

3.5 Units, Prime Moduli, and the Chinese Remainder Theorem

Section 3.4 made $\mathbb{Z}/n\mathbb{Z}$ a commutative ring, and Example (Multiplication modulo six and modulo five) put two of these rings side by side. In $\mathbb{Z}/5\mathbb{Z}$ every non-zero class has a partner whose product with it is $[1]$, so we may divide by it. In $\mathbb{Z}/6\mathbb{Z}$ the class $[2]$ has no such partner: the products $[2][x]$ are only $[0], [2], [4]$. Which classes can be divided by, and for which moduli can all non-zero classes? This section answers both questions with the gcd of Section 3.2, and finds a field with p elements for every prime p . It then solves two congruences at once, the Chinese remainder theorem, by the move of Section 3.3, multiply the Bézout identity: write 1 as a combination and multiply.

Throughout, $n \in \mathbb{Z}_{>0}$ and classes are taken in $\mathbb{Z}/n\mathbb{Z}$ unless another modulus is named. Two classes are equal exactly when their representatives are congruent:

$$[u] = [v] \iff u - v \in n\mathbb{Z} \iff n \mid u - v.$$

The first equivalence is Sets, Relations, and Cardinality, Theorem 2.5.1 (b) for the relation of Theorem 3.4.1 (a); the second is the definition of $n\mathbb{Z}$ (Definition 3.2.1) read with Sets, Relations, and Cardinality, Definition 2.2.1. We call it the **class test**. Products of classes are computed on representatives, $[u][v] = [uv]$ (Theorem 3.4.1 (b)).

3.5.1 Units of a commutative ring

In $\mathbb{Z}/6\mathbb{Z}$ the equation $[2][x] = [1]$ has no solution, while $[5][x] = [1]$ has the solution $[x] = [5]$. The elements that can be divided by are the ones that solve “ u times something is 1”, and they deserve a name in every commutative ring at once.

A unit is an element that has a multiplicative inverse in the ring itself.

Definition 3.5.1. Unit of a Commutative Ring

Let R be a commutative ring (Definition 2.3.1). An element $u \in R$ is a **unit** of R if **there exists** $v \in R$ with $uv = 1$. The set of units of R is written $R^\times$. For a unit u , the element v is **unique**; it is written u^{-1} and called the **inverse** of u .

In words: u is a unit when the equation $ux = 1$ can be solved **inside** R . The definition asks for one solution; it does not ask u to be non-zero.

Well-definedness of u^{-1} . Let $uv = 1$ and $uv' = 1$. Then, by (F7), (F5) and (F6),

$$v = v \cdot 1 = v(uv') = (vu)v' = (uv)v' = 1 \cdot v' = v'.$$

So the inverse is unique, and the notation u^{-1} names one element.

Closure. The element 1 is a unit, since $1 \cdot 1 = 1$. If u is a unit, so is u^{-1} , with $(u^{-1})^{-1} = u$, because $u^{-1}u = uu^{-1} = 1$ by (F6). If u and w are units, then

$$(uw)(u^{-1}w^{-1}) = (uu^{-1})(ww^{-1}) = 1 \cdot 1 = 1,$$

reordering the four factors by (F5) and (F6); so uw is a unit and $(uw)^{-1} = u^{-1}w^{-1}$, by uniqueness.

A unit is not a zero divisor. If u is a unit and $ux = 0$, then

$$x = (u^{-1}u)x = u^{-1}(ux) = u^{-1} \cdot 0 = 0,$$

by $u^{-1}u = 1$ (above) and $1 \cdot x = x \cdot 1 = x$ ((F6), (F7)) in the first equality, (F5) in the second, and Proposition 2.3.2 (b) in the third. So a unit times a non-zero element is never 0.

Examples.

- **The integers.** $\mathbb{Z}^\times = \{1, -1\}$. Indeed $1 \cdot 1 = 1$ and $(-1)(-1) = 1$ (Proposition 2.3.2 (c)). Conversely, $uv = 1$ says $u \mid 1$, so $u = 1$ or $u = -1$ by Proposition 3.1.1 (g).
- **The rationals.** $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$: every non-zero rational has an inverse by (F8) (Theorem 2.4.3), and 0 is not a unit, since $0 \cdot v = 0 \neq 1$ (Proposition 2.3.2 (b)).
- **The integers modulo six.** By the multiplication table of Example (Multiplication modulo six and modulo five), the units of $\mathbb{Z}/6\mathbb{Z}$ are $[1]$ and $[5]$, and $[5]^{-1} = [5]$.
- **The zero ring** $\{0\}$ of Section 2.3, where $1 = 0$. Here $0 \cdot 0 = 0 = 1$, so 0 is a unit and $R^\times = R$. This degenerate case is why “every non-zero element is a unit” is not by itself the definition of a field.

A non-example by minimal change. Change 5 to 2 in the third example. The class $[2] \in \mathbb{Z}/6\mathbb{Z}$ is non-zero, like $[5]$, but $[2][3] = [6] = [0]$: it is a zero divisor, so by the paragraph above it is **not** a unit. Concretely, the clause “there exists v with $uv = 1$ ” fails: the products $[2][x]$ for $x = 0, \dots, 5$ are $[0], [2], [4], [0], [2], [4]$, and $[1]$ is not among them.

Why this definition. With units, the field axiom (F8) reads: every non-zero element is a unit. So a field (Definition 2.3.1) is exactly a commutative ring with $1 \neq 0$ in which $R^\times = R \setminus \{0\}$; when $1 \neq 0$, the element 0 is never a unit, since $0 \cdot v = 0$ (Proposition 2.3.2 (b)). The definition asks for an inverse in R , not in some bigger ring: $2 \in \mathbb{Z}$ has the inverse $1/2$ in $\mathbb{Q}$, and it is still not a unit of $\mathbb{Z}$.

Warning. “Non-zero and not a zero divisor” does not make an element a unit. In $\mathbb{Z}$ there are no zero divisors at all (Proposition 2.3.5 (f)), yet 2 is not a unit, since $2 \nmid 1$. The paragraph above proves only one direction: a unit is never a zero divisor. So “not a unit” must be checked against the definition, or, in $\mathbb{Z}/n\mathbb{Z}$, by the next theorem.

The units of a commutative ring are closed under products and inverses and contain 1: they form what *Algebraic Preliminaries*, Chapter 3 calls a group. Here we only need to find them in $\mathbb{Z}/n\mathbb{Z}$.

