

Furthermore, if d is a gcd of a and b , then there exist λ and μ in D such that $d = \lambda a + \mu b$.

Proof Since $v(r_i) < v(r_{i-1})$ and $v(r_i)$ is a nonnegative integer, it follows that after some finite number of steps we must arrive at some $r_s = 0$.

If $r_1 = 0$, then $a = bq_1$, and b is a gcd of a and b . Suppose $r_1 \neq 0$. Then if $d | a$ and $d | b$, we have

$$d | (a - bq_1),$$

so $d | r_1$. However, if $d_1 | r_1$ and $d_1 | b$, then

$$d_1 | (bq_1 + r_1),$$

so $d_1 | a$. Thus the set of common divisors of a and b is the same set as the set of common divisors of b and r_1 . By a similar argument, if $r_2 \neq 0$, the set of common divisors of b and r_1 is the same set as the set of common divisors of r_1 and r_2 . Continuing this process, we see finally that the set of common divisors of a and b is the same set as the set of common divisors of r_{s-2} and r_{s-1} , where r_s is the first r_i equal to 0. Thus a gcd of r_{s-2} and r_{s-1} is also a gcd of a and b . But the equation

$$r_{s-2} = q_s r_{s-1} + r_s = q_s r_{s-1}$$

shows that a gcd of r_{s-2} and r_{s-1} is r_{s-1} .

It remains to show that we can express a gcd d of a and b as $d = \lambda a + \mu b$. In terms of the construction just given, if $d = b$, then $d = 0a + 1b$ and we are done. If $d = r_{s-1}$, then, working backward through our equations, we can express each r_i in the form $\lambda_i r_{i-1} + \mu_i r_{i-2}$ for some $\lambda_i, \mu_i \in D$. To illustrate using the first step, from the equation

$$r_{s-3} = q_{s-1} r_{s-2} + r_{s-1}$$

we obtain

$$d = r_{s-1} = r_{s-3} - q_{s-1} r_{s-2}. \quad (1)$$

We then express r_{s-2} in terms of r_{s-3} and r_{s-4} and substitute in Eq. (1) to express d in terms of r_{s-3} and r_{s-4} . Eventually, we will have

$$\begin{aligned} d &= \lambda_3 r_2 + \mu_3 r_1 = \lambda_3(b - r_1 q_2) + \mu_3 r_1 = \lambda_3 b + (\mu_3 - \lambda_3 q_2) r_1 \\ &= \lambda_3 b + (\mu_3 - \lambda_3 q_2)(a - bq_1) \end{aligned}$$

which can be expressed in the form $d = \lambda a + \mu b$. If d' is any other gcd of a and b , then $d' = ud$ for some unit u , so $d' = (\lambda u)a + (\mu u)b$. ◆

The nice thing about Theorem 35.9 is that it can be implemented on a computer. Of course, we anticipate that of anything that is labeled an “algorithm.”

35.10 Example Let us illustrate the Euclidean algorithm for the Euclidean norm $||$ on \mathbb{Z} by computing a gcd of 22,471 and 3,266. We just apply the division algorithm over and over again, and the last nonzero remainder is a gcd. We label the numbers obtained as in Theorem 35.9 to further illustrate the statement and proof of the theorem. The computations are easily checked.

	$a = 22,471$
	$b = 3,266$
22,471 = (3,266)6 + 2,875	$r_1 = 2,875$
3,266 = (2,875)1 + 391	$r_2 = 391$
2,875 = (391)7 + 138	$r_3 = 138$
391 = (138)2 + 115	$r_4 = 115$
138 = (115)1 + 23	$r_5 = 23$
115 = (23)5 + 0	$r_6 = 0$

Thus $r_5 = 23$ is a gcd of 22,471 and 3,266. We found a gcd without factoring! This is important, for sometimes it is very difficult to find a factorization of an integer into primes. \blacktriangle

