

Induction, Contradiction, and Finite Sets

Logic and Proof, Chapter 4 took one fact about the natural numbers on trust: induction. Everything else we have used about them came from school: that $7 - 3$ is a natural number, that none lies strictly between 3 and 4, and that every non-empty set of them has a least member. This chapter derives all of these from induction, extends them to the integers, and proves that the least-member property, **well-ordering**, is induction in another form. It then turns induction from a principle into a craft: which form fits a claim, where to start, when to argue by contrapositive, by contradiction or from a smallest counterexample, when to prove more than was asked, and how a flawed induction fails at exactly one step. It also proves that a starting value and a rule for the next value really do define a sequence, which is what makes $\sum$, $\prod$, $n!$ and powers definitions rather than abbreviations. The first motivating problem comes from *Logic and Proof*, Chapter 2, which reduced a fraction by halving numerator and denominator for as long as both were even: *what stops the halving from going on for ever?* It proves that there are infinitely many primes, and that $\sqrt[3]{2}$ is irrational.

The second half of the chapter is about size. Section 1.1 left a puzzle waiting for a principle: five objects in four boxes put two in one box. *What does “finite” mean, so that this can be proved?* The answer is a pairing: two sets have the same size when a bijection joins them, a set is finite when it pairs with $\{1, \dots, n\}$, and the pigeonhole principle becomes a theorem, with the facts about counting that the earlier chapters took on trust. The proofs of these facts are where proof by contradiction works at full scale.

What you need. *Logic and Proof*, Chapters 1–8, and *Sets and Functions*, Chapter 1. From *Logic and Proof*, Chapters 1 and 2: the $\rightarrow$ I box (Logic and Proof, Definition 1.4.1), proof by contradiction (Logic and Proof, Definition 2.5.1), De Morgan’s laws (Logic and Proof, Proposition 2.5.5), the contrapositive and the converse (Logic and Proof, Proposition 2.5.2), odd squares (Logic and Proof, Theorem 2.4.4), the irrationality of $\sqrt{2}$ (Logic and Proof, Theorem 2.2.1), whose fact (L) this chapter proves, and Logic and Proof, Theorem 2.1.3, whose parity fact Section 1.1 proved and Section 2.2 derives again. From *Logic and Proof*, Chapter 4: the principle of induction (Logic and Proof, Axiom 4.2.1) and strong induction (Logic and Proof, Theorem 4.2.2), with the worked examples that introduced them (Logic and Proof, Example (A sum of products of neighbors), Logic and Proof, Example (An inequality by induction), Logic and Proof, Example (Threes and fives)), the cure of proving more (Logic and Proof, Example (Prove more to prove less)), and structural recursion and induction (Logic and Proof, Theorem 4.3.4, Logic and Proof, Theorem 4.3.1), which appear here as pointers back and in one review exercise, with truth values (Logic and Proof, Definition 4.4.2) and the set $\{\wedge, \vee, \rightarrow\}$ that cannot express negation (Logic and Proof, Theorem 4.9.6). From *Logic and Proof*, Chapters 5 and 6: the rules for “for every” and “there exists” (Logic and Proof, Definition 5.4.1, Logic and Proof, Definition 5.6.1, Logic and Proof, Proposition 5.6.2), the rules for equality (Logic and Proof, Definition 5.7.1, Logic and Proof, Proposition 5.7.1), bounded quantifiers (Logic and Proof, Proposition 6.1.1), and negating quantifiers and implications (Logic and Proof, Proposition 6.2.3, Logic and Proof, Proposition 6.2.2). From *Logic and Proof*, Chapter 7: the counter-model exercises (Logic and Proof, Exercise (C1: True in every finite model, used later), Logic and Proof, Exercise (C2: A sentence with no finite model, used later)). From *Logic and Proof*, Chapter 8: how an induction is written in prose (Logic and Proof, Example (An induction, and a legitimate symmetry)), the three faces of “by contradiction” (Section 8.1; Logic and Proof, Example (One proof by contradiction, read two ways), the costume examples Logic and Proof, Example (A direct proof in costume) and Logic and Proof, Example

