

1.1 Proofs from Definitions

Logic and Proof taught the rules of proof and how to write them as prose. From here on the statements are about mathematical objects, and every word in them that matters has a definition. A proof begins by writing the hypotheses out by their definitions, writes out what the conclusion demands, and closes the gap between them. This section practices that on the integers, where the definitions are one line long and every claim can be tested by hand. It teaches five moves: direct proof, proof by cases, without loss of generality, disproof by counterexample, and proof of existence by an example.

1.1.1 A puzzle about lattice points

A **lattice point** is a point (a, b) of the plane whose coordinates a and b are both integers, as in school geometry: the corners of the squares on squared paper. The midpoint of (a, b) and (c, d) is

$$\left(\frac{a+c}{2}, \frac{b+d}{2}\right),$$

and it may or may not be a lattice point. The points $(0, 0)$ and $(2, 4)$ have midpoint $(1, 2)$, a lattice point; the points $(0, 0)$ and $(1, 4)$ have midpoint $(\frac{1}{2}, 2)$, which is not. That raises two questions.

- (Q1) Among **any five** lattice points, must there be two whose midpoint is a lattice point?
- (Q2) Among **any four** lattice points, must there be two whose midpoint is a lattice point?

Before reading on, place a few sets of points on squared paper and compute their midpoints.

Both answers come from two words this section defines, even and odd. Question (Q2) is settled in this section. Question (Q1) needs, besides parity, a principle about finite collections that sounds too obvious to need proof; we will state it but not yet prove it.

1.1.2 Definitions first

The first two words are the ones the puzzle needs.

Definition 1.1.1. Even and Odd

An integer n is **even** if $n = 2k$ for **some** $k \in \mathbb{Z}$, and **odd** if $n = 2k + 1$ for **some** $k \in \mathbb{Z}$.

Logic and Proof used these words informally, and wrote “ n is even” as $\exists k (n = 2k)$ in its derivations (for instance Logic and Proof, Example (The sum of two even integers is even)); from now on they mean exactly this, a “there exists”.

Evenness is divisibility by 2, so the next word generalizes it. One might define “ a divides b ” as “ b/a is an integer”. That works for 3 and 12, but it says nothing when $a = 0$, since $0/0$ and $5/0$ are undefined; yet $0 = 0 \cdot 0$ suggests that 0 should divide 0. The definition avoids division altogether and asks for a multiplier.

Definition 1.1.2. 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 .

Quick check. Decide, from the definitions alone: (a) Is 0 even? (b) Does -4 divide 6? Does 0 divide 5? (c) Is -7 odd? (d) Does 12 divide 3?

Solution.

- (a) Yes: $0 = 2 \cdot 0$, with $k = 0 \in \mathbb{Z}$.
- (b) No. If $6 = k \cdot (-4)$ with $k \in \mathbb{Z}$, then $k \leq -2$ gives $-4k \geq 8$ and $k \geq -1$ gives $-4k \leq 4$, so $-4k \neq 6$ in either case. And no: $k \cdot 0 = 0 \neq 5$ for every k .
- (c) Yes: $-7 = 2 \cdot (-4) + 1$, with $k = -4 \in \mathbb{Z}$.
- (d) No. If $3 = 12k$ with $k \in \mathbb{Z}$, then $k \geq 1$ gives $12k \geq 12$ and $k \leq 0$ gives $12k \leq 0$.

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 “ $2 \mid n$ ”. We write $a \nmid b$ when a does not divide b .

The last definition singles out the integers with as few divisors as possible.

Definition 1.1.3. 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 $p \mid n$.

So 2, 3, 5 and 7 are prime (for 7: a positive divisor of 7 is at most 7, and none of 2, 3, 4, 5, 6 divides it); $9 = 3 \cdot 3$ and $15 = 3 \cdot 5$ are not, and neither is 1, which fails the clause $p \geq 2$.

1.1.3 Direct proof

The first claim to prove from these definitions is that divisibility passes along a chain.

Proposition 1.1.1. Divisibility Is Transitive

For all integers a, b, c , if $a \mid b$ and $b \mid c$, then $a \mid c$.

Idea (Scratch work). Unwind every defined word. The hypotheses $a \mid b$ and $b \mid c$ are two “there exists” statements, so each hands us a multiplier. Give them **different** names, k and l : nothing says the two multipliers agree, and one name for both is the error (N4) of Logic and Proof, Example (What is not allowed), met in Logic and Proof, Example (The sum of two even integers is even). The goal $a \mid c$ is also a “there exists”: we must **produce** an integer m with $c = ma$.

