# 7.2. The Gaussian Integers

**Note.** In this section, we introduce an algebraic structure (the Gaussian integers) and establish several number theoretic results in this structure. The algebraic structure is a complex analogy of the (real) integers.

**Note 7.2.A.** The *complex numbers* are the set , $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$. For complex numbers $a + bi$ and $c + di$ we have the sums and products:

$$(a + bi) + (c + di) = (a + c) + (b + d)i \text{ and } (a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

The complex numbers form a field (which effectively means that all the usual algebraic properties, such as commutativity and distribution, hold). Every nonzero complex number has a multiplicative inverse, $1/(a + bi) = (a - bi)/(a^2 + b^2)$. The *modulus* (or *absolute value*) of a complex number $z = a + bi$ is $|z| = \sqrt{a^2 + b^2}$, and the *conjugate* of $z = a + bi$ is $\overline{z} = a - bi$. Notice that $|z|^2 = z\overline{z}$. The *norm* of $z$, denoted $N(z)$, is the modulus squared of $z$: $N(z) = N(a + bi) = a^2 + b^2$. The norm of an Gaussian integer is itself a nonnegative integer, and $N$ satisfies: (1) $N(\alpha) = 0$ if and only if $\alpha = 0$, and (2) $N(\alpha\beta) = N(\alpha)N(\beta)$. A mapping satisfying these two properties is sometimes called a *multiplicative norm* (see my online notes for Introduction to Modern Algebra 2 [MATH 4137/5137] on Section IX.47. Gaussian Integers and Multiplicative Norms and notice Definition 47.6).

**Definition 7.13.** The *Gaussian integers* is the subset $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ of $\mathbb{C}$.

**Note 7.2.B.** The Gaussian integers form a commutative ring, but do not form a field since multiplicative inverses may not be present. Since $N$ is an integer valued multiplicative norm on the Gaussian integers, then for $\alpha \in \mathbb{Z}[i]$ invertible, we must have $\alpha\alpha^{-1} = 1$ so that $1 = N(1) = N(\alpha\alpha^{-1}) = N(\alpha)N(\alpha^{-1})$. Since $N$ is integer valued, then $N(\alpha) = N(\alpha^{-1}) = 1$. So, the only elements of $\mathbb{Z}[i]$ that have multiplicative inverses (in a ring, these are called *units*) are $-1$, $1$, $i$, and $-i$; these are called *Gaussian units* of *G-units*.

**Definition.** For $\alpha, \beta \in \mathbb{Z}[i]$, if $\beta = \alpha\gamma$ for some $\gamma \in \mathbb{Z}[i]$, the $\alpha$ *divides* $\beta$, denoted $\alpha \mid \beta$. If $\alpha \in \mathbb{Z}[i]$ and $\varepsilon$ is a Gaussian unit, then $\alpha = \varepsilon(\varepsilon^{-1}\alpha)$ is a *trivial factorization* in $\mathbb{Z}[i]$. A *nontrivial factorization* of an element $\alpha \neq 0$ in $\mathbb{Z}[i]$ is a factorization of the form $\alpha = \beta\gamma$ in which both $\beta$ and $\gamma$ are non-Gaussian-units.

**Note.** Notice that if $\alpha = \beta\gamma$ is a nontrivial factorization of $\alpha$, then $|\alpha|^2 = |\beta|^2|\gamma|^2$ or $N(\alpha) = N(\beta)N(\gamma)$. Since neither $\beta$ nor $\gamma$ is a unit, then $1 < N(\beta), N(\gamma) < N(\alpha)$, $N(\beta) \mid N(\alpha)$, and $N(\gamma) \mid N(\alpha)$. So a nontrivial factorization in $\mathbb{Z}[i]$ gives a nontrivial factorization of positive integers in $\mathbb{Z}$ (namely of the associated norms). Repeated factoring then yields a descending sequence of positive integers of norms; a decreasing sequence of positive integers must end, so that the nontrivial factoring must end. We then have for any nonzero unit $\alpha \in \mathbb{Z}[i]$ has a factorization of the form $\alpha = \pi_1\pi_2 \cdots \pi_r$ where each $\pi_i$ is a nonunit which has no nontrivial factorization in $\mathbb{Z}[i]$. This gives us a way to define a prime Gaussian integer, which will lead to our Fundamental Theorem of Arithmetic in $\mathbb{Z}[i]$.

**Definition.** Nonzero nonunit $\pi_i \in \mathbb{Z}[i]$ is a *Gaussian prime* (or *G-prime*) if it has no nontrivial factorization in $\mathbb{Z}[i]$.