- 35.11 Example** Note that the division algorithm Condition 1 in the definition of a Euclidean norm says nothing about r being “positive.” In computing a gcd in \mathbb{Z} by the Euclidean algorithm for $|r|$, as in Example 35.10, it is surely in our interest to make $|r_i|$ as small as possible in each division. Thus, repeating Example 35.10, it would be more efficient to write

$$\begin{array}{ll} a = 22,471 & \\ b = 3,266 & \\ 22,471 = (3,266)7 - 391 & r_1 = -391 \\ 3,266 = (391)8 + 138 & r_2 = 138 \\ 391 = (138)3 - 23 & r_3 = -23 \\ 138 = (23)6 + 0 & r_4 = 0 \end{array}$$

We can change the sign of r_i from negative to positive when we wish since the divisors of r_i and $-r_i$ are the same. \blacktriangle

■ EXERCISES 35

Computations

In Exercises 1 through 5, state whether the given function v is a Euclidean norm for the given integral domain.

1. The function v for \mathbb{Z} given by $v(n) = n^2$ for nonzero $n \in \mathbb{Z}$
2. The function v for $\mathbb{Z}[x]$ given by $v(f(x)) = (\text{degree of } f(x))$ for $f(x) \in \mathbb{Z}[x], f(x) \neq 0$
3. The function v for $\mathbb{Z}[x]$ given by $v(f(x)) = (\text{the absolute value of the coefficient of the highest degree nonzero term of } f(x))$ for nonzero $f(x) \in \mathbb{Z}[x]$
4. The function v for \mathbb{Q} given by $v(a) = a^2$ for nonzero $a \in \mathbb{Q}$
5. The function v for \mathbb{Q} given by $v(a) = 50$ for nonzero $a \in \mathbb{Q}$
6. By referring to Example 35.11, actually express the gcd 23 in the form $\lambda(22,471) + \mu(3,266)$ for $\lambda, \mu \in \mathbb{Z}$. [Hint: From the next-to-last line of the computation in Example 35.11, $23 = (138)3 - 391$. From the line before that, $138 = 3,266 - (391)8$, so substituting, you get $23 = [3,266 - (391)8]3 - 391$, and so on. That is, work your way back up to actually find values for λ and μ .]
7. Find a gcd of 49,349 and 15,555 in \mathbb{Z} .
8. Following the idea of Exercise 6 and referring to Exercise 7, express the positive gcd of 49,349 and 15,555 in \mathbb{Z} in the form $\lambda(49,349) + \mu(15,555)$ for $\lambda, \mu \in \mathbb{Z}$.
9. Find a gcd of

$$x^{10} - 3x^9 + 3x^8 - 11x^7 + 11x^6 - 11x^5 + 19x^4 - 13x^3 + 8x^2 - 9x + 3$$

and

$$x^6 - 3x^5 + 3x^4 - 9x^3 + 5x^2 - 5x + 2$$

in $\mathbb{Q}[x]$.

10. Describe how the Euclidean Algorithm can be used to find the gcd of n members a_1, a_2, \dots, a_n of a Euclidean domain.
11. Using your method devised in Exercise 10, find the gcd of 2178, 396, 792, and 726.

Concepts

12. Let us consider $\mathbb{Z}[x]$.

- a. Is $\mathbb{Z}[x]$ a UFD? Why?
- b. Show that $\{a + xf(x) \mid a \in 2\mathbb{Z}, f(x) \in \mathbb{Z}[x]\}$ is an ideal in $\mathbb{Z}[x]$.
- c. Is $\mathbb{Z}[x]$ a PID? (Consider part (b).)
- d. Is $\mathbb{Z}[x]$ a Euclidean domain? Why?
13. Determine whether each of the following is true or false.
- Every Euclidean domain is a PID.
 - Every PID is a Euclidean domain.
 - Every Euclidean domain is a UFD.
 - Every UFD is a Euclidean domain.
 - A gcd of 2 and 3 in \mathbb{Q} is $\frac{1}{2}$.
 - The Euclidean algorithm gives a constructive method for finding a gcd of two integers.
 - If v is a Euclidean norm on a Euclidean domain D , then $v(1) \leq v(a)$ for all nonzero $a \in D$.
 - If v is a Euclidean norm on a Euclidean domain D , then $v(1) < v(a)$ for all nonzero $a \in D, a \neq 1$.
 - If v is a Euclidean norm on a Euclidean domain D , then $v(1) < v(a)$ for all nonzero nonunits $a \in D$.
 - For any field F , $F[x]$ is a Euclidean domain.
14. Does the choice of a particular Euclidean norm v on a Euclidean domain D influence the arithmetic structure of D in any way? Explain.

