

3.1 Divisibility and Division with Remainder

Chapter 2 built $\mathbb{Z}$ as an ordered commutative ring, and a Quick check in Section 2.3 showed that it is not a field: $2x = 1$ has no solution in $\mathbb{Z}$. So “ a/b ” is not available among the integers. What remains is a relation, “ b is a multiple of a ”, and the next best thing to division: dividing with a quotient and a remainder. *Sets, Relations, and Cardinality*, Section 2.2 defined the relation and proved division with remainder for the school integers. This section does both again for the integers of Chapter 2, where every step must come from the ordered-ring axioms and from the least-element property of $\mathbb{Z}$.

Throughout, $\mathbb{Z}$ is the ordered ring of Theorem 2.3.4, with $\mathbb{N} \subseteq \mathbb{Z}$ and $\mathbb{Z}_{>0} = \{n \in \mathbb{Z} : n > 0\}$ (Theorem 2.3.4 (b)), and $a - b := a + (-b)$. Numerals $2 := 1 + 1$, $3 := 2 + 1$, and so on, are the natural numbers of those names, as in Section 2.6; a sum or product of numerals may be computed in $\mathbb{N}$, because the embedding of Proposition 2.2.3 preserves $+$ and $\cdot$, and a sign is moved by Proposition 2.3.2 (c), as in $(-4) \cdot 5 = -(4 \cdot 5) = -20$.

3.1.1 Divisibility on the constructed integers

The definition of divisibility needs nothing that the ring $\mathbb{Z}$ lacks. We restate it, and the definition of a prime, from *Sets, Relations, and Cardinality*, Section 2.2, with $\mathbb{Z}$ now the ring of Chapter 2.

Divisibility (*Sets, Relations, and Cardinality*, Definition 2.2.1). Let $a, b \in \mathbb{Z}$. Then a **divides** b , written $a \mid b$, if **there exists** $k \in \mathbb{Z}$ with $b = ka$. Then a is a **divisor** of b , and b is a **multiple** of a . We write $a \nmid b$ when a does not divide b .

Prime (*Sets, Relations, and Cardinality*, Definition 2.2.2). An integer p is **prime** if $p \geq 2$ and the only **positive** divisors of p are 1 and p . A **prime factor** of an integer n is a prime p with $p \mid n$.

Both definitions use only the multiplication of $\mathbb{Z}$, its order $\leq$, and the set $\mathbb{Z}_{>0}$, and Chapter 2 provides all three. They are the same definitions as before; what changes is that every fact about them must now be proved from Chapter 2.

Divisibility is a question about existence: is b some integer times a ?

Some instances. $3 \mid -12$, since $-12 = (-4) \cdot 3$. $-4 \mid 0$, since $0 = 0 \cdot (-4)$. Even $0 \mid 0$ holds, since $0 = 1 \cdot 0$: the definition asks for **some** k , and here every k works. On the other hand $5 \nmid 12$. That is a statement that **no** $k \in \mathbb{Z}$ has $12 = 5k$, and to prove it we need the theorem on division with remainder below.

The relation “ $a \mid b$ ” is not a fraction. It is a statement, true or false, about two integers. The expression b/a , for $a \neq 0$, is a rational number, and this chapter does not use it to decide divisibility.

Here are the rules for divisibility that the rest of the chapter uses. Each is a short consequence of the ring laws or of the order.

Proposition 3.1.1. Rules for Divisibility in $\mathbb{Z}$

Let $a, b, c, x, y \in \mathbb{Z}$.

- (a) $a \mid 0$, $1 \mid a$ and $a \mid a$. If $0 \mid a$, then $a = 0$.
- (b) If $a \mid b$ and $b \mid c$, then $a \mid c$.

- (c) If $a \mid b$ and $a \mid c$, then $a \mid bx + cy$.
- (d) If $a \mid b$, then $(-a) \mid b$ and $a \mid (-b)$.
- (e) If $a \mid b$, $a > 0$ and $b > 0$, then $a \leq b$.
- (f) If $a, b \in \mathbb{N}$, $a \mid b$ and $b \mid a$, then $a = b$.
- (g) If $a \mid 1$, then $a = 1$ or $a = -1$.
- (h) If $a \neq 0$, then **exactly one** of $a, -a$ lies in $\mathbb{Z}_{>0}$.

