m + ni) \in \mathbb{Z}[i]$,

$$u = (a + bi)(j + ki) + (c + di)(m + ni).$$

However, since every unit in $\mathbb{Z}[i]$ divides 1, we can more specifically say that $(a + bi)$ and $(c + di)$ are relatively prime if

$$1 = (a + bi)(j + ki) + (c + di)(m + ni).$$

Example 2.3: We can say that $(4 + 3i)$ and $(-9 - 12i)$ are relatively prime since

$$(4 + 3i)(1 - 3i) + (-9 - 12i)(-i) = (13 - 9i) + (-12 + 9i) = 1.$$

Theorem 2.4: Let $(a + bi), (c + di) \in \mathbb{Z}[i]$. Then $(a + bi)$ and $(c + di)$ are relatively prime if and only if $(a + bi)$ is invertible modulo $(c + di)$ in $\mathbb{Z}[i]$.

Proof: Let $(a + bi), (c + di) \in \mathbb{Z}[i]$, and assume $(a + bi)$ and $(c + di)$ are relatively prime. Then $(a + bi)(j + ki) + (c + di)(m + ni) = 1$ for some $(j + ki), (m + ni) \in \mathbb{Z}[i]$. Rearranging, we see that $(c + di)(-m - ni) = (a + bi)(j + ki) - 1$. This implies that $(c + di)|(a + bi)(j + ki) - 1$. Therefore, we know that $(a + bi)(j + ki) \equiv 1 \pmod{c + di}$.

Next, assume that $(a + bi)$ is invertible modulo $(c + di)$. Then $(a + bi)(x + yi) \equiv 1 \pmod{c + di}$ for some $(x + yi) \in \mathbb{Z}[i]$. Therefore, we know $(c + di)(w + zi) = (a + bi)(x + yi) - 1$. Rearranging, we see that $(a + bi)(x + yi) + (c + di)(-w - zi) = 1$. So $(a + bi)$ and $(c + di)$ are relatively prime in $\mathbb{Z}[i]$. ■

We can also generalize the notion of common divisors to $\mathbb{Z}[i]$.

Definition 2.5: For $(a + bi), (c + di) \in \mathbb{Z}[i]$, we say that a *common divisor* of $(a + bi)$ and $(c + di)$, is a non-zero Gaussian Integer $(x + yi)$ such that $(a + bi)(j + ki) + (c + di)(m + ni) = (x + yi)$ for some $(j + ki), (m + ni) \in \mathbb{Z}[i]$.

We will often be concerned with the largest of these common divisors. The definition of greatest common divisor in $\mathbb{Z}[i]$ is analogous to its definition in \mathbb{Z} .

Definition 2.6: For $(a + bi), (c + di) \in \mathbb{Z}[i]$, we say that we say that a *greatest common divisor*, denoted $\gcd((a + bi), (c + di))$ of $(a + bi)$ and $(c + di)$, is a non-zero Gaussian Integer $(x + yi)$ such that $(x + yi)$ is a common divisor $(a + bi)$ and $(c + di)$ with the smallest norm.

It is important to note that, because of the multiple units in the set of Gaussian Integers, gcd's are not unique in $\mathbb{Z}[i]$. That is to say, if $\gcd((a + bi), (c + di)) = (x + yi)$, then $-(x + yi)$ and $\pm i(x + yi)$ are also greatest common divisors of $(a + bi)$ and $(c + di)$.

Similarly to common divisors in the set of integers, relative primality in $\mathbb{Z}[i]$ implies certain properties. Theorem 1.4 also applies to the Gaussian Integers.

Theorem 2.7: Let $(a + bi), (c + di), (j + ki) \in \mathbb{Z}[i]$ such that $(a + bi)$ and $(c + di)$ are relatively prime and $(j + ki) = (a + bi)(c + di)$. Then for all $(m + ni) \in \mathbb{Z}[i]$, $\gcd((j + ki), (m + ni)) = 1$ if and only if $\gcd((a + bi), (m + ni)) = 1$ and $\gcd((c + di), (m + ni)) = 1$.

Proof: Let $(a + bi), (c + di), (j + ki) \in \mathbb{Z}[i]$ such that $(a + bi)$ and $(c + di)$ are relatively prime and $(j + ki) = (a + bi)(c + di)$.

First, assume that $\gcd((a + bi), (m + ni)) \neq 1$ or $\gcd((c + di), (m + ni)) \neq 1$. Without loss of generality, assume that $\gcd((a + bi), (m + ni)) = (x + yi)$ for some non-unit $(x + yi) \in \mathbb{Z}[i]$. Then $(x + yi)|(a + bi)$ and $(x + yi)|(m + ni)$. Furthermore, since $(a + bi)|(j + ki)$, we know that $(x + yi)|(j + ki)$. Since $(x + yi)|(j + ki)$ and $(x + yi)|(m + ni)$, we know $(x + yi)$ is a non-unit common divisor of $(j + ki)$ and $(m + ni)$. So $(j + ki)$ and $(m + ni)$ are not relatively prime.

Next, assume that $\gcd((a + bi), (m + ni)) = 1$ and $\gcd((c + di), (m + ni)) = 1$. Then $(a + bi)(f + gi) + (m + ni)(r + ti) = 1$ and $(c + di)(w + zi) + (m + ni)(p + qi) = 1$ for some $(f + gi), (r + ti), (w + zi), (p + qi) \in \mathbb{Z}[i]$. Then we know

$$((a + bi)(f + gi) + (m + ni)(r + ti))((c + di)(w + zi) + (m + ni)(p + qi)) = (1)(1)$$

Simplifying this equation, we can see that

$$(j + ki)((f + gi)(w + zi) + (m + ni)((a + bi)(f + gi)(p + qi) + (r + ti)(c + di)(w + zi) + (r + ti)(m + ni)(p + qi)) = 1$$

Therefore, $(j + ki)$ and $(m + ni)$ are relatively prime. ■

The Gaussian Norm Function

The natural ordering we have in \mathbb{Z} does not translate to \mathbb{C} or its subsets. Therefore, evaluation of the ϕ -function within the set could be problematic. However, because the Gaussian Integers form a Euclidean Domain, we know that there exists a function mapping them to the set of positive integers. In particular, the Norm Function of $\mathbb{Z}[i]$ is one such mapping.

Definition 3.1: The Norm function of the Gaussian Integers is a mapping $N : \mathbb{Z}[i] \rightarrow \mathbb{Z}^+$ where $N(a + bi) = |a^2 - (bi)^2| = (a^2 + b^2)$ for $(a + bi) \in \mathbb{Z}[i]$.