(A contrapositive in costume), Euclid’s list argument Logic and Proof, Exercise (C1: Euclid without the contradiction)), existence without a witness (Section 8.7, Logic and Proof, Theorem 8.7.1), and the catalogue of what a proof may not do (Logic and Proof, Example (What is not allowed)). From Chapter 1: the method boxes for direct proof, cases, counterexamples, double inclusion, injectivity and surjectivity (Example (Method: direct proof from a definition), Example (Method: proof by cases), Example (Method: disproof by counterexample, proof by example), Example (Method: two inclusions), Example (Method: proving injectivity), Example (Method: proving surjectivity)); even, odd, divides and prime (Definition 1.1.1, Definition 1.1.2, Definition 1.1.3, Theorem 1.1.2, Example (The parity of a sum), Proposition 1.1.1, Example (Divisors of a combination), Example (Same pattern, lattice midpoint)); Russell’s paradox (Theorem 1.2.4) and equality of sets by two inclusions (Proposition 1.2.1); sets cut out by a property (Definition 1.2.3), power sets (Definition 1.3.2), unions of families (Definition 1.3.4); ordered pairs and products (Definition 1.4.1, Definition 1.4.2); relations and functions, equality of functions, the empty function (Definition 1.4.3, Definition 1.5.1, Proposition 1.5.1, Proposition 1.5.2); injections, surjections, composites and inverses (Definition 1.5.3, Definition 1.5.4, Example (Deciding injective and surjective), Definition 1.5.2, Definition 1.6.2, Theorem 1.5.4, Theorem 1.6.4, Theorem 1.6.1); images and preimages (Definition 1.7.1, Definition 1.7.2). The arithmetic and order of $\mathbb{R}$ are school facts, as in the earlier chapters; *Analysis on the Real Line*, Chapter 1 states them as axioms.

Time. About 30 hours on the core track (all of A, one B and one C per section, the exit checks); about 40 hours for everything.

2.-1.1 Roadmap

- **The natural numbers and well-ordering.** From induction alone, the arithmetic of $\mathbb{N}$ and $\mathbb{Z}$, the proof that every non-empty set of natural numbers has a least element, and the theorem that induction and well-ordering are equivalent, with a witness for each hypothesis it needs, and the least element as a tool of proof.
- **Induction, strong induction and divisibility.** Induction from any integer, finding the inductive hypothesis inside the step and choosing the base, the division algorithm, lowest terms and prime factors, and a gallery of broken inductions, each located at one step.
- **Definition by recursion.** The theorem that a starting value and a rule define exactly one sequence, its variants from another base and with two previous values, sums, products and powers defined by it, and inductions that follow a definition’s clauses or prove more than was asked.
- **Contrapositive and contradiction in practice.** Choosing among a direct proof, the contrapositive and a contradiction; infinitely many primes; an irrational cube root by lowest terms; the smallest counterexample as a method; existence without a witness.
- **Equinumerous sets and finite sets.** “The same size” defined by a bijection, finite sets and their number of elements, the pigeonhole principle, which settles the five lattice points of Section 1.1, and the uniqueness of that number, subsets, disjoint unions and the 2^n subsets of an n -element set, and the theorem that no finite set is equinumerous with a proper subset, which Hilbert’s hotel turns into a proof that $\mathbb{N}$ is infinite.

2.-1.2 Named moves

The first five are method boxes; each section that introduces one cites it from then on.

- **The least element** (Example (Method: the least element)). Name a set whose least element would help, show it is a non-empty set of natural numbers, take its least element, and use leastness: an element below it is a contradiction, or leastness says what it must

be. (Section 2.1)

- **Finding $P(n)$ inside $P(n+1)$** (Example (Method: finding $P(n)$ inside $P(n+1)$)). Write $P(n+1)$ out, split off the part that is $P(n)$, apply the induction hypothesis to it, close the rest by computation, and choose the base as the first n from which this works. (Section 2.2)
- **Choosing direct, contrapositive or contradiction** (Example (Method: choosing direct, contrapositive or contradiction)). Unwind P , Q and their negations: go direct when P gives something to compute with, prove the contrapositive when $\neg Q$ is the richer hypothesis, and assume the positive statement when the claim is a negation. (Section 2.4)
- **Smallest counterexample** (Example (Method: the smallest counterexample)). Suppose the claim fails; well-ordering gives a least failure m ; below m the claim holds, and from that produce a failure smaller than m , or the claim at m itself. (Section 2.4)
- **Pigeonhole** (Example (Method: the pigeonhole principle)). Choose pigeons and fewer holes, define “the hole of a pigeon”, conclude that two pigeons share a hole, and translate “same hole” back into the property you want. (Section 2.5)
- **Prove more (strengthen the hypothesis)**. When the inductive step will not go through, ask what the induction hypothesis would need to say, and prove that stronger statement instead.
- **Recursion, then induction**. Define an object by a recursion, and prove facts about it by an induction that follows the same clauses: the base case uses the starting value, and the step uses the rule.