3.5.2 Which classes are units

In $\mathbb{Z}/6\mathbb{Z}$ the units $[1]$ and $[5]$ are the classes of the integers coprime to 6, and the non-units $[0], [2], [3], [4]$ share a factor with 6. The equation $[a][x] = [1]$ says $n \mid ax - 1$, that is, $ax + ny = 1$ for some integer y : a Bézout identity. So the question is answered by Section 3.2.

Theorem 3.5.1. Units Modulo n

Let $n \in \mathbb{Z}_{>0}$ and $a \in \mathbb{Z}$. Then $[a]$ is a unit of $\mathbb{Z}/n\mathbb{Z}$ **if and only if** $\gcd(a, n) = 1$. In that case, for **any** $x, y \in \mathbb{Z}$ with $ax + ny = 1$, $[a]^{-1} = [x]$.

Idea. Both directions translate between one equation in $\mathbb{Z}/n\mathbb{Z}$ and one equation in $\mathbb{Z}$. A solution of $[a][x] = [1]$ is an integer combination $ax + ny = 1$, and Corollary 3.2.2 says that such a combination exists exactly when $\gcd(a, n) = 1$. The class test does the translation.

Proof. ($\Leftarrow$) Suppose $\gcd(a, n) = 1$. By Corollary 3.2.2 there are $x, y \in \mathbb{Z}$ with $ax + ny = 1$. Let x, y be any such pair. Then $ax - 1 = -ny = (-y)n$, so $n \mid ax - 1$, and by the class test $[ax] = [1]$. Hence $[a][x] = [ax] = [1]$, where the first equality is the definition of the product on classes (Theorem 3.4.1 (b)). So $[a]$ is a unit, and $[x]$ is its inverse, which is unique (Definition 3.5.1); thus $[a]^{-1} = [x]$ for every such pair.

($\Rightarrow$) Suppose $[a]$ is a unit. Every element of $\mathbb{Z}/n\mathbb{Z}$ is the class of an integer (Sets, Relations, and Cardinality, Definition 2.5.4), so $[a][x] = [1]$ for some $x \in \mathbb{Z}$. Then $[ax] = [1]$, so $n \mid ax - 1$ by the class test: $ax - 1 = yn$ for some $y \in \mathbb{Z}$. Hence $ax + n(-y) = 1$, and $\gcd(a, n) = 1$ by Corollary 3.2.2. This proves the theorem. ■

The theorem turns “is $[a]$ invertible?” into a gcd, and the Euclidean algorithm (Theorem 3.2.4) computes the gcd. Back-substitution, as in Example (Two runs of the algorithm), then produces the x with $ax + ny = 1$, and with it the inverse. Whether $\gcd(a, n) = 1$ depends only on the class $[a]$, since by the theorem it is equivalent to a statement about $[a]$; so any representative may be used.

Example. Inverting a class modulo sixty

Decide whether $[17]$ and $[12]$ are units of $\mathbb{Z}/60\mathbb{Z}$, and find the inverse of each one that is.

Solution. The class $[17]$. Run the Euclidean algorithm on $(60, 17)$:

$$\begin{aligned} 60 &= 3 \cdot 17 + 9, & 17 &= 1 \cdot 9 + 8, \\ 9 &= 1 \cdot 8 + 1, & 8 &= 8 \cdot 1 + 0. \end{aligned}$$

The last non-zero remainder is 1, so $\gcd(60, 17) = 1$ (Theorem 3.2.4 (c)), and $[17]$ is a unit by Theorem 3.5.1. Back-substitute, using the lines from the bottom up:

$$\begin{aligned} 1 &= 9 - 8 = 9 - (17 - 9) = 2 \cdot 9 - 17 \\ &= 2 \cdot (60 - 3 \cdot 17) - 17 = 2 \cdot 60 - 7 \cdot 17. \end{aligned}$$

So $17 \cdot (-7) + 60 \cdot 2 = 1$, and Theorem 3.5.1 gives $[17]^{-1} = [-7]$. The representative in $\{0, \dots, 59\}$ is 53, since $-7 - 53 = -60$. Check: $17 \cdot 53 = 901 = 15 \cdot 60 + 1$, so $[17][53] = [1]$.

The class $[12]$. Here $12 \mid 60$, so 12 is a common divisor of 12 and 60, and every common divisor of them divides 12; hence $\gcd(12, 60) = 12 \neq 1$ (Definition 3.2.2, with Proposition 3.1.1 (e) for the comparison), and $[12]$ is not a unit by Theorem 3.5.1. A witness: $[12][5] = [60] = [0]$ with $[5] \neq [0]$, so $[12]$ is a zero divisor, and a unit never is (Definition 3.5.1 and the paragraph after it).

Quick check. Find the inverse of $[3]$ in $\mathbb{Z}/7\mathbb{Z}$.

Solution. $[3]^{-1} = [5]$: $3 \cdot 5 = 15 = 2 \cdot 7 + 1$, so $[3][5] = [1]$. In the form of [Theorem 3.5.1](#), $3 \cdot 5 + 7 \cdot (-2) = 1$.

3.5.3 The field of integers modulo a prime

By [Theorem 3.5.1](#), every non-zero class of $\mathbb{Z}/n\mathbb{Z}$ is a unit exactly when every a with $n \nmid a$ is coprime to n . For a prime, Corollary 3.3.2 (a) says precisely this. For a composite n , a proper factor of n is neither divisible by n nor coprime to it. So the field property sorts the moduli into primes and the rest.

Theorem 3.5.2. The Integers Modulo n Form a Field Exactly When n Is Prime

Let $n \in \mathbb{Z}$ with $n \geq 2$. Then $\mathbb{Z}/n\mathbb{Z}$ is a field in the sense of Definition 2.3.1, that is, a commutative ring with $[1] \neq [0]$ in which every non-zero element is a unit, **if and only if** n is prime.

Idea. For a prime p , a non-zero class $[a]$ has $p \nmid a$, so the only common divisors left are ± 1 , and [Theorem 3.5.1](#) inverts $[a]$. For a composite $n = rs$ with $1 < r, s < n$, the classes $[r]$ and $[s]$ are non-zero with product $[n] = [0]$; a zero divisor cannot be a unit, so (F8) fails.

Proof. By Theorem 3.4.3 (a), $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring, and by Theorem 3.4.3 (c), $[1] \neq [0]$ since $n \geq 2$. So it is a field if and only if every non-zero class is a unit (Definition 2.3.1, (F8), and [Definition 3.5.1](#)).

($\Leftarrow$) Let n be prime, and let $[a] \neq [0]$. By Theorem 3.4.1 (d), $a \notin n\mathbb{Z}$, that is, $n \nmid a$. By Corollary 3.3.2 (a), $\gcd(n, a) = 1$, and $\gcd(a, n) = \gcd(n, a)$ (Definition 3.2.2). So $[a]$ is a unit by [Theorem 3.5.1](#).