This function allows us to identify the units of $\mathbb{Z}[i]$.

Theorem 3.2: $(a + bi)$ is a unit in $\mathbb{Z}[i]$ if and only if $N(a + bi) = 1$.

Proof: First, assume for some $(a + bi) \in \mathbb{Z}[i]$ that $N(a + bi) = 1$. Then $(a^2 + b^2) = 1$, which implies that $a^2 = 1 - b^2$. Since $a^2 \geq 0$, we consider two cases:

Case 1: Let $b^2 = 0$. Then $b = 0$ and $a^2 = 1 - 0 = 1$. So $a = 1$ or $a = -1$. If $a = 1$, then $(a + bi) = (1 + 0i)$. Since $(1 + 0i)(1 + 0i) = (1 + 0i) = e$, $(a + bi)$ is a unit in $\mathbb{Z}[i]$. If $a = -1$, then $(a + bi) = (-1 + 0i)$. Since $(-1 + 0i)(-1 + 0i) = (1 + 0i) = e$, $(a + bi)$ is a unit in $\mathbb{Z}[i]$.

Case 2: Let $b^2 = 1$. Then $a^2 = 1 - 1 = 0$. So $a = 0$ and $b = 1$ or $b = -1$. If $b = 1$, $(a + bi) = (0 + i)$. Since $(0 + i)(0 - i) = (1 + 0i) = e$, we know $(a + bi)$ is a unit in $\mathbb{Z}[i]$. If $b = -1$, $(a + bi) = (0 - i)$. Since $(0 - i)(0 + i) = (1 + 0i) = e$, we know $(a + bi)$ is a unit in $\mathbb{Z}[i]$.

Next, assume there exists some $(a + bi) \in \mathbb{Z}[i]$ where $(a + bi)$ is a unit. Then there exists some $(c + di) \in \mathbb{Z}[i]$, where c and d do not both equal zero, such that $(a + bi)(c + di) = e = (1 + 0i)$. Then we know $N((a + bi)(c + di)) = N(1 + 0i)$ and by Theorem 3.2, we can say $N(a + bi)N(c + di) = N(1 + 0i)$. So $(a^2 + b^2)(c^2 + d^2) = (1^2 + 0^2) = 1$. Since $(a^2 + b^2), (c^2 + d^2) \in \mathbb{Z}^+$ and $(a^2 + b^2)(c^2 + d^2) = 1$, we know $(a^2 + b^2)$ and $(c^2 + d^2)$ are units in \mathbb{Z} . Because $(a^2 + b^2)$ and $(c^2 + d^2)$ are both nonnegative, they must both be equal to 1. So $1 = (a^2 + b^2) = N(a + bi)$. ■

There are a few additional properties of the Gaussian Norm Function that will be helpful when we apply the ϕ function in $\mathbb{Z}[i]$. The Gaussian Norm Function's multiplicativity is one such property.

Theorem 3.3: $N((a + bi)(c + di)) = N(a + bi)N(c + di)$ for all $(a + bi), (c + di) \in \mathbb{Z}[i]$.

Proof: Let $(a + bi), (c + di) \in \mathbb{Z}[i]$. Then

$$\begin{aligned} N((a + bi)(c + di)) &= N((ac - bd) + (ad + bc)i) \\ &= (ac - bd)^2 + (ad + bc)^2 \\ &= (a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2) \\ &= a^2(c^2 + d^2) + b^2(c^2 + d^2) \\ &= (a^2 + b^2)(c^2 + d^2) \\ &= N(a + bi)N(c + di) \quad \blacksquare \end{aligned}$$

Additionally, we know that divisibility in $\mathbb{Z}[i]$ implies divisibility in \mathbb{Z} .

Theorem 3.4: For $(a + bi), (x + yi) \in \mathbb{Z}[i]$, we say if $(a + bi)|(x + yi)$ then $N(a + bi)|N(x + yi)$

Proof: Let $(a + bi), (x + yi) \in \mathbb{Z}[i]$ such that $(a + bi)|(x + yi)$. Then $(a + bi)(c + di) = (x + yi)$ for some $(c + di) \in \mathbb{Z}[i]$. Then we can say $((ac - bd) + (ad + bc)i) = (x + yi)$ By definition of equality in $\mathbb{Z}[i]$, this means that $(ac - bd) = x$ and $(ad + bc) = y$. This implies that

$$\begin{aligned} N(x + yi) &= x^2 + y^2 \\ &= (ac - bd)^2 + (ad + bc)^2 \\ &= (a^2c^2 - 2abcd + b^2d^2) + (a^2d^2 + 2abcd + b^2d^2) \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2d^2 \\ &= a^2(c^2 + d^2) + b^2(c^2 + d^2) \\ &= (a^2 + b^2)(c^2 + d^2) \\ &= N(a + bi)N(c + di). \blacksquare \end{aligned}$$

$\mathbb{Z}[i]$ as a Euclidean Domain

Definition 4.1: An integral domain D is called a *Euclidean Domain* if there is a function d from the non-zero elements of D to the positive integers such that the following hold true:

1. $d(a) \leq d(ab)$ for all $a, b \in D$ such that $a, b \neq 0$.
2. For all $a, b \in D$ where $b \neq 0$, there exist $q, r \in D$ such that $a = bq + r$ where $d(r) < d(b)$ (Gallian 329).

As an example, the next theorem shows that the Gaussian norm function satisfies the properties of d above, making $\mathbb{Z}[i]$ a Euclidean Domain.

Theorem 4.2: The set of Gaussian Integers forms a Euclidean Domain.

Proof: Let $(w + zi), (u + vi)$ be non-zero elements of $\mathbb{Z}[i]$. We know $1 \leq N(u + vi)$. Since $a \leq N(w + zi)$, this implies that $N(w + zi) \leq N(w + zi)N(u + vi)$.