Idea. Parts (a)–(d) are identities in the commutative ring $\mathbb{Z}$: write each hypothesis as an equation $b = ka$ and rearrange. Part (e) is the one that needs the order. If $b = ka$ with $a, b > 0$, the factor k cannot be zero or negative, so by discreteness it is at least 1, and multiplying a by something at least 1 cannot make it smaller. Parts (f) and (g) then follow from (e), and (h) is (P2) for the positives of $\mathbb{Z}$.

Proof. We use the ring laws (F1)–(F7) and (F9) of $\mathbb{Z}$ (Theorem 2.3.1) without further mention.

- (a) $0 = a \cdot 0 = 0 \cdot a$ by Proposition 2.3.2 (b) and (F6), so $a \mid 0$ with $k = 0$. Also $a = a \cdot 1$ by (F7), so $1 \mid a$ with $k = a$; and $a = 1 \cdot a$, so $a \mid a$ with $k = 1$. If $0 \mid a$, then $a = k \cdot 0 = 0$ for some $k \in \mathbb{Z}$, by Proposition 2.3.2 (b).
- (b) Let $b = ka$ and $c = lb$ with $k, l \in \mathbb{Z}$. Then $c = l(ka) = (lk)a$ by (F5), so $a \mid c$.
- (c) Let $b = ka$ and $c = la$. Then

$$bx + cy = (ka)x + (la)y = (kx)a + (ly)a = (kx + ly)a$$

by (F5), (F6) and (F9), and $kx + ly \in \mathbb{Z}$. So $a \mid bx + cy$.

- (d) Let $b = ka$. By Proposition 2.3.2 (c), $(-k)(-a) = ka = b$, so $(-a) \mid b$; and $(-k)a = -(ka) = -b$, so $a \mid (-b)$.
- (e) Let $a \neq 0$. By the converse part of Proposition 2.3.3, applied to the ordered ring $\mathbb{Z}$, the set $\{x \in \mathbb{Z} : x > 0\}$ satisfies (P2), so exactly one of $a > 0, -a > 0$ holds. That set is $\mathbb{Z}_{>0}$ by Theorem 2.3.4 (b).
- (f) Let $b = ka$ with $k \in \mathbb{Z}$, $a > 0$ and $b > 0$. We show first that $k > 0$. If $k = 0$, then $b = 0 \cdot a = 0$ by Proposition 2.3.2 (b), against $b > 0$. If $k < 0$, then $ka < 0 \cdot a = 0$ by Proposition 2.3.5 (c) (multiplying $k < 0$ by $a > 0$), again against $b > 0$. So $k > 0$, and by discreteness (Theorem 2.3.4 (c), with $0 < k$) $1 \leq k$. If $k = 1$, then $b = a$. If $1 < k$, then $k - 1 > 0$ by Proposition 2.3.5 (a), so $(k - 1)a > 0 \cdot a = 0$ by Proposition 2.3.5 (c), that is, $b - a = ka + (-1)a = (k - 1)a > 0$ (Proposition 2.3.2 (c), (F7) and (F9)), and $a < b$ by Proposition 2.3.5 (a). In both cases $a \leq b$.
- (g) Let $a, b \in \mathbb{N}$ with $a \mid b$ and $b \mid a$. If $a = 0$, then $0 \mid b$, so $b = 0 = a$ by (a). If $b = 0$, then $a = 0$ in the same way. Otherwise $a, b \in \mathbb{N}$ are non-zero, hence positive (Theorem 2.3.4 (b)), and (e) gives $a \leq b$ and $b \leq a$. Since $\leq$ is a total order (Proposition 2.3.5 (i)), it is antisymmetric, and $a = b$.
- (h) Let $a \mid 1$, say $1 = ka$. Then $a \neq 0$: otherwise $1 = k \cdot 0 = 0$, against $1 \neq 0$ in $\mathbb{Z}$ (Theorem 2.3.1). By (h), one of $a, -a$ is positive; call it e . Then $e \mid 1$, by (d) if $e = -a$. Since $1 > 0$ (Proposition 2.3.5 (e)), part (e) gives $e \leq 1$; and $e > 0$ gives $1 \leq e$ by discreteness. So $e = 1$. If $e = a$, then $a = 1$; if $e = -a$, then $a = -(-a) = -1$ by Proposition 2.3.2 (a). This proves the proposition.

