The Arithmetic of the Gaussian Integers

Alexandria, Kaeli, William

MATH 444
Assignment 8

June 29, 2020

History and Outline

Carl Friedrich Gauss

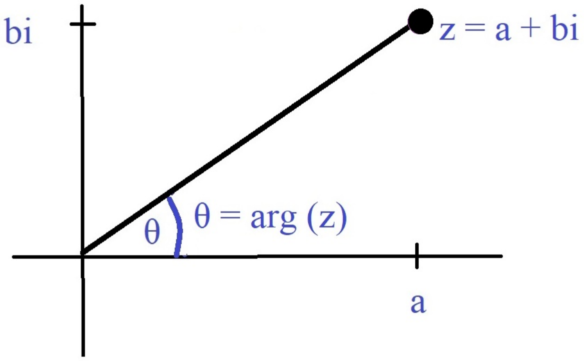
Carl Friedrich Gauss (1777-1855) was a German number theorist who influenced many diverse fields of mathematics. The investigations described in this paper were first addressed in his 1832 monograph *Theoria Residuorum Biquadraticorum,* in which Gauss laid the foundation for much of modern number theory. One of his innumerable contributions to the field was the discovery of the *Gaussian Integers,* which he defined and proved various results about. The properties of this particular subset of the complex numbers is the topic of this paper.

The Gaussian integers are the complex numbers of the form $a + bi$ where a and b are integers. The set of all such numbers is denoted $\mathbb{Z}[i]$. One can add and multiply Gaussian integers as one would with any complex numbers. This definition suggests that the Gaussian integers have analogous arithmetic properties to the integers. Indeed, this paper will show that the Gaussian integers can be used to investigate the properties of the integers, and simplify various problems in number theory by translating them into the setting of the Gaussian integers.
In this paper, we will first develop the theory of the Gaussian integers, then we will apply our results to give a novel proof of Fermat's theorem on the sum of two squares. The reader will observe the similarities between arithmetic in $\mathbb{Z}$ and $\mathbb{Z}[i]$, while at the same time, she will notice the simplifying tactic of reframing problems in terms of the Gaussian integers.

Background - The Complex Numbers $\mathbb{C}$

The complex numbers $\mathbb{C}$ are defined as the set $\{x + iy \mid x, y \in \mathbb{R}\}$. Here, the symbol i refers to the *imaginary unit*, a number such that $i^2 = -1$. Geometrically, the complex numbers can be understood as a plane where the point $(A, B) \in \mathbb{R}^2$ corresponds to the complex number

$A + Bi \in \mathbb{C}$. We can measure the length of a complex number using the complex modulus; $\mid a + bi \mid = \sqrt{a^2 + b^2} \in \mathbb{R}_{\geq 0}$ is interpreted as the distance from the origin, $0 + 0i$, to the complex number $a + bi$. If z is a non zero complex number, there is an associated angle measurement called $arg(z)$, the argument of z, which measures the angle described in the diagram:



The argument of a complex number z

We use $Arg(z)$ with a capital "A" for $arg(z) \in [0, 2\pi)$, and we call this function the principal argument of a complex number z. We note that, of course, angles are measured in radians during our analysis.

The complex numbers exhibit many familiar algebraic properties. We see that $\mathbb{C}$ is associative, commutative, and distributive with respect to $+$ and $\cdot$. That is, for all $\alpha, \beta, \gamma \in \mathbb{C}$, the following properties always hold:

Associativity:

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$$

$$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$$

Commutativity:

$$\alpha + \beta = \beta + \alpha$$

$$\alpha \cdot \beta = \beta \cdot \alpha$$

Distributivity:

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$$

We often write $\alpha \cdot \beta$ as $\alpha\beta$.

We wish to study a particular subset of $\mathbb{C}$, namely, the *Gaussian integers,* denoted $\mathbb{Z}[i]$. Since $\mathbb{Z}[i] \subseteq \mathbb{C}$, we see that the algebraic properties listed above also apply for all $\alpha, \beta, \gamma \in \mathbb{Z}[i]$. As with the ordinary integers, we begin our investigations with a close examination of the operations on the set $\mathbb{Z}[i]$, namely, addition and multiplication.

