

3.3 Euclid's Lemma and the Fundamental Theorem of Arithmetic

Section 3.2 gave every pair of integers, not both zero, a greatest common divisor, and wrote it as a combination $ax + by$ (Theorem 3.2.1). This section spends that identity. Take 60. It splits as $2 \cdot 30$, as $6 \cdot 10$, as $4 \cdot 15$, and every way of splitting it further, until no factor splits again, ends with the same primes 2, 2, 3, 5. *Sets, Relations, and Cardinality*, Section 2.2 proved, for the school integers, that every integer at least 2 has a prime factor, and set the uniqueness of the full splitting aside. Here we prove both, for the integers of Chapter 2. The key is a property of primes that the definition ("no positive divisors except 1 and itself") does not obviously give: a prime that divides a product divides one of the factors.

As in Section 3.1, numerals are the natural numbers of those names, and their sums and products may be computed in $\mathbb{N}$ (Proposition 2.2.3 (a)).

3.3.1 Euclid's lemma

The definition of a prime p speaks about the divisors **of** p . The property we want speaks about the numbers that p **divides**. Something has to connect the two, and the connection is the Bézout identity of Section 3.2. We first prove a version for any divisor that shares no factor with one of the two numbers multiplied.

Theorem 3.3.1. Euclid's Lemma

Let $a, b, c \in \mathbb{Z}$. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

Idea. The hypothesis $\gcd(a, b) = 1$ is a statement about common divisors, which is hard to use directly. By Corollary 3.2.2 it is the same as an equation $1 = ax + by$, and an equation can be multiplied. Multiplying it by c writes c as $acx + bcy$. The first term is a multiple of a on sight, and the second is one because bc is.

Proof. Suppose $a \mid bc$ and $\gcd(a, b) = 1$. By Corollary 3.2.2 there are $x, y \in \mathbb{Z}$ with $ax + by = 1$. Since $a \mid bc$, there is $k \in \mathbb{Z}$ with $bc = ka$ (*Sets, Relations, and Cardinality*, Definition 2.2.1). Multiplying the identity by c , with (F7), (F9), (F5) and (F6),

$$c = c(ax + by) = a(cx) + (bc)y = a(cx) + a(ky) = a(cx + ky).$$

Since $cx + ky \in \mathbb{Z}$, this shows $a \mid c$. ■

We call the move of this proof **multiply the Bézout identity**: from $1 = ax + by$, multiply by c and read off what divides c . It turns a statement about divisors into an equation, which is where the work can be done.

Each hypothesis has a job. Without $\gcd(a, b) = 1$ the conclusion fails: $4 \mid 2 \cdot 6 = 12$, but $4 \nmid 6$, since $6 = 1 \cdot 4 + 2$ leaves a non-zero remainder (uniqueness in Theorem 3.1.2 (a)); here $\gcd(4, 2) = 2$. The common factor 2 of 4 and 2 let 4 divide the product without dividing 6.

3.3.2 Lists, products and prime factorizations

To say that a factorization is unique, we must first say what a factorization is. The products $2 \cdot 2 \cdot 3 \cdot 5$ and $3 \cdot 2 \cdot 5 \cdot 2$ are equal and use the same primes, and we want to count them as one. We do so by writing the primes in order, smallest first. A factorization also has a length, and the length may be 0: the number 1 is the product of no primes at all.

Products of lists are defined by the recursion of Sets, Relations, and Cardinality, Definition 2.3.1. That definition was made for sequences of real numbers, and we use it as a pattern, as group (iii) of the citing rule of Section 1.7 allows, with the ordered field $\mathbb{Q}$ (Theorem 2.5.1) in place of $\mathbb{R}$. A product of integers is an integer (Proposition 2.4.4), so the products of lists below lie in $\mathbb{Z}$; the paragraph “Why the product exists” below checks directly that the recursion runs in $\mathbb{Z}$.

Definition 3.3.1. List, Product of a List, Prime Factorization

Let $k \in \mathbb{N}$. A **list** of length k in $\mathbb{Z}$ is a function $p: \{1, \dots, k\} \rightarrow \mathbb{Z}$, written $(p_1, \dots, p_k)$ with $p_i := p(i)$; for $k = 0$ it is the **empty list**. Its **product** $\prod_{i=1}^k p_i \in \mathbb{Z}$ is given by the recursion

$$\prod_{i=1}^0 p_i = 1, \quad \prod_{i=1}^{j+1} p_i = \left(\prod_{i=1}^j p_i \right) p_{j+1} \quad \text{for } j < k,$$

where $\prod_{i=1}^j p_i$ is the product of the shortened list $(p_1, \dots, p_j)$.

A **prime factorization** of $n \in \mathbb{Z}_{>0}$ is a list $(p_1, \dots, p_k)$ such that **every** entry p_i is prime (Sets, Relations, and Cardinality, Definition 2.2.2), the list is **non-decreasing** ($i \leq j$ implies $p_i \leq p_j$), and $\prod_{i=1}^k p_i = n$.

In words: a list is a finite sequence of integers, possibly empty; its product starts at 1 and multiplies by one more entry at each stage; and a prime factorization lists primes in non-decreasing order with the right product.

