

Divisibility, Division with Remainder, and Modular Arithmetic

Chapter 2 built $\mathbb{Z}$ out of pairs of natural numbers and proved it an ordered ring, but it said nothing about which integers divide which. *Sets, Relations, and Cardinality*, Section 2.2 did, for the school integers: it proved division with remainder, showed that every integer from 2 on has a prime factor, and set the uniqueness of prime factorization aside as a fact it neither proved nor used. This chapter proves that arithmetic again for the constructed $\mathbb{Z}$, and goes further, using the ordered-ring axioms and two properties of the order of $\mathbb{Z}$: there is no integer strictly between 0 and 1 (Theorem 2.3.4 (c)), and a non-empty set of integers with a lower bound has a least element (Proposition 2.3.6); the field $\mathbb{Q}$ enters chiefly for the integer part $\lfloor a/n \rfloor$ and for lowest terms. The second property gives division with remainder at once. Then one move does most of the work. In a set of integers closed under sums and under multiplication by any integer, the **least positive element** divides every element, and dividing by it with remainder is how one sees this. Applied to the combinations $ax + by$, it makes the greatest common divisor a combination of a and b (Bézout's theorem), and the Euclidean algorithm computes it. Multiplying that combination by a third integer gives Euclid's lemma, that a prime dividing a product divides one of the factors, and with it the uniqueness of prime factorization and the lowest terms of a rational number.

The second half returns to the clock of *Sets, Relations, and Cardinality*, Section 2.5. There, and again for $\mathbb{Z}$ and $\mathbb{Q}$ in Chapter 2, each sum and product of classes was checked separately to be well defined. Section 3.4 makes the check once, for the quotient of any commutative ring by an ideal, and $\mathbb{Z}/n\mathbb{Z}$ becomes a commutative ring with n elements on which, for $n \geq 2$, no order fits. In it the classes that can be divided by are exactly the classes of the integers coprime to n . So $\mathbb{Z}/p\mathbb{Z}$ is a field with p elements for every prime p , and two congruences with coprime moduli have exactly one class of solutions modulo the product of the moduli, the Chinese remainder theorem. Chapter 5 builds $\mathbb{R}$ in the same shape, as classes of rational Cauchy sequences whose difference is null (the null sequences play the part of the ideal), though it checks its operations directly; *Algebraic Preliminaries*, Chapter 5 runs division with remainder, gcd and unique factorization again for polynomials over a field.

Two integers, one theory. *Sets, Relations, and Cardinality*, Chapter 2 proved its facts about divisibility for the school integers, from school facts such as the closure of $\mathbb{Z}$ under $+$, $-$ and $\cdot$ (*Sets, Relations, and Cardinality*, Proposition 2.1.2). This chapter keeps their definitions of divisibility, prime and congruence (*Sets, Relations, and Cardinality*, Definition 2.2.1, *Sets, Relations, and Cardinality*, Definition 2.2.2, *Sets, Relations, and Cardinality*, Definition 2.5.5), read word for word on the ring of Chapter 2, and proves the results again; no proof in it cites a result of *Sets, Relations, and Cardinality* about integers. Each such result has a twin here, named in the section that proves it: division with remainder (*Sets, Relations, and Cardinality*, Theorem 2.2.3) and the antisymmetry of divisibility on $\mathbb{N}$ (*Sets, Relations, and Cardinality*, Proposition 2.4.1) in Section 3.1; a prime factor of every $n \geq 2$ (*Sets, Relations, and Cardinality*, Theorem 2.2.5) and lowest terms (*Sets, Relations, and Cardinality*, Lemma 2.2.4) in Section 3.3; and the arithmetic of congruence classes (*Sets, Relations, and Cardinality*, Proposition 2.5.5) in Section 3.4. Nothing earlier was circular: the earlier chapters used these facts about the school integers as stated facts, and this chapter proves them for the constructed ones.