Operations on the Gaussian Integers

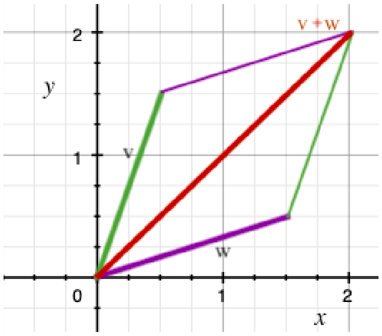
The Gaussian Integers are defined by the set: $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$. The sum and product of two Gaussian integers is inherited from the sum and product of two complex numbers, that is:

$$(a + bi) + (c + di) := (a + c) + (b + d)i$$

and

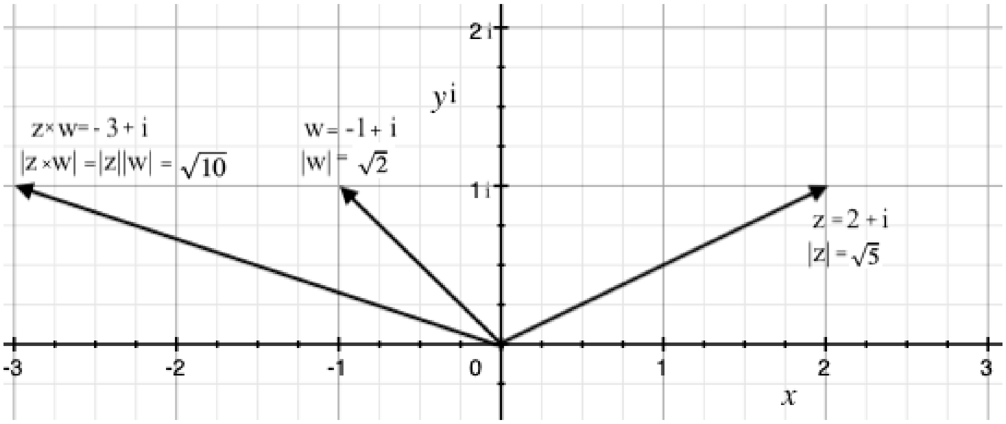
$$(a + bi)(c + di) := (ac - bd) + (ad + bc)i.$$

From this it follows that if $\alpha, \beta \in \mathbb{Z}[i]$ then both $\alpha \pm \beta \in \mathbb{Z}[i]$ and $\alpha\beta \in \mathbb{Z}[i]$.
We note that addition and multiplication of Gaussian integers (and indeed any complex numbers) have a nice geometric interpretation, i.e.:



The parallelogram rule for adding $v, w \in \mathbb{C}$

Also, multiplying $w \in \mathbb{C}$ by a complex number z amounts to rotating w by $Arg(z)$ and scaling w by $\mid z \mid$:



The geometry of $z \times w$, $z, w \in \mathbb{C}$

Hence, one sees that all the integer multiples of a Gaussian integer z consist of those integer points in the plane through which the line connecting z and 0 passes. These geometric properties will help us gain intuition about the arithmetic of the Gaussian integers.

Notice that it is uncommon for the division of one Gaussian Integer by another to yield a Gaussian Integer as its quotient (the analogous statement in $\mathbb{Z}$ is also seen to be true). For example, we can divide these two elements in $\mathbb{C}$ to find:

$$\frac{1+6i}{4+7i} = \frac{46}{75} + \frac{17}{65}i$$

is not a Gaussian integer. However, we find that some particular divisions do yield a quotient in $\mathbb{Z}[i]$:

$$\frac{2+5i}{i} = 5-2i$$
$$\frac{-6+8i}{1+7i} = 1+i$$

To further understand this divisibility behavior, we develop a tool to measure the size of a Gaussian integer called the *Norm.*

The Norm on $\mathbb{Z}[i]$

The Norm on the Gaussian integers is a function:

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$$

Defined by:

$$N(a+bi) = a^2 + b^2.$$

The norm of a Gaussian integer $z = a + bi$ is the same as the product $zz^* \in \mathbb{C}$, where z^* denotes the complex conjugate of the complex number z (if $z = a + bi$ then $z^* = a - bi$). To see this, note that:

$$\begin{aligned} N(z) =& a^2 + b^2 \\ =& a^2 + abi - abi + b^2 \\ =& (a+bi)(a-bi) \\ =& zz^* \end{aligned}$$