Now, let $(a + bi), (c + di) \in \mathbb{Z}[i]$ where $(c + di) \neq (0 + 0i)$. Since $(c + di) \neq (0 + 0i)$, we know $(c + di)^{-1} = \frac{1}{c + di} = \left(\frac{c}{c^2 + d^2} - \frac{d}{c^2 + d^2}i\right)$ where $\frac{c}{c^2 + d^2}$ and $-\frac{d}{c^2 + d^2}$ are rational numbers. Thus, $(c + di)^{-1} \in \mathbb{Q}[i]$, the field of Gaussian rationals. Furthermore, we know that $(a + bi)(c + di)^{-1} = (x + yi)$ for some $(x + yi) \in \mathbb{Q}[i]$. Let $s, t \in \mathbb{Z}$ such that $\frac{-1}{2} \leq (s - x) \leq \frac{1}{2}$ and $\frac{-1}{2} \leq (t - y) \leq \frac{1}{2}$. So

$$\begin{aligned} (a + bi)(c + di)^{-1} &= (x + yi) \\ &= (x + s - s) + (y + t - t)i \\ &= x + s - s + yi + ti - ti. \end{aligned}$$

Since we want a Gaussian Integer, we can rearrange and get $(s + ti) + (x - s) + (y - t)i$. So $(a + bi)(c + di)^{-1} = (s + ti) + (x - s) + (y - t)i$ Multiplying through

by $(c + di)$ on the left yields $(a + bi) = (s + ti)(c + di) + ((x - s) + (y - t)i)(c + di)$. We know $(s + ti) \in \mathbb{Z}[i]$ since $s, t \in \mathbb{Z}$. So $(s + ti)$ is our q , making $((x - s) + (y - t)i)(c + di)$ our remainder, r . Solving for our remainder in our equation shows $r = (a + bi) - (s + ti)(c + di)$. Since $\mathbb{Z}[i]$ forms a ring, the set is closed under to multiplication and addition. So $r \in \mathbb{Z}[i]$. Finally, we know

$$\begin{aligned} N([(x - s) + (y - t)i](c + di)) &= N((x - s) + (y - t)i)N(c + di) \\ &= ((x - s)^2 + (y - t)^2)(c^2 + d^2) \\ &\leq ((\frac{1}{2})^2 + (\frac{1}{2})^2)(c^2 + d^2) \\ &= (\frac{1}{2})(c^2 + d^2) \\ &< (c^2 + d^2) \\ &= N(c + di). \blacksquare \end{aligned}$$

Example 4.3: Consider $(3 - 4i)$ and $(2 + 5i)$. We know $(2 + 5i)^{-1} = (\frac{4}{58} + \frac{-5}{29}i)$, since $(2 + 5i)^{-1}(\frac{4}{58} + \frac{-5}{29}i) = (1 + 0i)$. Let s and t be the integers closest to $\frac{4}{58}$ and $\frac{-5}{29}$, respectively. Then $s = 0$ and $t = -1$. So $(3 - 4i) = (2 + 5i)(0 - i) + r$. So $r = (3 - 4i) - (5 - i) = (2 - 3i)$. Thus, $(3 - 4i) = (2 + 5i)(0 - i) + (2 - 3i)$.

Sums of Squares

Many integers can be written as the sum of two squares. For this paper, we are particularly interested in primes that can be written in this form. Looking at the first few primes, we can categorize them in the following way:

- Primes that can be written as the sum of two squares: 2,5,13,17,29,37,41,...
- Primes that cannot be written as the sum of two squares: 3,7,11,19,23,31,39...

If we consider this set of primes modulo 4, we can see

- Primes that can be written as the sum of two squares: 2,1,1,1,1,1,...
- Primes that cannot be written as the sum of two squares: 3,3,3,3,3,3,...

In this section, we will prove that an odd prime can be written as the sum of two squares if and only if it is congruent to 1 modulo 4. In order to do so, we will need the following definitions and lemmas.

Definition 5.1: Let $a, b \in \mathbb{Z}$. Then a is a *quadratic residue modulo b* if the equation $x^2 \equiv a \pmod{b}$ has a solution in \mathbb{Z} . Otherwise, a is called a *quadratic nonresidue modulo b* (Strayer 103).

Definition 5.2: Let $a, p \in \mathbb{Z}$ such p is an odd prime and $p \nmid a$. Then the Legendre Symbol (Strayer 108), denoted $\left(\frac{a}{p}\right)$, is defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p \end{cases}$$

Lemma 5.3: Euler's Criterion states that if $a, p \in \mathbb{Z}$ where p is an odd prime and $p \nmid a$, then $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}$ (Strayer 110).

Lemma 5.4: If p is a prime in \mathbb{Z} such that $p \equiv 1 \pmod{4}$, then there exist some $a, b, m \in \mathbb{Z}$ where $a^2 + b^2 = pm$ with $0 < m < p$.

Proof: Let p be a prime in \mathbb{Z} where $p \equiv 1 \pmod{4}$. Let us consider the Legendre Symbol $\left(\frac{-1}{p}\right)$. By Euler's Criterion, we know $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Since $p \equiv 1 \pmod{4}$, we know p is odd, making $(p-1)$ and $\frac{p-1}{2}$ even. Therefore, $(-1)^{\frac{p-1}{2}} = 1$, which implies that -1 is a quadratic residue \pmod{p} . By the definition of quadratic residue, we know there exists an $a \in \mathbb{Z}$ where $0 < a \leq \frac{p-1}{2}$ such that $a^2 \equiv -1 \pmod{p}$. So $p \mid a^2 + 1$, and we can say $pm = a^2 + 1$ for some $m \in \mathbb{Z}$. Since $a \leq \frac{p-1}{2}$, we know $a < \frac{p}{2}$, which implies that $a^2 < \left(\frac{p}{2}\right)^2$. Then $a^2 + 1 < \left(\frac{p}{2}\right)^2 + 1$. So $pm < \left(\frac{p}{2}\right)^2 + 1$. Since $3 \leq p$, we know $\left(\frac{p}{2}\right)^2 + 1 < p^2$. So $pm < p^2$, implying that $m < p$. Since $0 < a^2 + 1 = pm$, we know $0 < m$. Thus, $0 < m < p$. ■

Lemma 5.5: If $a, b \in \mathbb{Z}$ such that a and b can each be written as the sum of two squares, then the product ab can also be written as the sum of two squares.

Proof: Let $a, b \in \mathbb{Z}$ such that $a = (c^2 + d^2)$ and $b = (x^2 + y^2)$ for some $c, d, x, y \in \mathbb{Z}$. Then

$$\begin{aligned} ab &= (c^2 + d^2)(x^2 + y^2) \\ &= c^2x^2 + c^2y^2 + d^2x^2 + d^2y^2 \\ &= c^2x^2 + c^2y^2 + d^2x^2 + d^2y^2 + 2cxdy - 2cxdy \\ &= (c^2x^2 + 2cxdy + d^2y^2) + (c^2y^2 - 2cxdy + d^2x^2) \\ &= (cx + dy)^2 + (cy - dx)^2. \end{aligned}$$

Since $(cx + dy), (cy - dx) \in \mathbb{Z}$, the product ab can be written as the sum of two squares. ■

Now we are in a position to prove the following theorem.

Theorem 5.6: If p is a prime in \mathbb{Z} such that $p \equiv 1 \pmod{4}$, p is expressible as the sum of two squares.