**Note 7.2.C.** Determining which Gaussian integers are Gaussian primes is more involved that finding prime integers. One approach to test nonzero nonunit $\alpha$ for primeness is to test each nonunit $\beta$ satisfying $M(\beta) \mid N(\alpha)$ to see if its a divisor of $\alpha$. Notice that an integer prime in $\mathbb{Z}$ may not be prime in $\mathbb{Z}[i]$; we have $2 = (1+i)(1-i)$ in $\mathbb{Z}[i]$ and $5 = (1+2i)(1-2i)$. However, 3 is both a prime and a Gaussian prime because for nontrivial factorization $3 = \beta\gamma$ in $\mathbb{Z}[i]$, we would have $9 = N(3) = N(\beta)N(\gamma)$ and hence $N(\beta) = N(\gamma) = 3$, but there is no $a + bi \in \mathbb{Z}[i]$ with $N(a+bi) = a^2 + b^2 = 3$. We now work our way through several results that eventually yield our Fundamental Theorem of Arithmetic in $\mathbb{Z}[i]$.

**Theorem 7.14. Division Algorithm in $\mathbb{Z}[i]$.**
Let $\alpha, \beta \in \mathbb{Z}[i]$, with $\beta \neq 0$. Then there exist $q, r \in \mathbb{Z}[i]$ such that $\alpha = \beta q + r$, with $0 \leq N(r) < N(\beta)$.

**Example 7.15.** Consider $\alpha = 12 + 8i$ and $\beta = 4 - i$. To illustrate the Division Algorithm in $\mathbb{Z}[i]$, we seek $q$ and $r$ in $\mathbb{Z}[i]$ such that $\alpha = 12+8i = (4-i)q+r = \beta q+r$. First, we express $\alpha/\beta$ in the form $u + vi$:

$$\frac{12+8i}{4-1} = \frac{12+8i}{4-i}\frac{4+i}{4+i} = \frac{40+44i}{17} = \frac{40}{17} + \frac{44}{17}i = u + vi.$$

With $u = 40/17 = 2 + 6/17$ and $v = 44/17 = 2 + 10/17$, we take $x = 2$ and $y = 3$ to get $q = x + yi = 2 + 3i$. For $r$, we know that $\alpha = \beta q + r$ or $r = \alpha - \beta q$ so

$r = (12 + 8i) - (4 - i)(2 + 3i) = (12 + 8i) - (11 + 10i) = 1 - 2i$. Notice that $N(r) = N(1 - 2i) = 5 < 17 = N(4 - i) = N(\beta)$, as needed.

**Note.** We now largely follow the proof of the Fundamental Theorem of Arithmetic in $\mathbb{Z}$ (Theorem 6.29). The condition of "least positive" in the setting of $\mathbb{Z}$ is replaced in $\mathbb{Z}[i]$ with "of minimal norm."

**Definition 7.16.** Let $\alpha, \beta \in \mathbb{Z}[i]$, not both 0. A common divisor $d$ of $\alpha$ and $\beta$ in $\mathbb{Z}[i]$ is a *greatest common divisor* of $\alpha$ and $\beta$ if every common divisor of $\alpha$ and $\beta$ is a divisor of $d$.

**Note.** In the setting of $\mathbb{Z}$ we have an ordering, namely the usual greater-than/less-than of $>$ and $<$, so that "greatest" takes its meaning from the ordering. However, there is no corresponding ordering in $\mathbb{C}$; see my supplemental notes for Complex Analysis 1 (MATH 5510) on Ordering the Complex Numbers. So we cannot use the ordering in $\mathbb{Z}[i]$ to choose *a* greatest common divisor (though we could use the norm $N$). Also, we may not have unique greatest common divisors; for any given greatest common divisor $d$ of two Gaussian integers, unit multiples of $d$ are also greatest common divisors: $d$, $-d$, $di$, and $-di$.

**Theorem 7.17.** If Gaussian integers $\alpha$ and $\beta$ are not both 0, then they have a greatest common divisor $d$, and there are elements $x, y \in \mathbb{Z}[i]$ such that $d = x\alpha + y\beta$.

**Note.** Theorem 7.17 is the $\mathbb{Z}[i]$ version of Theorem 6.20 for $\mathbb{Z}$. However, (strict) uniqueness of a greatest common divisor need not hold in $\mathbb{Z}[i]$, as mentioned above.