The norm is related to the complex modulus, in that $N(z) =\mid z \mid^2$. We use the square of the complex modulus as the norm on $\mathbb{Z}[i]$ since in our algebraic analysis, it is often more helpful to consider the size of a Gaussian integer as a positive integer instead of a potentially irrational number. The norm is useful for studying divisibility, due to the fact that it translates divisibility in $\mathbb{Z}[i]$ to divisibility in $\mathbb{Z}$, a domain where divisibility is well understood. More precisely: the norm is a multiplicative function. By this we mean that if $\alpha, \beta \in \mathbb{Z}[i]$ then $N(\alpha\beta) = N(\alpha)N(\beta)$. A direct computation proves this fact. Suppose that $\alpha = a_1 + a_2 i$ and $\beta = b_1 + b_2 i$ are Gaussian integers. Then we have:

$$\begin{aligned}
N(\alpha\beta) =& N((a_1 + a_2 i)(b_1 + b_2 i)) \\
=& N(a_1 b_1 - a_2 b_2 + (a_2 b_1 + a_1 b_2)i) \\
=& (a_1 b_1 - a_2 b_2)^2 + (a_2 b_1 + a_1 b_2)^2 \\
=& a_1^2 b_1^2 - \cancel{2a_1 a_2 b_1 b_2} + a_2^2 b_2^2 + a_2^2 b_1^2 + \cancel{2a_1 a_2 b_1 b_2} + a_1^2 b_2^2 \\
=& (a_1^2 + a_2^2)(b_1^2 + b_2^2) \\
=& N(\alpha)N(\beta)
\end{aligned}$$

We now define divisibility in $\mathbb{Z}[i]$ in an analogous way to divisibility in $\mathbb{Z}$, using the norm's multiplicativity to great effect.

Divisibility in $\mathbb{Z}[i]$

Let α and β be Gaussian integers. We say that α divides β when there exists a Gaussian integer X such that $\alpha X = \beta$. In this case, β is a multiple of α, and α is a factor of β. We use the notation $\alpha \mid \beta$ to state that α divides β.

For example, we know that $(1+i) \mid (-3+5i)$ since the following equation is true:

$$(1+i)(1+4i) = (-3+5i).$$

Let us collect some facts and definitions regarding divisibility.

Definition 1 (Unit): A Gaussian integer u is said to be a *unit* if it has a multiplicative inverse. That is, $u \in \mathbb{Z}[i]$ is a unit if and only if there exists $x \in \mathbb{Z}[i]$ such that $ux = 1$.

We identify all the units in $\mathbb{Z}[i]$ using the norm in the following proposition.

Proposition 1: A Gaussian integer u is a unit if and only if $N(u) = 1$. Furthermore, $u \in \{1, -1, i, -i\} = \{i^k \mid k = 0, 1, 2, 3\}$.
Proof: $(\rightarrow)$ Suppose $u \in \mathbb{Z}[i]$ is a unit. Then, there exists $x \in \mathbb{Z}[i]$ such that $ux = 1$. Taking the norm of this equation we find that $N(ux) = N(u)N(x) = 1$. Hence $N(u) = 1$. $(\leftarrow)$ Conversely, suppose $u \in \mathbb{Z}[i]$ is such that $N(u) = 1$. Then, if $u = a + bi$ for $a, b \in \mathbb{Z}$, it would follow that $N(u) = N(a + bi) = a^2 + b^2 = 1$. We see that the following set of ordered pairs (a, b) is an exhaustive set of solutions to $a^2 + b^2 = 1$:

$$\{(1,0), (0,1), (-1,0), (0,-1)\}$$

These ordered pairs correspond to the Gaussian integers $1, i, -1, -i$ respectively. Indeed, $\{\pm 1, \pm i\}$ are all the units of $\mathbb{Z}[i]$.

Definition 2 (Associates): Two Gaussian integers α, β are said to be associates if $\alpha = \beta u$ for some unit u. By Proposition 1 this is equivalent to $\alpha = i^k \beta$ for some positive integer k. Moreover, we note that associates have the same norm since:

$$\alpha = i^k \beta \implies N(\alpha) = N(i^k)N(\beta) = N(\beta)$$

We denote by $\overline{\alpha} := \{i^k \alpha \mid k \in \{0, 1, 2, 3\}\}$.

Definition 3 (the Ideal of a Gaussian integer): Let $\beta \in \mathbb{Z}[i]$. We define the Ideal of β to be the set of all $\mathbb{Z}[i]$-multiples of β :

$$< \beta >:= \{\beta x \mid x \in \mathbb{Z}[i]\}$$

From this definition it follows that $\beta \mid \alpha$ if and only if $\alpha \in< \beta >$. One also sees that if $u \in \mathbb{Z}[i]$ is a unit then $< u >= \mathbb{Z}[i]$.