Why the product exists. Extend the list to a sequence $\bar{p}$ on $\mathbb{Z}_{>0}$ by $\bar{p}_i := p_i$ for $i \leq k$ and $\bar{p}_i := 1$ for $i > k$. Then Sets, Relations, and Cardinality, Theorem 2.3.1, read on $\mathbb{N} = \omega$ through Corollary 1.7.3 (b), with $X = \mathbb{Z}$, starting value 1 and step $g(j, x) := x\bar{p}_{j+1}$, gives exactly one function $P: \mathbb{N} \rightarrow \mathbb{Z}$ with $P_0 = 1$ and $P_{j+1} = P_j \bar{p}_{j+1}$; we set $\prod_{i=1}^j p_i := P_j$ for $j \leq k$. The “Finite lists” remark after Sets, Relations, and Cardinality, Definition 2.3.1 shows that P_j depends only on $p_1, \dots, p_j$, not on how the list was extended. Its proof is an induction on j that uses only the recursion and the multiplication of the target set, so it runs unchanged in $\mathbb{Q}$, and, since $\mathbb{Z}$ is closed under multiplication, with target set $\mathbb{Z}$. In particular P_j is also the product of the shortened list $(p_1, \dots, p_j)$, which is the displayed recursion. We cite it as **the recursion of Definition 3.3.1**: it peels the **last** entry off a product.

Examples.

- $(2, 2, 3, 5)$ is a prime factorization of 60. Its entries are prime by the small-primes remark of Section 3.1; it is non-decreasing; and the recursion gives the products 1, 2, 4, 12, 60.
- (5) is a prime factorization of 5, with products 1, 5. A prime p has the one-entry factorization (p) .
- The degenerate case: the empty list is a prime factorization of 1. Its product is 1 by the first clause of the recursion, and the conditions “every entry is prime” and “non-decreasing” hold vacuously. Without this case the number 1 would have no factorization, and the theorem below would fail for $n = 1$; its existence proof uses this case to rule out $n = 1$.

Non-examples by minimal change. Exchange two entries of the first example: $(2, 3, 2, 5)$ has prime entries and product 60, but it is not non-decreasing, since positions $2 \leq 3$ carry $3 > 2$. Merge two entries: $(2, 2, 15)$ is non-decreasing with product 60, but $15 = 3 \cdot 5$ is not prime.

Why these clauses. Without “non-decreasing”, 60 would have twelve factorizations, its four primes in every order, and uniqueness could only be stated up to rearrangement, which needs a theory of permutations. Without “prime”, splitting would stop anywhere. And the requirement $p \geq 2$ in Sets, Relations, and Cardinality, Definition 2.2.2 is what keeps $(1, 2, 2, 3, 5)$ out: if 1 counted as a prime, every factorization could be padded with as many 1s as we like.

Quick check. Find the prime factorization of 360, and check each clause of Definition 3.3.1.

Solution. $(2, 2, 2, 3, 3, 5)$. Its entries are prime by the small-primes remark of Section 3.1. It is non-decreasing. Its products, by the recursion, are 1, 2, 4, 8, 24, 72, 360. By the theorem below there is no other.

3.3.3 Primes dividing products

For a prime, the coprimality that Euclid’s lemma asks for comes almost free: a prime shares no factor with a number unless it divides that number.

Corollary 3.3.2. A Prime Dividing a Product

Let p be prime.

- (a) For every $a \in \mathbb{Z}$: $p \mid a$ or $\gcd(p, a) = 1$.
- (b) For all $b, c \in \mathbb{Z}$: if $p \mid bc$, then $p \mid b$ or $p \mid c$.
- (c) If $(q_1, \dots, q_l)$ is a list of primes, with $l \in \mathbb{N}$, and $p \mid \prod_{j=1}^l q_j$, then $p = q_j$ for some $j \in \{1, \dots, l\}$.

Idea. For (a), the gcd of p and a is a positive divisor of p , so it is 1 or p , and the second case says $p \mid a$. Then (b) is Euclid’s lemma in the case $\gcd(p, b) = 1$ of (a). For (c), peel the last prime off the product and apply (b) to the two factors; an induction on the length handles the rest, and a prime that divides a prime is equal to it.

Proof. (a) Since $p \geq 2$, $(p, a) \neq (0, 0)$, so $g := \gcd(p, a) \geq 1$ (Definition 3.2.2). As a common divisor, $g \mid p$ and $g \mid a$. So g is a positive divisor of the prime p , and $g = 1$ or $g = p$ (Sets, Relations, and Cardinality, Definition 2.2.2). If $g = p$, then $p \mid a$.

(b) Let $p \mid bc$. By (a), $p \mid b$ or $\gcd(p, b) = 1$. In the second case Theorem 3.3.1, with $a = p$, gives $p \mid c$.

(c) We use Logic and Proof, Axiom 4.2.1 (through Corollary 1.7.3 (b)) on l , for $P(l)$: “for every list of primes $(q_1, \dots, q_l)$, if $p \mid \prod_{j=1}^l q_j$, then $p = q_j$ for some $j \leq l$ ”.

Base case $P(0)$. The empty product is 1 (the recursion of Definition 3.3.1). If $p \mid 1$, then $p = 1$ or $p = -1$ (Proposition 3.1.1 (g)), and both contradict $p \geq 2$. So the hypothesis of

$P(0)$ never holds, and $P(0)$ is true.

Step. Assume $P(l)$, and let $(q_1, \dots, q_{l+1})$ be a list of primes with $p \mid \prod_{j=1}^{l+1} q_j$. By the recursion of [Definition 3.3.1](#),

$$\prod_{j=1}^{l+1} q_j = \left(\prod_{j=1}^l q_j \right) q_{l+1},$$

where the first factor is the product of the list of primes $(q_1, \dots, q_l)$. By (b), p divides that first factor or $p \mid q_{l+1}$. In the first case $P(l)$ gives $j \leq l$ with $p = q_j$. In the second, $p \geq 2 > 0$ is a positive divisor of the prime q_{l+1} , so $p \in \{1, q_{l+1}\}$, and $p \neq 1$; hence $p = q_{l+1}$. This proves $P(l+1)$, and with it the corollary. ■

Part (b) is the property promised at the start of the section, and it is what makes primes the right atoms for multiplication. It fails for 6, which is not prime: $6 \mid 2 \cdot 3$, but $6 \nmid 2$ and $6 \nmid 3$, since $0 < 2 < 6$ and $0 < 3 < 6$ rule both out by Proposition 3.1.1 (e).

