Gaussian Integers and Their Properties

Yicheng Zhou (周奕成)

High School Affiliated to Renmin University of China, Beijing, China

Abstract

This article explores the fundamental properties of Gaussian integers, the ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, as introduced by Carl Friedrich Gauss. We establish that $\mathbb{Z}[i]$ is a Euclidean domain and a principal ideal domain (PID), leveraging its norm function $N(a + bi) = a^2 + b^2$ to derive key results. The paper classifies Gaussian primes into three distinct cases based on their norms and rational prime analogs, and constructs a complete residue system for modular arithmetic in $\mathbb{Z}[i]$.

1 Introduction

The Gaussian integers were discovered by *Carolus Fridericus Gauss* and are defined as

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

These numbers played an essential role in Gauss's work, bridging the gap in the study of binary quadratic forms and quadratic residues. Gauss's profound understanding of the ring $\mathbb{Z}[i]$ allowed him to provide his first proof of the famous quadratic reciprocity law. However, since quadratic residues are relatively prevalent, we can hardly provide any insightful arguments about them here. Instead, this article focuses on the primary attributes of the ring $\mathbb{Z}[i]$ discovered by Gauss and explores its relation to quadratic forms.

2 Basic Properties

To study $\mathbb{Z}[i]$, we first define its Euclidean function and show that it is a Euclidean ring. The fractional field of $\mathbb{Z}[i]$ is $\mathbb{Q}[i]$. The Euclidean function of a ring measures the "magnitude" of its elements, and for complex numbers, this can be represented using their conjugates: $\overline{a + bi} = a - bi$. We define the *Norm*, which quantifies the "distance" of an element.

Definition 2.1 (Norm)**.** For $a, b \in \mathbb{Q}$, the norm $N(a + bi)$ is defined as:

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

The norm is a completely multiplicative function. We immediately derive some properties of $N(\alpha)$ in $\mathbb{Z}[i]$:

Lemma 2.1. *For $\alpha, \beta \in \mathbb{Z}[i]$, $N(\alpha\beta) = N(\alpha)N(\beta)$, and thus $\alpha \mid \beta \iff N(\alpha) \mid N(\beta)$.*

Lemma 2.2. *An element $\alpha \in \mathbb{Z}[i]$ is a unit if and only if $N(\alpha) = 1$. Therefore, the only units in $\mathbb{Z}[i]$ are $1, i, -1, -i$.*

The proofs of these lemmas are left to the reader. The ring $\mathbb{Z}[i]$ is generated by its units $\{1, i, -1, -i\}$, so the concept of associated elements ($\sim$) is clear. We define $D := \{\alpha \in \mathbb{Z}[i] \mid \forall a, b \in D, a \nsim b\}$. Since $N(\alpha)$ has a finite number of factors, α must also have a finite number of factors. Therefore, every $\alpha \in \mathbb{Z}[i]$ can be factorized, and $\mathbb{Z}[i]$ is a unique factorization domain (UFD).

3 Principal Ideals in $\mathbb{Z}[i]$

We now determine the structure of principal ideals for Gaussian integers to prepare for modular arithmetic in $\mathbb{Z}[i]$, which involves the set of multiples of a given Gaussian integer.

Theorem 3.1. *If $\mu = a + bi \in \mathbb{Z}[i] \setminus \{0\}$ and $C, C' \in \mathbb{Z}$, then*

$$\theta \in \langle \mu \rangle \iff \theta = \frac{CN(\mu)}{(a, b)} + C'\theta_0,$$

where

$$\theta_0 = ax_0 - by_0 + (a, b)i, \quad ay_0 + bx_0 = (a, b).$$

Proof. If $\mu \mid \theta$, there exists $\delta = x + yi$ such that $\theta = \mu\delta$. Expanding these numbers:

$$\theta = (ax - by) + (ay + bx)i,$$

and we define

$$C' = \frac{ay + bx}{(a, b)}.$$

For the same θ_0 as in the theorem, the subtraction yields:

$$\theta - C'\theta_0 = ax - by + (ay + bx)i - \frac{(ax_0 - by_0)(ay + bx)}{(a, b)} - (ay + bx)i = \frac{(xy_0 - yx_0)N(\mu)}{(a, b)},$$

since

$$ax - by - \frac{(ax_0 - by_0)(ay + bx)}{ay_0 + bx_0} = \frac{(xy_0 - yx_0)(a^2 + b^2)}{ay_0 + bx_0}.$$

Let $C = xy_0 - yx_0$, so θ takes the form given in the theorem. The construction confirms that $\theta \in \langle \mu \rangle$. $\square$

4 Modular System in $\mathbb{Z}[i]$

We first prove that $\mathbb{Z}[i]$ is a Euclidean domain.

Theorem 4.1. *For all $\alpha, \beta \in \mathbb{Z}[i]$, there exist $\gamma, \delta \in \mathbb{Z}[i]$ such that*

$$\beta = \delta\alpha + \gamma, \quad 0 \leq N(\gamma) \leq N(\alpha),$$

and $\gamma = 0 \iff \alpha \mid \beta$.