What you need. Chapters 1 and 2, chiefly Section 2.3, and *Sets, Relations, and Cardinality*,

Chapters 1–3, chiefly Sections 2.2 and 2.5. From Chapter 2: the commutative ring $\mathbb{Z}$ and its algebra (Definition 2.3.1, Theorem 2.3.1, Proposition 2.3.2), its order, its positive elements, the rules for inequalities and discreteness (Proposition 2.3.3, Proposition 2.3.5, Theorem 2.3.4), the least element of a set of integers bounded below (Proposition 2.3.6), the copy of $\mathbb{N}$ inside $\mathbb{Z}$ (Proposition 2.2.3), the lemma that a rule on classes is a function when equivalent inputs give equivalent outputs (Theorem 2.2.1), the two-element field that cannot be ordered (Example (A field with two elements that cannot be ordered)), and the field $\mathbb{Q}$ with $\mathbb{Z}$ inside it, its order, reciprocals and integer part (Definition 2.4.2, Theorem 2.4.3, Proposition 2.4.4, Theorem 2.5.1, Proposition 2.5.2, Proposition 2.5.5). From Chapter 1, the citing rule of Section 1.7 (Corollary 1.7.3), by which induction (Logic and Proof, Axiom 4.2.1) and the recursion theorem (Sets, Relations, and Cardinality, Theorem 2.3.1, Theorem 1.5.1) apply to $\mathbb{N}$; and powers and parity on $\mathbb{N}$ (Proposition 1.6.4), compared with in Section 3.1 and used in review exercise R2. From *Sets, Relations, and Cardinality*, Section 2.2, the definitions of divisibility and prime (Sets, Relations, and Cardinality, Definition 2.2.1, Sets, Relations, and Cardinality, Definition 2.2.2); from its Section 2.3, finite products (Sets, Relations, and Cardinality, Definition 2.3.1), used in Section 3.3 as a pattern for products of lists; from its Section 2.5, equivalence relations, classes and quotient sets (Sets, Relations, and Cardinality, Definition 2.5.1, Sets, Relations, and Cardinality, Definition 2.5.4, Sets, Relations, and Cardinality, Theorem 2.5.1) and congruence (Sets, Relations, and Cardinality, Definition 2.5.5); from its Section 2.6, suprema and the divisibility order (Sets, Relations, and Cardinality, Definition 2.6.5, Sets, Relations, and Cardinality, Example (The supremum under divisibility is the least common multiple)), in a remark of Section 3.2 and in Section 3.3's B2. From *Sets, Relations, and Cardinality*, Chapter 1: products, equality of functions and bijections (Sets, Relations, and Cardinality, Definition 1.3.2, Sets, Relations, and Cardinality, Proposition 1.4.1, Sets, Relations, and Cardinality, Definition 1.4.5); and from its Section 3.1, finite sets and equinumerous sets (Sets, Relations, and Cardinality, Definition 3.1.2, Sets, Relations, and Cardinality, Proposition 3.1.1), to count $\mathbb{Z}/n\mathbb{Z}$, with more on finite sets (Sets, Relations, and Cardinality, Proposition 3.1.6, Sets, Relations, and Cardinality, Corollary 3.1.4, Sets, Relations, and Cardinality, Theorem 3.1.9, Sets, Relations, and Cardinality, Exercise (C2: Counting products and functions), Sets, Relations, and Cardinality, Corollary 3.1.3) in Section 3.5's B3 and C2. From *Logic and Proof*, Chapter 8, the catalogue of what a proof may not do (Logic and Proof, Example (What is not allowed)), for Section 3.3's B1 and C2 and Section 3.5's C2. A few results are compared with and not used: the twins listed above; the even square of *Logic and Proof*, Section 2.1 (Logic and Proof, Theorem 2.1.3) in Section 3.1; Euclid's argument in *Logic and Proof*, Section 8.1's C1 (Logic and Proof, Exercise (C1: Euclid without the contradiction)) in Section 3.3's C3; a rule on classes that is not a function (Sets, Relations, and Cardinality, Example (A rule on classes that is not a function)) in Section 3.4's C1; lowest terms in *Sets, Relations, and Cardinality*, Section 2.2's C2 (Sets, Relations, and Cardinality, Exercise (C2: Lowest terms)) in Section 3.3; and, in the review exercises, the countable product of *Sets, Relations, and Cardinality*, Section 3.2 (Sets, Relations, and Cardinality, Exercise (B2: Putting a proof in order), Sets, Relations, and Cardinality, Theorem 3.2.6) in R2, the two proofs that $\sqrt{2}$ is not rational (Logic and Proof, Theorem 2.2.1, Theorem 2.6.1) in R3. Review exercise R1 also returns to the integers as classes of pairs (Definition 2.1.1).

