

2.4 Contrapositive and Contradiction in Practice

Section 1.1 proved statements straight from their definitions, and Section 1.2 met the first contradiction about sets. *Logic and Proof*, Section 8.1 sorted the arguments called “by contradiction” into three faces: refuting a statement ($\neg I$), proving the contrapositive, and genuine reductio (RAA), with the rule “use the weakest form that works, and say which one you use”. This section is about choosing. Which form a proof takes is decided by the shape of the claim and by what each assumption hands over to compute with. The section proves that there are infinitely many primes and that $\sqrt[3]{2}$ is irrational, makes the smallest counterexample of Section 2.2 a method of its own, and ends with a word on existence proofs that name no witness.

2.4.1 Choosing the form

To prove “if P , then Q ” there are three ways to start. Assume P and work towards Q : a direct proof (Example (Method: direct proof from a definition)). Assume $\neg Q$ and work towards $\neg P$: the contrapositive, which proves the original by Logic and Proof, Proposition 2.5.2. Or assume P and $\neg Q$ together and work towards a contradiction. A claim that is itself a negation, such as “irrational”, “no solution” or “no bijection”, has one natural start, face (i): assume the positive statement, reach $\perp$, and conclude the negation by $\neg I$. The choice is not a matter of taste. Unwind each candidate assumption by its definitions, and ask which one hands over something to compute with.

Example. A negative hypothesis

Let $n \in \mathbb{Z}$. Show that if $n^2 + n + 1$ is not divisible by 3, then n leaves remainder 0 or 2 on division by 3.

Idea (Scratch work). *Direct*. The hypothesis $3 \nmid n^2 + n + 1$ says that no integer k has $n^2 + n + 1 = 3k$. That is a “there is no”, and it gives nothing to compute with: no equation, no object.

Contrapositive. The negation of “remainder 0 or remainder 2” is “remainder not 0 and not 2” (Logic and Proof, Proposition 2.5.5). The remainder lies in $\{0, 1, 2\}$ and is unique (Theorem 2.2.3), so this says: remainder 1. So the new assumption is $n = 3q + 1$, an equation, and the new goal $3 \mid n^2 + n + 1$ asks for a witness, which the equation may produce.

Givens	Goal
$3 \nmid n^2 + n + 1$	the remainder of n is 0 or 2
(contrapositive) $n = 3q + 1, q \in \mathbb{Z}$	$3 \mid n^2 + n + 1$
$n^2 + n + 1 = 9q^2 + 9q + 3$	$n^2 + n + 1 = 3m: m = 3q^2 + 3q + 1$, the gap is closed

The direct start stalled at the first line; the contrapositive closed the gap in two.

Solution. We prove the contrapositive: if n does not leave remainder 0 or 2 on division by 3, then $3 \mid n^2 + n + 1$. Divide n by 3 (Theorem 2.2.3): $n = 3q + r$ with $q \in \mathbb{Z}$ and $r \in \{0, 1, 2\}$ (by discreteness, Proposition 2.1.2 (c)), and r is unique. By assumption $r \neq 0$ and $r \neq 2$, so $r = 1$. Then

$$n^2 + n + 1 = (9q^2 + 6q + 1) + (3q + 1) + 1 = 9q^2 + 9q + 3 = 3(3q^2 + 3q + 1),$$

and $3q^2 + 3q + 1 \in \mathbb{Z}$, so $3 \mid n^2 + n + 1$.

The contrapositive turned a “not divisible” in the hypothesis into a witness to produce, and an “or” in the conclusion into a single case to compute with. The statement is not vacuous: $n = 0$ and $n = 2$ give $n^2 + n + 1 = 1$ and 7, neither divisible by 3.

Quick check. Write the contrapositive and the negation of the statement of [Example \(A negative hypothesis\)](#). Which one is equivalent to it?

Solution. Contrapositive: “if n leaves remainder 1 on division by 3, then $3 \mid n^2 + n + 1$ ”; it is equivalent to the statement. Negation: “there is an integer n with $3 \nmid n^2 + n + 1$ that leaves remainder 1”; it is not equivalent, and it is false by the example.

The example shows the questions to ask before any proof, and they are worth fixing as a method.