Part (f) is the antisymmetry of divisibility on $\mathbb{N}$, Sets, Relations, and Cardinality, Proposition 2.4.1 of *Sets, Relations, and Cardinality*, Section 2.4, now proved on $\mathbb{N} \subseteq \mathbb{Z}$ for the constructed integers. On all of $\mathbb{Z}$ it fails: $2 \mid -2$ and $-2 \mid 2$, by (d), yet $2 \neq -2$. That is why (f) is stated for $a, b \in \mathbb{N}$, and why (e) needs $b > 0$: $3 \mid -3$, but $3 > -3$. (The hypothesis $a > 0$ is a convenience for the proof: $a = 0$ cannot divide $b > 0$, by (a), and if $a < 0 < b$, then $a \leq b$ holds anyway.)

Quick check. Which hypothesis of (e) fails for $a = 3$, $b = 0$, and is the conclusion $a \leq b$ true there?

Solution. $3 \mid 0$ by (a), and $a = 3 > 0$, but $b = 0$ is not positive. The conclusion $3 \leq 0$ is false. Every integer divides 0, so no bound of the form $a \leq b$ can hold for $b = 0$; that is the reason for the hypothesis $b > 0$.

3.1.2 Division with remainder

Now the substitute for division. Given $a \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>0}$, we want to write a as a multiple of n plus something small, and we want “small” to make the answer unique. The obvious attempt subtracts n from a until what is left lies in $\{0, \dots, n-1\}$, adding n instead when a is negative. That is a process; the theorem replaces it by a least element.

Theorem 3.1.2. Division with Remainder in $\mathbb{Z}$

Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>0}$.

(a) There are **unique** $q, r \in \mathbb{Z}$ with

$$a = qn + r \quad \text{and} \quad 0 \leq r < n.$$

(b) Moreover $q = \lfloor a/n \rfloor$, the integer part of the rational number a/n (Proposition 2.5.5), so $r = a - n\lfloor a/n \rfloor$.

The integers q and r are the **quotient** and the **remainder** of a on division by n .

Idea. Among the integers $a - kn$, $k \in \mathbb{Z}$, look at the non-negative ones. If there is at least one, Proposition 2.3.6 hands us the least, r . It must be below n : otherwise $r - n$ would be a smaller non-negative one of the same form. Finding a non-negative $a - kn$ is easy for $a \geq 0$ (take $k = 0$) and needs one inequality for $a < 0$ (take $k = a$). For uniqueness, two remainders differ by a multiple of n and yet by less than n , and (e) of the rules above forbids a positive multiple of n below n . Part (b) moves the inequalities $qn \leq a < qn + n$ into $\mathbb{Q}$ and divides by n .

Proof.

(a) *Existence.* Let

$$R := \{a - kn : k \in \mathbb{Z}\} \cap \{x \in \mathbb{Z} : x \geq 0\}.$$

We show $R \neq \emptyset$. If $a \geq 0$, take $k = 0$: $a - 0 \cdot n = a - 0 = a \geq 0$, by (F6), Proposition 2.3.2 (b) and $-0 = 0$ ($0 + 0 = 0$ and Proposition 2.3.2 (a)). If $a < 0$, take $k = a$: then $a - an = a + a(-n) = a(1 - n)$ by Proposition 2.3.2 (c), (F7) and (F9). Since $n > 0$, discreteness (Theorem 2.3.4 (c)) gives $1 \leq n$. If $n = 1$, then $a(1 - n) = a \cdot 0 = 0$ by Proposition 2.3.2 (b). If $1 < n$, then $-n < -1$ by Proposition 2.3.5 (a), so $1 - n < 0$ by (O3); multiplying $a < 0$ by $1 - n < 0$ reverses the inequality (Proposition 2.3.5 (d)), so $a(1 - n) > 0 \cdot (1 - n) = 0$. In every case R has an element.

