Definition. Let α and β be Gaussian integers. A *greatest common divisor* of α and β is a Gaussian integer γ with these two properties:

(i) $\gamma \mid \alpha$ and $\gamma \mid \beta$;

and

(ii) if $\delta \mid \alpha$ and $\delta \mid \beta$, then $\delta \mid \gamma$.

If γ is a greatest common divisor of the Gaussian integers α and β, then it is straightforward to show that all associates of γ are also greatest common divisors of α and β (see Exercise 5). Consequently, if γ is a greatest common divisor of α and β, then $-\gamma$, $i\gamma$, and $-i\gamma$ are also greatest common divisors of α and β. The converse is also true, that is, any two greatest common divisors of two Gaussian integers are associates, as we will prove later in this section. First, we will show that a greatest common divisor exists for every two Gaussian integers.

Theorem 14.3. If α and β are Gaussian integers, not both zero, then

(i) there exists a greatest common divisor γ of α and β;

and

(ii) if γ is a greatest common divisor of α and β, then there exist Gaussian integers μ and ν such that $\gamma = \mu\alpha + \nu\beta$.

Proof Let S be the set of norms of nonzero Gaussian integers of the form

$$\mu\alpha + \nu\beta,$$

where μ and ν are Gaussian integers. Because $\mu\alpha + \nu\beta$ is a Gaussian integer when μ and ν are Gaussian integers and the norm of a nonzero Gaussian integer is a positive integer, every element of S is a positive integer. S is nonempty, which can be seen because $N(1 \cdot \alpha + 0 \cdot \beta) = N(\alpha)$ and $N(0 \cdot \alpha + 1 \cdot \beta) = N(\beta)$ both belong to S and both cannot be 0.

Because S is a nonempty set of positive integers, by the well-ordering property, it contains a least element. Consequently, a Gaussian integer γ exists with

$$\gamma = \mu_0\alpha + \nu_0\beta,$$

where μ_0 and ν_0 are Gaussian integers and $N(\gamma) \leq N(\mu\alpha + \nu\beta)$ for all Gaussian integers μ and ν.

We will show that γ is a greatest common divisor of α and β. First, suppose that $\delta \mid \alpha$ and $\delta \mid \beta$. Then there exist Gaussian integers ρ and σ such that $\alpha = \delta\rho$ and $\beta = \delta\sigma$. It follows that

$$\gamma = \mu_0\alpha + \nu_0\beta = \mu_0\delta\rho + \nu_0\delta\sigma = \delta(\mu_0\rho + \nu_0\sigma).$$

We see that $\delta \mid \gamma$.

To show that $\gamma \mid \alpha$ and $\gamma \mid \beta$ we will show that γ divides every Gaussian integer of the form $\mu\alpha + \nu\beta$. So suppose that $\varepsilon = \mu_1\alpha + \nu_1\beta$ for Gaussian integers μ_1 and ν_1. By

Theorem 14.6, the division algorithm for Gaussian integers, we see that

$$\iota = \gamma\eta + \xi,$$

where η and ξ are Gaussian integers with $0 \le N(\xi) < N(\gamma)$. Furthermore, ξ is a Gaussian integer of the form $\mu\alpha + \nu\beta$. To see this note that

$$\xi = \iota - \gamma\eta = (\mu_1\alpha + \nu_1\beta) - (\mu_0\alpha + \nu_0\beta)\eta = (\mu_1 - \mu_0\eta)\alpha + (\nu_1 - \nu_0\eta)\beta.$$

Recall that γ was chosen as an element with smallest possible norm among the nonzero Gaussian integers of the form $\mu\alpha + \nu\beta$. Consequently, because ξ has this form and $0 \le N(\xi) < N(\gamma)$, we know that $N(\xi) = 0$. By Theorem 14.1, we see that $\xi = 0$. Consequently, $\iota = \gamma\eta$. We conclude that every element Gaussian integer of the form $\mu\alpha + \nu\beta$ is divisible by γ. ∎

We now show that any two greatest common divisors of two Gaussian integers must be associates.

Theorem 14.8. If both γ_1 and γ_2 are greatest common divisors of the Gaussian integers α and β, not both zero, then γ_1 and γ_2 are associates of each other.