Example. Method: choosing direct, contrapositive or contradiction

Template. Unwind P , Q , $\neg P$ and $\neg Q$ by their definitions. If P gives something to compute towards Q , go direct. If $\neg Q$ gives an equation, a case split or an object, and $\neg P$ is a statement you can reach, prove the contrapositive and announce it (“We prove the contrapositive”). If the claim is a negation (irrational, no solution, no bijection, no largest), assume the positive statement and derive a contradiction ($\neg I$). Otherwise assume P and $\neg Q$ together, and use both.

When to use it. Before every proof; at once when the direct attempt stalls, or when the conclusion is an “or”, a “not”, a “no” or “infinitely many”.

The usual failure. A wrong negation: the negation of “ A or B ” is “not A and not B ” (Logic and Proof, Proposition 2.5.5). A “contradiction” that never uses its assumption $\neg Q$, which is a direct proof in costume (Logic and Proof, Example (A direct proof in costume); for the contrapositive, Logic and Proof, Example (A contrapositive in costume)). Not saying which form is used.

Quick check. Which form, and what first sentence, for the following?

- (a) For $x \in \mathbb{R}$, if $x^2 \neq x$, then $x \neq 1$.
- (b) There is no integer n with $n^2 = 2$.
- (c) For $f: X \rightarrow Y$ and $g: Y \rightarrow Z$, if $g \circ f$ is injective, then f is injective.

Solution. (a) Contrapositive: “Suppose $x = 1$; then $x^2 = 1 = x$.” (b) Face (i), since the claim is a negation: “Suppose $n \in \mathbb{Z}$ and $n^2 = 2$.” (Then $|n| \leq 1$ gives $n^2 \leq 1$, and $|n| \geq 2$ gives $n^2 \geq 4$.) (c) Direct, by the method of Example (Method: proving injectivity): “Let $x_1, x_2 \in X$ with $f(x_1) = f(x_2)$.” Then $g(f(x_1)) = g(f(x_2))$, and injectivity of $g \circ f$ gives $x_1 = x_2$.

2.4.2 Infinitely many primes

Logic and Proof, Section 8.1 met Euclid’s argument for a finite list of primes (Logic and Proof, Exercise (C1: Euclid without the contradiction)); here is a version that puts, for each n , a prime above n , and Exercise C2 turns the list argument into a bound of its own. Theorem 2.2.5 gives every integer $n \geq 2$ a prime factor. To show that the primes never run out, it is enough to build, for each n , a number all of whose prime factors exceed n . Multiplying $1, 2, \dots, n$ together and adding 1 does it.

Theorem 2.4.1. There Are Infinitely Many Primes

For every $n \in \mathbb{N}$ there is a prime p with $p > n$.

Idea. The number $n! + 1$ leaves remainder 1 on division by every k with $2 \leq k \leq n$, so none of them divides it. Its prime factor (Theorem 2.2.5) must therefore exceed n . The last step is a face (i) argument inside the proof: suppose $p \leq n$.

Proof. Step 1. For every $n \in \mathbb{N}$, $n!$ is a positive integer and $k \mid n!$ for every $k \in \{1, \dots, n\}$. We use induction on n , following the clauses of $n!$ (Definition 2.3.1). For $n = 0$, $0! = 1$, and there is no k . Suppose the claim holds for n . Then $(n+1)! = n! \cdot (n+1)$ is a positive integer. For $k \leq n$, the hypothesis gives $n! = kj$ with $j \in \mathbb{Z}$, so $(n+1)! = k \cdot j(n+1)$; and $k = n+1$ divides $(n+1)! = n! \cdot (n+1)$. Every $k \in \{1, \dots, n+1\}$ has $k \leq n$ or $k = n+1$ (Lemma 2.1.1 (e)).

