

2.2 Induction, Strong Induction and the Smallest Counterexample

Logic and Proof, Chapter 4 gave the principle of induction (Logic and Proof, Axiom 4.2.1), its strong form (Logic and Proof, Theorem 4.2.2), and the first worked proofs: a sum (Logic and Proof, Example (A sum of products of neighbors)), an inequality (Logic and Proof, Example (An inequality by induction)), and a strong induction with three base cases (Logic and Proof, Example (Threes and fives)). *Logic and Proof*, Chapter 8 showed how an induction is written in prose and which rule each phrase stands for (Logic and Proof, Example (An induction, and a legitimate symmetry)). This section is about the craft: which form of induction fits a claim, where it starts, how a smallest counterexample becomes a proof, and how an induction goes wrong, each failure located at one step. On the way it proves facts that *Logic and Proof*, Chapters 1, 2 and 8 took from school: every integer is even or odd and not both, a fraction can be reduced until numerator and denominator are not both even, and every integer $n \geq 2$ has a prime factor.

2.2.1 Induction from any integer

Logic and Proof, Chapter 4 already started inductions at numbers other than 0 (*Logic and Proof*, Section 4.2, “Starting from another number”), for a starting point $b \in \mathbb{N}$. With $\mathbb{Z}$ and Proposition 2.1.2 in hand, the starting point may be any integer, negative ones included.

To prove a statement for every integer from n_0 on, prove it at n_0 and show that it passes from each integer to the next.

Theorem 2.2.1. Induction from a Base

Let n_0 be an integer, and for each integer $n \geq n_0$ let $P(n)$ be a statement. Suppose

- (i) **(base case)** $P(n_0)$ is true, and
- (ii) **(inductive step)** for **every** integer $n \geq n_0$, if $P(n)$ is true then $P(n+1)$ is true.

Then $P(n)$ is true for every integer $n \geq n_0$.

Idea. Count from the base. The integers $n \geq n_0$ are exactly $n_0 + k$ with $k \in \mathbb{N}$, and moving from n to $n+1$ moves k to $k+1$. So the statement “ $P(n_0 + k)$ ” about $k \in \mathbb{N}$ is ready for Logic and Proof, Axiom 4.2.1, and its base case is $P(n_0)$.

Proof. For $k \in \mathbb{N}$, let $Q(k)$ be the statement $P(n_0 + k)$. This makes sense: $n_0 + k$ is an integer by Proposition 2.1.2 (a), and $n_0 + k \geq n_0$ since $k \geq 0$ by Lemma 2.1.1 (a).

Base case. $Q(0)$ is $P(n_0)$, which holds by (i).

Inductive step. Let $k \in \mathbb{N}$, and suppose $Q(k)$, that is, $P(n_0 + k)$. The integer $n := n_0 + k$ satisfies $n \geq n_0$, so (ii) gives $P(n+1)$. Since $n+1 = n_0 + (k+1)$, this is $Q(k+1)$.

By Logic and Proof, Axiom 4.2.1, $Q(k)$ holds for every $k \in \mathbb{N}$. Now let n be an integer with $n \geq n_0$. Then $k := n - n_0$ is an integer by Proposition 2.1.2 (a), and $k \geq 0$, so $k \in \mathbb{N}$ by Proposition 2.1.2 (b). Hence $Q(k)$ holds, and $Q(k)$ is $P(n_0 + k) = P(n)$. This proves the

theorem. ■

For $n_0 = 0$ the theorem is Logic and Proof, Axiom 4.2.1 itself, and for $n_0 \in \mathbb{N}$ it is *Logic and Proof*, Chapter 4's induction started at n_0 . In the inductive step, " $P(n)$ is true" is the induction hypothesis: one implication, proved once, inside a $\rightarrow$ I box whose assumption is $P(n)$ for one fixed but arbitrary integer $n \geq n_0$.

The strong form moves to a base in the same way.

Theorem 2.2.2. Strong Induction from a Base

Let n_0 be an integer, and for each integer $n \geq n_0$ let $P(n)$ be a statement. Suppose that, **for every** integer $n \geq n_0$: if $P(k)$ is true for **every** integer k with $n_0 \leq k < n$, then $P(n)$ is true. Then $P(n)$ is true for every integer $n \geq n_0$.

Proof. For $j \in \mathbb{N}$, let $Q(j)$ be $P(n_0 + j)$, as in the proof of Theorem 2.2.1. We check the hypothesis of Logic and Proof, Theorem 4.2.2 for Q . Let $j \in \mathbb{N}$, and suppose $Q(i)$ holds for every $i \in \mathbb{N}$ with $i < j$. Put $n := n_0 + j$, an integer with $n \geq n_0$. Let k be an integer with $n_0 \leq k < n$. Then $i := k - n_0$ is an integer with $i \geq 0$, so $i \in \mathbb{N}$ by Proposition 2.1.2 (b), and $i < n - n_0 = j$; so $Q(i)$, which is $P(k)$, holds. The hypothesis of the theorem at n now gives $P(n)$, that is, $Q(j)$. By Logic and Proof, Theorem 4.2.2, $Q(j)$ holds for every $j \in \mathbb{N}$, and every integer $n \geq n_0$ is $n_0 + j$ with $j = n - n_0 \in \mathbb{N}$, as in the proof of Theorem 2.2.1. This proves the theorem. ■

So Theorem 2.2.2 is a corollary of Logic and Proof, Theorem 4.2.2, by the same shift. When $n_0 \in \mathbb{N}$, it says what Logic and Proof, Example (Threes and fives) achieved with a guard: there the property was "if $n \geq 8$, then ...", stated for every $n \in \mathbb{N}$ and vacuous below 8. Here the property is stated only for $n \geq n_0$, and the hypothesis speaks only about $k \geq n_0$. The two are the same argument in two notations, and the base cases sit in the same place: they are the n for which the step reaches below n_0 .