Givens	Goal
$a \mid b, b \mid c$	$a \mid c$
$b = ka, c = lb$, with $k, l \in \mathbb{Z}$	$c = ma$ for some $m \in \mathbb{Z}$: find m

$$b = ka, c = lb$$

$c = l(ka) = (lk)a$: try $m = lk$, and check that $lk \in \mathbb{Z}$

The last row closes the gap. The proof writes this forwards: the witness m is named, then checked.

Proof. Let $a, b, c \in \mathbb{Z}$ with $a \mid b$ and $b \mid c$. By [Definition 1.1.2](#) there are $k, l \in \mathbb{Z}$ with $b = ka$ and $c = lb$. Then $c = l(ka) = (lk)a$, and $lk \in \mathbb{Z}$, as a product of integers. So $a \mid c$, with witness lk , by [Definition 1.1.2](#). ■

The proof used only the definition of divisibility and integer arithmetic, and it read the definition in both directions: once to unwind the hypotheses, once to rewind the conclusion.

Example. Method: direct proof from a definition

Template. To prove “if P , then Q ”: (1) assume P and write it out by its definition, giving each witness a new name; (2) write out what Q demands, for example which object must be produced; (3) close the gap by computation, on scrap paper if need be; (4) write the proof forwards: assume, unwind, compute, and rewind into the definition of Q , naming the witness and checking that it is of the required kind.

When to use it. The hypotheses and the conclusion are defined notions, and the gap between them is computation.

The usual failure. Stopping at the computation, as in “ $c = (lk)a$, done”, without checking that $lk \in \mathbb{Z}$, which is the clause the definition demands. Also one name for two witnesses (N4), and using what is to be proved (N9).

Example. Divisors of a combination

Let $a, b, c \in \mathbb{Z}$ with $a \mid b$ and $a \mid c$. Show that $a \mid bx + cy$ for all $x, y \in \mathbb{Z}$.

Solution. By the method of [Example \(Method: direct proof from a definition\)](#): unwind both hypotheses with two names, then look for a multiplier of a in $bx + cy$.

Let $x, y \in \mathbb{Z}$. By [Definition 1.1.2](#) there are $k, l \in \mathbb{Z}$ with $b = ka$ and $c = la$. Then

$$bx + cy = kax + lay = (kx + ly)a,$$

and $kx + ly \in \mathbb{Z}$, since sums and products of integers are integers. So $a \mid bx + cy$, with witness $kx + ly$.

Three special cases are used constantly. With $x = y = 1$, $a \mid b + c$; with $x = 1$ and $y = -1$, $a \mid b - c$; with $y = 0$, $a \mid bx$. With $a = 2$ and $x = y = 1$, the first case is “even plus even is even”, the claim derived in Logic and Proof, Example (The sum of two even integers is even).

Quick check. The proof of [Proposition 1.1.1](#) named two witnesses, k and l . Find integers a, b, c with $a \mid b$ and $b \mid c$ for which one name could not serve for both.

Solution. Take $a = 1$, $b = 2$, $c = 6$. Then $b = 2a$ and $c = 3b$, and no single k has both $2 = k \cdot 1$ and $6 = k \cdot 2$: the first forces $k = 2$, the second $k = 3$. Writing one name would claim that the two multipliers are equal, which is (N4).

1.1.4 Proof by cases

Some claims depend on what kind of integer we have. The first such fact is the one behind every parity argument.

Theorem 1.1.2. Every Integer Is Even or Odd

Every integer is even or odd, and no integer is both.

Idea (Scratch work). Start on $\mathbb{N}$, where induction is available (Logic and Proof, Axiom 4.2.1), with $P(n)$: “ n is even or n is odd”. The base $P(0)$ is $0 = 2 \cdot 0$. The step needs $P(n+1)$ from $P(n)$. But $P(n)$ is an “or”, and knowing that n is even **or** odd does not tell us which. So split into the two cases, as $\forall E$ does (Logic and Proof, Definition 1.6.1). Each case is a new given, and each must reach the same goal.