Proof: Let p be a prime in \mathbb{Z} such that $p \equiv 1 \pmod{4}$. By Lemma 5.4, we know there exists at least one $m \in \mathbb{Z}$ such that $a^2 + b^2 = pm$ where $0 < m < p$. Let n be the least integer such that there exists $x, y \in \mathbb{Z}$ so $x^2 + y^2 = np$ with $0 < n < p$. So $1 \leq n$. Note, if $n = 1$, we get $p = a^2 + b^2$. So assume $1 < n$. Let $h, k \in \mathbb{Z}$ such that h is the least absolute residue of $x \pmod{n}$ and k is the least absolute residue of $y \pmod{n}$. Then $h \equiv x \pmod{n}$ where $-\lceil \frac{n}{2} \rceil < h < \lfloor \frac{n}{2} \rfloor$ and $k \equiv y \pmod{n}$ where $-\lceil \frac{n}{2} \rceil < k < \lfloor \frac{n}{2} \rfloor$. Since $h \equiv x \pmod{n}$, $h^2 \equiv x^2 \pmod{n}$. Likewise, we can say $k^2 \equiv y^2 \pmod{n}$. So $(h^2 + k^2) \equiv (x^2 + y^2) \pmod{n}$. Since $x^2 + y^2 = np$, we know $(x^2 + y^2) \equiv 0 \pmod{n}$. Thus, $(h^2 + k^2) \equiv 0 \pmod{n}$. Therefore, there exists a $z \in \mathbb{Z}$ such that $h^2 + k^2 = nz$. So $(x^2 + y^2)(h^2 + k^2) = (np)(zh) = n^2pz$. By Lemma 5.5, we know $(x^2 + y^2)(h^2 + k^2) = (xh + yk)^2 + (xk - yh)^2$. By the transitive property, we know $(xh + yk)^2 + (xk - yh)^2 = n^2pz$. Since $h \equiv x \pmod{n}$ and $k \equiv y \pmod{n}$, we can say $(xh + yk)^2 \equiv (x^2 + y^2)^2 \pmod{n}$. Thus, $(xh + yk) \equiv 0 \pmod{n}$. Also, $(xk - yh)^2 \equiv (xy - yx)^2 \equiv 0 \pmod{n}$. Since $(xh + yk) \equiv (xk - yh) \equiv 0 \pmod{n}$, we can say $\frac{xh+yk}{n}, \frac{k-yh}{n} \in \mathbb{Z}$. We know $(xh + yk)^2 + (xk - yh)^2 = n^2pz$. Dividing by n^2 yields $\frac{(xh+yk)^2}{n^2} + \frac{(xk-yh)^2}{n^2} = pz$. Rewriting, we see that $\left(\frac{xh+yk}{n}\right)^2 + \left(\frac{xk-yh}{n}\right)^2 = pz$. We previously stated that $zn = h^2 + k^2$, and we defined h, k so that $-\lceil \frac{n}{2} \rceil < h, k < \lfloor \frac{n}{2} \rfloor$. Therefore, we know $h^2, k^2 \leq \lfloor \frac{n}{4} \rfloor^2 \leq \lfloor \frac{n^2}{4} \rfloor \leq \frac{n^2}{4}$. Thus, $h^2 + k^2 \leq \frac{n^2}{4} + \frac{n^2}{4} = \frac{n^2}{2}$. Since $zn = h^2 + k^2$, we know $zn \leq \frac{n^2}{2}$. This implies that $z \leq \frac{n}{2}$. Since $n > 0$, we know $\frac{n}{2} < n$, and thus $z < n$. Also, since $n > 0$ and $zn = (h^2 + k^2)$, $z > 0$. Thus, $0 < z < n$. Since $\left(\frac{xh+yk}{n}\right)^2 + \left(\frac{xk-yh}{n}\right)^2 = pz$ where $\frac{xh+yk}{n}, \frac{k-yh}{n} \in \mathbb{Z}$, we have contradicted our original assumption that n is the smallest integer where pn is the sum of two squares. So $n = 1$ and therefore, $p = x^2 + y^2$. ■

Now, for the converse:

Theorem 5.7: If p is an odd prime in \mathbb{Z} and $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$, then $p \equiv 1 \pmod{4}$.

Proof: Let $p, x, y \in \mathbb{Z}$ where p is an odd prime in \mathbb{Z} . Furthermore, assume $x^2 + y^2 = p$. Note, when $a \in \mathbb{Z}$ is odd, $a^2 \equiv 1 \pmod{4}$, and when a is even, $a^2 \equiv 0 \pmod{4}$. For some $h \in \mathbb{Z}$, $b^2 = (2h)^2 = 4h^2 \equiv 0 \pmod{4}$. So the sum of any two squares is congruent to 0, 1, or 2 modulo 4. If we assume $p = (x^2 + y^2) \equiv 0 \pmod{4}$, then $4 \mid (x^2 + y^2)$ which implies that p is even and contradicts our original assumption that p is an odd prime. If we assume $p = (x^2 + y^2) \equiv 2 \pmod{4}$, then $4 \mid (x^2 + y^2) - 2$. So $(x^2 + y^2) - 2 = 4k$ for some $k \in \mathbb{Z}$. So $(x^2 + y^2) = 4k + 2 = 2(2k + 1)$, which implies that p is even. Thus, we have arrived at a contradiction. So $p = (x^2 + y^2) \equiv 1 \pmod{4}$. ■

Now that we have established properties of prime integers that can be written as the sum of squares, we can use these properties to aid us in the identification of Gaussian Primes.

Gaussian Primes

Since $\mathbb{Z}[i]$ is a Euclidean Domain, every Gaussian Integer has a prime factorization, which is unique up to order and associates. In order to analyze the prime factorization of a Gaussian Integer, it is necessary to define primality in $\mathbb{Z}[i]$.

Definition 6.1: We call a Gaussian Integer $(a + bi)$ a *Gaussian Prime* if its only divisors are $\pm(a + bi)$, ± 1 , and $\pm i$.

Using Fermat's Theorem regarding the sums of squares, we can classify the Gaussian Primes as follows:

- Let u be a Gaussian unit and a be a non-zero element of \mathbb{Z} . Then ua is a Gaussian Prime if and only if a is an odd prime and $a \equiv 3 \pmod{4}$.
- Let $(a + bi)$ be a Gaussian Integer such that $a \neq 0$ and $b \neq 0$. Then $(a + bi)$ is a Gaussian Prime if and only if $N(a + bi)$ is a prime in \mathbb{Z} .