**Note.** Notice that if $d$ is a greatest common divisor of $\alpha$ and $\beta$, then so is $\varepsilon d$ for any G-units $\varepsilon$ (recall that in $\mathbb{Z}[i]$ the only G-units are $\pm 1$ and $\pm i$). Greatest common divisors can be computed using the Euclidean Algorithm in $\mathbb{Z}[i]$, just as in $\mathbb{Z}$. For the use of the Euclidean Algorithm in $\mathbb{Z}$, see Note 6.23 in Section 6.3. Divisibility: The Fundamental Theorem of Arithmetic. For the use of the Euclidean Algorithm in the setting of positive integers, see my online notes for Elementary Number Theory (MATH 3120) on Section 1. Integers and notice Theorem 1.3.

**Definition.** Let $\alpha \in \mathbb{Z}[i]$. Then any $\beta = \varepsilon\alpha$ where $\varepsilon$ is a Gauss unit (either $\pm 1$ or $\pm i$) is an *associate* of $\alpha$.

**Note.** Notice that for $\alpha \in \mathbb{Z}[i]$ and $\pi$ a Gauss prime, $\pi \mid \alpha$ if and only if $\alpha = \pi\beta = (\varepsilon\pi)(\varepsilon^{-1})\beta)$ for some $\beta \in \mathbb{Z}[i]$ and for every Gauss unit $\varepsilon$. That is, Gauss prime $\pi$ divides $\alpha$ is and only if every associate of $\pi$ divides $\alpha$. Hence if $\pi \nmid \alpha$ then no associate of $\pi$ divides $\alpha$ do that the greatest common divisor of $\pi$ and $\alpha$ is 1.

**Theorem 7.19.** Let $\pi$ be a Gauss prime, let $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{Z}[i]$, and suppose $\pi \mid \prod_{i=1}^k \alpha_i$. Then $\pi \mid \alpha_i$ for some $i$.

**Theorem 7.20. Fundamental Theorem of Arithmetic in $\mathbb{Z}[i]$**

Every nonzero nonunit Gaussian integer $\alpha$ is a product of $G$-primes. This factorization is unique in the following sense: If $\alpha = \pi_1\pi_2 \cdots \pi_r = \sigma_1\sigma_2 \cdots \sigma_s$ are two factorizations of $\alpha$ into $G$-primes, then $r = s$ and the $\sigma_i$'s are associates of the $\pi_i$'s; more precisely, there is a permutation of the subscripts $1, 2, \ldots, r$ making $\sigma_i$ an associate of $\pi_i$ for $1 \leq i \leq r$.

**Note.** The next theorem gives a way to recognize Gaussian primes in terms of the multiplicative norm and prime integers. Notice that Gerstein now refers to prime integers as "$\mathbb{Z}$-primes."

**Theorem 7.21.** The Gaussian primes are of the following two kinds.

**(a)** Gaussian integers of the form $\alpha = a + bi$ with $ab \neq 0$ such that $N(\alpha)$ is a $\mathbb{Z}$-prime.

**(b)** $\mathbb{Z}$-primes that are not sums of two squares in $\mathbb{Z}$, and their associates in $\mathbb{Z}[i]$.

**Note.** We now shift our attention to the condition given in Theorem 7.21(b). It has become desirable to determine which $\mathbb{Z}$-primes are also Gaussian primes. For example, as shown above in Note 7.2.C, 2 and 5 are $\mathbb{Z}$-primes but are not Gauss primes. In exploring this question, we need the following number theory result.

**Theorem 7.22. Wilson's Theorem.**

If $p$ is a prime number then $(p-1)! \equiv -1 \pmod{p}$.

**Note.** We also see Wilson's Theorem in Elementary Number Theory (MATH 3120). See my online notes for that class on Section 6. Fermat's and Wilson's Theorems and notice Theorem 6.2. As a corollary, we have the following.

**Corollary 7.23.** If $p$ is prime and $p \equiv 1 \pmod{4}$ then the congruence $x^2 \equiv -1 \pmod{p}$ is solvable.

**Note.** We now have the equipment to classify the $\mathbb{Z}$-primes which are also Gaussian primes. The following result also appears in Elementary Number Theory (MATH 3120); see Section 18. Sums of Two Squares and notice Lemma 18.4.

**Theorem 7.24.** An odd prime number $p$ is a Gaussian prime if and only if $p \equiv 3 \pmod{4}$.

**Note.** Notice that most of these results deal with "odd primes," and so omit prime 2 from the conversation. The next corollary is consistent with our previous observation that 5 is not a Gaussian prime.

**Corollary 7.25.** Let $p$ be an odd prime number. Then $p$ is a sum of two squaes in $\mathbb{Z}$ if and only if $p \equiv 1 \pmod{4}$.