($\Rightarrow$) Let $n \geq 2$ be not prime. By Sets, Relations, and Cardinality, Definition 2.2.2, n has a positive divisor $r \notin \{1, n\}$; write $n = rs$ with $s \in \mathbb{Z}$. Then $1 \leq r$ by discreteness (Theorem 2.3.4 (c)) and $r \leq n$ by Proposition 3.1.1 (e), so $1 < r < n$. Next, $s > 0$: if $s \leq 0$, then $rs \leq 0$ ($rs = 0$ if $s = 0$ by Proposition 2.3.2 (b), and $rs < r \cdot 0 = 0$ if $s < 0$ by Proposition 2.3.5 (c)), against $n > 0$. So s is a positive divisor of n , and $s \leq n$ by Proposition 3.1.1 (e). Also $s \neq n$: otherwise $rn = n$, so $(r - 1)n = 0$ and $r = 1$ by Proposition 2.3.5 (f), since $n \neq 0$. Hence $0 < s < n$ as well.

Now $[r] \neq [0]$: if $n \mid r$, then $n \leq r$ by Proposition 3.1.1 (e), since $n, r > 0$, against $r < n$. In the same way $[s] \neq [0]$. But $[r][s] = [rs] = [n] = [0]$, by the class test. Suppose $[r]$ were a unit. Then $[s] = [0]$, since a unit is not a zero divisor (the paragraph after [Definition 3.5.1](#)). This contradiction shows that the non-zero class $[r]$ is not a unit, so $\mathbb{Z}/n\mathbb{Z}$ is not a field. This proves the theorem. ■

So for every prime p there is a field with exactly p elements (Theorem 3.4.3 (b)). The smallest is $\mathbb{Z}/2\mathbb{Z}$, whose tables are those of the two-element field of Example (A field with two elements that cannot be ordered) with 0, 1 renamed $[0]$, $[1]$. *Algebraic Preliminaries*, Chapter 2 studies fields in general and gives these finite fields a name of their own.

Remark. In particular $\mathbb{Z}/5\mathbb{Z}$ is a field, since 5 is prime (the small-primes remark of Section 3.1). In it $5 \cdot [1] = [5] = [0]$ (Theorem 3.4.3 (d)), so $[1] + [1] + [1] + [1] + [1] = [0]$ with $[1] \neq [0]$, and no order makes it an ordered field (Theorem 3.4.3 (e)). Being a field does not help a finite ring to be ordered.

Warning. In $\mathbb{Z}/p\mathbb{Z}$, “ $[a] \neq [0]$ ” means $p \nmid a$, not $a \neq 0$. The class $[7]$ is the zero of $\mathbb{Z}/7\mathbb{Z}$, and it has no inverse, although $7 \neq 0$. The proof above applies Corollary 3.3.2 (a) to the condition $p \nmid a$; with only $a \neq 0$ in hand, the case $p \mid a$, $\gcd(p, a) = p$, is left open.

3.5.4 Two congruences at once

A number leaves the remainder 2 on division by 3 and the remainder 3 on division by 5. What can it be? Each condition alone is a single class. The question is whether the two classes meet, and in how much. The next theorem says that for coprime moduli they always meet, and in exactly one class modulo the product.

Theorem 3.5.3. Chinese Remainder Theorem for Two Moduli

Let $m, n \in \mathbb{Z}_{>0}$ with $\gcd(m, n) = 1$, and choose $u, v \in \mathbb{Z}$ with $mu + nv = 1$ (Corollary 3.2.2).

- (a) For all $a, b \in \mathbb{Z}$, the integer $x := a \cdot nv + b \cdot mu$ satisfies

$$x \equiv a \pmod{m} \quad \text{and} \quad x \equiv b \pmod{n},$$

and an integer x' satisfies both congruences **if and only if** $x' \equiv x \pmod{mn}$.

- (b) The rule $\Phi([x]_{mn}) := ([x]_m, [x]_n)$ is a well-defined **bijection** $\mathbb{Z}/mn\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. With $+$ and $\cdot$ on $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ taken componentwise, for all $x, y \in \mathbb{Z}$,

$$\begin{aligned} \Phi([x]_{mn} + [y]_{mn}) &= \Phi([x]_{mn}) + \Phi([y]_{mn}), \\ \Phi([x]_{mn}[y]_{mn}) &= \Phi([x]_{mn}) \Phi([y]_{mn}), \end{aligned}$$

and $\Phi([1]_{mn}) = ([1]_m, [1]_n)$.

Try it first (ten minutes): find an x with $x \equiv 2 \pmod{3}$ and $x \equiv 3 \pmod{5}$ by trying. Then use $1 = 2 \cdot 3 - 1 \cdot 5$ to find a formula that works for every pair of right-hand sides.

Idea. Trying works: among 3, 8, 13, ..., the numbers that are 3 modulo 5, the second one is 2 modulo 3. But trial and error gives one answer and no reason, and it does not say why no answer can be missing. The identity $mu + nv = 1$ supplies two special integers:

$$e := nv = 1 - mu, \quad f := mu = 1 - nv.$$

The first is $\equiv 1 \pmod{m}$ and $\equiv 0 \pmod{n}$; the second the other way round. So $ae + bf$ is

a modulo m and b modulo n , like a vector built from two coordinate vectors. For 3 and 5, $e = -5$ and $f = 6$, and $2e + 3f = 8$. Uniqueness modulo mn is Proposition 3.3.3: a difference divisible by m and by n is divisible by mn .

Proof.

- (a) Since $nv - 1 = -mu$ and $mu - 1 = -nv$,

$$\begin{aligned} x - a &= a(nv - 1) + bmu = m(bu - au), \\ x - b &= anv + b(mu - 1) = n(av - bv). \end{aligned}$$

So $m \mid x - a$ and $n \mid x - b$: $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ (Sets, Relations, and Cardinality, Definition 2.5.5).

Let $x' \in \mathbb{Z}$. Suppose first that $x' \equiv a \pmod{m}$ and $x' \equiv b \pmod{n}$. Then $x' - x = (x' - a) - (x - a)$ is divisible by m , and $x' - x = (x' - b) - (x - b)$ by n (Proposition 3.1.1 (c)). Since $\gcd(m, n) = 1$, Proposition 3.3.3 gives $mn \mid x' - x$, that is, $x' \equiv x \pmod{mn}$. Conversely, suppose $mn \mid x' - x$. Since $m \mid mn$, $m \mid x' - x$ (Proposition 3.1.1 (b)), and then $m \mid (x' - x) + (x - a) = x' - a$ by Proposition 3.1.1 (c). In the same way $n \mid x' - b$. So x' satisfies both congruences.