Givens	Goal
$P(n)$: n even or n odd	$n+1$ even or $n+1$ odd
Case 1: $n = 2k$	$n+1 = 2k+1$: odd
Case 2: $n = 2k+1$	$n+1 = 2(k+1)$: even

The negative integers come next, by cases again: for $n < 0$, $-n \in \mathbb{N}$ is already known to be even or odd, and the sign can be moved inside. Finally “not both” is a negation: assume $n = 2a$ and $n = 2b+1$, and aim for a contradiction ($\neg I$). The two equations give $2(a-b) = 1$, and no integer doubles to 1.

Proof. Every natural number is even or odd. We argue by induction on n . For $n = 0$, $0 = 2 \cdot 0$ is even. Let $n \in \mathbb{N}$ be even or odd. *Case 1:* $n = 2k$ with $k \in \mathbb{Z}$. Then $n+1 = 2k+1$ is odd. *Case 2:* $n = 2k+1$ with $k \in \mathbb{Z}$. Then $n+1 = 2(k+1)$, with $k+1 \in \mathbb{Z}$, is even. In either case $n+1$ is even or odd. By Logic and Proof, Axiom 4.2.1, every $n \in \mathbb{N}$ is even or odd.

Every integer is even or odd. Let $n \in \mathbb{Z}$. If $n \geq 0$, then $n \in \mathbb{N}$, and we are done. If $n < 0$, then $-n \in \mathbb{N}$ is even or odd. If $-n = 2k$, then $n = 2(-k)$ is even. If $-n = 2k+1$, then $n = -2k-1 = 2(-k-1)+1$ is odd.

No integer is both. Suppose $n = 2a$ and $n = 2b+1$ with $a, b \in \mathbb{Z}$. Then $2(a-b) = 1$, with $c := a-b \in \mathbb{Z}$. If $c \geq 1$, then $2c \geq 2$; if $c \leq 0$, then $2c \leq 0$. Either way $2c \neq 1$, a contradiction. So no integer is both even and odd ($\neg I$).



A fact *Logic and Proof* took from school is now proved from the definitions. The proof has four case splits, each into cases that together cover everything.

Example. Method: proof by cases

Template. Find a disjunction you already have, such as “ n is even or n is odd” ([Theorem 1.1.2](#)), “ $x \geq 0$ or $x < 0$ ”, or excluded middle (Logic and Proof, Proposition 2.5.3). Write one paragraph per case, labeled *Case 1.*, *Case 2.*. In each, add the case to the givens, unwind it, and reach the **same** goal.

When to use it. The definitions or the algebra behave differently on different kinds of input, so the givens give no grip until you know which kind you have.

The usual failure. Cases that do not cover every possibility (N8), or a case forgotten (N7). Before splitting, say why the cases are exhaustive.

Example. A proof by cases

Show that $n^3 + 5n$ is even for every integer n .

Idea. A general n gives no grip, but $2k$ and $2k + 1$ can be expanded, and by [Theorem 1.1.2](#) these two cases cover $\mathbb{Z}$. So use [Example \(Method: proof by cases\)](#), and in each case pull out a factor 2.

Solution. Let $n \in \mathbb{Z}$. By [Theorem 1.1.2](#), n is even or odd.

Case 1: $n = 2k$ with $k \in \mathbb{Z}$. Then $n^3 + 5n = 8k^3 + 10k = 2(4k^3 + 5k)$.

Case 2: $n = 2k + 1$ with $k \in \mathbb{Z}$. Then $n^3 = 8k^3 + 12k^2 + 6k + 1$ and $5n = 10k + 5$, so

$$n^3 + 5n = 8k^3 + 12k^2 + 16k + 6 = 2(4k^3 + 6k^2 + 8k + 3).$$

In each case the bracket is an integer, so $n^3 + 5n$ is even by [Definition 1.1.1](#).

Quick check. Why does the proof of [Example \(A proof by cases\)](#) need no third case?

Solution. By [Theorem 1.1.2](#) every integer is even or odd, so the two cases already cover every $n \in \mathbb{Z}$.

1.1.5 Without loss of generality

When two cases are mirror images, a proof writes one and says that the other is “the same with the roles exchanged”. *Logic and Proof*, Section 8.2 read the phrase “without loss of generality” as a $\forall E$ whose second box is the first with the letters swapped, and it is licensed only when the statement and the hypotheses are unchanged by the swap (*Logic and Proof*, Example (An induction, and a legitimate symmetry) (b)).