Quick check. Every integer $n \geq 24$ is $5a + 7b$ for some integers $a, b \geq 0$. A proof by Theorem 2.2.2 writes $n = (n - 5) + 5$ in its step. How many base cases does it need, and which? Can the base 24 be lowered?

Solution. The step uses $P(n - 5)$, which the hypothesis supplies only when $n - 5 \geq 24$, that is, $n \geq 29$. So $n = 24, 25, 26, 27, 28$ are base cases, five of them, checked directly:

$$\begin{aligned} 24 &= 5 \cdot 2 + 7 \cdot 2, & 25 &= 5 \cdot 5, & 26 &= 5 \cdot 1 + 7 \cdot 3, \\ 27 &= 5 \cdot 4 + 7 \cdot 1, & 28 &= 7 \cdot 4. \end{aligned}$$

The base cannot be lowered: 23 is not of the form. With $b = 0, 1, 2, 3$ the remainder $23 - 7b$ is 23, 16, 9, 2, none a multiple of 5, and $b \geq 4$ gives $23 - 7b < 0$.

2.2.2 The smallest counterexample

Well-ordering gives the same power as strong induction, in a form that often reads more naturally. To prove a claim about every integer from n_0 on, suppose it fails somewhere. The failures form a non-empty set of integers with the integer lower bound n_0 , so Corollary 2.1.5 gives a least one. Below it the claim holds. If that is enough to produce a failure that is smaller still, or to show the claim at the least failure after all, we have a contradiction.

Algorithm. To prove “ $P(n)$ for every integer $n \geq n_0$ ” by a **smallest counterexample**:

- *Suppose it fails:* some integer $n \geq n_0$ has $P(n)$ false.
- *Take the least failure:* the set F of integers $n \geq n_0$ with $P(n)$ false is non-empty and has the integer lower bound n_0 , so it has a least element m (Corollary 2.1.5; Theorem 2.1.3 when $n_0 = 0$).
- *Use the claim below m :* $P(k)$ holds for every integer k with $n_0 \leq k < m$, since such a k is not in F .
- *Produce a contradiction:* a failure $k < m$, or $P(m)$ itself.

Then F is empty, and $P(n)$ holds for every integer $n \geq n_0$.

The method is strong induction with an RAA box drawn around it. The work done inside the box, “if $P(k)$ for every k with $n_0 \leq k < m$, then $P(m)$ ”, is exactly the hypothesis of [Theorem 2.2.2](#) at m ; so any smallest-counterexample proof can be rewritten as a strong induction, and the reverse rewriting works too. Which one to write is a matter of which reads better. A smallest counterexample suits claims whose failure has a natural “smaller failure”, like a fraction that can be reduced, or a number with a factor.

2.2.3 Divisibility and the division algorithm

The first uses of the method are about divisibility, and here is the vocabulary.

Definition 2.2.1. Divisibility

Let $a, b \in \mathbb{Z}$. We say that 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 .

So $3 \mid 12$, with $k = 4$, and $-3 \mid 12$, with $k = -4$. Every integer a divides 0, with $k = 0$; this is the degenerate case, and it shows that “ $a \mid b$ ” is a statement, not the number b/a : $0 \mid 0$ is true, while $0/0$ is not defined. Also $1 \mid b$ and $b \mid b$ for every integer b , and “ n is even” is “ $2 \mid n$ ”. If $a \mid b$ and $b \mid c$, then $a \mid c$: from $b = ka$ and $c = lb$ we get $c = (lk)a$, with $lk \in \mathbb{Z}$ by Proposition 2.1.2 (a).

Change 12 to 14: $3 \nmid 14$. The witness k would have to be $14/3$, and $4 < 14/3 < 5$, so $14/3$ is not an integer, by the discreteness clause of Proposition 2.1.2. The clause that fails is “ $k \in \mathbb{Z}$ ”: the equation $14 = k \cdot 3$ has a real solution, just not an integer one.

Divisibility claims about powers are a staple of induction, because the step usually factors out one copy. For instance, $3 \mid 4^n - 1$ for every $n \in \mathbb{N}$, with 4^n in its school meaning ($4^0 = 1$, $4^{n+1} = 4^n \cdot 4$; Section 2.3 makes this a definition). Base case: $4^0 - 1 = 0 = 3 \cdot 0$. Step: if $4^n - 1 = 3k$ with $k \in \mathbb{Z}$, then

$$4^{n+1} - 1 = 4(4^n - 1) + 3 = 3(4k + 1),$$

and $4k + 1 \in \mathbb{Z}$. By Logic and Proof, Axiom 4.2.1, the claim holds for every $n \in \mathbb{N}$.

Definition 2.2.2. Prime Number

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 $p \mid n$.