Step 2. Let $n \in \mathbb{N}$, and let $N := n! + 1$. By Step 1 and Proposition 2.1.2 (b), $n! \geq 1$, so $N \geq 2$, and N has a prime factor p (Theorem 2.2.5). Suppose $p \leq n$. Since $p \geq 2$, $p \in \{1, \dots, n\}$, so $p \mid n!$ by Step 1. From $p \mid N$ and $p \mid n!$, $p \mid N - n! = 1$ (Example (Divisors of a combination)). So $1 = kp$ with $k \in \mathbb{Z}$; then $k > 0$, so $k \geq 1$, and $p \leq kp = 1$, against $p \geq 2$. Hence $p > n$, by trichotomy. This proves the theorem. ■

Warning. The proof does not say that $n! + 1$ is prime. For $n = 4$, $n! + 1 = 25 = 5 \cdot 5$. The proof uses only that $n! + 1$ has some prime factor, and shows that every one of them exceeds n .

Quick check. Run the proof at $n = 5$: compute N and a prime $p > 5$ dividing it. Is N prime?

Solution. $N = 5! + 1 = 121 = 11 \cdot 11$, and $p = 11 > 5$. N is not prime.

Remark (Looking ahead). Section 2.5 defines infinite sets; with that definition, the set of primes is infinite.

2.4.3 An irrational number by lowest terms

Logic and Proof proved $\sqrt{2}$ irrational (Logic and Proof, Theorem 2.2.1) with the fact (L), which Lemma 2.2.4 now proves. The same lemma settles a cube root. Here $\sqrt[3]{2}$ is the real number x with $x^3 = 2$; its existence and uniqueness are school facts, as in Section 1.6.

Proposition 2.4.2. The Cube Root of 2 Is Irrational

$\sqrt[3]{2}$ is irrational.

Idea. The claim is a negation, so face (i): suppose $\sqrt[3]{2} = p/q$ in the form of Lemma 2.2.4, and show that p and q are both even. One step, “ p^3 even $\Rightarrow p$ even”, is itself a contrapositive.

Proof. A contrapositive first. For $p \in \mathbb{Z}$, if p^3 is even, then p is even. Suppose p is not even. Then p is odd (Theorem 1.1.2), $p = 2k + 1$ with $k \in \mathbb{Z}$, and

$$p^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$$

is odd, hence not even (Theorem 1.1.2).

The claim. Suppose $\sqrt[3]{2}$ is rational. By Lemma 2.2.4, $\sqrt[3]{2} = p/q$ with $p \in \mathbb{Z}$, $q \in \mathbb{Z}_{>0}$, and p and q not both even. Cubing, $p^3 = 2q^3$, so p^3 is even, and p is even: $p = 2s$ with $s \in \mathbb{Z}$. Then $8s^3 = 2q^3$, so $q^3 = 4s^3 = 2(2s^3)$ is even, and q is even. So p and q are both even, a contradiction. Hence $\sqrt[3]{2}$ is irrational ($\neg$ I). ■

The outer frame is face (i), with no RAA: the proof refutes “ $\sqrt[3]{2}$ is rational”. The step inside it is face (ii), a contrapositive whose conclusion “ p even” is not a negation, so it rests on Logic and Proof, Proposition 2.5.2. (It could also avoid RAA: by Theorem 1.1.2, p is even or odd, and the odd case closes by $\perp$ E.) The lemma’s “not both even” is the given that the contradiction breaks; without the lemma there would be nothing to contradict.

Quick check. Why does the same proof not show that $\sqrt[3]{3}$ is irrational?

Solution. $p^3 = 3q^3$ gives no parity contradiction: with q odd, p^3 is odd and p is odd, and “not both even” survives. The proof needs “no common divisor 3”, which Exercise C2 of

Section 2.2 provides.

2.4.4 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 $n_0 \geq 0$, since then $F \subseteq \mathbb{N}$).
- *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.

Section 2.2 used it in Lemma 2.2.4 and in the proof sketched before Theorem 2.2.5, and its Exercise B2 asks for one.

Example. Method: the smallest counterexample

Template. The four steps of the list above, opening with “Suppose not, and let m be the least integer $\geq n_0$ for which $P(m)$ fails”. The least failure is Example (Method: the least element) applied to the set of failures. Worked examples: Lemma 2.2.4 (Section 2.2) and [Example \(Taking out the threes\)](#) below.

When to use it. A failure would give a smaller failure: a number with a factor, a fraction that can be reduced, a representation that can be shortened.

The usual failure. Not checking that the smaller object is still $\geq n_0$ (or positive), so that it lies in the set of failures. Forgetting the case in which no smaller object exists, which must be ruled out directly (in the example below, m not divisible by 3).