- (b) *Well defined.* Let $k \in \{m, n\}$. If $x \equiv x' \pmod{mn}$, then $k \mid mn \mid x - x'$, so $x \equiv x' \pmod{k}$ (Proposition 3.1.1 (b)). By Sets, Relations, and Cardinality, Theorem 2.5.1 (b) and Theorem 2.2.1 (a), applied to the identity map of $\mathbb{Z}$, with congruence modulo mn on the source and modulo k on the target, there is exactly one function $\mathbb{Z}/mn\mathbb{Z} \rightarrow \mathbb{Z}/k\mathbb{Z}$ sending $[x]_{mn}$ to $[x]_k$. Pairing the two values for $k = m$ and $k = n$ gives the function Φ into $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (Sets, Relations, and Cardinality, Definition 1.3.2).

Surjective. Let $(\alpha, \beta) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. By Sets, Relations, and Cardinality, Definition 2.5.4, $\alpha = [a]_m$ and $\beta = [b]_n$ for some $a, b \in \mathbb{Z}$. With x as in (a), $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$, so $\Phi([x]_{mn}) = ([x]_m, [x]_n) = ([a]_m, [b]_n)$ by Sets, Relations, and Cardinality, Theorem 2.5.1 (b).

Injective. Let $z, z' \in \mathbb{Z}$ with $\Phi([z]_{mn}) = \Phi([z']_{mn})$. Then $[z']_m = [z]_m$ and $[z']_n = [z]_n$, so $m \mid z' - z$ and $n \mid z' - z$ by Sets, Relations, and Cardinality, Theorem 2.5.1 (b). By Proposition 3.3.3, $mn \mid z' - z$, that is, $[z']_{mn} = [z]_{mn}$. So Φ is a bijection (Sets, Relations, and Cardinality, Definition 1.4.5).

The operations. By the definition of $+$ on each of the three rings (Theorem 3.4.1 (b)) and of the componentwise sum,

$$\begin{aligned} \Phi([x]_{mn} + [y]_{mn}) &= \Phi([x + y]_{mn}) = ([x + y]_m, [x + y]_n) \\ &= ([x]_m + [y]_m, [x]_n + [y]_n) = \Phi([x]_{mn}) + \Phi([y]_{mn}). \end{aligned}$$

The same lines with xy in place of $x + y$ give the product, and $\Phi([1]_{mn}) = ([1]_m, [1]_n)$ is the definition. This proves the theorem. ■

The theorem answers the opening question: the numbers with remainder 2 modulo 3 and remainder 3 modulo 5 form one class modulo 15, and the formula of (a) names a representative. Clause (b) says the same thing as a bijection. Each class modulo mn is the same information as a pair of classes, one modulo m and one modulo n , and the sums and products of classes can

be computed in either form. Each coordinate of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is a commutative ring, so with zero $([0]_m, [0]_n)$, one $([1]_m, [1]_n)$ and negatives taken componentwise, every axiom (F1)–(F7), (F9) holds in each coordinate and hence for the pairs; then Φ matches two commutative rings, element for element and operation for operation.

Example. Two remainders at once, and two failures

- (i) Find every $x \in \mathbb{Z}$ with $x \equiv 2 \pmod{3}$ and $x \equiv 3 \pmod{5}$.
- (ii) Show that $x \equiv 0 \pmod{2}$, $x \equiv 1 \pmod{4}$ has no solution, and that the solutions of $x \equiv 0 \pmod{2}$, $x \equiv 2 \pmod{4}$ are not one class modulo 8. Which hypothesis of [Theorem 3.5.3](#) fails, and what happens to its map $\Phi: \mathbb{Z}/8\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$?

Solution.

- (i) Here $m = 3$, $n = 5$, and $1 = 2 \cdot 3 + (-1) \cdot 5$, so $\gcd(3, 5) = 1$ (Corollary 3.2.2) with $u = 2$, $v = -1$. By [Theorem 3.5.3](#) (a),

$$x = 2 \cdot 5 \cdot (-1) + 3 \cdot 3 \cdot 2 = -10 + 18 = 8.$$

Check: $8 = 2 \cdot 3 + 2$ and $8 = 1 \cdot 5 + 3$. The solutions are exactly the x' with $x' \equiv 8 \pmod{15}$, the class $8 + 15\mathbb{Z} = \{\dots, -7, 8, 23, 38, \dots\}$.

- (ii) Here $\gcd(2, 4) = 2 \neq 1$: 2 divides both, and every common divisor divides 2, since $2 = 1 \cdot 2 + 0 \cdot 4$ (Proposition 3.1.1 (c), (e)). The hypothesis $\gcd(m, n) = 1$ fails, and both halves of the conclusion fail with it.

Existence fails. If $x \equiv 1 \pmod{4}$, then $x = 4k + 1 = 2(2k) + 1$ for some $k \in \mathbb{Z}$, so x has the form $2q + 1$. If also $x \equiv 0 \pmod{2}$, then $x = 2q'$. No integer has both forms (Corollary 3.1.3 (a)), so there is no solution.

Uniqueness modulo mn fails. If $x \equiv 2 \pmod{4}$, then $x = 4k + 2 = 2(2k + 1)$, so $x \equiv 0 \pmod{2}$ holds automatically, and the solutions are exactly the class $2 + 4\mathbb{Z}$. It contains 2 and 6, but $6 - 2 = 4$ and $8 \nmid 4$ (Proposition 3.1.1 (e)), so $2 \not\equiv 6 \pmod{8}$: the solutions form two classes modulo 8, $[2]_8$ and $[6]_8$.

The map. The rule $\Phi([x]_8) := ([x]_2, [x]_4)$ is still well defined, since $2 \mid 8$ and $4 \mid 8$ (the first step of the proof of (b) used only these divisibilities). It is not injective: $\Phi([0]_8) = ([0]_2, [0]_4) = \Phi([4]_8)$, since $4 \equiv 0$ modulo 2 and modulo 4, while $[4]_8 \neq [0]_8$. It is not surjective either: by the existence part, no x has $\Phi([x]_8) = ([0]_2, [1]_4)$.