Theory

15. Let D be a Euclidean domain and let v be a Euclidean norm on D . Show that if a and b are associates in D , then $v(a) = v(b)$.
16. Let D be a Euclidean domain and let v be a Euclidean norm on D . Show that for nonzero $a, b \in D$, one has $v(a) < v(ab)$ if and only if b is not a unit of D . [Hint: Argue from Exercise 15 that $v(a) < v(ab)$ implies that b is not a unit of D . Using the Euclidean algorithm, show that $v(a) = v(ab)$ implies $\langle a \rangle = \langle ab \rangle$. Conclude that if b is not a unit, then $v(a) < v(ab)$.]
17. Prove or disprove the following statement: If v is a Euclidean norm on Euclidean domain D , then $\{a \in D \mid v(a) > v(1)\} \cup \{0\}$ is an ideal of D .
18. Show that every field is a Euclidean domain.
19. Let v be a Euclidean norm on a Euclidean domain D .
- Show that if $s \in \mathbb{Z}$ such that $s + v(1) > 0$, then $\eta : D^* \rightarrow \mathbb{Z}$ defined by $\eta(a) = v(a) + s$ for nonzero $a \in D$ is a Euclidean norm on D . As usual, D^* is the set of nonzero elements of D .
 - Show that for $t \in \mathbb{Z}^+$, $\lambda : D^* \rightarrow \mathbb{Z}$ given by $\lambda(a) = t \cdot v(a)$ for nonzero $a \in D$ is a Euclidean norm on D .
 - Show that there exists a Euclidean norm μ on D such that $\mu(1) = 1$ and $\mu(a) > 100$ for all nonzero nonunits $a \in D$.
20. Let D be a UFD. An element c in D is a **least common multiple** (abbreviated lcm) of two elements a and b in D if $a \mid c, b \mid c$ and if c divides every element of D that is divisible by both a and b . Show that every two nonzero elements a and b of a Euclidean domain D have an lcm in D . [Hint: Show that all common multiples, in the obvious sense, of both a and b form an ideal of D .]
21. Use the last statement in Theorem 35.9 to show that two nonzero elements $r, s \in \mathbb{Z}$ generate the group $(\mathbb{Z}, +)$ if and only if r and s , viewed as integers in the domain \mathbb{Z} , are **relatively prime**, that is, have a gcd of 1.
22. Using the last statement in Theorem 35.9, show that for nonzero $a, b, n \in \mathbb{Z}$, the congruence $ax \equiv b \pmod{n}$ has a solution in \mathbb{Z} if a and n are relatively prime.
23. Generalize Exercise 22 by showing that for nonzero $a, b, n \in \mathbb{Z}$, the congruence $ax \equiv b \pmod{n}$ has a solution in \mathbb{Z} if and only if the positive gcd of a and n in \mathbb{Z} divides b . Interpret this result in the ring \mathbb{Z}_n .
24. Following the idea of Exercises 6 and 23, outline a constructive method for finding a solution in \mathbb{Z} of the congruence $ax \equiv b \pmod{n}$ for nonzero $a, b, n \in \mathbb{Z}$, if the congruence does have a solution. Use this method to find a solution of the congruence $22x \equiv 18 \pmod{42}$.