Example. Taking out the threes

Show that every positive integer n is $3^a \cdot b$ with $a \in \mathbb{N}$, $b \in \mathbb{Z}$ and $3 \nmid b$.

Idea (Scratch work). This is the argument of Exercise C1 of Section 2.3, with 3 in place of 2; here each step of the method is named. Suppose some positive integer has no such form, and let m be the least one. Unwind what m can be. If $3 \mid m$, say $m = 3m'$, then m' is a smaller positive integer, so it has the form, and one more factor 3 gives m the form too. If $3 \nmid m$, there is no smaller object to pass to; but then $m = 3^0 \cdot m$ already has the form, so m was not a failure at all.

Givens	Goal
m the least positive integer with no form	a contradiction
$3^a b$, $3 \nmid b$; every k with $1 \leq k < m$ has one	
case $3 \nmid m$	$m = 3^0 \cdot m$: m has the form after all
case $m = 3m'$: $1 \leq m' < m$, so $m' = 3^a b$	$m = 3^{a+1}b$: m has the form; the gap is
with $3 \nmid b$	closed

Solution. Suppose not, and let F be the set of positive integers with no such form. F is a non-empty subset of $\mathbb{N}$, so it has a least element m (Theorem 2.1.3). If $3 \nmid m$, then $m = 3^0 \cdot m$ with $3 \nmid m$, so $m \notin F$, a contradiction. So $m = 3m'$ with $m' \in \mathbb{Z}$; $m' > 0$ since $m > 0$, so $m' \in \mathbb{Z}_{>0}$ (Proposition 2.1.2 (b)), and $m' < 3m' = m$. As m is least in F , $m' \notin F$: $m' = 3^a b$ with $a \in \mathbb{N}$, $b \in \mathbb{Z}$ and $3 \nmid b$. Then $m = 3^{a+1}b$ (Definition 2.3.2), so $m \notin F$, a contradiction. Hence $F = \emptyset$.

Quick check. Write 54 and 45 in the form of [Example \(Taking out the threes\)](#), and say why $m' \notin F$ in the proof.

Solution. $54 = 3^3 \cdot 2$ and $45 = 3^2 \cdot 5$. And m' is a positive integer smaller than the least element of F , so it cannot lie in F .

2.4.5 Existence without a witness

A proof of “there exists” by contradiction, an RAA on a statement $\exists x \varphi(x)$, may finish without naming any object. Theorem 2.1.3 was proved so, and the remark after its proof said what that means: the proof shows that a least element exists, not how to find one. *Logic and Proof*, Section 8.7 gave the classical example, an irrational power of an irrational number that is rational, shown to exist between two candidates without saying which one works (Logic and Proof, Theorem 8.7.1). It also gave the book’s position: classical rules are allowed, and a proof that names no witness is still a proof.

The proof of [Theorem 2.4.1](#) and the contrapositive of [Example \(A negative hypothesis\)](#) went the other way. The proof of [Theorem 2.4.1](#) names its witness: a prime factor of $n! + 1$, and trying $2, 3, 4, \dots$ in turn finds the least one. The contrapositive in [Example \(A negative hypothesis\)](#) turned an existence goal into an explicit witness, $m = 3q^2 + 3q + 1$. (The smallest-counterexample proof of [Example \(Taking out the threes\)](#) is formally an RAA, but its two cases describe how to find a and b .) A named witness says more than bare existence, and it can be checked by computation. So the advice is: when a witness is cheap, name it.

2.4.6 Exercises

2.4.6.1 A. Check your understanding

Exercise. A1

- (a) Write the converse, the contrapositive and the negation of “if n is prime and $n \geq 3$, then n is odd”. Which are true?
- (b) Name the form you would choose and write the first sentence (no proofs): (i) $\sqrt[3]{3}$ is irrational; (ii) for $a, b \in \mathbb{Z}$, if $a^2 + b^2$ is odd, then a is even or b is even; (iii) for sets A, B , if $A \cup B = A \cap B$, then $A = B$.
- (c) Run the proof of [Theorem 2.4.1](#) at $n = 6$: find N , its least prime factor, and check that it exceeds 6.
- (d) “Suppose p is the largest prime. Then $p! + 1$ has a prime factor $q > p$, a contradiction.” Which face of “by contradiction” is this, and does the proof name a prime larger than p ?