Remark. For a map from a finite set to itself, injectivity alone gives surjectivity, by counting. Take $g: \mathbb{Z}/5\mathbb{Z} \rightarrow \mathbb{Z}/5\mathbb{Z}$, $g([x]) := [2][x]$. It is injective: if $[2][x] = [2][y]$, multiplying by $[3]$, with $[3][2] = [6] = [1]$, gives $[x] = [y]$ ((F5)–(F7)). Let $T := g(\mathbb{Z}/5\mathbb{Z})$. With codomain T , g is a bijection $\mathbb{Z}/5\mathbb{Z} \rightarrow T$, and $\mathbb{Z}/5\mathbb{Z}$ is finite (Theorem 3.4.3 (b)); so T is not a proper subset of $\mathbb{Z}/5\mathbb{Z}$ (Sets, Relations, and Cardinality, Theorem 3.1.9), that is, $T = \mathbb{Z}/5\mathbb{Z}$, and g is surjective. Could injectivity of Φ alone have given its surjectivity in the same way? Its source and target are different sets, so their sizes must be compared first; Exercise B3 asks for this. The formula of (a) is kept because it does more: it **computes** the solution.

Warning. The coprimality hypothesis is used twice in [Theorem 3.5.3](#): for the identity $mu + nv = 1$, which builds x , and in Proposition 3.3.3, which makes the solution unique modulo mn . Part (ii) of [Example \(Two remainders at once, and two failures\)](#) shows each use failing on its own: the moduli 2, 4 with right-hand sides 0, 1 have no solution, and with 0, 2 they have solutions spread over two classes modulo 8.

In this section the identity $1 = ax + by$ of Section 3.2 gave inverses ([Theorem 3.5.1](#)) and the solutions of two congruences ([Theorem 3.5.3](#)), inside the rings that Section 3.4's quotient construction built.

3.5.5 Exercises

3.5.5.1 A. Check your understanding

Exercise. A1

- (a) Find $[5]^{-1}$ in $\mathbb{Z}/12\mathbb{Z}$.
- (b) List the units of $\mathbb{Z}/12\mathbb{Z}$.
- (c) True or false: $\mathbb{Z}/1\mathbb{Z}$ is a field. Justify your answer.
- (d) Find every $x \in \mathbb{Z}$ with $x \equiv 1 \pmod{4}$ and $x \equiv 2 \pmod{9}$.
- (e) In the proof of [Theorem 3.5.2](#), where is it used that a unit is not a zero divisor?

Solution.

- (a) $[5]^{-1} = [5]$, since $5 \cdot 5 = 25 = 2 \cdot 12 + 1$.
- (b) By [Theorem 3.5.1](#), $[a]$ is a unit exactly when $\gcd(a, 12) = 1$, and by Theorem 3.4.3 (b) each class is $[a]$ for exactly one $a \in \{0, \dots, 11\}$. Among these, 0, 2, 4, 6, 8, 10 share the divisor 2 with 12, and 3, 9 share 3. The rest are coprime to 12: $1 \cdot 1 = 1$, $5 \cdot 5 = 25$, $7 \cdot 7 = 49$ and $11 \cdot 11 = 121$ are each 1 more than a multiple of 12, so each class is its own inverse. The units are $[1], [5], [7], [11]$.
- (c) **False.** In $\mathbb{Z}/1\mathbb{Z}$ every a has $1 \mid a - 0$, so $[1] = [0]$ (Theorem 3.4.3 (c)), and a field requires $1 \neq 0$ (Definition 2.3.1). It is the zero ring. (Every element of it is a unit, as in the zero ring of the examples after [Definition 3.5.1](#); that is not enough.)
- (d) $\gcd(4, 9) = 1$, from $4 \cdot (-2) + 9 \cdot 1 = 1$ (Corollary 3.2.2), so [Theorem 3.5.3](#) applies with $m = 4$, $n = 9$, $u = -2$, $v = 1$:

$$x = 1 \cdot 9 \cdot 1 + 2 \cdot 4 \cdot (-2) = 9 - 16 = -7.$$

The solutions are the $x' \equiv -7 \pmod{36}$, that is, the class $29 + 36\mathbb{Z}$, since $-7 + 36 = 29$. Check: $29 = 7 \cdot 4 + 1 = 3 \cdot 9 + 2$.

- (e) In the direction $(\Rightarrow)$, at the end: $[r][s] = [0]$ with $[s] \neq [0]$, so $[r]$, a non-zero class, cannot be a unit. That is how the proof shows (F8) fails.

3.5.5.2 B. Practice

Exercise. B1

Let p be prime and $a \in \mathbb{Z}$. Prove that if $[a]^2 = [1]$ in $\mathbb{Z}/p\mathbb{Z}$, then $[a] = [1]$ or $[a] = [-1]$. Show by an example that this fails in $\mathbb{Z}/8\mathbb{Z}$.

Solution. $[a]^2 = [a][a] = [a^2]$, so $[a^2] = [1]$, and $p \mid a^2 - 1$ by the class test. Expanding (Proposition 2.3.2), $a^2 - 1 = (a - 1)(a + 1)$. By Corollary 3.3.2 (b), $p \mid a - 1$ or $p \mid a + 1$. In the first case $[a] = [1]$; in the second, $a + 1 = a - (-1)$, so $[a] = [-1]$, again by the class test.

In $\mathbb{Z}/8\mathbb{Z}$, $[3]^2 = [9] = [1]$, since $9 - 1 = 8$. But $[3] \neq [1]$, since $8 \nmid 2$, and $[3] \neq [-1]$, since $3 - (-1) = 4$ and $8 \nmid 4$ (Proposition 3.1.1 (e)). The proof breaks at Corollary 3.3.2 (b): $8 \mid 2 \cdot 4 = (3 - 1)(3 + 1)$, yet 8 divides neither factor. (So do $[5]$ and $[7]$: all four units of $\mathbb{Z}/8\mathbb{Z}$ square to $[1]$.)

Exercise. B2

- Let $m, n \in \mathbb{Z}_{>0}$ and $x \in \mathbb{Z}$. Show that $[x]_{mn}$ is a unit of $\mathbb{Z}/mn\mathbb{Z}$ if and only if $[x]_m$ and $[x]_n$ are units of $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$.
- Now let m and n be coprime. Deduce that the map Φ of Theorem 3.5.3 (b) maps $(\mathbb{Z}/mn\mathbb{Z})^\times$ bijectively onto $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$.
- Which of (a) and (b) uses coprimality? Illustrate with $m = n = 2$.

Solution.

- $(\Rightarrow)$ Let $[x]_{mn}[s]_{mn} = [1]_{mn}$, with $s \in \mathbb{Z}$. Then $mn \mid xs - 1$ by the class test, and $m \mid mn$, so $m \mid xs - 1$ (Proposition 3.1.1 (b)); thus $[x]_m[s]_m = [1]_m$. Likewise $[x]_n[s]_n = [1]_n$. So both are units.
 $(\Leftarrow)$ Let $[x]_m[s]_m = [1]_m$ and $[x]_n[s']_n = [1]_n$. By the class test, $xs - 1 = -mt$ and $xs' - 1 = -nt'$ for some $t, t' \in \mathbb{Z}$, so $xs + mt = 1$ and $xs' + nt' = 1$. Multiplying the two equations and expanding,

$$x(xss' + snt' + s'mt) + mn \cdot tt' = 1.$$

So $\gcd(x, mn) = 1$ (Corollary 3.2.2), and $[x]_{mn}$ is a unit (Theorem 3.5.1).