For example, 2 is prime. Let $d > 0$ divide 2, say $2 = kd$ with $k \in \mathbb{Z}$. Then $k > 0$, so $k \geq 1$ by Proposition 2.1.2 (b), and $d \leq kd = 2$; by discreteness $d \in \{1, 2\}$. The same argument shows that 3 and 7 are prime, once the candidates $d = 2$ (and $d = 2, \dots, 6$ for 7) are ruled out as $3 \nmid 14$ was. Non-examples: 9 is not prime, since $9 = 3 \cdot 3$ gives the positive divisor $3 \notin \{1, 9\}$; and 1 is not prime, though its only positive divisor is 1, because the definition demands $p \geq 2$. The clause $p \geq 2$ keeps 1 out so that factorizations into primes can be unique, a fact this chapter does not prove or use: Exercise B2 below is about existence only.

Every integer, divided by a positive integer n , leaves a remainder between 0 and $n - 1$. This is school arithmetic, and it is the tool behind “even or odd”.

Theorem 2.2.3. Division Algorithm

Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>0}$. Then there are **unique** integers q and r with

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

The hypothesis $n > 0$ matters: for $n = 0$ no r satisfies $0 \leq r < 0$.

Try it first (ten minutes): which set of non-negative integers should have a least element, and why is that least element the remainder?

Idea. The obvious attempt subtracts n from a again and again until what is left lies in $[0, n)$, adding n instead when a is negative. “Again and again until” is a process, not yet a proof: why does it stop, and why at a number below n ? Well-ordering replaces the process by its outcome. Among all the non-negative integers $a - qn$, take the **least**. If it were n or more, subtracting one more n would leave a smaller non-negative one. For uniqueness: two remainders differ by a multiple of n , yet lie less than n apart, so the multiple is 0.

Proof. Existence. Let

$$R := \{a - qn : q \in \mathbb{Z}\} \cap \{x \in \mathbb{Z} : x \geq 0\},$$

the set of non-negative integers of the form $a - qn$ (each $a - qn$ is an integer by Proposition 2.1.2 (a)). The set R is non-empty. If $a \geq 0$, take $q = 0$: then $a - 0 \cdot n = a \in R$. If $a < 0$, take $q = a$: then $a - an = a(1 - n) \geq 0$, since $a < 0$ and $1 - n \leq 0$ (as $n \geq 1$ by Proposition 2.1.2 (b)). The set R is a non-empty set of integers with the integer lower bound 0, so by Corollary 2.1.5 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 $r - n = a - (q + 1)n$ is an integer of the required form with $r - n \geq 0$, so $r - n \in R$; and $r - n < r$, since $n > 0$. This contradicts the choice of r . 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 $r \neq r'$. By symmetry (exchanging (q, r) and (q', r') changes neither the hypotheses nor the goal) we may suppose $r' < r$. Then $r - r' = (q' - q)n$, and $k := q' - q$ is an integer with $kn = r - r' > 0$. Since $n > 0$, also $k > 0$, so $k \geq 1$ by Proposition 2.1.2 (b), and

$$r - r' = kn \geq n.$$

But $r - r' \leq r < n$, since $r' \geq 0$. This contradiction shows $r = r'$. Then $qn = q'n$, and since $n \neq 0$, $q = q'$. This proves the theorem. ■

The integers q and r are the **quotient** and the **remainder** of a on division by n . For negative a the remainder is still non-negative: $-7 = 3 \cdot (-3) + 2$, with remainder 2, not -1 . Existence and uniqueness do separate jobs, and the case $n = 2$ shows both:

- **Existence** says that every integer a is $2q$ or $2q + 1$: every integer is **even or odd**.
- **Uniqueness** says that no integer is both. If $a = 2q = 2q' + 1$, then a would have remainders 0 and 1.

This is the school fact that *Logic and Proof*, Chapter 1 used in Argument A and *Logic and Proof*, Chapter 2 used in the proof of Logic and Proof, Theorem 2.1.3, now proved. The same uniqueness shows that no integer m has $2m = 1$, since $1 = 2 \cdot 0 + 1$ has remainder 1 and $2m = 2m + 0$ has remainder 0; this is the fact *Analysis on the Real Line*, Chapter 1 uses to show that $\mathbb{Z}$ is not a field. An integer $4k + 1 = 2(2k) + 1$ or $4k + 3 = 2(2k + 1) + 1$ is odd. With $n = 3$, every integer is $3k$, $3k + 1$ or $3k + 2$, for exactly one of the three forms.

Warning. “The remainder” is the r of the theorem, with $0 \leq r < n$. The equations $17 = 5 \cdot 4 - 3$ and $17 = 5 \cdot 2 + 7$ are true, but -3 and 7 are not remainders, and allowing them destroys uniqueness: 17 would have the three “remainders” -3 , 2 and 7. Every argument above that concludes from “remainder 1” that a number is not a multiple of 2 uses the range $0 \leq r < n$, through uniqueness.

2.2.4 Lowest terms and prime factors

Logic and Proof, Chapter 2 needed one more fact about fractions, the fact (L) in the proof of Logic and Proof, Theorem 2.2.1: every rational number can be written with numerator and denominator not both even. The reason given there was that halving cannot go on for ever. Here is that reason as a proof, written in the steps of the smallest-counterexample method, each step named.

Lemma 2.2.4. Lowest Terms, Up to Factors of Two

Every rational number can be written as p/q with $p \in \mathbb{Z}$, $q \in \mathbb{Z}_{>0}$, and p and q **not both** even.

Idea. A representation with both entries even can be halved. Halving makes the denominator smaller, so a least denominator cannot belong to a representation that can be halved. Well-ordering supplies the least denominator.