Example. The parity of a sum

Let $m, n \in \mathbb{Z}$.

- (a) If m and n have the same parity (both even or both odd), then $m + n$ is even.
- (b) If they have opposite parity (one even and the other odd), then $m + n$ is odd.

Solution.

- (a) *Case 1: both even.* Then $2 \mid m + n$ by [Example \(Divisors of a combination\)](#) with $a = 2$, $x = y = 1$. *Case 2: both odd,* say $m = 2k + 1$ and $n = 2l + 1$ with $k, l \in \mathbb{Z}$. Then $m + n = 2(k + l + 1)$, with $k + l + 1 \in \mathbb{Z}$. In both cases $m + n$ is even.
- (b) The statement is symmetric in m and n : $m + n = n + m$, and “opposite parity” does not change when the two are exchanged. So, without loss of generality, m is even and n is odd, say $m = 2k$ and $n = 2l + 1$ with $k, l \in \mathbb{Z}$. Then $m + n = 2(k + l) + 1$ is odd. The case m odd and n even is the same with m and n exchanged.

Warning. Check the symmetry first. “Without loss of generality $m \leq n$ ” is legitimate for a claim about $m + n$, and not for a claim about $m - 2n$: exchanging m and n changes that claim. Before writing the phrase, exchange the letters in the statement and in the hypotheses, and check that nothing changes.

1.1.6 Counterexamples and examples

A universal claim, “for every x , if $P(x)$ then $Q(x)$ ”, is refuted by one x with $P(x)$ true and $Q(x)$ false. That is the negation laws at work (*Logic and Proof*, Proposition 6.2.1, *Logic and Proof*, Proposition 6.2.2): $\neg \forall x (P(x) \rightarrow Q(x))$ is equivalent to $\exists x (P(x) \wedge \neg Q(x))$, and an existential is proved by one example ($\exists I$).

Example. A pattern that breaks

Is $2p + 1$ prime for every prime p ?

Solution. For $p = 2, 3, 5$ we get 5, 7, 11, all prime. At $p = 7$ the pattern breaks: 7 is prime, and $2 \cdot 7 + 1 = 15 = 3 \cdot 5$ has the positive divisor $3 \notin \{1, 15\}$, so 15 is not prime ([Definition 1.1.3](#)). The claim is false, and $p = 7$ is a counterexample. The three successes proved nothing, since verifying instances never gives a “for all” ($N1$); one failure settles the question.

Warning. A counterexample must satisfy the hypothesis. The choice $p = 4$ makes $2p + 1 = 9$, which is not prime; but 4 is not prime either, so $p = 4$ says nothing about the claim. A counterexample to “if $P(x)$, then $Q(x)$ ” needs $P(x)$ true **and** $Q(x)$ false, and both are checked on the page.

Example. Two divisors, one product

Prove or disprove: for all integers a, b, c , if $a \mid c$ and $b \mid c$, then $ab \mid c$.

Idea (Scratch work). Try small a and b . For $a = 2$, $b = 3$, the c with $2 \mid c$ and $3 \mid c$ are $0, \pm 6, \pm 12, \dots$, and 6 divides each of them: no counterexample there. The pair $a = 2$, $b = 5$ resists too. What made those work? The two divisors had nothing in common, so c had to contain both separately. Try a and b sharing a factor, as small as possible: $a = b = 2$, and then $c = 2$.

Givens	Goal
(none: we are looking for an example)	integers a, b, c with $a \mid c$, $b \mid c$, $ab \nmid c$
$a = b = 2$, $c = 2$	$2 \mid 2$ (twice), and $4 \nmid 2$
$2 = 1 \cdot 2$	$4 \nmid 2$: no $k \in \mathbb{Z}$ with $2 = 4k$

Solution. False. Take $a = b = c = 2$. Then $2 = 1 \cdot 2$, so $a \mid c$ and $b \mid c$. But $ab = 4$, and $4 \nmid 2$: if $2 = 4k$ with $k \in \mathbb{Z}$, then $k \geq 1$ gives $4k \geq 4$ and $k \leq 0$ gives $4k \leq 0$, so $4k \neq 2$.

The search failed while a and b had no common factor greater than 1, and that is no accident: for coprime a and b the statement is true, a fact *Number Systems*, Chapter 3 proves.