Primality in \mathbb{Z} does not imply primality in $\mathbb{Z}[i]$. That is to say, if a is a prime integer, a is not necessarily a Gaussian prime. We can use the Norm Function to determine if any given Gaussian Integer is prime in $\mathbb{Z}[i]$.

Theorem 6.2: If $N(a + bi)$ is prime in \mathbb{Z} , then $(a + bi)$ is prime and therefore irreducible in $\mathbb{Z}[i]$.

Proof: Assume $(a + bi)$ is a reducible element in $\mathbb{Z}[i]$. Then for some non-unit elements $(c + di), (x + yi) \in \mathbb{Z}[i]$, $(a + bi) = (c + di)(x + yi)$. Applying the Norm Function to both sides yields $N(a + bi) = N((c + di)(x + yi)) = N(c + di)N(x + yi)$. Since $(c + di)$ and $(x + yi)$ are not units, $N(c + di), N(x + yi) > 1$. Since $N(a + bi)$ can be written as the product of two non-units, and \mathbb{Z} is a Euclidean Domain, $N(a + bi)$ is not a prime in \mathbb{Z} . ■

The converse of Theorem 6.2 is not necessarily true. A Gaussian Prime does not necessarily have a prime Norm. By Definition 6.1, 7 is a prime in $\mathbb{Z}[i]$. However, $N(7) = 49$, which is not a prime integer.

Many facts regarding prime integers are also true for Gaussian Primes.

Theorem 6.3: If $(x + yi)$ is a prime in $\mathbb{Z}[i]$ and $(x + yi)|(a + bi)(c + di)$ for some $(a + bi), (c + di) \in \mathbb{Z}[i]$, then $(x + yi)|(a + bi)$ or $(x + yi)|(c + di)$.

Proof: Let $(x + yi)$ be a Gaussian Prime, such that $(x + yi)|(a + bi)(c + di)$ for some $(a + bi), (c + di) \in \mathbb{Z}[i]$. Assume $(x + yi)$ and $(a + bi)$ are relatively prime. Then by Theorem 2.2, we know that $(x + yi)(j + ki) + (a + bi)(m + ni) = 1$ for some $(j + ki), (m + ni) \in \mathbb{Z}[i]$. Multiplying across the equation by $(c + di)$

yields $(x + yi)(j + ki)(c + di) + (a + bi)(c + di)(m + ni) = (c + di)$. Since $(x + yi)|(a + bi)(c + di)$, we know that $(x + yi)(w + zi) = (a + bi)(c + di)$ for some $(w + zi) \in \mathbb{Z}[i]$. Substituting into our equation, we see that $(x + yi)((j + ki)(c + di) + (w + zi)(m + ni)) = (c + di)$. Therefore, we know that $(x + yi)|(c + di)$. ■

The previous Theorem gives us the following Lemma:

Lemma 6.4: Let $a, b, p \in \mathbb{Z}$ such that p is a prime, $p \equiv 3 \pmod{4}$. If $p|(a^2 + b^2)$, then $p|a$ and $p|b$.

Proof: Let $a, b, p \in \mathbb{Z}$ such that p is a prime, $p \equiv 3 \pmod{4}$. Assume $p|(a^2 + b^2)$. Since $p \equiv 3 \pmod{4}$, we know it is also prime in $\mathbb{Z}[i]$. Furthermore, since $p|(a^2 + b^2)$, we also know that $p|(a + bi)(a - bi)$. By Theorem 6.3, this means that $p|(a + bi)$ or $p|(a - bi)$. In either case, we see that $p|a$ and $p|b$. ■

Now that we have established properties of Gaussian Primes, we can look at prime factorizations in $\mathbb{Z}[i]$.

Prime Factorization in $\mathbb{Z}[i]$

Because $\mathbb{Z}[i]$ is a Unique Factorization Domain, we know that each non-zero Gaussian Integer has a prime factorization. Finding this factorization in $\mathbb{Z}[i]$ can be tedious. Instead, we can use the Norm Function to identify these factorizations. We will follow the methodology defined by Keith Conrad to find prime factorizations in $\mathbb{Z}[i]$ (Conrad 15).

Method

Conrad's method first identifies the prime factorization of the Norm of a Gaussian Integer. He then writes each prime as the sum of two squares, and determine the possible Gaussians whose Norms map to those sums. Finally he manipulates these Gaussian primes with units until their product yields the desired result. The prime factorizations in \mathbb{Z} that Conrad addresses all have prime factorizations whose primes are all congruent to 1 modulo 4. We will further expand on his method to include prime factorizations with primes congruent to 3 modulo 4.

Example 7.1: Consider the Gaussian Integer $(23 + 24i)$. We know that $N(23 + 24i) = 529 + 576 = 1105$. The prime factorization of 1105 is $5 \cdot 13 \cdot 17$. Since each of these primes is congruent to 1 (mod 4), we can write each of them as the sum of two squares:

$$5 = 1^2 + 2^2 \qquad 13 = 2^2 + 3^2 \qquad 17 = 1^2 + 4^2$$

Next, we need to determine which unique Gaussian Integers (up to associates) are mapped to each of these sums by the Norm Function.

- The Gaussians with Norm 5 are $(1 + 2i)$ and $(1 - 2i)$.
- The Gaussians with Norm 13 are $(2 + 3i)$ and $(2 - 3i)$.
- The Gaussians with Norm 17 are $(1 + 4i)$ and $(1 - 4i)$.

By analyzing the multiple combinations of our possible Gaussian Primes, we can find the prime factorization of our original Gaussian Integer. We find that

$$(24 + 23i) = (1 + 2i)(2 + 3i)(1 - 4i).$$

In the previous example, the prime factorization of our Norm had only primes congruent to 1 modulo 4. We know that primes congruent to 3 modulo 4 cannot be written as the sum of two squares. This causes a problem in the method above. The next Theorem will help us address this.

Theorem 7.2: Let $n \in \mathbb{Z}$ such that $n = (a^2 + b^2)$ for $a, b \in \mathbb{Z}$. If p^α occurs in the prime factorization of n where $p \equiv 3 \pmod{4}$, then α is even.

Proof: Let $n \in \mathbb{Z}$ such that $n = (a^2 + b^2)$ for $a, b \in \mathbb{Z}$. Assume $p|n$ for some prime p where $p \equiv 3 \pmod{4}$. By Lemma, we know that $p|a$ and $p|b$. Therefore, $px = a$ and $py = b$ for some $x, y \in \mathbb{Z}$. So $n = (px)^2 + (py)^2 = p^2(x^2 + y^2)$. Again, if we assume p also divides $(x^2 + y^2)$, we will get a second factor of p^2 . We can continue this process until p no longer divides the smaller sum of squares. Thus, p has an even power in the prime factorization of n . ■

With this Theorem, we can see that Conrad's method is still applicable to Gaussian Integers whose Norms have primes congruent to 3 modulo 4 in their factorizations. Since these primes must occur to even powers, we know that the prime will occur in the Gaussian Prime factorization to an appropriate power.