Definition 4 (Greatest Common Divisor): Given two Gaussian integers α, β not both equal to zero, we define the set of common divisors of α, β as:

$$\{X \in \mathbb{Z}[i] : X \mid \alpha \text{ and } X \mid \beta\}$$

There will be an X with maximal norm in this set, and it is this X that we call the greatest common divisor of α and β. We denote this as $\gcd(\alpha, \beta) = X$. The gcd is unique up to associates, as $\delta = \gcd(\alpha, \beta) \mid \alpha, \beta$ implies that for any unit u, $u\delta \mid \alpha$ and $u\delta \mid \beta$. When $\gcd(\alpha, \beta) = 1$ we say α and β are coprime.

Our first theorem will establish a general "long division" of Gaussian integers which is indeed very similar to long division in $\mathbb{Z}$.

Theorem 1 (The Division Theorem):

Given Gaussian integers $\alpha, \beta \neq 0$, there exists $Q, R \in \mathbb{Z}[i]$ such that

$$\alpha = Q\beta + R \text{ and } N(R) \leq \frac{N(\beta)}{2}$$

Proof: We begin by performing the following division in $\mathbb{C}$:

$$\frac{\alpha}{\beta} = x + iy$$

Where $x, y \in \mathbb{R}$. In constructing the desired quotient $\alpha = Q\beta + R$ we choose integers m, n such that:

$$\mid x - m \mid \leq \frac{1}{2}$$

and

$$\mid y - n \mid \leq \frac{1}{2}.$$

We can certainly find such an m and n since every real number is at most distance $\frac{1}{2}$ from the nearest integer. This choice of m, n yields:

$$N(x-m+i(y-n)) = (x-m)^2 + (y-n)^2 \leq (\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{2}.$$

Setting $Q = m + in$ and $R = \beta(x - m + i(y-n))$ gives the desired quotient since:

$$\beta Q + R = \beta(m+in) + \beta(x-m+i(y-n)) = \beta(m-m+in-in+x+iy) = \beta(x+iy) = a.$$

Where the last equality follows from $\frac{\alpha}{\beta} = x + iy$.
It remains to show that the remainder R has the desired norm $\leq \frac{N(\beta)}{2}$. This follows from the calculation:

$$N(R) = N(\beta)N(x-m+i(y-n)) = N(\beta)((x-m)^2 + (y-n)^2) \leq \frac{N(\beta)}{2}$$

Proving Theorem 1. □

Notice that unlike the analog of this theorem in $\mathbb{Z}$, the choice of Q, R is not guaranteed to be unique. One can impose additional restrictions on the remainder to secure uniqueness.

With these definitions and results, we may define the notion of primality in $\mathbb{Z}[i]$.

Gaussian Primes

In order to avoid ambiguity in the terms ”integer” and ”prime,” we provide clarification in Definition 5.

Definition 5 (Rational Integer and Rational Prime): A rational integer is simply an element of $\mathbb{Z}$. A prime in $\mathbb{Z}$ is called a rational prime.

Definition 6 (Trivial Factorization): Let $\gamma \in \mathbb{Z}[i]$. Suppose γ factors in $\mathbb{Z}[i]$ as $\gamma = \alpha\beta$. This factorization is called trivial when one of α or β is a unit. In this case, one notes that the other factor is associated to γ.

Now on to Gaussian Primes.

Definition 7 (Gaussian Prime): A Gaussian prime π is a Gaussian integer which cannot be written as the product of two non units. That is, if we have a factorization

$$\pi = \alpha\beta \in \mathbb{Z}[i],$$

then α is a unit and β is associate to π. Equivalently, π cannot be written as the product of two Gaussian integers, each smaller in norm than π, and π has no non trivial factorization.

There are a few immediately interesting observations about primes in $\mathbb{Z}[i]$. For instance, the integers 2 and 5 are rational primes, yet in $\mathbb{Z}[i]$, these integers have the non trivial factorizations:

$$(1+i)(1-i) = 2$$

$$(2+i)(2-i) = 5,$$

and so neither 2 nor 5 are Gaussian primes. Notice that each of the factors is smaller in norm than the product, and neither factor is a unit. We will come to see that p a rational prime is also a Gaussian prime if and only if $p \equiv 3 \pmod 4$. Furthermore, one notes that $(1+i)$ and $(2+i)$ are Gaussian primes with a direct application of Proposition 2, shown below. The following propositions will be useful in our study of the Gaussian primes:

Proposition 2: Let $\alpha, \beta \in \mathbb{Z}[i]$. If $\beta \mid \alpha$ then $N(\beta) \mid N(\alpha)$.
Proof: If $\beta \mid \alpha$ then for some $X \in \mathbb{Z}[i]$ we have $X\beta = \alpha$. Evaluating the norm on this equation gives:

$$N(\alpha) = N(X)N(\beta)$$

Which implies that $N(\beta) \mid N(\alpha)$ as required.