Example. Method: disproof by counterexample, proof by example

Template. To refute “for every x , if $P(x)$ then $Q(x)$ ”: name one x , check $P(x)$, and check that $Q(x)$ fails. To prove “there is an x with $P(x)$ ”: name one x and check $P(x)$.

When to use it. The claim survives a few tries, yet you doubt it; or the statement is existential. Search small and extreme cases first: 0, 1, negative numbers, the smallest sets.

The usual failure. A “counterexample” that does not satisfy the hypothesis; refuting a different claim from the one stated; and the mirror error, concluding “for every” from examples (N1). One example refutes a universal claim, and no number of examples proves one.

An existence claim, proved by one example: there is an integer $n > 1$ with $n \mid 2^n + 1$, namely $n = 3$, since $2^3 + 1 = 9 = 3 \cdot 3$.

Quick check. Is $p = 2$ a counterexample to the claim of [Example \(A pattern that breaks\)](#)? Is $p = 11$?

Solution. No and no. For $p = 2$, $2p + 1 = 5$ is prime; for $p = 11$, $2p + 1 = 23$ is prime. In each case the conclusion holds.

1.1.7 Back to the lattice points

(Q2) is false. Take the four corners of a unit square, $(0, 0)$, $(0, 1)$, $(1, 0)$, $(1, 1)$. Their six midpoints are

$$(0, \tfrac{1}{2}), \quad (\tfrac{1}{2}, 0), \quad (\tfrac{1}{2}, \tfrac{1}{2}), \quad (\tfrac{1}{2}, 1), \quad (\tfrac{1}{2}, 1), \quad (1, \tfrac{1}{2}),$$

and none is a lattice point. A counterexample to a universal claim is also an existence proof by example: there are four lattice points no two of which have a lattice point as midpoint.

The **parity pattern** of a lattice point (a, b) is the pair of words (parity of a , parity of b): even–even, even–odd, odd–even or odd–odd. By [Theorem 1.1.2](#) every integer is even or odd and not both, so every lattice point has exactly one of the four patterns. The four corners above have one pattern each, and that is why they fail.

Example. Same pattern, lattice midpoint

Show that if two lattice points have the same parity pattern, then their midpoint is a lattice point.

Solution. Let (a, b) and (c, d) have the same parity pattern. Then a and c have the same parity, so $a + c$ is even by [Example \(The parity of a sum\)](#) (a): $a + c = 2s$ with $s \in \mathbb{Z}$, and $(a + c)/2 = s \in \mathbb{Z}$. Likewise b and d have the same parity, so $(b + d)/2 \in \mathbb{Z}$. Hence the midpoint is a lattice point.

Quick check. Which pattern does $(-3, 8)$ have? Find a second point with the same pattern, and their midpoint.

Solution. Odd–even: $-3 = 2 \cdot (-2) + 1$ and $8 = 2 \cdot 4$. For example $(1, 0)$, with midpoint $(-1, 4)$.

(Q1), almost. Among five lattice points, each point has one of only four patterns, so two of the points must share a pattern, and then [Example \(Same pattern, lattice midpoint\)](#) finishes. The step “five objects in four boxes put two in one box” is the **pigeonhole principle**. It is stated here, not proved, and so the answer to (Q1) is “yes, once the principle is proved”. The four corners show that five cannot be lowered to four.

Remark (Looking ahead). Section 2.5 proves the pigeonhole principle, from a precise definition of “finite”, and comes back to these five points.

1.1.8 Exercises

1.1.8.1 A. Check your understanding

Exercise. A1

- (a) Write out “ $6 \mid n$ ” and “ n is odd” by their definitions, each as a “there exists”.
- (b) True or false, with reasons: -1 is odd; $7 \mid 0$; $0 \mid 7$; 1 is prime.
- (c) What must a counterexample to “every multiple of 4 is a multiple of 8” satisfy? Give one.
- (d) In the proof of [Theorem 1.1.2](#), name the four case splits and say why each is exhaustive.

Solution.

