We review the structure of the integers; see Section 1.3, "Euclid," and the part of Section 2.1 subtitled "Unique Factorization."

1. Basic Properties and Notation

The set of **integers**, denoted $\mathbb{Z}$, is

$$\mathbb{Z} \;=\; \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}\,.$$

The subset of integers called **natural numbers** is defined differently in different texts; in our text the set of natural numbers includes zero:

$$\mathbb{N} \;=\; \{0, 1, 2, 3, \ldots\}\,.$$

Domain Structure. We take for granted that the integers, with addition and multiplication, have all the properties of a commutative ring, as well as the domain property: if integers a, b, and c satisfy $ab = ac$ and if $a \neq 0$, then $b = c$.

Order and Size. We take the concepts of order (less than, greater than) and size (absolute value) of integers for granted.

Well Ordering Axiom. We take the following property as an axiom: every nonempty set of natural numbers has a least element. This is also called the **Least Integer Axiom**. See page 21.

2. Divisibility and Primes

Divisibility. Given integers a and b, to say that a **divides** b (written $a|b$) means that there exists an integer c such that $b = ac$. Equivalently, we say that a is a **divisor** (or **factor**) of b and b is a **multiple** of a.

Note that every integer a satisfies $a|0$, and if an integer a satisfies $0|a$, then $a = 0$.

Also, note that if two integers divide each other, they are the same (up to multiplication by ±1). More precisely: given integers a and b, if $a|b$ and $b|a$, then $a = \pm b$; if, in addition, both integers are positive, they are equal. See Exercise 1.44, page 29.

One simple, but useful, fact about divisibility is the "two out of three" rule.

Two Out of Three. Given integers a, b, c, and m with $a + b = c$, if m divides any two of a, b, c, then m divides the third: if m divides a and b, then m divides c; if m divides a and c, then m divides b; and if m divides b and c, then m divides a; see Exercise 1.46, page 29.

Linear Combinations. A linear combination of integers a and b is an integer of the form $sa + tb$, where s and t are integers.

A simple consequence of the two-out-of-three rule is that if an integer m divides two integers, a and b, then m divides every linear combination of a and b.

The following result is a useful connection between divisibility and size, in the integers:

Lemma 1.13. Given positive integers a and b, if $a|b$, then $a \leq b$.

Note that the concepts of divisibility and linear combinations extend to the setting of an abstract commutative ring, and the corresponding generalization of the two-out-of-three rule holds in that setting; the concepts of order and size however, do not have analogues in every commutative ring.

Primes. To say that an integer $p \geq 2$ is **prime** means that the only divisors of p are ± 1 and $\pm p$.

Note. This property does generalize in the setting of an abstract domain; however, in that setting such an element is called "irreducible," not prime. The idea is that such an element cannot be broken down or "reduced" into factors except in trivial ways. (A familiar example would be irreducible quadratics, like $x^2 + 1$, which cannot be factored into linear factors.)

Factorization into Primes. Every integer $a \geq 2$ is a product* of primes. (*We consider a single prime to be a "product" of one prime.) Moreover, every integer a with $a \neq 0$, $a \neq \pm 1$ can be written in the form: $a = (\pm 1) \cdot p_1 \dots p_n$, where n is an integer with$n \geq 1$ and $p_1, \dots, p_n$ are primes (not necessarily distinct). See Proposition 1.14, page 22.

3. Remainders and the Division Algorithm

Given integers a and b with a *not necessarily* dividing b, we may consider the "remainder," which, if nonzero, indicates that a does *not* divide b.

Division Algorithm. Given integers a and b with $a \neq 0$, there exist unique integers q and r (called the quotient and remainder, respectively) such that $b = qa + r$ and $0 \leq r < |a|$. (See Theorem 1.15, page 23, and Exercise 1.41, page 29.)

Note. Notice that the Division Algorithm relies critically on the notion of size in the integers. Because of this, the Division Algorithm does *not* generalize to the setting of an abstract domain; domains which do have a suitable notion of size and for which a suitable generalization of the Division Algorithm do hold are called Euclidean domains; see page 333. As it turns out, the Gaussian and Eisenstein Integers, $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$, are both Euclidean domains.

4. GCDs, Linear Combinations, Euclid's Lemma

GCD. A **common divisor** of two integers, a and b, is an integer that divides both a and b; a greatest common divisor is a common divisor that is greater than or equal to all other common divisors. More explicitly, a **greatest common divisor (gcd)** of a and b is an integer d with the properties that (i) $d|a$ and $d|b$ and (ii) if there is an integer c with $c|a$ and $c|b$, then $d \geq c$.