Proposition 3: If $z \in \mathbb{Z}[i]$ and $N(z) = p$, a rational prime, then z is a Gaussian prime.
Proof: We take a factorization of z as a product of two Gaussian integers:

$$z = \alpha\beta,$$

for some $\alpha, \beta \in \mathbb{Z}[i]$. By the previous Proposition we have: $N(\alpha) \mid N(z) = p$, and since p is a rational prime, it follows that either $N(\alpha) = 1$ or $N(\alpha) = p$. If $N(\alpha) = 1$ then by Proposition 1, α is a unit and so z is a Gaussian prime. On the other hand, if $N(\alpha) = p$ then $N(\beta) = 1$ and thus β is a unit. Since any factorization of z includes a unit, we deduce that z is indeed a Gaussian prime, as required.

Our next theorem gives a helpful representation of the gcd of two Gaussian integers. This is the analog of ”Bézout’s Theorem” in number theory.

Theorem 2 (Bézout’s Theorem in $\mathbb{Z}[i]$):

Let $\delta \in \mathbb{Z}[i]$ be a greatest common divisor of $\alpha, \beta \in \mathbb{Z}[i]$. Then, there exists $x, y \in \mathbb{Z}[i]$ such that

$$\alpha x + \beta y = \delta.$$

Proof: We consider the set S :

$$S := \{\alpha x + \beta y \mid x, y \in \mathbb{Z}[i] \text{ and } N(\alpha x + \beta y) > 0\}$$

There is an element in this set with the smallest norm (there may be multiple elements with the smallest norm – in this case, we select one of them), call it d. Since $d \in S$, we can write:

$$d = \alpha x_0 + \beta y_0,$$

for some $x_0, y_0 \in \mathbb{Z}[i]$.
Claim 1: $d \mid \alpha$ and $d \mid \beta$.
Proof of Claim: Using Theorem 1 we preform this division in $\mathbb{Z}[i]$:

$$\alpha = dQ + R \text{ where Q,R} \in \mathbb{Z}[i] \text{ and } 0 \leq N(R) \leq \frac{N(d)}{2}$$

This yields that:

$$R = \alpha - dQ = \alpha(1 - Qx_0) + \beta(-y_0Q)$$

and thus if $N(R) > 0$, then R would be an element of S. However, R cannot be an element of S since $N(R) < N(d)$ and d has minimal norm. Hence, $N(R) = 0$ and thus $R = 0$. We have found that $\alpha = dQ$ and so $d \mid \alpha$. An identical argument yields that $d \mid \beta$. This concludes the proof of Claim 1.
Hence d is a common divisor of α, β. Additionally, since:

$$d = \alpha x_0 + \beta y_0$$

we see that any common divisor of α, β is also a divisor of d. This proves that $\gcd(\alpha, \beta) = d = \delta$, and setting $X = x_0, Y = y_0$ we get:

$$\gcd(\alpha, \beta) = \delta = \alpha X + \beta Y$$

as required for Theorem 2. □

Corollary 1: Let $\alpha, \beta \in \mathbb{Z}[i]$. Then, there exists $X, Y \in \mathbb{Z}[i]$ such that $\alpha X + \beta Y = 1$ if and only if $\gcd(\alpha, \beta) = 1$.
Proof: ($\leftarrow$): If $\gcd(\alpha, \beta) = 1$ then by Theorem 2 there exists $X, Y \in \mathbb{Z}[i]$ with the property that $\alpha X + \beta Y = 1$. ($\rightarrow$): If $\alpha X + \beta Y = 1$ then any common divisor of α, β will divide 1. The only elements of $\mathbb{Z}[i]$ which divide 1 are the units, and so $\gcd(\alpha, \beta) = 1$.

Corollary 2: Let $\alpha, X, Y \in \mathbb{Z}[i]$. If $\gcd(\alpha, X) = 1$ and $\alpha \mid XY$, then $\alpha \mid Y$.
Proof: By Theorem 2 we have:

$$\alpha x_0 + X y_0 = 1$$

for some $x_0, y_0 \in \mathbb{Z}[i]$. Multiplying this equation by Y gives:

$$Y\alpha x_0 + XY y_0 = Y.$$

Since $\alpha \mid Y\alpha x_0$ and $\alpha \mid XYy_0$, we deduce that α divides the sum of these two terms, and thus $\alpha \mid Y$ as required.