The second application of Euclid's lemma combines two coprime divisors into one.

Proposition 3.3.3. Coprime Divisors of a Number

Let $m, n, c \in \mathbb{Z}$ with $m \mid c$, $n \mid c$ and $\gcd(m, n) = 1$. Then $mn \mid c$.

Proof. Write $c = km$ with $k \in \mathbb{Z}$. Then $n \mid km$, and $\gcd(n, m) = \gcd(m, n) = 1$ (Definition 3.2.2), so [Theorem 3.3.1](#) gives $n \mid k$, say $k = ln$ with $l \in \mathbb{Z}$. Hence $c = (ln)m = l(mn)$, by (F5) and (F6), and $mn \mid c$. ■

The coprimality is needed: $4 \mid 12$ and $6 \mid 12$, but $24 \nmid 12$, since a positive divisor of 12 is at most 12 (Proposition 3.1.1 (e)); here $\gcd(4, 6) = 2$.

3.3.4 The least divisor is prime

The existence half of unique factorization needs a supply of primes: every integer $n \geq 2$ must have a prime factor. *Sets, Relations, and Cardinality*, Section 2.2 proved this for the school integers by strong induction (*Sets, Relations, and Cardinality*, Theorem 2.2.5). On the constructed $\mathbb{Z}$ the least-element property gives a shorter route: the least divisor bigger than 1 is already prime.

Lemma 3.3.4. The Least Divisor Is Prime

Let $n \in \mathbb{Z}$ with $n \geq 2$. The set $D := \{d \in \mathbb{Z} : d \geq 2 \text{ and } d \mid n\}$ has a least element, and that element is prime. In particular, n has a prime factor.

Proof. Since $n \geq 2$ and $n \mid n$ (Proposition 3.1.1 (a)), $n \in D$, so D is non-empty; and 2 is a lower bound of D by its definition. By Proposition 2.3.6, D has a least element p .

Suppose p were not prime. Since $p \geq 2$, the clause of *Sets, Relations, and Cardinality*,

Definition 2.2.2 that fails is the one about divisors: p has a positive divisor e with $e \neq 1$ and $e \neq p$. Then $e \geq 1$ by discreteness (Theorem 2.3.4 (c)), and $e \leq p$ by Proposition 3.1.1 (e). So $1 < e < p$, and $e \geq 2$ by discreteness again. Also $e \mid p$ and $p \mid n$ give $e \mid n$ (Proposition 3.1.1 (b)). So $e \in D$ and $e < p$, against the choice of p . Hence p is prime, and $p \mid n$ because $p \in D$. ■

Remark. This is Sets, Relations, and Cardinality, Theorem 2.2.5 on the constructed $\mathbb{Z}$, proved by a least element instead of strong induction. It also shortens the primality test of Section 3.1's small-primes remark. If $p \geq 2$ is not prime, its least divisor $e \geq 2$ is prime by the lemma, so it is not p itself, and $p = ef$ with $f \in \mathbb{Z}$; then $f > 0$ (as $e, p > 0$), $f \neq 1$, so $f \geq 2$ and $f \mid p$, and therefore $e \leq f$ by the choice of e . Multiplying by $e > 0$ gives $e \cdot e \leq ef = p$ (Proposition 2.3.5 (c), or equality if $e = f$). So to prove $p \geq 2$ prime it is enough to check that **no** d with $d \geq 2$ and $d \cdot d \leq p$ divides p . For 11 only $d = 2, 3$ need checking, since $4 \cdot 4 = 16 > 11$.

3.3.5 The fundamental theorem

Everything is now in place for the main result of the chapter's first half.

Theorem 3.3.5. Fundamental Theorem of Arithmetic

Every $n \in \mathbb{Z}_{>0}$ has **exactly one** prime factorization.

Idea. Existence. Take the least n with no factorization. It is at least 2, so it has prime factors, and a largest one, p . Then $n = pm$ with $m < n$, so m has a factorization. Every entry of it divides n , so it is at most p , and appending p at the end keeps the list non-decreasing.

Uniqueness. Take two factorizations with the same product, $(p_1, \dots, p_k)$ and $(q_1, \dots, q_l)$. The largest entry p_k divides the product of the q 's, so by Corollary 3.3.2 (c) it is one of the q_j , and that is at most the largest, q_l . By symmetry $q_l \leq p_k$. So the two last entries are equal; cancel them and induct on the length.

Before reading on: why compare the largest primes, p_k and q_l , and not the first ones?

Proof. Existence. Let $B := \{n \in \mathbb{Z}_{>0} : n \text{ has no prime factorization}\}$, and suppose $B \neq \emptyset$. It has the lower bound 0, so it has a least element n (Proposition 2.3.6). The empty list is a prime factorization of 1, so $n \neq 1$; as $n \geq 1$ (discreteness, Theorem 2.3.4 (c)), $n > 1$, and so $n \geq 2$ by discreteness.

The set F of prime factors of n is non-empty by Lemma 3.3.4. Each $q \in F$ is positive and divides $n > 0$, so $q \leq n$ (Proposition 3.1.1 (e)). By Proposition 2.3.6, F has a greatest element p . Write $n = mp$ with $m \in \mathbb{Z}$. If $m \leq 0$, then $mp \leq 0$ ($m = 0$: Proposition 2.3.2 (b); $m < 0$: $mp < 0 \cdot p = 0$ by Proposition 2.3.5 (c)), against $n > 0$. So $m > 0$, that is, $m \in \mathbb{Z}_{>0}$ (Theorem 2.3.4 (b)). Moreover $m < n$: since $p \geq 2$ and $m > 0$, $n = pm \geq 2m = m + m > m$, by Proposition 2.3.5 (c) (or equality if $p = 2$), (F9) with (F7), and (O3).