Solution. (a) Converse: if n is odd, then n is prime and $n \geq 3$. False: $9 = 3 \cdot 3$. Contrapositive: if n is even, then n is not prime or $n < 3$. It is equivalent to the statement, and true: an even $n \geq 3$ has the divisor $2 \notin \{1, n\}$. Negation: some prime $n \geq 3$ is even. False. (“Not odd” is “even” by Theorem 1.1.2.)

(b) (i) Face (i): “Suppose $\sqrt[3]{3} = p/q$ with $p \in \mathbb{Z}$, $q \in \mathbb{Z}_{>0}$ and no common divisor $d \geq 2$ ” (Exercise C2 of Section 2.2; “not both even” is not enough, as the last Quick check of the subsection on $\sqrt[3]{2}$ shows). (ii) Contrapositive: “Suppose a and b are both odd”, the negation of “ a even or b even” by Logic and Proof, Proposition 2.5.5 and Theorem 1.1.2; then a^2 and b^2 are odd (Logic and Proof, Theorem 2.4.4), and $a^2 + b^2$ is even (Example (The parity of a sum)). (iii) Direct, by Example (Method: two inclusions): “Let $x \in A$.”

(c) $N = 6! + 1 = 721$. It is not divisible by 2, 3 or 5: $721 = 2 \cdot 360 + 1 = 3 \cdot 240 + 1 = 5 \cdot 144 + 1$. And $721 = 7 \cdot 103$. The least prime factor is $7 > 6$, and 721 is not prime.

(d) Face (i): it refutes “there is a largest prime”. Its body names q , so it can be rewritten without contradiction: for every prime p , a prime factor of $p! + 1$ is a larger prime ([Theorem 2.4.1](#) with $n = p$). This is the rewrite of Logic and Proof, Exercise (C1: Euclid without the contradiction), applied to $p! + 1$ in place of Euclid’s product.

2.4.6.2 B. Practice

Exercise. B1: Contrapositive

Prove:

- (a) for all $a, b \in \mathbb{Z}$, if $3 \nmid a + b$, then $3 \nmid a$ or $3 \nmid b$;
- (b) for every $x \in \mathbb{R}$, if $x^2 > 2x + 8$, then $x > 4$ or $x < -2$.

Solution. (a) We prove the contrapositive: if $3 \mid a$ and $3 \mid b$, then $3 \mid a + b$; its hypothesis is the negation of “ $3 \nmid a$ or $3 \nmid b$ ” by Logic and Proof, Proposition 2.5.5. With $a = 3k$ and $b = 3l$, $a + b = 3(k + l)$ (Example (Divisors of a combination)).

(b) We prove the contrapositive. Suppose $x \leq 4$ and $x \geq -2$ (the negation of the conclusion, by Logic and Proof, Proposition 2.5.5 and trichotomy). Then $x - 4 \leq 0$ and $x + 2 \geq 0$, so $x^2 - 2x - 8 = (x - 4)(x + 2) \leq 0$, that is, $x^2 \leq 2x + 8$.

Exercise. B2: Contradiction

Prove:

- (a) there is no rational number r with $r^2 = r + 1$;
- (b) there are no integers m, n with $m^2 - 8n = 5$.

Solution. (a) Suppose $r^2 = r + 1$, with $r = p/q$ as in Lemma 2.2.4. Multiplying by q^2 , $p^2 = pq + q^2$. Two facts about products: odd times odd is odd, since $(2k + 1)(2l + 1) = 2(2kl + k + l) + 1$, and an even number times any integer is even. Since p and q are not both even, three cases remain. If p, q are odd: p^2 is odd, and $pq + q^2$ is odd plus odd, even (Example (The parity of a sum)). If p is even and q odd: p^2 is even, and $pq + q^2$ is even plus odd, odd. If p is odd and q even: p^2 is odd, and $pq + q^2$ is even. Each case equates an odd and an even integer, against Theorem 1.1.2.