Proof. Suppose it fails. Fix $r \in \mathbb{Q}$, and suppose that r has no representation p/q with $p \in \mathbb{Z}$, $q \in \mathbb{Z}_{>0}$, and p and q not both even. Let

$$F := \{q \in \mathbb{Z}_{>0} : r = p/q \text{ for some } p \in \mathbb{Z}\}.$$

Under the supposition, every $q \in F$ is the denominator of a failing representation.

Take the least failure. By the definition of $\mathbb{Q}$, $r = p/q$ for some $p \in \mathbb{Z}$ and $q \in \mathbb{Z}_{>0}$, so F is non-empty; and $F \subseteq \mathbb{Z}_{>0} \subseteq \mathbb{N}$. By Theorem 2.1.3, F has a least element m . Write $r = p/m$ with $p \in \mathbb{Z}$.

Use the supposition at m . The representation $r = p/m$ fails, so p and m are both even: $p = 2p'$ and $m = 2m'$ with $p', m' \in \mathbb{Z}$.

Produce a smaller failure. Since $m > 0$, $m' = m/2 > 0$, so $m' \in \mathbb{Z}_{>0}$ by Proposition 2.1.2 (b). Moreover $r = 2p'/(2m') = p'/m'$, so $m' \in F$; and $m' < m' + m' = m$. So m' is an element of F smaller than its least element m , a contradiction.

Hence r has a representation of the required kind. As $r \in \mathbb{Q}$ was arbitrary, this proves the lemma. ■

This is (L), with more: the denominator can be taken positive, not merely non-zero. The proof of Logic and Proof, Theorem 2.2.1 now rests on a proved lemma. The same argument with “not both even” replaced by “no common divisor $d \geq 2$ ” puts every fraction in lowest terms in the full sense; that is Exercise C2. Two of the proof’s steps adapt those of the smallest-counterexample method above: the failures are the denominators in F , and the supposition makes every element of F one, so the third step needs only the supposition at m , not the claim below m , and the contradiction of the fourth step is the smaller failure m' . This proof is written out in full; two later exercises use the same move with less given: Exercise B2 below leaves its last step blank, and Exercise C1 of Section 2.3 leaves the last half blank.

The next result is the prime-factor fact that *Logic and Proof*, Chapter 8 used. Its proof is a strong induction from base 2; the same argument inside an RAA box is a smallest-counterexample proof, in which the least failure m gets a prime factor from its divisor a , contradicting the choice of m (compare Exercise B2).

Theorem 2.2.5. Every Integer at Least Two Has a Prime Factor

Every integer $n \geq 2$ has a prime factor.

Idea. A prime is its own prime factor. A number that is not prime has a divisor strictly between 1 and itself; that divisor is smaller, so it has a prime factor by the strong hypothesis, and divisibility passes it on.

Proof. We use Theorem 2.2.2 with $n_0 = 2$. Let $n \geq 2$ be an integer, and suppose every integer k with $2 \leq k < n$ has a prime factor.

If n is prime, then n is a prime factor of itself, since $n = 1 \cdot n$.

If n is not prime, then, as $n \geq 2$, it has a positive divisor $a \notin \{1, n\}$ (Definition 2.2.2). Write $n = ka$ with $k \in \mathbb{Z}$. Since $n > 0$ and $a > 0$, also $k > 0$, so $k \geq 1$ and $a \geq 1$ by Proposition 2.1.2 (b). Hence $a \leq ka = n$. With $a \neq 1$ and $a \neq n$ this gives $1 < a < n$, and so $2 \leq a < n$ by the discreteness clause of Proposition 2.1.2. By the hypothesis, a has a prime factor p , say $a = lp$ with $l \in \mathbb{Z}$. Then $n = ka = (kl)p$, with $kl \in \mathbb{Z}$ by Proposition 2.1.2 (a), so $p \mid n$.

In both cases n has a prime factor. By Theorem 2.2.2, every integer $n \geq 2$ has one. This proves the theorem. ■

The hypothesis was used at a , which can be far below $n - 1$: for $n = 91 = 7 \cdot 13$ it is used at 7 or at 13. Ordinary induction, which offers only $n - 1$, would have nothing to say about 91 from 90.

2.2.5 How induction proofs go wrong

An induction proof has few moving parts: a property, a base case, a step, and a citation of the right principle. Each can fail, and each failure has a place in the proof where it can be pointed at. Two questions are kept apart throughout: is the conclusion true, and does the argument prove it?

Example. All Numbers Are Equal

Here is a “theorem” and a “proof”. Find the line that fails.

“*Theorem.*” For every integer $n \geq 1$ and all real numbers $x_1, \dots, x_n$, we have $x_1 = x_2 = \dots = x_n$.

“*Proof.*” For an integer $n \geq 1$, let $P(n)$ be the statement “for all real numbers $x_1, \dots, x_n$, all the entries of the list $x_1, \dots, x_n$ are equal”. We use Theorem 2.2.1 with $n_0 = 1$.

- (1) *Base case.* A list x_1 of one number has only one entry, so all its entries are equal: $P(1)$ holds.
- (2) *Step.* Let $n \geq 1$ be an integer, suppose $P(n)$, and let $x_1, \dots, x_{n+1}$ be real numbers.
- (3) The list $x_1, \dots, x_n$ has n entries, so by $P(n)$ its entries are all equal.
- (4) The list $x_2, \dots, x_{n+1}$ has n entries, so by $P(n)$ its entries are all equal.
- (5) The entry x_2 lies in both lists, so every entry of either list equals x_2 .
- (6) Hence $x_1 = x_2 = \dots = x_{n+1}$, which is $P(n + 1)$. By Theorem 2.2.1, $P(n)$ holds for every $n \geq 1$.