Proof. Rewrite the equation as:

$$\frac{\beta}{\alpha} = \delta + \frac{\gamma}{\alpha}, \quad 0 \leq N\left(\frac{\gamma}{\alpha}\right) < 1.$$

Since α and β are arbitrary, it suffices to show that for all $\eta = a + bi \in \mathbb{Q}[i]$, there exists $\delta \in \mathbb{Z}[i]$ such that $0 \leq N(\eta - \delta) < 1$. Choose the nearest integers c, d to a, b satisfying $\max(|a - c|, |b - d|) \leq \frac{1}{2}$, and let $\delta = c + di$. Then:

$$N(\eta - \delta) = (a - c)^2 + (b - d)^2 \leq \frac{1}{2} < 1.$$

□

This theorem justifies the use of the Euclidean algorithm in $\mathbb{Z}[i]$. Using the Euclidean algorithm, we can further prove:

Theorem 4.2. *$\mathbb{Z}[i]$ is a principal ideal domain (PID).*

Proof. Let S be a non-zero ideal in $\mathbb{Z}[i]$. There exists $\alpha_0 \in S$ such that $N(\alpha_0) = n_0 = \min\{N(\alpha) \mid \alpha \in S\}$. For any $\alpha \in S$, we can write $\alpha = \beta\alpha_0 + \gamma$ for some $\beta, \gamma \in \mathbb{Z}[i]$, with $N(\gamma) < N(\alpha_0)$. By the definition of an ideal, $\gamma \in S$, which contradicts the minimality of n_0 unless $\gamma = 0$. Therefore, $S = \langle\alpha_0\rangle$. □

The fact that $\mathbb{Z}[i]$ is a PID implies it is also a UFD. With these properties established, we can explore number-theoretic identities, such as the classification of Gaussian primes.

Theorem 4.3. *An element $\pi \in \mathbb{Z}[i]$ is a Gaussian prime if and only if it satisfies one of the following conditions:*

1. $N(\pi) = 2$,
2. $N(\pi) = p \equiv 1 \pmod 4$, *where p is a rational prime,*
3. $\pi \sim p \equiv 3 \pmod 4$, *where p is a rational prime.*

Proof. *Sufficiency:* If $N(\pi)$ is prime, π cannot be factored further due to Lemma 2.2. If $\pi \sim p \equiv 3 \pmod 4$ and $\pi = \alpha\beta$ for non-units α, β, then $N(\pi) = N(\alpha)N(\beta) = p^2$. This implies $N(\alpha) = N(\beta) = p$, but for $p = 4n + 3$, p cannot be expressed as $a^2 + b^2$, leading to a contradiction.

Necessity: Let π be a Gaussian prime. Factorize its norm:

$$N(\pi) = \pi\overline{\pi} = \prod_{i=1}^{r} p_i^{\alpha_i}.$$

There exists a prime p_1 such that $\pi \mid p_1$. Then $N(\pi) \mid N(p_1) = p_1^2$, so $N(\pi)$ divides either p_1 or p_1^2. If $N(\pi) \mid p_1$, π falls into the first or second case. Otherwise, $N(\pi) = p_1^2$ and $\pi \sim p_1$, which corresponds to the third case. □

Theorem 4.4. *For $\mu = a + bi$, the set*

$$S = \left\{ m + ni \mid 0 \le m \le \frac{N(\mu)}{(a,b)} - 1, 0 \le n \le (a,b) - 1 \right\}$$

forms a complete system of residues modulo μ in $\mathbb{Z}[i]$.

Proof. The theorem is equivalent to:

1. For all $\alpha, \beta \in S$, $\alpha \not\equiv \beta \pmod \mu$,
2. For all $\alpha \in \mathbb{Z}[i]$, there exists $\beta \in S$ such that $\alpha \equiv \beta \pmod \mu$.

(1) If $m+ni \equiv m'+n'i \pmod \mu$, then $\mu \mid (m-m')+(n-n')i$. By Theorem 2.4, $(a,b) \mid (n-n')$, so $n = n'$. Similarly, $m - m' \mid \theta = \frac{CN(\mu)}{(a,b)}$ implies $m = m'$.

(2) Let $\alpha = c + di \in \mathbb{Z}[i]$. Write:

$$d = q(a,b) + r, \quad q \in \mathbb{Z},$$

and

$$c - q(ax_0 - by_0) = \frac{q'N(\mu)}{(a,b)} + r', \quad 0 \leq r' \leq \frac{N(\mu)}{(a,b)} - 1,$$

where $ax_0 - by_0$ is as defined in Theorem 2.4. Combining these:

$$c + di = \frac{q'N(\mu)}{(a,b)} + q(ax_0 - by_0) + q(a,b)i + r' + ri.$$

Thus, $\alpha \equiv r' + ri \pmod{\mu}$, where $r' + ri \in S$. □

5 Conclusion

The Gaussian integers $\mathbb{Z}[i]$ form a rich algebraic structure with properties that generalize many concepts from ordinary integers. As a Euclidean domain and a principal ideal domain, $\mathbb{Z}[i]$ shares similarities with $\mathbb{Z}$ but also exhibits unique features, such as its classification of primes and modular arithmetic. These properties make Gaussian integers a powerful tool in number theory, particularly in the study of quadratic forms and Diophantine equations. Further exploration could delve into applications of $\mathbb{Z}[i]$ in cryptography or algorithmic number theory, where its structure provides elegant solutions to complex problems.