(b) Suppose $m^2 = 8n + 5 = 2(4n + 2) + 1$. Then m^2 is odd, so m is odd (Logic and Proof, Theorem 2.4.4), and $m^2 = 8t + 1$ with $t \in \mathbb{Z}$ by Exercise (B3, used later) (b). So $8(t - n) = 4$, and $2(t - n) = 1$: 1 would be even, against Theorem 1.1.2.

Exercise. B3: Name the move, then complete it

Claim: $n < 2^n$ for every integer $n \geq 1$. Here is a proof with its last step blank.

Suppose not. Then the set F of integers $n \geq 1$ with $n \geq 2^n$ is non-empty and has the integer lower bound 1, so it has a least element m (Corollary 2.1.5). Since $1 < 2 = 2^1$, $m \neq 1$, so $m \geq 2$, and $m - 1$ is an integer with $1 \leq m - 1 < m$.

...

Solution. The move is the smallest counterexample (Example (Method: the smallest counterexample)), and the blank is its last step. As $m - 1 < m$, $m - 1 \notin F$: $m - 1 < 2^{m-1}$. Since $2^{m-1} \in \mathbb{N}$ (Proposition 2.3.4 (d)), discreteness gives $m \leq 2^{m-1}$. And $2^{m-1} < 2^{m-1} \cdot 2 = 2^m$ (Definition 2.3.2, with $m - 1 \in \mathbb{N}$, and $2^{m-1} > 0$ by Proposition 2.3.4 (e)). So $m < 2^m$, that is, $m \notin F$, a contradiction.

Exercise. B4: Prove or disprove

Prove each true statement; refute each false one with a concrete counterexample.

- (a) For every $n \in \mathbb{Z}$: if $n^2 - 1$ is not divisible by 5, then n is divisible by 5.
- (b) For every $n \in \mathbb{Z}$: if $4 \nmid n^2$, then n is odd.
- (c) For every $x \in \mathbb{R}$: if x is irrational, then x^2 is irrational.

- (d) For every $x \in \mathbb{R}$: if x^2 is irrational, then x is irrational.
- (e) For all positive integers a, b : $a^2 - b^2 \neq 10$.
- (f) For every $n \in \mathbb{N}$ there is a prime p with $n < p \leq n + 6$.

Solution.

- (a) **False.** Take $n = 2$: $n^2 - 1 = 3$ is not divisible by 5, and neither is 2.
- (b) **True.** We prove the contrapositive. If n is not odd, it is even (Theorem 1.1.2), $n = 2k$, and $n^2 = 4k^2$, so $4 \mid n^2$. (Its look-alike “if $4 \mid n^2$, then $4 \mid n$ ” is false at $n = 2$.)
- (c) **False.** Take $x = \sqrt{2}$, irrational by Logic and Proof, Theorem 2.2.1: $x^2 = 2$ is rational.
- (d) **True.** We prove the contrapositive: if $x = p/q$ is rational, so is $x^2 = p^2/q^2$.
- (e) **True**, by contradiction (face (i)). Suppose $a^2 - b^2 = (a - b)(a + b) = 10$. Since $a + b = (a - b) + 2b$ and $2b$ is even (Theorem 1.1.2), the two factors have the same parity (Example (The parity of a sum)). If both are odd, the product is odd, since $(2k+1)(2l+1) = 2(2kl+k+l)+1$ as in B2 (a), but 10 is even. If both are even, 4 divides the product, but $10 = 4 \cdot 2 + 2$ is not a multiple of 4 (uniqueness in Theorem 2.2.3).
- (f) **False.** Take $n = 89$. The numbers $90, \dots, 95$ are not prime: $90, 92, 94$ are even, $91 = 7 \cdot 13$, $93 = 3 \cdot 31$, $95 = 5 \cdot 19$. (89 is the smallest counterexample.)

Verdicts: three true, (b), (d), (e); three false.

2.4.6.3 C. Going deeper

Exercise. C1: Two proofs by contradiction

For each proof below: is the conclusion true? Is the argument valid? Name each flaw, and write a proof in the form that [Example \(Method: choosing direct, contrapositive or contradiction\)](#) recommends.