The set $R \subseteq \mathbb{Z}$ is non-empty and has the lower bound 0, so by Proposition 2.3.6 it has a least element r . Write $r = a - qn$ with $q \in \mathbb{Z}$. Then $a = qn + r$ and $r \geq 0$.

Suppose $r \geq n$. Then $r - n \geq 0$: if $r = n$, then $r - n = 0$ by (F4); if $r > n$, then $r - n > 0$ by Proposition 2.3.5 (a). Also $r - n = a - qn - n = a + (-1)(qn) + (-1)n = a + (-1)((q + 1)n) = a - (q + 1)n$, since $-x = (-1)x$ for every x (Proposition 2.3.2 (c) and (F7)) and by (F9), so $r - n \in R$. But $-n < -0 = 0$ (Proposition 2.3.5 (a), since $n > 0$), so $r - n < r$ by (O3). This contradicts the choice of r as least. Hence $r < n$.

Uniqueness. Let $a = qn + r = q'n + r'$ with $q, q', r, r' \in \mathbb{Z}$, $0 \leq r < n$ and $0 \leq r' < n$. Suppose $r \neq r'$. Exchanging (q, r) and (q', r') changes neither the hypotheses nor the goal, so we may suppose $r' < r$. Then

$$r - r' = (q' - q)n,$$

so $n \mid r - r'$. Here $r - r' > 0$ by Proposition 2.3.5 (a), and $n > 0$, so Proposition 3.1.1 (e) gives $n \leq r - r'$. But adding $r - r'$ to $0 \leq r'$ gives $r - r' \leq (r - r') + r' = r$ (Proposition 2.3.5 (b)), and $r < n$; so $r - r' < n$, a contradiction. Hence $r = r'$. Then $qn = q'n$, so $(q - q')n = 0$, and since $n \neq 0$, Proposition 2.3.5 (f) gives $q - q' = 0$, that is, $q = q'$.

(b) From (a), $0 \leq r < n$; adding qn (Proposition 2.3.5 (b)) gives

$$qn \leq a < qn + n.$$

These are inequalities between integers, and by Theorem 2.5.1 (b) and Proposition 2.4.4 they hold in $\mathbb{Q}$ as well, with the same sums and products. In $\mathbb{Q}$, $n > 0$, so $n^{-1} > 0$ (Proposition 2.5.2 (a)). Multiplying by n^{-1} preserves strict inequalities (Proposition 2.3.5 (c)) and equalities, so

$$q = qn \cdot n^{-1} \leq a \cdot n^{-1} < (qn + n) \cdot n^{-1} = q + 1.$$

That is, $q \leq a/n < q + 1$, with $q \in \mathbb{Z}$. By the uniqueness in Proposition 2.5.5, $q = \lfloor a/n \rfloor$, and then $r = a - qn = a - n\lfloor a/n \rfloor$. This proves the theorem. ■

The hypothesis $n > 0$ is used four times in (a): to find an element of R when $a < 0$ (through $1 - n \leq 0$), to see that $r - n < r$, and in the uniqueness both to apply Proposition 3.1.1 (e) and, as $n \neq 0$, to cancel n from $(q - q')n = 0$. For $n = 0$ the statement fails outright: no r satisfies $0 \leq r < 0$. Exercise B1 handles $n < 0$.

Uniqueness is what turns the theorem into a test for divisibility: $n \mid a$ **if and only if the remainder of a on division by n is 0**. Indeed, if $a = kn$, then $a = kn + 0$ is a division with remainder, and by uniqueness it is the only one; conversely $a = qn + 0$ says $n \mid a$. For instance $12 = 2 \cdot 5 + 2$ with $0 \leq 2 < 5$, so the remainder is $2 \neq 0$, and $5 \nmid 12$.

Remark. The statement of (a) is Sets, Relations, and Cardinality, Theorem 2.2.3 of *Sets, Relations, and Cardinality*, Section 2.2, which was proved there for the school integers. The existence proof above follows the same route, with each school fact replaced by a result of Chapter 2: the closure of $\mathbb{Z}$ under $+$, $-$, $\cdot$ by Theorem 2.3.1; “a positive integer is at least 1” by Theorem 2.3.4 (b), (c); and the least element of a set of integers bounded below by Proposition 2.3.6. The uniqueness argument there is the one packaged here as [Proposition 3.1.1](#) (e). For $n = 2$ and $a \in \mathbb{N}$, (a) is Proposition 1.6.4 (d) of Section 1.6, which we compare with but do not use.

