**Definition.** Let $\alpha$ and $\beta$ be Gaussian integers. A *greatest common divisor* of $\alpha$ and $\beta$ is a Gaussian integer $\gamma$ 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 $\gamma$ is a greatest common divisor of the Gaussian integers $\alpha$ and $\beta$, then it is straightforward to show that all associates of $\gamma$ are also greatest common divisors of $\alpha$ and $\beta$ (see Exercise 5). Consequently, if $\gamma$ is a greatest common divisor of $\alpha$ and $\beta$, then $-\gamma$, $i\gamma$, and $-i\gamma$ are also greatest common divisors of $\alpha$ and $\beta$. 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 14.7.** If $\alpha$ and $\beta$ are Gaussian integers, not both zero, then

(i) there exists a greatest common divisor $\gamma$ of $\alpha$ and $\beta$;

and

(ii) if $\gamma$ is a greatest common divisor of $\alpha$ and $\beta$, then there exist Gaussian integers $\mu$ and $\nu$ 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 $\mu$ and $\nu$ are Gaussian integers. Because $\mu\alpha + \nu\beta$ is a Gaussian integer when $\mu$ and $\nu$ 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 $\gamma$ exists with

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

where $\mu_0$ and $\nu_0$ are Gaussian integers and $N(\gamma) \leq N(\mu\alpha + \nu\beta)$ for all Gaussian integers $\mu$ and $\nu$.

We will show that $\gamma$ is a greatest common divisor of $\alpha$ and $\beta$. First, suppose that $\delta \mid \alpha$ and $\delta \mid \beta$. Then there exist Gaussian integers $\rho$ and $\sigma$ 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 $\gamma|\alpha$ and $\gamma|\beta$ we will show that $\gamma$ divides every Gaussian integer of the form $\mu\alpha + \nu\beta$. So suppose that $\tau = \mu_1\alpha + \nu_1\beta$ for Gaussian integers $\mu_1$ and $\nu_1$. By

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

$$\tau = \gamma\eta + \zeta,$$

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

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

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

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

**Theorem 14.8.** If both $\gamma_1$ and $\gamma_2$ are greatest common divisors of the Gaussian integers $\alpha$ and $\beta$, not both zero, then $\gamma_1$ and $\gamma_2$ are associates of each other.

*Proof.* Suppose that $\gamma_1$ and $\gamma_2$ are both greatest common divisors of $\alpha$ and $\beta$. 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 $\epsilon$ and $\theta$ such that $\gamma_2 = \epsilon\gamma_1$ and $\gamma_1 = \theta\gamma_2$. Combining these two equations, we see that

$$\gamma_1 = \theta\epsilon\gamma_1.$$

Divide both sides by $\gamma_1$ (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

$$\theta\epsilon = 1.$$

We conclude that $\theta$ and $\epsilon$ are both units. Because $\gamma_1 = \theta\gamma_2$, we see that $\gamma_1$ and $\gamma_2$ 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 $\alpha$ and $\beta$ are *relatively prime* if 1 is a greatest common divisor of $\alpha$ and $\beta$.

Note that 1 is a greatest common divisor of $\alpha$ and $\beta$ if and only if the associates of 1, namely $-1$, $i$, and $-i$, are also greatest common divisors of $\alpha$ and $\beta$. For example, if we know that $i$ is a greatest common divisor of $\alpha$ and $\beta$, 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