- (a) $6 \mid n$: there exists $k \in \mathbb{Z}$ with $n = 6k$ ([Definition 1.1.2](#)). n is odd: there exists $k \in \mathbb{Z}$ with $n = 2k + 1$ ([Definition 1.1.1](#)).
- (b) True: $-1 = 2 \cdot (-1) + 1$. True: $0 = 0 \cdot 7$. False: $k \cdot 0 = 0 \neq 7$ for every $k \in \mathbb{Z}$. False: $1 < 2$, so 1 fails the clause $p \geq 2$ of [Definition 1.1.3](#).
- (c) It must be a multiple of 4 that is not a multiple of 8. For example $4 = 1 \cdot 4$; and $4 = 8k$ has no integer solution, since $k \geq 1$ gives $8k \geq 8$ and $k \leq 0$ gives $8k \leq 0$.
- (d) First, even or odd in the induction step: this is the induction hypothesis itself, a disjunction already derived. Second, $n \geq 0$ or $n < 0$: every integer is one or the other, by the order of $\mathbb{Z}$. Third, $-n$ even or $-n$ odd, for $n < 0$: the first half of the proof, applied to $-n \in \mathbb{N}$. Fourth, $c \geq 1$ or $c \leq 0$: no integer lies strictly between 0 and 1.

1.1.8.2 B. Practice

Exercise. B1: Direct proofs

Prove, for all integers a, b, c, d :

- (a) if $a \mid b$, then $a^2 \mid b^2$;
- (b) if $a \mid b$ and $c \mid d$, then $ac \mid bd$.

Solution.

- (a) Let $a \mid b$. By [Definition 1.1.2](#), $b = ka$ with $k \in \mathbb{Z}$. Then $b^2 = k^2 a^2$, and $k^2 \in \mathbb{Z}$, so $a^2 \mid b^2$.
- (b) Let $a \mid b$ and $c \mid d$. By [Definition 1.1.2](#), $b = ka$ and $d = lc$ with $k, l \in \mathbb{Z}$, two different names since nothing says the multipliers agree. Then $bd = (ka)(lc) = (kl)(ac)$, and $kl \in \mathbb{Z}$, so $ac \mid bd$.

Exercise. B2: Two cases

Prove that for every integer n , either $4 \mid n^2$ or $4 \mid n^2 - 1$.

Solution. Let $n \in \mathbb{Z}$. By [Theorem 1.1.2](#), n is even or odd. *Case 1:* $n = 2k$ with $k \in \mathbb{Z}$. Then $n^2 = 4k^2$, so $4 \mid n^2$. *Case 2:* $n = 2k + 1$ with $k \in \mathbb{Z}$. Then $n^2 - 1 = 4k^2 + 4k = 4(k^2 + k)$, with $k^2 + k \in \mathbb{Z}$, so $4 \mid n^2 - 1$. In either case one of the two divisibilities holds.

Exercise. B3: Name the move, then complete it

Here is the frame of a proof that if $m, n \in \mathbb{Z}$ have opposite parity, then $m^2 + n^2$ is odd.

The statement is unchanged when m and n are exchanged, so we may assume

...

$\vdots$

... Hence $m^2 + n^2$ is odd.

Name the move, then complete it.

Solution. The move is *without loss of generality*: the statement and the hypothesis are symmetric in m and n , so we may assume that m is even and n is odd, say $m = 2k$ and $n = 2l + 1$ with $k, l \in \mathbb{Z}$. Then

$$m^2 + n^2 = 4k^2 + 4l^2 + 4l + 1 = 2(2k^2 + 2l^2 + 2l) + 1,$$

with $2k^2 + 2l^2 + 2l \in \mathbb{Z}$. Hence $m^2 + n^2$ is odd. The case m odd and n even is the same with m and n exchanged.

Exercise. B4: Prove or disprove

Prove each true statement and refute each false one with a counterexample.

- (a) For all integers a, b, c : if $a \mid b + c$ and $a \mid b$, then $a \mid c$.
- (b) For all integers a, b, c : if $a \mid b + c$, then $a \mid b$ or $a \mid c$.
- (c) For every integer n , $n^4 + n^2 + 1$ is odd.
- (d) The sum of any three odd integers is even.
- (e) There is an integer $n > 5$ with $n \mid n + 6$.
- (f) For all integers m, n : if mn is even, then m and n are both even.

Solution.