Modular Arithmetic in $\mathbb{Z}[i]$

Because our definition of the Euler- ϕ function depends on invertible elements and modular arithmetic, we must explore these ideas within $\mathbb{Z}[i]$.

Definition 8.1: For $(a + bi), (c + di), (x + yi) \in \mathbb{Z}[i]$, we say $(a + bi) \equiv (c + di) \pmod{x + yi}$ if and only if $(x + yi)|(a + bi) - (c + di)$.

Example 8.2: Since $(3 + 4i)(2 + i) = (2 + 11i) = (4 + 15i) - (2 + 4i)$, we know that $(3 + 4i)|(4 + 15i) - (2 + 4i)$. Therefore, we can say that $(4 + 15i) \equiv (2 + 4i) \pmod{3 + 4i}$.

Many properties of integral modular congruence also hold in $\mathbb{Z}[i]$.

Theorem 8.3: If $(a_1 + b_1i) \equiv (a_2 + b_2i) \pmod{x + yi}$ and $(c_1 + d_1i) \equiv (c_2 + d_2i) \pmod{x + yi}$, then $(a_1 + b_1i) + (c_1 + d_1i) \equiv (a_2 + b_2i) + (c_2 + d_2i) \pmod{x + yi}$.

Proof: Let $(a_1 + b_1i), (a_2 + b_2i), (c_1 + d_1i), (c_2 + d_2i), (x + yi) \in \mathbb{Z}[i]$, and assume that $(a_1 + b_1i)$ and $(c_1 + d_1i)$ are congruent to $(a_2 + b_2i)$ and $(c_2 + d_2i)$ modulo $(x + yi)$, respectively. Since $(a_1 + b_1i) \equiv (a_2 + b_2i) \pmod{x + yi}$, we know

$$\begin{aligned}(x + yi)|(a_1 + b_1i) - (a_2 + b_2i) \\(x + yi)(j_1 + k_1i) &= (a_1 + b_1i) - (a_2 + b_2i) \\(x + yi)(j_1 + k_1i) + (a_2 + b_2i) &= (a_1 + b_1i)\end{aligned}$$

for some $(j_1 + k_1i) \in \mathbb{Z}[i]$. Additionally, since $(c_1 + d_1i) \equiv (c_2 + d_2i) \pmod{x + yi}$, we can say

$$\begin{aligned}(x + yi)|(c_1 + d_1i) - (c_2 + d_2i) \\(x + yi)(j_2 + k_2i) &= (c_1 + d_1i) - (c_2 + d_2i) \\(x + yi)(j_2 + k_2i) + (c_2 + d_2i) &= (c_1 + d_1i)\end{aligned}$$

for some $(j_2 + k_2i) \in \mathbb{Z}[i]$. Therefore, we can say

$$((a_1 + b_1i) + (c_1 + d_1i)) - ((a_2 + b_2i) + (c_2 + d_2i)) = (x + yi)((j_1 + k_1i) + (j_2 + k_2i))$$

This implies that $(x + yi)|((a_1 + b_1i) + (c_1 + d_1i)) - ((a_2 + b_2i) + (c_2 + d_2i))$. Thus, $(a_1 + b_1i) + (c_1 + d_1i) \equiv (a_2 + b_2i) + (c_2 + d_2i) \pmod{x + yi}$. ■

Theorem 8.4: If $(a_1 + b_1i) \equiv (a_2 + b_2i) \pmod{x + yi}$ and $(c_1 + d_1i) \equiv (c_2 + d_2i) \pmod{x + yi}$, then $(a_1 + b_1i)(c_1 + d_1i) \equiv (a_2 + b_2i)(c_2 + d_2i) \pmod{x + yi}$.

Proof: Let $(a_1 + b_1i), (a_2 + b_2i), (c_1 + d_1i), (c_2 + d_2i), (x + yi) \in \mathbb{Z}[i]$, and assume that $(a_1 + b_1i)$ and $(c_1 + d_1i)$ are congruent to $(a_2 + b_2i)$ and $(c_2 + d_2i)$ modulo $(x + yi)$, respectively. Using our analysis of these congruences in Theorem 8.3, we can see that

$$\begin{aligned}(a_1 + b_1i)(c_1 + d_1i) &= ((x + yi)(j_1 + k_1i) + (a_2 + b_2i))((x + yi)(j_2 + k_2i) + (c_2 + d_2i)) \\&= (x + yi)^2(j_1 + k_1i)(j_2 + k_2i) + (x + yi)(j_1 + k_1i)(c_2 + d_2i) \\&\quad + (x + yi)(j_2 + k_2i)(a_2 + b_2i) + (a_2 + b_2i)(c_2 + d_2i).\end{aligned}$$

Rewriting, we can see that

$$\begin{aligned}(a_1 + b_1i)(c_1 + d_1i) - (a_2 + b_2i)(c_2 + d_2i) &= (x + yi)((x + yi)(j_1 + k_1i)(j_2 + k_2i) \\&\quad + (j_1 + k_1i)(c_2 + d_2i) + (j_2 + k_2i)(a_2 + b_2i))\end{aligned}$$

Thus, $(x + yi)|(a_1 + b_1i)(c_1 + d_1i) - (a_2 + b_2i)(c_2 + d_2i)$, and we know $(a_1 + b_1i)(c_1 + d_1i) \equiv (a_2 + b_2i)(c_2 + d_2i) \pmod{x + yi}$. ■

Congruences of Gaussian Integers give information regarding congruences of their conjugates.

Theorem 8.5: If $(a + bi) \equiv (c + di) \pmod{x + yi}$ for $(a + bi), (c + di), (x + yi) \in \mathbb{Z}[i]$, then $(a - bi) \equiv (c - di) \pmod{x - yi}$.

Proof: Let $(a + bi), (c + di), (x + yi) \in \mathbb{Z}[i]$ such that $(a + bi) \equiv (c + di) \pmod{x + yi}$. Then $(x + yi)(j + ki) = (a + bi) - (c + di)$ for some $(j + ki) \in \mathbb{Z}[i]$. By definition of equality in $\mathbb{Z}[i]$, we know that $xj - yk = a - c$ and $xk + yj = b - d$. We know that

$$\begin{aligned}(x - yi)(j - ki) &= (xj - yk) - (xk + yj)i \\ &= (a - c) - (b - d)i \\ &= (a - bi) - (c - di).\end{aligned}$$

Therefore, $(a - bi) \equiv (c - di) \pmod{x - yi}$. ■

Modular congruences in $\mathbb{Z}[i]$ also have implications for congruences in \mathbb{Z} .