In particular, Corollary 2 tells us that if π is a Gaussian prime with the property that $\pi \nmid X$, and $\pi \mid XY$, then $\pi \mid Y$. This is the statement of Euclid's Lemma in $\mathbb{Z}[i]$.

We now ask whether the Fundamental Theorem of Arithmetic can be generalized to the Gaussian integers. Indeed, one can assert a suitable generalization of the Fundamental Theorem of Arithmetic in $\mathbb{Z}[i]$. To prove this important fact, we will need the following Proposition:

Proposition 4: Let π be a Gaussian prime and $z_i \in \mathbb{Z}[i]$. If $\pi \mid z_1 \dots z_n$ for $n \geq 1$, then $\pi \mid z_j$ for some $j \in \{1, \dots, n\}$.
Proof: We proceed with induction. When $n = 1, 2$ the result follows by Corollary 2. Assume that Proposition 4 is true for all k with $2 < k < n$. Next we show the result is true for n. Suppose that $\pi \mid z_1 \dots z_n$. By Corollary 2, either $\pi \mid z_1$ or $\pi \mid z_2 \dots z_n$. If $\pi \mid z_1$ then we are done. If $\pi \mid z_2 \dots z_n$, then we have a prime dividing a product of $n - 1$ terms. Since the number of terms in the product is less than n, we can apply the inductive hypothesis to find that $\pi \mid z_j$ for some $j \in \{2, \dots, n\}$. This proves the proposition.

On to our third Theorem.

Theorem 3 (Unique Gaussian Prime Factorization):

A Gaussian integer α can be written uniquely as a product of Gaussian primes up to a reordering of the factors and multiplication by a unit. That is:

$$\alpha = u \prod_{i=1}^{n} \pi_i^{\gamma_i}$$

is a unique expression where u is a unit, π_i for $i \in \{1, \dots, n\}$ are distinct (nonassociate) Gaussian primes, and n, γ_i are nonnegative integers.
Proof: We first prove that such a prime factorization exists, then we show that it is essentially unique.
(Existence) We use induction on the norm of α. For the base case, note that if $N(\alpha) = 1$ then $\alpha \in \{\pm 1, \pm i\}$ is written as the empty product of primes times the unit α. Suppose that all Gaussian integers z with $1 < N(z) < m$ have prime factorizations. We show that also α with $N(\alpha) = m$ has a prime factorization. If α is a Gaussian prime then we have its prime factorization as simply α. Hence, we may assume α is not a Gaussian prime. But this implies there is a nontrivial factorization:

$$\alpha = XY \text{ for some } X, Y \in \mathbb{Z}[i]$$

Applying the norm, we find that $N(X), N(Y) < N(\alpha) = m$, and thus we can apply the inductive hypothesis to both X and Y to find that:

$$X = u \prod_{i=1}^{r} \pi_i \text{ and } Y = u' \prod_{j=1}^{s} \rho_j$$

for Gaussian primes π_i, ρ_j and units u, u'. Hence we get that:

$$\alpha = uu' \prod_{i=1}^{r} \pi_i \prod_{j=1}^{s} \rho_j$$

Showing that α can be written as a product of primes. By induction, the Existence claim follows.
(Uniqueness) Assume that α is a Gaussian integer which can be expressed as a product of two different collections of primes. That is:

$$\alpha = \pi_1 \ldots \pi_k = \rho_1 \ldots \rho_\ell$$

where $\{\overline{\pi_i} \mid 1 \leq i \leq k\} \neq \{\overline{\rho_j} \mid 1 \leq j \leq \ell\}$ and all of π_i, ρ_j are Gaussian primes. Further assume that among the Gaussian integers which have two different prime factorizations, α has the smallest norm (we choose α to have minimal norm even if the choice is not unique). Thus we can form a new Gaussian integer called β according to:

$$\beta := \frac{\alpha}{\pi_1} = \pi_2 \ldots \pi_k = \frac{\rho_1 \ldots \rho_\ell}{\pi_1}$$

From this we find that $\pi_1 \mid \rho_1 \ldots \rho_\ell$, and so applying Proposition 4 gives: $\pi_1 \mid \rho_j$ for some $j \in \{1, \ldots, \ell\}$. Using a suitable renumbering, we can assert that $\pi_1 \mid \rho_1$. Then we know that $\{\overline{\pi_2}, \ldots \overline{\pi_k}\} \neq \{\overline{\rho_2}, \ldots, \overline{\rho_\ell}\}$, and so β has two different prime factorizations:

$$\beta = \pi_2 \ldots \pi_k = \rho_2 \ldots \rho_\ell$$

Noting that $N(\beta) = \frac{N(\alpha)}{N(\pi_1)} < N(\alpha)$ we encounter a contradiction regarding the minimality of α, since we found a Gaussian integer β smaller than α which has two different prime factorizations. This proves Theorem 3. □

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

We develop a theory of modular arithmetic in $\mathbb{Z}[i]$ which is a generalization of modular arithmetic in $\mathbb{Z}$. We define the notion of congruence and prove essential facts about modular arithmetic in $\mathbb{Z}[i]$.