SECTION 36**NUMBER THEORY**

In this section we will show how the ideas in Section 35 can be used to derive some interesting results in number theory. We usually think of number theory as a study of properties of the integers, but Gauss expanded the study of numbers to include what is now called the Gaussian integers. The Gaussian integers form a subring of the complex numbers that, like the integers, form a Euclidean domain, but not a field. After studying the Gaussian integers, we will prove that for any prime number $p \in \mathbb{Z}^+$ that is equivalent to 1 modulo 4, p can be written as the sum of two squares.

Gaussian Integers

36.1 Definition A **Gaussian integer** is a complex number $a + bi$, where $a, b \in \mathbb{Z}$. For a Gaussian integer $\alpha = a + bi$, the **norm** $N(\alpha)$ of α is $a^2 + b^2$. ■

Although we defined $N(\alpha)$ for a Gaussian integer α , we can also think of N as defined on any complex number using the same formula $N(a + bi) = a^2 + b^2$. This norm can also be written as $N(\alpha) = |\alpha|^2$.

We shall let $\mathbb{Z}[i]$ be the set of all Gaussian integers. The following lemma gives some basic properties of the norm function N on $\mathbb{Z}[i]$ and leads to a demonstration that the function v defined by $v(\alpha) = N(\alpha)$ for nonzero $\alpha \in \mathbb{Z}[i]$ is a Euclidean norm on $\mathbb{Z}[i]$. Note that the Gaussian integers include all the **rational integers**, that is, all the elements of \mathbb{Z} .

HISTORICAL NOTE

In his *Disquisitiones Arithmeticae*, Gauss studied in detail the theory of quadratic residues, that is, the theory of solutions to the congruence $x^2 \equiv p \pmod{q}$ and proved the famous quadratic reciprocity theorem showing the relationship between the solutions of the congruences $x^2 \equiv p \pmod{q}$ and $x^2 \equiv q \pmod{p}$ where p and q are primes. In attempting to generalize his results to theories of quartic residues, however, Gauss realized that it was much more natural to consider the Gaussian integers rather than the ordinary integers.

Gauss's investigations of the Gaussian integers are contained in a long paper published in 1832 in which he proved various analogies between them and the ordinary integers. For example, after noting that there are four units (invertible elements)

among the Gaussian integers, namely $1, -1, i$, and $-i$, and defining the norm as in Definition 36.1, he generalized the notion of a prime integer by defining a prime Gaussian integer to be one that cannot be expressed as the product of two other integers, neither of them units. He was then able to determine which Gaussian integers are prime: A Gaussian integer that is not real is prime if and only if its norm is a real prime, which can only be 2 or of the form $4n + 1$. The real prime $2 = (1+i)(1-i)$ and real primes congruent to 1 modulo 4 like $13 = (2+3i)(2-3i)$ factor as the product of two Gaussian primes. Real primes of the form $4n + 3$ like 7 and 11 are still prime in the domain of Gaussian integers. See Exercise 10.

36.2 Lemma In $\mathbb{Z}[i]$, the following properties of the norm function N hold for all $\alpha, \beta \in \mathbb{Z}[i]$:

1. $N(\alpha) \geq 0$.
2. $N(\alpha) = 0$ if and only if $\alpha = 0$.
3. $N(\alpha\beta) = N(\alpha)N(\beta)$.

Proof If we let $\alpha = a_1 + a_2i$ and $\beta = b_1 + b_2i$, these results are all straightforward computations. We leave the proof of these properties as an exercise (see Exercise 11). ♦

The proof of Lemma 36.2 does not depend on the complex numbers α and β being Gaussian integers. In fact the three properties listed in the lemma are true for all complex numbers.