Time. About 25 hours on the core track (all of A, one B and one C per section, the exit checks); about 30 hours for everything.

3.-1.1 Roadmap

- **Divisibility and Division with Remainder.** Divisibility and primes read on the constructed $\mathbb{Z}$, the rules for divisibility proved from the ring and its order, division with a unique quotient and remainder from a least element, the quotient as the integer part $\lfloor a/n \rfloor$, even and odd integers, and the small-primes remark that 2, 3, 5 and 7 are prime.

- **The Greatest Common Divisor, Bézout, and the Euclidean Algorithm.** The combinations $a\mathbb{Z} + b\mathbb{Z}$ and the multiples $n\mathbb{Z}$, the greatest common divisor with $\gcd(0, 0) := 0$, Bézout's theorem (the least positive combination is the gcd, and every combination is a multiple of it), coprime integers, and the Euclidean algorithm as a recursion that keeps the set of combinations fixed, with back-substitution for the coefficients.
- **Euclid's Lemma and the Fundamental Theorem of Arithmetic.** Euclid's lemma from the Bézout identity, a prime dividing a product of primes equal to one of them, coprime divisors, the least divisor above 1 as a prime, existence and uniqueness of non-decreasing prime factorizations by comparing the largest primes, a monoid in which factorization is not unique, and lowest terms in $\mathbb{Q}$.
- **Ideals, Quotient Rings, and the Integers Modulo n .** Ideals as the subsets that a quotient needs, the quotient ring R/I of a commutative ring by an ideal, the failure for $\mathbb{Z} \subseteq \mathbb{Q}$, the ideals of $\mathbb{Z}$ as the sets $n\mathbb{Z}$, and $\mathbb{Z}/n\mathbb{Z}$ as a commutative ring with n elements that no order fits when $n \geq 2$.
- **Units, Prime Moduli, and the Chinese Remainder Theorem.** Units of a commutative ring, the units of $\mathbb{Z}/n\mathbb{Z}$ as the classes coprime to n with inverses from back-substitution, $\mathbb{Z}/n\mathbb{Z}$ a field exactly when n is prime, and the Chinese remainder theorem for two coprime moduli, with the failures when the moduli share a factor; the review exercises reach back to Chapters 1 and 2, *Logic and Proof*, Chapter 2, and *Sets, Relations, and Cardinality*, Chapter 3.

3.-1.2 Named moves

- **Least positive element, then divide.** Take the least positive element d of a set of integers closed under integer combinations; divide any element of the set by d ; the remainder lies in the set and is smaller than d , so it is 0. This proves Bézout's theorem in Section 3.2 and the description of the ideals of $\mathbb{Z}$ in Section 3.4, and Section 3.3's B2 and Section 3.4's C2 use it for common multiples and for sets closed under subtraction.
- **Multiply the Bézout identity.** From $1 = ax + by$, multiply by c : $c = acx + bcy$, and read off what divides c . It turns a statement about common divisors into an equation, and it gives Euclid's lemma in Section 3.3; in Section 3.5 the same identity, read modulo n , gives inverses, and read modulo m and modulo n at once, the Chinese remainder theorem.
- **Compute on representatives; the ideal absorbs the change.** An operation on classes $a + I$ is well defined because a change of representative is an element of I , and multiplying it by the other argument keeps it in I . This is Chapter 2's check one argument at a time, now made once for every commutative ring and every ideal.