Part (b) pays a debt of Section 2.5. There, after Proposition 2.5.5, the integer part $\lfloor p/q \rfloor$ was announced as a quotient; (b) says exactly that, and it gives a second way to compute q and r . Exercise C1 turns (b) around and proves the existence half of (a) from the integer part.

Quick check. Find the quotient and the remainder of $a = -17$ on division by $n = 5$, and check them against (b).

Solution. $q = -4$ and $r = 3$: $(-4) \cdot 5 + 3 = -20 + 3 = -17$, and $0 \leq 3 < 5$. For (b), $-4 \leq -17/5 < -3$, since $(-4) \cdot 5 = -20 \leq -17$ and $-17 < -15 = (-3) \cdot 5$ (Theorem 2.5.1 (a)); so $\lfloor -17/5 \rfloor = -4$.

Warning. “The remainder” means the r with $0 \leq r < n$. The equation $-17 = (-3) \cdot 5 - 2$ is true, but -2 is **not** the remainder of -17 on division by 5; the remainder is 3. If negative “remainders” were allowed, uniqueness would fail at once: $-17 = (-3) \cdot 5 + (-2) = (-4) \cdot 5 + 3$. For negative a , the quotient is not “ a/n with the fraction dropped”: that would give -3 here, while $\lfloor -17/5 \rfloor = -4$.

3.1.3 Even and odd

Recall that an integer a is **even** if $a = 2k$ for some $k \in \mathbb{Z}$, that is, $2 \mid a$, and **odd** if $a = 2k + 1$ for some $k \in \mathbb{Z}$. These are the words *Logic and Proof*, Chapter 1 used, now read on the constructed $\mathbb{Z}$. Section 2.6 had parity for natural numbers from Proposition 1.6.4 (d). With $n = 2$, the theorem gives it for every integer, negative ones included, with one citation.

Corollary 3.1.3. Even and Odd Integers

- (a) Every $a \in \mathbb{Z}$ is even or odd, and **not both**. More precisely, either $a = 2q$ for exactly one $q \in \mathbb{Z}$ and a is not of the form $2k + 1$, or $a = 2q + 1$ for exactly one $q \in \mathbb{Z}$ and a is not of the form $2k$.
- (b) If $a \in \mathbb{Z}$ and a^2 is even, then a is even.

Idea. Divide by 2. The remainder lies in $\{0, 1\}$, by discreteness, and it is unique, so each integer has exactly one of the two forms. For (b), square the odd form and read off the remainder.

Proof.

- (a) Since $2 = 1 + 1 > 0$, the theorem with $n = 2$ gives unique $q, r \in \mathbb{Z}$ with $a = 2q + r$ and $0 \leq r < 2$. Then $r \in \{0, 1\}$: if $r \neq 0$, then $0 < r$, so $1 \leq r$ by discreteness (Theorem 2.3.4 (c)); and if moreover $1 < r$, then $2 = 1 + 1 \leq r$ by discreteness again, against $r < 2$. If $a = 2k$ and $a = 2k' + 1$ for some $k, k' \in \mathbb{Z}$, then $(k, 0)$ and $(k', 1)$ would be two pairs as in the theorem, and $0 \neq 1$ contradicts its uniqueness. The same uniqueness shows that q is the only integer with $a = 2q + r$.
- (b) Suppose a is not even. By (a), $a = 2q + 1$ with $q \in \mathbb{Z}$. Then

$$a^2 = (2q + 1)^2 = 4q^2 + 4q + 1 = 2(2q^2 + 2q) + 1,$$

by Proposition 2.3.2 (d) and (F5), (F6), (F9), so a^2 is odd, and by (a) it is not even. This proves (b) by contraposition. ■

Part (b) is Logic and Proof, Theorem 2.1.3 of *Logic and Proof*, Section 2.1, proved there from the school facts (E1)–(E3) about the integers. Part (a) proves (E1) and (E2) for the constructed $\mathbb{Z}$, and the computation in (b) is (E3). We compare with that proof and do not use it. *Sets, Relations, and Cardinality*, Section 2.2 proved (E1) and (E2) for the school integers right after Sets, Relations, and Cardinality, Theorem 2.2.3.