Lemma 1.17. Given a prime p and an integer b, if $p|b$, then $\gcd(p, b) = p$; otherwise $\gcd(p, b) = 1$.

GCD as Linear Combination. Given two integers a and b, their gcd is a linear combination of a and b; if at least one of a and b is nonzero, their gcd is the smallest positive linear combination of a and b. (See Theorem 1.19 and its proof.)

Note. The proof of Theorem 1.19 is worth studying. It uses the Well Ordering Axiom, the Division Algorithm, and the "two out of three" rule. Moreover, ideas in this proof can be used to prove some interesting related results (Exercises 1.48 and 1.49), which can be rephrased using a concept called an "ideal," which we will discuss in Section 5.3.

Theorem 1.19 also allows us to reformulate the definitions of gcd and prime.

Corollary 1.20 (page 25) assures us that the second condition in the definition of gcd may be replaced with the following equivalent condition: (ii$'$) if there is an integer c such that $c|a$ and $c|b$, then $c|d$. This allows generalization of the notion of gcd to an abstract commutative ring which may not have a notion of size. However, the fact that we may define gcds in an abstract setting does not guarantee existence or uniqueness of gcds.

In the integers, the existence and uniqueness of gcds can be proven using the notion of size in $\mathbb{Z}$.

Theorem 1.21 (**Euclid's Lemma**, page 25-26) gives an alternate way of defining prime integers. An integer $p \geq 2$ is prime if and only if it has this property: if p divides a product ab, where a and b are integers, then p necessarily divides one of the factors, a or b.

Note. Both the original criterion for being prime and this criterion generalize in the setting of an abstract domain; however the two properties are not always equivalent. As mentioned above, in the abstract setting, a domain element with the appropriate analogue of the first property is called "irreducible." A domain element with the appropriate analogue of the second property is called "prime." In an abstract domain, a prime element is always irreducible, but an irreducible element is not always prime.

Note. Euclid's Lemma holds in an abstract Euclidean Domain; the arguments in the proofs of Exercise 1.49 and Theorem 1.21 generalize to prove this.

5. Euclidean Algorithm

GCDs in the integers can be computed efficiently, using a repeated application of the Division Algorithm; the last nonzero remainder in the process is the gcd. See pages 30-32. Moreover, running this algorithm "backwards" allows us to write the gcd as an explicit linear combination. See pages 32-33.

6. Unique Prime Factorization

Roughly speaking, the Fundamental Theorem of Arithmetic says that every integer besides zero and one can be written as (± 1 times) a product of primes in essentially one way. A more formal statement follows.

Fundamental Theorem of Arithmetic. Given an integer a with $a \neq 0$, $a \neq \pm 1$, there is an integer $n \geq 1$ and there are primes $p_1, \dots, p_n$ (not necessarily distinct) such that $a = (\pm 1) \cdot p_1 \dots p_n$. Moreover this factorization is unique in the following sense. Let u be the factor of ± 1 in the given factorization. If a has another factorization $a = w \cdot q_1 \dots q_m$, where $w = \pm 1$, $m \geq 1$, and $q_1, \dots, q_m$ are primes, then in fact $w = u$, $m = n$, and, after re-indexing if necessary, $q_i = p_i$ for all $1 \leq i \leq n$. (See Theorem 2.10, page 54.)

Note that we have already proven the existence of such a factorization. The proof of uniqueness uses Euclid's Lemma and the Principal of Mathematical Induction. Thus we will be able to prove uniqueness of "prime factorization" in any abstract domain in which a suitable generalization Euclid's Lemma holds (for example, any Euclidean Domain).

7. Looking Ahead: Polynomial Rings

In Section 5.2, we will show that the set of all polynomials with coefficients in a given field is a domain; in fact, it is a Euclidean domain. In Chapter 6, we will develop a theory for such polynomial rings parallel to that of the integers. In particular, we develop analogues of

- the size of an integer (analogue is degree of polynomial),
- prime number (irreducible polynomial),
- multiplication by factor of ± 1 (multiplication by a nonzero constant), and
- positive integer (polynomial with leading coefficient of 1).

And we prove analogues of:

- Lemma 1.13, the connection between divisibility and size (Lemma 6.1),
- Proposition 1.4, factorization of integers into primes (Proposition 6.8 and Corollary 6.9),
- Theorem 1.15, the Division Algorithm (Theorem 6.11),
- Theorem 1.21, Euclid's Lemma (Theorem 6.31),
- Theorems 1.29 and 1.30, Euclidean Algorithm I and II (Theorems 6.34 and 6.38), and
- Theorem 2.10, the Fundamental Theorem of Arithmetic (Theorem 6.40).

Moreover, we will discuss the connection between gcds and linear combinations, and draw connections to the ideal theoretic perspective.