Proof A. Claim: if $n \in \mathbb{Z}$ is odd, then $n^2 + n$ is even. “Suppose n is odd and $n^2 + n$ is odd. Write $n = 2k + 1$. Then $n^2 + n = (2k + 1)(2k + 2) = 2(2k + 1)(k + 1)$ is even, which contradicts $n^2 + n$ odd.”

Proof B. Claim: for every $n \in \mathbb{Z}$, if $n^2 \geq 10$, then $n \geq 4$ or $n \leq -4$.

- (1) Suppose $n^2 \geq 10$.
- (2) Suppose, for a contradiction, that $n < 4$ or $n > -4$.
- (3) Say $n < 4$, so $n \leq 3$.
- (4) If also $n \geq -3$, then $n^2 \leq 9 < 10$; so $n \leq -4$.
- (5) So $n \leq -4$, which proves the claim.

Solution. *Proof A.* The conclusion is true and the argument is valid, but the assumption “ $n^2 + n$ odd” is used only to clash with the result: a direct proof in costume (Logic and Proof, Example (A direct proof in costume)). Written directly: “Let $n = 2k + 1$ with $k \in \mathbb{Z}$; then $n^2 + n = 2(2k + 1)(k + 1)$ is even.” The hypothesis is not even needed: $n^2 + n = n(n + 1)$, and one of $n, n + 1$ is even.

Proof B. The conclusion is true; the argument is not a proof. Line (2) negates “ $n \geq 4$ or

$n \leq -4$ ” wrongly, entry (N11) of Logic and Proof, Example (What is not allowed): the negation is “ $n < 4$ and $n > -4$ ” (Logic and Proof, Proposition 2.5.5). Line (3) takes one disjunct of its own “or” and drops the other, a missing case (N7). Line (5) reaches no contradiction at all. A proof by the contrapositive: if $n < 4$ and $n > -4$, then $-3 \leq n \leq 3$ (Proposition 2.1.2 (c)), so $|n| \leq 3$ and $n^2 \leq 9 < 10$. Or by cases: if $n \geq 4$, done; if $n \leq 3$, then $n \leq -4$ by the computation of line (4).

Marking scheme. (10 points) - 2: judges A’s conclusion true and its argument valid, and names the assumption it never uses. - 1: rewrites A as a direct proof. - 3: names the wrong negation in line (2) and gives the correct one (citing (N11) is optional). - 1: names the missing case (N7). - 1: notes that B reaches no contradiction. - 2: gives a correct proof of B’s claim.

Exercise. C2: A bound from Euclid’s list

Logic and Proof, Section 8.1 proved that for primes $p_1, \dots, p_k$, with $k \geq 1$, the number $p_1 p_2 \cdots p_k + 1$ has a prime factor different from each p_i (Logic and Proof, Exercise (C1: Euclid without the contradiction)). Here that argument becomes a bound. Let $p_1 := 2$, and let p_{n+1} be the least prime greater than p_n ; it exists by [Theorem 2.4.1](#) and Theorem 2.1.3, and Corollary 2.3.2 makes $(p_n)_{n \geq 1}$ a sequence. So $p_2 = 3$, $p_3 = 5$.

- (a) Prove that for every $n \geq 1$, every prime $q \leq p_n$ is one of $p_1, \dots, p_n$.
- (b) Prove that $p_{n+1} \leq p_1 p_2 \cdots p_n + 1$ for every $n \geq 1$.
- (c) Deduce that $p_n \leq 2^{2^{n-1}}$ for every $n \geq 1$.
- (d) Compute $P = p_1 \cdots p_k + 1$ and its prime factors for the lists 3, 5 and 2, 7. Is P prime?

Solution. (a) By Theorem 2.2.1 with base 1. For $n = 1$: a prime $q \leq 2$ has $q \geq 2$, so $q = 2 = p_1$. Suppose the claim for n , and let $q \leq p_{n+1}$ be prime. If $q \leq p_n$, then q is one of $p_1, \dots, p_n$ by the hypothesis. Otherwise $q > p_n$, by trichotomy; then q is a prime greater than p_n , so $p_{n+1} \leq q$, as p_{n+1} is the least one, and $q = p_{n+1}$.