Proof Suppose that γ_1 and γ_2 are both greatest common divisors of α and β. By part (ii) of the definition of greatest common divisor, it follows that $\gamma_1 \mid \gamma_2$ and $\gamma_2 \mid \gamma_1$. This means there are Gaussian integers ε and θ such that $\gamma_2 = \varepsilon\gamma_1$ and $\gamma_1 = \theta\gamma_2$. Combining these two equations, we see that

$$\gamma_1 = \theta\varepsilon\gamma_1.$$

Divide both sides by γ_1 (which does not equal 0 because 0 is not a common divisor of two Gaussian integers if they are not both zero) to see that

$$\theta\varepsilon = 1.$$

We conclude that θ and ε are both units. Because $\gamma_1 = \theta\gamma_2$, we see that γ_1 and γ_2 are associates. ∎

The demonstration that the converse of Theorem 14.8 is also true is left as Exercise 5 at the end of this section.

Definition. The Gaussian integers α and β are *relatively prime* if 1 is a greatest common divisor of α and β.

Note that 1 is a greatest common divisor of α and β if and only if the associates of 1, namely -1, i, and $-i$, are also greatest common divisors of α and β. For example, if we know that i is a greatest common divisor of α and β, then these two Gaussian integers are relatively prime.

We can adapt the Euclidean algorithm (Theorem 3.11) to find a greatest common divisor of two Gaussian integers.

Theorem 14.9. ***A Euclidean Algorithm for Gaussian Integers.*** Let $\rho_0 = \alpha$ and $\rho_1 = \beta$ be nonzero Gaussian integers. If the division algorithm for Gaussian integers is

successively applied to obtain $\rho_j = \rho_{j+1}y_{j+1} + r_{j+2}$, with $N(\rho_{j+2}) < N(\rho_{j+1})$ for $j = 0, 1, 2, \ldots, n-2$ and $\rho_{n+1} = 0$, then ρ_n, the last nonzero remainder, is a greatest common divisor of α and β.

We leave the proof of Theorem 14.9 to the reader; it is a straightforward adaption of the proof of Theorem 3.11. Note that we can also work backward through the steps of the Euclidean algorithm for Gaussian integers to express the greatest common divisor found by the algorithm as a linear combination of the two Gaussian integers provided as input to the algorithm. We illustrate this in the following example.

Example 14.9. Suppose that $\alpha = 97 + 210i$ and $\beta = 123 + 16i$. The version of the Euclidean algorithm based on the version of the division algorithm in the proof of Theorem 4.6 can be used to find the greatest common divisors of α and β with the following steps.

$$\begin{aligned}
97 + 210i &= (123 + 16i)(1 + 2i) + (-26 - 52i) \\
123 + 16i &= (-26 - 52i)(-2i) + (39 + 4i) \\
-26 - 52i &= (39 + 4i)(-1 - 3i) + (-6 + 5i) \\
39 + 4i &= (-6 + 5i)(-2 - 2i) + (-3 + 2i) \\
-6 + 5i &= (-3 + 2i)2 + i \\
-3 + 2i &= i(2 + 3i) + 0
\end{aligned}$$

We conclude that i is a greatest common divisor of $97 + 210i$ and $123 + 16i$. Consequently, all greatest common divisors of these two Gaussian integers are the associates of i, namely 1, -1, i, and $-i$. It follows that $97 + 210i$ and $123 + 16i$ are relatively prime.

Because $97 + 210i$ and $123 + 16i$ are relatively prime, we can express 1 as a linear combination of these Gaussian integers. We can find Gaussian integers μ and ν such that $1 = \mu\alpha + \nu\beta$ by working backward through these steps and then multiplying both sides by $-i$ to obtain 1. These computations, which we leave to the reader, show that

$$(97 + 210i)(-2i + 21i) + (123 + 16i)(37 + 12i) = 1. \quad \blacktriangleleft$$

Unique Factorization for Gaussian Integers

The fundamental theorem of arithmetic states that every rational integer has a unique factorization into primes. Its proof depends on the fact that if the rational prime p divides the product of two rational integers ab, then p divides either a or b. We now prove an analogous fact about the Gaussian integers which will play the crucial role in proving unique factorization for the Gaussian integers.