36.3 Lemma $\mathbb{Z}[i]$ is an integral domain.

Proof It is obvious that $\mathbb{Z}[i]$ is a commutative ring with unity. We show that there are no divisors of 0. Let $\alpha, \beta \in \mathbb{Z}[i]$. Using Lemma 36.2, if $\alpha\beta = 0$ then

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(0) = 0.$$

Thus $\alpha\beta = 0$ implies that $N(\alpha) = 0$ or $N(\beta) = 0$. By Lemma 36.2 again, this implies that either $\alpha = 0$ or $\beta = 0$. Thus $\mathbb{Z}[i]$ has no divisors of 0, so $\mathbb{Z}[i]$ is an integral domain. \blacklozenge

Of course, since $\mathbb{Z}[i]$ is a subring of \mathbb{C} , where \mathbb{C} is the field of complex numbers, it is really obvious that $\mathbb{Z}[i]$ has no 0 divisors. We gave the argument of Lemma 36.3 to illustrate the use of the multiplicative property 3 of the norm function N and to avoid going outside of $\mathbb{Z}[i]$ in our argument.

However, in the proof of Theorem 36.4, we will use property 3 for complex numbers that are not Gaussian integers and therefore we will stay outside the Gaussian integers.

36.4 Theorem The function v given by $v(\alpha) = N(\alpha)$ for nonzero $\alpha \in \mathbb{Z}[i]$ is a Euclidean norm on $\mathbb{Z}[i]$. Thus $\mathbb{Z}[i]$ is a Euclidean domain.

Proof Note that for $\beta = b_1 + b_2i \neq 0$, $N(b_1 + b_2i) = b_1^2 + b_2^2$, so $N(\beta) \geq 1$. Then for all $\alpha, \beta \neq 0$ in $\mathbb{Z}[i]$, $N(\alpha) \leq N(\alpha)N(\beta) = N(\alpha\beta)$. This proves Condition 2 for a Euclidean norm in Definition 35.1.

It remains to prove the division algorithm, Condition 1, for N . Let $\alpha, \beta \in \mathbb{Z}[i]$, with $\alpha = a_1 + a_2i$ and $\beta = b_1 + b_2i$, where $\beta \neq 0$. We must find σ and ρ in $\mathbb{Z}[i]$ such that $\alpha = \beta\sigma + \rho$, where either $\rho = 0$ or $N(\rho) < N(\beta) = b_1^2 + b_2^2$. Let $\alpha/\beta = r + si$ for $r, s \in \mathbb{Q}$. Let q_1 and q_2 be integers in \mathbb{Z} as close as possible to the rational numbers r and s , respectively. Let $\sigma = q_1 + q_2i$ and $\rho = \alpha - \beta\sigma$. If $\rho = 0$, we are done. Otherwise, by construction of σ , we see that $|r - q_1| \leq \frac{1}{2}$ and $|s - q_2| \leq \frac{1}{2}$. Therefore

$$\begin{aligned} N\left(\frac{\alpha}{\beta} - \sigma\right) &= N((r + si) - (q_1 + q_2i)) \\ &= N((r - q_1) + (s - q_2)i) \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}. \end{aligned}$$

Thus we obtain

$$N(\rho) = N(\alpha - \beta\sigma) = N\left(\beta\left(\frac{\alpha}{\beta} - \sigma\right)\right) = N(\beta)N\left(\frac{\alpha}{\beta} - \sigma\right) \leq N(\beta)\frac{1}{2},$$

so we do indeed have $N(\rho) < N(\beta)$ as desired. \blacklozenge

36.5 Example We can now apply all our results of Section 35 to $\mathbb{Z}[i]$. In particular, since $N(1) = 1$, the units of $\mathbb{Z}[i]$ are exactly the $\alpha = a_1 + a_2i$ with $N(\alpha) = a_1^2 + a_2^2 = 1$. From the fact that a_1 and a_2 are integers, it follows that the only possibilities are $a_1 = \pm 1$ with $a_2 = 0$, or $a_1 = 0$ with $a_2 = \pm 1$. Thus the units of $\mathbb{Z}[i]$ are ± 1 and $\pm i$. One can also use the Euclidean Algorithm to compute a gcd of two nonzero elements. We leave such computations to the exercises. Finally, note that while 5 is an irreducible in \mathbb{Z} , 5 is no longer an irreducible in $\mathbb{Z}[i]$, for $5 = (1 + 2i)(1 - 2i)$, and neither $1 + 2i$ nor $1 - 2i$ is a unit. \blacktriangle