By the minimality of n , $m \notin B$: let $(q_1, \dots, q_l)$ be a prime factorization of m . If $l \geq 1$, the recursion of [Definition 3.3.1](#) gives $m = (\prod_{j=1}^{l-1} q_j)q_l$, so $q_l \mid m$; with $m \mid n$ this gives $q_l \mid n$ (Proposition 3.1.1 (b)), so $q_l \in F$ and $q_l \leq p$. As the list is non-decreasing, $q_i \leq q_l \leq p$ for every $i \leq l$. Now let $(q_1, \dots, q_l, p)$ be the list of length $l + 1$ whose first l entries are those of $(q_1, \dots, q_l)$ and whose last entry is p . Its entries are prime. It is non-decreasing: two positions among the first l compare as before, and every entry is at most p (for $l = 0$ it is the one-entry list (p) , and there is nothing to check). By the recursion its product is

$$\left(\prod_{j=1}^l q_j\right)p = mp = n.$$

So n has a prime factorization, against $n \in B$. Hence $B = \emptyset$.

Uniqueness. We prove, by Logic and Proof, Axiom 4.2.1 (through Corollary 1.7.3 (b)) on k , the statement $P(k)$: “for every $l \in \mathbb{N}$, if $(p_1, \dots, p_k)$ and $(q_1, \dots, q_l)$ are non-decreasing lists of primes with $\prod_{i=1}^k p_i = \prod_{j=1}^l q_j$, then $l = k$ and $p_i = q_i$ for every $i \leq k$ ”. Two prime factorizations of the same n are such lists, so $P(k)$ for every k gives the uniqueness.

First, a non-empty list of primes $(r_1, \dots, r_h)$ does not have product 1: by the recursion its product is $(\prod_{i=1}^{h-1} r_i)r_h$, so r_h would divide 1, and $r_h = \pm 1$ (Proposition 3.1.1 (g)) contradicts $r_h \geq 2$.

Base case $P(0)$. If $k = 0$, then $\prod_{j=1}^l q_j = 1$, so $l = 0$ by the previous paragraph, and both lists are empty.

Step. Assume $P(k)$. Let $(p_1, \dots, p_{k+1})$ and $(q_1, \dots, q_l)$ be non-decreasing lists of primes with the same product N . Since $k+1 \geq 1$, $N \neq 1$, so $l \geq 1$. By the recursion, $p_{k+1} \mid N = \prod_{j=1}^l q_j$, so [Corollary 3.3.2](#) (c) gives $p_{k+1} = q_j$ for some $j \leq l$, and $q_j \leq q_l$ because the q -list is non-decreasing. In the same way $q_l \mid N = \prod_{i=1}^{k+1} p_i$ gives $q_l = p_i \leq p_{k+1}$ for some $i \leq k+1$. So $p_{k+1} \leq q_l \leq p_{k+1}$, and $p_{k+1} = q_l$ (Proposition 2.3.5 (i)). By the recursion,

$$\left(\prod_{i=1}^k p_i\right)p_{k+1} = N = \left(\prod_{j=1}^{l-1} q_j\right)p_{k+1}.$$

Subtracting, $(\prod_{i=1}^k p_i - \prod_{j=1}^{l-1} q_j)p_{k+1} = 0$ by (F9) and Proposition 2.3.2 (c), and $p_{k+1} \neq 0$, so the bracket is 0 (Proposition 2.3.5 (f)). The shortened lists $(p_1, \dots, p_k)$ and $(q_1, \dots, q_{l-1})$ are non-decreasing lists of primes with equal products, so $P(k)$, applied with $l-1 \in \mathbb{N}$, gives $l-1 = k$ and $p_i = q_i$ for $i \leq k$. With $p_{k+1} = q_l = q_{k+1}$, the two lists have the same length $k+1$ and the same entries, so they are equal (Sets, Relations, and Cardinality, Proposition 1.4.1). This proves $P(k+1)$, and the theorem. ■

The answer to the prompt lies in the recursion of [Definition 3.3.1](#). It peels off the **last** factor, so once the two last entries are known to be equal they can be canceled at once, leaving two shortened lists to which $P(k)$ applies. And the comparison “largest with largest” needs only that both lists are non-decreasing. Comparing the first entries would also show $p_1 = q_1$, but removing a first entry shifts every index, and the recursion says nothing directly about that.

Remark. *Sets, Relations, and Cardinality*, Section 2.2 named unique factorization as a fact it did not prove or use, and *Sets, Relations, and Cardinality*, Exercise (B2: Putting a proof in order) lists, as line (vii), a step that cites it and is therefore not available there. On the

constructed $\mathbb{Z}$ the fact is now proved, and Exercise R2 of Section 3.5 uses it.

Warning. Uniqueness is not automatic. Let $H := \{4k+1 : k \in \mathbb{N}\} = \{1, 5, 9, 13, 17, 21, \dots\}$. It is closed under multiplication, since $(4k+1)(4l+1) = 4(4kl+k+l)+1$. Call $h \in H$ with $h > 1$ an **H -prime** if it is not a product of two elements of H both greater than 1. Then 9, 21 and 49 are H -primes, and

$$441 = 9 \cdot 49 = 21 \cdot 21$$

gives two different factorizations into H -primes. What breaks is Euclid's lemma: 9 divides $21 \cdot 21$ inside H , but $9 \nmid 21$. The proof of [Theorem 3.3.1](#) wrote $1 = ax + by$, with **sums** and with negative coefficients, and H is closed under neither. The proof of uniqueness above is only as good as Euclid's lemma.