Definition 7 (Congruence modulo μ): The Gaussian integers α and β are said to be congruent modulo μ when $\mu \mid (\alpha - \beta)$. When this is the case, we write $\alpha \equiv \beta \pmod{\mu}$.

One finds that the relation "is congruent to modulo μ" satisfies the following three statements:

(i) $\alpha \equiv \alpha \pmod{\mu}$ for all $\alpha \in \mathbb{Z}[i]$
(ii) if $\alpha \equiv \beta \pmod{\mu}$ then $\beta \equiv \alpha \pmod{\mu}$
(iii) if $\alpha \equiv \beta \pmod{\mu}$ and $\beta \equiv \gamma \pmod{\mu}$ then $\alpha \equiv \gamma \pmod{\mu}$

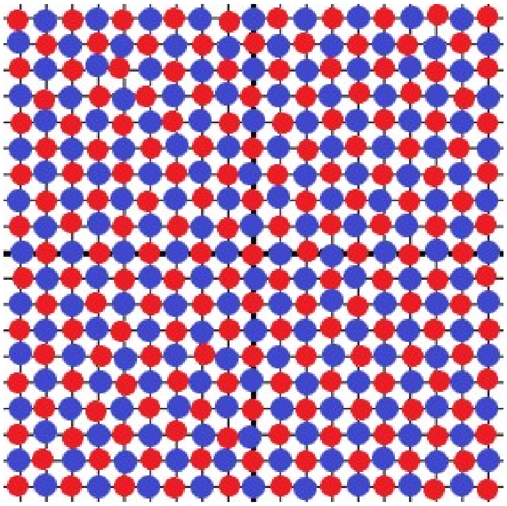
And hence, $\equiv$ is an equivalence relation on $\mathbb{Z}[i]$ whose equivalence classes partition the Gaussian integers.

Definition 8 (Residue Classes modulo μ): The residue class of α modulo μ is defined and denoted as:

$$[\alpha]_\mu := \{z \in \mathbb{Z}[i] \mid z \equiv \alpha \pmod{\mu}\}$$

The residue classes modulo μ partition $\mathbb{Z}[i]$.

Using modular arithmetic in $Z[i]$, we can suitably generalize evenness and oddness to $\mathbb{Z}[i]$. The Gaussian integer $1+i$ functions a lot like the integer 2 does in determining the parity of an integer. We illustrate this with a diagram showing the partition formed by the residue classes with respect to the modulus $1+i$:



The even (red) and odd (blue) Gaussian integers

Notice that all the ordinary even integers are also even Gaussian integers, ditto for the odds. We see that when we select the modulus $\mu = 1+i$, there form two equivalence classes partitioning $\mathbb{Z}[i]$, the even Gaussian integers and the odd Gaussian integers.

We now apply the Gaussian integers to prove a famous result of Fermat, that every prime congruent to 1 modulo 4 can be expressed as a sum of two squares.

Fermat's Theorem on Sums of Two Squares

We begin with three propositions that will aid us in our proof.

Proposition 5: If p is a prime then:

$$(p-1)! \equiv -1 \pmod{p}$$

Proof: If $p = 2$ then $(2-1)! \equiv -1 \pmod 2$. Hence we may assume p is an odd prime. In this case, we note that the only elements which are their own multiplicative inverses modulo p are 1 and $p-1$ since:

$$x^2 \equiv 1 \pmod p \implies (x+1)(x-1) \equiv 0 \pmod p$$

Hence, each element in the set $\{2, \ldots, p-2\}$ has a unique, distinct inverse modulo p which is also in the set. Moreover, there are an even number of elements in this set. Therefore, cancelling the pairs of multiplicative inverses in the factorial, we can form this congruence:

$$(p-1)! = (1)(2)\ldots(p-1) \equiv (p-1) \equiv -1 \pmod p$$

as desired.