Solution. Is the conclusion true? No: the list $x_1 = 0, x_2 = 1$ has unequal entries, so $P(2)$ is false.

Does the argument prove it? No, and the failing line is (5) at $n = 1$. Then the two lists of lines (3) and (4) are x_1 and x_2 , one entry each, and x_2 is not in the first. They share an entry exactly when the first list, $x_1, \dots, x_n$, contains x_2 , that is, when $n \geq 2$. In the terms of Logic and Proof, Example (What is not allowed), line (5) cites a “fact” that is false in the case at hand: entry (N9).

Everything else is correct. The base case (1) is true. For every $n \geq 2$ the step (2)–(6) is valid: if all lists of n reals had equal entries, so would all lists of $n + 1$. So the induction fails at exactly one transition, from 1 to 2, and the valid transitions from 2 on carry nothing, because $P(2)$ is false and every later $P(n)$ with it. A counterexample to the illegal step, as opposed to the conclusion: $n = 1$, $x_1 = 0$, $x_2 = 1$, where lines (3) and (4) hold and (5) does not.

statement	true?	proved by the argument?
$P(1)$	yes	yes, line (1)
$P(1) \Rightarrow P(2)$	no	no: line (5) fails
$P(n) \Rightarrow P(n + 1)$ for $n \geq 2$	yes	yes, lines (2)–(6)
$P(n)$ for every $n \geq 1$	no	no

This is the failure that *Logic and Proof*, Chapter 4’s warning about $2^n \geq n^2$ foreshadowed: a step that holds only from some point on, with a gap at the first transition. A step must be proved for **every** $n \geq n_0$, and the place to look for a gap is the smallest n , where the objects the step talks about are smallest.

The other failures are quicker to state.

The missing base case. “ $n = n + 1$ for every $n \in \mathbb{N}$.” The step is valid: if $n = n + 1$, adding 1 to both sides gives $n + 1 = n + 2$. But $P(0)$, “ $0 = 1$ ”, is false, and so is every $P(n)$. The step is a true implication between false statements, and an induction with no true base proves nothing.

The hypothesis used out of range. A strong induction from a base n_0 may use $P(k)$ only for $n_0 \leq k < n$. A step that writes n in terms of $n - 3$ needs $n - 3 \geq n_0$, and for the first few n that fails. *Logic and Proof*, Example (Threes and fives) handled this correctly, with three base cases; the exit check C1 below is a proof that did not.

The claim too weak to carry its own step. Sometimes the statement is true and the base case holds, but the inductive step cannot be completed, because the hypothesis gives too little. The repair is to prove **more**. Section 2.3 shows a sum bounded by 2 whose own step will not go through, and which a stronger bound carries.

Warning. The induction hypothesis is “ $P(n)$ ” for one fixed but arbitrary n : the assumption of the $\rightarrow I$ box inside the $\forall I$ box of the step (*Logic and Proof*, Definition 5.4.1). A step that begins “assume that $P(n)$ holds for every n ” assumes the conclusion of the theorem, and whatever follows is circular: entry (N9) of *Logic and Proof*, Example (What is not allowed). The witness is a “for every n ” in the assumption that binds the induction variable n itself; it should not be there. A quantifier over another variable is part of the statement and may stay: “for every k with $n_0 \leq k < n$ ” in strong induction, or the “for every n ” inside $P(m)$ in the proof of Lemma 2.1.1 (d), where the induction is on m .

2.2.6 Exercises

2.2.6.1 A. Check your understanding

Exercise. A1

- (a) For each claim, name the form of proof that fits it most naturally (ordinary induction from 0, induction from another base, strong induction from a base with several base cases, or a smallest counterexample), and say in one clause why. Do not prove the claims. (i) $6 \mid 7^n - 1$ for every $n \in \mathbb{N}$. (ii) $2^n > n^2$ for every integer $n \geq 5$. (iii) Every integer $n \geq 12$ is $3a + 7b$ for some integers $a, b \geq 0$. (iv) There are no $m, n \in \mathbb{Z}_{>0}$ with $n^2 = 2m^2$.
- (b) Negate “every integer $n \geq 2$ has a prime factor”, and say what a smallest counterexample to it would be.
- (c) In [Example \(All Numbers Are Equal\)](#), what is the smallest n for which the two lists $x_1, \dots, x_n$ and $x_2, \dots, x_{n+1}$ of lines (3) and (4) share an entry?
- (d) *Find the error.* Here is a “proof” that $a^n = 1$ for every real $a \neq 0$ and every $n \in \mathbb{N}$; the powers a^n , $a^0 = 1$ and $a^{-1} = 1/a$ have their school meaning (Section 2.3 defines a^n for $n \in \mathbb{N}$ only, so negative exponents lie outside that definition). “Fix $a \neq 0$. Base: $a^0 = 1$. Step: let $n \in \mathbb{N}$ and suppose $a^k = 1$ for every $k \in \mathbb{N}$ with $k \leq n$. Then $a^{n+1} = a^n \cdot a^n / a^{n-1} = 1 \cdot 1 / 1 = 1$.” The conclusion is false (take $a = 2$, $n = 1$). Which transition fails, and why?