3.3.6 Lowest terms

Every rational number is a fraction in many ways: $6/4 = 3/2 = 9/6$. Section 2.4 found, in its Exercise C1, a least positive denominator by the least-element property, and *Sets, Relations, and Cardinality*, Section 2.2 removed common factors of 2 only (Sets, Relations, and Cardinality, Lemma 2.2.4). With the gcd we can remove every common factor at once, and Euclid's lemma shows that the result is unique. Recall that after the identification of Section 2.4, $p/q := pq^{-1}$ in $\mathbb{Q}$ for $p \in \mathbb{Z}$ and $q \in \mathbb{Z}_{>0}$, and $p/q = r/s$ holds if and only if $ps = rq$ (Proposition 2.4.4 (b)).

Proposition 3.3.6. Lowest Terms

Let $x \in \mathbb{Q}$.

- (a) There are $p \in \mathbb{Z}$ and $q \in \mathbb{Z}_{>0}$ with $x = p/q$ and $\gcd(p, q) = 1$, and the pair (p, q) is **unique**.
- (b) If $x = r/s$ with $r \in \mathbb{Z}$ and $s \in \mathbb{Z}_{>0}$, then $r = tp$ and $s = tq$ for some $t \in \mathbb{Z}_{>0}$. In particular $q \mid s$ and $q \leq s$: q is the least positive denominator of x .

Idea. For existence, divide numerator and denominator by their gcd d ; the Bézout identity for d , divided by d , is a Bézout identity $1 = px_0 + qy_0$ for the new pair. For (b), cross-multiplying gives $ps = rq$, so $q \mid ps$, and Euclid's lemma removes p . Uniqueness is (b) applied to a second coprime pair.

Proof. Existence in (a). By Proposition 2.4.4 (b), $x = r/s$ for some $r \in \mathbb{Z}$, $s \in \mathbb{Z}_{>0}$. Since $s \neq 0$, $d := \gcd(r, s) \geq 1$, and by Theorem 3.2.1 (d) there are $x_0, y_0 \in \mathbb{Z}$ with $d = rx_0 + sy_0$. As $d \mid r$ and $d \mid s$, write $r = dp$ and $s = dq$ with $p, q \in \mathbb{Z}$. If $q \leq 0$, then $dq \leq 0$ (as in the existence proof of [Theorem 3.3.5](#)), against $s > 0$; so $q \in \mathbb{Z}_{>0}$. Now

$$d \cdot 1 = d = (dp)x_0 + (dq)y_0 = d(px_0 + qy_0),$$

so $d(px_0 + qy_0 - 1) = 0$, and since $d \neq 0$, $px_0 + qy_0 = 1$ (Proposition 2.3.5 (f)). Hence $\gcd(p, q) = 1$ by Corollary 3.2.2. Finally $rq = dpq = p(dq) = ps$, so $r/s = p/q$ by Proposition 2.4.4 (b), and $x = p/q$.

(b), for any such pair. Let $x = p/q$ with $\gcd(p, q) = 1$, and $x = r/s$ with $s > 0$. By Proposition 2.4.4 (b), $ps = rq$. So $q \mid ps$, and $\gcd(q, p) = 1$, hence $q \mid s$ by Theorem 3.3.1; write $s = tq$ with $t \in \mathbb{Z}$. Since $s > 0$ and $q > 0$, $t > 0$, by the sign argument used for q above. Then $q(pt) = ps = rq$, so $q(pt - r) = 0$, and $r = tp$ because $q \neq 0$ (Proposition 2.3.5 (f)). As q and s are positive, $q \mid s$ gives $q \leq s$ (Proposition 3.1.1 (e)).

Uniqueness in (a). Let (r, s) be a second pair with $x = r/s$, $s > 0$ and $\gcd(r, s) = 1$. By (b), $r = tp$ and $s = tq$ with $t > 0$. So t is a common divisor of r and s , and it divides $\gcd(r, s) = 1$ (Theorem 3.2.1 (c), (d)). Hence $t = 1$ (Proposition 3.1.1 (g), with $t > 0$), and $(r, s) = (p, q)$. ■

So the least denominator $N(x)$ of Section 2.4's Exercise C1 is the q of (a), and every other denominator of x is a multiple of it. For example $252/198$ has $\gcd(252, 198) = 18$ (Example (Two runs of the algorithm)), and $252 = 18 \cdot 14$, $198 = 18 \cdot 11$, so its lowest terms are $14/11$.

Remark. The twins in *Sets, Relations, and Cardinality*, Section 2.2 are Sets, Relations, and Cardinality, Lemma 2.2.4, which removes only factors of 2, and Sets, Relations, and Cardinality, Exercise (C2: Lowest terms), which asks for lowest terms in the full sense, for the school $\mathbb{Q}$. Proposition 3.3.6 is the full statement, with uniqueness, for the constructed $\mathbb{Q}$.

3.3.7 Exercises

3.3.7.1 A. Check your understanding

Exercise. A1

These questions are about the uniqueness half of the proof of Theorem 3.3.5.

- Why must the empty list count as a prime factorization?
- Run the induction step on $(p_1, p_2, p_3, p_4) = (2, 2, 3, 5)$ and a second prime factorization $(q_1, \dots, q_l)$ of 60. Which equalities does the proof derive, and to which two lists is $P(3)$ applied?
- Which line of the proof uses Euclid's lemma, and through which result?
- Where is "non-decreasing" used?
- Give the idea of the uniqueness proof in two sentences.