- By (a), $\Phi([x]_{mn}) = ([x]_m, [x]_n)$ lies in $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ exactly when $[x]_{mn}$ is a unit. So Φ maps $(\mathbb{Z}/mn\mathbb{Z})^\times$ into that set, and the restriction is injective, since Φ is. Each element of that set is $\Phi(c)$ for some $c \in \mathbb{Z}/mn\mathbb{Z}$, since Φ is surjective, and that c is a unit by (a). So the restriction is a bijection.
- Only (b), through Theorem 3.5.3; (a) holds for all m, n . For $m = n = 2$, (a) says that $[x]_4$ is a unit exactly when $[x]_2$ is, and both hold exactly for odd x : the units of $\mathbb{Z}/4\mathbb{Z}$ are $[1], [3]$ and that of $\mathbb{Z}/2\mathbb{Z}$ is $[1]$. Yet $\Phi([x]_4) := ([x]_2, [x]_2)$ sends both units $[1]_4$ and $[3]_4$ to $([1]_2, [1]_2)$, so it is not injective on the units, and it is not a bijection $\mathbb{Z}/4\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ either (compare Example (Two remainders at once, and two failures) (ii)).

Exercise. B3

Let $m, n \in \mathbb{Z}_{>0}$ be coprime. Show by counting that injectivity of the map Φ of Theorem 3.5.3 (b) already forces its surjectivity, without using the formula of part (a).

Solution. By Theorem 3.4.3 (b), applied to the modulus mn , the set $\mathbb{Z}/mn\mathbb{Z}$ has mn elements: there is a bijection $\varphi: \{1, \dots, mn\} \rightarrow \mathbb{Z}/mn\mathbb{Z}$. Let $T := \Phi(\mathbb{Z}/mn\mathbb{Z})$ be the image of Φ . Since Φ is injective, Φ with codomain T is a bijection, and so is its composite with φ (Sets, Relations, and Cardinality, Proposition 3.1.1 (c)): T has mn elements.

The target $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ also has mn elements, by Theorem 3.4.3 (b) for m and for n , and the count of a product, part (a) of Sets, Relations, and Cardinality, Exercise (C2: Counting products and functions). Suppose T were a proper subset of the target. Then Sets, Relations, and Cardinality, Proposition 3.1.6 gives it k elements for some $k < mn$, and Sets, Relations, and Cardinality, Corollary 3.1.4 gives $k = mn$: a contradiction. So T is the whole target, and Φ is surjective. (Equivalently: composing the two bijections from $\{1, \dots, mn\}$ gives a bijection from the target onto T , which Sets, Relations, and Cardinality, Theorem 3.1.9 forbids when T is a proper subset.)

3.5.5.3 C. Going deeper
Exercise. C1: Exit check: units and the field $\mathbb{Z}/p\mathbb{Z}$

Let $n \in \mathbb{Z}_{>0}$ and $a \in \mathbb{Z}$. Prove that $[a] \in \mathbb{Z}/n\mathbb{Z}$ is a unit if and only if $\gcd(a, n) = 1$. Deduce that $\mathbb{Z}/p\mathbb{Z}$ is a field for every prime p .

Solution. Units, ($\Leftarrow$). If $\gcd(a, n) = 1$, then $ax + ny = 1$ for some $x, y \in \mathbb{Z}$ (Corollary 3.2.2). The product on $\mathbb{Z}/n\mathbb{Z}$ is well defined and computed on representatives (Theorem 3.4.1 (b)), so $[a][x] = [ax]$. Since $ax - 1 = (-y)n$, $n \mid ax - 1$, and $[ax] = [1]$ by the class test. So $[a]$ is a unit with inverse $[x]$.

Units, ($\Rightarrow$). If $[a][x] = [1]$ for some $x \in \mathbb{Z}$, then $[ax] = [1]$, so $ax - 1 = yn$ with $y \in \mathbb{Z}$, and $ax + n(-y) = 1$. By Corollary 3.2.2, $\gcd(a, n) = 1$.

The field. Let p be prime. $\mathbb{Z}/p\mathbb{Z}$ is a commutative ring (Theorem 3.4.3 (a)), and $[1] \neq [0]$, since $[1] = [0]$ would give $p \mid 1$, so $p \leq 1$ by Proposition 3.1.1 (e), while $p \geq 2$. Let $[a] \neq [0]$. Then $p \nmid a$. The integer $g := \gcd(p, a) \geq 1$ divides p , so $g \in \{1, p\}$ by Sets, Relations, and Cardinality, Definition 2.2.2; and $g = p$ would give $p \mid a$. So $g = 1$, and $[a]$ is a unit by the first part. Every non-zero class is a unit, which is (F8), so $\mathbb{Z}/p\mathbb{Z}$ is a field.

Marking scheme. (10 points) - 3: ($\Leftarrow$) of units: a Bézout identity $ax + ny = 1$ and the class computation $[a][x] = [ax] = [1]$, naming that the product is well defined (computed on representatives). - 3: ($\Rightarrow$) of units: from $[a][x] = [1]$ to an integer combination of a and n equal to 1, then $\gcd(a, n) = 1$ with a cited reason. - 2: $[a] \neq [0]$ gives $p \nmid a$, and $\gcd(a, p) = 1$ because the gcd divides p and is not p . - 1: $[1] \neq [0]$ for $p \geq 2$. - 1: concludes with (F8): every non-zero class is a unit. Fatal errors (0 for the step): canceling $[a]$ in $\mathbb{Z}/p\mathbb{Z}$ without justification (circular, since cancellation is what inverses give); “ $\gcd(a, p) = 1$ because p is prime” with no treatment of the case $p \mid a$. A proof of the field part that cites Corollary 3.3.2 (a) instead of the divisor argument earns the same 2 points.

Exercise. C2: Find the error

Here is an argument.

Claim. For every prime p , $\mathbb{Z}/p\mathbb{Z}$ is a field.