Section 2.6 proved that no rational squares to 2 by a descent on denominators (Theorem 2.6.1), a route that needs only the order and the least-element property of $\mathbb{Z}$ and adapts to other non-squares. With (b), and with lowest terms from Section 3.3, the classical parity proof of *Logic and Proof*, Chapter 2 can also be run on the constructed $\mathbb{Q}$, every step citable; one of the review exercises at the end of this chapter does so.

3.1.4 Small primes

Later sections need to know that a few small integers are prime in the constructed $\mathbb{Z}$. *Sets, Relations, and Cardinality*, Section 2.2 checked some of these after Sets, Relations, and Cardinality, Definition 2.2.2, for the school integers; that check is not a proof about the ring of Chapter 2, so we redo it here.

Remark. The small-primes remark. The integers 2, 3, 5 and 7 are prime in $\mathbb{Z}$. Let $p \in \{2, 3, 5, 7\}$. Then $p \geq 2$. Let d be a positive divisor of p . Then $1 \leq d$ by discreteness (Theorem 2.3.4 (c)) and $d \leq p$ by Proposition 3.1.1 (e), so d is one of $1, 2, \dots, p$: applying discreteness repeatedly (if $d \neq 1$ then $2 \leq d$; if $d \neq 2$ then $3 \leq d$; and so on up to p) leaves no other value. Each d with $1 < d < p$ leaves a non-zero remainder:

$$\begin{aligned} 3 &= 1 \cdot 2 + 1, & 5 &= 2 \cdot 2 + 1 = 1 \cdot 3 + 2 = 1 \cdot 4 + 1, \\ 7 &= 3 \cdot 2 + 1 = 2 \cdot 3 + 1 = 1 \cdot 4 + 3 = 1 \cdot 5 + 2 = 1 \cdot 6 + 1. \end{aligned}$$

(For $p = 2$ there is no such d .) So $d \nmid p$ for these d , by the divisibility test after Theorem 3.1.2: $p = kd$ would give $p = kd + 0$, a second division of p by d , with remainder 0, against the uniqueness in Theorem 3.1.2 (a). Hence the positive divisors of p are 1 and p , and p is prime.

The later sections of this chapter cite this paragraph as “the small-primes remark”. The same

procedure decides, for any given $p \geq 2$, whether p is prime; Section 3.3 shortens it.

3.1.5 Exercises

3.1.5.1 A. Check your understanding

Exercise. A1

- (a) Find the quotient and the remainder on division by $n = 6$ of $a = 47$, of $a = -47$ and of $a = 0$.
- (b) Where is $n > 0$ used in the existence half of [Theorem 3.1.2](#) (a)?
- (c) True or false, with a reason: $0 \mid 0$.
- (d) True or false, with a reason: for all $a, b \in \mathbb{Z}$, if $a \mid b$ and $b \mid a$, then $a = b$.

Solution.

- (a) $47 = 7 \cdot 6 + 5$, so $(q, r) = (7, 5)$. $-47 = (-8) \cdot 6 + 1$, since $-48 + 1 = -47$, so $(q, r) = (-8, 1)$. $0 = 0 \cdot 6 + 0$, so $(q, r) = (0, 0)$. In each case $0 \leq r < 6$, so by uniqueness these are the quotient and remainder. Note $(-8, 1)$, not $(-7, -5)$.
- (b) Twice. For $a < 0$, the element $a - an = a(1 - n)$ of R is non-negative because $1 - n \leq 0$, which comes from $n \geq 1$, that is, from $n > 0$ and discreteness. And the contradiction “ $r - n < r$ ” needs $-n < 0$, that is, $n > 0$.
- (c) True: $0 = 1 \cdot 0$, so $k = 1$ witnesses $0 \mid 0$ ([Proposition 3.1.1](#) (a)).
- (d) False: $2 \mid -2$ and $-2 \mid 2$ ([Proposition 3.1.1](#) (d)), but $2 \neq -2$. The statement is true for $a, b \in \mathbb{N}$ ([Proposition 3.1.1](#) (f)).