Solution.

- Otherwise the number 1 would have no prime factorization, and the theorem would be false for $n = 1$. The existence proof uses it to exclude $n = 1$ from B . (The base case $P(0)$ of the uniqueness proof concerns the empty list as a list of primes with product 1, which it is in any case.)
- The step first gets $l \geq 1$, since the product is $60 \neq 1$. Then $p_4 = 5$ divides $\prod q_j$, so $5 = q_j \leq q_l$ for some j ; and q_l divides $60 = 2 \cdot 2 \cdot 3 \cdot 5$, so $q_l = p_i \leq 5$ for some i . Hence $q_l = 5$. Canceling 5 gives $\prod_{j=1}^{l-1} q_j = 2 \cdot 2 \cdot 3 = 12$, and $P(3)$ is applied to $(2, 2, 3)$ and $(q_1, \dots, q_{l-1})$, which gives $l - 1 = 3$ and $(q_1, q_2, q_3) = (2, 2, 3)$.

- (c) The lines “ $p_{k+1} = q_j$ for some j ” and “ $q_l = p_i$ for some i ”. They cite [Corollary 3.3.2](#) (c), whose step uses (b), which is [Theorem 3.3.1](#) applied with $a = p$.
- (d) In $q_j \leq q_l$ and in $p_i \leq p_{k+1}$: the entry found in the other list is at most that list's last entry.
- (e) The largest prime of one factorization divides the other product, so by Euclid's lemma it is an entry there, hence at most the other's largest; by symmetry the two largest entries are equal. Canceling them leaves two shorter factorizations with equal products, and induction on the length finishes.

3.3.7.2 B. Practice

Exercise. B1: Put the proof in order

The following lines contain a proof of [Theorem 3.3.1](#), shuffled, together with two lines that do not belong. Write the seven correct lines in an order that makes a proof, say which other orders are also admissible, and say why each of the other two lines fails.

- (i) Suppose $a \mid bc$ and $\gcd(a, b) = 1$.
- (ii) There are $x, y \in \mathbb{Z}$ with $ax + by = 1$.
- (ii') Since $\gcd(a, b) = 1$ and $a \mid bc$, we have $a \mid b$ or $a \mid c$.
- (iii) Multiplying by c : $c = acx + bcy$.
- (iii') Dividing $1 = ax + by$ by a : $1/a = x + (b/a)y$.
- (iv) $a \mid acx$, since $acx = a(cx)$.
- (v) Write $bc = ak$; then $bcy = a(ky)$, so $a \mid bcy$.
- (vi) Hence $a \mid acx + bcy$.
- (vii) So $a \mid c$.

Solution. An admissible order is (i), (ii), (iii), (iv), (v), (vi), (vii):

Suppose $a \mid bc$ and $\gcd(a, b) = 1$. There are $x, y \in \mathbb{Z}$ with $ax + by = 1$ (Corollary 3.2.2). Multiplying by c : $c = acx + bcy$. Then $a \mid acx$, since $acx = a(cx)$. Write $bc = ak$; then $bcy = a(ky)$, so $a \mid bcy$. Hence $a \mid acx + bcy$ (Proposition 3.1.1 (c)). So $a \mid c$.

Line (i) comes first, and (ii) needs its hypothesis $\gcd(a, b) = 1$. Lines (iii), (iv) and (v) each need only (ii): (iii) multiplies its equation, and (iv) and (v) mention its x and y ; (v) also uses the hypothesis $a \mid bc$ of (i). None of these three uses another of them. Line (vi) needs both (iv) and (v), but not (iii), since $acx + bcy$ is just an expression in a, b, c, x, y . Line (vii) rewrites (vi) through the equation of (iii), so it needs both and comes last. The admissible orders are therefore those that start (i), (ii), end with (vii), and place (vi) after (iv) and (v); there are eight. For example, (i), (ii), (iv), (v), (vi), (iii), (vii) is admissible: (iii) may come anywhere before (vii).

The distractor (ii') cites a “fact” that is not available as a step for arbitrary a . For a prime a it is [Corollary 3.3.2](#) (b), which is proved **from** this lemma, so citing it here is circular. For a general integer a the line is the lemma itself in a weaker form, so citing it is circular again; only special cases are available (for $a = \pm 1$, $a \mid b$ by Proposition 3.1.1 (a), with (d) for -1), and the proof must work for every a . Either way the line uses what has not been established, which is (N9) of Logic and Proof, Example (What is not allowed).

The distractor (iii') divides in $\mathbb{Z}$, where there is no division: a may be 0 ($\gcd(0, 1) = 1$), and then the line divides by 0; for $a \neq 0$, $1/a$ is not an integer unless $a = \pm 1$. Divisibility is defined by multiplication (Sets, Relations, and Cardinality, Definition 2.2.1), not by fractions.

Exercise. B2: The least common multiple

Let $a, b \in \mathbb{Z}_{>0}$, and let $M := \{m \in \mathbb{Z}_{>0} : a \mid m \text{ and } b \mid m\}$. Prove that M has a least element L , and that $L \mid c$ for **every** $c \in \mathbb{Z}$ with $a \mid c$ and $b \mid c$.

The first part of a proof is given.

$ab > 0$ by (O4), and $a \mid ab$, $b \mid ab$, so $ab \in M$; and 0 is a lower bound of M . By Proposition 2.3.6, M has a least element L . Let $c \in \mathbb{Z}$ with $a \mid c$ and $b \mid c$. By Theorem 3.1.2 (a), $c = qL + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < L$. Since $r = c + (-q)L$, and a divides c and L , $a \mid r$ (Proposition 3.1.1 (c)); likewise $b \mid r$.