Solution. (a) (i) Ordinary induction from 0: the step factors out one copy of 7, as in the example $3 \mid 4^n - 1$ after [Definition 2.2.1](#). (ii) Induction from base 5 ([Theorem 2.2.1](#)): the claim fails at $n = 2, 3, 4$, so it cannot start at 0, and the step $2^{n+1} = 2 \cdot 2^n > 2n^2 \geq (n+1)^2$ works for $n \geq 5$. (iii) Strong induction from base 12 with three base cases $12 = 3 \cdot 4$, $13 = 3 \cdot 2 + 7$, $14 = 7 \cdot 2$: the step reaches back three, from n to $n - 3$. (iv) A smallest counterexample: in a solution (m, n) with least n , n^2 is even, so $n = 2n'$ is even (Logic and Proof, Theorem 2.1.3), and then $m^2 = 2n'^2$, so (n', m) is a solution whose second entry m is smaller than n , since $n^2 = 2m^2 > m^2$. (Strong induction would also do; the forms are interchangeable, and the answers above name the natural fit.)

(b) The negation is: there is an integer $n \geq 2$ with no prime factor. A smallest counterexample would be an integer $m \geq 2$ with no prime factor such that every integer k with $2 \leq k < m$ has one.

(c) $n = 2$. For $n = 1$ the lists are x_1 and x_2 ; for $n \geq 2$ both contain x_2 .

(d) The transition from 0 to 1 fails. At $n = 0$ the step writes $a^1 = a^0 \cdot a^0 / a^{-1}$ and uses $a^{-1} = 1$, which is “ $P(-1)$ ”; but the hypothesis covers only $k \in \mathbb{N}$ with $k \leq 0$, that is, $k = 0$, and $-1 \notin \mathbb{N}$. In fact $a^{-1} = 1/a \neq 1$ unless $a = 1$. The base case $a^0 = 1$ is true, and every transition from $n \geq 1$ on is valid, since then $n - 1 \in \mathbb{N}$ and $n - 1 \leq n$, and $a^n a^n / a^{n-1} = a^{n+1}$ for $n \geq 1$. As in [Example \(All Numbers Are Equal\)](#), the valid transitions carry nothing, because $P(1)$ is already false.

2.2.6.2 B. Practice

Exercise. B1

Prove that $5 \mid 6^n - 1$ for every $n \in \mathbb{N}$, without adding up the powers of 6. Here 6^n has its school meaning: $6^0 = 1$, $6^{n+1} = 6^n \cdot 6$, and 6^n is an integer; Section 2.3 makes these official.

Solution. For $n \in \mathbb{N}$, let $P(n)$ be “there is $k \in \mathbb{Z}$ with $6^n - 1 = 5k$ ”. *Base case:* $6^0 - 1 = 0 = 5 \cdot 0$. *Step:* let $n \in \mathbb{N}$ and suppose $6^n - 1 = 5k$ with $k \in \mathbb{Z}$. Then

$$6^{n+1} - 1 = 6 \cdot 6^n - 1 = 6(6^n - 1) + 5 = 5(6k + 1),$$

and $6k + 1 \in \mathbb{Z}$ by Proposition 2.1.2 (a). So $P(n+1)$ holds. By Logic and Proof, Axiom 4.2.1, $5 \mid 6^n - 1$ for every $n \in \mathbb{N}$.

Exercise. B2: Products of primes

An integer is a **product of primes** if it equals $p_1 p_2 \cdots p_k$ for some $k \geq 1$ and primes $p_1, \dots, p_k$ (a single prime counts, with $k = 1$). Here $p_1 p_2 \cdots p_k$ has its school meaning, and multiplying two such products gives the product of the joined list; Section 2.3 defines finite products (Definition 2.3.1). Here is a proof that every integer $n \geq 2$ is a product of primes, with its last step blank. *Name the move, then complete it.*

Suppose not. Then the set F of integers $n \geq 2$ that are not products of primes is non-empty and has the integer lower bound 2, so it has a least element m by Corollary 2.1.5. Since a prime is a product of primes, m is not prime; as $m \geq 2$, it has a positive divisor $a \notin \{1, m\}$, and $m = ab$ with $b \in \mathbb{Z}$. As in the proof of Theorem 2.2.5, $b > 0$ and $2 \leq a < m$. Since $a < m = ab$ and $a > 0$, we get $b > 1$, so $b \geq 2$ by discreteness; and since $a \geq 2$, $b < 2b \leq ab = m$. So $2 \leq a < m$ and $2 \leq b < m$, and as m is the least element of F , neither a nor b lies in F : both are products of primes.

...

Solution. The move is the **smallest counterexample**, and the blank is its last step, *produce a contradiction*. Write $a = p_1 \cdots p_k$ and $b = p'_1 \cdots p'_l$ with primes p_i, p'_j . Then

$$m = ab = p_1 \cdots p_k p'_1 \cdots p'_l$$

is a product of primes, which contradicts $m \in F$. Hence F is empty, and every integer $n \geq 2$ is a product of primes.

Exercise. B3

- Find the quotient and remainder of Theorem 2.2.3 for $a = 17$, $n = 5$, and for $a = -17$, $n = 5$.
- Prove that the square of an odd integer leaves remainder 1 on division by 8.
- Prove that if $2 \mid n$ and $3 \mid n$, then $6 \mid n$, for every integer n .

Hint for (c): Theorem 2.2.3, dividing by 3.