3.1.5.2 B. Practice

Exercise. B1: Negative divisors

Let $a, n \in \mathbb{Z}$ with $n < 0$. Prove that there are unique $q, r \in \mathbb{Z}$ with $a = qn + r$ and $0 \leq r < -n$.

Solution. Since $n < 0$, $-n > 0$ by [Proposition 2.3.5](#) (a), so $-n \in \mathbb{Z}_{>0}$.

Existence. By [Theorem 3.1.2](#) (a) applied to a and $-n$, there are $q_0, r \in \mathbb{Z}$ with $a = q_0(-n) + r$ and $0 \leq r < -n$. Let $q := -q_0$. Then $q_0(-n) = (-q_0)n = qn$ by [Proposition 2.3.2](#) (c), so $a = qn + r$.

Uniqueness. Let $a = qn + r = q'n + r'$ with $0 \leq r, r' < -n$. By [Proposition 2.3.2](#) (c), $qn = (-q)(-n)$ and $q'n = (-q')(-n)$, so $a = (-q)(-n) + r = (-q')(-n) + r'$ are two divisions of a by $-n$. The uniqueness in [Theorem 3.1.2](#) (a) gives $r = r'$ and $-q = -q'$, hence $q = -(-q) = -(-q') = q'$ by [Proposition 2.3.2](#) (a).

Exercise. B2: Three in a row

Let $a \in \mathbb{Z}$. Prove that **exactly one** of $a, a + 1, a + 2$ is divisible by 3.

Solution. At least one. By [Theorem 3.1.2](#) (a), $a = 3q + r$ with $0 \leq r < 3$, and $r \in \{0, 1, 2\}$ by discreteness, as in the proof of [Corollary 3.1.3](#). If $r = 0$, then $3 \mid a$. If $r = 1$, then $a + 2 = 3q + 3 = 3(q + 1)$. If $r = 2$, then $a + 1 = 3q + 3 = 3(q + 1)$.

At most one. Suppose $3 \mid a + i$ and $3 \mid a + j$ with $0 \leq i < j \leq 2$. By [Proposition 3.1.1](#) (c) (with $x = 1$, $y = -1$), $3 \mid (a + j) - (a + i) = j - i$, and $j - i \in \{1, 2\}$ is positive. By [Proposition 3.1.1](#) (e), $3 \leq j - i \leq 2$, which is false. So no two of the three are divisible by 3.

(Equivalently: the remainders of a , $a + 1$, $a + 2$ on division by 3 are r , and then the other two of $0, 1, 2$, and uniqueness of remainders allows only one of them to be 0.)

3.1.5.3 C. Going deeper

Exercise. C1: Division from the integer part

Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>0}$. Prove the existence half of [Theorem 3.1.2](#) (a) directly from [Proposition 2.5.5](#), without the set R : put $q := \lfloor a/n \rfloor$ and $r := a - qn$, and show that $0 \leq r < n$. Say where $n > 0$ is used.

Solution. By [Proposition 2.5.5](#), $q := \lfloor a/n \rfloor \in \mathbb{Z}$ satisfies

$$q \leq a/n < q + 1$$

in $\mathbb{Q}$, where $a/n = a \cdot n^{-1}$ and $n \neq 0$ in $\mathbb{Q}$. Since $n > 0$, multiplying by n preserves the strict inequality ([Proposition 2.3.5](#) (c)) and the equality case, so

$$qn \leq (a \cdot n^{-1}) \cdot n = a < (q + 1)n = qn + n.$$

Subtracting qn (that is, adding $-qn$, (O3)) gives $0 \leq a - qn < n$. Here $r := a - qn$ is an integer, and by [Theorem 2.5.1](#) (b) the inequalities $0 \leq r < n$, proved in $\mathbb{Q}$, hold in $\mathbb{Z}$. So $a = qn + r$ with $0 \leq r < n$.

The hypothesis $n > 0$ is used when multiplying by n : for $n < 0$, multiplication reverses inequalities ([Proposition 2.3.5](#) (d)), and the same q would give $qn \geq a > qn + n$, so $n < r \leq 0$ instead. (This exercise is practice with a result already proved; nothing later rests on it.)