Theorem 8.6: If $(a + bi) \equiv (c + di) \pmod{x}$ in for $(a + bi), (c + di) \in \mathbb{Z}[i]$ and $x \in \mathbb{Z}$, then $a \equiv c \pmod{x}$ and $b \equiv d \pmod{x}$.

Proof: Let $(a + bi), (c + di) \in \mathbb{Z}[i]$ and $x \in \mathbb{Z}$ such that $(a + bi) \equiv (c + di) \pmod{x}$. Then $(x)(m + ni) = (a + bi) - (c + di)$. By definition of equality in $\mathbb{Z}[i]$, we know $xm = a - c$ and $xn = b - d$. Therefore, $a \equiv c \pmod{x}$ and $b \equiv d \pmod{x}$. ■

We know that $|\mathbb{Z}_n| = n$ for any $n \in \mathbb{Z}$. However, the size of $\mathbb{Z}[i]_{(a+bi)}$ is not necessarily so apparent. By Theorem 4.2, we know that for any $(a + bi), (c + di) \in \mathbb{Z}[i]$, $(c + di)$ can be written as $(a + bi)(j + ki) + (m + ni)$ for some $(j + ki), (m + ni) \in \mathbb{Z}[i]$ Where $N(m + ni) < N(a + bi)$. Since $N(a + bi)$ is a positive integer, we know that the set of integers less than $N(a + bi)$ is finite. Although this does not tell us the exact size of $\mathbb{Z}[i]_{(a+bi)}$, the cardinality of this set can be evaluated using the following theorems.

Theorem 8.7: If $x \in \mathbb{Z}$, then $|\mathbb{Z}[i]_x| = x^2$.

Proof: Let $x \in \mathbb{Z}$. By Theorem 8.6, we know that If $(a + bi) \equiv (c + di) \pmod{x}$, $a \equiv c \pmod{x}$ and $b \equiv d \pmod{x}$. Therefore,

$$|\mathbb{Z}[i]_x| = |\mathbb{Z}_x \times \mathbb{Z}_x| = x^2. \quad \blacksquare$$

Theorem 8.8: Let $(a + bi)$ be a nonzero element of $\mathbb{Z}[i]$. Then $|\mathbb{Z}[i]_{(a+bi)}| = N(a + bi)$.

Proof: Let $(a + bi) \in \mathbb{Z}[i]$ such that $(a + bi)$ is non-zero. By Theorems 8.5 and 8.7, we know

$$\begin{aligned}|\mathbb{Z}[i]_{(a+bi)}|^2 &= |\mathbb{Z}[i]_{(a+bi)(a-bi)}| \\ &= |\mathbb{Z}[i]_{(a^2+b^2)}| \\ &= (a^2 + b^2)^2 \\ &= N(a + bi)^2.\end{aligned}$$

Taking the square roots of both sides yields $|\mathbb{Z}[i]_{(a+bi)}| = N(a + bi)$. ■

Using the previously defined properties of $\mathbb{Z}[i]$, we can begin our application of the ϕ function within the set.

The Euler- ϕ Function in $\mathbb{Z}[i]$

We know the ϕ function, when applied in \mathbb{Z} , counts the number of integers less than or equal to an integer n that are relatively prime to n . As we have previously stated, inequality is not defined on subsets of the Complex Numbers. To understand the meaning of the function within $\mathbb{Z}[i]$, we will instead look at $\phi(a + bi)$ as the number of Gaussian Integers which are invertible modulo $(a + bi)$.

We know that a Gaussian Prime $(p_1 + p_2i)$ has no divisors other than $\pm 1, \pm i$, and $\pm(p_1 + p_2i)$. Therefore, we can determine which Gaussians are relatively prime to $(p_1 + p_2i)$ with the following theorem.

Theorem 9.1: Let $(a + bi), (p_1 + p_2i) \in \mathbb{Z}[i]$ such that $(p_1 + p_2i)$ is a Gaussian Prime. If $(p_1 + p_2i) \nmid (a + bi)$, then $(a + bi)$ is invertible modulo $(a + bi)$.

Proof: Let $(a + bi), (p_1 + p_2i) \in \mathbb{Z}[i]$ such that $(p_1 + p_2i)$ is a Gaussian Prime and $(a + bi)$ is a non-unit, and assume $(p_1 + p_2i) \nmid (a + bi)$. Since $(p_1 + p_2i)$ is prime, this implies that $(a + bi)$ and $(p_1 + p_2i)$ are relatively prime. By Theorem 2.4, we know that $(a + bi)$ is invertible modulo $(p_1 + p_2i)$. ■

The previous theorem allows us to evaluate the ϕ function for Gaussian Primes.

Theorem 9.2: Let $(p_1 + p_2i)$ be a prime in $\mathbb{Z}[i]$, then $\phi(p_1 + p_2i) = N(p_1 + p_2i) - 1$.

Proof: Let $(p_1 + p_2i)$ be a prime in $\mathbb{Z}[i]$. By Theorem 8.8, we know that $|\mathbb{Z}[i]_{(p_1+p_2i)}| = N(p_1 + p_2i)$. Additionally, by Theorem 9.2, we can say that any non-zero element of $\mathbb{Z}[i]_{(p_1+p_2i)}$ is also an element of $U(\mathbb{Z}[i]_{(p_1+p_2i)})$. Since the number of non-zero elements in $\mathbb{Z}[i]_{(p_1+p_2i)}$ is $N(p_1 + p_2i) - 1$, we know that

$$\phi(p_1 + p_2i) = |U(\mathbb{Z}[i]_{(p_1+p_2i)})| = N(p_1 + p_2i) - 1. \quad \blacksquare$$

The proof that the ϕ function is multiplicative in $\mathbb{Z}[i]$ is analogous to the proof in \mathbb{Z} .

Theorem 9.3: For $(a + bi), (c + di) \in \mathbb{Z}[i]$ where $(a + bi)$ and $(c + di)$ are relatively prime, $\phi((a + bi)(c + di)) = \phi(a + bi)\phi(c + di)$.