The last step is blank. *Name the move, then complete it.*

Solution. The move is **least positive element, then divide**: the remainder lies in the set and is smaller than its least positive element, so it is not positive.

Completion: if $r > 0$, then $r \in \mathbb{Z}_{>0}$ is a common multiple of a and b , so $r \in M$, and $r < L$, against the choice of L . Hence $r = 0$ (as $r \geq 0$), and $c = qL$, that is, $L \mid c$.

The same argument proved Theorem 3.2.1 (b), with the set of positive combinations in place of M . This is the twin of Sets, Relations, and Cardinality, Example (The supremum under divisibility is the least common multiple), now on the constructed $\mathbb{Z}$.

Exercise. B3: Two factorizations and a gcd

Find the prime factorizations of 1001 and of $2^{10} - 1$, proving that each entry is prime. Then show that $\gcd(1001, 1023) = 11$ in two ways. First, use the factorizations to write $1001 = 11 \cdot 91$ and $1023 = 11 \cdot 93$: show $\gcd(91, 93) = 1$, and deduce $\gcd(1001, 1023) = 11$ from a Bézout identity for 91 and 93 (Corollary 3.2.2). Second, use the Euclidean algorithm.

Hint: the remark after Lemma 3.3.4 shortens each primality check. Do not use the school rule “the gcd is the product of the shared primes”: this chapter does not prove it.

Solution. Factorizations. $1001 = 7 \cdot 143 = 7 \cdot 11 \cdot 13$, and $2^{10} - 1 = 1024 - 1 = 1023 = 3 \cdot 341 = 3 \cdot 11 \cdot 31$. So the prime factorizations are $(7, 11, 13)$ and $(3, 11, 31)$, both non-decreasing, once the entries are known to be prime. The primes 3 and 7 are covered by the small-primes remark of Section 3.1. For 11, 13 and 31 we use the remark after Lemma 3.3.4: it suffices that no $d \geq 2$ with $d \cdot d \leq p$ divides p .

- $p = 11$ and $p = 13$: $d \in \{2, 3\}$, since $d \geq 4$ gives $d \cdot d \geq 16$. The divisions $11 = 5 \cdot 2 + 1 = 3 \cdot 3 + 2$ and $13 = 6 \cdot 2 + 1 = 4 \cdot 3 + 1$ leave non-zero remainders.
- $p = 31$: $d \in \{2, 3, 4, 5\}$, since $d \geq 6$ gives $d \cdot d \geq 36$. The divisions $31 = 15 \cdot 2 + 1 = 10 \cdot 3 + 1 = 7 \cdot 4 + 3 = 6 \cdot 5 + 1$ leave non-zero remainders.

A non-zero remainder means $d \nmid p$, by the uniqueness in Theorem 3.1.2 (a). By Theorem 3.3.5 these are the only prime factorizations.

The gcd from the factorizations. We do not use a rule “the gcd is the product of the shared primes”, which this chapter does not prove. We have $1001 = 11 \cdot 91$ and $1023 = 11 \cdot 93$. First, $\gcd(91, 93) = 1$: a common divisor of 91 and 93 divides $93 - 91 = 2$ (Proposition 3.1.1 (c)), so a positive one is 1 or 2 (Proposition 3.1.1 (e) and discreteness), and $2 \nmid 91 = 45 \cdot 2 + 1$. By Corollary 3.2.2, $91x + 93y = 1$ for some $x, y \in \mathbb{Z}$; indeed $91 \cdot 46 - 93 \cdot 45 = 4186 - 4185 = 1$. Multiplying by 11,

$$1001 \cdot 46 - 1023 \cdot 45 = 11.$$

So every common divisor of 1001 and 1023 divides 11 (Proposition 3.1.1 (c)), and a positive one is at most 11 (Proposition 3.1.1 (e)). Since 11 is itself a common divisor, $\gcd(1001, 1023) = 11$ (Definition 3.2.2).

The gcd by the algorithm (Theorem 3.2.4): $1023 = 1 \cdot 1001 + 22$, $1001 = 45 \cdot 22 + 11$, $22 = 2 \cdot 11 + 0$. The last non-zero remainder is 11.

3.3.7.3 C. Going deeper

Exercise. C1: Exit check: unique factorization

Prove that two prime factorizations of the same positive integer are equal: the uniqueness half of Theorem 3.3.5. You may cite Theorem 3.3.1 and Corollary 3.3.2.

Solution. The proof of uniqueness in Theorem 3.3.5 is a complete answer. Its steps, in order: set up $P(k)$ for non-decreasing lists of primes of length k and arbitrary length l , with equal products; base case $k = 0$, where a non-empty list of primes cannot have product 1; in the step, $l \geq 1$, then $p_{k+1} = q_j \leq q_l$ and $q_l = p_i \leq p_{k+1}$ by Corollary 3.3.2 (c) (proved from Euclid's lemma by induction on the length of the product) and the order of the lists; so $p_{k+1} = q_l$; cancel this non-zero factor (Proposition 2.3.5 (f)); apply $P(k)$ to the shortened lists.