2.-1.3 Threads

- **The halving**. Section 2.1 opens its subsection on well-ordering with the halving question of *Logic and Proof*, Chapter 2, and answers it with the first use of the least element (Example (No endless descent in the natural numbers)). Section 2.2 writes the argument out as the existence of lowest terms (Lemma 2.2.4), and Section 2.4 uses lowest terms to prove that $\sqrt[3]{2}$ is irrational (Proposition 2.4.2).
- **The lattice points**. Section 1.1 asks why, among any five points with integer coordinates, two have a midpoint with integer coordinates, and leaves the principle it needs unproved. Section 2.5 opens on the puzzle, proves the pigeonhole principle (Theorem 2.5.2) under the heading “Back to the pigeons”, and finishes the five points (Example (Back to the five lattice points)).
- **Same size**. The bijections of Section 1.6 are how the book says that two sets have the same size; Section 2.5 makes this a definition (Definition 2.5.1), and Section 4.2 meets it again as an example of an equivalence-like relation.
- **Infinitely many primes**. Section 2.4 proves that above every natural number there is a prime (Theorem 2.4.1), before “infinite” has a definition; Section 2.5 defines infinite sets, and a Quick check there concludes that the set of primes is one.

2.-1.4 Summary

Induction and well-ordering are one principle (Theorem 2.1.4). Every integer can be divided by a positive integer with a unique quotient and remainder (Theorem 2.2.3). Every integer at least 2 has a prime factor (Theorem 2.2.5), and there are infinitely many primes (Theorem 2.4.1). A starting value and a rule define exactly one sequence (Theorem 2.3.1), which makes sums, products and powers definitions. The number $\sqrt[3]{2}$ is irrational (Proposition 2.4.2), by lowest terms and a smallest counterexample. For $m > n$ there is no injection from $\{1, \dots, m\}$ to $\{1, \dots, n\}$ (Theorem 2.5.2), so a finite set has exactly one number of elements (Corollary 2.5.4), and no finite set is equinumerous with a proper subset of itself (Theorem 2.5.9).

What is open: are $\mathbb{Q}$ and $\mathbb{R}$ the same size as $\mathbb{N}$? Chapter 3.

2.-1.5 Terms

- **equinumerous:** there is a bijection between the two sets (Definition 2.5.1).
- **factorial:** $n! = \prod_{k=1}^n k$, with $0! = 1$ (Definition 2.3.1).
- **finite, has n elements:** equinumerous with $\{1, \dots, n\}$ for some $n \in \mathbb{N}$ (Definition 2.5.2).
- **greatest element:** an element $m \in S$ with $s \leq m$ for every $s \in S$ (Section 2.1, before Theorem 2.1.3).
- **infinite:** not finite (Definition 2.5.3).
- **least element:** an element $m \in S$ with $m \leq s$ for every $s \in S$ (Section 2.1, before Theorem 2.1.3).
- **maximum, minimum:** the greatest and the least element of a set (Section 2.3, before Proposition 2.3.8).
- **power:** $u^0 = 1$, $u^{n+1} = u^n u$ (Definition 2.3.2).
- **prime factor:** a prime that divides the integer (Definition 1.1.3, Section 1.1); every integer ≥ 2 has one (Theorem 2.2.5).
- **quotient, remainder:** the q and r of $a = qn + r$, $0 \leq r < n$ (Theorem 2.2.3).
- **smallest counterexample:** the least integer at which a claim fails, given by well-ordering (Example (Method: the smallest counterexample)).
- **sum, product:** $\sum_{k=m}^n a_k$ and $\prod_{k=m}^n a_k$, defined by recursion, empty sum 0, empty product 1 (Definition 2.3.1).