Proof. (0) By Theorem 3.4.3 (a) and (c), $\mathbb{Z}/p\mathbb{Z}$ is a commutative ring with $[1] \neq [0]$, since $p \geq 2$. (1) Let $[a] \neq [0]$ in $\mathbb{Z}/p\mathbb{Z}$. (2) If $[a][x] = [a][y]$, then canceling $[a]$ gives $[x] = [y]$. (3) So the map $f: \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$, $f([x]) := [a][x]$, is injective. (4) With codomain its image, f is a bijection from $\mathbb{Z}/p\mathbb{Z}$ onto $f(\mathbb{Z}/p\mathbb{Z})$, a subset of the finite set $\mathbb{Z}/p\mathbb{Z}$ (Theorem 3.4.3 (b)). By Sets, Relations, and Cardinality, Theorem 3.1.9 the image is not a proper subset, so f is surjective. (5) So some $[x]$ has $[a][x] = [1]$, and $[a]$ is a unit. So (F8) holds, and $\mathbb{Z}/p\mathbb{Z}$ is a field.

Is the claim true? Does the argument prove it? Name the line that fails and the reason, give a counterexample to the illegal step, and repair the argument.

Solution (Hint 1). List the properties of $\mathbb{Z}/p\mathbb{Z}$ that each line uses. Which of them have been proved in this chapter, and which are things a field has?

Solution (Hint 2). Write $[a][x] = [a][y]$ as a divisibility statement about integers.

Solution. **The claim is true:** it is [Theorem 3.5.2](#). **The argument does not prove it as written.**

Line (2) fails. “Cancel a non-zero factor” is a rule of fields (multiply by the inverse) or of rings without zero divisors, and neither has been established for $\mathbb{Z}/p\mathbb{Z}$: it is close to what the argument is trying to prove, and it is false in general. So the line cites a “fact” that is neither proved nor true, entry (N9) of Logic and Proof, Example (What is not allowed). Counterexample to the step: in $\mathbb{Z}/6\mathbb{Z}$, $[2][1] = [2]$ and $[2][4] = [8] = [2]$, so $[2][1] = [2][4]$ with $[2] \neq [0]$, yet $[1] \neq [4]$. There is no counterexample to the conclusion.

Repair of line (2). If $[a][x] = [a][y]$, then $[a(x - y)] = [0]$, so $p \mid a(x - y)$ by the class test. Since $[a] \neq [0]$, $p \nmid a$, so $p \mid x - y$ by Corollary 3.3.2 (b), and $[x] = [y]$. This uses that p is prime, the hypothesis the flawed line never touched. With this repair, the argument is a correct second proof.

Marking scheme. (10 points) - 2: says the claim is true and the argument, as written, does not prove it. - 3: names line (2) and the reason: cancellation by a non-zero class is unproved here and false in general, (N9), or an equivalent statement of the reason. - 2: a counterexample to the step, such as $[2][1] = [2][4]$ in $\mathbb{Z}/6\mathbb{Z}$. - 3: repairs line (2) without assuming the field property: $p \mid a(x - y)$ by the class test and Euclid’s lemma for a prime (Corollary 3.3.2 (b), from Theorem 3.3.1); or $\gcd(a, p) = 1$ (Corollary 3.3.2 (a)) and an inverse of $[a]$ from [Theorem 3.5.1](#), which earns full points even though it makes lines (3)–(5) redundant. Fatal errors (0 for the step): a counterexample to the conclusion (there is none); a repair that cancels $[a]$ by appeal to the field property being proved (citing [Theorem 3.5.1](#) is not such an appeal).

Exercise. C3

Find every $x \in \mathbb{Z}$ with

$$x \equiv 1 \pmod{3}, \quad x \equiv 2 \pmod{5}, \quad x \equiv 3 \pmod{7},$$

by applying [Theorem 3.5.3](#) twice.

Solution. The first two congruences. $1 = 2 \cdot 3 + (-1) \cdot 5$, so $\gcd(3, 5) = 1$ (Corollary 3.2.2), with $m = 3$, $n = 5$, $u = 2$, $v = -1$. By [Theorem 3.5.3](#) (a),

$$x_1 = 1 \cdot 5 \cdot (-1) + 2 \cdot 3 \cdot 2 = -5 + 12 = 7,$$

and an integer satisfies the first two congruences **if and only if** it is $\equiv 7 \pmod{15}$.

Adding the third. So the three congruences together say exactly $x \equiv 7 \pmod{15}$ and $x \equiv 3 \pmod{7}$. Now $1 = 1 \cdot 15 + (-2) \cdot 7$, so $\gcd(15, 7) = 1$, with $m = 15$, $n = 7$, $u = 1$, $v = -2$. By [Theorem 3.5.3](#) (a) again,

$$x_2 = 7 \cdot 7 \cdot (-2) + 3 \cdot 15 \cdot 1 = -98 + 45 = -53,$$

and the solutions are the $x \equiv -53 \pmod{105}$, that is, the class $52 + 105\mathbb{Z}$.

Check: $52 = 17 \cdot 3 + 1 = 10 \cdot 5 + 2 = 7 \cdot 7 + 3$. (Coprimalty of 3 and 5, and of 15 and 7, also follows from the small-primes remark of Section 3.1 with Corollary 3.3.2 (a).) The “if and only if” in the first step is what allows replacing two congruences by one; with “if” alone, the second step could lose solutions.

3.5.5.4 R. Review
Exercise. R1

Let $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$ be the integers built as classes of pairs, with $(a, b) \sim (c, d) \iff a + d = b + c$. Show that $[(a, b)] \mapsto [a + b]_2$ is a well-defined function $\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$, and identify it.

Solution. This is the method of Theorem 2.2.1 (a), from the construction Definition 2.1.1. Take $X = \mathbb{N} \times \mathbb{N}$ with $\sim$, $Y = \mathbb{Z}$ with congruence modulo 2, the equivalence relation $\sim_{2\mathbb{Z}}$ whose quotient set is $\mathbb{Z}/2\mathbb{Z}$ (Definition 3.4.2, Theorem 3.4.1 (a)), and $f(a, b) := a + b$. Let $(a, b) \sim (a', b')$, so $a + b' = a' + b$. Then, in $\mathbb{Z}$,

$$\begin{aligned} (a + b) - (a' + b') &= (a + b' - a' - b) + 2b - 2b' \\ &= 0 + 2(b - b'), \end{aligned}$$

so $a + b \equiv a' + b' \pmod{2}$. By Theorem 2.2.1 (a) there is exactly one function $F: \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$ with $F([(a, b)]) = [a + b]_2$.

Identification. By the remark after Theorem 2.3.1, $[(a, b)] = a - b$ in $\mathbb{Z}$. Since $(a + b) - (a - b) = 2b$, $[a + b]_2 = [a - b]_2$ by the class test. So $F(z) = [z]_2$ for every $z \in \mathbb{Z}$: F is the quotient map of $\mathbb{Z}/2\mathbb{Z}$, which sends an integer to its parity class.