Proof: Let $(a + bi), (c + di) \in \mathbb{Z}[i]$ where $(a + bi)$ and $(c + di)$ are relatively prime. By Theorem 2.7, we can say

$$\begin{aligned} \phi((a + bi)(c + di)) &= |U(\mathbb{Z}[i]_{(a+bi)(c+di)})| \\ &= |U(\mathbb{Z}[i]_{(a+bi)}) \times U(\mathbb{Z}[i]_{(c+di)})| \\ &= |U(\mathbb{Z}[i]_{(a+bi)})| |U(\mathbb{Z}[i]_{(c+di)})| \\ &= \phi(a + bi)\phi(c + di). \quad \blacksquare \end{aligned}$$

Assuming this multiplicativity, we can arrive at a closed formula for the evaluation of the function in $\mathbb{Z}[i]$.

Theorem 9.4: Let $(a + bi) \in \mathbb{Z}[i]$. Then $\phi(a + bi) = N(p_1 + k_1i)^{\alpha_1-1}(N(p_1 + k_1i) - 1)N(p_2 + k_2i)^{\alpha_2-1}(N(p_2 + k_2i) - 1)\dots N(p_n + k_ni)^{\alpha_n-1}(N(p_n + k_ni) - 1)$ where $(p_1 + k_1i)^{\alpha_1}(p_2 + k_2i)^{\alpha_2}\dots(p_n + k_ni)^{\alpha_n}$ is the prime factorization of $(a + bi)$.

Note: Let $(a + bi) \in \mathbb{Z}[i]$ such that $(p_1 + k_1i)^{\alpha_1}(p_2 + k_2i)^{\alpha_2}\dots(p_n + k_ni)^{\alpha_n}$ is the prime factorization of $(a + bi)$. Since the function is multiplicative, we know

$$\begin{aligned}\phi(a + bi) &= \phi((p_1 + k_1i)^{\alpha_1}(p_2 + k_2i)^{\alpha_2}\dots(p_n + k_ni)^{\alpha_n}) \\ &= \phi((p_1 + k_1i)^{\alpha_1})\phi((p_2 + k_2i)^{\alpha_2})\dots\phi((p_n + k_ni)^{\alpha_n})\end{aligned}$$

So it suffices to show that $\phi((p_m + k_mi)^{\alpha_m}) = N(p_m + k_mi)^{\alpha_m-1}(N(p_m + k_mi) - 1)$ for any prime $(p_m + k_mi) \in \mathbb{Z}[i]$.

Proof: Let $(p_m + k_mi)$ be a prime element of $\mathbb{Z}[i]$. We must consider two cases.

Case 1: Assume p_m and k_m are nonzero. By Theorem 8.8, we know

$$|\mathbb{Z}[i]_{(p_m+k_mi)^{\alpha_m}}| = N((p_m + k_mi)^{\alpha_m}) = (N(p_m + k_mi))^{\alpha_m}.$$

This tells us the number of Gaussian Integers modulo $(p_m + k_mi)^{\alpha_m}$. To calculate $\phi(a+bi)$, we must subtract from this all elements of this set that are not invertible. That is to say, we must subtract all elements that divide $(p_m + k_mi)^{\alpha_m}$. By Theorem 3.4, we know that

$$\{(a + bi) \in \mathbb{Z}[i] : (a + bi)|(p_m + k_mi)^{\alpha_m}\} = \{(a + bi) \in \mathbb{Z}[i] : N(a + bi)|N((p_m + k_mi)^{\alpha_m})\}$$

By Definition 6.1, we know $N(p_m + k_mi)$ must be prime in \mathbb{Z} . So the only divisors of $N(p_m + k_mi)^{\alpha_m}$ are $1, N(p_m + k_mi), N(p_m + k_mi)^2, \dots, N(p_m + k_mi)^{\alpha_m-1}, N(p_m + k_mi)^{\alpha_m}$. There are $N(p_m + k_mi)^{\alpha_m-1}$ of these divisors. So

$$\begin{aligned}\phi((p_m + k_mi)^{\alpha_m}) &= (N(p_m + k_mi))^{\alpha_m} - N(p_m + k_mi)^{\alpha_m-1} \\ &= N(p_m + k_mi)^{\alpha_m-1}(N(p_m + k_mi) - 1)\end{aligned}$$

Case 2: Let $(p_m + k_mi) = ua$ where u is a Gaussian unit and a is an odd prime in $\mathbb{Z}[i]$ such that $a \equiv 3 \pmod{4}$. By Theorem 8.8, we know

$$|\mathbb{Z}[i]_{(p_m+k_mi)^{\alpha_m}}| = N((p_m + k_mi)^{\alpha_m}) = (N(p_m + k_mi))^{\alpha_m}.$$

So the total number of Gaussians modulo $(p_m + k_mi)^{\alpha_m}$ is $a^{2\alpha_m}$. Similarly to Case 1, we must subtract out all integers which are not relatively prime to $a^{2\alpha_m}$ to account for the Gaussians not relatively prime to $(p_m + k_mi)^{\alpha_m}$. Since a is a prime, the only divisors of $a^{2\alpha_m}$ are $a^2, a^3, \dots, (a^2)^{\alpha_m-1}, (a^2)$. There are $(a^2)^{\alpha_m-1}$ of these elements, so we know

$$\begin{aligned}\phi((p_m + k_mi)^{\alpha_m}) &= a^{2\alpha_m} - (a^2)^{\alpha_m-1} \\ &= N((p_m + k_mi)^{\alpha_m-1})(N((p_m + k_mi)^{\alpha_m}) - 1). \blacksquare\end{aligned}$$

Now that we have a closed formula, let's evaluate the phi function for the Gaussian Integer in Example 7.1.

Example 9.5: Consider $(24 + 23i)$. We know a prime factorization of this Gaussian Integer is $(1 + 2i)(2 + 3i)(1 - 4i)$. Using our formula we can see that

$$\begin{aligned}\phi(24 + 23i) &= (N(1 + 2i) - 1)(N(2 + 3i) - 1)(N(1 - 4i) - 1) \\ &= (4)(12)(16) \\ &= 768.\end{aligned}$$

Conclusion

The Euler- ϕ function can be evaluated in $\mathbb{Z}[i]$ using a closed formula dependent on Gaussian Prime Factorizations and the Gaussian Norm Function. The evaluation of this function gives us insight to the number of invertible elements of $\mathbb{Z}[i]$ relative to any Gaussian Integer. The methods defined in this paper could be used to analyze other integral functions and properties in $\mathbb{Z}[i]$ and other subsets of \mathbb{C} . The fact that integral properties of modular arithmetic hold in $\mathbb{Z}[i]$ suggests that other number theoretic theorems typically applied to \mathbb{Z} , including many of Fermat's theorems, could potentially have analogous applications within $\mathbb{Z}[i]$.