Solution. (a) $17 = 5 \cdot 3 + 2$, so $q = 3$, $r = 2$. And $-17 = 5 \cdot (-4) + 3$, so $q = -4$, $r = 3$; in both cases $0 \leq r < 5$, so by uniqueness these are the quotient and remainder. (Not $-17 = 5 \cdot (-3) - 2$: a remainder is never negative.)

(b) Let $x = 2k + 1$ with $k \in \mathbb{Z}$. Then $x^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$. By Theorem 2.2.3

with $n = 2$, $k = 2j$ or $k = 2j + 1$ with $j \in \mathbb{Z}$. In the first case $k(k + 1) = 2 \cdot j(2j + 1)$; in the second, $k(k + 1) = (2j + 1)(2j + 2) = 2(2j + 1)(j + 1)$. Either way $k(k + 1) = 2t$ with $t \in \mathbb{Z}$, so $x^2 = 8t + 1$. Since $0 \leq 1 < 8$, the uniqueness in [Theorem 2.2.3](#) says that the remainder of x^2 on division by 8 is 1.

(c) Let $n = 2a$ with $a \in \mathbb{Z}$, and divide a by 3: $a = 3q + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < 3$, so $r \in \{0, 1, 2\}$ by discreteness. Then $n = 6q + 2r$. Since $3 \mid n$, say $n = 3s$ with $s \in \mathbb{Z}$, we get $2r = 3(s - 2q)$, so $3 \mid 2r$, where $2r \in \{0, 2, 4\}$. But $2 = 3 \cdot 0 + 2$ and $4 = 3 \cdot 1 + 1$ have non-zero remainders on division by 3, while a multiple $3t = 3t + 0$ has remainder 0; by uniqueness, neither 2 nor 4 is a multiple of 3. So $2r = 0$, $r = 0$, and $n = 6q$: $6 \mid n$.

2.2.6.3 C. Going deeper

Exercise. C1: Exit check: a flawed induction

Here is a claim and a “proof”.

Claim. Every integer $n \geq 18$ is $4a + 7b$ for some integers $a, b \geq 0$.

- (1) For an integer $n \geq 18$, let $P(n)$ be “ $n = 4a + 7b$ for some integers $a, b \geq 0$ ”. We use strong induction from base 18 ([Theorem 2.2.2](#)).
- (2) *Base case.* $18 = 4 \cdot 1 + 7 \cdot 2$, so $P(18)$ holds.
- (3) *Step.* Let $n \geq 18$ be an integer, and suppose $P(k)$ holds for every integer k with $18 \leq k \leq n$.
- (4) Write $n + 1 = (n - 3) + 4$.
- (5) Since $n - 3 < n$, the induction hypothesis gives $n - 3 = 4a + 7b$ with integers $a, b \geq 0$.
- (6) Then $n + 1 = 4(a + 1) + 7b$, with $a + 1 \geq 0$ and $b \geq 0$, so $P(n + 1)$ holds.
- (7) By [Theorem 2.2.2](#), $P(n)$ holds for every integer $n \geq 18$.

Answer each question. (i) Is the claim true? (ii) Does the argument prove it? (iii) Which line fails, and for which n ? (iv) Which rule does that line break? (v) Give a counterexample to the failing step, not merely to some conclusion. (vi) Repair the proof.

Solution. (i) The claim is **true**. Directly,

$$18 = 4 \cdot 1 + 7 \cdot 2, \quad 19 = 4 \cdot 3 + 7, \quad 20 = 4 \cdot 5, \quad 21 = 7 \cdot 3,$$

and from these four the repaired induction in (vi) reaches every larger integer.

(ii) The argument does **not** prove it, although its conclusion is true.

(iii) Line (5) fails for $n = 18, 19$ and 20 . There $n - 3$ is 15, 16, 17, all below 18, and the induction hypothesis says nothing about them. For $n \geq 21$, $18 \leq n - 3 < n$, and line (5) is correct. Lines (1)–(4), (6) and (7) are correct. Line (7) needs one remark, because the step is written from n to $n + 1$ and not in the theorem’s own form. At $N = 18$ the theorem’s hypothesis has a vacuous “if” part, so it asks for $P(18)$ outright, which is line (2). At an integer $N \geq 19$, put $n = N - 1 \geq 18$. By the discreteness clause of Proposition 2.1.2, the integers k with $18 \leq k < N$ are exactly those with $18 \leq k \leq n$, so lines (3)–(6), were they valid for every $n \geq 18$, would prove the hypothesis at N .

(iv) Line (5) applies $\forall E$ to the hypothesis “for every integer k with $18 \leq k \leq n$, $P(k)$ ” at

$k = n - 3$. That is a bounded quantifier, and its elimination needs the line “ $18 \leq n - 3$ ” (Logic and Proof, Proposition 6.1.1); for $n \leq 20$ that line is false. The proof checked only half of the bound, $n - 3 < n$.

(v) Run the same argument with base $14 = 7 \cdot 2$: it “proves” that every integer $n \geq 14$ is $4a + 7b$. That conclusion is false at 17: with $b = 0, 1, 2$ the remainder $17 - 7b$ is 17, 10, 3, none a multiple of 4, and $b \geq 3$ makes it negative. The step that breaks is line (5) at $n = 16$: it takes $P(13)$ from the hypothesis, but $13 < 14$ is outside it, and 13 is not of the form (13 and 6 are not multiples of 4). At $n = 16$ the induction hypothesis is true ($14 = 7 \cdot 2$, $15 = 4 \cdot 2 + 7$, $16 = 4 \cdot 4$), and the step concludes the false $P(17)$. So line (5) is an illegal step, not merely an unlucky one.