Exercise. R2

Let $m, n, m', n' \in \mathbb{N}$ with $2^m 3^n = 2^{m'} 3^{n'}$. Prove that $m = m'$ and $n = n'$. Conclude that $(m, n) \mapsto 2^m 3^n$ is injective on $\mathbb{N} \times \mathbb{N}$.

Solution. The tool is unique factorization, Theorem 3.3.5. The powers are those of $\mathbb{N} = \omega$ (Proposition 1.6.4), carried into $\mathbb{Z}$, which preserves products (Proposition 2.2.3); $b^0 = 1$ and $b^{j+1} = b^j \cdot b$.

A factorization. For $m, n \in \mathbb{N}$, let $L_{m,n}$ be the list of length $m+n$ whose first m entries are 2 and whose last n entries are 3. Its entries are prime, by the small-primes remark of Section 3.1, and it is non-decreasing, since $2 \leq 3$. Its product is $2^m 3^n$. Indeed, with P_j the product of the first j entries, the recursion of Definition 3.3.1 and induction on $j \leq m$ give $P_j = 2^j$ ($P_0 = 1 = 2^0$; $P_{j+1} = P_j \cdot 2 = 2^{j+1}$), and then induction on $i \leq n$ gives $P_{m+i} = 2^m 3^i$. So $L_{m,n}$ is a prime factorization of $2^m 3^n$, which is positive, being a product of positive integers (Proposition 2.3.5 (c)).

Uniqueness. If $2^m 3^n = 2^{m'} 3^{n'}$, then $L_{m,n}$ and $L_{m',n'}$ are prime factorizations of the same positive integer, so they are equal (Theorem 3.3.5): $m+n = m'+n'$, with equal entries. Suppose $m < m'$. Then the entry of index m' is 2 in $L_{m',n'}$, and in $L_{m,n}$ it is 3, since $m < m' \leq m+n$: a contradiction. Exchanging the two lists rules out $m' < m$. So $m = m'$, and then $n = n'$ by canceling m in $m+n = m'+n'$.

This is line (vii) of Sets, Relations, and Cardinality, Exercise (B2: Putting a proof in order), which was not available when that exercise was set; Sets, Relations, and Cardinality, Theorem 3.2.6 proves the same injectivity by parity instead.

Exercise. R3

Prove that no $x \in \mathbb{Q}$ satisfies $x^2 = 2$, by the parity argument: write x as a fraction and show that numerator and denominator are both even. Then show that, for every prime p , no $x \in \mathbb{Q}$ satisfies $x^2 = p$.

Solution. This is the school argument of Logic and Proof, Theorem 2.2.1, now with every step citable.

The case 2. Suppose $x \in \mathbb{Q}$ and $x^2 = 2$. By Proposition 3.3.6, $x = a/b$ with $a \in \mathbb{Z}$, $b \in \mathbb{Z}_{>0}$ and $\gcd(a, b) = 1$. By Definition 2.4.2, $x^2 = a^2/b^2$, and $2 = 2/1$, so $a^2 = 2b^2$ (Proposition 2.4.4 (b)). Then a^2 is even, so a is even by Corollary 3.1.3 (b): $a = 2c$ with $c \in \mathbb{Z}$. Then $4c^2 = 2b^2$, and canceling the non-zero factor 2 (Proposition 2.3.5 (f), applied to $2(b^2 - 2c^2) = 0$) gives $b^2 = 2c^2$. So b is even as well. Now 2 divides a and b , hence divides $\gcd(a, b) = 1$ (Theorem 3.2.1 (c), (d)), so $2 \in \{1, -1\}$ (Proposition 3.1.1 (g)): a contradiction.

A prime p . The same argument works with “ $p \mid$ ” in place of “even”: from $a^2 = pb^2$, $p \mid a \cdot a$, so $p \mid a$ by Corollary 3.3.2 (b); $a = pc$ gives $p^2 c^2 = pb^2$, so $b^2 = pc^2$ (cancel $p \neq 0$), and $p \mid b$ in the same way. Then $p \mid \gcd(a, b) = 1$, against $p \geq 2$.

Comparison. Chapter 2’s proof, Theorem 2.6.1, needed neither parity nor gcd: it descended to a smaller denominator using order alone. The argument here is shorter, but it stands on

lowest terms, and lowest terms stands on Bézout (Proposition 3.3.6 uses Corollary 3.2.2).

Exercise. R4

Find all $x \in \mathbb{Z}$ with $6x \equiv 4 \pmod{10}$.

Solution. Answer: the class $4 + 5\mathbb{Z}$.

The tool is to divide the congruence by $\gcd(6, 10) = 2$, and then invert a unit ([Theorem 3.5.1](#)). Since $6x - 4 = 2(3x - 2)$ and $10 = 2 \cdot 5$,

$$10 \mid 6x - 4 \iff 5 \mid 3x - 2 :$$

if $2(3x - 2) = 10k = 2(5k)$, cancel $2 \neq 0$ (Proposition 2.3.5 (f)); conversely, multiply $3x - 2 = 5k$ by 2. So the condition is $[3][x] = [2]$ in $\mathbb{Z}/5\mathbb{Z}$. There $[3]^{-1} = [2]$, since $3 \cdot 2 = 6 = 5 + 1$. Multiplying by $[2]$, $[x] = [2][2] = [4]$; and conversely $[3][4] = [12] = [2]$. So the solutions are exactly the $x \equiv 4 \pmod{5}$. Check: $6 \cdot 4 - 4 = 20$ and $6 \cdot 9 - 4 = 50$ are multiples of 10.

Why the look-alikes fail. “Multiply by $[6]^{-1}$ in $\mathbb{Z}/10\mathbb{Z}$ ” fails: $\gcd(6, 10) = 2$, so $[6]$ is not a unit there ([Theorem 3.5.1](#)). Canceling the 2 from every term but keeping the modulus gives $3x \equiv 2 \pmod{10}$, and that is wrong: it keeps 4 and loses 9 ($6 \cdot 9 - 4 = 50$, while $3 \cdot 9 - 2 = 25$). The modulus must be divided too. The Chinese remainder theorem is not a look-alike that fails: splitting $10 = 2 \cdot 5$, [Theorem 3.5.3](#) (b) turns the condition $[6]_{10}[x]_{10} = [4]_{10}$ into $[0]_2[x]_2 = [0]_2$, which always holds, and $[x]_5 = [4]_5$, since $[6]_5 = [1]_5$; so it is a second route to the same answer. Note also that the answer is a class modulo 5, not modulo 10: it is the two classes $[4]_{10}$ and $[9]_{10}$.