Proposition 6: If $p \equiv 1 \pmod 4$ is a prime, then there exists an integer m such that:

$$p \mid (m^2+1)$$

Proof: Proposition 5 gives us $(p-1)! \equiv -1 \pmod p$. Since p is an odd prime, we can manipulate this factorial to give:

$$\begin{aligned} -1 &\equiv (1)(2)\ldots(\frac{p-1}{2})(\frac{p+1}{2})\ldots(p-1) \\ &\equiv (\frac{p-1}{2})!(-\frac{p-1}{2})(-\frac{p-3}{2})\ldots(-1) \\ &\equiv (-1)^{\frac{p-1}{2}}((\frac{p-1}{2})!)^2 \\ &\equiv ((\frac{p-1}{2})!)^2 \pmod p \end{aligned}$$

Setting $m := (\frac{p-1}{2})!$ we get the desired congruence $m^2 \equiv -1 \pmod p$ and so $p \mid m^2+1$ as required.

Proposition 7: $\gamma \in \mathbb{Z}[i]$ is a Gaussian prime if and only if $\gamma \mid \alpha\beta$ implies $\gamma \mid \alpha$ or $\gamma \mid \beta$.
Proof: $(\rightarrow)$: The forward implication follows directly from Corollary 2.
$(\leftarrow)$: Assume that if $\gamma \mid \alpha\beta$ then $\gamma \mid \alpha$ or $\gamma \mid \beta$. We wish to prove γ is a Gaussian prime. Assume for contradiction that γ has a nontrivial factorization in $\mathbb{Z}[i]$, say $\gamma = \mu\nu$ with $N(\mu), N(\nu) < N(\gamma)$. Then, $\gamma \mid \mu\nu$, and so by hypothesis we get: $\gamma \mid \mu$ or $\gamma \mid \nu$, both of which are impossible since μ and ν are each smaller than γ in norm. Hence γ does not have a nontrivial factorization, and therefore we find that γ is a Gaussian prime.

With these facts, we can state and prove Fermat's Theorem on the sum of two squares, a theorem that without the use of the Unique factorization of the Gaussian integers is harder to prove.

Theorem 4 (Fermat's Sum of Two Squares):

Let p be an odd prime. Then, there exists integers x, y such that $x^2 + y^2 = p$ if and only if $p \equiv 1 \pmod 4$.
Proof: $(\rightarrow)$: One finds by squaring the numbers $\{0, 1, 2, 3\}$ and reducing modulo 4 that 0 and 1 are the only possible residues produced by squaring an integer modulo 4. Assume $x^2 + y^2 = p$ for some integers x, y. Reducing this equation modulo 4 gives:

$$x^2 + y^2 \equiv p \equiv \pm 1 \pmod 4$$

But since $x^2 + y^2$ can only ever be congruent to one of $0, 1, 2$ modulo 4, we deduce that $p \not\equiv 3 \pmod 4$ and hence $p \equiv 1 \pmod 4$.
$(\leftarrow)$: Assume $p \equiv 1 \pmod 4$. From Proposition 6 we know that there exists an integer m such that $p \mid m^2 + 1$. We note that though $p \nmid m + i$ and $p \nmid m - i$, p does in fact divide the product $(m + i)(m - i) = m^2 + 1$. By Proposition 7, we know that p cannot be a Gaussian prime. Thus, by Theorem 3, p has a Gaussian prime factorization:

$$p = \prod_{i=1}^{n} \pi_i,$$

where each of the π_i are Gaussian primes. Also:

$$N(p) = p^2 = \prod_{i=1}^{n} N(\pi_i)$$

Which in turn implies that each π_i has $N(\pi_i) = p$ and thus $n = 2$. Let $\pi_1 = x + iy \in \mathbb{Z}[i]$. Then we have that:

$$p = N(\pi_1) = (x + iy)(x - iy) = x^2 + y^2$$

and thus we have written the prime $p \equiv 1 \pmod 4$ as a sum of two squares, proving the theorem. $\square$

References

[1] Peiffer, J., Dahan-Dalmedico, A., "Wege und Irrwege - Eine Geschichte der Mathematik", Springer-Verlag, 2013, pp. 293-294.

[2] Stein, Robert G., Exploring the Gaussian Integers, The Two-Year College Mathematics Journal, vol. 7, no. 4 (1976), pp. 4-10.

[3] Sándor S., A Paper-and-Pencil gcd Algorithm for Gaussian Integers, The College Mathematics Journal, vol. 36, no. 5 (2005), pp. 374-380.

[4] Willerding, M., Divisibility and Factorization of Gaussian Integers. The Mathematics Teacher, vol. 59, no. 7 (1966), pp. 634–637.

[5] Thierry, V., "Handbook of Mathematics", HDBom, BoD - Books on Demand, 2015, pp. 56.