(b) Let $n \geq 1$ and $P := p_1 \cdots p_n + 1$. Each $p_i \geq 2$, so $P \geq 3$, and P has a prime factor q (Theorem 2.2.5). Suppose $q = p_i$ for some $i \leq n$. Then p_i divides $p_1 \cdots p_n$, which is p_i times the product of the other entries (school arithmetic of finite products, Definition 2.3.1), so $q \mid P - p_1 \cdots p_n = 1$ (Example (Divisors of a combination)), and $q \leq 1$ as in the proof of [Theorem 2.4.1](#), against $q \geq 2$. So q is none of $p_1, \dots, p_n$, and by (a) $q \not\leq p_n$: $q > p_n$. Hence $p_{n+1} \leq q$, by the choice of p_{n+1} . Finally $P = kq$ with $k \in \mathbb{Z}$, and $k > 0$ since $P, q > 0$, so $k \geq 1$ and $q \leq kq = P$.

(c) By Theorem 2.2.2 with base 1. For $n = 1$, $p_1 = 2 = 2^{2^0}$. Let $n \geq 1$, and suppose $p_k \leq 2^{2^{k-1}}$ for every k with $1 \leq k \leq n$. By (b), multiplying these n inequalities between positive numbers, Proposition 2.3.4 (a) and Proposition 2.3.6 with $r = 2$,

$$p_{n+1} \leq p_1 \cdots p_n + 1 \leq 2^{2^0+2^1+\cdots+2^{n-1}} + 1 = 2^{2^n-1} + 1 \leq 2 \cdot 2^{2^n-1} = 2^{2^n},$$

where the last inequality uses $1 \leq 2^{2^n-1}$.

(d) $3 \cdot 5 + 1 = 16 = 2^4$, with prime factor 2. $2 \cdot 7 + 1 = 15 = 3 \cdot 5$, with prime factors 3 and 5. Neither P is prime; each has a prime factor off its list, and neither list is an initial segment $p_1, \dots, p_k$, so (b) says nothing about them.

Marking scheme. (10 points) - 3: (a), with the base case and the use of leastness of p_{n+1} . - 3: (b): a prime factor q of P off the list, $q > p_n$ by (a), and $p_{n+1} \leq q \leq P$. - 3: (c): strong induction, the geometric sum in the exponent, and $2^{2^n-1} + 1 \leq 2^{2^n}$. - 1: both computations in (d).

Exercise. C3: Challenge: primes of the form $3k + 2$

Prove that for every integer $n \geq 1$ there is a prime $p > n$ with $p = 3k + 2$ for some $k \in \mathbb{Z}$.

Hint: consider $N := 3 \cdot n! - 1$, and Exercise (B2: Products of primes, used later).

Solution. $N = 3(n! - 1) + 2 \geq 2$, since $n! \geq 1$. By Exercise (B2: Products of primes, used later), $N = q_1 \cdots q_r$ with primes q_i . Each $q_i > n$: if $q_i \leq n$, then $q_i \mid n!$ (Step 1 of the proof of [Theorem 2.4.1](#)), and $q_i \mid N$ (school arithmetic of finite products, as in Exercise C2), so $q_i \mid 3 \cdot n! - N = 1$ (Example (Divisors of a combination)), which is impossible. No q_i is 3, since N leaves remainder 2 on division by 3. Dividing q_i by 3 (Theorem 2.2.3) and using discreteness, each q_i is $3t$, $3t + 1$ or $3t + 2$. So each q_i is $3t + 1$ or $3t + 2$: if $q_i = 3t$, then $3 \mid q_i$, and $q_i = 3$ since q_i is prime. If every q_i were of the form $3t + 1$, then N would be too, since $(3a + 1)(3b + 1) = 3(3ab + a + b) + 1$ and an induction on r carries this along the product; but $N = 3(n! - 1) + 2$, against the uniqueness in Theorem 2.2.3. So some q_i is $3t + 2$, and $q_i > n$.

Marking scheme. (10 points) - 2: shows $N \geq 2$ and a factorization into primes. - 2: shows each $q_i > n$ via $q_i \mid n!$. - 1: shows $q_i \neq 3$. - 2: shows each q_i is $3t + 1$ or $3t + 2$. - 2: shows a product of factors $3t + 1$ is $3t + 1$, by induction. - 1: the contradiction with remainder 2.