- (a) True. Let $a \mid b + c$ and $a \mid b$: $b + c = ka$ and $b = la$ with $k, l \in \mathbb{Z}$. Then $c = (b + c) - b = (k - l)a$, with $k - l \in \mathbb{Z}$, so $a \mid c$.
- (b) False. Take $a = 2$, $b = c = 1$. Then $b + c = 2 = 1 \cdot 2$, so $a \mid b + c$. But $2 \nmid 1$: $1 = 2 \cdot 0 + 1$ is odd, hence not even ([Theorem 1.1.2](#)), and the same holds for $c = 1$.
- (c) True. By [Theorem 1.1.2](#), n is even or odd. *Case 1:* $n = 2k$. Then $n^4 + n^2 + 1 = 16k^4 + 4k^2 + 1 = 2(8k^4 + 2k^2) + 1$. *Case 2:* $n = 2k + 1$. Then $n^2 = 4k^2 + 4k + 1 = 2j + 1$

with $j := 2k^2 + 2k \in \mathbb{Z}$, so

$$n^4 + n^2 = n^2(n^2 + 1) = (2j + 1)(2j + 2) = 2(2j + 1)(j + 1),$$

and $n^4 + n^2 + 1 = 2(2j + 1)(j + 1) + 1$. In both cases the bracket $(8k^4 + 2k^2, \text{ respectively } (2j + 1)(j + 1))$ is an integer, so $n^4 + n^2 + 1$ is odd by [Definition 1.1.1](#).

- (d) False. Take 1, 1, 1: their sum $3 = 2 \cdot 1 + 1$ is odd, hence not even ([Theorem 1.1.2](#)).
- (e) True. Take $n = 6$: $n + 6 = 12 = 2 \cdot 6$, so $6 \mid 12$.
- (f) False. Take $m = 2$, $n = 1$. Then $mn = 2 = 2 \cdot 1$ is even, but $n = 1 = 2 \cdot 0 + 1$ is odd, hence not even ([Theorem 1.1.2](#)).

1.1.8.3 C. Going deeper

Exercise. C1: Three cases

- (a) By the method of [Theorem 1.1.2](#), show that every integer has the form $3k$, $3k + 1$ or $3k + 2$ for some $k \in \mathbb{Z}$, and that no integer has two of these forms.
- (b) Deduce that for every integer n , n^2 has the form $3k$ (exactly when $3 \mid n$) or the form $3k + 1$.
- (c) Prove that for all integers a, b : if $3 \mid a^2 + b^2$, then $3 \mid a$ and $3 \mid b$.

Solution (Hint 1). For (c), use (b) on a and on b , and look at the cases.

Solution (Hint 2). First line: “Suppose $3 \mid a^2 + b^2$, and suppose $3 \nmid a$.”

Solution.

- (a) *Every natural number has one of the forms*, by induction on n . For $n = 0$, $0 = 3 \cdot 0$. In the step, $n = 3k$ gives $n + 1 = 3k + 1$; $n = 3k + 1$ gives $n + 1 = 3k + 2$; $n = 3k + 2$ gives $n + 1 = 3(k + 1)$. So every $n \in \mathbb{N}$ has one of the forms (Logic and Proof, Axiom 4.2.1). *Every integer*. For $n < 0$, write $-n \in \mathbb{N}$ in one of the forms; then $-3k = 3(-k)$, $-(3k + 1) = 3(-k - 1) + 2$ and $-(3k + 2) = 3(-k - 1) + 1$. *No two forms*. Suppose $3a + r = 3b + s$ with $a, b \in \mathbb{Z}$ and $0 \leq r < s \leq 2$. Then $3(a - b) = s - r \in \{1, 2\}$. With $c := a - b \in \mathbb{Z}$, $c \geq 1$ gives $3c \geq 3$ and $c \leq 0$ gives $3c \leq 0$, so $3c \notin \{1, 2\}$, a contradiction ($\neg$ I).
- (b) By (a), n has one of the three forms. If $n = 3k$, then $n^2 = 3(3k^2)$. If $n = 3k + 1$, then $n^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$. If $n = 3k + 2$, then $n^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$. So n^2 has the form $3k$ in the first case and $3k + 1$ in the other two. Since no integer has two forms, n^2 has the form $3k$ exactly in the first case, that is, exactly when $3 \mid n$.
- (c) Suppose $3 \mid a^2 + b^2$, and suppose $3 \nmid a$. By (b), $a^2 = 3j + 1$ with $j \in \mathbb{Z}$. *Case 1: $3 \mid b$* . Then $b^2 = 3l$ by (b), and $a^2 + b^2 = 3(j + l) + 1$. *Case 2: $3 \nmid b$* . Then $b^2 = 3l + 1$ by (b), and $a^2 + b^2 = 3(j + l) + 2$. In both cases $a^2 + b^2$ has a form other than $3k$; but $3 \mid a^2 + b^2$ says it has the form $3k$, against the “no two forms” half of (a). This contradiction refutes $3 \nmid a$, so $3 \mid a$ (by RAA, or by excluded middle on $3 \mid a$, with the

case $3 \nmid a$ closed by $\perp E$). The statement and the hypothesis are unchanged when a and b are exchanged, so the same argument gives $3 \mid b$.