(vi) Take four base cases, 18, 19, 20, 21, as in (i), and run the step only for $n \geq 21$, where $n - 3 \geq 18$. In the form of [Theorem 2.2.2](#): for $n \in \{18, 19, 20, 21\}$, $P(n)$ holds directly; for $n \geq 22$, $n - 4 \geq 18$ and $n - 4 < n$, so the hypothesis gives $n - 4 = 4a + 7b$ and $n = 4(a + 1) + 7b$.

Marking scheme. (10 points) - 2: judges the conclusion **true**, with the small cases 18, 19, 20, 21 written as $4a + 7b$. - 3: identifies the failing line exactly: the appeal to the hypothesis for $n - 3$, for $n = 18, 19, 20$. - 2: states the reason as a hypothesis used outside its range ($\forall E$ at a k with $k < 18$). - 2: gives a counterexample **to the step**: the same step carrying a true statement to a false one (for example, base 14 and the failure at 17), not merely a false conclusion. - 1: gives a correct repair (four base cases, or any equivalent). Fatal errors (0 for the item): calling the conclusion false; blaming the base case.

Exercise. C2: Lowest terms

Prove that every rational number can be written as p/q with $p \in \mathbb{Z}$, $q \in \mathbb{Z}_{>0}$, and no common divisor $d \geq 2$ of p and q : there is no integer $d \geq 2$ with $d \mid p$ and $d \mid q$.

Solution (Hint 1). Follow the proof of [Lemma 2.2.4](#), step by step.

Solution (Hint 2). Suppose $r \in \mathbb{Q}$ has no such representation, and let m be the least element of $F := \{q \in \mathbb{Z}_{>0} : r = p/q \text{ for some } p \in \mathbb{Z}\}$.

Solution. Fix $r \in \mathbb{Q}$, and suppose that r has no representation of the required kind. Let F be as in Hint 2. By the definition of $\mathbb{Q}$, F is non-empty, and $F \subseteq \mathbb{Z}_{>0} \subseteq \mathbb{N}$, so by Theorem 2.1.3 it has a least element m . Write $r = p/m$ with $p \in \mathbb{Z}$.

By the supposition, this representation fails: there is an integer $d \geq 2$ with $d \mid p$ and $d \mid m$, say $p = dp'$ and $m = dm'$ with $p', m' \in \mathbb{Z}$. Since $m > 0$ and $d > 0$, $m' = m/d > 0$, so $m' \in \mathbb{Z}_{>0}$ by Proposition 2.1.2 (b). Then $r = dp'/(dm') = p'/m'$, so $m' \in F$. And $m = dm' \geq 2m' > m'$, since $d \geq 2$ and $m' > 0$. So m' is an element of F smaller than its least element, a contradiction. Hence r has a representation p/q with no common divisor $d \geq 2$.

The statement contains [Lemma 2.2.4](#), since $d = 2$ is one of the excluded common divisors. The only change in the proof is the size of the step down: $m' = m/d$ instead of $m/2$, and

$d \geq 2$ is what makes it a step **down**.

Marking scheme. (10 points) - 2: sets up the smallest counterexample: fixes r , supposes no good representation, and defines the set of denominators. - 2: shows that set is a non-empty subset of $\mathbb{N}$ and takes its least element by Theorem 2.1.3. - 3: extracts the common divisor $d \geq 2$ and writes the reduced representation p'/m' , checking $m' \in \mathbb{Z}_{>0}$. - 2: shows $m' < m$, using $d \geq 2$ and $m' > 0$. - 1: concludes, with the contradiction to the choice of m . A strong induction on the denominator earns the same points step for step. Fatal errors (0 for the step): taking a least element of a set not shown to lie in $\mathbb{N}$; dividing by d without $d \neq 0$.

Exercise. C3: Smallest, not largest

- (a) Prove that a set $A \subseteq \mathbb{R}$ has at most one least element.
- (b) Deduce that a claim “ $P(n)$ for every $n \in \mathbb{N}$ ” that is false has exactly one smallest counterexample.
- (c) Show that a false claim about $\mathbb{N}$ need not have a **largest** counterexample, by examining the claim “ $n < 5$ for every $n \in \mathbb{N}$ ”.

Solution. (a) Let m and m' be least elements of A . Since $m' \in A$ and m is least, $m \leq m'$; since $m \in A$ and m' is least, $m' \leq m$. Hence $m = m'$.

(b) The smallest counterexamples are the least elements of the set $F := \{n \in \mathbb{N} : P(n) \text{ is false}\}$. The claim is false, so F is non-empty, and Theorem 2.1.3 gives a least element. By (a), there is only one.

(c) The claim is false, and its counterexamples form $F = \{n \in \mathbb{N} : n \geq 5\}$, which is non-empty. It has no greatest element: for every $n \in F$, also $n + 1 \in \mathbb{N}$ by (NS), and $n + 1 \geq 5$, so $n + 1 \in F$ and $n + 1 > n$. So the claim has a smallest counterexample, 5, and no largest one. Well-ordering has no upward twin in $\mathbb{N}$: a non-empty subset of $\mathbb{N}$ has a greatest element when it is bounded above (Exercise (C1: A greatest element from a least upper bound)), and not in general.