Marking scheme. (10 points) - 2: sets up an induction on the length of one list (or a least counterexample), with the statement quantified over all lengths of the other list, and proves the base case. - 3: shows that the largest (or any chosen) prime of one list divides the other product, and identifies it with an entry of the other list by Euclid's lemma for products of several factors (cited as Corollary 3.3.2 (c), or proved by induction from Euclid's lemma). - 2: uses the symmetric step and the non-decreasing order to get equality of the two chosen extreme entries (both largest, or both smallest). - 1: justifies the cancellation by the absence of zero divisors. - 2: applies the induction hypothesis (or minimality) to the shortened lists and concludes equality of length and entries. Fatal errors (0 for the step): using the uniqueness of the factorization of a smaller number without an induction or a least counterexample set up; applying Euclid's lemma for two factors to a product of many with no induction. Canceling a prime without noting that it is non-zero costs 1 point and is not fatal. A least-counterexample proof on n (the least positive integer with two different factorizations) maps to the same points: its set-up and the case $n = 1$ take the first 2, and “the cofactor m in $n = mp_k$ has only one factorization” takes the last 2. A proof that compares the smallest entries $p_1 = q_1$ earns the same points, provided it proves (for example by induction on the length) that a product equals its first entry times the product of the re-indexed list $(p_2, \dots, p_{k+1})$, and states the re-indexing of the shortened lists $(p_2, \dots, p_{k+1})$.

and $(q_2, \dots, q_l)$ before applying the induction hypothesis; asserting that identity without proof costs the 1 cancellation point.

Exercise. C2: Find the error

Here is a statement and an argument for it.

Claim. Let $m, n, c \in \mathbb{Z}$. If $m \mid c$, $n \mid c$ and $\gcd(m, n) = 1$, then $mn \mid c$.

Argument. (1) Write $c = mk$ and $c = nl$ with $k, l \in \mathbb{Z}$. (2) Then $c^2 = c \cdot c = (mk)(nl) = mn \cdot kl$. (3) So $mn \mid c^2$. (4) Hence $mn \mid c$.

Is the claim true? Does the argument prove it? If not, name the line that fails, explain why, and give a counterexample to the step.

Solution. The claim is **true**: it is [Proposition 3.3.3](#). The argument does **not** prove it.

Lines (1)–(3) are correct. The failing line is (4). It rests on a general “fact”: $x \mid c^2$ implies $x \mid c$. That has not been proved, and it is false, so the line cites nothing: entry (N9) of Logic and Proof, Example (What is not allowed). A counterexample to the step: $x = 4$, $c = 2$, with $4 \mid 4 = c^2$ and $4 \nmid 2$ (a positive divisor of 2 is at most 2, Proposition 3.1.1 (e)). There is no counterexample to the conclusion, which is true.

A sign that something is wrong: the argument never uses $\gcd(m, n) = 1$, and without that hypothesis the claim is false ($4 \mid 12$, $6 \mid 12$, $24 \nmid 12$). The repair is the proof of [Proposition 3.3.3](#), which spends the coprimality in Euclid's lemma.

Exercise. C3: There is no last prime

Prove that no finite list contains every prime: for every list of primes $(p_1, \dots, p_k)$, with $k \in \mathbb{N}$, there is a prime that is not an entry of the list.

Solution (Hint 1). Consider $N := \prod_{i=1}^k p_i + 1$, and ask which primes can divide it.

Solution (Hint 2). First prove, by induction on k , that every entry of a list of primes divides its product, and that the product is at least 1.

Solution. *A lemma on products.* For a list of primes $(p_1, \dots, p_k)$, write $P_j := \prod_{i=1}^j p_i$ for $j \leq k$. We prove, by Logic and Proof, Axiom 4.2.1 (through Corollary 1.7.3 (b)) on j , the statement “if $j \leq k$, then $P_j \geq 1$ and $p_i \mid P_j$ for every $i \leq j$ ”. Base $j = 0$: $P_0 = 1$ (the recursion of [Definition 3.3.1](#)), and there are no entries to check. Step: let $j + 1 \leq k$; then $j \leq k$, so the statement holds for j , and $P_{j+1} = P_j p_{j+1}$ by the recursion. Each p_i with $i \leq j$ divides P_j , which divides P_{j+1} , so $p_i \mid P_{j+1}$ (Proposition 3.1.1 (b)); and $p_{j+1} \mid P_{j+1}$ by Sets, Relations, and Cardinality, Definition 2.2.1. Since $P_j \geq 1 > 0$ and $p_{j+1} \geq 2 > 0$, $P_{j+1} > 0 \cdot p_{j+1} = 0$ (Proposition 2.3.5 (c), Proposition 2.3.2 (b)), so $P_{j+1} \geq 1$ by discreteness

(Theorem 2.3.4 (c)).

The new prime. Let $N := P_k + 1$. Then $N \geq 2$, so its least divisor $q \geq 2$ is prime (Lemma 3.3.4), and $q \mid N$. If $q = p_i$ for some i , then $q \mid P_k$ by the lemma, so q divides $N - P_k = 1$ (Proposition 3.1.1 (c)), and $q = \pm 1$ (Proposition 3.1.1 (g)), against $q \geq 2$. So q is a prime that is not an entry of the list.

For the empty list, $N = 2$ and $q = 2$. For $(2, 3, 5, 7)$, $N = 211$, which happens to be prime; for $(2, 3, 5, 7, 11, 13)$, $N = 30031 = 59 \cdot 509$ is not, and the new prime is 59. The proof promises a new prime factor of N , not that N itself is prime.

This is the direct proof asked for in part (c) of Logic and Proof, Exercise (C1: Euclid without the contradiction), now on the constructed $\mathbb{Z}$ and including the empty list. Its two school facts are replaced by Lemma 3.3.4 and Proposition 3.1.1 (c).

Marking scheme. (10 points) - 2: defines N as the product plus 1 and shows $N \geq 2$, with a reason that the product is positive. - 2: shows that each p_i divides the product, by an induction or a cited result. - 2: produces a prime factor q of N , citing Lemma 3.3.4 or an equivalent. - 3: shows q is not any p_i , since it would divide 1. - 1: concludes with the quantifiers in order: for every list there is a prime outside it. Fatal errors (0 for the step): claiming that N is prime; assuming “the set of primes is finite” and taking its product without a list (no list, no product).