Marking scheme. (10 points) - 2: (a) existence on $\mathbb{N}$ by induction, with the three step cases. - 1: (a) the negative integers. - 1: (a) uniqueness of the form, by the bound on $3c$. - 1: (b) the three cases computed. - 1: (b) “exactly when” derived from uniqueness, not only from the computation. - 2: (c) the case split complete (cases on b under $3 \nmid a$, or all four cases on a and b), each giving the right form. - 1: (c) the contradiction named as one with the uniqueness in (a). - 1: (c) both conclusions $3 \mid a$ and $3 \mid b$ obtained (by licensed symmetry, or by the full case split). Fatal errors (0 for the step): treating $3 \nmid a$ as “ $a = 3k + 1$ ” only, forgetting $3k + 2$ (N7); concluding $3 \mid a$ from $3 \mid a^2$ without (b).

Exercise. C2: Find the error

Claim: if $n \in \mathbb{Z}$ and n^2 is odd, then n is odd.

“Proof”: Let n be odd, $n = 2k + 1$. Then $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ is odd.

- (a) Is the conclusion true?
- (b) Does the argument prove it? Name the failing line.
- (c) Give a counterexample to the illegal step itself.
- (d) Write a correct proof.

Solution. The conclusion is true: it is one half of Logic and Proof, Theorem 2.4.4.

The argument does not prove it. Its first line assumes the conclusion, “ n is odd”, and its last line reaches the hypothesis, so it proves the converse, “if n is odd, then n^2 is odd”: entry (N5) of Logic and Proof, Example (What is not allowed). The $\rightarrow I$ box must open with “ n^2 is odd”. The step “from $Q \rightarrow P$, conclude $P \rightarrow Q$ ” is illegal, and one instance shows it: “if $n > 0$, then $n^2 > 0$ ” is true, but the converse “if $n^2 > 0$, then $n > 0$ ” is false at $n = -1$.

A correct proof, by cases on n (Theorem 1.1.2). Let $n \in \mathbb{Z}$ with n^2 odd. *Case 1:* $n = 2k$. Then $n^2 = 2(2k^2)$ is even, hence not odd (Theorem 1.1.2), against the hypothesis; so this case cannot occur ($\perp E$). *Case 2:* $n = 2k + 1$. Then n is odd, as claimed. So n is odd.

Marking scheme. (6 points) - 1: (a) the conclusion is true, with the citation. - 2: (b) the error named as proving the converse (N5), pointing at the first line. - 1: (c) a false instance of the pattern “ $Q \rightarrow P$, hence $P \rightarrow Q$ ”. - 2: (d) a correct proof, using Theorem 1.1.2 (cases on the parity of n with the even case shown impossible, or the contrapositive). Fatal errors (0 for the step): calling the conclusion false; “fixing” the proof by assuming n odd again.

Exercise. C3: Lattice points in space

A lattice point of space is a point (a, b, c) with $a, b, c \in \mathbb{Z}$.

- (a) Give eight lattice points of space no two of which have a lattice point as midpoint.
- (b) Show that two lattice points of space with the same three parities have a lattice point as midpoint.

- (c) Which principle, stated in this section and not yet proved, would show that among any nine lattice points of space two have a lattice point as midpoint?

Solution.

- (a) The eight points whose coordinates all lie in $\{0, 1\}$. Two different such points differ in some coordinate, where one has 0 and the other 1; the sum there is 1, and $1/2 \notin \mathbb{Z}$, so the midpoint is not a lattice point.
- (b) As in [Example \(Same pattern, lattice midpoint\)](#), coordinate by coordinate: in each coordinate the two entries have the same parity, so their sum is even by [Example \(The parity of a sum\)](#) (a), and half of it is an integer.
- (c) The pigeonhole principle. Each coordinate is even or odd, so there are $2 \cdot 2 \cdot 2 = 2^3 = 8$ parity patterns; nine points in eight patterns put two points in one pattern, and (b) finishes.